The Bulletin of Symbolic Logic
Volume 11, Number 1, March 2005

2004 ANNUAL MEETING OF THE ASSOCIATION FOR SYMBOLIC LOGIC

Carnegie Mellon University, Pittsburgh, PA
May 19–23, 2004

The Annual Meeting of the Association was held on the campus of Carnegie Mellon University, May 19–23, 2004. The program included the Fifteenth Annual Gödel Lecture, two tutorials, 11 one-hour invited talks, two special evening lectures and a special lecture at a joint session with the co-located annual meeting of Mathematical Foundations of Programming Semantics (MFPS). The program also featured four special sessions, a panel discussion, 19 contributed talks, and five abstracts presented by title. The members of the Program Committee were Sergei Artemov (Chair), Tomek Bartoszynski, Denis Hirschfeldt, Chris Laskowski, and Wilfried Sieg. The members of the Local Organizing Committee were Jeremy Avigad (Chair), Steve Awodey, Lenore Blum, James Cummings, Ernest Schimmerling, and Wilfried Sieg. There were 156 registered participants at the meeting, including 64 graduate students. Generous financial support was provided by Carnegie Mellon University. The ASL hosted a conference dinner.

The co-located MFPS meeting and the special lectures, presented by individuals who have made fundamental contributions to logic over long careers, were novel features of the ASL annual meeting program. Indications are that both proved highly successful.

The Fifteenth Annual Gödel Lecture, *Proofs persuasions and randomness in mathematics*, was presented by Michael O. Rabin (Harvard University). The tutorials were given by Jeremy Avigad (Carnegie Mellon University) on *Proof mining* and Toniann Pitassi (University of Toronto) on *Recent advances in proof complexity*. The other hour-long invited addresses were:

John Baldwin (University of Illinois at Chicago), *Categoricity transfer in infinitary logic*.

Lev Beklemishev (Utrecht University and Steklov Mathematical Institute, Moscow), *From provability logic to combinatorial independence results*.

Michael Hallett (McGill University), *Reflections on the purity of method in Hilbert's "Grundlagen der Geometrie"*.

Valentina Harizanov (The George Washington University), *Effectiveness in algebraic structures*.

Steve Jackson (University of North Texas), *Regular markers and countable equivalence relations*.

Kenneth Kunen (University of Wisconsin), *Elementary submodels in topology and analysis*.

Angus J. MacIntyre (University of Edinburgh), *Schanuel's conjecture and its significance for the logic of the real and complex exponentials*.

Penelope Maddy (University of California, Irvine), *Mathematical existence*.

Joe Miller (Victoria University of Wellington), *Measuring the randomness of random reals*.

Michael Rathjen (Ohio State University), *Equiconsistency results and open problems in constructive and intuitionistic set theories*.

Paul Vitanyi (CWI and University of Amsterdam), *Extracting meaning with Kolmogorov and Shannon*.

1079-8986/05/1101-0005/$3.80

Two special evening lectures were delivered by:

John McCarthy (Stanford University), *What more does artificial intelligence want from mathematical logic?*

William A. Howard (University of Illinois at Chicago), *Aspects of proof theory and foundations, 1950–1985*.

There were four special sessions and a panel discussion (with organizers given in parentheses): Gödel and Mathematical Logic in the 20th Century (John W. Dawson, Jr., Solomon Feferman, Warren Goldfarb, Charles Parsons, and Wilfried Sieg), Logic and Games (Rohit Parikh), Logical Foundations of Programming Semantics, joint with MFPC (Steve Awodey), Set Theory (Ernest Schimmerling and James Cummings), and a Panel Discussion on Logic in Computer Science Education (Jeff Hirst). These had a total of 32 speakers.

Abstracts of the invited talks and the contributed talks given (in person or by title) by members of the Association for Symbolic Logic follow.

For the Program Committee
SERGEI ARTEMOV

Abstract of the 15th Annual Gödel Lecture

► MICHAEL O. RABIN, *Proofs persuasions and randomness in mathematics*.
Division of Engineering and Applied Sciences, Harvard University, Pierce Hall, 29 Oxford St., Cambridge, MA 02138, USA.
E-mail: rabin@deas.harvard.edu.

It is customary to hold up mathematical proofs as ideal models of certainty. In principle a proof can be completely formalized and annotated and then it can be handed to other mathematicians and logicians who can "automatically" and efficiently verify it beyond any doubt. In practice the establishment of a mathematical statement is a social process. Someone proposes a proof, he and others check it and errors are often uncovered and corrected, until finally the community of mathematicians accepts the statement and its proof as correct.

Over the past three decades computer scientists have injected a number of revolutionary ideas and methods into the realm of proofs. These innovations mainly involve the use of randomness, an idea that flies in the face of the proverbial absolute certainty of mathematical proofs. Another salient feature of these novel methods of proofs is that in a well-defined sense they constitute self-persuasions rather than proofs. We shall discuss three outstanding examples of these innovations.

Randomized or probabilistic proofs. Consider the statement: $n = 2^{400} - 593$ is a prime number. You prove it by randomly choosing 100 integers $a_1, \dots, a_{100}$, and performing on each an easily computable test $W_n(a_j)$. If all these tests produce the truth value F, you declare n to be prime. If n is composite rather then prime, the probability of erroneously concluding that it is a prime is smaller than $(1/4)^{100}$. Now, first we have established a mathematical fact with a probability of error, albeit provably a very small one. Second, the proof is non-transferable. If you hand the integers $a_1, \dots, a_{100}$, to somebody else and he verifies that $W_n(a_j) = F$ for $1 \leq j \leq 100$, it does not prove anything for him. Namely, n is perhaps in reality composite and you have deliberately chosen the integers a_j in order to mislead him. A person must persuade himself of the primality of n by the randomized method, by effecting the random choice of the a_js on his own. This raises additional profound questions as to what randomness means in the real world and whether, assuming that we know the meaning of randomness, random processes exist in nature.

Zero Knowledge and Interactive Proofs. Assume that P know, for a propositional formula $A(p_1, \dots, p_k)$, a satisfying truth value assignment for the propositional variables $p_1, \dots, p_k$.

The Prover P can cooperate with a Verifier V in an interactive Zero Knowledge Proof (ZKP) that he, the Prover, knows a satisfying truth value assignment for the formula $A(p_1, \dots, p_k)$. The Verifier V poses to P a small number m of randomly chosen challenges. If P correctly responds to all challenges, then V is persuaded that P knows a satisfying truth value assignment. The probability that V was mislead is smaller the $(1/2)^m$. The Zero Knowledge aspect of the proof means that besides being persuaded of the Prover's claim of knowledge, V learns *nothing*, not just about the assignment but about anything else. Hence the name Zero Knowledge Proofs. The theory of ZKPs provides precise and convincing definitions for the concepts of Zero Knowledge and of proof of knowledge by P, in addition to the surprising fact that ZKPs are possible.

The method of interactive proofs has other surprising applications. A computationally powerful (in a precisely defined sense) Prover can provide to any Verifier an interactive proof that a given quantified prepositional formula is true. This has far reaching, albeit purely theoretical, consequences.

Probabilistically Checkable Proofs (PCPs). Assume that P has, as before, a satisfying truth value assignment for the propositional variables $p_1, \dots, p_k$, of a prepositional formula $A(p_1, \dots, p_k)$. He can effectively, i.e., by a polynomially long computation, transform the formula A into a formula $B(q_1, \dots, q_m)$ so that A is satisfiable if and only if B is satisfiable. P then writes satisfying truth values $v_1, \dots, v_m$ into, say, a computer memory. Now, the verifier V can randomly choose a small number, say 20, memory locations, read the stored truth values (i.e., either F or T) and perform a very simple test. If the test comes out correctly, V concludes that B, and hence A, is satisfiable. The probability that he will be mislead is smaller than $(3/4)^{20}$. The startling aspect is that the number of truth values or bits that he reads for this verification is *independent* of the size or number of variables of the formula A. By some transformations we can conclude that one can convince himself of the existence of a proof of Fermat's Last Theorem by examining just 20 randomly chosen bits of a certain formalized form of the proof written into memory by A. Wiles.

Computer generated proofs. In the past two decades proofs of some significant results were generated by computers, or at least by man-computer cooperation, where the computer has played a pivotal role. Examples are the proof, due to Appel and Haken, of the four-color conjecture by computer, and the extensive work by Doron Zilberger. We shall discuss the meaning and implications of these developments.

Abstracts of invited talks

► JOHN BALDWIN, *Categoricity transfer in infinitary logic*.
University of Illinois at Chicago, USA.
E-mail: jbaldwin@uic.edu.

We distinguish two themes in generalizing Morley's theorem to infinitary logic. One is focused primarily on the logic $L_{\omega_1,\omega}$ and does not assume that there are arbitrarily large models. Major steps in the analysis begin with the hypothesis that a sentence has few models in small cardinalities (below $\aleph_\omega$). This leads to the theory of excellence, which has applications in understanding complex exponentiation. The other theme concerns the more general setting of Abstract Elementary Classes (AEC): a class with a notion of strong submodel that satisfies a variant of the Jónsson axioms. Most progress has been made by assuming both the amalgamation property and that the class has arbitrarily large models, so the Ehrenfeucht-Mostowski technology can be invoked. We will expound recent work by Shelah, Grossberg and VanDieren towards the conjecture: if an AEC is categorical in a sufficiently large cardinal, it is categorical in all sufficiently large cardinals.

► LEV BEKLEMISHEV, *From provability logic to combinatorial independence results*.
Utrecht University and Steklov Mathematical Institute, Moscow, Russia. Contact address: Steklov Mathematical Institute, Gubkina 8, 119991 Moscow, Russia.
E-mail: `lev@phil.uu.nl`.

The questions of naturality and canonicity of proofs lie at the heart of difficult conceptual problems in proof theory. One possible way to approach these questions is to consider them from a more abstract, algebraic standpoint.

Provability algebras are boolean algebras with additional "provability" operators developed to provide an abstract approach to proof-theoretic analysis. The subject brings together traditional methods of proof theory and those of modal provability logic. Potential aims are, for example,

- getting insight from a new perspective into the foundational questions such as the problem of canonicity of ordinal notations.
- providing a technically simple and clean treatment of traditional proof-theoretic results such as consistency proofs, combinatorial independent principles, etc.

We give an overview of these methods and formulate some simple statements of combinatorial character independent from Peano arithmetic arising from the provability algebra approach. Interesting connections with some examples of Friedman and Schütte–Simpson and Buchholz will be indicated.

► MICHAEL HALLETT, *Reflections on the 'purity of method' in Hilbert's* Grundlagen der Geometrie.
Department of Philosophy, McGill University, 855 Sherbrooke Street, Montreal, Quebec H3A 2T7, Canada.
E-mail: `michael.hallett@mcgill.ca`.

Hilbert's *Grundlagen der Geometrie* presents a new way of looking at the foundations of mathematical theories, one which has become the dominant one in foundational investigations. This approach seems incompatible with traditional 'purity of method' concerns which concentrate on the supposed superiority of certain theoretical frameworks. Nevertheless, this paper argues that this impression is only partially correct. (1) It illustrates several cases where Hilbert uses 'purity' questions, traditionally posed, to provide new foundational information. (2) But more strongly, the investigations throw open the question of the mathematical presuppositions of foundational investigation itself.

