Mathematisches Forschungsinstitut Oberwolfach

Report No. 53/2017

DOI: 10.4171/OWR/2017/53

Mathematical Logic: Proof Theory, Constructive Mathematics

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

5 November – 11 November 2017

Abstract. The workshop "Mathematical Logic: Proof Theory, Constructive Mathematics" was centered around proof-theoretic aspects of core mathematics and theoretical computer science as well as homotopy type theory and logical aspects of computational complexity.

Mathematics Subject Classification (2010): 03Fxx.

Introduction by the Organisers

The workshop *Mathematical Logic: Proof Theory, Constructive Mathematics* was held November 5-11, 2017 and included 5 talks of 50 minutes as well as 26 talks of 40 minutes. The purpose of the workshop was:

To promote the interaction of proof theory and computability theory with core areas of mathematics as well as computer science and philosophical logic via the use of proof interpretations and other proof-theoretic methods.

Concerning interactions of proof theory with core mathematics, A. Sipoş and A. Nicolae talked about applications of proof mining in convex optimization, H. Towsner showed how to obtain bounds on fluctuations from convergence proofs in ergodic theory, A. Weiermann discussed independence results for generalized Goodstein sequences and H. Lombardi and P. Schuster used geometric theories and cut-elimination arguments to obtain effective versions of results in abstract algebra. A finitary version of geometric logic, the so-called coherent logic, was proof-theoretically studied in the talk by U. Buchholtz. K. Yokoyama showed how

a combination of indicator arguments, forcing and proof interpretations can be used to establish feasible conservation results e.g. for Ramsey's theorem for pairs, while A. Freund talked about proof length and the Paris-Harrington principle. S. Sanders gave results on the higher order reverse mathematics of fundamental covering principles in analysis and topology which involve arbitrary (in general uncountable) families. P. Oliva showed how to interpret noneffective theorems in mathematics in terms of higher-order games. The interaction between computability theory and core mathematics was the topic of V. Brattka's talk which calibrated the Weihrauch degree of the Brouwer fixed point theorem depending on additional properties of the function and the dimension of the space in question. Finally, also addressing computability issues in algebra, A. Macintyre discussed residue rings built up from models of Peano arithmetic.

To explore connections between proof theory and computer science. T. Powell showed how to enhance functional interpretations to include imperative features. U. Berger used non-deterministic concurrent programs to interpret proofs using the law-of-excluded-middle, while H. Schwichtenberg extracted proof-theoretically verified programs in exact real number arithmetic using Tsuiki's infinite Gray code representation of reals. S. Hetzl showed how proof theory can facilitate inductive theorem proving and A. Miquel gave a survey on Krivine's classical realizability emphasizing the use of important devices from programming languages made in this method. S. Berardi talked about a new interpretation of polymorphism and M. Baaz showed how (in general) unsound proof rules can be used to speed-up proofs of correct formulas in predicate logic. Other talks addressed proof-theoretic aspects of modal logic (B. Afshari, A. Visser), epistemic logic (S. Artemov) and counterfactual reasoning (S. Negri). P. Aczel outlined an approach towards a core conceptual foundations of mathematics and F. Pakhomov presented refinements of Gödel's second incompleteness theorem.

To further develop proof-theoretic and constructive aspects of homotopy type theory. Three talks were concerned with models, proof-theoretic strength, expressiveness and independence results for type theory with Voevodsky's *univalence axiom*, known as *homotopy type theory*, $HoTT$. T. Coquand reported that the metatheory for the constructive modeling of $HoTT$ via cubical sets can be found in versions of *Constructive Zermelo-Fraenkel Set Theory*. One also gets the independence of the axiom of dependent choices and Brouwer's fan theorem from $HoTT$. N. Gambino talked about constructive obstructions to working with Voevodsky's model of simplicial sets. In joint work with C. Sattler it was recently shown that this problem can be overcome by remaining in the category of simplicial sets, but working with uniform Kan fibrations. S. Awodey's talk addressed the use of impredicative methods for the construction of inductive types in homotopy type theory.

To investigate further the connections between logic and computational complexity: L. Kolodziejczyk talked about separation results for systems of relativized bounded arithmetic, including separating T_2^2 from APC_2. N. Thapen presented new equivalent characterizations of the Cobham recursive set functions in terms of the provable recursive functions of a Kripke-Platek-like feasible set theory, and in terms of infinitary Boolean circuits.

Mathematical Logic: Proof Theory, Constructive Mathematics

Table of Contents

Abstracts

Generalized indicator and forcing

Keita Yokoyama
(joint work with Leszek Kołodziejczyk and Tin Lok Wong)

The indicator argument is a model-theoretic approach to investigate the provably total functions of systems of arithmetic. The original form of the indicator argument is introduced by Kirby and Paris [1] for the study of the strength of infinitary combinatorial principles. Kaye [2] gave a general definition of indicators and developed its frame work in models of first-order arithmetic. Recently, indicator arguments are used to analyze the proof-theoretic strength of Ramsey's theorem for pairs [4, 5].

In the talk, we considered new formulation of indicator arguments with the idea of generic cuts and forcing. Here, the notion of generic cuts was introduced by Kaye [3], and the idea can be combined with a slightly generalized version of indicators. With this method, we see that there are feasible (canonical polynomial) proof interpretations for the following conservation results:

- $\mathrm{B}\Sigma_{n+1}$ is a Π^0_{n+2}-conservative extension of $\mathrm{I}\Sigma_n$ $(n \geq 1)$,
- $\mathsf{WKL}_0 + \mathrm{RT}^2_2$ is a Π^0_3-conservative extension of RCA_0.

Moreover, we discussed when a polynomial proof interpretation is available with the indicator arguments.

References

[1] L. A. S. Kirby and J. B. Paris, Initial segments of models of Peano's axioms, *Set theory and hierarchy theory, V (Proc. Third Conf., Bierutowice, 1976)*, Lecture Notes in Mathematics, Vol. 619, Springer, Berlin, 1977, pp. 211–226.
[2] Richard Kaye, *Models of Peano Arithmetic*, Oxford University Press, 1991.
[3] Richard Kaye, Generic cuts in models of arithmetic, *Math. Log. Quart.* 54, No. 2, 2008, pp. 129–144.
[4] Andrey Bovykin and Andreas Weiermann, The strength of infinitary Ramseyan principles can be accessed by their densities, accepted for publication in Annals of Pure Appllied Logic, available at `http://logic.pdmi.ras.ru/~andrey/research.html`, 2005.
[5] Ludovic Patey and Keita Yokoyama, The proof-theoretic strength of Ramsey's theorem for pairs and two colors, available at `http://arxiv.org/abs/1601.00050`.

Functional interpretations with imperative features

Thomas Powell

Gödel's functional interpretation has played a central role in proof theory ever since its conception back in the 1930s. In particular, numerous adaptations of the interpretation have been developed, ranging from the sophisticated monotone variants essential to the proof mining program [5], to the more abstract categorical formulations which focus on the interpretation's underlying semantics [3, 4].

Typically, terms extracted by the functional interpretation belong to some typed lambda calculus (originally Gödel's system T of primitive recursive functionals in all finite types), and when viewed as *programs* it is natural to envisage these terms being written in a functional language. I report on some current research which aims to instead formulate and understand the functional interpretation using ideas from imperative programming, incorporating notions such as a *global state* into the underlying machinery of the interpretation. There are two main motivating factors for this, which at first glance might seem somewhat orthogonal:

(1) Applications of proof theory in computer science, for instance the synthesis of verified programs, should be oriented towards programming paradigms which are used in practice.
(2) The way in which the functional interpretation gives a computational meaning to classical principles can be elegantly understood and expressed in terms of *actions* such as backtracking and updating.

This way of thinking about proof interpretations is certainly not new. The operational behaviour of extracted programs is studied in [2,6], and more implicitly in [1], to name just a few sources. It has also been a topic of my own research over the last couple of years [7]. However, there is still a great deal of potential in this direction, not just for developing new applications of proof interpretations, but for understanding the mathematical subtleties which underlie them.

I present some work in progress along these lines, which pertains to Gödel's original functional interpretation. Firstly, an extension of the interpretation with a global state which collects information that has been 'learned' through the interpretation of contraction. This leads naturally to a more general question of whether we can construct a uniform monadic interpretation, which extracts not just a program but some additional information about how that program was evaluated. Finally, I discuss how suitable extensions of Hoare logic could be used to verify extracted terms, in a manner which is particularly concise and perspicuous when it comes to complex classical principles such as countable choice.

References

[1] F. Aschieri and S. Berardi. Interactive learning-based realizability for Heyting arithmetic with EM1 *Logical Methods in Computer Science*, 6(3):1-22, 2010.
[2] U. Berger, M. Seisenberger and G. Woods. Extracting imperative programs from proofs: In-place quicksort. In *Proceedings of TYPES 2013*, volume 26 of *LIPIcs*, pages 84-106, 2014.
[3] V. de Paiva. The Dialectica Categories. PhD thesis, University of Cambridge, 1991.

[4] J. M. E. Hyland Proof theory in the abstract. *Annals of Pure and Applied Logic*, 114:43-78, 2002.
[5] U. Kohlenbach. Applied Proof Theory: Proof Interpretations and their Use in Mathematics. Monographs in Mathematic. Springer, 2008.
[6] P-M. Pedrot A Materialist Dialectica PhD thesis, Université Paris Diderot, 2015.
[7] T. Powell Gödel's functional interpretation and the concept of learning. In *Proceedings of Logic in Computer Science (LICS 2016)*, pages 136-145. IEEE Computer Society, 2016.

Proof Length and the Paris-Harrington Principle

Anton Freund

I present a recent result [1], stating that certain combinatorial statements

(1) have short proofs if arbitrary inductions over the natural numbers are allowed, but
(2) only have extremely long proofs if induction is restricted in a certain way.

The combinatorial statements considered are instances of the strengthened finite Ramsey theorem: Writing $[N]^n$ for the n-element subsets of $N = \{0, \dots, N-1\}$, consider the relation

$$\mathrm{PH}(k,n,N) :\equiv \begin{array}{l}\text{“for any function (colouring) } f : [N]^n \to k \text{ there is a set} \\ a \subseteq N \text{ with } n < \mathrm{card}(a) \text{ and } \min a \leq \mathrm{card}(a) \text{ such that the} \\ \text{restriction of } f \text{ to } [a]^n \text{ is constant.”}\end{array}$$

By the famous result of Paris and Harrington [7] the statement $\forall_{k,n}\exists_N\ \mathrm{PH}(k,n,N)$ is true but unprovable in Peano arithmetic (**PA**). At the same time, the instances $\exists_N\ \mathrm{PH}(k,n,N)$ for fixed numbers k and n have trivial proofs in very weak theories: Simply “guess” the correct number N and verify that the finitely many functions $f : [N]^n \to k$ all have the desired property (Σ_1-completeness). However, as the minimal witnesses N for the strengthened finite Ramsey theorem are extremely large, these naive proofs will be very long. Much shorter (and mathematically meaningful) proofs can be given via the infinite Ramsey theorem. In view of these observations I want to ask the following question: What is the minimal theory needed to formalize such short proofs? Recall that $\mathbf{I\Sigma}_n$ is the fragment of **PA** which restricts induction to formulas with n unbounded quantifiers. According to [4, Section II.2(c)] proofs of $\exists_N\ \mathrm{PH}(k,n,N)$ in the fragment $\mathbf{I\Sigma}_{n-1}$ can be constructed by primitive recursion. I show that this is best possible:

Theorem ([1])**.** *There is no primitive recursive construction which maps each number n to a proof of $\exists_N\ \mathrm{PH}(10^{35(n-2)^2}, n, N)$ in the theory $\mathbf{I\Sigma}_{n-2}$.*

In fact, the result established in [1] is considerably stronger: It states that any proof of $\exists_N\ \mathrm{PH}(10^{35(n-2)^2}, n, N)$ in $\mathbf{I\Sigma}_{n-2}$ has code at least $F_{\varepsilon_0}(n-3)$, for sufficiently large n. Here F_{ε_0} is the function at stage ε_0 of the fast-growing hierarchy. It eventually dominates any provably total function of Peano arithmetic, and in particular any primitive recursive function. It is somewhat unsatisfactory that the theorem relies on the large number $10^{35(n-2)^2}$ of colours. This can be avoided if one is prepared to forsake the optimal fragment $\mathbf{I\Sigma}_{n-2}$:

Theorem ([1])**.** *There is no primitive recursive construction which maps each number n to a proof of $\exists_N \mathrm{PH}(8, n, N)$ in the theory $\mathbf{I\Sigma}_{n-3}$.*

It is open whether one can keep the optimal fragment $\mathbf{I\Sigma}_{n-2}$ and make the number of colours constant. One of the main challenges in proving the above theorems is to control the interplay between the lenght of a proof and the amount of induction that it uses. It turns out that this interplay is encapsulated in S.-D. Friedman, Rathjen and Weiermann's [3] notion of slow consistency, which is defined as

$$\mathrm{Con}^*(\mathbf{PA}) :\equiv \forall_x(\exists_y F_{\varepsilon_0}(x) = y \to \mathrm{Con}(\mathbf{I\Sigma}_x)).$$

As F_{ε_0} dominates all provably total functions of Peano arithmetic, the statement $\forall_x \exists_y F_{\varepsilon_0}(x) = y$ is unprovable in **PA**. Indeed, it is shown in [3] that the usual consistency statement $\mathrm{Con}(\mathbf{PA})$ is unprovable in $\mathbf{PA} + \mathrm{Con}^*(\mathbf{PA})$, while $\mathrm{Con}^*(\mathbf{PA})$ is still unprovable in **PA**. The literature now contains several results on the consistency strength (Π_1-consequences) of slow consistency [2, 5, 8]. For the present application the computational content (Π_2-consequences) is crucial: Define a slow proof of φ as a pair $\langle q, M\rangle$ such that

- q is a (usual) proof of φ in the fragment $\mathbf{I\Sigma}_m$, for some m, and
- we have $M = F_{\varepsilon_0}(m)$.

Thus a slow proof may use any amount of induction. However, complicated induction axioms make the slow proof extremely long (because the component M becomes very large). We write $\mathrm{Pr}^*_{\mathbf{PA}}(\varphi)$ to express that φ has a slow proof. It is easy to see that we indeed have

$$\mathrm{Con}^*(\mathbf{PA}) \equiv \neg\, \mathrm{Pr}^*_{\mathbf{PA}}(0 = 1).$$

Given the notion of slow proof, we may now consider the corresponding uniform Π_2-reflection principle, i.e. the collection of statements

$$\forall_x(\mathrm{Pr}^*_{\mathbf{PA}}(\varphi(\dot{x})) \to \varphi(x)),$$

where $\varphi \equiv \varphi(x)$ ranges over Π_2-statements. It is well-known that the usual Π_2-reflection principle over **PA** is equivalent to the statement $\forall_x \exists_y F_{\varepsilon_0}(x) = y$. Similarly, we show in [1] that the Π_2-reflection principle for slow provability is equivalent to the totality of a certain function

$$F^*_{\varepsilon_0} : \mathbb{N} \to \mathbb{N}.$$

The crucial step in the proof of the above theorems is a computational analysis of this function: On the one hand, $F^*_{\varepsilon_0}$ still dominates any provably total function of Peano arithmetic. On the other hand, any provably total function of $\mathbf{PA} + \forall_x \exists_y F^*_{\varepsilon_0}(x) = y$ is dominated by the usual function F_{ε_0} (see [1, Theorem 3.10]). Recall from [6] that the existential witnesses N in the strengthened finite Ramsey theorem are closely related to the values of the function F_{ε_0}. As a result of our computational analysis we learn that any slow proof of the statement $\exists_N \mathrm{PH}(k, n, N)$ (for appropriate values of k) must be very large relative to n. There are two possible explanations for the size of such a slow proof $\langle q, M\rangle$: Either the component M is large, which means that q uses strong induction principles.

Or the proof q itself is very large, as required for the above theorems. We refer to [1] for full details of the argument.

References

[1] A. Freund, *Proof lengths for instances of the Paris-Harrington principle*, Annals of Pure and Applied Logic **168(7)**, 2017, pp. 1361–1382.

[2] A. Freund, *Slow reflection*, Annals of Pure and Applied Logic **168(12)**, 2017, pp. 2103–2128.

[3] S.-D. Friedman, M. Rathjen and A. Weiermann, *Slow consistency*, Annals of Pure and Applied Logic **164(3)**, 2013, pp. 382–393.

[4] P. Hájek and P. Pudlák, *Metamathematics of First-Order Arithmetic*, Perspectives in Mathematical Logic **3**, Springer, 1993.

[5] P. Henk and F. Pakhomov, *Slow and Ordinary Provability for Peano Arithmetic*, arXiv:1602.01822, 2016.

[6] J. Ketonen and R. Solovay, *Rapidly growing Ramsey functions*, Annals of Mathematics **113**, 1981, pp. 267–314.

[7] J. Paris and L. Harrington, *A mathematical incompleteness in Peano Arithmetic*, in: J. Barwise (ed.), Handbook of Mathematical Logic, 1977, pp. 1133–1142.

[8] M. Rathjen, *Long Sequences of Descending Theories and other Miscellanea on Slow Consistency*, Journal of Logics and their Applications **4(4)**, Special Issue Dedicated to the Memory of Grigori Mints, 2017, pp. 1411–1426.

Proof mining and the proximal point algorithm

Andrei Sipoş

(joint work with Laurenţiu Leuştean and Adriana Nicolae)

Proof mining is a research program introduced by U. Kohlenbach in the 1990s ([2] is a comprehensive reference, while [3] is a survey of recent results), which aims to obtain explicit quantitative information (witnesses and bounds) from proofs of an apparently ineffective nature. This offshoot of interpretative proof theory has successfully led so far to obtaining some previously unknown effective bounds, primarily in nonlinear analysis and ergodic theory. A large number of these are guaranteed to exist by a series of logical metatheorems which cover general classes of bounded or unbounded metric structures.

For the first time, this paradigm is applied to the field of convex optimization (for an introduction, see [1]). We focus our efforts on one of its central results, the proximal point algorithm. This algorithm, or more properly said this class of algorithms, consists, roughly, of an iterative procedure that converges (weakly or strongly) to a fixed point of a mapping, a zero of a maximally monotone operator or a minimizer of a convex function. Similarly to other cases previously considered in nonlinear analysis, we may obtain rates of metastability or rates of asymptotic regularity. What is interesting here, however, is that for a relevant subclass of inputs to the algorithm – "uniform" ones, like uniformly convex functions or uniformly monotone operators – we may obtain an effective rate of convergence. The notion of convergence, being represented by a Π_3-sentence, has been usually excluded from the prospect of being quantitatively tractable, unless its proof exhibits a significant isolation of the use of reductio ad absurdum (see

[4,5]). Here, however, a peculiarity of the input, namely its uniformity, translates into a logical form that makes possible this sort of extraction.

References

[1] H. Bauschke, P. Combettes, ***Convex Analysis and Monotone Operator Theory in Hilbert Spaces***, Springer-Verlag, 2010.

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

[3] U. Kohlenbach, *Recent progress in proof mining in nonlinear analysis*, to appear in forthcoming special issue of ***IFCoLog Journal of Logic and its Applications*** with invited articles by recipients of a Gödel Centenary Research Prize Fellowship, 2016.

[4] L. Leuştean, *An application of proof mining to nonlinear iterations*, ***Annals of Pure and Applied Logic***, vol. 165 (2014), pp. 1484–1500.

[5] A. Sipoş, *Effective results on a fixed point algorithm for families of nonlinear mappings*, ***Annals of Pure and Applied Logic***, vol. 168 (2017), pp. 112–128.

