Report from Dagstuhl Seminar 15401

Circuits, Logic and Games

Edited by

Mikołaj Bojańczyk[1], Meena Mahajan[2], Thomas Schwentick[3], and Heribert Vollmer[4]

1 **University of Warsaw, PL,** bojan@mimuw.edu.pl
2 **The Institute of Mathematical Sciences, IN,** meena@imsc.res.in
3 **TU Dortmund, DE,** thomas.schwentick@udo.edu
4 **Leibniz Universität Hannover, DE,** vollmer@thi.uni-hannover.de

Abstract

Over the years, there has been a lot of interplay between circuit complexity and logic. There are tight connections between small-depth circuit classes and fragments and extensions of first-order logic, and ideas from games and finite model theory have provided powerful lower bound techniques for circuits.

In recent years, there has been an impressive and sustained growth of interest and activity in the intersection of finite model theory and Boolean circuit complexity. The central aim of the seminar was to bring together researchers from these two areas to further strengthen the mutual fertilisation. The seminar focussed on the following specific topics:

- The algebraic approach to circuit complexity with its applications to finite model theory
- The logic-circuit connection, with a particular emphasis on circuit lower bounds that trigger results in finite model theory like separations between logics
- New connections between uniformity conditions on circuit families and logical predicates
- Structural complexity and circuit lower bounds inherently using methods from logic and algebra
- Proof systems with low circuit complexity
- Dynamic complexity: understanding the dynamic expressive power of small depth circuit classes

The seminar had 43 participants from 11 countries and was very successful with respect to the exchange of recent results, ideas and methodological approaches.

Seminar September 27 to October 2, 2015 – http://www.dagstuhl.de/15401

1998 ACM Subject Classification F.1.1 Models of Computation, F.1.3 Complexity Measures and Classes, F.2.2 Non-Numerical Algorithms and Problems, F.4.1 Mathematical Logic

Keywords and phrases computational complexity theory, finite model theory, Boolean circuits, regular languages, finite monoids, Ehrenfeucht-Fraïssé-games

Digital Object Identifier 10.4230/DagRep.5.9.105

Edited in cooperation with Nils Vortmeier

Circuits, Logic and Games, *Dagstuhl Reports*, Vol. 5, Issue 9, pp. 105–124
Editors: Mikołaj Bojańczyk, Meena Mahajan, Thomas Schwentick, and Heribert Vollmer
Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1 Executive Summary

Mikołaj Bojańczyk
Meena Mahajan
Thomas Schwentick
Heribert Vollmer

This report documents the programme and outcomes of Dagstuhl Seminar 15401 "Circuits, Logic and Games". This seminar was the third in this series, the earlier two being Dagstuhl Seminars 06451 in November 2006 and 10061 in February 2010.

Goals of the Seminar

Over the years, there has been a lot of interplay between circuit complexity and logic. There are tight connections between small-depth circuit classes and fragments and extensions of first-order logic, and ideas from games and finite model theory have provided powerful lower bound techniques for circuits.

In recent years, there has been an impressive and sustained growth of interest and activity in the intersection of finite model theory and Boolean circuit complexity. The central aim of the seminar was to bring together researchers from these two areas to further strengthen the mutual fertilisation. Given the ubiquitousness of algebraic techniques in circuit complexity, the seminar also included arithmetic circuit complexity in its ambit.

The seminar focussed on the following specific topics:

- The algebraic approach to circuit complexity with its applications to finite model theory
- The logic-circuit connection, with a particular emphasis on circuit lower bounds that trigger results in finite model theory like separations between logics
- New connections between uniformity conditions on circuit families and logical predicates
- Structural complexity and circuit lower bounds inherently using methods from logic and algebra
- Proof systems with low circuit complexity
- Dynamic complexity: understanding the dynamic expressive power of small depth circuit classes

Organization of the Seminar and Activities

The seminar had the participation of 43 members from 11 countries.

The organisers attempted to create a schedule with a judicious mix of survey talks, focussed talks, and free time for unstructured discussions. Participants were invited to present their work and to communicate state-of-the-art advances. Since the participants came from diverse communities, the organisers invited some of them to give long survey-style talks in specific sub-areas. There were five such talks, listed below.

1. Olaf Beyersdorff. Lower bounds: from circuits to QBF proof systems.
   This talk surveyed the relatively new area of proof systems for establishing falseness of fully quantified Boolean formulas. It demonstrated techniques by which lower bounds in ciruit complexity can be tranferred to lower bounds on the sizes of such proofs.

2. Thomas Colcombet. Combinatorial Expressions and Lower Bounds.
   This talk described an elegant formalism, combinatorial expressions, that captures bounded depth circuits manipulating infinite data in specified restrictive ways, and showed how one may obtain indefinability results in this model.
3. Anuj Dawar. Lower Bounds for Symmetric Circuits.
   This talk described the recently formalised circuit model of symmetric circuits, its connections with logical definability, and a lower bound technique using games.
4. Martin Grohe. Color Refinement: A Simple Partitioning Algorithm with Applications From Graph Isomorphism Testing to Machine Learning.
   This talk described exciting connections between higher-dimensional generalisations of the extremely simple colour refinement aglorithm and a linear programming approach to testing isomorphism.
5. Nutan Limaye. Arithmetic Circuit Lower Bounds.
   This talk surveyed the recent explosion of results concerning size lower bounds in restricted models of algebraic computation, using techniques which seem essentially combinatorial in nature.

In addition, 20 other participants gave short talks on some of their recent work relevant to the seminar theme. These talks covered results in two-variable first-order logic; dynamic complexity; graph colouring; database theory; circuit lower bounds; logics on words; and semigroup techniques. There was also a short session on Thursday devoted to discussing interesting open problems.

Concluding Remarks and Future Plans

The organizers regard the seminar as being quite successful. Most participants felt that they learnt new things from other areas, and were hopeful of using such ideas to make progress in their own research areas.

