THE BULLETIN OF SYMBOLIC LOGIC
Volume 9, Number 1, March 2003

2002 ANNUAL MEETING OF THE ASSOCIATION FOR SYMBOLIC LOGIC

University of Nevada, Las Vegas, Las Vegas, Nevada
June 1–4, 2002

The Annual Meeting of the Association was held on the campus of the University of Nevada, Las Vegas, June 1–4, 2002. The program included the Thirteenth Annual Gödel Lecture, eleven invited talks, four special sessions, and sixteen contributed talks. The members of the Program Committee were G. Cherlin, D. Dubose, W. Goldfarb, J. Larson, A. Scedrov, and T. Slaman (Chair). The members of the Local Organizing Committee were D. Burke, D. DuBose (Chair), and K. J. Mourad. There were 84 registered participants at the meeting, including 16 graduate students. Generous financial support was provided by the University of Nevada, Las Vegas and the Association for Symbolic Logic. The ASL hosted a welcoming reception.

The Thirteenth Annual Gödel Lecture, *Issues in the foundations of mathematics*, was presented by Harvey Friedman (Ohio State University). On doctor's advice, Professor Friedman did not travel to the meeting, and his paper was read in his absence by Theodore A. Slaman. The hour-long invited addresses included:

Scot Adams (University of Minnesota), *The origins of lattice superrigidity and dynamical superrigidity*.

Edmund Clarke (Carnegie Mellon University), *Symbolic model checking "with" and "without" BDDs*.

Greg Hjorth (UCLA), *An "easy" proof of a theorem by Adams and Kechris*.

Shaughan Lavine (University of Arizona), *The axiomatic method*.

Zlil Sela (Hebrew University), *Diophantine geometry over groups and the elementary theory of free and hyperbolic groups*.

Natarajan Shankar (SRI International), *Little engines of proof*.

Stephen Simpson (Pennsylvania State University), *Reverse mathematics*.

Stevo Todorcevic (University of Toronto and CNRS-Paris 7), *Metamathematical methods in Ramsey Theory*.

William Tait (University of Chicago), *Dialectic and logic: the truth of axioms*.

W. Hugh Woodin (University of California, Berkeley), *Beyond Σ^2_1 absoluteness*.

Jessica Young (MIT), *On Martin's conjecture*.

There also were special sessions (with organizers given in parentheses) on Set Theory (W. H. Woodin), Computers in Logic Education (J. Larson), Logic in Computer Science (E. Clarke and N. Shankar), and Philosophy of Mathematics (W. Tait), with a total of 28 speakers.

Abstracts of talks given in person or by title by members of the Association for Symbolic Logic follow.

For the Program Committee
THEODORE A. SLAMAN

1079-8986/03/0901-0005/$3.00

Abstracts of invited plenary talks

► SCOT ADAMS, *The origins of lattice superrigidity and dynamical superrigidity*.
School of Mathematics, Vincent Hall, 206 Church St. SE, University of Minnesota, Minneapolis, Minnesota 55455, USA.
E-mail: adams@math.umn.edu.

I will discuss G. Margulis' superrigidity theorem. I will indicate how it arose and how R. Zimmer adapted it to dynamics as part of a larger program initiated by G. Mackey. I will also attempt to explain how this dynamical reformulation found application to the study of Borel reducibility of equivalence relations.

► EDMUND M. CLARKE, JR., *Symbolic model checking "with" and "without" BDDs*.
Department of Computer Science, Carnegie Mellon University, Pittsburgh, Pennsylvania 15228, USA.
E-mail: emc@cs.cmu.edu.

Logical errors in finite-state concurrent systems such as sequential circuit designs and communication protocols are an important problem for computer scientists. They can delay getting a new product on the market or cause the failure of some critical device that is already in use. *Temporal logic model checking* is an automatic verification technique for this class of systems. In this approach specifications are expressed in a propositional temporal logic, while circuits and protocols are modeled as state-transition systems. An efficient search procedure is used to determine automatically if a specification is satisfied by some transition system. The technique has been used in the past to find subtle errors in a number of non-trivial examples.

During the past decade, the size of the state-transition systems that can be verified by model checking techniques has increased dramatically. By representing transition relations implicitly using Binary Decision Diagrams (BDDs), it is possible to check some examples that would have required 10^{20} states with the original algorithm. Various refinements of the BDD-based techniques have pushed the state count up to 10^{100}. By combining model checking with various abstraction techniques, even larger systems can be handled. For example, this technique has been used to verify the cache coherence protocol in the IEEE Futurebus+ Standard. Several errors were found that had been previously undetected. Apparently, this is the first time that formal methods have been used to find nontrivial errors in an IEEE standard.

Although model checking is already useful for verifying many circuit and protocol designs that arise in industry, additional research is needed to exploit the full power of this method. For example, a new technique called *bounded model checking* has been developed that uses fast propositional decision procedures like GRASP and Stahlmarck's algorithm instead of BDDs to handle even larger examples. The new technique has been used to verify twenty-one complex circuits from the Power PC Microprocessor. Traditional model checking techniques based on BDDs were only able to handle one of the circuits we tried.

► GREG HJORTH, *An "easy" proof of a theorem by Adams and Kechris*.
Department of Mathematics, Mathematical Sciences Building 7340, University of California at Los Angeles, Los Angeles, California 90095-1555, USA.
E-mail: greg@math.ucla.edu.

I will sketch a proof of a theorem by Adams and Kechris, which if not all that easy is at least relatively elementary.

► SHAUGHAN LAVINE, *The axiomatic method.*
Department of Philosophy, University of Arizona, P. O. Box 210027, Tucson, Arizona 85721-0027, USA.
E-mail: shaughan@ns.arizona.edu.

Skolem concluded mathematics is "irreducibly relative." Few followed him. But he drew a widely accepted prior conclusion: There are no non-question-begging categorical axiomatizations of mathematical structures like the natural numbers and the pure sets. But categorical axioms *can* be devised for the natural numbers and *quasicategorical* axioms can be devised for the sets—axioms that guarantee categoricity modulo a choice of height.

Skolem divided logical systems into first-order logic and higher-order and infinitary logic. He proved that first-order logic cannot categorically axiomatize any nontrivial mathematical structure, and he argued that stronger logics presuppose too much. He concluded that axiomatic categorization fails—that is what I contest.

Feferman's full schematic logic suffices for proving the (quasi)categoricity of suitable axiom systems. The proofs are adaptations of some used, though Skolem would argue in a question-begging way, for second-order axiomatizations.

The suggested axioms and theorems in full schematic logic beg no questions. This is the heart of the argument, and the issues are entirely philosophical.

The acceptance of Skolem's criticism of the axiomatic method has led to the belief that, for example, the continuum hypothesis is neither determinately true nor determinately false. In fact, many such problems concerning sets are well-posed problems about a well-characterized system and hence must have determinate answers.

► ZLIL SELA, *Diophantine geometry over groups and the elementary theory of free and hyperbolic groups*.
Mathematics Department, Hebrew University, Jerusalem 91904, Israel.
E-mail: zlil@math.huji.ac.il.

We study sets of solutions to equations over a free group, projections of such sets, and the structure of elementary sets defined over a free group. The structure theory we obtain enables us to answer some questions of A. Tarski's, and classify those finitely generated groups that are elementary equivalent to a free group. Connections with low dimensional topology, and a generalization to general hyperbolic groups and their elementary classification will also be discussed.

► NATARAJAN SHANKAR, *Little engines of proof*.
SRI International Computer Science Laboratory, Menlo Park, California 94025, USA.
E-mail: shankar@csl.sri.com.

Verification aims to show that computer hardware and software designs achieve their intended function. The construction of a mathematical proof is one method for debugging and verifying the correctness of complex designs. Proofs of this scale can be reliably constructed only through the use of efficient automation. In the absence of a single sledgehammer for automating proofs, some quite modest decision procedures are finding limited success. These include propositional satisfiability solvers, ground decision procedures for equality and arithmetic, quantifier elimination procedures for integers and reals, and abstraction techniques for finding finite approximations of problems over infinite domains. We describe some of these "little engines of proof" and the challenge of building proofs that combine individual decision methods.

