

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Zurich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology Madras, Chennai, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbrücken, Germany

More information about this series at <http://www.springer.com/series/7408>

Shuvendu K. Lahiri · Chao Wang (Eds.)

Automated Technology for Verification and Analysis

16th International Symposium, ATVA 2018
Los Angeles, CA, USA, October 7–10, 2018
Proceedings

Editors

Shuvendu K. Lahiri
Microsoft Research
Redmond, WA
USA

Chao Wang
University of Southern California
Los Angeles, CA
USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-01089-8 ISBN 978-3-030-01090-4 (eBook)
<https://doi.org/10.1007/978-3-030-01090-4>

Library of Congress Control Number: 2018955278

LNCS Sublibrary: SL2 – Programming and Software Engineering

© Springer Nature Switzerland AG 2018

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This volume contains the papers presented at the 16th International Symposium on Automated Technology for Verification and Analysis (ATVA 2018) held during October 7–10, 2018, in Los Angeles, California, USA.

ATVA is a series of symposia dedicated to the promotion of research on theoretical and practical aspects of automated analysis, verification, and synthesis by providing a forum for interaction between the regional and the international research communities and industry in the field. Previous events were held in Taipei (2003–2005), Beijing (2006), Tokyo (2007), Seoul (2008), Macao (2009), Singapore (2010), Taipei (2011), Thiruvananthapuram (2012), Hanoi (2013), Sydney (2014), Shanghai (2015), Chiba (2016), and Pune (2017).

ATVA 2018 received 82 high-quality paper submissions, each of which received three reviews on average. After careful review, the Program Committee accepted 27 regular papers and six tool papers. The evaluation and selection process involved thorough discussions among members of the Program Committee through the Easy-Chair conference management system, before reaching a consensus on the final decisions.

To complement the contributed papers, we included in the program three keynote talks and tutorials given by Nikolaj Bjørner (Microsoft Research, USA), Corina Păsăreanu (NASA Ames Research Center, USA), and Sanjit Seshia (University of California, Berkeley, USA), resulting in an exceptionally strong technical program.

We would like to acknowledge the contributions that made ATVA 2018 a successful event. First, we thank the authors of all submitted papers and we hope that they continue to submit their high-quality work to ATVA in future. Second, we thank the Program Committee members and external reviewers for their rigorous evaluation of the submitted papers. Third, we thank the keynote speakers for enriching the program by presenting their distinguished research. Finally, we thank Microsoft and Springer for sponsoring ATVA 2018.

We sincerely hope that the readers find the ATVA 2018 proceedings informative and rewarding.

October 2018

Shuvendu K. Lahiri
Chao Wang

Organization

Steering Committee

E. Allen Emerson	University of Texas, Austin, USA
Teruo Higashino	Osaka University, Japan
Oscar H. Ibarra	University of California, Santa Barbara, USA
Insup Lee	University of Pennsylvania, USA
Doron A. Peled	Bar Ilan University, Israel
Farn Wang	National Taiwan University, Taiwan
Hsu-Chun Yen	National Taiwan University, Taiwan

Program Committee

Aws Albarghouthi	University of Wisconsin-Madison, USA
Cyrille Valentin Artho	KTH Royal Institute of Technology, Sweden
Gogul Balakrishnan	Google, USA
Roderick Bloem	Graz University of Technology, Austria
Tevfik Bultan	University of California, Santa Barbara, USA
Pavol Cerny	University of Colorado at Boulder, USA
Sagar Chaki	Mentor Graphics, USA
Deepak D'Souza	Indian Institute of Science, Bangalore, India
Jyotirmoy Deshmukh	University of Southern California, USA
Constantin Enea	University Paris Diderot, France
Grigory Fedyukovich	Princeton University, USA
Masahiro Fujita	The University of Tokyo, Japan
Sicun Gao	University of California, San Diego, USA
Arie Gurfinkel	University of Waterloo, Canada
Fei He	Tsinghua University, China
Alan J. Hu	The University of British Columbia, Canada
Joxan Jaffar	National University of Singapore, Singapore
Akash Lal	Microsoft, India
Axel Legay	IRISA/Inria, Rennes, France
Yang Liu	Nanyang Technological University, Singapore
Zhiming Liu	Southwest University, China
K. Narayan Kumar	Chennai Mathematical Institute, India
Doron Peled	Bar Ilan University, Israel
Xiaokang Qiu	Purdue University, USA
Giles Reger	The University of Manchester, UK
Sandeep Shukla	Indian Institute of Technology Kanpur, India
Oleg Sokolsky	University of Pennsylvania, USA
Armando Solar-Lezama	MIT, USA
Neeraj Suri	TU Darmstadt, Germany