One aspect noted by the organizers was that a lot of the work discussed at the seminar used techniques from algebra. In fact, there was even a suggestion that if there is a future seminar in this series, it could be called “Circuits, Logic, and Algebra” instead of “Circuits, Logic, and Games”.

The organizers are grateful to the Scientific Directorate of the Center for its support of this seminar.

2 Table of Contents

Executive Summary
Mikołaj Bojańczyk, Meena Mahajan, Thomas Schwentick, and Heribert Vollmer . . 106

Overview of Talks

Crane Beach conjecture and modulo counting quantifiers
Sreejith Ajithkumar 110

Limitations of Algebraic Approaches to Graph Isomorphism Testing
Christoph Berkholz 110

Lower bounds: from circuits to QBF proof systems
Olaf Beyersdorff 110

Transductions: From circuits to continuity
Michaël Cadilhac 111

Combinatorial Expressions and Lower Bounds
Thomas Colcombet 112

Model checking distributed algorithms against propositional dynamic logic with data
Aiswarya Cyriac 112

Lower Bounds for Symmetric Circuits
Anuj Dawar 113

Canonizing Graphs of Bounded Tree Width in Logspace
Michael Elberfeld 113

Colour Refinement: A Simple Partitioning Algorithm with Applications From Graph Isomorphism Testing to Machine Learning
Martin Grohe 113

Bipartite Matching is in Quasi-NC
Rohit Gurjar 114

Backdoors into Two Occurrences
Jan Johannsen 114

Quantifying over tuples with Algebra – the multidimensional blockproduct
Klaus-Jörn Lange 115

Arithmetic circuit complexity and lower bounds
Nutan Limaye 115

Unary temporal and two-variable FO logic with threshold
Kamal Lodaya 115

QBF Resolution: How important is width?
Meena Mahajan 116

A Strongly Exponential Separation of DNNFs from CNF Formulas
Stefan Mengel 116

Dynamic Complexity of Reachability and Related Problems
Anish Mukherjee 117

Word transducers: from 2-way to 1-way
Anca Muscholl 117

Finite-Degree Predicates and Two-Variable First-Order Logic
Charles Paperman 118

AC^0 and first order logic, a new approach based on ultrafilters on words
Jean-Eric Pin 118

An exponential lower bound for the sum of products of read once formulas
B. V. Raghavendra Rao 118

On the generalised colouring numbers of graphs that exclude a fixed minor
Sebastian Siebertz 119

Converse elimination in the algebra of binary relations
Dimitri Surinx 120

Static Analysis for Logic-Based Dynamic Programs
Nils Vortmeier 120

Small Dynamic Complexity Classes
Thomas Zeume 121

Open Problems

Perfect matchings for grid graphs and AC^0
Kristoffer Arnsfelt Hansen 121

AC^0 on trees
Mikołaj Bojańczyk 122

Prefix diversity
Michaël Cadilhac 122

Proof systems computed by NC^0 circuit families.
Karteek Sreenivasaiah 123

Participants 124

3 Overview of Talks

3.1 Crane Beach conjecture and modulo counting quantifiers

Sreejith Ajithkumar (University of Paris VII, FR)

Joint work of Krebs, Andreas; Sreejith, A. V.
Main reference Andreas Krebs, A. V. Sreejith: Non-definability of Languages by Generalized First-order Formulas over (N, +). LICS 2012: 451-460
URL http://dx.doi.org/10.1109/LICS.2012.55

We show that the crane beach conjecture holds for first order logic with modulo counting quantifiers (or group quantifiers) in the presence of less than and addition relation.

3.2 Limitations of Algebraic Approaches to Graph Isomorphism Testing

Christoph Berkholz (HU Berlin, DE)

Joint work of Berkholz, Christoph; Grohe, Martin
Main reference C. Berkholz, M. Grohe, "Limitations of Algebraic Approaches to Graph Isomorphism Testing," in Proc. of the 42nd Int'l Colloquium on Automata, Languages and Programming (ICALP'15), pp. 451–460, IEEE, 2015.
URL http://dx.doi.org/10.1007/978-3-662-47672-7_13

We investigate the power of graph isomorphism algorithms based on algebraic reasoning techniques like Gröbner basis computation. The idea of these algorithms is to encode two graphs into a system of multivariate polynomial equations that is satisfiable if and only if the graphs are isomorphic, and then to (try to) decide satisfiability of the system using, for example, the Gröbner basis algorithm. In some cases this can be done in polynomial time, in particular, if the equations admit a bounded degree refutation in an algebraic proof systems such as Nullstellensatz or polynomial calculus.

We show that the strength of this algebraic approach is closely related to the Weisfeiler-Lehman algorithm or, equivalently, to the equivalence problem for the k-variable fragment of first-order counting logic. This shows that logical methods can be used to understand the strength of algebraic approaches for graph isomorphism testing, complementing previous connections of logic and linear programming approaches.

3.3 Lower bounds: from circuits to QBF proof systems

Olaf Beyersdorff (University of Leeds, GB)

Joint work of Beyersdorff, Olaf; Bonacina, Ilario; Chew, Leroy
Main reference O. Beyersdorff, I. Bonacina, L. Chew, "Lower bounds: from circuits to QBF proof systems," in Proc. of the 7th ACM Conf. on Innovations in Theoretical Computer Science (ITCS'16)), pp. 249–260, ACM, 2016; pre-print available ECCC TR15-133, 2015.
URL http://dx.doi.org/10.1145/2840728.2840740
URL http://eccc.hpi-web.de/report/2015/133

The main aim in proof complexity is to understand the complexity of theorem proving. Arguably, what is even more important is to establish techniques for lower bounds, and the recent history of computational complexity speaks volumes on how difficult it is to develop general lower bound techniques. Understanding the size of proofs is important for at least two reasons. The first is its tight relation to the separation of complexity classes: NP vs. coNP for propositional proofs, and NP vs. PSPACE in the case of proof systems for quantified boolean formulas (QBF). The second reason to study lower bounds for proofs is the analysis of SAT and QBF solvers: powerful algorithms that efficiently solve the classically hard problems of SAT and QBF for large classes of practically relevant formulas.