► VALENTINA S. HARIZANOV, *Effectiveness in algebraic structures*.
Department of Mathematics, The George Washington University, Washington, D.C., 20052, USA.
E-mail: `harizanv@gwu.edu`.

We apply ideas, notions and methods from computability theory to study algorithmic phenomena (effectiveness) in countable algebraic structures. We focus on the computability theoretic complexity of structures, the complexity of their isomorphisms, and of relations that are not named in the languages of the structures. Since complexity can be described syntactically (for example, using computable infinitary formulae) and measured semantically (for example, using Turing degrees), this study also relates definability to computability. Classically isomorphic structures can have very different algorithmic properties. When complexity bounds for some property of a structure are preserved under isomorphisms, we call the bounds intrinsic. We are interested in intrinsically and nonintrinsically complicated relations on computable and hyperarithmetical structures. Results establishing equivalences of syntactic conditions and the corresponding algorithmic properties in computable isomorphic copies of a computable structure $\mathcal{A}$ usually require additional effectiveness in $\mathcal{A}$. If we allow arbitrary isomorphic copies of $\mathcal{A}$, we obtain analogous results for relativized algorithmic properties, without requiring additional effectiveness. We investigate both general structures and specific ones, such as partial and linear orderings, Boolean algebras, and groups.

[1] C. J. Ash and J. F. Knight, ***Computable Structures and the Hyperarithmetical Hierarchy***, Elsevier, 2000.

[2] S. S. Goncharov, V. S. Harizanov, J. F. Knight, and C. F. D. McCoy, *Simple and immune relations on countable structures*. ***Archive for Mathematical Logic***, vol. 42 (2003), pp. 279–291.

[3] S. Goncharov, V. Harizanov, J. Knight, C. McCoy, R. Miller, and R. Solomon, *Enumerations in computable structure theory*, ***Annals of Pure and Applied Logic***, submitted.

[4] S. S. Goncharov, V. S. Harizanov, J. F. Knight, and R. A. Shore, Π^1_1 *relations and paths through* $\mathcal{O}$, ***The Journal of Symbolic Logic***, to appear.

[5] V. Harizanov and R. Miller, *Spectra of structures and relations*, preprint.

► STEVE JACKSON, *Regular markers and countable equivalence relations*.
Department of Mathematics, University of North Texas, P. O. Box 311430, Denton, TX 76203-1430, USA.
E-mail: jackson@unt.edu.

We use the existence of markers with regular geometric properties to study countable Borel equivalence relations. In particular we obtain a new proof of the hyperfiniteness of Z^n actions and the existence of a continuous embedding of 2^Z into E_0.

► KENNETH KUNEN, *Elementary submodels in topology and analysis*.
Department of Mathematics, 480 Lincoln Drive, University of Wisconsin, Madison, WI 53706, USA.
E-mail: kunen@math.wisc.edu.

In this technique, one takes an elementary submodel of the universe (or, to be formal, of some suitably large $H(\theta)$), to facilitate some combinatorial proof. The basic idea goes back to Gödel's proof of the GCH in L, and is now well-known in set-theoretic arguments. The talk will discuss some applications of this technique to general topology and functional analysis.

► PENELOPE MADDY, *Mathematical existence*.
Department of Logic and Philosophy of Science, University of California, Irvine, Irvine, CA 92697-5100, USA.
E-mail: pjmaddy@uci.edu.

This talk will explore some interrelated issues of mathematical method, truth and existence.

► ANGUS MACINTYRE, *Schanuel's Conjecture and its significance for the logic of the real and complex exponentials*.
The University of Edinburgh, James Clerk Maxwell Building, Kings Buildings, Mayfield Road, Edinburgh, EH9 3JZ.
E-mail: angus@maths.ed.ac.uk.

I will survey the use of Schanuel's Conjecture for the metamathematics of the exponential function. The first applications were to decidability, culminating in its use in the decidability of the real exponential function. Here the key point is that the conjecture links naturally to a normal form for existential formulas, and a notion of exponential-algebraic. The more recent work of Zilber has a different flavour, as the basic facts about the two exponentials are so different. I will discuss the relation between Zilber's exponential and the classical complex exponential.

► JOSEPH S. MILLER, *Measuring the randomness of random reals*.
School of Mathematical and Computing Sciences, Victoria University of Wellington, P.O. Box 600, Wellington, New Zealand.
E-mail: `Joe.Miller@mcs.vuw.ac.nz`.

What does it mean to say that one real number is *more random* than another? A variety of quasi-orders have been introduced to answer this question; in other words, to measure the "degree of randomness" of a real. We argue that the reducibilities introduced by Solovay (unpublished) and by Downey, Hirschfeldt, and LaForte [1] are too strong to compare the randomness of random reals. We examine two weaker measures of randomness (already introduced by André Nies in the study of highly non-random sets) and relate the new and old reducibilities. This is done by proving that certain properties of a real can be inferred from the (plain or prefix-free) Kolmogorov complexity of its initial segments.

Closely related to this investigation is the inverse correlation between the degree of randomness of a real and its power as an oracle. Although a random real has "high information content", it need not have high Turing complexity. For sufficiently random reals, the opposite is true. We support this thesis with several results, both old and new. For example, a 1-random real Turing below an n-random is also n-random; so randomness strength can be gained by bounding computational strength from above.

This talk includes joint work with Liang Yu.

[1] Rod G. Downey, Denis R. Hirschfeldt, and Geoff LaForte, *Randomness and reducibility*, ***Mathematical foundations of computer science 2001*** (***Mariánské Lázně***), Lecture Notes in Computer Science, vol. 2136, Springer Berlin, 2001, pp. 316–327.

► MICHAEL RATHJEN, *Equiconsistency results and open problems in constructive and intuitionistic set theories*.
Department of Mathematics, Ohio State University, Columbus, OH 43210, USA.
E-mail: `rathjen@math.ohio-state.edu`.

Constructive Zermelo-Fraenkel Set Theory, CZF, has emerged as a standard reference theory that relates to constructive predicative mathematics as ZFC relates to classical Cantorian mathematics. A hallmark of this theory is that it possesses a type-theoretic model.

Following a brief review of the history of CZF, the talk will be concerned with equiconsistency results and open problems relating to CZF, IZF and even ZF; principally questions concerning choice principles (presentation axiom, axiom of multiple choice), large set axioms (the regular extension axiom and its variants), subset collection versus exponentiation, and replacement versus collection.

► PAUL VITANYI, *Extracting meaning with Kolmogorov and Shannon*.
CWI and University of Amsterdam, CWI, Kruislaan 413, 1098 SJ Amsterdam, The Netherlands.
E-mail: `paulv@cwi.nl`.

As perhaps the last mathematical innovation of an extraordinary scientific career, Kolmogorov in 1974 proposed to found statistical theory on finite combinatorial and computability principles independent of probabilistic assumptions, as the relation between the individual data and its explanation (model), expressed by Kolmogorov's structure function. It turns out that this proposal is formally a Shannon's rate distortion function for individual data and related to lossy compression.

In classical probabilistic statistics the goodness of the selection process is measured in terms of expectations over probabilistic ensembles. For current applications, average relations are often irrelevant, since the part of the support of the probability density function that will ever be observed has about zero measure. This may be the case in, for example, complex video and sound analysis. There arises the problem that for individual cases the selection performance may be bad although the performance is good on average, or vice versa. There is also the problem of what probability means, whether it is subjective, objective, or exists at all. Kolmogorov's proposal outlined strives for the firmer and less contentious ground expressed in finite combinatorics and effective computation.

This Kolmogorov's structure function, its variations and its relation to model selection, have obtained some notoriety but have not before been comprehensively analyzed and understood. It has always been questioned why Kolmogorov chose to focus on a mysterious function denoted as h_x, rather than on a more evident function denoted as β_x (for details see paper referred to below). Our main result, with the beauty of truth, justifies Kolmogorov's intuition. One easily stated consequence is: For all data, minimizing a two-part code consisting of one part model description and one part data-to-model code (essentially the celebrated MDL code), subject to a given model-complexity constraint, as well as minimizing the one-part code consisting of just the data-to-model code (essentially the maximum likelihood estimator), *in every case* (and not only with high probability) selects a model that is a "best explanation" of the data within the given constraint. In particular, when the "true" model that generated the data is not in the model class considered, then the ML or MDL estimator still give a model that "best fits" the data. This notion of "best explanation" and "best fit" is understood in the sense that the data is "most typical" for the selected model in a rigorous mathematical sense that is discussed below. A practical consequence is as follows: While the best fit (minimal randomness deficiency under complexity constraints on the model) cannot be computationally monotonically approximated, we can monotonically minimize the two-part code, or the one-part code, and thus monotonically approximate *implicitly* the best fitting model. But this should be sufficient: we want the best model rather than a number that measures its goodness. These results open the possibility of model selection and prediction that are best possible for *individual* data samples, and thus usher in a completely new era of statistical inference that is *always* best rather than *expected*. It turns out that the structure function can be viewed as a rate distortion function for individual data. With this change of viewpoint we connect Kolmogorov's approach to non-probabilistic statistics and model selection with Claude Shannon's rate distortion theory and the theory of lossy compression. This leads to a theory of rate distortion for individual data and a general class of structure functions. Based on joint work with Nikolai Vereshchagin presented partially at the 47th IEEE Symposium on Foundations of Computer Science, 2002, Vancouver, Canada. See paper at `http://www.cwi.nl/~paulv/selection.html` or `http://arXiv.org/abs/cs.CC/0204037` and recent work with Peter Grunwald and Nikolai Vereshchagin.

Abstracts of invited tutorials

► JEREMY AVIGAD, *Proof mining*.
Department of Philosophy, Carnegie Mellon University, Pittsburgh, PA 15213, USA.
E-mail: `avigad@cmu.edu`, `http://www.andrew.cmu.edu/~avigad`.

Hilbert's program can be viewed as an attempt to study infinitary, nonconstructive mathematics in more "concrete" terms. Gödel's incompleteness theorems show the impracticability of Hilbert's original goal of proving the consistency of full-blown set-theoretic reasoning using only finitary methods. But proof theorists have since been pursuing modified programs that aim to justify, interpret, or understand restricted portions of mathematical practice, with respect to constructive, computational, or otherwise explicit forms of reasoning.

The general strategy has been to show that workable developments of, say, infinitary algebra and analysis can be obtained in formal theories representing restricted fragments of set-theoretic reasoning; and that, for interesting classes of formulas, such theories are conservative over finitary or constructive counterparts. This tells us that, at least in *principal*, proofs in the general frameworks have more explicit translations.

"Proof mining" involves putting this strategy into *practice*, that is, using metamathematical techniques to obtain useful information from proofs where it is not readily apparent. Although this general idea can be found in suggestions by Georg Kreisel as early as the 1950's, it has received remarkably little attention since then. In recent years, however, there have been some interesting advances. Most notably, Ulrich Kohlenbach has had some striking successes with applications to functional analysis.

