Mathematisches Forschungsinstitut Oberwolfach

Report No. 18/2008

Mathematical Logic: Proof Theory, Constructive Mathematics

Organised by
Samuel R. Buss, San Diego
Ulrich Kohlenbach, Darmstadt
Helmut Schwichtenberg, München

April 6th – April 12th, 2008

Abstract. The workshop "Mathematical Logic: Proof Theory, Constructive Mathematics" brought together a carefully selected group of mathematicians, computer scientists and logicians in other fields to discus the impact of proof-theoretic and constructive methods in their various areas. A key topic in the meeting was the unwinding of proofs to obtain computational information. This hidden computational information has already lead to new mathematical insights. Computational information is more directly present in constructive approaches to mathematics, a fact that makes it worthwhile to carefully investigate these approaches and also study their proof-theoretic properties. The precise quantitative information proof theory yields about proofs and proof transformations can directly be applied to computational complexity.

Mathematics Subject Classification (2000): 03Fxx.

Introduction by the Organisers

The workshop *Mathematical Logic: Proof Theory, Constructive Mathematics* was held April 6-12, 2008 and had the following main aims:

To promote the interaction of proof theory with core areas of mathematics. This, in particular, refers to uses of proof theoretic techniques (most notably various forms of functional and realizability interpretations) to unwind prima facie ineffective proofs in mathematics. For instance a number of talks presented such applications in the areas of fixed point theory, ergodic theory, topological dynamics and symbolic dynamics resulting in new theorems, surprising to the experts in the respective fields (Avigad, Briseid, Gerhardy, Leuştean, Simpson). Another talk addressed uses of analytic number theory in connection with new unprovability results and phase transitions in provability (Bovykin).

To further develop new directions in both the foundations as well as applied forms of constructive mathematics. There were a number of talks focusing on new formal frameworks for constructive mathematics and their proof theoretic properties (Aczel, Iemhoff, J. Moschovakis, Palmgren, Streicher), but also new constructive (and partly computer generated) developments in specific areas such as algebra, analysis, combinatorics and quantum theory (Bauer, Delzell, Lombardi, Paule, Spitters).

To explore further the connections between proof theory and computational complexity (e.g. in connection with the study of systems of so-called bounded arithmetic, Beckmann, Pollett, Thapen). Another topic in this area was the study of implicit computational complexity and the design of functional programming languages corresponding to specific complexity classes (Aehlig, Hofmann, Matthes). Yet another approach to the issue of the intrinsic complexity for general classes of algorithmic problems was developed in a talk by Y. Moschovakis.

In order to provide the participants with an overview over new developments in the study of functional and realizability interpretations (as mentioned above) two invited lecture series were given.
The first one (given by Fernando Ferreira and Paulo Oliva) focussed on novel (so-called monotone and bounded) variants of Gödel's functional interpretation (first published exactly 50 years ago) and its decomposition into an interpretation of linear logic combined with Girard's embedding of intuitionistic logic into linear logic. The second course was delivered by Ulrich Berger and presented a number of proof theoretic approaches for analyzing proofs based on dependent choice (such as Spector's bar recursive solution, the realizability solution by modified bar recursion due to Berger and Oliva and a novel approach based on open induction and its relation to previous work by Berardi, Bezem and Coquand). Moreover, Berger reported on recent experiments (with Schwichtenberg) concerning the automated extraction (based on the MinLog tool) of efficient algorithms from proofs in constructive analysis.

Mathematical Logic: Proof Theory, Constructive Mathematics

Table of Contents

Abstracts

Proving with Computer Algebra: Selected Examples from Combinatorics and Special Functions

Peter Paule

The overall theme of the talk is to present some thoughts on the role of computer algebra algorithms for proving. Elementary examples executed in the computer algebra system Mathematica (e.g., Wallis' integral over powers of the sine function on the interval from 0 to $\pi/2$) illustrate various algorithmic paradigms for problem solving in special functions and combinatorics. This includes, for instance, the classical hypergeometric machinery, based on rewriting and table look-up, and Zeilberger's "holonomic systems approach", based on recurrences and differential equations. The discussion also includes aspects of independent proof verification using "certificates" as well as mathematical knowledge management.

The talk concludes with a case study on the symbolic evaluation of a definite integral arising in work described by Victor Moll in "The evaluation of integrals: A personal story" [1]. In this context the key ingredient is a family of polynomials originally described as a hypergeometric double sum. Moll conjectured the log-concavity of the respective coefficient sequences. "Algorithms can be combined to new methods for problem solving" is a key message of the talk. An example is provided by the proof of Moll's conjecture by using Collins' Cylindrical Algebraic Decomposition (CAD) together with the RISC packages "MultiSum" (by K. Wegschaider) and "SumCracker" (by M. Kauers). For further details see "A Computer Proof of Moll's Log-Concavity Conjecture" [2]. The RISC software used in this proof is freely available at `http://www.risc.uni-linz.ac.at/research/combinat/software`.

References

[1] V. Moll, The evaluation of integrals: a personal story, *Notices of the American Mathematical Society*, 49, 2002.

[2] M. Kauers, P. Paule, A computer proof of Moll's log-concavity conjecture, *Proceedings of the American Mathematical Society*, 2007.

A topos for algebraic quantum theory

Bas Spitters

(joint work with Chris Heunen, Nicolaas P. Landsman)

In this talk we relate algebraic quantum mechanics to topos theory, so as to construct new foundations for quantum logic and quantum spaces. Motivated by Bohr's idea that the empirical content of quantum physics is accessible only through classical physics, we show how a C*-algebra of observables A induces a topos $\mathcal{T}(A)$ in which the amalgamation of all of its commutative subalgebras comprises a single *commutative* C*-algebra $\underline{A}$. According to the constructive Gelfand

duality theorem of Banaschewski and Mulvey, the latter has an internal spectrum $\underline{\Sigma}(\underline{A})$ in $\mathcal{T}(A)$, which in our approach plays the role of a quantum phase space of the system. Thus we associate a locale (which is the topos-theoretical notion of a space and which intrinsically carries the intuitionistic logical structure of a Heyting algebra) to a C*-algebra (which is the noncommutative notion of a space). In this setting, states on A become probability measures (more precisely, valuations) on $\underline{\Sigma}$, and self-adjoint elements of A define continuous functions (more precisely, locale maps) from $\underline{\Sigma}$ to Scott's interval domain. Noting that open subsets of $\underline{\Sigma}(\underline{A})$ correspond to propositions about the system, the pairing map that assigns a (generalised) truth value to a state and a proposition assumes an extremely simple categorical form. Formulated in this way, the quantum theory defined by A is essentially turned into a classical physical theory, internal to the topos $\mathcal{T}(A)$.

These results were partly inspired by the topos-theoretic approach to physics recently proposed by Döring and Isham.

Spatial logic. In classical mechanics, the logical structure of a physical system is encoded in its phase space M, the subsets of which can be considered either as a Boolean or a Heyting algebra. For an observable $a : M \to \mathbb{R}$, like position or energy, and an interval $\Delta \subset \mathbb{R}$, the subset $a \in \Delta := a^{-1}(\Delta)$ is then a proposition. Our aim is to extend this pleasant picture to quantum theory. Thus we present a spatial notion of quantum logic aimed to replaced von Neumann's lattice of subspaces of a Hilbert space. This is program accomplished by:

(1) Identifying an appropriate notion of a quantum phase 'space' Σ.
(2) Defining suitable 'subsets' of Σ that act as elementary logical propositions of quantum mechanics.
(3) Describing observables and states in terms of Σ.
(4) Associating a proposition $a \in \Delta$ (and hence a 'subset' $[a \in \Delta]$ of Σ) to an observable a and an open subset $\Delta \subseteq \mathbb{R}$.
(5) Finding a pairing between pysical states and 'subsets' of Σ (and hence between states and propositions of the type $a \in \Delta$) to obtain a truth value.

Generalised notions of space. To achieve our program we relate two generalised notions of space: noncommutative C*-algebra s and locales in arbitrary topoi by combining the following ideas:

(1) *Algebraic quantum theory*
(2) *Constructive Gelfand duality*
(3) *Bohr's doctrine of classical concepts*

From the first, we just adopt the methodology of describing a quantum system by a noncommutative C*-algebra A (defined in the usual topos **Sets**). As to the second, the constructive Gelfand duality of Banaschewski and Mulvey states that: if A is a unital commutative C*-algebra in a topos $\mathcal{T}$, there exists a compact completely regular locale Σ such that $A \cong C(\Sigma, \mathbb{C})$. Third, Niels Bohr's "doctrine of classical concepts" states that we can only look at the quantum world through classical glasses, measurement merely providing a "classical snapshot of

reality". The combination of all such snapshots should then provide a complete picture. This doctrine has a transparent formulation in algebraic quantum theory, to the effect that the empirical content of a quantum theory described by a certain noncommutative C*-algebra A is contained in suitable commutative C*-algebras associated to A.

The following construction weaves these three threads together. Let A be a unital C*-algebra and let $\mathbb{C}A$ be the collection of its unital commutative C^*-subalgebras, partially ordered by inclusion. This is a catalogue of all 'classical snapshots of reality' one may take of the quantum system described by A. We then consider the topos $\mathcal{T}(A) := \mathbf{Sets}^{\mathcal{C}}$. The philosophical idea is that as observers we are confined to the topos $\mathcal{T}(A)$, whereas the physical system itself exists in the ambient topos **Sets**. According to Bohr and Heisenberg, the system might seem to behave probabilistically from our limited classical perspective, but this behaviour is just a consequence of our confinement to $\mathcal{T}(A)$.

It turns out that the tautological functor $\underline{A} : C \mapsto C$, is a unital commutative C*-algebra in $\mathcal{T}(A)$. We call $\underline{A}$ the *Bohrification* of A. It has an associated Gelfand spectrum $\underline{\Sigma}(\underline{A})$, which is a locale in $\mathcal{T}(A)$. The map $A \mapsto \underline{\Sigma}(\underline{A})$ associates a 'space' $\underline{\Sigma}(\underline{A})$ in the sense of topos theory to a 'space' A in the sense of noncommutative geometry.

Considering an observable, a self-adjoint element a in A, of a quantum system described by a C*-algebra A. We should approximate a within each classical snapshot C of A, where $C \in \mathcal{C}(A)$ is some commutative subalgebra. The difficulty is, of course, that a need not lie in C. The best one can do is approximate a by a family of elements of C. In this way we arrive at an internal locale map $\delta(a) : \underline{\Sigma} \to \underline{\mathbb{IR}}$, where $\underline{\mathbb{IR}}$ is the *interval domain* $\mathbb{IR}$, familiar from domain theory.

In principle, this construction leads to the solution of all five problems listed above:

(1) The quantum phase space of the system described by A is the locale $\underline{\Sigma} \equiv \underline{\Sigma}(\underline{A})$ in the topos $\mathcal{T}(A)$.
(2) The elementary propositions are simply the 'opens' in $\underline{\Sigma}$. Thus the quantum logic of A is given by the Heyting algebra underlying $\underline{\Sigma}(\underline{A})$.
(3) Observables $a \in A$ define locale maps $\delta(a) : \underline{\Sigma} \to \underline{\mathbb{IR}}$. States ρ on A yield probability measures (more precisely, valuations) μ_ρ on $\underline{\Sigma}$.
(4) An open interval $\Delta \subseteq \mathbb{R}$ defines an element of the internal interval domain to which we can apply the frame map $\delta^{-1}(a)$ to obtain a proposition.
(5) State-proposition pairing is defined as $\langle \rho, U \rangle :=$'$\mu_\rho(U) = 1$'$\in \underline{\Omega}$.

References

[1] T. Coquand, B. Spitters. An elementary constructive proof of Gelfand duality for C*-algebras, 2007. *Submitted for publication.*

[2] ———Integrals and valuations. *To appear*, 2008.

[3] ———Formal topology and constructive mathematics: the Gelfand and Stone-Yosida representation theorems. *Journal of Universal Computer Science*, 11(12):1932–1944, 2005.

[4] C. Heunen, K. Landsman, B. Spitters. A topos presentation of algebraic quantum theory. `http://arxiv.org/abs/0709.4364`, 2008.

A New, Simpler Finitary Construction of the Real Closure of a Discrete Ordered Field

Charles Delzell

We give a new, simple (one-page) finitary construction of the real closure R of a discrete field $(K, \leq)$, as the set of equivalence classes of ι-terms involving certain formulae in the language of ordered rings $(+, -, \cdot, 0, 1, \leq)$ with equality, augmented by a constant symbol c_r for each element $r \in K$. It is routine to verify, finitarily, that this R satisfies the axioms of real closed, ordered fields, with the exception of the axiom $0 \neq 1$, for which the verification is difficult and depends on (and is equivalent to) a finitary proof of the consistency of the theory of real closed fields augmented by the diagram of $(K, \leq)$.

Recent Developments around the Dialectica Interpretation

Fernando Ferreira

We present Gödel's *dialectica* interpretation in the setting of Heyting arithmetic in all finite types. The interpretation is not intuitionistically faithful. This is one feature that makes it interesting. It has, nevertheless, an intuitionistically faithful interpretation of disjunction, and we show why this is required (vis a vis a more simple classical alternative). We discuss the heuristics of the interpretation of implication and show how the so-called characteristic principles (and the unfaithfulness to intuitionism) show up in this heuristics. We state Gödel's soundness theorem in this setting and present some corollaries. The interpretation yields closed terms which, in a certain sense, give computational information about the formal deductions and, in favorable cases, extract mathematically meaningful computational information. We state the characterization theorem of Yasugi. A benefit of Yasugi's theorem is that it shows that no characteristic principles are missing.

We define Howard-Bezem's notion of strong majorizability, state Howard's majorizability theorem for this notion and show (after Howard) that full extensionality does not have a *dialectica* interpretation. It is observed that continuity implies majorizability in type 2, but not in type 3. We insist that it is majorizability, not continuity, that makes the new majorizabilty interpretations (monotone, bounded, uniform) tick. We introduce Kohlenbach's monotone interpretation and state the corresponding soundness theorem. It is observed that in the *dialectica* interpretation we may add universal axioms (Kreisel's observation) and that a great benefit of the monotone functional interpretation is that we may add further axioms (e.g., weak König's lemma). We explain why is it the case that the monotone interpretation is able to give bounds which are uniform with respect to certain parameters. The monotone interpretation can be generalized to full second-order arithmetic via Spector's bar-recursive functionals, similarly to the case of the *dialectica* interpretation (the bar-recursive interpretation of the "double negation shift" scheme is

instrumental in this regard). We briefly explain how this theoretical work relates to Kohlenbach's program of Proof Mining.

In the last part of the first lecture, we introduce the bounded functional interpretation (bfi) of Ferreira and Oliva. Intensional (or rule governed) majorizability is defined, and a corresponding majorizability theorem is stated. Bounded and monotone quantifiers are introduced. We do not present the clauses of the bfi but focus instead on its characteristics principles. Particularly, we discuss the intensional collection scheme (uniform boundedness) and the intensional bounded contra-collection principle (introduction of ideal elements). We show how Bishop's limited principle of omniscience is refuted by the characteristic principles, as well as full extensionality. On the other hand, we mention that Bishop's lesser limited principle of omniscience, as well as weak König's lemma, follow from the characteristic principles of bfi. The soundness theorem of bfi is stated. The passageway from the intensional world of bfi to the set theoretical world is obtained through flattening. This is obtained by substituting the intensional majorizability relation by Howard-Bezem's relation. Note that this substitution can only be effected after applying the soundness theorem, according to which the characteristic principles are not needed in the verifying theory. NB the flattened versions of the characteristics principles lead to *inconsistency*. We end up the first lecture by showing (using bfi) how to get uniform bounds from suitable theorems (roughly, mathematically meaningful variations of forall-exists statements) and, at the same time, weaken (epsilon weakenings) the hypothesis of the theorems.

