Tagungsbericht 13/1995

Mathematische Logik

2. - 8. 4. 1995

This years Oberwolfach meeting on Mathematical Logic was chaired by Walter Felscher (Tübingen), Helmut Schwichtenberg (München) and Anne S. Troelstra (Amsterdam). There were participants from 11 countries. The focus was on proof theory, lambda calculus and constructive mathematics. Subfields like modal logic, provability logic, many valued logic, type theory, intutitionism, linear logic and the interpretation of aspects of traditional mathematics in type theory were treated. Several talks dealt as well with the contributions of mathematical logic to computer science. Here problems like the relationship between proofs and programs, logical foundations of computer science and finding good syntax and semantics for programming were discussed. This demonstrates that foundational questions and applications are very close in mathematical logic.
One highlight of the meeting was the first presentation of the proof theoretical analysis of Π^1_2–CA by Michael Rathjen (currently at Stanford), a problem open for 20 years.
All participants enjoyed very much the excellent opportunities the insitute offered for having private discussions, some more directly focused on mathematical work, in which the knowledge from different areas was brought together, others more on the general direction in which mathematical logic is currently developing.

Vortragsauszüge

Proof theory and nonclassical logics

Sergei N. Artemov

Abstract Propositional Operations over proofs (APO) are defined as operations over proofs that can be specified in arithmetic by propositional conditions and invariant with respect to a choice of a proof predicate. We prove that APO admits a finite basis. It allows to give a complete axiomatization for a logic with propositional formulas, formulas $[\![t]\!]A$ which stands for *"t is a proof of A"* (t is a proof term, A is a formula), boolean connectives for formulas and APO over proof terms. The resulting *Dynamic Logic of Proofs (DLP)* is a constructive variant of the modal logic S5. For example DLP enjoys the reflexivity property

$$[\![t]\!]A \rightarrow A$$

which is clearly missing in the traditional provability logic. The decidability and the arithmetical completeness of DLP are established.

Iterated local reflection vs. iterated consistency

Lev Beklemishev

For "natural enough" systems of ordinal notation we show that α-times iterated local reflection schema over a sufficiently strong arithmetic T proves the same Π^0_1-sentences as ω^α-times iterated consistency. A corollary is that the two hierarchies catch up modulo relative interpretability exactly at ϵ-numbers.
We also derive the following "mixed" formulas: for all $\alpha \geq 1$ and all β

$$(T^\alpha)_\beta \equiv_{\Pi^0_1} T_{\omega^\alpha \cdot (1+\beta)}$$

$$(T_\beta)^\alpha \equiv_{\Pi^0_1} T_{\beta+\omega^\alpha}$$

where T^α stands for α times iterated local reflection over T, T_β stands for β times iterated consistency, and $\equiv_{\Pi^0_1}$ denotes (provable in T) mutual Π^0_1 conservativity.
We show that "natural enough" ordinal notation systems do exist for every recursive ordinal.

Constructive interpretations of inductive definitions

Ulrich Berger

A realizability interpretation of intuitionistic positive inductive definitions is sketched. Since strict positiveness is not required the classical theory can be embedded easily via a negative translation. Hence also classical Π_2 theorems can be interpreted constructively in the usual way. The intuitionistic theory is interpreted via an extension of Kreisel's modified realizability interpretation. Since non strictly positive definitions are allowed the realizing term language needs constructs going beyond Gödels system T+ recursion over wellfounded tress (see e.g. Zuckers work in Troelstra's SLNM 344). The main problem is the constructive interpretation of the new term calculus, i.e. the definition of a reduction relation which is on the one hand strong enough to prove the soundness theorem and on the other hand strongly normalizing.

Logical foundations for formal specifications

Egon Börger

We demonstrate by two examples how Gurevich's notion of "evolving algebra" from 1988 can be used for transparent and falsifiable specifications and analysis of complex computing systems. The first example is the new correctness proof of Lamport's mutual exclusion protocol "bakery" (joint work with Y. Gurevich, D. Rosenzweig). The second example is the theorem that pipelining is correct on RISC machines (joint work with S. Mazzanti).

