Mathematisches Forschungsinstitut Oberwolfach

Report No. 52/2011

DOI: 10.4171/OWR/2011/52

Mathematical Logic: Proof Theory, Constructive Mathematics

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

November 6th – November 12th, 2011

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 (2000): 03Fxx.

Introduction by the Organisers

The workshop *Mathematical Logic: Proof Theory, Constructive Mathematics* was held November 6-12, 2011 and included three tutorials:

(1) Sergei N. Artemov: Provability vs. computational semantics for intuitionistic logic (2 times 1 hour),
(2) Jan Krajíček: Search for hard tautologies (3 times 1 hour),
(3) Angus MacIntyre: Issues around proving Fermat's Last Theorem (FLT) in Peano Arithmetic (3 times 1 hour).

Artemov's tutorial gave an introduction to the provability semantics (based on explicit proof polynomials) for intuitionistic logic as developed for propositional logic by the author since 1995 and its very recent 2011 extension to a first-oder logic of proofs by himself and T. Yavorskaya. Krajíček's tutorial gave a survey on recent developments in the area of proof complexity and bounded arithmetic. Macintyre presented some of the key ingredients of Wiles' proof of FLT and outlined how the necessary mathematics could in principle be formalized in a suitable conservative extension of Peano Arithmetic PA.

In addition to these tutorials, 24 short talks of 25 minutes were given aiming:

To promote the interaction of proof theory with core areas of mathematics via the use of proof theoretic techniques to unwind ineffective proofs in mathematics. Two talks (L. Leuştean, P. Safarik) reported on recent extractions of explicit rates of metastability (in the sense of T. Tao) from proofs in nonlinear ergodic theory, while J. Gaspar gave an unwinding of a proof in metric fixed point theory and reported on proof-theoretic results concerning different finitizations (again in the sense of Tao) of the infinite pigeonhole principle. Applications of the method of cut-elimination to proofs in theories with axioms having a suitable logical form were the subject of another talk (S. Negri). A. Kreuzer talked about a proof-theoretic analysis of important principles in Ramsey theory and their connection to analytic principles. Other talks focussed on the more theoretical side of proof interpretations such as a novel functional interpretation for nonstandard analysis (B. van den Berg), refined negative interpretations (H. Ishihara), connections between Spector's bar recursion and methods to compute Nash equilibria based on products of selection functions (P. Oliva) and recent developments on the ε-substitution method (G. Mints). P. Schuster gave a constructive reformulation of certain type of ineffective proofs in algebra while D.S. Bridges talked about different constructive formulations of the Riemann series theorem. A talk by H. Schwichtenberg was concerned with a novel inductive/coinductive treatment of continuous functions. Real numbers as an abstract data type for the extraction of programs from proofs was presented by A. Setzer.

To further develop foundational aspects of proof theory and constructive mathematics. Two talks (G.E. Leigh, T. Strahm) investigated proof-theoretic properties of theories of truth. Other talks dealt with new conservation results for systems of constructive set theory (L. Gordeev) and recent developments in Voevodsky's program of 'univalent foundations' which was the subject of another Oberwolfach workshop in October (P. Aczel). Two further talks discussed approaches to ordinal notations based on reflection principles (L. Beklemishev) and 'patterns of resemblance' due to T.J. Carlson (G. Wilken), respectively. A talk by G. Jäger investigated the proof-theoretic strength of operational systems of set theory (formulated in the framework of Feferman's explicit mathematics). A talk by A. Visser was concerned with the provability logic of arithmetics.

To explore further the connections between logic and computational complexity: this concerns both proof-theoretic results of systems of bounded arithmetic (A. Beckmann) as well as an understanind of what makes certain formulas hard for current SAT-solvers while even very large formulas stemming from concrete applications often can be decided rather efficiently by these tools. (J. Nordström). An axiomatic approach to the issue of the intrinsic complexity for general classes of algorithmic problems in arithmetic and algebra in terms of absolute lower bounds was developed in a talk by Y. Moschovakis based on a so-called homomorphism method.

Workshop: Mathematical Logic: Proof Theory, Constructive Mathematics

Table of Contents

Abstracts

On Voevodsky's Univalence Axiom

Peter Aczel

The aims of my talk were (1) to state the Univalence Axiom, a new axiom to be added to Per Martin-Löf's Dependent type theory **MTT**, and (2) to motivate the axiom as an expression of a strong form of the Structure Identity Principle (**SIP**). This principle expresses that isomorphic structures are structurally identical; i.e. have the same structural properties. But what is a structural property?

In mathematical practise, the notion is not precisely defined, but is usually intuitively understood.

In logic, there can be a precise answer: Given a signature s for a certain kind of structure and a suitable logical formal language L, each set of sentences T of L determines the structural property P_T where, for s-structures $\mathcal{A}$,

$$P_T(\mathcal{A}) \text{ iff } \mathcal{A} \text{ is a model of } T.$$

In category theory, when working with a category of structures, equality between structures is considered not to be meaningful and so not allowed to be expressed in the language used to express properties of the category, so that all properties of the objects of the category are structural.

It seems to turn out that, in MTT with the Univalence Axiom for a given type universe of small types, all properties of a small structure that can be expressed in the language of MTT can be taken to be structural, as isomorphic small structures are identical in the sense of the type theoretic identity relation on the type of such small structures.

Provability vs. computational semantics for intuitionistic logic

Sergei N. Artemov

The intended semantics of intuitionistic logic is Brouwer-Heyting-Kolmogorov (BHK) provability semantics (cf. [8, 10, 13]). It starts from Brouwer's thesis that intuitionistic truth is provability, i.e., a proposition is true if it has a proof. In particular, it stipulates that

(1) a proof of $A \to B$ is a construction which, given a proof of A, returns a proof of B;
(2) a proof of $A \wedge B$ consists of a proof of A and a proof of B;
(3) a proof of $A \vee B$ is given by presenting either a proof of A or a proof of B;
(4) a proof of $\forall x A(x)$ is a function converting c into a proof of $A(c)$;
(5) a proof of $\exists x A(x)$ is a pair (c, d) where d is a proof of $A(c)$.

Speaking informally, BHK semantics deals with both proofs and computable functions (constructions). Since in a formal mathematical setting, a computational program does not yield a proof of its correctness, one should not expect a purely computational model to provide an adequate account of BHK. On the other hand, a formal proof of a sigma-formula yields a corresponding computational program, hence a proof-based semantics could, in principle, represent BHK in its entirety.

BHK ideas inspired Kleene's realizability [9], which led to the class of *computational interpretations* for intuitionistic logic with their vast applications in constructive logic, Computer Science, etc. Despite basic similarities, there are conceptual differences between provability and computational BHK models, e.g., the basic proof predicate *'p is a proof of F'* is **decidable**, whereas the basic realizability assertion *'p realizes F'* is **not decidable**. Realizability does not satisfy the original BHK clause concerning disjunction. In realizability, there is the extra requirement of a bit indicator that points at the proper disjunct (cf. [14, 15, 16]) which was not present in the original BHK since, given a proof p, we always 'know' which of the disjuncts it proves. As it was pointed out by Kreisel in [11], in clause (4), BHK semantics should provide a proof that the corresponding function has the property required, but realizability does not appear to do this. A good example of computational BHK semantics is given by Martin-Löf type theory [12]. Though it uses a BHK proof terminology, Martin-Löf 'proofs' or 'constructions' are not identified with formal proofs (cf. [15]), but rather have a natural computational interpretation.

The original provability reading of BHK, despite early progress made by Gödel in [6, 7], turned out to be quite elusive. An exact provability BHK semantics for the propositional intuitionistic logic IPC was found only in 1995 within the framework of the logic of proofs LP [1, 2]. This led to a mathematical theory of justifications with a fast growing area of applications, e.g., in epistemology [3, 4].

In this talk, in addition to surveying the aforementioned results, we present the *first-order logic of proofs* FOLP capable of realizing the first-order intuitionistic logic HPC and enjoying a provability interpretation (a joint work with Tatiana Yavorskaya [5], 2011). We show that FOLP provides an exact provability semantics for intuitionistic logic, meets the original BHK specifications, and escapes the discussed defects of the computational BHK semantics.

References

[1] S. Artemov. *Operational modal logic.* Technical Report MSI 95-29, Cornell University, 1995.

[2] S. Artemov. Explicit provability and constructive semantics. *Bulletin of Symbolic Logic*, 7(1):1–36, 2001.

[3] S. Artemov. The logic of justification. *The Review of Symbolic Logic*, 1(4):477–513, 2008.

[4] S. Artemov and M. Fitting. Justification Logic. *The Stanford Encyclopedia of Philosophy* (Fall 2011 Edition), Edward N. Zalta (ed.), 2011. http://plato.stanford.edu/archives/fall2011/entries/logic-justification/

[5] S. Artemov and T. Yavorskaya (Sidon). *First-Order Logic of Proofs.* Technical Report TR-2011005, CUNY Ph.D. Program in Computer Science, 2011. http://tr.cs.gc.cuny.edu/tr/techreport.php?id=418

[6] K. Gödel. Eine Interpretation des intuitionistischen Aussagenkalkuls. *Ergebnisse Math. Kolloq.*, 4:39–40, 1933. English translation in: S. Feferman et al., editors, *Kurt Gödel Collected Works, Volume I*, pages 301–303. Oxford University Press, 1986.

[7] K. Gödel. Vortrag bei Zilsel, 1938. English translation in: S. Feferman et al., editors, *Kurt Gödel Collected Works. Volume III*, pages 86–113. Oxford University Press, 1995.

[8] A. Heyting. *Mathematische Grundlagenforschung. Intuitionismus. Beweistheorie.* Springer, Berlin, 1934.

[9] S. Kleene. On the interpretation of intuitionistic number theory. *The Journal of Symbolic Logic*, 10(4):109–124, 1945.

[10] A. Kolmogoroff. Zur Deutung der intuitionistischen Logik. *Mathematische Zeitschrift,* 35:58 65, 1932. English translation in *Selected works of A.N. Kolmogorov. Volume I: Mathematics and Mechanics*, (V.M. Tikhomirov, editor), Kluwer,1985.

[11] G. Kreisel. *Foundations of intuitionistic logic.* In E. Nagel, P. Suppes, and A. Tarski, editors. *Logic, methodology and philosophy of science. Proceedings of the 1960 International Congress*, Stanford University Press, pp. 198–210, 1962.

[12] P. Martin-Löf. *Intuitionistic Type Theory.* Bibliopolis, Napoli, 1984.

[13] A.S. Troelstra. *Aspects of Constructive Mathematics.* In J. Barwise, editor. *Handbook of Mathematical Logic*, Elsevier, pp. 973–1052, 1977.

[14] A.S. Troelstra. *Realizability.* In S. Buss, editor. *Handbook of Proof Theory*, pp. 407-474, Elsevier, 1998

[15] A.S. Troelstra and D. van Dalen. *Constructivism in mathematics. An introduction.* Elsevier, 1988.

[16] D. van Dalen. *Intuitionistic logic.* In D. Gabbay and F. Guenther, editors. *Handbook of Philosophical Logic. Volume 3.* Dordrecht, The Netherlands: Reidel, pp. 225–340, 1988.

Provable Total NP Search Problems and Improved Witnessing Arguments

Arnold Beckmann

(joint work with Samuel R. Buss)

A typical "old-style" witnessing argument relates an arithmetic theory and a formula class Φ to a complexity class $\mathcal{C}$ in the following way: If T proves $\forall x \exists y \varphi(x,y)$ for some property φ in Φ, then there exists a function f in $\mathcal{C}$ whose graph G_f can be described by some formula in Φ, such that T proves (a) the totality of f using G_f, and (b) that f solves $\forall x \exists y \varphi(x,y)$, i.e. $\forall x \forall y (G_f(x,y) \to \varphi(x,y))$.

Recent witnessing arguments, which were used implicitly or explicitely by several authors who studied provable total NP search problems of various theories of bounded arithmetic (cf. [1, 2, 3, 4, 5]), improved the "old-style" ones in the way that (b) can now be proven in a theory of bounded arithmetic weaker than T, which is suitable to formalise feasible reasoning (like the theory S^1_2).

In the talk, we have described such new style witnessing arguments for 2nd order theories of bounded arithmetic (U^1_2 and V^1_2) related to the complexity classes $PSPACE$ and $EXPTIME$. We have then used these results to improve on recent characterisations of provable total NP search problems of 2nd order theories of bounded arithmetic U^1_2 and V^1_2 in terms of combinatorial games, called local improvement principles [3].

References

[1] A. Beckmann and S. R. Buss. Polynomial local search in the polynomial hierarchy and witnessing in fragments of bounded arithmetic. *Journal of Mathematical Logic,* 9, 2009, 103–138

[2] A. Beckmann and S. R. Buss. Characterization of Definable Search Problems in Bounded Arithmetic via Proof Notations. Ontos Verlag, 2010, 65–134.

[3] L. A. Kołodziejczyk, P. Nguyen, and N. Thapen. The provably total NP search problems of weak second-order bounded arithmetic. Annals of Pure and Applied Logic, 162 (2011), 419–446

[4] P. Pudlák and N. Thapen. Alternating minima and maxima, Nash equilibria and bounded arithmetic. Typeset manuscript, November 2009.

