Logic and Algorithms

16 January to 7 July 2006

Report from the Organisers:
A Dawar (Cambridge) and MY Vardi (Rice)

S Wilkinson

A Dawar and MY Vardi

Scientific Background and Themes

Two central concerns dominate the field of theoretical computer science: (i) how to ensure and verify the correctness of computing systems; and (ii) how to measure the resources required for computations and ensure their efficiency. These concerns have led to the development of fields of study in formal methods and semantics on the one hand, and in algorithmics and computational complexity on the other. The two fields have interacted little with each other, partly because of the divergent mathematical techniques they have employed. While semantics is based in large part on logic, complexity theory has relied mainly on combinatorial methods. This division runs deep, as can be seen, for instance, in the two volumes of the *Handbook of Theoretical Computer Science* published in the early 1990s, where Volume A deals with algorithms and complexity, while Volume B covers formal methods and semantics.

There are, however, areas of computer science that straddle the divide. The stated aim of this programme was to focus attention on areas of research that bridge the gap between the two broad divisions. The specific areas chosen for this focus were Computer-Aided Verification, Algorithmic Model Theory, Proof Complexity, Constraint Satisfaction and Games. These cross-cut the dichotomy between Volume A and Volume B methods in interesting ways. For instance, one important concern in finite model theory has been to bring logical, particularly model theoretic, methods to bear on the study of the complexity of computation. Similarly, work in computer-aided verification through model-checking has done much to make combinatorial, rather than just deductive, methods available for the verification of program properties. Proof complexity seeks to analyse the complexity of logical deduction and relate this to the structural properties of computational complexity classes. In constraint satisfaction, methods inspired by logic have found application in the study of the complexity of an important class of combinatorial problems.

Furthermore, the study of combinatorial games has emerged as an important field of research in its own right. The range and depth of mathematical methods that are deployed in these areas has also greatly increased over recent years.

Computer-Aided Verification

Computer-aided verification studies algorithms and structures for verifying properties of computing systems. More precisely, it aims to develop methods for verifying that a mathematical model of a system satisfies a formal specification. There are two distinct paradigms of verification. One, of *proof-based* methods, is based on attributing the design with assertions in a formal specification language and constructing a proof that relates these assertions. The other, of *state-exploration* or *model-checking* methods, depends on navigating through the mathematical model of the design.

State-exploration methods are restricted to finite-state models. Circuits and a large number of communication and synchronization protocols have, in essence, a finite state space, and many infinite-state designs can be abstracted to finite-state ones.

Research in computer-aided verification draws upon logic, especially the study of modal and temporal logics often used in formal specifications, as well as combinatorics. Moreover, the study of the expressive power of such logics, the complexity of algorithms for exploring the state space and of automating the verification process have drawn on techniques from areas of mathematics including graph theory, automata theory, complexity theory, Boolean functions and algebras, Ramsey theory and linear programming. Significant work has focussed on methods based on alternating automata, which are closely related to the study of combinatorial games.

Algorithmic Model Theory

The model theory of finitely presented structures has been a meeting point for research in computer science, combinatorics, and mathematical logic. The finite presentation allows one to consider algorithmic issues in relation to such structures, which leads us to call this area *algorithmic model theory*. Results and techniques from this theory have found interesting applications to several other areas, including database theory, complexity theory and verification. The theory is concerned with the expressive power of logical languages on finitely presented structures. Since first-order logic has rather weak expressive power when restricted to such models, a variety of extensions have been studied in the area, including second and higher-order logics, logics with fixed-point operators, temporal logics, infinitary logics and logics with cardinality and other generalised quantifiers. The relation with complexity theory comes from the fact that the expressive power of many logics on finite structures can be exactly characterised by natural complexity classes. Moreover, the methods developed within finite model theory for analysing the expressive power of logics, particularly centred on combinatorial games, have found application in other areas such as studying database query languages and the power and complexity of specification languages, and these methods are now being extended beyond finite structures to infinite, finitely presented structures.

