Report from Dagstuhl Seminar 24421

SAT and Interactions

Olaf Beyersdorff[*1], **Laura Kovács**[*2], **Meena Mahajan**[*3], **Martina Seidl**[*4], **and Kaspar Kasche**[†5]

1 **Friedrich-Schiller-Universität Jena, DE.** olaf.beyersdorff@uni-jena.de
2 **TU Wien, AT.** laura.kovacs@tuwien.ac.at
3 **The Institute of Mathematical Sciences (a CI of Homi Bhabha National Institute) – Chennai, IN.** meena@imsc.res.in
4 **Johannes Kepler Universität Linz, AT.** martina.seidl@jku.at
5 **Friedrich-Schiller-Universität Jena, DE.** kaspar.kasche@uni-jena.de

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar "SAT and Interactions" (24421). The seminar brought together theoreticians and practitioners from the areas of proof complexity, SAT and QBF solving, and first-order theorem proving, who discussed recent developments in their fields and embarked on an interdisciplinary exchange of ideas and techniques between these neighbouring subfields of SAT.

Seminar October 13–18, 2024 – https://www.dagstuhl.de/24421

2012 ACM Subject Classification Theory of computation → Proof complexity; Theory of computation → Proof theory; Theory of computation → Automated reasoning; Theory of computation → Complexity theory and logic

Keywords and phrases SAT, QBF, proof complexity, solving, first-order logic, automated theorem proving

Digital Object Identifier 10.4230/DagRep.14.10.22

1 Executive Summary

Olaf Beyersdorff (Friedrich-Schiller-Universität Jena, DE, olaf.beyersdorff@uni-jena.de)
Laura Kovács (TU Wien, AT, lkovacs@forsyte.at)
Meena Mahajan (The Institute of Mathematical Sciences – Chennai, IN, meena@imsc.res.in)
Martina Seidl (Johannes Kepler Universität Linz, AT, martina.seidl@jku.at)

The problem of deciding whether a propositional formula is satisfiable (SAT) is one of the most fundamental problems in computer science. Its theoretical significance derives from the Cook-Levin Theorem, identifying SAT as the first NP-complete problem. Since then SAT has become a reference for an enormous variety of complexity statements, among them the celebrated P vs NP problem.

There are many generalisations of SAT to logics such as quantified Boolean formulas (QBF), modal and first-order (FO) logics. Often these logics present harder satisfiability problems (e.g. PSPACE-complete for QBF), but can express many practically relevant problems more succinctly, thus applying to more real-world problems.

[*] Editor / Organizer
[†] Editorial Assistant / Collector

SAT and Interactions, *Dagstuhl Reports*, Vol. 14, Issue 10, pp. 22–38
Editors: Olaf Beyersdorff, Laura Kovács, Meena Mahajan, and Martina Seidl
DAGSTUHL REPORTS Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Due to its practical implications, intensive research has been performed to solve SAT problems in an automated fashion. The last decades have seen the development of practically efficient algorithms for SAT, QBF, and further logics, and their implementation as solvers, which successfully solve huge industrial instances.

As the fourth in its series, the Dagstuhl Seminar took a broad perspective on the theory of SAT, encompassing propositional logic, QBF, and first-order theorem proving. Its main aim was to bring together researchers from different areas of activity in SAT and first-order logic, including computational complexity, proof complexity, proof theory, theorem proving, and solving, so that they can communicate state-of-the-art advances and embark on a systematic interdisciplinary interaction.

The Dagstuhl Seminar placed particular emphasis on the three following fields: propositional logic (complexity, proof complexity, solving), QBF (proof complexity and solving), and FO theorem proving. A particularly novel feature was the interaction of the communities active in proof complexity and solving of SAT/QBF (the propositional logics) with the first-order theorem proving community. There appeared to be overall consensus among the participants that this interchange of ideas between SAT solving techniques and first-order theorem proving was very stimulating and might particularly prove useful towards further efficient implementations of first-order proof rules.

To facilitate interactions between participants from the different fields, the seminar included a number of survey talks to introduce neighbouring communities to the main notions, results, and challenges of the represented areas. The following survey talks were given towards the beginning of the seminar:

- Marc Vinyals: SAT Solving and Proof Complexity;
- Friedrich Slivovsky: QBF Solving and Proof Complexity;
- Cesare Tinelli: An introduction to Satisfiability Modulo Theories;
- Stephan Schulz: First-order Theorem Proving.

Each of these surveys was accompanied by one or more sessions with contributed talks dedicated to recent specific results of the field.