[5] A. Skelley and N. Thapen. The provably total search problems of bounded arithmetic. Proceedings of the London Mathematical Society, 103 (2011), pp. 106–138.

Provability algebras for theories of Tarskian truth

Lev D. Beklemishev
(joint work with Evgeny Dashkov)

We study theories in the language of Peano arithmetic augmented by new a unary predicate $T(x)$ representing the set of Gödel numbers of all true arithmetical sentences. Formulas in the language with T are naturally classified into a hierarchy of classes Π^0_α, where $\alpha < \omega 2$ is an ordinal. Our basic system is elementary arithmetic EA together with the standard full Tarski commutation conditions for truth. We consider extensions of this basic system by restricted forms of induction (in the language with T) and show that these induction axioms are equivalent to the reflection principles of appropriate logical complexity.

Reflection principles in the language with T are then studied using methods of provability algebras [1]. In particular, we define a sound and complete propositional *reflection calculus* that adequately describes the interaction of such reflection principles and provides a system of ordinal notation suitable for a proof-theoretic analysis of these systems. It is a novel form of provability logic whose formulas correspond to (arithmetized) schemata rather than individual sentences. As a consequence we obtain a generalization of Schmerl's formula for the iterated reflection principles of restricted arithmetical complexity to the hierarchy of classes Π^0_α. This yields natural axiomatizations of the fragments of the systems with induction of any specific logical complexity class Π^0_α, $\alpha < \omega 2$, in terms of iterated reflection principles and allows us to compute the corresponding proof-theoretic ordinals.

This is joint work with Evgeny Dashkov (Moscow M. V. Lomonosov State University). It extends and bears upon the results of H. Kotlarsky and Z. Ratajczyk [2, 3] on the inductive satisfaction classes.

References

[1] L. Beklemishev. *Operational modal logic.* Russian Mathematical Surveys, v. 60 (2), p. 197-268, 2005.

[2] H. Kotlarski. *Bounded induction and satisfaction classes.* Mathematical Logic Quarterly, v.32 (31-34), p. 531-544, 1986.

[3] H. Kotlarski, Z. Ratajczyk. *Inductive full satisfaction classes.* Annals of Pure and Applied Logic, v. 47 (3), p. 199-223, 1991.

A functional interpretation for nonstandard arithmetic

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

In the work we presented we started a proof-theoretic investigation of systems for nonstandard analysis in the style of Nelson's Internal Set Theory (IST) using functional interpretations (see [1]).

The idea of Nelson was to add a new unary predicate symbol st to ZFC for "being standard". In addition, he added three new axioms to ZFC governing the use of this new unary predicate, called Idealization, Standardization and Transfer. The resulting system he called Internal Set Theory or IST. The main logical result about IST is that it is a conservative extension of ZFC, so any theorem provable in IST which does not involve the st-predicate is provable in ZFC as well.

The conservativity of IST over ZFC was proved twice. In the original paper where he introduces Internal Set Theory [6][1], Nelson gives a model-theoretic argument which he attributes to Powell. In a later publication [7], he proves the same result syntactically by providing a "reduction algorithm" (a rewriting algorithm) for converting proofs performed in IST to ordinary ZFC-proofs. There is a remarkable similarity between his reduction algorithm and the Shoenfield interpretation [8]; this observation was the starting point for our work.

Instead of working with extensions of ZFC, we work in the context of Heyting and Peano arithmetic in all finite types (HA^ω and PA^ω). We begin with HA^ω and proceed in a similar way as Nelson: we add a new unary predicate st to its language (in fact, we will add unary predicates st^σ for every type σ) and add nonstandard axioms in the extended language. Our main result is the existence of an algorithm which rewrites proofs performed in this constructive nonstandard system to ordinary proofs performed in HA^ω. This algorithm is a functional interpretation in the style of Gödel, with features reminiscent of the Diller-Nahm [2] and the bounded functional interpretation [3] (the relation to the latter is especially close). Then by combining this rewriting algorithm with negative translation one obtains a Shoenfield-type functional interpretation for a nonstandard extension of PA^ω.

The existence of such a rewriting algorithm has two corollaries: first of all, it shows that the nonstandard systems we consider are conservative extensions of HA^ω and PA^ω, respectively. Secondly, they show how one can extract terms in Gödel's $\mathcal{T}$ (and hence computational content) from nonstandard proofs. In the future we would like to investigate if this second feature can be used for proof-mining nonstandard proofs (as in [5]).

Other questions which we hope to take up in future work are the following: we believe that we have not obtained the optimal conservation result in the classical context, so we still hope to be able to make some further progress here. In addition, we would like to understand proof-theoretically the role of saturation

[1] This paper was reprinted with a foreword by G. F. Lawler in volume 48, no. 4, of the *Bulletin of the American Mathematical Society* in recognition of its status as a classic.

principles in nonstandard proofs: we have shown that constructively they do not add any strength. But we have also shown that classically they make the system much stronger (something similar happened in [4]). Presently, we are working on determining their exact strength over our classical nonstandard system.

References

[1] B. van den Berg, E. Briseid, and P. Safarik. A functional interpretation for nonstandard arithmetic. Preprint submitted for publication. Available as arXiv:1109.3103, 2011.

[2] J. Diller and W. Nahm. Eine Variante zur Dialectica-Interpretation der Heyting-Arithmetik endlicher Typen. *Arch. Math. Logik Grundlagenforsch.*, 16:49–66, 1974.

[3] F. Ferreira and P. Oliva. Bounded functional interpretation. *Ann. Pure Appl. Logic*, 135(1-3):73–112, 2005.

[4] C.W. Henson and H.J. Keisler. On the strength of nonstandard analysis. *J. Symbolic Logic*, 51(2):377–386, 1986.

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

[6] E. Nelson. Internal set theory: a new approach to nonstandard analysis. *Bull. Amer. Math. Soc.*, 83(6):1165–1198, 1977.

[7] E. Nelson. The syntax of nonstandard analysis. *Ann. Pure Appl. Logic*, 38(2):123–134, 1988.

[8] J.R. Shoenfield. *Mathematical logic.* Association for Symbolic Logic, Urbana, IL, 2001. Reprint of the 1973 second printing.

Constructive Complements on Riemann's Series Theorems

Douglas S. Bridges

In the nineteenth century, Bernhard Riemann proved two now-famous theorems about rearrangements of an infinite series $\sum a_n$ of real numbers:

RST$_1$: If $\sum a_n$ is absolutely convergent, then every rearrangement of it converges to the same sum.

RST$_2$: If $\sum a_n$ is convergent but not absolutely convergent, then for any real number x, there exists a rearrangement of the series that converges to x. Moreover, there are rearrangements that diverge to $\pm\infty$.

In 1974, Michael Beeson asked whether one could prove these theorems in **BISH**: Bishop-style constructive mathematics, which is, roughly, mathematics with intuitionistic logic [3, 4, 6]. The affirmative answer was given in 2009 by Berger and Bridges [1].

It is not hard to extend the conclusion of **RST$_2$** to what we call its *full, extended version*, which includes the existence of permutations of the series $\sum a_n$ that diverge to ∞ and to $-\infty$. In consequence, a simple reductio ad absurdum argument proves classically that if a real series $\sum a_n$ is ***permutably convergent***—that is, every permutation of $\sum a_n$ converges in **R**—then it is absolutely convergent. An intuitionistic proof of this last result was provided by Troelstra ([14], pages 95 ff.), using Brouwer's continuity principle for choice sequences. That result actually has one serious intuitionistic application: Spitters ([13], pages 2101–2) uses it to give an intuitionistic proof of the characterisation of normal linear functionals on the space of bounded operators on a Hilbert space; he also asks whether there is a proof of the Riemann-Troelstra result within **BISH** alone. To deal with Spitters' question, we first recall a definition and a principle due to Ishihara [8].

A subset S of the set $\mathbf{N}$ of natural numbers is said to be ***pseudobounded*** if for each sequence $(s_n)_{n\geq 1}$ in S, there exists N such that $s_n/n < 1$ for all $n \geq N$—or, equivalently, if $s_n/n \to 0$ as $n \to \infty$. Every bounded subset of $\mathbf{N}$ is pseudobounded. The converse holds classically, intuitionistically, and in recursive constructive mathematics, but Lietz [10] and Lubarsky [11] have produced models of **BISH** in which it fails to hold for inhabited, countable, pseudobounded sets. Thus the principle

BD-N: *Every inhabited, countable, pseudobounded subset of* $\mathbf{N}$ *is bounded*

is independent of **BISH.** It is a serious problem of constructive reverse mathematics [5, 9] to determine which classical theorems are equivalent to **BISH** + **BD-N**.

Berger et al. [2] have proved the following:

Theorem 1. **BISH** + **BD-N** $\vdash$ *Every permutably convergent series of real numbers is absolutely convergent.*

While this result steps outside unadorned **BISH**, it is valid in both intuitionistic and constructive recursive mathematics, in which **BD-N** is derivable.

Theorem 1 raises the question: over **BISH**, does the absolute convergence of every permutably convergent series imply **BD-N**? Thanks to Diener and Lubarsky [7], we now know that the answer is negative. In turn, this raises another question: is there a proposition that is *classically* equivalent to, and clearly cognate with, the absolute convergence of permutably convergent series and that, added to **BISH**, implies **BD-N**? In order to answer this question affirmatively, we work with a new notion, defined as follows.

By a ***bracketing*** of a real series $\sum a_n$ we mean a series of the form

$$\sum_{n=1}^{\infty} \sum_{k=f(n)}^{f(n+1)-1} a_k,$$

where f is a strictly increasing mapping of the set $\mathbf{N}^+$ of positive integers into itself with $f(1) = 1$. We say that $\sum a_n$ is ***weak-permutably convergent*** if it is convergent and if for each permutation σ of $\mathbf{N}^+$, there exists a convergent bracketing of $\sum a_{\sigma(n)}$. Clearly, permutable convergence implies weak-permutable convergence.

A nontrivial argument involving the careful construction of an appropriate permutation of $\sum a_n$ leads to this result:

Lemma 2. **BISH** $\vdash$ *Let* $\sum a_n$ *be a weak-permutably convergent series of real numbers, and* σ *a permutation of* $\mathbf{N}^+$*. Then it is impossible that* $\sum \left|a_{\sigma(n)}\right|$ *diverge.*

It follows *classically* from this lemma and $\mathbf{RST}_1$ that if $\sum a_n$ is weak-permutably convergent, then $\sum a_n$ is permutably convergent; in view of the Diener-Lubarsky results in [7], the latter cannot be proved within **BISH**.

Constructively, Lemma 2 enables us to prove that if $\sum a_n$ is permutably convergent, then for each permutation σ of $\mathbf{N}^+$, every convergent bracketing of $\sum a_{\sigma(n)}$ converges to the same sum as $\sum a_n$ itself.

An extremely complicated argument leads to:

Lemma 3. $\mathbf{BISH} \vdash$ *Let $S \equiv \{s_1, s_2, \ldots\}$ be an inhabited, countable, pseudobounded subset of $\mathbf{N}$. Then there exists a sequence $(a_n)_{n\geq 1}$ of nonnegative rational numbers with the following properties.*

(i) $\sum (-1)^n a_n$ is convergent and weak-permutably convergent.
(ii) If $\sum a_n$ converges, then S is bounded.

It is then relatively straightforward to prove our second main result:

Theorem 4. $\mathbf{BISH} \vdash$ *If every weak-permutably convergent series in $\mathbf{R}$ is absolutely convergent, then* **BD-N** *holds.*

To summarise: in **BISH** + **BD-N** the Riemann permutability theorem is derivable; in **BISH**, the absolute convergence of every weak-permutably convergent series implies **BD-N**; and, by the work of Diener and Lubarsky, we can neither drop **BD-N** from the first of these statements nor replace *weak-permutably* by *permutably* in the second.

References

[1] J. Berger and D.S. Bridges: 'Rearranging series constructively', J. Univ. Comp. Sci. **15**(17), 3160–3168, 2009.

[2] J. Berger, D. Bridges, H. Diener, and H. Schwichtenberg: 'Constructive aspects of Riemann's permutation theorem for series', preprint, University of Munich, Germany, 2011.

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

[4] E.A. Bishop and D.S. Bridges: *Constructive Analysis*, Grundlehren der Math. Wiss. **279**, Springer Verlag, Heidelberg, 1985.

[5] D.S. Bridges: 'A reverse look at Brouwer's fan theorem', in: *One Hundred Years of Intuitionism (1907–2007)* (Eds: van Atten, M.; Boldini, P.; Bourdeau, M.; Heinzmann, G.), Publications of the Henri Poincaré Archives, Birkhäuser, Basel, 316–325, 2008.

[6] D.S. Bridges and L.S. Vîţă: *Techniques of Constructive Analysis*, Universitext, Springer-Verlag, Heidelberg, 2006.

[7] H. Diener and R. Lubarsky: 'Principles weaker than **BD**-$\mathbb{N}$', preprint, Florida Atlantic University, Boca Raton, FL, 2011.

[8] H. Ishihara: 'Continuity properties in metric spaces', J. Symb. Logic **57**(2), 557–565, 1992.

