MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

T a g u n g s b e r i c h t 03/1998

Mathematical Logic

18.01 - 24.01. 1998

The conference was organized by Y.N. Moschovakis (Los Angeles), H. Schwichtenberg (München), and A.S. Troelstra (Amsterdam). It focussed on constructive aspects of mathematical logic, in particular on constructive set theory, term rewriting and proof theory, intuitionistic logic and type theory, complexity theory, lambda-calculus, and algorithmic randomness.

There were 15 plenary talks and two lecture series, one on constructive set theory, given by P. Aczel and M. Rathjen (4 lectures), another on term rewriting and proof theory, given by A. Weiermann and W. Buchholz (3 lectures).

The organizer's strategy, to have less talks in favour of more time for self organized activities, found an extremely positive echo among the participants. Quite a number of informal talks and discussions were organized giving room for fruitful scientific and personal exchange.

The list of abstracts includes those talks which, although of highest quality, had to be sacrificed to the new strategy.

Vortragsauszüge:

P. Aczel:
Constructive Set Theory

Lecture 1: What is constructive set theory?

I discuss a conception of generalised predicative constructive mathematics. I then explain informally the iterative-combinatorial notion of set that is made precise in constructive type theory and leads to an interpretation of the axiom system CZF in a suitable version of constructive type theory.

Lecture 2: Inductive definitions in constructive set theory.

1. Inductive definitions of classes
2. Inductive definitions of sets
3. A set compactness theorem
4. An example of an inductive recursive definition

J. Avigad:
Proof Theory and Typed Computation

Both ordinal recursion and higher-typed recursion can be used to give natural characterizations of the provably total recursive functions of classical theories. I will discuss two results that yield characterizations of the second kind. The first result is a Dialectica-style interpretation of the theories $\hat{ID}_n$, in functional theories P_n using predicative polymorphism and Martin-Löf universes. The second is a realizability interpretation that applies directly to classical arithmetic in a Tait calculus.

U. Berger:
Modelling dependent types and universes using the Kleene-Kreisel functionals

We will try to argue that it is useful to have a constructive set-theoretic model of dependent types, and will discuss in some detail one such model generalizing the Kleene-Kreisel continuous functionals. Using a density/co-density theorem it can be shown that this is isomorphic to (a variant of) Beeson's realizability model of type theory. Finally we state some open problems, among them generalizations of Plotkin's resp. Normann's (cf. his talk on Tuesday) theorems on S1-S9/PCF-computability in the partial resp. total hierarchy.

W. Buchholz:
Term rewriting and proof theory III: Termination proofs by interpretation.

We give an interpretation of the Gentzen-Takeuti reduction procedure for finitary derivations in (Tait style) sequent-calculi of first-order arithmetic and the subsystem Π^1_1-CA of second-order arithmetic, respectively. Each finitary derivation d is interpreted as a certain well-founded infinite derivation d^∞ in such a way that if d reduces to red(d) by a Gentzen-Takeuti reduction step, then red$(d)^\infty$ is a proper sub-derivation of d^∞. Hence the procedure red terminates, i.e. there is no infinite sequence of derivations $(d_i)_{i<\omega}$ with $d_{i+1} = \text{red}(d_i)$ for all i. The main point of our approach is that red can actually be *derived* from infinitary cut-elimination (and collapsing) procedures.

A. Cichon:

Termination proofs for rewrite systems and their relevance to proof theory

Equational definitions of number-theoretic functions are natural models of certain kinds of rewrite systems. The interaction of proof theory and term rewriting theory has given rise to new and interesting results and techniques in both domains. This talk will survey some of the recent developments in the analysis of termination proofs for rewrite systems and their implications for proof theory.

P. Clote:

Type 2 parallel computable functions

The parallel random access machine, or PRAM, is a parallel computing model developed at the end of the 1970's, and is the virtual machine for existent parallel machines like the Connection Machine, Mas Par, and ICE "Greeneyes" board. The intuition for programming such SIMD models is to use divide and conquer paradigm together with data parallelism. NC is the most important parallel computation class and corresponds to polylogarithmic time with polynomially many active processors.

In this paper, we extend PRAM to allow different processors to simultanously make function oracle calls, then define a very natural type 2 function algebra $\mathcal{A}$, and prove that the type 2 analogue of NC equals $\mathcal{A}$. The full proof is long (60 pages), relies on extension of techniques of Cook and Kapron, and is a strong improvement of a paper of Clote-Ignjatovic-Kapron from FOCS 1994.

T. Coquand

Formal topology and inductive definitions

The purpose of this talk is to illustrate how ideas from the theory of locale (point-free topology) can illuminate some facts in proof theory, and suggest appropriate definitions of mathematical concepts, like well-quasi-ordering or noetherianity in a framework such as Constructive Set Theory or Intuitionistic Set Theory.

First, we present a simple example in algebra: a special case of Jacobson's commutativity theorem for rings. In the framework of point-free topology, the usual representation theorem of rings as rings of continuous section over a boolean space have an elementary reading, and Jacobson's proof can be read as an elementary proof of commutativity, with no mention of prime ideals. This can be compared to the analysis by H. Lombardi (Annals of Pure and Applied Logic, 1997) of some non-constructive arguments in algebra.

