Mathematisches Forschungsinstitut Oberwolfach

Report No. 52/2014

DOI: 10.4171/OWR/2014/52

Mathematical Logic: Proof theory, Constructive Mathematics

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

16 November – 22 November 2014

Abstract. The workshop "Mathematical Logic: Proof Theory, Constructive Mathematics" was centered around proof-theoretic aspects of current mathematics, constructive mathematics 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 16-22, 2014 and included two tutorials:

(1) Thierry Coquand: Univalent Foundation and Constructive Mathematics (2 times 1 hour),
(2) Ulrich Kohlenbach, Daniel Körnlein, Angeliki Koutsoukou-Argyraki, Laurenţiu Leuştean: Proof-Theoretic Methods in Nonlinear Analysis (2 times 50 min plus 2 times 30).

Coquand's tutorial gave a general introduction on the univalent foundation program of Voevodsky and discussed the construction of the cubical set model of type theory in a constructive metatheory. This model satisfies the computation rules for equality introduced by P. Martin-Löf as judgemental equality.
The second tutorial developed the proof-theoretic framework for the unwinding of proofs in nonlinear analysis and outlined recent applications to: image recovery problems (Part I, Kohlenbach), fixed point theory of pseudocontractive mappings

(Part II, Körnlein), convex optimization (Part III, Leuştean) and abstract Cauchy-problems given by accretive operators (Part IV, Koutsoukou-Argyraki).

In addition to these tutorials, 29 talks of mostly 25 minutes were given aiming:

To promote the interaction of proof theory and computability theory with core areas of mathematics as well as computer science via the use of proof interpretations. J. Avigad's talk studied the amount of algorithmic randomness needed in Weyl's theorem on uniform distributions. H. Towsner showed how to arrive at Tao's version of Szemerédi's regularity lemma as the functional interpretation of a measure-theoretic Π_3-statement. H. Schwichtenberg reported on a machine extracted program from the Nash-Williams minimal bad sequence argument for Higman's lemma. V. Brattka introduced a concept of Las Vegas computable functions to calibrate the computational power of randomized computations on real numbers. A. Weiermann described a general formula for the computation of the maximal order types for well quasi orders arising in the combinatorics of finite multisets. P. Schuster showed how a reformulation of transfinite methods in algebra as admissible rules can be used to eliminate uses of such methods from proofs of sufficiently simple statements in abstract algebra. On the side of applications to concrete applications in computer science, M. Seisenberger reported on applications of logic to the verification of railway control systems and U. Berger developed a proposal to optimize programs extracted by proof-theoretic methods to be able to e.g. control their complexity, allow for partial data and to override data that are no longer used.

To further develop foundational aspects of proof theory and constructive mathematics. S. Artemov talked on intuitionistic epistemic logic which is based on the BHK-semantics and treats intuitionistic knowledge as the result of a verification. F. Aschieri reported on a new proof-theoretic method to extract Herbrand disjunctions from classical first-order natural deduction proofs. B. Afshari's talk also studied Herbrand's theorem, this time in terms of certain tree grammars assigned to proofs of existential statements in first-order logic. The talk by G.E. Leigh addressed the issue of cut-elimination for first-order theories of truth. P. Oliva presented new results on a game-theoretic interpretation of Spector's bar recursion, a more efficient novel variant of bar recursion and recent uses in the analysis of the Podelski-Rybalchenko termination theorem. F. Ferreira showed how a suitable functional interpretation can be used to give an ordinal analysis of Kripke-Platek set theory. B. van den Berg reported on new developments in the functional interpretation of systems of nonstandard analysis. T. Streicher talked on models of classical realizability (in the sense of J.-L. Krivine) arising from domain-theoretic models of λ-calculus with control. The talks by L.D. Beklemishev and J.J. Joosten addressed recent progress in the area of provability logic with applications to ordinal analysis. Also on the side of ordinal analysis was a talk by T. Strahm, who developed a so-called flexible type system in the spirit of S. Feferman whose strength is measured by the small Veblen ordinal. S. Berardi presented

a new rule-learning based approach to the proof-theoretic analysis of second order arithmetic. A. Bauer talked about constructive homotopy theory and models of intensional type theory. I. Petrakis proposed a formalization of so-called Bishop spaces as a constructive foundation for point-function topology. A. Swan studied the existence property for intuitionistic set theories where this property has to be understood in terms of definability. M. Rathjen reported on his recent proof of a conjecture due to Feferman which states that the continuum hypothesis CH is not definite in the technical sense that a certain semi-intuitionistic set theory does not prove CH$\vee\neg$CH.

To explore further the connections between logic and computational complexity. Talks in this area spanned the topics of propositional proof complexity, set-theoretic computation, and complexity theoretic aspects of bounded arithmetic. P. Pudlák reported on work-in-progress and new conjectures for two propositional proof systems based on integer linear programming, the cutting planes proof system and the Lovász-Schrijver proof system. N. Thapen reported new results about size and width tradeoffs for propositional resolution refutations, including new lower bounds via the colored PLS (polynomial local search) principle. S. Buss presented a new framework of polynomial-time computation for set functions based on Cobham-style limited recursion using $\in$-recursion. A. Beckmann described a proof-theoretic analysis for the polynomial-time computable set functions based on safe/normal $\in$-recursion. L. Kołodziejczyk discussed recent progress on complexity-theoretic aspects of the Paris-Wilkie problem on the relationship between bounded arithmetic, the (negation) of exponentiation, and collection.

Acknowledgement: The MFO and the workshop organizers would like to thank the National Science Foundation for supporting the participation of junior researchers in the workshop by the grant DMS-1049268, "US Junior Oberwolfach Fellows".

Workshop: Mathematical Logic: Proof theory, Constructive Mathematics

Table of Contents

Abstracts

Provability vs. computational semantics for intuitionistic logic

Sergei N. Artemov

We outline an intuitionistic view of knowledge which maintains the original Brouwer-Heyting-Kolmogorov (BHK) semantics of intuitionism and is consistent with Williamson's suggestion that intuitionistic knowledge be regarded as the result of verification. We argue that on this view co-reflection $A \to \mathbf{K}A$ is valid and reflection $\mathbf{K}A \to A$ is not; the latter is a distinctly classical principle, too strong as the intuitionistic truth condition for knowledge which is more adequately expressed by other modal means, e.g. $\neg A \to \neg\mathbf{K}A$ "false is not known."

This is a joint work of 2014 with Tudor Protopopescu a preliminary version of which can be found in [1].

We define a system of **intuitionistic epistemic logic,** IEL^-, incorporating a BHK-compliant notion of belief. The language is that of intuitionistic propositional logic augmented with the propositional operator $\mathbf{K}$. Postulates of IEL^-:

1. *Axioms and rules of propositional intuitionistic logic*
2. $\mathbf{K}(A \to B) \to (\mathbf{K}A \to \mathbf{K}B)$
3. $A \to \mathbf{K}A$.

Logic $\mathsf{IEL} = \mathsf{IEL}^- + \neg\mathbf{K}\bot$ incorporates a BHK version of knowledge.

Logic $\mathsf{IEL}^+ = \mathsf{IEL} + (\mathbf{K}\mathbf{K}A \to \mathbf{K}A)$ incorporates type-theoretical/strict knowledge, that correspond to knowledge operator given by "truncated proposition" $inh(A)$ (squash types, mono types, bracket types) in intuitiinistic type theory stating informally that type A is inhabited, i.e. has a proof. A truncated type has at most one designated proof (if A has a proof). From the epistemic point of view, $inh(A)$ behaves like a verification which certifies that A has a proof without providing a specific proof of A. The verification encoded by $inh(A)$ ends up in producing a specific object - a fixed and unique proof p of $inh(A)$. The task of verifying the claim 'A *is verified*,' reduces to checking this designated indicator p.

All three systems IEL^-, IEL, and IEL^+ are supplied with a self-explanatory Kripke semantics, with soundness/completeness theorems.

Within this framework, the knowability paradox is resolved in a constructive manner which, as we hope, reflects its intrinsic meaning.

References

[1] S. Artemov and T. Protopopescu *Intuitionistic Epistemic Logic.* Technical Report arXiv 1406.1582v1, Cornell University, June 2014.

Probabilistic Choice and Las Vegas Computability

Vasco Brattka
(joint work with Guido Gherardi and Rupert Hölzl)

We study the computational power of randomized computations on infinite objects, such as real numbers. In particular, we introduce the concept of a Las Vegas computable multi-valued function, which is a function that can be computed on a probabilistic Turing machine that receives a random binary sequence as auxiliary input. The machine can take advantage of this random sequence, but it always has to produce a correct result or to stop the computation after finite time if the random advice is not successful. With positive probability the random advice has to be successful. We characterize the class of Las Vegas computable functions in the Weihrauch lattice with the help of probabilistic choice principles and Weak Weak Kőnig's Lemma. Among other things we prove an Independent Choice Theorem that implies that Las Vegas computable functions are closed under composition. In a case study we show that Nash equilibria are Las Vegas computable, while zeros of continuous functions with sign changes cannot be computed on Las Vegas machines. However, we show that the latter problem admits randomized algorithms with weaker failure recognition mechanisms. The last mentioned results can be interpreted such that the Intermediated Value Theorem is reducible to the jump of Weak Weak Kőnig's Lemma, but not to Weak Weak Kőnig's Lemma itself. These examples also demonstrate that Las Vegas computable functions form a proper superclass of the class of computable functions and a proper subclass of the class of non-deterministically computable functions. (The preprint [5] contains most of the presented results.)

Keywords: Computable analysis, Weihrauch lattice, computability theory, reverse mathematics, randomized algorithms.

References

[1] Vasco Brattka, Matthew de Brecht, and Arno Pauly. Closed choice and a uniform low basis theorem. *Annals of Pure and Applied Logic* 163 (2012) 986–1008.
[2] Vasco Brattka and Guido Gherardi. Effective choice and boundedness principles in computable analysis. *The Bulletin of Symbolic Logic* 17(1) (2011) 73–117.
[3] Vasco Brattka and Guido Gherardi. Weihrauch degrees, omniscience principles and weak computability. *The Journal of Symbolic Logic*, 76(1) (2011) 143–176.
[4] Vasco Brattka, Guido Gherardi, and Alberto Marcone. The Bolzano-Weierstrass theorem is the jump of weak Kőnig's lemma. *Annals of Pure and Applied Logic* 163 (2012) 623–655.
[5] Vasco Brattka, Guido Gherardi, and Rupert Hölzl. Probabilistic Computability and Choice. `http://arxiv.org/abs/1312.7305` (2013) 47 pages.
[6] Vasco Brattka and Arno Pauly. Computation with advice. *Electronic Proceedings in Theoretical Computer Science* 24 (2010) 41–55.
[7] Arno Pauly. How incomputable is finding Nash equilibria? *Journal of Universal Computer Science*, 16(18) (2010) 2686–2710.

A flexible type system for the small Veblen ordinal

Thomas Strahm
(joint work with Florian Ranzi)

The small Veblen ordinal $\Theta\Omega^\omega 0$ is a well-known ordinal in proof theory; it can be described by making use of Veblen functions of arbitrary finite arity and it is the ordinal that measures the strength of Kruskal's theorem. A natural subsystem of second order arithmetic for the small Veblen ordinal is obtained by augmenting ACA_0 by Π^1_2 bar induction, see Rathjen and Weiermann [3].

We propose a natural and flexible type system FIT whose strength is measured by $\Theta\Omega^\omega 0$. The acronym FIT stands for **F**unction(al)s, **I**nductive definitions, and **T**ypes. FIT is patterned in a variant of Feferman's explicit mathematics: it contains partial combinatory logic as its operational core and builds types on top by using positive comprehension and accessibility inductive definitions. Induction on the natural numbers as well as accessible parts is given in natural type 1 level functional form.

The formulation of FIT bears some similarities with Feferman's flexible type system $\mathsf{QL}(\mathsf{F}_0\text{-}\mathsf{IR})$, see [1]. Whereas our system FIT accounts for infinitary inductive definitions, $\mathsf{QL}(\mathsf{F}_0\text{-}\mathsf{IR})$ only allows finitary inductive types. It is shown in [1] that $\mathsf{QL}(\mathsf{F}_0\text{-}\mathsf{IR})$ is a conservative extension of primitive recursive arithmetic PRA.

The lower bound proof for the novel type system FIT proceeds via a wellordering proof for each initial segment of the small Veblen number, thereby using a natural notation system which is directly based on finitary Veblen functions. The upper bound of FIT is obtained by a suitable interpretation in the subsystem of second order arithmetic based on ACA_0 and extended by the schema of ω model reflection for Π^1_3 statements; this principle is equivalent to Π^1_2 bar induction, see Jäger and Strahm [2].

References

[1] S. Feferman, *Logics for termination and correctness of functional programs II: Logics of strength PRA*, in: P. Aczel, H. Simmons, and S. S. Wainer, editors, *Proof Theory*, 195–225, Cambridge University Press, 1992.

[2] G. Jäger and T. Strahm, *Bar induction and ω model reflection*, Annals of Pure and Applied Logic **97** (1999), 221–230.

[3] M. Rathjen and A. Weiermann, *Proof-theoretic investigations on Kruskal's theorem*, Annals of Pure and Applied Logic **60** (1993), 49–88.

Higman's lemma and its computational content

Helmut Schwichtenberg
(joint work with Monika Seisenberger)

Higman's Lemma is a fascinating result in infinite combinatorics, with manyfold applications in logic and computer science, that has been proven using different methods several times. The aim of this talk is to look at Higman's Lemma from a computational point of view. We give a proof of Higman's Lemma that uses

the same combinatorial idea as Nash-Williams' indirect proof using the so-called minimal bad sequence argument, but which is constructive. For the case of a two letter alphabet such a proof was given by Coquand. Using more flexible structures, we present a proof that works for an arbitrary well-quasiordered alphabet. We report on a formalization of this proof in the proof assistant Minlog, and discuss machine extracted terms (in an extension of Goedel's system T) expressing its computational content.

References

[1] U. Berger, K. Miyamoto, H. Schwichtenberg, and M. Seisenberger. Minlog - A Tool for Program Extraction Supporting Algebras and Coalgebras. In A. Corradini, B. Klin, and C. Cîrstea, editors, *Algebra and Coalgebra in Computer Science, CALCO'11*, volume 6859 of *LNCS*, pages 393–399. Springer Verlag, Berlin, Heidelberg, New York, 2011.

[2] T. Coquand. A proof of Higman's lemma by structural induction. Unpublished Manuscript, April 1993.

[3] D. Fridlender. *Higman's Lemma in Type Theory*. PhD thesis, Chalmers University of Technology, Göteborg, 1997.

[4] C. Nash-Williams. On well-quasi-ordering finite trees. *Proc. Cambridge Phil. Soc.*, 59:833–835, 1963.

[5] M. Seisenberger. An Inductive Version of Nash-Williams' Minimal-Bad-Sequence Argument for Higman's Lemma. In *Types for Proofs and Programs*, volume 2277 of *LNCS*. Springer Verlag, Berlin, Heidelberg, New York, 2001.

[6] M. Seisenberger. *On the Constructive Content of Proofs*. PhD thesis, Mathematisches Institut der Universität München, 2003.

Uniform distribution and algorithmic randomness

Jeremy Avigad

A seminal theorem due to Weyl [2] states that if (a_n) is any sequence of distinct integers, then, for almost every $x \in \mathbb{R}$, the sequence $(a_n x)$ is uniformly distributed modulo one. In particular, for almost every x in the unit interval, the sequence $(a_n x)$ is uniformly distributed modulo one for every *computable* sequence (a_n) of distinct integers. Call such an x *UD random*. Here it is shown that every Schnorr random real is UD random, but there are Kurtz random reals that are not UD random. On the other hand, Weyl's theorem still holds relative to a particular effectively closed null set, so there are UD random reals that are not Kurtz random. These results are presented in Avigad [1].