[9] H. Ishihara: 'Constructive reverse mathematics: compactness properties', In: *From Sets and Types to Analysis and Topology: Towards Practicable Foundations for Constructive Mathematics* (L. Crosilla and P.M. Schuster, eds), Oxford Logic Guides **48**, Oxford Univ. Press, 245–267, 2005.

[10] P. Lietz and T. Streicher: 'Realizability models refuting Ishihara's boundedness principle', preprint, Tech. Universität Darmstadt, Germany, 2011.

[11] R. Lubarsky: 'On the failure of **BD**-$\mathbb{N}$', preprint, Florida Atlantic University, Boca Raton, FL, 2010.

[12] G.F.B. Riemann: 'Ueber die Darstellbarkeit einer Function durch eine trigonometrische Reihe', in *Gesammelte Werke*, 227–264. Originally in: *Habilitationsschrift*, 1854, Abhandlungen der Königlichen Gesellschaft der Wissenschaften zu Göttingen, **13**.

[13] B. Spitters: ‘Constructive results on operator algebras’, J. Univ. Comp. Sci. **11**(12), 2096–2113, 2005.

[14] A.S. Troelstra: *Choice Sequences. A Chapter of Intuitionistic Mathematics*, Oxford Logic Guides, Clarendon Press, Oxford, 1977.

Infinite pigeonhole principle

Jaime Gaspar

The infinite pigeonhole principle is one of the world's most evident statements: if we colour the natural numbers with finitely many colours, then some colour occurs infinitely often. Despite its obviousness, its treatment in both proof theory and mathematics can be surprisingly challenging. We are going to illustrate this with two case studies.

Case study 1: Tao's "finitary" infinite pigeonhole principle[1]. Terence Tao [5, 6] wrote on his blog essays about finitising principles in analysis: finding for infinite qualitative "soft analysis" statements equivalent finitary quantitative "hard analysis" statements. One of his prime examples is an (almost) finitisation of the infinite pigeonhole principle. Tao's finitisation turned out to be mistaken and we [2] gave a counterexample. Then Tao and we independently proposed corrections.

In this case study we:

- try to determine, in the context of reverse mathematics, which one of the corrections is a more faithful finitisation of the infinite pigeonhole principle;
- argue that Tao's finitisations can be done systematically by proof theoretic tools, namely the monotone functional interpretation.

Then we finish with an open problem.

Case study 2: Infinite pigeonhole principle in proof mining. Proof mining [4] is a research program that seeks to extract computational content from proofs in mathematics using proof theoretic tools, notably the monotone functional interpretation. We [1] proof mined Hillam's [3] theorem which characterises the convergence of fixed point iterations.

The proof of Hillam's theorem uses the Bolzano-Weierstrass theorem, an ineffective principle. To proof mine Hillam's theorem, we improved the situation by replacing the Bolzano-Weierstrass theorem by the infinite pigeonhole principle. But then, contrarily to what usually happens, it seems that we cannot eliminate the infinite pigeonhole principle, at least without strengthening our hypotheses.

In this case study we study two ways to deal with the infinite pigeonhole principle:

- to interpret the infinite pigeonhole principle with the monotone functional interpretation, getting a stronger but more complicated proof mining of Hillam's theorem;
- to strength the hypotheses and eliminate the infinite pigeonhole principle, getting a weaker but simpler proof mining of Hillam's theorem.

[1] This is a joint work with Ulrich Kohlenbach.

Then, again, we finish with an open problem.

Acknowledgments. Financially supported by the Portuguese Fundação para a Ciência e a Tecnologia under grant SFRH/BD/36358/2007 co-financed by Programa Operacional Potencial Humano / Quadro de Referência Estratégico Nacional / Fundo Social Europeu (União Europeia).

References

[1] Jaime Gaspar. *Proof interpretations: theoretical and practical aspects.* PhD thesis, Technical University of Darmstadt, October 2011. Submitted.

[2] Jaime Gaspar and Ulrich Kohlenbach. On Tao's "finitary" infinite pigeonhole principle. *The Journal of Symbolic Logic*, 75(1):355–371, March 2010.

[3] Bruce P. Hillam. A characterization of the convergence of successive approximations. *The American Mathematical Monthly*, 83:273, April 1976.

[4] Ulrich Kohlenbach. *Applied Proof Theory: Proof Interpretations and their Use in Mathematics.* Springer Monographs in Mathematics. Springer, Berlin, Heidelberg, Germany, first edition, 2008.

[5] Terence Tao. Soft analysis, hard analysis, and the finite convergence principle. http://terrytao.wordpress.com/2007/05/23, May 2007. Appeared elsewhere [7].

[6] Terence Tao. The correspondence principle and finitary ergodic theory. http://terrytao.wordpress.com/2008/08/30, August 2008.

[7] Terence Tao. *Structure and Randomness: Pages from Year One of a Mathematical Blog.* American Mathematical Society, Providence, Rhode Island, the United States of America, first edition, 2008.

Proof-theoretic conservations of weak weak intuitionistic constructive set theories

Lev Gordeev

J. Myhill [4] and H. Friedman [1] introduced several constructively meaningful principles and formal systems of *weak* extensional intuitionistic set theory of proof-theoretic strengths shown in [1] to range between that of standard first- and second-order Arithmetic, **PA** (or **HA**) and $\mathbf{PA}_2$ (or $\mathbf{HA}_2$), respectively, thus being essentially weaker than standard classical set theory **ZF**. Furthermore [1] posed a deeper problem conjecturing that intuitionistic set theories under consideration are conservative extensions of the underlying arithmetical intuitionistic formalisms. These conjectures (et al) have been confirmed [3] for the set theories of proof-theoretic strengths up to Howard Ordinal $|\mathbf{ID}_1|$; the proofs were based on the author's constructive semantics [2] of analogous weak set theories. Moreover [3] strengthened Friedman's conjectures by also proving conservations in the presence of consistent combinations of other constructive principles like an anti-foundation axiom **Cpl** and/or finite-types axiom of choice $\mathbf{AC}_{\mathrm{FT}}$. Actually for every weak set theory **T** in question [3] expressed the solution in the most conservative form $\mathbf{T} \vdash A \Leftrightarrow \mathbf{HA} + TI\,(< |\mathbf{T}|) \vdash A$, for any arithmetical statement A, where $TI\,(< |\mathbf{T}|)$ denotes the arithmetical transfinite induction scheme below proof theoretic ordinal of **T**.

Working in classical logic and using analogous set theoretic semantics K. Sato [5] introduced several weak refinements of basic weak set theory – both intensional and extensional – and determined their proof-theoretic ordinals. Notably Sato's *weak weak* classical set theories are less expressive than Myhill-Friedman's *weak* intuitionistic formalisms, which can (arguably) simulate the full expressive power of **ZF**. In particular, Zermelo's classical power set axiom

Pow : "*for every x there exists the set of all subsets of x*"

has natural constructive interpretation in the form

Exp : "*for every x and y there exists the set of all functions from x to y*"

occurring in Myhill-Friedman's formalisms. Since constructive functions are thought to simulate only algorithms, **Exp** is weaker than **Pow** in the intuitionistic environment. This might on one hand illuminate proof-theoretic weakness of Myhill-Friedman's intuitionistic constructive formalisms, and on the other hand explain the lack of **Exp** in Sato's classical ones. However, adding **Exp** to the intuitionistic versions of the *weak weak* set theories would hardly affect their proof-theoretic strengths. It is thus natural to investigate proof-theoretic strengths of the resulting extended *weak weak* intuitionistic constructive set theories and ask whether they are conservative extensions of the underlying arithmetical intuitionistic formalisms. We recall basic results of [5] :

Theorem 5. $|\mathbf{Basic}+\mathbf{Ext}|=\varepsilon_0$, $|\mathbf{Basic}+\mathbf{Ext}+\Delta_0\textbf{-Sep}|=\Gamma_0$.

and observe that the increase of proof theoretic strength of $\mathbf{Basic}+\mathbf{Ext}+\Delta_0$-**Sep**, relative to $\mathbf{Basic}+\mathbf{Ext}$, is caused by essentially classical argument that allows to infer the comparability of arbitrary countable well-orderings fom **Basic**'s collapsing axiom **Clps**. However, this argument fails intuitionistically and we refine Sato's results by the following intuitionistic counterpart.

Theorem 6. $\left|\mathbf{Basic}^{(\mathbf{i})}+\mathbf{Ext}\right|=\left|\mathbf{Basic}^{(\mathbf{i})}+\mathbf{Ext}+\Delta_0\textbf{-Sep}+\mathbf{Exp}\right|=\varepsilon_0$. *Moreover* $\mathbf{Basic}^{(\mathbf{i})}+\mathbf{Ext}+\Delta_0\textbf{-Sep}+\mathbf{Exp}$ *is a conservative extension of* HA.

The latter theorem, in turn, is strengthened as follows, where
$\mathbf{\Theta}=\mathbf{SC}+\mathbf{Ful}+\mathbf{AC}!+\mathbf{Enm}$ and:

$$\mathbf{SC}\equiv\begin{array}{l}(\forall x\in a)\,\exists y\varphi\,(x,y)\to\\ \exists z\,((\forall x\in a)\,(\exists y\in z)\,\varphi\,(x,y)\wedge(\forall y\in z)\,(\exists x\in a)\,\varphi\,(x,y))\end{array},$$

$$\mathbf{AC}!\equiv\begin{array}{l}(\forall u\in x)\,(\exists! v\in y)\,\varphi\,(u,v)\to\\ \exists f\,(\mathrm{Func}\,(f,x,y)\wedge(\forall u\in x)\,\varphi\,(u,f\,(u)))\end{array},$$

$$\mathbf{Ful}\equiv(\exists z)\left((\forall r\in z)\,\mathrm{Tot}\,(r,x,y)\wedge\forall r\left(\begin{array}{c}\mathrm{Tot}\,(r,x,y)\to(\exists s\in z)\\ (s\subset r\wedge\mathrm{Tot}\,(s,x,y))\end{array}\right)\right),$$

where $\mathrm{Tot}\,(r,x,y)\equiv r\subset x\times y\wedge\ (\forall u\in x)\,(\exists v\in y)\,(\langle u,v\rangle\in r)$,

$$\mathbf{Anti\text{-}Reg}\equiv\begin{array}{l}\mathrm{Ord}\,(x)\wedge(\forall s,t\in x)\,(\langle s,t\rangle\in r\leftrightarrow\langle s,t\rangle\notin r')\to\\ (\exists f,y)\,\mathrm{TrClps}\,(f,x,r,y)\end{array},$$

$\mathbf{Cpl}\equiv r\subset x\times x\to(\exists f,y)\,\mathrm{TrClps}\,(f,x,r,y)$,

$\mathbf{Enm}\equiv(\exists y\subset\omega)\,(\exists f)\,\mathrm{Surj}\,(f,y,x)$.

Note that **Cpl** and **Anti-Reg** are both incompatible with **Fnd**.

Theorem 7.

$$\mathbf{Basic}^{(\mathbf{i})} + \mathbf{Ext} + \Delta_0\textbf{-Sep} + \mathbf{\Theta} + \mathbf{Fnd}$$

and

$$\mathbf{Basic}^{(\mathbf{i})} + \mathbf{Ext} + \Delta_0\textbf{-Sep} + \mathbf{\Theta} + \mathbf{Cpl}$$

are both conservative extension of HA.

Remark 8. (1) $\mathbf{Basic}^{(\mathbf{i})} + \mathbf{Ext} + \Delta_0\textbf{-Sep} + \mathbf{\Theta} + \mathbf{Fnd}$ *is a proper extension of Friedman's* $\mathbf{T_1}$.

(2) *Within* $\mathbf{Basic}^{(\mathbf{i})} + \Delta_0\textbf{-Sep} + \mathbf{\Theta}$ *:* **Ful** *implies* **Exp** *(but not otherwise), both being much weaker (in the proof theoretic sense) than* **Pow**.

(3) *Within* $\mathbf{Basic}^{(\mathbf{i})} + \Delta_0\textbf{-Sep} + \mathbf{Enm}$ *:* **Cpl** *is equivalent to* **Anti-Reg**.

(4) *For brevity we use standard constructive version of* $\mathrm{Ord}(x)$ *:*

$$\mathrm{Ord}(x) \equiv \begin{array}{l} \mathrm{POrd}(x) \wedge \varnothing \in x \wedge \\ (\forall u)\left((\forall y \in x)(y \subset u \leftrightarrow y \in u) \rightarrow x \subset u\right) \end{array}.$$

References

[1] H. Friedman, *Set-theoretic foundation for constructive analysis*, Annals of Math. **105** (1977) 1–28

[2] L. Gordeev, *Constructive models for set theory with extensionality*, in: The L.E.J. Brouwer Centenary Symposium (Noordwijkerhout 1981), North-Holland (1982) 123–147

[3] L. Gordeev, *Proof-theoretical analysis: weak systems of functions and classes*, Annals of Pure and Applied Logic **38**(1) (1988) 1–122

[4] J. Myhill, *Constructive set theory*, J. Symbolic Logic **40** (1975), 374–382

[5] K. Sato, *The strength of extensionality I – weak weak set theories with infinity*, Annals of Pure and Applied Logic **157** (2009) 234–268

Some conservative extension results of classical logic over intuitionistic logic

Hajime Ishihara

It is well known that classical predicate logic is conservative over intuitionistic predicate logic with respect to negative formulas; see Troelstra and van Dalen [12, 2.3.6] or van Dalen [3, 5.2.9]. A number of papers in the literature contain extensions of the conservative extension result, such as Mints and Orevkov [6], Orevkov [9] and Cellucci [2]. Leivant [5] gave another systematization of the conservative extension results, not only for predicate logic but also for mathematical theories; see also [12, 2.3.11–26].

