Mathematisches Forschungsinstitut Oberwolfach

Report No. 14/2005

Mathematical Logic: Proof Theory, Type Theory and Constructive Mathematics

Organised by
Samuel R. Buss (La Jolla)
Yiannis N. Moschovakis (Los Angeles)
Helmut Schwichtenberg (München)

March 20th – March 26th, 2005

Abstract. The workshop “Mathematical Logic: Proof Theory, Type Theory and Constructive Mathematics” covered various topics of mathematical logic dealing with proofs as formal objects and computations induced by proofs.

Mathematics Subject Classification (2000): 03Fxx.

Introduction by the Organisers

The workshop *Mathematical Logic: Proof Theory, Type Theory and Constructive Mathematics*, was held March 20th–March 26th, 2005 and had several aims.

To promote interaction between traditional proof theory and a more structural mathematical proof theory. It is hoped to encourage the application-oriented to consider their tools more abstractedly and those with foundational leaning to focus on possible applications. Questions of feasibility should play an essential role here.

To further develop constructive mathematics. For instance, there has been recent progress in designing some central notions for a constructive treatment of algebraic topology (like that of a scheme, in Peter Schuster’s Habilitationsschrift 2003). An essential tool is the so-called formal or point-free topology, developed by Sambin, Coquand and others. Type theory offers some unifying concepts for a useful dicussion of the notions involved.

To explore the relevance of classical mathematics to algorithms. Recent work of Kohlenbach, Lombardi, Roy and others showed, in very different ways, that mathematical proofs that use a priory highly non computational concepts, such as Zorn’s lemma or compactness principles, may contain implicitely very interesting computational information. For instance, recent work of Kohlenbach –using a modification of Gödel's Dialectica interpretation– could extract not only algorithmic information but also new theorems, surprising to the expert (here in the field of metric fixed point theory).

To understand in depth mathematical concepts in connection with algorithms and proofs, and also to further develop the notion of a certificate, aimed at unifying attempts to connect proof systems and computer algebra systems.

To develop connections between proof theory and computational complexity. Specifically to understand the connections between the complexity of formal proofs, computational complexity and descriptive complexity.

The variety of these aims is well reflected by the many talks given. As can be seen from their abstracts, presented in chronological order, they cover a broad range of topics — without losing their common theme, that is, mathematical logic and the formal reasoning about proofs and computations.

In order to provide the participants with an overview of some of the recent developments in some of the covered topics two invited lecture series were given. Both highlighted applications of proof theory to other areas of mathematics. Ulrich Kohlenbach presented proof mining as an area of applications of proof theory to analysis; Thierry Coquand's talk on infinite objects in constructive mathematics showed applications of proof theory to algebra.

Workshop: Mathematical Logic: Proof Theory, Type Theory and Constructive Mathematics

Table of Contents

Abstracts

Proof Mining: Applications of Proof Theory to Analysis

Ulrich Kohlenbach

In recent years (though influenced by papers of G. Kreisel going back to the 50's as well as subsequent work by H. Luckhardt ([20]) and others, see [21]) an applied form of proof theory systematically evolved which sometimes is called "Proof Mining" ([18], see also [1, 3, 2]).
A particularly fruitful area of applications of proof theory in mathematics has been numerical and nonlinear functional analysis.
This 3-part course gives a survey on the logical foundations of this approach and its applications in analysis.

The **first part** discusses various so-called proof interpretations (such as Gödel's functional interpretation and its monotone variants ([6]) and extensions) and derives general meta-theorems on the extractability of effective uniform bounds from ineffective proofs in the context of **concrete Polish spaces** X (such as $C[0,1]$ or L_p for $1 \leq p < \infty$ etc.), compact Polish spaces K and continuous functions between such spaces ([6, 8, 9]). "Uniform" here refers to the fact that the bounds are guaranteed to be independent from parameters in K but only depend on given representations of elements of X. We show that the various conditions involved in these meta-theorems are all necessary and indicate their realm of applicability ([18]) including

(1) the extractability of rates of strong unicity ('moduli of uniqueness') from uniqueness proofs in analysis,
(2) the extractability of rates of convergence from proofs of monotone convergence.

In particular, we present new results in the context of best polynomial Chebycheff and L_1-approximations ([7, 17, 22]).

In the **second part** we develop extended meta-theorems ([13]) which guarantee under quite general conditions the extractability of effective bounds which are even independent from parameters in noncompact (but only metrically bounded) subsets of general classes of axiomatically added **abstract structures** such as metric spaces, hyperbolic spaces, CAT(0)-spaces, normed spaces, uniformly convex and inner product spaces and various classes of functions between them (quasi-nonexpansive, asymptotically and directionally nonexpansive as well as Lipschitz continuous and uniformly continuous functions, among others). We also discuss recent refinements ([5]) which only require weak local boundedness conditions on certain terms (rather than the boundedness of whole substructures).

In the **third part** we apply the extended meta-theorems from the 2nd part to obtain numerous new results in the area of metric fixed point theory ([4, 10, 11, 12, 14, 15, 16, 19]). These results concern both new qualitative information (independence from parameters) as well as new effective bounds on the asymptotic regularity as well as convergence towards a fixed point for Krasnoselski-Mann iterations of nonexpansive, directionally nonexpansive and asympticaly quasi-nonexpansive functions.

References

[1] Berger, U., Buchholz, H., Schwichtenberg, H., Refined program extraction from proofs. Ann. Pure Appl. Logic **114**, pp. 3-25 (2002).

[2] Coquand, T., Hofmann, M., A new method for establishing conservativity of classical systems over their intuitionistic version. Lambda-calculus and logic. Math. Structures Comput. Sci. **9**, pp. 323-333 (1999).

[3] Delzell, C., Kreisel's unwinding of Artin's proof-Part I. In: Odifreddi, P., Kreiseliana, 113-246, A K Peters, Wellesley, MA (1996).

[4] Gerhardy, P., A quantitative version of Kirk's fixed point theorem for asymptotic contraction. Submitted.

[5] Gerhardy, P., Kohlenbach, U., General logical metatheorems for functional analysis. In preparation.

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

[7] Kohlenbach, U., New effective moduli of uniqueness and uniform a–priori estimates for constants of strong unicity by logical analysis of known proofs in best approximation theory. Numer. Funct. Anal. and Optimiz. **14**, pp. 581–606 (1993).

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

[9] Kohlenbach, U., Arithmetizing proofs in analysis. In: Larrazabal, J.M., Lascar, D., Mints, G. (eds.), Logic Colloquium '96, Springer Lecture Notes in Logic **12**, pp. 115-158 (1998).

[10] Kohlenbach, U., A quantitative version of a theorem due to Borwein-Reich-Shafrir. Numer. Funct. Anal. and Optimiz. **22**, pp. 641-656 (2001).

[11] Kohlenbach, U., On the computational content of the Krasnoselski and Ishikawa fixed point theorems. In: Proceedings of the Fourth Workshop on Computability and Complexity in Analysis, J. Blanck, V. Brattka, P. Hertling (eds.), Springer LNCS **2064**, pp. 119-145 (2001).

[12] Kohlenbach, U., Uniform asymptotic regularity for Mann iterates. J. Math. Anal. Appl. **279**, pp. 531-544 (2003).

[13] Kohlenbach, U., Some logical metatheorems with applications in functional analysis. Trans. Amer. Math. Soc. vol. 357, no. 1, pp. 89-128 (2005).

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

[15] Kohlenbach, U., Lambov, B., Bounds on iterations of asymptotically quasi-nonexpansive mappings. In: Falset, J.G., Fuster, E.L., Sims, B. (eds.), Proc. International Conference on Fixed Point Theory and Applications, Valencia 2003, pp. 143-172, Yokohama Publishers (2004)

[16] Kohlenbach, U., Leuştean, L., Mann iterates of directionally nonexpansive mappings in hyperbolic spaces. Abstr. Appl. Anal. vol. 2003, no.8, pp. 449-477 (2003).

[17] Kohlenbach, U., Oliva, P., Effective bounds on strong unicity in L_1-approximation. Ann. Pure Appl. Logic **121**, pp. 1-38 (2003).

[18] Kohlenbach, U., Oliva, P., Proof mining: a systematic way of analysing proofs in mathematics. Proc. Steklov Inst. Math. **242**, pp. 1-29 (2003).

[19] Lambov, B., Rates of convergence of recursively defined sequences. In: Brattka, V., Staiger, L., Weihrauch, E., Proc. of the 6th Workshop on Computability and Complexity in Analysis, vol. 120 of Electronic Notes in Theoretical Computer Science, pp. 125-133 (2005).

[20] Luckhardt, H., Herbrand-Analysen zweier Beweise des Satzes von Roth: Polynomiale Anzahlschranken. J. Symbolic Logic **54**, pp. 234-263 (1989).

[21] Odifreddi, P. (ed.), Kreiseliana. About and around Greorg Kreisel. A K Peters, Wellesley, Massachusetts, xiii+495 pp. (1996).

[22] Oliva, P., On the computational complexity of best L_1-Approximation. Math. Logic. Quart. **48, suppl. I**, pp. 66-77 (2002).

A Prametrized Functional Interpretation

Paulo Oliva

We present a parametrised functional interpretation with two parameters. The first parameter captures the degree of freedom in the interpretation of “negation”, while the second expresses the amount of information about witnesses one is interested in. Instantiations of the parametrised interpretation give rise to well-known functional interpretations, among these: Gödel’s original Dialectica interpretation, Kreisel’s modified realisability and Kohlenbach’s monotone interpretations.

Strong Normalization for Applied Lambda Calculi

Ulrich Berger

We prove a general strong normalisation theorem for higher type rewrite systems based on a strictly continuous domain-theoretic semantics. The result can be stated as follows. If the underlying type theory is strongly normalising with respect to β-conversion and all constants have a total value in the model, then every typable term is strongly normalising with respect to β-conversion and rewriting. The theorem applies to extensions of Gödel’s system T and system F by various forms of bar recursion for which strong normalisation was hitherto unknown.

On Σ_2-Theorems of Fragments of PA

Lev Beklemishev

We give some characterisations of Σ_2-consequences of fragments of Peano Arithmetic, PA. Consider the following inference rule, over elementary arithmetic with terms for all Kalmar elementary functions.

$$\frac{\exists m \forall n \geq m \quad t(n+1) \leq t(n)}{\exists m \forall n \geq m \quad t(n) = t(m)}$$

where $t(x)$ is a term with a free variable. We show that this rule axiomatises the set of Σ_2-consequences of the Σ_1-induction schema, $I\Sigma_1$. Non-nested applications of the rule give an alternative axiomatisation of $I\Pi_1^-$, parameter free induction schema.

