Report from Dagstuhl Seminar 20061

SAT and Interactions

Edited by

Olaf Beyersdorff[1], Uwe Egly[2], Meena Mahajan[3], and Cláudia Nalon[4]

1 **Universität Jena, DE,** olaf.beyersdorff@uni-jena.de
2 **TU Wien, AT,** uwe.egly@tuwien.ac.at
3 **Institute of Mathematical Sciences – Chennai, IN,** meena@imsc.res.in
4 **University of Brasilia, BR,** nalon@unb.br

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 20061 "SAT and Interactions". The seminar brought together theoreticians and practitioners from the areas of proof complexity and proof theory, SAT and QBF solving, MaxSAT, and modal logics, who discussed recent developments in their fields and embarked on an interdisciplinary exchange of ideas and techniques between these neighbouring subfields of SAT.

Seminar February 2–7, 2020 – http://www.dagstuhl.de/20061
2012 ACM Subject Classification Theory of computation → Proof theory, Theory of computation → Modal and temporal logics, Theory of computation → Automated reasoning, Theory of computation → Description logics, Theory of computation → Proof complexity, Theory of computation → Complexity theory and logic
Keywords and phrases SAT, MaxSAT, QBF, proof complexity, deep inference, modal logic, solving
Digital Object Identifier 10.4230/DagRep.10.2.1
Edited in cooperation with Joshua Lewis Blinkhorn

1 Executive Summary

Olaf Beyersdorff
Uwe Egly
Meena Mahajan
Cláudia Nalon

The problem of deciding whether a propositional formula is satisfiable (SAT) is one of the most fundamental problems in computer science, both theoretically and practically. 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: one of seven million-dollar Clay Millennium Problems. Due to its NP hardness, SAT has been classically perceived as an intractable problem, and indeed, unless $\mathsf{P} = \mathsf{NP}$, no polynomial-time algorithm for SAT exists.

There are many generalisations of the SAT problem to further logics, including quantified Boolean formulas (QBFs) and modal and temporal logics. These logics present even harder satisfiability problems as they are associated with complexity classes such as PSPACE, which encompasses NP. However, QBFs, modal and temporal logics can express many practically relevant problems far more succinctly, thus applying to more real-world problems from artificial intelligence, bioinformatics, verification, and planning.

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

Very often, these developments take place within different communities, e.g., there has been almost no interaction between the areas of SAT/QBF solving and solving for modal logics.

The main aim of the proposed Dagstuhl Seminar therefore was to bring together researchers from proof complexity and proof theory, SAT, MaxSAT and QBF solving, and modal logics 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. As such the seminar was the first workshop (in Dagstuhl and elsewhere) to unite researchers working on both theory and practice of propositional SAT, QBF, and modal logics. One of the specific aims was to foster more interaction between these different communities with the goal to transfer the success of theoretical research on SAT to further logics and SAT problems.

To facilitate such interactions, 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 during the seminar:

- Massimo Lauria: Proof Complexity: A Survey,
- Lutz Straßburger: Introduction to Deep Inference,
- Vijay Ganesh: Machine Learning and Logic Solvers: The Next Frontier,
- Mikoláš Janota: QBF Solving and Calculi: An Overview,
- João Marques-Silva: Practical MaxSAT Solving: A Survey,
- Cláudia Nalon: Modal Logics: An Overview.

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 discussion session on ‘Future Directions of Research’, where ideas for a closer interaction between theoretical fields such as proof theory and proof complexity and practical fields such as SAT/QBF and modal solving were discussed.

The organisers believe that the seminar fulfilled their original high goals: most talks were a great success and 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

Future Directions of Research

3 Overview of Talks

3.1 Hardness Characterisations and Size-Width in QBF Resolution

Joshua Lewis Blinkhorn (Universität Jena, DE), Olaf Beyersdorff (Universität Jena, DE), and Meena Mahajan (Institute of Mathematical Sciences – Chennai, IN)

Main reference Olaf Beyersdorff, Joshua Blinkhorn, Meena Mahajan: "Hardness Characterisations and Size-Width Lower Bounds for QBF Resolution", in Proc. of the 35th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS '20, p. 209–223, Association for Computing Machinery, 2020.
URL https://doi.org/10.1145/3373718.3394793

We provide a tight characterisation of proof size in resolution for quantified Boolean formulas (QBF) by circuit complexity. Such a characterisation was previously obtained for a hierarchy of QBF Frege systems [1], but leaving open the most important case of QBF resolution. Different from the Frege case, our characterisation uses a new version of decision lists as its circuit model, which is stronger than the CNFs the system works with. Our decision list model is well suited to compute countermodels for QBFs. Our characterisation works for both Q-Resolution and QU-Resolution, which we show to be polynomially equivalent for QBFs of bounded quantifier alternation.