► STEPHEN G. SIMPSON, *Reverse mathematics*.
Department of Mathematics, Pennsylvania State University, University Park, State College, Pennsylvania 16802, USA.
E-mail: simpson@math.psu.edu.

Foundations of mathematics is the study of the most basic concepts and logical structure of mathematics as a whole. Reverse mathematics is the foundational program of discovering which set existence axioms are needed to prove known theorems in core mathematical areas such as algebra, analysis, geometry, countable combinatorics. It turns out that a large number of theorems fall into a small number of equivalence classes with respect to provable equivalence over a weak base theory. (See my book ***Subsystems of Second Order Arithmetic***, Springer-Verlag, 1999.) The equivalence classes appear to reflect well known philosophical/foundational programs such as constructivism (Bishop), finitistic reductionism (Hilbert), predicativism (Weyl, Feferman), predicative reductionism, and impredicative analysis. In this talk I comment on the mathematical, philosophical, and foundational significance of reverse mathematics as it has developed from the early 1970's to the present. I also comment on the significance of reverse mathematics for the principal subdivisions of mathematical logic: model theory, set theory, recursion theory, proof theory.

► W. W. TAIT, *Dialectic and logic*: *the truth of axioms*.
The University of Chicago, 5522 S. Everett Ave., Chicago, Illinois 60637, USA.
E-mail: wwtx@midway.uchicago.edu.

I will discuss the question of what determines truth in mathematics and, expanding on [1], advance the (now fairly unfashionable) thesis of Hilbert (and of Plato) that it is (in a certain sense) defined by the axioms. I particularly want to confront the sense one has that questions of truth are involved in the choice of basic concepts and axioms.

[1] W. W. TAIT, *Beyond the axioms*: *the question of objectivity in mathematics*, ***Philosophia Mathematica***, vol. 9 (2001), pp. 21–26.

► STEVO TODORCEVIC, *Metamathematical methods in Ramsey Theory*.
Université de Paris 7 – C. N. R. S., U. F. R. de Mathématiques – U. M. R. 7056, 2, Place Jussieu – Case 7012, 75251 Paris Cedex 05, France.
E-mail: stevo@math.jussieu.fr.

This will be a survey of recent work in Ramsey theory with a particular emphasis on the use of Forcing in proving theorems rather than independence results in this area of mathematics.

► W. HUGH WOODIN, *Beyond* Σ^2_1 *absoluteness*.
Department of Mathematics, University of California at Berkeley, Berkeley, California 94720-3840, USA.
E-mail: woodin@math.berkeley.edu.

Assuming there exists a proper class of measurable Woodin cardinals then Σ^2_1 sentences are absolute between generic extensions of V satisfying CH.

A sentence is $\Sigma^2_2(\mathcal{I}_{\mathrm{NS}})$ if it is logically equivalent (over ZFC) to the assertion that

$$\langle H(c^+), \mathcal{I}_{\mathrm{NS}}, \in\rangle \vDash \phi$$

for some Σ_2 sentence ϕ. Here $\mathcal{I}_{\mathrm{NS}}$ denotes the nonstationary ideal on ω_1. Thus $\Sigma^2_2(\mathcal{I}_{\mathrm{NS}})$ sentences are at worst Σ^2_3.

The Ω Conjecture implies that $\Sigma^2_2(\mathcal{I}_{\mathrm{NS}})$ absoluteness fails conditioned on *any* Σ_2 sentence. This leaves open the case of Σ^2_2 absoluteness.

If M is an iterable Mitchell-Steel model in which there is a proper class of Woodin cardinals then necessarily Σ^2_2 absoluteness fails in M conditioned on any Σ_2 sentence which can hold is a generic extension of M. This strongly suggests that no large cardinal hypothesis below that of superstrong can suffice to prove conditional Σ^2_2 absoluteness.

We shall discuss various further results on obtaining Σ^2_2 absoluteness.

► JESSICA M. YOUNG, *On Martin's conjecture*.
Department of Mathematics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA.
E-mail: jessica@math.mit.edu.

Given a consistent first order theory T, let L' be the language fragment generated by the consistent types of T. Martin's conjecture states that if T has fewer than continuum many countable models, then for every model M of T, the L' theory of M is $\aleph_0$ categorical. Martin's conjecture is a substantial strengthening of Vaught's conjecture. We provide a counterexample to Martin's conjecture. The example stems from research on the structure of theories with finitely many countable models.

Abstracts of invited talks in the Special Session on Computers in Logic Education

▶ ALDO ANTONELLI, *Teaching logic with LPL*.
Department of Logic and Philosophy of Science, University of California at Irvine, Irvine, California 92697-5100, USA.
E-mail: aldo@uci.edu.

This talk presents an overview of the instructor's experience teaching logic using J. Barwise and J. Etchemendy's software/textbook package "Language, Proof, and Logic". Both practical and theoretical issues are considered. Among the former: advantages and disadvantages of using LPL compared to more traditional instruction; automated grading using the "Grade Grinder", and grade distribution issues; problems related to licensing and costs; student's reactions. Among the latter, we look at the logical properties of the LPL framework and consider issues such as soundness, completeness, etc.

▶ STANLEY N. BURRIS, *Computer enhancements to my course "Logic for mathematics and computer science"*.
Department of Pure Mathematics, University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada.
E-mail: snburris@thoralf.uwaterloo.ca.

This talk will focus on the software that I use in conjunction with the course in logic that I have taught several times at the University of Waterloo. The object of the course is to combine the traditional treatment of logic with the logic needed in automated theorem provers such as "Otter". I wrote a number of simple interactive web programs that I use to demonstrate key ideas, and these will be discussed in my talk.

▶ DAVID KAPLAN, *Logic 2000*.
Department of Philosophy, University of California at Los Angeles, Los Angeles, California 90095-1451, USA.
E-mail: kaplan@ucla.edu.

Logic 2000 is a *system* for computer and Internet assisted classroom instruction in first order logic. Versions of the program have been used at UCLA since 1985. It contains modules for doing derivations, symbolizations, truth tables, invalidity by finite models, and parsing. The system of derivation is based on the natural deduction system created by Kalish and Montague. In this version, our aim has been to construct a system in which Instructors instruct, while tutorials, grading, and clerical work are done by the system.

Instructors create Assignments on a web page for students to complete within the program, which contains a variety of handy tools to simplify the mechanics of entering work. The program corrects the student's work and provides several layers of detailed error messages along with hints and explanations. When satisfied, students submit their work to a Course Database. Students can access their own Assignment Page showing the assignments, work completed, and their score on each problem. Instructors can view a Summary of the work of all students, individual student Assignment Pages, a statistical summary of the Difficulty students had with each problem, etc. Exams are simply another assignment with error messages disabled. *Incorrect* exam work is printed; it receives a "partial credit" review by an instructor.

In the classroom, we use a "big-font" version of the program with a projector. Students learn the use of the program in the background while focusing on learning logic. Following class, we post work done in class on our website.

Students may create their own User Problems, and in the derivation module, students can create and justify their own rules. Derived rules become available as students prove the underlying theorems. Command Mode allows students to construct complete derivations by providing only the justification (which may be "queued") for each line.

► CATHY KESSEL, *Software for undergraduate logic courses*.
Berkeley, California, USA.
E-mail: kessel@soe.berkeley.edu.

This session will discuss various softwares used in undergraduate logic courses. Research findings about the design and use of technology for instruction will provide a context for this discussion.

► WILFRIED SIEG, *Computer based logic instruction*.
Department of Philosophy, Carnegie Mellon University, Pittsburgh, Pennsylvania 15213, USA.
E-mail: sieg@cmu.edu.