We also show that

(1) Σ_2-consequences of $I\Sigma_n$ are axiomatisable by $\omega_n = \left.\omega^{\omega^{\cdot^{\cdot^{\cdot^{\omega}}}}}\right\} n$ iterated local Σ_2-reflection schema

(2) Σ_2-consequences of PRA are axiomatisable by ω times iterated local Σ_1-reflection schema. Hence, $I\Sigma_1$ and PRA have different Σ_2-theorems.

Towards a Minimalistic Foundation of Constructive Mathematics

Giovanni Sambin

I claim that

(1) to develop mathematics in such a way that it can be formalised on a computer

(2) to design a common core which can be understood as it is by all mathematicians, whatever foundation they adopt

it is necessary to use an intensional type theory mTT, which is obtained form Martin-Löf's type theory by relaxing the equation Prop = Set. This ground type theory mTT is needed for formalisation, and a "tool box" of extensional concepts built on it is needed to do mathematics. The common core is obtained at this level, by subtraction.

This approach involves two conceptual novelties:

- two different (but connected) levels of abstraction are necessary
- the common core cannot be the complete description of an intended semantics

Cut Elimination in Set Theory

Gills Dowek

We define a notion of cut for all theories that can be expressed by a set of computation rules, included arithmetic, the simple theory of types and set theory. We then present two general theorems allowing to prove that some theory has the cut elimination property:

(1) a theory has the cut elimination property if it has many valued model whose truth values are reducibility candidates

(2) a theory has the cut elimination property if we can translate it in a theory that has an ω-model.

Level-Two Recursion Schemes and Finite Automata

Klaus Aehlig

(joint work with Jolie G. de Miranda and C.-H. Luke Ong)

Since Rabin [4] showed the decidability of the monadic second order (MSO) theory of the binary tree this result has been applied and to various mathematical structures. The interest arose in recent years in the context of verification of infinite state systems [3].

Recently Knapik, Niwiński and Urzyczyn [2] showed that the MSO theory of any infinite tree generated by a level-2 grammar satisfying a certain "safety" condition is decidable. This result can be extended [1] in that the "safety" condition can be dropped.

To do so, one first observes that MSO properties of trees can be represented as the languages of appropriate tree automata. This allows to encode in a set of fixed size the behaviour of a first-order λ-definable function with respect to a fixed given MSO property.

By this observation a tree automaton can (non-deterministically) verify an MSO-property of a tree while walking over a λ-tree defining it. Since the non-emptiness problem for the languages of these automata is decidable the said decidability result follows.

References

[1] Klaus Aehlig, Jolie G. de Miranda, and C.-H. Luke Ong. The monadic second order theory of trees given by arbitrary level-two recursion schemes is decidable. In *Proceedings of the 7th International Conference on Typed Lambda Calculi and Applications (TLCA '05)*, April 2005.

[2] T. Knapik, D. Niwiński, and P. Urzyczyn. Deciding monadic theories of hyperalgebraic trees. In Samson Abramsky, editor, *Proceedings of the 5th International Conference on Typed Lambda Caculi and Applications (TLCA '01)*, volume 2044 of *Lecture Notes in Computer Science*, pages 253–267. Springer Verlag, 2001.

[3] Orna Kupferman and Moshe Y. Vardi. An automata-theoretic approach to reasoning about infinite-state systems. In E Allen Emerson and A Prasad Sistla, editors, *12th International Conference on Computer Aided Verification (CAV '00)*, volume 1855 of *Lecture Notes in Computer Science*, pages 36–52. Springer Verlag, 2000.

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

Making Sense of Bounded Arithmetic: A Complexity Theorist's Point of View

Stephen A. Cook

This talk is based on my survey paper "Theories for Complexity Classes and their Propositional Translations" which has just appeared in the collection edited by Jan Krajíček, published by Quaderni, see also chapters in my forthcoming book with Phuong Nguyen "Introduction to Proof Complexity" on my web page.

Consider the sequence of complexty classes

$$(*) \qquad \mathrm{AC}^0 \subset \mathrm{AC}^0(2) \subset \mathrm{TC}^0 \subset \mathrm{NC}^1 \subset \mathrm{L} \subset P$$

where P is polynomial time. Our motivating question is "Given a combinatorial principle, what is the least complexity class containing enough concepts to prove the principle?" Examples of principles are

(1) The pigeonhole principle, for which the answer seems to be TC^0, and

(2) the matrix principle $AB = U \supset BA = I$, for which the answer is at most P, but we conjecture lower down.

For each complexity class $(*)$ we define a minimal theory for which the Σ_1^1-definable functions are precisely the functions in the class. Each theory has the same underlying language $\mathcal{L}_A^2 = [0, 1, +, \cdot, |\,|, \in, \leq, =]$ in the two-sorted predicate calculus, described by Zamella. Then one way to formalise our motivating question is "What is the least such theory which proves the question."

There are quantified propositional proof systems associated with each complexity class $(*)$, and we explain a general method of translating the Σ_1^B theories of each theory into polynomial size families of proofs in the associated theory.

Forcing with Random Variables

Jan Krajíček

Proof complexity studies the time complexity of non-deterministic algorithms. The main problem is the $\mathcal{NP}$ *versus co*$\mathcal{NP}$ problem, a question whether the computational complexity class $\mathcal{NP}$ is closed under the complementation. Central objects studied are propositional proof systems (non-deterministic algorithms for accepting the set of propositional tautologies). Time lower bounds correspond then to lengths-of-proofs lower bounds.

Bounded arithmetic is a generic name for a collection of first-order theories of arithmetic linked to propositional proof systems (and to a variety of other computational complexity topics). The qualification *bounded* refers to the fact that the induction axiom is typically restricted to a subclass of bounded formulas.

The links between propositional proof systems and bounded arithmetic theories have many facets but informally one can view them as two sides of the same thing: The former is a non-uniform version of the latter. In particular, it is known that proving lengths-of-proofs lower bounds for propositional proof systems is very much related to proving independence results in bounded arithmetic. In fact, proving such lower bounds is *equivalent* to constructing non-elementary extensions of particular models of bounded arithmetic. This offers a very clean and coherent framework for thinking about lengths-of-proofs lower bounds, a one that has been quite successful in the past (let us mention just Ajtai's [1] lower bound for the pigeonhole principle in constant-depth Frege systems).

We describe a new method for constructing (extensions of) bounded arithmetic models, and hence for proving independence results and lengths-of-proofs lower bounds. The models are Boolean valued and are built from families of random variables defined on (possibly on a subset of) $\{0,1\}^n$ with non-standard n, and sampled by functions of some restricted complexity. This is considered inside an $\aleph_1$-saturated non-standard model of true arithmetic. The relevant complete Boolean algebra $\mathcal{B}$ is obtained from $\mathcal{A} := \{A \in M \mid A \subseteq \Omega\}$ by taking a quotient by the ideal I of sets of infinitesimal counting measure (as in the construction of Loeb's measure [5]). The truth value of an atomic sentence of the form $R(\alpha_1, \ldots, \alpha_k)$ (α_i random variables from the family defining the model) is $\{\omega \in \Omega \mid R(\alpha_1(\omega), \ldots, \alpha_k(\omega))\}/I$. This is extended to all sentences using the familiar rules going back to Boole [2] and Rasiowa-Sikorski [6].

References

[1] M. Ajtai, The complexity of the pigeonhole principle, in: *Proc. IEEE 29th Annual Symp. on Foundation of Computer Science*, (1988), pp. 346-355.

[2] G. Boole, *The mathematical analysis of logic*, Barclay and Macmillan, Cambridge, (1847).

[3] J. Krajíček, *Bounded arithmetic, propositional logic, and complexity theory*, Encyclopedia of Mathematics and Its Applications, Vol. **60**, Cambridge University Press, (1995).

[4] J. Krajíček, *Forcing with random variables*, evolving lecture notes available through `http://www.math.cas.cz/~krajicek`.

[5] P. A. Loeb, Conversion from nonstandard to standard measure spaces and applications in probability theory, *Trans. Am. Math. Soc.*, Vol.**211**, (1975), pp.113-122.

[6] H. Rasiowa and R. Sikorski, Algebraic treatment of the notion of satisfiability, *Fundamenta Mathematicae*, **40**, (1953), pp.62-65.

Equivalents of the Weak Multifunction Pigeonhole Principle

Chris Pollett

(joint work with Norman Danner)

I began the talk by presenting a recent result of Jeřábek [1] on the surjective weak pigeonhole principle for p-time functions. Namely, that over the theory S^1_2 this principle is equivalent to the existence of a string which is hard for any circuit of size n^k. This shows that T^2_2, a slightly stronger theory, can prove a predicate exists which is hard for circuits of size n^k. Krajíček and Pudlák [2] have shown if the injective weak pigeonhole principle for p-time functions is witnessable from a class $\mathcal{C}$ satisfying $\mathcal{P}^{\mathcal{C}} = \mathcal{C}$ then RSA is insecure against attacks from $\mathcal{C}$. As the multifunction weak pigeonhole principle implies both the injective and surjective principles, it is natural to wonder if there is any circuit class such that the existence of a hard string for this class is equivalent to the multifunction weak pigeonhole principle for the analogous uniform class. We show that for R^2_2, a theory between T^2_2 and S^1_2 in strength, the multifunction weak pigeonhole principle for quasi-log iterated p-time relations is equivalent to circuit lower bounds for quasi-log iterated p-size circuits. Thus, we show if R^2_2 could prove lower bounds for this class of circuits, one can also show RSA is insecure against quasi-polynomial time attacks.

References

[1] E. Jeřábek. Dual weak pigeonhole principle, Boolean complexity, and derandomization. *Annals of Pure and Applied Logic.* Vol. 129 Issue. 1–3. pp. 1–37. 2004.

[2] J. Krajíček, P. Pudlák. Some consequences of cryptographic conjectures for S^1_2 and EF. *Information and Computation.* Vol. 140. Issue 1. pp. 82–89. 1998.

