Report from Dagstuhl Seminar 22072

New Perspectives in Symbolic Computation and Satisfiability Checking

Erika Abraham*[1], James H. Davenport*[2], Matthew England*[3], and Alberto Griggio*[4]

1 **RWTH Aachen University, DE.** `abraham@informatik.rwth-aachen.de`
2 **University of Bath, GB.** `J.H.Davenport@bath.ac.uk`
3 **Coventry University, GB.** `Matthew.England@coventry.ac.uk`
4 **Fondazione Bruno Kessler – Trento, IT.** `griggio@fbk.eu`

Abstract

Dagstuhl Seminar 22072 gathered researchers from Symbolic Computation and Satisfiability Checking. These communities have independent histories but worked together in recent years (e.g. Dagstuhl Seminar 15471 and the EU SC-Square Project). We seek to tackle problems which are in the interest of both communities, and require the expertise of both to overcome.

Seminar February 13–18, 2022 – http://www.dagstuhl.de/22072
2012 ACM Subject Classification Computing methodologies → Symbolic and algebraic manipulation; Theory of computation → Automated reasoning
Keywords and phrases computer algebra systems, SMT Solvers, verification
Digital Object Identifier 10.4230/DagRep.12.2.67

1 Executive Summary

Matthew England (Coventry University, GB)
Erika Abraham (RWTH Aachen University, DE)
James H. Davenport (University of Bath, GB)
Alberto Griggio (Fondazione Bruno Kessler, IT)

Introduction

Symbolic Computation refers to algorithms for computers to perform symbolic mathematics, usually implemented in Computer Algebra Systems (CASs). Satisfiability Checking refers to algorithms to efficiently check the satisfiability of a logical statement, developed originally for the Boolean domain and implemented in SAT solvers, but now extended to a wide variety of different theories in satisfiability modulo theories (SMT) solvers. This Dagstuhl Seminar is on Symbolic Computation and Satisfiability Checking, with the emphasis on the "and" to indicate the scope is strictly work of interest to both communities.

Traditionally, the two communities have been largely disjoint and unaware of the achievements of one another, despite there being strong reasons for them to discuss and collaborate, since they share many central interests. Many of the theories tackled by SMT have been traditionally studied within Symbolic Computation; while in the opposite direction, the integration of SAT solvers into computer algebra systems can allow more powerful logical reasoning and inspire new algorithmic approaches in computer algebra.

* Editor / Organizer

New Perspectives in Symbolic Computation and Satisfiability Checking, *Dagstuhl Reports*, Vol. 12, Issue 2, pp. 67–86
Editors: Erika Abraham, James H. Davenport, Matthew England, and Alberto Griggio
Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Recent History

The first global meeting dedicated to both symbolic computation and satisfiability checking was Dagstuhl Seminar 15471 (Symbolic Computation and Satisfiability Checking) [1] which took place in November 2015. This was followed soon after by EU Horizon 2020 Grant 712689 which ran from 2016-2018. The aim of that project was to bridge the gap between the communities to produce individuals who can combine the knowledge and techniques of both fields to resolve problems currently beyond the scope of either [2]. The project funded new collaborations, new tool integrations, proposals on extensions to the SMT-LIB language standards, new collections of benchmarks, two summer schools (in 2017 and 2018) and the SC-Square Workshop Series.

The Workshop Series (`http://www.sc-square.org/workshops.html`) has taken place annually for six years, with two further editions already planned:

2016 Timişoara, Romainia (as part of SYNASC 2016).
2017 Kaiserslautern, Germany (alongside ISSAC 2017).
2018 Oxford, UK (as part of FLoC 2018).
2019 Bern, Switzlerland (as part of SIAM AG19)
2020 Paris, France (online) (alongside IJCAR 2020)
2021 Texas, USA (online) (as part of SIAM AG21)
2022 Haifa, Israel (as part of FLoC 2022)
2023 Tromsø Norway (alongside ISSAC 2023)

It takes place as part of, or alongside, established conferences (alternating between computational algebra and logic). Each year there are two chairs, one from each community.

In 2020 a special issue of the Journal of Symbolic Computation was published, on the theme of SC-Square [3]. A further special issue is in development.

Motivation for new Seminar

The seminar call defined its scope with these research questions.

Decision Procedures: How to efficiently leverage CAS for SMT over hard arithmetical theories? How to exploit conflict-driven learning and non-chronological backtracking in symbolic computation algorithms? How can CAS and SMT be combined to reason about bit-precise machine (i.e. floating point) arithmetic?

Abstraction and Linearization: How can abstraction techniques commonly adopted in SMT be exploited in symbolic computation? How to leverage techniques in CASs for iterative abstraction refinement in SMT?

Optimization: Can SMT and symbolic computation be combined for successfully attacking non-linear optimization problems? Can new optimization techniques be leveraged for heuristic choices in solvers?