I will talk about two related projects that have been pursued at Carnegie Mellon for more than a decade. The first project, VALID, is based on an introduction to logic that was developed at Stanford up through the early 1980s by Patrick Suppes and collaborators. This is a "classical" introduction to first order logic; it has been thoroughly revised and is now fully web based. The second project, APROS (Automated PROof Search), provides the framework in which VALID students can construct natural deduction proofs. The distinctive and pedagogically very effective feature is that they can work "forward" and "backward." APROS, guided by logical strategies, searches itself for natural deduction proofs; I will describe our attempts to use APROS as a tutor providing systematic help to students and also (plans for) a new course in which proof construction takes center stage.

► DANIEL J. VELLEMAN, *Proof Designer*: *Software for learning to write proofs*.
Department of Mathematics and Computer Science, Amherst College, Amherst, Massachusetts 01002-5000, USA.
E-mail: djvelleman@amherst.edu.

I will demonstrate a java applet called Proof Designer that is intended to help students learn to write proofs. Proof Designer acts as a "referee" while the student tries to construct a proof in elementary set theory. Proof Designer allows the student to choose from a variety of proof strategies and rules of inference, but it refuses to tolerate incorrect reasoning or nonsense. Proof Designer can be found at http://www.cs.amherst.edu/~djv/pd/pd.html.

Abstracts of invited talks in the Special Session on Logic in Computer Science

► GILLES DOWEK, *Binding logic*: *proofs and models*.
INRIA, BP 105, 78153 Le Chesnay Cedex, France.
E-mail: Gilles.Dowek@inria.fr.

In many applications of logic to computing science, we need to construct theories where some parts of mathematics can be formalized, not only in principle, but also in facts. To this end, usual frameworks such as predicate logic and set theory require slight modifications. For example, it may be useful to be able to distinguish proofs that require a genuine deduction and those that require just a computation. It may be also useful to be able to express terms in a language that allows variable binding, like the "informal" language of mathematics.

In this talk, we will define an extension of predicate logic where variables can be bound in terms and in propositions. We will introduce a notion of model for this logic and we prove a completeness theorem. Finally, we will give simple examples of independence results that can be obtained with such models.

This is joint work with Thérèse Hardin and Claude Kirchner.

► E. ALLEN EMERSON, *Parameterized model checking*.
Computer Sciences Department, Taylor Hall 2.124, University of Texas, Austin, Texas 78712, USA.
E-mail: emerson@cs.utexas.edu.

Traditional model checking deals with systems of a fixed, finite size, e.g., systems composed of three or ten finite state processes running in parallel. In the Parameterized Model Checking Problem (PMCP) we consider infinite uniform families of systems each comprised of n homogeneous processes running in parallel. The problem is to determine whether such a system is correct for every size n. This provides a solution to the state explosion and scaling problems in one fell swoop. Unfortunately, PMCP is in general algorithmically unsolvable.

Because of its importance for applications, PMCP has nonetheless garnered a great deal of attention yielding various partial or restricted solutions. We overview some of those and then describe some of our recent work with Vineet Kahlon, identifying useful frameworks permitting the reduction of PMCP to model checking over systems composed of c homogeneous processes, for small constant c. It follows that in this framework PMCP is decidable, in some cases efficiently.

► AMY FELTY, *An introduction to proof-carrying code*.
School of Information Technology and Engineering (SITE), University of Ottawa, 800 King Edward Ave., Ottawa, Ontario K1N 6N5, Canada.
E-mail: afelty@site.uottawa.ca.

Proof-carrying code (PCC) is an application of formal logic and formal proof that provides a mechanism which allows a host, or code consumer, to safely run code delivered by an untrusted code producer. The host specifies a safety policy as a set of axioms and inference rules. The code producer delivers both a program and a formal proof that verifies that the code meets the desired safety policies. PCC safety policies typically include properties that prohibit the code from harmful behavior such as accessing private data, overwriting important data, accessing unauthorized resources, or consuming too many resources. Ideally, a proof is constructed automatically, and proof search may be directed using information that is passed on from the code producer's compiler. Proofs provided semi-automatically or interactively using a proof assistant are possible as well. Upon receiving the code and proof, the code consumer uses a mechanical proof checker to check the proof before executing the code. A principal advantage of this approach to software safety is that the trusted code base is extremely small; it includes only the proof checker for verifying the proof of safety.

This talk will present an overview of PCC and also introduce our approach to PCC, called foundational proof-carrying code, which provides increased security and greater flexibility in the construction of proofs of safety.

► JOHN R. HARRISON, *Formal verification of mathematical algorithms*.
Intel Labs, Intel Corporation, JF1-13, 2111 NE 25th Avenue, Hillsboro, Oregon 97124, USA.
E-mail: johnh@ichips.intel.com.

An important feature of typical computer systems is the computation of basic mathematical functions, mainly in floating-point arithmetic. This includes basic arithmetic operations like division as well as common transcendental functions like "exp" and "sin" and more obscure ones like gamma and Bessel functions. Since they often depend on some non-trivial mathematics and subtly exploit the special features of floating-point operations, they are relatively difficult to design without error. The costs to a company like Intel of a failure, especially at the hardware level, can be huge. For example, the error in the FDIV (floating-point division) instruction in early Pentium processors in 1994 is believed to have cost Intel about \$500M.

We will describe our work at Intel on the formal verification of some mathematical algorithms that are implemented in microcode and in software libraries on some of Intel's current and forthcoming processors. The work uses the HOL theorem prover, a programmable interactive proof checker for classical higher-order logic. We will describe how a body of classical mathematics (e.g., elementary real analysis) is completely formalized in HOL, and applied to typical applications, exploiting programmability. HOL has the unusual feature of explicitly generating all proofs in terms of basic low-level primitive inferences of the kind typically considered in proof theory. Some of the algorithm verifications involve of the order of 100 million primitive inferences. This can be seen as a realization of the "Principia Mathematica" ideal of actually doing proofs using simple proof systems—with the help of the computer.

► SOMESH JHA, *Applications of model checking to security*.
Computer Sciences Department, University of Wisconsin, Madison, Wisconsin 53706, USA.
E-mail: jha@cs.wisc.edu.

First, I will briefly survey various applications of model checking to security. Next, I will discuss a specific application of model checking to vulnerability analysis of networks.

An attack graph is a succinct representation of all paths through a system that end in a state where an intruder has successfully achieved his goal. Today Red Teams determine the vulnerability of networked systems by drawing gigantic attack graphs by hand. Constructing attack graphs by hand is tedious, error-prone, and impractical for large systems. By viewing an attack as a violation of a safety property, we can use model checking to produce attack graphs automatically: a successful path from the intruder's viewpoint is a counterexample produced by the model checker. In this paper we present an algorithm for generating attack graphs using model checking.

Security analysts use attack graphs for detection, defense, and forensics. In this paper we present a minimization technique that allows analysts to decide which minimal set of security measures would guarantee the safety of the system. We provide a formal characterization of this problem: we prove that it is polynomially equivalent to the minimum hitting set problem and we present a greedy algorithm with provable bounds. We also present a reliability technique that allows analysts to perform a simple cost-benefit analysis depending on the likelihoods of attacks. By interpreting attack graphs as Markov Decision Processes we can use a standard MDP value iteration algorithm to compute the probabilities of intruder success for each attack in the graph.

We illustrate our work in the context of a small example that includes models of a firewall and an intrusion detection system.

► JON MILLEN, *Applications of logic in computer security*.
SRI International, Computer Science Laboraty EL233, 333 Ravenswood Ave., Menlo Park, California 94025, USA.
E-mail: millen@csl.sri.com.

Logics have had both direct and indirect roles in the modelling and analysis of secure systems, including operating systems and Internet protocols. Traditional mathematical logic supports the construction of general-purpose verification environments used in this area. Specialized modal logics have been used to model and verify authentication protocols and schemes for authentication and delegation using digital signature certificates.