Topology in Constructive Set Theory (Background and Motivations)

Peter Aczel

Introduction

I started my talk by reviewing the classical Galois adjunction, $\Omega : Top \rightarrow loc$ left adjoint to $Pt : Loc \rightarrow Top$ between the category Top of topological spaces and the category Loc of locales which associates with each space X the locale $\Omega(X)$ of open subsets and with each locale A the space $Pt(A)$ of its formal points. This adjunction is Galois in the sense that it restricts to an equivalence between the subcategories of sober topological spaces and spatial locales, where a topological space is sober if it is isomorphic to $Pt(A)$ for some locale A and a locale is spatial if it is isomorphic to $\Omega(X)$ for some topological space X.

I then stated a theorem that gives a Galois adjunction in the constructive set theory CZF between a category of *standard ct-spaces* and a category of *standard formal topologies*. This result, when viewed in IZF, gives a Galois adjunction that is equivalent to the classical Galois adjunction.

The rest of my talk was taken up with giving the background and motivations for this work.

General Topology in Constructive Mathematics

Traditionally the main constructive interest in topological notions has been in connection with constructive analysis, where attention has been restricted mostly to separable metric spaces. An exception was the PhD thesis of Anne Troelstra, [6], on Intuitionistic General Topology which takes the usual notion of a topology of open sets as its starting point. Also Bishop, in his book, [3] introduced the notion of a neighborhood space, which is essentially just a topological space given by a set of basic open sets. But Bishop did not make significant use of this general notion. Later Grayson, [4], developed further some general constructive topology in the context of the impredicative set theory IZF.

Over the last 30 years or so there has been a growing interest in the *point-free* approach to general topology. In this approach the focus is not on the points of a topological space but on the algebraic structure of the lattice of open sets, which forms a frame/locale. A *frame* is a sup semilattice with finite meets that distribute over sups and a frame map preserves that structure. The category of *locales* is just the opposite of the category of frames and frame maps. It has been argued that in many respects the category of locales has nicer properties than the category of topological spaces and moreover that these properties can be proved more constructively than corresponding properties for the category of topological spaces; e.g. with proofs that avoid AC.

It has been natural to consider the development of point-free topology in topos mathematics; i.e. the brand of mathematics that generally holds in toposes with a natural numbers object. Topos mathematics is based on intuitionistic logic and does not assume any choice principles, but is fully impredicative in that it has a powerset operation.

Giovanni Sambin and Per Martin-Löf initiated the subject of *formal topology*, [5], a treatment of point-free topology within the setting of Martin-Löf's Intuitionistic Type Theory. The aim has been to give a treatment of point-free topology that avoids the impredicativity of topos mathematics. An alternative approach with the same aim is to work in a system of constructive set theory such as CZF. One advantage of working in constructive set theory to working in intuitionistic type theory is that the mathematical developments can be carried out in a more familiar set theoretical language. Another advantage is that CZF makes no explicit choice assumptions while intuitionistic type theory, because it uses the Curry-Howard correspondence to represent logical notions, has a type-theoretic axiom of choice that implies relative dependent choices, an axiom that does not generally hold in toposes.

The aim of my talk was to advocate a balanced approach to constructive general topology in which both the point-set and point-free approaches are developed and compared in a set-theoretical setting compatible with both Bishop style constructive mathematics and topos mathematics. Some steps in this direction have been taken in [1]. There, among other topics I have obtained a version of the classical Galois adjunction theorem. See also [2], which focuses on the topological separation properties.

The Galois adjunction Theorem in CZF

In order to obtain a constructive Galois adjunction theorem it is necessary to overcome a series of problems arising out of the fact that what are sets in an impredicative context can sometimes only be given in CZF as classes that cannot be proved to be sets. Let us call such classes here *large classes.* Often these large classes can be proved to be small, i.e. sets, by assuming additional impredicative axioms such as the powerset axiom.

To start with, there is the problem that the opens of any topological space that has at least one point form a large class, so that the category of topological spaces is superlarge; i.e. its objects are large-sized. It is possible to work with superlarge categories even in CZF. Nevertheless this fact suggests a focus on the category of Bishop's neighborhood spaces, whose objects are small. The next problem is that non-trivial frames/locales are large so that the category of locales is superlarge. This suggests restricting to the category of set-presented locales, these locales being essentially small. This category turns out to be equivalent to the category of set-presented formal topologies. In fact the category of formal topologies is equivalent to the, still superlarge, category of set-generated locales. Now even if we restrict attention to the set-presented locales/formal topologies we have another problem. In general the formal points of a set-presented locale may form a large class. So if we want to have a topological space of such formal points we need to have a notion of topological space which allows the points to form a large class. This leads to the notion of a *constructive topological space*, abbreviated ct-*space*. A ct-space can have a large class of points, but as soon as the powerset axiom is assumed, as in IZF, it becomes small; i.e. the class of points becomes a set. The small ct-spaces are essentially just Bishop's neighborhood spaces. Unfortunately in order to construct a formal topology from a ct-space the ct-space needs to satisfy an additional condition. When this extra condition holds we call the ct-space a *standard* ct-*space* and finally we call a formal topology a standard formal topology if the ct-space of its formal points is standard. All small ct-spaces are standard. There is a weaker notion of *quasi-small* ct-space and such ct-spaces are also all standard. We have now explained much of the motivation behind the notions used in the statement of our constructive Galois adjunction theorem.

Theorem: 1 (CZF).

(1) *There is a Galois adjunction between the superlarge category of standard* ct-*spaces and standard continuous maps and the category of standard formal topologies and standard formal topology maps.*
(2) *The above Galois adjunction restricts to a Galois adjunction between the category of quasi-small* ct-*spaces and the category of set-presentable formal topologies and formal topology maps.*
(3) *The Galois adjunction further restricts to a Galois adjunction between the category of regular small* ct-*spaces and continuous maps and the category of regular set-presentable formal topologies and formal topology maps.*
(4) *Working in IZF, the Galois adjunctions in (1) and (2) are each equivalent to the classical Galois adjunction between topological spaces and locales.*

The notions of *regular* ct-space and regular formal topology are constructive versions of the usual classical separation properties for topological spaces and locales. For more details on this and other aspects of the theorem see [1, 2].

References

[1] P. Aczel. *Aspects of General Topology in Constructive Set Theory*, to appear in the Annals of Pure and Applied Logic, 2005?

[2] P. Aczel and C. Fox. *Separation properties in Constructive Topology*, to appear in 'From Sets and Types to Topology and Analysis'. Towards Practicable Foundations of Constructive Mathematics (L. Crosilla, P. Schuster, eds.), Oxford Logic Guides, Oxford University Press, 2005?.

[3] E. Bishop and D.S. Bridges. Constructive Analysis (Springer, Berlin) 1985

[4] R. Grayson. *Concepts of General Topology in Constructive Mathematics and in Sheaves*, Annals of mathematical Logic, Vol 20, pp. 1-41, 1981.

[5] G. Sambin. *Intuitionistic Formal Spaces - a first communication*, In Skordev, D. (ed.) Mathematical Logic and its Applications, Plenum Press, New York, pp 187-204, 1987.

[6] A. Troelstra *Intuitionistic General Topology*, PhD thesis, University of Amsterdam, 1966.

The Disjunction Property for CZF

Michael Rathjen

While Constructive Zermelo-Fraenkel set theory, CZF, has gained the status of a standard reference theory for developing constructive predicative mathematics, surprisingly little is known about certain pleasing metamathematical properties such as the disjunction and the numerical existence property which are often considered to be the hallmarks of intuitionistic theories.

The talk will present a self-validating semantics for CZF that combines extensional Kleene realisability and truth. This realisability semantics will be put to use in showing that CZF has the disjunction property and the numerical existence property. CZF is also shown to be closed under Church's rule. The same properties remain for CZF plus the Regular Extension Axiom.

Realizability Models for $\mathrm{CZF} + \neg$Pow

Thomas Streicher

Without restricting the metatheory (i.e., working in ZFC with countably many strongly incaccesible cardinals) we construct a realisability model for $\mathrm{CZF}+\neg\mathrm{Pow}$. Let $\mathcal{A}$ be a partial combinatory algebra with $|\mathcal{A}| < \mathcal{I}_\omega$ then $V_U = (WA \in U)A$ with $U = \mathrm{Mod}(\mathcal{A})$ provides a model for CZF where the powerset axiom Pow fails. For $\mathcal{A} = \mathcal{K}_1$ (first Kleene algebra) it holds that in $V_{\mathrm{Mod}(\mathcal{K}_1)}$ all sets are subcountable, i.e., can be enumerated by a subset of ω.

Alas, our models all validate the Separation axiom. If we could find natural models for genuinely predicative type theory with a universe then this would give rise to a model for $\mathrm{CZF} + \neg\mathrm{Pow} + \neg\mathrm{Sep}$.

Cut Elimination in Provability Logic

Sara Negri

Following the method developed in Negri and von Plato (1998) and in Negri (2003), we present a uniform Gentzen-style approach to the proof theory of a large family of normal modal logics. The method covers all the modal logics characterized by geometric conditions on their Kripke models. Each modal system is obtained by adding in a modular way the rules for the accessibility relation to a basic modal system. The resulting (labelled) sequent calculi have all the structural rules–weakening, contraction, and cut–admissible.

A natural challenge is to extend the method to treat also Gödel-Löb provability logic. After Solovay's landmark paper (1976), that characterized axiomatically the modal logic of arithmetical provability G (later called GL), a great effort was directed to producing an adequate sequent calculus and proving cut elimination for it. Semantic completeness proofs for Gentzen's formulations for GL were provided (Sambin and Valentini 1982, Avron 1984) but syntactic proofs of cut elimination (Leivant 1981, Valentini 1983) turned out to be problematic (Moen 2001).

Gödel-Löb provability logic is characterized by irreflexive, transitive, and Noetherian Kripke frames. The non-first-order frame condition of Noetherianity cannot be encoded in the geometric rule scheme, but it becomes part of the characterization of forcing for modal formulas

$$x \Vdash \Box A \textit{ iff for all } y,\ xRy \textit{ and } y \Vdash \Box A \textit{ implies } y \Vdash A$$

This meaning explanation justifies a left and right rule for $\Box$. The resulting sequent calculus derives the Löb axiom, has all the rules invertible, the necessitation, weakening, and contraction rules admissible. Cut elimination is proved by induction on a triple parameter, given by the size of the cut formula, the range of the label of the cut formula (i.e., the set of worlds accessible from it in the derivation) and the sum of the heights of the premisses of cut.

A full proof is presented in Negri (2005).

References

[1] Avron (1984) On modal systems having arithmetical interpretations, *The Journal of Symbolic Logic*, vol. 49, pp. 935–942.