Moduli of regularity and rates of convergence for Fejér monotone sequences

Adriana Nicolae

(joint work with Ulrich Kohlenbach and Genaro López-Acedo)

Various problems in applied mathematics can be brought into the following format:

Let (X,d) be a metric space and $F : X \to \overline{\mathbb{R}}$ be a function: find a zero of F,

where as usual $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, \infty\}$. This statement covers many equilibrium, fixed point and minimization problems. Numerical methods, e.g. based on suitable iterative techniques, usually yield sequences (x_n) in X of approximate zeros, i.e. $|F(x_n)| < 1/n$. Based on extra assumptions (e.g. the compactness of X, the Fejér monotonicity of (x_n) and the continuity of F) one then shows that (x_n) converges to an actual zero z of F. An obvious question then concerns the speed of the convergence of (x_n) towards z and whether there is an effective rate of convergence.

In the case of unique zeros, it is in general possible to give an effective rate of convergence due to the existence of a so-called modulus of uniqueness (see [3,4]). Let (X,d) be a metric space, $F : X \to \overline{\mathbb{R}}$ with zer $F = \{z\}$ and $r > 0$.

Definition. *We say that $\phi : (0,\infty) \to (0,\infty)$ is a modulus of uniqueness for F w.r.t.* zer F *and $\overline{B}(z,r)$ if for all $\varepsilon > 0$ and $x \in \overline{B}(z,r)$ we have the following implication*

$$|F(x)| < \phi(\varepsilon) \;\Rightarrow\; d(x,z) < \varepsilon.$$

Suppose now that (x_n) is a sequence of $(1/n)$-approximate zeros contained in $\overline{B}(z,r)$. If ϕ is a modulus of uniqueness for F w.r.t. zer F and $\overline{B}(z,r)$, then

$$\forall k \geq \lceil 1/\phi(\varepsilon) \rceil \, (d(x_k,z) < \varepsilon).$$

In this talk we focused on a generalization of this concept introduced in [5] which is called modulus of regularity and is applicable also in the non-unique case. Let (X, d) be a metric space, $F : X \to \overline{\mathbb{R}}$ with zer $F \neq \emptyset$, $z \in$ zer F and $r > 0$.

Definition. *We say that* $\phi : (0, \infty) \to (0, \infty)$ *is a modulus of regularity for* F *w.r.t.* zer F *and* $\overline{B}(z, r)$ *if for all* $\varepsilon > 0$ *and* $x \in \overline{B}(z, r)$ *we have the following implication*

$$|F(x)| < \phi(\varepsilon) \;\Rightarrow\; \operatorname{dist}(x, \operatorname{zer} F) < \varepsilon,$$

where $\operatorname{dist}(x, \operatorname{zer} F) = \inf\{d(x, z') : z' \in \operatorname{zer} F\}$.

Note that this concept coincides with that of a modulus of uniqueness if zer F is a singleton. Again, whenever (x_n) is a sequence of $(1/n)$-approximate zeros of F in $\overline{B}(z, r)$, x_k is ε-close to some zero $z_k \in$ zer F for all $k \geq \lceil 1/\phi(\varepsilon) \rceil$. A condition which converts this into a rate of convergence is that (x_n) is Fejér monotone w.r.t. zer F, i.e. for all $z' \in$ zer F and $n \in \mathbb{N}$

$$d(x_{n+1}, z') \leq d(x_n, z').$$

In this case we can infer that for all $k, m \geq \lceil 1/\phi(\varepsilon) \rceil$

$$d(x_k, x_m) < 2\varepsilon.$$

So if X is complete and zer F is closed, then (x_k) converges with rate $\lceil 1/\phi(\varepsilon/2) \rceil$ to a zero of F.

The concept of a modulus of regularity is thus a tool to analyze the speed of convergence, including the finite termination, for classes of Fejér monotone sequences which appear in fixed point theory, monotone operator theory, and convex optimization. Moreover, it allows for a unified approach to a number of notions from these fields such as metric subregularity (see [6]), Hölder regularity (see [1]), or weak sharp minima (see [2]), as well as to obtain effective rates of convergence for several algorithms.

References

[1] J. M. Borwein, G. Li, M. K. Tam, *Convergence rate analysis for averaged fixed point iterations in common fixed point problems*, SIAM J. Optim. **27** (2017), 1–33.

[2] J. V. Burke, M. C. Ferris, *Weak sharp minima in mathematical programming*, SIAM J. Control Optim. **31** (1993), 1340–1359.

[3] U. Kohlenbach, *Effective moduli from ineffective uniqueness proofs. An unwinding of de La Vallée Poussin's proof for Chebycheff approximation*, Ann. Pure Appl. Logic **64** (1993), 27–94.

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

[5] U. Kohlenbach, G. López-Acedo, A. Nicolae, *Moduli of regularity and rates of convergence for Fejér monotone sequences*, arXiv:1711.02130 [math.OC], 2017.

[6] A. L. Dontchev, R. T. Rockafellar, *Implicit functions and solution mappings. A view from variational analysis*, Springer Monographs in Mathematics, Springer, Dordrecht, 2009.

Syntactic Forcing Models for Coherent Logic

Ulrik Buchholtz
(joint work with Marc Bezem and Thierry Coquand)

We present three syntactic forcing models for coherent logic, all of which are complete for geometric implications in the language without equality. As an application we give a coherent theory T and a T-redundant sentence (i.e., one which does not yield any new geometric implications when added to T) that is nevertheless false in the generic model of T, answering in the negative a question by Wraith. We also describe the models in terms of classifying toposes of specific extensions of T. These extensions can be seen as axiomatizing in a precise way what the forcing models mean for equality.

The forcing models are given in terms of categories of forcing conditions together with coverages generating Grothendieck topologies. Fix a first-order signature Σ. We then define three categories, all of which on the same collection of objects, namely pairs $(X; A)$ where X is a finite set of variables, and A a finite set of atoms in the language defined by Σ, using only variables from X.

The category $\mathbb{C}_{\mathrm{ts}}$ has morphisms $f : (Y; B) \to (X; A)$, where $f : X \to \mathrm{Tm}(Y)$ is a *term substitution* such that $Af \subseteq B$. Here and below, Af denotes the application of the substitution f to A. The category $\mathbb{C}_{\mathrm{vs}}$ is restricted such that the morphisms $f : (Y; B) \to (X; A)$ are required to be *variable substitutions*. These are simply functions $X \to Y$ thought of as functions $X \to \mathrm{Tm}(Y)$. Finally, the category $\mathbb{C}_{\mathrm{rn}}$ is further restricted such that the morphisms are required to be *renamings*, i.e., injective variable substitutions.

To describe the coverages, recall that a coherent theory T has an axiomatization in which every axiom is of the form

$$\forall \vec{x}.\, \varphi_0 \to \bigvee_{i=1}^{n} \exists z_1, \ldots, z_{m_i}.\varphi_i, \tag{1}$$

where the φ_i are conjunctions of atoms. We define for each such coherent theory T an inductively generated covering relation $\lhd_T$ for the categories $\mathbb{C}_{\mathrm{rn}}$. Since $\mathbb{C}_{\mathrm{rn}}$ is a subcategory of $\mathbb{C}_{\mathrm{ts}}$ and $\mathbb{C}_{\mathrm{vs}}$ containing all isomorphisms, we have then also defined coverages $\lhd_T$ for $\mathbb{C}_{\mathrm{ts}}$ and $\mathbb{C}_{\mathrm{vs}}$. The clauses are:

$$\frac{f \text{ isomorphism with codomain } (X; A)}{(X; A) \lhd_T \{f\}} \qquad \frac{\left\{(X, z_1, \ldots, z_{m_i}; A, \varphi_i) \lhd_T U_i\right\}_{i=1}^{n}}{(X; A) \lhd_T \bigcup_{1 \le i \le n} (e_i U_i)}(*)$$

Here $(*)$ is the set of conditions sanctioning the application of the rule: the existence of an instance $\varphi_0 \to \bigvee_{i=1}^{n} \exists \vec{z}_1, \ldots, z_{m_i}.\varphi_1$ of an axiom in T with all free variables in X and $\varphi_0 \subseteq A$. We tacitly assume that name conflicts are avoided, either by using de Bruijn indices, or by renaming the bound variables z_j so that they are disjoint from X. The morphisms $e_i : (X, z_1, \ldots, z_{m_i}; A, \varphi_i) \to (X; A)$ restrict to identities on X, and $e_i U_i$ denotes the collection of morphisms $e_i f$ with $f \in U_i$. The resulting coverages $\lhd_T$ have nice saturation properties.

In each of the corresponding sheaf toposes, $\mathrm{Sh}(\mathbb{C}_{\mathrm{rn}}, \lhd_T)$, $\mathrm{Sh}(\mathbb{C}_{\mathrm{vs}}, \lhd_T)$, and $\mathrm{Sh}(\mathbb{C}_{\mathrm{ts}}, \lhd_T)$, we find a model of T, and in fact we have the following diagram

of geometric morphisms into the classifying topos of T:

$$\mathrm{Sh}(\mathbb{C}_{\mathrm{rn}}, \lhd_T) \to \mathrm{Sh}(\mathbb{C}_{\mathrm{vs}}, \lhd_T) \to \mathrm{Sh}(\mathbb{C}_{\mathrm{ts}}, \lhd_T) \to \mathbf{Set}[T]$$

Using the Beth-Kripke-Joyal semantics for these models of T, we obtain purely syntactic forcing models that we denote $\Vdash_{\mathrm{rn}}$, $\Vdash_{\mathrm{vs}}$, and $\Vdash_{\mathrm{ts}}$, and these are sound for (infinitary) intuitionistic logic. We prove completeness in the language without equality for the fragment of *generalized geometric implications*, which is generated by the following grammar:

$$\varphi ::= \alpha \mid (\varphi_1 \wedge \varphi_2) \mid \left(\bigvee_{i \in I} \varphi_i\right) \mid (\exists x.\varphi) \mid (\forall x.\varphi) \mid (\alpha \to \varphi)$$

where I ranges over small index sets and α denotes an atomic formula.

Using these forcing models we can answer the following question of Wraith:

> *The problem of characterising all the non-geometric properties of a generic model appears to be difficult. If the generic model of a geometric theory T satisfies a sentence α then any geometric consequence of $T+(\alpha)$ has to be a consequence of T. We might call α T-redundant. Does the generic T-model satisfy all T-redundant sentences?* [3, p. 336]

Indeed, let T be the theory with one axiom $\forall x, z.\, P(x) \to (Q(x,z) \vee R(x,z))$ over the minimal relational signature in which this axiom can be expressed, and consider:

$$\varphi := \exists x, y.\ (P(x) \wedge P(y) \wedge \neg\forall z.\, (Q(x,z) \vee R(y,z))).$$

Then $\Vdash_{\mathrm{vs}} \neg\varphi$, and $\Vdash_{\mathrm{rn}} \neg\neg\varphi$. Then $\alpha := \neg\neg\varphi$ is T-redundant, because if ψ is a geometric consequence of $T + (\alpha)$, then $\Vdash_{\mathrm{rn}} \alpha \to \psi$ by soundness, which implies $\Vdash_{\mathrm{rn}} \psi$, so by completeness, $T \vdash \psi$. However, in this case we see from [2] that the generic T-model is the one in $\mathrm{Sh}(\mathbb{C}_{\mathrm{vs}}, \lhd_T)$, so α is false there.

A slight technical wrinkle is that the completeness theorem stated above concerns the language without equality, but we need T-redundancy for the full language. In order to overcome this difficulty, we deduce for our forcing models a completeness theorem for the (non-generalized) geometric fragment with equality with respect to a theory T^+, which is the same as T in the case of a relational signature. More precisely, let T^+ denote T in the signature expanded with an equality symbol, together with the following (coherent) *constructor axioms* ensuring all function symbols behave like constructors:

(I) distinct function symbols f, g have disjoint values: $f(\vec{x}) = g(\vec{y}) \to \bot$.
(II) function symbols are injective: $f(\vec{x}) = f(\vec{y}) \to \vec{x} = \vec{y}$.
(III) there are no proper cycles: $x = f(\vec{s}) \to \bot$ whenever x occurs anywhere in the sequence of terms $\vec{s}$.

This concludes our treatment of Wraith's question, and all of the above can be done in a predicative, constructive metatheory.

The enhanced completeness theorem and the theory T^+ naturally led us to wonder whether we could describe the toposes $\mathrm{Sh}(\mathbb{C}_x, \lhd_T)$ as classifying toposes for certain theories T_x related to T, where $x = \mathrm{ts}, \mathrm{vs}, \mathrm{rn}$. Using the theory of classifying

toposes for infinitary geometric theories, which on currently existing accounts relies on impredicativity or on the axiom of choice, we get such a description.[1]

In fact, $\mathrm{Sh}(\mathbb{C}_{\mathrm{ts}}, \lhd_T)$ is the classifying topos of the theory $T_{\mathrm{ts}} := T^+$. In the cases $x = \mathrm{vs}, \mathrm{rn}$ with the presence of non-constant function symbols, our theories T_x are *geometric*, i.e., they contain infinite disjunctions. To handle the restriction to variable substitutions in $\mathbb{C}_{\mathrm{vs}}$, let T_{vs} denote the following variation of T_{ts} over the signature expanded with a fresh unary relation symbol V together with the following *variable axioms*:

(IV) for a non-variable term t: $V(t) \to \bot$.

(V) $\forall x. \bigvee_t \exists y_1, \ldots, y_n. x = t \wedge \left(\bigwedge_{i=1}^n V(y_i)\right)$ where the disjunction ranges over all terms t in free variables $y_1, \ldots, y_n$, taking one representative in each α-equivalence class.

The variation for T_{vs} consists in replacing each axiom (1) of T with the axiom,

$$\forall \vec{x}. \varphi_0 \to \bigvee_{i=1}^{n} \exists z_1, \ldots, z_{m_i}. \varphi_i \wedge \left(\bigwedge_{j=1}^{m_i} V(z_j)\right). \tag{2}$$

For a purely relational signature, T_{vs} is a definitional extension of T_{ts} since then (V) reads $\forall x \exists y.\, x = y \wedge V(y)$, which is equivalent to $\forall x. V(x)$.

Finally, to handle the restriction to renamings in $\mathbb{C}_{\mathrm{rn}}$, let T_{rn} denote the following variation of T_{vs} over the signature further expanded with a fresh binary relation symbol $\neq$ together with the following *inequality axioms*:

(VI) $x \neq x \to \bot$, (VII) $x = y \vee x \neq y$.

For T_{rn} we replace each axiom (1) of T with the collection of axioms:

$$\forall \vec{y}. \varphi_0 \to \bigvee_{i=1}^{n} \exists z_1 \cdots z_{m_i}. \varphi_i \wedge \left(\bigwedge_{j=1}^{m_i} V(z_j)\right) \wedge \left(\bigwedge_{j=1}^{m} \bigwedge_{k=1}^{m_i} y_j \neq z_k\right) \wedge \left(\bigwedge_{j<k} z_j \neq z_k\right), \tag{3}$$

where $\vec{y} = y_1, \ldots, y_m$ is any list of variables extending $\vec{x}$.

The upshot is that $\mathrm{Sh}(\mathbb{C}_x, \lhd_T)$ is the classifying topos of T_x, for $x = \mathrm{ts}, \mathrm{vs}, \mathrm{rn}$.

Finally, although we have settled Wraith's question in the negative in the general case, there remains the possibility of a positive answer in the case of algebraic theories. We leave this as an open problem.

References

[1] M. Bezem, U. Buchholtz, and Th. Coquand. Syntactic Forcing Models for Coherent Logic. In: D. van Dalen, J.W. Klop, J. van Mill, G. Jongbloed (Eds.), *L.E.J. Brouwer, 50 years later*. Indagationes Mathematicae special issue, to appear.

[2] M.-F. Coste and M. Coste. Théories cohérentes et topos cohérents. Séminaire de théorie des catégories digigé par Jean Bénabou, Paris, 1975.

[3] G.C. Wraith. Intuitionistic algebra: some recent developments in topos theory. In: O. Lehto (Ed.), *Proceedings of the international congress of mathematicians* (*Helsinki, 1978*), pages 331–337, 1980.

[1] We conjecture that it would be possible to give a predicative, constructive account of these topos-theoretic results using ideas from homotopy type theory.

A Framework for a Core Conceptual Foundations of Mathematics

Peter Aczel

My talk was aimed at giving motivations, and informally describing ideas, for a core *Conceptual Foundations of Mathematics* (In brief a core CFOM). I consider that today the standard idea for a Foundations of Mathematics is a *Formal Foundations of Mathematics* (FFOM); i.e. it is a search for the simplest and most coherent formal systems for the representation of modern pure mathematics and the development of metamathematical results about such formal systems. For example the standard classical FFOM uses the formal system of **ZFC** set theory for its basic mathematical ontology and classical first order logic for its basic logic that gets a formal semantics using the set theory.

During the last 100-150 years of thought on the philosophy of mathematics many conflicting philosophical isms, such as versions of platonism, constructivism, logicism, nominalism, etc., have been considered by a variety of philosophers and mathematicians. In contrast to FFOM, I consider that a Conceptual FOM should be concerned with a presentation of the fundamental concepts and their properties needed to understand the nature of modern mathematics from the perspective of one or more philosophical isms.

My idea for a *core* CFOM is that it should involve a framework of concepts that might be agreed on by several of the mainstream philosophical isms in their discussions with each other, thereby avoiding some of the excessive *talk at cross purposes* that is often a feature of philosophical discussion.

Can there be such a core CFOM? I am not sure. It would require some flexibility on the part of the core concepts and some adaptability on the part of a philosopher willing to adapt their ideas to the core concepts.

My approach to a core CFOM has been heavily influenced by ideas of Per Martin-Löf. In particular I take over his notion of judgement as being fundamental. He has introduced the possibility of having many forms of judgement, particularly in his dependent type theory, and I will follow his lead. It is important to be clear about the distinction between a judgement and a proposition. A proposition may be true, but can be used without intending it to be true. The usual intention in making a judgement is that it be correct, even though the judgement may be mistaken.

I wish to view the fundamental notions of mathematics as belonging to a combination of Logic for mathematics and Ontology for mathematics, both using the notion of judgement. I try to avoid considering issues outside the realm of pure mathematics. So my Ontology will be an ontology of (mathematical) objects. But among the entities that I will need to work with will be things like (mathematical) propositions and (mathematical) types that I do not wish to assume are (mathematical) objects, although they may certainly be *assumed* to be (mathematical) objects, or some of them may be *re-presented* as (mathematical) objects, in some approaches to the philosophy of mathematics. So I drop the word 'mathematical' from 'mathematical object' and just write 'judgement, 'proposition', 'type', etc.

for mathematical entities such as these that I do not wish to assume are objects in my CFOM.

My talk was intended to initiate a project to develop a core CFOM; i.e. a core conceptual foundations for mathematics. I did this by presenting, fairly informally, some of the fundamental concepts that I think may be needed by a variety of philosophical approaches to mathematics. The most fundamental are the notions of *judgement, proposition, true proposition, type and objects of a type.* At the end of my talk I discussed the important distinctions between the collection-like notions of type, class and set. In the modern history of the philosophy of mathematics these notions have often been confused.

Please contact Peter Aczel at petera@cs.man.ac.uk if you would like to receive a pdf copy of the slides of my talk. The following two papers, together with further references in those papers, are relevent to my talk.

References

[1] N. Gambino, P. Aczel, *The Generalised Type-theoretic Interpretation of Constructive Set Theory*, JSL, **71** (2006), 67-103,

[2] P.Martin-Löf. *On the meanings of the logical constants and the justifications of the logical laws.* Written version of lectures given in 1983 in Sienna. Nordic Journal of Philosophical Logic, 1(1):11–60, 1996.

Proof-theoretical methods for counterfactual reasoning

Sara Negri

(joint work with Marianna Girlando and Nicola Olivetti)

The problem of developing a general proof theory for counterfactual reasoning is addressed. Starting from the known failure of the truth-functional or even Kripkean interpretation of counterfactuals, as well as the limitations of the selection function semantics of Stalnaker, we propose a semantics based on neighbourhood models, an extension and formalization of the semantics of sphere models originally proposed by David Lewis in [2].