On Gentzen's consistency proofs for arithmetic

Wilfried Buchholz

We present a modified version of Gentzen's first consistency proof for Peano-Arithmetic PA [Math. Ann. 112 (1936)] and relate it to the standard cut-elimination procedure for ω-arithmetic. For each derivation d of PA (formulated in Tait's sequent calculus) and each $n \in \mathrm{N}$ the following objects are defined (by prim. recursion on the build-up of d):

- an expression $\mathsf{tp}_n(d)$ which either describes some inference of ω-arithmetic or is the symbol $\star$,
- a family of PA-derivations $d[i]_n$ $(i \in I)$ (with I determined by $\mathsf{tp}_n(d)$) such that

(1) $\mathsf{tp}_n(d) \neq \star \Longrightarrow \dfrac{\ldots\ \Gamma(d[i]_n)\ \ldots\ (i \in I)}{\Gamma(d)}$ is an inference of kind $\mathsf{tp}_n(d)$
(e.g. if $\mathsf{tp}_n(d) = (\exists x A, m)$ then $I = \{0\}$ and $\Gamma(d[0]_n) = \Gamma(d), A(m)$),
(2) $\mathsf{tp}_n(d) = \star \Longrightarrow \Gamma(d[0]_n) = \Gamma(d)$,
(3) $o_n(d[i]_n) < o_n(d) \quad (\forall i \in I)$.

Here $\Gamma(d)$ denotes the endsequent of d, and $o_n(d)$ is Gentzen's ordinal assignment from his second consistency proof [Leipzig 1938] as presented in [Mints, *A new reduction sequence for arithmetic*]. From (1),(2),(3) the consistency of PA follows immediately by transfinite induction up to ε_0.

Now let $d \mapsto d^\infty$ be the canonical embedding of PA-derivations into ω-arithmetic, and let $\mathcal{E}_n$ be the standard cut-elimination operator which lowers the cut-rank of each derivation in ω-arithmetic down to n. Then the following holds:

(1)' $\mathsf{tp}_n(d) \neq \star \implies \mathcal{E}_n(d^\infty) = \dfrac{\ldots\ \mathcal{E}_n(d[i]_n^\infty)\ \ldots}{\Gamma(d)}$, (2)' $\mathsf{tp}_n(d) = \star \implies \mathcal{E}_n(d[0]_n^\infty) = \mathcal{E}_n(d^\infty)$.

In the last part of the talk precise connections between Gentzen's first and second consistency proof are established.

Formal topology and constructive mathematics

Thierry Coquand

We show how some techniques of local theory or formal topology (topology without points) can be used in the proof-theoretical analysis of some non constructive proofs. We present two examples:

- the existence of minimal invariant compact subspace of a compact space X, with $f : X \to X$ continuous.

- the existence of non principal ultrafilters over N.

More about the intuitionistic continuum

Dirk van Dalen

In intuitionistic mathematics $\mathbb{R}$ is indecomposable, i.e. $\mathbb{R} = A \cup B$, $A \cap B \neq \emptyset \Rightarrow \mathbb{R} = A \vee \mathbb{R} = B$ (Brouwer). This result is extended to $\mathbb{Q}^c$ $(= x \in \mathbb{R} | x \notin \mathbb{Q}\})$ by using the continuity principle, bar induction and Kripke's Schema. A further exploitation of the above techniques + some intuitionistic topology yields the following: If $A \subset \mathbb{R}$ is negative and $A = B + C$, A located, B and C inhabited, then there is a $p \in \mathbb{R}$, such that p has positive distance to B and C.
As a corollary we get: If A is negative and dense in $\mathbb{R}$, then A is decomposable. Example: $A = \mathbb{Q}^{cc}$. One hence has lots of connected and 1-dimensional subsets of $\mathbb{R}$.

What is a model of Martin-Löf's type theory?

Peter Dybjer

We first introduce a notion of model of a basic framework of dependent types and call it "category with families" ("cwf"). It is a variant of Cartmell's categories with attributes, but has a more direct connection with the syntax of type theory. Then we show how to define cwfs using Martin-Löf's type theory as a metalanguage. This internal notion of cwf is "relaxed", as opposed to strict, and hence has a coherence problem. Finally, we show how to solve the problem as a corollary of a normalization theorem.

Nested proof theory

Lev Gordeev

Various results in algebraic and/or computer science logic address the following problem: How to formalize predicate logic (with or without equality) in the presence of $n < \infty$ distinct variables by using only direct (cut-free) rules of inference? The solution proposed has the form of term-rewriting systems such that a formula A is said to be derivable (provable) if there is a reduction chain starting with A and ending by $\top$. The resulting "reduction calculi" RPC_n (without equality) and $RPCE_n$ (with equality) can also be addressed as suitable nested versions of cut-free sequent calculi with n distinct variables. The corresponding nested cut elimination theorem is proved, which implies the equivalence to the familiar modus-ponens formalizations. These techniques enable to provide e.g. the negative solution to Problem 2.12 of [Henkin-Monk-Tarski: Cylindric Algebra I].