Next, we give a satisfactory definition of well-quasi-orders and noetherian rings in Intuitionistic Type Theory (joint work with H. Persson; the inductive definition of noetherian, that the property $u_n \in (u_1, ..., u_{n-1})$ is a bar on finite sequences, was suggested by P. Martin-Löf). We can prove for instance in this way Hilbert's basis theorem. The proof uses a point-free analysis of the Open Induction Principle:

If $P(x)$ is open, and $\forall x[[(y < x)P(y)] \rightarrow P(x)]$ then $\forall x P(x)$.

This principle can be stated over [0,1], Cantor space or Baire space. The analysis of this principle over Cantor space uses ID1, and this suggests that the pointwise version may not be conservative over HA. Similarly, the pointwise version over Baire space should not be provable in usual intuitionistic systems (of strength ID1) like FIM (Kleene) or CS (Kreisel-Troelstra).

R. David:
Traces of some primitive recursive schemata

This talk is concerned with primitive recursive algorithms. I will introduce the trace (of the computation of a p.r. algorithm on some arguments). The trace is closely related to the notion of sequential algorithms on concrete data structures (cf Berry and Curien). I will use this powerful tool to prove some results as

- The ultimate obstination theorem of L. Colson and its extensions to other situations.
- A backtracking property for p.r. algorithms using any kind of first order data type.
- The characterisation of the intentional behaviour of some p.r. algorithms.
- The existence or non existence of (trace preserving) simulations between various extensions of p.r. algorithms (new recursive schemata, ...).

R. Dyckhoff:
Some contraction-free calculi

We present two results (joint work with Sara Negri in Helsinki).

First, we give a direct proof of admissibility of the structural rules for the terminating contraction-free intuitionistic sequent calculus **G4ip** from [1] (cf [2]). Previous proofs have all used induction in sequent weight or semantics (or both). This new proof uses only induction on formulae weight and derivation height, and thus extends to a proof of completeness for a similar first-order calculus **G4i** (and to several other related calculi) and also to a proof of admissibility of the structural rules for **G4ip** extended with various positive notions such as "apartness" and "excess", thus allowing easier proofs of conservativity for such theories over, for example, the theory of equality or partial order.

Second, we show the completeness of a terminating contraction-free calculus for Dummett's logic **LC**; this calculus has the property that all its inference rules are invertible, with clear advantages for automated proof search and raising an interesting question about the relationship between invertibility of all rules and the linearity of the Kripke models.

[1]. RD, "Contraction-free calculi for intuitionistic logic", J. Symbolic Logic 1992.

[2] A.S. Troelstra & H. Schwichtenberg, "Basic Proof Theory", Cambridge Univ. Press 1996.

[3] RD & S. Negri, "Admissibility of structural rules for contraction-free intuitionistic sequent calculi", in preparation, 1998.

L. Gordeev:

How to rescue Hilbert's Programme using Integral Calculus

Hilbert's rejection of the "ignorabimus" might still make sense beyond the naive finitism. Some remarkable results about Lukasiewicz' real valued logic make even "hopeless" problems (like Quine's Con(NF)) computable using basic Riemann/Lebesgue Integral Calculus.

J. R. Hindley:

Curry's last problem: imitating lambda-beta reduction in combinatory logic

The last problem on which Curry worked before he died in 1982 was that of defining a reduction in combinatory logic to correspond closely to the usual β-reduction in λ-calculus. Several solutions to this problem have been posed since then, but despite some ingenuity in their formulation, none has been really clean and simple enough to make its development attractive. I believe the task of finding a workable combinatory β-reduction is one of the main unsolved problems in combinatory logic. (It is not a "tidy" problem and it promises no beautiful solution, but then, neither does real life.) This talk would discuss criteria for acceptability of a β-reduction, and describe the known candidates and how far they succeed or fail in satisfying these.

J. Hudelmaier:

On a "real" tableau calculus for intuitionistic propositional logic

The well known tableau calculus TK for classical propositional logic has two features which distinguish it from usual tableau calculi for intuitionistic propositional logic:

A) TK-*derivations* allow extraction of classical models.

B) TK-*rules* allow extraction of classical semantics.

Obviously condition B) is much stronger than condition A). For instance condition B) makes the completeness proof completely trivial. Now for intuitionistic logic there are a number of calculi satisfying the analogue of A). In this talk we present a calculus TJ which in addition also satises B) and thus yields a very perspicuous completeness proof for intuitionistic logic with respect to Kripke semantics.

U. Kohlenbach:

The no-counterexample interpretation and restricted forms of comprehension

In the first part of this talk we address the question to what extent the use of higher types is necessary for a local and modular analysis of proofs and the extraction of constructive data. Whereas Gödel's functional interpretation or various realizability interpretations, which use functionals of arbitrary finite types, respect the logical deduction rules with low complexities involved, this is not true for the so-called no-counterexample interpretation (n.c.i.) of Peano arithmetic **PA** which only uses functionals of low (≤ 2) types.