Proof Complexity

Two related notions of *proof complexity* currently motivate research at the interface between computer science and logic. One notion centres on the length of a proof, and the other on the complexity of the inference steps within the proof. It is well known that NP = co-NP if, and only if, all propositional tautologies have short proofs. But the connection between proof length and complexity theory goes much deeper. Some of the most powerful methods of proving complexity lower bounds, those based on circuits, are closely tied to proof length in restricted systems, and advances on one front often lead quickly to progress on the other. By restricting the complexity of inference steps within a proof, one obtains a fragment of Peano Arithmetic called Bounded Arithmetic, which defines exactly the predicates in the polynomial hierarchy. It has been shown that if certain theories of bounded arithmetic can prove lower bounds in complexity theory, then corresponding cryptographic systems cannot be secure. Methods for proving lower bounds on proof complexity have drawn on sophisticated methods from algebra, combinatorics and logic.

Constraint Satisfaction

Since the pioneering work of Montanari in 1974, researchers in artificial intelligence have investigated a class of combinatorial problems that became known as *constraint-satisfaction problems*. The input to such a problem consists of a set of variables, a set of possible values for the variables, and a set of constraints between the variables; the question is to determine whether there is an assignment of values to the variables that satisfies the given constraints. Many problems that arise in different areas can be modelled as constraint-satisfaction problems in a natural way: these areas include Boolean satisfiability, temporal reasoning, belief maintenance, machine vision, and scheduling. In its full generality, constraint satisfaction is an NP-complete problem. It generalises well-studied problems such as graph colouring and graph homomorphism, where a classification of tractable cases has long been sought. An algebraic way of formulating the constraint satisfaction problem is: given two finite relational structures A and B, is there a

homomorphism $h : A \to B$? The grand challenge in the area is to obtain general classes of pairs (A, B) for which the problem has polynomial time solutions. Research in the area has drawn on a rich variety of techniques from algebra, logic and graph theory.

Games

The study of games is a thread that runs through all of the areas outlined above. Games have been used as a tool for analysing logics and systems and have also come to be the object of study in their own right. Here we are talking of two-person games on (finite or infinite) graphs with (finite or infinite) plays. Our focus is on their extensive form, rather than on the strategic form typically used in economics or in optimisation. Besides their role as a tool, as discussed above, games capture in a natural way the aspect of interaction between open systems and their environments. This approach has recently led to new algorithmic directions in verification. An emerging theory combines games with automata and logic into a powerful tool for the analysis of such systems. Some of the fundamental questions concern the algorithmic complexity of determining a winner or constructing a winning strategy, given a game and a winning condition. The methods have much in common with all the areas discussed above.

Workshops and Seminars

Six workshops, each of one week's duration, were held over the course of the programme. Four of these were at the Isaac Newton Institute, while one was a satellite workshop in Durham and one was held in Oxford. In addition, a regular seminar series was held at the Institute with between two and five seminars per week. All participants were invited to present a talk in the seminar series. In addition, several short courses were offered, including five lectures on *Game Semantics and its Applications* by Luke Ong, four lectures on *Basic Proof Complexity* by Jan Krajíček, four lectures on *Graph Searching Games and Graph Decompositions* by Stephan Kreutzer, three lectures on *Post's Lattice with Applications to Complexity Theory* by Heribert Vollmer and three lectures on *Analysis of Recursive Markov Chains, Recursive Markov Decision Processes and Recursive Stochastic Games* by Kousha Etessami. The Rothschild Visiting Professor, Stephen Cook, delivered a lecture of general interest on *Computational Complexity and Proofs of Combinatorial Principles*.

The six workshops were designed around topics that combined more than one of the themes identified as key areas of the programme.

Finite and Algorithmic Model Theory

Satellite Meeting at the University of Durham, 9–13 January 2006

Organiser: I Stewart

The programme kicked off with a satellite meeting at Durham that consisted entirely of tutorial presentations that touched on most of the themes of the programme. The goal was to explore both emerging and potential connections and applications between the two areas of finite and infinite model theory. In this respect, the workshop was extremely successful, involving around 60 participants, not including those local to Durham. The participants came from a mix of mathematics and computer science backgrounds and a large number were from overseas. Many are leading figures in the field.