Machine Learning: What are the common challenges and opportunities on the use of Machine Learning (ML) for heuristic choices in algorithms? How best to define problem features for classic ML? How best to encode formulae for deep ML? How to develop good datasets for ML? Tool development: How to share data structures, low-level libraries, input formats and interaction pipelines for more effective development of robust, mature and interoperable symbolic reasoning tools?

Application Problem Encoding: How best encode high-level application problems to be more amenable to symbolic reasoning? How to provide more expressive problem definition languages which can still be handled efficiently? How to automate problem encoding?

Seminar Overview

The seminar was organised into eight session by broad topic (with some exceptions to allow for online participants). We invited three extended tutorials on key topics of interest to the seminar: Ahmed Irfan spoke on the incremental linearization techniques developed for MathSAT to tackle non-linear problems, including ones involving transcendental functions; Haniel Barbosa and Gereon Kremer described the new work on proof certificates in CVC5, and the possibilities for extensions into non-linear real arithmetic; and Curtis Bright spoke on isomorphism free exhaustive generation techniques which used a combination of computer algebra and SAT solvers. Other talks were contributed by seminar participants.

Upcoming Development

Erika Ábrahám, Chris Brown, James Davenport, Pascal Fontaine and Thomas Sturm are the joint editors of a Journal of Symbolic Computation Special Issue on the topic of "Symbolic Computation and Satisfiability Checking". Contributions coming out of this workshop would be especially welcomed. The timeline is given below.

31 March Submissions Open
31 August Submissions Close
(early notification to `abraham@cs.rwth-aachen.de` is welcomed.)
31 December Authors notified
3–6 months Articles published

Special issues are now "virtual" and so the articles appear online as ready.

Acknowledgements

The present seminar was originally scheduled for November 2020 but was re-organised for February 2022 following the COVID19 pandemic. It was held in a hybrid format, with participants both in person and online. The organisers thank all participants for their contribution, and extend a special thanks to the team at Schloss Dagstuhl for their excellent organisation and support, particularly in the difficult circumstance which the pandemic imposed.

References

1 E. Ábrahám and P. Fontaine and T. Sturm and D. Wang. *Symbolic Computation and Satisfiability Checking (Dagstuhl Seminar 15471).* Dagstuhl Reports 5(11):71-89. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2016. URL: `http://drops.dagstuhl.de/opus/volltexte/2016/5765`

2 E. Ábrahám, J. Abbott, B. Becker, A.M. Bigatti, M. Brain, B. Buchberger, A. Cimatti, J.H. Davenport, M. England, P. Fontaine, S. Forrest, A. Griggio, D. Kroening, W.M. Seiler, and T. Sturm. *SC2: Satisfiability checking meets symbolic computation.* In M. Kohlhase, M. Johansson, B. Miller, L. de Moura, and F. Tompa, editors, Intelligent Computer Mathematics: Proceedings CICM 2016, volume 9791 of Lecture Notes in Computer Science, pages 28–43. Springer International Publishing, 2016. URL: `https://doi.org/10.1007/978-3-319-42547-4_3`

3 J.H. Davenport, M. England, A. Griggio, T. Sturm, and C. Tinelli. *Symbolic computation and satisfiability checking: Editorial.* Journal of Symbolic Computation, 100:1–10, 2020. URL: `https://doi.org/10.1016/j.jsc.2019.07.017`

2 Table of Contents

Executive Summary

Overview of Talks

3 Overview of Talks

3.1 Better SMT Proofs for Certifying Compliance

Haniel Barbosa (Federal University of Minas Gerais-Belo Horizonte, BR)

Joint work of Haniel Barbosa, Andrew Reynolds, Gereon Kremer, Hanna Lachnitt, Aina Niemetz, Andres Nötzli, Alex Ozdemir, Mathias Preiner, Arjun Viswanathan, Scott Viteri, Yoni Zohar, Cesare Tinelli, Clark Barrett

SMT solvers can be hard to trust, since it generally means assuming their large and complex codebases do not contain bugs that lead to wrong results. Machine-checkable certificates, via proofs of the logical reasoning the solver has performed, address this issue by decoupling confidence in the results from the solver's implementation.

Despite previous work, in several SMT solvers, to produce and check proofs, users still have to choose among solvers that may not produce fine-grained proofs, may not produce proofs for some of their crucial-for-efficiency components, or have proofs that are checkable only as part of a specific proof assistant.

To facilitate the use of SMT proof certificates, the cvc5 developers team has completely redesigned its proof-production infrastructure, aiming for a sufficiently general and extensible infrastructure to allow: the generation of coarse- and fine-grained proofs for all parts of the solver, particularly for previously unsupported components such as the rewriter and the strings subsolver; and the printing of proofs in different formats to enable the use of different proof checkers. Specifically, we are working on producing cvc5 proofs for LFSC, Isabelle/HOL, Lean4, and Coq, while also creating proof calculi for previously unsupported SMT-LIB theories in these settings. While the project is still ongoing, we will report on significant progress on all of these fronts.