A Contraction free calculus for S4

Jörg Hudelmaier

Theorem proving in the modal logic S4 is notoriously difficult. This is due to the fact that in ordinary sequent calculi for this logic lengths of predeductions are not bounded in terms of the length of their endsequent. Here we propose a calculus for which there is a measure such that all premisses of all rules have smaller measure than their conclusions. Thus lengths of predeductions are bounded by the measure of their endsequent and we obtain a straight forward depth first proof search procedure.

Standard parts of classical analysis where provable functionals have polynomial growth relatively to the data
Ulrich Kohlenbach

To measure the growth of uniform bounds which are extractable from proofs in various parts of analysis we introduce a hierarchy $(G_nA^\omega)_{n\in\mathbb{N}}$ of subsystems of PA^ω and determine the impact of various analytical principles Γ on the growth (relatively to $G_nA^\omega + AC - qf$). We define a set Γ of analytical axioms which cover (relatively to $G_2A^\omega + AC - qf$) large parts of the usual analysis of continuous functions and show that from a proof

$$G_nA^\omega + \Gamma + AC - qf \vdash \forall u^1, k^0 \forall v \leq_\tau tuk \exists w^0 A_0$$

(where A_0 is quantifier-free, t is a closed term and $AC-qf$ denotes the schema of quantifier-free choice) one can extract a bound $\phi : \forall u, k \forall v \leq_\tau tuk \exists w \leq_0 \phi uk A_0$, where ϕ is a polynomial in $u^M := \lambda x^0.max(u0, \ldots, ux)$ and k if $n = 2$ resp. elementary recursive in u^M, k if $n = 3$ (ϕuk does not depend on v). Furthermore we determine the impact on the growth of bounds caused by the use of single sequences of instances of principles which involve arithmetical comprehension as the Bolzano-Weierstraß principle, the Arzelà Ascoli lemma and others.

***TAUT*-decision procedures and their complexity**
Horst Luckhardt (in cooperation with O. Kullmann)

We systematically develop methods deciding propositional tautology for DNF and coNP-complete subclasses and establish complexity upper bounds for them with exponential part $2^{\alpha \cdot m(F)}$ where $m(F)$ is one of the measures $\#\{variables\}$, $\#\{literalinstances\}$, $\#\{clauses\}$, and α varies between $\frac{1}{15}$ and 1. Combining these aspects differentiates $TAUT/SAT$-complexity on DNF/CNF in a new way.

Modal logic, linear logic, optimal lambda reduction
Simone Martini

We presented systems of indexed sequents for several modal logics (K,D,T,4 and their combinations), all formulated as local modifications of the basic system for the logic KD. The systems enjoy cut-elimination (or normalization and confluence in their natural deduction formulation). When they are tailored to linear logic and interpreted in proof-nets, the indexes have a natural interpretation in terms of box-depth. This interpretation suggests an improvement on the current formulation of graph-rewriting systems for optimal lambda-reduction (à là Levy-Lamping-Gonthier).

Cut-elimination for indexed systems of sequents
Grigori Mints

Cut reductions are defined and proved to be sufficient for cut elimination in Kripke-style formulation of modal logic in terms of indexed systems of sequents.

Zermelo-Fraekel algebras
Ieke Moerdijk (together with A. Joyal)

We extend the Lawvere-Tierney axioms for elementary toposes by axioms for a class of 'small maps'. An internal (in a topos $\mathcal{E}$) ZF-algebra is defined as a poset L, equipped with a unary operation $s : L \to L$, in which moreover all 'small' suprema exist. The cumulative hierarchy of sets (relative to $\mathcal{E}$), as well as various types of constructive ordinals, can be described as ZF-algebras defined by generators and relations. This provides a uniform approach to sheaf-, forcing- and realizability interpretations of set theory. A full description will appear in our book "Algebraic Set Theory" (Cambridge University Press, 1995).

A Classical view of the intuitionistic continuum

Joan Rand Moschovakis

We extend Gödels [1933] observation that intuitionistic number theory "is only apparently narrower than the classical one, and in fact contains it", to second order intuitionistic number theory ("analysis"). Let $i, j, \ldots; a, b, \ldots, h; \alpha, \beta, \ldots$ range over numbers, lawlike sequences, and arbitrary choice sequences respectively. Let $RLS(\alpha) \equiv \forall b[\forall w(Seq(w) \supset Seq(b(w))) \supset \exists x\ \alpha \in \overline{\alpha}(x) * b(\overline{\alpha}(x))]$ express "α is lawless relative to R", where R is the class of lawlike sequences. Using a set-theoretic hypothesis we build by ordinal induction a countable well-ordered class $(R, \prec)$ of "lawlike sequences" which leads to a classical realizability interpretation for a formal system $S^+[\prec]$ extending Kleene and Vesley's [1965] intuitionistic analysis, with Open Data and lawlike classical analysis included.