We determine exactly the complexity of the n.c.i. of the modus ponens rule

1. pointwise for given functionals of fixed complexity satisfying the n.c.i. of arbitrary premises in $\mathcal{L}(\textbf{PA})$

2. uniformly in arbitrary functionals satisfying the n.c.i. of arbitrary premises in $\mathcal{L}(\mathbf{PA})$.

It turns out that the n.c.i. of **PA** in Gödels's T (or -equivalently- by $\alpha(<\epsilon_0)$-recursive functionals) can be obtained by a local procedure (on the level of the n.c.i. of the formulas involved), but that is not possible for the n.c.i. of its fragments $\mathbf{PA}_n$ (with Σ_n-induction only) in the correspondingly restricted classes of functionals.

As the main technical tool we use a detailed analysis of terms which are built up in a specific way out of a weak form of bar recursion and T. This also gives rise to a new **PA**-conservative extension $\mathcal{A}$ of the system ACA_0 (arithmetical induction and comprehension) whose Π^1_1-theorems have a n.c.i. in T which can be obtained **directly** *from their proofs in* $\mathcal{A}$.

In the second part of this talk we determine the computational and proof-theoretic strength of fragments of $\mathcal{A}$ with **restricted** forms of arithmetical comprehension and choice thereby generalizing classical results due to H.Friedman and J.Paris.

R. Matthes:
Lambda Calculi with Monotone Inductive Types

Systems in natural deduction style of terms denoting proofs of second-order propositional logic including least fixed-points are considered. The β-reduction rules for those proof terms are giving rise to strongly normalizing and confluent term rewrite systems. It is well-known that iteration may be coded in Girard's System F. For this reason special focus is on full primitive recursion. Which are the restrictions of building inductive types? Systems with positive inductive types, with monotone inductive types (there is a term whose type expresses monotonicity) and even any inductive type are considered. The last system is in the spirit of Mendler's LICS 1987 system. It turns out that there is a reduction-preserving embedding of the systems of monotone inductive types into the system of (strictly) positive non-interleaved inductive types—strictness being possible in the introduction-based *monotone system* including the (second-order) existential quantifier. An extension of Mendler's system and its dualization are the only systems for which a direct normalization proof has to be carried out, and they are free from restrictions such as *monotonicity* which in turn allows for very elegant structural proofs. In summa: Monotonicity instead of positivity does not even make the systems stronger with respect to reduction.

The open question is if this reduction is also possible in systems where universal quantification is left out. *This seems to be needing the study of permutative* conversions as well as variable elimination reductions for sums and μ-types.

Short talk of < 30 minutes: Two very easy proofs of normalization of simply typed λ-calculus using inductive definitions

(A proof of weak normalization by induction on normal forms. A proof of strong *normalization by induction on a set* SN.)

I. Moerdijk:
Models for Martin-Löf Type Theory

We discuss the possible interpretation of such type theories in categories of sheaves. the eventual goal being a better understanding of the relation between topos theory and type theory (respectively models of IZF [1] versus CZF).

[1] Joyal-Moerdijk: *Algebraic Set Theory* (Cambridge U.P.)

K.-H. Niggl:
The μ-Measure as a Tool for Classifying Computational Complexity

The two simply typed term systems PR_1 and PR_2 are considered, both for representing algorithms computing primitive recursive functions. PR_1 is based on primitive recursion, and PR_2 on recursion on notation. .

The *μ-measure* [Ni95] is employed to determine the computational complexity of algorithms in PR_i and to uniformly integrate traditional results in subrecursion theory with resource-free characterisations of sub-elementary complexity classes.

To set the stage, μ-based *modified Heinermann classes* $\mathcal{R}_i^n$ are defined. Extending the Schwichtenberg/Müller characterisation of the Grzegorczyk classes $\mathcal{E}_n$ for $n \geq 3$, it is shown $\forall n \geq 1.\mathcal{E}_{n+1} = \mathcal{R}_1^n$. The proof does not refer to any machine-based computation model, unlike the Schwichtenberg and Müller proofs. This is due to the notion of *modified recursion lying on top of each other* provided by the μ-measure. By Ritchie's result, $\mathcal{R}_1^1$ characterises the linear-space computable functions. Accordingly, a short and straightforward proof is presented showing that $\mathcal{R}_2^1$ characterises the polynomial time computable functions, thus streamlining the proof and result of Bellantoni and Cook. Furthermore, the classes $\mathcal{R}_2^n$ and $\mathcal{R}_1^n$ coincide at and above level 2.

Rounding off the talk, it is outlined how to extend the μ-measure to subsystems $\mathcal{N}_1$ and $\mathcal{N}_2$ of Gödel's T which do not support recursion in all higher types.

D. Normann:
Computability over the partial continuous functionals

Let $\{P(k)\}_{k \in \mathbb{N}}$ be the hierarchy of partial continuous functionals. We show that every equivalence class of total functionals containing a recursive one will also contain one S1-S9-computable, or equivalently, one that is *PCF*-definable in the sense of Plotkin. This involves replacing nondeterministic parallellism in higher types by deterministic sequentiality.