In the beginning of Lecture 2, we point that we can compose bfi with a negative translation in order to analyze classical finite-order arithmetic. Nevertheless, the interpretation of classical arithmetic can also be obtained directly, in the style of Shoenfield. We present the clauses of a bfi-based direct interpretation of classical arithmetic – the so-called uniform interpretation. Its characteristic principles are very simple: (1) a version of choice (which includes the axiom of choice from type 1 to type 0, with quantifier-free matrix); (2) the intensional bounded collection principle (equivalently, the intensional bounded contra-collection principle); and (3) the majorizability axioms. We show how, with these principles, extensional type 2 functionals are necessarily uniformly continuous on the Cantor space. We also recapture Kohlenbach's uniform boundedness principles. We state the soundness theorem for the uniform interpretation. For convenience, we call the sentences that are automatically interpreted by the new interpretation "tame" principles. When the flattenings of these "tame" principles are true, the role of the terms extracted by the interpretation is verified in a true theory and, hence, the extraction is sound. These "tame" principles include the universal sentences (Kreisel), the wider class considered by Kohlenbach in the monotone interpretation, but also other principles. We mention three. An intensional version of bounded induction, a bounded version of choice and (intensional) bounded comprehension. Other (mathematically) interesting "tame" principles may perhaps be formulated. On this regard, we mention that the usual "less than or equal" relation in the real numbers has an intensional counterpart which interpolates between the strict less

than relation and the less than or equal relation. This may be of help in formulating interesting "tame" principles. We briefly mention that our representation of the reals is based on a modification of the signed digit representation. This representation is particularly suitable for majorizability considerations because if a positive real number is majorized by a certain natural number then its type 1 representations are also majorizable (by a simple type 1 function which depends on the given natural number). We finish this discussion by demarcating the limits of the uniform interpretation. We conjecture that it can be extended to full second-order arithmetic (via bar-recursion). On the other hand, we show that *normal* functionals cannot be present in uniform interpretations. In other words, we can have arbitrary numerical comprehension, but not even very simple forms of type 1 comprehension.

The final part of Lecture 2 is dedicated to the introduction of new base types (after Kohlenbach), namely a type for normed spaces. Due to the lack of extensionality, the axioms for normed spaces need to be stated in an unfamiliar form, but in the end extensionality is guaranteed for the notions introduced. Intensional majorizability is extended to the new types, where the bounding terms are in the familiar type numerical structure. A majorizability theorem holds. We mention that it is possible to define a uniform interpretation in this setting, and prove a soundness theorem with similar characteristic principles as in the numerical case. As an example of the power of these characteristic principles, we show that they imply that Cauchy sequences with a modulus of Cauchyness do converge. Flattening is briefly discussed in this setting. At this point we introduce some recent work (with P. Engrácia). We mention that (intensional) bounded collection fails for universal matrices, but local versions of it hold in the Baire space. Really, this is a novel reading of the Baire category theorem applied to the Baire space. A logical version of this theorem (local bounded collection for universal matrices) can, in fact, be proved with the aid of the characteristic principles of the uniform interpretation together with "tame" bounded choice. We introduce linear operators in our setting (which are automatically bounded because of the characteristic principles) and state that the Banach-Steinhaus (aka, uniform boundedness) and the open maping theorems of functional analysis can be proved in finite-type Peano arithmetic together with the characteristic principles and the Baire category theorem. We remark that both theorems can be read as cases of bounded collection for universal matrices (the collection can be lifted from local - Baire category - to global collection because of linearity). We point that the proof of the open mapping theorem does not follow the usual textbook proof, but instead relies on an unsound compactness principle. The latter is, of course, a consequence of the characteristic principles of the uniform interpretation.

The axiomatic derivation of absolute lower bounds

Yiannis N. Moschovakis

In [2] (and the forthcoming [1]), we establish several lower bound results for problems in arithmetic, among them the following, where $\mathrm{iq}(x,y), \mathrm{rem}(x,y), x \dot{-} y$ are the integer quotient, remainder and arithmetic subtraction operations on $\mathbb{N}$ and $c^s_\alpha(x,y)$ counts the number of applications of the primitives in the computation:

Theorem 1 ([2])**.** *If an algorithm α decides the coprimeness relation $x \perp\!\!\!\perp y$ on $\mathbb{N}$ from the primitives $\leq, +, \dot{-}, \mathrm{iq}, \mathrm{rem}$, then for infinitely many a, b*

$$(*) \qquad c^s_\alpha(a,b) > \frac{1}{10}\log\log(\max(a,b));$$

in fact (*) holds for all solutions of Pell's equation, $a^2 = 1 + 2b^2$.

This is (small) step towards establishing the optimality of the Euclidean algorithm which decides coprimemess with

$$c^s_\epsilon(a,b) \leq 2\log(\min(a,b)) \quad (\min(a,b) \geq 2).$$

My aim in this lecture was to provide a justification for the sweeping claim of applicability of this result to *all algorithms*, by formulating (natural) axioms for algorithms in the style of *abstract model theory*, and showing how Theorem A can be derived from them. The proposed axioms utilize natural definitions of *partial algebras* and *imbeddings* between them and they are the following:

- I, **Locality Axiom**: An algorithm α of arity n of a partial algebra $\mathbf{M} = (M, 0, 1, \Phi^{\mathbf{M}})$ assigns to each (partial) subalgebra $\mathbf{U} \subseteq_p \mathbf{M}$ an n-ary, strict partial function
$$\overline{\alpha}^{\mathbf{U}} : U^n \rightharpoonup U.$$
We write $\mathbf{U} \models \overline{\alpha}(\vec{x}) = w \iff \overline{\alpha}^{\mathbf{U}}(\vec{x}) = w$.
- II, **Embedding Axiom**: If $\mathbf{U}, \mathbf{V} \subseteq_p \mathbf{M}$, and $\iota : \mathbf{U} \rightarrowtail \mathbf{V}$ is an embedding, then
$$\mathbf{U} \models \overline{\alpha}(\vec{x}) = w \implies \mathbf{V} \models \overline{\alpha}(\iota\vec{x}) = \iota w \quad (x_1, \ldots, x_n, w \in U).$$
- III, **Finiteness Axiom**:

$$\mathbf{M} \models \overline{\alpha}(\vec{x}) = w \implies \textit{there is an } m \textit{ such that } \vec{x}, w \in G_m(\vec{x}) \text{ and } \mathbf{M}\restriction G_m(\vec{x}) \models \overline{\alpha}(\vec{x}) = w$$

where $G_m(\vec{x})$ is the set of all objects in M which can be defined by terms of depth no more than m.

The axioms are in rather severe logical form, but it is fairly easy to see that they are satisfied by all known models of computation (RAMs, recursive programs, etc.) and they determine a "logical" (depth) complexity for algorithms:

The complexity of an algorithm. If α is an algorithm of $\mathbf{M}$ (satisfying I – III) and $\mathbf{M} \models \overline{\alpha}(\vec{x}) = w$, set

$$c^{\iota}_{\alpha}(\vec{x}) = \text{the least } m \text{ such that } \mathbf{M}\restriction G_m(\vec{x}) \models \overline{\alpha}(\vec{x}) = w.$$

This is defined by the Finiteness Axiom.

Intuitively, if $m = c^{\iota}_{\alpha}(\vec{x})$, then any implementation of α will need to "consider" (use) some $u \in M$ of depth m; and so it will need at least m steps to construct this u from the input using the primitives. The complexity measure c^{ι}_{α} is (easily) majorized by all usual time-complexity measures, including the number of calls to the primitives.

The embedding complexity of a (computable) function. Fix $f : M^n \to M$. An embedding $\iota : \mathbf{M}\restriction G_m(\vec{x}) \rightarrowtail \mathbf{M}$ *respects* f *at* $\vec{x}$ if

$$f(\vec{x}) \in G_m(\vec{x}) \;\&\; \iota(f(\vec{x})) = f(\iota(\vec{x}))$$

It is easy to check that *if some algorithm computes* f *in* $\boldsymbol{M}$*, then for each* $\vec{x}$*, there is some* m *such that every embedding* $\iota : \boldsymbol{M}\restriction G_m(\vec{x}) \rightarrowtail \boldsymbol{M}$ *respects* f *at* $\vec{x}$, and so we can set

$$c^{\iota}_{f}(\vec{x}) = \text{the least } m \text{ such that every } \iota : \mathbf{M}\restriction G_m(\vec{x}) \rightarrowtail \mathbf{M} \text{ respects } f \text{ at } \vec{x}.$$

It is immediate from the definition that $c^{\iota}_{f}(\vec{x}) \leq c^{\iota}_{\alpha}(\vec{x})$ for every algorithm α of $\mathbf{M}$ which satisfies the axioms; now the arguments in [2] establish Theorem A for with c^{ι}_{f} in place of c^{s}_{α} (with f the characteristic function of coprimeness), providing evidence that this lower bound is universal; and the true, universal lower bound from the indicated primitives should be single- rather than double-log, but no proof of this in sight at the moment.

References

[1] Lou van den Dries and Yiannis N, Moschovakis. Arithmetic complexity. To appear in *ACM Transactions on Computational Logic*.

[2] ———. Is the Euclidean algorithm optimal among its peers? *Bulletin of Symbolic Logic*, 10:390–418, 2004.

Proof Mining in Metric Fixed Point Theory

Eyvind Martol Briseid

We report on further developments of the uses of proof mining in metric fixed point theory. "Proof mining" is a label assigned to a general project of applying proof theory to ordinary mathematics, developed by U. Kohlenbach and various coauthors in recent years (see e.g. [4], [5]). In [2] we develop a method for finding, under general conditions, explicit and highly uniform rates of convergence for the Picard iteration sequences for selfmaps on bounded metric spaces from ineffective proofs of convergence to a unique fixed point. We are able to extract full rates of convergence by extending the use of a logical metatheorem recently proved by Kohlenbach. In recent case studies we found such explicit rates of convergence in two concrete cases, namely for asymptotic contractions in the sense of Kirk, and

earlier for the so-called uniformly continuous uniformly generalized p-contractive mappings (see [3] and [1]). Our novel method now provides an explanation in logical terms for these findings. This amounts, loosely speaking, to general conditions under which we in this specific setting can transform a $\forall\exists\forall$-sentence into a $\forall\exists$-sentence via an argument involving product spaces. This reduction in logical complexity allows us to use the existing machinery to extract quantitative bounds of the sort we need.

The formal framework involves a formal system $\mathcal{A}^\omega$ for analysis. $\mathcal{A}^\omega$ is basically Peano arithmetic in all finite types with quantifier free axiom of choice, dependent choice and countable choice, but with only a certain quantifier-free rule of extensionality instead of the full axiom of extensionality. Following Kohlenbach we "add" an abstract bounded metric space on top of this, obtaining the theory $\mathcal{A}^\omega[X,d]$. For details regarding this and other definitions, see [4] and [2]. Our result will employ product spaces and will rely on a combinatorial lemma given below. For a metric space (X,d) and an integer $m \geq 1$ we let (X^m, d_m) be the product space defined in the obvious way, and given $f : X \to X$ we define the mapping $f_m : X^m \to X^m$ by $f_m(\vec{x}) = \big(f(x^1), \ldots, f(x^m)\big)$, where $\vec{x} = (x^1, \ldots, x^m)$.

Lemma. *Let (X,d) be a metric space and let $f : X \to X$ be a mapping. Assume that there exists a function $\Phi : \mathbb{N} \to \mathbb{N}$ such that*

$$\forall k \in \mathbb{N} \forall \vec{x}, \vec{y} \in X^m \exists n \leq \Phi(k) \left(d_m\left(f_m^n(\vec{x}), f_m^n(\vec{y})\right) < 2^{-k-3}\right)$$

holds for all natural numbers $m \geq 1$. Then

$$\forall k \in \mathbb{N} \forall x, y \in X \forall l, n \geq \Phi(k) \left(d\left(f^l(x), f^n(y)\right) < 2^{-k}\right).$$

The following definition involves a condition which loosely says that not only should (X,d) and $f : X \to X$ give rise to a model of a suitable formal theory for the class of selfmappings to which $f : X \to X$ belongs, but so should (X^m, d_m) and f_m (for all $m \geq 1$), and moreover, the moduli introduced when formalizing the class of selfmappings should be majorizable, uniformly in m. Both the definition and the theorem below are somewhat less general than the corresponding definition and theorem in [2].

Definition. *Let $\mathcal{A}^\omega[X,d]+\Delta$ be the theory $\mathcal{A}^\omega[X,d]$ extended with a new constant c_f of type $X \to X$ and with new constants $c_1, \ldots, c_{n_1}$ of types of degree 1 and new constants $c_{n_1+1}, \ldots, c_{n_2}$ of types of degree $(1,X)$, and also with purely universal closed axioms which do not contain $\vee$ and with the types of all quantifiers of degree 2 or $(1,X)$. We say that a nonempty bounded metric space (X,d) and a selfmap $f : X \to X$ together* provide a uniform product space model *for $\mathcal{A}^\omega[X,d]+\Delta$ if there exist closed terms $c_1^*, \ldots, c_{n_1}^*$ of $\mathcal{A}^\omega[X,d]+\Delta$ such that for all $m \geq 1$ one can obtain a model of $\mathcal{A}^\omega[X,d]+\Delta$ by:*

(i) *letting the variables range over the appropriate universes of the full set-theoretic type structure $\mathcal{S}^{\omega,X^m}$ with the set X^m as the universe for the base type X, letting 0_X be interpreted by an arbitrary element of X^m, and*

letting $c_{n_1+1}, \ldots, c_{n_2}$ *be interpreted by functionals from the appropriate universes of* $\mathcal{S}^{\omega,X^m}$,

(ii) *letting* b_X *be interpreted by an integer upper bound* b *for* d_m, *letting* d_X *be interpreted by* $\lambda x, y.\,(d_m(x,y))_\circ$, *and letting* c_f *be interpreted by* f_m,

(iii) *and finally by letting* $c_1, \ldots, c_{n_1}$ *be interpreted such that*

$$\mathcal{S}^{\omega,X^m} \models c_i^*\ s\text{-}maj_{\sigma_i}\ c_i \qquad \text{for } 1 \le i \le n_1,$$

where σ_i *is the type of* c_i.

And furthermore for all $m \ge 1$ *the terms* $c_1^*, \ldots, c_{n_1}^*$ *should be interpreted by the* same *functionals* $F_1, \ldots, F_{n_1}$ *in the models above.*

The relevance of the theorem below comes from the fact that it has been possible to find such theories $\mathcal{A}^\omega[X,d]+\Delta$ and uniform majorizers $\vec{F}$ of the moduli introduced (i.e., of the interpretations of the new constants of relevant type) such that conditions (1) and (2) below are provable and such that all members of certain classes of selfmappings of metric spaces considered in the literature satisfy the conditions in the definition above, i.e., provide uniform product space models for the theory.

Theorem. *Let* $\mathcal{A}^\omega[X,d]+\Delta$ *be as in the definition above. Suppose that* $\mathcal{A}^\omega[X,d]+\Delta$ *proves*

$$\forall x^X \forall y^X\,(c_f(x) =_X x \wedge c_f(y) =_X y \to x =_X y) \tag{1}$$

and

$$\forall x_0^X, y_0^X \forall k^0 \exists n^0\left(d_X(x_n, x_{n+1}) <_{\mathbb{R}} (2^{-k})_{\mathbb{R}} \wedge d_X(y_n, y_{n+1}) <_{\mathbb{R}} (2^{-k})_{\mathbb{R}}\right), \tag{2}$$

where x_n *and* y_n *are the* n*-th members of the defined Picard iteration sequences*[1] *starting with respectively* x_0 *and* y_0. *If there exist a nonempty bounded metric space* (X,d) *and a mapping* $f: X \to X$ *which provide a uniform product space model for* $\mathcal{A}^\omega[X,d]+\Delta$, *then from the proofs in* $\mathcal{A}^\omega[X,d]+\Delta$ *of (1) and (2) one can extract a functional* $\Phi: \mathbb{N}\times\mathbb{N}\times S_{\sigma_1}\times\cdots\times S_{\sigma_{n_1}} \to \mathbb{N}$, *which can be defined in the calculus* $T+BR$ *of the so-called bar recursive functionals, such that whenever we have a nonempty metric space* (X,d) *bounded by* $b \in \mathbb{N}$ *and a mapping* $f: X \to X$, *which together provide a uniform product space model for* $\mathcal{A}^\omega[X,d]+\Delta$, *then*

$$\forall k \in \mathbb{N} \forall x, y \in X \forall l, n \ge \Phi(k, b, \vec{F})\left(d\left(f^l(x), f^n(y)\right) < 2^{-k}\right)$$

holds in (X,d), *where* $\vec{F}$ *is as in the definition above.*

References

[1] E. M. Briseid. Fixed points of generalized contractive mappings. To appear in *Journal of Nonlinear and Convex Analysis*.