The Lewis' counterfactual $A \mathrel{\Box\!\!\rightarrow} B$ is neither a material $(A \rightarrow B)$ nor a strict conditional $(\Box(A \rightarrow B))$ but a *variably strict conditionals*, with the following truth condition:

$A \mathrel{\Box\!\!\rightarrow} B$ *true* (at the actual world / at w) iff either:

1 A is impossible or

2 there is a set of possible worlds *similar* to the actual world/to w, that contains a world where A is true and where whenever A is true, B is also true.

Although Lewis based the explanation of the counterfactual on the intuition provided by his sphere semantics, in order to develop a formal analysis he adopted a

reformulation of the semantics based on a primitive notion of *comparative similarity*, in effect a *ternary* accessibility relation, also known as *preferential semantics*, that allows a framing of conditionals closer to standard relational semantics [6].

Our aim is to bridge the gap between the intuition of sphere semantics and the formal level needed to define well-behaved and general proof systems. Sequent calculi are particularly useful to the purpose as they give the most general logical framework for reasoning with counterfactual scenarios, i.e. in the presence of counterfactual hypotheses, nested counterfactuals, etc. This aim is fulfilled through an extension of the formalism of labelled sequent calculi ([3, 5]) now featuring both worlds and neighbourhood labels to internalize *neighbourhood semantics*, a generalization of possible worlds semantics (for its history, extensive coverage, and plenty of examples and applications see [10]).

A neighbourhood frame is a pair $\mathcal{F} \equiv (W, I)$, where W is a set of worlds (states), and I is a neighbourhood function

$$I : W \longrightarrow \mathcal{P}(\mathcal{P}W)$$

that assigns a collection of sets of worlds to each world in W.

The intuition in neighbourhood semantics varies with the target logic; however, for the semantics of conditionals, membership in a neighbourhood of the actual world x corresponds to Lewis' intuition of similarity to x, where an increased degree of similarity correspond to a smaller neighbourhood.

The conditional of $\mathbb{PCL}$ [7] has the following truth condition (here we use for the conditional a notation more compact than the original one)

$x \Vdash A > B$ iff
$\forall \alpha \in I(x)(\alpha \cap [\![A]\!] \neq \emptyset \rightarrow \exists \beta \in I(x)(\beta \subseteq \alpha \ \& \ \beta \cap [\![A]\!] \neq \emptyset \ \& \ \beta \subseteq [\![A \supset B]\!]))$.

A good sequent calculus is then obtained through the following stages (cf. [4]):

(1) Turn the semantic explanation into introduction rules of natural deduction;
(2) Through inversion principles find the corresponding elimination rules and obtain a system of natural deduction with general elimination rules;
(3) Translate the natural deduction system thus obtained into a sequent calculus with independent contexts;
(4) Refine the calculus into a G3-style sequent calculus: rules that are not already invertible are made so; initial sequents have only atomic formulas as principal and have arbitrary contexts; all rules have shared contexts.

With the BHK explanation of logical constants the recipe gives the standard G3 sequent calculi (see ch. 1 of [9]); with relational semantics, basic labelled sequent systems in the style of the calculus **G3K** of [3]. To obtain specific systems a final step is needed:

(5) Add the rules for the accessibility relation following the method of "axioms as rules" [8] and of "geometrization of first-order logic" [1] for arbitrary first-order conditions.

The procedure for neighbourhood semantics requires the addition of new primitives, local forcing relations ($\Vdash^\exists$ and $\Vdash^\forall$) and a forcing for a local conditional ($\Vdash_a A|B$), with the following resulting rules:

$$\frac{x \in a, \Gamma \Rightarrow \Delta, a \Vdash^\exists A, x : A}{x \in a, \Gamma \Rightarrow \Delta, a \Vdash^\exists A} \; R\Vdash^\exists \qquad \frac{x \in a, x : A, \Gamma \Rightarrow \Delta}{a \Vdash^\exists A, \Gamma \Rightarrow \Delta} \; L\Vdash^\exists \; (x \textit{ fresh})$$

$$\frac{x \in a, \Gamma \Rightarrow \Delta, x : A}{\Gamma \Rightarrow \Delta, a \Vdash^\forall A} \; R\Vdash^\forall \; (x \textit{ fresh}) \qquad \frac{x \in a, x : A, a \Vdash^\forall A, \Gamma \Rightarrow \Delta}{x \in a, a \Vdash^\forall A, \Gamma \Rightarrow \Delta} \; L\Vdash^\forall$$

$$\frac{c \in I(x), c \subseteq a, \Gamma \Rightarrow \Delta, x \Vdash_a A|B, c \Vdash^\exists A \quad c \in I(x), c \subseteq a, \Gamma \Rightarrow \Delta, x \Vdash_a A|B, c \Vdash^\forall A \supset B}{c \in I(x), c \subseteq a, \Gamma \Rightarrow \Delta, x \Vdash_a A|B} \; RC$$

$$\frac{c \in I(x), c \subseteq a, c \Vdash^\exists A, c \Vdash^\forall A \supset B, \Gamma \Rightarrow \Delta}{x \Vdash_a A|B, \Gamma \Rightarrow \Delta} \; LC(c \textit{ fresh})$$

$$\frac{a \in I(x), a \Vdash^\exists A, \Gamma \Rightarrow \Delta, x \Vdash_a A|B}{\Gamma \Rightarrow \Delta, x : A > B} \; R> \; (a \textit{ fresh})$$

$$\frac{a \in I(x), x : A > B, \Gamma \Rightarrow \Delta, a \Vdash^\exists A \quad x \Vdash_a A|B, a \in I(x), x : A > B, \Gamma \Rightarrow \Delta}{a \in I(x), x : A > B, \Gamma \Rightarrow \Delta} \; L>$$

Sequent calculi for extensions of the basic systems are obtained by translating into rules the following frame properties:

(N) *Normality*: $\forall x \in W.\exists \alpha \in I(x).\alpha \neq \emptyset$

(T) *Total reflexivity* $\forall x \in W.\exists \alpha \in I(x).x \in \alpha$

(W) *Weak centering*: $\forall x \in W \exists \alpha \in I(x)$ and $\forall x \in W.\forall \alpha \in I(x).\ x \in \alpha$

(C) *(Strong) centering*: $\forall x \in W.\forall \alpha \in I(x)(\{x\} \in I(x) \,\&\, x \in \alpha)$

(U) *Uniformity* : $\forall x, y, z \in W.\forall \alpha \in I(x)(\exists \beta \in I(x).z \in \beta \;\rightarrow\; \exists \gamma \in I(y).z \in \gamma)$

(A) *Absoluteness*: $\forall x, y \in W.I(x) = I(y)$

(Nes) *Nesting*: $\forall \alpha, \beta \in I_i(x)(\alpha \subseteq \beta \;\vee\; \beta \subseteq \alpha)$

Simplifications of the calculus are possible in the presence of nesting and absoluteness and the following results are proved:

- Structural properties established uniformly for all systems: invertibility of all the rules, admissibility of weakening and contraction (height-preserving) and of cut;
- Equivalence of preferential semantics with neighbourhood semantics for $\mathbb{PCL}$;
- Indirect completeness using known completeness results for preferential semantics;
- Tait-Schütte-Takeuti-style completeness result: for any given sequent root-first application of the rules of the calculus gives either a derivation or a countermodel which is automatically in the appropriate class for each extension;

- Through a suitable modification of the left rule for the conditional and a prescribed order of application of rules in proof search (strategy), decidability and the finite model property is established in a constructive way for all systems.

References

[1] R. Dyckhoff and S. Negri, *Geometrization of first-order logic*, ***The Bulletin of Symbolic Logic***, vol. 21 (2015), pp. 123–163.

[2] D. Lewis, *Counterfactuals*, Blackwell (1973).

[3] S. Negri, *Proof analysis in modal logic*, ***Journal of Philosophical Logic*** vol. 34 (2005), pp. 507–544.

[4] S. Negri, *Non-normal modal logics: a challenge to proof theory*, ***The Logica Yearbook 2016*** (P. Arazim and T. Lavička, editors), College Publications (2017), pp. 125–140.

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

[6] S. Negri and G. Sbardolini, *Proof analysis for Lewis counterfactuals*, ***The Review of Symbolic Logic***, vol. 9 (2016), no. 1, pp. 44–75.

[7] S. Negri and N. Olivetti, *A sequent calculus for preferential conditional logic based on neighbourhood semantics*, ***Automated Reasoning with Analytic Tableaux and Related Methods*** (H. De Nivelle, editor), Lecture Notes in Computer Science, vol. 9323, Springer (2015), pp. 115–134.

[8] S. Negri and J. von Plato, *Cut elimination in the presence of axioms*, ***Bulletin of Symbolic Logic***, vol. 4 (1998), pp. 418–435.

[9] S. Negri and J. von Plato, *Structural Proof Theory* (2001), Cambridge University Press.

[10] E. Pacuit, *Neighborhood Semantics for Modal Logic* (2017), Springer

An unprovability result for Jeřábek's theory of approximate counting

Leszek Kołodziejczyk

(joint work with Neil Thapen)

Relativized bounded arithmetic is a family of arithmetic theories formulated in a language that extends the traditional language of ordered rings $+, \cdot, 0, 1, \leq$ by the symbols $\lfloor x/2^y \rfloor, |x|, x\#y$, and α. Here $|x|$ stands roughly for the integer part of $\log_2 x$, while $x\#y$ stands for $2^{|x|\cdot|y|}$. The symbol α is an additional unary predicate intended to represent an arbitrary oracle (which may be used to code a larger number of oracle predicates and/or predicates of higher arities).

The most important theories of relativized bounded arithmetic are obtained by restricting the induction scheme to certain classes of bounded formulas. Let the class $\Sigma^b_n(\alpha)$ consist of formulas with at most n alternating blocks of bounded quantifiers (beginning with an existential block), followed by a matrix that contains only quantifiers bounded by terms of the form $|t|$ (so-called sharply bounded quantifiers). The theory $T^n_2(\alpha)$ is axiomatized by a finite list of purely universal axioms fixing the meaning of the non-logical symbols (except α) and the induction scheme for $\Sigma^b_n(\alpha)$ formulas. Theories of this sort are studied largely because of their connections to computational complexity and the complexity of proofs in propositional logic. For instance, the theory $T^1_2(\alpha)$ is very closely connected to polytime computations with access to an oracle which is in NP relative to α: on

the one hand, $T^1_2(\alpha)$ proves that each $\mathrm{P}^{\mathrm{NP}(\alpha)}$ computation terminates, and on the other hand, whenever a $\forall\Sigma^b_2(\alpha)$ sentence is provable in $T^1_2(\alpha)$, the first block of existential quantifiers can be witnessed by a function computable in $\mathrm{P}^{\mathrm{NP}(\alpha)}$.

It has been known since the early 1990's that for each n, $T^{n+1}_2(\alpha)$ is strictly stronger than $T^n_2(\alpha)$. However, the quantifier complexity of the separating sentences grows with n. The question whether $T^{n+1}_2(\alpha)$ can be separated from $T^n_2(\alpha)$ by a $\forall\Sigma^b_k(\alpha)$ sentence for some fixed k is a major open problem. A particularly difficult subcase of the problem is whether there is a $\forall\Sigma^b_1(\alpha)$ sentence provable in some $T^n_2(\alpha)$ but not in $T^2_2(\alpha)$.

On the other hand, techniques for separating $T^1_2(\alpha)$ from somewhat stronger theories by means of $\forall\Sigma^b_1(\alpha)$ sentences are well-known. One such technique relies on a propositional translation into *narrow resolution*. The idea is that for a $\Sigma^b_1(\alpha)$ formula $\sigma(x)$ and a given natural number m, the statement $\neg\sigma(m)$ can be translated into a propositional CNF with clauses of size polylog(m). If $T^1_2(\alpha)$ proves $\forall x\,\sigma(x)$, then for each m such a CNF can be refuted in resolution using only polylog-size clauses. Intuitively, if somebody claims to have an oracle satisfying $\neg\sigma(m)$, one can force him into a contradiction by querying bits of the oracle α but only keeping track of polylog(m) of them at any given time. This is usually impossible, which leads to the unprovability in $T^1_2(\alpha)$ of such statements as:

- the injective weak pigeonhole principle iWPHP: if f is a map from x^2 into x for $x \geq 2$, then there are distinct $w_1, w_2 < x^2$ such that $f(w_1) = f(w_2)$,
- the Herbrandized ordering principle HOP: if $\preceq$ is a linear order on x, and h maps x into x, then for some $w < x$ we have $w \preceq h(w)$,
- the Ramsey principle RAM: if R is a 2-colouring of $[x]^2$, then there exists a homogeneous subset w of x of size $\frac{\log x}{2}$.

Here in each case a number x is identified with $\{0, \ldots, x-1\}$, and the objects $f, \preceq, h, R$ are encoded by the oracle α. All of the above statements are known to be provable in either $T^2_2(\alpha)$ or at most $T^3_2(\alpha)$.

Around 2010, it was noted that the difficulty of proving unprovability of low-complexity statements in $T^n_2(\alpha)$ for higher n might be due to the fact that most of these theories can formalize some counting arguments. Particular attention was focused on a theory extending $T^1_2(\alpha)$ by the *surjective* weak pigeonhole principle for $\mathrm{P}^{\mathrm{NP}(\alpha)}$ functions, sWPHP$(\mathrm{P}^{\mathrm{NP}(\alpha)})$: "no $\mathrm{P}^{\mathrm{NP}(\alpha)}$ function is a surjection from x onto x^2". This theory, later called $\mathrm{APC}_2(\alpha)$, is contained in $T^3_2(\alpha)$ and possibly incomparable with $T^2_2(\alpha)$. It was introduced by Jeřábek, who showed in [Jeř09] that it can define a well-behaved notion of "approximate cardinality" of a bounded $\Sigma^b_1(\alpha)$-definable set. Jeřábek also showed that $\mathrm{APC}_2(\alpha)$ can use this ability to prove each of the statements iWPHP, HOP, and RAM described above. This led to the natural question: is there a $\forall\Sigma^b_1(\alpha)$ sentence provable in some $T^n_2(\alpha)$ but not in $\mathrm{APC}_2(\alpha)$? The talk surveyed the history of results related to this question.

The first results, obtained by Buss et al. in [BKT14], concerned fragments of $\mathrm{APC}_2(\alpha)$ obtained by restricting either the induction scheme or the weak pigeonhole principle. Buss et al. showed that the principle HOP is unprovable in $T^1_2(\alpha) + \mathrm{iWPHP}(\mathrm{P}(\alpha))$ and in $T^0_2(\alpha) + \mathrm{sWPHP}(\mathrm{P}^{\mathrm{NP}(\alpha)})$. They also showed that

proofs of $\forall\Sigma^b_1(\alpha)$ sentences in $T^1_2(\alpha) + \mathrm{sWPHP}(\mathrm{P}(\alpha))$ translate into a randomized version of narrow resolution. Despite this, [BKT14] did not prove any unprovability result for $T^1_2(\alpha) + \mathrm{sWPHP}(\mathrm{P}(\alpha))$, not to mention the full theory $\mathrm{APC}_2(\alpha)$.

The case of $T^1_2(\alpha) + \mathrm{sWPHP}(\mathrm{P}(\alpha))$ was settled slightly later by Atserias and Thapen [AT14]: that theory is also unable to prove HOP. Interestingly, the unprovability proof did not use the translation into randomized narrow resolution, but took advantage of some specific features of sWPHP for polytime computations. Very roughly, it turned out that for sufficiently large x, it is possible to fix a part of the oracle ordering $\preceq$ and associated Herbrand function h so that on each input $u < x$ a given polytime function $f\colon x \to x^2$ is restricted to take one of at most two specific values. Since $x^2 \gg 2x$, this means that some $v < x^2$ is guaranteed to be outside the range of f, thus revealing a witness to sWPHP. On the other hand, the undetermined part of the oracle is large enough that typical methods for showing unprovability of HOP in $T^1_2(\alpha)$ can still be applied.

This is where things stood for a number of years. It was unclear whether the methods of [AT14] could be adapted to obtain a lower bound on refutation size in randomized narrow resolution. It was clear, though, that all methods used up to that point were demonstrably inadequate for the problem of finding a $\forall\Sigma^b_1(\alpha)$ sentence unprovable in $\mathrm{APC}_2(\alpha)$. One reason for this was that those methods always yielded the unprovability of HOP, which *is* provable in $\mathrm{APC}_2(\alpha)$.

Further progress came in the last year or so. Pudlák and Thapen [PT17] considered the $\forall\Sigma^b_1(\alpha)$ principle CPLS ("coloured polynomial local search"), which says the following. If R is a ternary relation on x (intuitively, $R(z, y, t)$ means that element z has colour y at time t), it cannot happen that:

- for each $z < x$, $R(z, f_0(z), 0)$,
- for each $y < x$, $\neg R(0, y, x - 1)$,
- for each $t < x - 1$ and $z, y < x$, if $R(f_{t+1}(z), y, t)$, then $R(z, y, t + 1)$.

(The relation R and the Herbrand functions h, f_t are encoded by the oracle.) CPLS is a particular herbrandization of the induction axiom for $\Sigma^b_2(\alpha)$ formulas, and as such is quite easy to prove in $T^1_2(\alpha)$. Pudlák and Thapen showed that propositional translations of $\neg$CPLS cannot be refuted in randomized narrow resolution. Furthermore, they developed a technical tool known as a "fixing lemma": essentially, there is a probability distribution on partial restrictions ρ of the CPLS oracle $\langle R, \{f_t\}_{t<x}\rangle$ such that for any $\mathrm{NP}(R, \{f_t\}_{t<x})$ query "φ?", w.h.p. ρ either forces φ or forces $\neg\varphi$ (in a finitary version of the usual technical notion of forcing), but also w.h.p., ρ leaves enough of the oracle intact that arguments against narrow resolution can be applied.

Recently, Thapen and the speaker [KT17] were able to exploit the fixing lemma and finally give a solution to the problem concerning $\mathrm{APC}_2(\alpha)$: namely, $\mathrm{APC}_2(\alpha)$ does not prove CPLS, and is thus separated from $T^2_2(\alpha)$ by a $\forall\Sigma^b_1(\alpha)$ sentence. The proof is based on some logical witnessing arguments connecting surjective and injective pigenhole principles and on the following idea: given $f\colon x^2 \to x$ which is now a $\mathrm{P}^{\mathrm{NP}(\alpha)}$ function, the fixing lemma can be used to obtain some ρ that determines the value $f(v)$ for most arguments $v < x^2$, in particular for more than

x arguments. Showing this required the observation that in many cases, the fixing lemma can be extended to work with conditional probabilities.

Some questions remain. Most immediate among them is probably the question whether propositional translations of HOP are provable in randomized narrow resolution. More long-term problems concern the power of fixing lemmas: for instance, can they be used to obtain an unprovability result for $T^2_2(\alpha)$?

References

[AT14] A. Atserias and N. Thapen. The ordering principle in a fragment of approximate counting. *ACM Trans. Comput. Log.*, 15(4):Art. 29, 11, 2014.

[BKT14] S. R. Buss, L. A. Kołodziejczyk, and N. Thapen. Fragments of approximate counting. *J. Symb. Log.*, 79(2):496–525, 2014.

[Jeř09] E. Jeřábek. Approximate counting by hashing in bounded arithmetic. *J. Symb. Log.*, 74(3):829–860, 2009.

[KT17] L. A. Kołodziejczyk, N. Thapen. Approximate counting does not prove CPLS. Preprint, 2017. Available upon request.

[PT17] P. Pudlák and N. Thapen. Random Resolution Refutations. In *32nd Computational Complexity Conference (CCC 2017)*, pages 1:1–1:10. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2017.