In 2000, the author showed the following conservative extension result, based on the translation $A^{\$} \equiv A^g[\perp/\$]$ where A^g is the Gödel-Gentzen negative translation and \$ is a special proposition letter (place holder). We define simultaneously classes $\mathcal{R}$, $\mathcal{J}$, $\mathcal{Q}$ and $\mathcal{K}$ of formulas as follows. Let P range over atomic formulas distinct from $\perp$, R and R' over $\mathcal{R}$, J and J' over $\mathcal{J}$, Q and Q over $\mathcal{Q}$, and K and K' over $\mathcal{K}$. Then $\mathcal{R}$, $\mathcal{J}$, $\mathcal{Q}$ and $\mathcal{K}$ are inductively generated by the clauses

(1) $\perp, R \wedge R', R \vee R', \forall x R, J \rightarrow R \in \mathcal{R}$;

(2) $\perp, P, J \wedge J', J \vee J', \exists x J, R \rightarrow J \in \mathcal{J}$;

(3) $\bot, P, Q \wedge Q', Q \vee Q', \forall x Q, \exists x Q, J \to Q \in \mathcal{Q}$;
(4) $J, K \wedge K', \forall x K, Q \to K \in \mathcal{K}$.

A set Γ of formulas is closed under the translation $(\cdot)^\$$ if $\Gamma \vdash_i A^\$[\$/C]$ for each A in Γ and each formula C which is free for \$ in $A^\$$. We showed that

> if Γ is a set of formulas closed under $(\cdot)^\$$ and $A \in \mathcal{K}$, then $\Gamma \vdash_c A$ implies $\Gamma \vdash_i A$,

where $\vdash_c$ and $\vdash_i$ denote derivability in classical and intuitionistic logic, respectively; see [4, Theorem 10]. Since formulas in $\mathcal{Q}$ were proved to be closed under $(\cdot)^\$$ in [4, Proposition 7], we have, as a corollary,

$$\text{if } \Gamma \subseteq \mathcal{Q} \text{ and } A \in \mathcal{K}, \text{ then } \Gamma \vdash_c A \text{ implies } \Gamma \vdash_i A.$$

This result extends the Orevkov σ-classes $\{\to^+, \neg^+, \forall^+\}$ and $\{\to^-, \neg^-, \vee^+, \exists^+\}$; see [9].

An application of the result is the conservative extension result, *Barr's theorem*, for geometric theories, that is, theories axiomatized by (universal closures of) implications, called geometric implications, between formulas which do not contain $\to$ nor $\forall$. Note that (universal closure of) geometric implications belong to $\mathcal{Q}$ and $\mathcal{K}$; see Palmgren [10] and Negri [7] for other syntactic proofs of Barr's theorem.

Since it is straightforward to show that the axioms and the axiom schema of the first-order arithmetic are closed under $(\cdot)^\$$, we have an application of the theorem:

$$\text{if } A \in \mathcal{K}, \text{ then } \mathbf{PA} \vdash A \text{ implies } \mathbf{HA} \vdash A.$$

As a corollary, we have the well known result that **PA** is conservative over **HA** with respect to Π^0_2 formulas, and, moreover, we are able to know that **PA** is conservative over **HA** with respect to formulas of the form

$$\forall x[\forall u_1 \exists v_1 \ldots \forall u_n \exists v_n (s(\vec{u}, \vec{v}, x) = 0) \to \exists y(t(x, y) = 0)].$$

See also Berger, Buchholz and Schwichtenberg [1] and Schwichtenberg and Wainer [11, Chapter 7] for related classes of formulas in extracting computational content of proofs.

Helmut Schwichtenberg has asked the author about a possibility of introducing $\exists$ and $\forall$ in the clauses for the classes $\mathcal{R}$ and $\mathcal{J}$, respectively. This talk answers him with the following result.

We define simultaneously classes $\mathcal{R}_0$, $\mathcal{J}_0$, $\mathcal{Q}_m$ and $\mathcal{K}_m$ $(m = 1, 2)$ of formulas as follows. Let P range over atomic formulas distinct from $\bot$ (and the proposition letter $*$ which will be introduced later), R and R' over $\mathcal{R}_0$, J and J' over $\mathcal{J}_0$, Q_m and Q'_m over $\mathcal{Q}_m$, and K_m and K'_m over $\mathcal{K}_m$ $(m = 1, 2)$. Then $\mathcal{R}_0$, $\mathcal{J}_0$, $\mathcal{Q}_m$ and $\mathcal{K}_m$ $(m = 1, 2)$ are inductively generated by the clauses

(1) $\bot, R \wedge R', R \vee R', \forall x R, \exists x R, J \to R \in \mathcal{R}_0$;
(2) $\bot, P, J \wedge J', J \vee J', \forall x J, \exists x J, R \to J \in \mathcal{J}_0$;
(3) $P, R, Q_1 \wedge Q'_1, Q_1 \vee Q'_1, \exists x Q_1, J \to Q_1 \in \mathcal{Q}_1$;
(4) $P, R, Q_2 \wedge Q'_2, \forall x Q_2, \exists x Q_2, J \to Q_2 \in \mathcal{Q}_2$;
(5) $J, K_m \wedge K'_m, \forall x K_m, Q_m \to K_m \in \mathcal{K}_m$ $(m = 1, 2)$.

We will show that, for each $m = 1, 2$,

$$\text{if } \Gamma \subseteq \mathcal{Q}_m \text{ and } A \in \mathcal{K}_m, \text{ then } \vdash_c \Gamma \Rightarrow A \text{ implies } \vdash_i \Gamma \Rightarrow A,$$

where $\vdash_c$ and $\vdash_i$ denote derivability of the sequent $\Gamma \Rightarrow A$ in the classical and intuitionistic sequent calculi **G3c** and **G3i**, respectively; see [13] and [8] for **G3c** and **G3i**. This result extends the Orevkov σ-classes $\{\to^+, \neg^+, \vee^-\}$ and $\{\to^+, \neg^+, \forall^-\}$; see [9].

References

[1] Ulrich Berger, Wilfried Buchholz and Helmut Schwichtenberg, *Refined program extraction from classical proofs*, Ann. Pure Appl. Logic **114** (2002), 3–25.

[2] Carlo Cellucci, *Un' osservazione sul theorema di Minc-Orevkov*, Boll. Un. Mat. Ital. **1** (1969), 1–8.

[3] Dirk van Dalen, *Logic and Structure*, 4th ed., Springer-Verlag, Berlin-Heidelberg, 2004.

[4] Hajime Ishihara, *A note on the Gödel-Gentzen translation*, MLQ Math. Log. Q. **46** (2000), 135–137.

[5] Daniel Leivant, *Syntactic translations and provably recursive functions*, J. Symbolic Logic **50** (1985), 682-688.

[6] Grigori Mints and Vladimir Orevkov, *On imbedding operators*, Sem. Math. V.A. Steklov **4** (1967), 64–66.

[7] Sara Negri, *Contraction-free sequent calculi for geometric theories with an application to Barr's theorem*, Arch. Math. Logic **42** (2003), 389–401.

[8] Sara Negri and Jan von Plato, *Structural Proof Theory*, Cambridge University Press, Cambridge, 2001.

[9] Vladimir P. Orevkov, *On Glivenko sequent classes*, in: Logical and logico-mathematical calculi I, Trudy Matematicheskogo Instituta imeni V.A. Steklova, **98** (1968), 131–154; English translation, The calculi of symbolic logic I, Proceedings of the Steklov Institute of Mathematics, **98** (1971), 147–173.

[10] Erik Palmgren, *An intuitionistic axiomatisation of real closed fields*, MLQ Math. Log. Q. **48** (2002), 297–299.

[11] Helmut Schwichtenberg and Stanley S. Wainer, *Proofs and Computations*, Cambridge University Press, Cambridge, 2011.

[12] Anne S. Troelstra and Dirk van Dalen, *Constructivism in Mathematics*, Vol. I and II, North-Holland, Amsterdam, 1988.

[13] Anne S. Troelstra and Helmut Schwichtenberg, *Basic Proof Theory*, Cambridge Tracts in Theoretical Computer Science, 43, Cambridge University Press, Cambridge, 1996.

Operational closure and stability

Gerhard Jäger

After introducing the basic formalism of operational set theory OST and mentioning some basic facts about OST, the notion of an operationally closed set – $Opc[d]$ – is presented. Then it is show that operationally closed sets resemble many aspects of stability. Finally, the proof-theoretic strength of the theory

$$\mathsf{OST} + \forall x \exists y (x \in y \land Opc[y])$$

is characterized in terms of Kripke-Platek set theory with infinity extended by the schema of Σ_1 separation.

References

[1] S. Feferman. Operational set theory and small large cardinals. *Information and Computation*, 207:971–979, 2009.

[2] G. Jäger. On Feferman's operational set theory OST. *Annals of Pure and Applied Logic*, 150(1–3):19–39, 2007.

[3] G. Jäger. Full operational set theory with unbounded existential quantification and power set. *Annals of Pure and Applied Logic*, 160(1):33–52, 2009.

Search for hard tautologies

Jan Krajíček

In this three-part tutorial I first recalled the classical relation between short provability of tautologies expressing the soundness of a proof system and the existence of a simulation of the system, although I have modified the whole set-up for SAT algorithms. I then outlined the framework of proving lengths-of-proofs lower bounds via constructions of extensions of models of suitable bounded arithmetic theories. In the last lecture I presented some basic ideas of the theory of proof complexity generators and constructed a model of the true universal theory in the language of PV where the range of a Nisan-Wigderson type function based on a hard $NP \cap coNP$-function intersects any given infinite NP set.

Program extraction and Ramsey's theorem for pairs

Alexander P. Kreuzer

We study with proof-theoretic methods the function(al)s provably recursive relative to Ramsey's theorem for pairs and the chain-antichain-principle.

Ramsey's theorem for pairs (RT^2_2) is the statement that every coloring of pairs of natural numbers with two colors has an infinite homogeneous set. The *chain antichain principle* (CAC) states that each partial ordering over $\mathbb{N}$ contains an infinite chain or an infinite antichain. CAC is a consequence of RT^2_2.

For RT^2_2 we obtain the upper bounded that the type 2 functionals provable recursive relative to $\mathsf{WKL}_0 + \Sigma^0_2\text{-}\mathsf{IA} + \mathsf{RT}^2_2$ are in T_1. This is the fragment of Gödel's system T containing only type 1 recursion — roughly speaking it consists of functions of Ackermann type. With this we also obtain a uniform method for the extraction of T_1-bounds from proofs that use RT^2_2. Moreover, this yields a new proof of the fact that $\mathsf{WKL}_0 + \Sigma^0_2\text{-}\mathsf{IA} + \mathsf{RT}^2_2$ is Π^0_3-conservative over $\mathsf{RCA}_0 + \Sigma^0_2\text{-}\mathsf{IA}$.

Our main result on CAC is that the type 2 functionals provably recursive from $\mathsf{WKL}_0 + \mathsf{CAC}$ are primitive recursive. This also provides a uniform method to extract bounds from proofs that use this principle. As a consequence we could obtain of proof of the fact that $\mathsf{WKL}_0 + \mathsf{CAC}$ is Π^0_2-conservative over PRA. This refines a result by Chong, Slaman, Yang.

Since CAC implies a weak variant of the Bolzano-Weierstraß principle, this result can be applied not only to combinatorial but also analytical proofs.

The results are obtained in two steps: in the first step a term including Skolem functions for the above principles is extracted from a given proof. This is done using Gödel's functional interpretation. After this the term is normalized, such that only specific instances of the Skolem functions are used. In the second step this term is interpreted using Π^0_1-comprehension. The comprehension is then eliminated in favor of induction using Howard's ordinal analysis of bar recursion (for RT^2_2) or a refinement of Howard's ordinal analysis (for CAC).

References

[1] Alexander P. Kreuzer, Ulrich Kohlenbach, *Term extraction and Ramsey's theorem for pairs*, accepted for publication in the Journal of Symbolic Logic.

[2] Alexander P. Kreuzer, *Primitive recursion and the chain antichain principle*, accepted for publication in the Notre Dame Journal of Formal Logic.

[3] Alexander P. Kreuzer, *The cohesive principle and the Bolzano-Weierstraßprinciple*, Mathematical Logic Quarterly, vol. 57, no. 3, pp. 292–298 (2011).

Truth over intuitionistic logic

Graham E. Leigh

In this talk I investigated the role classical logic plays in restricting the free use of principles of truth. I presented two examples of classical theories of truth with which certain attractive principles of truth are inconsistent, but consistent with their intuitionistic sub-theories. Moreover, it was shown that these new principles of truth do not add any new truth-free theorems. We argue that in the analysis of formal theories of truth, intuitionistic logic can play an intermediary role between full classical logic in which paradoxes abound and much weaker logics such as partial or para-consistent logic which are hard to reason in and mathematically not well understood.