M. Rathjen:
Constructive set theory

I gave two lectures following two lectures by Peter Aczel.

Lecture 1: (i) *The Regular Extension Axiom (***REA***).* The axiom **REA** asserts that any set is contained in a regular set. The addition of **REA** to **CZF** has the effect that bounded inductive definitions define sets, i.e.their least fixed points. After explaining the role of **REA** in the proof of the latter result, I put forward several reasons why **REA** should be considered the constructive analogue of the Powerset Axiom.

(ii) *Constructive Choice Principles.* The general axiom of choice is taboo in constructive set theory as it implies excluded middle. But several mathematically important forms of choice are legitimate, the strongest being the Presentation Axiom (**PA**). **PA** implies the axiom of dependent choices which implies countable choice.

(iii) *Proof-theoretic strengths.* **CZF** has the same proof-theoretical strength as the classical system $\mathbf{ID}_1$ (theory of non-iterated inductive definitions) or Kripke-Platek set theory. The latter still holds when Subset Collection is omitted. The theory $\mathbf{CZF} + \mathbf{REA}$ is much stronger. It is proof-theoretically equivalent to a fragment of second order arithmetic based on Δ^1_2 comprehension and bar induction.

Lecture II: (i) I discussed the notions of inaccessibility and Mahlo's hierarchy of inaccessibility in **CZF**.

(ii) Friedman and Scedrov have investigated large set axioms on the basis of **IZF**, to the effect that **IZF + LSA** and **ZF + LCA** have the same strength, where **LCA** is a large cardinal axiom and **LSA** its pertinent large set axiom. The situation is completely different when the large set axioms are considered in the framework of **CZF**. To give an example:

$$\mathbf{CZF} + \forall x \exists y [x \in y \wedge y \text{ is a Mahlo set}]$$

and

$$\mathbf{KP} + \forall \alpha \exists \kappa [\alpha \leq \kappa \wedge \kappa \text{ is recursively Mahlo}]$$

are of the same strength. Another example is weak compactness. The pattern seems to propagate.

A. Scedrov:

Proof Games, Optimization, and Complexity

Linear logic proof game is played on linear logic formulas. Its moves are instances of reverse inference rules of linear logic. There are two players, called proponent and opponent, and a separate verifier. Proponent's goal is to play a sequence of moves that constitute a formal proof of an input formula. Opponent tries to force the direction of proponent's evidence in a way that makes it impossible for proponent to obtain a formal proof. Several versions of this game are discussed, each with a numeric score that reflects the number of certain preferred axioms used in a complete or partial formal proof. The capabilities of the players may differ. While proponent is always omnipotent, in some versions of the game opponent's decisions are based only on a fair coin toss.

Probabilistic games considered in computational complexity theory, such as so-called interactive protocols, may be represented in the proof game. The polynomial-time representations we consider preserve proponent's moves, opponent's moves, proponent's strategies, as well as proponent's optimal strategies. In this way, one transfers to the linear logic proof game the complexity lower bounds for the approximation of the expected score when proponent plays almost optimally. Let us say that a q-heuristic, 0 ¡ q ¡ 1, is a function from formulas to instances of reverse inference rules (that is, proponent's strategy) such that the optimum score arising from the use of this inference rule instance is within multiplicative ratio q of the optimal score. Any polynomial-time q-heuristic for MLLT, propositional multiplicative fragment extended with additive propositional constants, would yield P = NP. Furthermore, computing any q-heuristic H for the propositional multiplicative-additive fragment, MALL, would decide membership in any language in PSPACE, using time and space at most a polynomial greater than the time and space needed to compute H. This is joint work with J.C. Mitchell and P.D. Lincoln.

P. Selinger:

Finite lambda models

It is well-known that a model of the untyped lambda calculus, in the traditional sense, can never be finite or even recursive. By contrast, we present a notion of finite models for the lambda calculus. These finite models are models of reduction, rather than of conversion, and therefore they are not subject to the usual limitations on size and complexity. A model of reduction has an underlying set which is partially ordered, and it satisfies a soundness property of the form

$$M \longrightarrow_\beta N \Rightarrow [\![M]\!] \leq [\![N]\!].$$

We work with a definition of syntactical models of reduction that was given by Plotkin (1994) in the spirit of the familiar syntactical lambda models. Models of reduction are easily constructed, and in fact there exists an abundance of finite ones. Moreover, we observe that models of reduction satisfy a limited form of soundness for convertibility: $M =_\beta N \Rightarrow [\![M]\!] \bigcirc [\![N]\!]$, where $a \bigcirc b$ means that a and b are compatible, i.e. $(\exists c)\, a, b \leq c$. We exploit this property to give simple finitary proofs of term inequalities. In examples, we show that models with as few as four elements are sufficient to distinguish certain unsolvable terms.