► A. PRASAD SISTLA, *Symmetry and model-checking*.
Department of Computer Science (M/C 152), University of Illinois at Chicago, 851 South

Morgan Street, Chicago, Illinois 60607, USA.
E-mail: sistla@cs.uic.edu, sistla@surya.eecs.uic.edu.

Much research has been conducted on using temporal logic model checking for automatic verification of finite state concurrent programs. In this approach, the global state graph of a concurrent program is constructed (explicitly or implicitly) and then its correctness against a temporal logic specification is checked using efficient algorithms. The main bottleneck for this approach is the state explosion problem, i.e., the rapid explosion (exponential) in the number of states to be explored.

One of the major techniques for containing the state explosion problems is to exploit symmetries in the concurrent program. We outline a number of results on exploiting such symmetries for model-checking. Symmetries in the concurrent program induce an equivalence relation on the state space. One approach is to construct a quotient structure corresponding to this equivalence relation and perform model-checking on the quotient structure. In order to make this approach work, in general, we also need to consider the symmetries in the temporal logic formula. We show how the symmetries in the program as well as the formula can be used for model-checking purposes. We also outline a second approach where we only consider program symmetry and construct an Annotated Quotient Structure (AQS). The AQS can be partially unwound to check the correctness of any given formula. More importantly, it can be used to check for correctness under different fairness conditions. The AQS can be extended and used for verification of asymmetric systems also.

► HELMUT VEITH, *Counterexamples in model checking*.
Institut für Informationssysteme, Technische Universität Wien, Favoritenstrasse 9-11, A-1040 Wien, Austria.
E-mail: veith@dbai.tuwien.ac.at.

Model checking is a technique for verifying that a system satisfies its specification by representing the system as a Kripke structure, writing the specification in a suitable temporal logic, and algorithmically checking that the Kripke structure is a model of the specification formula. When the model checking software detects the violation of a specified property, it can in many cases provide the engineer with a diagnostic counterexample. This counterexample exhibits the erroneous behavior and facilitates efficient debugging. Therefore, counterexamples are considered a crucial feature in practical applications of model checking.

In more recent work, we have used the counterexample feature of model checking also to improve the performance of model checking algorithms in large state spaces. In this method, increasingly accurate approximations of the state space are obtained by an adaptive algorithm which analyzes counterexamples over approximate ("abstract") state spaces.

This motivates a systematic investigation of counterexamples in model checking. We introduce a general framework for counterexamples, and show that a large class of universal branching time logics based on ω-regular operators admits counterexamples of a simple combinatorial form similar to finite trees. Such counterexamples can be efficiently generated by symbolic algorithms and render the approximation technique described above complete for important logics such as ACTL.

Abstracts of invited talks in the Special Session on Philosophy of Mathematics

► ALDO ANTONELLI, *Logicism without logic*.
Department of Logic and Philosophy of Science, University of California at Irvine, Irvine, California 92697-5100, USA.
E-mail: aldo@uci.edu.

It is well known that in his only foray into metatheory (1906), Frege proposed an independence test for propositions vaguely reminiscent of Tarski's later permutation method for the characterization of logical constants. We have elsewhere showed that indeed one can further refine the Fregean approach to characterize a class of logically true propositions (and, indirectly, of logical terms), thereby supplying the missing component in Frege's 1906 independence test. (The absence of a general characterization of the logical terms is purportedly the reason why Frege did not further pursue his 1906 approach.) On this approach, one can give conditions on which broader or narrower classes of propositions will turn out to be logically true. These conditions, typically, will deal with the question of what concepts can be assigned value ranges. For Frege, of course, they all did, but after the paradoxes the question takes on a more open-ended character. In this talk we consider the status of this Fregean "New Science" (metatheory), and in particular we look at its existential presuppositions. It will turn out that Fregean metatheory, far from being itself a branch of logic, must be considered a special science with its own specific extra-logical assumptions, on the same footing as, say, geometry or physics. On this basis, it is possible to characterize a "neo-logicist" project in terms that perhaps other recent supporters of neo-logicism did not quite envisage.

This is joint work with Robert May.

► STEVE AWODEY, CARSTEN BUTZ, ALEX SIMPSON, AND THOMAS STREICHER, *Developments in Mac Lane Set Theory*.
Department of Philosophy, Carnegie Mellon University, Pittsburgh, Pennsylvania 15213, USA.
E-mail: awodey@cmu.edu.

This talk reports on the status of recent work in "Mac Lane set theory" (**ML**). Two years ago in [2], S. Mac Lane called for a categorical set theory with a global membership relation $A \in B$ between the sets. In contrast to elementary topos theory with its many different (and useful) interpretations, the idea was to axiomatize categories of *sets* specifically. Mac Lane's proposal was for the category Sets of sets and functions to have a subcategory of distinguished monomorphisms $A \hookrightarrow B$, called *inclusions*, which partially order the objects. Some progress toward this goal has recently been made using the methods of algebraic set theory developed by Joyal and Moerdijk [1]. This approach employs an axiomatic notion of *small maps* in a category, which serve to limit comprehension in a new and flexible way. The axioms of **ML** are a variant of those recently given by Simpson [3] for categorical models of **IZF**.

An apparently new result in this connection is that the axiom scheme of (full) Replacement is conservative over bounded intuitionistic Zermelo set theory.

[1] A. Joyal and I. Moerdijk, ***Algebraic set theory***, LMS Lecture Notes, vol. 220, Cambridge University Press, 1995.

[2] S. Mac Lane, *Foundations by using categories with elements*, Annual Meeting of the Association for Symbolic Logic, Urbana, June 2000.

[3] A. Simpson, *Elementary axioms for categories of classes*, ***14th IEEE Symposium on Logic in Computer Science***, 1999, pp. 77–85.

► MARK BALAGUER, *Intuitionism, psychologism, and excluded middle*.
Department of Philosophy, California State University at Los Angeles, 5151 State University Drive, Los Angeles, California 90032, USA.
E-mail: mbalagu@calstatela.edu.

It is argued here that intuitionism is not related to the law of excluded middle, or psychologistic philosophies of mathematics, in the way that it's commonly thought to be. In particular, it is argued that (a) intuitionism is not entailed by, or even a "natural outgrowth" of, psychologism; rather it is a further claim that advocates of psychologism needn't make. And (b) given intuitionism, psychologism doesn't follow, because intuitionism fits just as well (or poorly, as the case may be) with anti-psychologistic philosophies of mathematics such as platonism and nominalism. And (c) contrary to the traditional wisdom, intuitionism does not involve a rejection of excluded middle (or for that matter, any of the laws of classical logic). And (d) rejecting excluded middle in mathematics doesn't commit one to intuitionism; now, by itself, claim (d) isn't very surprising, but it is also argued here that (i) in mathematics, the law of excluded middle *is* false, but that (ii) this doesn't give rise to reasons to endorse intuitionism, and it doesn't give rise to reasons for abandoning classical proof procedures in mathematics that use excluded middle.

► MATT FRANK, *Working outward from the philosophy of mathematics*.
Committee on the Conceptual and Historical Studies of Science, University of Chicago, 1126 E. 59th St., Chicago, Illinois 60637, USA.
E-mail: mfrank@math.uchicago.edu.

This talk focuses on the interface between philosophy of mathematics and philosophy of science. Often, philosophers' views on mathematics seem guided by their views of science (and I will review some examples), but that is the opposite of the approach to be taken here. I will work outward from the philosophy of mathematics to the philosophy of science, specifically from formalism to instrumentalism. One might work even further outward to other areas of philosophy as well.

► CHRISTOPHER PINCOCK, *The structure of indispensability arguments*.
Department of Philosophy, University of California at Berkeley, Berkeley, California 94720, USA.
E-mail: pincock@mindspring.com.

Indispensability arguments for a realistic interpretation of mathematics have exerted considerable influence on the development of the philosophy of mathematics since they were originally formulated by Quine and Putnam. In this paper I argue that these arguments are not valid. This conclusion is reached based on the assumption that applications of mathematics depend on mappings between physical situations and mathematical domains. While this approach to applications is not universally accepted, it fits in quite naturally with how many philosophers and scientists think about applications.