Recent developments in proof mining

Laurentiu Leuştean
(joint work with Ulrich Kohlenbach)

The talk is a report on joint work [2, 3] with Ulrich Kohlenbach and presents new developments in the *proof mining* program, which is concerned with the extraction, using proof-theoretic tools, of hidden finitary and combinatorial content from mathematical proofs that make use of highly infinitary principles

We present effective uniform rates of metastability (in the sense of Tao [6, 7]) on two nonlinear generalizations of the classical von Neumann mean ergodic theorem, due to Saejung [4] and Shioji-Takahashi [5]. These results constitute a significant extension of the actual context of proof mining, as both Saejung's and Shioji-Takahashi's proofs make use of Banach limits, whose existence requires the use of the axiom of choice. We develop a method to convert such proofs into elementary ones which no longer use Banach limits.

Let X be a CAT(0) space, $C \subseteq X$ a convex subset X and $T : C \to C$ be nonexpansive. The *Halpern iteration* starting from $x \in C$ is defined as follows:

$$x_0 := x, \quad x_{n+1} := \lambda_{n+1} u \oplus (1 - \lambda_{n+1}) T x_n,$$

where $x, u \in C$ and $(\lambda_n)_{n \geq 1}$ is a sequence in $[0, 1]$. In a geodesic space (X, d), given a geodesic segment $[x, y]$ and $\alpha \in [0, 1]$, we denote by $(1 - \alpha)x \oplus \alpha y$ the unique point $z \in [x, y]$ satisfying $d(x, z) = \alpha d(x, y)$ and $d(y, z) = (1 - \alpha) d(x, y)$.

One can see easily that if X is a Hilbert space, T is linear and $\lambda_n := \frac{1}{n+1}$, then x_n coincides with the Cesàro mean. The most important result on the convergence of Halpern iterations in Hilbert spaces was obtained by Wittmann [8]. The following theorem, proved by Saejung [4] using Banach limits, generalizes Wittmann's theorem to CAT(0) spaces.

Theorem 9. *Let C be a bounded closed convex subset of a complete CAT(0) space X and $T : C \to C$ a nonexpansive mapping. Assume that (λ_n) satisfies*

$$\lim_{n \to \infty} \lambda_n = 0, \quad \sum_{n=1}^{\infty} \lambda_{n+1} = \infty \quad \textit{and} \quad \sum_{n=1}^{\infty} |\lambda_{n+1} - \lambda_n| \textit{ converges.}$$

Then for any $u, x \in C$, (x_n) converges to the projection $P_{Fix(T)} u$ of u on $Fix(T)$.

While one cannot expect to get effective rates of convergence for the sequence (x_n) in the above theorem, an effective and highly uniform rate of metastability is guaranteed to exist, after the elimination of Banach limits from the proof, by [1, Theorem 3.7.3].

Theorem 10. [2] *In the hypotheses of Theorem 9, let α be a rate of convergence of (λ_n), β be a Cauchy modulus of $s_n := \sum_{i=1}^{n} |\lambda_{i+1} - \lambda_i|$ and θ be a rate of divergence of $\sum_{n=1}^{\infty} \lambda_{n+1}$. Then for all $\varepsilon \in (0, 2)$ and $g : \mathbf{N} \to \mathbf{N}$,*

$$\exists N \leq \Sigma(\varepsilon, g, M, \theta, \alpha, \beta)\ \forall m, n \in [N, N + g(N)]\ (d(x_n, x_m) \leq \varepsilon),$$

where $M \in \mathbb{Z}_+$ is an upper bound on the diameter of C.

The rate of metastability Σ, extracted in [2, Theorem 4.2], depends on the error ε, the counterfunction g, the diameter of C and on (λ_n) via θ, α, β, but it is uniform in the nonexpansive mapping T, the starting point $x \in C$ of the iteration or other data related with C and X. We remark that in practical cases, such as $\lambda_n = \frac{1}{n+1}$, the rates α, β, θ are easy to compute.

In [3] we apply the same method of eliminating Banach limits from the proof of Shioji-Takahashi's generalization of Wittmann's theorem to Banach spaces with a uniformly Gâteaux differentiable norm. Furthermore, we prove a logical metatheorem for a class of Banach spaces, called by us *spaces with a uniformly continuous duality selection map*, that guarantee the extractability of a highly uniform rate of metastability for the Halpern iterations in this setting.

Acknowledgement: Laurenţiu Leuştean has been supported by the grant "Proof mining in metric analysis, geometric group theory and ergodic theory" - PN-II-ID-PCE-2011-3-0383 of CNCS Romania.

References

[1] U. Kohlenbach, Some logical metatheorems with applications in functional analysis. Trans. Amer. Math. Soc. 357 (2005), 89-128.

[2] U. Kohlenbach, L. Leuştean, Effective metastability of Halpern iterates in CAT(0) spaces, arXiv:1107.3215v3 [math.FA], 2011.

[3] U. Kohlenbach, L. Leuştean, On the computational content of convergence proofs via Banach limits, to appear in Philosophical Transactions of the Royal Society A.

[4] S. Saejung, Halpern's iterations in CAT(0) spaces, Fixed Point Theory Appl. 2010, Article ID 471781, 13pp..

[5] N. Shioji, W. Takahashi, Strong convergence of approximated sequences for nonexpansive mappings in Banach spaces, Proc. Amer. Math. Soc. 125 (1997), 3641-3645.

[6] T. Tao, Soft analysis, hard analysis, and the finite convergence principle, 2007, http://terrytao.wordpress.com/2007/05/23/.

[7] T. Tao, Norm convergence of multiple ergodic averages for commuting transformations, Ergodic Theory Dynam. Systems 28 (2008), 657-688.

[8] R. Wittmann, Approximation of fixed points of nonexpansive mappings, Arch. Math 58 (1992), 486-491.

Issues around proving FLT in PA

Angus John MacIntyre

I present some of the dramatic personae in Wiles's proof, and give an idea of what is needed to code them in PA.

Non-Deterministic Epsilon Substitution for ID_1: effective proof

Grigori Mints

In another paper [7] we defined a simplified non-deterministic epsilon substitution method for PA and ID_1 and gave a short but non-effective termination proof for it. Here we present an effective termination proof via cut-elimination using ideas from [4], [6] and [5]. For historical introduction and motivation (including comparison with the first effective termination proof for more complicated formulation by T. Arai in [1]) see [7]. Definitions and proofs in the present paper are independent of [7].

To simplify technical details we use a formulation with special (but still universal) form of inductive definition: the system S_1 of constructive ordinals [9]. It was introduced by S. Kleene [3] using slightly different notation. The general scheme of the termination proof for the ϵ-substitution method and resulting proof-theoretic analysis is as follows.

(1) The problem of termination is reduced to provability of some existential statement: existence of solving substitution for a given finite set E of axioms (critical formulas).

(2) Simple (but non-effective) recursion-theoretic proof of existence of such solving substitution is expanded into a proof (called *original derivation*) in some infinitary system with a rule similar to Ω-rule introduced by W. Buchholz [2].
(3) Cut-elimination procedure from [2] with suitable adjustments is applied to the original derivation.
(4) The result of cut-elimination is a “complete protocol” including all steps of the epsilon substitution method leading from the empty substitution to the solution of given system E of critical formulas.

References

[1] T. Arai, Epsilon substitution method for $ID_1(\Pi^0_1 \vee \Sigma^0_1)$. Ann. Pure Appl. Logic 121, No.2-3, 163-208 (2003).

[2] W. Buchholz, Explaining the Gentzen-Takeuti Reduction Steps, Arch. Math. Logic, 40, pp. 255-272, 2001

[3] S. Kleene, On notation for ordinal numbers, J. Symb. Log., 3, 150-155, 1938

[4] G. Mints, Gentzen-type Systems and Hilbert's Epsilon Substitution Method. I. In: D. Prawitz, B.Skyrms, D. Westerstahl (Eds.), Logic, Method. and Philos. of Sci. IX, Elsevier, 1994, 91-122

[5] G. Mints, Cut Elimination for a Simple Formulation of PAϵ, APAL 152, 2008, 148-160

[6] G. Mints, S. Tupailo, W. Buchholz, Epsilon Substitution Method for Elementary Analysis, Archive for Math. Logic 35 (1996) 103-130

[7] G. Mints, Non-deterministic substitution method for ID1, submitted to Gentzen volume

[8] W.Pohlers, Proof theory : the first step into impredicativity, Cambridge University Press, 2009

[9] Rogers H., Theory of Recursive Functions and Effective Computability, McGraw-Hill, New York, 1967

The axiomatic derivation of absolute lower bounds

Yiannis N. Moschovakis

My lecture was based on [5], whose main aim is to develop, explain and discuss some applications of the *homomorphism method* for establishing lower bounds for problems in arithmetic and algebra. These lower bounds apply to many complexity measures, and they are provably *robust* with respect to the choice of computation model and plausibly *absolute*, i.e., they restrict all algorithms which compute a given function from specified primitives. In this abstract I will omit a discussion of its justification—which is an important foundational aspect of this work—and I will report on just one, typical application in algebraic complexity.

The idea for this research project came from analysing the derivations of lower bounds for arithmetic decision problems (e.g., *coprimeness*) in [3, 4], most of which are grounded on the fact that the natural complexity measures of recursive programs are preserved under *embeddings.* In the process of abstracting a general theory from those results and then applying it to problems in algebra, it became clear that one should use homomorphisms rather than embeddings, so that *equality tests* (which are important in algebra) can also be counted.

(Partial) structures and homomorphisms. A (partial) Φ-*structure* is a tuple

$$\mathbf{M} = (M, \Phi^{\mathbf{M}}) = (M, \{\phi^{\mathbf{M}} : \phi \in \Phi\})$$

where each $\phi^{\mathbf{M}}$ is a *partial function* or a *partial relation* of $n_\phi \geq 0$ arguments on M, as specified by the *vocabulary* Φ. (We view an n-ary partial relation as a partial function $R : M^n \rightharpoonup \{\mathrm{tt}, \mathrm{ff}\}$.) The *restriction* $\mathbf{M} \restriction \Phi_0$ of $\mathbf{M}$ to part of its vocabulary and its *expansion* $(\mathbf{M}, \Psi^{\mathbf{M}})$ to a larger set of primitives are defined as usual.

The (equational) *diagram* of $\mathbf{M}$ is the set of all formal equations satisfied in $\mathbf{M}$ by the primitives,

$$\mathrm{eqdiag}(\mathbf{M}) = \{(\phi, \vec{x}, w) : \phi \in \Phi, \vec{x} \in M^n, w \in M \cup \{\mathrm{tt}, \mathrm{ff}\} \text{ and } \phi^{\mathbf{M}}(\vec{x}) = w\}.$$

If $\mathbf{M}$ is finite, then the cardinal number $|\mathrm{eqdiag}(\mathbf{M})|$ is a good measure of its size.

A *homomorphism* $\pi : \mathbf{U} \to \mathbf{V}$ of one Φ-structure to another is any function $\pi : U \to V$ such that

$$[\vec{x} \in U^{n_\phi} \ \& \ \ \phi^{\mathbf{U}}(\vec{x}) = w] \implies \phi^{\mathbf{V}}(\pi(\vec{x})) = \pi(w) \quad (\phi \in \Phi),$$

where (by convention) $\pi(\mathrm{tt}) = \mathrm{tt}$ and $\pi(\mathrm{ff}) = \mathrm{ff}$; it is an *embedding* if it is injective.

A (partial) *substructure* $\mathbf{U} \subseteq_p \mathbf{V}$ is a Φ-structure such that $U \subseteq V$ and the identity function $\mathrm{id} : U \to V$ is an embedding.

For example,

$$\mathbf{R} = (\mathbb{R}, 0, 1, +, -, \cdot, \div, =)$$

is the expansion of the real field by the equality relation. We will be mostly concerned with $\mathbf{R}$ and its substructures, and it is important to keep in mind that $\mathbf{U} \subseteq_p \mathbf{R}$ *does not insure that* U *is a subfield of* $\mathbb{R}$; in fact, of most interest to us will be the *finite* substructures of $\mathbf{R}$, which are never subfields.