Such a program requires a general understanding of the appropriate formal theories and their metamathematical properties, as well as issues that arise when one tries to formalize mathematics in restricted frameworks. It also requires specialized techniques that are adapted to the specific domains of application. In this series of lectures, I will try to convey a sense of some of the tools and methods available, and the kinds of information that can be obtained.

► TONIANN PITASSI, *Recent advances in proof complexity*.
Department of Computer Science, University of Toronto, 10 Kings College Rd., Toronto ON M5S 3G4, Canada, and Institute for Advanced Study, Princeton, New Jersey, USA.
E-mail: toni@cs.toronto.edu.

One of the most basic questions of logic is the following: Given a universally true statement (tautology) what is the length of the shortest proof of the statement in some standard axiomatic proof system? The propositional logic version of this question is particularly important in computer science for both theorem proving and complexity theory. Important related algorithmic questions are: Is there an efficient algorithm that will produce a proof of any tautology? Is there an efficient algorithm to produce the shortest proof of any tautology? Such questions of theorem proving and complexity inspired Cook's seminal paper on NP-completeness and were contemplated even earlier by Gödel in his now well-known letter to von Neumann.

The above questions have fundamental implications for complexity theory. As formalized by Cook and Reckhow, there exists a propositional proof system giving rise to short (polynomial-size) proofs of all tautologies if and only if NP equals coNP. Cook and Reckhow were the first to propose a program of research aimed at attacking the NP versus coNP problem by systematically studying and proving strong lower bounds for standard proof systems of increasing complexity. This program has led to many beautiful results as well as to new connections with circuit complexity within the last twenty years.

In this tutorial, we will try to highlight some of the main discoveries, with emphasis on the interplay and connections with bounded arithmetic, complexity theory, and machine learning.

Abstracts of invited special lectures

► WILLIAM A. HOWARD, *Aspects of proof theory and foundations, 1950–1985*.
Department of Mathematics, Statistics, and Computer Science, University of Illinois at Chicago, 851 South Morgan Street, Chicago, IL 60607-7045, USA.
E-mail: wahow@uic.edu.

The motivating question for me in the early 1950s was as follows. Functional analysis, developed within the framework of set theory including the axiom of choice, is very abstract. What is the relation between this and the physical world? Even Peano arithmetic, PA, is problematic, since it is based on an idea of truth whose empirical meaning is not clear. Two tools for the investigation of questions of this kind within the framework of constructive reasoning have been: the descending chain principle within some system of constructive ordinal notations (Gentzen, 1938), and Gödel's interpretation of intuitionistic systems by means of functionals of finite type (1958).

New perspectives were opened up by Spector (1962) and Kreisel. This led to the pursuit of the following program. Take a suitable subsystem of classical analysis, translate this into an intuitionistic system, then give a proof theoretic treatment of the latter by means of Gödel's functional interpretation, using the appropriate system of functionals of finite type.

When one considers functionals of finite type within a constructive framework, the question arises: What is a type? In investigating this question, Curry found a striking relation between the types of elementary functionals and the theorems of positive implicational logic. This generalizes to the intuitionistic predicate calculus and to various systems of intuitionistic mathematics. The relation between types and intuitionistic logic has been found useful in the study of strongly typed programming languages.

In summary, the philosophical goals have been only partially achieved, and may very well be unachievable, but there have been some useful practical consequences.

► JOHN MCCARTHY, *What more does artificial intelligence want from mathematical logic?*
Computer Science Department, Room 208, Gates Building 2A, Stanford University, Stanford, CA 94305-2140, USA.
E-mail: `jmc@cs.Stanford.edu`.

Leibniz, Boole and Frege all expected the mathematical logic they were developing to be applicable to human affairs outside mathematics and science. Leibniz explicitly wanted to replace disputation by calculation. Unfortunately, this didn't happen.

A complete system of first order logic was essentially developed by Frege and proved complete by Gödel. The Zermelo-Fraenkel set theory formally adequate for classical mathematics was available by 1920. However, no-one was able to replace disputation by calculation by formulating common sense facts and arguments in mathematical logic.

Logical artificial intelligence (AI) since 1959 has represented facts about the common sense world in logical languages and has expressed rules giving the effects of actions and other events as sentences in languages of mostly first order logic. The plan was and is for a computer program to decide what to do by logically inferring that a certain reasoning strategy was appropriate for attempting to achieve a certain goal.

Difficulties arose that required extensions of logical formalisms. The most important extension is to nonmonotonic reasoning, in which allows brave inferences that may later have to be withdrawn. There are several systems for this, all of which can be understood in terms of preferred models. This lecture will mention circumscription, essentially minimization of a tuple of predicates subject to an axiom constraining the interpretations, with some symbols variable and others held constant.

More than just nonmonotonic reasoning is needed, but then matters become controversial even within AI. The lecture will discuss individual concepts and propositions as first order objects, contexts as objects, and approximate objects without defined extensions.

All these matters come up in connection with the common sense informatic situation that people face in trying to achieve goals. It is not decided in advance what concepts and facts are relevant.

Human-level logical AI needs the following, and logicians have helped and can help more.

1. Languages covering more and more of common sense knowledge. This work has gone slowly, because the needed concepts are often incompletely definable, i.e., don't have if-and-only-if definitions.

2. A "heavy duty" set theory within which a system can do its reasoning. Present systems are limited in scope and require too much human intervention. However, some substantial theorems, e.g., Gödel's first incompleteness theorem, have been proved by interactive systems where a person provides guidance.

3. Logical problem solving programs that can use domain dependent heuristic information. This is necessary, because present general purpose problem solvers generate too much junk.

4. A language capable of expressing meta-reasoning about theories in the language. Almost all research in mathematical logic has involved informal reasoning about theories from above rather than formal reasoning within the theory. A human-level system must not require human supervision. Making such a system requires accepting incompleteness and avoiding paradoxes by suitable weakening of axioms.

► DANA S. SCOTT, *Sets, topologies, categories*.
School of Computer Science, 5000 Forbes Ave., Carnegie Mellon University, Pittsburgh, PA 15213-3890, USA.
E-mail: dana.scott@cs.cmu.edu.

Sets and arbitrary maps form a rich category, as everyone knows, but it may not be so clear that there are natural subcategories (i.e., with fewer maps). For example, every set has an intrinsic, generally non-discrete topology. The reason is that every powerset has a natural topology (in fact, more than one, but we concentrate on the non-Hausdorff topology of "finite information"), and, in the usual formulation of Zermelo-Fraenkel set theory (ZF), every set is a subset of the powerset of its unionset. In this way a set inherits a subspace topology, and consequently set inclusion becomes the same as subspace inclusion. The intrinsic topology is easily defined, as is the notion of continuous function (a property of the usual set-theoretic notion of function), and the category of sets and continuous functions is equivalent to the category of topological T_0-spaces and continuous functions as usually defined in pointset topology. This topological category of sets can be expanded to a category of equivalence relations and continuous, equivariant functions by equally easy set-theoretic definitions, and the resulting category has interesting closure properties and applications not seen in the topological category. In intuitionistic Zermelo-Fraenkel (IZF) it is even possible to postulate the existence of a small subcategory with extensive closure properties, an inconsistent assumption in classical logic. The lecture is intended as a survey.

Abstract of invited panel discussion

► PANELISTS: KIM B. BRUCE, PETER B. HENDERSON, DANIEL LEIVANT, AND JOHN S. SCHLIPF, *Panel discussion on logic in computer science education*.
Department of Computer Science, Williams College, Williamstown, MA 01267, USA.
E-mail: kim@cs.williams.edu.
Department of Computer Science and Software Engineering, Butler University, 4600 Sunset Avenue, Indianapolis, IN 46208-3485.
E-mail: phenders@butler.edu.
Department of Computer Science, Indiana University Bloomington, Bloomington, IN 47405.
E-mail: leivant@cs.indiana.edu.
Department of Electrical and Computer Engineering and Computer Science, University of Cincinnati, Cincinnati, OH 45221.
E-mail: john.schlipf@uc.edu.

Logic is as important in computer science as calculus is in the natural science and traditional engineering fields. Yet many curricula play only lip service to its role, with logic being touched on in a discrete mathematics course that is usually poorly integrated with the rest of the computing curriculum. We argue that topics in logic should pervade the computing curriculum and point out courses where logic should play a major role. The courses and topics involving logic include architecture (logic gates), software engineering (modeling, specification and verification), programming languages (types, semantics, logic programming), database (relational algebra and SQL), artificial intelligence (automatic theorem proving, knowledge representation, and commonsense reasoning), algorithms (complexity and expressiveness), and theory of computation (general notions of computability).

Questions to be addressed include:

- What depth of logical knowledge is required of CS students?
- When and how should we teach logic (e.g., in a separate logic or discrete math course or integrated with computer science topics)?
- What materials and courseware are available and useful for teaching logic?
- How can we help students understand the importance of logical concepts to computer science?
- How can logic be reinforced throughout the CS curriculum?
- Should logic be presented to CS students differently than to mathematics and philosophy students?

Abstracts of invited talks in the Special Session on Gödel and Mathematical Logic in the 20th Century

► MARTIN DAVIS, *What did Gödel believe and when did he believe it?*
3360 Dwight Way, Berkeley, California 94704, USA.
E-mail: martin@eipye.com.

In Gödel's (unsent) reply to the questionnaire sent to him by B. D. Grandjean he asserted that since 1925 he had held a position of "mathematical realism" whereby "mathematical concepts [and sets] and theorems are describing objects of some kind." (The words in square brackets were added by Gödel.) A more nuanced story emerges from the hints made available with the publication of the magnificent five volume set of Gödel's ***Collected Works***.

► JOHN W. DAWSON, JR. AND CHERYL A. DAWSON, *Future tasks for Gödel Scholars*.
Penn State York, 393 Waters Road, York, Pennsylvania 17403, USA.
E-mail: jwd7@psu.edu.

As initially envisioned, Gödel's ***Collected Works*** were to include transcriptions of material from his mathematical workbooks. In the end that material, as well as some other manuscript items from Gödel's *Nachlass*, had to be left out. This talk will highlight unpublished items in the *Nachlass* that appear to be of interest to scholars and will survey the extent of transcription efforts undertaken hitherto. Some suggestions concerning untapped sources outside the *Nachlass* will also be given.

► SOLOMON FEFERMAN, *Gödel on the installment plan*.
Department of Mathematics, Stanford University, Stanford, CA 94305-2125, USA.
E-mail: sf@csli.stanford.edu.

I will trace the (at times halting, at other times intense) development of the Gödel editorial project from the first initiatives following Gödel's death in 1978 through the publication in 2003 of the final volumes, IV and V, of his Collected Works. This will be a mix of personal and intellectual retrospective with a pointer to the future: though our edition aimed to be (and indeed, was) comprehensive, it was, fittingly, not complete.

► WARREN GOLDFARB, *Gödel and Carnap: influence and opposition*.
Department of Philosophy, Harvard University, Emerson Hall, Cambridge, MA 02138, USA.
E-mail: goldfarb@fas.harvard.edu.

Kurt Gödel and Rudolf Carnap had significant interaction in the period 1928–1932. In fact, it was Carnap's 1928 lectures that played a crucial role in stimulating Gödel's interest in logic and foundations of mathematics. Even more specifically, Gödel's inquiries into questions of completeness were elicited by Carnap's attempt to treat similar questions in those years, and the flaws that Gödel found in it. Drawing on the analysis of Carnap's attempt in [1], I survey their interaction, the consequent nature of their influence on each other, and how it shaped the formulation of Gödel's first remarkable contributions to logic.