3.2 Comprehensive Groebner Systems (with CoCoA)

Anna Maria Bigatti (University of Genova, IT)

Joint work of Elisa Palezzato, Michele Torielli, Anna Maria Bigatti

A comprehensive Groebner system (CGS) is a collection of Groebner bases and algebraic sets describing a parametric polynomial system. For a specialization of parameters, a Groebner basis of the specialized ideal can be immediately recovered from a branch of the associated CGS. This property makes its computation attractive in applications where a family of problems can be formulated as a parametric polynomial system.

The first algorithms [7, 8, 3, 5] required computations in polynomial ring over a coefficient field of rational functions, $K(A)[X]$, where A are the parameters, and X the actual indeterminates, together with delicate handling of the case distinctions over the parameters. This last fact makes these algorithms hard to implement in computer algebra systems.

In 2006 Suzuki-Sato [6] introduced a new approach, further improved in [2, 4], which just needs the computation of Groebner bases in $K[A, X]$, so that that can be easily implemented in any computer algebra system.

In this seminar we present a short history of this latter method, we describe our implementation in CoCoA [1] of their algorithms and of our iterative alternative.

References

1 J. Abbott, A. M. Bigatti, and L. Robbiano. *CoCoA: a system for doing Computations in Commutative Algebra*. URL: `https://cocoa.dima.unige.it`

2 D. Kapur, Y. Sun, D. Wang. *A new algorithm for computing comprehensive Groebner systems*. In: Watt, S. (ed.) International Symposium on Symbolic and Algebraic Computation, pp. 29–36. ACM Press, 2010.

3 M. Manubens, and A. Montes. *Improving the DISPGB algorithm using the discriminant ideal*. J. Symb. Comp. 41(11), 1245–1263, 2006.

4 K. Nabeshima. *Stability Conditions of Monomial Bases and Comprehensive Groebner Systems*. CASC'12: Proceedings of the 14th international conference on Computer Algebra in Scientific ComputingSeptember 2012, 248–259, 2012.

5 A. Suzuki, and Y. Sato. *An Alternative approach to Comprehensive Gröbner Bases*. J. Symb. Comp. 36(3-4), 649–667, 2003.

6 A. Suzuki, and Y. Sato. *A Simple Algorithm to Compute Comprehensive Gröbner Bases Using Gröbner Bases*. ISSAC '06: Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation, 326–331, 2006.

7 V. Weispfenning. *Comprehensive Gröbner bases*, J. Symb. Comp. 14(1), 1–29, 1992.

8 V. Weispfenning. *Canonical Comprehensive Gröbner bases*, J. Symb. Comp. 36, 669–683, 2003.

3.3 Sinful Behaviour

Martin Brain (City – University of London, GB)

This talk presents an exposition on the nature of sin, and other trigonometric functions and the consequences for the verification of software that use standard mathematical libraries. The counter-intuitive properties of even the ideal implementation are compounded by the underspecified and ambiguous nature of current implementations. We discuss the difficulties of implementing and verifying trigonometric functions and finish with some challenges for how computer algebra might help.

3.4 Isomorph-Free Exhaustive Generation in SAT Solving

Curtis Bright (University of Windsor, CA)

This tutorial will provide an introduction to methods for exhaustively generating combinatorial objects while avoiding isomorphic copies of those objects. The "recorded objects" and "orderly generation" methods from the symbolic computation literature will be described and contrasted with the "symmetry breaking" approach from the satisfiability literature. A method of combining isomorph-free exhaustive generation with a SAT solver will be applied to two problems and shown to improve the performance of the solver by orders of magnitude. It will be argued there is great potential to be unlocked by exploiting both the symbolic and SAT approaches simultaneously.

References

1 Curtis Bright, Kevin K. H. Cheung, Brett Stevens, Ilias Kotsireas, and Vijay Ganesh. A SAT-based resolution of Lam's problem. In *Proceedings of the Thirty-Fifth AAAI Conference on Artificial Intelligence*, pages 3669–3676, 2021.

2 Michael Codish, Alice Miller, Patrick Prosser, and Peter J Stuckey. Constraints for symmetry breaking in graph representation. *Constraints*, 24(1):1–24, 2019.

3 I. A. Faradžev. Constructive enumeration of combinatorial objects. In *Problèmes combinatoires et théorie des graphes*, pages 131–135, 1978.

4 Tommi Junttila, Matti Karppa, Petteri Kaski, and Jukka Kohonen. An adaptive prefix-assignment technique for symmetry reduction. *Journal of Symbolic Computation*, 99:21–49, 2020.

5 Brendan D. McKay and Adolfo Piperno. Practical graph isomorphism, II. *Journal of Symbolic Computation*, 60:94–112, 2014.

6 Ronald C. Read. Every one a winner or how to avoid isomorphism search when cataloguing combinatorial configurations. In B. Alspach, P. Hell, and D.J. Miller, editors, *Algorithmic Aspects of Combinatorics*, volume 2 of *Annals of Discrete Mathematics*, pages 107–120. Elsevier, 1978.