Based on the assumption that applications depend on mappings I argue that the indispensable role of mathematics in science does not imply a realistic interpretation of mathematics. Briefly, the existence of such mappings depends only on the relational properties of mathematical entities. Any position that recovers these relations will be able to give a mapping-based account of applications. Given that the debate between the realist and the nominalist concerns the non-relational or 'intrinsic' character of mathematical objects, it follows that applications cannot resolve the realist-nominalist debate. Realists and many kinds of nominalists can give interpretations of mathematics that allow for the applicability of mathematics.

The paper concludes with my response to the objection that no nominalist interpretation of mathematics can support the relations between mathematical objects on which applications depend. I point out that this objection amounts to the claim that no nominalist interpretation of pure mathematics is possible. If this claim is added to an indispensability argument for realism, then the argument becomes circular.

► ERICH H. RECK, *Carnap, logicism, and metamathematics*.
Department of Philosophy, University of California at Riverside, Riverside, California 92521-0201, USA.
E-mail: reck@citrus.ucr.edu.

Rudolf Carnap is usually classified as a representative of logicism in the philosophy of mathematics. However, recent discoveries about his early work in "general axiomatics", in the 1920s, call this classification into question (cf. [1], [4]). In this talk I first describe the historical and conceptual background for this work, including some questions concerning the notion, or notions, of completeness raised in Abraham Fraenkel's *Einleitung in die Mengenlehre* (cf. [2]). Then I discuss how Carnap tried to answer these questions. Carnap's attempts, flawed in important respects, nevertheless had two noteworthy results: first, he put Fraenkel's questions into the framework of the simple theory of types, a framework new at the time and especially appropriate in this connection (see also [3]); second, he provided a significant part of the setup and motivation for the subsequent incompleteness theorems of his student Kurt Gödel (cf. [1]).

[1] STEVE AWODEY and ANDRE CARUS, *Carnap, completeness, and categoricity*: *The Gabelbarkeitssatz of* 1928, ***Erkenntnis***, vol. 54 (2001), pp. 145–172.

[2] STEVE AWODEY and ERICH H. RECK, *Completeness and categoricity, Part I*: 19*th century axiomatics to* 20*th century metalogic*, ***History and Philosophy of Logic***, forthcoming.

[3] STEVE AWODEY and ERICH H. RECK, *Completeness and categoricity, Part II*: 20*th century metalogic to* 21*st century semantics*, ***History and Philosophy of Logic***, forthcoming.

[4] ERICH H. RECK, *From Frege and Russell to Carnap*: *Logic and logicism in the* 1920*s*, in ***Rudolf Carnap: From Jena to L. A.*** (S. Awodey and C. Klein, editors), Open Court, Chicago, forthcoming.

► WILFRIED SIEG, *Analysis of computations—without theses*.
Department of Philosophy, Carnegie Mellon University, Pittsburgh, Pennsylvania 05213, USA.
E-mail: ws15@andrew.cmu.edu.

To investigate computations is to analyze symbolic processes that can, in principle, be carried out by calculators. That is a philosophical lesson we owe to Turing. Drawing on, and recasting, work of [1] and [2], I formulate finiteness and locality conditions for two types of calculators, *human computing agents* and *mechanical computing devices*; the distinctive feature of the latter is that they operate in parallel.

Church's and Turing's Thesis assert, dogmatically, that an informal notion of effective calculability is captured by a particular precise mathematical concept. The conceptual analysis of computations I present dispenses with theses. Instead, it leads to axioms for discrete dynamical systems (that represent abstractly human and machine computations) and allows the reduction of models of these axioms to Turing machine computations.

[1] A. TURING, *On computable numbers with an application to the Entscheidungsproblem*, ***Proceedings of the London Mathematical Society***, vol. 42 (1936), pp. 230–265.

[2] R. GANDY, *Church's Thesis and principles for mechanisms*, in ***The Kleene symposium*** (J. Barwise, H. J. Keisler, and K. Kunen, editors), North-Holland, 1980, pp. 123–148.

[3] W. SIEG, *Calculations by man and machine*: *conceptual analysis*, to appear in ***Reflections on the foundations of mathematics*** (W. Sieg, R. Sommer, and C. Talcott, editors), Assocation for Symbolic Logic, 2002, pp. 396–415.

► GABRIEL UZQUIANO, *Abstraction principles and structure*.
Department of Philosophy, University of Rochester, 523 Lattimore Hall, Rochester, New York 14627, USA.
E-mail: gabriel.uzquiano@rochester.edu.

At the center of the neo-Fregean program in the philosophy of mathematics is the search for abstraction principles that can serve as legitimate foundations for mathematical theories. The model theory of some proposed abstraction principles for arithmetic and real analysis is very attractive. Two models of Hume's principle, for example, need not be isomorphic to each other, but the numbers of one model must be isomorphic to an initial segment of the numbers of the other. Likewise for some of the recently proposed neo-Fregean foundations for real analysis. There is a combination of abstraction principles that provides us with a categorical characterization of the structure of the real numbers.

The case of set theory, it is argued, is not very different. New V, once a firm candidate for a neo-Fregean development of set theory, provides us with a partial characterization of the structure of the universe of well-founded sets. Two models of New V of the same cardinality need not be isomorphic, but the well-founded hereditary sets of one must be isomorphic to the well-founded hereditary sets of the other. There is, in fact, a family of abstraction principles based on the limitation of size doctrine that are able to characterize the structure of the universe of well-founded hereditary sets up to isomorphism. Some of these categoricity results are proved within standard set theory, but others are recoverable from within the perspective of a neo-Fregean for whom the tools of standard set theory need not be available.

This is joint work with Ignacio Jané.

Abstracts of invited talks in the Special Session on Set Theory

► ILIJAS FARAH, *Luzin gaps*.
CUNY – College of Staten Island, 2800 Victory Blvd., Staten Island, New York 10314, USA and Matematicki Institut, Kneza Mihaila 35, 11000 Beograd, Yugoslavia.
E-mail: IFarah@gc.cuny.edu.

Many questions about the Boolean algebra $P(\mathbb{N})/\mathrm{Fin}$ are resolved assuming the Continuum Hypothesis and a recursive construction. If the size of the continuum is greater than $\aleph_1$, the existence of Hausdorff gaps stand in the way of such approach. In order to prove that a particular consequence of CH fails, one usually needs more than just assuming that CH fails. The technique of freezing gaps in $P(\mathbb{N})/\mathrm{Fin}$ originated in the work of Luzin and Kunen and it was developed further by Abraham-Rubin-Shelah and Todorcevic. Extending this technique to related quotient algebras presents new technical difficulties, in particular because of the existence of 'analytic Hausdorff gaps' in some of these quotients. I will discuss the current state of knowledge on this topic and several applications.

► ALEXANDER S. KECHRIS, *Rigidity theorems for actions of product groups and countable Borel equivalence relations*.
Department of Mathematics 253-37, California Institute of Technology, Pasadena, California 91125, USA.
E-mail: kechris@caltech.edu.

Under certain circumstances, if a countable group acts on a standard measure space, the orbit equivalence relation (together with the measure), and sometimes even the purely set theoretic object of the Borel cardinality of the orbit space, "encodes" or "remembers" many properties of the acting group. Starting with work of Zimmer, many important such "rigidity" phenomena have been discovered over the last two decades in ergodic theory and have been applied recently in solving several problems in the descriptive set theory of equivalence relations and the study of complexity of classification problems. In this talk, I will survey recent work by Gaboriau and Hjorth-Kechris to the effect that products of free groups (and related groups, like word-hyperbolic) exhibit such rigidity phenomena, and I will discuss the implications of such work in the theory of countable Borel equivalence relations.

► RICHARD KETCHERSID, *Determinacy and large cardinals from ideals*.
Department of Mathematics, University of California at Los Angeles, 405 Hilgard Ave., Los Angeles, California 90095-1555, USA.
E-mail: ketchers@math.ucla.edu.