Forcing and certification. Suppose $\mathbf{M}$ is a Φ-structure, $f : M^n \rightharpoonup W$ (with $W = M$ or $W = \{\mathrm{tt}, \mathrm{ff}\}$), $\mathbf{U} \subseteq_p \mathbf{M}$, and $f(\vec{x})\downarrow$. A homomorphism $\pi : \mathbf{U} \to \mathbf{M}$ *respects* f *at* $\vec{x}$ if

$$\vec{x} \in U^n \ \& \ f(\vec{x}) \in U \cup \{\mathrm{tt}, \mathrm{ff}\} \ \& \ \pi(f(\vec{x})) = f(\pi(\vec{x})). \tag{1}$$

Next come *forcing* and *certification*, the two basic notions of this work:

$$\begin{aligned}
\mathbf{U} \Vdash^{\mathbf{M}} f(\vec{x}) = w \quad &\iff \quad f(\vec{x}) = w \\
&\qquad \ \& \text{ every homomorphism } \pi : \mathbf{U} \to \mathbf{M} \text{ respects } f \text{ at } \vec{x}, \\
\mathbf{U} \Vdash^{\mathbf{M}}_c f(\vec{x}) = w \quad &\iff \quad \mathbf{U} \text{ is finite, generated by } \vec{x} \ \ \& \ \mathbf{U} \Vdash^{\mathbf{M}} f(\vec{x}) = w, \\
\mathbf{U} \Vdash^{\mathbf{M}}_c f(\vec{x})\downarrow \quad &\iff \quad (\exists w)[\mathbf{U} \Vdash^{\mathbf{M}}_c f(\vec{x}) = w].
\end{aligned}$$

If $\mathbf{U} \Vdash^{\mathbf{M}}_c f(\vec{x}) = w$, we call $\mathbf{U}$ a *certificate* for f at $\vec{x}$ in $\mathbf{M}$.[1]

It can be shown that if $f : M^n \to W$ is computed from the primitives of $\mathbf{M}$ by any one of the standard (deterministic or non-deterministic) computation models

[1] To the best of my knowledge, certificates were first introduced in [7], Pratt's proof that primality is NP. The present notion is model theoretic and more abstract than Pratt's, but the idea is the same.

of algorithms from primitives, then f is certified in $\mathbf{M}$ at every $\vec{x}$. More is true: *if C is a computation of $f(\vec{x})$ from $\Phi^{\mathbf{M}}$ by one of the standard models, then*

$$\{(\phi, \vec{u}, \phi^{\mathbf{M}}(\vec{u})) : C \text{ calls } \phi \text{ at } \vec{u}\} = \text{eqdiag}(\mathbf{U})$$

for some $\mathbf{U} \subseteq_p \mathbf{M}$ such that $\mathbf{U} \Vdash_c^{\mathbf{M}} (f(\vec{x}))\downarrow$. This is the robustness of the homomorphism method mentioned above. On the other hand, it is easy to check that *every $f : \mathbb{N}^n \to \mathbb{N}$ is certified at every $\vec{x} \in \mathbb{N}^n$ in* $(\mathbb{N}, 0, S)$: certification captures some aspects of the *uniformity* of algorithms from primitives—that they apply "the same process" on all inputs—but not their *effectiveness.*

The intrinsic number-of-calls complexity measure. If $\Phi_0 \subseteq \Phi$ is part of the vocabulary and f is certified at $\vec{x}$ in $\mathbf{M}$, we set

$$\text{calls}_{\Phi_0}(\mathbf{M}, f, \vec{x}) = \min\{|\text{eqdiag}(\mathbf{U}\restriction\Phi_0)| : \mathbf{U} \Vdash_c^{\mathbf{M}} f(\vec{x})\downarrow\}.$$

By the analysis above, if C is a computation of $f(\vec{x})$ from $\Phi^{\mathbf{M}}$ by any of the standard computation models, then

$$\text{calls}_{\Phi_0}(\mathbf{M}, f, \vec{x}) \leq \text{the number of calls to } \Phi_0^{\mathbf{M}} \text{ in } C.$$

One can also argue that $\text{calls}_{\Phi_0}(\mathbf{M}, f, \vec{x})$ is an "absolute" lower bound to the number of calls to primitives in $\Phi_0^{\mathbf{M}}$, that is it restricts *every algorithm* that computes $f(\vec{x})$ from $\Phi^{\mathbf{M}}$. This cannot, of course, be proved without a precise definition of what algorithms are.

Horner's rule is optimal for nullity. For $n \geq 1$ and $a_0, \ldots, a_n, x \in \mathbb{R}$, let

$$N_{\mathbb{R}}(a_0, a_1, \ldots, a_n, x) \iff a_0 + a_1 x + \cdots + a_n x^n = 0.$$

This is the *nullity relation* (0-testing) for real polynomials. The classical Horner's rule decides $N_{\mathbb{R}}$ using no more than n multiplications, n additions and one equality test. Its optimality for computing the *value* $a_0 + a_1 x + \cdots + a_n x^n$ by straight line programs is proved in [6], in which Pan introduced the *substitution method*, an early and basic tool of algebraic complexity theory.

Theorem 11. *Let $\mathbf{R} = (\mathbb{R}, 0, 1, +, -, \cdot, \div, =)$. If $n \geq 1$ and $a_0, \ldots, a_n, x$ are algebraically independent, then:*

(1) $\text{calls}_{\{\cdot,\div\}}(\mathbf{R}, N_{\mathbb{R}}, \vec{a}, x) = n$,
(2) $\text{calls}_{\{+,-\}}(\mathbf{R}, N_{\mathbb{R}}, \vec{a}, x) = n - 1$,
(3) $\text{calls}_{\{+,-,=\}}(\mathbf{R}, N_{\mathbb{R}}, \vec{a}, x) = n + 1$.

For *algebraic decision trees*, (1) is proved in [2], and a result equivalent to (3) is proved in [1]. The methods in these papers are quite different from ours. We follow closely Winograd's argument in [8, 9] for polynomial evaluation: we show by induction on n three much stronger (and somewhat different) results which include (1) – (3) as special cases. For (3) which requires the use of homomorphisms rather than embeddings, we show the following lemma about an arbitrary substructure $\mathbf{U} \subseteq_p \mathbf{R}$, where $\mathbb{K}$ = the field of real algebraic numbers and for $a_1, \ldots, a_n > 0$,

$$\text{Roots}(\vec{a}) = \{\sqrt[m]{a_i} : m \in \mathbb{N}, i = 1, \ldots, n\}.$$

An addition $u+v$, subtraction $u-v$ or equality test $u=v, u \neq v$ in eqdiag($\mathbf{U}$) is *trivial* if $u, v \in \mathbb{K}(x,z)$.

Lemma 12. *Suppose $n \in \mathbb{N}$, $\overline{g} \in \mathbb{K}$, $\overline{g} \neq 0$, $z, a_1, \ldots, a_n, x$ are positive, algebraically independent real numbers, and $\mathbf{U}$ is a finite substructure of $\mathbf{R}$ generated by*

$$(U \cap \mathbb{K}) \cup \{x, z\} \cup (U \cap \mathrm{Roots}(\vec{a}))$$

which has $< (n+1)$ non-trivial additions, subtractions and equality tests. Then there is a field homomorphism $\pi : \mathbb{K}(x, z, \mathrm{Roots}(\vec{a})) \to \mathbb{K}(x, \mathrm{Roots}(\vec{a}))$ such that

(a) *$\pi(u) = u$ for every $u \in \mathbb{K}(x)$,*
(b) *π is totally defined on U, and*
(c) *$\pi(z) + \overline{g}\Big(\pi(a_1)x^1 + \cdots + \pi(a_n)x^n\Big) = 0$.*

References

[1] P. Bürgisser, T. Lickteig, and M. Shub. Test complexity of generic polynomials. *Journal of Complexity*, 8:203–215, 1992.

[2] P. Bürgisser and T. Lickteig. Verification complexity of linear prime ideals. *Journal of pure and applied algebra*, 81:247–267, 1992.

[3] Lou van den Dries and Yiannis N. Moschovakis. Is the Euclidean algorithm optimal among its peers? *Bulletin of Symbolic Logic*, 10:390–418, 2004.

[4] Lou van den Dries and Yiannis N. Moschovakis. Arithmetic complexity. *ACM Trans. Comput. Logic*, 10(1):1–49, 2009.

[5] Yiannis N. Moschovakis. The axiomatic derivation of absolute lower bounds. In preparation.

[6] V. Ya. Pan. Methods for computing values of polynomials. *Russian Mathematical Surveys*, 21:105 – 136, 1966.

[7] Vaughan Pratt. Every prime has a succint certificate. *SIAM Journal of computing*, 4:214 – 220, 1975.

[8] Shmuel Winograd. On the number of multiplications required to compute certain functions. *Proceedings of the National Academy of Sciences, USA*, 58:1840 – 1842, 1967.

[9] Shmuel Winograd. On the number of multiplications required to compute certain functions. *Communications on pure and applied mathematics*, 23:165 – 179, 1970.

The geometry of proof analysis: from rule systems to systems of rules

Sara Negri

The basic goal of proof analysis is a maximal extraction of information from the analysis of proofs in a formal inference system. This is made possible through the determination of complete analytic sequent calculi with good structural properties such as admissibility of cut, weakening, and contraction.

The goal has been achieved fully for classical and intuitionistic logic, but the extension to mathematical theories and to modal and other non-classical logics presents well known difficulties. When a purely logical system is extended by axioms, the generalized Hauptsatz permits only to reduce cuts to cuts on axioms, so full analyticity is lost.

In previous work, it has been shown how the conversion of axioms into rules of inference allows full cut elimination for theories with universal axioms [7], geometric theories [5], cogeometric theories [8] and for a wide class of non-classical logics, including provability logic, substructural logics [6], and intermediate logics [1].

The conversion of axioms into rules of inference is obtained by a uniform procedure that eliminates the logical constants by absorbing them into the geometry of the rules of inference. The added rules are are either all left or all right rules; depending on whether the left or right rule paradigm is chosen, conjunction/disjunction correspond to commas/branchings, implication to the split of antecedent/succedent into conclusion/premisses and negative existential/positive universal quantifiers to variable conditions in left/right rules. The result is a calculus that is complete for the theory or logic under consideration and that has the same structural properties as the logical calculus one started with.

An application of proof analysis to epistemic logic has lead to the need of an extension of the conversion of axioms into rules of inference for axioms that have a more complex structure than that of geometric or cogeometric implications. It has been shown [4] that the frame condition that corresponds to the knowability principle, expressed in natural language by "If A is true, then it is possible to know A" and in the language of bimodal logic by $A \supset \Diamond\mathcal{K}A$, is the condition

$$\forall x \exists y (x R_{\Diamond} y \,\&\, \forall z (y R_{\mathcal{K}} z \supset x \leqslant z))$$

Here $\leqslant$, $R_{\Diamond}$, and $R_{\mathcal{K}}$ indicate the intuitionistic, alethic, and epistemic accessibility relations, respectively. This condition can in turn be converted into two inference rules

$$\frac{xR_{\Diamond}y, \Gamma \to \Delta}{\Gamma \to \Delta}\, {\scriptstyle Ser_{\Diamond}} \qquad \frac{x \leqslant z, xR_{\Diamond}y, yR_{\mathcal{K}}z, \Gamma \to \Delta}{xR_{\Diamond}y, yR_{\mathcal{K}}z, \Gamma \to \Delta}\, {\scriptstyle \Diamond\mathcal{K}\text{-}Tr}$$

The rules come with additional conditions, namely that y is not in the conclusion of $Ser_{\Diamond}$, that $\Diamond\mathcal{K}$-Tr is applied above $Ser_{\Diamond}$, and that the middle term y of $\Diamond\mathcal{K}$-Tr is the eigenvariable of $Ser_{\Diamond}$.

A set of rules subject to an interdependency expressed by certain conditions on their order of applicability and by a mutual variable condition is called a *system of rules.*

As another example, the conversion of the axiom of least upper bound into a system of two rules is considered. It is shown that the axiom

$$\forall xy \exists z ((x \leqslant z \,\&\, y \leqslant z) \,\&\, \forall w (x \leqslant w \,\&\, y \leqslant w \supset z \leqslant w)) \qquad \textit{lub-A}$$

is derivable by the system of rules

$$\frac{x \leqslant z, y \leqslant z, \Gamma \to \Delta}{\Gamma \to \Delta}\, {\scriptstyle lub\text{-}E} \qquad \frac{z \leqslant w, x \leqslant w, y \leqslant w, \Gamma \to \Delta}{x \leqslant w, y \leqslant w, \Gamma \to \Delta}\, {\scriptstyle lub\text{-}U}$$

Here the condition is that in rule *lub-E* the variable z is not in Γ, Δ, that in a derivation rule *lub-U* should always be applied above (but not necessarily immediately above) rule *lub-E*, and that the variable z is the eigenvariable of *lub-E*.

Conversely, it is shown that any derivation that uses the two rules in compliance with the side conditions can be converted into a derivation that uses cuts on the axiom in place of the extra rules.

The procedure of conversion of axioms into systems of rules is generalized by defining inductively a class of *generalized geometric implications* and of *generalized geometric rule schemes*. The base case is given by geometric implications, also called geometric axioms, denoted by GA, and by the geometric rule scheme GRS:

$$GA_0 \equiv GA, \; GRS_0 \equiv GRS$$

The inductive step is defined as follows:

$$GA_{n+1} \equiv \forall \overline{x}(\,\&\, P_i \supset \exists y_1 \,\&\, GA_n \vee \cdots \vee \exists y_m \,\&\, GA_n)$$

Here $\&\, GA_i$ denotes a conjunction of GA_i-axioms.

