Report from Dagstuhl Seminar 16381

SAT and Interactions

Edited by

Olaf Beyersdorff[1], Nadia Creignou[2], Uwe Egly[3], and Heribert Vollmer[4]

1 **University of Leeds, GB,** o.beyersdorff@leeds.ac.uk
2 **Aix-Marseille University, FR,** nadia.creignou@lif.univ-mrs.fr
3 **TU Wien, AT,** uwe@kr.tuwien.ac.at
4 **Leibniz Universität Hannover, DE,** vollmer@thi.uni-hannover.de

Abstract

This report documents the programme and outcomes of Dagstuhl Seminar 16381 "SAT and Interactions". The seminar brought together researchers from different areas from theoretical computer science involved with various aspects of satisfiability. A key objective of the seminar has been to initiate or consolidate discussions among the different groups for a fresh attack on one of the most important problems in theoretical computer science and mathematics.

Seminar September 18–23, 2016 – http://www.dagstuhl.de/16381
1998 ACM Subject Classification E.1 Data Structures, F.2 Analysis of Algorithms and Problem Complexity, G.2.1 Combinatorics
Keywords and phrases Combinatorics, Computational Complexity, P vs. NP, Proof Complexity, Quantified Boolean formulas, SAT-solvers, satisfiability problem
Digital Object Identifier 10.4230/DagRep.6.9.74
Edited in cooperation with Joshua Blinkhorn

1 Executive Summary

Olaf Beyersdorff
Nadia Creignou
Uwe Egly
Heribert Vollmer

Brief Introduction to the Topic

Propositional satisfiability (or Boolean satisfiability) is the problem of determining whether the variables of a Boolean formula can be assigned truth values in such a way as to make the formula true. This satisfiability problem, SAT for short, stands at the crossroads of logic, graph theory, computer science, computer engineering and computational physics. Indeed, many problems originating from one of these fields typically have multiple translations to satisfiability. Unsurprisingly, SAT is of central importance in various areas of computer science including algorithmics, verification, planning, hardware design and artificial intelligence. It can express a wide range of combinatorial problems as well as many real-world ones.

SAT is very significant from a theoretical point of view. Since the Cook-Levin theorem, which identified SAT as the first **NP**-complete problem, it has become a reference for an enormous variety of complexity statements. The most prominent one is the question "is

P equal to **NP**?" Proving that SAT is not in **P** would answer this question negatively. Restrictions and generalizations of the propositional satisfiability problem play a similar rôle in the examination of other complexity classes and relations among them. In particular, quantified versions of SAT (QSAT, in which Boolean variables are universally or existentially quantified) as well as variants of SAT in which some notion of minimality is involved, provide prototypical complete problems for every level of the polynomial hierarchy.

During the past three decades, an impressive array of diverse techniques from mathematical fields, such as propositional and first-order logic, model theory, Boolean function theory, complexity, combinatorics and probability, has contributed to a better understanding of the SAT problem. Although significant progress has been made on several fronts, most of the central questions remain unsolved so far.

One of the main aims of the Dagstuhl seminar was to bring together researchers from different areas of activity in SAT so that they can communicate state-of-the-art advances and embark on a systematic interaction that will enhance the synergy between the different areas.

Concluding Remarks and Future Plans

The organizers regard the seminar as a great success. Bringing together researchers from different areas of theoretical computer science fostered valuable interactions and led to fruitful discussions. Feedback from the participants was very positive as well. Many attendants expressed their wish for a continuation.

Finally, the organizers wish to express their gratitude toward the Scientific Directorate of the Center for its support of this seminar, and hope to be able to continue this series of seminars on *SAT and Interactions* in the future.

2 Table of Contents

3 Organization of the Seminar and Activities

The seminar brought together 39 researchers with complementary expertise from different areas of theoretical computer science and mathematics, such as logic, complexity theory, algorithms and proof complexity. The participants consisted of both senior and junior researchers, including a number of postdocs and a few advanced graduate students.

Participants were invited to present their work and to communicate state-of-the-art advances. Twenty-three talks of various lengths took place over the five days of the seminar. Introductory and tutorial talks of 60 minutes, introducing one particular aspect of the satisfiability problem, were scheduled to open the first four days of the seminar. The rest of the days were filled mostly with shorter talks picking up the topic of the morning talk. The organizers considered it important to leave ample free time for discussion.

In this way, the following topics evolved:

1. Proof complexity
   - Sam Buss: Satisfiability Testing and Proof Complexity (Tutorial)
   - Barnaby Martin: Resolution and the Binary Encoding of Weak Pigeonhole Principles
   - Jakob Nordström: Supercritical Space-Width Trade-offs for Resolution
   - Jan Johannsen: On Linear Resolution – an Update
   - Ilario Bonacina: Strong Size Lower bounds in Regular Resolution via Games
2. Quantified Boolean Formulas: Solvers and Proof Complexity
   - Florian Lonsing: QBF Solving (Tutorial)
   - Marijn Heule: Practical Proof Systems for SAT and QBF
   - Meena Mahajan: QBF Proof Complexity (Tutorial)
   - Joshua Blinkhorn: On Soundness of QBF Calculi Parameterized by Dependency Schemes
   - Anil Shukla: Understanding Cutting Planes for QBFs
   - Leroy Chew: A Class of Hard Formulas for QBF Resolution
3. Exact Algorithms for SAT
   - Rahul Santhanam: Exact Algorithms for SAT – an Overview (Tutorial)
   - Dominik Scheder: The PPSZ Algorithm: Making Hertli's Analysis Simpler and 3-SAT Faster
   - Uwe Schöning: Classroom Analysis of Random Walk Algorithm for 3-SAT and Practical Extension to ProbSAT
   - Victor Lagerkvist: Partial Polymorphisms and the Time Complexity of SAT Problems
4. Knowledge Compilation
   - Stefan Mengel: An Introduction to Knowledge Compilation (Tutorial)
   - Florent Capelli: Compilation of CNF-formulas: Lower and Upper Bounds

There were additionally a few shorter talks covering further topics related to satisfiability.