The seminar also included an open problem session where participants discussed open research directions and specific problems. The following topics were discussed:

- Stephan Schulz: Can we achieve good engineering and long-term viability of systems?
  Software projects often get abandoned over time, especially if the original authors leave. We are looking for technical and organisational solutions to mitigate this.
- Sophie Tourret: Beyond critical.
  There are established techniques to compare the hardness of propositional formulas. Can we find analogous techniques for first-order logic and SMT? Particularly interesting are cases outside the decidable fragments of these theories.
- Neil Thapen: Where is symmetry breaking in TFNP?
  Symmetry breaking techniques can be understood as the optimisation problem of finding a lexically minimal assignment, which is in TFNP. We know it is in PLS, it might be in CLS, but can we at least show that it is not in FP? This has implications on the strength of Extended Frege.
- Adrian Rebola-Pardo: How should we design future proof formats?
  There is a variety of practical proof formats that need to be suitable for verification and querying. Is it possible to design good universal proof formats? Important considerations include binary encodings, non-clausal representations, specific addition and deletion rules, the needs of incremental SAT solvers, and parallel proof checking.

- Florent Capelli: Properties of a hypergraph measure. The β-hyperorderwidth is a purely graph-theoretic measure on hypergraphs. How does it compare to established hypergraph measures? For example, there is a hypergraph that has β-hyperorderwidth 1, but its incidence graph has treewidth n. Is this possible the other way around? Can we generalize the definition of β-hyperorderwidth?

The seminar included ample time for discussions and informal interactions, a feature that appeared to be largely welcomed and productively used. On Wednesday afternoon we organised a traditional well-attended hike. On Thursday evening, we had a joyful music night with contributions from Sophie Tourret, Ilario Bonacina, Dominik Scheder, Florent Capelli, and Kaspar Kasche. They played music by Marin Marais, Georg Philipp Telemann, Wolfgang Amadeus Mozart, Francis Poulenc, and George Gershwin.

The organisers believe that the seminar fulfilled their original high goals: the talks were well received and triggered many discussions. Many participants reported about the inspiring seminar atmosphere, fruitful interactions, and a generally positive experience. The organisers and participants wish to thank the staff and the management of Schloss Dagstuhl for their assistance and excellent support in the arrangement of a very successful and productive event.

2 Table of Contents

Executive Summary

Overview of Talks

3 Overview of Talks

3.1 Generalized Satisfiability Problems via Operator Assignments

Albert Atserias (UPC Barcelona Tech, ES)

Joint work of Albert Atserias, Phokion G. Kolaitis, Simone Severini
Main reference Albert Atserias, Phokion G. Kolaitis, Simone Severini: "Generalized satisfiability problems via operator assignments", J. Comput. Syst. Sci., Vol. 105, pp. 171–198, 2019.
URL https://doi.org/10.1016/J.JCSS.2019.05.003

Schaefer introduced a framework for generalized satisfiability problems on the Boolean domain and characterized the computational complexity of such problems. We investigate an algebraization of Schaefer's framework in which the Fourier transform is used to represent constraints by multilinear polynomials in a unique way. The polynomial representation of constraints gives rise to a relaxation of the notion of satisfiability in which the values to variables are linear operators on some Hilbert space. For the case of constraints given by a system of linear equations over the two-element field, this relaxation has received considerable attention in the foundations of quantum mechanics, where such constructions as the Mermin-Peres magic square show that there are systems that have no solutions in the Boolean domain, but have solutions via operator assignments on some finite-dimensional Hilbert space. We obtain a complete characterization of the classes of Boolean relations for which there is a gap between satisfiability in the Boolean domain and the relaxation of satisfiability via operator assignments. To establish our main result, we adapt the notion of primitive-positive definability (pp-definability) to our setting, a notion that has been used extensively in the study of constraint satisfaction problems. Here, we show that pp-definability gives rise to gadget reductions that preserve satisfiability gaps. We also present several additional applications of this method. In particular and perhaps surprisingly, we show that the relaxed notion of pp-definability in which the quantified variables are allowed to range over operator assignments gives no additional expressive power in defining Boolean relations.