3.5 What SAT/SMT Has Taught Me

Christopher W. Brown (U.S. Naval Academy – Annapolis, US)

SAT/SMT solvers follow a very different paradigm than algorithms from the computer algebra community. In particular, there is an emphasis on bottom-up, conflict-driven approaches. I will look at how this new (to us) paradigm has changed real polynomial constraint solving so far, and where it might take us in the future.

3.6 Towards Scalable Computation of Semi-Algebraic Systems Driven by Applications

Changbo Chen (Chinese Academy of Sciences – Chongqing, CN)

Real applications require to solve semi-algebraic systems with number of variables ranging from a few to dozens, hundreds, thousands, or even millions or billions. It is a great challenge to make the nonlinear solvers in computer algebra scalable to solve large systems. In this talk, we first review our recent works on increasing the scale of semi-algebraic systems solving by exploiting structures from applications. Then we discuss some possible ways to make RC-CAD, which is an approach for computing CAD based on regular chains, scalable.

3.7 SMT-based analysis of Switching Kirchhoff networks

Alessandro Cimatti (Fondazione Bruno Kessler, IT)

Complex dynamical systems require automated analysis techniques and tools. In this talk I focus on a challenging class of systems that can be described as switching multi-domain Kirchhoff networks (SMDKN), where the global behaviour result from combining the behaviour of components by way of conservation laws. In the first part of the talk, I present a comprehensive, long-term picture where the problems of validating and reformulating an SMDKN description in terms of Differential-Algebraic Equations (DAE) into hybrid automata equipped with Ordinary Differential Equations (DAE). The approach is based on modern satisfiability and verification modulo theory (SMT and VMT) techniques over nonlinear and transcendental functions (NTA) [3]. In the second part of the talk, I discuss a practical subcase, proposing an engineering-oriented approach for the formal analysis of Relay-based Railways Interlocking Systems, developed in the context of an industrial collaboration with the Italian Railway Network company [2, 1].

References

1 Arturo Amendola, Anna Becchi, Roberto Cavada, Alessandro Cimatti, Andrea Ferrando, Lorenzo Pilati, Giuseppe Scaglione, Alberto Tacchella, and Marco Zamboni. *NORMA: a tool for the analysis of Relay-based Railway Interlocking Systems.* Proc. TACAS '22, Lecture Notes in Computer Science, 13243, pages 125–142. Springer, 2022.

2 Roberto Cavada, Alessandro Cimatti, Sergio Mover, Mirko Sessa, Giuseppe Cadavero, Giuseppe Scaglione. *Analysis of Relay Interlocking Systems via SMT-based Model Checking of Switched Multi-Domain Kirchhoff Networks*, Proc. FMCAD '18, pages 1–9. IEEE, 2018.

3 Alessandro Cimatti, Sergio Mover, Mirko Sessa. *SMT-based analysis of switching multi-domain linear Kirchhoff networks*, Proc. FMCAD '17, pages 188–195. IEEE, 2017.

3.8 Varieties of Doubly-Exponential behaviour in Quantifier Elimination and Cylindrical Algebraic Decomposition

James H. Davenport (University of Bath, GB)

It is 45 years since Davenport and Heintz drafted "Real Quantifier Elimination is Doubly Exponential". In the natural representation, both the number of polynomials and the degree are doubly exponential in the number of variables. This talk looks at the varieties of doubly exponential behaviour for various algorithms. These can be growing doubly exponentially in both the number and degree of the polynomials involved [1]. This is inherent in resultant-based processes. We ask whether this in inherent in other methods, such as Virtual Term Substitution and Comprehensive Gröbner Systems. It *may* not be, but this is a significant research question.

References

1 M. England and J.H. Davenport. *The Complexity of Cylindrical Algebraic Decomposition with Respect to Polynomial Degree.* Proceedings CASC 2016, V.P. Gerdt, W. Koepf and W.M. Seiler (eds), LNCS 9890, pages 172–192. Springer, 2016. URL: `https://doi.org/10.1007/978-3-319-45641-6_12`

3.9 Using Machine Learning in SC^2

Tereso del Rio (Coventry University, GB)

This talk exposes many possible uses of Machine Learning (ML) in the context of $\mathcal{SC}^2$, and how this approach differs from human-made heuristics. Different ML paradigms are presented and it is discussed how symbolic data could be encoded. This talk also intends to motivate a discussion about which datasets should be used for training and testing ML models.

3.10 A Note on SMT-LIB NRA

Bruno Dutertre (Amazon – Cupertino, US)

The talk discusses some consequences of the semantics of division by zero adopted by the SMT-LIB standard.

3.11 SMT Solving in the Cloud

Bruno Dutertre (Amazon – Cupertino, US)

We will discuss challenges and opportunities in large-scale parallelism for SMT solving.