The logic of functional recursion

Yannis N. Moschovakis

The expressions of the Formal Language of Recursion FLR=FLR(τ) are defined by the following induction, where $x, \vec{x}, \ldots$ are individual variables, $p_i, \ldots$ are functions variables and the function(al) symbols f are from some specified signature (vocabulary) τ:

Terms: A	$:\equiv$	true | false (Booleans)
		| if A then B else C fi (Conditional)
		| $p(V_1, \ldots, V_n)$ (Function calls)
		| $f(E_1, \ldots, E_n)$ (Calls to primitives)
		| A_0 where $\{p_1(\vec{x}_1) = A_1, \ldots, p_n(\vec{x}_n) = A_n\}$ (Recursion)
Var. or Term: V	$:\equiv$	$x \mid A$
λ-terms: α	$:\equiv$	$\lambda(\vec{x})A$
Expressions: E	$:\equiv$	$x \mid A \mid \alpha$

Ultimately we are interested in the terms of FLR, which in the intended interpretations represent programs, while the remaining formal expressions are auxiliary. We consider the classical semantics on this language.

(1) **Strict semantics.** The structures are of the form (M, F), where M is an arbitrary set and the interpretation F assigns to the function symbols in the signature monotone, partial functionals on M to M, including the Booleans and a strict conditional; the individual variables vary over M, and the function variables over partial functions on M to M. Calls are by strict composition.

This is the natural interpretation for ideal "functional," side-effect-free programming like pure LISP, and it is also used in the study of classical, abstract recursion.

(2) **Continuous semantics.** The structures are of the form (W, F), where W is a directed, complete poset, and F interprets the function symbols by continuous functionals on W,

including fixed, discrete points 0 and 1 to denote the Booleans and a natural (strict) conditional. The individual variables vary over W and the function variables over continuous functions on W to W. Calls are by composition.

This is (perhaps) the most natural interpretation of FLR, from the mathematical point of view, and it also gives a faithful, abstract expression of *call-by-name* interpretations of programming languages. Neither (1) not (2) can be used, however, to model the natural semantics for the most natural *call-by-value* programing languages, as they both validate the identity

$$p(c) \text{ where } \{p(x) = p(c)\} = \bot;$$

while if c stands for an act like *ring the bell*, then the program on the left will produce an infinite string of *rings* in a call-by-value interpretation.

We introduce a new class of **liftup structures** of the form $(M, W, \jmath, F)$, where M is a set in which we interpret the individual variables; W is a complete poset, and we interpret the function variables by functions $p : M^n \to W$; F interprets the function by monotone functionals from M to W (suitably defined); and the $\jmath = \{\jmath_n\}_n$ is a sequence of monotone, liftup operation

$$\jmath_n : (M^n \to W) \to \text{Mon}(W^n \to W)$$

which we use to interpret "composition" in the formal expressions of FLR. It can be shown that liftup structures model faithfully most of the known interpretation of programming languages.

The main result is that *the class $\mathcal{V}$ of liftup valid* FLR *identities is decidable*, and in fact *there is a simple, natural and useful axiomatization for $\mathcal{V}$.*

Toric desingularizations and proofs in many-valued logic

Daniele Mundici

Every formula $\varphi(x_1, \ldots, x_n)$ of the infinite-valued calculus of Lukasiewicz has a DNF-reduction as a sum of Schauder hat formulas of some triangulation of the cube $[0,1]^n$, with rational vertices. The positive answer to the weak conjecture of Oda allows one to connect any two DNF tautologies by a path whose deduction steps are the natural counterparts of the blow up and blow down operations. Using the DeConcini-Proceri theorem on elimination of points of indeterminacy, Panti gives a novel proof of the completeness of the Lukasiewicz axioms. Conversely, in a joint paper with Aguzzoli, the author gives an algorithmic procedure to desingularize every 3-dimensional toric variety, keeping as small as possible the Euler characteristic of the resulting nonsingular variety.

D.M.: *A constructive proof of McNaughton theorem*, JSL 59 (1994), 596-602.

D.M.: *Lukasiewicz normal forms and toric desingularizations*, Proc. Keele Logic Coll., Oxford University Press.

G. Panti: *A proof of the completeness of the Lukasiewicz calculus*, JSL 60.

D. M., S. Aguzzoli: *An algorithmic desingularization of 3-dimensional toric varieties*, Tohoku Mathematical Journal 46 (1994) 557 - 572.