Using our characterisation we obtain a size-width relation for QBF resolution in the spirit of the celebrated result for propositional resolution [2]. However, our result is not just a replication of the propositional relation – intriguingly ruled out for QBF in previous research [3] – but shows a different dependence between size, width, and quantifier complexity.

References

1 O. Beyersdorff and J. Pich. Understanding Gentzen and Frege systems for QBF. In: *Symposium on Logic in Computer Science* (*LiCS*), pp. 146–155, ACM, 2016.

2 E. Ben-Sasson and A. Wigderson. Short proofs are narrow – resolution made simple. *Journal of the ACM*, 48(2):149–169, 2001.

3 O. Beyersdorff, L. Chew, M. Mahajan, and A. Shukla. Are short proofs narrow? QBF resolution is *not* so simple. *ACM Transactions on Computational Logic*, 19(1):1–26, 2018.

3.2 Tractable QBF via Knowledge Compilation

Florent Capelli (Lille I University, FR)

Joint work of Florent Capelli, Stefan Mengel

We show how knowledge compilation can be used as a tool for solving QBF and more. More precisely, we show that one can apply quantification on certain data structures used in knowledge compilation which in combination with the fact that restricted classes of CNF-formulas can be compiled into these data structures can be used to show fixed-parameter tractable results for QBF. In particular, we rediscover a result by Hubie Chen [1] on FPT-tractability of QBF on bounded treewidth CNF and generalise it to aggregation problems such as counting or enumerating the models of the input quantified CNF.

References

1 H. Chen. Quantified constraint satisfaction and bounded treewidth. In: *European Conference on Artificial Intelligence* (*ECAI*), pp. 161–165, IOS Press, 2004.

3.3 The Equivalences of Refutational QRAT

Leroy Nicholas Chew (Carnegie Mellon University – Pittsburgh, US) and Judith Clymo (University of Leeds, GB)

The solving of Quantified Boolean Formulas (QBF) has been advanced considerably in the last two decades. In response to this, several proof systems have been put forward to universally verify QBF solvers. QRAT by Heule et al. is one such example of this and builds on technology from DRAT, a checking format used in propositional logic. Recent advances have shown conditional optimality results for QBF systems that use extension variables. Since QRAT can simulate Extended Q-Resolution, we know it is strong, but we do not know if QRAT has the strategy extraction property as Extended Q-Resolution does. In this paper, we partially answer this question by showing that a simple restriction on the reduction rule in QRAT is enough to show it has strategy extraction (and consequentially is equivalent to Extended Q-Resolution modulo NP). We also extend equivalence to another system, as we show an augmented version of QRAT known as QRAT+, developed by Lonsing and Egly, is in fact equivalent to the basic QRAT. We achieve this by constructing a line-wise simulation of QRAT+ using only steps valid in QRAT.

3.4 How QBF Expansion Makes Strategy Extraction Hard

Judith Clymo (University of Leeds, GB) and Leroy Nicholas Chew (Carnegie Mellon University – Pittsburgh, US)

Main reference Leroy Chew, Judith Clymo: “How QBF Expansion Makes Strategy Extraction Hard”, Electronic Colloquium on Computational Complexity (ECCC), Vol. 26, p. 157, 2019.
URL https://eccc.weizmann.ac.il/report/2019/157

In this talk we show that the QBF proof checking format QRAT (Quantified Resolution Asymmetric Tautologies) by Heule, Biere and Seidl cannot have polynomial-time strategy extraction unless P=PSPACE. In our proof, the crucial property that makes strategy extraction PSPACE-hard for this proof format is universal expansion, even expansion on a single variable.

While expansion reasoning used in other QBF calculi can admit polynomial time strategy extraction, we find this is conditional on a property studied in proof complexity theory. We show that strategy extraction on expansion based systems can only happen when the underlying propositional calculus has the property of feasible interpolation.