3.12 Observations and Questions on the SMT-LIB

Matthew England (Coventry University, GB)

In this seminar we start by giving an overview on the SMT-LIB initiative [1]: an incredible community driven and volunteer run resource. The SMT-LIB provides rigourous descriptions of background theories, developes a common input language for AMT-solvers, and maintains a large and growing library of benchmarks. The author, whose background is Symbolic Computation, was impressed by the SMT-LIB as there was no comparitable resource for computer algebra. The paper [2] offers a good explanation of benchmarking in SAT/SMT to the newcomer from computer algebra.

However, he notes that some care must be taken when using it for the training of machine learning models, or benchmarking more generally. Focussing on the non-linear arithmetic section, we note for example: how very different conclusions can be drawn by the exclusion/inclusion of the MetiTarski dataset (which is an order of magnitude larger than all other datasets in this section); how a large part of these benchmarks can be solved without theory calls, and the vast majority without recourse to complete NRA algorithms; and how some basic simplification routines can change many problems from one theory to a simpler one.

Such issues raise questions about the best way to use this resource and how the resouce itself may be improved. The author suggests that a follow up paper to [2] may be required to outline best practice in use of these benchmarks.

References

1 C. Barrett, P. Fontaine, and C. Tinelli. *The Satisfiability Modulo Theories Library (SMT-LIB)*. URL: `https://smtlib.cs.uiowa.edu/`

2 M. Brain, J.H. Davenport, and A. Griggio. *Benchmarking solvers, SAT-style*. In M. England and V. Ganesh, editors, Proceedings of the 2nd International Workshop on Satisfiability Checking and Symbolic Computation (SC^2 2017), number 1974 in CEUR Workshop Proceedings, 2017. URL: `http://ceur-ws.org/Vol-1974/`

3.13 Scalable Optimal Deployment in the Cloud of Component-based Applications using Contraint Programming, Optimization Modulo Theory, Mathematical Programming and Symmetry Breaking

Madalina Erascu (West University of Timisoara, RO)

Joint work of Erascu, Madalina; Micota, Flavia; Zaharie, Daniela
Main reference Madalina Erascu, Flavia Micota, Daniela Zaharie: "Scalable optimal deployment in the cloud of component-based applications using optimization modulo theory, mathematical programming and symmetry breaking", J. Log. Algebraic Methods Program., Vol. 121, p. 100664, 2021.
URL http://dx.doi.org/10.1016/j.jlamp.2021.100664

Automated deployment of component-based applications in the Cloud consists in the allocation of virtual machines (VMs) offers from various Cloud Providers such that the constraints induced by the interactions between components and by the components hardware/software requirements are satisfied and the performance objectives are optimized (e.g. costs are minimized). It can be formulated as a constraint optimization problem, hence, in principle, the optimization can be carried out automatically. In the case the set of VM offers is large (several hundreds), the computational requirement is huge, making the automatic optimization practically impossible with the current general optimization modulo theory (OMT) and mathematical programming (MP) tools. We overcame the difficulty by methodologically analyzing the particularities of the problem with the aim of identifying search space reduction methods. These are methods exploiting: (1) the symmetries of the general Cloud deployment problem, (2) the graph representation associated to the structural constraints specific to each particular application, and (3) their combination. An extensive experimental analysis has been conducted on four classes of real-world problems, using six symmetry breaking strategies and two types of optimization solvers. As a result, the combination of a variable reduction strategy with a column-wise symmetry breaker leads to a scalable deployment solution, when OMT is used to solve the resulting optimization problem.

3.14 Recent Logic Improvements in Maple

Jürgen Gerhard (Maplesoft – Waterloo, CA)

The presentation will focus on some of the new features and improvements in recent releases of Maple in the areas of computational logic, which are of particular interest to the participants of this seminar. Topics included are Boolean logic and SAT solvers, SMTLIB, polyhedral sets, and nonlinear real arithmetic.

3.15 A Tutorial on Incremental Linearization

Ahmed Irfan (Amazon – Cupertino, US)

Incremental linearization is a simple and practical approach to decide the satisfiability of first-order formulas containing nonlinear arithmetic and transcendental functions. The key idea is to use the abstraction-refinement method by abstracting nonlinear multiplication and transcendental functions as uninterpreted functions, allowing us to leverage efficient methods for linear arithmetic. The abstraction is refined iteratively by axiomatizing the uninterpreted functions by upper- and lower-bounding piecewise linear constraints.

In this tutorial talk, I will walk through the key ideas of the technique and give details for practical consideration. I will also touch upon its recent developments and related open research directions.

3.16 Heuristic Techniques for Natural Style Proofs in Elementary Analysis

Tudor Jebelean (Universität Linz, AT)

Automatic construction of proofs in rich theories (like e. g. elementary analysis) is difficult because the purely logic approach cannot efficiently handle the relatively large number of necessary properties and especially the algorithms based on them. Therefore it looks promising to combine logic with domain specific methods, which is basically equivalent to SMT solving. Our goal goes a little beyond, that is we are aiming at producing automatically proofs that can be easily understood by human readers. For this purpose we identified several heuristic techniques:

- the S-decomposition method for formulae with alternating quantifiers;
- quantifier elimination by cylindrical algebraic decomposition;
- analysis of terms behavior in zero;
- bounding the ϵ-bounds;
- semantic simplification of expressions involving absolute value;

- polynomial arithmetic and solving;
- usage of equal arguments to arbitrary functions; and
- reordering of proof steps in order to insure the admissibility of solutions to meta-variables.