Constructive Nonstandard Analysis

Erik Palmgren

We present two approaches to nonstandard analysis which are constructive in the strict sense of E. Bishop. The first bing a constructivization of C. Schmieden and D. Langwitz' infinitesimal calculus from 1958. Their idea was essentially to use reduced powers modulo the Fréchet filter rather than ultrapowers as in more modern, but nonconstructive approaches. We obtain nonstandard characterizations of some standard notions pertaining to pointwise limits. The second approach is based on I. Moerdijk's topos of sheaves over a natural site of filters. Here full transfer- and overspill principles are true. The nonstandard characterization can here be extended to uniform notions (e.g. uniform continuity). However in both approaches a counterpart to the standard part map is lacking.

Pure proof theory - aims, methods and results

Wolfram Pohlers

Pursuing Hilbert's program of consistency proofs we introduce the notion of partial models for axiom system within the constructible hierarchy. It is shown how this approach is connected to Gentzen's original work. After outlining the basic methods we give a list of results obtained by ordinal analyses in the spirit of the outlined program.

Ordinal analysis of Π^1_2 comprehension

Michael Rathjen

We provide ordinal analyses of Π^1_2-comprehension and theories which can be reduced to iterated Π^1_2-comprehension, like Σ^1_3 dependent choices.
The analyses employ cut elimination in infinitary calculi of ramified set theory endowed with a transfinite hierarchy of reflection rules. The reflection rules that hold good for particular ordinals in the calculus are supposed to mirror their degree of stability.
The case of first order reflection rules was dealt with in M. Rathjen, "Proof theory of reflection", APAL 68 (1994) 181 - 224.

Proof-nets, Geometry of Interaction and L-calculus

Laurent Regnier

Proof nets (short *PN*) are a graphical syntax for proof in *linear logic* enjoying a strong topological property. This, together with the natural duality of linear logic ($A^\perp$) and the decomposition of structural rules into logical connectives (!, ?) makes PN a very useful tool for studying normalization processes, especially β-reduction.
However, as for β-reduction, the cut-elimination procedure in PN is far from being *local* and *asynchronous*. An attempt to fix these defects maybe to switch from β-reduction (cut-elimination) to some new operational semantics: the *geometry of interaction* (GoI).
In GoI, the computation of the normal form is replaced by the computation of the *regular paths* in the term; regular paths are defined by the *dynamic algebra* Λ^*. From this one may define a new reduction: *virtual reduction* which is a particular protocol for computing regular paths. Also regular paths are easily shown identical to *consistent paths*, the invariant of Lamping's sharing reduction. Both reductions are local and asynchronous, achieving the claimed goal.

Lambda calculus and intuitionistic linear logic

Simona Ronchi della Rocca

The intuitionistic fragment of linear logic, invented by Girard, can be seen as a model for a computational environment with an explicit control of resources management, since the use of structural rules is explicitly controlled by a modal operator.

A language is proposed for reasoning about this kind of computation. The relation between the language and the logic is established by the Curry-Howard isomorphism ("formulae-as-types" principle). Namely, terms of the language codify proofs in a logical system (in natural deduction style) equivalent (w.r.t. provable formulas) to the intuitionistic fragment of linear logic. The natural deduction system is designed in such a way that the resulting language has a very simple syntax, reduction rules which are extensions of the classical beta-rule, and in particular no commuting conversions are needed.

Applications of linear logic to the proof theory of classical logic

Harold A. J. M. Schellinx

We introduce a deterministic normalization scheme (tq-reduction) for sequent calculus for 2^{nd} order classical logic in a slightly extended language (LK^{tq}). The set of LK^{tq}-proofs can be mapped in a canonical way to a subset $D(LK^{tq})$ of derivations in 2^{nd} order classical linear logic., closed under reductions in linear logic; moreover, the tq-reduction of an LK^{tq}-proof π corresponds to the normalization of the proofnet-representation of $D(\pi)$.

This method of modal interpretation of sequent calculus *proofs* in linear logic provides a generally applicable mechanism for proving strong normalization of tq-like reductions in most of the standard sequent calculus formulations for (2^{nd} order) classical, intuitionistic and modal logics. It also enables us to give alternative proofs of strong normalization for several of the different "constructive" proof-systems for classical logic that have been proposed over the past five years.

Strict functionals for termination proofs

Helmut Schwichtenberg (joint work with Jaco van de Pol)

A semantical method to prove termination of higher order rewrite systems (HRS) is presented. Its main tool is the notion of a strict functional, which is a variant of Gandy's notion of a hereditarily monotonic functional. The main advantage of the method is that it makes it possible to transfer ones intuitions about why an HRS should be terminating into a proof: one has to find a "strict" interpretation of the constants involved in such a way that the left hand side of any rewrite rule gets a bigger value than the right hand side. The applicability of the method is demonstrated in three examples: (1) An HRS involving map and append; (2) The usual rules for the higher order primitive recursion operators in Gödel's T; (3) Derivation terms for natural deduction systems. We prove termination of the rules for β–conversion and permutative conversion for logical rules including introduction and elimination rules for the existential quantifier. This has already been proved by Prawitz; however, our proof seems to be more perspicuous.