3.5 From QBFs to MALL and Back via Focussing

Anupam Das (University of Birmingham, GB)

In this work we investigate how to extract alternating time bounds from "focussed" proof systems. Our main result is the obtention of fragments of MALLw (MALL with weakening) complete for each level of the polynomial hierarchy. In one direction we encode QBF satisfiability and in the other we encode focussed proof search, and we show that the composition of the two encodings preserves quantifier alternation, yielding the required result. By carefully composing with well-known embeddings of MALLw into MALL, we obtain a similar delineation of MALL formulas, again carving out fragments complete for each level of the polynomial hierarchy. This refines the well-known results that both MALLw and MALL are PSPACE-complete.

A key insight is that we have to refine the usual presentation of focussing to account for deterministic computations in proof search, which correspond to invertible rules that do not branch. This is so that we may more faithfully associate phases of focussed proof search to their alternating time complexity. This presentation seems to uncover further dualities at the level of proof search than usual presentations, so could be of further proof theoretic interest in its own right.

3.6 Consistent Query Answering via SAT Solving

Akhil Dixit (University of California – Santa Cruz, US)

Consistent Query Answering is a rigorous and principled approach to the semantics of queries posed against inconsistent databases, i.e., the databases that violate one or more integrity constraints set over its schema. Computing the consistent answers to a fixed conjunctive query on a given inconsistent database can be a coNP-hard problem, even though every fixed conjunctive query is efficiently computable on a given consistent database. In this talk, we will first introduce some database problems, their connections to SAT, and some recent theoretical results in the literature. In the later half, we will present CAvSAT (Consistent Answers via SAT), our SAT-based system for consistent query answering.

3.7 Clausal Resolution for Temporal Logics

Clare Dixon (University of Liverpool, GB)

Joint work of Michael Fisher, Clare Dixon, Martin Peim
Main reference Michael Fisher, Clare Dixon, Martin Peim: "Clausal Temporal Resolution", ACM Trans. Comput. Logic, Vol. 2(1), p. 12–56, Association for Computing Machinery, 2001.
URL https://doi.org/10.1145/371282.371311

A clausal temporal resolution calculus has been developed [1] and implemented [2] for linear-time temporal logics (LTL). This involves translation to a clausal normal form, resolution rules that apply to formulae holding at the same time moment and a loop resolution rule that applies across time moments. This approach has been extended to other temporal (and modal [6, 5]) logics such as the branching time temporal logic CTL [7] and first-order temporal logic [3, 4]. We discuss the main elements of this approach applied to LTL and its extensions to other non-classical logics.

References

1 M. Fisher, C. Dixon, and M. Peim. Clausal temporal resolution. *ACM Transactions on Computational Logic*, 2(1):12–56, 2001.

2 U. Hustadt and Boris Konev. TRP++ 2.0: A temporal resolution prover. In: *Conference on Automated Deduction* (*CADE*), pp. 274–278. Springer, 2003.

3 B. Konev, A. Degtyarev, C. Dixon, M. Fisher, and U. Hustadt. Mechanising first-order temporal resolution. *Information and Computation*, 199(1-2):55–86, 2005.

4 M. Ludwig and U. Hustadt. Implementing a fair monodic temporal prover. *AI Communications*, 23(2-3):68–96, 2010.

5 C. Nalon, U. Hustadt, and C. Dixon. KSP: A resolution-based theorem prover for K_n: architecture, refinements, strategies and experiments. *Journal of Automated Reasoning*, 64(3):461–484, 2020.

6 Cláudia Nalon, Clare Dixon, and Ullrich Hustadt. Modal resolution: proofs, layers, and refinements. *ACM Transactions on Computational Logic*, 20(4):23:1–23:38, 2019.

7 L. Zhang, U. Hustadt, and C. Dixon. A resolution calculus for the branching-time temporal logic CTL. *ACM Transactions on Computational Logic*, 15(1):1529–3785, 2014.