- Jacobo Torán: Isomorphism of Solution Graphs
- Arne Meier, Irena Schindler: Approaching Backdoors in Two Non-Classical Logics
- Christoph Wintersteiger: Lifting SAT to Richer Theories: Bit-vectors, Finite Bases, and Theory Combination
- Oliver Kullmann: Look-ahead for Solving Hard SAT Problems
- Miki Hermann: Minimal Distance of Propositional Models
- John Franco: Adding Unsafe Constraints to Improve Satisfiability Performance (Redux)

Thursday afternoon was closed with an open problem session (see later in this report).

Wednesday afternoon was devoted to the usual hike. The day ended with a musical event that was highly appreciated by the seminar participants. The programme can be found in this report.

The above classification of topics and talks is necessarily rough, as several talks crossed the boundaries between these areas, in keeping with the theme of the seminar. The broad scope of the talks extended even to areas not anticipated by the organizers, such as dependence logic. The seminar thus achieved its aim of bringing together researchers from various related communities to share state-of-the-art research.

4 Overview of Talks

4.1 On Soundness in QBF Calculi Parameterized by Dependency Schemes

Joshua Blinkhorn (University of Leeds, GB)

Joint work of Olaf Beyersdorff, Joshua Blinkhorn
Main reference O. Beyersdorff, J. Blinkhorn, "Dependency Schemes in QBF Calculi: Semantics and Soundness", in Proc. of the 22nd Int'l Conf. Principles and Practice of Constraint Programming (CP'16), LNCS, Vol. 9892, pp. 96–112, Springer, 2016.
URL http://dx.doi.org/10.1007/978-3-319-44953-1_7

In the talk, we consider the parameterization of QBF resolution calculi by dependency schemes. One of the main problems in this area is to understand for which dependency schemes the resulting calculi are sound. It is known that a property called *full exhibition* is sufficient for soundness in Q-resolution [2]. We demonstrate that this approach generalizes to the dependency versions of all CDCL-based QBF calculi. Moreover, we show that the most important schemes in the literature possess this property; in particular, the reflexive resolution path dependency scheme is fully exhibited.

The talk also presents some new work, exposing similarities between the two currently disparate fields of QBF dependency schemes and dependency quantified Boolean formulas (DQBF). In particular, using results from [1] we show that the DQBF interpretation of dependency schemes leads to a complete characterisation of soundness for expansion-based QBF calculi. The new interpretation also provides a fresh insight for Q-resolution. We show that the phenomenon of incompleteness in the DQBF calculi, observed by [3], is directly related to the characterization of soundness for the dependency QBF systems.

References

1 Beyersdorff, O., Chew, L,. Schmidt, R. A., Suda, M.: Lifting QBF Resolution Calculi to DQBF. International Conference on Theory and Applications of Satisfiability Testing (SAT). pp. 490–499 (2016).
2 Slivovsky, F.: Structure in #SAT and QBF. Ph. D. Thesis, Vienna University of Technology (2015).
3 Balabanov, V., Chiang, H. K., Jiang, J. R.: Henkin quantifiers and Boolean formulae: A certification perspective of DQBF. Theoretical Computer Science 523, pp. 86–100 (2014).

4.2 Strong Size Lower Bounds in Regular Resolution via Games

Ilario Bonacina (KTH Royal Institute of Technology – Stockholm, SE)

Joint work of Ilario Bonacina, Navid Talebanfard
Main reference I. Bonacina, N. Talebanfard, "Strong ETH and Resolution via Games and the Multiplicity of Strategies", Algorithmica, pp. 1–13, Springer, 2016.
URL http://dx.doi.org/10.1007/s00453-016-0228-6

The Strong Exponential Time Hypothesis (SETH) says that solving the SAT problem on formulas that are k-CNFs in n variables requires running time $2^{n(1-c_k)}$, where c_k goes to 0 as k goes to infinity. Beck and Impagliazzo (2013) proved that regular resolution cannot disprove SETH; that is, there are unsatisfiable k-CNF formulas in n variables such that each regular resolution refutation has size at least $2^{n(1-c_k)}$, where c_k goes to 0 as k goes to infinity. We give a different/simpler proof of such a lower bound based on the known characterisations of width and size in resolution, and our technique indeed works for a proof system stronger than regular resolution. The problem of finding k-CNF formulas for which we can prove such strong size lower bounds in general resolution is still open.