[1] S. AWODEY AND A. W. CARUS, *Carnap, Completeness and Categoricity: the* Gabelbarkeitssatz *of 1928*, ***Erkenntnis***, vol. 54 (2001), pp. 145–72.

► DONALD MARTIN, *Gödel's set-theoretic Platonism: one view or two?*
Department of Mathematics, UCLA, Los Angeles, CA 90095-1555, USA.
E-mail: dam@math.ucla.edu.

There is no doubt that Gödel was a Platonist about set theory (and about mathematics in general). There is, however, room for doubt about what form Gödel's set-theoretic Platonism took. Two seemingly distinct Platonistic positions can be found in his writings: (1) *object Platonism*, which holds that sets exist and are the subject of set theory; and (2) *concept Platonism* which holds that the concept of set is something objective and that it is the subject of set theory. These two positions are not obviously equivalent, and some of the consequences of Platonism that Gödel cites would appear to be consequences of (1) or of (2) but not of both.

► WILFRIED SIEG, *Only two letters: the correspondence between Herbrand and Gödel.*
Department of Philosophy, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213, USA.
E-mail: sieg@cmu.edu.

In 1931, two young logicians—whose work impacted the direction of logic dramatically and is even now central for logic and computer science—exchanged two letters. Herbrand initiated the correspondence on April 7, 1931, and Gödel responded on July 25, two days before Herbrand died in a mountaineering accident.

Herbrand's letter was to play a significant role in the development of computability theory. As Gödel first noted in his 1934 Princeton Lectures, it suggested to him a crucial part of the definition of a *general recursive function*. Understanding this role in detail is of deep interest: the notion is central, the letter had not been available until recently, and its content as reported by Gödel was not fully in accord with Herbrand's contemporaneous work.

Together, the letters reflect the broader intellectual currents of the time: they are intimately linked to the discussion of the incompleteness theorems, their potential impact on Hilbert's Program, and the concept of a finitist or intuitionist function. The analysis of the letters and their proper context undermines some deeply held convictions concerning our logical past.

► W. W. TAIT, *Gödel's reformulation of Gentzen's first consistency proof for arithmetic: the no-counterexample interpretation.*
Department of Philosophy, University of Chicago, Chicago, IL 60637, USA.
E-mail: wwtx@earthlink.net.

In *1938a, Gödel rather briefly describes a reformulation of Gentzen's first consistency proof that applies directly to the Hilbert-style formalization of *PA* rather than to formalizations in the sequence calculus or natural deduction. He asserts that, from each proof of an arithmetic formula A in *PA*, we effectively obtain a sequence $\vec{\Phi}$ of third-order functionals, defined by recursion up to some ordinal $< \epsilon_0$, and a proof of $\forall \vec{f} B(\vec{\Phi}, \vec{f})$, where $\exists \vec{G} \forall \vec{f} B(\vec{G}, \vec{f})$ is (what came to be called) a no-counterexample interpretation of A. I will present a more detailed exposition of the argument.

Abstracts of invited talks in the Special Session on Logic and Games

► CRISTINA BICCHIERI, *A taste for fairness*.
Department of Philosophy, College of Humanities and Social Sciences, Carnegie Mellon University, 161 Baker Hall, Pittsburgh, PA 15213, USA.
E-mail: cb36@andrew.cmu.edu.

In recent years, a number of experimental games have pointed to the importance of fairness considerations in shaping players' behavior. Experiments on Ultimatum bargaining reveal that the subjects' payoff values do not reflect just their own monetary gains. Subjects seem to have a shared idea of a fair outcome, as well as a tendency to enact it. Several models have been advanced to explain the data, all of them introducing modified utility functions that either assume an individual's preference for fair outcomes, a sensitivity to the intentions of other players, or a propensity to recognize and follow established norms. I present a social norms approach and assume that, whenever a social norm exists and is made focal, individuals will have an incentive to follow it. A player's propensity to follow a norm is represented in a new kind of utility function. I will test my approach on 'anomalous' experimental data that challenge the view that subjects have simple fairness preferences, or a desire to reciprocate good (bad) behavior.

► STEVEN J. BRAMS, D. MARC KILGOUR, AND M. REMZI SANVER, *A minimax procedure for electing committees*.
Department of Politics, New York University, New York, NY 10003, USA.
E-mail: steven.brams@nyu.edu.
Department of Mathematics, Wilfrid Laurier University, Waterloo, Ontario N2L 3C5, Canada.
E-mail: mkilgour@wlu.ca.
Department of Economics, Istanbul Bilgi University, 80310, Kustepe, Istanbul, Turkey.
E-mail: sanver@bilgi.edu.tr.

A procedure for electing committees of two or more members, called the minimax procedure, is described. While based on approval voting (AV), it does not aggregate approval votes in the usual manner. Instead of electing those candidates that get the most approval, the minimax procedure chooses the committee that minimizes the maximum "Hamming distance" to the voters (minimax outcome). It is shown that such an outcome may be diametrically opposed to the usual AV outcome, which minimizes the sum of the Hamming distances to all voters (minisum outcome). Although the minimax outcome—unlike the minisum outcome—is manipulable in theory, in practice it almost surely is not because of (i) a lack of information voters have about each others' preferences and (ii) the computational complexity of manipulating such information, even if it were available.

The minimax procedure is applied to the 2003 Game Theory Society (GTS) election of a council of 12 new members from a list of 24 candidates. The 9th and 10th biggest vote-getters would have been displaced by the 16th and 17th biggest vote-getters if the minimax procedure had been used. If the number of candidates to be elected had been endogenous rather than being fixed at 12, the minisum outcome would have been election of the five candidates that received majority approval from the 161 voters, whereas the minimax outcome would have been the election of ten candidates, two of whom would not have received the most votes. It is argued that when few if any voters cast identical AV ballots, as with true in the GTS election (there were $2^{24} \approx 16.8$ million possible ballots), a minimax committee will better represent the interests of all voters than a minisum committee.

► ADAM BRANDENBURGER AND H. JEROME KEISLER, *An impossibility theorem on beliefs in games*.

Stern School of Business, New York University, 44 West Fourth Street, New York, NY 10012, USA.
E-mail: abranden@stern.nyu.edu.
Department of Mathematics, University of Wisconsin-Madison, Madison, WI 53706, USA.
E-mail: keisler@math.wisc.edu.

A paradox of self-reference for beliefs in games is identified, which yields a game-theoretic impossibility theorem akin to Russell's paradox. An informal version of the paradox is that the following configuration of beliefs is impossible:

> Ann believes that Bob assumes that
> Ann believes that Bob's assumption is wrong.

This can be formalized to show that any belief model of a certain kind must have a "hole".

► ROHIT PARIKH, *Social software and the logical properties of real life procedures*.
City University of New York, CUNY Graduate Center, 365 Fifth Avenue, New York, NY 10016, USA.
E-mail: rparikh@gc.cuny.edu.

Social software is the study of procedures in ordinary life, carried out either by individuals or by groups, and the latter is of course the more interesting and difficult case.

Techniques from the Logic of Programs and the Analysis of Algorithms sometimes come in handy. But so do techniques from Game theory, as people's actions depend on their preferences (as well as their beliefs).

An interesting fact to observe is that the physical structures used in certain procedures have logical properties. For instance queues in real life preceded the (abstract) queues as data types, and they have the same requisite (FIFO) properties needed for fairness as does the (more convenient) mechanism of tickets. The logical properties of electoral systems are even more interesting, and some recent techniques allow us to study such systems.

In this talk we discuss individual procedures, group procedures and the flow of knowledge needed for them to work.

Abstracts of invited talks in the Special Session on Logical Foundations of Programming Semantics

► ANDREJ BAUER AND CHRISTOPHER STONE, *From theories to signatures*.
Department of Mathematics and Physics, University of Ljubljana, Jadranska 19, Slovenia.
E-mail: Andrej.Bauer@andrej.com.
Computer Science Department, Harvey Mudd College, 1250 North Dartmouth Avenue, Claremont, CA 91711, USA.
E-mail: stone@cs.hmc.edu.

Much work has been done on extraction of programs from proofs. A less ambitious, but possibly equally rewarding, endeavor is extraction of abstract data types from axiomatizations of first-order theories. We use a realizability interpretation of an (intuitionistic) first-order theory to translate an axiomatization of a mathematical structure to an ML signature for a structure which implements it. In addition, the interpretation gives us a set of negative formulas which express criteria that a concrete implementation of the signature must satisfy, if it is to be a correct implementation of the original first-order theory. The fact that the correctness criteria are expressed as negative formulas is desirable, because their classical reading is the same as their intuitionistic reading. One practical benefit of this is that also programmers who are not familiar with intuitionistic logic will correctly understand correctness.

► MARTÍN ESCARDÓ, *Topology via higher-order logic*.
School of Computer Science, The University of Birmingham, Birmingham B15 2TT, UK.
E-mail: m.escardo@cs.bham.ac.uk.

For suitable topologies, computable functions are continuous, and semidecidable properties of their inputs/outputs are open, but the converses of these two statements fail. Some authors attempted to resolve this mismatch by considering effective or constructive versions of topology.

In recent work [1], we instead propose a synthetic approach, in which both classical topology and various computational flavours arise as special cases. The idea is to (i) take continuity to mean definability in a given base language, and (ii) reduce other topological notions (such as open set, closed set, compact set, discrete space, Hausdorff space) to that of continuity with the aid of the Sierpinski space, (iii) use the lambda calculus to prove theorems about them. We shall give an overview, with some interesting computational applications.

However, the main aim of this talk is to reformulate and redevelop synthetic topology in the internal language of a topos. Exploiting the fact that excluded middle fails, one can define a non-trivial topology on the one-point set, where not all unions of open sets are necessarily postulated to be open. Technically, one obtains a subset of the subobject classifier, known as a dominance, which is to be thought of as a "Sierpinski set". This induces topologies on all sets, making all functions continuous.

However, because virtually all theorems of classical topology require excluded middle (and even choice), it would be useless to reduce all other topological notions to the notion of open set in the usual way. So, for example, our synthetic definition of compactness for a set X says that, for any Sierpinski-valued predicate p on X, the truth value of the statement "for all x in X, $p(x)$" lives in the Sierpinski set. The proposed synthetic notions interact in the expected way. Moreover, we show that there are embeddings of full subcategories of topological spaces into toposes that translate the classical notions into the synthetic ones, and, similarly, we look at computational manifestations of the synthetic notions by embedding programming languages into toposes.

[1] M. H. Escardo, ***Topology of data types and computability concepts***, 93pp. School of Computer Science, University of Birmingham, UK.
http://www.cs.bham.ac.uk/~mhe/papers/barbados.pdf

► NICOLA GAMBINO AND MARTIN HYLAND, *Wellfounded trees, fixpoints, and free monads*.
DPMMS, University of Cambridge, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, UK.
E-mail: N.Gambino@dpmms.cam.ac.uk.
E-mail: M.Hyland@dpmms.cam.ac.uk.