In this talk we give an overview of the relatively young field of QBF proof complexity. We explain the main resolution-based proof systems for QBF, modelling CDCL and expansion-based solving. In the main part of the talk we will give an overview of current lower bound techniques (and their limitations) for QBF systems. In particular, we exhibit a new and elegant proof technique for showing lower bounds in QBF proof systems based on strategy extraction. This technique provides a direct transfer of circuit lower bounds to lengths of proofs lower bounds.

By using the full spectrum of state-of-the-art circuit lower bounds, our new lower bound method leads to very strong lower bounds for QBF Frege systems:

1. exponential lower bounds and separations for $\mathrm{AC}^0[p]$-Frege+$\forall$red for all primes p;
2. an exponential separation of $\mathrm{AC}^0[p]$-Frege+$\forall$red from TC^0-Frege+$\forall$red;
3. an exponential separation of the hierarchy of constant-depth systems AC^0_d-Frege+$\forall$red by formulas of depth independent of d.

In the propositional case, all these results correspond to major open problems.

3.4 Transductions: From circuits to continuity

Michaël Cadilhac (Universität Tübingen, DE)

Joint work of Cadilhac, Michaël; Krebs, Andreas; Ludwig, Michael; Paperman, Charles
Main reference M. Cadilhac, A. Krebs, M. Ludwig, C. Paperman, "A Circuit Complexity Approach to Transductions," in Proc. of the 40th Int'l Symp. on Mathematical Foundations of Computer Science (MFCS'15), LNCS, Vol. 9234, pp. 141–153, Springer, 2015.
URL http://dx.doi.org/10.1007/978-3-662-48057-1_11

Low circuit complexity classes and regular languages exhibit very tight interactions that shade light on their respective expressiveness. We propose to study these interactions at a functional level, by investigating the deterministic rational transductions computable by constant-depth, polysize circuits. To this end, a circuit framework of independent interest that allows variable output length is introduced. Relying on it, there is a general characterization of the set of transductions realizable by circuits. It is then decidable whether a transduction is definable in AC^0 and, assuming a well-established conjecture, the same for ACC^0. This study unveils a crucial property of the functions at hand: the preservation under inverse image of classes of languages. More precisely, with C a class of languages, a function f is C-continuous if every language of C is mapped by f^{-1} to another language in C. In this talk, an emphasis is put on the pervasiveness of this notion, and the key problems that arise, in particular deciding C-continuity of deterministic transductions.

3.5 Combinatorial Expressions and Lower Bounds

Thomas Colcombet (CNRS / University Paris-Diderot, FR)

Joint work of Colcombet, Thomas; Manuel, Amaldev

In this talk, I present a new paradigm, combinatorial expressions, for computing functions expressing properties over an infinite domain. The main result is a generic technique, for showing indefinability of certain functions by the expressions. It is based the Hales-Jewett theorem, from Ramsey theory. I also show how this formalims is a conveninent tool for separating logics over data words.

These results are based on a joint works with Amaldev Manuel, and received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 259454.

References

1 Thomas Colcombet and Amaldev Manuel. *Fragments of Fixpoint Logic on Data Words*. FSTTCS 2015, pp. 98–111, http://dx.doi.org/10.4230/LIPIcs.FSTTCS.2015.98.
2 Thomas Colcombet and Amaldev Manuel. *Combinatorial Expressions and Lower Bounds*. STACS 2015, pp. 249–261, http://dx.doi.org/10.4230/LIPIcs.STACS.2015.249.

3.6 Model checking distributed algorithms against propositional dynamic logic with data

Aiswarya Cyriac (Uppsala University, SE)

Joint work of Aiswarya, C.; Bollig, Benedikt; Gastin, Paul
Main reference C. Aiswarya, B. Bollig P. Gastin, "An Automata-Theoretic Approach to the Verification of Distributed Algorithms," in Proc. of the 26th Int'l Conf. on Concurrency Theory (CONCUR'15), LIPIcs, Vol. 42, pp. 340–353, Schloss Dagstuhl, 2015.
URL http://dx.doi.org/10.4230/LIPIcs.CONCUR.2015.340

In a distributed algorithm, an arbitrary number of processes cooperate to achieve a common goal (e.g., elect a leader). Processes have unique identifiers (pids) from an infinite, totally ordered domain. An algorithm proceeds in synchronous rounds, each round allowing a process to perform a bounded sequence of actions such as send or receive a pid, store it in some register, and compare register contents wrt. the associated total order. An algorithm is supposed to be correct independently of the number of processes. We introduce a logic to specify correctness of distributed algorithms. This logic is inspired by data logics, and can reason about processes and pids. The model checking problem is undecidable in general; we will see some ideas to regain decidability for distributed algorithms over ring topologies. Since the verification of distributed algorithms is undecidable, we propose an underapproximation technique, which bounds the number of rounds. This is an appealing approach, as the number of rounds needed by a distributed algorithm to conclude is often exponentially smaller than the number of processes. We show that round-bounded verification of distributed algorithms over rings is PSPACE-complete.

3.7 Lower Bounds for Symmetric Circuits

Anuj Dawar (University of Cambridge, GB)

Joint work of Anderson, Matthew; Dawar, Anuj
Main reference M. Anderson, A. Dawar, "On Symmetric Circuits and Fixed-Point Logics," in Proc. of the 31st Int'l Symp. on Theoretical Aspects of Computer Science (STACS'14), LIPIcs, Vol. 25, pp. 41–52, Schloss Dagstuhl, 2014.
URL http://dx.doi.org/10.4230/LIPIcs.STACS.2014.41

Symmetric Circuits provide a natural model for studying the complexity of problems on graphs and similar relational structures. Recent work by Anderson and Dawar establishes a close link between families of symmetric circuits and definability in fixed-point logics. This link can be used to show lower bounds on families of symmetric circuits, using methods from finite model theory. In this talk, we show how this can be done, without reference to logical definability by combining the support theorem of Anderson-Dawar with the bijection games of Hella.