4.3 SAT Solvers and Proof Complexity

Sam Buss (University of California – San Diego, US)

This talk is a survey about proof complexity and Satisfiability (SAT) solvers. We first cover the exponential time hypothesis (ETH) and the strong exponential time hypothesis (SETH), abstract proof systems, and the Frege and extended Frege proof systems. We then discuss different resolution proof systems including tree-like and regular, and their relationships with the SAT algorithms DPLL and CDCL as well as pool resolution and regWRTI. It concludes with a discussion of the D-RAT verification method and its relationship with extended resolution.

4.4 Compilation of CNF-formulas: Lower and Upper Bounds

Florent Capelli (University Paris-Diderot, FR)

Joint work of Simone Bova, Florent Capelli, Stefan Mengel, Friedrich Slivovsky
Main reference S. Bova, F. Capelli, S. Mengel, F. Slivovsky, "Knowledge Compilation Meets Communication Complexity", in Proc. of the 25th Int'l Joint Conf. on Art. Intelligence (IJCAI'16), pp. 1008–1014, AAAI Press, 2016.
URL http://www.ijcai.org/Abstract/16/147

In this talk, we review recent results obtained in collaboration with Simone Bova, Stefan Mengel and Friedrich Slivovsky on compilation of CNF-formulas. The aim of knowledge compilation in this case is to transform the input CNF-formula into a succinct data structure that can be queried efficiently to solve various problems such as decision, counting or enumeration.

We start by showing how we can use tools from communication complexity to prove that CNF-formulas cannot always be compiled into succinct DNNF, a family of restricted boolean circuits that will be presented in Stefan Mengel's talk. Our result does not rely on complexity hypotheses such as $\mathbf{P} \neq \mathbf{NP}$. Having established this negative result, we then explain how the structure of the formula can be used to compile it succinctly in many cases.

4.5 A Class of Hard Formulas for QBF Resolution

Leroy Chew (University of Leeds, GB)

Joint work of Leroy Chew, Olaf Beyersdorff, Mikolás Janota
Main reference O. Beyersdorff, L. Chew, M. Janota, "Proof Complexity of Resolution-based QBF Calculi", in Proc. of the 32nd Int'l Symposium on Theoretical Aspects of Computer Science (STACS'15), LIPIcs, Vol. 30, pp. 76–89, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2015.
URL http://dx.doi.org/10.4230/LIPIcs.STACS.2015.76

Proof systems for quantified Boolean formulas (QBFs) provide a theoretical underpinning for the performance of important QBF solvers. However, the proof complexity of these proof systems is currently not well understood and lower bound techniques in particular are missing. We show the hardness of the prominent formulas of Kleine Büning et al. [1] for the strong expansion-based calculus IR-calc. This, along with the strategy extraction technique, allows us to show all strict separations for the known QBF resolution calculi.

References

1 Kleine Büning, H., Karpinski, M., Flögel, A.: Resolution for Quantified Boolean Formulas. Information and Computation, Vol. 117(1), pp. 12–18 (1995).

4.6 Adding Unsafe Constraints to Improve the Performance of SAT Algorithms

John Franco (University of Cincinnati, US)

For many families of SAT formulas, the difficulty in solving an instance escalates exponentially with increasing instance size. A possible reason for this is that inferred contraints that reduce search space significantly are learned too late in the search to be effective. One attempt to control this is to add safe, uninformed constraints that are obtained from an analysis of the problem or the structure of the formula: symmetry breaking constraints, for example. This approach proves effective in some but not all cases. We propose an alternative approach which is to add unsafe, uninformed constraints early on to reduce search space breadth at shallow depth and then retract those constraints when the search breadth is still small and will not get much bigger as the search continues. By 'unsafe constraint' we mean a constraint that may eliminate one or more satisfying assignments – hence there is a risk that all assignments of a satisfiable instance may be eliminated.

We show, for example that in the case of formulas for solving van der Waerden number $W(2,6)$, adding unsafe constraints produces a bound that turns out to be $W(2,6)$. Knowledge of this bound and the conjecture that it was $W(2,6)$ was eventually used by Kouril to custom

design a solver that could prove definitively the value of $W(2,6)$. Notable is the fact that the unsafe constraints are obtained from an analysis of solutions to smaller instances of the van der Waerden family and not from an analysis of the structure of the formulas or problem properties.

4.7 Minimal Distance of Propositional Models

Miki Hermann (Ecole Polytechnique – Palaiseau, FR)

Joint work of Mike Behrisch, Miki Hermann, Stefan Mengel, Gernot Salzer
Main reference M. Behrisch, M. Hermann, S. Mengel, and G. Salzer, "Minimal Distance of Propositional Models", arXiv:1502.06761v1 [cs.CC], 2015.
URL https://arxiv.org/abs/1502.06761v1

We investigate the complexity of three optimisation problems in Boolean propositional logic related to information theory: Given a conjunctive formula over a set of relations, find a satisfying assignment with minimal Hamming distance to a given assignment that satisfies the formula (Next Other Solution, NOSol) or that does not need to satisfy it (Nearest Solution, NSol). The third problem asks for two satisfying assignments with a minimal Hamming distance among all such assignments (Minimal Solution Distance, MSD).

For all three problems we give complete classifications with respect to the relations admitted in the formula. We give polynomial time algorithms for several classes of constraint languages. For all other cases we prove hardness or completeness regarding APX, polyAPX, or equivalence to well-known hard optimisation problems.