We will study the consequences of the assumption of types of wellfounded trees in dependent type theories. In order to do so, we investigate the categorical notion of wellfounded tree recently introduced by Moerdijk and Palmgren. Our main results show that wellfounded trees allow us to define initial algebras for a wide class of endofunctors on locally cartesian closed categories. We give some applications of this result to the theory of fixpoints and free monads.

► ALEX SIMPSON, *Axioms for synthetic domain theory*.
LFCS, School of Informatics, University of Edinburgh, JCMB, King's Buildings, Edinburgh EH9 3JZ, UK.
E-mail: Alex.Simpson@ed.ac.uk.

Synthetic domain theory aims to provide a simple theory of "domains", for use in programming language semantics, in which domains are merely (special) sets, and morphisms of domains are arbitrary set-theoretic functions. For several reasons, no such theory is possible within ordinary classical set theory. However, Dana Scott, long ago indicated that such a theory should be compatible with intuitionistic set theory. In this talk I will outline the synthetic domain theory program, and summarize recent progress towards finding simple and usable set-theoretic axioms which finally make synthetic domain theory a viable tool for applications to the semantics of programming languages.

Abstracts of invited talks in the Special Session on Set Theory

► ELIZABETH THETA BROWN, *Uncountable tree forcing*.
Department of Mathematics and Statistics, James Madison University, Harrisonburg, Virginia 22807, USA.
E-mail: brownet@math.jmu.edu.

Forcing via partial orders whose conditions are trees on omega, introduced by Sacks, Laver, Miller and others, has been applied to produce results in diverse areas, including cardinal invariants, degrees of constructibility, and nonstandard analysis.

We will discuss forcing with trees over regular uncountable cardinals. As filters over uncountable cardinals behave differently than filters over omega, properties of the generic function and applications do not always parallel the countable case. Even where results can be directly generalized, they are often true for different reasons than at omega. The talk will describe uncountable versions of Miller and Laver forcing, characterize their generic functions, and give sufficient conditions for cardinal preservation, along with some applications.

A short bibliography of some other work in the general area of uncountable forcing will also be provided.

► JOHN CLEMENS, *Complemented sets and difference sets*.
Mathematics Department, Penn State University, University Park, State College, PA 16802, USA.
E-mail: clemens@math.psu.edu.

A set X of natural numbers is complemented if there is another set Y of natural numbers such that every natural number n is uniquely represented as $n = x + y$ with x in X and y in Y. A set X is a difference set if there is another set Y such that $X = \{|n - m| : n, m \text{ in } Y\}$. I will discuss several descriptive complexity results concerning these sets, in particular that the collection of complemented sets is a complete analytic set, as is the collection of sets which contain an infinite difference set.

► NATASHA DOBRINEN, *κ-stationary sets are necessary in the investigation of relationships between general distributive laws and infinitary games in Boolean algebras*.
Mathematics Department, Penn State University, University Park, State College, PA 16802, USA.
E-mail: dobrinen@math.psu.edu.

For some time, we have been investigating relationships between general distributive laws and infinitary cut-and-choose games (first introduced and investigated by Jech) in complete Boolean algebras. When $\mu \leq \kappa \leq \lambda$ there is an interesting interplay between the $(\kappa, \lambda, <\mu)$-distributive law, whether Player I has a winning strategy for the game $\mathcal{G}^{\kappa}_{<\mu}(\lambda)$, and κ-stationarity of $V \cap [\lambda]^{\leq\kappa}$. The flavor of our results is represented by the following two theorems. If $\mu \leq \kappa^{<\kappa} = \kappa \leq \lambda$ and B is $(<\kappa, \kappa)$-distributive, then B is $(\kappa, \lambda, <\mu)$-distributive and B preserves κ-stationarity of $[\check{\lambda}]^{\leq\kappa} \cap V$ iff Player I does not have a winning strategy for $\mathcal{G}^{\kappa}_{<\mu}(\lambda)$. If B preserves stationarity of $[\check{\lambda}]^{\omega} \cap V$, then B satisfies the weak (ω, ω)-d.l. iff B satisfies the weak (ω, λ)-d.l.

► TODD EISWORTH, *Generalizing properness*.
Department of Mathematics, University of Northern Iowa, Cedar Falls, IA 50614, USA.
E-mail: eisworth@math.uni.edu.

Proper forcing is an important concept because of two salient properties: (1) it does not collapse $\aleph_1$, and (2) it is preserved by countable support iterations.

We look at the problem of generalizing proper forcing to cardinals larger than $\aleph_1$. We outline the obstacles that show that naive generalizations cannot work, and then discuss recent progress together with some applications.

► TETSUYA ISHIU, *Applications of guessing sequences to general topology*.
Department of Mathematics, University of Kansas, Lawrence, Kansas 66045-7523, USA.
E-mail: ishiu@math.ukans.edu.

Guessing sequences, including $\diamondsuit$-sequences, $\clubsuit$-sequences, and club guessing sequences, have been effectively used in general topology. I will talk about recent applications of the sequences and new methods to construct a guessing sequence with some properties, which were motivated by interests in topology.

► BERNHARD KOENIG, *Preservation of forcing axioms*.
Department of Mathematics, UC Irvine, Irvine, CA 92697-3875, USA.
E-mail: bkoenig@math.uci.edu.

We show that in Banach-Mazur games of length ω_1, it makes a huge difference if we allow either player Empty or Nonempty to play at limit stages. It is folklore, that we can add a $\square$-sequence with a poset for which Nonempty wins but only if he's allowed to play at limit stages. This is optimal in the following sense: If we force over a model of MM and Nonempty wins the game on the forcing poset in even the stronger sense, then neither ω_2-Aronszajn-trees nor non-reflecting sets are added. We go on to show that full PFA is not preserved by this stronger closure property, but PFA is actually preserved by $< \omega_2$-closed forcings.

This is joint work with Yasuo Yoshinobu.

► BEN MILLER, *Unwed and without direction*.
University of California, Berkeley, USA.
E-mail: bdm@its.caltech.edu.

Modifications of ideas of Dougherty-Jackson-Kechris and Shelah-Weiss can be used to classify a variety of objects other than hyperfinite equivalence relations. We will describe one such example. A Borel forest of lines is undirectable if it is not the (orbit) graph generated by an aperiodic Borel automorphism. Up to a descriptive version of Kakutani equivalence, there is exactly one such forest (in fact, there are exactly three Borel forests of lines up to this notion of equivalence). Such forests are intimately related to the sorts of Borel marriage problems which were studied by Laczkovich and Klopotowski-Nadkarni-Sarbadhikari-Srivastava, and our proofs shed new light on these problems.

Abstracts of contributed talks

► PETER B. ANDREWS AND CHAD E. BROWN, *Proving theorems and teaching logic with TPS and ETPS*.
Department of Mathematical Sciences, Carnegie Mellon University, Pittsburgh, PA 15213, USA.
E-mail: andrews@cmu.edu.
E-mail: cebrown@andrew.cmu.edu.

The Theorem Proving System TPS can be used to construct and check formal proofs interactively, semi-automatically, and automatically. Theorems are expressed in Church's type theory. This includes first-order logic, but in a practical sense it has greater expressive power, and it is particularly well suited to the formalization of mathematics and other disciplines. In automatic mode, TPS first searches for an *expansion proof*, which is a higher-order analogue of a Herbrand expansion, and then transforms this into a proof in natural deduction style.

We show how TPS can prove various theorems automatically or semi-automatically. Some examples of theorems which TPS can prove automatically are:

THM15B: If some iterate of function f has a unique fixed point, then f has a fixed point.

THM136: The transitive closure of a relation is transitive.

THM145: In a complete lattice, every monotone function has a fixed point.

THM531E: A subset of a finite set is finite.

A related program called ETPS contains only interactive facilities, and is used by logic students to construct formal proofs in natural deduction style.

Both TPS and ETPS are available from the web. For more information see [1], [2], and `http://gtps.math.cmu.edu/tps.html`.

Research supported by NSF Grant CCR-0097179.

[1] Peter B. Andrews, Matthew Bishop, Sunil Issar, Dan Nesmith, Frank Pfenning, and Hongwei Xi, *TPS: A theorem proving system for classical type theory*, ***Journal of Automated Reasoning***, vol. 16 (1996), pp. 321–353.

[2] Peter B. Andrews, Matthew Bishop, Chad E. Brown, Sunil Issar, Frank Pfenning, and Hongwei Xi, *ETPS: A system to help students write formal proofs*, ***Journal of Automated Reasoning***, vol. 32 (2004), pp. 75–92.

► CHAD E. BROWN, *Set comprehension in Church's type theory*.

Department of Mathematical Sciences, Carnegie Mellon University, Pittsburgh, PA 15213, USA.

E-mail: `cebrown@andrew.cmu.edu`.

In order to prove theorems involving sets and functions, one often uses comprehension principles asserting the existence of certain sets. We explore the consequences of restricting which logical constants are allowed in these comprehension principles in the context of Church's type theory.

Church's type theory is a formulation of higher-order logic that allows quantification over sets and functions. In this logic, any set definable by an expression of the language can be proved to exist. This expressive power allows a natural formalization of much of mathematics.

The logical constants we consider are propositional connectives, equality and quantifiers over various types. For example, we consider fragments of Church's type theory which satisfy comprehension with respect to quantifiers over individuals, but not over sets of individuals. There are natural sequent calculi and corresponding semantics for any given signature. In some cases, adding logical constants to a signature does not increase the set of theorems (giving conservation results). In other cases, adding logical constants does increase the set of theorems (giving independence results). We establish these results using models of fragments of type theory.

For example, the usual proof of Cantor's theorem that there is no surjection from a set S onto its power set $\mathcal{P}(S)$ uses a diagonal set whose definition involves a negation. We construct a model showing that this theorem cannot be proven in a fragment of Church's type theory which lacks comprehension principles involving negation. To prove the version of Cantor's theorem that there is no injection from $\mathcal{P}(S)$ into S requires comprehension principles involving quantifiers over sets in $\mathcal{P}(S)$ and equality of objects in S as well as negation.

Research supported by NSF Grand CCR-0097179.

► WALTER DEAN, *From Church's thesis to extended Church's thesis*.
Research Group in Logic and Computation, Department of Computer Science, CUNY Graduate Center, 365 5th Avenue, New York, NY 10016, USA.
E-mail: wdean@www.cs.gc.cuny.edu.

Extended Church's Thesis [ECT] is the claim that any informal algorithm (e.g., Euclid's algorithm, Mergesort) can be analyzed as an instance of a formal model of computation such (e.g., a particular Turing machine) in a manner that preserves its identifying computational properties. ECT is thus a far stronger statement than that traditionally identified as Church's Thesis [CT]: the latter seeks to analyze only the extension of the concept 'function computed by an algorithm' while the former seeks to analyze the intensional properties of individual mathematical procedures.

There is a modern tendency to either misidentify CT as ECT or to consider arguments originally given in favor of CT as having actually established ECT. Gödel, Kreisel, Davis, Sipser and Lewis & Papadimitriou have all made statements to this effect, the latter describing CT as follows:

> [W]e take the Turing machine to be a precise formal equivalent of the intuitive notion of "algorithm": nothing will be considered an algorithm if it cannot be rendered as a Turing machine. The principle that Turing machines are formal versions of algorithms and that no computational procedure will be considered an algorithm unless it can be presented as a Turing machine is known as Church's Thesis . . .