3.8 Canonizing Graphs of Bounded Tree Width in Logspace

Michael Elberfeld (RWTH Aachen, DE)

Joint work of Elberfeld, Michael; Schweitzer, Pascal
Main reference M. Elberfeld, P. Schweitzer, "Canonizing Graphs of Bounded Tree Width in Logspace," arXiv:1506.07810v1 [cs.CC], 2015.
URL http://arxiv.org/abs/1506.07810v1

Graph canonization is the problem of computing a unique representative, a canon, from the isomorphism class of a given graph. This implies that two graphs are isomorphic exactly if their canons are equal. We show that graphs of bounded tree width can be canonized by logarithmic-space (logspace) algorithms. This implies that the isomorphism problem for graphs of bounded tree width can be decided in logspace. In the light of isomorphism for trees being hard for the complexity class logspace, this makes the ubiquitous class of graphs of bounded tree width one of the few classes of graphs for which the complexity of the isomorphism problem has been exactly determined.

3.9 Colour Refinement: A Simple Partitioning Algorithm with Applications From Graph Isomorphism Testing to Machine Learning

Martin Grohe (RWTH Aachen, DE)

Colour refinement is a simple algorithm that partitions the vertices of a graph according their "iterated degree sequences". It has very efficient implementations, running in quasilinear time, and a surprisingly wide range of applications. The algorithm has been designed in the context of graph isomorphism testing, and it is used as important subroutine in almost all practical graph isomorphism tools. Somewhat surprisingly, other applications in machine learning, probabilistic inference, and linear programming have surfaced recently.

In my talk, I introduce the basic algorithm as well as higher dimensional extensions known as the k-dimensional Weisfeiler-Lehman algorithm. Then I discuss an unexpected connection between colour refinement and a natural linear programming approach to graph isomorphism testing and an application of colour refinement as a pre-processing routine for linear progarmming.

3.10 Bipartite Matching is in Quasi-NC

Rohit Gurjar (Universität Ulm, DE)

The bipartite matching problem is known to be in P but not in NC. However, it has a randomized NC algorithm using the famous isolation lemma of Mulmuley, Vazirani and Vazirani, 1987. The isolation lemma states that assigning random weights (polynomially bounded) to the edges of a graph ensures that there is a unique minimum weight perfect matching with a good probability. Derandomizing the isolation lemma, that is constructing such a weight assignment deterministically, would give an NC algorithm for matching. We make a step towards this. We construct such a weight assignment for bipartite graphs with quasi-polynomially bounded weights. This implies that bipartite matching is in Quasi-NC (circuits with polylog depth and quasi-poly size).

3.11 Backdoors into Two Occurrences

Jan Johannsen (LMU München, DE)

Backdoor sets for the class CNF(2) of CNF-formulas in which every variable has at most two occurrences are studied in terms of parameterized complexity. The question whether there exist a CNF(2)-backdoor set size k is hard for the class W[2], for both weak and strong backdoors, and in both cases it becomes fixed-parameter tractable when restricted to inputs in d-CNF for a fixed d. Besides that, upper bounds in the W-hierarchy are given for a problem related to the existence of weak backdoor sets, for CNF(2) and other tractable cases of SAT. These imply the first W[2]-completeness results for the problem of finding weak backdoor sets for any tractable cases.

3.12 Quantifying over tuples with Algebra – the multidimensional blockproduct

Klaus-Jörn Lange (Universität Tübingen, DE)

The close connections between polynomially sized circuits of constant depth and first-order logic have been mirrored by algebraic constructions using the blockproduct. This algebraic view had been restricted up to now by only allowing for unary quantifiers using single variables. In this talk the multidimensional blockproduct is introduced which provides a way for the algebraic simulation of first-order quantifiers over tuples of variables.

3.13 Arithmetic circuit complexity and lower bounds

Nutan Limaye (Indian Institute of Technology – Mumbai, IN)

In this talk we will start with a brief introduction to the area of arithmetic circuit complexity. We will then discuss the history of the field and motivation behind some of the important questions being studied in this area.

We will then closely look at the frontier of the current knowledge and discuss some interesting open problems. If time permits, we will discuss some of the recent results.

3.14 Unary temporal and two-variable FO logic with threshold

Kamal Lodaya (The Institute of Mathematical Sciences, IN)

Joint work of Krebs, Andreas; Lodaya, Kamal; Pandya, Paritosh; Straubing, Howard

On words, two-variable logic $\mathrm{FO}^2[<]$ is well mapped out (Schutzenberger, Therien-Wilke, Etessami-Vardi-Wilke, Schwentick-Therien-Vollmer, Lodaya-Pandya-Shah). Its quantifier structure has also been recently studied (Kufleitner-Weil, Krebs-Straubing). Extensions $\mathrm{FO}^2[\mathrm{Num}]$, $\mathrm{FO}^2[\mathrm{Reg}]$ and $\mathrm{Maj}^2[<]$, the last one going out of first order logic, were studied in the complexity context (Koucky-Pudlak-Therien, Behle-Krebs-Refferscheid).

At the level of alphabet letters we look at an extension $\mathrm{FO}^2[<,\mathrm{Th}]$ with binary predicates $a(x, y)$ which stand for the letter a occurring during the "open" interval (x, y) (Pratt, Segerberg). Alternately we can think of a subalphabet B occurring invariantly during the interval (Manna-Moszkowski).