3.2 A new hypergraph measure for #SAT

Florent Capelli (University of Artois/CNRS – Lens, FR)

Joint work of Florent Capelli, Oliver Irwin
Main reference Florent Capelli, Oliver Irwin: "Direct Access for Conjunctive Queries with Negations", in Proc. of the 27th International Conference on Database Theory, ICDT 2024, March 25-28, 2024, Paestum, Italy, LIPIcs, Vol. 290, pp. 13:1–13:20, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2024.
URL https://doi.org/10.4230/LIPICS.ICDT.2024.13

The problem #SAT of counting the number of satisfying assignments of a CNF formula is a notoriously hard combinatorial problem, even for very restricted classes of CNF formulas, such as monotone 2-CNF. Islands of tractability have been however discovered for the problem by restricting the way clauses and variables interact inside the formula. CNF formulas whose hypergraph is beta-acyclic have been shown tractable for #SAT and knowledge compilation. This result gave hope toward proving tractability for a larger family of formulas, those having bounded beta-hypertreewidth. However, the definition of beta-hypertreewidth is not based on graph decomposition and hence are hard to deal with algorithmically. The hardness of #SAT on such formulas remains open. In this talk, I will present a new hypergraph parameter, called beta-hyperorder width, for which #SAT and knowledge compilation are tractable. This measure naturally generalizes primal treewidth and beta-acyclicity while being defined via elimination orders which can be leveraged into an algorithm.

The results presented in this talk are adapted from recent work with Oliver Irwin, "Direct Access for Conjunctive Queries with Negations" which appeared at ICDT 2025, which present a more database flavor version of the results.

3.3 Propositional Proofs for PSPACE problems (including #SAT)

Leroy Nicholas Chew (TU Wien, AT)

Joint work of Leroy Nicholas Chew, Sravanthi Chede, Anil Shukla

We show how to use the correctness of a polynomial space algorithm that decides some language L as a basis for an L-proof system. The first example is a proof system for #SAT.

The proofs consist of a non-deterministically guessed multi circuit. The circuit takes in a binary integer to represent the time and outputs the memory of the algorithm at said timepoint. In #SAT we can simplify this to calculating the cumulative function (or running count) of models counted up to a point. Checking the circuit for correctness is a CoNP problem so we only need a propositional proof that proves the circuit is in fact correct.

Our proof system is called Circuit Linear Induction Proposition (CLIP), CLIP for #SAT simulates all previous #SAT proof systems. This gives us a new opportunity to create strong proof systems for PSPACE languages that do not rely on a direct translation to Quantified Boolean Formulas (QBF). In this paper we explore some proof complexity results of systems of this form and study the connection to QBF proof complexity.

This talk adapts both the FSTTCS paper "Circuits Proofs and Propositional Model Counting" (to appear) by Sravanthi Chede, Leroy Chew and Anil Shukla and an upcoming paper "Propositional Proofs for PSPACE Problems" by Leroy Chew.

3.4 Pudlák-Buss games for (non)deterministic branching programs

Anupam Das (University of Birmingham, GB)

Joint work of Anupam Das, Avgerinos Delkos

A natural nonuniform version of (N)L is given by (non)deterministic branching programs. These may be naturally given a proof theoretic treatment via a system for (non)deterministic decision trees with extension to represent dagness. Such systems, eL(N)DT, were proposed by Buss, Das and Knop in '20, who also established their basic proof complexity results.

In this talk I will speak about recent work with Avgerinos Delkos recasting those systems as Prover-Adversary games, à la Pudlák & Buss. Our main result is a correspondence between strategies and proofs. Along the way, we establish a proof complexity theoretic version of the Immerman-Szelepcsényi theorem that NL=coNL. One novelty here is that our proof exploits the ability to count at the proof level rather than the formula level, significantly simplifying our construction.

3.5 Truly Supercritical Trade-offs for Resolution, Cutting Planes, and Monotone Circuits

Susanna de Rezende (Lund University, SE)

Joint work of Susanna F. de Rezende, Noah Fleming, Duri Andrea Janett, Jakob Nordström, Shuo Pang
Main reference Susanna F. de Rezende, Noah Fleming, Duri Andrea Janett, Jakob Nordström, Shuo Pang: "Truly Supercritical Trade-offs for Resolution, Cutting Planes, Monotone Circuits, and Weisfeiler-Leman", Electron. Colloquium Comput. Complex., Vol. TR24-185, 2024.
URL https://eccc.weizmann.ac.il/report/2024/185

We present supercritical trade-off for monotone circuits, showing that there are functions computable by small circuits for which any circuit must have depth super-linear or even super-polynomial in the number of variables, far exceeding the linear worst-case upper bound. We obtain similar trade-offs in proof complexity, where we establish the first size-depth trade-offs for cutting planes and resolution that are truly supercritical, i.e., in terms of formula size rather than number of variables, and we also show supercritical trade-offs between width and size for treelike resolution. Our results build on a new supercritical width-depth trade-off for resolution, obtained by refining and strengthening the compression scheme for the Cop-Robber game in [1], which we will have heard about in the previous talk. The supercritical size-depth trade-offs for monotone circuits, cutting planes and resolution, and the supercritical size-width trade-off for tree-like resolution follow from improved lifting theorems that might be of independent interest. This is joint work with Noah Fleming, Duri Andrea Janett, Jakob Nordström, and Shuo Pang.