References

[1] Jeremy Avigad. Uniform distribution and algorithmic randomness. *Journal of Symbolic Logic*, 78:334–344, 2013

[2] Hermann Weyl. Über die Gleichverteilung von Zahlen mod. Eins. *Mathematische Annalen*, 77(3):313–352, 1916.

Recent results on provability algebras

Lev D. Beklemishev

We report on two results on provability algebras recently obtained in Moscow by Daniyar Shamkanov [1] and by Fedor Pakhomov [2], respectively.

Shamkanov introduces a new 'circular' proof system for the standard provability logic GL of Gödel and Löb. A circular proof of a formula A (or of a sequent Γ) is a derivation of A in the usual sense from a set of hypotheses. Each of the hypotheses must be justified in one of the two possible ways: either it is, as in the usual case, an axiom, or it occurs strictly later in the given derivation. It is usually justly expected that such a notion of proof yields a contradictory system.

In contrast, by a careful design of the proof system that lacks the cut and the structural rules and by exploiting the fixed-point properties of the provability logic GL, Shamkanov provides a sound and complete axiomatization of GL. His system is a version of a Tait-style cut-free sequent calculus for the (weaker) modal logic K4.

Formulas are built from propositional variables, negated variables and the constants $\top$ and $\bot$ by $\wedge, \vee, \Box, \Diamond$. Sequents are multisets of formulas, treated as disjunctions. Axioms are sequents of the form $\Gamma, A, \overline{A}$ and $\Gamma, \top$. Inference rules are as follows:

$$\frac{\Gamma, \bot}{\Gamma} \qquad \frac{\Gamma, A \quad \Gamma, B}{\Gamma, A \wedge B} \qquad \frac{\Gamma, A, B}{\Gamma, A \vee B} \qquad \frac{\Gamma, \Diamond\Gamma, A}{\Diamond\Gamma, \Box A, \Delta}$$

Based on this system, Shamkanov gives a syntactic proof of the Lyndon interpolation property for GL. He has earlier obtained this result by model-theoretic arguments.

Pakhomov deals with the question of decidability of the elementary theory of the 0-generated subalgebra of the polymodal provability algebra of arithmetic. Let $\mathcal{M}$ denote the Lindenbaum boolean algebra of Peano arithmetic PA endowed by a sequence of unary operators $d_n : \mathcal{M} \to \mathcal{M}$, where d_n maps the equivalence class of a sentence A to that of a sentence naturally expressing the n-consistency of A over PA. The structure $(\mathcal{M}; d_0, d_1, \dots)$ is called the *polymodal provability algebra of* PA.

It follows from the results of Volodya Shavrukov that this structure is quite complicated, in particular its first-order theory is undecidable, even when the language is restricted to just one operator d_0. In contrast, its minimal subalgebra (generated from 0 and 1 by all the operations of the structure) is much more regular. This subalgebra has been studied in a number of papers in connection with the ordinal analysis of PA.

A few years ago we asked whether this structure has a decidable first-order theory, see [3]. Pakhomov succeeded in obtaining a positive answer to this question. His paper, in fact, develops new interesting machinery of decomposition of such algebras into some kind of products. The product construction preserves

the decidability of the first-order theory. Thus, Pakhomov's work not only provides us with the answer to the original problem, but also with a deep structural information about the algebras in question.

References

[1] D. Shamkanov, *Circular Proofs for the Gödel–Löb Provability Logic*, Math. Notes, 96:4 (2014), 575–585.
[2] F. Pakhomov, *On elementary theories of GLP-algebras*, arXiv: 1412.4439, 2014.
[3] L. Beklemishev, A. Visser, *Problems in the Logic of Provability*. In: Mathematical Problems from Applied Logics. New Logics for the XXIst Century. Edited by D. Gabbay, S. Goncharov and M. Zakharyaschev. International Mathematical Series, Springer, 2005, p. 77–136.

The Paris-Wilkie problem of the consistency of no collection and no exponentiation

Leszek Kołodziejczyk

$\mathrm{B}\Sigma_1$ is the theory extending $\mathrm{I}\Delta_0$ by all instances of the Σ_1 collection scheme, that is, by

$$\forall x < v\, \exists y\, \varphi(x,y) \Rightarrow \exists w\, \forall x < v\, \exists y < w\, \varphi(x,y),$$

where φ ranges over Σ_1 formulas. Σ_1 collection is Π_1-conservative, and frequently also Π_2-conservative, over reasonably well-behaved weak fragments of arithmetic, but it is also known to be unprovable even from the true Π_2 theory of $\mathbb{N}$ [1]. However, all proofs of this unprovability result make use of exponential-size objects (often in the form of a Σ_1 universal formula). This led Paris and Wilkie [2] to ask:

$$\text{Does } \mathrm{I}\Delta_0 + \neg\mathrm{Exp} \text{ prove } \mathrm{B}\Sigma_1? \tag{1}$$

Here Exp is an axiom expressing the totality of the exponential function. It is generally expected that the answer to the question is negative. In fact, there are some results of the form "the answer is negative under some assumptions", where the assumptions are unproved statements from computational complexity theory. Despite numerous efforts, an unconditional negative answer remains elusive.

In an attempt to explain why the Paris-Wilkie problem is so difficult, we present a complexity-theoretic statement which implies that the answer to "Does ¬Exp imply Σ_1 collection?" is actually *positive*, at least over the true Π_1 theory of $\mathbb{N}$ as the base theory:

Theorem 1. *If for every $k \in \mathbb{N}$ there is a non-decreasing time-constructible function f of fractional-exponential growth rate such that Σ_k-TIME$(f^{O(1)})$ is contained in the linear-time hierarchy, then $\Pi_1(\mathbb{N}) + \neg\mathrm{Exp} \vdash \mathrm{B}\Sigma_1$.*

In order to replace $\Pi_1(\mathbb{N})$ by $\mathrm{I}\Delta_0$ as the base theory, one has to assume that the containments are provable in $\mathrm{I}\Delta_0$, which has to be formulated in a special way and makes for a rather complicated statement. The assumption of Theorem 1 is not at all likely to be true; however, it seems plausible that disproving it might be beyond the reach of the present-day methods of complexity theory. In particular,

the assumption of Theorem 1 is designed to evade typical diagonalization-based arguments used to disprove slightly stronger statements.

We also prove a theorem which essentially says that any proof of the unprovability of a fixed *finite* fragment of Σ_1 collection in $\mathrm{I}\Delta_0 + \neg\mathrm{Exp}$ would have to be non-relativizing, in the sense that it would not work in the presence of an arbitrary oracle:

Theorem 2. *Let α be a new unary relation symbol. Then for every finite fragment $\mathrm{B}(\alpha)$ of $\mathrm{B}\Sigma_1(\alpha)$ there exists a consistent recursively axiomatized $\Pi_1(\alpha)$ theory $\mathrm{T}_\mathrm{B}(\alpha) \supseteq \mathrm{I}\Delta_0(\alpha)$ such that $\mathrm{T}_\mathrm{B}(\alpha) + \neg\mathrm{Exp} \vdash \mathrm{B}(\alpha)$.*

To prove Theorem 2, we have to go through a lemma in pure computational complexity theory: for every k, there exists an oracle relative to which the k-th level of the exponential time hierarchy, i.e. Σ_k-TIME$(2^{O(n)})$, is contained in the linear-time hierarchy.

References

[1] C. Parsons, *On a number-theoretic choice schema and its relation to induction*, in: A. Kino, R.E. Vesley, J. Myhill, editors, *Intuitionism and Proof Theory. Proceedings of the Summer Conference at Buffalo, N.Y., 1968*, pages 459–473. North-Holland, 1970.

[2] A. Wilkie and J. Paris, *On the existence of end-extensions of models of bounded induction*, in: J.E. Fenstad, I.T. Frolov, and R. Hilpinen, editors, *Logic, Methodology, and Philosophy of Science VIII (Moscow 1987)*, pages 143–161. North-Holland, 1989.

Proof-theoretic methods in nonlinear analysis I: Logical Foundations and Some Applications

Ulrich Kohlenbach

During the last two decades a systematic program of 'proof mining' emerged as a new applied form of proof theory and has successfully been applied to a number of areas of core mathematics ([3]). This program has its roots in Georg Kreisel's pioneering ideas of 'unwinding of proofs' going back to the 1950's.

We are primarily concerned with the extraction of hidden finitary and combinatorial content from proofs that make use of infinitary noneffective principles. The main logical tools for this are so-called proof interpretation. Logical metatheorems based on such interpretations have been applied with particular success in the context of nonlinear analysis including fixed point theory, ergodic theory, continuous optimization and - most recently - abstract Cauchy problems. The combinatorial content can manifest itself both in explicit effective bounds as well as uniformity results.

In this first part of a tutorial on proof mining we will

- outline the general background of this proof-theoretic approach,
- report on recent results (with D. Günzel, [1]) adapting the framework to the treatment of abstract L^p- and $C(K)$-spaces and bands in the $L^p(L^q)$-lattice and clarifying its relation to the model-theoretic work in the context of continuous or positive bounded logic (see e.g. [2]),

- and indicate some recent applications (with M.A.A. Khan) in the context of nonlinear analysis ([4, 5]).

Further applications will be discussed in Parts II-IV of the tutorial by D. Körnlein, A. Koutsoukou-Argyraki and L. Leuştean.

Acknowledgment: The author was supported by the German Science Foundation (DFG Project KO 1737/5-2).

References

[1] D. Günzel, U. Kohlenbach, *Logical metatheorems for abstract spaces axiomatized in positive bounded logic*, Preprint 2014.
[2] C.W. Henson, J. Iovino, *Ultraproducts in analysis*. In: Analysis and Logic, London Math. Soc. Lecture Note Ser. *262* (2002), 1–115.
[3] U. Kohlenbach, *Applied Proof Theory: Proof Interpretations and their Use in Mathematics*. Springer Monograph in Mathematics, xx+536pp., 2008.
[4] M.A.A. Khan, U. Kohlenbach, *Bounds on Kuhfittig's iteration schema in uniformly convex hyperbolic spaces*, J. Math. Anal. Appl. **403** (2013), 633–642.
[5] M.A.A. Khan, U. Kohlenbach, *Quantitative image recovery theorems*, Nonlinear Analysis **106** (2014), 138–150.

Proof-theoretic methods in nonlinear analysis II: Fixed Point Theory

Daniel Körnlein

This is the third part of a tutorial on proof mining, in which we discuss applications of proof mining to metric fixed point theory. In fixed point theory, a general problem of interest is the following. Given an operator $T : X \to X$ which has a fixed point $p = Tp$, find a suitable explicit iteration scheme $x_{n+1} = f_n(x_n, T)$ that converges to a fixed point of T. In these situations, rates of convergence, i.e. bounds on the existential quantifier in the convergence statement, do not exist.

In fact, Avigad, Gerhardy and Towsner [1] have shown that, in the context of von Neumann's Mean Ergodic Theorem, the ergodic averages do not have a computable rate of convergence. This already rules out effective rates for many of the iterations used in fixed point theory. Recently, E. Neumann [5] obtained further results in this vein. However, logical metatheorems [2] guarantee the extractability of rates of metastability Φ in the sense of Tao [6]:

$$\forall k^{\mathbb{N}}, g^{\mathbb{N}\to\mathbb{N}} \exists n \leq \Phi(k, g) \forall i, j \in [n; n + g(n)](\|x_i - x_j\| \leq 2^{-k}).$$

We present two recent examples of metastability results for pseudocontractive mappings in Hilbert space [3, 4].

Acknowledgment: The author was supported by the German Science Foundation (DFG Project KO 1737/5-2).

References

[1] J. Avigad and P. Gerhardy and Henry Towsner, *Local stability of ergodic averages*, Trans. Amer. Math. Soc. (2010)

[2] U. Kohlenbach, *Applied Proof Theory: Proof Interpretations and their Use in Mathematics*. Springer Monograph in Mathematics, xx+536pp., 2008.

[3] D. Körnlein, U. Kohlenbach, *Rate of Metastability for Bruck's iteration of pseudocontractive mappings in Hilbert space*, Numer. Funct. Anal. Optim. **35** (2014), 20–31

[4] D. Körnlein, *Quantitative results for Bruck iterations of demicontinuous pseudocontractions*, submitted

[5] E. Neumann, *Computational Problems in Metric Fixed Point Theory and their Weihrauch Degrees*, Master Thesis 124pp., Technische Universität Darmstadt, 2014.

[6] T. Tao, *Soft analysis, hard analysis, and the finite convergence principle*, Essay posted May 23, 2007, appeared in: T. Tao, Structure and Randomness: Pages from Year One of a Mathematical Blog, AMS, 2008.

Eliminating cuts in theories of truth

Graham E. Leigh

Fix a first order theory S that has (i) a finite language, (ii) an elementary axiomatisation and (iii) interprets a modicum of arithmetic (say elementary arithmetic). For example, standard presentations of Peano arithmetic and Zermelo-Fraenkal set theory. We define $\mathsf{CT}[\mathsf{S}]$ as the expansion of S by a fresh unary predicate symbol T and the *compositional axioms of truth for* T (see, e.g. [3]). Importantly, schemata of S are *not* extended to the new language. A formula of $\mathsf{CT}[\mathsf{S}]$ is *T-free* if it does not feature the predicate T.

In the talk I outlined a proof-theoretic argument for the following two theorems.

Theorem 3. *$\mathsf{CT}[\mathsf{S}]$ is a conservative extension of S, i.e. every T-free theorem of $\mathsf{CT}[\mathsf{S}]$ is derivable in S. Moreover, this fact is verifiable in hyper-exponential arithmetic.*

Theorem 4. *Let $\mathrm{Ax}(x)$ be a formula expressing that x encodes the universal closure of an axiom of S. The theory $\mathsf{CT}[\mathsf{S}] + \forall x(\mathrm{Ax}(x) \to T(x))$ is a conservative extension of S and this fact is verifiable in S.*

The first part of Theorem 1 was first established by Barwise and Schlipf in the early 70s (see Theorem IV.5.3 of [1]) and later reproved by Kotlarski, Krajewski and Lachlan [5], which also establishes the first part of Theorem 2. Both proofs are model-theoretic, however, showing that a countable non-standard model of S contains a full satisfaction class if it is recursively saturated. Since every model of S is elementarily extended by a recursively saturated model of the same cardinality, conservativity is obtained. Recently, Enayat and Visser [2] provided an alternative model-theoretic argument for conservativity which is formalisable within weak arithmetic and yields both theorems.

Halbach [4] offers a proof-theoretic approach to Theorem 3 by means of cut elimination. The strategy proceeds as follows. First the theory $\mathsf{CT}[\mathsf{S}]$ is reformulated as a finitary sequent calculus with a cut rule and rules of inference in place

of each of the compositional axioms for truth. A typical derivation in this calculus features cuts on formulæ involving the truth predicate and in general the system does not permit cut elimination. Instead, Halbach outlines a method of partial cut elimination whereby every cut on a formula involving the truth predicate is systematically replaced by a derivation with cuts only on T-free formulæ. Halbach's proof, however, contains a critical error (see, for example, Theorem 8.5 of [3]). Nevertheless, the argument yields a method to eliminate cuts of a very particular kind, namely those on formulæ $T(s)$ for which it is derivable (within, say, S) that the logical complexity of the formula coded by s is bounded by some closed term.

During the talk I discussed the link between the system $\mathsf{CT}[\mathsf{S}]$ and its fragment with bounded cuts that is necessary to achieve cut eliminaiton. This takes the form of the following lemma.