[2] ———. Logical aspects of rates of convergence in metric spaces, *in preparation.*

[3] ———, A rate of convergence for asymptotic contractions, *Journal of Mathematical Analysis and Applications* 330 (2007), 364–376.

[1] That is, we write x_n for $P(x_0, n)$, where $P := \lambda x^X, n^0.\, R_X n^0 x^X z$, with $z := \lambda x^X, m^0.\, c_f x$.

[4] U. Kohlenbach, Some logical metatheorems with applications in functional analysis, *Transactions of the American Mathematical Society* 357 (2005), 89–128.
[5] ———. Applied proof theory: Proof interpretations and their use in mathematics, *Springer Monographs in Mathematics*, Springer, Berlin and Heidelberg, 2008.

Proofs as programs in analysis

Ulrich Berger

In this tutorial I give an overview of some old and new results on program extraction from proofs in analysis.

The first lecture is about the computational interpretation of proofs in *classical* analysis. The main problem here is to assign computational content to the axiom of countable (dependant) choice. We compare Spector's solution by bar recursion in finite types with other forms of recursion including the Berardi/Bezem/Coquand functional and open recursion.

In the second lecture I report on recent advances in program extraction for *constructive* analysis. The main example of a case study implemented in the proof system Minlog (due to H Schwichtenberg) is a constructive proof of the Inverse Function Theorem together with its extracted program. Finally, I describe an alternative approach to exact real number computation based on a coinductive definition of uniform continuity. I show how this can be used to extract memoised programs for functions operation on reals represented by infinite streams of digits -1, 0, 1.

Parallel Time and Proof Complexity

Klaus Aehlig

Consider the following variant of quantified propositional logic. Quantifiers can only be witnessed by variables, but there is a parallel extension rule that is aware of independence of the introduced variables.

$$\frac{\Gamma, \neg(p_1 \leftrightarrow \varphi_1), \dots, \neg(p_k \leftrightarrow \varphi_k)}{\Gamma} \qquad \begin{array}{l}\text{provided } p_1, \dots, p_k \\ \text{not free in } \Gamma, \varphi_1, \dots, \varphi_k\end{array}$$

This awareness of dependencies is motivated by looking at the height of boolean circuits. Adding an uninterpreted predicate on bit strings—like an oracle in relativised complexity classes—this statement can be made precise. The height of the most shallow proof that a circuit can be evaluated is, up to an additive constant, the height of that circuit.

The main tool for showing lower bounds on proof heights is a variant of an iteration principle introduced by Takeuti. This variant allows for polynomial size formulae in the relativised language that require proofs of exponential height. An arithmetical formulation of the iteration principle yields a strength measure for theories in the language of relativised two-sorted Bounded Arithmetic.

References

[1] K. Aehlig and A. Beckmann. Propositional logic for circuit classes. In J. Duparc and T. Henzinger, editors, *Proceedings of the sixteenth Annual Conference on Computer Science and Logic*, volume 4646 of *Lecture Notes in Computer Science*, pages 512–526. Springer Verlag, Sept. 2007.

[2] S. A. Cook. Theories for complexity classes and their propositional translations. In J. Krajíček, editor, *Complexity of computations and proofs*, Quaderni die Matematica, pages 175–227. Dipartimento di Matematica, Seconda Universitá degli Studi di Napoli, 2003.

[3] G. Takeuti. Separations of theories in weak bounded arithmetic. *Annals of Pure and Applied Logic*, 71:47–67, 1995.

Pure Pointer Programs with Universal Iteration

Martin Hofmann

(joint work with Ulrich Schöpp)

Many LOGSPACE programs are naturally described as programs that operate on a structured input, e.g., a graph, that store in memory only a constant number of pointers into the input and, in particular, do not use pointer arithmetic.

We define a programming language that captures this intuition by extending Cook and Rackhoff's Jumping Automata on Graphs with a universal iteration construct that allows one to visit all nodes in an *unspecified* order. We show that in this way both, Jumping Automata on Graphs and Deterministic Transitive Closure logic, are subsumed, yet not all of LOGSPACE can be programmed, thus arithmetic is not introduced "through the backdoor" as is the case in Deterministic Transitive Closure logic with order. Concretely, we show that the property "the number of nodes is a power of two" is not expressible.

Bounded Arithmetic and Search Problems

Neil Thapen

(joint work with Alan Skelley)

The main open problem in bounded arithmetic is to show that the full theory $T_2 =_{def} \bigcup_i T_2^i$ does not collapse to some finite level T_2^j. This is equivalent to showing that bounded arithmetic does not prove that the polynomial hierarchy collapses [3, 1, 7] (it is known that the relativized bounded arithmetic hierarchy does not collapse [3]). A natural conjecture is that the theories T_2^i are already separated by $\forall\Pi_1^b$ formulas, by analogy with the classical theories $\mathrm{I}\Sigma_i$ which are separated by Π_1 consistency statements. However direct consistency arguments will not work, since even strong bounded arithmetic theories are known not to prove the consistency of weak ones [6, 5].

This talk is concerned with what seems to be the most tractable approach to getting more information about the hierarchy, which is to look for a $\forall\Sigma_1^b$ separation between the bounded arithmetic theories in the relativized setting (this is also closely connected to the problem of improving the lower bounds for constant depth

Frege systems in propositional proof complexity). The witnessing theorem method is available to study such sentences: first show that if a $\forall\Sigma^b_1(\alpha)$ sentence is provable in a theory, then witnessing it is reducible to finding a witness to some NP property of a combinatorial structure built up out of polynomial time oracle machines; then show a limit to how much information such a witness can give about the oracle [2]. The problem of finding a witness to an NP predicate when one is known to exist is called an NP search problem. There is a rich variety of classes of such problems, often characterized by the combinatorial lemma which guarantees that solutions to the problems in the class exist.

We give combinatorial principles GI_k which are complete for the class of NP search problems provably total at the kth level T^k_2 of the bounded arithmetic hierarchy and which in fact characterize the $\forall\Sigma^b_1$ consequences of T^k_2, generalizing the results of [4].

Our characterization will be in terms of games with two players and a fixed finite number k of turns. The two players A and B take alternate turns, with A going first. Formally a game is given by a k-ary relation G and a size parameter a. The moves are numbers smaller than a and $G(x_1,\dots,x_k)$ holds if the second player wins in the game with the sequence of moves $x_1,\dots,x_k$.

Suppose G and H are two k-turn games. We say that G is *polynomial time reducible* to H if there are polynomial time functions $f_1,\dots,f_k$ such that for all possible sequences of moves $\bar{x}$ in G and $\bar{y}$ in H, if $y_i = f_i(x_1,\dots,x_i,y_1,\dots,y_{i-1})$ for every odd i and $x_i = f_i(x_1,\dots,x_{i-1},y_1,\dots,y_i)$ for every even i, then $H(\bar{y})$ implies $G(\bar{x})$. In pictures, here for even k:

$$\begin{array}{rccccc} H: & y_1 & y_2 & y_3 & \dots & y_k \\ & f_1\uparrow & f_2\downarrow & f_3\uparrow & \dots & f_k\downarrow \\ G: & x_1 & x_2 & x_3 & \dots & x_k \end{array}$$

The functions $f_1,\dots,f_k$ give a reduction if, whenever $\bar{x}$ and $\bar{y}$ are matched as in the picture and Player B wins in H with these moves, then Player B also wins in G.

An instance of the *k-game induction principle* GI_k is given by a size parameter a, a uniform sequence $G_1,\dots,G_a$ of polynomial time relations, polynomial time functions U and V and a uniform sequence $W_1,\dots,W_{a-1}$ of polynomial time functions. It states that, interpreting each G_i as a k-turn game in which the moves are bounded by a, the following things cannot all be true:

(1) U is an explicit winning strategy for B in G_1;
(2) V is an explicit winning strategy for A in G_a;
(3) For each i, W_i gives a reduction of G_{i+1} to G_i.

The principle is $\forall\Sigma^b_1$. It is provable in T^k_2 by induction up to a on i in the formula "Player B has a winning strategy in game G_i" which is Π^b_k. The argument for the other direction, showing that it is complete for sentences provable in T^k_2, uses a translation of first order proofs into large, uniform propositional proofs in a system in which the soundness of the rules can be witnessed by polynomial time reductions between games.

References

[1] S. Buss. Relating the bounded arithmetic and polynomial time hierarchies. *Annals of Pure and Applied Logic*, 75(1–2):67–77, 1995.

[2] M. Chiari and J. Krajíček. Witnessing functions in bounded arithmetic and search problems. *Journal of Symbolic Logic*, 63(3):1095–1115, 1998.

[3] J. Krajíček, P. Pudlák, and G. Takeuti. Bounded arithmetic and the polynomial hierarchy. *Annals of Pure and Applied Logic*, 52:143–153, 1991.

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

[5] P. Pudlák. A note on bounded arithmetic. *Fundamenta Mathematicae*, 136(2):86–89, 1990.

[6] A. Wilkie and J. Paris. On the scheme of induction for bounded arithmetic formulas. *Annals of Pure and Applied Logic*, 35:261–302, 1987.

[7] D. Zambella. Notes on polynomially bounded arithmetic. *Journal of Symbolic Logic*, 61(3):942–966, 1996.

Weak Definability Notions for Independence Results in Bounded Arithmetic

Chris Pollett

One of the most important problems in bounded arithmetic is whether the hierarchy $S_2 := \cup_i T_2^i$, $i \geq 2$ collapses. Here T_2^i is defined over the language 0, S, $+$, $\cdot$, $\lfloor \frac{x}{2^x} \rfloor$, $\dot{-}$, $|x|$, $2^{|x||y|}$, $\leq$, $=$, and has open axioms for these, together with induction for Σ_i^{b}-formulas. The Σ_i^{b}-formulas roughly correspond to the complexity classes Σ_i^{p} of the polynomial hierarchy. The hierarchies S_2^i, and R_2^i are defined similarly, except with length or length-length bounded induction, respectively. It is known that $R_2^i \subseteq S_2^i \subseteq T_2^i$, $T_2^i \preceq_{\Sigma_{i+1}^{\mathsf{b}}} S_2^{i+1} \subset R_2^{i+2}$, and that if $S_2^{i+1} = T_2^i$ then the polynomial hierarchy collapses. So if the bounded arithmetic hierarchy is infinite then S_2 cannot prove the polynomial hierarchy collapses. One way to separate these theories would be to show that the Δ_j^b predicates of these theories differ. For $j > 1$ the Δ_j^b-predicates of even $BASIC$ contain at least the $\Sigma_{j-1}^{\mathsf{p}}$ and Π_{j-1}^{p} relations of the polynomial hierarchy, so such separations seems to involve proving separations of the polynomial hierarchy. If one looks at the Δ_1^b predicates of R_2^1, S_2^1, T_2^1, T_2^2, ... one has exactly the relations in $\mathsf{NC} \subseteq \mathsf{P} \subseteq \mathsf{PLS} \subseteq$ games generalizing $\mathsf{PLS} \subseteq \mathsf{NP}$. So to separate based on these would involve at least separating NC versus NP or P versus NP. There are several strategies that have been tried to avoid these difficulties: reflection principles, propositional translations, dynamic ordinals, etc. Recently, Jeřábek [1] has shown that $T_2^0 \preceq_{\Sigma_1^{\mathsf{b}}} S_2^1$. In this talk, we consider a sub-theory of T_2^0, T_2^{-1}, where the cut rule has been restricted to allow only Σ_0^{b} formulas for both the principal and side formulas of the rule. By cut-elimination, T_2^0 is conservative over T_2^{-1} with respect to Σ_0^{b}-formulas. From a well-known block-counting argument this theory cannot Σ_1^{b}-define $\lfloor \frac{x}{3} \rfloor$. We argue that analogs of T_2^{-1} for other theories in the bounded arithmetic hierarchy might serve as a setting for separating the hierarchy. As an example of what an analog of T_2^{-1} might be, we consider what happens to the $T_2^0 \preceq_{\Sigma_1^{\mathsf{b}}} S_2^1$ proof when converted to a theory not quite R_2^1 versus the theory $T_2^{i,\{2^{||p(x)||}\}}$. We then define new notions of definability and

show that theories such as *BASIC* extended by sharply bounded μ operators can be separated from a conservative extension of T_2^{-1} with respect to Σ_0^{b}-formulas.

References

[1] E. Jeřábek. The strength of sharply bounded induction. *Mathematical Logic Quarterly*. Vol. 52. No. 6. pp. 613–624. October, 2006.

Proof Notations for Bounded Arithmetic

Arnold Beckmann

A recurring theme in the study of axiom systems is to determine the class of those computable functions whose totality can be shown in the axiom system. Ordinal informative proof theory [6] offers well developed tools for this endeavour: Proof theoretic ordinals capture the strength of axiom systems by characterising the supremum of order-types of well-orderings which can be recognised as such in the axiom system. Proof theoretic ordinals can be computed by eliminating cuts of unravelled proofs in corresponding infinitary propositional calculi using a natural translation of formal proofs to infinitary ones [8]. A similar path via eliminating cuts in infinitary calculi can be used to characterise also the computable functions of axiom systems. For this to work, cut-elimination has to be replaced by Mints' continuous cut-elimination [5] to ensure that cut-eliminated propositional proofs can be explored in a finite, computable way. One of the best descriptions of this setting is given via Buchholz-style notation systems [3] for infinitary propositional proofs, where finite descriptions of infinitary proofs are given by simple term structures based on inference symbols.

Bounded Arithmetic theories as introduced by Buss [4] form a collection of axioms systems whose class of computable functions connects them to complexity classes like the polynomial time hierarchy of functions. In this setting, it matters how complex descriptions of graphs of functions are. Therefore, we speak of definable functions, with NP-definability being of particular interest. Ordinal informative proof theory has been adapted to Bounded Arithmetic in terms of Dynamic Ordinal Analysis [2], providing a suitable measure of proof strength of Bounded Arithmetic theories. At the meeting "Mathematical Logic: Proof Theory, Type Theory and Constructive Mathematics" (Mathematisches Forschungsinstitut Oberwolfach, 20–26 March 2005) we proposed to understand whether Dynamic Ordinals can play a similar role for characterising the definable functions of Bounded Arithmetic as proof theoretic ordinals do for computable functions of stronger theories. This has been successfully achieved now by introducing a Buchholz-style notation system for the class of propositional proofs which are obtained by translating proofs in Bounded Arithmetic to propositional logic. The propositional translation used here is the one mentioned above, which in the Bounded Arithmetic community is known as the *Paris-Wilkie-translation* [7]. Employing the fact that cut-reduction operates feasibly on proof notations [1], we explained how this

setting can be used to obtain new uniform proofs of various known characterisations of definable functions in Bounded Arithmetic.

Furthermore, we are now able to extend our characterisations via proof notations to all NP-definable functions of Bounded Arithmetic theories. We characterise NP-definable functions of Bounded Arithmetic theories in terms of a new generalisation of Polynomial Local Search (PLS) problems which we call Π^p_k-Polynomial Local Search—this is joined work in progress together with Samuel R. Buss.

References

[1] K. Aehlig, A. Beckmann. On the computational complexity of cut-reduction. Accepted for LICS 2008. Technical Report CSR15-2007, Department of Computer Science, Swansea University, December 2007. `http://arxiv.org/abs/0712.1499`.

[2] A. Beckmann. Dynamic ordinal analysis. *Arch. Math. Logic*, 42:303–334, 2003.

[3] W. Buchholz. Notation systems for infinitary derivations. *Archive for Mathematical Logic*, 30:277–296, 1991.

[4] S. R. Buss. *Bounded arithmetic*, volume 3 of *Studies in Proof Theory. Lecture Notes*. Bibliopolis, Naples, 1986.