The workshop consisted of 4 three- to four-hour tutorials and 6 two-hour and one-hour research expositions. This format was designed to introduce researchers and graduate students to those topics that are of fundamental interest and importance, to survey current research, and to discuss major unsolved problems and directions for future research. Four-hour tutorials were given by Richard Elwes, Bart Kuijpers, Dugald Macpherson, Martin Otto, Jan van den Bussche, Igor Walukiewicz and Thomas Wilke. Two-hour talks were given by Marko Djordjevic, Kousha Etessami, Erich Grädel, Stephan Kreutzer, Sasha Rubin and Nicole Schweikardt. One-hour talks were given by Albert Atserias and Manuel Bodirsky.

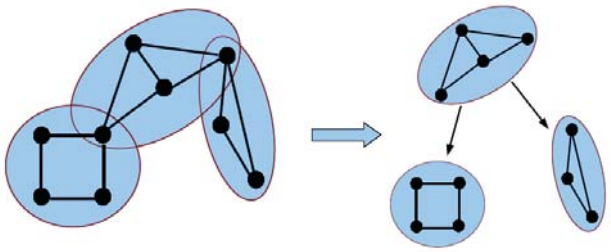
Logic and Databases

Workshop, 27 February–3 March 2006

Organisers: A Dawar and M Grohe

Logic and databases have been intimately linked since the rise of relational database systems in the 1970s. Relational databases can be modelled by finite relational structures, and first-order logic lies at the core of standard database query languages such as the Structured Query Language, SQL. As

S Kreutzer



The tree-width of a graph measures its similarity to a tree

another example, closer to current research, XML documents can be modelled by labelled unranked trees, and XML query languages as logics on trees.

The workshop focussed on recent research on logical aspects of the theory of database systems. Invited talks and tutorials presented a broad survey of the state of the art in the field. The speakers were Christoph Koch, Phokion Kolaitis, Leonid Libkin, Frank Neven, Nicole Schweikardt, Luc Segoufin, Dan Suciu and Victor Vianu. In addition there were 14 contributed talks covering a wide area of current research in database theory. In all, 85 participants took part in the workshop.

Mathematics of Constraint Satisfaction: Algebra, Logic and Graph Theory

Satellite Meeting at the University of Oxford, 20–24 March 2006

Organisers: A Krokhin and P Jeavons

The constraint satisfaction problem (CSP) provides a general framework in which it is possible to express, in a natural way, a wide variety of problems encountered in artificial intelligence, combinatorial optimisation, logic, algebra, graph theory and database theory. There are strong links between the study of CSPs and many areas of mathematics. One of the most striking features of current CSP research is that, despite computational aspects being its primary motivation, it influences (and is influenced by) many branches of mathematics. The theoretical side of CSP research has been dominated by the analysis of algorithms and computational complexity for constraint problems, and a number of deep mathematical approaches to this involving in particular algebra, logic and combinatorics have been suggested in the literature.

The workshop brought together, for the first time, all the leading specialists on various mathematical approaches to constraint satisfaction as well as many researchers from different areas of mathematics and computer science with an interest in this exciting interdisciplinary area. The programme included three substantial tutorials outlining the basics of the algebraic, logical and combinatorial approaches to the CSP, given by Peter Jeavons, Phokion Kolaitis and Pavol Hell respectively. These tutorials were designed to ensure that all participants were equipped with the necessary preliminary knowledge of all of the fundamental mathematical approaches. The main part of the programme consisted of 11 one-hour plenary lectures given by world-leading specialists in the above topics. This ensured that all participants gained a complete state-of-the-art picture of the research area. The plenary lectures were given by Andrei Bulatov, Hubie Chen and Peter Jonsson (algebra), Albert Atserias and Iain Stewart (logic), Georg Gottlob and Jaroslav Nešetřil (combinatorics), Victor Dalmau and Benoit Larose (combinations of the three approaches), and Nadia Creignou (Boolean CSP) and Johan Hastad (inapproximability of CSP). In addition to these plenary talks, there were 11 invited 30-minute talks which covered a broad range of other topics, including the use of mathematics in more applied CSP research. The workshop could be called a "community-creating event" because many leading researchers in different aspects of the area met for the first time and discussed and compared different approaches to a significant extent. As a result, researchers from different areas are more aware of the mathematical insights and challenges present in the theory of constraint satisfaction. In all, 81 participants took part.