A transparent version of a well-ordering proof for Martin-Löf's type theory

Anton G. Setzer

In his thesis, the author proved that Martin-Löf's type theory with W-type and one Universe has proof theoretical strength $|\psi_{\Omega_1}(\Omega_{I+\omega^+})|$. In this proof we will present a new simplified version of the well ordering proof, by which we get a lower bound for the strength, in which we avoid the use of fundamental sequences and all the technical proofs needed to prove properties about them. Instead we will directly formalize the sets $C_I(a)$, used for the definition of the collapsing function, in MLT. This version is more transparent, since it is very close to the set theoretic definition of the ordinal functions.

Wissenslogik: Wisser und Mitwisser

Ernst Specker

Es wird gezeigt, daß in der Wissenslogik $S_5^{(n)}$ - d.h. der Logik mit n Wissensoperatoren K_i und den Axiomen der Modallogik S_5 - aus $X_i \leftrightarrow K_j X_i (j \neq i)$, $K_i X_i \leftrightarrow K_j K_i X_i$ $(i = 1, \ldots, n)$ folgt

$$K_1 K_2 K_3 \ldots K_n (X_1 \vee \cdots \vee X_n) \rightarrow K_1 X_1 \vee K_2 X_2 \vee \cdots \vee K_n X_n$$

Anwendung auf das Paradoxon des unerwarteten Ereignisses.

A transformation of propositional Prolog programs into classical logic

Robert F. Stärk

We transform a propositional Prolog program into a set of propositional formulas for which Prolog, using its depth-first left-to-right search, is sound and complete. This means that a goal succeeds in Prolog if and only if it follows from the transformed program in classical propositional logic. The transformation is formulated in an extended language with syntactic operators for success, failure and termination. The obvious generalization to predicate logic leads to a first-order theory for which Prolog is still sound but unfortunately not complete. If one changes, however, the definition of the termination operator then one obtains a theory that allows to prove termination of arbitrary non-floundering goals under Prolog. The new theory is called the ℓ-completion of a Prolog program. The change of the termination operator is justified by the fact that for most programs used in practice the computations terminate independently of the order of the clauses in the program. By adding suitable induction principles to the ℓ-completion one obtains a framework for verifying pure Prolog programs. Verification of Prolog programs here means proving termination and proving equivalence of predicates.

Polynomial time operations in applicative theories

Thomas Strahm

Theories with self-application provide an elementary framework for many activities in (the foundations of) mathematics and computer science. They were first introduced by Feferman as a basis for his systems of explicit mathematics, e.g., the theory T_0; these theories are broadly discussed in the literature from a proof-theoretic and model-theoretic point of view.

It is the aim of the present work to propose a first order theory PTO of operations and binary words, which allows full self-application and whose provably total functions on

W = $\{0,1\}^*$ are exactly the polynomial time computable functions. In spite of its proof-theoretic weakness, PTO has an enormous expressive power due to the presence of full (partial) combinatory logic, i.e. there are terms for every partial recursive function. The formulation of PTO is very much akin to well-known theories of operations and numbers, namely PTO can be viewed as the polynomial time analogue of the theory BON plus set induction of Feferman and Jäger.

The proof of the fact that PTO captures exactly polynomial time is very much in the spirit of reductive proof theory. More precisely, we show that PTO contains Ferreira's system of polynomial time computable arithmetic PTCA via a natural embedding. Furthermore, PTO is reducible to the theory $\mathsf{PTCA}^+ + (\mathsf{BCP})$, where PTCA^+ denotes the extension of PTCA by NP induction and (BCP) is the collection principle for bounded formulas. $\mathsf{PTCA}^+ + (\mathsf{BCP})$ is known to be a Π^0_2 conservative extension of PTCA by the work of Buss, Cantini, or Ferreira.

Forcing in Bounded Arithmetic
Gaisi Takeuti (joint work with M. Yasumoto)

We present boolean valued - forcing theory on a countable nonstandard model of the true arithmetic, more precisely on the cut which is a model of S_2. Then we discuss the relation between the natures of its generic model and the $P = NP$ problem.