[5] G. E. Mints. Finite investigations of transfinite derivations. *Journal of Soviet Mathematics*, 10:548–596, 1978. Translated from: Zap. Nauchn. Semin. LOMI 49 (1975). Cited after Grigori Mints. *Selected papers in Proof Theory.*Studies in Proof Theory. Bibliopolis, 1992.

[6] W. Pohlers. Subsystems of set theory and second order number theory. In *Handbook of proof theory*, volume 137 of *Stud. Logic Found. Math.*, pages 209–335. North-Holland, Amsterdam, 1998.

[7] J. Paris and A. Wilkie. Counting problems in bounded arithmetic. In A. Dold and B. Eckmann, editors, *Methods in Mathematical Logic (Proceedings Caracas 1983)*, number 1130 in Lecture Notes in Mathematics, pages 317–340. Springer, 1985.

[8] W. W. Tait. Normal derivability in classical logic. In J. Barwise, editor, *The Syntax and Semantics of Infinitatry Languages*, number 72 in Lecture Notes in Mathematics, pages 204–236. Springer, 1968.

An Analysis of Gödel's Dialectica Interpretation via LL

Paulo Oliva

We have recently [2] presented an analysis of Gödel's Dialectica interpretation via a refinement of intuitionistic logic known as linear logic. We use the fact that the Dialectica interpretation of intuitionistic logic can be viewed as a composition of Girard's embedding [1] of intuitionistic logic into linear logic (assuming $!\exists z A \multimap \exists z !A$)

$$
\begin{aligned}
(A_{\mathsf{at}})^\star &:\equiv A_{\mathsf{at}} \\
(A \diamond_z B)^\star &:\equiv A^\star \diamond_z B^\star \\
(A \to B)^\star &:\equiv !A^\star \multimap B^\star \\
(\forall z A)^\star &:\equiv \forall z A^\star \\
(\exists z A)^\star &:\equiv \exists z A^\star.
\end{aligned}
$$

followed by de Paiva's [3, 4] Dialectica interpretation of linear logic

$$
\begin{array}{lcl}
|A \multimap B|^{\boldsymbol{f},\boldsymbol{g}}_{\boldsymbol{x},\boldsymbol{w}} & :\equiv & |A|^{\boldsymbol{x}}_{\boldsymbol{f}\boldsymbol{w}} \multimap |B|^{\boldsymbol{g}\boldsymbol{x}}_{\boldsymbol{w}} \\
|A \diamond_z B|^{\boldsymbol{x},\boldsymbol{v}}_{\boldsymbol{y},\boldsymbol{w}} & :\equiv & |A|^{\boldsymbol{x}}_{\boldsymbol{y}} \diamond_z |B|^{\boldsymbol{v}}_{\boldsymbol{w}} \\
|\exists z A(z)|^{\boldsymbol{x},z}_{\boldsymbol{f}} & :\equiv & |A(z)|^{\boldsymbol{x}}_{\boldsymbol{f}z} \\
|\forall z A(z)|^{\boldsymbol{f}}_{\boldsymbol{y},z} & :\equiv & |A(z)|^{\boldsymbol{f}z}_{\boldsymbol{y}} \\
|!A|^{\boldsymbol{x}}_{\boldsymbol{f}} & :\equiv & !|A|^{\boldsymbol{x}}_{\boldsymbol{f}\boldsymbol{x}}.
\end{array}
$$

where $A \diamond_z B$ denotes the if-then-else constructor on the level of formulas. This is a refinement of conjunction and disjunction, since we can define $A \vee B :\equiv \exists z^b (A \diamond_z B)$, for instance (where b is the type of booleans).

The interpretation of linear logic is such that if A is provable in LL then there exists a sequence of terms $\boldsymbol{t}$ such that the quantifier-free formula $|A|^{\boldsymbol{t}}_{\boldsymbol{y}}$ is also provable in linear logic. Gödel's original interpretation $A_D(\boldsymbol{x};\boldsymbol{y})$ can then be viewed as a combination of Girard's embedding of IL into LL followed by de Paiva's interpretation of LL as:

Theorem. $(A_D(\boldsymbol{x};\boldsymbol{y}))^\star \equiv |A^\star|^{\boldsymbol{x}}_{\boldsymbol{y}}$.

The theorem above assumes that the Dialectica interpretation has been stated with a slightly modified (although intuitionistically equivalent) interpretation of conjunction, disjunction and existential quantifiers:

$$
\begin{array}{lcl}
(A \wedge B)_D(\boldsymbol{x},\boldsymbol{v};\boldsymbol{y},\boldsymbol{w},z^b) & :\equiv & A_D(\boldsymbol{x}z;\boldsymbol{y}) \diamond_z B_D(\boldsymbol{v}z;\boldsymbol{w}) \\
(A \vee B)_D(\boldsymbol{x},\boldsymbol{v},z^b;\boldsymbol{y},\boldsymbol{w}) & :\equiv & A_D(\boldsymbol{x};\boldsymbol{y}z) \diamond_z B_D(\boldsymbol{v};\boldsymbol{w}z) \\
(\exists z^\tau A)_D(\boldsymbol{x},z;\boldsymbol{f}) & :\equiv & A_D(\boldsymbol{x};\boldsymbol{f}z).
\end{array}
$$

We have also shown that in the interpretation of linear logic a (linear logic) formula A is interpreted as $\exists\!\!\forall^{\boldsymbol{x}}_{\boldsymbol{y}} |A|^{\boldsymbol{x}}_{\boldsymbol{y}}$, where $\exists\!\!\forall^{\boldsymbol{x}}_{\boldsymbol{y}}$ is a simple form of branching quantifier. This new branching quantifier can also be given an interpretation as:

$$|\exists\!\!\forall^{\boldsymbol{v}}_{\boldsymbol{w}} A(\boldsymbol{v},\boldsymbol{w})|^{\boldsymbol{f},\boldsymbol{v}}_{\boldsymbol{g},\boldsymbol{w}} :\equiv |A(\boldsymbol{v},\boldsymbol{w})|^{\boldsymbol{f}\boldsymbol{w}}_{\boldsymbol{g}\boldsymbol{v}}.$$

Having the branching quantifier in hand we can then state characterisation principles for the interpretation of LL which refine the characterisation principles of Gödel's original interpretation. These are:

$$
\begin{array}{ll}
(\mathsf{SC}) & \forall z \exists\!\!\forall^{\boldsymbol{x}}_{\boldsymbol{y}} A_{\mathsf{qf}}(\boldsymbol{x},\boldsymbol{y},z) \multimap \exists\!\!\forall^{\boldsymbol{f}}_{\boldsymbol{y},z} A_{\mathsf{qf}}(\boldsymbol{f}z,\boldsymbol{y},z) \\
(\mathsf{PC}) & (\exists\!\!\forall^{\boldsymbol{x}}_{\boldsymbol{y}} A_{\mathsf{qf}}(\boldsymbol{y}) \multimap \exists\!\!\forall^{\boldsymbol{v}}_{\boldsymbol{w}} B_{\mathsf{qf}}(\boldsymbol{v})) \multimap \exists\!\!\forall^{\boldsymbol{f},\boldsymbol{g}}_{\boldsymbol{x},\boldsymbol{w}} (A_{\mathsf{qf}}(\boldsymbol{g}\boldsymbol{w}) \multimap B_{\mathsf{qf}}(\boldsymbol{f}\boldsymbol{x})) \\
(\mathsf{MP}) & \forall \boldsymbol{x} !A_{\mathsf{qf}} \multimap !\forall \boldsymbol{x} A_{\mathsf{qf}} \\
(\mathsf{TA}) & !\exists\!\!\forall^{\boldsymbol{x}}_{\boldsymbol{y}} A \multimap \exists \boldsymbol{x} !\forall \boldsymbol{y} A
\end{array}
$$

sequential choice, parallel choice, Markov principle and a new principle *trump advantage*, respectively. Note that $!\exists z A \multimap \exists z !A$ is a special case of (TA).

Theorem. *The equivalence between A and $\exists\!\!\forall^{\boldsymbol{x}}_{\boldsymbol{y}} |A|^{\boldsymbol{x}}_{\boldsymbol{y}}$ can be derived in* LL *extended with the four principles stated above.*

References

[1] J.-Y. Girard. Linear logic. *Theoretical Computer Science*, 50(1):1–102, 1987.

[2] P. Oliva. An analysis of Gödel's Dialectica interpretation via linear logic. To appear in: *Dialectica*.
[3] V. C. V. de Paiva. The Dialectica categories. In J. W. Gray and A. Scedrov, editors, *Proc. of Categories in Computer Science and Logic, Boulder, CO, 1987*, pages 47–62. Contemporary Mathematics, vol 92, American Mathematical Society, 1989.
[4] ———. A Dialectica-like model of linear logic. In D. Pitt, D. Rydeheard, P. Dybjer, A. Pitts, and A. Poigné, editors, *Category Theory and Computer Science, Manchester, UK*, pages 341–356. Springer-Verlag LNCS 389, 1989.

Computability in Ergodic Theory

Jeremy Avigad

Let T be a measure-preserving transformation of a space $(X, \mathcal{B}, \mu)$, let f be a measurable function from X to $\mathbb{R}$, and let x be any element of X. Think of x as denoting the state of a system, Tx as denoting the state a unit of time later, and f as being some measurement that one can perform. Imagine now performing a sequence of measurements $f(x), f(Tx), f(T^2x), \ldots, f(T^nx)$ and taking their average. The pointwise ergodic theorem says that this sequence of averages will converge almost everywhere; the mean ergodic theorem says that, as a function of x, the averages converge in the L^2 norm.

In general, one cannot compute rates of convergence from the initial data, and, indeed, the limit may not be computable (given reasonable notions of computability for the relevant objects). In short, the ergodic theorems cannot be given a direct computational interpretation. I will explain how proof-theoretic methods yield classically equivalent formulations of the ergodic theorems which are computably valid, and additional information besides.

References

[1] J. Avigad. The metamathematics of ergodic theory. To appear in *Ann. Pure Appl. Logic*.
[2] J. Avigad, P. Gerhardy, and H. Towsner. Local stability of ergodic averages. To appear in *Trans. Am. Math. Soc.*
[3] J. Avigad and Ksenija Simic. Fundamental notions of analysis in subsystems of second-order arithmetic. *Ann. Pure Appl. Logic*, 139:138–184, 2006.

Proof Mining in Topological Dynamics

Philipp Gerhardy

A famous theorem by van der Waerden ([3]) states the following: Given any finite colouring of the integers, one colour contains arbitrarily long arithmetic progressions. Equivalently, the theorem states that for every number of colours q and length of progression k there is an $N = N(q, k)$ such that for every q-colouring of intervals of length N one colour contains a progression of length k. An obvious question is: What is the growth rate of $N(q, k)$?

Some proofs, like van der Waerden's combinatorial argument, answer this question directly, by giving an upper bound on $N(q, k)$ which is basically of Ackermann

complexity. There is a topological proof of van der Waerden's Theorem by Furstenberg and Weiss ([1]) – via the so-called Multiple Birkhoff Recurrence Theorem in topological dynamics – that does not provide any bounds, so the question is: what is the computational content of that particular proof.

The techniques to unwind and extract the computational content of these proofs are taken from the field of "proof mining". This subfield of mathematical logic, or more precisely: proof theory, roughly falls into two parts: On the one hand, one developes general techniques for analysing proofs that allow one to classify theorems and proofs from which extraction is possible. On the other hand, one carries out case studies by analysing concrete mathematical proofs. Here, the focus is on the latter aspect of proof mining.

We present an analysis of a variant due to Girard ([2]) of Furstenberg and Weiss' proof. Girard analysed his proof of the Multiple Birkhoff Recurrence Theorem using cut elimination, though only in a setting specialised to van der Waerden's Theorem. Girard obtained the same bounds as van der Waerden. The analysis presented here is based on monotone functional interpretation and treats the general case of the Multiple Birkhoff Recurrence Theorem. It both yields bounds and provides a general illustration of proof mining in topological dynamics. The bounds do not improve the previous results by Girard, but only – as is also revealed by the analysis – because the combinatorial proof and the topological dynamics proof in principle are identical. We also argue briefly that an interpretation of the original argument by Furstenberg and Weiss would lead to bounds of even worse complexity, as it contains an unneccesary non-trivial appeal to compactness.

References

[1] H. Furstenberg, B. Weiss. Topological Dynamics and Combinatorial Number Theory, *Journal d'Analyse Mathematique*, 34 (1978), 61–85.
[2] J.-Y. Girard. Proof Theory and Logical Complexity. Volume I, Bibliopolis, Naples, 1987.
[3] B. L. van der Waerden. Beweis einer Baudetschen Vermutung, *Nieuw Archief voor Wiskunde*, 15 (1927), 212–216.

Recent results in proof mining

Laurenţiu Leuştean
(joint work with Ulrich Kohlenbach)

The talk is a report on joint work [7, 8] with Ulrich Kohlenbach and presents two applications of proof mining. By proof mining we mean the logical analysis of mathematical proofs with the aim of extracting new numerically relevant information hidden in the proofs (we refer to [5] for a book treatment).

In 1939, Garrett Birkhoff proved the following generalization of von Neumann's Mean Ergodic Theorem.

Theorem 2. [2] *Let X be a uniformly convex Banach space and $T : X \to X$ be a linear operator with $\|Tx\| \leq \|x\|$ for all $x \in X$. Then for any $x \in X$, the Cesaro mean (x_n) is convergent.*

In [1], Avigad, Gerhardy and Towsner address the issue of finding an effective rate of convergence for (x_n) in Hilbert spaces. They show that even for the separable Hilbert space L_2 there are simple computable such operators T and computable points $x \in L_2$ such that there is no computable rate of convergence of (x_n). In such a situation the best one can hope for is an effective bound on the Herbrand normal form of the Cauchy property of (x_n):

$$\forall \varepsilon > 0 \, \forall g : \mathbb{N} \to \mathbb{N} \, \exists N \in \mathbb{N} \, \forall i, j \in [N, N + g(N)] \; (\|x_i - x_j\| < \varepsilon). \tag{1}$$

The mathematical relevance of this reformulation of convergence was recently pointed out by T. Tao ([9, 10]), who also uses the term 'metastability'.

In [4], a general logical metatheorem is proved that guarantees (given a proof of (1)) the extractability of an effective bound $\Phi(\varepsilon, g, b, \eta)$ on '$\exists N$' in (1) that is highly uniform in the sense that it only depends on g, ε, an upper bound $\mathbb{N} \ni b \geq \|x\|$ and a modulus η of uniform convexity for X, but otherwise is independent from x, X and T.

We extract [8, Theorem 2.1] such a bound from the proof of Theorem 2: $\Phi(\varepsilon, g, b, \eta) := M \cdot \tilde{h}^K(1)$, with $\|x\| \leq b \in \mathbb{N}$, $M := \left\lceil \frac{16b}{\varepsilon} \right\rceil$, $K := \left\lceil \frac{b}{\gamma} \right\rceil$, $\gamma := \frac{\varepsilon}{16} \eta \left(\frac{\varepsilon}{8b} \right)$, $h, \tilde{h} : \mathbb{N} \to \mathbb{N}$, $h(n) := 2(Mn + g(Mn))$, $\tilde{h}(n) := \max_{i \leq n} h(i)$. In the case of Hilbert spaces, $K := \left\lceil \frac{512 b^2}{\varepsilon^2} \right\rceil$.

In this way, we provide a finitary version in the sense of T. Tao [9, 10] of the Mean Ergodic Theorem for uniformly convex Banach spaces and so generalize similar results obtained for Hilbert spaces by Avigad, Gerhardy and Towsner [1] and T. Tao [10]. Despite of our result being significantly more general then the Hilbert space case treated in [1], the extraction of our bound is considerably more easy compared to [1] and even numerically better.

The second application is in metric fixed point theory, more specifically in the approximate fixed point theory of asymptotically nonexpansive mappings, introduced in [3].

One typical result is the following theorem which is otained in [6, Corollary 8] as corollary of a quantitative result.