Lemma (Bounding lemma)**.** *If Γ and Δ are finite sets consisting of only truth-free and atomic formulæ, and the sequent $\Gamma \Rightarrow \Delta$ is derivable in $\mathsf{CT}[\mathsf{S}]$, then there exists a derivation of this sequent in which all cuts are either on T-free formulæ or bounded in the sense above.*

Let $\mathsf{CT}^*[\mathsf{S}]$ denote the subsystem of $\mathsf{CT}[\mathsf{S}]$ featuring only bounded cuts of the form described above. Since this calculus permits the elimination of all cuts containing the truth predicate, the first part of Theorem 3 is a consequence of the above lemma. Moreover, the proof yields bounds on the size of the resulting derivation, from which the second part of Theorem 3 can be deduced.

Considering Theorem 4, we observe that the reduction of $\mathsf{CT}[\mathsf{S}]$ to $\mathsf{CT}^*[\mathsf{S}]$ also yields a reduction of $\mathsf{CT}[\mathsf{S}] + \forall x(\mathrm{Ax}(x) \to T(x))$ to an analogous extension of $\mathsf{CT}^*[\mathsf{S}]$. Despite not admitting cut elimination in the same style, this latter system is relatively interpretable in $\mathsf{CT}[\mathsf{S}]$, whence Theorem 3 provides the desired result.

Full proofs of the results can be found in [6].

References

[1] J. Barwise. *Admissible Sets and Structures: An Approach to Definability Theory.* Springer–Verlag. 1975.

[2] A. Enayat and A. Visser. Full satisfaction classes in a general setting (Part 1). Available at *Logic Group Preprint Series* (URL: www.phil.uu.nl/preprints/lgps/).

[3] V. Halbach. *Axiomatic theories of truth*, second edition. Cambridge University Press, 2014.

[4] V. Halbach. Conservative theories of classical truth. *Studia Logica 62* (1999):353–370

[5] H. Kotlarski, S. Krajewski and A.H. Lachlan. Construction of satisfaction classes for non-standard models. *Canadian Mathematical Bulletin 24* (1981):283–93.

[6] G.E. Leigh. Conservativity for theories of compositional truth via cut elimination. To appear in *Journal of Symbolic Logic*. Available at arxiv.org/abs/1308.0168.

Some recents results on Herbrand's Theorem

Federico Aschieri
(joint work with Margherita Zorzi)

We present a new Curry-Howard correspondence for classical first-order natural deduction [5]. We add to the lambda calculus an operator which represents, from the viewpoint of programming, a mechanism for raising and catching multiple exceptions, and from the viewpoint of logic, the excluded middle over arbitrary prenex formulas. Treating the excluded middle as primitive, rather than deriving it from the double negation elimination as in [7, 6], has a key advantage. The logically obscure concept of "continuation" used in programming languages is no longer primitive; instead, the execution of classical programs can be described as a logical process of *making hypotheses*, *testing* and *correcting them* when they are *learned* to be wrong. The machinery thus allows to extend the idea of learning – originally developed in Arithmetic [1, 2, 3, 4] – to pure logic. So our reduction rules for classical natural deduction appear very natural and can even be described in a pure logical manner, without any reference to lambda calculus. Indeed, this double perspective is stressed in [5].

We prove that our typed calculus is strongly normalizing and show that proof terms for simply existential statements reduce to a list of individual terms forming a Herbrand disjunction. A by-product of our approach is thus a natural-deduction proof and a computational interpretation of Herbrand's Theorem. This interpretation is far and away more direct that the one based on negative translations of classical natural deduction into the intuitionistic counterpart followed by a normal form argument for proofs of $\neg\forall xP$ statement. Moreover, as opposed to [7, 6] or other double-negation-elimination-based natural deduction systems, the simply existential formulas are interpreted as *data types*, because terms of that type normalize to lists of witnesses. This just not happen in systems based on call/cc or $\lambda\mu$-calculus. Moreover, our computational interpretation also *explains* Herbrand's theorem and in particular what it is the real reason why Hebrand's disjunctions are produced and not single witnesses. Without studying the excluded middle as primitive concept and the correspondent logical process of making hypotheses and learning, this would not be possible.

References

[1] F. Aschieri, S. Berardi, *A New Use of Friedman's Translation: Interactive Realizability*, in: Logic, Construction, Computation, Berger et al. eds, Ontos-Verlag Series in Mathematical Logic, 2012.

[2] F. Aschieri, *Interactive Realizability for Classical Peano Arithmetic with Skolem Axioms*. Proceedings of Computer Science Logic 2012, Leibniz International Proceedings in Informatics, vol. 16, 2012.

[3] F. Aschieri, *Interactive Realizability for Second-Order Heyting Arithmetic with $EM1$ and $SK1$*, Mathematical Structures in Computer Science, 2013.

[4] F. Aschieri, S. Berardi, G. Birolo, *Realizability and Strong Normalization for a Curry-Howard Interpretation of HA + EM1*, Proceedings of Computer Science Logic 2013, Leibniz International Proceeding in Computer Science, vol. 23, 2013.

[5] F. Aschieri, M. Zorzi, *On Natural Deduction in Classical First-Order Logic: Curry-Howard Correspondence, Strong Normalization and Herbrand's Theorem*, manuscript on HAL, 2014.
[6] P. de Groote, *Strong Normalization for Classical Natural Deduction with Disjunction*, Proceedings of TLCA 2001: 182–196.
[7] J.-L. Krivine, *Classical Realizability.* In Interactive models of computation and program behavior. Panoramas et synthèses , 2009, 197–229. Société Mathématique de France.

Cobham Recursive Set Functions

Sam Buss
(joint work with A. Beckmann, S.D. Friedman, M. Müller, N. Thapen)

This talk discusses a new notion of polynomial time computability for general sets, based on ϵ-recursion with a Cobham style bounding using a new smash function tailored for sets. This class of functions is called the Cobham Recursive Set Functions (CRSF), and gives a notion of polynomial time computability intrinsic to sets. The smash ($\#$) function accommodates polynomial growth rate of both the size of the transitive closure and the rank of sets. For suitable encodings of binary strings as hereditarily finite sets, the CRSF functions are precisely the usual polynomial time computable functions. The goal in defining the CRSF functions is to give a model of computation on sets which

- Is analogous to complexity classes on bit strings,
- Is natural and intrinsic to sets
- Reduces to standard complexity classes on hereditarily finite sets with suitable encodings.

Definition. *The* set composition *function $a\odot b$ and the* set smash *function $a\#b$ are defined by $\in$-recursion as*

$$\begin{aligned} \emptyset\odot b &= b \\ a\odot b &= \{x\odot b : x\in a\}, \quad \textit{for } a\neq\emptyset \end{aligned}$$

and

$$a\#b \;=\; b\odot\{x\#b : x\in a\}.$$

Theorem.

1. $\mathrm{rank}(a\#b)+1 = (\mathrm{rank}(b)+1)(\mathrm{rank}(a)+1)$.
2. $|\mathrm{tc}(a\#b)|+1 = (|\mathrm{tc}(a)|+1)(|\mathrm{tc}(b)|+1)$.

Definition. *If g is an $(n+1)$-ary function, h is an n-ary function and τ is a n-ary function, then* **(Cobham Recursion$_{\preccurlyeq}$)** *gives the n-ary function f:*

$$f(a,\vec{c}) \;=\; g(\{f(b,\vec{c}) : b\in a\}, a, \vec{c}),$$

provided that, for all $a,\vec{c}$, we have $\tau(x,a,\vec{c}) : f(a,\vec{c}) \preccurlyeq h(a,\vec{c})$.

Definition. *The* Cobham Recursive Set Functions, CRSF*, are the set functions obtained from a finite set of initial functions and the set smash function $\#$ by closing under* **(Composition)** *and* **(Cobham Recursion$_{\preccurlyeq}$)**.

Theorem. *For $f(\vec{a}) \in$* CRSF*, there are polynomials p and q so that*

- $\mathrm{rank}(f(\vec{a})) \leq p(\max_i\{\mathrm{rank}(a_i)\})$ *and*
- $|\mathrm{tc}(f(\vec{a}))| \leq q(\max_i(|\mathrm{tc}(a_i)|))$.

Theorem. *Under a suitable encoding of finite binary strings as hereditarily finite sets, the* CRSF *functions (on sets encoding finite binary strings) are precisely the polynomial time computable functions.*

In earlier work, Beckmann, Buss and Friedman [2] defined safe/normal set functions, inspired by the safe/normal functional definition of polynomial time due to Bellantoni and Cook [3]. Arai [1] gave an alternate characterization of polynomial time using a modified version of safe/normal set functions.

Definition. *The* PCSF^+ *functions are defined like Arai's class of Predicatively Computable Set Functions (*PCSF*) but with closure under* **(Normal Separation$^{\mathrm{SN}}$)**.

Theorem. *The following are equivalent: For any set function f, $f(\vec{x})$ is in* CRSF *if and only if $g(\vec{x}/) = f(\vec{x})$ is a* PCSF^+ *function.*

References

[1] T. Arai, *Predicatively computabole functions on sets*, technical report, arXiv:1204.5582v2, 2012.

[2] A. Beckmann, S. Buss, S. Friedman, *Safe recursive set functions*, preprint 2012, to appear.

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

Transfinite Methods as Admissible Rules

Peter Schuster

(joint work with Davide Rinaldi)

Let $\vdash$ be a mono-conclusion entailment relation on a semigroup $(S, *)$ such that

$$\frac{U, a \vdash c \qquad U, b \vdash c}{U, a * b \vdash c}$$

holds [6, 7, 8] for all finite subsets U and elements a, b, c of S. Let $\vdash_*$ be the multi-conclusion entailment relation on S that is generated by $\vdash$ and the axioms

$$a * b \vdash_* a, b \qquad d \vdash_*$$

where $a, b \in S$ are arbitrary but d is a distinguished element of S. Then every proof of $U \vdash_* v$ can be converted into a proof of $U \vdash v$ whenever U is a finite subset and v an element of S. As a by-product, the cut rule is eliminated.

For example, the theory of integral domains is conservative for definite Horn clauses over the theory of reduced rings, which might help to settle an issue raised in [9]; other applications to algebra are about local rings, valuation rings and ordered fields. The conversion also allows to eliminate, from indirect proofs of statements of elementary wording, instances of the appropriate incarnation of Zorn's

Lemma: the Krull–Lindenbaum Lemma in universal form [6, 8, 10]. Yet the relation to cut elimination proper and to related work [1, 2, 3, 4, 5] is to be clarified.

References

[1] Jan Cederquist and Thierry Coquand. Entailment relations and distributive lattices. In S. Buss et al., editor, *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 Henrik Persson. Valuations and Dedekind's Prague theorem. *J. Pure Appl. Algebra*, 155:121–129, 2001.

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

[4] Henri Lombardi. Le contenu constructif d'un principe local-global avec une application à la structure d'un module projectif de type fini. *Publ. Math. Besançon. Théorie des nombres*, 94–95, 95–96, 1997.

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

[6] Gillman Payette and Peter K. Schotch. Remarks on the Scott–Lindenbaum Theorem. *Studia Logica*, 102:1003–1020, 2014.

[7] Davide Rinaldi. *Topologie basic in algebra commutativa*. Tesi di laurea specialistica in matematica, Università degli Studi di Padova, 2010.

[8] Davide Rinaldi and Peter Schuster. A universal Krull–Lindenbaum Theorem. Preprint, University of Leeds, 2014.

[9] Helmut Schwichtenberg and Christoph Senjak. Minimal from classical proofs. *Ann. Pure Appl. Logic*, 164:740–748, 2013.

[10] Dana Scott. Completeness and axiomatizability in many-valued logic. In *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.

Applications of Logic to the Verification of Railway Control Systems

Monika Seisenberger

(joint work with Andrew Lawrence, Ulrich Berger, Phil James, Fredrik Nordvall-Forsberg, and Markus Roggenbach)

The objective of this talk is to give an overview on logical methods used in (1) the verification of traditional solid state interlockings and (2) the modelling and analysis of the Eurepean Rail Traffic Management System (ERTMS). The research is done in cooperation with Siemens Rail Automaton, UK.

Traditionally, railway interlockings are specified using a graphical language, called Ladder Logic. In the first part of the talk, we give a semantics for this language and show how to get from a specification of an interlocking in Ladder Logic to a SAT solving problem. This process has been automated and realistic Interlocking examples, provided by the Railway company, have been verified using a) MiniSat and b) SCADE, an industrial tool developed for safety critial applications (see [1] for an overview of the work done in this part). We further applied our own SAT solver, which we extracted (via modified realisability) from a formal

constructive proof that a set of clauses (in conjunctive normal form) is either satisfiable or not. The extracted SAT solver is a verified DPLL algorithm, which either yields a model or a derivation indicating why the clause set is not satifiable (for more detail see [2] or [3]). In addition we extracted a resolution solver which either yields a model, or a resolution derivation that the set of clauses is unsatisfiable. Our extracted solver is not as fast as the solver used by SCADE, but it is proven correct and complete.

In the second part of the talk, we present our modelling of ERTMS. The European Train Control System is a next generation train control system, currently in UK only in test use on a few lines, which aims at improving the performance/capacity of the rail traffic systems, without compromising their safety. It generalizes from traditional discrete interlockings to a system that includes onboard equipment and communication between trains and interlockings via radio block processors. Whilst the correctness of traditional interlocking systems is well-researched in the literature, it is challenging to verify ERTMS based systems for safety properties such as collision freedom due to the involvement of continuous data. It is further an open field of how to substantiate the claim that the ERTMS approach offers a better performance of the railway compared to the traditional control. We model ERTMS, specifically trains, interlockings, radioblock processors, and controllers as hybrid automata. (They are hybrid because they combine discrete and continuous data.) We provide a formalization in Real Time Maude [4] for simple scenarios which allow to simulate runs, i.e. discuss performance, and also to apply LTL modell checking (see [5]) to prove safety conditions such as collision freedom and as well as the fact that points do no change their direction when trains are on the respective segment.

References

[1] P. James, A. Lawrence, F. Moller, M. Roggenbach, M. Seisenberger, A. Setzer, S. Chadwick, and K. Kanso, *Verification of Solid State Interlocking Programs*, In SEFM'13, LNCS **8368** (2014), 253–268.

[2] A. Lawrence, U. Berger, M. Seisenberger, *Extracting a DPLL Algorithm*, MFPS 2012, Electronic Notes in Theoretical Computer Science **286** (2012), 243–256.

[3] U. Berger, A. Lawrence, F. Nordvall Forsberg, M. Seisenberger, *Extraction of Verified Decision Procedures*, LMCS (2014), to appear.

[4] P. C. Ölveczky, and J. Meseguer, *Specification and Analysis of Real-Time Systems using Real-Time Maude*, FASE'04, LNCS **2984** (2004).

[5] A. Lawrence, U. Berger , P. James, M. Roggenbach, M. Seisenberger. *Modelling and Analysing the European Rail Traffic Control System*, FTSCS Preprodeedings (2014).