3.8 Machine Learning and Logic Solving: the Next Frontier

Vijay Ganesh (University of Waterloo, CA)

Over the last two decades, software engineering has witnessed a silent revolution in the form of Boolean SAT solvers. These solvers are now integral to many analysis, synthesis, verification, and testing approaches. This is largely due to a dramatic improvement in the scalability of these solvers vis-a-vis large real-world formulas. What is surprising is that the Boolean satisfiability problem is NP-complete, believed to be intractable in general, and yet these solvers easily solve instances containing millions of variables and clauses in them. How can that be?

In my talk, I will address this question of why SAT solvers are so efficient through the lens of machine learning as well as ideas from (parameterized) proof complexity. I will argue that SAT solvers are best viewed as proof systems, composed of prediction engines that optimize some metric correlated with solver running time. These prediction engines can be built using ML techniques, whose aim is to structure solver proofs in an optimal way. Thus, two major paradigms of AI, namely machine learning and logical deduction, are brought together in a principled way to design efficient SAT solvers. A result of my research is the MapleSAT solver, that has been the winner of several recent international SAT competitions, and is now widely used in industry and academia.

3.9 Semi-Algebraic Proofs, IPS Lower Bounds and the τ-Conjecture: Can a Natural Number be Negative?

Edward A. Hirsch (Steklov Institute – St. Petersburg, RU)

Joint work of Yaroslav Alekseev, Dima Grigoriev, Edward A. Hirsch, Iddo Tzameret
Main reference Yaroslav Alekseev, Dima Grigoriev, Edward A. Hirsch, Iddo Tzameret: "Semi-Algebraic Proofs, IPS Lower Bounds, and the τ-Conjecture: Can a Natural Number Be Negative?", in Proc. of the 52nd Annual ACM SIGACT Symposium on Theory of Computing, STOC 2020, p. 54–67, Association for Computing Machinery, 2020.
URL https://doi.org/10.1145/3357713.3384245

We show that the equivalence between algebraic and semialgebraic proofs represented by circuits is tightly connected to refuting the bit value principle (BVP): $\sum x_i 2^i = -1$. We relate the complexity of BVP to previously known conjectures in algebraic complexity.

3.10 Benchmarking Modal Logic Theorem Provers

Ullrich Hustadt (University of Liverpool, GB)

Modal logics are extensions of propositional and first-order logic with operators that are not truth-functional. The contemporary era of modal logics started in the late 50s and development of theorem provers started in earnest in the late 80s. Since then there has been an interest in the evaluation of the practical performance of such provers. I will discuss some of the approaches that have been used for such evaluations over the past thirty years.

3.11 QBF Solving and Calculi: An Overview

Mikoláš Janota (IST – Lisbon, PT)

Quantified Boolean Formulas (QBFs) enrich the SAT problem with quantifiers taking the problem from NP to PSPACE. Recent years have seen a number of novel approaches to QBF solving. At the same time, QBF calculi were developed to match the solvers. However, there are calculi with no solving counterparts.

In this talk I will overview the two prominent paradigms in QBF solving: conflict-driven and expansion-based. I will also discuss the connection between solving and the existing proof systems as well as challenges for future research.

3.12 Simplified and Improved Separation Between Regular and General Resolution by Lifting

Jan Johannsen (LMU München, DE)

Joint work of Marc Vinyals, Jan Elffers, Jan Johannsen, Jakob Nordström
Main reference Marc Vinyals, Jan Elffers, Jan Johannsen, Jakob Nordström: "Simplified and improved separations between regular and general resolution by lifting". 2020 (submitted for publication).

We give a significantly simplified proof of the exponential separation between regular and general resolution of Alekhnovich et al. (2007) as a general theorem lifting proof depth to regular proof length in resolution. This simpler proof then allows us to strengthen the separation further, and to construct families of theoretically very easy benchmarks that are surprisingly hard for SAT solvers in practice.

3.13 Proof Complexity: A Survey

Massimo Lauria (Sapienza University of Rome, IT)

Running a SAT solver on an UNSAT formula produces (implicitly or explicitly) a proof that the formula is unsatisfiable, usually expressible in an established formal language called a proof system. This observation leads to study SAT solving methods by looking at the generated proofs. That is, if an UNSAT formula has no short proof in a given proof system, the corresponding SAT solvers cannot solve the formula efficiently.

We introduce the area and the methods of proof complexity, that studies the length and the structure of proofs of UNSAT. In particular we define and discuss Resolution, Polynomial Calculus, Cutting Planes and DRAT/Extended Resolution, which are the most relevant proof systems for current SAT solver technology.