Theorem. *Let $(X, \|\cdot\|)$ be a uniformly convex normed space, $C \subseteq X$ a convex subset and $T : C \to C$ an asymptotically nonexpansive mapping with sequence (k_n) in $[0, \infty)$ satisfying $\sum_{i=0}^{\infty} k_i < \infty$. Let (λ_n) be a sequence in $[a, b]$ for $0 < a < b < 1$ and define the Krasnoselski-Mann iteration of T starting from $x \in X$ by*

$$x_0 := x, \;\; x_{n+1} := (1 - \lambda_n) x_n + \lambda_n T^n(x_n).$$

If T has a fixed point, then $d(x_n, T(x_n)) \overset{n \to \infty}{\to} 0$.

While there does not seem to exist a computable rate of convergence (see the discussion in[6]), the general logical metatheorems from [4] guarantee an effective bound on the $\exists N$ in the Herbrand normal form of the convergence of $(\|x_n - T(x_n)\|)$

towards 0:

$$(2) \qquad \forall \varepsilon > 0 \, \forall g : \mathbb{N} \to \mathbb{N} \, \exists N \in \mathbb{N} \, \forall m \in [N, N + g(N)] \, (\|x_m - T(x_m)\| < \varepsilon).$$

Such a bound was extracted in [6, Theorem 22]. In [7] we take the proofs from [6] as our point of departure and generalize the results to uniformly convex hyperbolic spaces. This, in particular, covers the important class of CAT(0)-spaces (in the sense of Gromov) and, a-fortiorily, $\mathbb{R}$-trees in the sense of Tits. For CAT(0)-spaces we get a quadratic bound on the approximate fixed point property of (x_n).

References

[1] J. Avigad, P. Gerhardy, H. Towsner. Local stability of ergodic averages. `arXiv:0706.1512v2`, 2007.

[2] G. Birkhoff. The mean ergodic theorem. *Duke Math. J.* 5(1) (1939), 19–20.

[3] K. Goebel, W. A. Kirk. A fixed point theorem for asymptotically nonexpansive mappings. Proc. Amer. Math. Soc. 35 (1972), 171–174.

[4] U. Kohlenbach. Some logical metatheorems with application in functional analysis. *Trans. Am. Math. Soc.* 357 (2005), 89-128.

[5] ———. Applied Proof Theory: Proof Interpretations and their Use in Mathematics. Springer Monographs in Mathematics, Springer Verlag, Berlin-Heidelberg, 2008. xix+532pp.

[6] U. Kohlenbach, B. Lambov. Bounds on iterations of asymptotically quasi-nonexpansive mappings. In: J. Garcia Falset, E. Llorens Fuster, B. Sims (eds.), *International Conference on Fixed Point Theory and Applications (Valencia, 2003)*, 143–172, Yokohama Publ., Yokohama, 2004.

[7] U. Kohlenbach, L. Leuştean. Asymptotically nonexpansive mappings in uniformly convex hyperbolic spaces. `arXiv:0707.1626v2`, 2007. To appear in *J. of the European Math. Soc.*

[8] ———A quantitative Mean Ergodic Theorem for uniformly convex Banach spaces. `arXiv:0804.3844v1`, 2008.

[9] T. Tao. Soft analysis, hard analysis, and the finite convergence principle. Essay posted May 23, 2007. Available at `http://terrytao.wordpress.com/2007/05/23/soft-analysis-hard-analysis-and-the-finite-convergence-principle/`.

[10] T. Tao. Norm convergence of multiple ergodic averages for commuting transformations. `arXiv:0707.1117v1`, 2007. To appear in *Ergodic Theory and Dynamical Systems.*

Remarks on Constructive Set Theory

Rosalie Iemhoff

In this talk we study two techniques which first appeared in the context of Heyting Arithmetic. The first is an analogue of the Friedman translation, which translates Heyting Arithmetic into itself using a formula that is fixed in advance. In the case of Heyting Arithmetic the translation is simple: to every atomic formula the translating formula is added as a disjunct. One can then easily see that the derivability of a formula implies the derivability of its translation. This technique allows one to prove the admissibility, in Heyting Arithmetic, of certain rules, for example the Harrop rule and the Markov rule.

For Constructive Set Theory the Friedman translation does not apply due to the fact that the extensionality axiom becomes unprovable under this translation. The translation for Constructive Set Theory that we introduce here is more complicated and resembles the treatment of the extensionality axiom in the realizability

interpretation of Michael Rathjen and in classical forcing in set theory. Again, derivability is preserved under the translation, and from this the admissibility of certain rules follow.

In the second part of the talk we introduce a technique to build models of Constructive Set Theory in which Strong Collection is restricted to bounded formulas. Given any finite frame we let the domains at the leaves be models of classical set theory that contain the (unrelativized) class of constructible sets L. In all the nodes that are not leaves we let the domain consist of the constructible sets. Atomic formulas are interpreted as in the models. It follows from this technique that the propositional logic of Constructive Set Theory in which Strong Collection is restricted to bounded formulas is intuitionistic propositional logic.

Unavoidable Sequences in Constructive Analysis

Joan R. Moschovakis

Kleene's formalization of intuitionistic analysis **FIM** (Kleene and Vesley [1965]) includes bar induction, countable and continuous choice, but cannot prove that the constructive arithmetical hierarchy is proper. Veldman showed that in **FIM** the constructive analytical hierarchy collapses at Σ^1_2. These are serious obstructions to interpreting the constructive content of classical analysis, just as the collapse of the arithmetical hierarchy at Σ^0_3 in $\mathbf{HA} + \mathrm{MP}_0 + \mathrm{ECT}_0$ limits the scope and effectiveness of recursive analysis.

Brouwer and Bishop agreed that constructive mathematics was an intellectual work in progress. Bishop and Markov agreed on the primary role of computation. Brouwer and Markov agreed on the importance of continuity. Their insights can be implemented as *admissible rules* for constructive formal systems which may be compatible with larger parts of classical mathematics.[1]

We work in a two-sorted language $\mathcal{L}$ with variables over numbers and one-place number-theoretic functions (*choice sequences*). Our base theory **M** is the minimal theory used by Kleene [1969] to formalize the theory of recursive partial functionals, function realizability and q-realizability. **M** extends Heyting arithmetic to the two-sorted language and includes primitive recursive definitions for the function constants, a λ-reduction schema, and the function-comprehension schema $\forall \mathrm{x} \exists! \mathrm{y} \mathrm{A}(\mathrm{x}, \mathrm{y}) \to \exists \alpha \forall \mathrm{x} \mathrm{A}(\mathrm{x}, \alpha(\mathrm{x}))$.

An *$\mathcal{L}$-theory* is a consistent axiomatic extension of **M** in the language $\mathcal{L}$ (possibly enriched by additional primitive recursive function constants). An $\mathcal{L}$-theory may be *intuitionistic*, *classical* or *intermediate* depending on its underlying logic.

The $\mathcal{L}$-theories which have been proposed so far to express parts of constructive mathematics typically have one or more of the following properties. An *explicit* $\mathcal{L}$-theory **T** provides explicit witnesses for existential theorems:

(1) If $\exists \mathrm{x} \mathrm{A}(\mathrm{x})$ is closed and $\vdash_{\mathbf{T}} \exists \mathrm{x} \mathrm{A}(\mathrm{x})$ then $\vdash_{\mathbf{T}} \mathrm{A}(\mathbf{n})$ for some numeral $\mathbf{n}$.

[1] Kohlenbach's "proof mining" implicitly uses this idea to extract constructive information from classical proofs.

(2) If $\exists\alpha \mathrm{A}(\alpha)$ is closed and $\vdash_{\mathbf{T}} \exists\alpha \mathrm{A}(\alpha)$, then for some $\mathrm{B}(\alpha)$ with only α free:
$$\vdash_{\mathbf{T}} \forall\alpha[\mathrm{B}(\alpha) \to \mathrm{A}(\alpha)] \;\&\; \exists!\alpha \mathrm{B}(\alpha).$$

A *Brouwerian* $\mathcal{L}$-theory $\mathbf{T}$ satisfies *Brouwer's Rule*:

"If $\vdash_{\mathbf{T}} \forall\alpha\exists\beta \mathrm{A}(\alpha,\beta)$ then $\vdash_{\mathbf{T}} \exists\sigma\forall\alpha[\forall \mathrm{x}\exists \mathrm{y}(\{\sigma\}[\alpha](\mathrm{x}) \simeq \mathrm{y}) \;\&\; \mathrm{A}(\alpha,\{\sigma\}[\alpha])]$."

A *recursively acceptable* $\mathcal{L}$-theory $\mathbf{T}$ satisfies *Markov's Rule*:

"If $\vdash_{\mathbf{T}} \neg\neg\exists \mathrm{x}\mathrm{A}(\mathrm{x}) \;\&\; \forall \mathrm{x}[\mathrm{A}(\mathrm{x}) \vee \neg\mathrm{A}(\mathrm{x})]$ then $\vdash_{\mathbf{T}} \exists \mathrm{x}\mathrm{A}(\mathrm{x})$"

and *Church's Rule*:

"If $\vdash_{\mathbf{T}} \exists\alpha \mathrm{A}(\alpha)$ with $\exists\alpha \mathrm{A}(\alpha)$ closed, then
$$\vdash_{\mathbf{T}} \exists \mathrm{e}[\forall \mathrm{x}\exists!\mathrm{y}\mathrm{T}(\mathrm{e},\mathrm{x},\mathrm{y}) \;\&\; \forall\alpha[\forall \mathrm{x}\forall \mathrm{y}[\mathrm{T}(\mathrm{e},\mathrm{x},\mathrm{y}) \to \alpha(\mathrm{x}) = \mathrm{U}(\mathrm{y})] \to \mathrm{A}(\alpha)]]$$."

A recursively acceptable, explicit theory $\mathbf{T}$ also satisfies the *Church-Kleene Rule*:

"If $\vdash_{\mathbf{T}} \exists\alpha \mathrm{A}(\alpha)$ where $\exists\alpha \mathrm{A}(\alpha)$ is closed, then for a suitable number e:
$$\vdash_{\mathbf{T}} \exists\alpha[\forall \mathrm{x}(\alpha(\mathrm{x}) \simeq \{\mathbf{e}\}(\mathrm{x})) \;\&\; \mathrm{A}(\alpha)]."$$

Definition. If $\mathbf{T}$ is an $\mathcal{L}$-theory and $\mathrm{A}(\mathrm{x},\mathrm{y})$ a formula (perhaps with other free variables of both sorts) such that $\vdash_{\mathbf{T}} \forall \mathrm{x}\neg\neg\exists!\mathrm{y}\mathrm{A}(\mathrm{x},\mathrm{y})$ (equivalently, such that $\vdash_{\mathbf{T}} \forall \mathrm{x}\forall \mathrm{y}\forall \mathrm{z}[\mathrm{A}(\mathrm{x},\mathrm{y}) \;\&\; \mathrm{A}(\mathrm{x},\mathrm{z}) \to \mathrm{y} = \mathrm{z}]$ and $\vdash_{\mathbf{T}} \forall \mathrm{x}\neg\neg\exists \mathrm{y}\mathrm{A}(\mathrm{x},\mathrm{y})$), we say that $\mathrm{A}(\mathrm{x},\mathrm{y})$ *classically defines an infinite sequence in* $\mathbf{T}$ (*from* the other free variables, if any).

Proposition. If $\mathbf{T}$ is an $\mathcal{L}$-theory extending $\mathbf{M}$ and $\vdash_{\mathbf{T}} \neg\neg\exists!\alpha\forall \mathrm{x}\mathrm{A}(\mathrm{x},\alpha(\mathrm{x}))$, then $\mathrm{A}(\mathrm{x},\mathrm{y})$ classically defines an infinite sequence in $\mathbf{T}$.

Proof. From $\neg\neg\exists!\alpha\forall \mathrm{x}\mathrm{A}(\mathrm{x},\alpha(\mathrm{x}))$ follow $\neg\neg\forall \mathrm{x}\forall \mathrm{y}\forall \mathrm{z}[\mathrm{A}(\mathrm{x},\mathrm{y}) \;\&\; \mathrm{A}(\mathrm{x},\mathrm{z}) \to \mathrm{y} = \mathrm{z}]$ and $\neg\neg\forall \mathrm{x}\exists \mathrm{y}\mathrm{A}(\mathrm{x},\mathrm{y})$, so $\forall \mathrm{x}\forall \mathrm{y}\forall \mathrm{z}[\mathrm{A}(\mathrm{x},\mathrm{y}) \;\&\; \mathrm{A}(\mathrm{x},\mathrm{z}) \to \mathrm{y} = \mathrm{z}]$ and $\forall \mathrm{x}\neg\neg\exists \mathrm{y}\mathrm{A}(\mathrm{x},\mathrm{y})$ by intuitionistic logic with the stability of number-theoretic equality.

Remarks:

(1) The converse fails. Let $\mathrm{A}(\mathrm{x},\mathrm{y})$ be $\mathrm{y} \leq 1 \,\&\, [\mathrm{y} = 0 \leftrightarrow \forall \mathrm{z}\neg\mathrm{T}(\mathrm{x},\mathrm{x},\mathrm{z})]$. Then $\mathrm{A}(\mathrm{x},\mathrm{y})$ classically defines an infinite sequence in $\mathbf{M}$ but $\neg\neg\exists\alpha\forall \mathrm{x}\mathrm{A}(\mathrm{x},\alpha(\mathrm{x}))$ contradicts weak Church's Thesis $\forall\alpha\neg\neg\exists \mathrm{e}\forall \mathrm{x}\exists \mathrm{y}[\mathrm{T}(\mathrm{e},\mathrm{x},\mathrm{y}) \;\&\; \mathrm{U}(\mathrm{y}) = \alpha(\mathrm{x})]$, which is consistent with $\mathbf{M}$ and even with **FIM**.

(2) $\mathrm{A}(\mathrm{x},\mathrm{y})$ classically defines an infinite sequence in $\mathbf{T}$ if and only if $\neg\neg\mathrm{A}(\mathrm{x},\mathrm{y})$ classically defines an infinite sequence in $\mathbf{T}$.

(3) If $\mathrm{A}(\mathrm{x},\mathrm{y})$ classically defines an infinite sequence in $\mathbf{T}$ and α is a choice sequence such that $\forall x A(x,\alpha(x))$ holds under an interpretation $\mathcal{I}$ of $\mathbf{T}$, we may say that α is classically defined by $\mathrm{A}(\mathrm{x},\mathrm{y})$ under the interpretation.

(4) If $\mathbf{T}$ is Brouwerian and $\vdash_{\mathbf{T}} \neg\neg\exists!\alpha\mathrm{A}(\alpha)$ then $\nvdash_{\mathbf{T}} \forall\alpha[\mathrm{A}(\alpha) \vee \neg\mathrm{A}(\alpha)]$.

(5) $\vdash_{\mathbf{M}} \exists!\mathrm{x}\mathrm{A}(\mathrm{x}) \to \forall \mathrm{x}(\mathrm{A}(\mathrm{x}) \vee \neg\mathrm{A}(\mathrm{x}))$.

(6) $\vdash_{\mathbf{FIM}} \neg\neg\exists!\alpha\mathrm{A}(\alpha) \to \neg\forall\alpha[\mathrm{A}(\alpha) \vee \neg\mathrm{A}(\alpha)]$.

Definition. If $\mathbf{T}$ is an $\mathcal{L}$-theory and $\vdash_{\mathbf{T}} \neg\neg\exists!\alpha\mathrm{A}(\alpha)$, then the sequence α classically defined by $\forall\beta[\mathrm{A}(\beta) \to \beta(\mathrm{x}) = \mathrm{y}]$ under any interpretation of $\mathbf{T}$ will be called *unavoidable over* $\mathbf{T}$.

Only classically recursive sequences are unavoidable over **FIM**; but the characteristic functions of all arithmetical relations (with or without sequence parameters) and of all classically Δ^1_1 relations are unavoidable over the Brouwerian, recursively acceptable $\mathcal{L}$-theory $\mathbf{T}_1 = \mathbf{M} + \mathrm{BI}_1 + \mathrm{MP}_1$ which proves the constructive arithmetical hierarchy is proper. Here BI_1 is a bar induction schema and MP_1 is the strong analytic form $\forall\alpha[\neg\neg\exists \mathrm{x}\alpha(\mathrm{x}) = 0 \to \exists \mathrm{x}\alpha(\mathrm{x}) = 0]$ of Markov's Principle.