The generalized geometric scheme GRS_{n+1} is defined inductively with the same conditions as above, once the schemes GRS_n have been defined, as follows:

$$\dfrac{\begin{array}[b]{c}\Gamma'_1 \to \Delta'_1\\ \vdots\\ \mathcal{D}^1_n\\ \vdots\\ \Gamma''_1 \to \Delta''_1\\ \vdots\\ \mathcal{D}^1\\ \vdots\\ z_1 = z_1, \overline{P}, \Gamma \to \Delta\end{array} \quad \dots \quad \begin{array}[b]{c}\Gamma'_m \to \Delta'_m\\ \vdots\\ \mathcal{D}^m_n\\ \vdots\\ \Gamma''_m \to \Delta''_m\\ \vdots\\ \mathcal{D}^m\\ \vdots\\ z_m = z_m, \overline{P}, \Gamma \to \Delta\end{array}}{\overline{P}, \Gamma \to \Delta}$$

Here z_i are the eigenvariables of the last inference step, the derivations indicated with $\mathcal{D}^i_n$ use rules of the form $GRS_n(z_i)$ that correspond to the geometric axioms $GA_n(z_i/x_i)$ in addition to logical rules, and the $\mathcal{D}^i$ use only logical rules.

It is shown by induction on n that the generalized geometric axioms GA_n and the generalized geometric rule schemes GRS_n are equivalent (in the sense of being interderivable) and that the addition of systems of generalized geometric rules to a classical or intuitionistic sequent calculus of $G3$-type, such as **G3c** and **G3im**, maintains the admissibility of all the structural rules.

As an immediate application, a generalized Barr theorem is proved: *For all n, if a geometric implication is derivable in* **G3c** $+GRS_n$*, it is derivable in* **G3im** $+GRS_n$.

Related results on conservative classes are based on permutation and translation arguments [9, 2, 3]. Further work includes an extension of the method to cover properties, such as well foundedness, not expressible by first-order sentences, and the determination of analytic proof systems for a wide class of non-classical logics.

References

[1] R. Dyckhoff and S. Negri. Proof analysis in intermediate logics. *Archive for Mathematical Logic*, 2011, DOI 10.1007/s00153-011-0254-7.

[2] H. Ishihara. A note on the Gödel-Gentzen translation. *Mathematical Logic Quarterly*, vol. 46, 2000, pp. 135–139.

[3] H. Ishihara. Some conservative extension results on classical and intuitionistic sequent calculi. Ms., 2011.

[4] P. Maffezioli, A. Naibo, and S. Negri. The Church-Fitch knowability paradox in the light of structural proof theory. Ms., 2011.

[5] S. Negri. Contraction-free sequent calculi for geometric theories, with an application to Barr's theorem. *Archive for Mathematical Logic*, vol. 42, pp. 389–401, 2003.

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

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

[8] S. Negri and J. von Plato. *Proof Analysis: A Contribution to Hilbert's Last Problem.* Cambridge University Press, 2011.

[9] V. Orevkov. On Glivenko sequent classes. In V. Orevkov (ed) *The calculi of symbolic logic I*, American Mathematical Society, Providence, 1971, pp. 147–173. (English translation of the Proceedings of the Steklov Institute of Mathematics, vol. 98, 1968).

Understanding the Hardness of Proving Formulas in Propositional Logic

Jakob Nordström

(joint work with Eli Ben-Sasson)

Proving formulas in propositional logic is a fundamental problem in computer science and mathematics. On the one hand, this problem is believed to be theoretically intractable in general, and deciding whether this is the case is one of the famous million dollar Millennium Problems. On the other hand, these days automated theorem provers, or so-called SAT solvers, are routinely used to solve large-scale real-world applications of this problem with millions of variables. This is in contrast to that there are also known small example formulas with just hundreds of variables that causes even state-of-the-art SAT-solvers to stumble.

What lies behind the spectacular success of SAT-solvers? And how can one determine whether a particular formula is hard or tractable? In this talk, we will discuss what the field of proof complexity has to say about these questions.

In particular, we propose that the space complexity of a formula could be a good measure of its hardness. We prove that this would have drastic implications for the impossibility of simultaneously optimizing time and memory consumption, the two main resources of SAT solvers. Somewhat surprisingly, our results are obtained by relatively elementary means from combinatorial pebble games on graphs, studied extensively in the 70s and 80s.

This talk is based on joint work with Eli Ben-Sasson at the Technion in Haifa, Israel.

Bar Recursion and the Product of Selection Functions

Paulo Oliva
(joint work with Martín Escardó)

1. Selection Functions

In recent joint work with Martín Escardó [2] we have identified a family of functionals of finite type, so-called *selection functions*, which play a major role in the computational interpretation of classical proof in arithmetic and analysis. Formally, selection functions are functionals ε of type

$$\varepsilon : \ (X \to R) \to X,$$

where X and R are finite types. Such types are abbreviated as $J_R X \equiv (X \to R) \to X$, as they are a strong monad J_R, for any fixed R. The terminology "selection function" derives from the observation that in the particular case when R is the type of booleans, then ε "picks" an element of X given a predicate over X, i.e. $\varepsilon p \in X$ for $p\colon X \to \mathbb{B}$. An example of such selection function is the family of Hilbert's epsilon terms, which for any primitive recursive predicate $p_y(x)$, over variable x and y, was such that

$$p_y(t) \to p_y(\varepsilon_y p_y).$$

Such "critical axioms" allow one to define the existential quantifier in terms of ε as

$$\exists x\, p_y(x) \equiv p_y(\varepsilon_y p_y).$$

In our terminology we would say that ε is a selection function for the existential quantifier. Generalising this idea to arbitrary types X and R led to the concept of an arbitrary quantifier $\phi\colon (X \to R) \to R$ and the set (possibly empty) of its corresponding selection functions $\varepsilon\colon (X \to R) \to X$ satisfying the equation

$$\phi p = p(\varepsilon p). \tag{1}$$

For instance, the supremum functional $\sup\colon ([0,1] \to \mathbb{R}) \to \mathbb{R}$ is an attainable quantifier with $\mathrm{argsup}\colon ([0,1] \to \mathbb{R}) \to [0,1]$ as its selection function since we have

$$\sup p = p(\mathrm{argsup}\, p).$$

Moreover, any fixed point operator $\mathrm{fix}\colon (X \to X) \to X$ can be viewed as both a selection function and a quantifier, and the fixed point equation

$$\mathrm{fix}\, p = p(\mathrm{fix}\, p),$$

says that fix is an attainable quantifier with fix itself as its selection function.

In the same way that quantifiers over types X and Y can be nested to produce a quantifier over the product space $X \times Y$, so can selection functions. The product of two selection functions $\varepsilon\colon J_R X$ and $\delta\colon J_R Y$ (cf. [2]) is given by

$$(\varepsilon \otimes \delta)(q^{X \times Y \to R}) \overset{X \times Y}{=} (\underbrace{\varepsilon(\lambda x.q(x, b(x)))}_{a}, \underbrace{\delta(\lambda y.q(a, y))}_{b(a)}) \tag{2}$$

where $b(x) = \delta(\lambda y.q(x,y))$.

2. Bar Recursion

Moreover, given a family of selection function $(\varepsilon_n)_{n\in\mathbb{N}}\colon \Pi_{n\in\mathbb{N}} J_R X_i$ we can simply iterate the binary product above as

$$\mathsf{IPS}_n(\varepsilon) = \varepsilon_n \otimes \mathsf{IPS}_{n+1}(\varepsilon) \tag{3}$$

to obtain a selection function on the product space $\mathsf{IPS}_n\colon J_R \Pi_{i\geq n} X_i$. This is called the *implicitly controlled product of selection function* and has been first defined in [2] and shown to be primitive recursively equivalent to modified bar recursion in [1, 3]. For this product to be well-defined, however, one must require that R be a discrete type (e.g. $\mathbb{N}$ or $\mathbb{B}$) and continuity of $q\colon \Pi_i X_i \to R$ must be assumed.

Alternatively, one can drop the assumption that R is discrete by having a "measure" function $l\colon R \to \mathbb{N}$ so that the product can be iterated as

$$\mathsf{EPS}_n(\varepsilon) = \lambda q. \begin{cases} \mathbf{0} & \text{if } \ l(q(\mathbf{0})) < n \\ (\varepsilon_n \otimes \mathsf{EPS}_{n+1}(\varepsilon))\,(q) & \text{otherwise,} \end{cases} \tag{4}$$

where $\mathbf{0}$ is the constant zero functional. This, as also shown in [1, 3], is primitive recursively equivalent to Spector's bar recursion [6]. We have also recently shown (together with Thomas Powell) [5] that Gödel's system T can alternatively be formulated with the finite product of selection function (where l is a constant function $\lambda r.n$), since having such finite product allows one to define the primitive recursive recursors for all finite types.

3. Sequential Games

Finally, the most novel aspect of selection functions and their corresponding products, is in the connection with sequential games and the computation of optimal strategies and plays. As explained in [2, 4], we can think of the types X_i as the set of possible moves at round i, and R as the set of possible outcomes of the game. They $q\colon \Pi_i X_i \to R$ is the usual utility function (also called payoff function), which for any play $\alpha\colon \Pi_i X_i$ calculates the outcome $q\alpha\colon R$. Moreover, the selection functions $\varepsilon_i\colon J_R X_i$ specify the goal of the player at round i, as it calculates a move $\varepsilon p\colon X_i$ given any mapping $p\colon X_i \to R$ which can be thought of as a mapping from possible moves to their respective outcome. What we have shown is that, looking at these types as such, the product of selection functions computes an optimal play

$$\alpha = \mathsf{IPS}_0(\varepsilon)(q)$$

in the corresponding sequential game. The play is optimal in the sense that for some family $p_i\colon X_i \to R$ we have that $\alpha(i) = \varepsilon_i p_i$ (so each move was chosen according to the given selection function) and that $p_i(\alpha(i)) = q(\alpha)$ (so that from the point of view of player i the function p_i indeed maps the chosen move to the corresponding outcome.

We found surprising that such construction not only appears in Game Theory (backward induction) but is also the same construction behind Bekic's lemma, viewing fixed point operators as selection functions, when $R = X$ (see [4] for details).

References

[1] M. H. Escardó and P. Oliva. Computational interpretations of analysis via products of selection functions. In F. Ferreira, B. Lowe, E. Mayordomo, and L. M. Gomes, editors, *Computability in Europe 2010, LNCS 6158*, pages 141–150. Springer, 2010.

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

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

[4] M. H. Escardó and P. Oliva. Sequential games and optimal strategies. *Royal Society Proceedings A*, 467:1519–1545, 2011.

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

[6] 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.

A quantitative nonlinear strong ergodic theorem for Hilbert spaces

Pavol Safarik

In [5], R. Wittmann presented the following strong nonlinear ergodic theorem for (a class of possibly even discontinuous) selfmappings of an arbitrary subset of a Hilbert space:

Theorem 13 (Wittmann)**.** *Let S be a subset of a Hilbert space and $T : S \to S$ be a mapping satisfying*

$$\text{(W)} \qquad \forall u, v \in S \ (\|Tu + Tv\| \leq \|u + v\|).$$

Then for any starting point $x \in S$ the sequence of the Cesàro means

$$A_n x := \frac{1}{n+1} \sum_{i=0}^{n} T^i x$$

is norm convergent.

In my talk, we investigate the computational content of this theorem. Although in general the sequence of the ergodic averages does not have a computable rate of convergence (even for the von Neumann's mean ergodic theorem for a separable space and computable x and T), as was shown by Avigad, Gerhardy and Towsner in [1], the so called metastable (or quantitative) version nevertheless has a primitive recursive bound. In our case this means that given the assumptions from Wittmann's theorem, the following holds

$$\forall b, l \in \mathbb{N}, g : \mathbb{N} \to \mathbb{N}, x \in S \exists m \leq M(l, g, b) \big(\|x\| \leq b \to \|A_m x - A_{m+g(m)} x\| \leq 2^{-l}\big),$$

for a primitive recursive M. Such a bound M can be defined as follows:

$$\begin{aligned}
M(l,g,b) &:= (N(2l+7,g^M) + P(2l+7,g^M,b))b2^{2l+8}+1,\\
P(l,g,b) &:= P_0(l,F(l,g,N(l,g),b),b),\\
F(l,g,n,b)(p) &:= p+n+\tilde{g}((n+p)b2^{l+1}),\\
N(l,g,b) &:= \big(H(l,g,b)\big)^{b^2 2^{l+2}}(0),\\
H(l,g,b)(n) &:= n+P_0(l,F(l,g,n,b))+\tilde{g}((n+P_0(l,F(l,g,n,b)))b2^{l+1}),
\end{aligned}$$

where

$$P_0(l,f,b) := \tilde{f}^{b^2 2^l}(0), \quad \tilde{g}(n) := n+g(n),\; g^M(n) := \max_{i\leq n+1} g(i).$$

Note that apart from the counterfunction g and the precision l, this bound depends only on b (a bound for the norm of x) and not on S, T, or x itself.
It is one of the goals of this talk to demonstrate that there are proof-theoretic means to systematically obtain such uniform bounds. In fact, for many theorems the existence of a uniform bound is guaranteed by Kohlenbach's metatheorems introduced in [3] and refined in [2]. Additionally, proof theoretic methods such as Kohlenbach's monotone functional interpretation (see [4]) can be used to systematically obtain these effective bounds.
On the other hand, we have here a rare example of an application of these techniques to not necessarily continuous operators. In logical terms this amounts to the subtlety that only a weak version of extensionality is available. Also, for the first time, we obtain a bound which in fact makes use of nested iteration. One can see this quickly on the term M above. While F as a function is defined via iteration of the counterfunction g, it itself is being iterated by P. This is a direct consequence of the logical form of Wittmann's original proof.
It is a surprising observation that so far for all metastable versions of strong ergodic theorems primitive recursive bounds could be obtained.