Univalent Foundation and Constructive Mathematics

Thierry Coquand

This talk was in two parts. The first part was a general introduction/tutorial on the univalent foundation program of Voevodsky [Voe]. The second part was a presentation of a variation of the cubical set model analysed in [BCH]. Let **C** be

the following category: the objects are finite sets $I, J, K, \ldots$ and a map $I \to J$ is a monotone map $2^I \to 2^J$, where 2 is the poset $0 \leq 1$. (Alternatively, such a map can be described as a set theoretic map $J \to D(I)$ where $D(I)$ is the free bounded distributive lattice on I.) A *cubical set* is defined to be a presheaf on $\mathbf{C}$. In particular, the interval $\mathbf{I}$ can be defined to be the representable functor defined by any singleton. We extend in this way the model of [BCH] by adding diagonal and connection operations. Using the diagonal operation, we get a direct interpretation of function extensionality, and we can think of the set of path of a cubical set X as the exponential $\mathbf{I} \to X$. Using connections, we get a direct interpretation of the fact that any "singleton" type $(\Sigma x : A)\mathbf{Id}(A, a, x)$ is contractible. It is then possible to refine the Kan condition [Kan], that any open box can be filled, and get a model of type theory which justifies the axiom of univalence and which is developped in a constructive metatheory. Contrary to the model presented in [BCH], this model interprets the computation rule for equality introduced in [M-L] as a judgemental equality. We can also in this way justify the propositional truncation operation [UnFo, Voe] introduced by Voevodsky as well as some higher inductive types [UnFo] such as the push-out operation.

References

[APW] S. AWODEY, A. PELAYO and M.A. WARREN – *Voevodsky's Univalence Axiom in homotopy type theory*, Notices Amer. Math. Soc. 60 (2013), 1164–1167.

[BCH] M. BEZEM, TH. COQUAND and S. HUBER – *A cubical set model of type theory*, Types for Proofs and Programs, post-proceeding of TYPES 2013.

[Kan] D. KAN. – *Abstract homotopy. I.*, Proc. Nat. Acad. Sci. U.S.A. 41, p. 1092–1096, 1955.

[M-L] P. MARTIN-LÖF – *An Intuitionistic Theory of Types: Predicative Part*, in Logic Colloquium '73, H.E. Rose and J.C. Shepherdson eds., (1975), 73–118.

[UnFo] THE UNIVALENT FOUNDATIONS PROGRAM – *Homotopy Type Theory: Univalent Foundations*, Institute for Advanced Study, 2013.

[Voe] V. VOEVODSKY – *Experimental library of univalent formalization of mathematics*, à paraître dans Mathematical Structures in Computer Science (arXiv:1401.0053), 2013.

Recent Applications of Bar Recursion and Selection Functions

Paulo Oliva

1. Introduction

Bar recursion was introduced by Spector [7] as an extension of Gödel's system T. The aim was to extend Gödel's dialectica interpretation [1] of arithmetic to full classical analysis, by computationally interpreting countable choice, dependent choice and arithmetical comprehension. I list here some of the recent work I have done (jointly with several collaborators) on both trying to have a better understanding of bar recursion, and on applying it in different settings.

2. Recent Developments

Most of the work below is motivated by a novel understanding of bar recursion as a process of calculating optimal strategies in a general form of sequential game. This sparked interest both in the Game Theory and Proof Theory communities.

2.1. **Higher-order Sequential Games.** The crucial observation in order to understand the connection between bar recursion and sequential games is that functionals of type $(X \to R) \to X$, called *selection functions*, can be viewed as an abstract description of a player who has to choose a move $x \in X$ having in mind the possible outcomes $r \in R$. We think of the mapping $p\colon X \to R$ as the context of the player, which says what outcome will result for each given move. The functional $(X \to R) \to X$ then describes the preferred outcome for each given game context. For more details see [2, 3].

2.2. **Selection Functions and Game Theory.** Our novel modelling of players as higher-order functionals $(X \to R) \to X$ has interesting consequences to the theory of games, as developed in (classical) Game Theory as developed by Von Neumann. In [5] we explain how peculiar games can be directly modelled in our framework, leading to a more general framework where games that were previously considered to be of a different nature can be all modelled uniformly. The higher-order approach to model games also has several other advantages, e.g. gain in modularity and compositionally of games; computational and resource-aware strategies can be naturally captured; and previous restrictions on the ordering of preferences can be avoided.

2.3. **Herbrand Functional Interpretation of DNS.** The Herbrand functional interpretation [8] has been recently introduced as a variant of Gödel's dialectica interpretation capable of interpreting principles from non-standard arithmetic. In recent joint work with Martín Escardó [4] we have been able to extend the Herbrand functional interpretation to full analysis by giving an interpretation of the double negation shift (and hence countable choice) using Spector's bar recursion. In fact, the interpretation is more naturally presented using a variant of the product of selection functions over the finite power-set monad, which we show is equivalent (over system T) to Spector's original bar recursion.

2.4. **Proof Mining the Podelski-Rybalchenko "Termination Theorem".** In joint work with Stefano Berardi and Silvia Steila we have used bar recursion to give a (sub-recursive) computational interpretation to the *Podelski-Rybalchenko termination theorem* [6]. This is work currently in progress and we hope to finish writing our paper by the end of the year.

2.5. **More Efficient Spector Bar Recursion.** In recent joint work with Thomas Powell we have developed a novel variant of Spector's bar recursion which in practical cases seems to run much more efficiently than Spector's original definition. The crucial idea is to make use of the *control functional* of the bar recursion (i.e. the functional Y for which we need to check $Y(\hat{s}) < |s|$) to guide the recursion. In

this way we replace finite sequence by finite partial functions σ, and replace the usual stopping condition with $Y(\hat{\sigma}) \in \mathrm{dom}(\sigma)$. At the same time, we perform bar recursive updated at the point $n = Y(\hat{\sigma})$ so that we are always trying to fill the gap that led to a bar recursive call.

References

[1] J. Avigad and S. Feferman. Gödel's functional ("Dialectica") interpretation. In S. R. Buss, editor, *Handbook of proof theory*, volume 137 of *Studies in Logic and the Foundations of Mathematics*, pages 337–405. North Holland, Amsterdam, 1998.

[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. Sequential games and optimal strategies. *Royal Society Proceedings A*, 467:1519–1545, 2011.

[4] M. H. Escardó and P. Oliva. The herbrand functional interpretation of the double negation shift. ArXiv, 2014.

[5] Jules Hedges, Paulo Oliva, Evguenia Winschel, Viktor Winschel, and Philipp Zahn. A higher-order framework for decision problems and games. ArXiv, http://arxiv.org/abs/1409.7411.

[6] Andreas Podelski and Andrey Rybalchenko. Transition invariants. In *LICS*, pages 32–41, 2004.

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

[8] Benno van den Berg, Eyvind Briseid, and Pavol Safarik. A functional interpretation for nonstandard arithmetic. *Annals of Pure and Applied Logic*, 163(12):1962–1994, 2012.

Bishop spaces: constructive point-function topology

Iosif Petrakis

A *Bishop space* is a structure $\mathcal{F} = (X, F)$, where X is an inhabited set and F is a set of functions of type $X \to \mathbb{R}$ which includes the constant functions and it is closed under addition, uniform limits and composition with elements of $\mathrm{Bic}(\mathbb{R})$. By $\mathbb{R}$ we denote the Bishop reals and by $\mathrm{Bic}(\mathbb{R})$ the set of Bishop continuous functions of type $\mathbb{R} \to \mathbb{R}$. Bishop used the term *function space* for $\mathcal{F}$ and *topology* for F. A *Bishop morphism* between two Bishop spaces $\mathcal{F} = (X, F)$ and $\mathcal{G} = (Y, G)$ is a function $h : X \to Y$ such that $\forall_{g \in G}(g \circ h \in F)$. We denote the set of Bishop morphisms by $\mathrm{Mor}(\mathcal{F}, \mathcal{G})$. If $h \in \mathrm{Mor}(\mathcal{F}, \mathcal{G})$, we call h *open*, if $\forall_{f \in F} \exists_{g \in G}(f = g \circ h)$.

The theory of Bishop spaces is so far the least developed approach to constructive topology with points. Bishop introduced them in [1], some comments on them were added in [2], while in [3] Bridges revived the subject. Ishihara in [5] studied the relation of the subcategory **Fun** of the category **Bis** of Bishop spaces with the category of neighborhood spaces **Nbh**. We develop the theory of Bishop spaces within BISH putting the emphasis on function-theoretic concepts rather than set-theoretic ones.

Most of the new Bishop spaces generated from old ones are defined through Bishop's inductive concept of the least topology $\mathcal{F}(F_0)$ generated by a given base

F_0 of real-valued functions on X. It is easy to see that $h \in \mathrm{Mor}(\mathcal{F}, \mathcal{F}(G_0))$ iff $\forall_{g_0 \in G_0}(g_0 \circ h \in F)$. More interestingly, if $h : X \to Y$ is an epimorphism, and $\mathcal{F} = (X, \mathcal{F}(F_0))$, then h is open iff $\forall_{f_0 \in F_0} \exists_{g \in G}(f_0 = g \circ h)$. The product of Bishop spaces was already defined by Bishop, while we introduce the exponential Bishop space $\mathcal{F} \to \mathcal{G} = (\mathrm{Mor}(\mathcal{F}, \mathcal{G}), F \to G)$, which corresponds to the point-open topology within **Top**. It seems that the category of Bishop spaces **Bis** behaves like the category of topological spaces **Top** w.r.t. the cartesian closure property. Although Ishihara and Palmgren constructed in [6] the quotient topological space using predicative methods, our definition of the quotient Bishop space is straightforward and permits a smooth translation of the standard classical theory of quotient topological spaces into the theory of Bishop spaces.

We call a Bishop space $\mathcal{F}$ *completely regular*, if the apartness relation induced by its topology F is tight, and we show that the completely regular Bishop spaces behave in **Bis** as the completely regular topological spaces in **Top**. Namely, the Stone-Čech isomorphism between $C(\rho X)$ and $C(X)$, the Embedding lemma and the Tychonoff embedding theorem for completely regular topological spaces have their constructive counterpart within the theory of Bishop spaces.

Using Bishop's version of the Tietze theorem for metric spaces we prove the Urysohn lemma for zero sets. This is the first step to constructivise parts of the classical theory of rings of continuous functions within Bishop spaces. We study various embeddings of one Bishop space to another and we translate results from [4] into Bishop spaces. This translation is not always constructive. For example, we need the LPO to prove without restrictions to its formulation the fundamental Urysohn extension theorem within Bishop spaces.

The application of the general theory of Bishop spaces to concrete spaces like the Cantor and the Baire space, the Hilbert cube etc., viewed as Bishop spaces, shows how close to standard topology, as a mathematical tool, the theory of Bishop spaces can be. Moreover, based on the work [7] of Palmgren, a reconstruction of the basic homotopy theory within Bishop spaces seems possible.

References

[1] E. Bishop: Foundations of Constructive Analysis, McGraw-Hill, 1967.

[2] E. Bishop and D. Bridges: Constructive Analysis, Grundlehren der Math. Wissenschaften 279, Springer-Verlag, Heidelberg-Berlin-New York, 1985.

[3] D. S. Bridges: *Reflections on function spaces*, Annals of Pure and Applied Logic **163** (2012), 101–110.

[4] L. Gillman and M. Jerison: Rings of Continuous Functions, Van Nostrand, 1960.

[5] H. Ishihara: *Relating Bishop's function spaces to neighborhood spaces*, Annals of Pure and Applied Logic **164** (2013), 482–490.

[6] H. Ishihara and E. Palmgren: *Quotient topologies in constructive set theory and type theory*, Annals of Pure and Applied Logic **141** (2006), 257–265.

[7] E. Palmgren: *From Intuitionistic to Point-Free Topology: On the Foundations of Homotopy Theory*, in S. Lindström et al. (eds.), Logicism, Intuitionism, and Formalism, Synthese Library 341, Springer Science+Buiseness Media B.V. 2009.

Well quasi orders

Andreas Weiermann
(joint work with Michael Rathjen, Jeroen Van der Meeren)

An important characteristic of a well quasi order or better its associated well partial order is provided by its maximal order type which is the order type of a maximal possible linear extension. We describe a general formula which can be used to predict maximal order types for well quasi orders when they are given by a certain class of recursive tree constructions. To this end we consider effective constructions W which map effectively given well quasi orders to effectively presented well quasi orders. Using W we define the set $T(W)$ of generalized trees T where the immediate subtrees of T are arranged into a term relative to $W(T(W))$. $T(W)$ comes with a naturally induced quasi order. The general conjecture is that $T(W)$ will become a well quasi order with maximal order type equal to $\vartheta(o(W(\Omega)))$ where Ω denotes the first uncountable ordinal, $o(W(\Omega))$ denotes the maximal order type of $W(\Omega)$ and ϑ denotes a certain standard collapsing function [1]. Our conjecture has been verified for a large class of examples and comes with several applications to independence results for systems of second order arithmetic [2].

References

[1] A. Weiermann, *A Computation of the Maximal Order Type of the Term Ordering on Finite Multisets*, Lecture Notes in Computer Science **5635** (2009), 11 pages.
[2] M. Rathjen, J. Van der Meeren, A. Weiermann, *Well-partial-orderings and the big Veblen number* Archive for Mathematical Logic **32** (2015), DOI 10.1007/s00153-014-0408-5.

Proof-theoretic methods in nonlinear analysis III: Quantitative results on Fejér monotone sequences

Laurenţiu Leuştean
(joint work with Ulrich Kohlenbach, Adriana Nicolae)

This is the third part of a tutorial on proof mining. We report on recent applications of proof mining [3], providing in a unified way quantitative forms of strong convergence results for numerous iterative procedures which satisfy a general type of Fejér monotonicity, where the convergence uses the compactness of the underlying set. These quantitative versions are in the form of explicit rates of so-called metastability in the sense of T. Tao [4] .

Fejér monotonicity is a key notion employed in the study of many problems in convex optimization and programming, fixed point theory and the study of (ill-posed) inverse problems (see e.g. [5, 1]).

Our approach covers examples ranging from the proximal point algorithm for maximal monotone operators to various nonlinear iterations: Picard iteration for firmly nonexpansive mappings, Ishikawa iteration for nonexpansive mappings, Mann iteration for strict pseudo-contractions, asymptotically nonexpansive mappings and a class of generalized nonexpansive mappings. Our results cover the

ones obtained in [2], which in fact, has been the point of departure of our present investigation

Many of the results hold in a general metric setting with some convexity structure added (so-called W-hyperbolic spaces). Sometimes uniform convexity is assumed still covering the important class of CAT(0)-spaces due to Gromov.

Acknowledgement: Laurenţiu Leuştean was supported by a grant of the Romanian National Authority for Scientific Research, CNCS - UEFISCDI, project number PN-II-ID-PCE-2011-3-0383

References

[1] P.L. Combettes, *Fejér monotonicity in convex optimization*, in: C.A. Floudas, P.M. Pardalos (eds.), Encyclopedia of Optimization, Kluwer Academic Publishers, 2001, pp. 106–114.

[2] U. Kohlenbach, *Some computational aspects of metric fixed point theory*, Nonlinear Analysis **61** (2005), 823–837.

[3] U. Kohlenbach, L. Leuştean, A. Nicolae, *Quantitative results on Fejér monotone sequences*, ArXiv:1412.5563, 2014.

[4] T. Tao, *Soft analysis, hard analysis, and the finite convergence principle*, Essay posted May 23, 2007, appeared in: T. Tao, Structure and Randomness: Pages from Year One of a Mathematical Blog, AMS, 2008.

[5] V.V. Vasin, I.I. Eremin, *Operators and Iterative Processes ofFejér type. Theory and Applications*, de Gruyter, 2009.

Proof-theoretic methods in nonlinear analysis IV: Rates of convergence and metastability for abstract Cauchy problems generated by accretive operators

Angeliki Koutsoukou-Argyraki

(joint work with Ulrich Kohlenbach)

We present a work that is the first application of proof mining to the theory of partial differential equations and was recently published in [3].

In this work we extract rates of convergence and rates of metastability (in the sense of Tao) for convergence results regarding abstract Cauchy problems generated by ϕ-accretive at zero operators $A : D(A)(\subseteq X) \to 2^X$ where X is a real Banach space, proved in [1], by proof-theoretic analysis of the proofs in [1] and having assumed a new, stronger notion of *uniform accretivity at zero*, yielding a new notion of *modulus of accretivity*. We compute the rate of metastability for the convergence of the solution of the abstract Cauchy problem generated by a uniformly accretive at zero operator A to the unique zero of A via proof mining and based on a result in [2].