Ideals on small cardinals are known to exist in forcing extensions where some large cardinal is collapsed. Conversely, the ideals themselves imply the existence of inner models for various large cardinals. Unfortunately the gap between the large cardinals required to get the ideals and the large cardinals that the ideals give rise to is enormous. I will discuss some techniques in closing this gap just a tiny bit.

▶ PAUL LARSON, *Iterations of countable models*.
Department of Mathematics, University of Toronto, Toronto, Ontario M5S 3G3, Canada.
E-mail: larson@math.toronto.edu.

We discuss iterated embeddings of countable models of ZFC by generic ultrapowers derived from the nonstationary ideal on ω_1. We show that for each such model and each real number there is a unique shortest iteration of the model picking up the given real, if any. We also discuss some open problems in the area.

▶ JUSTIN MOORE, *Weak diamond and open colorings*.
Department of Mathematics, Boise State University, 1910 University Dr., Boise, Idaho 83725, USA.
E-mail: justin@diamond.boisestate.edu.

I will discuss the relative consistency of certain statements about open colorings with $2^{\aleph_0} < 2^{\aleph_1}$. In particular both OCA and the statement that every one-to-one function of size $\aleph_1$ is σ-monotonic are consistent with $2^{\aleph_0} < 2^{\aleph_1}$. As a corollary we have that $2^{\aleph_0} < 2^{\aleph_1}$ does not admit a $\mathbb{P}_{\max}$ variation (in the presence of an inaccessible cardinal).

▶ MARTIN ZEMAN, *Stationary non-reflection in extender models*.
Department of Mathematics, University of California at Irvine, Irvine, California 92697-3875, USA.
E-mail: mzeman@math.uci.edu.

Work in any extender model. I present an argument that allows to construct a non-reflecting stationary subset of κ^+, granting that for any $\mu < \kappa$ we have a sufficiently local definition for a non-reflecting stationary subset of μ^+. (We consider only stationary sets that concentrate on ordinals of small cofinality.)

Abstracts of contributed talks

▶ GURAM BEZHANISHVILI AND JOHN HARDING, *Functional monadic Heyting algebras*.
New Mexico State University, Las Cruces, New Mexico 88003, USA.
E-mail: gbezhani@nmsu.edu.
E-mail: jharding@nmsu.edu.

In the 1950s Halmos introduced the notion of a monadic (Boolean) algebra as an algebraic counterpart of the one variable fragment of (classical) predicate logic. Halmos proved a representation theorem for monadic algebras by showing that every monadic algebra can be embedded into one constructed from the collection of all functions from a set X into a complete Boolean algebra C. Soon after Halmos' results, Monteiro and Varsavsky introduced the notion of monadic Heyting algebras as the algebraic counterpart of the one variable fragment of intuitionistic predicate logic. In their 1957 paper they posed the question whether a representation theorem along the lines of Halmos' holds also for monadic Heyting algebras. We solve this problem positively.

▶ WESLEY CALVERT, *The isomorphism problem for familiar classes of computable structures*.
Department of Mathematics, 255 Hurley Hall, University of Notre Dame, Notre Dame, Indiana 46556, USA.
E-mail: wcalvert@nd.edu.

Shelah's theory of classification identifies some classes of structures which in high cardinalities exhibit great complexity. Another notion, based on Borel reducibility, identifies classes of countable structures which are very complex. In some classes which are non-classifiable in the Shelah sense, the complexity is in some way so intrinsic to the theory that it shows up even in the countable case, in the form of high Borel complexity. In this talk, I will explore a sense in which this complexity sometimes shows up even in the computable members of the class.

For some classes (undirected graphs, fields of fixed characteristic, and real closed fields) the isomorphism problem is Σ^1_1 complete (that is, even the class of computable models is very complicated), and for others it is of relatively low complexity. For instance, for algebraically closed fields or vector spaces, the isomorphism problem is Π^0_3 complete. For equivalence structures, it is Π^0_4 complete. Abelian p-groups of bounded ulm height and archimedean real closed fields also have simple isomorphism problems. I will try to give a sense of the way the calculations are made and of what is known of the partial order on classes given by the isomorphism problem.

► JONAS ELIASSON, *Ultrapowers as sheaves*.
Department of Mathematics, Uppsala University, P. O. Box 480, S-751 06 Uppsala, Sweden.
E-mail: jonase@math.uu.se, eliasson@cmu.edu.

In 1995 I. Moerdijk [3] presented a new model of nonstandard arithmetic in the topos of sheaves on a category of filters, Sh($\mathbb{F}$). This was later extended by E. Palmgren to a model of nonstandard analysis [4]. The model makes use, in particular, of the sheaves ${}^*S$, defined, at any filter $\mathcal{F}$, as the reduced power of the set S over $\mathcal{F}$, ${}^*S(\mathcal{F})$.

In this talk we focus our attention on the sheaves on the subcategory of ultrafilters, Sh($\mathbb{U}$). This topos is the subject of my licentiate thesis [2]. The sheaves of the form ${}^*S$ now, at an ultrafilter $\mathcal{U}$, represent the ultrapower of S over $\mathcal{U}$, ${}^*S(\mathcal{U})$.

The category of ultrafilters has a strong connection with ultrafilters under the Rudin-Keisler ordering, for instance we have $\mathcal{U} \leq_{RK} \mathcal{V}$ if and only if $\mathrm{Hom}_{\mathbb{U}}(\mathcal{V}, \mathcal{U}) \neq \emptyset$. From this we get a new understanding of a result by A. Blass [1], relating the Rudin-Keisler ordering to elementary embeddings.

The internal logic in the topos is classical since Sh($\mathbb{U}$) is an atomic topos. In fact, Sh($\mathbb{U}$) is the double negation topos of Sh($\mathbb{F}$). By introducing the new concept of factorising ultrafilters we prove that the internal logic does not coincide with the logic in any of the ultrapowers ${}^*S(\mathcal{U})$.

For Sh($\mathbb{U}$), we establish a transfer principle corresponding to Łos' theorem, relating the internal and external logics. Among other results on the topos one can, interestingly enough, show that the topos theoretic axiom of choice does not hold in Sh($\mathbb{U}$).

[1] A. Blass, *Orderings of ultrafilters*, ***Ph. D. thesis***, Harvard University, 1970.

[2] J. Eliasson, *Ultrapowers as sheaves on a category of ultrafilters*, preprint. Available at http://www.math.uu.se/~jonase/research.html.

[3] I. Moerdijk, *A model for intuitionistic non-standard arithmetic*, ***Annals of Pure and Applied Logic***, vol. 73 (1995), no. 1, pp. 37–51.

[4] E. Palmgren, *A sheaf-theoretic foundation of nonstandard analysis*, ***Annals of Pure and Applied Logic***, vol. 85 (1997), no. 1, pp. 68–86.

► LEONA F. FASS, *Modeling "as best one can"*.
P. O. Box 2914, Carmel, California 93921, USA.
E-mail: lff4@cornell.edu.

We describe our *theoretical* behavioral-modeling research in specific problem domains where finite-state realizations actually can be found. There we show that with precise *model-based design* and perfect *model checking* we may obtain such results by effective constructive inference, adequate testing and verification-by-default.

Next we describe applications of these techniques to some "realistic" behavioral-modeling problems, such as logic-based program synthesis and collaborative learning-agent design.

There we conclude that the finite-state *approximate* modeling of complex "unspecifiable" behaviors can be achieved effectively, and may produce the only behavioral representations that are *feasible*.

These results support, and are consistent with, the finite-modeling approach employed by theoreticians and practitioners of program synthesis and agent design that we see today. By approximately specifying a behavior, and producing a finite model of that approximation, we believe they model "as best one can".

[1] L. F. Fass, *Determining software models that are less incorrect*, ***Papers from the AAAI Spring Symposium on model-based validation of intelligence***, Stanford University, March 2001, AAAI Press SS01-04, pp. 113–116.