References

1 Martin Grohe, Moritz Lichter, Daniel Neuen, and Pascal Schweitzer. Compressing CFI graphs and lower bounds for the Weisfeiler-Leman refinements. In *Proceedings of the 64th Annual IEEE Symposium on Foundations of Computer Science (FOCS '23)*, pages 798–809, November 2023.

3.6 SAT modulo IPASIR-UP

Katalin Fazekas (TU Wien, AT)

Joint work of Katalin Fazekas, Aina Niemetz, Mathias Preiner, Markus Kirchweger, Stefan Szeider, Armin Biere, Airna Niemetz, Mathias Fleury, Florian Pollitt
Main reference Katalin Fazekas, Aina Niemetz, Mathias Preiner, Markus Kirchweger, Stefan Szeider, Armin Biere: "IPASIR-UP: User Propagators for CDCL", in Proc. of the 26th International Conference on Theory and Applications of Satisfiability Testing, SAT 2023, July 4-8, 2023, Alghero, Italy, LIPIcs, Vol. 271, pp. 8:1–8:13, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2023.
URL https://doi.org/10.4230/LIPICS.SAT.2023.8

Modern SAT solvers are often integrated as sub-reasoning engines into more complex tools to address problems beyond Boolean satisfiability. Consider, for example, solvers for Satisfiability Modulo Theories (SMT), combinatorial optimization, model enumeration, and model counting. In our work, we have proposed a general interface for CDCL SAT solvers to capture the essential functionalities necessary to simplify and improve use cases that require more fine-grained interaction with the SAT solver than provided by the standard IPASIR interface.

In this talk I will briefly describe the interface and highlight the main changes made since its introduction. I will also present our ongoing work and the challenges and future work we are currently considering. The aim of the talk is to initiate further discussions with the other participants of the seminar to get a better understanding of the required features and typical use cases.

3.7 First-order theorem proving for operator statements

Clemens Hofstadler (Universität Kassel, DE)

Joint work of Clemens Hofstadler, Clemens G. Raab, Georg Regensburger
Main reference Clemens Hofstadler, Clemens G. Raab, Georg Regensburger: “Universal truth of operator statements via ideal membership”,CoRR, Vol. abs/2212.11662 2024.
URL https://doi.org/10.48550/arXiv.2212.11662

Algebraic statements involving matrices or linear operators appear in various branches of mathematics and related disciplines. In linear algebra and geometry, we study matrices and their properties as fundamental objects, while in functional analysis, linear operators help to analyse function spaces. Their applications range from the study of integral and differential equations to different tasks in the field of signal processing. In quantum mechanics, linear operators describe the evolution of quantum systems through the Schrödinger equation.

In this talk, we present a recently developed framework for proving first-order statements about identities of matrices or linear operators by performing algebraic computations. Our main result is a semi-decision procedure that allows to prove any true operator statement based on a single algebraic computation. We also discuss our software package `operator_gb` [2], which offers functionality for automating such computations, and we present the results of a recent case study [1].

References

1 K. Bernauer, C. Hofstadler, and G. Regensburger. *How to Automatise Proofs of Operator Statements: Moore–Penrose Inverse; A Case Study.* International Workshop on Computer Algebra in Scientific Computing, pp. 39–68, 2023.

2 C. Hofstadler. *Noncommutative Gröbner bases and automated proofs of operator statements.* PhD thesis. Johannes Kepler University Linz, Austria, 2023.

3.8 Proof Complexity for Model Counting

Kaspar Kasche (Friedrich-Schiller-Universität Jena, DE)

Joint work of Olaf Beyersdorff, Johannes Klaus Fichte, Joachim Giesen, Andreas Goral, Markus Hecher, Tim Hoffmann, Kaspar Kasche, Christoph Staudt
Main reference Olaf Beyersdorff, Johannes Klaus Fichte, Markus Hecher, Tim Hoffmann, Kaspar Kasche: “The Relative Strength of #SAT Proof Systems”, in Proc. of the 27th International Conference on Theory and Applications of Satisfiability Testing, SAT 2024, August 21-24, 2024, Pune, India, LIPIcs, Vol. 305, pp. 5:1–5:19, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2024.
URL https://doi.org/10.4230/LIPICS.SAT.2024.5

The propositional model counting problem #SAT asks to compute the number of satisfying assignments for a given propositional formula. Recently, three #SAT proof systems kcps[1] (knowledge compilation proof system), MICE[2] (model counting induction by claim extension), and CPOG[3] (certified partitioned-operation graphs) have been introduced with the aim to model #SAT solving and enable proof logging for solvers. Prior to this paper, the relations between these proof systems have been unclear and very few proof complexity results are known. We completely determine the simulation order of the three systems, establishing that CPOG simulates both MICE and kcps, while MICE and kcps are exponentially incomparable. This implies that CPOG is strictly stronger than the other two systems.