[2] Leivant, D. (1981) On the proof theory of the modal logic for arithmetic provability, *The Journal of Symbolic Logic*, vol. 46, pp. 531–538.

[3] Moen, A. (2001) The proposed algorithms for eliminating cuts in the provability calculus GLS do not terminate, Nordic Workshop on Programming Theory.

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

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

[6] Negri, S. (2005) Proof analysis in modal logic, *Journal of Philosophical Logic*, in press.

[7] Sambin, G. and S. Valentini (1982) The modal logic of provability. The sequential approach, *Journal of Philosophical Logic*, pp. 311–342.

[8] Solovay, R. (1976) Provability interpretations of modal logic, *Israel Journal of Mathematics*, vol. 25, pp. 287–304.

[9] Valentini, S. (1983) The modal logic of provability: cut-elimination, *Journal of Philosophical Logic*, vol. 12, pp. 471–476.

Majorisability Interpretations in Finite-Type Arithmetic

Fernando Ferreira

We introduce and discuss new notions of realisability and functional interpretation in the framework of finite-type arithmetic. These notions are based on assignments of formulas that systematically *disregard* decisions concerning disjunctions and precise witnesses concerning existential statements. Instead, the new assignments of formulas only care for majorants of the existential statements. The notion of majorisability at play is the Howard-Bezem notion.

We state the soundness theorem for both notions. They both interpret a version of choice, a version of independence of premises and the statement saying that every functional is majorisable. From this it follows that both notions interpret a very general bounded collection principle which includes the FAN theorem as a particular case (although only in an *intensional* version in the case of the functional interpretation). It is a fact that the principle lead to classical inconsistencies.

In order to make the majorisability relations computationally empty in the case of the functional interpretation, we must use *intensional* majorisability relations governed (partly) by rules. The new functional interpretation interprets the so-called bounded collection principle (which entails WKL) and the so-called bounded universal disjunction principle (which entails LLPO – lesser limited principle of omniscience).

The new interpretations shed, in my view, the monotone interpretations of Ulrich Kohlenbach, even though they are conceptionally quite different.

Approximate Fixed Point Property in Product Spaces

Laurenţiu Leuştean
(joint work with Ulrich Kohlenbach)

We present another case study in the general program of *proof mining* in functional analysis, or more specifically metric fixed-point theory. Thus, we are concerned with the general theme of what is known about the existence of approximate fixed points for nonexpansive mappings in product spaces.

A metric space (X, ρ) is said to have the *approximate fixed point property (AFPP)* for nonexpansive mappings if any nonexpansive mapping $T : X \to X$ has an approximate fixed point sequence; that is, a sequence $(u_n)_{n\in\mathbb{N}}$ in X for which $\lim_n \rho(u_n, T(u_n)) = 0$.

If (X, ρ) and (Y, d) are metric spaces, we denote by $(X \times Y)_\infty$ the metric space $(X \times Y, d_\infty)$, where the distance d_∞ is defined in the usual way:

$$d_\infty((x, u), (y, v)) = \max\{\rho(x, y), d(u, v)\}$$

for $(x, u), (y, v) \in X \times Y$.

A basic question now becomes:

If (X, ρ), (Y, d) have the AFPP for nonexpansive mappings, then when does $(X \times Y)_\infty$ have the AFPP for nonexpansive mappings?

Espínola and Kirk [2] proved that the product space $H = (K \times M)_\infty$ has the AFPP for nonexpansive mappings whenever M is a metric space which has AFPP for such mappings and K is a bounded convex closed subset of a Banach space. Later, Kirk [5] extended this result to bounded convex closed subsets of spaces of hyperbolic type.

In the first part of the talk, we present generalizations of these results to *unbounded* convex subsets (satisfying certain conditions) of *hyperbolic* spaces. We can extend the results further, to families $(C_u)_{u\in M}$ of unbounded convex subsets of a hyperbolic space (X, ρ, W). All these are carried out in detail together with many further generalizations in a forthcoming paper [9]. The key ingredient in obtaining these generalizations is a quantitative version [8, Theorem 3.9] of a theorem due to Borwein-Reich-Shafrir [1].

The notion of hyperbolic space we use is that one introduced by Kohlenbach [7], inspired by the related notions of convex metric space [13], space of hyperbolic type [4], and hyperbolic space in the sense of Reich-Shafrir [10]. The class of hyperbolic spaces contains all normed linear spaces and convex subsets thereof, but also the open unit ball in complex Hilbert spaces with the hyperbolic metric as well as Hadamard manifolds and CAT(0)-spaces in the sense of Gromov.

In the second part of the talk, we present ongoing work on the logical analysis of the characterization of subsets of hyperbolic spaces having AFPP for nonexpansive mappings obtained by Shafrir [11] using the notion of *directionally bounded* set. Using logical tools as bar-recursion [12], monotone functional interpretations [6], and general logical metatheorems [7, 3], we obtain a uniform version of directionally bounded subsets and we can give a partial answer to an open problem raised by Kirk [5].

References

[1] J. Borwein, S. Reich, I. Shafrir, Krasnoselski-Mann iterations in normed spaces, Canad. Math. Bull **35** (1992), 21–28.

[2] R. Espínola, W. A. Kirk, Fixed points and approximate fixed points in product spaces, Taiwanese J. Math. **5** (2001), 405–416.

[3] P. Gerhardy, U. Kohlenbach, General logical metatheorems for functional analysis, in preparation.

[4] K. Goebel, W.A. Kirk, Iteration processes for nonexpansive mappings, in: Singh, S.P., Thomeier, S., Watson, B., eds., Topological Methods in Nonlinear Functional Analysis. Contemporary Mathematics **21** (1983), AMS, 115–123.

[5] W.A. Kirk, Geodesic geometry and fixed point theory II, in: García Falset, J., Llorens Fuster, E., Sims, B., (eds.), Proceedings of the International Conference on Fixed Point Theory and Applications, Valencia (Spain), July 2003, Yokohama Publishers (2003), 113–142.

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

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

[8] U. Kohlenbach, L. Leuştean, Mann iterates of directionally nonexpansive mappings in hyperbolic spaces, Abstract and Applied Analysis **2003** (2003), 449–477.

[9] U. Kohlenbach, L. Leuştean, The approximate fixed point property in product spaces, in preparation.

[10] S. Reich, I. Shafrir, Nonexpansive iterations in hyperbolic spaces, Nonlinear Analysis, Theory, Methods and Applications **15** (1990), 537–558.

[11] I. Shafrir, The approximate fixed point property in Banach and hyperbolic spaces, Israel J. Math. 71 (1990), 211–223.

[12] C. Spector, Provably recursive functionals of analysis: a consistency proof of analysis by an extension of principles formulated in current intuitionistic mathematics, in: J.C.E. Dekker (ed.), Recursive function theory, Proceedings of Symposia in Pure Mathematics, vol. 5 (1962), AMS, Providence, R.I., 1–27.

[13] W. Takahashi, A convexity in metric space and nonexpansive mappings, I., Kodai Math. Sem. Rep. **22** (1970), 142–149.

A Case Study in Proof Mining: An Effective Version of Kirk's Fixed-point Theorem for Asymptotic Contractions

Philipp Gerhardy

Using techniques of proof mining (as developed for example by Ulrich Kohlenbach) we analyse a very ineffective proof by W. A. Kirk for a fixedpoint theorem for so-called asymptotic contractions. Kirk's original proof uses an ultrapower construction and contains no information about uniformities, nor any effective rate of convergence (of the Picard iteration to the unique fixed point). Mainly by enriching the input to the theorem (by making explicit the computational meaning of the premises and the conclusion of the theorem) we obtain an elementary proof of an almost fully effective version of Kirk's fixed point theorem (where the "almost fully effectiveness" is conjectures to be optimal), including a full rate of convergence, if the convergence in monotone.

Infinite Objects in Constructive Mathematics: Applications of Proof Theory to Algebra

Thierry Coquand

In this two part tutorial I give a survey of recent progress in constructive mathematics, mainly in the filed of algebra and abstract functional analysis.

In the first part I introduce the basic idea, which is to represent an infinite object by a logical theory that describes its observable properties. We can in this way make sense for instance of basic results such as "the intersection of all prime ideals is the set of nilpotent elements" which we cannot do if we represent naïvely a prime ideal as a subset of the ring.

In the second part we apply this basic idea to some noetherian commutative algebra. We give a concrete inductive definition of Krull dimension of a ring. We explain then how to use this definition to simplify and improve breakthrough results of Heitmann (1984) to get a non-noetherian version of Serre's splitting-off theorem and Forster-Swan theorem.

The Effect of Markov's Principle on the Intuitionistic Continuum

Joan Rand Moschovakis

Let **M** be the minimal two-sorted extension of Heyting Arithmetic, with full induction in the extended language, which was used e.g. by Kleene [1] to formalize the theory of recursive partial functions of type 2. In addition to the defining equations for finitely many primitive recursive function constants, **M** has the function existence (or "non-choice") axiom schema

AC$_0$! : $\quad \forall x \exists ! y A(x,y) \rightarrow \exists \alpha \forall x A(x, \alpha(x)),$

but no axiom of countable or dependent choice. Let $\mathbf{T}$ be $\mathbf{M} + \mathrm{BI}_1 + \mathrm{MP}_1$, where BI_1 is Brouwer's principle of bar induction in the form

$$\mathrm{BI}_1: \quad \forall\alpha[\exists x\rho(\overline{\alpha}(x)) = 0 \wedge \forall x(\rho(\overline{\alpha}(x)) = 0 \vee \forall s A(\overline{\alpha}(x) * \langle s\rangle) \rightarrow A(\overline{\alpha}(x)))] \rightarrow A(\langle\,\rangle)$$

and MP_1 is Markov's Principle in the form

$$\mathrm{MP}_1: \qquad \forall\alpha[\neg\forall x\neg\alpha(x) = 0 \rightarrow \exists x\alpha(x) = 0].$$

Then $\mathbf{T}$ proves:

(i) Every predicate $A(x_1, \ldots, x_n, \alpha_1, \ldots, \alpha_m)$ without function quantifiers, indeed every (classically or constructively) Δ^1_1 predicate, is classically decidable with respect to its number variables; that is,

$$\neg\neg\forall x_1 \ldots \forall x_n[A(x_1, \ldots, x_n, \alpha_1, \ldots, \alpha_m) \ \vee \ \neg A(x_1, \ldots, x_n, \alpha_1, \ldots, \alpha_m)].$$

Hence $\neg\neg\exists\beta\forall x_1 \ldots \forall x_n[\beta(\langle x_0, \ldots, x_n\rangle) = 1 \leftrightarrow A(x_1, \ldots, x_n, \alpha_1, \ldots, \alpha_m)]$.