These techniques allow to produce natural-style proofs for many interesting examples [1], like convergence of sum and product of sequences, continuity of sum, product and compositions of functions, etc. As proving in the theory of reals is akin to satisfiability modulo this theory, one expects that these heuristic techniques may inspire more general methods for SMT solving.

References

1 T. Jebelean. *A Heuristic Prover for Elementary Analysis in Theorema*. Intellegent Computer Mathematics (CICM 2021), Lecture Notes in Computer Science 12833:130–134. Springer, 2021. URL: `https://doi.org/10.1007/978-3-030-81097-9_10`

3.17 Guessing with Little Data

Manuel Kauers

Joint work of Manuel Kauers, Christoph Koutschan
Main reference Manuel Kauers, Christoph Koutschan: “Guessing with Little Data”, CoRR, Vol. abs/2202.07966, 2022.
URL https://arxiv.org/abs/2202.07966

Reconstructing a hypothetical recurrence equation from the first terms of an infinite sequence is a classical and well-known technique in experimental mathematics. We say that such an equation is found by guessing. The success of this approach depends on how big the recurrence equation is and how many terms of the sequence are known. The bigger the equation, the more terms are needed to reliably find it.

There are sequences for which it is difficult to generate a lot of terms, and they may satisfy recurrence equations that out of reach of the common guessing algorithm. We present a variation of the guessing algorithm which can succeed with significantly fewer input terms.

This is joint work with Christoph Koutschan [1].

References

1 Manuel Kauers and Christoph Koutschan. Guessing with little data. Arxiv 2202.07966.

3.18 Satisfiable Algebraic Circuit Verification

Daniela Kaufmann (Johannes Kepler Universität Linz, AT)

Joint work of Daniela Kaufmann, Armin Biere, Jakob Nordström, Paul Beame

Although algebraic reasoning is one of the most successful methods for verifying gate-level integer multipliers, it has limitations with particular components, necessitating the use of SAT solvers in addition. As a result, proofs in two different formats are required for validation certifications. The validation results can only be trusted up to compositional reasoning, because approaches to unifying certificates are not scalable. The use of dual variables in the algebraic encoding and replicating SAT-based notions in polynomial reasoning, on the other hand, eliminates the need for SAT solvers in the verification flow, resulting in a single, uniform proof certificate. In this session, I will discuss open issues in incorporating dual variables into algebraic reasoning.

3.19 20+ Years of Legendre Pairs

Ilias S. Kotsireas (Wilfrid Laurier University – Waterloo, CA)

Legendre pairs were introduced in 2001 by Seberry and her students, as a means to construct Hadamard matrices via a two-circulant core construction. A Legendre pair consists of two sequences of the same odd length ℓ, with elements from -1, $+1$, such that their respective autocorrelation coefficients sum to -2, or (equivalently) their respective power spectral density coefficients sum to $2\ell + 2$. Legendre pairs of every odd prime length exist, via a simple construction using the Legendre symbol. We will review known constructions for Legendre pairs. We will discuss various results on Legendre pairs during the past 20 years, including the concept of compression, introduced in a joint paper with Djokovic, as well as the computational state-of-the-art of the search for Legendre pairs. In particular, we recently contributed the only known Legendre pair of length $\ell = 77$ in a joint paper with Turner/Bulutoglu/Geyer. In addition, we recently contributed in a joint paper with Koutschan, several Legendre pairs of new lengths $\ell \equiv 0 \pmod 3$, as well as an algorithm that allows one to determine the full spectrum of values for the $\ell/3$-rd power spectral density value. The importance of Legendre pairs lies in the fact that they constitute a promising avenue to the Hadamard conjecture.

3.20 Formal Proofs for Cylindrical Algebraic Coverings

Gereon Kremer (Stanford University, US)

Formally verifiable proofs can be used to boost trust in SMT solvers in cases of unsatisfiability. We show how cvc5 generates such formal proofs for theory calls to the arithmetic theory. So far, we do not produce verifiable proofs for cylindrical algebraic coverings: we present our current approach and discuss challenges and open questions we face.

3.21 Proving Satisfiability in NTA via Unconstrained Optimization and the Topological Degree Test

Enrico Lipparini (Fondazione Bruno Kessler, IT)

Non-linear arithmetic over the reals augmented with transcendental functions (NTA) is well-known to be a though theory, and proving satisfiability in NTA is expecially hard. In this talk, I present a novel procedure to tackle this challenge. Our procedure makes use of two main ingredients: unconstrained optimisation, to generate a set of candidate solutions, and a result from topology called the topological degree test, to guarantee the existence of a model in a bounded region. We implemented the procedure in a prototype tool called ugotNL, proposing both an eager and a lazy approach (the former being integrated within the MathSAT SMT solver). Our experimental evaluation over a wide range of benchmarks shows that both our tools outperform existing methods for satisfiable formulas, significantly advancing the whole state of the art for NTA. At the end, I discuss the potential of our ideas for future works.