This talk will consider the historical and conceptual passage from CT to ECT. I will first argue that while it is doubtful that ECT would have been accepted during the 1930s, Kleene and Rogers both present traditional arguments for CT as establishing a claim similar to ECT. Next, I will introduce a framework for evaluating versions of ECT given in terms of arbitrary models of computation. Finally, I will argue that even relative to the models recently proposed by Moschovakis and Gurevich, the corresponding versions of ECT are likely to be false.

► ROD DOWNEY AND LIANG YU, *There are no maximal low d.c.e. degrees*.
School of Math and Computing Sciences, Victoria University of Wellington, 6001, Wellington, New Zealand.
E-mail: rod.downey@mcs.vuw.ac.nz.
E-mail: yuliang@mcs.vuw.ac.nz.

In [1], Arslanov, Cooper and Li claimed that for every low L and c.e. set A with $L <_T A$, there exists a c.e. splitting $A_1 \sqcup A_2 = A$ such that $A_1 \oplus L|_T A_2 \oplus L$. As a consequence Arslanov, Cooper and Li observed that there is no maximal low d.c.e. Turing degree. Unfortunately, the proof of Arslanov et al. contains a fatal flaw. We give a direct proof of the latter claim of Arslanov et al. by showing that there is no maximal low d.c.e. degree.

The technique is of some interest, since it would seem one of the few results which use lowness via the "Robinson trick" outside of the c.e. degrees. We also prove that for any low d.c.e. degree, there is a low d.c.e. degree above it and so there are infinitely many d.c.e. degrees above it. But we do not know whether there is a d.c.e. splitting of $0'$ above it.

[1] M. Arslanov, S. B. Cooper and Angsheng Li, *There is no low maximal d.c.e. degree*, ***Mathematical Logic Quarterly***, vol. 46 (2000), pp. 409–416.

► SERGIO FRATARCANGELI, *Elimination of imaginaries in generic expansions of o-minimal theories*.
Department of Mathematics and Statistics, McMaster University, 1280 Main Street West, Hamilton, Ontario L8S 4K1, Canada.
E-mail: fratars@math.mcmaster.ca.

Let T be a complete first-order L-theory with quantifier elimination and the uniform finiteness property. Let P be a unary predicate not contained in L. Pillay and Chatzidakis showed that T has a model companion, T_P, in the language $L \cup \{P\}$. In addition, they proved that if T is stable and eliminates imaginaries, then T_P also eliminates imaginaries. In this talk, we'll sketch a proof that this result holds when "stable" is replaced by "o-minimal".

► THOMAS KENT, *Results on non-splitting Σ^0_2 enumeration degrees*.
University of Wisconsin, Madison, 2207 Woodview Ct. #12, Madison, WI 53713, USA.
E-mail: kent@math.wisc.edu.

We will define enumeration reducibility and give a brief history of the enumeration degrees. We show that these non-splitting Σ^0_2 degrees are downward dense in the Δ^0_2 e-degrees and show the existence of a properly Σ^0_2 e-degree. We will examine current progress towards determining the decidability of the Π_2 theory of the Σ^0_2 e-degrees.

► ROMAN KUZNETS, *On decidability of the logic of proofs with arbitrary constant specifications*.
Computer Science, CUNY Graduate Center, 365 Fifth Avenue, New York, NY 10016, USA.
E-mail: rkuznets@gc.cuny.edu.

Logic of Proofs $\mathcal{LP}$ introduced by Artemov gave an exact intended semantics for Gödel's logic of provability $S4$ [1], [2]. This Logic of Proofs considers statements of the form $t\colon F$ where a proof term t (called proof polynomial) denotes a proof for F. Proof polynomials are built from variables and proof constants c which stand for proofs of axioms of the theory. Logic of Proofs has a natural arithmetical semantics where $t\colon F$ is interpreted as a formal arithmetical statement "t is a proof of F in $\mathcal{PA}$." Proof constants are specified by accepting as postulates constant specifications $\mathcal{CS}$ which are sets of formulas of sort $\{c_1\colon A_1, c_2\colon A_2, \dots\}$ where c_i is a proof constant and A_i an axiom. A theory $\mathcal{LP}_{\mathcal{CS}}$ is a theory with constant specification $\mathcal{CS}$. Logic $\mathcal{LP}_0$ corresponding to the empty $\mathcal{CS}$ was shown to be decidable in [1]. Mkrtychev in [3] has shown that if $\mathcal{CS}$ contains only a finite number of axiom schemes for each constant then $\mathcal{LP}_{\mathcal{CS}}$ is decidable. We show that those results do not extend to all decidable constant specifications.

THEOREM 1. *There is a decidable constant specification $\mathcal{CS}$ such that the logic $\mathcal{LP}_{\mathcal{CS}}$ is undecidable.*

Moreover, it can be shown that even a decidable constant specification involving only one constant already may lead to an undecidable theory $\mathcal{LP}_{\mathcal{CS}}$.

[1] SERGEI N. ARTEMOV, *Operational modal logic*, Technical Report MSI95-29, Cornell University, 1995.

[2] ———, *Explicit provability and constructive semantics*, ***The Bulletin of Symbolic Logic***, vol. 7 (2001), no. 1, pp. 1–36.

[3] ALEXEY MKRTYCHEV, *Models for the Logic of Proofs*, ***LFCS***, Lecture Notes in Computer Science, vol. 1234 (1997), pp. 266–275.

► DANIEL LEIVANT, *Second order logic and the metamathematics of logics of programs*.
Department of Computer Science, Indiana University, 150 S. Woodlawn Avenue, Bloomington, IN 47405, USA.
E-mail: leivant@cs.indiana.edu.

Deductive reasoning about imperative programs has been formalized in various settings, using e.g., programs as modalities, temporal modalities, fixpoint operators, first order renditions of program-semantics, and infinitary logic. Pursuing ideas first presented in [1], we use instead second order logic (with restricted Comprehension), and establish a gamut of new as well as known meta-mathematical properties of modal logics of programs. In particular, we characterize the proof theoretic power of first order Dynamic Logics, and of their extension with a fixpoint operator.

[1] Daniel Leivant, *Logical and mathematical reasoning about programs*, ***Conference Record of the Twelfth Annual Symposium on Principles of Programming Languages***, ACM, New York, 1985, pp. 132–140.

► BENEDIKT LÖWE, *Measure assignments and Kleinberg sequences*.
Institute for Logic, Language and Computation, Universiteit van Amsterdam, Plantage Muidergracht 24, 1018 TV Amsterdam, The Netherlands.
E-mail: `bloewe@science.uva.nl`.

Jackson has developed his description theory in order to compute the projective ordinals in the theory ZF + AD. The main technical tool of description theory is the assignment of measures (more exactly, of descriptions) to cardinals below the supremum of the projective ordinals.

In this talk, we shall discuss further consequences of the existence of such a measure assignment. As a corollary, we develop algorithms to compute the regular cardinals, all cofinalities and all Kleinberg sequences below the supremum of the projective ordinals.

The work described is joint work with Steve Jackson (Denton, TX).

► YEVGENIY MAKAROV, *Classical proofs viewed as functional programs with control operators*.
Department of Computer Science, Indiana University, Bloomington, IN 47405-7104, USA.
E-mail: `emakarov@cs.indiana.edu`.

In [2], Griffin extended Curry-Howard isomorphism to classical logic by observing that inference by contradiction corresponds to Felleisen's control operator $\mathcal{C}$. However, the exact correspondence between the program extracted from a classical derivation and the constructive content of its derived formula has remained unclear to date.

We formulate and prove such a correspondence for proofs of Π^0_2 formulas. The main idea is the following. Fix a closed formula F not containing $\perp$ and replace all occurrences of $\perp$ in a classical natural deduction derivation $\mathcal{D}$ by F. This, of course, makes $\mathcal{D}$ not a valid derivation because now it may contain nodes of the form

$$\frac{F}{D} \quad \text{and} \quad \frac{(D \to F) \to F}{D},$$

which correspond to intuitionistic and classical rules for negation, respectively. However, if $\mathcal{D}$ is a closed derivation of F, these nodes may be eliminated by conversions on derivations which by Curry-Howard isomorphism correspond to conversions for control operators $\mathcal{A}$ and $\mathcal{C}$.

We propose some extensions to Griffin's method that handle equality and atomic inference rules. Applying this method, we are able to extract SCHEME programs from a broad class of classical proofs including several interesting ones considered in [1].

[1] Ulrich Berger, Wilfried Buchholz, and Helmut Schwichtenberg, *Refined program extraction from classical proofs*, ***Annals of Pure and Applied Logic***, vol. 114 (2002), no. 1–3, pp. 3–25.

[2] Timothy G. Griffin, *Formulas-as-types notion of control*, ***Conference record of the seventeenth annual ACM symposium on principles of programming languages***, 1990, pp. 47–58.

► RUSSELL MILLER, *The curious case of order-computable sets*.
Department of Mathematics, Queens College–CUNY, 65-30 Kissena Blvd., Flushing, NY 11367, USA.
E-mail: `rmiller@forbin.qc.edu`.

Let S be a subset of ω, and consider the structure $(\omega, <, S)$, in the language of linear orders with an additional unary predicate. We say that S is *order-computable* if this structure is computably presentable, i.e., if there is a computable set C and a computable order $\prec$ on ω such that $(\omega, \prec, C) \cong (\omega, <, S)$.

This simple concept resists any straightforward characterization by purely computability-theoretic properties. We present a survey of results about order-computable sets, with proofs described or sketched as time permits, including the following. All low c.e. sets are order-computable, but there exist c.e. sets and low d.c.e. sets which are not. Every n-c.e. set is Turing-equivalent to an n-c.e. order-computable set, and similarly for ω-c.e. sets. However, there exist Turing degrees below $\mathbf{0}'$ containing no order-computable set. There also exist (noncomputable) Turing degrees containing only order-computable sets. No 1-random set is order-computable. Finally, we prove that there exist an order-computable set and an order-noncomputable set which are computably isomorphic to each other. This last result suggests the extent to which the property of order-computability differs from most computability-theoretic properties.

This work is joint with Denis Hirschfeldt and Sergey Podzorov. Additional related results have recently been obtained by Downey, Khoussainov, J. Miller, Nies, and Yu.

► PAVEL NAUMOV, *On modal logic of partial computable functions*.
Computer Science, Penn State Harrisburg, Middletown, PA 17057, USA.
E-mail: `naumov@psu.edu`.

The classical propositional logic is sound and complete with respect to the set semantics τ under which propositional connectives conjunction, disjunction, and negation are interpreted as operations intersection, union, and complement on subsets of any infinite universe. In particular, the universe could be the set of all words in some alphabet Σ. We extend the language of the classical propositional logic by a new binary modality $\rhd$. The set semantics is extended to interpret modality $\rhd$ as the following operation on subsets of Σ^*: $\tau(\phi \rhd \psi)$ is equal to the set of all $x \in \Sigma^*$ such that for any $y \in \tau(\phi)$ if Turing machine x terminates on input y then it returns an element of $\tau(\psi)$ as output. The modal logic of partial computable functions is the set of all propositional modal formulas whose interpretation is equal to Σ^* for any interpretation of propositional variables.