New Directions in Proof Complexity

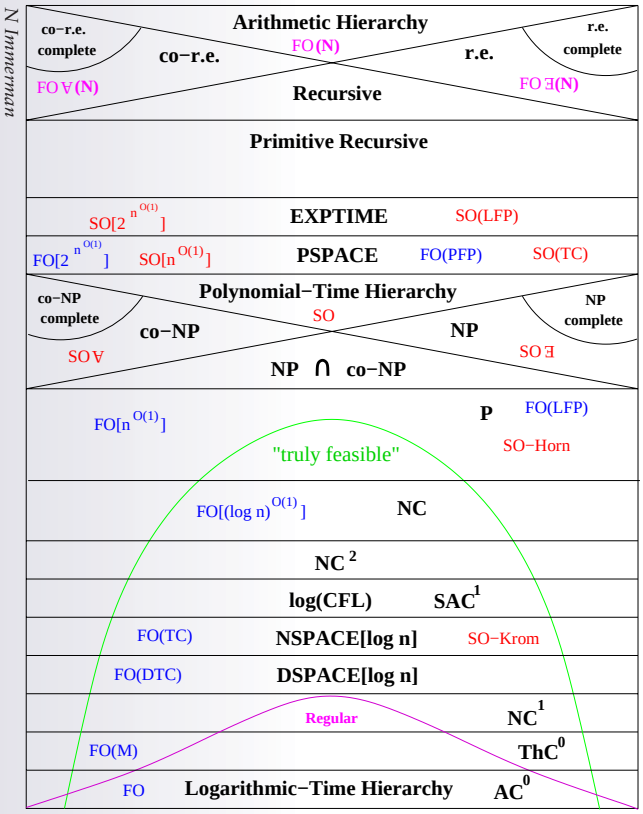
Workshop, 10–13 April 2006

Organisers: J Krajíček and SR Buss

Proof complexity is an area of mathematics centred around the problem of whether the complexity class NP is closed under complementation. With a suitable general definition of a propositional proof system this becomes a lengths-of-proofs question: Is there a propositional proof system in which every tautology admits a proof whose length is bounded above by a polynomial in the length of the tautology? The ultimate goal of proof complexity is to

show that there is no such proof system; that is, to demonstrate superpolynomial lower bounds for all proof systems.

The purpose of the workshop was to expose, through invited and contributed lectures, current developments in proof complexity as well as new ideas and directions of research pursued most recently. The ambitious dictum in the title, "new directions", was actually fully vindicated. In particular, quite a few of the speakers were young researchers with new results and new approaches to proof complexity. Several speakers (Pudlak, Thapen) reported on new approaches to an old problem of conservativity relations among fragments of bounded arithmetic, or described (Jerabek, Nguyen, Pollett, Soltys) expansions of the theory to include various combinatorial constructions. Vardi reported on new types of proof systems based on constraint propagation and Beckmann sketched basic ideas of uniform proof complexity, while Dantchev explained his ideas about parameterised proof complexity. Riis presented new ideas on a topic he calls sporadic propositional proofs and Naumov outlined the new concept of meta-complexity (of proofs). Tzameret presented his interesting work with Raz on algebraic systems which generalise traditional proof systems. There were also talks reporting new results for traditional proof systems like resolution (Bonet, Galesi, Nordstrom) or Lovasz–Schrijver system (Alekhnovich, Segerlind), as well as lectures discussing basic concepts and problems (Cook, Impagliazzo, Pitassi). In all, 66 people attended the workshop.



The world of descriptive and computational complexity, from Neil Immerman's talk at the 'Games and Verification' workshop

Constraints and Verification

Workshop, 8–12 May 2006

Organisers: M Vardi and A Podelski

In recent years there has been an increasing interest in the application of constraint-programming and constraint-solving technology to the verification of hardware and software systems. Constraint solvers for Boolean (SAT) and arithmetic domains (Presburger, polyhedra, linear constraints) are widely used as subprocedures of various model checkers. Constraint solving is also used for static analysis of programs with numerical data variables and for concurrent systems. Constraints are also used extensively in automated test generation. The aim of this workshop, attended by 95 people in all, was to bring together researchers working in constraints and verification and to investigate the theoretical foundations, new applications and future developments in this area.