A. Setzer:
Ordinal systems

Ordinal systems are the abstract description of what "good" ordinal notation systems should be like: new ordinals are defined using smaller ones and when introducing a new ordinal, all ordinals below it are known before the new one. Using ordinal systems we can describe in a different, and as we hope more intuitive way ordinal notation systems which are usually considered as impredicative ones. Since we have a more abstract notion, the well-ordering proofs become easier. We hope - that is of course more a philosophical rather than a mathematical question - that they can be regarded as intutively well-ordered, which would justify in a rather direct way the consistency of the theories of that strength as well. We will define ordinal systems up to the level of Mahlo.

R. Stärk:
Why the constant undefined? Logics of partial terms for strict and non-strict functional programming languages

The world of functional programming is split into two parts, the world of strict evaluation (ML,Scheme) and the world of lazy evaluation (Haskell,Miranda). We are interested in the logical foundation common to both worlds. For this purpose we introduce the *Basic Logic of Partial Terms (BPT)*. This logic proves properties of programs which are valid under both strict and lazy evaluation. BPT contains a definedness predicate but no constant denoting the object 'undefined'. In this respect it is similar to Beeson's logic of partial terms. In addition, the system BPT contains a scheme of induction for least fixed-point recursion. This scheme can be used to prove useful program transformation rules like the reduction of nested as well as iterated recursion to simultaneous recursion (cf. Moschovakis' Formal Language of Recursion FLR). Moreover, logics for strict (call-by-value) and lazy (call-by-name) evaluation can be obtained from BPT in a very simple way. For call-by-value we add axioms saying that variables are defined; for call-by-name we require axiomatically that each type contains undefined objects. Since both extensions are adequate for the corresponding evaluation strategy, we have a simple logical explanation of call-by-value and call-by-name evaluation.

T. Strahm:
Large Metapredicativity

Metapredicativity is a new general term in proof theory which describes the analysis and study of formal systems whose proof-theoretic strength is beyond the Feferman-Schütte ordinal Γ_0 but which are nevertheless amenable to predicative methods.

In this talk we give a general survey and introduction to metapredicativity. In particular, we discuss various examples of metapredicative systems, including (i) subsystems of second order arithmetic, (ii) first and second order fixed point theories, (iii) extensions of Kripke-Platek set theory without foundation, and (iv) systems of explicit mathematics with universes.

Relevant keywords for our talk are: arithmetical transfinite recursion and dependent choice; restricted bar induction; transfinite hierarchies of fixed points; transfinite fixed point recursion; hyper inaccessibility, Mahloness without foundation and beyond; universe operators.

G. Takeuti:
Forcing and complexity theory

This is a joint work with M. Yasumoto.

Let N be a countable model of the true arithmetic $Th(\mathbb{N})$ where $\mathbb{N}$ is a standard model of arithmetic. Let $n \in N$ be a nonstandard element.
Then

$$M = \{x \in N \mid x \leq n\#\cdots\#n \text{ for some } n\#\cdots\#n\}$$

is a model of bounded arithmetic S_2. Let $n_0 = \mid n \mid$ and $M_0 = \{\mid x \mid \mid x \in M\}$ where $\mid a \mid$ is the length of the binary expression of a. Now introduce boolean variables $p_0, p_1, \ldots, p_{n_0-1}$ and generate a boolean algebra obtained from polynomial size circuit from $p_0, p_1, \ldots, p_{n_0-1}, 0, 1$. We define $M^B := \{X \in M \mid \exists y \in M_0(X : y \to B)\}$. Let I be an ideal of B. I is said to be M_0-complete if

$$a_0 \in M \qquad \forall i < a_0(b_i \in I) \to \bigvee_{i<a_0} b_i \in I.$$

Since M, B, I are all countable, if $i \in I$ then by forcing we can have a generic ultrafilter G such that $G \cap I = \emptyset$. Let us denote a morphism made by G by h_G, and define $M[G] = \{h_G(X) \mid X \in M^B\}$ where for $X : y \to B$, $h_G(X) : y \to \{0,1\}$ is defined by $i < y \to h_G(X)(i) = h_G(a) = a$.

$M[G]$ satisfies:

1. Polynomial time computable functions are defined in $M[G]$.
2. Let $\varphi(a)$ be a sharply bounded formula. Then $M \models \forall x\varphi(x) \longrightarrow M[G] \models \forall x\varphi(x)$.
3. If $M[G]$ is not a model of S_2, then $P \neq NP$.

We conjecture that most $M[G]$ are not a model of S_2, since the true definition $[\![\varphi]\!] \in B$ is defined for every sharply bounded formula φ by

$$[\![\exists x \leq |t|\, \varphi(x)]\!] = \bigvee_{x\leq|t|} [\![\varphi(x)]\!] \qquad |t| \in M_0 [\![\forall x \leq |t|\, \varphi(x)]\!] = \bigwedge_{x\leq|t|} [\![\varphi(x)]\!]$$

but $[\![\varphi]\!]$ cannot be defined for not sharply bounded formulas.

This is the basic theory of forcing. We discuss two specific cases.