4.8 Practical Proof Sytems for SAT and QBF

Marijn J. H. Heule (University of Texas – Austin, US)

Several proof systems have been proposed to verify results produced by satisfiability (SAT) and quantified Boolean formula (QBF) solvers. However, existing proof systems are not very suitable for validation purposes: It is either hard to express the actions of solvers in those systems or the resulting proofs are expensive to validate. We present two new proof systems (one for SAT and one for QBF) which facilitate validation of results in a time similar to proof discovery time. Proofs for SAT solvers can be produced by making only minor changes to existing conflict-driven clause-learning solvers and their preprocessors. For QBF, we show that all preprocessing techniques can be easily expressed using the rules of our proof system and that the corresponding proofs can be validated efficiently.

4.9 Linear Resolution – an Update

Jan Johannsen (LMU München, DE)

Joint work of Sam Buss, Jan Johannsen

Linear Resolution is a refinement of propositional resolution that is notoriously difficult to understand. We report on the state of our knowledge about its complexity, providing some new upper bounds and some structural properties of the system. In particular, we show that it is preserved under restrictions if and only if it is equivalent to full resolution.

4.10 Look-ahead for Solving Hard SAT Problems

Oliver Kullmann (University of Swansea, GB)

Joint work of Marijn J. H. Heule, Oliver Kullmann, Victor W. Marek

The boolean Pythagorean Triples problem has been a longstanding open problem in Ramsey Theory: Can the set $N = 1, 2, \ldots$ of natural numbers be divided into two parts, such that no part contains a triple (a, b, c) with $a^2+b^2 = c^2$? A prize for the solution was offered by Ronald Graham over two decades ago. We solve this problem, proving in fact the impossibility, by using the Cube-and-Conquer paradigm, a hybrid SAT method for hard problems, employing both look-ahead and CDCL solvers. An important role is played by dedicated look-ahead heuristics, which indeed allowed to solve the problem on a cluster with 800 cores in about 2 days. Due to the general interest in this mathematical problem, our result requires a formal proof. Exploiting recent progress in unsatisfiability proofs of SAT solvers, we produced and verified a proof in the DRAT format, which is almost 200 terabytes in size. From this we extracted and made available a compressed certificate of 68 gigabytes, that allows anyone to reconstruct the DRAT proof for checking.

4.11 Partial Polymorphisms and the Time Complexity of SAT Problems

Victor Lagerqvist (TU Dresden, DE)

Joint work of Peter Jonsson, Gustav Nordh, Magnus Wahlström, Bruno Zanuttini
Main reference P. Jonsson, V. Lagerkvist, G. Nordh, and B. Zanuttini, "Strong Partial Clones and the Time Complexity of SAT Problems", J. of Computer and System Sciences, Vol. 84, pp. 52–78, 2017.
URL http://dx.doi.org/10.1016/j.jcss.2016.07.008

The generalized SAT(S) problem is the computational decision problem of determining whether a conjunctive formula over the constraint language S is satisfiable. Even though all **NP**-complete SAT(S) problems are polynomial-time interreducible, there appears to be a vast difference in their worst-case time complexity. The question that we will concentrate on is how to explain this phenomenon using the language of universal algebra. For this purpose it is possible to associate each constraint language to a set of partial functions, so-called partial polymorphisms, satisfying certain closure properties. It has been proven that the

partial polymorphisms of a constraint language S determine the complexity of SAT(S) up to $O(c^n)$ time complexity, where n denotes the number of variables in a given instance. Unfortunately, the resulting theory is highly complex, and we will look at some unavoidable theoretical limitations of this approach. Despite this, non-trivial results can be obtained. We will give a brief survey of some of these results, and then look at how partial polymorphisms can be used to obtain kernelization procedures for SAT(S). In particular we will concentrate on SAT(S) problems admitting kernels with a linear number of constraints, and see how partial polymorphisms can be used to characterize such languages.

4.12 An Overview of QBF Reasoning Techniques

Florian Lonsing (TU Wien, AT)

We give an overview of techniques to solve quantified Boolean formulas (QBFs). At the beginning of QBF solving in the late 1990s, two main solving approaches emerged: backtracking search and expansion of variables. Backtracking search is a QBF-specific variant of the DPLL algorithm for propositional logic (SAT), called QDPLL. Variable expansion relies on the successive elimination of variables from a QBF until the formula reduces to true or false. Conflict-driven clause learning (CDCL) has been successfully adapted from SAT to QBF, resulting in the QCDCL algorithm. Analogously to resolution in CDCL, Q-resolution is the theoretical foundation of QCDCL. Unlike in SAT solving, where CDCL is the dominating approach, in QBF solving QCDCL is complemented by variable expansion. Modern implementations of expansion-based QBF solvers apply the principle of counterexample guided abstraction refinement (CEGAR). Recently, it has been shown that, from a proof complexity point of view, Q-resolution and expansion are orthogonal approaches. This theoretical result confirms related experimental observations and motivates further research in QBF proof complexity and its implications on the design of QBF solvers in practice.

4.13 QBF Proof Complexity – an Overview

Meena Mahajan (The Institute of Mathematical Sciences, India, IN)

How do we prove that a false QBF is indeed false? How big a proof is needed? The special case when all quantifiers are existential is the well-studied setting of propositional proof complexity. Expectedly, universal quantifiers change the game significantly. Several proof systems have been designed in the last couple of decades to handle QBFs, starting from the most basic Q-Resolution and Expansion+$\forall$-Reduction and going up to Frege+$\forall$-Reduction. Lower-bound paradigms from propositional proof complexity cannot always be extended – in most cases feasible interpolation and consequent transfer of circuit lower bounds works, but obtaining lower bounds on size by providing lower bounds on width fails dramatically. A new paradigm with no analogue in the propositional world has emerged in the form of strategy extraction, again allowing for transfer of circuit lower bounds. This talk will provide a broad overview of some of these developments.