The Heyting algebra of Heyting's arithmetic is not recursive
Albert Visser

This lecture reports work together with Dick de Jongh. We show that an extension of HA, called HA^* has the following property: every prime, RE Heyting Algebra can be embedded in the Heyting Algebra of HA^*. The method of proof is an adaptation of a proof due to Shavrukov, which was simlified by Zambella. From earlier results of de Jongh it follows that a Heyting Algebra on 2 generators exists, which is prime and non-recursive. Combining the two above results, the theorem claimed in the title easily follows

Logic of primitive recursion (LPR)
Stan S. Wainer

This is a report on some joint work with W. Sieg (Carnigie Mellon). An attempt is made, to analyze the structural relationships between primitive recursive programs (over $\mathbb{N}$) and their inductive termination proofs, where the proofs are formalized in a "sub-linear" sequent calculus without Contraction or Weakening, and without Exchange. Programs are introduced as relational sequents, ordered in such a way that values are passed from left-to-right. Thus e.g.

$$f_0(x) = y_0, f_1(x, y_0) = y_1, f_2(x, y_0, y_1) = y_2 \vdash f_3(x) = y_2$$

axiomatizes the composition $f_3(x) = f_2(x, f_0(x), f_1(x, f_0(x)))$.
The lack of Exchange necessitates two Cut-rules - one cutting away the left-most premise and another cutting a formula within context (called cvc, "call-by-value" cut). Basic Induction is the rule: $\vdash B(0)$, and $B(z) \vdash B(z+1) \Rightarrow \vdash B(z)$ without any side formulas, and one inductive call on $B(z)$.
Theorem (1) Primitive Recursive $\equiv LPR(\exists)$-verifiable.

(2) Primitive Recursive with Parameter Substitution ≡ $LPR(\forall\exists)$-verifyable.
(3) Tail-Primitive Recursive ≡ $(LPR(\forall\exists) - (cvc))$-verifiable.
Allowing side-formulas in the Induction rule, and multiple inductive calls, leads beyond the "boundaries" of primitive recursion.

Subrecursive hierarchies in logic and computer science
Andreas Weiermann

We present the Buchholz, Cichon and Weiermann 1994 approach to subrecursive hierarchies. As results of this theory we obtain: a uniform local predicativity style characterization of the provably recursive functions of PA, $PA + TI(\prec\restriction)$, KPl, KPi, $KPM, \ldots$, an optimal subrecursive bound for Higman's lemma and Kruskal's theorem, a strong generalization of the Girard Wainer hierarchy comparison theorem, a general bounding result for derivation lengths of terminating rewrite systems in terms of the slow growing hierarchy of ordinal level determined by the ordertype of the termination ordering, a proof of Cichon's conjecture on the derivation lengths of rewrite systems which model parameter recursion and unnested multiple recursion, an illuminating proof of some classical results of Peter on primitive recursive functions, a solution of Cichon's problem on the relationship of the hydra battle rewrite system and the Howard Bachmann ordinal, a term rewriting characterization of several subclasses of the ordinal recursive functions.

Generalizing proofs in monadic languages
Piotr Wojtylak (joint work with Matthias Baaz)

Suppose that π is a formal proof of a theorem A, can we construct from π a proof of another (similar or more general theorem)?
1. We deal with generalizing short proofs with deep terms and let us distinguish between
a) generalization of proofs: from a proof of $A(t)$ to a proof of $A(s)$ preserving the logical form of the proof;
b) generalization of theorems: from a proof of $A(t)$ to a proof of (more or less) $\forall x A(x)$.

Generalization of proofs leads to a relation between distribution of terms in proofs of a given logical form and solutions of sets of linear diophantine equations. Generalization of theorem can be achieved by several methods used in literature: by reflection principle, cut elimination and operating with blocks of like quantifiers instead of one quantifier at each step.

Berichterstatter: Anton Setzer.

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

Tagungsteilnehmer

Prof.Dr. Sergei N. Artemov
Steklov Mathematical Institute
MIAN
Academy of Sciences
42, Vavilova str.

Moscow 117 966 GSP-1
RUSSIA

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

S-41296 Göteborg

Dr. Lev D. Beklemishev
Steklov Mathematical Institute
MIAN
Academy of Sciences
42, Vavilova str.