We are interested in the general question of determining all the unavoidable sequences over an arbitrary constructive $\mathcal{L}$-theory including bar induction, e.g.:

Theorem. There is a Brouwerian theory $\mathbf{T}_2$ which extends **FIM** and proves

(i) $\neg\neg\forall$x[A(x) $\vee$ $\neg$A(x)] for arithmetical A(x) with parameters allowed (e.g. $\forall\rho\neg\neg\forall$x[$\exists$y$\rho(<$ x, y $>) = 0 \vee \forall$y$\rho(<$ x, y $>) \neq 0$]), and so the characteristic function of $A(x)$ is unavoidable over $\mathbf{T}_1$:

$$\neg\neg\exists!\alpha\forall\text{x}[\alpha(\text{x}) \leq 1 \;\&\; (\alpha(\text{x}) = 0 \leftrightarrow \text{A(x)})].$$

(ii) "There are no sequences which are not classically Σ^1_1":

$$\forall\alpha\neg\neg\exists e\forall x\forall y[\alpha(x) = y \leftrightarrow \neg\neg\exists\beta\forall z\neg T(e, x, y, \overline{\beta}(z))].$$

(iii) "Every Π^1_1 sequence is unavoidable":

$$\forall\text{e}[\forall\text{x}\neg\neg\exists!\text{y}\forall\beta\exists\text{z}\text{T}(\text{e}, \text{x}, \text{y}, \overline{\beta}(\text{z})) \rightarrow \neg\neg\exists\alpha\forall\text{x}\forall\text{y}[\alpha(\text{x}) = \text{y} \leftrightarrow \forall\beta\exists\text{z}\text{T}(\text{e}, \text{x}, \text{y}, \overline{\beta}(\text{z}))]].$$

The consistency proof uses the Spector-Gandy Theorem with a modified special realizability interpretation ($^{\Delta^1_1}$realizability). The model satisfies first-order Peano arithmetic **PA** and Vesley's Schema VS (which refutes MP_1 in **FIM**). We conjecture that $\mathbf{T}_2$ is recursively acceptable.

Sheaf Models for CZF Refuting Powerset and Full Separation

Thomas Streicher
(joint work with Alex Simpson)

We construct some natural sheaf models for CZF which refute both the Full Separation scheme and the Powerset axiom.[1] Models for CZF with the same properties can be obtained by performing realizability model constructions within L_α for an appropriate ordinal α (e.g. ω_1^{CK}).

In the 1980ies M. Hyland and D. Scott showed how to interpret IZF in presheaf toposes $\widehat{\mathbb{C}} = \mathbf{Set}^{\mathbb{C}^{\text{op}}}$ employing the class-valued presheaf

$$V(\mathbb{C}) = \bigcup_{\alpha\in\mathbf{Ord}} V(\mathbb{C})_\alpha \qquad \text{where } V(\mathbb{C})_\alpha = \bigcup_{\beta\in\alpha} \mathcal{P}(V(\mathbb{C})_\beta)$$

with $\mathcal{P}$ the covariant powerset functor in $\widehat{\mathbb{C}}$. This interpretation can be adapted to Grothendieck toposes $\mathsf{Sh}(\mathbb{C}, \mathcal{J})$ by (re)defining the forcing clauses for elementhood and equality as

$I \Vdash a \in b$ iff for some $\mathcal{J}$-cover $(u_j : I_j \to I)_{j\in J}$ for all $j \in J$ there exists a $c \in U(I_j)$ with $\langle u_j, c\rangle \in b$ and $I_j \Vdash c = a{\cdot}u_j$

$I \Vdash a = b$ iff for all $u : J \to I$ and $c \in U(J)$ it holds that
$\langle u, c\rangle \in a$ implies $J \Vdash c \in b{\cdot}u$ and
$\langle u, c\rangle \in b$ implies $J \Vdash c \in a{\cdot}u$

[1] Previously, the second named author, R. Lubarsky and B. van den Berg independently constructed a realizability model for CZF which refutes the Powerset axiom but still validate the Full Separation scheme. This model can most naturally be understood as the *hereditarily subcountable* sets in the Friedman-McCarty realizability model for IZF (see [1]).

by implicit transfinite recursion on the rank of a and b. Notice that the clause for membership implicitly performs the $\mathcal{J}$-closure of $b \subseteq \mathsf{y}(I)\times V(\mathbb{C})$. The forcing clauses for the logical connectives and quantifiers are as usual (see e.g. [3]). One can show that the quotient of $V(\mathbb{C})$ by $=$ (as defined above) gives rise to an initial fixpoint of $\mathcal{P}$ in $\mathsf{Sh}(\mathbb{C},\mathcal{J})$ as considered in [2] where it is shown to provide a model of IZF. Our forcing version, however, is much simpler than Fourman's interpretation in [2] and also much closer to the set theorist's way of thinking.

In order to obtain models for CZF we consider particular sites, namely locally cartesian closed pretoposes $\mathcal{E}$, so-called Π-pretoposes, with stable and disjoint countable sums which we think as endowed with the *countable cover* topology. Let us assume that **Set** is so big that $\mathcal{E}$ is a category internal to **Set**. We will work within the presheaf topos $\widehat{\mathcal{E}} = \mathbf{Set}^{\mathcal{E}^{\mathrm{op}}}$ and define in it a cumulative hierarchy $U(\mathcal{E})$ which is a "miniature version" of the $V(\mathcal{E})$ considered above.

An $X \in \widehat{\mathcal{E}}$ is *countably generated* (c.g.) iff there exists a countable family $\big(x_i \in X(I_i)\big)$ such that for every $x \in X(I)$ there is a map $u : I \to I_i$ in $\mathcal{E}$ with $x = x_i{\cdot}u$. We write $\mathrm{Sub}_{cg}(X)$ for the collection of countably generated subpresheaves of X. For $X \in \widehat{\mathcal{E}}$ let $\mathcal{P}_{cg}(X)$ be the presheaf over $\mathcal{E}$ with

$$\mathcal{P}_{cg}(X)(I) = \mathrm{Sub}_{cg}(\mathsf{y}(I)\times X)$$

for $I \in \mathcal{E}$ and

$$S{\cdot}u = \{(v,x) \mid (uv,x) \in S\}$$

for $u : J \to I$ in $\mathcal{E}$ and $S \in \mathcal{P}_{cg}(X)(I)$. Now we define

$$U(\mathcal{E}) = \bigcup_{\alpha\in\mathbf{Ord}} U(\mathcal{E})_\alpha \qquad \text{where } U(\mathcal{E})_\alpha = \bigcup_{\beta\in\alpha} \mathcal{P}_{cg}(U(\mathcal{E})_\beta)$$

Since $U(\mathcal{E})$ is defined inductively by rules which all have only countably many premisses we get that $U(\mathcal{E}) = U(\mathcal{E})_{\omega_1}$ is the least fixpoint of $\mathcal{P}_{cg}$. One can show that

Theorem 1
For every Π-pretopos $\mathcal{E}$ with stable and disjoint countable sums in $U(\mathcal{E})$ all axioms of $\mathrm{CZF}_{\mathrm{Exp}}$ are forced[2]. If $\mathcal{E}$ validates also the type-theoretical fullness axiom then in $U(\mathcal{E})$ all axioms of CZF are forced.

Intuitively, the type-theoretical fullness axioms says that (in every context) for all types A and B there exists a type C and a C-indexed family $(R_c)_{c\in C}$ of total relations from A to B such that for every total relation S from A to B there is a $c \in C$ with $R_c \subseteq S$.

A typical example of such a Π-pretopos is $(\omega\mathrm{Top}_0)_{\mathrm{ex/reg}}$, the ex/reg completion of the category $\omega\mathrm{Top}_0$ of countably based T_0-spaces, which is not a topos. Other examples in this vein are $\mathsf{Mod}(\mathcal{A})_{\mathrm{ex/reg}}$ where $\mathcal{A}$ is the partial combinatory algebra $\mathcal{P}\omega$ (Scott's graph model) or the second Kleene algebra K_2 (Baire space) employed in function realizability.[3]

[2] $\mathrm{CZF}_{\mathrm{Exp}}$ is obtained from CZF replacing the fullness axiom by the exponentiation axiom.
[3] $\mathsf{Mod}(\mathcal{A})$ stands for the category of modest sets over the partial combinatory algebra $\mathcal{A}$.

Theorem 2
For every Π-pretopos $\mathcal{E}$ with stable and disjoint countable sums the model $U(\mathcal{E})$ does not validate the Full Separation scheme.

Proof (Idea) : With every (external) countable ordinal α one may associate a global element $\widehat{\alpha}$ of $U(\mathcal{E})$ such that $\widehat{\alpha} \notin U(\mathcal{E})_\alpha$. One can show that in $U(\mathcal{E})$ Brouwer's Second Number Class W_1 can be defined as subclass of the set $\omega^{(\omega^\omega)}$. If Full Separation held in $U(\mathcal{E})$ then W_1 were a set from which it follows that there exists a set containing all $\widehat{\alpha}$ as elements. Contradiction!

One can show that $U(\mathcal{E})$ validates the Powerset axiom iff $\mathcal{E}$ is a topos. Using this observation we obtain the following independence results.

Theorem 3
If $\mathcal{E}$ is a Grothendieck topos then $U(\mathcal{E})$ validates the Powerset axiom but not Full Separation schema.
If $\mathcal{E}$ is a Π-pretopos with stable and disjoint countable sums but not a topos then $U(\mathcal{E})$ refutes both the Powerset axiom and the Full Separation scheme. Typical examples of such $\mathcal{E}$ are $(\omega\mathrm{Top}_0)_{\mathrm{ex/reg}}$, $\mathsf{Mod}(\mathcal{P}\omega)_{\mathrm{ex/reg}}$ and $\mathsf{Mod}(K_2)_{\mathrm{ex/reg}}$.

References

[1] B. van den Berg. Predicative Topos Theory and Models of Constructive Set Theory PhD Thesis, Univ. Utrecht, 2006.
[2] M. Fourman Sheaf models for set theory *Journal of Pure and Applied Algebra* 19 (1980), 91-101.
[3] S. MacLane, I. Moerdijk Sheaves in Geometry and Logic. A First Introduction to Topos Theory. Springer, 1992.

Recent Aspects of Mass Problems: Symbolic Dynamics and Intuitionism

Stephen G. Simpson

Mass Problems. A set $P \subseteq \{0,1\}^{\mathbb{N}}$ may be viewed as a *mass problem*, i.e., a decision problem with more than one solution. By definition, the *solutions* of P are the elements of P. A mass problem is said to be *solvable* if at least one of its solutions is recursive. A mass problem P is said to be *weakly reducible* to a mass problem Q if for each solution of Q there exists a solution of P which is Turing reducible to the given solution of Q. A *weak degree* is an equivalence class of mass problems under mutual weak reducibility. The lattice $\mathcal{D}_w$ of all weak degrees is due to Muchnik 1963. There is an obvious embedding of the Turing degrees into $\mathcal{D}_w$.

A set $P \subseteq \{0,1\}^{\mathbb{N}}$ is said to be Π^0_1 if it is *effectively closed*, i.e., it is the complement of the union of a recursive sequence of basic open sets. Let $\mathcal{P}_w$ denote the sublattice of $\mathcal{D}_w$ consisting of the mass problems associated with nonempty Π^0_1 subsets of $\{0,1\}^{\mathbb{N}}$. The lattice $\mathcal{P}_w$ has been investigated by Simpson and his collaborators. There is a non-obvious but natural embedding of the recursively

enumerable Turing degrees into $\mathcal{P}_w$. It is known that $\mathcal{P}_w$ contains many specific, natural weak degrees which are related to various topics in the foundations of mathematics. Among these topics are reverse mathematics, algorithmic randomness, Kolmogorov complexity, almost everywhere domination, hyperarithmeticity, effective Hausdorff dimension, resource-bounded computational complexity, and subrecursive hierarchies.

Symbolic Dynamics. Let A be a finite set of symbols. The *full two-dimensional shift* on A is the dynamical system consisting of the natural action of the group $\mathbb{Z} \times \mathbb{Z}$ on the compact space $A^{\mathbb{Z}\times\mathbb{Z}}$. A *two-dimensional subshift* is a nonempty closed subset of $A^{\mathbb{Z}\times\mathbb{Z}}$ which is invariant under the action of $\mathbb{Z} \times \mathbb{Z}$. A two-dimensional subshift is said to be *of finite type* if it is defined by a finite set of excluded configurations. The two-dimensional subshifts of finite type are known to form an important class of dynamical systems, with connections to mathematical physics, etc.

Clearly every two-dimensional subshift of finite type is a nonempty Π^0_1 subset of $A^{\mathbb{Z}\times\mathbb{Z}}$, hence its weak degree belongs to $\mathcal{P}_w$. Conversely, we prove that every weak degree in $\mathcal{P}_w$ is the weak degree of a two-dimensional subshift of finite type. The proof of this result uses tilings of the plane. We present an application of this result to symbolic dynamics. Namely, we obtain an infinite family of two-dimensional subshifts of finite type which are, in a certain sense, mutually incompatible. Our application is stated purely in terms of two-dimensional subshifts of finite type, with no mention of weak degrees.

Intuitionism. Historically, the study of mass problems originated from intuitionistic considerations. Kolmogorov 1932 proposed to view intuitionism as a "calculus of problems." Muchnik 1963 introduced weak degrees as a rigorous elaboration of Kolmogorov's proposal. As noted by Muchnik, the lattice $\mathcal{D}_w$ of all weak degrees is Brouwerian.

The question arises, is the sublattice $\mathcal{P}_w$ Brouwerian? We prove that it is not. The proof uses our adaptation of a technique of Posner and Robinson.

References

[1] S. Binns, S. G. Simpson. Embeddings into the Medvedev and Muchnik lattices of Π^0_1 classes, *Archive for Math. Logic*, 43 (2004), 399–414.

[2] J. A. Cole and S. G. Simpson. Mass problems and hyperarithmeticity, 20 pages, 2006, to appear in *Journal of Mathematical Logic*.

[3] A. N. Kolmogorov, Zur Deutung der intuitionistischen Logik, *Mathematische Zeitschrift*, 35 (1932), 58–65.

[4] A. A. Muchnik. On strong and weak reducibilities of algorithmic problems, *Sibirskii Matematicheskii Zhurnal*, 4, 1963, 1328–1341, in Russian.

[5] D .B. Posner, R. W. Robinson. Degrees joining to $0'$, *Journal of Symbolic Logic*, 46 (1981), 714–722.

[6] S. G. Simpson. Mass problems and randomness, *Bulletin of Symbolic Logic*, 11 (2005), 1–27.

[7] ———. An extension of the recursively enumerable Turing degrees, *Journal of the London Mathematical Society*, 75 (2007), 287–297.

[8] ———. Mass problems and almost everywhere domination, *Mathematical Logic Quarterly*, 53 (2007), 483–492.

[9] ———. Mass problems and intuitionism, 9 pages, 2007, *Notre Dame Journal of Formal Logic*, 49, 2008, 127–136.
[10] ———. Medvedev degrees of 2-dimensional subshifts of finite type, 8 pages, 2007, *Ergodic Theory and Dynamical Systems*, to appear.

Programming with and Reasoning about a Monad of Lambda Terms that has Explicit Monad Multiplication

Ralph Matthes

Untyped lambda-calculus modulo alpha-equivalence can be represented in many ways. One of them is a typeful de Bruijn representation that keeps track of the set of possibly freely occurring variables in form of a type parameter. This is an instance of an inductive family, also called nested datatype [4]. The representation has been proposed in 1999 by Altenkirch & Reus [2], and, independently, by Bird & Paterson [5]. It allows to express monad multiplication directly (first studied for lambda-calculus in [3]). To recall, monad multiplication is an alternative view to parallel substitution that amounts to the Kleisli extension operation.