References

1 Florent Capelli: Knowledge Compilation Languages as Proof Systems. SAT 2019: 90-99

2 Johannes Klaus Fichte, Markus Hecher, Valentin Roland: Proofs for Propositional Model Counting. SAT 2022: 30:1-30:24

3 Randal E. Bryant, Wojciech Nawrocki, Jeremy Avigad, Marijn J. H. Heule: Certified Knowledge Compilation with Application to Verified Model Counting. 6:1-6:20

3.9 The packing chromatic number of the infinite square lattice

Barnaby Martin (Durham University, GB)

The packing chromatic number of a graph is the minimum n so that the graph may be vertex-coloured with n colours so that vertices coloured $i < n + 1$ never appear at distance i or less from one another (thus colour 1 behaves as in a usual proper colouring). We survey results about the packing chromatic number of various infinite lattices and present bounds for the infinite square lattice that have been found by various methods, including SAT-solving, which were recently perfected to the answer 15.

3.10 Supercritical and Robust Trade-offs for Resolution Depth Versus Width and Weisfeiler-Leman

Jakob Nordström (University of Copenhagen, DK & Lund University, SE)

Joint work of Duri Andrea Janett, Jakob Nordström, Shuo Pang

We prove robust supercritical trade-off results for depth versus width in resolution and for the Weisfeiler-Leman algorithm, where optimizing one complexity measure even approximately causes worse than brute-force worst-case behaviour for the other measure. These are the first trade-offs in these settings that are truly supercritical measured not only in the number of variables but in the size of the input.

3.11 AVATAR: 10 years on

Michael Rawson (TU Wien, AT)

Joint work of Michael Rawson, Martin Suda

AVATAR is a powerful but poorly-understood component of the Vampire theorem prover, first introduced by Andrei Voronkov circa 2014 [1]. In essence, AVATAR allows a SAT solver to manage the propositional structure of splitting decisions during proof search. I introduce AVATAR, chart its development over the last ten years (such as practical experiments [2] and AVATAR modulo theories [3]), and give some future directions [4].

References

1 Andrei Voronkov. *AVATAR: the architecture for first-order theorem provers*. CAV 2014, Springer.

2 Giles Reger Martin Suda Andrei Voronkov. *Playing with AVATAR*. CADE-25, Springer.

3 Nikolaj Bjorner Giles Reger Martin Suda Andrei Voronkov. *AVATAR modulo theories*. GCAI 2016.

4 Sólrún Halla Einarsdóttir. *Lemma Discovery and Strategies for Automated Induction*. IJCAR 2024, Springer.

3.12 Open problems in interference and proofs for SAT solving

Adrian Rebola-Pardo (TU Wien, AT & Johannes Kepler Universität Linz, AT)

Joint work of Adrian Rebola-Pardo, Georg Weissenbacher
Main reference Adrián Rebola-Pardo: "Even Shorter Proofs Without New Variables", in Proc. of the 26th International Conference on Theory and Applications of Satisfiability Testing, SAT 2023, July 4-8, 2023, Alghero, Italy, LIPIcs, Vol. 271, pp. 22:1–22:20, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2023.
URL https://doi.org/10.4230/LIPICS.SAT.2023.22

Enormous progress has been made over the last decade in proofs for SAT solving. The combination of satisfiability-preserving inferences, deletion instructions and clausal proofs allowed the development of effective and compact proof formats, such as DRAT. Further advancements include extended inference power, featured in DPR and (W)SR proofs, as well as hinted proofs that can be checked with verified tools, like LRAT and FRAT.

This fast evolution has left some problems unsolved, and some paths unexplored. In this talk I will argue that these gaps in our understanding and development of proofs for SAT are relevant for certification, and for SAT solving itself. In my talk I will focus on (at most, depending on time restrictions) four of these problems.

First, the proliferation of proof systems has created a cornucopia of different checkers and formats with slightly different properties, capabilities and even semantics. Some approaches are to every extent superior, yet their implementation is still spotty; some approaches have been accepted at face value without considering drawbacks or alternatives. We will review some design decisions in proof systems that may be worth revisiting.