Definition 1. [3] *Let X be a real Banach space. An accretive operator $A : D(A) \to 2^X$ with $0 \in Az$ is called uniformly accretive at zero if*

$$\forall k \in \mathbb{N}\ \forall K \in \mathbb{N}^*\ \exists m \in \mathbb{N}\ \forall (x,u) \in A$$

$$(\|x - z\| \in [2^{-k}, K] \to \langle u, x - z\rangle_+ \geq 2^{-m})(*).$$

Any function $\Theta_{(\cdot)}(\cdot) : \mathbb{N} \times \mathbb{N}^* \to \mathbb{N}$ *is called a modulus of accretivity at zero for* A *if* $m := \Theta_K(k)$ *satisfies* $(*)$.

Our central result is the following theorem:

Theorem 1. [3] *Let* X *be a real Banach space. Suppose that* $A : D(A) \to 2^X$ *is a uniformly accretive at zero operator on* X *with the range condition that has a modulus of accretivity* Θ. *Suppose that the problem*

$$u'(t) + A(u(t)) \ni 0, t \in [0, \infty)$$

$$u(0) = x_0,$$

has a strong solution for each $x_0 \in D(A)$. *Then, for each* $x \in \overline{D(A)}$ *the integral solution* $u(\cdot)$ *of the problem*

$$u'(t) + A(u(t)) \ni f(t), t \in [0, \infty)$$

$$u(0) = x,$$

where $f \in L^1(0, \infty, X)$, *converges strongly to the zero* z *of* A *as* $t \to \infty$ *and one has*

$$\forall k \in \mathbb{N}\ \forall \bar{g} : \mathbb{N} \to \mathbb{N}\ \exists \bar{n} \leq \Psi(k, \overline{g}, M, B, \Theta)\ \forall x \in [\bar{n}, \bar{n} + \bar{g}(\bar{n})]\ (\|u(x) - z\| < 2^{-k})$$

with rate of metastability

$$\Psi(k, \overline{g}, M, B, \Theta) = \tilde{g}^{(M \cdot 2^{k+1})}(0) + h(\tilde{g}^{(M \cdot 2^{k+1})}(0)),$$

where

$$\tilde{g}(n) := g(n) + n$$

with

$$g(n) := \overline{g}(n + h(n)) + h(n),$$

$$h(n) := (B(n) + 2) \cdot 2^{\Theta_{K(n)}(k+2)+1},$$

$$K(n) := \ulcorner \sqrt{2(B(n) + 1)} \urcorner.$$

Here $B(n) \in \mathbb{N}$ *is any nondecreasing upper bound on* $\frac{1}{2}\|u(n) - z\|^2$ *and* $M \in \mathbb{N}$ *is any upper bound on the integral* $I := \int_0^\infty \|f(\xi)\| d\xi$.

The rate obtained is extremely uniform, depending only on general bounds on the initial data and the modulus of accretivity Θ of A.

References

[1] J. García-Falset, *The asymptotic behavior of the solutions of the Cauchy problem generated by ϕ-accretive operators*, J. Math. Anal. Appl. vol. 310, 594-608 (2005).

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

[3] U. Kohlenbach, A. Koutsoukou-Argyraki, *Rates of convergence and metastability for abstract Cauchy problems generated by accretive operators*, J. Math. Anal. Appl. vol. 423, 1089-1112 (2015)

Grammars for first-order proofs

Bahareh Afshari
(joint work with Stefan Hetzl and Graham E. Leigh)

We look at the *combinatorial structure* of first-order proofs, in particular cut elimination. This study is motivated by the aim to compress automatically generated analytic proofs. For this we make connections to formal language theory and specifically regular and context-free tree grammars. The role of the grammars is to provide a *template* for introducing cuts into the proof.

Let π be a proof of $\exists x F$ where F is quantifier-free. By Herbrand's Theorem [4] (see, e.g. [1]) there exist closed terms $t_0, t_1, \ldots, t_k$ such that $\bigvee_{i=0}^{k} F(x/t_i)$ is a tautology. There are various ways to find such a Herbrand disjunction, most commonly via cut-elimination and Gentzen's midsequent theorem.

In [5] it was shown that this cumbersome process can be circumvented in some cases. Suppose π is a proof of an existential formula in which all cuts have complexity at most Σ_1. From this proof one can directly define a *regular* tree grammar $\mathcal{G}_\pi$ (of size no greater than that of the proof) such that its language, denoted $\mathcal{L}(\mathcal{G}_\pi)$, is finite and contains the Herbrand set $\mathcal{H}(\pi')$ where π' is any cut-free proof obtained from π via standard cut-elimination.

$$\begin{array}{ccc} \pi \vdash \exists x F & \xrightarrow{c.e.} & \pi' \vdash_{cf} \exists x F \\ {\scriptstyle \text{defn}}\downarrow & & \downarrow{\scriptstyle \text{Herbrand extraction}} \\ \mathcal{G}_\pi \text{ (of size} \leq |\pi|) & \xrightarrow{\mathcal{L}} & \mathcal{L}(\mathcal{G}_\pi) \supseteq \mathcal{H}(\pi') \end{array}$$

Figure 1. Proof grammars

Furthermore, it was proved that the anticlockwise arrows of Figure 1 are reversible: given a Herbrand set one can compute a *concise* grammar and determine suitable cut-formulæ to assemble a proof with Σ_1-cuts.

In the talk I showed how the correspondence in Figure 1 can be expanded to the level of Π_2-cuts. A simple Π_2-proof is a formal proof in first-order logic presented in sequent calculus with explicit contraction and weakening in which all cut-formulæ are of the form $\forall x \exists y A$ or $\exists x \forall y A$ with A quantifier free.

Theorem (Afshari, Hetzl & Leigh)**.** *Let π be a simple Π_2-proof of a Σ_1 formula. There is an associated context-free rigid tree grammar $\mathcal{G}_\pi$ (whose number of production rules is bounded by the size of π) with a finite language such that every Herbrand set obtained via (standard) cut-elimination rules from π is contained in the language of $\mathcal{G}_\pi$.*

In contrast to the case of Σ_1-cuts, the new grammars are built over λ-terms and involve production rules for function type variables. We give both a diagrammatic and recursive definition of the grammars associated to Π_2-proofs. The latter provides a neat formalisation in which the flow of information through cuts can

be visualised readily and derivations in the grammar $\mathcal{G}_\pi$ can be matched with corresponding traces in the proof π.

From a theoretical point of view this work provides an abstraction of proofs with cuts which focuses only on the aspects relevant to the extraction of Herbrand sets. Compared to other approaches in the literature, including Herbrand nets [7], proof forests [3] and functional interpretation [2], proof grammars offer, in my opinion, a conceptually clear representation of Herbrand's theorem. We expect that further investigation of Π_2-proofs will yield a Herbrand-confluence result analogous to [6] as well as techniques for the systematic introduction of Π_2-cuts.

References

[1] Buss, S.R. On Herbrand's Theorem. In *Logic and Computational Complexity*, Springer LNCS 960, 195–209, 1995.

[2] Gerhardy P. and Kohlenbach U. Extracting Herbrand disjunctions by functional interpretation. *Archive for Mathematical Logic* 44(5)(2005), 633–644.

[3] Heijltjes, W. Classical proof forestry. *Annals of Pure and Applied Logic*, 161(11)(2010), 1346–1366.

[4] Herbrand, J. *Recherches sur la théorie de la démonstration.* PhD thesis, Université de Paris, 1930.

[5] Hetzl, S. Applying tree languages in proof theory. In *Language and Automata Theory and Applications (LATA) 2012*, A.-H. Dediu, C. Martìn-Vide (eds.), Springer LNCS 7183, 228–242, 2012.

[6] Hetzl, S. and Straßburger L. Herbrand-confluence for cut elimination in classical first order logic. *Computer Science Logic (CSL) 2012*, P. Cégielski and A. Durand (eds.), Leibniz International Proceedings in Informatics (LIPIcs) 16, 320–334, 2012.

[7] McKinley, R. Proof nets for Herbrand's Theorem. *ACM Transactions on Computational Logic*, 14(1)(2013), 5:1–5:31.

Ordinal analysis based on Turing progressions

Joost J. Joosten

1. Provability logics and Turing progressions

By Gödel's Second Incompleteness Theorem any Σ^0_1 sound c.e. theory allowing coding of syntax can be strengthened by adding its consistency statement. *Turing progressions* arise by transfinitely iterating this process along some computable well-order. We denote the the αth Turing progression of T by T^α and define the Π^0_1 ordinal of a theory U as $|U|_{\Pi^0_1} := \sup\{\alpha \mid \mathrm{EA}^\alpha \subseteq U\}$ where EA stands for *Kalmar Elementary Arithmetic*. Various concrete examples were presented in U. Schmerl's [11] like $|\mathrm{PA}|_{\Pi^0_1} = \varepsilon_0$ and $|\mathrm{PA} + \mathtt{RFN}(\mathrm{PA})|_{\Pi^0_1} = \varepsilon_1$ where ε_i denotes the ith fixpoint of $\alpha \mapsto \omega^\alpha$.

It turns out that provability logics with various provability modalities are very well suited to talk about Turing progressions. Let Λ, ξ, $\zeta, \ldots$ denote ordinals. The logic GLP_Λ is the propositional modal logic that has for each $\xi{<}\Lambda$ a modality $[\xi]$. The rules of GLP_Λ are Modus Ponens and necessitation $\frac{\psi}{[\zeta]\psi}$ and the axioms are all tautologies together with the following schemata: $[\xi](A \to B) \to ([\xi]A \to [\xi]B)$;

$[\xi]([\xi]A \to A) \to [\xi]A$; $\langle\xi\rangle A \to [\zeta]\langle\xi\rangle A$ for $\xi < \zeta$; and $[\xi]A \to [\zeta]A$ for $\xi < \zeta$. By interpreting $[n]$ into arithmetic as "provable in T together with all true Π^0_n formulas" the logic GLP_ω –which is sound and complete for this interpretation– can naturally be used to denote fragments of arithmetic via a theorem that is essential due to Leivant ([10]) to the effect that provably we have $\langle n+2\rangle_{\mathrm{EA}}\top \equiv \mathrm{I}\Sigma_{n+1}$. This link between modal logic is actually within the closed fragment GLP^0_ω (no propositional variables). Within GLP^0_ω one can consider so-called *worms* which are iterated consistency statements like $\langle 1\rangle\langle 0\rangle\langle 1\rangle\top$ and order them via $A < B :=$ $\mathsf{GLP}_\omega \vdash B \to \langle 0\rangle A$. This yields ([9]) a well-order of order-type ε_0. Beklemishev could set these features of GLP_ω to work in [1] so that an ordinal analysis for PA and its kin can almost entirely be performed within the modal logic yielding results like $|\mathrm{PA} + \mathtt{Con}(\mathrm{PA})|_{\Pi^0_1} = \varepsilon_0 \cdot 2$.

2. Beyond first order theories

A first step in generalizing the above beyond first order has been established by studying the logics GLP_Λ for $\Lambda \geq \omega$. These logics are now well understood ([2, 3]). In particular, a universal model for GLP^0_Λ contains most information about the closed fragment ([6]) and the well-orders therein ([8]). It turns out that an adequate study of these well-orders requires the development of a new notion of transfinite 'iterations' of normal ordinal functions and left-inverses of such iterations ([5]). A second step is constituted by showing that reading $[\xi]$ as a formalization of "provable in T using an omega rule of nesting at most ξ" yields a sound and complete interpretation of GLP_Λ under some fairly non-restrictive conditions on Λ and T ([7]). Moreover, using this reading one can relate ([4]) the predicative second order theory ATR_0 to what is called *predicative oracle reflection* very much in the spirit of Leivant's result mentioned above. With these recent developments it seems that a Π^0_1 ordinal analysis of theories like ATR_0 becomes well within reach.

References

[1] L. D. Beklemishev. Provability algebras and proof-theoretic ordinals, I. *Annals of Pure and Applied Logic*, 128:103–124, 2004.

[2] L. D. Beklemishev. Veblen hierarchy in the context of provability algebras. In P. Hájek, L. Valdés-Villanueva, and D. Westerståhl, editors, *Logic, Methodology and Philosophy of Science, Proceedings of the Twelfth International Congress*, pages 65–78. Kings College Publications, 2005.

[3] L. D. Beklemishev, D. Fernández-Duque, and J. J. Joosten. On provability logics with linearly ordered modalities. *Studia Logica*, 102:541–566, 2014.

[4] A. Cordón Franco, D. Fernández-Duque, J. J. Joosten, and F. Lara Martín. Predicativity through transfinite reflection. *ArXiv*, 1412.5521 [math.LO], 2015.

[5] D. Fernández-Duque and J. J. Joosten. Hyperations, Veblen progressions and transfinite iteration of ordinal functions. *Annals of Pure and Applied Logic*, 164(7-8):785–801, 2013.

[6] D. Fernández-Duque and J. J. Joosten. Models of transfinite provability logics. *Journal of Symbolic Logic*, 78(2):543–561, 2013.

[7] D. Fernández-Duque and J. J. Joosten. The omega-rule interpretation of transfinite provability logic (submitted). *ArXiv*, 1205.2036 [math.LO], 2013.

[8] D. Fernández-Duque and J. J. Joosten. Well-orders in the transfinite Japaridze algebra. *ArXiv*, 1212.3468 [math.LO], 2013. Accepted for publication in the Logic Journal of the Interest Group in Pure and Applied Logic.
[9] K. N. Ignatiev. On strong provability predicates and the associated modal logics. *The Journal of Symbolic Logic*, 58:249–290, 1993.
[10] D. Leivant. The optimality of induction as an axiomatization of arithmetic. *Journal of Symbolic Logic*, 48:182–184, 1983.
[11] U. R. Schmerl. A fine structure generated by reflection formulas over primitive recursive arithmetic. In *Logic Colloquium '78 (Mons, 1978)*, volume 97 of *Stud. Logic Foundations Math.*, pages 335–350. North-Holland, Amsterdam, 1979.

On proof systems for integer linear programing

Pavel Pudlák

This is a report on a work in progress. A number of proof systems for integer linear programing have been proposed. Among the most important ones are *Cutting Planes* (CP) of Gomory and Chvátal, and *Lovász-Schrijver* (LS) of Lovász and Schrijver. Both systems are strictly stronger than *Resolution*, but their mutual relation is still unclear. We will give an argument that suggests that in some cases LS is stronger than CP. Our tool is the following version of the *feasible interpolation theorems* proved for CP and LS.

Theorem 5. *Let $\Gamma(\bar{x})$ and $\Delta(\bar{y})$ be two sets of inequalities with disjoint sets of variables $\bar{x}$ and $\bar{y}$. Let a CP (respectively LS) proof P of*

$$\Gamma(\bar{x}), \Delta(\bar{y}) \vdash \sum_j c_j x_j \leq \sum_i b_i y_i$$

be given. Then one can construct in polynomial time a number d and a CP (LS) proof of

$$\Gamma(\bar{x}), \Delta(\bar{y}) \vdash \sum_j c_j x_j \leq d \leq \sum_i b_i y_i.$$

Note that this theorem gives us *quantitative* information when $\Gamma(\bar{x}), \Delta(\bar{y})$ is consistent. The proofs are straightforward generalizations of the proofs of the feasible interpolation theorems for CP and LS [1, 2]. One can also derive additional information about the form of polynomial size circuits computing d.