Moscow 117 966 GSP-1
RUSSIA

Prof.Dr. Dirk van Dalen
Filosofische Faculteit
Postbus 80126

NL-3508 TC Utrecht

Dr. Ulrich Berger
Mathematisches Institut
Universität München
Theresienstr. 39

80333 München

Prof.Dr. Justus Diller
Institut für Mathematische
Logik und Grundlagenforschung
Universität Münster
Einsteinstr. 62

48149 Münster

Prof.Dr. Egon Börger
Dipartimento di Informatica
Universita di Pisa
Corso Italia, 40

I-56125 Pisa

Dr. Peter Dybjer
Department of Computer Science
Chalmers University of Technology
and University of Göteborg

S-41296 Göteborg

Prof.Dr. Wilfried Buchholz
Mathematisches Institut
Universität München
Theresienstr. 39

80333 München

Prof.Dr. Walter Felscher
Wilhelm-Schickard-Institut für
Informatik
Mathematische Logik
Morgenstelle 10/Bau C

72076 Tübingen

Dr. Lev Gordeev
Mathematisches Institut
Universität Tübingen
Auf der Morgenstelle 10

72076 Tübingen

Dr. Simone Martini
Dipartimento di Informatica
Universita di Pisa
Corso Italia, 40

I-56125 Pisa

Dr. Jörg Hudelmaier
WSI
Universität Tübingen
Sand 13

72076 Tübingen

Prof.Dr. Grigori Mints
Dept. of Philosophy
Stanford University

Stanford , CA 94305
USA

Prof.Dr. Gerhard Jäger
Institut für Informatik
und angewandte Mathematik
Länggasstraße 51

CH-3012 Bern

Prof.Dr. Ieke Moerdijk
Mathematisch Instituut
Rijksuniversiteit te Utrecht
P. O. Box 80.010

NL-3508 TA Utrecht

Dr. Ulrich Kohlenbach
Mathematisches Seminar
Fachbereich Mathematik
Universität Frankfurt
Postfach 111932

60054 Frankfurt

Prof.Dr. Joan Rand Moschovakis
721 - 24th Street

Santa Monica , CA 90402
USA

Prof.Dr. Horst Luckhardt
Weißenburgstr. 21

61184 Karben

Prof.Dr. Yiannis N. Moschovakis
Dept. of Mathematics
University of California
405 Hilgard Avenue

Los Angeles , CA 90024-1555
USA

Prof.Dr. Daniele Mundici
Dept. of Computer Science
University of Milan
via Comelico 39-41

I-20135 Milano

Dr. Michael Rathjen
Department of Mathematics
Stanford University

Stanford , CA 94305-2125
USA

Prof.Dr. Piergiorgio Odifreddi
Dip. di Informatica
Universita di Torino
Corso Svizzera 185

I-10149 Torino

Dr. Laurent Regnier
Laboratoire de Mathematiques
Discretes
Case 930
163 Avenue de Luminy

F-13288 Marseille Cedex 9

Dr. Erik Palmgren
Department of Mathematics
University of Uppsala
P.O. Box 480

S-75106 Uppsala

Prof.Dr. Simona Ronchi Della Rocca
Dip. di Informatica
Universita di Torino
Corso Svizzera 185

I-10149 Torino

Dr. Michel Parigot
Equipe Logique Mathematique
Universite Paris VII
2, Place Jussieu

F-75251 Paris Cedex 05

Prof.Dr. Harold A.J.M. Schellinx
Equipe de logique CNRS UA 753
Universite Paris VII
2 Place Jussieu

F-75251 Paris Cedex 05

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

48149 Münster

Prof.Dr. Helmut Schwichtenberg
Mathematisches Institut
Universität München
Theresienstr. 39

80333 München

Dr. Anton Setzer
Mathematisches Institut
Universität München
Theresienstr. 39

80333 München

Prof.Dr. Gaisi Takeuti
Department of Mathematics
University of Illinois
273 Altgeld Hall MC-382
1409, West Green Street

Urbana , IL 61801-2975
USA

Prof.Dr. Ernst Specker
Mathematik Department
ETH Zürich
ETH-Zentrum
Rämistr. 101

CH-8092 Zürich

Prof.Dr. Anne S. Troelstra
Fakulteit Wiskunde en Informatica
Universiteit van Amsterdam
Plantage Muidergracht 24

NL-1018 TV Amsterdam

Robert F. Stärk
Department of Mathematics
Stanford University

Stanford , CA 94305
USA

Prof.Dr. Albert Visser
Filosofische Faculteit
Postbus 80126

NL-3508 TC Utrecht

Prof.Dr. Viggo Stoltenberg-Hansen
Department of Mathematics
University of Uppsala
P.O. Box 480

S-75106 Uppsala

Dr. Stanley S. Wainer
School of Mathematics
University of Leeds

GB-Leeds , LS2 9JT

Thomas Strahm
Institut für Informatik und
Angewandte Mathematik
Universität Bern
Länggass Str. 51

CH-3012 Bern

Dr. Andreas Weiermann
Institut für Mathematische
Logik und Grundlagenforschung
Universität Münster
Einsteinstr. 62

48149 Münster

Prof.Dr. Piotr Wojtylak
Institute of Mathematics
Silesian University
Bankowa 14

40-007 Katowice
POLAND