Cut elimination for modal mu-calculus

Bahareh Afshari

(joint work with Graham E. Leigh)

Modal μ-calculus is an important extension of propositional modal logic which captures the essence of inductive and co-inductive reasoning. The first proof system for the modal μ-calculus was a Hilbert-style axiomatisation proposed in 1983 by Kozen [6] which expanded the standard axioms of the modal system K by fixed point and induction rules for the the least (μ) and greatest (ν) fixed point quantifiers:

$$\begin{array}{lllll} \mu\text{-rules:} & A(\mu x A(x)) \to \mu x A(x) & \& & A(B) \to B \vdash \mu x A(x) \to B \\ \nu\text{-rules:} & \nu x A(x) \to A(\nu x A(x)) & \& & B \to A(B) \vdash B \to \nu x A(x) \end{array}$$

Completeness for Kozen's system was established in 2000 by Walukiewicz [8]. The proof, imitated for the natural sequent formulation of the system, makes essential use of the cut rule and it remains a significant open problem whether Kozen's system without cut is still complete. To date, cut elimination algorithms have only been established for very weak fragments, such as the one-variable fragment [7] and the system of common knowledge [4], and both these arguments rely on intricate techniques from impredicative proof theory.

Putting cut elimination aside, until recently, the only complete cut-free proof system for the modal μ-calculus is the semi-formal (i.e. infinitary) system introduced in [5]. This year, two new complete finitary cut-free sequent calculi for μ-calculus were proposed in [1]. The first of these systems is a natural variant of

Kozen's original axiomatisation wherein cut is dropped and the induction rule is strengthened in the following form

$$\frac{\Gamma, A(\bar{\Gamma})}{\Gamma, \nu x A(x)}\,\mathsf{induction} \qquad \rightsquigarrow \qquad \frac{\Gamma, \nu x A(\bar{\Gamma} \vee x)}{\Gamma, \nu x A(x)}\,\mathsf{strong\ induction}$$

where $\bar{\Gamma}$ is the negation of $\bigvee \Gamma$ written in negation normal form. The new inference rule can be seen as combining the usual induction rule with two general fixed-point principles:

$$\nu x \nu y A(x, y) \leftrightarrow \nu x A(x, x) \qquad\qquad \nu x A(x \vee x) \leftrightarrow \nu x A(x)$$

the first of which is an instance of Arnold and Niwinski's "golden lemma of μ-calculus" [3].

The second finitary proof system introduced in [1], discards the induction rule in favour of a generalisation of the ν-regeneration rule. The new inference has the form

$$\frac{\begin{array}{c}\big[\Gamma, \nu x A\big] \\ \vdots \\ \Gamma, A(\nu x A)\end{array}}{\Gamma, \nu x A}$$

where the sequent within the brackets is understood as an assumption of the proof which is discharged. Applications of the rule are subject to the condition that there is a thread from the formula $A(\nu x A)$ in the premise to the formula $\nu x A$ in the discharged sequent that does not regenerate fixed point variables subsuming x. This restriction is formalised by annotating formulæ: each formula in the proof is labelled by a word from a finite set of *names* in such a way as to record the regenerations of formulæ induced by the μ and ν inferences; the condition on applications of the inference above is then represented by the local requirement that the premise and discharged assumptions of the rule have identical annotations.

The proofs of completeness for the two proof systems above are constructive and rely on finitary methods only, hence they lay the groundwork for a fresh investigation of syntactic cut elimination. Completeness for the system with strong induction reduces the open problem of whether Kozen's axiomatisation without cut is complete to whether the strong induction rule is admissible in Kozen's system without cut. This is in turn equivalent to the admissibility of the inference

$$\frac{\Gamma, \sigma y \sigma x A(y \vee x)}{\Gamma, \sigma x A(x)}\,\sigma \in \{\mu, \nu\}$$

which permits contracting quantifiers of the same kind in simple contexts. The annotated proof system, on the other hand, is inter-translatable with the infinatry system of [5], and it may prove more viable for the study of effective cut elimination due to its analytic form.

References

[1] B. Afshari and G.E. Leigh, *Cut-free completeness for modal mu-calculus*. In: Proceedings of Thirty-Second Annual ACM/IEEE Symposium on Logic in Computer Science, LNCS. Springer (2017), 1–12.

[2] B. Afshari and G.E. Leigh, *Finitary proof systems for Kozen's μ*, In: Oberwolfach Preprints. OWP 2016-26.

[3] A. Arnold and D. Niwinski, *Rudiments of μ-calculus*, ser. Studies in Logic. North Holland **146** (2001).

[4] K. Brünnler and T. Studer. *Syntactic cut-elimination for common knowledge*, Annals of Pure and Applied Logic **160.1** (2009), 82–95.

[5] G. Jäger, M. Kretz and T. Studer, *Canonical completeness of infinitary μ*, Journal of Logic and Algebraic Programming **76.2** (2008), 270–292.

[6] D. Kozen, *Results on the propositional μ-calculus*, Theoretical Computer Science **27** (1983), 333–354.

[7] G. Mints and T. Studer, *Cut-elimination for the mu-calculus with one variable*, In: Fixed points in Computer Science (FICS) (2012), 47–54.

[8] I. Walukiewicz, *Completeness of Kozen's axiomatisation of the propositional μ-calculus*, Information and Computation **157** (2000), 142–182.

The Uniform Computational Content of the Brouwer Fixed Point Theorem Revisited

Vasco Brattka

(joint work with Stéphane Le Roux, Joseph S. Miller and Arno Pauly)

We present some recent results on the classification of the computational content of the Brouwer Fixed Point Theorem in the Weihrauch lattice [1]. For one we show that the two-dimensional version of the Brouwer Fixed Point Theorem is strongly Weihrauch equivalent to Weak Kőnig's Lemma [2]. In contrast to the three and higher dimensional cases for which there is a simple geometric (algebraic) proof of this fact, the only known proof for the two dimensional case requires a comparably involved inverse limit construction. This construction also shows that connected choice is strongly Weihrauch equivalent to Weak Kőnig's Lemma from dimension two onwards. An open problem that remains is whether this is also true for pathwise connected choice in dimension two (the geometric proof yields this for dimension three and higher). A second line of results that we present is related to the Brouwer Fixed Point Theorem for Lipschitz continuous functions [2]. We show that any Lipschitz constant larger than one does not reduce the Weihrauch complexity of the Brouwer Fixed Point Theorem if it is restricted to functions that obey the respective Lipschitz constant. The case of Lipschitz constant exactly one is a special case of the Brouwder-Göhde-Kirk Fixed Point Theorem that was studied by Eike Neumann, who proved that this theorem is equivalent to convex choice of the respective dimension [3]. In this case the complexity strictly increases with the dimension, which follows from results of Stéphane Le Roux and Arno Pauly [4].

References

[1] V. Brattka, G. Gherardi, A. Pauly, *Weihrauch Complexity in Computable Analysis*, arXiv **1707.03202** (2017), 49 pages. https://arxiv.org/abs/1707.03202

[2] V. Brattka, S. Le Roux, J.S. Miller, A. Pauly, *Connected Choice and the Brouwer Fixed Point Theorem*, arXiv **1206.4809** (2016), 36 pages. https://arxiv.org/abs/1206.4809

[3] E. Neumann, *Computational Problems in Metric Fixed Point Theory and their Weihrauch Degrees*, Logical Methods in Computer Science **11** (2015) 4:20,44

[4] S. Le Roux, A. Pauly, *Finite choice, convex choice and finding roots*, Logical Methods in Computer Science **11:4** (2015) 4:6, 31

Ineffective Theorems and Higher-order Games

Paulo Oliva

(joint work with Martín Escardó and Thomas Powell)

In any game where a player needs to choose a move from a set X having in mind an outcome (or result) in a set R, we can think of maps from moves to outcomes $p\colon X \to R$ as *game continuations*. These can also be viewed as "oracles", determining for each choice of move what the final outcome would be.

For instance, in the game of naughts-and-crosses the starting player has nine options $X = \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)\}$ and the possible results of the game are $R = \{\text{win}, \text{lose}, \text{draw}\}$. The game continuations in this case are all maps from X to R, determining for each possible move what the outcome of the game would be. A player does not have access to the actual game continuation, unless both players have fixed their strategies. But the key insight here is that we can *describe the goal* of the player as a function on game continuations.

In the example above, a player who is hoping to win the game, and has a draw as the second-best option, would rank the result set as win $>$ lose $>$ draw. For any given game continuation $p\colon X \to R$, the player's best moves would be those which maximise the game outcome. That is precisely the argmax function

$$\text{argmax}\colon (X \to R) \to \mathcal{P}(X)$$

where $\mathcal{P}(X)$ denotes the power-set of X. Any move which leads to the player winning the game is equally good. And if no such move exists for that particular game continuation, then any move that leads to a draw is equally good, and so on. We will model player's goals as such higher-order functions, which we have been calling *selection functions*. They determine for each game continuation the player's best moves.

In general, in a sequential game with n rounds, the set of alternatives at round i will be some set X_i, and the game continuation at this round are maps $X_i \to R$. We describe the goal of the player at round i as a selection function

$$\varepsilon_i\colon (X_i \to R) \to \mathcal{P}(X_i)$$

A sequence of moves $x_1, \ldots, x_n \in \Pi_{i=1}^n X_i$ is called a *play*, and the function that maps plays to outcomes is called an outcome function $q\colon \Pi_{i=1}^n X_i \to R$. The selection functions together with an outcome function define a *higher-order game*.

Note that such games generalise extensive form games as studied in classical Game Theory, where $R = \mathbb{R}^n$ is a tuple of payoffs, and $q\colon \Pi_{i=1}^n X_i \to \mathbb{R}^n$ are the payoff functions. In this case it is assumed that all players are trying to maximise their own payoff, so the selection function are indeed argmax.

A *strategy profile* in a higher-order game (as in a classical game), is a family of maps $\eta_i\colon \Pi_{j=1}^{i-1} X_j \to X_i$, $i \in \{1, \ldots, n\}$, producing the next move given all the previous moves. We will denote by $\eta^*\colon \Pi_{i=1}^n X_i$ the play that one obtains by following the strategy η, i.e.

$$\eta_1^* = \eta_1 \qquad \eta_{i+1}^* = \eta_{i+1}(\eta_1^*, \ldots, \eta_i^*)$$

We will say that a strategy profile is *optimal* if, for each i,

$$\eta_i^* \in \varepsilon_i(p_i)$$

where $p_i(x_i) = q(\eta_1^*, \ldots, x_i, \eta_{i+1}(\eta_1^*, \ldots, x_i), \ldots)$ is the game continuation obtained by consideration the different outcomes when player i deviates from his/her strategy and plays x_i instaead of η_i^*. We have shown (see [2–4, 6]) that

- The type construction $J_R X = (X \to R) \to X$ of single-valued selection functions has the structure of a strong monad, and as such admits a product-like operation $J_R X \times J_R Y \to J_R(X \times Y)$.
- This product when iterated calculates optimal strategies in higher-order games, and can be seen as a generalisation of the *backward induction* algorithm from game theory.
- Various forms of bar recursion can be understood as different unbounded products of selection functions.
- Combining the selection monad with the powerset monad one can give a Herbrand functional interpretation for the double negation shift.

In this talk I have focused on applying these higher-order games in order to give a game-theoretic interpretation to the functional interpretation of various non-constructive theorem. This can be seen as a meta-interpretation. For instance, consider the drinkers paradox

$$\exists x^X (P(x) \to \forall y^Y P(x))$$

This is a theorem of classical logic assuming the type X is inhabited, i.e. $a \in X$ for some a. Although it is not straightforward to check the validity of this statement, it is very clear what it say: there exists a person x such that, if that person is drinking $P(x)$ then everybody is drinking $\forall y P(y)$. Its dialectica interpretation, however, becomes

$$\exists \varepsilon^{(X\to X)\to X} \forall p^{X\to X} (P(\varepsilon p) \to P(p(\varepsilon p)))$$

which is a higher-order statement that at first sight does not have much meaning. But once we understand that $(X \to X) \to X$ are single-valued selection function, and as such implement a player's goal, we can see what the higher-order statement

above is saying: *there exists a player* $\varepsilon\colon (X \to X) \to X$ *such that for any game continuation* $p\colon X \to X$*, if the move of the player satisfies* P *then the outcome of the game also satisfies* P.

In the talk I have used this example considering a particular instance where X is the set of possible inflation rates, and P determines whether an inflation rate is within target. *We can think of the desired player* $\varepsilon\colon (X \to X) \to X$ *as a central bank which is required to predict next year's interest rate in such a way that if its prediction is within target then the actual inflation will also be within target.* In this way a possible strategy for the central bank is this:

$$\varepsilon(p) = \begin{cases} 0 & P(p(0)) \\ p(0) & \neg P(p(0)) \end{cases}$$

One can check that indeed if $P(\varepsilon p)$ then $P(p(\varepsilon p))$, i.e. if by predicting zero inflation we will have an actual rate of inflation $p(0)$ which is within target, then 0 is a good prediction. If on the other hand $p(0)$ is not within target we can safely use that $p(0)$ as a prediction.

I have also briefly discussed two more examples of such game-theoretic (meta) interpretation, namely the infinite pigeon-hole principle and the (classical) axiom of countable choice. The infinite pigeon-hole principle says that if we colour the natural numbers with n colours, then one of the colours $i < n$ will be used infinitely often:

$$\forall n \forall c^{\mathbb{N}\to n} \exists i < n \forall k \exists j (j \geq k \wedge c(j) = i)$$

The functional interpretation of this statement is

$$\forall n \forall c^{\mathbb{N}\to n} \forall \varepsilon_{(\cdot)} \exists p^{\mathbb{N}\to\mathbb{N}} \exists i < n (p(\varepsilon_i p) \geq \varepsilon_i p \wedge c(p(\varepsilon_i p)) = i)$$

As we did with the drinker's paradox, we can view $\varepsilon_{(\cdot)}$ as a sequence of players, and read this higher-order statement as a theorem on higher-order games: *Given* n *players* $(\varepsilon_i)_{i<n}$ *and a mapping from natural numbers to these* n *players, there exists a game continuation* $p\colon \mathbb{N} \to \mathbb{N}$ *such that the player* i *associated with the outcome of the game has played a move* $x_i = \varepsilon_i p$ *which is higher than the game outcome* $r = p(\varepsilon_i p)$. Moreover, we can easily construct such game continuation using the product of selection functions mentioned above.

Other application of this game theoretic approach to non-constructive proofs in analysis can be found in [1, 7, 8].

References

[1] S. Berardi, P. Oliva, and S. Steila. A analysis of the Podelski-Rybalchenko termination theorem via bar recursion. *Journal of Logic and Computation*, 2015.

[2] M. H. Escardó and P. Oliva. Selection functions, bar recursion, and backward induction. *Mathematical Structures in Computer Science*, 20(2):127–168, 2010.

[3] M. H. Escardó and P. Oliva. Computational interpretations of analysis via products of selection functions. Submitted for publication, 2011.

[4] M. H. Escardó and P. Oliva. The Herbrand functional interpretation of the double negation shift. *The Journal of Symbolic Logic*, to appear.

[5] M. H. Escardó, P. Oliva, and T. Powell. System T and the product of selection functions. *Proceedings of CSL'11*, 2011.

[6] Martín H. Escardó and Paulo Oliva. Sequential games and optimal strategies. *Royal Society Proceedings A*, 467:1519–1545, 2011.
[7] P. Oliva and T. Powell. A constructive interpretation of Ramsey's theorem via the product of selection functions. to appear: Mathematical Structures in Computer Science, 2013.
[8] P. Oliva and T. Powell. A game-theoretic computational interpretation of proofs in classical analysis *Gentzen's Centenary: The Quest for Consistency*, , 501-531, Springer, 2015.

Proofs and Justifications in Epistemic Logic

Sergei Artemov

We discuss three major flaws of modal epistemic logic and outline well-principled ways of resolving them.

1. The dominant Kripke semantics contains a hidden assumption of common knowledge of the model manifested in condition "if a sentence is valid at all possible states then it is known? which significantly narrows the scope of epistemic logic. We define a general class of epistemic models which are free of this constraint and contains Kripke models as its special case, cf. [2].

2. A common malpractice in epistemic logic and applications is the semantic formalization standard, which covers only complete theories and ignores the rest. Imagine a mathematical logic in which only complete theories defined by a model are considered; this would leave out such theories as Peano Arithmetic, Analysis, all versions of Set Theory, etc. We offer a new standard: the syntactic formalization with the corresponding derivation machinery covering epistemic theories in full generality, including the good old semantic specifications. cf. [1].

3. Modal language does not represent justifications whereas the latter have been in the focus of epistemology since Plato. Introducing justifications as a designated sort of proof-like objects not reducible to propositions brings new hyperintensional capabilities to formal epistemology and significantly enhances its expressive power. Along with syntactic descriptions from (2), we introduce a natural class of epistemic models which represent justifications, awareness, knowledge and belief, etc. and subsume epistemic models from (1), including Kripke models, as special cases, cf. [3].

These and other modernizations of epistemic logic may open new research avenues with robust connections to applications.

References

[1] S. Artemov, *Syntactic epistemic logic*, In: Book of Abstracts, 15th Congress of Logic, Methodology and Philosophy of Science CLMPS (2015), 109–110.
[2] S. Artemov, *Knowing the Model*, arXiv preprint arXiv:1610.04955 (2016).
[3] S. Artemov, *Justification Awareness Models*, In International Symposium on Logical Foundations of Computer Science 2018, Springer LNCS **10703** (2018), 22–36.

A feasible set theory

Neil Thapen
(joint work with Arnold Beckmann, Sam Buss, Sy-David Friedman and Moritz Müller)

The *Cobham recursive set functions* (CRSF) were introduced in [1] to capture the notion of feasible, polynomial time computation on arbitrary sets. CRSF coincides with the usual polynomial time functions on finite binary strings, if strings in $\{0,1\}^k$ are identified with the corresponding set-theoretic function in ${}^k2$.

The definition of CRSF uses $\in$-recursion as the basic model for computation on sets. The power of $\in$-recursion is restricted by allowing new functions to be introduced only if their output is no more complex than the output of a function already known to be in CRSF. Here a set a is no more complex than a set b if a is embeddable in b in a certain sense. To allow a limited, "polynomial" increase in complexity, [1] adapts the smash function # of bounded arithmetic into an operation on sets, namely a kind of cartesian product on Mostowski graphs, and uses this as an initial function.

In this talk I describe some alternative characterizations of CRSF in [2] and [3]. The first is similar to [1]. We take some basic initial functions, including the smash function, and close under composition and *subset-bounded recursion*: if g and h are in the class, then so is the function f defined by the recursion

$$f(\bar{a}, b) = g(\bar{a}, b, \{f(\bar{a}, c) : c \in b\}) \cap h(\bar{a}, b).$$

We call this "subset-bounded" because it allows defining a function f by recursion provided we have in hand a function h such that $f(\bar{a}, b) \subseteq h(\bar{a}, b)$. It has the advantage of avoiding the rather complicated "embedding-bounded" recursion used in [1]. However, functions constructed this way are limited in what they can output, so we add a weak, "feasible" Mostowski collapse function as an initial function, which allows us to reconstruct sets from suitable descriptions of them.

Our second characterization uses a Boolean circuit model of computation. For this, we define (infinite) Boolean circuits, that act on Boolean values (*true* and *false*) and use the usual conjunction, disjunction, and negation gates. The inputs and output of a circuit are Boolean values which encode (possibly infinite) sets. To encode a set x using Boolean values, we form the Mostowski graph of the transitive closure of x, and encode this graph in a well-founded set using a bisimularity relation. In this way, the Boolean inputs and output of a circuit can describe arbitrary sets. The CRSF functions can then be precisely characterized as the functions which can be computed by a strongly uniform family of small Boolean circuits.

Our third characterization of CRSF is in terms of Jensen's rudimentary functions. We define the class RS to be the rudimentary functions, plus transitive closure (but not the smash function), closed under subset-bounded recursion. We then give a natural notion of an RS definition of the Mostowski graph of a set x, in a way that lets us code large sets without using smash. Using this, we can show

that CRSF functions can be defined in RS in a certain sense and thus that the function classes are essentially the same, except for issues of coding.