Let A be a matrix and b and c vectors. The *weak duality of linear programing* (WD) is the fact that

$$\{\sum_j A_{ij} x_j \leq b_i\}_i, \{\sum_i A_{ij} y_i \geq c_j\}_j \vdash \sum_j c_j x_j \leq \sum_i b_i y_i.$$

The proof is trivial: $\sum_j c_j x_j \leq \sum_{ij} A_{ij} x_j y_i \leq \sum_i b_i y_i$. However, if the elements of the matrix and the vectors are variables, this is not directly formalizable in CP and LS because it involves quadratic and cubic terms. We consider two situations.

(1) Let A be constant and b and c variables. One can introduce extension variables so that $\sum_j c_j x_j \leq \sum_i b_i y_i$ is transformed into a linear inequality and we can still use it in the interpolation theorems. Then WD is provable in LS by a

polynomial size proof. This is because $\sum_{ij} A_{ij}x_jy_i$ is a quadratic term and LS is able to argue about such terms at least to the extent we need. In contrast, it is unlikely that CP would prove such a form of WD by a polynomial size proof. The reason is that such a proof would give us, using the feasible interpolation theorem above, a polynomial size circuit for linear programing of a very special form; such a circuit would only use monotone arithmetic operations if the elements of the vector b are positive.

(2) Let all elements of A, b and c be variables. One can introduce introduce more extension variables to represent the quadratic inequalities $\sum_j A_{ij}x_j \leq b_i, \sum_i A_{ij}y_i \geq c_j$ by linear ones. We conjecture that this form of WD does not have a polynomial size proof in LS. The reason is that the interpolation theorem for LS gives us strongly polynomial circuits for computing d, so we would get strongly polynomial circuits for linear programing. Whether or not there are strongly polynomial circuits for linear programing is an open problem. So, in principle, it is not excluded that WD has short proofs in LS, but it seems unlikely that one could solve the open problem in such a way.

We conclude by noting that one can extend these results to a more natural context of proof systems for mixed linear programing (where some variables range over integers and some over reals).

The author is supported by the ERC Advanced Grant 339691 (FEALORA) and the institute grant RVO 67985840.

References

[1] P. Pudlák, *Lower bounds for resolution and cutting planes proofs and monotone computations*, J. of Symb. Logic **62(3)**, (1997), 981–998.

[2] P. Pudlák, *On the complexity of propositional calculus.* In Sets and Proofs, Invited papers from Logic Colloquium'97, S. Barry Cooper and John K. Truss eds., Cambridge Univ. Press 1999, 197–218.

A trade-off between length and width in resolution

Neil Thapen

Resolution is a well-known proof system for refuting propositional CNF formulas. A *literal* is a propositional variable or its negation. A *clause* is a disjunction of literals. We define a *conjunctive normal form formula* or CNF to be a set of clauses, which we treat semantically as though it were a conjunction of clauses. The *resolution rule* allows us to derive the clause $C \vee D$ from the two clauses $C \vee q$ and $D \vee \neg q$, where q is any propositional variable. A resolution refutation of a CNF F is a derivation of the empty clause from F using the resolution rule.

Every unsatisfiable CNF has a resolution refutation. However, interesting questions remain about the complexity of refutations. We consider two measures of complexity, *length* and *width*. The *length* (or *size*) of a resolution refutation Π is the number of clauses it contains. The *width* of Π is the maximum width of any

clause in Π, where the width of a clause is just the number of literals it contains. Similarly the width of a CNF F is the maximum width of any clause in F.

A result of [1] showed an interesting and useful connection between the minimal length and minimal width of refutations:

Theorem 1. *Let F be a CNF in n variables with width k. Suppose that F has a resolution refutation Π of length S. Then F also has a resolution refutation Π' of width at most $k + \sqrt{n \log S}$.* □

In other words, every short refutation can be transformed into a narrow refutation. However, the transformation of Π into Π' used in the proof of Theorem 1 may increase the length of the refutation exponentially. We address the natural question of whether the theorem can be strengthened to guarantee that the narrow refutation Π' is not substantially longer than the initial short refutation Π. We show that the expected answer ("no") is correct. Our main result is:

Theorem 2. *Fix a small constant $\epsilon > 0$. Take any sufficiently large m such that both m and m^ϵ are powers of two. There is a CNF Φ_m with $\Theta(m^{1+2\epsilon})$ variables and $\Theta(m^{1+3\epsilon})$ clauses, of width $O(\log m)$, such that*

(1) *Φ_m has a refutation of length $O(m^{1+3\epsilon})$ and width $m + O(\log m)$*
(2) *Φ_m has no subexponential length refutation of width strictly less than m.*

It follows from (1) that Φ_m has a refutation of width $O(m^{\frac{1}{2}+\epsilon}\sqrt{\log m})$, by Theorem 1. But by (2), as long as $\epsilon < \frac{1}{2}$ every such refutation has exponential length.

This kind of result is known as a *trade-off* between length and width. The reason for the name is that if we need a refutation of small length, we can find one; and if we need a refutation of small width, we can find one; but we must choose between small length and small width, since there is no way to minimize both in the same refutation.

The CNF Φ_m is a propositional version of the *coloured polynomial local search principle*, or CPLS, which was introduced in [2] as a combinatorial principle as strong as reflection for resolution. It thus in some sense captures the strength of resolution, and also of first-order theories built around bounded Π_2 induction (such as Buss's theory T_2^2), as these are closely connected with resolution.

The idea of the lower bound proof is, roughly, that we consider four senses in which a clause can be "narrow" – mostly these differ in which variables we are counting. Given a refutation Π, if Π has small width it follows immediately that every clause in Π is narrow in our first sense. If furthermore Π has subexponential length, then we can hit Π with a random restriction such that with high probability every clause in the resulting refutation is also narrow in the remaining three senses. We then use an adversary argument to show that no such narrow refutation of the restricted CNF can exist.

References

[1] E. Ben-Sasson and A. Wigderson, *Short proofs are narrow - resolution made simple*, Journal of the ACM **48:2** (2001), 149–169.

[2] J. Krajíček, A. Skelley and N. Thapen, *NP search problems in low fragments of bounded arithmetic*, Journal of Symbolic Logic **72:2** (2007), 649–672.

Finitary and Infinitary Approaches to Szemerédi Regularity

Henry Towsner

If U and V are finite sets and $E \subseteq U \times V$, there is a natural notion of density, the *edge density*:

$$d_E(U,V) = \frac{|E \cap (U \times V)|}{|U| \cdot |V|}.$$

If E is chosen randomly, with high probability it should be the case that when $U' \subseteq U$ and $V' \subseteq V$ are big enough, $d_E(U',V') \approx d_E(U,V)$. The pair U,V is said to be ϵ-*regular* if it resembles a random pair in the following precise sense:

> The pair U,V is ϵ-*regular* (with respect to E) if whenever $U' \subseteq U$ and $V' \subseteq V$ with $|U'| \geq \epsilon|U|$ and $|V'| \geq \epsilon|V|$,
>
> $$|d_E(U',V') - d_E(U,V)| < \epsilon.$$

Szemerédi's Regularity lemma says that any finite graph (G,E) can be partitioned $G = \bigcup_{i \leq K} G_i$ so that

$$\sum_{i,j | i \text{ and } j \text{ are not } \epsilon\text{-regular}} |G_i| \cdot |G_j| < \epsilon |G|^2,$$

where the bound K depends only on ϵ–in particular, $|G|$ can be much larger than K. The main idea in the proof is identifying the *energy* of a partition,

$$\mathcal{E}(\{G_i\}) = \sum_{i,j \leq K} d_E^2(G_i, G_j),$$

and observing that when a partition fails to satisfy the lemma, it can be refined to a partition with higher energy.

A very general, stronger version of this statement was formulated by Tao [1]: for any $F : \mathbb{N} \to \mathbb{N}$ and $\epsilon > 0$, there is a K so that any finite graph (G,E) can be partitioned $G = \bigcup_{i \leq K} G_i$ so that if $\bigcup_{i \leq F(K)} H_i$ is a partition refining $\{G_i\}$ then $\mathcal{E}(\{G_i\}) \leq \mathcal{E}(\{H_i\}) + \epsilon$: the partition $\{G_i\}$ has "nearly maximized" the energy. (Tao's version is actually slightly stronger even than this.)

This statement looks like the output of the functional interpretation. We "invert" the functional interpretation to identify a suitable Π_3 statement of which this is this functional interpretation.

Instead of a large finite graph we work with a non-standard graph (X,E) with hyperfinite size. In this setting there are two natural σ-algebras on X^2: the σ-algebra $\mathcal{B}_2$ generated by the definable sets, and the σ-algebra $\mathcal{B}_{2,1}$ generated only by definable rectangles. We can define a measure by taking the standard part—$\mu(S) = st(\frac{|S|}{|X|^2})$. Then standard measure theory tells us that there is a projection: for any $f \in L^2(\mathcal{B}_2)$, there is an $L^2(\mathcal{B}_{2,1})$ function $\mathbb{E}(f \mid \mathcal{B}_{2,1})$ best approximating f in the L^2 norm.

The existence of a projection is a Π_3 statement,

$$\forall \epsilon > 0 \exists g \in L^2(\mathcal{B}_{2,1}) \, \forall h \in L^2(\mathcal{B}_{2,1}) ||f - g||_{L^2} \leq ||f - h||_{L^2} + \epsilon.$$

Furthermore, when we investigate what the projection means in the case of χ_E, we see that the ϵ-almost projection of $\mathbb{E}(\chi_E \mid \mathcal{B}_{2,1})$ is, essentially, a partition of X into (standardly) finitely many pieces most of which are ϵ-regular.

Applying the functional interpretation to this Π_3 statement, we indeed get back Tao's version of the regularity lemma. We discuss generalizations and applications of this idea [2, 3].

References

[1] Terence Tao. Szemerédi's regularity lemma revisited. *Contrib. Discrete Math.*, 1(1):8–28, 2006.

[2] Isaac Goldbring and Henry Towsner. An approximate logic for measures. *Israel J. Math.*, 199(2):867–913, 2014.

[3] Henry Towsner. σ-Algebras for Quasirandom Hypergraphs. draft.

A rule-learning based interpretation for second order arithmetic (Stefano Berardi, Torino University)

Stefano Berardi

We introduce poly-trees, a notion of infinitary tree to represent infinitary proofs of second order logic, a simplification of Girard's Dilators ([1], [2], [3], [4], [5]). Our long-term goal is to define an infinitary sequent calculus for second order arithmetic, using poly-trees as proofs, then proving a normalization result for it and using it for studying an ordinal notation for second order arithmetic. However, this work is self-contained and centered on combinatorial results on poly-trees.

We plan to interpret the proof of a type $\forall \alpha.A$ as a construction $T = \bigvee^L_{i \in k} T_i$ which is indexed over a set k. We call k, using a machine learning terminology, a *training set*. From the set of values $\{T_i | i \in k\}$ over the training set the construction T is able to "learn" how to process new inputs with a "correct" result: we test our learning against a larger set of inputs $\mathtt{t}(k) \supset k$, which we call the *test set*, with the only request that for any $i \in \mathtt{t}(k)$ we may decide whether $i \in k$ or not. As a typical example, a constructor $\bigvee^L_{i \in h}(.)_i$ of $\mathtt{t}(k)$ may have type $h = k$, the very type we are defining. No circularity will arise: we will allow a very limited use of individuals of the form $\bigvee^L_{i \in h} U_i$ with h not "yet defined", taking into account the limited knowledge we have of them.

A type k is a set of trees closed under all at most countable branching, and some branching of uncountable index set h, for some type h defined before k. A type may be characterized by the set of its constructors having an uncountable index set h. We call `PTree` the set of all poly-trees we define. If $\prec$ is decidable, then we may take $\mathtt{t}(k) = \mathtt{PTree}$ for any type k.

We have now to precise how to extend a tree function $i \in k \mapsto T_i$ of training set k over any tree $U = \bigvee^L_{i \in h} U_i \in \mathtt{PTree}$, possibly defined by some constructor

$\bigvee^L_{i\in h}(.)$ not allowed in k. Assume we have in input a tree $U = \bigvee^L_{i\in h} U_i$ defined by a constructor which is *not yet known* when we define k: the two main examples are when $h = k$, or any countable set X which is not part of our current language. In this case the input channel of the tree itself is a kind of "black box", and it is not available to us: we cannot select an index $i \in h$. The only way of using U as input is to produce, as output, a tree $V = \bigvee^L_{i\in h} g(U_i)$ with *the same index set* h as U, defined by some map g. In this way we ask to the "external world" to provide index i in the unknown index set h. In the future we will find some $i \in h$. In this moment, we will use $i \in h$ to select the subtree U_i in the input tree. Then we compute the output $g(U_i)$ out of the value U_i. We call this way of computing *"polymorphism"*, because it works for *many possible shapes* of the unknown elements of the index type h, instead of working for an index type whose elements are known. Polymorphism may use its input only in a very simplified way: we recopy the index type and the label, and we right-compose the branching $i \in h \mapsto U_i$ of the argument with some other map g (maps in our interpretation should be closed by composition).

If we extend the index set k to `PTree`, we obtain a tree $T = \bigvee^L \{T_i | i \in \texttt{PTree}\}$ which may be instanced to any tree $i \in \texttt{PTree}$, not just to the trees i belonging to the training set k. The main property we are going to prove for this kind of trees is the following, which we call the **Lifting Theorem**: *if the restricted version of T is well-founded, then for all $i \in$ `PTree` which are well-founded trees, T_i is well-founded.*

References

[1] Girard Jean-Yves Pi12-logic. I. Dilators, Ann. Math. Logic 21, no. 2-3, 75–219, 1981

[2] Girard Jean-Yves Introduction to Pi12-logic, The present state of the problem of the foundations of mathematics (Florence, 1981). Synthese 62, no. 2, 191–216, 1985

[3] Girard Jean-Yves A survey of Pi-1-2-logic, Logic, methodology and philosophy of science, VI (Hannover, 1979), pp. 89–107, Stud. Logic Foundations Math., 104, North-Holland, Amsterdam-New York, 1982

[4] Jean-Yves Girard, Jacqueline Vauzeilles: Functors and Ordinal Notations. A Functorial Construction of the Bachmann Hierarchy. I:J. Symb. Log. 49(3): 713-729 (1984). II: J. Symb. Log. 49(4): 1079-1114 (1984).

[5] Girard Jean-Yves and Ressayre Jean-Pierre Elments de logique Pi1n [Elements of Pi1n-logic], Recursion theory (Ithaca, N.Y., 1982), 389–445, Proc. Sympos. Pure Math., 42, Amer. Math. Soc., Providence, R.I., 1985

Constructive homotopy theory and models of intensional type theory

Andrej Bauer

Classical homotopy theory is based on the idea of a path as a continuous map defined on a closed interval. Such paths form the fundamental groupoid because two paths may be joined if one ends where the other begins. The argument relies on the fact that by gluing two abutting closed intervals together we get a closed interval. Unfortunately, this need not be the case constructively, and so constructive homotopy theory falls even before it has made the first step.

This phenomenon was observed before by Michael Beeson [1] and Erik Palmgren [2] who each proposed a solution: we may limit attention to spaces with the *path-joining property* in which paths can actually be joined (complete separable metric spaces are such), or we may pass from ordinary spaces to point-free ones, in which case the problem disappears.

In this talk I report on work in a third direction: we may relax the notion of a path as a continuous map defined on a finite gluing of abutting intervals. That is, if $\gamma : [a, b] \to X$ and $\delta : [b, c] \to X$ are paths in X, then they may be joined to give a path $\gamma \cdot \delta : [a, b] \cup [b, c] \to X$, where crucially we do *not* assume that $[a, b] \cup [b, c] = [a, c]$. This leads to a Moore-style presentation of homotopy in which paths are parameterized by many interval-like objects.