4.14 Resolution and the Binary Encoding of Weak Pigeonhole Principles

Barnaby Martin (Durham University, GB) and Stefan Dantchev

We study the Resolution refutations of exponentially weak Pigeonhole Principles under both the normal and binary encodings of the stipulation that each pigeon must go in some hole. We prove that the minimal size of a Resolution refutation is $2^{\Omega(n/\log n)}$ in the binary encoding, contrasting with $2^{O(\sqrt{n \log n})}$ in the normal encoding. This is remarkable, since in tree-like Resolution the binary encoding is the easier to refute.

4.15 Approaching Backdoors in Two Non-Classical Logics

Arne Meier (Leibniz Universität Hannover, DE) and Irena Schindler (Leibniz Universität Hannover, DE)

Joint work of Johannes Fichte, Arne Meier, Sebastian Ordyniak, M. S. Ramanujan, Irena Schindler
Main reference J. K. Fichte, A. Meier, and I. Schindler, "Strong Backdoors for Default Logic", in Proc. of the 19th Int'l Conf. on Theory and Applications of Satisfiability Testing (SAT'16), LNCS, Vol. 9710, pp. 45–59, Springer, 2016.
URL http://dx.doi.org/10.1007/978-3-319-40970-2_4

In this talk, we investigate the applicability of the notion of backdoors to two non-classical logics: Reiter's propositional default logic and the global fragment of linear temporal logic. For default logic, we will see that backdoors have to incorporate the ternary character of reasoning in this logic. By a slight technical obstacle, called extended literals, we show that our provided notion is well-chosen. Then, we show parameterized complexity results for backdoor set detection and evaluation in default logic which yield upper bounds of FPT, paraNP, and paraDeltaP2. Concerning linear temporal logic, the definition of backdoors here requires the incorporation of consistency of assignments. In the next step, we will see that the parameterized complexity of backdoor set evaluation behaves rather unsatisfactorily: most fragments are intractable. However, we identify a novel tractable fragment of LTL which is expressive enough to express 'safety' properties of a reactive system. The problem of backdoor set detection stays in all investigated cases fixed-parameter tractable.

4.16 An Introduction to Knowledge Compilation

Stefan Mengel (Artois University – Lens, FR)

In this talk we will give an introduction to knowledge compilation. We will give motivations, show how conditional lower bounds are shown and present some representations used in practical knowledge compilation and the knowledge compilation map. Throughout the talk we will present open questions and current challenges in the field.

4.17 Supercritical Space-Width Trade-offs for Resolution

Jakob Nordström (KTH Royal Institute of Technology – Stockholm, SE)

Joint work of Christoph Berkholz, Jakob Nordström

We show that there are CNF formulas which can be refuted in resolution in both small space and small width, but for which any small-width resolution proof must have space exceeding by far the linear worst-case upper bound. This significantly strengthens the space-width trade-offs in [Ben-Sasson '09], and provides one more example of trade-offs in the 'supercritical' regime above worst case recently identified by [Razborov '16]. We obtain our results by using Razborov's new hardness condensation technique and combining it with the space lower bounds in [Ben-Sasson and Nordström '08]. This is joint work with Christoph Berkholz.

4.18 Exact Algorithms for Satisfiability – an Overview

Rahul Santhanam (University of Oxford, GB)

We survey recent work on exact algorithms for Satisfiability, as well as popular hardness hypotheses such as the Exponential-Time Hypothesis and its variants.

4.19 The PPSZ Algorithm: Making Hertli's Analysis Simpler and 3-SAT Faster

Dominik Scheder (Shanghai Jiao Tong University, CN)

Joint work of Dominik Scheder, John Steinberger

The currently fastest known algorithm for k-SAT is PPSZ, named after its inventors Paturi, Pudlak, Saks, and Zane. It is simple to state but challenging to analyse. Paturi et al. give an elegant analysis for Unique-k-SAT, i.e., the case where the input formula has a unique satisfying assignment. Their analysis for the general case of multiple satisfying assignments is difficult and incurs an exponential loss in running time. In a breakthrough result in 2011, Timon Hertli showed that the Unique-k-SAT bound holds in the general case, too. His proof, though ingenious, is quite difficult and technical.

In this work we achieve two goals. Firstly, we greatly simplify Hertli's analysis, also making clear why it works and why simpler approaches are most likely bound to fail. We replace Hertli's involved inductive proof by one that uses basic tools from information complexity and simple coupling arguments.

Secondly, a simple consequence of our analysis is that if you can improve the PPSZ algorithm for Unique-k-SAT, then you can improve it for general k-SAT.

Combining this with a result by Hertli from 2014, in which he gives an algorithm for Unique-3-SAT slightly beating PPSZ, we obtain an algorithm beating PPSZ for general 3-SAT, thus obtaining the so far best known worst-case bounds for 3-SAT.