The definable languages include dot depth two and the logic can define several standard languages above $\mathrm{FO}^2[<]$ which occur in the literature, for example $c^*(ac^*bc^*)^*$, for which it is open whether they can be defined in AC^0 circuits with a linear number of gates. As far as we are aware this is the smallest logic which can express these languages. In fact the logic intersects every level of the until and dot depth hierarchies.

So the question of interest is, where is this logic placed?

3.15 QBF Resolution: How important is width?

Meena Mahajan (The Institute of Mathematical Sciences, IN)

Joint work of Beyersdorff, Olaf; Chew, Leroy; Mahajan, Meena; Shukla, Anil
Main reference O. Beyersdorff,L. Chew, M. Mahajan, A. Shukla, "Are Short Proofs Narrow? QBF Resolution is not Simple," ECCC TR15-152, 2015.
URL http://eccc.hpi-web.de/report/2015/152/

One of the main techniques for proving size and space lower bounds in classical resolution proceeds via width: the results of Ben-Sasson and Wigderson (JACM 2001) and of Atserias and Dalmau (JCSS 2008) show that lower bounds on width imply lower bounds on size and space respectively. We assess the effectiveness of such a technique for the QRes system (used to prove QBFs false). We show through a series of examples that

1. The size-width and space-width relations fail to hold in QRes.
   However the failure is due to wide clauses with many universal variables. So we define existential-width (e-width), counting only the number of existential variables in a clause.
2. The tree-size-vs-e-width and tree-space-vs-e-width relations fail to hold in QRes.
3. The size-vs-e-width relation also fails to hold in QRes.
   Examples 2 and 3 have poly-size proofs but need linear e-width.
4. The QParity formula needs exponential-size proofs, and independently, needs linear e-width.

We also provide a direct and efficient (in size, space and e-width) simulation of tree-like QRes proofs by tree-like proofs in the expansion-based system ∀Exp+Res. Further, we show that the expansion-based systems ∀Exp+Res and IR-calc, provably separate in general, have the same power when restricted to tree-like proofs.

3.16 A Strongly Exponential Separation of DNNFs from CNF Formulas

Stefan Mengel (Artois University – Lens, FR)

Joint work of Bova, Simone; Capelli, Florent; Mengel, Stefan; Slivovsky, Friedrich
Main reference S. Bova, F. Capelli, S. Mengel, F. Slivovsky, "A Strongly Exponential Separation of DNNFs from CNF Formulas," arXiv:1411.1995v3 [cs.CC], 2015.
URL http://arxiv.org/abs/1411.1995v3

Decomposable Negation Normal Forms (DNNFs) are Boolean circuits in negation normal form where the subcircuits leading into each AND gate are defined on disjoint sets of variables. We prove a strongly exponential lower bound on the size of DNNFs for a class of CNF formulas built from expander graphs. As a corollary, we obtain a strongly exponential separation between DNNFs and CNF formulas in prime implicates form. This settles an open problem in the area of knowledge compilation (Darwiche and Marquis, 2002).

3.17 Dynamic Complexity of Reachability and Related Problems

Anish Mukherjee (Chennai Mathematical Institute, IN)

Joint work of Datta, Samir; Kulkarni, Raghav; Mukherjee, Anish; Schwentick, Thomas; Zeume, Thomas
Main reference S. Datta, R. Kulkarni, A. Mukherjee, T. Schwentick, T. Zeume, "Reachability is in DynFO," in Proc. of the 42nd International Colloquium on Automata, Languages, and Programming (ICALP'15) – Part 2, LNCS, Vol. 9135, pp. 159–170, Springer, 2015; pre-print available as arXiv:1502.07467v2 [cs.LO], 2015.
URL http://arxiv.org/abs/1502.07467

In most real-life databases data changes frequently and thus makes efficient query answering challenging. Auxiliary data might help to avoid computing query answers from scratch all the time. One way to study this incremental maintenance scenario is from the perspective of dynamic algorithms with the goal of reducing (re-)computation time. Another option is to investigate it from the perspective of low-level parallel computational complexity.

As the "lowest" complexity class AC^0 (with a suitable uniformity condition) and the core of the standard database query language SQL both coincide with first-order predicate logic, one naturally arrives at the question which queries can be maintained dynamically with first-order predicate logic (DynFO). The dynamic complexity framework introduced by Patnaik and Immerman models this setting.

Very recently we have shown that the Reachability query can be maintained in DynFO, confirming a two decade old conjecture of Patnaik and Immerman. After surveying previous known upper bounds for the Reachability query and related problems briefly, I will present the main ideas of the proof of this result.

The talk is based on joint work with Samir Datta, Raghav Kulkarni, Thomas Schwentick and Thomas Zeume.

3.18 Word transducers: from 2-way to 1-way

Anca Muscholl (University of Bordeaux, FR)

Joint work of Baschenis, Felix; Gauwin, Olivier; Muscholl, Anca; Puppis, Gabriele
Main reference F. Baschenis, O. Gauwin, A. Muscholl, G. Puppis, "One-way Definability of Sweeping Transducer.," in Proc. of the 35th IARCS Annual Conf. on Foundation of Software Technology and Theoretical Computer Science (FSTTCS'15), LIPIcs, Vol. 45, pp. 178–191, Schloss Dagstuhl, 2015.
URL http://dx.doi.org/10.4230/LIPIcs.FSTTCS.2015.178

Two-way finite-state transducers on words are strictly more expressive than one-way transducers. It has been shown recently how to decide if a two-way functional transducer has an equivalent one-way transducer, but the complexity of the algorithm is non-elementary. We propose an alternative and simpler characterization for sweeping functional transducers, namely, for transducers that can only reverse their head direction at the extremities of the input. Our algorithm works in 2ExpSpace and, in the positive case, produces an equivalent one-way transducer of doubly exponential size. We also show that the bound on the size of the transducer is tight, and that the one-way definability problem is undecidable for (sweeping) non-functional transducers.