References

[1] J. Avigad, P. Gerhardy, and H. Towsner. Local Stability of Ergodic Averages. *Trans. Amer. Math. Soc.*, 362:261–288, 2010.

[2] P. Gerhardy and U. Kohlenbach. General logical metatheorems for functional analysis. *Trans. Amer. Math. Soc.*, 360:2615–2660, 2008.

[3] U. Kohlenbach. Some logical metatheorems with application in functional. *Trans. Am. Math. Soc.*, 357:89–128, 2005.

[4] U. Kohlenbach. Analyzing proofs in analysis. In *W. Hodges, M. Hyland, C. Steinhorn, J. Truss, Editors, Logic: from Foundations to Applications* at *European Logic Colloquium (Keele, 1993)*, pages 225–260. Oxford University Press, 1996.

[5] R. Wittmann. Mean Ergodic Theorems for nonlinear operators. *Proceedings of the AMS*, 108(3):781–788, 1990.

Induction in Algebra: a Toy Example

Peter Schuster

As is well known, the statement ”every nonconstant coefficient of an invertible polynomial is nilpotent” can be reduced to the case, which in turn is readily settled, of polynomials over an integral domain. The reduction is usually done by an instance of Krull’s Lemma in combination with a proof by contradiction. From this however one can extract a direct proof without prime ideals that is based on induction over a finite poset.

Simultaneous inductive/coinductive definition of continuous functions

Helmut Schwichtenberg

When extracting computational content from proofs in constructive analysis it can be helpful to use simultaneous inductive/coinductive definitions of (uniformly) continuous real functions. The talk reports on an attempt to design the underlying theory, based on recent work of Ulrich Berger.

References

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

[2] Ulrich Berger, Kenji Miyamoto, Helmut Schwichtenberg, and Monika Seisenberger. Minlog - A Tool for Program Extraction Supporting Algebras and Coalgebras. In Corina Cirstea Andrea Corradini, Bartek Kli, editor, *Algebra and Coalgebra in Computer Science, CALCO’11*, volume 6859 of *LNCS*, pages 393–399. Springer, 2011.

[3] Ulrich Berger and Monika Seisenberger. Proofs, programs, processes. In F. Ferreira et al., editor, *Proceedings CiE 2010*, volume 6158 of *LNCS*, pages 39–48. Springer Verlag, Berlin, Heidelberg, New York, 2010.

[4] Helmut Schwichtenberg. Realizability interpretation of proofs in constructive analysis. *Theory of Computing Systems*, 43(3):583–602, 2008.

[5] Helmut Schwichtenberg and Stanley S. Wainer. *Proofs and Computations*. Perspectives in Logic. Association for Symbolic Logic and Cambridge University Press, to appear 2011.

Ideal and Concrete Objects in Type Theory

Anton Setzer
(joint work with Chi Ming Chuang)

Usually in type theory we work only with computationally meaningful objects, i.e. concrete objects. In this talk we explore the use of ideal objects in type theory, which will be represented as postulated axioms.

In the presence of postulated axioms, we loose in general the property that every element of an algebraic data type starts with a constructor. The reason is that there is no reduction, if we introduce an element by a postulated axiom and then eliminate it using an elimination rule.

However, if we add the restriction that all postulated axioms have as result type only postulated types, this problems doesn't occur any more. We prove this property assuming that the type theory is normalising.

We will apply this to exact real number computations. Natural numbers, integers and rationals are introduced as concrete data types. The real numbers are axiomatized as postulated types. Since we can embed the concrete numbers into the postulated real numbers we get a link between the ideal and concrete world. Then we can define the concrete real numbers as the ideal reals which are Cauchy reals or have a signed digit representation. This approach has been used for efficient exact real number computations for signed digit representable reals.

Finally we explore that in the ideal world we can add classical logic using postulated connectives. Negated axioms (using the concrete falsity) can be allowed provided the type theory is consistent. Here we obtain an instance of Hilbert's statement: consistency implies existence.

Weak theories of operations, truth and types

Thomas Strahm

(joint work with Sebastian Eberhard)

In this talk we survey recent developments in the study of proof-theoretically weak systems of Feferman's explicit mathematics and theories of truth. We start off from pure first-order applicative theories based on a version of untyped combinatory logic and augment them by the typing and naming discipline of explicit mathematics or, alternatively, by a truth predicate in the sense of Frege structures. We discuss the proof-theoretic strength of the so-obtained formalisms and the general relationship between weak truth theories and explicit mathematics. In particular, we consider two truth theories T_{PR} and T_{PT} of primitive recursive and feasible strength. The latter theory is a novel abstract truth-theoretic setting which is able to interpret expressive feasible subsystems of explicit mathematics and arithmetic.

References

[1] Cantini, A. Proof-theoretic aspects of self-referential truth. In *Tenth International Congress of Logic, Methodology and Philosophy of Science, Florence, August 1995*, Maria Luisa Dalla Chiara et. al., Ed., vol. 1. Kluwer, September 1997, pp. 7–27.

[2] Cantini, A. Choice and uniformity in weak applicative theories. In *Logic Colloquium '01*, M. Baaz, S. Friedman, and J. Krajíček, Eds., vol. 20 of *Lecture Notes in Logic*. Association for Symbolic Logic, 2005, pp. 108–138.

[3] Eberhard, S. A truth theory over an applicative framework of strength PT. Preliminary draft, February 2011.

[4] Eberhard, S., and Strahm, T. Weak theories of truth and explicit mathematics. Submitted for publication.

[5] Probst, D. The provably terminating operations of the subsystem PETJ of explicit mathematics. *Annals of Pure and Applied Logic 162*, 11 (2011), 934–947.

[6] Spescha, D., and Strahm, T. Elementary explicit types and polynomial time operations. *Mathematical Logic Quarterly 55*, 3 (2009), 245–258.

[7] Spescha, D., and Strahm, T. Realizability in weak systems of explicit mathematics. *Mathematical Logic Quarterly 57*, 6 (2011), 551–565.

[8] Strahm, T. Theories with self-application and computational complexity. *Information and Computation 185* (2003), 263–297.

The Provability Logic of All Arithmetics of a Theory

Albert Visser

In this talk, we first explain the notion of the provability logic of an (interpretation of) arithmetic in a theory.

We give an exposition of the state of the art concerning the scope of Solovay's theorem about the arithmetical completeness of Löb's Logic. There is a gap between the theories for which the soundness of Löb's Logic can be proved *sine ira et studio* and the theories for which we can prove Solovay's theorem. However, if we consider the simultaneous provability logic of all arithmetics of a given theory, we can give a definitive result in full generality.

We present an example to show that there is a sequential theory such that the provability logic of all arithmetics in that theory is not assumed as the provability logic of any arithmetic in that theory. The verification of the example employs a generalization of results by Jan Krajíček and, independently, Harvey Friedman. We have a brief look at the generalization.

On Elementary Patterns of Resemblance

Gunnar Wilken

We give a heuristically detailed illustration on elementary patterns of resemblance, an approach to ordinal notations discovered by Timothy J. Carlson, with a focus on the arithmetical analysis of patterns of orders 1 and 2. For further details see my Habilitationsschrift (Arithmetic Analysis of Elementary Patterns of Order 1 and 2., WWU Muenster 2011), which is available at the library.

Reporter: Pavol Safarik

Participants

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

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

Dr. Arnold Beckmann
Department of Computer Science
Swansea University
Singleton Park
GB-Swansea SA2 8PP

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

Dr. Benno van den Berg
Mathematisch Instituut
Universiteit Utrecht
Budapestlaan 6
P. O. Box 80.010
NL-3508 TA Utrecht

Dr. Ulrich Berger
Department of Computer Science
University of Wales Swansea
Singleton Park
GB-Swansea SA2 8PP

Prof. Dr. Douglas S. Bridges
Department of Mathematics
University of Canterbury
Private Bag 4800
Christchurch 8140
NEW ZEALAND

Dr. Eyvind Briseid
Department of Mathematics
University of Oslo
P. O. Box 1053 - Blindern
0316 Oslo
NORWAY

Ulrik Torben Buchholtz
Department of Mathematics
Stanford University
Stanford , CA 94305-2125
USA

Prof. Dr. Wilfried Buchholz
Mathematisches Institut
Ludwig-Maximilians-Universität
München
Theresienstr. 39
80333 München

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

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

Dr. Hannes Diener
Fakultät IV
-Mathematik-
Universität Siegen
Hölderlinstr. 3
57076 Siegen

Prof. Dr. Fernando Ferreira
Departamento de Matematica
FCUL - Universidade de Lisboa
Campo Grande, ED. C6, Piso 2
1749016 Lisboa
PORTUGAL

Jaime Gaspar
Fachbereich Mathematik
TU Darmstadt
Schloßgartenstr. 7
64289 Darmstadt

Dr. Lew Gordeew
WSI
Universität Tübingen
Sand 13
72076 Tübingen

Dr. Rosalie Iemhoff
Faculty of Philosophy
Utrecht University
Janskerkhof 13a
NL-3512 BL Utrecht

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

Prof. Dr. Gerhard Jäger
Institut für Informatik und
Angewandte Mathematik
Universität Bern
Neubrückstr. 10
CH-3012 Bern

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

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

Dr. Leszek Kolodziejczyk
Department of Mathematics
University of California, San Diego
9500 Gilman Drive
La Jolla , CA 92093-0112
USA

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

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

Alexander P. Kreuzer
Fachbereich Mathematik
Arbeitsgruppe Logik
TU Darmstadt
Schlossgartenstr. 7
64289 Darmstadt

Dr. Graham Leigh
Faculty of Philosophy
University of Oxford
10 Merton Street
GB-Oxford OX1 4JJ

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

Prof. Dr. Angus John MacIntyre
School of Mathematical Sciences
Queen Mary College
Mile End Road
GB-London E1 4NS

Prof. Dr. Per Martin-Loef
Matematiska Institutionen
Stockholms Universitet
S-10691 Stockholm

Prof. Dr. Grigori Mints
Department of Philosophy
Building 90
Stanford University
Stanford CA 94305-2155
USA

Prof. Dr. Ieke Moerdijk
Mathematisch Instituut
Universiteit Utrecht
P.O.Box 80.010
NL-3508 TA Utrecht

Prof. Dr. Joan Rand Moschovakis
Department of Mathematics
UCLA
405 Hilgard Ave.
Los Angeles , CA 90095-1555
USA

Prof. Dr. Yiannis N. Moschovakis
Department of Mathematics
UCLA
405 Hilgard Ave.
Los Angeles , CA 90095-1555
USA

Dipl.Math. Sebastian Müller
Faculty of Mathematics and Physics
Department of Algebra
Charles University
Sokolovska 83
186 75 Praha 8
CZECH REPUBLIC

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

Prof. Dr. Jakob Nordström
School of Computer Science and Communication
Royal Institute of Technology
S-10044 Stockholm

Dr. Paulo Oliva
School of Electronic Engineering and Computer Science
Queen Mary, University of London
Mile End Road
GB-London E1 4NS

Dr. Jaap van Oosten
Mathematisch Instituut
Universiteit Utrecht
Budapestlaan 6
P. O. Box 80.010
NL-3508 TA Utrecht

Prof. Dr. Erik Palmgren
Matematiska Institutionen
Stockholms Universitet
S-10691 Stockholm

Prof. Dr. Chris Pollett
Department of Computer Science
San Jose State University
214 MacQuarrie Hall
San Jose CA 95192-0103
USA

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
GB-Leeds LS2 9JT

Pavol Safarik
Fachbereich Mathematik
TU Darmstadt
Schloßgartenstr. 7
64289 Darmstadt

Dr. Peter Schuster
Department of Pure Mathematics
University of Leeds
GB-Leeds LS2 9JT

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

Dr. Anton G. Setzer
Department of Computer Science
Swansea University
Singleton Park
GB-Swansea SA2 8PP

Prof. Dr. Thomas Strahm
Institut für Informatik und
Angewandte Mathematik
Universität Bern
Neubrückstr. 10
CH-3012 Bern

Prof. Dr. Thomas Streicher
Fachbereich Mathematik
Arbeitsgruppe Logik
TU Darmstadt
Schlossgartenstr. 7
64289 Darmstadt

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

Prof. Dr. Albert Visser
Faculty of Humanities
Department of Philosophy
P.O.Box 80103
NL-3508 TC Utrecht

Prof. Dr. Stanley S. Wainer
School of Mathematics
University of Leeds
GB-Leeds LS2 9JT

Prof. Dr. Andreas Weiermann
Universiteit Gent
Vakgroep Zuivere Wiskunde en
Computeralgebra
Krijgslaan 281 Gebouw S22
B-9000 Gent

Dr. Gunnar Wilken
Okinawa Institute of Science
and Technology
1919-1 Tancha, Onna-son
Kunigami-gun
Okinawa 904-0412
JAPAN