4.20 A Classroom Proof of the Random Walk 3-SAT Algorithm and its Practical Extension to ProbSAT

Uwe Schöning (Universität Ulm, DE)

The random walk 3-SAT algorithm (FOCS 99) has become part of textbooks and is taught in many classrooms. The purpose of this talk is to present an easier analysis of the algorithm. It is based on the fact that $P(X \leq a \cdot n)$ is equal to $[(\frac{p}{a})^a(\frac{1-p}{1-a})^{1-a}]^n$, up to polynomial factors. Here, X is a binomially distributed random variable with parameters n and p. Now let X be $\mathrm{Bin}(n, 1/2)$, and let Y be $\mathrm{Bin}(n, 2/3)$. The random walk algorithm randomly guesses an initial assignment, and then, it performs n random walk steps by selecting a clause not being satisfied under the current assignment and flipping the value of a randomly selected literal in this clause. The success probability of this algorithm (in case of a satisfiable input formula) can be lower bounded by $P(X \leq 1/3) \cdot P(Y \leq 1/3)$ which is, by the above equality, $(3/4)^n$. The algorithm was extended to ProbSAT (with Adrian Balint) for to participate in (and win) the SAT competition. For this purpose the flip probability distribution $(1/3, 1/3, 1/3)$ regarding the selected clause $\{x, y, z\}$ had to be changed to be proportional to $(f(x), f(y), f(z))$ where the function $f(x)$ is defined in terms of make(x) and break(x). By experiments it turns out that the make-value can be completely ignored, so that, in the case of 3-SAT, $f(x) = 2.5^{-\mathrm{break}(x)}$ is a good choice.

4.21 Understanding Cutting Planes for QBF

Anil Shukla (The Institute of Mathematical Sciences, India, IN)

Joint work of Olaf Beyersdorff, Leroy Chew, Meena Mahajan, Anil Shukla

We define a new complete and sound cutting plane proof system for false quantified Boolean formulas. We analyse the proof-theoretic strength of the new system. We show that it can p-simulate QU-resolution (and therefore Q-resolution), and indeed is exponentially stronger than these systems. However, it is incomparable (under a natural circuit complexity assumption) to even the core expansion-based QBF proof systems. On the other hand, we show that it is exponentially weaker than the QBF proof system based on Frege (introduced by Beyersdorff et al. ITCS'16). We also establish two lower bound techniques for our new system: strategy extraction and feasible interpolation.

4.22 Isomorphism of Solution Graphs.

Jacobo Torán (Universität Ulm, DE) and Patrick Scharpfenecker

Main reference P. Scharpfenecker, J. Torán, "Solution Graphs of Boolean Formulas and Isomorphism", in Proc. of the 19th Int'l Conf. on Theory and Applications of Satisfiability Testing (SAT'16), LNCS, Vol. 9710, pp. 29–44, Springer, 2016.
URL http://dx.doi.org/10.1007/10.1007/978-3-319-40970-2_3

The solution graph of a Boolean formula on n variables is the subgraph of the hypercube H_n induced by the satisfying assignments of the formula. The structure of solution graphs has been the object of much research in recent years, since it is important for the performance of SAT-solving procedures based on local search. In this talk we concentrate on the complexity of the isomorphism problem of solution graphs of Boolean formulas and on how this complexity depends on the formula type. We observe that for general formulas the solution graph isomorphism problem can be solved in exponential time while in the cases of 2-CNF formulas as well as for CPSS formulas, the problem is in the counting complexity class $\mathbf{C}_{=}\mathbf{P}$, a subclass of **PSPACE**. In addition we prove that for 2-CNF as well as for CPSS formulas the solution graph isomorphism problem is hard for $\mathbf{C}_{=}\mathbf{P}$ under polynomial time many one reductions, thus matching the given upper bound.

4.23 Lifting SAT to Richer Theories: Bit-vectors, Finite Bases and Theory Combination

Christoph M. Wintersteiger (Microsoft Research UK – Cambridge, GB)

In this talk we take a look at lifting SAT solver technology up to higher levels of abstraction and complexity in the form of Satisfiability Modulo Theories (SMT) problems. After an overview of current conceptual work and abstract solver frameworks in the area, we discuss the example of a recently developed bit-vector solver based on the model-construction satisfiability calculus (mcSAT) and how it interfaces with other theories and solvers. Finally, we touch upon future work and open problems in this area.

5 Open problems

We give a brief account of the open problem session, and describe each of the four contributions in turn.

Meena Mahajan

This open problem relates to hardness measures for resolution proofs. Given a tree-like resolution proof, and an internal node u, let $f(u)$ denote the minimum, over all parents v of u, of the width of the clause at node v. The asymmetric width $\mathrm{width}(\pi)$ of a resolution proof π is the maximum $f(u)$ over all internal nodes u of π. It is shown in [1] that

$$\mathrm{width}(F \vdash \emptyset) \leq \mathrm{awidth}(F \vdash \emptyset) + \max\{\mathrm{awidth}(F \vdash \emptyset), \mathrm{width}(F)\} - 1\,,$$

shaving +1 off the upper bound given by [2]. It remains open whether the following upper bound holds:

$$\text{width}(F \vdash \emptyset) \leq \text{awidth}(F \vdash \emptyset) + \text{width}(F) - 1\,.$$

The relation was originally conjectured in [3].