3.19 Finite-Degree Predicates and Two-Variable First-Order Logic

Charles Paperman (University of Warsaw, PL)

Main reference C. Paperman, "Finite-Degree Predicates and Two-Variable First-Order Logic," in Proc. of the 24th EACSL Annual Conf. on Computer Science Logic (CSL'15), LIPIcs, Vol. 41, pp. 616–630, Schloss Dagstuhl, 2015.
URL http://dx.doi.org/10.4230/LIPIcs.CSL.2015.616

We consider two-variable first-order logic on finite words with a fixed number of quantifier alternations. In this talk, we will present results about definability of languages with a neutral letter definable using the order and finite-degree predicates. From these results we derive the strictness of the alternation hierarchy of two-variable logic over this signature as well as a "uniform" lower bounds for the function of addition.

3.20 AC^0 and first order logic, a new approach based on ultrafilters on words

Jean-Eric Pin (University of Paris VII, FR)

Joint work of Gehrke, Mai; Krebs, Andreas; Pin, Jean-Eric
Main reference M. Gehrke, A. Krebs, J.-E. Pin, "Ultrafilters on words for a fragment of logic," Theoretical Computer Science, Vol. 610, Part A, pp. 37–58, 2016.
URL http://dx.doi.org/10.1016/j.tcs.2015.08.007

We give a method for specifying ultrafilter equations and identify their projections on the set of profinite words. Let B be the set of languages captured by first-order sentences using unary predicates for each letter, arbitrary uniform unary numerical predicates and a predicate for the length of a word. We illustrate our methods by giving ultrafilter equations characterising B and then projecting these to obtain profinite equations characterising $B \cap \mathrm{Reg}$. This suffices to establish the decidability of the membership problem for $B \cap \mathrm{Reg}$.

3.21 An exponential lower bound for the sum of products of read once formulas

B. V. Raghavendra Rao (Indian Institute of Techology – Madras, IN)

Joint work of Ramya, C.; Rao, B. V. Raghavendra

Read once arithmetic formulas are formulas where every variable is read at most once. We study limitations of polynomials computed by depth two circuits built over read-once formulas of unbounded depth where the total leaf fan-in for + gates is sub- linear. We prove an exponential lower bound on the size of depth-2 arithmetic circuits with sub- linear product fan-in built over ROPs computing the permanent. Our results demonstrate a class of formulas of unbounded depth with exponential size lower bound against the permanent and can be seen as an exponential improvement over the multilinear formula size lower bounds given by Raz [2] for a sub-class of multilinear and non-multilinear formulas. Our proof techniques are built on the one developed by Raz [2] and later extended by Kumar et al. [1]. Our proofs exploit the structural weakness of CF-ROPs against random partitions

This is a joint work with C. Ramya.

References

1 Mrinal Kumar, Gaurav Maheshwari, and Jayalal Sarma. *Arithmetic circuit lower bounds via MaxRank*. In Automata, Languages, and Programming – 40th International Colloquium, ICALP 2013, Riga, Latvia, July 8-12, 2013, Proceedings, Part I, pages 661–672, 2013.

2 Ran Raz. *Multi-linear formulas for permanent and determinant are of super-polynomial size*. In Proceedings of the 36th Annual ACM Symposium on Theory of Computing, Chicago, IL, USA, June 13-16, 2004, pages 633–641, 2004.

3.22 On the generalised colouring numbers of graphs that exclude a fixed minor

Sebastian Siebertz (TU Berlin, DE)

Joint work of van den Heuvel, Jan; Ossona de Mendez, Patrice; Rabinovich, Roman; Siebertz, Sebastian
Main reference J. van den Heuvel, P. Ossona de Mendez, R. Rabinovich, S. Siebertz, "On the generalised colouring numbers of graphs that exclude a fixed minor," Electronic Notes in Discrete Mathematics, Vol. 49, pp. 523–530, 2015.
URL http://dx.doi.org/10.1016/j.endm.2015.06.072
URL http://eurocomb2015.b.uib.no/files/2015/08/endm1950.pdf

The colouring number $\mathrm{col}(G)$ of a graph G is the minimum integer k such that there exists a linear ordering of the vertices of G in which each vertex v has back-degree at most k, i.e., v has at most k neighbours u with $u < v$. The colouring number is a structural measure that measures the edge density of subgraphs of G. For $r \geq 1$, the numbers $\mathrm{col}_r(G)$ and $\mathrm{wcol}_r(G)$ generalise the colouring number, where $\mathrm{col}_1(G)$ and $\mathrm{wcol}_1(G)$ are equivalent to $\mathrm{col}(G)$. For increasing values of r these measures converge to the well-known structural measures tree-width and tree-depth. For an n-vertex graph, $\mathrm{col}_n(G)$ is equal to the tree-width of G and $\mathrm{wcol}_n(G)$ is equal to the tree-depth of G.

We show that if G excludes K_t as a minor, then $\mathrm{col}_r(G) \leq 3\binom{t-1}{2} \cdot (2r+1)$ and $\mathrm{wcol}_r(G) \leq (r+1)^{3\binom{t-1}{2}} \cdot (2r+1)$. These results improve earlier results published in [1].

