

Satisfiability Modulo Theories

21st International Workshop

SMT 2023

Proceedings

Rome, Italy
Affiliated with CADE-29
July 5 – 6, 2023

Stéphane Graham-Lengrand¹, Mathias Preiner²

¹*SRI International*

²*Stanford University*

SMT'23: 21st International Workshop on Satisfiability Modulo Theories, July 5–6, 2023, Rome, Italy


✉ stephane.graham-lengrand@cs.sri.com (S. Graham-Lengrand); preiner@cs.stanford.edu (M. Preiner)

🌐 <https://www.csl.sri.com/users/sgl/> (S. Graham-Lengrand); <https://cs.stanford.edu/~preiner/> (M. Preiner)

🆔 0000-0002-2112-7284 (S. Graham-Lengrand); 0000-0002-7142-6258 (M. Preiner)



© 2023 Copyright for the individual papers by the papers' authors. Copyright for the volume as a collection by its editors. This volume and its papers are published under the Creative Commons License Attribution 4.0 International (CC BY 4.0).

 CEUR Workshop Proceedings (CEUR-WS.org)

Preface

The 21st International Workshop on Satisfiability Modulo Theories was held in Rome, Italy, on July 5th and 6th in association with the International Conference on Automated Deduction (CADE-29).

The SMT workshop is an annual event dedicated to Satisfiability Modulo Theories (SMT).

Determining the satisfiability of first-order formulas modulo background theories, known as the Satisfiability Modulo Theories problem, has proved to be an enabling technology for verification, synthesis, test generation, compiler optimization, scheduling, and other areas.

The success of SMT techniques depends on the development of both domain-specific decision procedures for each background theory (e.g., linear arithmetic, the theory of arrays, or the theory of bit-vectors) and combination methods that allow one to obtain more versatile SMT tools, usually leveraging Boolean satisfiability (SAT) solvers. These ingredients together make SMT techniques well-suited for use in larger automated reasoning and verification efforts.

The aim of the workshop is to bring together researchers and users of SMT tools and techniques. Relevant topics include but are not limited to:

- Decision procedures and theories of interest
- Combinations of decision procedures
- Novel implementation techniques
- Benchmarks and evaluation methodologies
- Applications and case studies
- Theoretical results

SMT 2023 featured invited talks by Oded Padon from VMware Research and Michael Whalen from Amazon, and the presentation of 13 peer-reviewed papers. The workshop received 14 submissions, out of which 13 were accepted. Each submission was reviewed by three program committee members. Of the 13 accepted submissions, six are published in this volume: three as original papers, and three as extended abstracts. The remaining seven were submitted to the workshop for presentation only. For one of them, the authors agreed to include the paper abstract in this volume.

We would like to thank the program committee, the subreviewers, the authors, the invited speakers, the SMT-COMP organizers, workshop participants and the SMT Steering Committee for their contribution to the workshop. We would further like to thank the CADE organizers for hosting the workshop, EasyChair for the availability of their conference system, and CEUR for their help to publish these proceedings.

SMT 2023 was sponsored by AdaCore and Ethereum Foundation. We are grateful for their generosity in supporting the workshop.

Stéphane Graham-Lengrand and Mathias Preiner
Co-chairs, SMT 2023

Program Committee

Program Chairs

Stéphane Graham-Lengrand, SRI International

Mathias Preiner, Stanford University

Program Committee

Leonardo Alt, Ethereum Foundation

Clark Barrett, Stanford University

François Bobot, CEA

Martin Brain, City, University of London

Simon Cruanes, Imandra

Rayna Dimitrova, CISPA Helmholtz Center for Information Security

Bruno Dutertre, Amazon Web Services

Katalin Fazekas, TU Wien

Jochen Hoenicke, Certora

Antti Hyvärinen, Certora

Ahmed Irfan, SRI International

Mikolas Janota, Czech Technical University in Prague

Martin Jonáš, Masaryk University, Czech Republic

Daniela Kaufmann, TU Wien

Aina Niemetz, Stanford University

Andres Noetzli, Cubist Inc

Tanja Schindler, University of Liège

Hans-Jörg Schurr, University of Iowa

Sophie Touret, INRIA and MPI for Informatics

Yoni Zohar, Bar Ilan University

Subreviewers

Hichem Ait El Hara, OCamlPro

Thomas Hader, TU Wien

Contents

Invited Talks

Deductive Verification of Distributed Protocols in Decidable Logics	1
<i>Oded Padon</i>	
SAT and SMT Solving at Cloud Scale	2
<i>Michael Whalen</i>	

Regular Papers

Automated Analysis of Halo2 Circuits	3
<i>Fatemeh Heidari Soureshjani, Mathias Hall-Andersen, Mohammadmahdi Jahanara, Jeffrey Kam, Jan Gorzny and Mohsen Ahmadvand</i>	
Complete Trigger Selection in Satisfiability modulo First Order Theories	18
<i>Christopher Lynch and Stephen Miner</i>	
Exploiting Strict Constraints in the Cylindrical Algebraic Covering	33
<i>Philipp Bär, Jasper Nalbach, Erika Ábrahám and Christopher W. Brown</i>	

Extended Abstracts

Application of SMT in a Meta-Compiler: A Logic DSL for Specifying Type Systems	46
<i>Romain Béguet and Raphaël Amiard</i>	
Verifying Models with Dolmen	62
<i>Guillaume Bury and François Bobot</i>	
Selecting Quantifiers for Instantiation in SMT	71
<i>Jan Jakubův, Mikoláš Janota, Bartosz Piotrowski, Jelle Piepenbrock and Andrew Reynolds</i>	

Presentation-Only Papers (Abstracts)

Automatic Verification of SMT Rewrites in Isabelle/HOL	78
<i>Hanna Lachnitt, Mathias Fleury, Leni Aniva, Andrew Reynolds, Haniel Barbosa, Andres Noetzli, Clark Barrett and Cesare Tinelli</i>	