3.22 Implementation and Application of Chordality Preserving Top-Down Algorithms for Triangular Decomposition

Chenqi Mou (Beihang University – Beijing, CN)

Joint work of Chenqi Mou, Wenwen Ju, Mingyu Dong

Recently chordal graphs have been successfully used in the study of elimination methods like triangular decomposition and quantifier elimination. In this talk, I will first briefly review the underlying theories for studying top-down algorithms for triangular decomposition based on chordal graphs. Next I will talk about our implementations of chordality preserving sparse algorithms for triangular decomposition based on the Epsilon package for the computer algebra system Maple. These algorithms are then applied to exploit the variable sparsity of biological dynamical systems in computing their equilibria, and the experimental results will be reported.

3.23 Dynamical System Verification using Abstractions and Non-Linear Arithmetic

Sergio Mover (Ecole Polytechnique – Palaiseau, FR)

A semi-algebraic abstraction is a qualitative abstraction that partitions the state-space of a continuous dynamical system according to the sign of polynomials, obtaining as a result a finite-state, discrete transition system. Standard model checking techniques can then verify safety properties on such discrete system and, if that is the case, conclude safety for the original continuous system.

We can construct such abstraction that for polynomial dynamical systems using Non-Linear Real Arithmetic (NRA). However, the number of discrete states we have to enumerate is, in the worst case, exponential in the number of polynomials. We show how to avoid the up-front computation of the abstraction and, instead, provide an implicit encoding of the abstraction in a discrete transition system expressed symbolically with NRA formulas. We then solve the safety verification problem model checking such transition system.

We conclude evaluating the new technique and discussing some challenges to scale the verification and extend the encoding to hybrid, instead of dynamical, systems.

3.24 Levelwise Construction of a Single Cylindrical Algebraic Cell

Jasper Nalbach (RWTH Aachen University, DE)

Joint work of Jasper Nalbach, Erika Ábrahám, Philippe Specht, Christopher W. Brown, James H. Davenport, Matthew England

Satisfiability modulo theories (SMT) solving is a technique for checking the satisfiability of quantifier-free first-order logic formulas over different theories. We consider the theory of non-linear real arithmetic where the formulae are logical combinations of polynomial constraints. The most commonly used decision procedure is the cylindrical algebraic decomposition (CAD) which has doubly exponential complexity (in the number of real variables). It works through a projection and lifting framework, where the projection tracks the resultants, discriminants and coefficients of all polynomials involved.

A CAD encodes more information than necessary for checking satisfiability. Hence there has been the recent development of sample-based algorithms which reduce the computational effort in CAD by guessing samples and generalizing conflicts by constructing truth-invariant cells around conflicting samples. The most notable example of this is the NLSAT algorithm, an instantiation of the model-constructing satisfiability calculus (MCSAT). Conflict generalization improves on CAD by reducing the number of polynomials to project, and reducing the projection itself based on the sample for the conflict. The original NLSAT only reduces the number of coefficients tracked in projection, but it was followed by the single cell construction which reduces further the number of resultants and discriminants used. This construction involved refining a cell iteratively, polynomial by polynomial, meaning the shape and size of the resulting cell depends on the order in which the polynomials are considered.

Our paper (to be submitted) further develops these ideas by employing a levelwise approach to cell construction, so called as the cell is built level by level according to a variable ordering, rather than incrementally refined according to a polynomial ordering. We still use a reduced number of projection polynomials based on the sample being generalised, but we consider at once all the possibilities for these at a given level allowing for the use of heuristics to select the polynomials used to try and optimise on the shape of the cell

A further contribution is that we have formulated the necessary theory as a proof system, allowing for a decoupling of such heuristic decisions from the main algorithm and its proof of correctness.

Based on a first implementation, we validate experimentally the benefit of this levelwise approach. We compare three basic heuristics and observe that each heuristic has strength on different subsets of the dataset compared to the others; offering clear potential for further exploitation of the new approach.

3.25 Proof theory and computational algebra

Thomas Powell (University of Bath, GB)

I gave a high-level overview of proof interpretations and their role in applied proof theory, briefly describing their use in both proof mining and formal program synthesis. I then presented some recent work on applying proof theory in abstract algebra and outlined what I consider to be some interesting discussion points on the potential intersection of proof theory with the Symbolic Computation and Satisfiability Checking community. These include:

1. Are there interesting proof systems suited to reasoning about proofs and programs in computer algebra and satisfiability checking?
2. Can proof theoretic techniques be used as part of a verification strategy for key algorithms in these areas?
3. Are there examples of nonconstructive proofs where proof interpretations can yield useful quantitative information?