Second, deletion instructions, which first appeared in DRUP as a performance-related feature, have quietly become more relevant, and more problematic. CDCL-based SAT proofs are dominated by one specific flavor of deletion, which I call linear deletion. However, this is not the case in adjacent fields. Both VeriPB and WSR depart from this idea, and in doing so they enable new paths in proofs and in reasoning.

Third, satisfiability-preserving inferences have recently come to be understood as reasoning without loss of generality. This enabled very powerful proof systems, but in practice these features are underutilized. In the last couple of years, however, the interest on these techniques has rekindled. I will review what is new, and what theoretical and practical problems still remain to be solved.

Finally, I will explain how well (or not) these advancements extend to other solving paradigms, including non-CNF SAT solving, (D)QBF and model checking, and what roadblocks exist that need further research.

3.13 PPSZ is better than you think

Dominik Alban Scheder (TU Chemnitz, DE)

Main reference Dominik Scheder: "PPSZ is better than you think", TheoretiCS, Vol. 3, 2024.
URL https://doi.org/10.46298/THEORETICS.24.5

PPSZ, for long time the fastest known algorithm for k-SAT, works by going through the variables of the input formula in random order; each variable is then set randomly to 0 or 1, unless the correct value can be inferred by an efficiently implementable rule (like small-width resolution; or being implied by a small set of clauses).

We show that PPSZ performs exponentially better than previously known, for all $k \geq 3$. We achieve this through an improved analysis and without any change to the algorithm itself. The core idea is to pretend that PPSZ does not process the variables in uniformly random order, but according to a carefully designed distribution. We write "pretend" since this can be done while running the original algorithm, which does use a uniformly random order.

3.14 Tutorial: First-Order Automated Theorem Proving

Stephan Schulz (Duale Hochschule Baden-Württemberg – Stuttgart, DE)

I provide a short overview of modern first-order theorem proving, discussing the overall structure of a prover, including clausification and refutation core. For the latter part, we discuss saturation up to redundancy in the superposition setting. We also discuss implementation and search control.

3.15 QBF Solving and Proof Complexity

Friedrich Slivovsky (University of Liverpool, GB)

Quantified Boolean Formulas (QBF) extend propositional formulas with quantifiers ranging over truth values. Satisfiability testing of QBFs is PSPACE-complete, and they can succinctly encode many problems arising in verification and synthesis. This talk provides an introduction to the main paradigms in QBF solving, Quantified CDCL and Expansion, and their corresponding proof systems. It also gives an overview of QBF proof complexity, highlighting the unique role of strategy extraction.

3.16 Polynomial Calculus for QBF

Luc Spachmann (Friedrich-Schiller-Universität Jena, DE)

Joint work of Olaf Beyersdorff, Kasper Kasche, Luc Nicolas Spachmann
Main reference Olaf Beyersdorff, Tim Hoffmann, Kaspar Kasche, Luc Nicolas Spachmann: "Polynomial Calculus for Quantified Boolean Logic: Lower Bounds Through Circuits and Degree", in Proc. of the 49th International Symposium on Mathematical Foundations of Computer Science, MFCS 2024, August 26-30, 2024, Bratislava, Slovakia, LIPIcs, Vol. 306, pp. 27:1–27:15, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2024.
URL https://doi.org/10.4230/LIPICS.MFCS.2024.27

We initiate an in-depth proof-complexity analysis of polynomial calculus (Q-PC) for Quantified Boolean Formulas (QBF). In the course of this we establish a tight proof-size characterisation of Q-PC in terms of a suitable circuit model (polynomial decision lists). Using this correspondence we show a size-degree relation for Q-PC, similar in spirit, yet different from the classic size-degree formula for propositional PC by Impagliazzo, Pudlák and Sgall (1999). We use the circuit characterisation together with the size-degree relation to obtain various new lower bounds on proof size in Q-PC. This leads to incomparability results for Q-PC systems over different fields.

3.17 First-Order Finite Model Finding via SAT

Martin Suda (Czech Technical University – Prague, CZ)

Main reference Koen Claessen: "New Techniques that Improve MACE-style Finite Model Finding", 2007.
URL https://api.semanticscholar.org/CorpusID:15694927

I will present how the search for finite models in first-order logic is typically translated into a sequence of SAT formulas, what kinds of symmetry breaking can be used to make these formulas easier to tackle and what extra challenges the multi-sorted setting brings.