Lastly we show that CRSF consists of the "provably recursive" functions of a certain weak fragment of Kripke-Platek set theory. Namely, define a $\Sigma_1^{\preccurlyeq}$ formula to be one of the form $\exists y \preccurlyeq t(x)\phi(x, y)$, where ϕ is Δ_0, $\preccurlyeq$ is our notion of embedding, and $t(x)$ is a term. Expand the language of set theory by adding symbols for some basic functions, such as transitive closure and smash. Our theory then consists of defining axioms for the new symbols, extensionality, Δ_0-separation, Δ_0-collection, and set induction for $\Sigma_1^{\preccurlyeq}$ formulas. We weaken the induction scheme slightly further, by only including it for $\Sigma_1^{\preccurlyeq}$ formulas in which the witness to the existential quantifier is unique.

References

[1] A. Beckmann, S. Buss, S. Friedman, M. Müller, N. Thapen, *Cobham recursive set functions*, Annals of Pure and Applied Logic **167(3)** (2015), 335–369.

[2] A. Beckmann, S. Buss, S. Friedman, M. Müller, N. Thapen, *Cobham recursive set functions and weak set theories*, Lecture Notes Series, Institute for Mathematical Sciences, National University of Singapore: Volume 33 Sets and Computations (2017), 55–116.

[3] A. Beckmann, S. Buss, S. Friedman, M. Müller, N. Thapen, *Subset-bounded recursion and a circuit model for the Cobham recursive set functions*, submitted (2016).

Gödel's Second Incompleteness Theorem from Scratch

Fedor Pakhomov

In the talk we have presented a new approach to Gödel's Second Incompleteness Theorem that covers some theories that were not covered by earlier approaches.

We consider a class of theories T that are able to interpret a minimalistic theory of their own syntax $\mathsf{Syn}(\mathsf{T})$. And then prove that Gödel's second incompleteness theorem holds for all the theories in the class with respect to any formalization of provability that satisfies Hilbert-Bernays-Löb derivability conditions. Usual approach to the second incompleteness theorem that is going back to Gödel [Göd31] uses arithmetization of syntax. And in contrast to strong forms of second incompleteness theorem that were formulated using arithmetization of syntax (or relatives) (see for example [Fef60, Pud85, Vis09]), our class of theories contains some theories that doesn't interpret weak arithmetical theories like Robinson arithmetic Q and even weak Robinson arithmetic R_0 [TMR53, Šve07]. Moreover, our class contains some decidable theories. An alternative to arithmetization of syntax have been developed by S. Feferman [Fef89], where he have introduced system FS_0 of finitary presented inductive constructions that gave a straightforward formalization of syntax. Although we note that the interpretability strength of system FS_0 is quite high: there is an interpretation of $\mathsf{I}\Sigma_1$ in FS_0.

Let us give an outline of a definition of the theory $\mathsf{Syn}(\mathsf{T})$ of syntax of some first-order theory T. We fix a variant of inductive definition of first-order language of T. And formulate the theory $\mathsf{Syn}(\mathsf{T})$ to reflect this definition. For (one-sorted) theory T the theory $\mathsf{Syn}(\mathsf{T})$ is a 3-sorted theory. The intended domain for the first

sort frm is the set of all formulas of the first-order language of T, the intended domain for the second sort trm is the set of all terms of the first-order language of T, and the intended domain for the third sort var is the set of all first-order variables of the first-order language of T (we limit ourselves to countably many distinct variables). The language of $\mathsf{Syn}(\mathsf{T})$ contains a function for each case in the inductive definition of the language of T with the following intended interpretations: the function $\mathsf{conj}(x^{\mathsf{frm}}, y^{\mathsf{frm}})$ that maps formulas F_1, F_2 to the conjunction, the function $\mathsf{exists}(x^{\mathsf{var}}, y^{\mathsf{frm}})$ that maps a variable v and a formula F to the formula $\exists v\ F$, family of functions $\mathsf{trm}_f(x_1^{\mathsf{trm}}, \ldots, x_n^{\mathsf{trm}})$ that map terms $t_1, \ldots, t_n$ to the terms $f(t_1, \ldots, t_n)$, for all functional symbols $f(x_1, \ldots, x_n)$ of the language of T, etc. This way we have a unique closed $\mathsf{Syn}(\mathsf{T})$-term for each formula, term, and variable of the first-order language of T; for a formula F of the language of T we denote the corresponding term as $\ulcorner F \urcorner$. The axioms of the theory $\mathsf{Syn}(\mathsf{T})$ are:

(1) $\mathsf{f}(x_1, \ldots, x_n) \neq \mathsf{g}(y_1, \ldots, y_m)$, for all different $\mathsf{Syn}(\mathsf{T})$-functions f and g;
(2) $(x_1 \neq x_1' \vee \ldots \vee x_n \neq x_n') \to \mathsf{f}(x_1, \ldots, x_n) \neq \mathsf{f}(x_1', \ldots, x_n')$, for all $\mathsf{Syn}(\mathsf{T})$-functions f.

For theories T with a fixed interpretation of the theory $\mathsf{Syn}(\mathsf{T})$ we could naturally formulate Hilbert-Bernays-Löb derivability conditions [Löb55] for a given formula $\mathsf{Prv}(x^{\mathsf{frm}})$ (note that here we use an interpreted sort frm within the formula Prv). And we prove the following form of Gödel's second incompleteness theorem.

Theorem 1. ***(Second Incompleteness Theorem)*** *Suppose for a first-order theory* T *we have a fixed interpretation of* $\mathsf{Syn}(\mathsf{T})$ *in* T*. Then for any formula* $\mathsf{Prv}(x^{\mathsf{frm}})$ *of the language of* T *that satisfies Hilbert-Bernays-Löb derivability conditions,* $\mathsf{T} \nvdash \neg\mathsf{Prv}(\ulcorner \bot \urcorner)$*, where* $\bot$ *is any* T*-disprovable formula.*

In order to prove our version of Gödel's second incompleteness theorem we establish the following version of fixed point lemma for our class of theories and then use the standard proof of second incompleteness theorem.

Theorem 2. ***(Fixed Point Lemma)*** *Suppose for a first-order theory* T *we have a fixed interpretation of* $\mathsf{Syn}(\mathsf{T})$ *in* T*. Then for any formula* $\mathsf{F}(x^{\mathsf{frm}})$ *of the language of* T *there is a formula* G *such that* $\mathsf{T} \vdash \mathsf{F}(\ulcorner \mathsf{G} \urcorner) \leftrightarrow \mathsf{G}$*.*

Note that the usual proof of fixed point lemma doesn't work in our context. The straightforward adaptation of the standard proof of fixed point lemma to our terminology would require substitution function subst that should work as follows in $(F(x^{\mathsf{frm}}), G) \longmapsto F(\ulcorner G \urcorner)$. But this function is not definable in the language of the theory $\mathsf{Syn}(\mathsf{T})$.

We propose a different method of proving fixed point lemmas. For a first-order formula F, we denote by $\mathsf{dp}(\mathsf{F})$ the depth of the syntactical tree of the formula F. We express in the language of $\mathsf{Syn}(\mathsf{T})$ the restricted versions of this function: functions subst_n that are the restrictions of subst to formulas F with $\mathsf{dp}(\mathsf{F}) \leq 2^n$. Moreover, we ensure that the $\mathsf{Syn}(\mathsf{T})$-formulas $\mathsf{Subst}_n(x^{\mathsf{frm}}, y^{\mathsf{frm}}, z^{\mathsf{frm}})$ that are the definitions of graphs of functions subst_n are such that $\mathsf{dp}(\mathsf{Subst}_n)$ is $\mathcal{O}(n)$. Using this restricted versions of substitution function we are able to prove our version of fixed point lemma (Theorem 2) using a modification of the standard proof.

We prove that for all T with finite signature, the theory $\mathsf{Syn}(\mathsf{T})$ is mutually interpretable with the theory of Cantor's pairing function on an infinite domain Pair_2 [Vis08]. Note that the latter theory have complete decidable extensions, in particular there is a decidable elementary theory $\mathsf{Th}(\mathbb{N}, C)$, here $C\colon \mathbb{N}\times\mathbb{N}\to\mathbb{N}$ is the Cantor pairing function $C(n,m) = (n+m)(n+m+1)/2+m$ [PSD00]. More well-known example of complete decidable theory T that interpret $\mathsf{Syn}(\mathsf{T})$ is the monadic second-order theory of full binary tree $\mathsf{MSO}(2^{<\omega}, S_1, S_2)$ [Rab69].

In the case of complete theories T, our version of Gödel's second incompleteness theorem simply imply that the only predicates that satisfy Hilbert-Bernays-Löb derivability conditions are the inconsistent predicates $\mathsf{Prv}(x)$, i.e. predicates such that $\mathsf{T}\vdash \mathsf{Prv}(\ulcorner F\urcorner)$, for every formula F of the language of T. The following result is about "reasonable" formalizations of provability.

Theorem 3. *Suppose for a first-order theory* T *we have a fixed interpretation of* $\mathsf{Syn}(\mathsf{T})$ *in* T*. Moreover, suppose that a formula* $\mathsf{Prv}(x)$ *satisfy Hilbert-Bernays-Löb derivability conditions and the provability predicate* $\mathsf{Prv}(x)$ *have infinite height, i.e.*

$$\mathsf{T}\nvdash \underbrace{\mathsf{Prv}(\ulcorner\mathsf{Prv}(\ulcorner\ldots\mathsf{Prv}(\ulcorner\bot\urcorner)\urcorner)\urcorner)}_{n\ \text{times}},$$

for any T*-disprovable formula* $\bot$ *and number* n*. Then* T *is undecidable.*

References

[Fef60] S. Feferman. Arithmetization of metamathematics in a general setting. *Fundamenta mathematicae*, 49(1):35–92, 1960.

[Fef89] S. Feferman. Finitary inductively presented logics. *Studies in Logic and the Foundations of Mathematics*, 127:191–220, 1989.

[Göd31] K. Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Monatsh. Math. Phys.*, 38(2):173–198, 1931.

[Löb55] M. H. Löb. Solution of a problem of Leon Henkin. *The Journal of Symbolic Logic*, 20(2):115–118, 1955.

[PSD00] Cgielski P., Grigorieff S., and Richard D. La thorie lmentaire de la fonction de couplage de Cantor des entiers naturels est dcidable. *Comptes Rendus de l'Acadmie des Sciences - Series I - Mathematics*, 331(2):107–110, 2000.

[Pud85] P. Pudlák. Cuts, consistency statements and interpretations. *The Journal of Symbolic Logic*, 50(2):423–441, 1985.

[Rab69] M.O. Rabin. Decidability of second-order theories and automata on infinite trees. *Transactions of the american Mathematical Society*, 141:1–35, 1969.

[Šve07] V. Švejdar. Weak theories and essential incompleteness. *The Logica Yearbook*, pages 213–224, 2007.

[TMR53] A. Tarski, A. Mostowski, and R.M. Robinson. *Undecidable Theories*. Studies in logic and the foundations of mathematics. North-Holland, 1953.

[Vis08] Albert Visser. Pairs, sets and sequences in first-order theories. *Archive for Mathematical Logic*, 47(4):299–326, 2008.

[Vis09] Albert Visser. Can we make the second incompleteness theorem coordinate free? *Journal of Logic and Computation*, 21(4):543–560, 2009.

How uniform is provable convergence?

Henry Towsner

If we know that some kind of sequence always converges, we can ask how quickly and how uniformly it converges. Many convergent sequences converge non-uniformly and, relatedly, have no computable rate of convergence. However proof-theoretic ideas often guarantee the existence of a uniform "meta-stable" rate of convergence.

Definition. *Let $\mathcal{S}$ be a collection of sequences. This collection converges* uniformly metastably *if for every $\epsilon > 0$ and every $F : \mathbb{N} \to \mathbb{N}$ such that $n < F(n)$ and $F(n) \leq F(n+1)$ for all n, there is an M_F so that, for each $(a_n)_{n\in\mathbb{N}} \in \mathcal{S}$ there is an $m \leq M_F$ so that, for all $n, n' \in [m, F(m)]$, $d(a_n, a_{n'}) < \epsilon$.*

Many natural collections of convergent sequences exhibit a stronger notion of uniformity: bounds on jumps.

Definition. *Let $\mathcal{S}$ be a collection of sequences. This collection* has a uniform bound on jumps *if for each $\epsilon > 0$ there is a K so that, for each $(a_n)_{n\in\mathbb{N}} \in \mathcal{S}$ and each sequence $n_1 < n_2 < \cdots < n_K$, there is an $i < K$ with $d(a_{n_i}, a_{n_{i+1}}) < \epsilon$.*

In fact, this notion represents the first interesting level of a family of notions stratifying uniform metastability (depending on some fixed family of fundamental sequences):

Definition. *Let $F : \mathbb{N} \to \mathbb{N}$ be a function with $F(n) > n$ and $F(n) \leq F(n+1)$ for all n. We define the α-iteration of F by:*

- $F^0(n) = n$,
- *when $\alpha > 0$, $F^\alpha(n) = F^{\alpha[F(n)]}(F(n))$.*

Definition. *We say $\mathcal{S}$ converges* concretely α-uniformly *if for each $\epsilon > 0$ there is a $\beta < \alpha$ so that, for every $F : \mathbb{N} \to \mathbb{N}$ such that $F(n) > n$ for all n, for each $(a_n)_{n\in\mathbb{N}} \in \mathcal{S}$ there is an m with $F(m) \leq F^\beta(0)$ so that, for all $n, n' \in [m, F(m)]$, $d(a_n, a_{n'}) < \epsilon$.*

Then a uniform bound on jumps is precisely concrete ω-uniformity.

We can characterize the situation where a family has uniform bounds on jumps using nonstandard analysis:

Theorem. *$\mathcal{S}$ has uniform bounds on jumps if and only if, in every ultraproduct $(a_n)_{n\in\mathbb{N}^*}$ of the sequences in $\mathcal{S}$, the sequence $(a_n)_{n\in\mathbb{N}^*}$ converges in* every *cut of $\mathbb{N}^*$.*

This notion generalizes to Kohlenbach and Safarik's notion of effective learnability, which we think of as a generalization of bounded jumps to only consider "large enough" jumps.

Definition. *Let $\mathcal{S}$ be a collection of sequences. This collection* has a uniform bound on jumps of distance h *(where $n < h(n)$ for all n) if for each $\epsilon > 0$ there is a K so that, for each $(a_n)_{n\in\mathbb{N}} \in \mathcal{S}$ and each sequence $n_1 < n_2 < \cdots < n_K$ with $h(n_i) \leq n_{i+1}$ for all iK, there is an $i < K$ with $d(a_{n_i}, a_{n_{i+1}}) < \epsilon$.*

Theorem. *$\mathcal{S}$ has uniform bounds on jumps of distance h if and only if, in every ultraproduct $(a_n)_{n\in\mathbb{N}^*}$ of the sequences in $\mathcal{S}$, the sequence $(a_n)_{n\in\mathbb{N}^*}$ converges in every cut of $\mathbb{N}^*$ closed under h.*

A survey of classical realizability

Alexandre Miquel

Classical realizability [3–7] was introduced by Krivine in the mid-90's as a complete reformulation of the principles of Kleene realizability to make them compatible with classical reasoning, using the connection between classical reasoning and control operators discovered by Griffin [2]. Classical realizability provides new models for a wide range of impredicative theories (from second-order arithmetic [5] to Zermelo-Fraenkel set theory [3,7]), as well as its own interpretation of the axiom of dependent choices (DC) [4,5].

In the first part of the talk, I will recall the basics of classical realizability (connection between classical reasoning and control operators, Krivine's λ_c-calculus, truth/falsity value semantics), while emphasizing the key ideas underlying the approach. I will discuss the interest of interpreting classical proofs in direct style (rather than passing via a negative translation), before showing the connections between classical realizability and Cohen's forcing.

The second part of the talk will be devoted to the categorical interpretation of classical realizability, following the tradition initiated by Hyland, Johnstone and Pitts [1,11], and using recent work by Streicher [12]. For that, I will introduce the notion of implicative algebra, a simple algebraic structure generalizing complete Heyting algebras and abstract Krivine algebras, and based on a surprising identification between the notions of a realizer and of a type. Then I will show that this structure naturally induces a family of triposes — the implicative triposes — that encompass Heyting triposes, Boolean triposes, intuitionistic realizability triposes and classical realizability triposes, thus providing a unified framework for expressing forcing and realizability, both in intuitionistic and classical logic.

References

[1] J. M. E. Hyland, *The effective topos*, Proceedings of the L. E. J. Brouwer Centenary Symposium (Noordwijkerhout 1981), North Holland (1982), pp. 165–216.

[2] T. Griffin, *A formulæ-as-types notion of control*, Proceedings of *Principles of programming languages, POPL'90* (1990), p. 47–58.

[3] J.-L. Krivine, *Typed lambda-calculus in classical Zermelo-Frnkel set theory*, Archive for Mathematical Logic **40(3)** (2001), p. 189–205.

[4] J.-L. Krivine, *Dependent choice, 'quote' and the clock*, Theoretical Computer Science **308(1-3)** (2003), p. 259–276.

[5] J.-L. Krivine, *Realizability in classical logic.* In *Interactive models of computation and program behaviour*, Panoramas et synthèses, Société Mathématique de France, **27** (2009), p. 197–229.

[6] J.-L. Krivine, *Realizability algebras: a program to well order* $\mathbb{R}$. Logical Methods in Computer Science, **7(3:02)** (2011), p. 1–47.

[7] J.-L. Krivine, *Realizability algebras II : new models of ZF + DC*. Logical Methods in Computer Science, **8(1:10)** (2012), p. 1–28.
[8] A. Miquel, *Existential witness extraction in classical realizability and via a negative translation,* Logical Methods in Computer Science **7(2)** (2011).
[9] A. Miquel, *Forcing as a program transformation.* Proceedings of the 26th Annual IEEE Symposium on Logic in Computer Science, LICS 2011, IEEE Computer Society (2011), p. 197–206.
[10] P. Oliva, T. Streicher, *On Krivine's realizability interpretation of classical second-order arithmetic,* Fundamenta Informaticæ **84(2)** (2008), p. 207–220.
[11] J. van Oosten, *Realizability. An Introduction to its Categorical Side*, Elsevier (2008).
[12] T. Streicher, *Krivine's classical realisability from a categorical perspective.* Mathematical Structures in Computer Science **23(6)** (2013), p. 1234–1256.

From Hilbert-Bernays' Grundlagen to second-order arithmetic

Sam Sanders
(joint work with Dag Normann)

Large parts of mathematics are studied *indirectly* via *countable approximations*, also called *codes*. Perhaps the most prominent example is the program *Reverse Mathematics*, as founded by Harvey Friedman and developed extensively by Simpson (See [14]). Indeed, the framework for Reverse Mathematics is *second-order arithmetic*, although the original Hilbert-Bernays foundational framework in *Grundlagen der Mathematik* includes higher-order objects (See e.g. [6, p. 495]). Bishop's *Constructive Analysis* ([2]), and constructive mathematics in general, makes similar use of codes. This coding practice is generally deemed unproblematic.

Nonetheless, this coding practice *fundamentally* distort mathematics: we show that the following **classical** theorems involving type two objects **cannot be proved** in (any higher-type version of) any fragment Π^1_k-CA_0 of second-order arithmetic. They *can* be proved in full (higher-type) second-order arithmetic Z_2.