THEOREM 1. *The modal logic of partial computable functions is an extension of the classical propositional logic by the following axioms*:

$$\phi \rhd \psi \to (\phi \rhd \chi \to \phi \rhd (\psi \wedge \chi)) \quad \text{(C)}$$
$$\phi \rhd \psi \to (\chi \rhd \psi \to (\phi \vee \chi) \rhd \psi) \quad \text{(D)}$$
$$\bot \rhd \phi \quad \text{(F)} \qquad\qquad \phi \rhd \top \quad \text{(T)}$$

and, in addition to Modus Ponens, the following inference rules:

$$\frac{\phi \to \psi}{\psi \rhd \chi \to \phi \rhd \chi} \quad \text{(LM)} \qquad\qquad \frac{\phi \to \psi}{\chi \rhd \phi \to \chi \rhd \psi} \quad \text{(RM)}$$

THEOREM 2. *The modal logic of partial computable functions is decidable.*

► MICHAEL RAY OLIVER, *Many nonisomorphic Boolean algebras $\mathcal{P}(\omega)/\mathcal{I}$*.
Department of Mathematics, P.O. Box 311430, University of North Texas, Denton, TX 76203–1430, USA.
E-mail: `moliver@unt.edu`.

This talk presents a summary of work to appear in the JSL; time permitting; it may also touch on recent joint work with Su Gao.

I examine the question of how many Boolean algebras, distinct up to isomorphism, that are quotients of the powerset of the naturals by Borel ideals, can be proved to exist in ZFC alone. The maximum possible value is easily seen to be the cardinality of the continuum $2^{\aleph_0}$; earlier work by Ilijas Farah had shown that this was the value in models of Martin's

Maximum or some similar forcing axiom, but it was open whether there could be fewer in models of the Continuum Hypothesis.

I develop and apply a new technique for constructing many ideals whose quotients must be nonisomorphic in any model of ZFC. The technique depends on isolating a kind of ideal, called shallow, that can be distinguished from the ideal of all finite sets even after any isomorphic embedding, and then piecing together various copies of the ideal of all finite sets using distinct shallow ideals. In this way we are able to demonstrate that there are continuum-many distinct quotients by Borel ideals, indeed by analytic P-ideals, and in fact that there is in an appropriate sense a Borel embedding of the Vitali equivalence relation into the equivalence relation of isomorphism of quotients by analytic P-ideals.

Recent work with Gao examines whether an arbitrary Borel equivalence relation may be embedded into the isomorphism relation on quotients by Borel ideals.

► ERIC PACUIT AND ROHIT PARIKH, *A logic for communication graphs* (*Preliminary report*).
Department of Computer Science, Graduate Center, CUNY, New York, NY, USA.
E-mail: epacuit@cs.gc.cuny.edu.
Computer Science, Mathematics, Philosophy, City University of New York, New York, NY, USA.
E-mail: rparikh@gc.cuny.edu.

The *Topologic* of Moss and Parikh is extended to the case of many agents $\mathcal{A} = (1, \dots, n)$ who are assumed to have some private information at the outset, but may refine their information by acquiring information possessed by other agents, possibly via other agents. $\mathcal{P}_i$ is i's information partition; $\hat{\mathcal{P}} = (\mathcal{P}_1, \dots, \mathcal{P}_n)$. Partitions refine when information is exchanged.

In the *communication graph* on $\mathcal{A}$, an edge (i, j) means that agent i can directly receive information from agent j. W is the set of possible worlds and V some valuation on W of the propositional symbols, understood by all agents, but with only specific agents knowing their actual values at worlds $x \in W$.

L_0 is the propositional (base) language, L' its closure under the operators K_i, and L *its* closure (only) under $\diamond$ and the boolean operators. Given a partition $\mathcal{P}$, $\mathcal{P}(x)$ is that cell of the partition $\mathcal{P}$ in which x lies.

$x, \hat{\mathcal{P}} \models P$ means that $V(x, P) = 1$, booleans are interpreted n the obvious way.

$x, \hat{\mathcal{P}} \models K_i\phi$ iff $(\forall y \in \mathcal{P}_i(x), y, \hat{\mathcal{P}} \models \phi)$

$x, \hat{\mathcal{P}} \models \diamond\phi$ iff $(\exists\hat{\mathcal{Q}}$ such that $\hat{\mathcal{Q}}$ refines $\hat{\mathcal{P}}$ and $x, \hat{\mathcal{Q}} \models \phi)$

The formula scheme $K_i(\phi) \rightarrow \diamond K_j(\phi)$ holds iff agent j can directly or indirectly acquire information possessed by i. The validities of *Topologic* remain valid and the communication graph is completely determined by the validities of the resulting logic. Applications of our logic to the Bush–Tenet dilemma are obvious.

[1] Moss and Parikh, *Topological reasoning and the logic of knowledge*, ***TARK IV***, Y. Moses (editor), Morgan Kaufmann, 1992.

► ALEXANDER RAICHEV, *Relative randomness and real closed fields*.
University of Wisconsin-Madison, Department of Mathematics, 480 Lincoln Dr., Madison WI 53706, USA.
E-mail: raichev@math.wisc.edu.

We prove that for all $\beta \in {}^{\omega}2$, $\mathcal{R}^\beta := \langle \mathbb{R}^\beta, +, \cdot, < \rangle$ is a countable real closed field, where $\mathbb{R}^\beta$ is the set of all reals less random than β in the sense of rK reducibility. This generalizes the fact that the computable reals form a countable real closed field. One consequence of this and its proof is that the d.c.e. reals form a real closed subfield of the field of reals less random than Ω, Chaitin's random real.

[1] K. AMBOS-SPIES, K. WEIHRAUCH, AND X. ZHENG *Weakly computable real numbers*, ***Journal of Complexity***, vol. 16 (2000), pp. 676–690.

[2] R. G. DOWNEY, D. HIRSCHFELDT, AND G. LAFORTE, *Randomness and reducibility*, ***Journal of Computer and System Sciences***, vol. 68 (2004), pp. 96–114.

[3] D. MARKER, *Model theory: An introduction*, Springer-Verlag, Berlin/Heidelberg, Germany and New York, USA, 2002.

[4] M. B. POUR-EL AND J. I. RICHARDS, *Computability in analysis and physics*, Springer-Verlag, Berlin/Heidelberg, Germany and New York, USA, 1989.

► MARTIN K. SOLOMON, *Some remarks on Gödelian philosophy*.
Department of Computer Science and Engineering, Florida Atlantic University, Boca Raton, FL 33431, USA.
E-mail: martysolom@aol.com.

It is considered whether Kurt Gödel's philosophy of mathematics, especially as expressed in [2, p. 484], taken together with footnote 11 in [2, p. 475], can be viewed as a form of "epistemological structuralism" similar to (but more optimistic than) what is given in [5, p. 134]. Compare also with Gödel's letter to Greenberg in [1, p. 454].

It is shown that both Gödel's general relativity results concerning rotating universes, and certain special relativity results concerning tachyon inertial frames [4] can be used to support either the reality of time or the Gödelian view on the ideal nature of time, depending on one's metaphysical orientation concerning the relationship between the possible and the actual.

Similarly, it follows from [3] that the limiting theorems of logic can either be used to argue for a materialistic view of mind, or to argue (as Gödel does) for the nonmaterialistic view that the mind transcends the physical brain.

Finally, it is considered whether the sum of Gödel's published philosophy provides a sort of optimistic neo-Kantian epistemology superimposed on a Platonic metaphysics.

[1] S. FEFERMAN ET AL., editors, ***K. Gödel, Collected works IV: correspondence A–G***, Oxford University Press, Oxford, 2003.

[2] K. GÖDEL, *What is Cantor's continuum hypothesis?*, P. Benacerraf and H. Putnam (editors), ***Philosophy of mathematics: selected readings***, 2nd edition, Cambridge University Press, Cambridge, UK, 1983.

[3] A. E. LYNGZEIDETSON AND M. K. SOLOMON, *Abstract complexity theory and the mind-machine problem*, ***The British Journal for the Philosophy of Science***, vol. 45 (1994), pp. 549–554.

[4] L. PARKER, *Faster-than-light inertial frames and tachyons*, ***Physical Review***, vol. 188 (1969), pp. 2287–2292.

[5] M. STEINER, ***Mathematical knowledge***, Cornell University Press, Ithaca, NY, 1975.

► ELISA VASQUEZ, *An application of Crofton's formula to o-minimal structures*.
Department of Mathematics, University of Wisconsin, 480 Lincoln Drive, Madison, WI 53706, USA.
E-mail: vasquez@math.wisc.edu.

Any definable, bounded set A of an o-minimal expansion of $(\mathbb{R}, <, 0, +, -, \cdot, 1)$ can be decomposed into finitely many definable sets A_i such that there is a constant K and a definable families of curves λ_i in each A_i with the property that any pair of points $x, y \in A_i$ can be joined by a curve γ in the family λ_i with $l(\gamma) \leq K|x - y|$.

► MICHAEL A. WARREN, *Predicative categories of classes*.
Department of Philosophy, Carnegie Mellon University, Pittsburgh, PA 15217, USA.
E-mail: mwarren@andrew.cmu.edu.

Joyal and Moerdijk [3] initiated the category theoretic study of set theory and provided a category theoretic model of **IZF**. Recently this research has been extended by Awodey *et al.* [2], who have demonstrated the importance of *categories of classes* for providing models of set theories. Roughly, a category of classes is a Heyting category endowed with a system of distinguished *small maps*, a system of *small powerobjects*, and a *universal object* U. Such categories arise naturally as models of a particular intuitionistic set theory (**bIST**). Interestingly, any elementary topos $\mathcal{E}$ may be completed to a category of classes $\mathbf{Idl}(\mathcal{E})$, the category of ideals of $\mathcal{E}$, and **bIST** is complete with respect to such models: for any formula φ, if $\mathbf{Idl}(\mathcal{E})$ satisfies φ, for every elementary topos $\mathcal{E}$, then φ is provable in **bIST**.

However, topoi (and **bIST**) are impredicative and so the question naturally arises whether similar results to the aforementioned are possible for predicative set theories such as **CZF** (cf. [1]). I show that there is an affirmative answer to this question. In particular, any locally cartesian closed Heyting pretopos $\mathcal{C}$ may be completed to a 'predicative category of classes' $\mathbf{Idl}(\mathcal{C})$. Regarding such categories $\mathcal{C}$ as 'predicative topoi' I arrive at an analogous completeness result for a predicative set theory **bCST**.

[1] Peter Aczel and Michael Rathjen, *Notes on constructive set theory*, Technical Report 40, Institut Mittag–Leffler (Royal Swedish Academy of Sciences), 2001, `http://www.ml.kva.se/preprints/archive2000-2001.php`.

[2] Steve Awodey, Carsten Butz, Alex Simpson, and Thomas Streicher, *Relating set theory and topos theory using categories of classes*, Technical Report CMU-PHIL-116, Carnegie Mellon University, June 2003, `www.andrew.cmu.edu/~awodey/`.