1. A subset C of M is a *cut* in M iff

$$(i) \quad a \in C \rightarrow a+1 \in C$$
$$(ii) \quad b < a \in C \rightarrow b \in C$$

C in M is M_{00}-inaccessible ($M_{00} = \{|x| \mid x \in M_0\}$) iff $\forall a \in M_{00} \forall f \in M$:

$$f : a \rightarrow M \text{ mon. incr. } f(0) < C < f(a-1) \rightarrow \exists x \in a. f(x) < C < f(x+1)$$

Theorem: There exists an M_{00}-inaccessible cut C in M_0.

Let $G = (V, E)$ be a graph. $S \subseteq V$ is a *clique* in G iff

$$\forall v, v' \in S (v \neq v' \Rightarrow \{v, v'\} \in E).$$

The *clique number* of a graph $G = (V, E)$ is k iff

$$\forall S \text{ a clique } |S| \leq k \qquad \wedge \qquad \exists S \text{ a clique } |S| = k$$

The *independent number* of a graph $G = (V, E)$ is k iff

$$\forall S \text{ independent set } |S| \leq k \qquad \wedge \qquad \exists S \text{ independent set } |S| = k$$

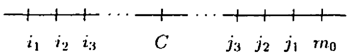
S is an *independent set* iff

$$\forall v, v' \in S (v \neq v' \Rightarrow \{v, v'\} \notin E)$$

Let C be M_{00}-inaccessible and

$$i_1 < i_2 < \ldots \rightarrow C \qquad ; \qquad j_1 > j_2 > \ldots \rightarrow C$$

$$i_1 > 3, \ldots, i_{k+1} - i_k > 3k, \ldots \qquad ; \qquad m_0 - j_1 > 3, \ldots, j_k - j_{k+1} > 3k, \ldots$$



Let $n_0 = \frac{m_0(m_0-1)}{2}$. Then we define a function $\{s_1, s_2\}$ such that

$$s_1 \neq s_2; \ s_1, s_2 < m_0 \longrightarrow \{s_1, s_2\} < n_0; \ \{s_1, s_2\} = \{s_2, s_1\}$$

Let $A : n_0 \rightarrow B$, $A(i) = p_i$, m_0 be the set of vertices. Let $[i] = \{0, 1, \ldots, i-1\}$. We define $b_1, b_2, \ldots, b'_1, b'_2, \ldots$ by

$$\neg b_{k+1} = [\![\, [i_{k+1}] - [i_k] \text{ has the clique number } i_{k+1} - i_k - k$$
$$\text{but } [i_{k+1} + 1] - [i_k] \text{ has no } (i_{k+1} + 1) - i_k - k \text{ clique} \,]\!]$$
$$b'_{k+1} = [\![\, [j_k + 1] - [j_{k+1} + 1] \text{ has the independent number } j_k - j_{k+1} - k$$
$$\text{but } [j_k + 1] - [j_{k+1}] \text{ has no } j_k + 1 - j_{k+1} - k \text{ independent set} \,]\!]$$

Conjecture: Let I be the M_0-complete ideal generated by $b_1, b_2, \ldots, b'_1, b'_2, \ldots$. Then $1 \notin I$.

Theorem: The conjecture implies $P \neq NP$.

2. This time we introduce Boolean variables p_i for every $i \in M$ and generate Boolean algebra B by polynomical size circuit from $p_1, p_2, \ldots, p_i, \ldots$. Let $a_0 \in M_0$ and

$d \in M$. Define $t_d : a_0 \to B$ by $t_d(i) = p_{a_0 d+i}$. For $d < d'$ define $b_{d,d'} = [\![t_{d'} \leq t_d]\!]$. Let I be an M_0-complete ideal from $b_{d,d'}$ $(d < d')$.

Theorem: $1 \notin I$.

We discuss the interesting model $M[G]$ obtained from this I.

S. Terwijn:
Algorithmic Randomness and Lowness II

This is the counterpart of the talk by D. Zambella. We present some joint work with Antonin Kucera.

We prove that there is a nonrecursive set A that is low for the class $\mathcal{R}$ of Martin-Löf-random sets, i.e. A is such that $\mathcal{R} = \mathcal{R}^A$.

S.Tupailo:
Finitary reductions for local predicativity

Using the concept of notations for infinitary derivations, introduced by Buchholz, we define finitary reductions corresponding to the method of local predicativity. First we consider infinitary system $T^{\infty}_{\Sigma_1}$ of recursively inaccessible ordinals and define continuous operators $\mathcal{E}_\gamma$ of predicative cut elimination, bounding operators $\mathcal{B}_{C,\beta}$, and collapsing operator $\mathcal{D}$. Their properties are:

$$\begin{array}{lcll} d \vdash^{\alpha}_{\sigma} \Gamma & \Rightarrow & \mathcal{E}_\gamma(d) \vdash^{\varphi(\gamma,\alpha)}_{\sigma - \omega^\gamma} \Gamma & \\ d \vdash^{\alpha}_{\sigma} \Gamma, C & \Rightarrow & \mathcal{B}_{C,\beta}(d) \vdash^{\alpha}_{\sigma} \Gamma, C^\beta & if \quad C \in \Sigma^1_1 \quad and \quad \alpha \leq \beta \\ d \vdash^{\alpha}_{\Omega} \Gamma & \Rightarrow & \mathcal{D}(d) \vdash^{\vartheta\alpha}_{\vartheta\alpha} \Gamma & \end{array}$$