Since a SAT solver's goal is, among other things, to look for proofs as short as possible, we briefly discuss the complexity of efficiently finding such short proofs.

3.14 Practical MaxSAT Solving: A Survey

João Marques-Silva (University of Toulouse, FR)

This talk presents an overview of practical algorithms for maximum satisfiability (MaxSAT) solving, highlighting the algorithms that are most effective in practice.

3.15 Revisiting Graph Width Measures for CNF-Encodings

Stefan Mengel (CNRS, CRIL – Lens FR)

We consider bounded width CNF-formulas where the width is measured by popular graph width measures on graphs associated to CNF-formulas. Such restricted graph classes, in particular those of bounded treewidth, have been extensively studied for their uses in the design of algorithms for various computational problems on CNF-formulas. Here we consider the expressivity of these formulas in the model of clausal encodings with auxiliary variables. We first show that bounding the width for many of the measures from the literature leads to a dramatic loss of expressivity, restricting the formulas to those of low communication complexity. We then show that the width of optimal encodings with respect to different measures is strongly linked: there are two classes of width measures, one containing primal treewidth and the other incidence cliquewidth, such that in each class the width of optimal encodings only differs by constant factors. Moreover, between the two classes the width differs at most by a factor logarithmic in the number of variables. Both these results are in stark contrast to the setting without auxiliary variables where all width measures we consider here differ by more than constant factors and in many cases even by linear factors.

3.16 Modal Logics: An Overview (Parts I and II)

Cláudia Nalon (University of Brasilia, BR)

Joint work of Clare Dixon, Ullrich Hustadt

The first talk was a gentle introduction to modal logics, focusing on the basic multimodal logic K_n. We have discussed the different reasoning tasks for this class of logics, local and global, and their complexity. We have also introduced two different calculi for dealing with reasoning in modal settings: tableaux and resolution.

The second talk was dedicated to the layered resolution calculus for local reasoning for K_n. The calculus is inspired by model-theoretical results concerning satisfiability in K_n: models can be restricted to finite tree-like structures and the satisfiability of a (sub)formula depends only of the subtree in which such a subformula occurs. Clauses are labelled by the height (the modal depth) they occur in such a tree. Inference rules can only be applied to clauses whose labels unify. This restricts the candidates for resolution whilst retaining completeness. Experimental results show that the theorem-prover which implements the calculus, KSP, works well on problems with high modal depth and uniform distribution of propositional symbols over the different depths.

References

1 Cláudia Nalon, Clare Dixon, and Ullrich Hustadt. Modal resolution: Proofs, layers, and refinements. *ACM Transactions on Computational Logic*, 20(4):23:1–23:38, 2019.

2 C. Nalon, U. Hustadt, and C. Dixon. KSP: A resolution-based theorem prover for K_n: architecture, refinements, strategies and experiments. *Journal of Automated Reasoning*, 64(3):461–484, 2020.

3.17 Proof and Refutation: An Adventure in Formalisation

Dirk Pattinson (Australian National University – Canberra, AU)

In this talk, we take the point of view that a simple ‘yes/no’ answer is not a sufficient output of an automated reasoning procedure or implementation. On top of the answer, we demand verifiable evidence, either for provability or refutability of a formula. Clearly, a (formal) proof satisfies this requirement in the case of a provable formula. Countermodels can be used to give evidence of non-provability, but suffer drawbacks: First, there may not be an agreed upon notion of semantics, and second, the mathematical details of countermodels vary widely depending on the underlying logic, while proofs have a very uniform representation.

For this reason, we complement the syntactic notion of proof with a syntactic (coinductively defined) notion of refutation. Our main theorem then states that ’every sequent either has a proof or a refutation’ (terms and conditions apply). We speak both on the notion of refutation in general, as well as highlight the challenges encountered in fully verifying the above theorem.