(i) *Cousin's lemma*: **any** open cover of $[0,1]$ has a finite sub-cover, i.e. *full* Heine-Borel compactness ([4]); also provable in intuitionistic mathemaitcs.
(ii) *Lindelöf's lemma*: **any** open cover of $\mathbb{R}$ has a countable sub-cover; also provable in recursive and intuitionistic mathematics ([16]).
(iii) *Besicovitsch and Vitali covering lemmas* as in [1, §2].
(iv) Basic properties (e.g. uniqueness) of the *gauge integral*; the latter is a generalisation of the Lebesgue and the improper Riemann integral ([15]), and provides a formalisation of Feynman's path integral.
(v) *Neighbourhood Function Principle*; also provable in intuitionism ([16]).
(vi) The existence of *Lebesgue numbers* for **any** open cover ([5]).
(vii) The *Banach-Alaoglu theorem* for **any** open cover ([14, X.2.4], [3, p. 140]).
(viii) The *Heine-Young* and *Lusin-Young* theorems, the *tile theorem* [7,17], and the latter's generalisation due to Rademacher ([12, p. 190]).

These results cast serious doubt on the elegant 'Big Five picture' of Reverse Mathematics. In particular, the latter signature characterisation seems to be an artefact

of coding. Furthermore, *Lindelöf's lemma* is in the intersection of (russian) recursive, intuitionistic, and classical mathematics, but much harder to prove than similar 'semi-constructive' theorems (like BD-N) in classical mathematics.

Finally, the above theorems exhibit surprising behaviour in Kohlenbach's *higher-order* Reverse Mathematics ([8]):

(1) Cousin's lemma plus higher-order ACA_0 implies ATR_0.
(2) Cousin's lemma plus higher-order Π^1_1-CA_0 implies the Π^1_3-theorems of Π^1_2-CA_0.
(3) Lindelöf's theorem for Baire space (given by a realiser) plus higher-order ACA_0 implies Π^1_1-CA_0 and Gandy's *superjump*.

These results are (often) established by connecting *higher-order computability* and *Nonstandard Analysis* in hitherto unseen ways ([9, 10, 13]). Finally, we establish the aforementioned results in [11] *without* the use of Nonstandard Analysis.

References

[1] Pascal Auscher and Lashi Bandara, *Real Harmonic Analysis*, ANU Press, 2010.
[2] Errett Bishop, *Foundations of constructive analysis*, McGraw-Hill, 1967.
[3] Douglas K. Brown, *Functional analysis in weak subsystems of second-order arithmetic*, PhD Thesis, The Pennsylvania State University, ProQuest LLC, 1987.
[4] Pierre Cousin, *Sur les fonctions de n variables complexes*, Acta Math. **19** (1895), 1–61.
[5] Mariagnese Giusto and Alberto Marcone, *Lebesgue numbers and Atsuji spaces in subsystems of second-order arithmetic*, Arch. Math. Logic **37** (1998), no. 5-6, 343–362.
[6] David Hilbert and Paul Bernays, *Grundlagen der Mathematik. II*, Zweite Auflage. Die Grundlehren der mathematischen Wissenschaften, Band 50, Springer, 1970.
[7] T. H. Hildebrandt, *The Borel theorem and its generalizations*, Bull. Amer. Math. Soc. **32** (1926), no. 5, 423–474.
[8] Ulrich Kohlenbach, *Higher order reverse mathematics*, Reverse mathematics 2001, Lect. Notes Log., vol. 21, ASL, 2005, pp. 281–295.
[9] Dag Normann and Sam Sanders, *Nonstandard Analysis, Computability Theory, and their connections*, Submitted; arXiv: `https://arxiv.org/abs/1702.06556` (2017).
[10] ———, *Metastability, Computability Theory, and Nonstandard Analysis*, In preparation (2017).
[11] ———, *On the mathematical and foundational significance of the uncountable*, Submitted, arXiv: `https://arxiv.org/abs/1711.08939` (2017).
[12] Hans Rademacher, *Eineindeutige Abbildungen und Meßbarkeit*, Monatsh. Math. Phys. **27** (1916), no. 1, 183–235.
[13] Sam Sanders, *To be or not to be constructive*, *Indagationes Mathematicae* and arXiv `https://arxiv.org/abs/1704.00462` (2017), pp. 68.
[14] Stephen G. Simpson, *Subsystems of second order arithmetic*, 2nd ed., Perspectives in Logic, CUP, 2009.
[15] Charles Swartz, *Introduction to gauge integrals*, World Scientific, 2001.
[16] Anne Sjerp Troelstra and Dirk van Dalen, *Constructivism in mathematics. Vol. I*, Studies in Logic and the Foundations of Mathematics, vol. 121, North-Holland, 1988.
[17] W. H. Young and G. H. Young, *On The Reduction Of Sets Of Intervals*, Proc. Lond. Math. Soc. **14** (1915), 111–130.

Some observations on the logical foundations of inductive theorem proving

Stefan Hetzl
(joint work with Tin Lok Wong)

This talk is about the recent work [3] on the logical foundations of automated inductive theorem proving. In it, we endeavour to connect two areas that have developed rather independently. On the one hand: theories of arithmetic as a part of mathematical logic and on the other hand: (automated) inductive theorem proving in computer science.

The aim of our work is to apply methods and results from the former tradition in mathematical logic to the tradition in computer science. The main advantage of this combination is that it is possible to obtain *unprovability* results (by model-theoretic means) where previously in the literature on inductive theorem proving only empirical observations could be made based on the failure of *a specific algorithm* to find a proof.

A first obstacle in realizing such an application is that there is a wealth of different approaches to inductive theorem proving. This makes it difficult to provide a common theoretical basis. However, the final result is typically, in one way or another, explicitly or implicitly, a proof of the goal from instances of an induction scheme and basic axioms from a background theory. We take this observation as a guiding principle for the development of a theoretical model of inductive theorem proving.

We then use this model to analyze a number of different aspects of methods for inductive theorem proving. In particular, we consider the choice of an induction rule; the question of how an inductive theorem prover should choose the induction rule to be applied to its current goal has received a great deal of attention in the literature, see, e.g., the techniques of "recursion analysis" in [1] or "induction revision in [2]. The interest in this question comes from the tension between the choice of the induction rule and the choice of the induction formula when proving a goal: the more flexibility we have in choosing the induction rule, the less flexibility we need in choosing the induction formula. In the very extreme case, one can fix an induction formula, e.g., the goal, and search for an induction rule with respect to which this formula is inductive. Thus one can dispose of the difficult task of finding a non-analytic induction formula and simply search for a suitable induction rule.

We carry out a comparison of different induction schemes from this point of view: we fix a formula $\varphi(x)$ and ask with respect to which induction schemes it is inductive. We obtain a complete mathematical characterization of the implications between the different resulting notions of inductiveness where previously in the literature, only empirical observations have been made.

References

[1] R. S. Boyer and J. Strother Moore. *A computational logic*. ACM monograph series. Academic Press, 1980.
[2] A. Bundy, D. Basin, D. Hutter, and A. Ireland. *Rippling: Meta-Level Guidance for Mathematical Reasoning*. Cambridge Tracts in Theoretical Computer Science. Cambridge University Press, 2005.
[3] S. Hetzl, T. L. Wong, *Some observations on the logical foundations of inductive theorem proving*, Logical Methods in Computer Science, **13(4)**, 2017.

Impredicativity in Homotopy Type Theory

Steve Awodey

We investigate the use of impredicative methods for the construction of inductive types in homotopy type theory. Inductive types have been constructed impredicatively in other systems of type theory in the past, but these generally fail have the correct the rules.

Using new methods from homotopy type theory [1] we are able to repair these prior constructions, and extend the impredicative methodology to include also the newly discovered higher inductive types that form the basis of the recent applications in homotopy theory.

References

[1] *Homotopy Type Theory: Univalent Foundations of Mathematics*, The Univalent Foundations Program, Institute for Advanced Study, 2013.

The Modal Logic of Extensions of Models of Peano Arithmetic

Albert Visser
(joint work with V. Yu. Shavrukov)

We study the modal logics of the big Kripke models with as nodes models of Peano Arithmetic and as accessibility relation one of the relations *extension*, *end-extension*, *internal model with parameters*, *internal model without parameters*. The logic of these models is $\mathsf{S4}$, as was proved by Shavrukov in 1998. See [Vis98]

We study how expressive the mixed modal language is where we allow arithmetical sentences as modal atoms. First, we illustrate that many familiar notions are modally definable. Then we discuss the complexity of the set of all arithmetical sentences for which it is valid that they are possibly necessary. Their complexity turns out to be complete Π^1_1.

We will briefly describe an alternative accessibility relation that gives a notion of necessity that is very close to, and, for some theories equal to, provability.

References

[Vis98] A. Visser. An Overview of Interpretability Logic. In M. Kracht, M. de Rijke, H. Wansing, and M. Zakharyaschev, editors, *Advances in Modal Logic*, volume 1, 87 of *CSLI Lecture Notes*, pages 307–359. Center for the Study of Language and Information, Stanford, 1998.

On the Benefit of Unsound Rules

Matthias Baaz
(joint work with Juan Pablo Aguilera)

The characteristic-variable condition of first-order Gentzen-style proof systems states that whenever a proof contains a strong-quantifier inference of the form

$$\frac{\Gamma, A(a,b)}{\Gamma, \forall x\, A(x,b)} \tag{4}$$

the variable a does not appear in $\Gamma, \forall x\, A(x,b)$. This condition ensures that quantifier inferences are sound, but is not necessary. By weakening the characteristic-variable condition, one obtains proof systems in which seemingly invalid reasoning, e.g., such as

$$\frac{\dfrac{A(a) \to A(a)}{A(a) \to \forall y\, A(y)}}{\exists x\, (A(x) \to \forall y\, A(y))}$$

is permitted. If π is a proof, write $a <_\pi b$ if a is the characteristic variable of an inference in whose principal formula b appears (e.g., as in equation (4)). The calculus LK^+ is defined like Gentzen's proof system for first-order logic, LK, except that the characteristic-variable condition is weakened by the following of a proof π requiring instead:

(1) (substitutability) no characteristic variable appears in the conclusion of π.
(2) (side-variable condition) the relation $<_\pi$ is acyclic.
(3) (weak regularity) every variable is the characteristic variable of at most one inference in π.

A feature of proofs in LK^+ is that subtrees of proofs need not be proofs.

Theorem. Every sequent provable in LK^+ is valid. There is no elementary function bounding the length of the shortest cut-free LK^+-proof of a sequent in terms of its shortest cut-free LK-proof.

The conditions above are motivated by the rules governing possible inferences in Hilbert's ε-calculus, whose language contains no quantifiers. In a way, thus, LK^+ is a first-order proof system that resembles the ε-calculus.

References

[1] J.P. Aguilera and M. Baaz, *Unsound Inferences Make Proofs Shorter*, To Appear.

A concurrent interpretation of the law of excluded middle

Ulrich Berger

(joint work with Hideki Tsuiki)

It is well-known that constructive proofs carry computational content. This phenomenon, which is known as the Brouwer-Heyting-Kolmogorov interpretation or the Curry-Howard correspondence, is the origin of various methods and implementations of proof systems that automatically extract certified programs from constructive formal proofs. Examples are Nuprl [1], PX [2], Coq [3], Isabelle [4], Agda [5], Minlog [6]. The programs extracted by these systems are usually functional; other programming paradigms, such as non-determinism or concurrency, are hardly covered by this methodology. This may be considered a weakness of program *extraction* compared with existing program *verification* techniques which *do* cover these programming paradigms. Another restriction of program extraction is that it is not able to deal with the law of excluded middle

$$\frac{B \to A \quad \neg B \to A}{A}\ \mathrm{LEM}$$

if the condition B is undecidable.

In this talk we propose a way to partly overcome these limitations. We give a computational interpretation of the law of excluded middle as a scheme for the concurrent execution of processes. The interpretation, which takes place within the framework of realizability, involves two new logical operators: $\mathrm{Set}_n(A)$, allowing for n concurrent processes to realize the formula A, and $A\|B$ ('A restricted to B'), a strengthening of the implication $B \to A$, which is realized by a computation that is guaranteed to terminate if B holds and, in case of termination, realizes A.

The realizable form of LEM using the new logical operators is

$$\frac{A \,\|\, B \quad A \,\|\, \neg B}{\mathrm{S}_2(A)}\ \text{Concurrent-LEM}$$

where B must be a Harrop formula. To compute a realizer of the conclusion of Concurrent-LEM one simple runs the realizers provided by the premises concurrently. The main rule to infer a strict implication is

$$\frac{B \to (A_0 \vee A_1) \quad \neg B \to (A_0 \wedge A_1)}{(A_0 \vee A_1) \parallel B}$$

where B, A_0, A_1 must be Harrop formulas.

We apply our interpretation to two examples of program extraction in computable analysis: Infinite Gray-code, due to Tsuiki [3] and matrix inversion via concurrent Gaussian elimination. An intensional version of infinite Gray-code was

used in [1] to extract conventional functional programs in the Minlog system. A precursor of our system of concurrent program extraction can be found in [9].

References

[1] R.L. Constable, S.F. Allen, H.M. Bromley, W.R. Cleaveland, J.F. Cremer, R.W. Harper, D.J. Howe, T.B. Knoblock, N.P. Mendler, P. Panangaden, J.T.Sasaki, S.F. Smith, *Implementing Mathematics with the Nuprl Proof Development System*, Prentice–Hall, 1986.

[2] S. Hayashi, H. Nakano, *PX: A Computational Logic*, MIT Press, 1988.

[3] C. Paulin–Mohring, *Inductive definitions in the system Coq; rules and properties*, M. Bezem and J.F. Groote, editors, Typed Lambda Calculi and Applications, LNCS **664** (1993), 328–345.

[4] S. Berghofer, *Program Extraction in simply-typed Higher Order Logic*, H. Geuvers and F. Wiedijk, editors, Types for Proofs and Programs (TYPES'02), LNCS **2646** (2003), 21-38.

[5] C.M. Chuang, *Extraction of Programs for Exact Real Number Computation Using Agda*, PhD thesis, Swansea University, 2011.

[6] U. Berger, K. Miyamoto, H. Schwichtenberg, M. Seisenberger, *Minlog - A Tool for Program Extraction for Supporting Algebra and Coalgebra*, CALCO-Tools, LNCS **6859** (2011), 393-399.

[7] H. Tsuiki, *Real Number Computation through Gray Code Embedding*, Theoretical Computer Science **284** (2002), 746–485.

[8] U. Berger, K. Miyamoto, H. Schwichtenberg, H. Tsuiki, *Logic for Gray-code computation*, D. Probst, P. Schuster, editors, Concepts of Proof in Mathematics, Philosophy, and Computer Science, de Gruyter, Ontos Mathematical Logic 6, 2016.

[9] U. Berger, *Extracting Non-Deterministic Concurrent Programs*, CSL 2016, LIPIcs **62** (2016), 26:1–26:21.

Generalized Goodstein sequences

Andreas Weiermann

(joint work with Toshiyasu Arai and Stan Wainer)

The classical Goodstein sequences provide one of the most elementary principles which although true are unprovable from the axioms of first order arithmetic. In this report we indicate recent progress (partly in joint work with T. Arai and S. Wainer) on extending the classical Goodstein sequences to more complex situations. The resulting principles lead to far reaching independence results for systems of arithmetic. Moreover they may lay the foundation of a new theory of notations systems for natural numbers.

1. The classics

Fix a natural number $k \geq 2$. Then there exist uniquely determined natural numbers p, q, r such that $m = k^r \cdot p + q$ and $0 < p < k$ and $q < k^r$. We call this representation the k normal form of m and write $m =_{NF} k^r \cdot p + q$.

The k normal form of m is natural in the sense that it produces a representation of m with a minimal syntactical amount when this is measured in terms of a natural norm function. For such an $m =_{NF} k^r \cdot p + q$ we define its base change with respect to k recursively via $m[k \leftarrow k+1] := (k+1)^{r[k \leftarrow k+1]} \cdot p + q[k \leftarrow k+1]$ where it is understood that $0[k \leftarrow k+1] := 0$.

Lemma 1. (1) *If $m < n$ then $m[k \leftarrow k+1] < n[k \leftarrow k+1]$.*
(2) *If $m =_{NF} k^r \cdot p + q$ then $m[k \leftarrow k+1] =_{NF} k^{r[k \leftarrow k+1]} \cdot p + q[k \leftarrow k+1]$.*

Given $m > 0$ let the Goodstein sequence m_l starting with m be recursively defined as follows: $m_0 := 0$, $m_{l+1} := m_l[l+2 \leftarrow l+3] - 1$ if $m_l > 0$. If $m_l = 0$ then $m_{l+1} := 0$.

Let G be the assertion $\forall m \exists l m_l = 0$.

Define $\psi_k : \mathrm{N} \to \varepsilon_0$ as follows.

$\psi_k 0 := 0$, $\psi_k m := \omega^{\psi_k r} p + \psi_k q$ if $m =_{NF} k^r \cdot p + q$.

Lemma 2. (1) *If $m < n$ then $\psi_k m < \psi_k n$.*
(2) *$\psi_{k+1}(m[k \leftarrow k+1]) = \psi_k m$.*

Theorem 1. *The assertion G is true.*

Proof. We tacitly apply Lemma 1 and Lemma 2. Define $o : \mathrm{N} \to \varepsilon_0$ via $o(l) := \psi_{l+2}(m_l)$. Then $l_l > 0$ yields $o(l+1) = \psi_{l+3}(m_{l+1}) = \psi_{l+3}(m_l[l+2 \leftarrow l+3] - 1) < \psi_{l+3}(m_l[l+2 \leftarrow l+3]) = \psi_{l+2}(m_l) = o(l)$. □

In fact this proof shows that the assertion G is provable in PA plus the principle that there is no infinite primitive recursive descending chain of ordinals below ε_0. (As a word of warning it should be noted that it is not possible to calculate a decimal expansion of the least l such that $100_l = 0$ in real life.)

Theorem 2. *The assertion G is not provable in first order Peano arithmetic.*

2. Goodstein sequences for the Ackermann function (first version).

Our goal is now to replace the base k representation by the Ackermann function which is defined as follows.

Definition 1. (1) $A_0(k,b) = k^b$.
(2) $A_{a+1}(k,0) = A_a(k,\cdot)^k(1)$ *where the upper index denotes the number of iterations.*
(3) $A_{a+1}(k,b+1) = A_a(k,\cdot)^k(A_{a+1}(k,b))$.

For all $c > 0$ there exist unique $a, b, m, n < \omega$ such that $c = A_a(k,b) \cdot m + n$, $A_a(k,0) \leq c < A_{a+1}(k,0)$, $A_a(k,b) \leq c < A_a(k,b+1)$, $0 < A_a(k,b) \cdot m < A_a(k,b+1)$, and $n < A_a(k,b)$ We write $c =_{NF} A_a(k,b) \cdot m + n$ in this case. This means that we have in mind an underlying context fixed by k and that for the number c we have uniquely associated the numbers a, b, m, n. Note that it could be possible that $A_{a+1}(k,0) = A_a(k,b)$ so that we have to choose the right representation for the context.

For such a c we define its base change with respect to k recursively via $0[k \leftarrow k+1] := 0$ and $c[k \leftarrow k+1] := A_{a[k \leftarrow k+1]}(k+1, b[k \leftarrow k+1]) \cdot m + n[k \leftarrow k+1]$ if $c =_{NF} A_a(k,b) \cdot m + n$.

Lemma 3. (1) *If $c < d$ then $c[k \leftarrow k+1] < d[k \leftarrow k+1]$.*
(2) *If if $c =_{NF} A_a(k,b) \cdot m + n$ then $c[k \leftarrow k+1] =_{NF} A_{a[k \leftarrow k+1]}(k+1, b[k \leftarrow k+1]) \cdot m + n[k \leftarrow k+1]$.*

We define a mapping $\chi_k : \mathrm{N} \to \varphi 20$ recursively as follows. $\chi_k 0 := 0$ and $\chi_k c := \omega^{\varepsilon_{\chi_k a}+\chi_k b} \cdot m + \psi_k n$ if $c =_{NF} A_a(k,b) \cdot m + n$.

Lemma 4. *If $c < d < \omega$ then $\chi_k c < \chi_k d$.*

Let G' be the assertion $\forall c \exists l c_l = 0$.

Theorem 3. $\mathrm{PA} + \mathrm{TI}(\varphi_2 0) \vdash G'$.