In fact, the whole development can be done constructively in extensional type theory, and we need not work specifically with gluings of abutting intervals. Instead, we formulate abstract properties of *an algebra of intervals* and show that they give a notion of fibration and a path object that can be assembled into a model of intensional type theory.

References

[1] M. Beeson, *Foundations of Constructive Mathematics*, Springer 1985.
[2] E. Palmgren, *From intuitionistic to formal topology: some remarks on the foundations of homotopy theory.* In: Logicism, Intuitionism and Formalism - what has become of them? (Eds.: S. Lindström, E. Palmgren, K. Segerberg and V. Stoltenberg-Hansen), Springer 2009, 237–253.

Proof Theoretic Characterisations of Feasible Set Functions

Arnold Beckmann

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

Recently, various restrictions of the primitive recursive set functions relating to feasible computation have been proposed, amongst them the *Safe Recursive Set Functions* [2], the *Predicatively Computable Set Functions* [1], and the *Cobham Recursive Set Functions* (Beckmann, Buss, Friedman, Müller, Thapen – this is work in progress). In this talk I have described ideas how some of these classes can be captured as the Σ_1-definable set functions in suitable restrictions of Kripke-Platek set theory, by elementary proof-theoretic means. In particular, I have described a theory whose Σ_1-definable set functions are exactly the Safe Recursive Set Functions, and another theory whose Σ_1 definable set functions are characterised by the Cobham Recursive Set Functions.

References

[1] T. Arai, *Predicately computable functions on sets.* arXiv:1204.5582, 2014.
[2] A. Beckmann, S. R. Buss, and S.-D. Friedman, *Safe recursive set functions.* Submitted for publication, 2011.

Classical Realizability arising from Domain Theoretic Models of Lambda Calculus with Control

Thomas Streicher

In the first decade of this millenium Jean-Louis Krivine introduced his notion of *classical realizability* giving rise to models of Zermelo-Fraenkel set theory (see [Kri01]). However, for the purpose of realizing the axiom DC of Dependent Choice in [Kri03] he used a kind of `quote` construct as known from the programming language Lisp in contrast to more traditional proof theory where usually *bar recursion* is used for this purpose.

In our talk we present classical realizability models arising from domain-theoretic models of λ-calculus with control by solving the domain equation $D \cong \Sigma^{D^\omega}$ (see [SR98]) where Σ is the 2 element lattice and D^ω is the countable product of D. As shown in [Str13] such realizability structures give rise to classical realizability toposes. When solving the domain equation for D in Scott domains the ensuing topos is equivalent to **Set**. The reason is that Scott domains host the join operation $\vee : \Sigma \times \Sigma \to \Sigma$. This operation does not exist in the category **Coh** of coherence spaces and stable continuous functions between them. When solving the domain equation for D in **Coh** one obtains a classical realizability topos $\mathcal{K}$ which is not a Grothendieck topos and thus, in particular, not a forcing model.

Since D allows for general recursive definitions one can construct within D a bar recursor by which one can realize DC. For verifying this we use bar induction on the meta level which is admissible since in D one can represent all sequences of elements in D. This also guarantees that $\mathcal{K}$ validates all true first order sentences of arithmetic.

We conclude with the following two open questions

(1) Is $\mathcal{K}$ 2-valued?
(2) Does DC still hold when restricting D to computable elements?

A negative answer to the second question would demonstrate that in general classical realizability does not validate dependent choice as conjectured by Krivine but unproved so far.

References

[Kri01] J.-L. Krivine *Typed lambda-calculus in classical Zermelo-Fraenkel set theory* Arch. Math. Logic 40(3), pp. 189-205, 2001.

[Kri03] J.-L. Krivine *Dependent choice, 'quote' and the clock* Theor. Comput. Sci., Vol. 308, pp. 259-276, 2003.

[Str13] T. Streicher *Krivine's classical realisability from a categorical prespective* Math. Struct. Comp. Sci., Vol. 23, pp. 1234-1256, 2013.

[SR98] T. Streicher and B. Reus *Classical logic, continuation semantics and abstract machines.* J. Funct. Prog. 8, no. 6, pp. 543-572, 1998.

Results around a nonstandard functional interpretation

Benno van den Berg
(joint work with Eyvind Briseid and Pavol Safarik)

In recent work with Eyvind Briseid and Pavol Safarik we defined functional interpretations for systems for nonstandard arithmetic. We used these interpretations to prove conservation and term extraction results.

In the talk I explained how the nonstandard functional interpretation could have been found without aiming for a proof-theoretic analysis of nonstandard systems, but rather by modifying certain ideas for refined term extraction. I started from Lifschitz' paper on calculable numbers [7]: his idea was that constructive arithmetic could be seen as an extension of classical arithmetic. He did this by adding a new unary predicate K to the language of arithmetic and defining a realizability interpretation of the extended theory where the old arithmetical quantifiers where interpreted uniformly, while x is the only realizer of $K(x)$. As a result, the relativised quantifiers are interpreted as in Kleene's 1945 realizability. Similar ideas with two kinds of quantifiers, one computationally empty and one with computational content, have surfaced in the work of many people (Troelstra, Berger, Hernest and many others).

In fact, in Lifschitz' work one does not just have two kinds of quantifiers, but also two kinds of disjunctions. To eliminate this one could weaken the meaning of $K(x)$ by saying that a realizer for $K(x)$ is a (coded) sequence $\langle s_1, \ldots, s_n \rangle$ with $x = s_i$ for some i. Clearly, this also changes (weakens) the computational content of the existential quantifiers. But it can be used to define a realizability interpretation which we have dubbed *Herbrand realizability*.

Herbrand realizability does not in itself provide a good analysis of nonstandard systems. However, the associated functional interpretation (which stands to Herbrand realizability in the same way as the Dialectica interpretation stands to modified realizability) has characteristic principles which are recognisable as principle from nonstandard analysis, especially in the approach taken by Edward Nelson in his Internal Set Theory [9, 10].

In this talk I also reported on other developments:

- In a recent preprint [2] with Sam Sanders we clarified the status of the transfer principle in our theories. We obtained an improved conservation result in the classical case; we also established a precise link between transfer principles and forms of comprehension.
- In ongoing work with Eyvind Briseid and Pavol Safarik, we show that countable saturation has no proof-theoretic strength intuitionistically; however, it follows from recent work by Escardo and Oliva [5] that, classically, it has the strength of full second-order arithmetic.
- This proof-theoretic work led to the definition of two new toposes [3, 4]. In his master thesis Amar Hadzihasanovic studied the relation between these toposes and the sheaf topos for nonstandard arithmetic found by Ieke

Moerdijk [8] and further investigated by Erik Palmgren. These results are reported in [6].

This framework also promises to be suitable for the purposes of Reverse Mathematics; in addition, it may provide a translation manual between the model-theoretic approaches and proof-theoretic approaches towards establishing uniformities (non-standard models versus proof-mining).

References

[1] B. van den Berg, E. Briseid and P. Safarik, *A functional interpretation for nonstandard arithmetic*, Ann. Pure Appl. Logic **163** (2012), number 12, 1962–1994.

[2] B. van den Berg and S. Sanders, *Transfer equals comprehension*. arXiv:1409.6881, 2014.

[3] B. van den Berg, *The Herbrand topos*, Math. Proc. Cambridge Philos. Soc. **155** (2013), number 2, 361–374.

[4] B. van den Berg, *A topos for a nonstandard functional interpretation*. arXiv:1301.3679, 2014.

[5] M. Escardo and P. Oliva, *The Herbrand Functional Interpretation of the Double Negation Shift*. arXiv:1410.4353, 2014.

[6] A. Hadzihasanovic and B. van den Berg, *Nonstandard functional interpretations and categorical models*. Accepted for publication in the *Notre Dame Journal of Formal Logic*. arXiv:1301.3679, 2014.

[7] V. Lifschitz, *Calculable natural numbers*. In: *Intensional mathematics*, 173–190, Stud. Logic Found. Math., 113, North-Holland, Amsterdam, 1985.

[8] I. Moerdijk, *A model for intuitionistic non-standard arithmetic*. A tribute to Dirk van Dalen. Ann. Pure Appl. Logic **73** (1995), no. 1, 37–51.

[9] E. Nelson, *Internal set theory: a new approach to nonstandard analysis*. Bull. Amer. Math. Soc. **83** (1977), no. 6, 1165–1198.

[10] E. Nelson, *The syntax of nonstandard analysis*. Ann. Pure Appl. Logic **38** (1988), no. 2, 123–134.

Definability and Non-Definability in Intuitionistic Logic

Andrew Swan

If T is a first order theory and $\psi(x)$ and $\phi(x)$ are formulas over T with one free variable, then we say $\psi(x)$ *defines a witness for* $\phi(x)$ if $T \vdash \exists! x\ \psi(x)$ and $T \vdash \psi(x) \to \phi(x)$. We say T has the *existence property* (EP) if whenever $T \vdash \exists x\ \phi(x)$, there is some $\psi(x)$ that defines a witness for ϕ.

The existence property is sometimes considered as something that ought to hold for constructive theories because of the BHK interpretation of existential quantifiers. It is therefore natural to ask whether commonly used constructive set theories satisfy the existence property.

In [1], Friedman and Ščedrov showed that **IZF**, an intuitionistic version of **ZF** does not have EP, even though it does have other "nice" constructive properties such as the numerical existence property, disjunctive property and Church's rule. The cause appears to be the "non explicit" collection axiom. However, in some cases set theories with collection can still have the existence property. Rathjen showed that three variants of **CZF** have EP: $\mathbf{CZF}^-$, $\mathbf{CZF}_E$ and $\mathbf{CZF}_{\mathcal{P}}$ (see [2]). All three satisfy collection.

In [2], it was left open whether or not **CZF** itself has EP. I showed in [3] that in fact **CZF** does not have EP. One of the main ideas in the proof is fairly simple and can be illustrated with an example using intuitionistic ordered fields. I will prove that the formula $\exists x\ (x^2-2)(x^2-3)=0$ has no definable witnesses when added as an axiom to the theory of intuitionistic ordered fields (although it does when added to the classical theory of ordered fields).

I will also cover some recent work relating the existence property to type theory. Propositional truncation can be added to type theory to allow one to "squash" a type down to a proposition (a type where any two elements are equal to each other). It has recently received a lot of attention due to its heavy use in homotopy type theory. I will show how propositional truncation can be used to state the existence property for variants of intensional type theory. This raises interesting questions regarding the status of the existence property for several variants of type theory.

References

[1] H. Friedman, A. Ščedrov, *The lack of definable witnesses and provably recursive functions in intuitionistic set theory*, Advances in Mathematics, **57** (1985), 1–13.

[2] M. Rathjen, *From the weak to the strong existence property*, Annals of Pure and Applied Logic, **163** (2012), 1400 – 1418,

[3] A.W. Swan, *CZF does not have the existence property*, Annals of Pure and Applied Logic, **165** (2014), 1115 – 1147.

A functional interpretation of $\mathsf{KP}\omega$

Fernando Ferreira

The Σ-ordinal of Kripke-Platek set theory (with infinity) $\mathsf{KP}\omega$ is by definition

$$||\mathsf{KP}\omega||_\Sigma := \min\{\alpha : L_\alpha \models \psi \text{ for all } \Sigma\text{-sentences } \psi \text{ such that } \mathsf{KP}\omega \vdash \psi\}.$$

In [1], William Howard introduced a term calculus for the so-called primitive recursive tree functionals of finite type. This typed calculus has two base types: one for the natural numbers and the other (denoted by Ω) for Howard's constructive ordinals. To each closed term q of type Ω it is naturally associated an ordinal height $|q|$. By means of a functional interpretation (based on the work of Jeremy Avigad and Henry Towsner in [2]), we show that $||\mathsf{KP}\omega||$ is

$$\sup\{|q| : q \text{ is a closed term of the base type } \Omega\}.$$

This is the well-known Bachmann-Howard ordinal. Hence, our work presents an alternative characterization of the Σ-ordinal of $\mathsf{KP}\omega$, one that does not rely on the traditional Gentzen type ordinal analysis. The functional interpretation gives extra information, namely it yields a "growth" characterization of the Π_2-consequences of $\mathsf{KP}\omega$ via suitable terms of Howard's calculus applied to the stages of Gödel's constructible hierarchy. The functional interpretation generalizes to a natural second-order extension of $\mathsf{KP}\omega$ with strict Π^1_1-reflection. We prove that this second-order extension is Σ-conservative over $\mathsf{KP}\omega$. It is an open question

whether it is also Π_2-conservative. This part of the presentation is based on the paper [3].

In the remainder of the presentation, we showed how a modification of the above functional interpretation is able to analyze the theory $\mathsf{KP}\omega(\mathcal{P})$, roughly Kripke-Platek set theory with a primitive power set operation (hence, quantification under set inclusion is considered a bounded quantification). The notion of $\Sigma^{\mathcal{P}}$-formula is naturally defined and it is shown that the relativized $\Sigma^{\mathcal{P}}$-ordinal of $\mathsf{KP}\omega(\mathcal{P})$, defined as

$$\min\{\alpha : V_\alpha \models \psi \text{ for all } \Sigma^{\mathcal{P}}\text{-sentences } \psi \text{ such that } \mathsf{KP}\omega(\mathcal{P}) \vdash \psi\}$$

is also the Bachmann-Howard ordinal. This reproves a recent result of Michael Rathjen reported in [4]. A "growth" characterization of the $\Pi^{\mathcal{P}}_2$-consequences of $\mathsf{KP}\omega(\mathcal{P})$ is also given, but now in terms of the the stages of the cumulative hierarchy (instead of the constructible hierarchy). These results are not yet published, nor fully checked.

References

[1] W. Howard, *A system of abstract constructive ordinals*, The Journal of Symbolic Logic **37(2)** (1972), 355–374.

[2] J. Avigad and H. Towsner, *Functional interpretation and inductive definitions*, The Journal of Symbolic Logic **74(4)** (2009), 1100–1120.

[3] F. Ferreira, *A new computation of the* Σ*-ordinal of* $\mathsf{KP}\omega$, The Journal of Symbolic Logic **79(1)** (2014), 306–324.

[4] M. Rathjen, *Relativized ordinal analysis: The case of Power Kripke-Platek set theory*, Annals of Pure and Applied Logic **165(1)** (2014), 316–339.

Logical representations of partial, mutable and reusable data

Ulrich Berger

In the talk we highlight some shortcomings of the proof-theoretic technique of program extraction from proofs regarding the representation of data and make proposals for overcoming them in a logic-oriented way.

1. Introduction

Program extraction (via realizability) from proofs in intuitionistic arithmetic and related systems generates terms in a suitable extension of Gödel's system T, that is in a *functional programming language*. This is fine in theory, but insufficient in practice. In order to extract programs that are of practical relevance one should be able to

- control the way computed data are stored so that they can be reused
- allow for partially defined data
- override data that are no longer used
- control the computational complexity of extracted programs

Quite a lot of work has been done on the last item. This talk will address the less explored first three items. As illustrating examples we use the signed digit and Gray-code representation of real numbers as well as in-place Quicksort.

2. Induction

Our background theory is first-order logic with inductive definitions: For every monotone operator $\Phi : \mathbf{Pow}(X) \to \mathbf{Pow}(X)$ we can define its least fixed point $\mu\Phi \subseteq X$. We call $\mu\Phi$ the set *inductively* defined by Φ. Instead of "$I := \mu\Phi$" we write "$I \stackrel{\mu}{=} \Phi(I)$" or "$I(x) \stackrel{\mu}{=} \Phi(I)(x)$". If $I \stackrel{\mu}{=} \Phi(I)$ we have for every subset A of X the *induction principle*

$$\Phi(A) \subseteq A \to I \subseteq A$$

Inductive definitions give rise to wellfounded trees and structural recursion.