3.18 Dependency Learning for QBF

Tomáš Peitl (Universität Jena, DE), Friedrich Slivovsky (TU Wien, AT), and Stefan Szeider

Main reference Tomás Peitl, Friedrich Slivovsky, Stefan Szeider: “Dependency Learning for QBF”, J. Artif. Intell. Res., Vol. 65, pp. 180–208, 2019.
URL http://dx.doi.org/10.1613/jair.1.11529

Quantified Boolean Formulas (QBFs) can be used to succinctly encode problems from domains such as formal verification, planning, and synthesis. One of the main approaches to QBF solving is Quantified Conflict Driven Clause Learning (QCDCL). By default, QCDCL assigns variables in the order of their appearance in the quantifier prefix so as to account for dependencies among variables. Dependency schemes can be used to relax this restriction and exploit independence among variables in certain cases, but only at the cost of nontrivial interferences with the proof system underlying QCDCL.

We introduce dependency learning, a new technique for exploiting variable independence within QCDCL that allows solvers to learn variable dependencies on the fly. The resulting version of QCDCL enjoys improved propagation and increased flexibility in choosing variables for branching while retaining ordinary (long-distance) Q-resolution as its underlying proof system. We show that dependency learning can achieve exponential speedups over ordinary QCDCL. Experiments on standard benchmark sets demonstrate the effectiveness of this technique.

3.19 Forgetting-Based Ontology Extraction

Renate Schmidt (University of Manchester, GB)

Joint work of Jieying Chen, Ghadah Alghamdi, Renate A. Schmidt, Dirk Walther, Yongsheng Gao
Main reference Jieying Chen, Ghadah Alghamdi, Renate A. Schmidt, Dirk Walther, Yongsheng Gao: "Ontology Extraction for Large Ontologies via Modularity and Forgetting", in Proc. of the 10th International Conference on Knowledge Capture, K-CAP 2019, Marina Del Rey, CA, USA, November 19-21, 2019, pp. 45–52, ACM, 2019.
URL https://doi.org/10.1145/3360901.3364424

Ontology extraction is an essential operation for the reuse, creation, evaluation, curation, decomposition, integration and general use of ontologies. A method with higher precision is forgetting, also known as uniform interpolation. Forgetting creates a compact representation of a part of the information contained in an ontology that preserves the underlying logical definitions of the specified terms (the interpolation signature) by hiding the remaining terms. This allows users to focus exactly on the information they are interested in.

After an introduction of the idea of forgetting in contrast to modularisation, another ontology extraction method, the presentation gave an overview of recent and current research on developing practical forgetting tools for description logic based ontologies. We also discussed the application of these tools to SNOMED CT, a comprehensive ontology of standardised medical content used in health care systems across several countries.

3.20 Spinal Atomic Lambda-Calculus

David R. Sherratt (Universität Jena, DE)

Joint work of Heijltjes, Willem; Gundersen, Tom; Parigot, Michel
Main reference David Sherratt: "A lambda-calculus that achieves full laziness with spine duplication", 2019.
URL http://ethos.bl.uk/OrderDetails.do?uin=uk.bl.ethos.787527

We present the spinal atomic lambda-calculus, a typed lambda-calculus with explicit sharing and atomic duplication that achieves spinal full laziness: duplicating only the direct paths between a binder and bound variables is enough for beta reduction to proceed. We show this calculus is the result of a Curry–Howard style interpretation of a deep-inference proof system, and prove that it has natural properties with respect to the lambda-calculus: confluence and preservation of strong normalisation.

References

1 David Rhys Sherratt. *A Lambda-Calculus that achieves full laziness with spine duplication*. PhD thesis, University of Bath, UK, 2019.

3.21 Computing Unique Strategy Functions by Interpolation

Friedrich Slivovsky (TU Wien, AT)

We present a new semantic gate extraction technique for propositional formulas based on interpolation. While known gate detection methods are incomplete and rely on pattern matching or simple semantic conditions, this approach can detect any definition entailed by an input formula. As an application, we consider the problem of computing unique strategy functions from Quantified Boolean Formulas (QBFs) and Dependency Quantified Boolean Formulas (DQBFs). Experiments with a prototype implementation demonstrate that functions can be efficiently extracted from formulas in standard benchmark sets, and that many of these definitions remain undetected by syntactic gate detection. We turn this into a preprocessing technique by substituting unique strategy functions for input variables and test solver performance on the resulting instances. Compared to syntactic gate detection, we see a significant increase in the number of solved 2QBF instances, as well as modest increases for general QBF and DQBF.