[2] ———, *Finite models for learning*, ***Proceedings of the Sixth Joint Conference on information sciences/Fifth International Conference on computational intelligence and neuroscience***, Research Triangle Park, North Carolina, March 2002, pp. 525–528.

▶ NOAM GREENBERG, *Lattice (non)-embeddings in admissible r. e. degrees*.
Department of Mathematics, Malott Hall, Cornell University, Ithaca, New York 14850, USA.
E-mail: erlkonig@math.cornell.edu.

For many admissible ordinals α, the 1-3-1 non-distributive lattice cannot be embedded in the α-r. e. degrees. Thus, with a generalization of coding techniques of Nies, Shore, Slaman and Woodin for other admissible ordinals, we can show that for all admissible α, the α-r. e. degrees and classical r. e. degrees are not elementarily equivalent (when we consider these structures as partial orderings).

▶ JAMES HIRSCHORN, *Random gaps*.
Institut für Formale Logik, University of Vienna, Austria.
E-mail: James.Hirschorn@logic.univie.ac.at.

Previous investigations into the "random gap" problem are completed by proving that a destructible (ω_1, ω_1) gap in $\mathcal{P}(\mathbb{N})/\mathrm{Fin}$ can always be constructed from $\aleph_1$ co-generic random reals. It is also proved that in this situation, there exists an indestructible (ω_1, ω_1) gap which is not equivalent to a gap with the Hausdorff property.

▶ CARL G. JOCKUSCH, JR., AND TAMARA J. LAKINS, *Generalized r-cohesiveness and the arithmetical hierarchy*.
Department of Mathematics, University of Illinois, 1409 W. Green Street, Urbana, Illinois 61801, USA.
E-mail: jockusch@math.uiuc.edu.
Department of Mathematics, Allegheny College, 520 N. Main St., Meadville, Pennsylvania 16335, USA.
E-mail: tlakins@allegheny.edu.

For $X \subseteq \omega$, let $[X]^n$ denote the class of all n-element subsets of X. An infinite set $A \subseteq \omega$ is called *n-r-cohesive* if for each computable function $f : [\omega]^n \to \{0, 1\}$ there is a finite set F such that f is constant on $[A - F]^n$. We show that for each $n \geq 2$ there is no Π^0_n set $A \subseteq \omega$ which is n-r-cohesive. For $n = 2$ this refutes a result previously claimed by the authors, and for $n \geq 3$ it answers a question raised by the authors.

[1] T. Hummel and C. G. Jockusch, Jr., *Generalized cohesiveness*, ***Journal of Symbolic Logic***, vol. 64 (1999), pp. 489–516.

[2] ———, *Ramsey's theorem for computably enumerable colorings*, ***Journal of Symbolic Logic***, vol. 66 (2001), pp. 873–880.

[3] C. G. Jockusch, Jr., *Ramsey's theorem and recursion theory*, ***Journal of Symbolic Logic***, vol. 37 (1972), pp. 268–280.

[4] F. P. RAMSEY, *On a problem in formal logic*, ***Proceedings of the London Mathematical Society***, vol. 30 (1930), pp. 264–286.

[5] R. I. SOARE, ***Recursively enumerable sets and degrees***, Springer-Verlag, Berlin, 1987.

▶ ALEXEI S. KOLESNIKOV, *Abstract dependence in non-elementary classes*.
Department of Mathematical Sciences, Carnegie Mellon University, Pittsburgh, Pennsylvania 15213, USA.
E-mail: alexei@andrew.cmu.edu.

In non-first order context, a model-theoretic dependence relation was first introduced by S. Shelah in [4]. Since then good dependence relations were defined and used in several non-first order frameworks. Our goal is to identify the properties of abstract dependence relations in certain non-elementary classes that, firstly, characterize the model-theoretic properties of those classes; and secondly, allow to uniquely describe an abstract dependence itself in a very concrete way. We investigate totally transcendental atomic models and finite diagrams, stable finite diagrams, and supersimple homogeneous models from this point of view.

The abstract approach to dependence relations goes back to the works of Van der Waerden. In model theory, the abstract treatment of dependence was introduced by J. Baldwin in 1970s, with many extensions in [1]. For simple first order theories, the characterization of forking was obtained by B. Kim and A. Pillay in [3]. On the non-first order front, a characterization of dependence was obtained by T. Hyttinen and O. Lessmann in [2] for superstable finite diagrams.

[1] JOHN BALDWIN, ***Fundamentals of stability theory***, Springer-Verlag, 1988.

[2] TAPANI HYTTINEN and OLIVIER LESSMANN, *A rank for the class of elementary submodels of a superstable homogeneous model*, preprint.

[3] BYUNGHAN KIM and ANAND PILLAY, *Simple theories*, ***Annals for Pure and Applied Logic***, vol. 88 (1997), pp. 149–164.

[4] SAHARON SHELAH, *Classification theory for non-elementary classes I: The number of uncountable models of $\psi \in L_{\omega_1,\omega}$, Parts A, B*, ***Israel Journal of Mathematics***, vol. 46 (1983), pp. 212–273.

▶ JOHN KRUEGER, *Fat sets and saturated ideals*.
Department of Mathematical Sciences, Carnegie Mellon University, 5000 Forbes Ave., Pittsburgh, Pennsylvania 15213, USA.
E-mail: jkrueger@andrew.cmu.edu.

In my talk I will discuss a strengthening of a theorem by Gitik and Shelah on the non-saturation of the ideal $NS_\kappa \restriction \mathrm{cof}(\theta)$ for $\theta < \theta^+ < \kappa$. I generalized this theorem by proving that if κ is either weakly inaccessible or the successor of a singular cardinal and S is a stationary subset of κ such that $NS_\kappa \restriction S$ is saturated, then S has a fat complement. Using this strengthening I prove some results on the existence of fat stationary sets.

▶ TIMOTHY H. MCNICHOLL, *Almost a non-trivial automorphism of the c. e. weak truth-table degrees*.
Department of Mathematics, University of Dallas, Irving, Texas 75062, USA.
E-mail: tmcnicho@acad.udallas.edu.

Let $\mathcal{D}^{\mathrm{wtt}}_{\mathrm{c.\,e.}}$ be the structure of the weak truth-table degrees. We show that there is a pair of non-trivial embeddings $\Phi, \Psi\colon \mathcal{D}^{\mathrm{wtt}}_{\mathrm{c.\,e.}} \to \mathcal{D}^{\mathrm{wtt}}_{\mathrm{c.\,e.}}$ such that for all $x \in \mathcal{D}^{\mathrm{wtt}}_{\mathrm{c.\,e.}}$ $x \leq \Phi(\Psi(x))$ and $x \leq \Psi(\Phi(x))$. We discuss current work on using these techniques to produce a non-trivial automorphism of the c. e. weak-truth table degrees.

▶ G. E. MINTS AND DARKO SARENAC, *Completeness of indexed ε-calculus*.
Department of Philosophy, Stanford, University, Stanford, California 94305, USA.
E-mail: mints@stanford.edu.
E-mail: sarenac@stanford.edu.

Indexing ε-terms has proven to be useful in semantic theory of natural language, in particular in representing definite and indefinite phrases [1]. We devise a formal system for operating with indexed choice functions.

Language. Context variables $i, j, \dots$ and constants $c, c_1, \dots$; object variables $x, y, \dots$; indexed ε-symbol ε_a where a is a context variable or constant; quantifiers $\exists i$ over contexts.

Semantics. ε-symbol is interpreted as a choice operator: $\varepsilon_i x\alpha$ is an x satisfying α. An *i-structure* is a tuple $\mathcal{A} = (|\mathcal{A}|, P^{\mathcal{A}}, \dots, f^{\mathcal{A}}, \dots, \mathbb{F}^{\mathcal{A}})$ consisting of a first order structure in a standard sense with object domain $|\mathcal{A}|$, and a non-empty set $\mathbb{F}^{\mathcal{A}}$ of choice functions for $|\mathcal{A}|$. The contexts i, c range over $\mathbb{F}^{\mathcal{A}}$.