(ii) Every Δ^0_1 predicate has a recursive characteristic function, and the graph of every recursive function is Δ^0_1 (both classically and constructively).

(iii) The constructive arithmetical hierarchy (with or without function parameters) is proper.

Result (i) for arithmetical predicates is due to Robert Solovay (personal communication). A proof of Solovay's result, and proofs of (ii), (iii), and (i) for classically Δ^1_1 predicates, appear in [4] along with other hierarchy results in consistent extensions of intuitionistic analysis. Observe that in $\mathbf{T}$, every constructively Δ^1_1 predicate is also classically Δ^1_1, since MP_1 implies

$$[\exists\alpha\forall x R(\overline{\alpha}(x), z) \leftrightarrow \forall\beta\exists y Q(\overline{\beta}(y), z)] \rightarrow [\neg\neg\exists\alpha\forall x R(\overline{\alpha}(x), z) \leftrightarrow \forall\beta\neg\neg\exists y Q(\overline{\beta}(y), z)]$$

if $R(w, z)$ and $Q(v, z)$ are quantifier-free. Results (ii) and (iii) use Kleene's normal form theorem; as an example, we sketch the proof of (iii).

Theorem. $\mathbf{T}$ proves $\Pi^0_n \neq \Delta^0_{n+1} \neq \Sigma^0_{n+1}$ and $\Sigma^0_n \neq \Delta^0_{n+1} \neq \Pi^0_{n+1}$ for $n \in \omega$, so the constructive arithmetical hierarchy (with or without function parameters) is proper.

Proof. Since $\Pi^0_0 = \Sigma^0_0 \neq \Delta^0_1$ by (ii), and $\Pi^0_n \cup \Sigma^0_n \subseteq \Delta^0_{n+1} = \Sigma^0_{n+1} \cap \Pi^0_{n+1}$, it will suffice to show by induction on n that $\Sigma^0_{n+1} \neq \Delta^0_{n+1}$ and $\Pi^0_{n+1} \neq \Delta^0_{n+1}$.

Basis. $n = 0$. Kleene's normal form theorem, proved in $\mathbf{M}$ (cf. [1]), gives enumerating predicates

$$R_1(x, y, \alpha) \equiv \exists z T(x, y, \overline{\alpha}(z)) \ \text{ and } \ P_1(x, y, \alpha) \equiv \forall z\neg T(x, y, \overline{\alpha}(z))$$

for $\Sigma^0_1(y, \alpha)$ and $\Pi^0_1(y, \alpha)$ respectively, where $T(x, y, w)$ is quantifier-free. $\mathbf{M}$ proves

$$(*)_1 \qquad \forall\alpha\forall x\forall y[\neg\neg R_1(x, y, \alpha) \leftrightarrow \neg P_1(x, y, \alpha)],$$

so $\mathbf{T}$ proves that $R_1(x, x, \alpha)$ is not Π^0_1 and $P_1(x, x, \alpha)$ is not Σ^0_1.

Induction Step. By the induction hypothesis with the normal form theorem, there are predicates

$$R_{n+1}(x, y, \alpha) \equiv \exists z C(x, y, z, \alpha) \ \text{ and } \ P_{n+1}(x, y, \alpha) \equiv \forall z D(x, y, z, \alpha)$$

which enumerate (provably in $\mathbf{M}$) $\Sigma^0_{n+1}(y,\alpha)$ and $\Pi^0_{n+1}(y,\alpha)$ respectively, such that $\mathbf{T}$ proves

$$(*)_n \qquad \forall\alpha\forall x\forall y\forall z[\neg\neg D(x,y,z,\alpha) \leftrightarrow \neg C(x,y,z,\alpha)].$$

Fix α. By (i), $\mathbf{T}$ proves

$$\neg\neg\exists\zeta\exists\eta\forall x\forall y\forall z[(\zeta((x,y,z)) = 0 \leftrightarrow C(x,y,z,\alpha)) \wedge (\eta((x,y,z)) = 0 \leftrightarrow D(x,y,z,\alpha))]$$

so $\neg\neg\forall x\forall y\forall z[D(x,y,z,\alpha) \leftrightarrow \neg C(x,y,z,\alpha)]$ by $(*)_n$, and hence

$$(*)_{n+1} \qquad \forall\alpha\forall x\forall y[\neg\neg R_{n+1}(x,y,\alpha) \leftrightarrow \neg P_{n+1}(x,y,\alpha)].$$

Thus $R_{n+1}(x,x,\alpha)$ is not Π^0_{n+1} and $P_{n+1}(x,x,\alpha)$ is not Σ^0_{n+1}.

By [3], Kleene and Vesley's theory **FIM** of intuitionistic analysis (a nonclassical extension of $\mathbf{M}$ + BI_1 including Brouwer's principle of continuous choice, from which the countable axiom of choice follows) is consistent with $\forall\alpha\neg\neg GR(\alpha)$. Results (i)-(iii) imply that the consistent extension **FIM** + MP_1 of $\mathbf{T}$ proves $\neg\forall\alpha\neg\neg GR(\alpha)$. Both $\mathbf{T}$ and **FIM** + MP_1, like other theories considered in [4], satisfy Kleene's recursive instantiation rule: If $\exists\alpha B(\alpha)$ is a closed theorem of the theory, so is $\exists\alpha[GR(\alpha) \wedge B(\alpha)]$ where $GR(\alpha)$ expresses "α is recursive." Thus Markov's Principle increases the classical (but not the constructive) content of the intuitionistic continuum.

Kleene's example in [2], of a recursive fan in which every recursive branch (but not every branch) is finite, shows that the recursive sequences are an inadequate basis for intuitionistic analysis. Markov's Principle helps to explain this fact without implying the constructive existence of nonrecursive sequences. From this point of view, results (i)-(iii) could be considered reasonably strong evidence for Markov's Principle.

References

[1] Kleene, S. C., *Formalized recursive functionals and formalized realizability*, Memoirs, no. 89, American Mathematical Society, 1969.

[2] Kleene, S. C. and Vesley, R. E., *The Foundations of Intuitionistic Mathematics, Especially in Relation to Recursive Functions*, North-Holland, Amsterdam 1965.

[3] Moschovakis, J. R., *Can there be no non-recursive functions*, Journal of Symbolic Logic, Volume 36 (1971), 309-315.

[4] Moschovakis, J. R., *Classical and constructive hierarchies in extended intuitionistic analysis*, Journal of Symbolic Logic, Volume 68 (2003), 1015-1043.

Classifying Dini's Theorem

Peter Schuster

(joint work with Josef Berger)

Dini's theorem says that compactness of the domain, a metric space, ensures the uniform convergence of every simply convergent monotone sequence of real–valued continuous functions whose limit is continuous. We show that Dini's theorem is equivalent to Brouwer's fan theorem for detachable bars, the classical contrapositive of weak König's lemma.

The programme of reverse mathematics founded by Friedman and Simpson [7] seems to lack a classification of Dini's theorem, which we now undertake within the informal constructive reverse mathematics put forward by Ishihara [5, 6]. In particular, we work over the constructive mathematics initiated by Bishop [1, 2].

We follow Bishop's choice of definitions for compactness and continuity: a metric space is compact precisely when it is totally bounded and complete; a continuous mapping on a compact metric space is a uniformly continuous one; a metric space is locally compact if and only if every bounded subset is contained in a compact one; a continuous mapping on a locally compact metric space is one that is uniformly continuous on every compact subset.

Throughout this note, let X be a locally compact metric space. We consider the conclusion of Dini's theorem as the following property of X.

> **DT$_X$:** *If a monotone sequence (f_n) of continuous functions $f_n : X \to \mathbb{R}$ converges simply to a continuous function $f : X \to \mathbb{R}$, then (f_n) converges uniformly to f.*

So Dini's theorem says that if X is compact, then DT_X holds. One arrives at equivalents of DT_X if one assumes that $f = 0$, or if 'monotone' is replaced by 'decreasing'.

As usual, let $\{0,1\}^{\mathbb{N}}$ denote the set of infinite binary sequences α, β, $\dots$, and let $\{0,1\}^*$ stand for the set of finite binary sequences. The n–th finite initial segment of some α is $\overline{\alpha}n = (\alpha(0), \dots, \alpha(n-1))$, including the case $n = 0$ of the empty sequence. It is well–known that $\{0,1\}^{\mathbb{N}}$ is a compact metric space under the metric $d(\alpha, \beta) = \inf\{2^{-n} : \overline{\alpha}n = \overline{\beta}n\}$. For a more detailed treatment of all this we refer to [4, 8].

A subset B of $\{0,1\}^*$ is detachable if $u \in B$ is a decidable predicate of $u \in \{0,1\}^*$; that B is a bar if for every $\alpha \in \{0,1\}^{\mathbb{N}}$ there is $n \in \mathbb{N}$ with $\overline{\alpha}n \in B$; and that B is a uniform bar if there exists $N \in \mathbb{N}$ such that for every $\alpha \in \{0,1\}^{\mathbb{N}}$ there is $n \leq N$ with $\overline{\alpha}n \in B$.

We can now formulate Brouwer's fan theorem for detachable bars.

> **FT:** *Every detachable bar is uniform.*

The classical contrapositive of FT is weak König's lemma (WKL) in the terminology of [7].

Theorem 1. *The following items are equivalent:* $\mathrm{DT}_{\{0,1\}^{\mathbb{N}}}$*;* DT_X *for all compact metric spaces X;* $\mathrm{DT}_{[0,1]}$*;* FT*.*

In particular, Dini's theorem is a classical equivalent of WKL. We anyway hold WKL for conceptually less appropriate than FT to classify uniformity theorems such as Dini's.