3.22 Introduction to Deep Inference

Lutz Straßburger (INRIA Saclay – Île-de-France, FR)

In the first half of the talk I gave a rough overview over the main research results of deep inference of the last 20 years. I discussed *atomicity* and *locality* of inference rules, I presented proof systems for classical logic and linear logic, and I showed how cut elimination can be proved using the techniques of *decomposition* and *splitting*. A good starting point for reading about this subject are the lecture notes for a course on deep inference given at ESSLLI 2019 (to be found at https://hal.inria.fr/hal-02390267). More information on deep inference can be found on the *deep inference webpage* (http://alessio.guglielmi.name/res/cos/index.html) maintained by Alessio Guglielmi.

In the second half of the talk I discussed proof systems for intuitionistic modal logics using nested sequents. I also presented the prover MOIN, for which a system description is available at https://hal.inria.fr/hal-02457240, where also more references on nested sequent proof systems can be found.

3.23 Hard Examples for Common Variable Decision Heuristics

Marc Vinyals (Technion – Haifa, IL)

Main reference Marc Vinyals: "Hard Examples for Common Variable Decision Heuristics", in Proc. of the The Thirty-Fourth AAAI Conference on Artificial Intelligence, AAAI 2020, The Thirty-Second Innovative Applications of Artificial Intelligence Conference, IAAI 2020, The Tenth AAAI Symposium on Educational Advances in Artificial Intelligence, EAAI 2020, New York, NY, USA, February 7-12, 2020, pp. 1652–1659, AAAI Press, 2020.
URL https://aaai.org/ojs/index.php/AAAI/article/view/5527

The CDCL algorithm, which is nowadays the top-performing algorithm to solve SAT in practice, is polynomially equivalent to resolution when we view it as a proof system, that is we replace some of its heuristics by nondeterministic choices.

In this talk we show that this is no longer true if we leave the heuristics in place; more precisely we build a family of formulas that have resolution proofs of polynomial size but require exponential time to decide in CDCL with a class of variable decision heuristics that includes the most common heuristics such as VSIDS.

3.24 Reversible Pebble Games and the Relation Between Tree-Like and General Resolution Space

Florian Wörz (Universität Ulm, DE) and Jacobo Torán (Universität Ulm, DE)

Joint work of Jacobo Torán, Florian Wörz
Main reference Jacobo Torán, Florian Wörz: "Reversible Pebble Games and the Relation Between Tree-Like and General Resolution Space", in Proc. of the 37th International Symposium on Theoretical Aspects of Computer Science, STACS 2020, March 10-13, 2020, Montpellier, France, LIPIcs, Vol. 154, pp. 60:1–60:18, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2020.
URL http://dx.doi.org/10.4230/LIPIcs.STACS.2020.60

We show a new connection between the space measure in tree-like resolution and the reversible pebble game in graphs. Using this connection we provide several formula classes for which there is a logarithmic factor separation between the space complexity measure in tree-like and general resolution. We show that these separations are almost optimal by proving upper bounds for tree-like resolution space in terms of general resolution clause and variable space. In particular we show that for any formula F, its tree-like resolution is upper bounded by $\mathrm{space}(\pi) \log \mathrm{time}(\pi)$, where π is any general resolution refutation of F. This holds considering as $\mathrm{space}(\pi)$ the clause space of the refutation as well as considering its variable space. For the concrete case of Tseitin formulas we are able to improve this bound to the optimal bound $\mathrm{space}(\pi) \log n$, where n is the number of vertices of the corresponding graph.

4 Future Directions of Research

The seminar featured a session in which participants were invited to give a short informal presentation on the theme *directions of future research*. Five partipants contributed presentations, summarised below.

4.1 Anupam Das

The community might like to explore what proof theory can give to solving, because techniques developed in the context of proof theory could have a much wider applicability. For instance, some solvers dealing with the logic K5 translate the formulas to QBF, while preserving some semantic meaning. Performance is heavily dependent on the encoding used. Instead, could one use proof-theoretic techniques like focussing, deep inference, or graph-based concepts? As long as these techniques preserve some measures of the formulas, it may be possible to transfer algorithmic bounds. A somewhat related question would ask what the appropriate measures may be.

4.2 Vijay Ganesh

Proof complexity theorists usually focus on proving lower bounds for various proof systems. However, we have a very poor understanding of why solvers perform well in practice. One approach to deepen this understanding is to establish some parametric upper bounds. The choice of parameters for such a study should be informed by practice. Analysing a solver directly may be hard, but it may be easier to establish a polynomial equivalence to algorithms that establish such parametric upper bounds.