As is done successfully with substitution in the form of explicit substitution, one can turn monad multiplication itself into a formal object of study, yielding "explicit monad multiplication". In the case of lambda-calculus, monad multiplication is flattening: there, free variable occurrences are themselves terms, and these terms are integrated into the ambient lambda term. A suggestive example would be a term that corresponds to $\lambda y.\, y\,\{\lambda z.\, z\, x_1\}\,\{x_2\}$, where the terms $\lambda z.\, z\, x_1$ and x_2 are considered as names of variables and hence the whole term as a lambda abstraction over y of the application of the variable y to two variables as arguments. Flattening yields the (here trivial) term $\lambda y.\, y\,(\lambda z.\, z\, x_1)\, x_2$. But recall that, in general, substitution can be defined from renaming and flattening.

The nested datatype that can represent this extension is truly nested and as such not directly supported by any type-theoretic environment that would guarantee the termination of basic algorithms on this data structure.

In collaboration with Andreas Abel and Tarmo Uustalu [1], I have proposed recursion schemes that do have these guarantees and that could be encoded into higher-order polymorphic lambda-calculus. Explicit monad multiplication is thus amenable to decent programming.

The newer developments by myself concerning logics for reasoning about truly nested datatypes form the body of this talk: I developed as an extension of the Calculus of Inductive Constructions (the constructive type theory underlying the Coq theorem prover) the Logic of Natural Mendler-style Iteration *LNMIt* that allows in particular to prove naturality (in the sense of category theory) of functions defined by these recursion schemes, and gave an implementation of *LNMIt* within Coq (assuming impredicative Set and propositional proof irrelevance) [6].

However, *LNMIt* makes an essential use of non-canonical elements that prevent the proof of basic properties such as injectivity of the datatype constructors for application, abstraction and explicit flattening. Through a relativization to hereditarily canonical elements (which are described by an inductive definition), the

problems with non-canonical elements can be overcome and yield a truly nested datatype where exhaustivity and injectivity of the datatype constructors can be proven.

This result has not been presented publicly before (although announced at the TYPES 2008 meeting, but abandoned due to time constraints). The whole proofs exist in form of Coq scripts, and the proof of injectivity of explicit flattening is amazingly complicated at the moment. The crucial auxiliary theorem is a form of injectivity of renaming that becomes difficult to treat with the terms that are seen as variable names.

References

[1] A. Abel, R. Matthes, T. Uustalu. Iteration and coiteration schemes for higher-order and nested datatypes. *Theoretical Computer Science*, 333(1–2) (2005), 3–66.

[2] T. Altenkirch, B. Reus. Monadic presentations of lambda terms using generalized inductive types. In Jörg Flum and Mario Rodríguez-Artalejo, editors, *Computer Science Logic, 13th International Workshop, CSL '99, Proceedings*, volume 1683 of *Lecture Notes in Computer Science*, pages 453–468. Springer Verlag, 1999.

[3] F. Bellegarde, J. Hook. Substitution: A formal methods case study using monads and transformations. *Science of Computer Programming*, 23 (1994), 287–311.

[4] R. Bird, L. Meertens. Nested datatypes. In Johan Jeuring, editor, *Mathematics of Program Construction, MPC'98, Proceedings*, volume 1422 of *Lecture Notes in Computer Science*, pages 52–67. Springer Verlag, 1998.

[5] R. Bird, R. Paterson. De Bruijn notation as a nested datatype. *Journal of Functional Programming*, 9(1) (1991), 77–91.

[6] R. Matthes. An induction principle for nested datatypes in intensional type theory. *Journal of Functional Programming*, 2008. To appear.

Automatic derivation of data structures from computable mathematics

Andrej Bauer

We report on how to use the realizability interpretation of constructive logic to automatically derive specifications from axiomatizations of mathematical theories. For example, the interpretation of the axioms of real numbers, when suitably interpreted, gives a specification for exact real arithmetic.

There are tools which use this idea (or the related idea of propositions-as-types) to automatically extract programs from formal proofs, such as Coq [5] and Minlog [4]. However, more often than not the extracted programs are orders of magnitude slower than hand-written versions, especially when complex mathematical structures are involved. It therefore makes sense to separate extraction of programs into two levels:

(1) Extract *specifications* for data structures and programs from definitions of structures and statements of theorems.
(2) Extract *implementations* of data structures and programs from constructions of structures and formal proofs of theorems.

In joint work with Christopher Stone we developed a tool RZ [2, 3] which performs the first level of extraction automatically. It outputs specifications as signatures in Objective Caml language [7]. The extraction works on "small scale" (specification of data types and values) as well as "large scale" (specification of whole program modules). It uses Objective Caml module system to express a hierachy of mathematical structures and connections between them. RZ performs a number of optimizations and simplifications in order to output readable and useful specifications.

In joint work with Iztok Kavkler [1] we showed that the extracted specifications are actually useful in practice. We implemented exact real numbers Era following a specification produced by RZ. Our implementation approaches the performance of the state-of-the-art implementations of exact real numbers such as RealLib [6] and iRRAM [8].

References

[1] A. Bauer, I. Kavkler. Implementing real numbers with RZ. In Weihrauch, K. and Zhong, N., editors, *Fourth International Conference on Computability and Complexity in Analysis*, Electronic Notes in Theoretical Computer Science, 2007.

[2] A. Bauer, C. Stone. RZ: a tool for bringing constructive and computable mathematics closer to programming practice. In *Computability in Europe 2007*, June 2007. To apear in a special issue of Journal of Logic and Computation.

[3] ———. *RZ*, `http://math.andrej.com/rz/`.

[4] H. Benl, U. Berger, H. Schwichtenberg, M. Seisenberger, W. Zuber. Proof theory at work: Program development in the Minlog system. In Bibel, W., Schmidt, P.H., eds.: Automated Deduction: A Basis for Applications. Volume II, Systems and Implementation Techniques. Kluwer Academic Publishers, Dordrecht (1998)

[5] Y. Bertot, P. Castéran. Interactive Theorem Proving and Program Development. Springer (2004)

[6] B. Lambov. RealLib: An efficient implementation of exact real arithmetic. *Mathematical Structures in Computer Science*, 17:81–98, 2007.

[7] X. Leroy, D. Doligez, J. Garrigue, D. Rémy, J. Vouillon. The Objective Caml system, documentation and user's manual - release 3.08. Technical report, INRIA (July 2004)

[8] N. Müller The iRRAM: Exact arithmetic in C++. In Jens Blanck, Vasco Brattka, and Peter Hertling, editors, *Computability and Complexity in Analysis: 4th International Workshop, CCA 2000 Swansea, UK, September 17, 2000, Selected Papers*, number 2064 in Lecture Notes in Computer Science, pages 222–252. Springer, 2001.

Concrete proofs with abstract objects in modern algebra

Henri Lombardi

The computer algebra system D5

Classical Theorem. Any field $\mathbf{K}$ is contained in an algebraically closed field.
But it is not possible to construct the algebraic closure of an arbitrary computable field.

First classical step. Given any polynomial f of degree $d \geq 1$ in $\mathbf{K}[X]$ there exists a field $\mathbf{L} \supseteq \mathbf{K}$ where f has at least one root.

A possible solution: D5. [4] *Computing dynamically* in a reliable way inside the algebraic closure, ... even if *this object does not exist as a constructive static object*.

The too abstract object "algebraic closure" is replaced by a dynamical object, a concrete one. Excluded middle (or uncertainty) is replaced by: when a problem seems to occur, try the two cases. Zorn's lemma is replaced by: wait and see.

Dynamic evaluation is nothing but lazy evaluation.

In classical mathematics, two algebraic closures of a field $\mathbf{K}$ are isomorphic. In order to capture a constructive equivalent of this theorem, we introduce a Galois variation on D5 [5].

Galois variation

Classical Galois approach. Given any polynomial f of degree $d \geq 1$ in $\mathbf{K}[X]$ there exists a field $\mathbf{L} \supseteq \mathbf{K}$ with $f(X) = \prod_{i=1}^{d}(X - x_i)$ inside $\mathbf{L}[X]$. This field carries some ambiguities, related to the Galois group of the equation.

A possible solution: computing in a reliable way inside the field $\mathbf{L}$ generated by the roots of f, even if, at any step of the computation we don't know the dimension of the $\mathbf{K}$-vector space $\mathbf{L}$. The field $\mathbf{L}$ is represented by the universal splitting algebra $\mathbf{A}$ of the polynomial, with "Galois group" $\mathfrak{S}_n$. Possibly the computations inside $\mathbf{L}$ show us that we have to pass to a quotient algebra, (a Galois quotient of the previous algebra) i.e., to improve the equality relation and to replace $\mathfrak{S}_n$ by a convenient subgroup. I.e., we improve step by step our knowlege of $\mathbf{L}$ without contradicting previous informations about it. At each improvement, we have to make an arbitrary choice (e.g., if the computation shows that the sum of 3 $x_i's$ is zero, we have to say something as: OK, we take x_1, x_2 and x_3).

The isomorphism theorem becomes: *If two computations lead to two Galois quotients* $\mathbf{L}_1$ *and* $\mathbf{L}_2$ *of* $\mathbf{A}$*, then there exists a third one,* $\mathbf{L}_3$ *such that* $\mathbf{L}_1 \simeq \mathbf{L}_3^{r_1}$ *and* $\mathbf{L}_2 \simeq \mathbf{L}_3^{r_2}$. The two distinct informations about $\mathbf{L}$ can be glued together!

Although we compute in a reliable way inside $\mathbf{L}$, our decomposition field $\mathbf{L}$ cannot be defined as a "set" in the Bishop style.

Bishop's sets are static (rigid) objects: we have to say at the beginning what is the meaning of the equality.

In the dynamical context, equality is constructed step after step, in an interactive way. It depends on the computations we need to perform.

Elimination of minimal primes

Reasoning with a generic prime ideal in order to prove some concrete thing is something like:

in order to prove that a ring is trivial, show that it doesn't contain any prime ideal, or equivalently:

"after localisation at a prime ideal the ring becomes trivial",

When rereading the classical proof you construct a finite tree by using the disjunctions

$$x \in \mathfrak{P} \quad \vee \quad x \notin \mathfrak{P}$$

At the leaves of the tree you get comaximal monoids S_i with $1 = 0$ in each localisation $\mathbf{A}_{S_i}$. This implies that $\mathbf{A}$ is trivial.

Let us try to do the samething with minimal primes.

Reasoning with a generic minimal prime in order to prove some concrete thing is something like:
in order to prove that a ring is trivial, show that it doesn't contain any minimal prime ideal, or equivalently:

"after localisation at a minimal prime ideal the ring becomes trivial",

This cannot be captured by an argument using only first order logic. Indeed, localising at a minimal prime gives a zero dimensional local ring. And a zero dimensional local ring is, up to nilpotent elements, a field. So adding the positive diagram of a reduced ring $\mathbf{A}$, the minimal models are not: *the ring* $\mathbf{A}$ *localised at a minimal prime ideal*, but *the field* $\mathrm{K}_{\mathbf{A}}(\mathfrak{P})$ *for any prime ideal* $\mathfrak{P}$.

In order to capture the notion of minimal prime ideal you have to use an infinite disjunction (a disjunction over all elements of the ring: this is **not** captured by an existential quantifier!).

If $\mathfrak{F}$ is the corresponding maximal filter (complement of the minimal prime) here is the infinite disjunction

$$x \in \mathfrak{F} \quad \vee \quad \bigvee_{y \in \mathfrak{F}} xy \text{ nilpotent}$$

In [1], T. Coquand gives a constructive proof of the celebrated Zariski Main Theorem in the generalised version due to Grothendieck. The constructive proof is based on a classical abstract proof by Peskine. A crucial non constructive step in the classical proof uses the localisation at a generic minimal prime in the ring $\mathbf{C} = \mathbf{A}/(\mathbf{A} : \mathbf{B})$ where $\mathbf{A} \subseteq \mathbf{B}$ in order to prove that $\mathbf{A} = \mathbf{B}$. Finding a contradiction when assuming the existence of a minimal prime shows that $\mathbf{C}$ is trivial, so $1 \in (\mathbf{A} : \mathbf{B})$ and $\mathbf{A} = \mathbf{B}$. For rereading this proof in a constructive way there are two possibilities.

The first one is the dynamical rereading of the classical "proof by contradiction" showing that the reduced $\mathbf{C}$ is trivial since it doesn't have a minimal prime, i.e. it doesn't have a localisation which is a field. In the infinite branching tree corresponding to the consideration of this generic minimal prime, we follow the computation in the proof by chosing always the branch "x invertible" (i.e. $x \in \mathfrak{F}$). When the classical computation finds a "contradiction", i.e. $1 = 0$ in the ring $\mathbf{C}[1/(c_1 \dots c_k)]$ we are very happy: it is a positive information saying that $c_k = 0$ in $\mathbf{C}[1/(c_1 \dots c_{k-1})]$. We go back one step ... Following this strategy we get at the end that $1 = 0$ inside $\mathbf{C}$.

The second possible deciphering of the "localisation at an arbitrary minimal prime" uses a constructive substitute to the classical "mysterious" ring

$$\prod_{\mathfrak{P} \in \mathsf{Min}\ \mathbf{A}} \mathbf{A}_{\mathfrak{P}} \ \simeq \ \prod_{\mathfrak{P} \in \mathsf{Min}\ \mathbf{A}} \mathrm{K}_{\mathbf{A}}(\mathfrak{P}) \ \simeq \ \mathrm{Quot}\left(\prod_{\mathfrak{P} \in \mathsf{Min}\ \mathbf{A}} \mathbf{A}/\mathfrak{P} \right)$$

The constructive substitute of $\prod_{\mathfrak{P}\in \mathsf{Min}\ \mathbf{A}} \mathbf{A}/\mathfrak{P}$ is the ring $\mathbf{A}_{\min}$ obtained by inductive iteration of the following construction (where $a \in \mathbf{A}$)

$$(\mathbf{A}, a) \longmapsto \mathbf{A}/\mathrm{Ann}(a) \times \mathbf{A}/\mathrm{Ann}(\mathrm{Ann}(a))$$

The constructive substitute of $\prod_{\mathfrak{P}\in \mathsf{Min}\ \mathbf{A}} \mathbf{A}_{\mathfrak{P}}$ is $\mathrm{Quot}(\mathbf{A}_{\min})$ and can be obtained by inductive iteration of the following construction (where $a \in \mathbf{A}$)

$$(\mathbf{A}, a) \longmapsto \mathbf{A}/\mathrm{Ann}(a) \times \mathbf{A}[1/a]$$

References

[1] T. Coquand. *Zariski Main Theorem.* Preprint (2007)

[2] T. Coquand, H. Lombardi, C. Quitté. Generating non-Noetherian modules constructively. *Manuscripta Mathematica*, 115 (2004), Pages 513-520

[3] T. Coquand, H. Lombardi, C. Quitté. *Dimension de Heitmann des treillis distributifs et des anneaux commutatifs.* Publications mathématiques de Besançon (2006), 51 pages.

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

[5] G. Díaz-Toca, H. Lombardi, C. Quitté L'algèbre de décomposition universelle. *Proceedings du colloque TC2006 (Granada)* 169–184.

[6] L. Español. Constructive Krull dimension of lattices. *Rev. Acad. Cienc. Zaragoza* 37(2) (1982), 5–9.

[7] ———. Dimension of Boolean valued lattices and rings. *Journal of Pure and Applied Algebra* 42(3) (1986), 223–236.

[8] A. Joyal. Le théorème de Chevalley-Tarski. *Cahiers de Topologie et Géometrie Differentielle* (1975).

[9] I. Yengui Making the use of maximal ideals constructive. *Theoretical Computer Science* 392 (2008), 174–178.

Intuitionistic Ramified Type Theory

Erik Palmgren

In this talk we examine the natural interpretation of a ramified type hierarchy into Martin-Löf type theory with an infinite sequence of universes. It is shown that under this interpretation some useful special cases of Russell's reducibility axiom are valid. This is enough to make the type hierarchy usable for development of constructive mathematics. We present a ramified type theory IRTT suitable for this purpose. IRTT allows for all the basic constructions of set theory: products, exponents, quotient sets, disjoint unions, equalisers. Their category-theoretic universal properties can be established.