The idea underlying our proof that $\mathrm{DT}_{[0,1]}$ implies FT is taken from the recursive counterexample to Dini's theorem which Bridges ascribes to Richman [3]; further proof ingredients stem from [4]. The complete version of this paper will appear in *Notre Dame J. Formal Logic.*

References

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

[2] Bishop, E., and D. Bridges, *Constructive Analysis.* Springer, Berlin etc., 1985

[3] Bridges, D.S., Dini's theorem: a constructive case study. In: C.S. Calude, M.J. Dinneen, and S. Sburlan, eds., *Combinatorics, Computability and Logic.* 3rd International Conference DMTCS01, Constanţa, Romania, 2001. Proceedings. Springer, London (2001), 69–80

[4] Bridges, D., and F. Richman, *Varieties of Constructive Mathematics.* Cambridge University Press, Cambridge, 1987

[5] Ishihara, H., An omniscience principle, the König lemma and the Hahn–Banach theorem. *Z. Math. Logik Grundlag. Math.* 36 (1990), 237–240

[6] Ishihara, H., Informal constructive reverse mathematics (Japanese). *Sūrikaisekikenkyūsho Kōkyūroku* 1381 (2004), 108–117

[7] Simpson, S.G., *Subsystems of Second Order Arithmetic.* Springer, Berlin etc., 1999

[8] Troelstra, A.S., and D. van Dalen, *Constructivism in Mathematics.* Two volumes. North–Holland, Amsterdam, 1988

An epsilon Substitution Method with Finite Sets

Gigori Mints
(joint work with Henry Towsner)

Consider an extension of the ordinary epsilon language by finite two-sided sets $S = \{n_1, ..., n_k; m_1, ..., m_\ell\}$, where n_i belong to S, m_j do not belong to S. Extend the definition of a computation with an epsilon substitution so that it is stable with respect to such terms. It is possible to prove termination of the corresponding epsilon substitution process for the theory of jump hierarchies. A definition suitable for ID_1 is still to be found.

Skolemization in Intuitionistic Logic

Rosalie Iemhoff

Classical Skolemization, the method that for a given formula produces a formula without strong quantifiers that is equi-derivable with the original one, does not hold for intuitionistic logic. We show that in the presence of an existence predicate one can define an alternative form of Skolemization for intuitionistic logic that has many of the nice properties that classical Skolemization has. The method covers strong existential quantifiers, and hence leads to a Herbrand theorem for intuitionistic logic for formulas in which all strong quantifiers are existential. Whether there is a reasonable Skolemization method that covers all formulas we do not know.

Categories of Interpretation

Albert Visser

We introduce categories of interpretations. These categories have various uses. They are a tool for conceptual analysis; they serve to define various notions of equality of theories; they allow us to make distinctions between kinds of interpretations.

We show how these categories can be used as a framework to study Tarski's Theorem on the Undefinability of Truth. We employ this framework for an easy proof that ZF is not bi-interpretable with extensions of Arithmetic (in the arithmetical language).

Implicit Characterizations

Isabel Oitavem

In this talk, we give an implicit characterization of the class of functions computable in polynomial space by deterministic Turing machines — *Pspace*. This is a characterization in the vein of the Bellantoni-Cook characterization of the polytime functions, *Ptime*, given in [2]. The main difference between these two characterizations is the formulation of the recursion scheme. To reach *Pspace* one introduces pointers (also called path information) in the recursion scheme. Complexity classes which can be described in terms of parallel computations are often characterized implicitly using recursion schemes with parameter substitution. This is the case of alternating logtime, alternating poly-logtime, *NC* and, in a three-sorted context, *Pspace* — see [1], [4] and [5]. Our work strengthens the idea that recursion with (full) parameter substitution is not necessarily needed to characterize parallel classes of complexity.

We work in an algebraic context. Therefore, we start discussing recursion schemes over free algebras. For each free algebra $\mathbb{A}$, we define a term system $\mathbf{T}_{\mathbb{A}} = \mathrm{COMP}/\mathrm{REC}_{\mathbb{A}}\{\mathbb{A}\text{-constructors}, \mathbb{A}\text{-destructors}, \mathbb{A}\text{-conditional}, \text{projections}\}$. This means that $\mathbf{T}_{\mathbb{A}}$ is the closure of a set of initial function terms under composition and "the" recursion induced by the constructors of the algebra $\mathbb{A}$. Notice that if $f(x)$ is defined by word-recursion on x — let us say $f(c_i) = g(c_i)$ if c_i is a nullary constructor and $f(c_ix) = h(c_ix, f(x))$ if c_i is a unary constructor — then all subwords of x which appear along the recursion process are uniquely identified by their lengths. In a tree algebra context we will have a tree-recursion. A subtree w of the recursion input x, encountered during such a recursion, could be located anywhere in x. The value of w itself does not uniquely identify which subtree is under consideration. To uniquely identify the subtree being considered at the current stage of the recursion, one also requires some "path information".

Here the starting free algebra is the tree algebra generated by $\epsilon, \star_0$ and $\star_1$ of arity 0, 2 and 2 respectively. When we restrict ourselves to balanced symmetric terms, we obtain a part of the algebra above which we denote by $\mathbb{TW}$. $\pi(\epsilon) = \epsilon$ and $\pi(x \star_i x) = S_i(\pi(x))$, for $i \in \{0, 1\}$, defines a bijection between $\mathbb{TW}$ and $\mathbb{W}$

— where $\mathbb{W}$ is the word algebra generated by ϵ, S_0 and S_1 of arity 0, 1 and 1 respectively. Thus, informally, $\mathbb{TW}$ can be seen as the algebra $\mathbb{W}$ together with a tree structure.

We define a term system, $\mathbf{T}_{\mathbb{TW}}$, as described above. Since $\mathbb{TW}$ is a part of a tree algebra, one includes pointers in the recursion scheme $\mathrm{REC}_{\mathbb{TW}}$. At this point we switch to a sorted context. Following notation introduced by Bellantoni and Cook in [2], we define the input-sorted version of the term system $\mathbf{T}_{\mathbb{TW}}$ and we denote it by $\mathbf{ST}_{\mathbb{TW}}$. We prove that $\mathbf{ST}_{\mathbb{TW}}$ characterizes the *Pspace* functions. To establish the upper bound one proves a bounding lemma similar to the one proved for *Ptime* in [2]. The difference is that here the proof must take into account the presence of the pointers in the recursion scheme. In this talk we focus on the lower bound. One knows, [3], that a function f (over $\mathbb{W}$) is in *Pspace* if, and only if, f is bitwise computable by an alternating Turing machine (ATM) in polynomial time, and $|f(w)|$ is polynomial in $|w|$. We simulate ATMs working in polynomial time by $\mathbf{ST}_{\mathbb{TW}}$ terms.

References

[1] S. Bellantoni. Characterizing parallel time by type 2 recursions with polynomial output length. In D. Leivant, editor, *Logic and Computational Complexity*, volume 960 of *LNCS*, pages 253–268. Springer-Verlag, 1995.

[2] S. Bellantoni and S. Cook. A new recursion-theoretic characterization of polytime functions. *Computational Complexity*, 2:97–110, 1992.

[3] A. K. Chandra, D. C. Kozen, and L. J. Stockmeyer. Alternation. *J.ACM*, 28:114–133, 1981.

[4] D. Leivant. A characterization of NC by tree recurrence. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science, FOCS 1998*, pages 716–724. IEEE Computer Society, 1998.

[5] D. Leivant and J. Marion. Ramified recurrence and computational complexity II: Substitution and poly-space. In *8th Proceedings of CSL*, volume 993 of *LNCS*, pages 486–500, 1994.

Bounded Arithmetic, Definable Functions and Dynamic Ordinals

Arnold Beckmann

Gentzen's consistency proof for Peano Arithmetic (PA) can be used to compute the proof theoretic ordinal of PA, i.e., the amount of transfinite induction needed to prove the consistency of PA. As we know since Gentzen, the proof theoretic ordinal of PA is ε_0. Proof theoretic ordinals usually also characterise in a suitable way the provable recursive functions and the order types of the provable well-founded wellorderings of the underlying theory.

Bounded arithmetic is a restriction of PA introduced by Samuel Buss in 1986 which is related to the polynomial time hierarchy. Questions about complexity classes like the "P versus NP" problem find their correspondence in the framework of bounded arithmetic. A suitable adaption of proof theoretic ordinals to the setting of bounded arithmetic is given by dynamic ordinals. In this talk I described what is known about the relationship between bounded arithmetic theories, definable functions, propositional proofs and dynamic ordinals. Especially, I explained why dynamic ordinals intrinsically characterise definable functions.

Domain-Theoretic Construction of Inverse Functions

Dirk Pattinson

We give an effective construction of a local inverse of a $\mathcal{C}^1$-function $f\colon O \subset \mathbb{R}^n \to \mathbb{R}^n$ with $\det f'(x_0) \neq 0$. By exhibiting a domain (in the sense of Dana Scott) by effective manipulations of $\mathcal{C}^1$-functions, the proof hinges on Kleene's fixedpoint theorem and in particular allows for arbitrary accurate computation of the derivative of the inverse.

On the Proof Theory of Type Two Functionals

Thomas Strahm

In this talk, I discuss various aspects relating to the proof theory of type two functionals in the framework of Feferman-style applicative theories; the latter form the operational core of explicit mathematics ([1]). The systems we consider range in strength from rather strong subsystems of analysis to theories of feasible strength.

I will start reviewing work of Feferman, Jäger, and Strahm on the proof-theoretic analysis of the non-constructive μ-operator ([2, 3, 4]), and Jäger and Strahm on the proof theory of the Suslin operator ([5]). The upshot is that systems based on the μ-operator and Suslin operator can be measured in proof-theoretic terms by subsystems of second order arithmetic based on Δ^1_1 and Δ^1_2 comprehension, respectively.

In more recent joint work with Steiner ([7, 8]), the above two functionals have been analyzed in the context of Schlüter's combinatory algebra for the primitive recursive functions ([6]). This weakening of the applicative basis results in a drastic decrease in proof-theoretic strength. More precisely, the two considered functionals have the respective strength of arithmetical and Π^1_1 comprehension.

In the last part of the talk, I will discuss the question of provability of type two functionals in weak applicative frameworks, thereby addressing the topic of type two feasibility ([9, 10]). In particular, a natural proof-theoretic characterization of the Melhorn-Cook-Urquhart basic feasible functionals will be discussed.

References

[1] Feferman, S. A language and axioms for explicit mathematics. In *Algebra and Logic*, J. Crossley, Ed., vol. 450 of *Lecture Notes in Mathematics*. Springer, Berlin, 1975, pp. 87–139.

[2] Feferman, S., and Jäger, G. Systems of explicit mathematics with non-constructive μ-operator. Part I. *Annals of Pure and Applied Logic 65*, 3 (1993), 243–263.