Keynote talks were given by Ed Clarke (Carnegie Mellon), Patrick Cousot (ENS), Enrico Giunchiglia (Genoa), Ziyad Hanna (Intel), Marta Kwiatkowska (Birmingham), Zohar Manna (Stanford), Ken McMillan (Cadence), Yehuda Naveh (IBM), Jean-François Puget (ILOG) and Pierre Wolper (Liege).

Games and Verification

Workshop, 3–7 July 2006

Organisers: L Ong, E Gradel, C-H Long and CP Stirling

The aim of this workshop was to bring together researchers who use games in computer science and neighbouring disciplines. The workshop had some 110 participants, a good number of them doctoral students and postdoctoral researchers. The workshop was also the final annual meeting of "Games and Automata for Synthesis and

Validation", a research training network funded by the European Commission under the Fifth Framework Programme, linking research teams from Aachen University, University of Bordeaux I, University of Edinburgh, University of Paris 7, Rice University and Warsaw University.

The workshop had a strong training component. It featured 6 tutorials (of 90 minutes each) given by such prominent researchers in the field as Rajeev Alur (*Nested words and trees*), Johan van Bentham (*Dynamic-epistemic logic of games*), Didier Caucal (*Deterministic grammars*), Georg Gottlob (*Hypertree decompositions*), Dov Monderer (*Mechanism design*) and Moshe Vardi (*Games as an algorithmic construct*). The expositions, all beautifully presented, surveyed topics of intense current interests. In addition, 21 leading researchers gave lectures (of 30 minutes) on their recent work; there were also short talks (of 15 minutes) by 9 doctoral students. By general consensus, the workshop was a success. Two pleasing features are worth mentioning: firstly, the meeting attracted an unusually high concentration of key thinkers in related fields, and secondly, the quality of the talks was extremely high, as researchers presented their best recent work.

Outcomes and Achievements

The programme generated a great deal of research activity and, at most times during its course, the Institute was abuzz with intense discussions. It is expected that, over the coming months and years, a number of publications will emerge from activity initiated or carried out during the programme. However, the greatest benefits of the programme may be the less tangible ones of "community creation". The programme brought together researchers from several distinct research communities in theoretical computer science and mathematics, and helped expose the common underlying elements of their problems and methods. In the process, it helped create bridges and collaborations between these communities and to give shape to Logic and Algorithms as a subject area. The impact of this may be less measurable than concrete publications, but will be felt by the research community for years to come.

S Wilkinson

Participants at the workshop on 'New Directions in Proof Complexity'

More concretely, among the scientific and mathematical achievements the following might be especially mentioned: a new combinatorial characterisation of NP (Nešetřil and Kun); the best currently known algorithms for discounted payoff games (Andersson and Vorobyov); advances in our understanding of preservation properties and relationship to definability of constraint satisfaction problems (Atserias, Dawar, Kreutzer and Weinstein); extensions of our understanding of tractability of CSPs in terms of algebra (Bulatov, Chen, Jeavons, Krokhin and Valeriote), games (Atserias, Bulatov and Dalmau) and dualities (Dalmau, Krokhin, Szeider); synthesis algorithms for temporal specifications (Kupferman, Piterman and Vardi); a combinatorial characterisation of search problems definable in low fragments of bounded arithmetic (Krajíček, Skelley and Thapen); results on the topological complexity of recognisable tree languages (Niwinski); advances on the computational complexity of the membership problem for functional clones (Vollmer); a study of formula size as a measure of complexity (Hella and Väänänen); and a new perspective on Gödel's Completeness Theorem (Väänänen and Vardi).

Publications

There are plans in place to produce a volume of expository articles based on the workshop on *Finite and Algorithmic Model Theory* held at Durham.It is anticipated that this volume will become a standard reference work describing the current state of the field. In addition, a number of papers based on research carried out during the programme have been written, some of which have appeared in the Newton Institute preprint series, and more are expected to follow.