1. Ramified Type Theory

Russell introduced in his ramified type theory a distinction between different levels of propositions in order to solve logical paradoxes, notably the Liar Paradox and the paradox he found in Frege's system (Russell 1908). A history and a modern reconstruction of Russell's type theory can be found in the article by

Kamareddine, Laan and Nederpelt (2002). To be able to carry out certain mathematical constructions he then introduced the reducibility axiom, which had the effect of making the system impredicative. In this talk we introduce an alternative axiom of reducibility only for functional relations, which in the context of intuitionistic logic does not lead to impredicativity.

We turn to the formal presentation of our theory. The set of *ramified type symbols* $\mathcal{R}$ is inductively defined by the constructions $\mathbf{P}_n(\cdot)$ (nth level power set), $\times$ (products) from basic symbols $\mathbf{1}$ (the one element type) and $\mathbf{N}$ (natural numbers). The *level* of a type symbol A, $\mathrm{lv}(A)$, is defined recursively $\mathrm{lv}(\mathbf{1}) = \mathrm{lv}(\mathbf{N}) = 0$,

$$\mathrm{lv}(A \times B) = \max(\mathrm{lv}(A), \mathrm{lv}(B)), \qquad \mathrm{lv}(\mathbf{P}_n(A)) = \max(n+1, \mathrm{lv}(A)).$$

Our system of *intuitionistic ramified type theory* (IRTT) is based on many-sorted intuitionistic logic. The sorts are the symbols in $\mathcal{R}$. We define simultaneously the set of terms $\mathrm{Term}(A)$ of type $A \in \mathcal{R}$ and the set of formulas of level $k \in \mathbb{N}$, denoted $\mathrm{Form}(k)$.

- For each $A \in \mathcal{R}$ there is a infinite sequence of variables of sort
$$A : \mathsf{v}_0^A, \mathsf{v}_1^A, \mathsf{v}_2^A, \ldots \text{ in } \mathrm{Term}(A);$$
- If $\varphi \in \mathrm{Form}(k)$ and x is a variable in $\mathrm{Term}(A)$, then the set abstraction term $\{x : A \mid \varphi\} \in \mathrm{Term}(\mathbf{P}_k(A))$.
- If $\mathrm{lv}(A) \leq k$ and $a, b \in \mathrm{Term}(A)$, then $(a =_A b) \in \mathrm{Form}(k)$;
- If $a \in \mathrm{Term}(A)$ and $b \in \mathrm{Term}(\mathbf{P}_n(A))$, then $(a \ \epsilon \ b) \in \mathrm{Form}(k)$ for any $k \geq n$;
- $\mathrm{Form}(k)$ is closed under propositional connectives. If $\varphi \in \mathrm{Form}(k)$ and x is a variable in $\mathrm{Term}(A)$ where $\mathrm{lv}(A) \leq k$, then $(\forall x : A)\varphi, (\exists x : A)\varphi \in \mathrm{Form}(k)$.

The axioms of ramified type theory are the following. First there is a group of standard axioms stating that each $=_A$ is an equivalence relation and that operations and predicates respect these equivalence relations. The arithmetical axioms are standard and there is a full induction scheme.

For subsets we have the axiom of extensionality and the defining axiom for comprehension terms:

- $(\forall X, Y : \mathbf{P}_k(A))((\forall z : A)(z \ \epsilon \ X \Leftrightarrow z \ \epsilon \ Y) \Rightarrow X =_{\mathbf{P}_k(A)} Y)$
- $(\forall z : A)(z \ \epsilon \ \{x : A \mid \varphi\} \Leftrightarrow \varphi[z/x])$.

To state the special reducibility axiom, which is the final axiom, we introduce some terminology. Mimicking the terminology in topos logic (Bell 1988) we let a *local set* be a type A together with an element X of some restricted power set $\mathbf{P}_n(A)$ of A. It is thus specified by a triple (A, X, n), where A is the underlying type, X is the propositional function defining the subset of A and n the level of the propositional function. A *map* from (A, X, m) to (B, Y, n) is some $R : \mathbf{P}_k(A \times B)$ which is a functional relation between X and Y.

- **Special reducibility axiom:** For $A, B \in \mathcal{R}$, $m, n \in \mathbb{N}$, we have for $k = \max(\mathrm{lv}(B), m, n)$ that for any $r \in \mathbb{N}$

$$(\forall X : \mathbf{P}_m(A))(\forall Y : \mathbf{P}_n(B))(\forall F : \mathbf{P}_r(A \times B))$$
$$\Big[F \text{ map from } (A, X, m) \text{ to } (B, Y, n) \Rightarrow$$
$$(\exists G : \mathbf{P}_k(A \times B))(\forall z : A \times B)(z \,\epsilon\, F \Leftrightarrow z \,\epsilon\, G)\Big]$$

We may also extend the basic theory IRTT with the principle of Relativized Dependent Choice (RDC).

2. Setoids

As interpreting theory we consider Martin-Löf type theory (Martin-Löf 1984) with an infinite sequence of universes $\mathrm{U}_0 \subseteq \mathrm{U}_1 \subseteq \mathrm{U}_2 \subseteq \cdots$, where also $U_n : U_{n+1}$. This theory $\mathrm{ML}_{<\omega}$ is predicative in the strict sense of Feferman and Schütte and its proof-theoretic ordinal is Γ_0.

Theorem. *IRTT + RDC can be interpreted in Martin-Löf type theory with an infinite sequence of universes.*

We indicate some important ingredients in the proof.

On the propositions-as-types interpretation U_n can be regarded as the type of propositions of level n. A setoid $A = (|A|, =_A)$ *is of index* (m, n), or is an (m, n)-*setoid,* if $|A| : \mathrm{U}_m$ and $=_A : |A| \to |A| \to \mathrm{U}_n$. Let $\Omega_n = (\mathrm{U}_n, \leftrightarrow)$, where equality is logical equivalence. This is an $(n+1, n)$-setoid of index.

Lemma. *If A is an (m, n)-setoid and B is a (k, ℓ)-setoid then function space setoid $B^A = [A \to B]$ has index* $(\max(m, n, k, \ell), \max(m, \ell))$.

The type symbols of $\mathcal{R}$ interpret naturally as an extensional hierarchy of setoids in the theory $\mathrm{ML}_{<\omega}$. Define setoids S^* by recursion on the structure of $S \in \mathcal{R}$: $\mathbf{1}^* = (\mathrm{N}_1, \mathrm{Id}(\mathrm{N}_1, \cdot, \cdot))$, $\mathbf{N}^* = (\mathrm{N}, \mathrm{Id}(\mathrm{N}, \cdot, \cdot))$, $(S \times T)^* = S^* \times T^*$ and

$$\mathbf{P}_k(S)^* = [S^* \to \Omega_k].$$

Lemma. *If $S \in \mathcal{R}$ and $\mathrm{lv}(S) \leq n$, then S^* is an (n, n)-setoid.*

The interpretation $(-)^*$ is now extended according to the standard practice for propositions-as-types interpretations of many-sorted intuitionistic logic. Each formula φ is interpreted as a type φ^*. Each term a of sort A is interpreted as an element a^* of type $|A^*|$.

Lemma. *For $\varphi \in \mathrm{Form}(n)$, the interpretation satisfies $\varphi^* : \mathrm{U}_n$.*

Next we consider the semantic version of a local set. A pair $M = (S_M, \chi_M)$ consisting of S_M, an (m, n)-setoid, and a propositional function $\chi_M \in [S_M \to \Omega_k]$ is called a *local set.* It gives rise to a setoid

$$\widehat{M} = ((\Sigma x : S_M)\chi_M(x), =')$$

where $(x,p) =' (y,q) \iff_{\text{def}} x =_{S_M} y$. This setoid has index $(\max(m,k),n)$. The validity of the special reducibility axiom under the interpretation, is verified by considering the setoids $(\widehat{A^*, X^*})$ and $(\widehat{B^*, Y^*})$ and using the principle of unique choice to show that all maps are respresented as graphs of functions of the setoid $[(\widehat{A^*, X^*}) \to (\widehat{B^*, Y^*})]$. Using Lemma 2 one computes the required level of the power set $\mathbf{P}_k(A \times B)$.

References

[1] J. L. Bell. *Toposes and Local Set Theories.* Oxford 1988.

[2] F. Kamareddine, T. Laan, R. Nederpelt. Types in Logic and Mathematics Before 1940. *Bulletin of Symbolic Logic* 8 (2002), 185 – 245.

[3] P. Martin-Löf. Intuitionistic Type Theory. Notes by Giovanni Sambin of a series of lectures given in Padova 1980. Bibliopolis 1984.

[4] B. Russell. Mathematical Logic as Based on the Theory of Types. *American Journal of Mathematics* 30 (1908), 222 – 262.

Local Constructive Set Theory

Peter Aczel

John Bell, in [5], introduced the notion of a local set theory as a syntactic counterpart to the category theoretic notion of a topos. The core local set theory (LST) is essentially intuitionistic higher order logic, a many sorted predicate logic, allowing the formation of finite product sorts $\alpha_1 \times \cdots \times \alpha_n$ $(n \geq 0)$ and power sorts $\mathcal{P}\alpha$; such a sort being the sort of *sets on* α. Comprehension terms $\{x : \alpha \mid \phi(x)\}$ of sort $\mathcal{P}\alpha$ can be formed as set terms on α whenever $\phi(x)$ is a formula, which may involve free occurences of a variable x of sort α. So LST is thoroughly impredicative.

The aim of my talk was to introduce local constructive set theory (LCST), a theory intended as a convenient setting for the development of extensional constructive mathematics. It can be viewed as a predicative version of LST. It has the same sort structure as LST and also uses intuitionistic logic, but in order to be predicative a distinction is made between classes and sets on a sort α. Classes on α are given by the comprehension expressions $\{x : \alpha \mid \phi(x)\}$ as in LST. But these expressions are not terms of sort $\mathcal{P}\alpha$, this sort still being the sort of sets on α. Instead the theory LCST needs to have set existence axioms and schemes. The axioms and schemes of set existence for the core LCST are based on those used to formulate CZF, a formal system for constructive set theory, [4]. So there are the axioms of pairing, union, infinity and the schemes of restricted separation, strong collection and subset collection. The infinity axiom is formulated using a basic sort of natural numbers satisfying the usual Peano axioms.

I claim that this core LCST is adequate for the extensional development of that part of elementary predicative constructive mathematics that does not use countable or dependent choices so as to be compatible with topos mathematics. In particular this includes the development of the Dedekind reals as a set, with a field structure that has a categorical axiomatisation.

The core LCST has an obvious interpretation in CZF that only uses the sets of CZF of finite rank above the set ω of von Neumann natural numbers. It also has an interpretation in Martin-Löf's constructive type theory using the same treatment of the notion of *set of* as I gave in my type theoretic interpretation of CZF, [1, 2, 3]. So a *set of* elements of a type A is given as a function $f : I \to A$ whose domain I is a small type, the $f(i)$, for $i \in I$, representing the elements of the set. The type theoretic interpretation of CZF uses an inductive type V whose introduction rule requires that any *set of* elements of V determines an element of V. For the interpretation of core LCST no inductive type is needed. For this reason I consider that core LCST has a more perspicuous constructive foundation than CZF and so may be a more suitable setting for elementary constructive mathematics.

References

[1] P. Aczel. The type theoretic interpretation of constructive set theory. In MacIntyre, A. and Pacholski, L. and Paris, J, editor, *Logic Colloquium '77*, Amsterdam, 1978. North Holland.

[2] P. Aczel. The type theoretic interpretation of constructive set theory: Choice principles. In S.S. Troelstra and D. van Dalen, editors, *The L.E.J. Brouwer Centenary Symposium*, Amsterdam, 1982. North Holland.

[3] P. Aczel. The type theoretic interpretation of constructive set theory: Inductive definitions. In R.B. et al. Marcus, editor, *Logic, Methodology and Philosophy of Science VII*, Amsterdam, 1986. North Holland.

[4] P. Aczel and M. Rathjen. *Notes on Constructive Set Theory,* Mittag-Leffler Technical Report No.40, 2000/2001. `http://www.ml.kva.se/preprints/meta/AczelMon_Sep_24_09_16_56.rdf.html`

[5] J. Bell. *Toposes and Local Set Theories: An Introduction.* Clarendon Press, Oxford, 1988. Reprinted by Dover, 2008.

Reporter: Klaus Aehlig

Participants

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

Dr. Klaus Aehlig
Dept. of Computer Science
Swansea University
Singleton Park
GB-Swansea SA2 8PP

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

Dr. Matthias Baaz
Institut für Algebra und
Diskrete Mathematik
Technische Universität Wien
Wiedner Hauptstraße 8 - 10
A-1040 Wien

Dr. Andrej Bauer
IMFM
Jadranska 19
1000 Ljubljana
Slovenia

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

Prof. Dr. Michael Beeson
Dept. of Computer Science
San Jose State University
214 MacQuarrie Hall
San Jose CA 95192-0103
USA

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

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

Dr. Andrey I. Bovykin
Department of Mathematics
University of Bristol
University Walk
GB-Bristol BS8 1TW

Eyvind Briseid
Fachbereich Mathematik
TU Darmstadt
Schloßgartenstr. 7
64289 Darmstadt

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

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

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

Prof. Dr. Charles N. Delzell
Dept. of Mathematics
Louisiana State University
Baton Rouge LA 70803-4918
USA

Patricia Engracia
Department of Mathematics
University of Lisboa
R. Ernesto Vasconcelos B1
C1-Piso 3
P-1700 Lisboa Codex

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

Dr. Philipp Gerhardy
Department of Mathematics
University of Oslo
P. O. Box 1053 - Blindern
N-0316 Oslo

Prof. Dr. Martin Hofmann
Institut für Informatik
Ludwig-Maximilians-Universität
München (LMU)
Oettingenstr. 67
80538 München

Prof. Dr. Pavel Hrubes
Mathematical Institute
ASCR
Zitna 25
115 67 Praha 1
Czech Republic

Dr. J.Martin E. Hyland
Dept. of Pure Mathematics and
Mathematical Statistics
University of Cambridge
Wilberforce Road
GB-Cambridge CB3 0WB

Dr. Rosalie Iemhoff
Faculty of Philosophy
Utrecht University
Heidelberglaan 8
NL-3584 CS Utrecht

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

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

Dr. Antonina Kolokolova
School of Computing Science
Simon Fraser University
8888 University Drive
Burnaby, B.C. V5A 1S6
CANADA

Prof. Dr. Jan Krajicek
Mathematical Institute
ASCR
Zitna 25
115 67 Praha 1
Czech Republic

Dr. Laurentiu Leustean
Fachbereich Mathematik
TU Darmstadt
Schloßgartenstr. 7
64289 Darmstadt

Prof. Dr. Henri Lombardi
Laboratoire de Mathematiques
Universite de Franche-Comte
16, Route de Gray
F-25030 Besancon Cedex

Dr. Ralph Matthes
IRIT
Universite Paul Sabatier
Equipe ACADIE
118 route de Narbonne
F-31062 Toulouse Cedex 9

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

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

Prof. Dr. Paulo Oliva
Department of Computer Science
Queen Mary, University of London
Mile End Road
GB-London E1 4NS

Prof. Dr. Erik Palmgren
Matematiska institutionen
Uppsala Universitet
Box 480
S-751 06 Uppsala

Prof. Dr. Peter Paule
Research Institute for Symbolic
Computation (RISC)
Johannes Kepler Universität
Altenberger Str. 69
A-4040 Linz

Prof. Dr. Wolfram Pohlers
Institut für Mathematische
Logik und Grundlagenforschung
Universität Münster
Einsteinstr. 62
48149 Münster

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

Prof. Dr. Michael Rathjen
School of Mathematics
University of Leeds
GB-Leeds LS2 9JT

PD Dr. Peter Schuster
Mathematisches Institut
Ludwig-Maximilians-Universität
München
Theresienstr. 39
80333 München

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

Prof. Dr. Stephen G. Simpson
Department of Mathematics
Pennsylvania State University
University Park, PA 16802
USA

Prof. Dr. Bas Spitters
Computing Science Department
Toernooiveld
University of Nijmegen
P.O. Box 9010
NL-6500 GL Nijmegen

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

Prof. Dr. Thomas Streicher
Fachbereich Mathematik
Arbeitsgruppe 1
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
Filosofische Faculteit
Postbus 80103
NL-3508 TC Utrecht

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

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