An example in another domain, where theoretical tools give a good explanation for why an algorithm that has bad worst-case behaviour nonetheless behaves extremely well in practice, is the smoothed analysis framework applied to the Simplex algorithm.

4.3 Ullrich Hustadt

There exists a plethora of logics – modal logics, description logics, and so on – each with its own calculi. A typical goal is to extend the reach of Resolution to these logics. As the calculi often arise from philosophy, it is not clear a priori that they all merit such a study. Therefore, it is natural to consider which logics amongst this huge zoo are really worth exploring. The community may then focus its attention there, since it is not large enough to explore them all.

4.4 Oliver Kullmann

Despite great effort, the use of SAT solvers – particularly in the solution of hard problems via schemes like cube-and-conquer – remains poorly understood. An informal “psychoanalysis” could partition the workflow into three phases:

1. the entirely predictable part, based on mathematical truths,
2. the intermediate part, lookahead using statistical tools,
3. the almost utterly unpredictable part – CDCL solvers lie here, and there seems to be some unstable chaos.

Restrictions by partial assignments take us outwards, from families that can be handled within phase 1 alone, to versions that are more chaotic or unstable. How can we explain this phenomenon and put it to use?

4.5 Lutz Straßburger

There are many very different proof systems, and proofs in a specific system are heavily tied to the specifics of the proof system. And yet, (almost) all proofs rely on a common mathematical underpinning. Can we seek proofs independent of the proof system? That is, can we speak of proofs independent of representations in specific proof systems? We want to somehow pinpoint the essential mathematical content of a proof, which will of course depend on the logic, but can it be independent of the proof system? For classical propositional logic, for example, combinatorial proofs is a candidate approach.

Participants

- Olaf Beyersdorff
Universität Jena, DE
- Joshua Lewis Blinkhorn
Universität Jena, DE
- Benjamin Böhm
Universität Jena, DE
- Ilario Bonacina
UPC Barcelona Tech, ES
- Florent Capelli
Lille I University, FR
- Leroy Nicholas Chew
Carnegie Mellon University – Pittsburgh, US
- Judith Clymo
University of Leeds, GB
- Nadia Creignou
Aix-Marseille University, FR
- Anupam Das
University of Birmingham, GB
- Susanna de Rezende
The Czech Academy of Sciences – Prague, CZ
- Akhil Dixit
University of California – Santa Cruz, US
- Clare Dixon
University of Liverpool, GB
- Uwe Egly
TU Wien, AT
- Vijay Ganesh
University of Waterloo, CA
- Azza Gaysin
Charles University – Prague, CZ
- Edward A. Hirsch
Steklov Institute – St. Petersburg, RU
- Ullrich Hustadt
University of Liverpool, GB
- Mikoláš Janota
IST – Lisbon, PT
- Jan Johannsen
LMU München, DE
- Hans Kleine Büning
Universität Paderborn, DE
- Oliver Kullmann
Swansea University, GB
- Massimo Lauria
Sapienza University of Rome, IT
- Meena Mahajan
Institute of Mathematical Sciences – Chennai, IN
- Joao Marques-Silva
University of Toulouse, FR
- Barnaby Martin
Durham University, GB
- Stefan Mengel
CNRS, CRIL – Lens FR
- Claudia Nalon
University of Brasilia, BR
- Jakob Nordström
University of Copenhagen, DK & Lund University, SE
- Dirk Pattinson
Australian National University – Canberra, AU
- Tomáš Peitl
Universität Jena, DE
- Renate Schmidt
University of Manchester, GB
- Uwe Schöning
Universität Ulm, DE
- David R. Sherratt
Universität Jena, DE
- Anil Shukla
Indian Institute of Technology Ropar – Rupnagar, IN
- Friedrich Slivovsky
TU Wien, AT
- Gaurav Sood
Institute of Mathematical Sciences – Chennai, IN
- Lutz Straßburger
INRIA Saclay – Île-de-France, FR
- Jacobo Torán
Universität Ulm, DE
- Marc Vinyals
Technion – Haifa, IL
- Florian Wörz
Universität Ulm, DE