Then we consider finitary system $T^{\bullet}_{\Sigma_1}$,which includes inference symbols

$$\frac{\emptyset}{\emptyset}(\mathcal{E}_\gamma) \qquad \frac{C}{C^\beta}(\mathcal{B}_{C,\beta}) \;, C \in \Sigma_1 \qquad \frac{\emptyset}{\emptyset}(\mathcal{D})$$

and show how reductions for this system are derived from infinitary ones.

Our work explains T.Arai's reductions for the system T_2 of Π_2-reflecting ordinals.

A. Visser:
The admissible rules of Heyting Arithmetic

We show that the admissible rules in the language of IPC for substitutions in HA are precisely the same as the admissible rules for substitutions in IPC. The proof uses a result due to Ghilardi who shows that the exact formulas are precisely the formulas with the extension property.

A. Voronkov:
Herbrand's theorem and equational reasoning

We discuss some decision problems for logic with equality related to Herbrand's theorem. Then we explain how results on these decision problems helped us to classify decidable prenex classes of intuitionistic logic.

A. Weiermann:
Term rewriting and Proof Theory

In the first talk we survey recursion- and proof-theoretic analyses of termination proofs for rewrite systems. In particular we analyze termination orderings in terms of the slow growing hierarchy. Finally we present some surprising results about the growth rate of the slow growing hierarchy. Remarkably the hierarchy $(G_\alpha)_{\alpha<\varepsilon_0}$ becomes fast growing if its underlying system of fundamental sequences is defined as follows: $(\omega^\alpha+\lambda)[x] = \omega^\alpha + \lambda[x+1]$; $\omega^\lambda[x] = \omega^{\lambda[x]}$; $\omega^{\alpha+1}[x] = \omega^\alpha \cdot (x+1)$. (Here we assume $\omega^\alpha + \lambda > \lambda \in Lim$.)

In the second talk we present a constructive termination proof for Gödel's system T which is of lowest possible proof-theoretic complexity. Using methods of Howard and Schütte we define a function $I : T \to \omega$ such that $(\forall s, t \in T)[s$ reduces to $t \Rightarrow I(s) > I(t)]$. Among other things this result yields an optimal derivation lengths classification for T and its fragments.

D. Zambella:
Algorithmic randomness and lowness

Abstract: I shall discuss Martin-Löf and Schorr random sets and sets that are low for these classes. I will give a recursion theoretic characterization (notably, not mentioning measure) of being low for Schorr random (a result obtained with S. Terwijn). I shall compare this result with one of Kucera and Terwijn on lowness for Martin-Löf random sets.

Berichterstatter: Ulrich Berger.

E-mail Adressen:

Aczel	petera@cs.man.ac.uk
Ambos-Spiess	ambos@math.uni-heidelberg.de
Avigad	avigad+@cmu.edu
Berger	berger@rz.mathematik.uni-muenchen.de
Bezem	Marc.Bezem@phil.ruu.nl
Buchholz	buchholz@rz.mathematik.uni-muenchen.de
Cantini	cantini@vm.idg.fi.cnr.it
Cichon	Adam.Cichon@loria.fr
Clote	clote@informatik.uni-muenchen.de
Coquand	coquand@cs.chalmers.se
David	Rene.David@univ-savoie.fr
Diller	dillerj@math.uni-muenster.de
Dyckhoff	rd@dcs.st-and.ac.uk
Gordeew	gordeew@informatik.uni-tuebingen.de
Hindley	j.r.hindley@swansea.ac.uk
Hudelmaier	joerg@informatik.uni-tuebingen.de
Jervell	herman.jervell@ilf.uio.no
Keimel	keimel@mathematik.tu-darmstadt.de
Kohlenbach	kohlenb@brics.dk
Matthes	matthes@informatik.uni-muenchen.de
Mints	mints@csli.stanford.edu
Moerdijk	moerdijk@math.ruu.nl
Moschovakis	ynm@math.ucla.edu
Niggl	niggl@rz.mathematik.uni-muenchen.de
Normann	dnormann@math.uio.no
Palmgren	palmgren@math.uu.se
Pohlers	pohlers@math.uni-muenster.de
Rathjen	rathjen@amsta.leeds.ac.uk
Scedrov	scedrov@saul.cis.upenn.edu
Schwichtenberg	schwicht@rz.mathematik.uni-muenchen.de
Selinger	selinger@brics.dk
Setzer	setzer@math.uu.se
Staerk	robert.staerk@unifr.ch
Stoltenberg-Hansen	viggo@math.uu.se
Strahm	strahm@iam.unibe.ch
Takeuti	takeuti@saul.cis.upenn.edu
Terwijn	terwijn@wins.uva.nl
Troelstra	anne@wins.uva.nl
Tupailo	sergei@cs.ioc.ee
Voronkov	voronkov@csd.uu.se
Wainer	pmt6ssw@sun.leeds.ac.uk
Weiermann	weierma@ESCHER.UNI-MUENSTER.DE
Zambella	domenico@wins.uva.nl