[3] Jäger, G., and Strahm, T. Totality in applicative theories. *Annals of Pure and Applied Logic 74*, 2 (1995), 105–120.

[4] Jäger, G., and Strahm, T. Some theories with positive induction of ordinal strength $\varphi\omega 0$. *Journal of Symbolic Logic 61*, 3 (1996), 818–842.

[5] Jäger, G., and Strahm, T. The proof-theoretic strength of the Suslin operator in applicative theories. In *Reflections on the Foundations of Mathematics: Essays in Honor of Solomon Feferman*, W. Sieg, R. Sommer, and C. Talcott, Eds., vol. 15 of *Lecture Notes in Logic*. Association for Symbolic Logic, 2002, pp. 270–292.

[6] SCHLÜTER, A. A theory of rules for enumerated classes of functions. *Archive for Mathematical Logic 34* (1995), 47–63.

[7] STEINER, D. Proof-theoretic strength of PRON with various extensions. Master's thesis, Institut für Informatik und angewandte Mathematik, Universität Bern, 2001.

[8] STEINER, D., AND STRAHM, T. On the proof theory of type two functionals based on primitive recursive operations. In preparation.

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

[10] STRAHM, T. A proof-theoretic characterization of the basic feasible functionals. *Theoretical Computer Science 329* (2004), 159–176.

Partiality via Coinductive Types

TARMO UUSTALU

(joint work with Thorsten Altenkirch, Venanzio Capretta)

I discuss a type-theoretically motivated approach to partiality due to non-termination. The approach is based on coinductive types and quotients and treats partiality as a monadic effect in the sense of E. Moggi. Looping is directly supported by the appropriate monad, fixpoints are supported in a more indirect fashion. I also discuss a systematic way of combining the monad with monads of other effects.

Monadic Stabilization for Operationalized Second-Order Classical Logic with Disjunction and Permutative Conversions

RALPH MATTHES

Parigot's second-order $\lambda\mu$-calculus [7] is an operationalization of second-order classical logic – based on *reductio ad absurdum*, i. e., indirect proofs. An important feature of this system is the avoidance of falsity $\bot$ in the formulation of the fact that every formula A is stable, i. e., that $\forall X.\, \neg\neg X \to X$ should be provable, with $\neg A$ shorthand for $A \to \bot$. This is achieved by the use of μ-variables $a, b, \dots$ which are considered to assume the negation of their type. If a of type A is applied to the term t of type A, this yields the "named term" $a\,t$ that morally has type $\bot$, but is only marked as being such a term. Indirect proof is represented by μ-abstraction: $\mu a.r$ with r a named term receives the type A of a. A may be a compound type, hence further elimination rules may be applied. And the operational rules (called μ-reductions) describe that the indirect proof may be used at the resulting type instead of A. For this, Parigot uses a special kind of substitution that replaces subterms of the form $a\,t$ for any t by some term – typically of the form $b\,(t\,s)$ for some term s.

A formulation of operationalized classical logic that makes full use of $\bot$ and only needs usual substitution has been given by Rehof and Sørensen [8]. Even this more liberal formulation and even its second-order version has been embedded by Joly [2] into the intuitionistic subsystem (System F) where one reduction step of the source system is translated into at least one step of the target system – thus inheriting strong normalization from that of the target system. However, this embedding certainly fails to extend to the corresponding systems that also include disjunction with their appropriate permutative/commuting conversions (without those additional conversions, disjunction would just be second-order definable). And the μ-reduction for disjunction oversteps our intuition that stability for compound formulas is reduced to stability for subformulas. In the case of disjunction elimination, we use the principle of indirect proof for the uncontrolled target type of that elimination in the μ-reduct.

For the systems without disjunction, the author has previously [3, 5] given a new embedding of $\lambda\mu$-calculus into its intuitionistic subsystem that is not based on a double negation but on stabilization $\sharp$ that can impredicatively be defined by

$$\sharp A := \forall X.\, (A \to X) \to (\neg\neg X \to X) \to X,$$

which can also be conceived as the least fixed point of the non-strictly positive operation $X \mapsto A + \neg\neg X$. For this embedding to simulate reduction steps, Parigot's refinement turned out to be crucial.

Unlike that iterative stabilization, *monadic stabilization* is now introduced. The classical part of the system is encapsulated in a monad, again called $\sharp$. In the Curry-style typing system, this comes with the following three new constructs:

$$\frac{\Gamma \vdash t : A}{\Gamma \vdash \mathsf{emb}\, t : \sharp A} \qquad \frac{\Gamma \vdash t : \neg\neg\sharp A}{\Gamma \vdash \mathsf{stab}\, t : \sharp A} \qquad \frac{\Gamma \vdash r : \sharp A \qquad \Gamma, x : A \vdash s : \sharp C}{\Gamma \vdash \mathsf{bind}(r,\, x.\, s) : \sharp C},$$

out of which only the second one is not standard. The known monad rules are $\mathsf{bind}(\mathsf{emb}\, t,\, x.\, s) \longrightarrow s[x := t]$ and the usual permutative/commuting conversion $\mathsf{bind}(\mathsf{bind}(r,\, x.\, s),\, y.\, t) \longrightarrow \mathsf{bind}(r,\, x.\, \mathsf{bind}(s,\, y.\, t))$, which will be needed in order to simulate the permutative conversion of disjunction in the embedding to come. The essentially new rule is the stability rule for this stable monad:

$$\mathsf{bind}(\mathsf{stab}\, t,\, x.\, s) \longrightarrow \mathsf{stab}\Big(\lambda y.\, t(\lambda z.\, y\, \mathsf{bind}(z,\, x.\, s))\Big).$$

An important feature of this new system, called $\mathsf{M}\sharp$, is its adherence to the introduction/elimination dichotomy of natural deduction – unlike the rule of indirect proof (as shown above for $\lambda\mu$-calculus) that may introduce formulas with arbitrary root symbol. This allows a modular termination proof of $\mathsf{M}\sharp$ that is better structured and conceptually easier than for classical natural deduction (see for comparison [4]). The embedding $-'$ into $\mathsf{M}\sharp$ is defined like Kolmogorov's translation on formulas, but with $\sharp$ in place of double negation. The compositional term translation is then determined. It is important that a μ-variable a of type A is translated into a variable of type $\neg A'$ and that there is no negation that has to be translated.

It has to be stressed that this translation does not erase reduction steps (as those based on double negation unfortunately do, see the report in [6]) and that it can accomodate positive fixed points (in source and target system). In order to treat the second-order quantifier properly, the systems have to be put into typing à la Church (also a necessity sometimes overlooked) which causes several technical burdens. Finally, one should remark that $\sharp A := 1 + A$ would certainly give an implementation of a monad (as observed in [1]), but that its stability is the problem we encapsulate in our abstract stable monad.

References

[1] Nick Benton, Gavin Bierman, and Valeria de Paiva. Computational types from a logical perspective. *Journal of Functional Programming*, 8(2):177–193, 1998.

[2] Thierry Joly. An embedding of 2nd order classical logic into functional arithmetic FA2. *C. R. Acad. Sci. Paris, Série I*, 325:1–4, 1997.

[3] Ralph Matthes. Parigot's second order $\lambda\mu$-calculus and inductive types. In Samson Abramsky, editor, *Proceedings of TLCA 2001*, vol. 2044 of *LNCS*, pp. 329–343. Springer, 2001.

[4] Ralph Matthes. Non-strictly positive fixed-points for classical natural deduction. *Annals of Pure and Applied Logic*, 133:205–230, 2005.

[5] Ralph Matthes. Stabilization—an alternative to double-negation translation for classical natural deduction. In Viggo Stoltenberg-Hansen and Jouko Väänänen, editors, *Proceedings of the Logic Colloquium 2003*, 2005. To appear.

[6] Koji Nakazawa and Makoto Tatsuta. Strong normalization proof with CPS-translation for second order classical natural deduction. *The Journal of Symbolic Logic*, 68(3):851–859, 2003. Corrigendum: vol. 68 (2003), no. 4, pp. 1415–1416.

[7] Michel Parigot. $\lambda\mu$-calculus: an algorithmic interpretation of classical natural deduction. In Andrei Voronkov, editor, LPAR '92, vol. 624 of *LNCS*, pp. 190–201. Springer, 1992.

[8] Jakob Rehof and Morten H. Sørensen. The λ_Δ-calculus. In Masami Hagiya and John C. Mitchell, editors,TACS '94, vol. 789 of *LNCS*, pp. 516–542. Springer, 1994.

Phase Transitions in Logic and Ramsey Theory

Andreas Weiermann

We present recent results on classifying natural independent statements for first order Peano arithmetic (and related systems) and we will survey surprising connections between this area of logic and other fields in mathematics, like analytic combinatorics and Ramsey theory.

To this end we consider combinatorial assertions, like Friedman, Paris Harrington or Kanamori McAloon style principles, and parameterize these with respect to a number-theoretic function. If this parameter function is bounded by a function of slow growth then the resulting assertion remains provable in the system under consideration but when the parameter function exceeds in growth a critical threshold then the resulting assertion, although still true, becomes unprovable.

The fine structure analysis of phase transitions yields applications to some classical open problems in mathematics. In particalur we will discuss how the asymptotic of the standard Ramsey function for triples and two or three colors (a classical Erdoes problem) is affected by the possible independence of a certain Paris Harrington principle.

Towards a More Algebraic Treatment of Ordinal Notation Systems

Anton Setzer

We reconsider some simple ordinal notation systems of predicative strength. Then we look at the abstract structure behind it and develop form this the notion of an ordinal system, an underlying structure common to most ordinal notation systems, the author has studied. Then we show that ID_1 shows that all PA-provable ordinal systems are well-ordered, adhere PA-provable means that the property of being an ordinal system can be shown in Peano Arithmetic. The well-ordering proof is relatively short since one doesn't have to deal with the exact details of the ordinal notation system but can concentrate on its abstract properties. Formally we introduce some simple constructions for forming well-orderings using 0, 1, $\mathbb{N}$, $+$, $\cdot$ and exponentiation. Using this one can develop easily an ordinal notation system up to ε_0 and show that PA proves transfinite induction over it, written as $\mathrm{OS}(\lambda\mathbb{X}.\mathbb{A}[\mathbb{X}])$. Then we show how to develop ordinal systems $\mathrm{OS}(\lambda\mathbb{X}.\mathbb{N}^{\mathbb{X}} + \mathbb{X}^{\cdot^{\cdot^{\cdot^{\mathbb{X}}}}})$, and that the limit of these ordinals reaches the Bachmann-Howard Ordinal $|\mathrm{ID}_1|$. This shows that the supremum of the ordertypes of PA-provable ordinal systems and as well of PRA provable ordinal systems is the Bachmann-Howard ordinal. Extensions have been developed up to $|\mathrm{KPM}|$ and are in development up to $|\mathrm{KP} + \Pi_3 - \mathrm{Refl}|$.