References

1 Krebs, A., Mahajan, M., Shukla, A.: Relating Two Width Measures for Resolution Proofs. Electronic Colloquium on Computational Complexity (ECCC) (2016).
2 Beyersdorff, O., Kullmann, O.: Unified Characterisations of Resolution Hardness Measures. International Conference on Theory and Applications of Satisfiability Testing (SAT), pp. 170–187. Springer (2014).
3 Beyersdorff, O., Kullmann, O.: Hardness Measures and Resolution Lower Bounds. Computing Research Repository (CoRR) (2014).

Nicola Galesi

Cutting Planes (CP) is a refutational calculus for propositional CNF formulas. The space complexity of a proof, roughly speaking, can be viewed as the amount of memory required to produce the proof.

A *memory configuration* M is a set of linear inqualities. A CP proof of I from F is a sequence $M_0, \ldots, M_k$ of memory configurations, satisfying (1) M_0 is empty, (2) $I \in M_k$, and (3) M_{i+1} is obtained from M_i by an axiom download, by inference, or by erasure. The *inequality space* of a CP refutation Π is the maximum size of memory configuration in Π.

It was shown in [1] that every unsatisfiable CNF has a CP refutation with inequality space ≤ 5, but the proof uses coefficients of exponential size. This leads naturally to the following open problem: Can every unsatisfiable CNF be refuted in CP in constant inequality space, if the coeffecients are polynomially bounded?

The next open problem concerns locality lemmas. The Locality Lemma for resolution, whose proof is trivial, states that, for any partial assignment α satisfying F, there exists a partial assignment $\alpha' \subseteq \alpha$ satisfying F such that $|\alpha'|$ is less than the space of F. A version of the Locality Lemma exists for the polynomial calculus [2, 3], and can be stated as follows. Let P be a set of polynomials, and let M be a disjoint 2-CNF with $M \vDash P$. Then there exists another disjoint 2-CNF M' such that (1) $M' \subseteq M$, (2) $M' \vDash P$, and (3) $|M'| \leq 4 \cdot \text{Sp}(P)$. We arrive at the second open problem: If we interpret P instead as a set of configurations, can we prove a version of the Locality Lemma for CP?

References

1 Galesi, N., Pudlák, P., Thapen, N.: The Space Complexity of Cutting Planes Refutations. Conference on Computational Complexity (CCC), pp. 433–447, LIPIcs (2015).
2 Alekhnovich, M., Ben-Sasson, E., Razborov, A. A., Wigderson, A.: Space Complexity in Propositional Calculus. Symposium on Theory of Computing (STOC), pp. 358–367 (2000).
3 Bonacina, I., Galesi, N.: Pseudo-partitions, Transversality and Locality: A Combinatorial Characterisation for the Space Measure in Algebraic Proof Systems. Innovations in Theoretical Computer Science (ITCS), pp. 455–472 (2013).

Oliver Kullmann

Both open problems concern the class SED of Boolean clause sets. The deficiency $\delta(F) \in \mathbb{Z}$ of a Boolean clause set F is equal to the number of clauses minus the number of variables.

The first open problem asks, simply, what is the decision complexity of SED? For the second open problem, let $\deg_F(v)$ be equal to the number of clauses in F containing variable v, and let $\mathrm{nM}(k)$ be the k^{th} non-Mersenne number. It was stated that, for a Boolean clause set $F \in \mathrm{SED}$, if $\delta(F) \geq 1$ and $\deg_F(v) \geq \mathrm{nM}(\delta(F))$ for every variable v in F, then F is satisfiable. The open problem asks whether, under these circumstances, an assignment for F can be found in polynomial time.

Stefan Mengel

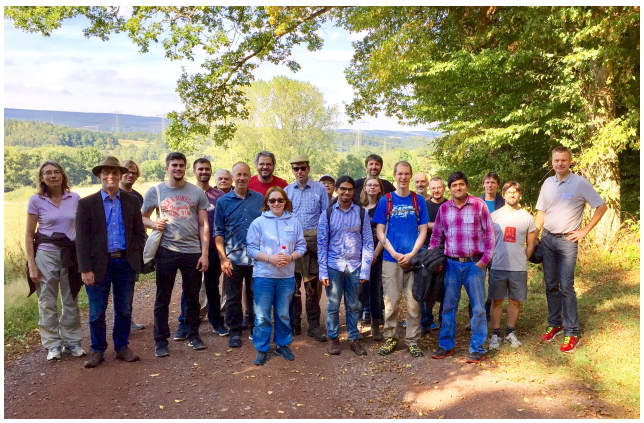
Let f be the function that maps an arbitrary collection Φ of n propositional CNF formulas $\phi_1, \ldots, \phi_n$ to a string of bits $a_1 \cdots a_n$, such that $a_i = 1$ if ϕ_i is satisfiable, and $a_i = 0$ otherwise. Can f be computed in polynomial time with $o(n)$ calls to a SAT-solver? It was noted by several participants that this topic bears a close relationship to the computation of maximal autarkies.