Aditya Thakur	University of California, Davis, USA
Willem Visser	Stellenbosch University, South Africa
Bow-Yaw Wang	Academia Sinica, Taiwan
Farn Wang	National Taiwan University, Taiwan
Georg Weissenbacher	Vienna University of Technology, Austria
Naijun Zhan	Chinese Academy of Sciences, China

Additional Reviewers

Akshay, S.	Lewchenko, Nicholas V.	Sangnier, Arnaud
Alt, Leonardo	Li, Yangjia	Sankaranarayanan, Sriram
Bastani, Osbert	Lin, Wang	Song, Fu
Bouajjani, Ahmed	Liu, Wanwei	Srivathsan, B.
Chen, Mingshuai	Luo, Chen	Suresh, S. P.
Chen, Wei	Maghareh, Rasool	Ting, Gan
Chen, Zhenbang	Matteplackel, Raj Mohan	Tizpaz Niari, Saeid
Ebrahim, Masoud	McClurg, Jedidiah	Trung, Ta Quang
Ge, Ning	Mordvinov, Dmitry	Wang, Chao
Habermehl, Peter	Pick, Lauren	Wang, Lingtai
Jansen, Nils	Poulsen, Danny	Xue, Bai
Karl, Anja	Poulsen, Dany	Yang, Zhibin
Katelaan, Jens	Praveen, M.	Yin, Liangze
Katis, Andreas	Qamar, Nafees	Zhang, Xin
Khalimov, Ayrat	Quilbeuf, Jean	
Koenighofer, Bettina	Riener, Martin	

Z3^{Azure} and Azure^{Z3}

(Abstract)

Nikolaj Bjørner¹, Marijn Heule², Karthick Jayaraman³,
and Rahul Kumar¹

¹ Microsoft Research

{nbjorner, rahulku}@microsoft.com

² UT Austin

marijn@heule.nl

³ Microsoft Azure

karjay@microsoft.com

Azure to the power of Z3: Cloud providers are increasingly embracing network verification for managing complex datacenter network infrastructure. Microsoft's Azure cloud infrastructure integrates the SecGuru tool, which leverages the Z3 SMT solver, for assuring that the network is configured to preserve desired intent. SecGuru statically validates correctness of access-control policies and routing tables of hundreds of thousands of network devices. For a structured network such as for Microsoft Azure data-centers, the intent for routing tables and access-control policies can be automatically derived from network architecture and metadata about address ranges hosted in the datacenter. We leverage this aspect to perform local checks on a per router basis. These local checks together assure reachability invariants for availability and performance. To make the service truly scalable, while using modest resources, SecGuru integrates a set of domain-specific optimizations that exploit properties of the configurations it needs to handle. Our experiences exemplify integration of general purpose verification technologies, in this case bit-vector solving, for a specific domain: the overall methodology available through SMT formalisms lowers the barrier of entry for capturing and checking contracts. They also alleviate initial needs for writing custom solvers. However, each domain reveals specific structure that produces new insights in the quest for scalable verification: for checking reachability properties in networks, methods for capturing symmetries in networks and header spaces can speed up verification by several orders of magnitude; for local checks on data-center routers we exploit common patterns in configurations to take the time it takes to check a contract from a few seconds to a few milliseconds.