3.18 SAT modulo Symmetries – an update

Stefan Szeider (TU Wien, AT) and Tomáš Peitl (TU Wien, AT)

Joint work of Mikoláš Janota, Markus Kirchweger, Tomáš Peitl, Stefan Szeider
Main reference Mikoláš Janota, Markus Kirchweger, Tomáš Peitl, Stefan Szeider: "Breaking Symmetries in Quantified Graph Search: A Comparative Study", 2025.
URL https://arxiv.org/abs/2502.15078

SAT modulo Symmetries (SMS) is a framework for the exhaustive isomorph-free generation of combinatorial objects with a prescribed property. SMS relies on the tight integration of a CDCL SAT solver with a custom dynamic symmetry-breaking algorithm that iteratively refines an ordered partition of the generated object's elements. This talk will discuss the basic concepts of SMS, some applications, and recent extensions to graph properties specified as general quantified Boolean formulas (QBF). In the second part of the talk, Tomáš Peitl will give a live demo of SMS and its QBF extension.

3.19 SLIM for MaxSAT

Stefan Szeider (TU Wien, AT)

Joint work of André Schidler, Stefan Szeider
Main reference André Schidler, Stefan Szeider: "Structure-Guided Local Improvement for Maximum Satisfiability", in Proc. of the 30th International Conference on Principles and Practice of Constraint Programming, CP 2024, September 2-6, 2024, Girona, Spain, LIPIcs, Vol. 307, pp. 26:1–26:23, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2024.
URL https://doi.org/10.4230/LIPICS.CP.2024.26

The enhanced performance of today's MaxSAT solvers has elevated their appeal for many large-scale applications, notably in software analysis and computer-aided design. Our research delves into refining anytime MaxSAT solving by repeatedly identifying and solving with an exact solver smaller subinstances that are chosen based on the graphical structure of the instance. We investigate various strategies to pinpoint these subinstances. This structure-guided selection of subinstances provides an exact solver with a high potential for improving the current solution. Our exhaustive experimental analyses contrast our methodology as instantiated in our tool MaxSLIM with previous studies and benchmark it against leading-edge MaxSAT solvers.

3.20 Resolution height and a candidate formula hard for CDCL without restarts

Neil Thapen (The Czech Academy of Sciences – Prague, CZ)

Joint work of Sam Buss, Neil Thapen
Main reference Sam Buss, Neil Thapen: "A Simple Supercritical Tradeoff between Size and Height in Resolution", Electron. Colloquium Comput. Complex., Vol. TR24-001, 2024.
URL https://eccc.weizmann.ac.il/report/2024/001

We describe a family of CNFs in n variables which have small resolution refutations but are such that any small refutation must have height larger than n (even exponential in n), where the height of a refutation is the length of the longest path in it (a similar result appeared in [1]). Small refutations of our formulas are thus highly irregular, containing paths querying the same variable many times. This makes it a plausible candidate to separate resolution from pool resolution, which amounts to separating CDCL with restarts from CDCL without. We are not able to show this, but in the other direction we show that a simpler version of our formula, with a similar irregularity property, does have polynomial size pool resolution refutations.

References

1 Noah Fleming, Toniann Pitassi, Robert Robere: Extremely Deep Proofs. ITCS 2022: 70:1-70:23

3.21 An introduction to Satisfiability Modulo Theories

Cesare Tinelli (University of Iowa – Iowa City, US)

The talk provides an overview of Satisfiability Modulo Theories (SMT), a subfield of automated reasoning that combines uniform methods to reason about formulas in first-order logic with specialized methods to reason about various data types of interest in computer science such as integer and real numbers, bit vectors, strings, finite sets, lists, and so on. The talk is in two parts: Part I focuses on motivation, functionality and applications. Part II describes at an abstract level, in terms of satisfiability proof systems, major approaches to build SMT solvers by combining SAT solvers with specialized solvers for individual theories of various data types.

3.22 Mechanizing the Splitting Framework

Sophie Tourret (INRIA Nancy – Grand Est, FR)

Joint work of Sophie Tourret, Ghilaien Bergeron, Florent Krasnopol

In this talk, I presented the current state of the Isabelle/HOL mechanization efforts that I am leading on the "splitting framework", that makes it possible to use propositional models and a SAT solver to guide the inferences of a saturation-based calculus, as is done in AVATAR. The Isabelle/HOL results do not cover AVATAR yet, but a simpler form of splitting. In ongoing work, we cover "splitting without backtracking" over resolution in FOL. The work was still ongoing at the time of the seminar and I explained where we stood then and why.

3.23 SAT and Proof Complexity

Marc Vinyals (University of Auckland, NZ)

We discuss connections between SAT solvers and proof complexity: how we can analyse the CDCL algorithm thanks to resolution, and how stronger proof systems can guide new developments.