3.26 Looking Backward and Forward

Stefan Ratschan (The Czech Academy of Sciences – Prague, CZ)

In the talk, I looked back at the influence of some principles from numerical analysis on the development of decision procedures for the theory of real closed fields, discussed how the topological degree can be used as an existence test in this context, and presented some ideas for future work.

3.27 Computational Limits of Using CAD and SMT Solvers in Logical Analysis of Regulatory Networks

AmirHosein Sadeghimanesh (Coventry University, GB)

The Multistationarity region of chemical reaction networks can be described as a system of polynomial inequalities on the parameters of the network. However the algebraic algorithms to do so have high computational complexity. Biologists usually break the model to smaller pieces and then describe the behavior of the big model as a function of the behavior of the smaller compartments of the model. This talk tries to start a discussion for creating new algorithms using CAD and SMT-solvers to find the possible boolean formulae expressing multistationarity of a large network according to multistationarity of its smaller compartments if any exists.

3.28 Expansion-Based QBF Solving for QBF

Martina Seidl (Johannes Kepler Universität Linz, AT)

Within the last years, several different solving approaches for quantified Boolean formulas (QBF) have been presented. One particular successful approach is based on the expansion of quantifiers. In this talk, we present a novel algorithm for expansion-based QBF solving.

3.29 Decidable Logics with Arithmetic and Uninterpreted Symbols for SMT

Baptiste Vergain (University of Liège, BE)

Joint work of Bernard Boigelot, Pascal Fontaine, Baptiste Vergain

The objective of this *work in progress* is to characterize decidable sublogics of the difference logic with uninterpreted predicates (e.g. UFIDL, UFRDL), i.e. formulas with first-order quantifiers, uninterpreted predicates, and atomic arithmetic expressions of the form $x - y \bowtie c$, where $\bowtie$ ranges over the relations $<$, $\leq$, $=$, $\neq$, $\geq$, $>$, where the intended domain is natural numbers, integers or real numbers.

In particular, we identified the fragment on integers where only unary predicates are allowed, the decidability of which can be established by stating its equivalence with Büchi automata (similarly to S1S), with an effective decision procedure. Our next objective is to adapt this decision procedure to the integers and to the reals.

It is straightforward for integers. The case of real numbers is although much harder. It is not clear to us yet what restrictions are necessary to ensure decidability of the fragment. We discuss the expressive power of the logic over this domain, and introduce an effective representations of the models of a formula based on words indexed by linear orderings. We then investigate how automata theory can lead us towards a decision procedure.

Participants

- Erika Abraham
RWTH Aachen University, DE
- Christopher W. Brown
U.S. Naval Academy –
Annapolis, US
- Alessandro Cimatti
Bruno Kessler Foundation –
Trento, IT
- James H. Davenport
University of Bath, GB
- Tereso del Rio
Coventry University, GB
- Matthew England
Coventry University, GB
- Jürgen Gerhard
Maplesoft – Waterloo, CA
- Alberto Griggio
Bruno Kessler Foundation –
Trento, IT
- Tudor Jebelean
Universität Linz, AT
- Konstantin Korovin
University of Manchester, GB
- Gereon Kremer
Stanford University, US
- Corin Lee
University of Bath, GB
- Sergio Mover
Ecole Polytechnique –
Palaiseau, FR
- Jasper Nalbach
RWTH Aachen University, DE
- Thomas Powell
University of Bath, GB
- Stefan Ratschan
The Czech Academy of Sciences –
Prague, CZ
- Ali K. Uncu
University of Bath, GB
- Baptiste Vergain
University of Liège, BE

Remote Participants

- Haniel Barbosa
Federal University of Minas
Gerais-Belo Horizonte, BR
- Anna Maria Bigatti
University of Genova, IT
- Russell Bradford
University of Bath, GB
- Martin Brain
City – University of London, GB
- Curtis Bright
University of Windsor, CA
- Martin Bromberger
MPI für Informatik –
Saarbrücken, DE
- Changbo Chen
Chinese Academy of Sciences –
Chongqing, CN
- Isabela Dramnesc
West University of
Timisoara, RO
- Bruno Dutertre
Amazon – Cupertino, US
- Madalina Erascu
West University of
Timisoara, RO
- Pascal Fontaine
University of Liège, BE
- Vijay Ganesh
University of Waterloo, CA
- Ahmed Irfan
Amazon – Cupertino, US
- Manuel Kauers
Johannes Kepler Universität
Linz, AT
- Daniela Kaufmann
Johannes Kepler Universität
Linz, AT
- Ilias S. Kotsireas
Wilfrid Laurier University –
Waterloo, CA
- Enrico Lipparini
Bruno Kessler Foundation –
Trento, IT

- Chenqi Mou
Beihang University – Beijing, CN
- Mizuhito Ogawa
JAIST – Ishikawa, JP
- AmirHosein Sadeghimanesh
Coventry University, GB
- Martina Seidl
Johannes Kepler Universität Linz, AT