References

1 Jan van den Heuvel, and Patrice Ossona de Mendez, and Roman Rabinovich, and Sebastian Siebertz *On the generalised colouring numbers of graphs that exclude a fixed minor*. Electronic Notes in Discrete Mathematics, 2015

3.23 Converse elimination in the algebra of binary relations

Dimitri Surinx (Hasselt University – Diepenbeek, BE)

Joint work of Surinx, Dimitri; Fletcher, George H. L.; Gyssens, Marc; Leinders, Dirk; Van den Bussche, Jan; Van Gucht, Dirk; Wu, Yuqing
Main reference D. Surinx, G. H. L. Fletcher, M. Gyssens, D. Leinders, J. Van den Bussche, D. Van Gucht, S. Vansummeren, Y. Wu, "Relative expressive power of navigational query on graphs using transitive closure," Logic Journal of the IGPL, 23(5):759–788, 2015.
URL http://dx.doi.org/10.1093/jigpal/jzv028

The algebra of binary relations has a long history, going back to Peirce and Schröder, and was greatly developed by Tarski and his collaborators. The simplest language has only the two operators union and composition, together with the identity relation. We can enrich this basic algebra by adding any of the following operators: converse; intersection; set difference; projection; coprojection; transitive closure; and the diversity relation. Boolean queries on relational structures are expressed in terms of the nonemptiness of an algebraic expression. The algebra without intersection, difference and transitive closure, but with projection, admits converse elimination: every expressible boolean query can already be expressed without using the converse operator. We show an exponential lower bound on the degree of the converse-free expression. Furthermore, we show that converse elimination fails in the presence of transitive closure.

3.24 Static Analysis for Logic-Based Dynamic Programs

Nils Vortmeier (TU Dortmund, DE)

Joint work of Schwentick, Thomas; Vortmeier, Nils; Zeume, Thomas
Main reference T. Schwentick, N. Vortmeier, T. Zeume, "Static Analysis for Logic-based Dynamic Programs," in Proc. of the 24th EACSL Annual Conf. on Computer Science Logic (CSL'15), LIPIcs, Vol. 41, pp. 308–324, Schloss Dagstuhl, 2015.
URL http://dx.doi.org/10.4230/LIPIcs.CSL.2015.308

A dynamic program, as introduced by Patnaik and Immerman (1994), maintains the result of a fixed query for an input database which is subject to tuple insertions and deletions. It can use an auxiliary database whose relations are updated via first-order formulas upon modifications of the input database.

This talk discusses static analysis problems for dynamic programs and investigates, more specifically, the decidability of the following three questions. Is the answer relation of a given dynamic program always empty? Does a program actually maintain a query? Is the content of auxiliary relations independent of the modification sequence that lead to an input database?

In general, all these problems can easily be seen to be undecidable for full first-order programs. Therefore we aim at pinpointing the exact decidability borderline for programs.

3.25 Small Dynamic Complexity Classes

Thomas Zeume (TU Dortmund, DE)

Joint work of Datta, Samir; Kulkarni, Raghav; Anish, Mukherjee; Schwentick, Thomas; Zeume, Thomas

In modern data management scenarios, data is subject to frequent changes. In order to avoid costly re-computations from scratch after each small update, one can try to (re-)use auxiliary data structures that have been already computed before to keep the information about the data up-to-date. However, the auxiliary data structures need to be updated dynamically whenever the data changes.

The descriptive dynamic complexity framework (short: dynamic complexity) introduced by Patnaik and Immerman models this setting. It was mainly inspired by relational databases. For a relational database subject to change, auxiliary relations are maintained with the intention to help answering a query Q. When an update to the database, i.e. an insertion or a deletion of a tuple, occurs, every auxiliary relation is updated through a first-order query that can refer to the database as well as to the auxiliary relations.

In this talk I introduced the dynamic complexity framework and discussed recent work on understanding the limits of expressive power of small dynamic complexity classes.

References

1 Samir Datta, Raghav Kulkarni, Anish Mukherjee, Thomas Schwentick, and Thomas Zeume. *Reachability is in DynFO*. ICALP 2015. Springer, 2015.
2 Thomas Zeume and Thomas Schwentick. *Dynamic conjunctive queries*. Proc. 17th International Conference on Database Theory (ICDT) 2014. OpenProceedings.org, 2014.
3 Thomas Zeume and Thomas Schwentick. *On the quantifier-free dynamic complexity of reachability*. Inf. Comput., 240:108-129, 2015.

4 Open Problems

4.1 Perfect matchings for grid graphs and AC^0

Kristoffer Arnsfelt Hansen (Aarhus University, DK)

The width w and length ℓ *full grid* is the graph with vertices $\{(i,j) \mid i \in \{1,\dots,\ell\}, j \in \{1,\dots,w\}\}$ and edges between vertices (i,j) and (i',j') whenever $|i-i'|+|j-j'|=1$. A width w and length ℓ *grid graph* G is simply a subgraph of the width w and length ℓ full grid. In [1] it was shown that deciding whether a perfect matching exists for *constant width* grid graphs can be decided in ACC^0. We will now describe an open question originating from that paper, although not appearing there explicitly. Resolving the question in the positive would imply improving the ACC^0 bound to AC^0.

Let G be a width w length ℓ grid graph where ℓ is odd. The left-end vertices $L(G)$ is the set of vertices of G of the form $(1,j)$ and similarly the right-end vertices $R(G)$ is the set of vertices of G of the form $\ell, j)$. If $L(G) = R(G)$ we can form the width w infinite grid graph G^∞ by an infinite concatenation of G identifying the left-end and right-end vertices of consecutive copies of G.

Assume now that G^∞ has a perfect matching M. Let M' be the perfect matching in G^∞ obtained from M by shifting it by one length of G to the right. We can now ask the question: Is it the case that a graph of the form $M \cup M'$ can never have an infinite path?

References

1 Kristoffer Arnsfelt Hansen, Balagopal Komarath, Jayalal Sarma, Sven Skyum and Navid Talebanfard: *Circuit Complexity of Properties of Graphs with Constant Planar Cutwidth*. MFCS 2014:336–347.