As an example we consider real numbers $(\mathbb{R}, 0, 1, +, *, <, \ldots)$ as an abstract structure described by true disjunction-free first-order axioms. Natural numbers are defined inductively as a subset of $\mathbb{R}$.

$$\mathbb{N}(x) \stackrel{\mu}{=} x = 0 \vee \mathbb{N}(x - 1)$$

This generates the unary representation of natural numbers. A program for addition is extracted from a proof that the predicate $\mathbb{N}$ is closed under addition.

In order to compute with real numbers, we first define the set $\mathbb{Q}$ of rational numbers and then define when a real number can be approximated arbitrarily well by rational numbers:

$$A(x) := \forall n \in \mathbb{N}\, \exists q\, \in \mathbb{Q} |x - q| \leq 2^{-n}$$

A realizer of $A(x)$ is a fast Cauchy sequence (given as a function from $\mathbb{N}$ to $\mathbb{Q}$) converging to x. We can extract addition w.r.t. the Cauchy representation from a proof that A is closed under addition.

3. Coinduction

We obtain a representation of reals by infinite *streams* instead of *functions* by *coinduction*: We extend the logic by allowing to define a set as the largest fixed point $\nu\Phi$ of a monotone operator $\Phi : \mathbf{Pow}(X) \to \mathbf{Pow}(X)$. We call $\nu\Phi$ the set *coinductively* defined by Φ. Instead of "$I := \nu\Phi$" we write "$I \stackrel{\nu}{=} \Phi(I)$" etc. If $I \stackrel{\nu}{=} \Phi(I)$ we have for every subset A of X the *coinduction principle*

$$A \subseteq \Phi(A) \to A \subseteq I$$

We define a coinductive predicate expressing that a real number x in the interval $[-1, 1]$ has a signed digit representation:

$$\mathrm{C}(x) \stackrel{\nu}{=} x \in [-1, 1] \wedge \exists d \in \{-1, 0, 1\}\ \mathrm{C}(2x - d)$$

A realizer of $\mathrm{C}(x)$ is an infinite stream of signed digits $d_0 : d_1 : \ldots$ such that

$$x = \sum_i d_i 2^{-(i+1)}$$

This representation can be generalized to a nested inductive/coinductive definition of continuous real functions yielding a representation of such functions as non-wellfounded trees. Programs with respect to these representations have been extracted in the Minlog system [2].

Remark. In mathematics we tend to identify infinite streams with functions defined on the natural numbers. In programming, streams and functions are very *different*: A *function* is stored as a *closure*, i.e. a piece of code (representing the λ-term defining the function) together with an environment for the free variables. On the other hand, a *stream* is stored as a dynamically linked list containing the elements of the stream computed so far, together with code defining the yet uncomputed rest of the stream. The crucial difference between functions and streams is that if a value of a function is needed again, it is recomputed, while if an element of a stream is needed again, it just needs to be looked up.

4. Dynamic induction

Gaining efficiency by remembering computed values of a recursively defined function is often called *dynamic programming*. Dynamic programming has a logical counterpart which we call *dynamic induction*. It consists in proving the induction scheme using coinduction and a trivial instance of induction.

The program extracted from dynamic induction realizes $\mathbb{N} \subseteq A$ as an infinite stream (coinduction) and looks up its elements (induction). Dynamic induction generalizes in a straightforward way from $\mathbb{N}$ to inductive definitions of the form

$$I(x) \stackrel{\mu}{=} B(x) \vee \exists y < x\, I(y)$$

for arbitrary predicates B and relations $<$. It is open whether this can be extended to arbitrary strictly positive inductive definitions. The problem seems to be related to work by Hinze [4] and Altenkirch [1].

5. Gray code

The Gray code (discovered by Frank Gray in 1946 who called it "reflected binary code") is an alternative to the binary representation of natural numbers where neighbouring numbers differ in only one digit. Tsuiki extended this to a representation of real numbers [5]. The Gray code of $x \in [-1, 1]$ is the itinerary of the tent map $\mathrm{t}(x) = 1 - 2|x|$, i.e. the n-th digit is 0 resp. 1 if $t^n(x) < 0$ resp. > 0. If $t^n(x) = 0$, the n-th digit is undefined. One easily sees that at most one digit of the Gray code can be undefined. Therefore, computation with the Gray code can be modelled by a *Two-Head-Turing-Machine*. Such a machine cannot be extracted from a proof in the current system since it exhibits a kind of parallelism that is absent in extracted programs. In ongoing work we try to develop a logic where this is possible.

6. Extracting programs with destructive update

The well-known Quicksort algorithm can be implemented by successively swapping the elements of the array to be sorted (in-place quicksort). This program cannot be extracted because it destructively changes the array. Extracted programs are purely functional and never destroy data.

However, one can give a proof that every array of natural numbers can be sorted in such a way that the extracted program can be canonically transformed to the imperative in-place quicksort program [3]. We are currently developing logic that directly extracts such programs.

References

[1] T. Altenkirch, *Representations of first order function types as terminal coalgebras*, LNCS **2044** (2001), 8–21.

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

[3] U. Berger, M. Seisenberger, G. Woods, *Extracting Imperative Programs from Proofs: In-place Quicksort*, LIPICS **26** (2014), 84–106.

[4] R. Hinze, *Generalizing generalized tries*, JFP **10** (2000), 327–351.

[5] H. Tsuiki. *Real Number Computation through Gray Code Embedding*, TCS **284** (2002), 467–485.

CH and semi-intuitionism

Michael Rathjen

Dummett's diagnosis of the failure of Frege's logicist focusses on the adoption of classical quantification over domains comprised of objects falling under an indefinitely extensible concept. He repudiates the classical view as illegitimate and puts forward reasons in favor of an intuitionistic interpretation of quantification. Solomon Feferman, in recent years, has argued that the Continuum Hypothesis (CH) might not be a definite mathematical problem (see [2, 3, 4]).[1] *"My reason for that is that the concept of arbitrary set essential to its formulation is vague or underdetermined and there is no way to sharpen it without violating what it is supposed to be about. In addition, there is considerable circumstantial evidence to support the view that CH is not definite."* ([2, p.1]) In particular the power set, $\mathcal{P}(A)$, of a given set A may be considered to be an indefinite collection whose members are subsets of A, but whose exact extent is indeterminate (open-ended). In [2], Feferman proposed a logical framework for what's definite and for what's not. *"One way of saying of a statement φ that it is definite is that it is true or false; on a deflationary account of truth that's the same as saying that the Law of Excluded Middle (LEM) holds of φ , i.e. one has $\varphi \vee \neg\varphi$. Since LEM is rejected in intuitionistic logic as a basic principle, that suggests the slogan, "What's definite is the domain of classical logic, what's not is that of intuitionistic logic." [...] And in the case of set theory, where every set is conceived to be a definite totality,*

[1] Incidentally, the paper [2] was written for Peter Koellner's *Exploring the frontiers of incompleteness* (EFI) Project, Harvard 2011-2012.

we would have classical logic for bounded quantification while intuitionistic logic is to be used for unbounded quantification." ([2, p. 23]) At the end of [2] he made that idea more precise by suggesting semi-intuitionistic set theories from [1] as frameworks for formulating questions of definiteness and studying the definiteness of specific set-theoretic statements. In relation to CH, he conjectured that this statement is not definite in the specific case of a semi-intuitionistic set theory $\mathbf{T}$, in the sense that $\mathbf{T}$ does not prove $CH \vee \neg CH$. The set-theoretical point of view expressed by $\mathbf{T}$ accepts the definiteness of the continuum in its guise as the arithmetical/geometric structure of the real line, but does not allow the powerset operation to be applied to arbitrary sets.

The objective of this talk to report on the paper [5] which proves Feferman's conjecture. [5] is a technical paper. It lays out new evidence for the reader to consider. However, as far as the ongoing discussions of the foundational status of CH are concerned, readers will have to form their own conclusions.

A chief technique applied in this article is realizability over relativized constructible hierarchies combined with forcing. More widely the impression is that CH is not an isolated case in that other statements could be proved to be indefinite relative to semi-intuitionistic set theories in this way. At any rate, it appears that the paper adds a hitherto unexplored tool for engineering specific realizability models and proving independence results.

References

[1] S. Feferman, *On the strength of some semi-constructive theories*, in: U.Berger, P. Schuster, M. Seisenberger (Eds.): *Logic, Construction, Computation* (Ontos Verlag, Frankfurt, 2012), 201–225.

[2] S. Feferman, *Is the continuum hypothesis a definite mathematical problem?*. Draft of paper for the lecture to the Philosophy Dept., Harvard University, Oct. 5, 2011 in the *Exploring the Frontiers of Incompleteness* project series, Havard 2011–2012.

[3] S. Feferman, *Three Problems for Mathematics: Lecture 2: Is the Continuum Hypothesis a definite mathematical problem?*, Slides for inaugural Paul Bernays Lectures, ETH, Zürich, Sept. 12, 2012.

[4] S. Feferman, *Why isn't the Continuum Problem on the Millennium ($1,000,000) Prize list?*. Slides for CSLI Workshop on Logic, Rationality and Intelligent Interaction, Stanford, June 1, 2013.

[5] M. Rathjen, *Indefiniteness in semi-intuitionistic set theories: On a conjecture of Feferman*, arXiv:1405.4481 (2014), 17 pages.

Reporter: Daniel Körnlein

Participants

Prof. Dr. Peter Aczel
Department of Computer Science
University of Manchester
Oxford Road
Manchester M13 9PL
UNITED KINGDOM

Dr. Bahareh Afshari
Institut f. Algebra & Diskrete Mathematik
Technische Universität Wien
Wiedner Hauptstraße 8 - 10
1040 Wien
AUSTRIA

Prof. Dr. Toshiyasu Arai
Graduate School of Sciences
Chiba University
Yayoi-cho 1-33, Inage
Chiba 263-8522
JAPAN

Prof. Dr. Sergei N. Artemov
Computer Science Program
CUNY Graduate Center
365 Fifth Avenue
New York, NY 10016
UNITED STATES

Dr. Federico Aschieri
Lab. de l'Informatique du Parallèlisme
Equipe Plume, E.N.S.
46, Allée d'Italie
69364 Lyon Cedex
FRANCE

Prof. Dr. Jeremy Avigad
Department of Philosophy
Carnegie Mellon University
Pittsburgh, PA 15213-3890
UNITED STATES

Prof. Dr. Matthias Baaz
Institut f. Algebra & Diskrete Mathematik
Technische Universität Wien
Wiedner Hauptstraße 8 - 10
1040 Wien
AUSTRIA

Prof. Dr. Andrej Bauer
Faculty of Mathematics & Physics
University of Ljubljana
Jadranska 21
1000 Ljubljana
SLOVENIA

Prof. Dr. Arnold Beckmann
Department of Computer Science
Swansea University
Singleton Park
Swansea SA2 8PP
UNITED KINGDOM

Prof. Dr. Lev D. Beklemishev
V.A. Steklov Institute of Mathematics
Russian Academy of Sciences
8, Gubkina St.
119991 Moscow GSP-1
RUSSIAN FEDERATION

Prof. Dr. Stefano Berardi
C. S. Department; Fac. SMFN
University of Torino
Via Pessinetto 12
10149 Torino
ITALY

Dr. Ulrich Berger
Department of Computer Science
Swansea University
Singleton Park
Swansea SA2 8PP
UNITED KINGDOM

Prof. Dr. Vasco Brattka
Institute for Theoretical Computer Science,
Mathematics and Operations Research
Faculty of Computer Science
Universität der Bundeswehr München
Werner-Heisenberg-Weg 39
85579 Neubiberg
GERMANY

Ulrik Torben Buchholtz
Department of Mathematical Sciences
University of Copenhagen
Universitetsparken 5
2100 Copenhagen
DENMARK

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

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

Prof. Dr. Fernando Ferreira
Departamento de Matematica
Universidade de Lisboa, FCUL
Campo Grande, ED. C6, piso 2
1749-016 Lisboa
PORTUGAL

Michal Garlik
Faculty of Mathematics & Physics
Charles University
118 00 Praha 1
CZECH REPUBLIC

Prof. Dr. J. Martin E. Hyland
Dept. of Pure Mathematics & Math. Statistics
University of Cambridge
Wilberforce Road
Cambridge CB3 0WB
UNITED KINGDOM

Dr. Rosalie Iemhoff
Department of Philosophy
Utrecht University
Janskerkhof 13
3512 BL Utrecht
NETHERLANDS

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

Prof. Dr. Joost Joosten
Dept. de Logica, Historia i Filosofia de la Ciencia
Universitat de Barcelona
Montalegre 6
08001 Barcelona
SPAIN

Prof. Dr. Ulrich Kohlenbach
Fachbereich Mathematik
TU Darmstadt
Schloßgartenstr. 7
64289 Darmstadt
GERMANY

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

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

Daniel Körnlein
Fachbereich Mathematik
TU Darmstadt
Schloßgartenstr. 7
64289 Darmstadt
GERMANY

Angeliki Koutsoukou-Argyraki
Department of Mathematics
Waseda University
3-4-1 Ohkubo, Shinjuku-ku
Tokyo 169-8555
JAPAN

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

Dr. Alexander P. Kreuzer
Department of Mathematics
National University of Singapore
13, Lower Kent Ridge Rd.
Singapore 119 260
SINGAPORE

Dr. Graham E. Leigh
Institut für Diskrete Mathematik & Geometrie
Technische Universität Wien
Wiedner Hauptstr. 8-10
1040 Wien
AUSTRIA

Dr. Laurentiu Leustean
Institute of Mathematics "Simion Stoilow"
of the Romanian Academy
P.O. Box 1-764
014 700 Bucharest
ROMANIA

Prof. Dr. Henri Lombardi
Faculté des Sciences et Techniques
Laboratoire Mathématiques de Besancon
Université de Franche-Comte
16, route de Gray
25030 Besancon Cedex
FRANCE

Prof. Dr. Per Martin-Löf
Matematiska Institutionen
Stockholms Universitet
106 91 Stockholm
SWEDEN

Dr. Sebastian Müller
Center for Exploring the Limits of Computation
Tokyo Institute of Technology
3-3-6 Shibaura, Minato-ku
108-0023 Tokyo
JAPAN

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

Dr. Iosif Petrakis
Mathematisches Institut
L.-M.-Universität Muenchen
Theresienstr. 39
80333 München
GERMANY

Dr. Thomas Powell
Fakultät f. Mathematik, Informatik & Physik
Universität Innsbruck
Technikerstraße 19a
6020 Innsbruck
AUSTRIA

Prof. Dr. Pavel Pudlak
Institute of Mathematics of the AV CR
Zitna 25
115 67 Praha 1
CZECH REPUBLIC

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

Prof. Dr. Peter M. Schuster
Department of Pure Mathematics
University of Leeds
Woodhouse Lane
Leeds LS2 9JT
UNITED KINGDOM

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

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

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

Prof. Dr. Thomas Streicher
Fachbereich Mathematik, AG Logik
TU Darmstadt
Schlossgartenstr. 7
64289 Darmstadt
GERMANY

Dr. Andrew Swan
School of Mathematics
University of Leeds
Leeds LS2 9JT
UNITED KINGDOM

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

Prof. Dr. Henry Towsner
Department of Mathematics
University of Pennsylvania
209 South 33rd St.
Philadelphia PA 19104-6395
UNITED STATES

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

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

Prof. Dr. Andreas Weiermann
Gent Universiteit
Vakgroep Wiskunde en Computeralgebra
Krijgslaan 281, Gebouw S22
9000 Gent
BELGIUM