Theorem 4. *Let $\gamma < \varphi_2 0$. Then* $\mathrm{PA} + \mathrm{TI}(\gamma) \nvdash G'$.

3. Goodstein sequences for the Ackermann function (second version).

Our last goal is to define Goodstein sequences which are characteristic for ATR_0.

For a given $m \in \mathrm{N}$ we are going to define the k-normal form of m by a sandwiching procedure.

If $m = 0$ then m is its own k normal form. Now assume that $m > 0$. First determine the unique a such that $A_a(0) \leq m < A_{a+1}(0)$ and let $a_0 := a$.

Next determine the unique b_0 such that $A_{a_0}(b_0) \leq m < A_{a_0}(b_0 + 1)$.

If $A_a(b_0) = m$, then by definition this is the k normal form of m and we abbreviate this by

$$m =_{k-NF} A_{a_0}(b_0).$$

Assume recursively that we have arrived at a situation

$$A_{a_r}(b_r) \leq m < A_{a_r}(b_r + 1).$$

If $A_{a_r}(b_r) = m$ then this we write $m =_{k-NF} A_{a_r}(b_r)$.

Otherwise we are in the situation that $A_{a_r}(b_r) < m < A_{a_r}(b_r + 1)$.

In the case $a_r = 0$ we have $k^{b_r} < m < k^{b_r+1}$. Then we can write $m = k^{b_r} \cdot p + q$ in a unique way where $q < k^{b_r}$ and $p < k$ and we write $m =_{k-NF} k^{b_r} \cdot p + q$.

Now assume $a_r > 0$. If $A_{a_r-1}(A_{a_r}(b_r)) \leq m < A_{a_r}(b_r + 1)$ let $a_{r+1} := a_r - 1$. Then there exists a unique b_{r+1} such that $A_{a_{r+1}}(b_{r+1}) \leq m < A_{a_{r+1}}(b_{r+1} + 1)$ such that $b_{r+1} \geq A_{a_r}(b_r)$. Here we can iterate.

If $A_{a_r}(b_r) < m < A_{a_r-1}(A_{a_r}(b_r))$ then there exists a minimal a^* such that $A_{a_r}(b_r) < m < A_{a^*}(A_{a_r}(b_r))$.

Assume first that $a^* = 0$. Then $A_{a_r}(b_r) < m < k^{A_{a_r}(b_r)}$ and we can write $m = A_{a_r}(b_r) \cdot p + q$ in a unique way where $q < A_{a_r}(b_r)$ and $p < m$ and we write $m =_{k-NF} A_{a_r}(b_r) \cdot p + q$.

Assume therefore that $a^* > 0$. Then $A_{a^*-1}(A_{a_r}(b_r)) \leq m < A_{a^*}(A_{a_r}(b_r))$ Let $a_{r+1} := a^* - 1$. Then there exists a unique b_{r+1} such that $A_{a_{r+1}}(b_{r+1}) \leq m < A_{a_{r+1}}(b_{r+1} + 1)$ such that $b_{r+1} \geq A_{a_r}(b_r)$. We can then again iterate.

The new Goodstein sequences are now defined as follows. Let us start with a given number m. Let $m_0 := m$ and define recursively $m_{l+1} := m_l[l+2 \leftarrow l+3] - 1$ if $m_l > 0$. We also put $m_{l+1} = 0$ if $m_l = 0$.

Let $G'' := \forall m \exists l m_l = 0$.

Theorem 5. (1) $\mathrm{PA} + \mathrm{TI}(\Gamma_0) \vdash G''$.

(2) $\mathrm{ATR}_0 \nvdash G''$.

By extending the hierarchy A_a to transfinite labels one can obtain even stronger Goodstein principles. If α ranges over ordinals less than ε_0 then the resulting principle is characteristic for ID_1. We are confident being able to classify the resulting principles of level reaching op to the ordinal of $(\Pi^1_1 - \mathrm{TR})_0$.

It is an open problem in as much the different k normal forms introduced here can be used to develop a decent theory of natural notations for natural numbers. One can verify in the considered examples that the base change produces maximal possible values when it is defined with respect to the k-normal forms in question.

References

[1] M. De Smet and A. Weiermann. *Goodstein sequences for prominent ordinals up to the Bachmann-Howard ordinal.* Ann. Pure Appl. Logic **163** (2012), no. 6, 669–680.

[2] R.L. Goodstein. *On the restricted ordinal theorem.* J. Symbolic Logic **9**, (1944). 33–41.

[3] R.L. Goodstein. *Transfinite ordinals in recursive number theory.* J. Symbolic Logic **12**, (1947). 123–129.

[4] L. Kirby and J. Paris. *Accessible independence results for Peano arithmetic.* Bull. London Math. Soc. **14** (1982), no. 4, 285–293.

[5] F. Meskens and A. Weiermann. *Classifying Phase Transition Thresholds for Goodstein Sequences and Hydra Games.* Gentzen's Centenary. The Quest for Consistency, R. Kahle and M. Rathjen (eds.), Springer 2015. 455-478.

[6] *Ackermannian Goodstein principles for first order Peano arithmetic.* Lecture Notes Series, Institute for Mathematical Sciences, National University of Singapore: Volume **33** Sets and Computations, 157-181.

[7] A. Weiermann and G. Wilken. *Goodstein sequences for prominent ordinals up to the ordinal of* $\Pi^1_1 - \mathrm{CA}_0$. Ann. Pure Appl. Logic **164** (2013), no. 12, 1493–1506.

Presheaf and sheaf models of type theory

Thierry Coquand

I presented some models of *univalent type theory*, which is dependent type theory with the axiom of univalence and the operation of propositional truncation. Two main applications of these models are the characterisation of the proof theoretic strength of this system and various independence and consistency results, e.g. that countable choice (suitably formulated using in a crucial way propositional trunction) cannot be proved, and consistency with Brouwer's fan theorem.

For this we make use of the bi-interpretability between dependent type theory (including the W type, but without identity types) and a constructive system of set theory (a suitable extension of CZF) which is explained in Peter Aczel's paper [1] , and we notice that all our model constructions can be carried out in this set theoretic system.

The first class of models can be described as "inner" models inside presheaf models of dependent type theory (without identity types). In order to give an interpretation of the identity type, we follow the "identity-as-path" interpretation. A path type will be obtained by exponentiation with an "interval" $\mathbb{I}$, which is a presheaf with two distinct elements 0 and 1 and satisfying some two further properties

(1) $\mathbb{I}$ has a connection structure, i.e. maps $(\wedge)$, $(\vee) : \mathbb{I} \to \mathbb{I} \to \mathbb{I}$ satisfying $x \wedge 1 = x = 1 \wedge x$, $x \wedge 0 = 0 = 0 \wedge x$ and $x \vee 1 = 1 = 1 \vee x$, $x \vee 0 = x = 0 \vee x$ and
(2) representables are closed by cartesian products with $\mathbb{I}$

The axiomatic conditions required for getting a model of type theory have been analysed in [5] and a complementary analysis can be found in [4].

Using the segment $\mathbb{I}$ we can define a set of "filling structures", inspired from homotopy theory. An element of this filling structure represents a generalized "path lifting" operation. It expresses that the type of all path liftings is a singleton up to homotopy (for a given path in the base and starting point).

One can then check that presheaves *together with* a filling structure form a model of univalent type theory. This has been done in the joint paper [2]

In order for this model to work, the only hypotheses on the base category $\mathcal{C}$ is that we can find an "interval" $\mathbb{I}$, i.e. a presheaf satisfying the conditions above. In particular, given another category $\mathcal{D}$ we can build a new model on $\mathcal{C} \times \mathcal{D}$ by defining a new interval $\mathbb{I}_{\mathcal{D}}(X, Y) = \mathbb{I}(X)$. We get in this way a presheaf model $M_{\mathcal{D}}$ of univalent type theory. If we furthermore assume that we have a notion of covering on $\mathcal{D}$, represented by a family Cov, F in $M_{\mathcal{D}}$ we can define internaly a notion of sheaf/stack A as a presheaf A such that all canonical maps $A \mapsto A^{F(c)}$, $c : Cov$ are equivalences. As soon as all maps $X \mapsto X^{F(c)}$ are *idempotent* monads, for instance if we have $\Pi(x\ y : F(c))\mathsf{Path}\ (F(c))\ x\ y$, these maps define *left exact modalities* for $M_{\mathcal{D}}$ in the sense of [3]. Using this, we can check that these sheaves/stacks form new models of univalent type theory. By appropriate choices of $\mathcal{D}$ and covering relations, we can get various consistency and independence results, generalizing to univalent type theory the use of sheaf models for higher order logic.

References

[1] P. Aczel *On relating type theories and set theories*, proceedings of TYPES 1998, pp. 1-18
[2] C. Cohen, Th. Coquand, S. Huber, A. Mörberg, *Cubical type theory: a constructive interpretation of the univalence axiom*, proceedings of TYPES 2015.
[3] M. Shulman, E. Rijke and B. Spitters, *Modalities in homotopy type theory*, submitted 2017.
[4] N. Gambino and Ch. Sattler, *The Frobenius condition, right properness, and uniform fibrations*, Journal of Pure and Applied Algebra, 221 (12), 2017, pp. 3027-3068.
[5] I. Orton and A. Pitts *Axioms for Modelling Cubical Type Theory in a Topos*, CSL 2016.

The Simply Typed System $\mathcal{N}$ and Extendable Recursion

Stefano Berardi
(joint work with Ugo de' Liguoro)

We define a simply typed λ-calculus ([3]), the system $\mathcal{N}$, from a set `Data` of data types using product and arrow types. Any $D \in$ `Data` is defined from a list $(D_0, \ldots, D_{n-1})$ of previously defined data types, a definition inspired by Martin-Lof nested data types [2]. The data type D denotes the smallest set of trees we may defined with finitely many constructors $c_0, \ldots, c_{n-1}$. The constructor c_i

has argument a family of elements of D indexed on D_i, represented by some map $f : D_i \to D$. $c_i(f)$ denotes the trees whose immediate sub-trees are $f(e)$ for any $e : D_i$. For instance, $D_0 = ()$ denotes the empty set, $D_1 = (D_0)$ denotes a singleton, $D_2 = (D_0, D_1)$ denotes the set of natural number, and $D_3 = (D_0, D_1, D_2)$ the set of well-founded trees, whose nodes have no children, or one child, or ω children. Maps of system $\mathcal{N}$ are defined by primitive recursion on trees. A recursive definition of a map $h : D \to A$ includes a special clause $r : A \to A$ we call the *polymorphic clause*, to be used when the domain D of the recursive map h is extended by adding some new constructor c_n.

For sake of simplicity we use no variables in $\mathcal{N}$, but this is but an arbitrary choice. Our results include termination of computations in $\mathcal{N}$ and that fact that all trees denoted by terms of $\mathcal{N}$ are well-founded. Termination is proved by combining the notion of totality introduced by Tait [4] with the notion of candidate introduced by Girard. These proofs may be found in [1].

Our long-term goal is defining a system as expressive as Girard's system $\mathcal{F}$, but using no explicit quantification on types. In particular we plan to prove that all maps $: D \to E$ between data types definable in $\mathcal{F}$ are definable in $\mathcal{N}$, and all well-founded trees definable in $\mathcal{F}$ are definable in $\mathcal{N}$. We consider system $\mathcal{N}$ as a good candidate for writing a denotational system for the provably well-orders of second order arithmetic.

References

[1] S. Berardi, U. de' Liguoro, The Simply Typed System $\mathcal{N}$ and Extendable Recursion, Torino University, Technical Report, November 2017. *www.di.unito.it/∼ stefano/SistemaN-definizioni-14-Luglio-2017.pdf*
[2] P. Martin-Lof, Intuitionistic Type Theory, June 1980, Bibliopolis.
[3] H. Barendregt, Lambda Calculus with Types. Cambridge University Press, 2013.
[4] William W. Tait: Intensional Interpretations of Functionals of Finite Type I. J. Symb. Log. 32(2): 198-212 (1967)

Recent advances in homotopy type theory

Nicola Gambino
(joint work with Christian Sattler)

Many of the connections between type theory and homotopy theory considered in Homotopy Type Theory Univalent Foundations of Mathematics involve the notions of a groupoid and of an ∞-groupoid (i.e. Kan complex). Recall that a *groupoid* is a category in which every morphism is invertible. Examples of groupoids abound: a group is essentially the same thing as a groupoid with a single object (with the morphisms of the groupoid being the elements of the group) and every set X with an equivalence relation R determines a groupoid having X as its set of objects and a unique morphism from x to y if and only if $(x, y) \in R$. Groupoids arise naturally in mathematics whenever there are equivalence relations for which taking a quotient in the most naive way is not suitable (cf. the development of the theory of stacks and higher stacks in algebraic geometry).

The connection between groupoids and type theory arose with the following fundamental result [4].

Theorem 1 (Hoffmann and Streicher, 1995)**.** *Martin-Löf type theory admits a model in the the category* **Gpd** *of groupoids and functors. Furthermore, the principle of Uniqueness of Identity Proofs is not valid in this model.*

In the groupoid model, types are interpreted as groupoids and dependent types as *isofibrations*, i.e. functors that satisfy a suitable version of the path-lifting property that defines fibrations of topological spaces. In their paper, Hofmann and Streicher showed also that a form of the Univalence Axiom was valid and suggested the possibility of using ∞-groupoids to obtain an even more informative model of type theory.

This suggestion was not taken up until Voevodsky showed how one could use the notion an ∞-groupoid studied in algebraic topology under the name of *Kan complex* to obtain a model of Martin-Löf type theory [5]. Kan complexes are defined as particular simplicial sets, which are familes of sets $X = (X_n)_{n\in\mathbb{N}}$ equipped with suitable maps that allow us to think of X as a space and of elements $x \in X_n$ as n-dimensional simplices making up the space.

Theorem 2 (Voevodsky, 2008)**.** *Martin-Löf type theory admits a model in the the category* **SSet** *of simplicial sets. Furthermore, the univalence axiom is valid in this model.*

In the simplicial model, types are interpreted as Kan complexes and dependent types are interpreted as *Kan fibrations*, which are a simplicial counterpart of topological fibrations. The validity of all the rules of type theory in the simplicial model combines a series of well-known facts from homotopy theory and some new concepts, such as that of a univalent fibration. In its original version, the proof of Theorem 2 was obtained working in ZFC extended with two inaccessible cardinals. Because of this, researchers began to investigate whether a constructive version of that result could be established. This turned out to be impossible, as the following result in [2] shows.

Theorem 3 (Bezem, Coquand and Parmann, 2014)**.** *It is not possible to show constructively that if X and Y are Kan complexes, then their exponential Y^X in* **SSet** *is again a Kan complex.*

In order to overcome this obstacle, Bezem, Coquand and Huber developed a model of Martin-Löf type theory using a variant of simplicial sets called *cubical sets*, obtaining the following result working in a constructive metatheory [1].

Theorem 4 (Bezem, Coquand, Huber, 2015)**.** *Martin-Löf type theory admits a model in the the category* **CSet** *of cubical sets. Furthermore, the univalence axiom is valid in this model.*

In the cubical model, dependent types are interpreted as *uniform Kan fibrations*, which are not just morphisms of cubical sets satisfying a lifting property,

like the standard Kan fibrations used in Voevodsky's simplicial model, but rather morphisms of cubical sets that come equipped with additional structure (which provides explicit solutions for the lifting problems, subject to a further naturality condition).

There is then a question of whether it was the switch from simplicial to cubical sets or the switch from standard to uniform fibrations that is essential to overcome the constructive obstruction of Theorem 3. As shown in joint work with Christian Sattler, that specific issue can be overcome remaining in the category of simplicial sets, but working with uniform fibrations. More precisely, the following result is proved in [3].

Theorem 5 (Gambino and Sattler, 2017)**.** *It is possible to show constructively that if X and Y are uniform Kan complexes, then their exponential Y^X in* **SSet** *is again a uniform Kan complex.*

While Theorem 5 provides a constructive version of a fragment of the simplicial model of type theory, it does not address the validity of the rules concerning universes, for which there are further constructivity issues. These issues remain to be explored; one promising direction, currently being investigated in joint work with Christian Sattler, is that of prismatic sets.

References

[1] M. Bezem, T. Coquand, S. Huber, *A Model of Type Theory in Cubical Sets*. In *19th International Conference on Types for Proofs and Programs (TYPES 2013)*, volume 26 of Leibniz International Proceedings in Informatics (LIPIcs), pages 107–128, 2014.

[2] M. Bezem, T. Coquand, E. Parmann, *Non-Constructivity in Kan Simplicial Sets*. In *13th International Conference on Typed Lambda Calculi and Applications (TLCA 2015)*, volume 38 of Leibniz International Proceedings in Informatics (LIPIcs), pages 92–106, 2015.

[3] N. Gambino and C. Sattler, *The Frobenius condition, right properness, and uniform fibrations* Journal of Pure and Applied Algebra, 221 (12), 2017, pp. 3027-3068.

[4] M. Hofmann and T. Streicher, *The groupoid model of type theory*, In *Twenty-five years of Constructive Type Theory*, Oxford University Press, 1995.

[5] C. Kapulkin and P. Lumsdaine, *The simplicial model of univalent foundations (after Voevodsky)*, arXiv:1211.2851v4, 2016.

Geometric theories for constructive algebra

Henri Lombardi

Introduction. We discuss the use of geometric theories in a constructive framework (Bishop style constructive mathematics, i.e. mathematics with intuitionistic logic [3–5, 12, 13, 16]).

In a classical framework, a good reference for geometric theories is [11, Chapter D1], see also [2] and [6]. Here we shall use constructive logic not only as the internal language of toposes, but also for the investigation of the whole mathematical world. E.g. the usual model theory is not valid anymore and its results have to be deciphered in a constructive way.

Our aim is to investigate whether geometric theories are sufficient for fully developing constructive algebra as e.g. in [12, 13, 16].

Our motivation is twofold. First, the deduction rules in geometric theories are extremely simple when used in dynamical proofs as explained in [9]. So geometric theories can be seen as purely computational, without logic. As a consequence, there is no conflict between classical and constructive mathematics about valid dynamical rules ("geometric theorems"). So using in a systematic way geometric theories is part of the general program of rereading constructively classical proofs and theorems in order to make their hidden constructive content explicit ([1, 7–9, 12, 15, 16]).

Another important goal is to describe as completely as possible the algebraic properties of $\mathbb{R}$ (including the usual o-minimal structures). Note that the real number field is not a discrete real closed field since there is no sign test for constructive real numbers. So the main algorithms of discrete real closed fields do not work constructively for real numbers. On this subject see (in French) `http://hlombardi.free.fr/Reels-geometriques.pdf`.

1. Hilbert's program revisited

References: [7, 9, 10, 12, 14]. Seminal papers are [10, 14].

The aim is to give a general method for deciphering the computational content of theorems in classical mathematic whose proof use nonconstructive principles as LEM and ZFC.

Examples. Consider some important classical nonconstructive theorems. E.g.

(1) Any field can be embedded in an algebraically closed field.
(2) Any real field can be ordered.
(3) If $\mathbf{K} \subseteq \mathbf{L}$ are fields and $\mathbf{V} \subseteq \mathbf{K}$ is a valuation ring of $\mathbf{K}$, there exists a valuation ring $\mathbf{W}$ of $\mathbf{L}$ such that $\mathbf{W} \cap \mathbf{K} = \mathbf{V}$.
(4) Let $\mathbf{A}$ be a commutative ring. Consider a linear system $AX = C$ over $\mathbf{A}$. If it has a solution in any localisation $\mathbf{A}_{\mathfrak{p}}$, then it has a solution in $\mathbf{A}$ (elementary local-global principle).
(5) Galois theory of a separable polynomial ...

Possible constructive rereadings are e.g.