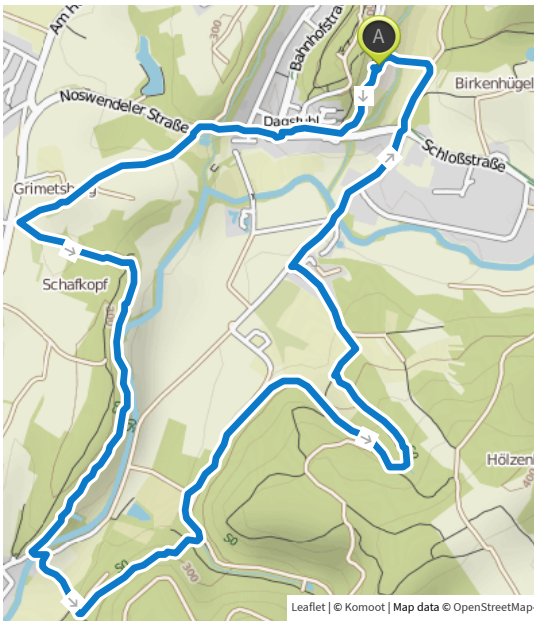
6 Social Activities

6.1 Hike

Arne Meier (Leibniz Universität Hannover, DE)

On Wednesday at 13:45 p.m., twenty-one of the seminar participants enjoyed the great weather and friendly atmosphere during the hike. The group walked a circular route of 9.6 *km* in the direction of hill *Schafkopf*, crossed the stream *Prims*, passed the rise *junger Hirschkopf* on roughly our half-way point and reached after a long curve at *Buttnicher Straße* to eventually finish back at *Schloss Dagstuhl*. The net walking time was two hours and 22 minutes and we had an elevation gain of 140 *m*. However, we were not in a hurry. Including breaks we arrived back at approximately 16:00 p.m. – perfectly timed to enjoy the deserved cake!





6.2 Musical Evening

Joshua Blinkhorn (University of Leeds, UK)

On Wednesday evening, beginning at 8:00 p.m., all seminar participants were welcome to attend the musical evening, which took place in the castle's music room. Prior to the event, any and all participants with musical tendencies were invited to contribute a performance to the programme, either as a solo act, or – in the spirit of collaboration – as a group.

In total, seven musicians took to the stage in an eclectic collection of performances, presenting music from the Baroque and Classical eras, some well-known jazz standards, and a handful of popular songs and instrumental pieces. Making use of the instruments and sheet music provided at Dagtuhl, the concert hosted several solo performances, featured an instrumental duo, and was closed by a jazz quartet.

Being a well-attended event, the hour-or-so of music was well-received by the audience, with warm applause for each contribution. The evening was organized and compèred by Jan Johannsen (LMU München). The programme is reproduced below.

Johannes Schmidt (piano)	Goldberg Variation (J. S. Bach) Türkischer Marsch (Mozart)
Dominic Scheder (piano) and Ilario Bonacina (flute)	Suite for Flute and Piano (J. S. Bach) Vieilles Danses (B. Bartók)
Jacobo Torán (guitar)	Milonga (J. Buscaglia)
Florent Capelli (guitar and voice)	La Javanaise (S. Gainsbourg) Paris 42 (L. Aragon, L. Leonardi)

Joshua Blinkhorn (guitar and voice)	Kid Charlemagne (W. Becker, D. Fagen)
Joshua Blinkhorn (guitar), Florent Capelli (voice), Jan Johannsen (saxophone) and Dominik Scheder (piano)	Summertime (G. Gershwin) Watermelon Man (H. Hancock)

Participants

- Olaf Beyersdorff
University of Leeds, GB
- Joshua Blinkhorn
University of Leeds, GB
- Ilario Bonacina
KTH Royal Institute of Technology – Stockholm, SE
- Sam Buss
University of California – San Diego, US
- Florent Capelli
University Paris-Diderot, FR
- Leroy Chew
University of Leeds, GB
- Nadia Creignou
Aix-Marseille University, FR
- Arnaud Durand
University Paris-Diderot, FR
- Uwe Egly
TU Wien, AT
- Shiguang Feng
Universität Leipzig, DE
- John Franco
University of Cincinnati, US
- Nicola Galesi
Sapienza University of Rome, IT
- Anselm Haak
Leibniz Universität Hannover, DE
- Miki Hermann
Ecole Polytechnique – Palaiseau, FR
- Marijn J. H. Heule
University of Texas – Austin, US
- Edward A. Hirsch
Steklov Institute – St. Petersburg, RU
- Kazuo Iwama
Kyoto University, JP
- Jan Johannsen
LMU München, DE
- Peter Jonsson
Linköping University, SE
- Oliver Kullmann
Swansea University, GB
- Victor Lagerqvist
TU Dresden, DE
- Florian Lonsing
TU Wien, AT
- Meena Mahajan
The Institute of Mathematical Sciences, India, IN
- Barnaby Martin
Durham University, GB
- Arne Meier
Leibniz Universität Hannover, DE
- Stefan Mengel
Artois University – Lens, FR
- Jakob Nordström
KTH Royal Institute of Technology – Stockholm, SE
- Steffen Reith
Hochschule RheinMain, DE
- Rahul Santhanam
University of Oxford, GB
- Dominik Scheder
Shanghai Jiao Tong University, CN
- Irena Schindler
Leibniz Universität Hannover, DE
- Johannes Schmidt
Jönköping University, SE
- Uwe Schöning
Universität Ulm, DE
- Anil Shukla
The Institute of Mathematical Sciences, India, IN
- Sarah Sigley
University of Leeds, GB
- Stefan Szeider
TU Wien, AT
- Jacobo Torán
Universität Ulm, DE
- Heribert Vollmer
Leibniz Universität Hannover, DE
- Christoph M. Wintersteiger
Microsoft Research UK – Cambridge, GB