A *finite choice* $a_1 \in S_1, \dots, a_n \in S_n$ is a partial choice function defined only for finitely many sets. An i-structure $\mathcal{A}$ *contains finite choices* if $\mathbb{F}^{\mathcal{A}}$ contains (total extensions of) all finite choices from subsets of $|\mathcal{A}|$ definable in $\mathcal{A}$ with parameters.

System $S\varepsilon_i$. *Axioms*: standard first-order axioms including critical formulas: $\alpha[x/t] \to \alpha[x/\varepsilon_a x\alpha]$, and extensionality schema: $\forall x\,(\alpha \leftrightarrow \beta) \to (\varepsilon_i x\alpha = \varepsilon_i x\beta)$; axioms for quantifiers over ε-indices.

Inference rules: Modus Ponens and elimination rule for $\exists$ over context variables.

System $S\varepsilon_i^{\text{fin}}$. Add the following schema to $S\varepsilon_i$ (existence of a finite choice):

$$\left[\bigwedge_{k<l}(\alpha_k[t_k] \vee \forall x\,\neg\alpha_k) \wedge \bigwedge_{k<m<l} \exists x\,\neg(\alpha_k \leftrightarrow \alpha_m)\right] \to \exists i\,\left(\bigwedge(\varepsilon_i x\alpha_k = t_k)\right).$$

THEOREM. *System* $S\varepsilon_i$ (*system* $S\varepsilon_i^{\text{fin}}$) *is sound and complete for i-structures* (*for i-structures containing finite choices*).

[1] K. VON HEUSINGER, *The reference of indefinites*, in ***Reference and anaphoric relations*** (K. von Heusinger and U. Egli, editors), Kluwer, 2000, pp. 265–284.

[2] MITSURU YASUHARA, *Cut elimination in ε-calculi*, ***Zeitschrift für mathematische Logik und Grundlagen der Mathematik***, vol. 28 (1982), pp. 311–316.

► R. GREGORY TAYLOR, *Symmetric propositions over finite domains*.
Computer Science Department, Trinity College, Hartford, Connecticut 06106, USA.
E-mail: `Gregory.Taylor@trincoll.edu`.

We investigate Zermelo's notion of a symmetric proposition. Following Tarski, we suggest that such propositions are precisely those giving expression to logical concepts. Application of computational methods for enumerating nonisomorphic subgraphs of complete directed graphs on n vertices enables us to investigate the frequency of symmetric propositions over domains of size n as n increases, and this frequency is then used to provide a measure of the ratio of the logical to the nonlogical.

► ALASDAIR URQUHART, *The complexity of propositional proofs with the substitution rule*.
Department of Philosophy, University of Toronto, 215 Huron Street, Toronto Ontario, Canada M5S 1A1.
E-mail: `urquhart@cs.toronto.edu`.

In his survey paper of 1995 on the lengths of propositional proofs, Buss mentions the possibility that the rule allowing multiple substitution for variables in a tautology may allow some speedup over the single-variable substitution rule in the context of propositional proof systems. We verify this conjecture by showing that the lower bounds on the number of lines proved for Frege systems (systems based on schematic axioms and rules) can be extended in a fairly simple way to Frege systems with the single-variable substitution rule, showing a speedup of the multiple-variable rule over the single-variable rule.

For sufficiently large N, there are simple tautologies of size $O(N)$ that require proofs containing $\Omega(N)$ lines in axiomatic systems of propositional logic based on axioms and the rule of substitution for single variables. These tautologies have proofs with $O(\log_2 N)$ lines in systems with the multiple substitution rule.

[1] SAMUEL R. BUSS, *Some remarks on lengths of propositional proofs*, ***Archive for Mathematical Logic***, vol. 34 (1995), pp. 377–394.

► VOJKAN VUKSANOVIC, *Canonical equivalence relations on $\mathbb{Q}^n$*.
Department of Mathematics, University of Toronto, 100 St. George Street, Toronto, Ontario, M5S 3G3, Canada.
E-mail: voja@math.toronto.edu.

We show that for each positive integer n there is a finite list of equivalence relations on $[\mathbb{Q}]^n$ with the property that for every other equivalence relation $\mathbb{E}$ on $[\mathbb{Q}]^n$ there is $X \subseteq \mathbb{Q}$ of order type equal to the order type of $\mathbb{Q}$, such that $\mathbb{E}\restriction[X]^n$ is equal to one of the equivalence relations from the list.

► DAN E. WILLARD, *A further investigation of the second incompleteness theorem*.
SUNY-Albany CS Department, Albany, New York 12222, USA.
E-mail: dew@cs.albany.edu.

Let α denote an axiom system and D denote a deduction method. Say (α, D) represents a Boundary-Case Exception to the Second Incompleteness Theorem if and only if: (1) α can prove there exists no proof of $0 = 1$ resting on α's axioms and on D's deduction method, and (2) α can also prove all Peano Arithmetic's Π_1 theorems (in a langauge that treats Addition and Multiplication as 3-variable atomic predicates). Our prior published work [1] has proved there exists such Boundary-Case Exceptions when either:

(i) D represents Semantic Tableaux Deduction, and α is an axiom system that recognizes Addition, *but not* Multiplication as a total function, i.e., α can not prove $\forall x\, \forall y\, \exists z\; x * y = z$.
(ii) Or D represents Hilbert Deduction, and α fails to recognize even Successor as total.

Part of the reason (i) and (ii) are interesting is that it is difficult to hybridize them. For example, Pudlák proved no consistent extension of Robinson's System Q can prove its Hilbert consistency, and Solovay generalized this result for systems recognizing only Successor as total.

Nevertheless, we have recently discovered a different type of feasible hybrid of (i) and (ii). Consider a list of ordered pairs $(t_1, p_1), (t_2, p_2), \dots, (t_n, p_n)$, where p_i is a Semantic Tableaux proof of the theorem t_i. Say such a list is an R-Tableaux proof of the theorem T from the axiom system α if and only if $T = t_n$ and

(A) The proper axioms permitted in the proof p_j are either one of $t_1, t_2, \dots, t_{j-1}$ or axioms from α.
(B) Each of the sentences $t_1, t_2, \dots, t_{j-1}$ are required to have what [1] called a Π_1^- or Σ_1^- format.

We have recently discovered analogs of the $\mathrm{IS}(A)$ and $\mathrm{IS}^\lambda(A)$ systems (from [1]) that recognize Addition as a total function and can confirm their self-consistency relative to R-Tableaux deduction. Conversely using methods from [2], we have determined that the Second Incompleteness Theorem takes force when either (1) Condition-B is relaxed to permit Π_2^- sentences, or (2) α recognizes Multiplication as total. In particular, if D^* is a deduction method similar to R-Tableaux except that its Rule-B permits $t_1, t_2, \dots, t_{j-1}$ to be Π_2^-, then there exists a single Π_1^- sentence W such that no consistent $\alpha \supseteq W$ can simultaneously verify the consistency of (α, D^*) and that Addition is total. Furthermore, if D^{**} differs from D^* by allowing $t_1, t_2, \dots, t_{j-1}$ to be Σ_2^-, rather than Π_2^-, then another variant of the Second

Incompletenes Theorem will disallow a consistent $\alpha \supseteq W$ from simultaneously verifying (α, D^{**})'s consistency and Addition is total.

[1] D. Willard, *Self-verifying systems, the incompleteness theorem and the tangibility reflection principle*, ***Journal of Symbolic Logic***, vol. 66 (June 2001), pp. 536–596.

[2] ———, *How to extend the semantic tableaux and cut-free versions of the second incompleteness theorem almost to Robinson's arithmetic Q*, ***Journal of Symbolic Logic***, vol. 67 (March 2002), pp. 465–496.