Monotone Inductive Definitions and the Consistency of New Foundations

Sergei Tupailo

New Foundations, **NF**, is a system of set theory named after Quine's 1937 article "New foundations for mathematical logic", where it was introduced. It was meant as a foundations of mathematics, alternative to Zermelo-Fraenkel set theory **ZF** and others. Obvious advantages of **NF** are that it's very easily formulated and many mathematical notions can be expressed in **NF** in a much more "natural" way than in **ZF**. However, in spite of efforts by many researches and many brilliant results, **NF** is still not known to be consistent relative to any theory in which we have reasonable confidence.

We investigate a possibility of reducing the Consis(**NF**) problem to consistency of various extensions of Jensen's **NFU**, "**NF** with Urelements", which is known to be consistent due to Jensen 1969. Extensions of **NFU** by different "large cardinal axioms" and their consistency strength have been studied by R. Jensen, S. Feferman, M. Boffa, R. Holmes, R. Solovay. Specifically, we describe a surprising connection between the Monotone Inductive Definitions principle and consistency of New Foundations.

Reporter: Klaus Aehlig

Participants

Prof. Dr. Peter Aczel
petera@cs.man.ac.uk
Dept. of Computer Science
University of Manchester
Oxford Road
GB-Manchester M13 9PL

Dr. Klaus Aehlig
aehlig@math.lmu.de
Mathematisches Institut
Universität München
Theresienstr. 39
80333 München

Dr. Arnold Beckmann
a.beckmann@swansea.ac.uk
Dept. of Computer Science
University of Wales Swansea
Singleton Park
GB-Swansea SA2 8PP

Dr. Lev D. Beklemishev
lev@phil.uu.nl
Faculty of Philosophy
Utrecht University
Heidelberglaan 8
NL-3584 CS Utrecht

Dr. Ulrich Berger
u.berger@swansea.ac.uk
Dept. of Computer Science
University of Wales Swansea
Singleton Park
GB-Swansea SA2 8PP

Prof. Dr. Wilfried Buchholz
buchholz@mathematik.uni-muenchen.de
Mathematisches Institut
Universität München
Theresienstr. 39
80333 München

Prof. Dr. Samuel R. Buss
sbuss@math.ucsd.edu
Dept. of Mathematics
University of California, San Diego
9500 Gilman Drive
La Jolla, CA 92093-0112
USA

Prof. Dr. Andrea Cantini
cantini@unifi.it
Dipt. di Filosofia
Universita degli Studi di Firenze
Via Bolognese 52
I-50139 Firenze

Prof. Dr. Stephen A. Cook
sacook@cs.toronto.edu
Dept. of Computer Science
University of Toronto
10 King's College Road
Toronto Ontario M5S 3G4
CANADA

Dr. Thierry Coquand
coquand@cs.chalmers.se
Department of Computer Science
Chalmers University of Technology
and University of Göteborg
S-41296 Göteborg

Prof. Dr. Gilles Dowek
Gilles.Dowek@polytechnique.fr
Laboratoire d'Informatique (Lix)
Ecole Polytechnique
F-91128 Palaiseau Cedex

Prof. Dr. Fernando Ferreira
ferferr@cii.fc.ul.pt
Departamento de Matematica
FCUL - Universidade de Lisboa
Campo Grande, ED.C6, Piso 2
P-1749016 Lisboa

Philipp Gerhardy
gerhardy@mathematik.tu-darmstadt.de
Fachbereich Mathematik
TU Darmstadt
Schloßgartenstr. 7
64289 Darmstadt

Dr. J.Martin E. Hyland
M.Hyland@dpmms.cam.ac.uk
Dept. of Pure Mathematics and
Mathematical Statistics
University of Cambridge
Wilberforce Road
GB-Cambridge CB3 OWB

Dr. Rosalie Iemhoff
iemhoff@logic.at
Institut für Diskrete Mathematik
und Geometrie
Technische Universität Wien
Wiedener Hauptstr. 8 - 10
A-1040 Wien

Prof. Dr. Gerhard Jäger
jaeger@iam.unibe.ch
Institut für Informatik
und angewandte Mathematik
Neubrückstr. 10
CH-3012 Bern

Dr. Jan Johannsen
jan.johannsen@ifi.lmu.de
Institut für Informatik
Ludwig-Maximilians-Universität
München (LMU)
Oettingenstr. 67
80538 München

Prof. Dr. Ulrich Kohlenbach
kohlenbach@mathematik.tu-darmstadt.de
Fachbereich Mathematik
TU Darmstadt
Schloßgartenstr. 7
64289 Darmstadt

Prof. Dr. Jan Krajicek
krajicek@math.cas.cz
Mathematical Institute
AV CR
Zitna 25
115 67 Praha 1
Czech Republic

Dr. Laurentiu Leustean
leustean@mathematik.tu-darmstadt.de
Fachbereich Mathematik
TU Darmstadt
Schloßgartenstr. 7
64289 Darmstadt

Tobias Loew
loew@mathematik.tu-darmstadt.de
Fachbereich Mathematik
TU Darmstadt
Schloßgartenstr. 7
64289 Darmstadt

Prof. Dr. Per Martin-Loef
pml@math.su.se
Dept. of Mathematics
University of Stockholm
S-10691 Stockholm

Dr. Ralph Matthes
matthes@tcs.informatik.uni-muenchen.de
Institut für Informatik
Ludwig-Maximilians-Universität
München (LMU)
Oettingenstr. 67
80538 München

Prof. Dr. Grigori Mints
mints@csli.stanford.edu
Department of Philosophy
Building 90
Stanford University
Stanford CA 94305-2155
USA

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

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

Dr. Sara Negri
sara.negri@helsinki.fi
Department of Philosophy
University of Helsinki
P.O. Box 9
FIN-00014 Helsinki

Dr. Isabel Oitavem
isarocha@ptmat.fc.ul.pt
CMAF & University of Lisbon
Centro de Matematica e Aplicacoes
Fundamentais
Av. Prof. Gama Pinto, 2
P-Lisboa 1649-003

Prof. Dr. Paulo Oliva
pbo@dcs.qmul.ac.uk
Department of Computer Science
Queen Mary, University of London
Mile End Road
GB-London E1 4NS

Prof. Dr. Erik Palmgren
palmgren@math.uu.se
Matematiska institutionen
Uppsala Universitet
Box 480
S-751 06 Uppsala

Dr. Dirk Pattinson
Institut für Informatik
Ludwig-Maximilians-Universität
München (LMU)
Oettingenstr. 67
80538 München

Prof. Dr. Wolfram Pohlers
pohlers@math.uni-muenster.de
Institut für Mathematische
Logik und Grundlagenforschung
Universität Münster
Einsteinstr. 62
48149 Münster

Dr. Chris Pollett
cpollett@yahoo.com
Pollett@cs.sjsu.edu
Dept. of Computer Science
San Jose State University
214 MacQuarrie Hall
San Jose CA 95192-0103
USA

Dr. Pavel Pudlak
pudlak@math.cas.cz
Institute of Mathematics of the
AV CR
Zitna 25
115 67 Praha 1
CZECH REPUBLIC

Prof. Dr. Michael Rathjen
rathjen@amsta.leeds.ac.uk
rathjen@math.ohio-state.edu
Department of Mathematics
The Ohio State University
100 Mathematics Building
231 West 18th Avenue
Columbus, OH 43210-1174
USA

Christian Reiher
ChristianReiher@gmx.de
Aidenbachstrasse 103A
81379 München

Prof. Dr. Giovanni Sambin
sambin@math.unipd.it
Dipartimento di Matematica Pura
ed Applicata
Universita di Padova
Via Belzoni, 7
I-35131 Padova

Stefan Schimanski
schimans@mathematik.uni-muenchen.de
Mathematisches Institut
Universität München
Theresienstr. 39
80333 München

PD Dr. Peter Schuster
Peter.Schuster@mathematik.uni-muenchen.de
Mathematisches Institut
Universität München
Theresienstr. 39
80333 München

Prof. Dr. Helmut Schwichtenberg
schwicht@mathematik.uni-muenchen.de
Mathematisches Institut
Universität München
Theresienstr. 39
80333 München

Dr. Anton Setzer
a.g.setzer@swan.ac.uk
Dept. of Computer Science
University of Wales Swansea
Singleton Park
GB-Swansea SA2 8PP

Dr. Michael Soltys
soltys@mcmaster.ca
Department of Computing and
Software
McMaster University
1280 Main St. West
Hamilton ONT L8S 4K1
Canada

Dr. Thomas Strahm
strahm@iam.unibe.ch
Institut für Informatik und
Angewandte Mathematik
Universität Bern
Neubrückstr. 10
CH-3012 Bern

Prof. Dr. Thomas Streicher
streicher@mathematik.tu-darmstadt.de
Fachbereich Mathematik
Arbeitsgruppe 1
Schlossgartenstr. 7
64289 Darmstadt

Dr. Sergei Tupailo
sergei@cs.ioc.ee
stupailo@hot.ee
tupailo1@osu.edu
Department of Mathematics
The Ohio State University
231 W 18th Avenue
Columbus, OH 43210
USA

Dr. Christian Urban
cu200@cam.ac.uk
urban@mathematik.uni-muenchen.de
Mathematisches Institut
Universität München
Theresienstr. 39
80333 München

Dr. Tarmo Uustalu
tarmo@cs.ioc.ee
Institute of Cybernetics
Akadeemia tee 21
EE-12618 Tallinn
ESTONIA

Prof. Dr. Albert Visser
Albert.Visser@phil.uu.nl
Filosofische Faculteit
Postbus 80103
NL-3508 TC Utrecht

Prof. Dr. Stanley S. Wainer
s.s.wainer@leeds.ac.uk
pmt6ssw@maths.leeds.ac.uk
School of Mathematics
University of Leeds
GB-Leeds, LS2 9JT

Dr. Andreas Weiermann
weierma@math.uni-muenster.de
Institut für Mathematische
Logik und Grundlagenforschung
Universität Münster
Einsteinstr. 62
48149 Münster