(1) [10] Let $\mathbf{K}$ be a commutative ring. Consider $\mathbf{K}$ as giving a dynamic algebraic structure of algebraically closed field. This works! More precisely, if $1 = 0$ in the dynamic structure, then $1 = 0$ in $\mathbf{K}$.
(2) [9] Let $\mathbf{K}$ be a real field. Consider $\mathbf{K}$ as giving a dynamic algebraic structure of ordered field. This works! More precisely, don't assume $\mathbf{K}$ to be real, if $1 = 0$ in the dynamic structure, then -1 is a sum of squares in $\mathbf{K}$.
(3) [9] If $\mathbf{K} \subseteq \mathbf{L}$ are fields and $\mathbf{V} \subseteq \mathbf{K}$ is a valuation ring of $\mathbf{K}$, consider $\mathbf{L}$ as a dynamical valued field with a valuation ring $\mathbf{W}$ such that $\mathbf{W} \cap \mathbf{K} = \mathbf{V}$. This works! More precisely, if $1 = 0$ in the dynamic structure, then $1 = 0$ in $\mathbf{K}$.
(4) [12] Elementary constructive local-global principle. Either

- consider **A** as giving a dynamic algebraic structure of local ring, if you find a solution of the linear system, you can also obtain solution in **A**; or
- consider **A** as giving a dynamic algebraic structure of local ring with a discrete residue field, if you find a solution of the linear system, you can also obtain solution in **A**; or
- replace localisation at any prime by localisation at finitely many comaximal elements.

(5) [12] Dynamical Galois theory of a separable polynomial ...

2. First-order geometric theories

Main reference: [9].

Dynamical theories and dynamical algebraic structures give a constructive understanding, without logic, of *coherent theories*, i.e. of *first-order geometric theories*.

First we insist on the following strong conservation result [9, Theorem 1.1].

Theorem 1. *Let $\mathcal{T}$ be a dynamical theory, $(G;R)$ a presentation of a dynamical algebraic structure* **A** *and $B(\mathbf{t})$ a fact of* **A**. *There is a construction associating to every proof of $R \vdash B(\mathbf{t})$ in the classical first-order theory corresponding to $\mathcal{T}$ a dynamical proof of $B(\mathbf{t})$.*

In other words, the extension of the purely computational theory $\mathcal{T}$ by means of connectors, quantifiers and classical logic, is conservative.

Note that this important result is not sufficient for deciphering all concrete results obtained via model theory in classical mathematics. In fact, classical mathematics may use very "strong" properties of ZFC in order to prove some facts about models of a first-order theory, and deduce in a nonconstructive way the existence of a proof of a theorem in the formal theory. Theorem 1 allows us only to transform this hypothetic proof in a dynamical one.

3. Infinitary geometric theories

Infinitary geometric theories have a much greater expressive power than first-order geometric theories.

E.g. it becomes possible to speak "geometrically" of the non-first-order crucial notions of flatness, Krull dimension, coherence, depth, Krull and Dedekind domains, Galois algebras, and so on.

An analogue of Theorem 1 for infinitary geometric theories is a theorem due to Barr.

Unfortunately the proof of this theorem cannot be made constructive, so that it serves only as heuristic. But this heuristic works in practice.

References

[1] M. E. Alonso, T. Coquand, and H. Lombardi. Revisiting Zariski main theorem from a constructive point of view. *J. Algebra*, 406:46–68, 2014.

[2] Thomas William Barrett and Hans Halvorson. Morita equivalence. `http://arxiv.org/abs/1506.04675`. Manuscript, 2015.

[3] Errett Bishop. *Foundations of constructive analysis*. McGraw-Hill, New York, 1967.

[4] Errett Bishop and Douglas Bridges. *Constructive analysis*, volume 279 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1985.

[5] Douglas Bridges and Fred Richman. *Varieties of constructive mathematics*, volume 97 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1987.

[6] Olivia Caramello. *Theories, Sites, Toposes*. Oxford University Press, 2017.

[7] Thierry Coquand and Henri Lombardi. A logical approach to abstract algebra. *Math. Structures Comput. Sci.*, 16(5):885–900, 2006.

[8] Thierry Coquand and Claude Quitté. Constructive finite free resolutions. *Manuscripta Math.*, 137(3-4):331–345, 2012.

[9] Michel Coste, Henri Lombardi, and Marie-Françoise Roy. Dynamical method in algebra: effective Nullstellensätze. *Ann. Pure Appl. Logic*, 111(3):203–256, 2001.

[10] Jean Della Dora, Claire Dicrescenzo, and Dominique Duval. About a new method for computing in algebraic number fields. In *EUROCAL '85. Lecture Notes in Computer Science no. 204, (Ed. Caviness B.F.)*, pages 289–290. Springer, Berlin, 1985.

[11] Peter T. Johnstone. *Sketches of an elephant: a topos theory compendium. Vol. 2*, volume 44 of *Oxford Logic Guides*. The Clarendon Press, Oxford University Press, Oxford, 2002.

[12] Henri Lombardi and Claude Quitté. *Commutative algebra: constructive methods*, volume 20 of *Algebra and Applications*. Springer, Dordrecht, revised edition, 2015. Translated from the French (Calvage & Mounet, 2011, revised and extended by the authors) by Tania K. Roblot.

[13] Ray Mines, Fred Richman, and Wim Ruitenburg. *A course in constructive algebra*. Universitext. Springer-Verlag, New York, 1988.

[14] Dag Prawitz. Ideas and results in proof theory. In *Proceedings of the Second Scandinavian Logic Symposium (Univ. Oslo, Oslo, 1970)*, pages 235–307. Studies in Logic and the Foundations of Mathematics, Vol. 63. North-Holland, Amsterdam, 1971.

[15] Ihsen Yengui. Making the use of maximal ideals constructive. *Theoret. Comput. Sci.*, 392(1-3):174–178, 2008.

[16] Ihsen Yengui. *Constructive commutative algebra*, volume 2138 of *Lecture Notes in Mathematics*. Springer, Cham, 2015. Projective modules over polynomial rings and dynamical Gröbner bases.

Abstract Cut Elimination

Peter Schuster
(joint work with Davide Rinaldi and Daniel Wessel)

The background of this work is the partial realisation of Hilbert's programme for abstract algebra (Coquand, Lombardi et al.) in constructive mathematics with, e.g., constructive set theory **CZF**. A constructive version of an abstract theorem is "*a theorem the proof of which is constructive, which has a clear computational content, and from which we can recover the usual version of the abstract theorem by an immediate application of a well-classified non-constructive principle*" [2].

Many an abstract theorem is an extension principle, e.g., a variant of the prime ideal theorem, asserting the pure existence of an ideal object by invoking Zorn's Lemma. Turning one of these semantic extension theorems "upside down"—in logical terms, as completeness rather than satisfiability—often prompts not only a proof [8] rather by Open Induction [7], but even a reformulation as a syntactical conservation theorem that has a constructive proof [1, 4, 5, 9, 10].

To represent ideal objects in algebra syntactically, *entailment relations* have proved utmost versatile [1]. This abstract form of sequent calculus goes back to Hertz, Carnap and Tarski for the single-conclusion case, and to Gentzen, Lorenzen and Scott for the multi-conclusion case. Here we focus on cut elimination for entailment relations, by which we can compare entailment relations systematically.

1. Cut elimination for entailment relations

Let S be an *arbitrary* set; its elements $a, b, \ldots$ are seen as *abstract sentences*. Uppercase letters $A, B, \ldots$ denote elements of $\mathrm{Fin}(S)$, i.e. finite subsets of S.

Definition 1 ([11])**.** *An* entailment relation *on S is a relation $\vdash \subseteq \mathrm{Fin}(S) \times \mathrm{Fin}(S)$ satisfying, for all $c \in S$ and finite subsets A, A', B, B' of S, the three* basic rules*:*[2]

$$\frac{A \between B}{A \vdash B}\ (R) \qquad \frac{A \vdash B}{A, A' \vdash B, B'}\ (M) \qquad \frac{A \vdash B, c \quad A', c \vdash B'}{A, A' \vdash B, B'}\ (T)$$

Notice that the definition of $\vdash$ is symmetric. Both in antecedent and succedent, comma stands for union, etc.; for instance, A, c is shorthand for $A \cup \{c\}$. While abstract sentences need not be formulas [11], the *intended reading* is as for Gentzen sequents: conjunctively on the left, disjunctively on the right. So the empty set or empty space means truth on the left and falsity on the right. Also, $a \in S$ may be viewed as $P(a)$ where P is the relevant predicate on the given set S.

Entailment relations arising from mathematical practice can typically be defined by imposing the conditions $C_j \vdash D_j$, called *axioms*, they are expected to satisfy. The entailment relation $\vdash$ *generated by axioms* $(C_j \vdash D_j)_{j \in J}$ satisfies

1. $C_j \vdash D_j$ for all $j \in J$;
2. if an entailment relation $\vdash'$ satisfies $C_j \vdash' D_j$ for all $j \in J$, then $\vdash \subseteq \vdash'$.

Every entailment relation $\vdash$ on S is trivially generated by $\{(A, B) : A \vdash B\}$. But normally finitely many axioms—or rather *axiom schemes*—will do. So *inductive generation* is possible: just close the axioms under the basic rules.

Lemma 2. *The entailment relation generated by the axioms $(C_j \vdash D_j)_{j \in J}$ equals the entailment relation $\vdash$ generated by the corresponding* axiom rules

$$\frac{A, d^j_1 \vdash B \quad \ldots \quad A, d^j_{m_j} \vdash B}{A, C_j \vdash B}\ (Ax_j)$$

on top of the basic rules where $D_j = \{d^j_1, \ldots, d^j_{m_j}\}$ for every $j \in J$.

[2]When we write and speak of rules we mean provability or validity rather than admissibility.

Of course this is not altogether new, nor is the consequence that $A \vdash B$ if and only if one can grow a *proof tree* π with root $A \vdash B$ by the rules (R), (M), (T) and (Ax_j). Let π be a proof tree for $A \vdash B$. Notice that

1. at the leaves there can only be instances of (R), or of (Ax_j) with empty premise corresponding to axioms $C_j \vdash D_j$ with empty conclusion;

2. every application of (M) can be lifted along each branch such that it will eventually be absorbed by (R); whence (M) can be eliminated.

Theorem 3. *Let $\vdash$ be an entailment relation generated by axioms $(C_j \vdash D_j)_{j\in J}$. For every proof tree π for $\vdash$ there is a proof tree π' for $\vdash$ that is free from (T).*

The main idea is the same as for *cut elimination in the presence of axioms* [6].

Corollary 4. *The entailment relation $\vdash$ generated by axioms $(C_j \vdash D_j)_{j\in J}$ equals the relation (!) generated by the rule (R) and all axiom rules (Ax_j) with $j \in J$.*

This can equally be achieved by the *hyperresolution rule* [3].

2. Comparing entailment relations systematically

Let entailment relations $\vdash$ and $\vdash'$ on a set S be generated as follows:

1. $\vdash$ by the axioms $(C_j \vdash D_j)_{j\in J}$ where $D_j = \{d_1^j, \ldots, d_{m_j}^j\}$;

2. $\vdash'$ by the axioms $(C'_k \vdash' D'_k)_{k\in K}$ where $D'_k = \{d_1'^k, \ldots, d_{m'_k}'^k\}$.

Let $B \in \mathrm{Fin}(S)$; we say that $\vdash$ and $\vdash'$ *prove B simultaneously* if

$$A \vdash B \iff A \vdash' B$$

for all $A \in \mathrm{Fin}(S)$. In particular, we say that $\vdash$ and $\vdash'$

1. *prove the same facts* if they prove $\{c\}$ simultaneously for all $c \in S$;

2. *collapse simultaneously* if they prove $\emptyset$ simultaneously.

The names of these concepts are translations from *dynamical algebra* [4], where already a wealth of algebraic instances has been settled.

Lemma 5. *Let $B \in \mathrm{Fin}(S)$. If $\vdash'$ satisfies the axiom rules for $\vdash$ relative to B, i.e.*

$$\frac{A, d_1^j \vdash' B \quad \ldots \quad A, d_{m_j}^j \vdash' B}{A, C_j \vdash' B}\ (P_j^B)$$

for all $j \in J$ and $A \in \mathrm{Fin}(S)$, then $A \vdash B$ implies $A \vdash' B$.

Theorem 6. *Let $B \in \mathrm{Fin}(S)$. The entailment relations $\vdash, \vdash'$ prove B simultaneously if and only if each of them satisfies the axiom rules for the other relative to B, that is, for all $j \in J$, $k \in K$, and $A \in \mathrm{Fin}(S)$ we have*

$$\frac{A, d_1^j \vdash' B \quad \ldots \quad A, d_{m_j}^j \vdash' B}{A, C_j \vdash' B}\ (P_j^B) \qquad \frac{A, d_1'^k \vdash B \quad \ldots \quad A, d_{m'_k}'^k \vdash B}{A, C'_k \vdash B}\ (P_k'^B)$$

Corollary 7. *The entailment relations $\vdash$ and $\vdash'$ prove the same facts if and only if for all $j \in J$, $k \in K$, $A \in \mathrm{Fin}(S)$ and $c \in S$ we have*

$$\frac{A, d_1^j \vdash' c \quad \ldots \quad A, d_{m_j}^j \vdash' c}{A, C_j \vdash' c}\ (P_j^c) \qquad \frac{A, d_1'^k \vdash c \quad \ldots \quad A, d_{m'_k}'^k \vdash c}{A, C'_k \vdash c}\ (P_k'^c)$$

Corollary 8. *The entailment relations $\vdash$ and $\vdash'$ collapse simultaneously if and only if for all $j \in J$, $k \in K$ and $A \in \mathrm{Fin}(S)$ we have*

$$\frac{A, d_1^j \vdash' \quad \dots \quad A, d_{m_j}^j \vdash'}{A, C_j \vdash'} \; (P_j^{\emptyset}) \qquad \frac{A, d_1'^k \vdash \quad \dots \quad A, d_{m'_k}'^k \vdash}{A, C'_k \vdash} \; (P_k'^{\emptyset})$$

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] Thierry Coquand and Henri Lombardi. Hidden constructions in abstract algebra (3): Krull dimension of distributive lattices and commutative rings. In M. Fontana, S.-E. Kabbaj, and S. Wiegand, editors, *Commutative Ring Theory and Applications*, volume 231 of *Lect. Notes Pure Appl. Mathematics*, pages 477–499, Reading, MA, 2002. Addison-Wesley.

[3] Thierry Coquand and Guo-Qiang Zhang. Sequents, frames, and completeness. In Peter G. Clote and Helmut Schwichtenberg, editors, *Computer Science Logic (Fischbachau, 2000)*, volume 1862 of *Lecture Notes in Comput. Sci.*, pages 277–291. Springer, Berlin, 2000.

[4] Michel Coste, Henri Lombardi, and Marie-Françoise Roy. Dynamical method in algebra: Effective Nullstellensätze. *Ann. Pure Appl. Logic*, 111(3):203–256, 2001.

[5] Christopher J. Mulvey and Joan Wick-Pelletier. A globalization of the Hahn-Banach theorem. *Adv. Math.*, 89:1–59, 1991.

[6] Sara Negri and Jan von Plato. Cut elimination in the presence of axioms. *Bull. Symb. Log.*, 4(4):418–435, 1998.

[7] Jean-Claude Raoult. Proving open properties by induction. *Inform. Process. Lett.*, 29(1):19–23, 1988.

[8] Davide Rinaldi and Peter Schuster. A universal Krull-Lindenbaum theorem. *J. Pure Appl. Algebra*, 220:3207–3232, 2016.

[9] Davide Rinaldi, Peter Schuster, and Daniel Wessel. Eliminating disjunctions by disjunction elimination. *Indag. Math. (N.S.)*, 2017. Virtual Special Issue – L.E.J. Brouwer, fifty years later. Communicated first in *Bull. Symb. Logic* 23 (2017), 181–200.

[10] Davide Rinaldi and Daniel Wessel. Some constructive extension theorems for distributive lattices. Technical report, University of Verona and University of Trento, 2017. Submitted.

[11] Dana Scott. Completeness and axiomatizability in many-valued logic. In Leon Henkin, John Addison, C.C. Chang, William Craig, Dana Scott, and Robert Vaught, editors, *Proceedings of the Tarski Symposium (Proc. Sympos. Pure Math., Vol. XXV, Univ. California, Berkeley, Calif., 1971)*, pages 411–435. Amer. Math. Soc., Providence, RI, 1974.

Logic for exact real arithmetic

Helmut Schwichtenberg

(joint work with Ulrich Berger, Kenji Miyamoto and Hideki Tsuiki)

Real numbers in the exact (as opposed to floating-point) sense can be given in different formats, for instance as Cauchy sequences (of rationals, with Cauchy modulus), or else as infinite sequences (streams) of (i) signed digits -1, 0, 1 or (ii) -1, 1, $\perp$ containing at most one copy of $\perp$ (meaning undefinedness), so-called Gray code ([2], [3], [1]). We are interested in formally verified algorithms on real numbers given as streams. To this end we consider formal (constructive) existence proofs M

and apply a proof theoretic method (realizability) to extract their computational content. We switch between different representations of reals by labelling universal quantifiers on reals x as non-computational and then relativising x to a predicate ${}^{\mathrm{co}}I$ coinductively defined in such a way that the computational content of x in ${}^{\mathrm{co}}I$ is a stream representing x. The desired algorithm is obtained as the extracted term of the existence proof M, and the required verification is provided by a formal soundness proof of the realizability interpretation. As an example we consider multiplication of reals.

References

[1] 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.

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

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

Quotient rings $\mathcal{M}/n\mathcal{M}$ of models of $\mathcal{P}A$: axioms and structure of definable sets

Angus Macintyre

(joint work with Paola d'Aquino)

B. Zilber used nonstandard integers $n \equiv 1$ modulo all *standard* k, in his work on the model theory of Weyl and Heisenberg algebras. He raised some questions about $\mathcal{M}/n\mathcal{M}$, where $\mathcal{M}$ is a nonstandard model of *true arithmetic* and n is as above.

We study the general case of $\mathcal{M}/n\mathcal{M}$, where $\mathcal{M}$ is a nonstandard model of $\mathcal{P}A$, and n is an infinite element of $\mathcal{M}$. We prove that the class of all such rings $\mathcal{M}/n\mathcal{M}$, as $\mathcal{M}$, n vary, is decidable and has a quantifier - elimination (of quite high complexity). We gave axioms for the class, and show that all such $\mathcal{M}/n\mathcal{M}$ are pseudofinite. The $\mathcal{M}/n\mathcal{M}$ are exactly the rings elementarily equivalent to infinite ultraproducts of rings $\mathbb{Z}/k\mathbb{Z}$.

From the pseudofiniteness it follows that no theory in which some definable $1-1$ function is not surjective can be interpreted as any $\mathcal{M}/n\mathcal{M}$. This answers Zilber's original question (about interpretability of *arithmetic* in some $\mathcal{M}/n\mathcal{M}$) in an extremely negative way.

Our analysis is in three stages.

Stage 1 - n prime. By putting Bombieri's elementary proof of the Riemann Hypothesis for curves into $\mathcal{P}A$ (Macintyre, 1978) one can use Ax's great work of 1968 to get axioms, simplicity of the theories, and pseudofiniteness.

Stage 2 - n a power of a prime. Now one shows, by Ax and some model theory of $\mathcal{P}A$, that $\mathcal{M}/n\mathcal{M}$ is isomorphic to a quotient ring of a Henselian valuation ring V with residue field pseudofinite of characteristic 0, and value group a $\mathbb{Z}$-group.

No *thorough* analysis of such rings has been given before. We get axioms and pseudofiniteness using Denef-Pas, and get the NTP_2 property by Cemikov, Kaplan and Simon.

Stage 3 - n divisible by several primes. Here we get the required results by Stage 2 and a refinement of Feferman-Vaught. At Stage 3 (in the general case) the $\mathcal{M}/n\mathcal{M}$ have TP_2, and so w ego beyond neostability. Despite this, Feferman-Vaught gets us to an illuminating set of axioms and a quantifier-elimination.

Reporter: Thomas Powell