Z3 to the power of Azure: Applications that rely on constraint solving may be in a fortunate situation where efficient solving technologies are adequately available. Several tools building on Z3 rely on this being the common case scenario. Then useful feedback can be produced within the attention span of a person performing program verification, and then the available compute time on a machine or a cluster is sufficient to complete thousands of small checks. As long as this fortunate situation holds, search techniques for SMT is a solved problem. Yet, in spite of rumors to the contrary, SAT

and SMT is by no means a solved problem. When current algorithmic techniques, in particular modern SAT solving search methods based on conflict-driven clause learning, are insufficient to quickly find solutions, a next remedy is to harness computational resources at problems. In the context of SAT solving, the method of Cube & Conquer, has been used with significant success to solve hard combinatorial problems from mathematical conjectures. These are relatively small formulas, but require a substantial search space for analysis. Formulas from applications, such as scheduling and timetabling, are significantly larger and have wildly different structural properties. In spite of these differences, we found that the Cube & Conquer methodology can make a substantial difference as fixing even a limited number of variables can drastically reduce the overhead solving subformulas. We describe a distributed version of Z3 that scales with Azure's elastic cloud. It integrates recent advances in lookahead and distributed SAT solving for Z3's engines for SMT. A multi-threaded version of the Cube & Conquer solver is also available parallelizing SAT and SMT queries.

Contents

Invited Papers

DeepSafe: A Data-Driven Approach for Assessing Robustness of Neural Networks	3
<i>Divya Gopinath, Guy Katz, Corina S. Păsăreanu, and Clark Barrett</i>	
Formal Specification for Deep Neural Networks	20
<i>Sanjit A. Seshia, Ankush Desai, Tommaso Dreossi, Daniel J. Fremont, Shromona Ghosh, Edward Kim, Sumukh Shivakumar, Marcell Vazquez-Chanlatte, and Xiangyu Yue</i>	

Regular Papers

Optimal Proofs for Linear Temporal Logic on Lasso Words	37
<i>David Basin, Bhargav Nagaraja Bhatt, and Dmitriy Traytel</i>	
What’s to Come is Still Unsure: Synthesizing Controllers Resilient to Delayed Interaction	56
<i>Mingshuai Chen, Martin Fränzle, Yangjia Li, Peter N. Mosaad, and Naijun Zhan</i>	
A Formally Verified Motion Planner for Autonomous Vehicles	75
<i>Albert Rizaldi, Fabian Immler, Bastian Schürmann, and Matthias Althoff</i>	
Robustness Testing of Intermediate Verifiers	91
<i>YuTing Chen and Carlo A. Furia</i>	
Simulation Algorithms for Symbolic Automata	109
<i>Lukáš Holík, Ondřej Lengál, Juraj Síc, Margus Veanes, and Tomáš Vojnar</i>	
Quantitative Projection Coverage for Testing ML-enabled Autonomous Systems	126
<i>Chih-Hong Cheng, Chung-Hao Huang, and Hirotooshi Yasuoka</i>	
Recursive Online Enumeration of All Minimal Unsatisfiable Subsets	143
<i>Jaroslav Bendik, Ivana Černá, and Nikola Beneš</i>	
Synthesis in pMDPs: A Tale of 1001 Parameters	160
<i>Murat Cubuktepe, Nils Jansen, Sebastian Junges, Joost-Pieter Katoen, and Ufuk Topcu</i>	