Tagungsteilnehmer

Prof.Dr. Peter Aczel
Dept. of Computer Science
University of Manchester
Oxford Road

GB-Manchester M13 9PL

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

80333 München

Prof.Dr. Klaus Ambos-Spies
Mathematisches Institut
Universität Heidelberg
Im Neuenheimer Feld 288

69120 Heidelberg

Prof.Dr. Andrea Cantini
Dipt. di Filosofia
Universita degli Studi di Firenze
Via Bolognese 52

I-50139 Firenze

Dr. Jeremy Avigad
Department of Philosophy
Carnegie Mellon University
Schenley Park

Pittsburgh , PA 15213-3890
USA

Dr. Adam Cichon
INRIA-Lorraine-CNRS-CRIN
BP 101

F-54602 Villes-les-Nancy

Dr. Ulrich Berger
Mathematisches Institut
Universität München
Theresienstr. 39

80333 München

Prof.Dr. Peter Clote
197 Commonwealth Avenue

Chestnut Hill , MA 02167
USA

Dr. Marc Bezem
Filosofische Faculteit
Universiteit Utrecht
Postbus 80126

NL-3508 TC Utrecht

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

S-41296 Göteborg

Prof.Dr. Rene David
Lab. de Mathematiques (LAMA)
Universite de Savoie

F-73376 Le Bourget du Lac Cedex

Dr. Jörg Hudelmaier
WSI
Universität Tübingen
Sand 13

72076 Tübingen

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

48149 Münster

Prof.Dr. Herman R. Jervell
Universitetet Oslo
ILF - Boks 1102, Blindern

N-0317 Oslo

Dr. Roy Dyckhoff
Dept. of Math. and Computational
Sciences
Computational Science Division
North Haugh

GB-St. Andrews , Fife KY16 9SS

Prof.Dr. Klaus Keimel
Fachbereich Mathematik
TU Darmstadt
Schloßgartenstr. 7

64289 Darmstadt

Lev Gordeev
WSI für Informatik, Logik und
Sprachtheorie
Köstlinstr. 6

72076 Tübingen

Dr. Ulrich Kohlenbach
BRICS, Dept. of Computer Science
University of Aarhus
Ny Munkegade Bldg. 540

DK-8000 Aarhus C

Dr. James Roger Hindley
Dept. of Mathematics
University College of Swansea
Singleton Park

GB-Swansea SA2 8PP

Prof.Dr. Horst Luckhardt
Weißenburgstr. 21

61184 Karben

Ralph Matthes
Mathematisches Institut
Universität München
Theresienstr. 39

80333 München

Prof.Dr. Dag Normann
Institute of Mathematics
University of Oslo
P. O. Box 1053 - Blindern

N-0316 Oslo

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

Stanford , CA 94305
USA

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

S-75106 Uppsala

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

NL-3508 TA Utrecht

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

48149 Münster

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

Los Angeles , CA 90095-1555
USA

Dr. Michael Rathjen
School of Mathematics
University of Leeds

GB-Leeds , LS2 9JT

Dr. Karl-Heinz Niggl
Mathematisches Institut
Universität München
Theresienstr. 39

80333 München

Prof.Dr. Andre Scedrov
Department of Mathematics
University of Pennsylvania
209 South 33rd Street

Philadelphia , PA 19104-6395
USA

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

80333 München

Dr. Thomas Strahm
Institut für Informatik und
Angewandte Mathematik
Universität Bern
Neubruckstr. 10

CH-3012 Bern

Dr. Peter Selinger
Dept. of Mathematics
The University of Michigan
525 East University Avenue

Ann Arbor , MI 48109-1109
USA

Prof.Dr. Gaisi Takeuti
Academy House 35R
1420 Locust St.

Philadelphia , PA 19102
USA

Dr. Anton Setzer
Department of Mathematics
University of Uppsala
P.O. Box 480

S-75106 Uppsala

Sebastiaan A. Terwijn
Fac. of Math. & Computer Sciences
University of Amsterdam
Plantage Muidergracht 24

NL-1018 TV Amsterdam

Dr. Robert F. Stärk
Institute of Informatics
University of Fribourg
Rue Faucigny 2

CH-1700 Fribourg

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

NL-1018 TV Amsterdam

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

S-75106 Uppsala

Dr. Sergei Tupailo
Dept. of Mathematics
Stanford University

Stanford , CA 94305
USA

Prof.Dr. Albert Visser
Filosofische Faculteit
Universiteit Utrecht
Postbus 80126

NL-3508 TC Utrecht

Prof.Dr. Andrei Voronkov
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

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

48149 Münster

Dr. Domenico Zambella
Fac. of Math. & Computer Sciences
University of Amsterdam
Plantage Muidergracht 24

NL-1018 TV Amsterdam