3.24 The Complexity of Enumerating Satisfying Assignments

Heribert Vollmer (Leibniz Universität Hannover, DE)

Joint work of Nadia Creignou, Arnaud Durand, Heribert Vollmer, Markus Kröll, Reinhard Pichler, Sebastian Skritek
Main reference Nadia Creignou, Arnaud Durand, Heribert Vollmer: "Enumeration Classes Defined by Circuits", in Proc. of the 47th International Symposium on Mathematical Foundations of Computer Science, MFCS 2022, August 22-26, 2022, Vienna, Austria, LIPIcs, Vol. 241, pp. 38:1–38:14, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022.
URL https://doi.org/10.4230/LIPICS.MFCS.2022.38
Main reference Nadia Creignou, Markus Kröll, Reinhard Pichler, Sebastian Skritek, Heribert Vollmer: "A complexity theory for hard enumeration problems", Discret. Appl. Math., Vol. 268, pp. 191–209, 2019.
URL https://doi.org/10.1016/J.DAM.2019.02.025

We study the algorithmic problem to enumerate all satisfying assignments of a given propositional formula. For formula classes with a polynomial-time decision problem, this can be done within the class DelayP, introduced by Johnson, Papadimitriou and Yannakakis in 1988 and regarded since then as a reasonable notion of "efficient" enumeration. We will present two results:

1. We generalize the class DelayP to a hierarchy analogous to the polynomial-time hierarchy of decision problems and show that Enum-SAT is complete in the Σ_1-level of this hierarchy under some form of enumeration Turing reductions.
2. We define a hierarchy of very efficiently enumerable problems within DelayP, based in the Boolean circuit class AC_0, and place the enumeration problems for monotone, IHS, Krom, and affine formulas in lower levels of this hierarchy.

Open remains an exact classification of the problem Enum-Horn-SAT.

Participants

- Albert Atserias
UPC Barcelona Tech, ES
- Olaf Beyersdorff
Friedrich-Schiller-Universität Jena, DE
- Ilario Bonacina
UPC Barcelona Tech, ES
- Florent Capelli
University of Artois/CNRS – Lens, FR
- Leroy Nicholas Chew
TU Wien, AT
- Anupam Das
University of Birmingham, GB
- Susanna de Rezende
Lund University, SE
- Katalin Fazekas
TU Wien, AT
- Mathias Fleury
Universität Freiburg, DE
- Pascal Fontaine
University of Liège, BE
- Marlene Gründel
Friedrich-Schiller-Universität Jena, DE
- Clemens Hofstadler
Universität Kassel, DE
- Kaspar Kasche
Friedrich-Schiller-Universität Jena, DE
- Phokion G. Kolaitis
University of California – Santa Cruz, US
- Wietze Koops
Lund University, SE & University of Copenhagen, DK
- Konstantin Korovin
University of Manchester, GB
- Laura Kovács
TU Wien, AT
- Massimo Lauria
Sapienza University of Rome, IT
- Meena Mahajan
The Institute of Mathematical Sciences – Chennai, IN
- Barnaby Martin
Durham University, GB
- Stefan Mengel
CNRS, CRIL – Lens, FR
- Claudia Nalon
University of Brasília, BR
- Jakob Nordström
University of Copenhagen, DK & Lund University, SE
- Tomáš Peitl
TU Wien, AT
- Florian Pollitt
Universität Freiburg, DE
- Michael Rawson
TU Wien, AT
- Adrian Rebola-Pardo
TU Wien, AT & Johannes Kepler Universität Linz, AT
- Rahul Santhanam
University of Oxford, GB
- Dominik Alban Scheder
TU Chemnitz, DE
- Tanja Schindler
Universität Basel, CH
- Stephan Schulz
Duale Hochschule Baden-Württemberg – Stuttgart, DE
- Martina Seidl
Johannes Kepler Universität Linz, AT
- Friedrich Slivovsky
University of Liverpool, GB
- Luc Spachmann
Friedrich-Schiller-Universität Jena, DE
- Martin Suda
Czech Technical University – Prague, CZ
- Stefan Szeider
TU Wien, AT
- Neil Thapen
The Czech Academy of Sciences – Prague, CZ
- Cesare Tinelli
University of Iowa – Iowa City, US
- Jacobo Torán
Universität Ulm, DE
- Sophie Tourret
INRIA Nancy – Grand Est, FR
- Marc Vinyals
University of Auckland, NZ
- Heribert Vollmer
Leibniz Universität Hannover, DE
- Andrei Voronkov
University of Manchester, GB