Temporal Logic Verification of Stochastic Systems Using Barrier Certificates	177
<i>Pushpak Jagtap, Sadegh Soudjani, and Majid Zamani</i>	
Bisimilarity Distances for Approximate Differential Privacy	194
<i>Dmitry Chistikov, Andrzej S. Murawski, and David Purser</i>	
A Symbolic Algorithm for Lazy Synthesis of Eager Strategies	211
<i>Swen Jacobs and Mouhammad Sakr</i>	
Modular Verification of Concurrent Programs via Sequential Model Checking	228
<i>Dan Rasin, Orna Grumberg, and Sharon Shoham</i>	
Quantifiers on Demand	248
<i>Arie Gurfinkel, Sharon Shoham, and Yakir Vizel</i>	
Signal Convolution Logic	267
<i>Simone Silveti, Laura Nenzi, Ezio Bartocci, and Luca Bortolussi</i>	
Efficient Symbolic Representation of Convex Polyhedra in High-Dimensional Spaces	284
<i>Bernard Boigelot and Isabelle Mainz</i>	
Accelerated Model Checking of Parametric Markov Chains	300
<i>Paul Gainer, Ernst Moritz Hahn, and Sven Schewe</i>	
Continuous-Time Markov Decisions Based on Partial Exploration	317
<i>Pranav Ashok, Yuliya Butkova, Holger Hermanns, and Jan Křetínský</i>	
A Fragment of Linear Temporal Logic for Universal Very Weak Automata . . .	335
<i>Keerthi Adabala and Rüdiger Ehlers</i>	
Quadratic Word Equations with Length Constraints, Counter Systems, and Presburger Arithmetic with Divisibility	352
<i>Anthony W. Lin and Rupak Majumdar</i>	
Round-Bounded Control of Parameterized Systems	370
<i>Benedikt Bollig, Mathieu Lehaut, and Nathalie Sznajder</i>	
PSense: Automatic Sensitivity Analysis for Probabilistic Programs	387
<i>Zixin Huang, Zhenbang Wang, and Sasa Misailovic</i>	
Information Leakage in Arbiter Protocols	404
<i>Nestan Tsiskaridze, Lucas Bang, Joseph McMahan, Teyfik Bultan, and Timothy Sherwood</i>	

Neural State Classification for Hybrid Systems	422
<i>Dung Phan, Nicola Paoletti, Timothy Zhang, Radu Grosu, Scott A. Smolka, and Scott D. Stoller</i>	
Bounded Synthesis of Reactive Programs	441
<i>Carsten Gersticker, Felix Klein, and Bernd Finkbeiner</i>	
Maximum Realizability for Linear Temporal Logic Specifications	458
<i>Rayna Dimitrova, Mahsa Ghasemi, and Ufuk Topcu</i>	
Ranking and Repulsing Supermartingales for Reachability in Probabilistic Programs	476
<i>Toru Takisaka, Yuichiro Oyabu, Natsuki Urabe, and Ichiro Hasuo</i>	
Bounded Synthesis of Register Transducers	494
<i>Ayrat Khalimov, Benedikt Maderbacher, and Roderick Bloem</i>	
Tool Papers	
ETHIR: A Framework for High-Level Analysis of Ethereum Bytecode	513
<i>Elvira Albert, Pablo Gordillo, Benjamin Livshits, Albert Rubio, and Ilya Sergey</i>	
MGHyper: Checking Satisfiability of HyperLTL Formulas Beyond the $\exists^*\forall^*$ Fragment	521
<i>Bernd Finkbeiner, Christopher Hahn, and Tobias Hans</i>	
Verifying Rust Programs with SMACK	528
<i>Marek Baranowski, Shaobo He, and Zvonimir Rakamarić</i>	
SBIP 2.0: Statistical Model Checking Stochastic Real-Time Systems	536
<i>Braham Lotfi Mediouni, Ayoub Nouri, Marius Bozga, Mahieddine Dellabani, Axel Legay, and Saddek Bensalem</i>	
Owl: A Library for ω -Words, Automata, and LTL	543
<i>Jan Křetínský, Tobias Meggendorfer, and Salomon Sickert</i>	
EVE: A Tool for Temporal Equilibrium Analysis	551
<i>Julian Gutierrez, Muhammad Najib, Giuseppe Perelli, and Michael Wooldridge</i>	
Author Index	559