[3] A. Joyal and I. Moerdijk, ***Algebraic set theory***, Cambridge University Press, Cambridge, 1995.

► REBECCA WEBER, *Invariance and orbits in the lattice of* Π^0_1 *classes*.
Mathematics Department, University of Notre Dame, 255 Hurley, Notre Dame, IN 46556-5659, USA.
E-mail: `rweber@nd.edu`.

The lattice of Π^0_1 classes, $\mathcal{E}_\Pi$, has been well-studied, but little is known about the orbits of its elements and degree invariant classes. This is not the case with $\mathcal{E}$, the lattice of c.e. sets. We present a way to transfer orbits from $\mathcal{E}$ to invariant classes of $\mathcal{E}_\Pi$ via a definable quotient substructure of $\mathcal{E}_\Pi$ which is isomorphic to $\mathcal{E}^*$; that is, $\mathcal{E}$ modulo finite difference. Unfortunately the method of obtaining invariant classes does not also result in orbits, except possibly in cases where all elements of the orbit are of maximal Cantor-Bendixson rank. We will discuss our continuing work in this area.

Abstracts presented by title

► ADIB BEN JEBARA, *An idea about time in cosmology*.
Apt. F3 Residence Badr Manar 1, Tunis 2092, Tunisia.
E-mail: `adib.jebara@topnet.tn`.

We are postulating that time is not finite because infinitary set theory and cosmology have to meet. For we know since Galileo and Descartes that physics is written mathematically. The counting of time before the Big Bang and beyond the Big Crush (if any Big Crush) can be not well defined because of a new mathematical theory. The new theory is that only CC(2 through m) is true, which is countable axiom of choice for sets of n elements, n from 2 to m. See web page: `http://www.math.lsa.umich.edu/~ablass/dpcc.pdf`. That the axiom of choice is not true would explain the difficulty to deal with time . . . . Indeed, time can be counted with $n + n + n + \dots$ and be well defined or it can be counted with $(m+1)+(m+1)+(m+1)+\dots$ or with $1+2+3+4+\dots$ and thus be not well defined. Time can be a pair wise disjoint countable union of well ordered sets of n elements and in such a case be well ordered with an origin or it can be a pair wise disjoint countable union of sets of $m + 1$ elements or of increasing integers as numbers of elements and in such a case be not even countable so without origin.

As Mr. Andreas Blass pointed out, the assumptions here are that time is discrete and need not be well ordered.

Time is considered as a continuum but for studying long periods of time we can use the approximation of considering it discrete.

The end of time will be when time equal the empty set by equaling a countable Cartesian products of sets of $m + 1$ elements or of sets of increasing integers as numbers of elements.

This idea does not answer many questions but it answers the following: Is the counting of time always well defined? Is there an origin of time? Is there an end of time?

► JOHN CORCORAN, *Meanings of word: type-occurrence-token*.
Philosophy, University at Buffalo, Buffalo, NY 14260-4150, USA.
E-mail: corcoran@buffalo.edu.

The four-letter written-English expression 'word', which plays important roles in applications and expositions of logic and philosophy of logic, is ambiguous (multisense, or polysemic) in that it has multiple normal meanings (senses, or definitions). Several of its meanings are vague (imprecise, or indefinite) in that they admit of borderline (marginal, or fringe) cases. This paper juxtaposes, distinguishes, and analyzes several senses of 'word' focusing on a constellation of senses analogous to constellations of senses of other expression words such as 'expression', 'symbol', 'character', 'letter', 'term', 'phrase', 'formula', 'sentence', 'derivation', 'paragraph', and 'discourse'. Consider, e.g., the word 'letter'. In one sense there are exactly twenty-six *letters* (letter-types or ideal letters) in the English alphabet and there are exactly four *letters* in the word-type 'letter'. In another sense, there are exactly six *letters* (letter-repetitions or letter-occurrences) in the word-type 'letter'. In yet another sense, every new inscription (act of writing or printing) of 'letter' brings into existence six new *letters* (letter-tokens or ink-letters) and one new word that had not previously existed. The number of letter-occurrences (occurrences of a letter-type) in a given word-type is the same as the number of letter-tokens (tokens of a letter-type) in a single token of the given word. Many logicians fail to distinguish "token" from "occurrence" and a few actually confuse the two concepts. Epistemological and ontological problems concerning word-types, word-occurrences, and word-tokens are described in philosophically neutral terms. This paper presents a theoretical framework of concepts and principles concerning logicography, including use of English in logic. The framework is applied to analytical exposition and critical evaluation of classic passages in the works of philosophers and logicians including Boole, Peirce, Frege, Russell, Tarski, Church and Quine. This paper is intended as a philosophical sequel to Corcoran et al. *String Theory*, ***The Journal of Symbolic Logic***, vol. 39 (1974), pp. 625–637.

► LEONA F. FASS, *A logical approach to real system design*.
P.O. Box 2914, Carmel, CA 93921, USA.
E-mail: lff4@cornell.edu.

There has long been debate as to whether logic-based formal methods could be used to synthesize and verify systems and engineered hardware designs or whether correct designs could be established empirically. Our position is that it would be unlikely to find a complex practical system whose entire behavior could be completely, correctly formally specified and realized effectively. Thus for complex systems and devices an original design could only be an approximation of the behavioral ideal. At best we can establish correctness of these approximate behavioral models, dealing with erroneous or anomalous behaviors as they are observed and, perhaps, revising the approximations. Empirically detecting design defects and behavioral errors is, we believe, a crucial and inevitable phase of establishing correct design.

We describe how model-based design and model checking can combine formal methods and empirical techniques to improve specifications and designs, and to detect defects and flaws in devices and systems. Model-based design formally analyzes a potential behavioral domain to determine necessary components of a realization. Model checking may then formally, automatedly, attempt to verify that a model-based specification is fulfilled. Checkers may mimic potential system/device behavior, e.g., by descriptive formula or finite-state machine. They then compute "all reachable states", searching for results or paths to indicate that specified behavioral properties are satisfied. But in real system design, it is most often the case that these formal behavioral modeling techniques are useful for detecting defects, producing counter-examples, and finding design flaws.

We discuss our own experience utilizing these techniques and some important research of others, using formal methods for design and for empirical error detection. These include applications to factory process modeling, Navy aviation software design, NASA fault-detection systems and system security.

► GRIGORI MINTS AND ARIST KOJEVNIKOV, *Intuitionistic Frege systems are polynomially equivalent*.

Department of Philosophy, Stanford University, CA 94305-2155, USA.
E-mail: mints@csli.stanford.edu.

In [1] it is shown that any two classical Frege systems polynomially simulate each other. The same proof does not work for the intuitionistic Frege systems, since they can have non-derivable admissible rules. In Lemma 1 we polynomially simulate one admissible rule. Therefore any two intuitionistic Frege system polynomially simulate each other. We need the following two facts and use notation from [1], [2].

THEOREM 1. [2] The set of most general unifiers of a formula is finite.

PROPOSITION 1. [2] An inference rule A/B is admissible in Frege system $\mathfrak{F}$ iff every unifier for A is also a unifier for B.

LEMMA 1. *For any Frege system $\mathfrak{F}_1$ and its extension $\mathfrak{F}_2$ with admissible rule $R \cong C/D$ there is a function f and constant c such that for all formulas $A_1, \dots, A_n, B$ and derivations π, if $A_1, \dots, A_n \vdash^{\pi}_{\mathfrak{F}_2} B$, then $A_1, \dots, A_n \vdash^{f(\pi)}_{\mathfrak{F}_1} B$, and $\lambda(f(\pi)) \leqslant c\lambda(\pi), \tau(f(\pi)) \leqslant c\rho(\pi)$.*

PROOF. Assume $\{\Theta_1, \dots, \Theta_s\}$ is a finite (by Theorem 1) complete set of unifiers for the formula C. For each $i = 1, \dots, s$, let π_i be a derivation of $\Theta_i(D)$ in $\mathfrak{F}_1$ (it exists by the Proposition 1). We fix c_1 to be the number of lines in the longest derivation π_i $(i = 1, \dots, s)$ and c_2 to be the maximum of sizes of formulas in all the derivations π_i $(i = 1, \dots, s)$. Now suppose π is a derivation of B from $A_1, \dots, A_n$ in $\mathfrak{F}_2$ and $\sigma C/\sigma D$ an application of the rule R in π. By Theorem 1 there is j such that $\sigma = \tau \circ \Theta_j$. Replace the application of R with derivation $\tau\pi_i$. Let $f(\pi)$ be the result of replacing all applications of R in π. This is an $\mathfrak{F}_1$-derivation. Clearly $\lambda(f(\pi)) \leqslant c_1\lambda(\pi)$. Finally, note that $\tau(f(\pi)) \leqslant c_2\rho(\pi)$. ⊣

[1] STEPHEN A. COOK AND ROBERT A. RECKHOW, *The relative efficiency of propositional proof systems*, ***The Journal of Symbolic Logic***, vol. 44 (1979), no. 1, pp. 36–50.

[2] SILVIO GHILARDI, *Unification in intuitionistic logic*, ***The Journal of Symbolic Logic***, vol. 64 (1999), no. 2, pp. 859–880.

► XUNWEI ZHOU, *Inductive composition v. decomposition are better than induction v. deduction*.

5 Beixiange Street, Beijing, China.
E-mail: zhouxunwei@263.net.

The author has invented two new methodologies: inductive composition and decomposition which can be depicted by truth tables. Take $\overset{-1}{\leqslant}$ (mutually inverse implication) as an example, its truth table of inductive composition is shown in Table 1, its truth tables of decomposition are shown in Tables 2 and 3.

Table 1

A	B	$A \overset{-1}{\leqslant} B$
F	F	T
F	T	F/T
T	F	F
T	T	T

Table 2

$A \overset{-1}{\leqslant} B$	A	B
F	F	F/T
F	T	F/T
T	F	F/T
T	T	T

Table 3

$A \overset{-1}{\leqslant} B$	B	A
F	F	F/T
F	T	F/T
T	F	F
T	T	F/T

In Tables 1 through 3, A and B are mutually inverse special propositions, $A \overset{-1}{\leqslant} B$ is a mutually inverse general proposition.

Table 1 is from the special to the general, Tables 2 and 3 are from the general to the special. Table 1 is mutually inverse with Tables 2 and 3. F/T in Table 1 means "needn't determine". F/T in Tables 2 and 3 mean "unable to determine". The aim of Table 1 is to establish $A \overset{-1}{\leqslant} B$. The aims of Tables 2 and 3 are to employ the established $A \overset{-1}{\leqslant} B$ to make hypothetical inference. Table 2 depicts modus ponens, Table 3 modus tollens. Inductive composition and decomposition are defined by truth tables, more stringent than the definitions of induction and deduction. Induction was formerly defined as from the particular to the general, deduction as from the general to the particular. But, what is the particular, what is the general cannot be defined. Later, induction is defined as that the conclusion surpasses the premise, deduction as that the conclusion doesn't surpass the premise. But under this definition, complete inductive inference, a pure induction, is classified as deduction. Therefore, the definitions of inductive composition and decomposition are better than those of induction and deduction.