4.2 AC^0 on trees

Mikołaj Bojańczyk (University of Warsaw, PL)

Normally, AC^0 circuits are indexed by lengths of their input. A family of circuits is then viewed as a set of words of arbitrary lengths, and the logical complexity of such word languages can then be studied. In my open problem, I propose to index circuits by unlabelled binary trees (other ideas, like unranked trees or maybe even graphs could also make sense). If the index of a circuit is a tree t, then each gate represents a node of t, and therefore a valuation of the gates represents a labelling of the tree with the alphabet $\{0, 1\}$. A family of circuits, indexed by all possible finite unlabelled binary trees, defines a language of trees labelled by $\{0, 1\}$. The question is: which languages of finite binary trees labelled by $\{0, 1\}$ are simultaneously regular and can be defined in AC^0? One conjecture is that these are exactly those languages which can be defined in first-order logic with the following predicates:

- $0(x)$, which says that position x has label 0;
- $x < y$, which says that y is a descendant of x;
- $\varphi(x)$ for every mso formula φ which only uses the left and right child predicates, and which cannot talk about labels.

This conjecture would be a natural generalisation of a characterisation for finite words, where the logic has modular predicates instead of the mso formulas, as shown in [1].

References

1 David A. Mix Barrington, Kevin J. Compton, Howard Straubing, Denis Thérien: *Regular Languages in NC^1*. J. Comput. Syst. Sci. 44(3):478–499 (1992)

4.3 Prefix diversity

Michaël Cadilhac (Universität Tübingen, DE)

Let L be a language over Σ. Its *prefix diversity* is the function $\mathsf{pd}_L \colon \mathbb{N} \to \mathbb{N}$ defined by:

$$\mathsf{pd}_L(n) = \max_{v_1,\ldots,v_n \in \Sigma^*} |\{(v_1 v, v_2 v, \ldots, v_n v) \mid v \in \Sigma^*\}| \ .$$

In words, for a given n, this is the maximum different number of behaviors one obtains by reading a word v in n different quotients of L.

This notion was used in different terms by Paz [1] and Turakainen [2] in link with probabilistic automata. They show in particular that any so-called $\mathbb{Q}$-stochastic language has a prefix diversity bounded by a polynomial.

Open questions: What is the entire class of languages of poly-bounded prefix diversity? Same question with linear? How does it relate to other notions, such as subword complexity?

References

1 Azaria Paz. *Introduction to probabilistic automata*. Academic Press, 1971.

2 Paavo Turakainen. *On nonstochastic languages and homomorphic images of stochastic languages*. Information Sciences, 24(3):229–253, 1981.

4.4 Proof systems computed by NC^0 circuit families.

Karteek Sreenivasaiah (MPI für Informatik – Saarbrücken, DE)

Main reference K. Sreenivasaiah, “On verifying proofs in constant depth, and polynomial identity testing,” Ph. D. Thesis, Institute of Mathematical Sciences (IMSc), India, 2014.
URL http://www.imsc.res.in/xmlui/handle/123456789/361

A computable function f is called a proof system for a language L if and only if $\mathrm{Range}(f) = L$. We study proof systems computable by NC^0 circuit families. A circuit family $\{C_n\}$ is in NC^0 if C_n has bounded fanin gates and constant depth. We say such a family computes a proof system for L if $\mathrm{Range}(C_n) = L \cap \{0,1\}^n$.

The main goal of this line of work is to characterize languages that have proof systems computable in NC^0. However, a list of realistic goals are as follows:

- Characterize regular languages that have NC^0 computable proof systems.
- Does the language of all directed graphs on n vertices with a path from vertex 0 to vertex n have an NC^0 proof system?

All related results and open problems can be found in the PhD Thesis available here: http://www.imsc.res.in/xmlui/handle/123456789/361.

Participants

- Sreejith Ajithkumar
University of Paris VII, FR
- Christoph Berkholz
HU Berlin, DE
- Olaf Beyersdorff
University of Leeds, GB
- Mikołaj Bojańczyk
University of Warsaw, PL
- Michaël Cadilhac
Universität Tübingen, DE
- Thomas Colcombet
CNRS / University Paris-Diderot, FR
- Aiswarya Cyriac
Uppsala University, SE
- Samir Datta
Chennai Mathematical Inst., IN
- Anuj Dawar
University of Cambridge, GB
- Michael Elberfeld
RWTH Aachen, DE
- Martin Grohe
RWTH Aachen, DE
- Rohit Gurjar
Universität Ulm, DE
- Anselm Haak
Leibniz Univ. Hannover, DE
- Kristoffer Arnsfelt Hansen
Aarhus University, DK
- Jan Johannsen
LMU München, DE
- Juha Kontinen
University of Helsinki, FI
- Andreas Krebs
Universität Tübingen, DE
- Klaus-Jörn Lange
Universität Tübingen, DE
- Nutan Limaye
Indian Institute of Technology – Mumbai, IN
- Kamal Lodaya
The Institute of Mathematical Sciences, IN
- Meena Mahajan
The Institute of Mathematical Sciences, IN
- Pierre McKenzie
University of Montréal, CA
- Arne Meier
Leibniz Univ. Hannover, DE
- Stefan Mengel
Artois University – Lens, FR
- David A. Mix Barrington
University of Massachusetts – Amherst, US
- Anish Mukherjee
Chennai Mathematical Inst., IN
- Anca Muscholl
University of Bordeaux, FR
- Charles Paperman
University of Warsaw, PL
- Jean-Eric Pin
University of Paris VII, FR
- B. V. Raghavendra Rao
Indian Institute of Techology – Madras, IN
- Thomas Schwentick
TU Dortmund, DE
- Luc Segoufin
ENS – Cachan, FR
- Sebastian Siebertz
TU Berlin, DE
- Karteek Sreenivasaiah
MPI für Informatik – Saarbrücken, DE
- Howard Straubing
Boston College, US
- Dimitri Surinx
Hasselt Univ. – Diepenbeek, BE
- Thomas Thierauf
Hochschule Aalen, DE
- Jacobo Torán
Universität Ulm, DE
- Jan Van den Bussche
Hasselt Univ. – Diepenbeek, BE
- Jonni Virtema
Leibniz Univ. – Hannover
- Heribert Vollmer
Leibniz Univ. Hannover, DE
- Nils Vortmeier
TU Dortmund, DE
- Thomas Zeume
TU Dortmund, DE