

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/7407>

Hana Chockler · Georg Weissenbacher (Eds.)

Computer Aided Verification

30th International Conference, CAV 2018

Held as Part of the Federated Logic Conference, FloC 2018


Oxford, UK, July 14–17, 2018


Proceedings, Part I



Springer Open

Editors

Hana Chockler 
King's College
London
UK

Georg Weissenbacher 
TU Wien
Vienna
Austria



ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-96144-6 ISBN 978-3-319-96145-3 (eBook)
<https://doi.org/10.1007/978-3-319-96145-3>

Library of Congress Control Number: 2018948145

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

© The Editor(s) (if applicable) and The Author(s) 2018. This book is an open access publication.

Open Access This book is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this book are included in the book's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the book's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

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

It was our privilege to serve as the program chairs for CAV 2018, the 30th International Conference on Computer-Aided Verification. CAV is an annual conference dedicated to the advancement of the theory and practice of computer-aided formal analysis methods for hardware and software systems. CAV 2018 was held in Oxford, UK, July 14–17, 2018, with the tutorials day on July 13.

This year, CAV was held as part of the Federated Logic Conference (FLoC) event and was collocated with many other conferences in logic. The primary focus of CAV is to spur advances in hardware and software verification while expanding to new domains such as learning, autonomous systems, and computer security. CAV is at the cutting edge of research in formal methods, as reflected in this year’s program.

CAV 2018 covered a wide spectrum of subjects, from theoretical results to concrete applications, including papers on application of formal methods in large-scale industrial settings. It has always been one of the primary interests of CAV to include papers that describe practical verification tools and solutions and techniques that ensure a high practical appeal of the results. The proceedings of the conference are published in Springer’s *Lecture Notes in Computer Science* series. A selection of papers were invited to a special issue of *Formal Methods in System Design* and the *Journal of the ACM*.

This is the first year that the CAV proceedings are published under an Open Access license, thus giving access to CAV proceedings to a broad audience. We hope that this decision will increase the scope of practical applications of formal methods and will attract even more interest from industry.

CAV received a very high number of submissions this year—215 overall—resulting in a highly competitive selection process. We accepted 13 tool papers and 52 regular papers, which amounts to an acceptance rate of roughly 30% (for both regular papers and tool papers). The high number of excellent submissions in combination with the scheduling constraints of FLoC forced us to reduce the length of the talks to 15 minutes, giving equal exposure and weight to regular papers and tool papers.

The accepted papers cover a wide range of topics and techniques, from algorithmic and logical foundations of verification to practical applications in distributed, networked, cyber-physical, and autonomous systems. Other notable topics are synthesis, learning, security, and concurrency in the context of formal methods. The proceedings are organized according to the sessions in the conference.

The program featured two invited talks by Eran Yahav (Technion), on using deep learning for programming, and by Somesh Jha (University of Wisconsin Madison) on adversarial deep learning. The invited talks this year reflect the growing interest of the CAV community in deep learning and its connection to formal methods. The tutorial day of CAV featured two invited tutorials, by Shaz Qadeer on verification of concurrent programs and by Matteo Maffei on static analysis of smart contracts. The subjects of the tutorials reflect the increasing volume of research on verification of

concurrent software and, as of recently, the question of correctness of smart contracts. As every year, one of the winners of the CAV award also contributed a presentation. The tutorial day featured a workshop in memoriam of Mike Gordon, titled “Three Research Vignettes in Memory of Mike Gordon,” organized by Tom Melham and jointly supported by CAV and ITP communities.

Moreover, we continued the tradition of organizing a LogicLounge. Initiated by the late Helmut Veith at the Vienna Summer of Logic 2014, the LogicLounge is a series of discussions on computer science topics targeting a general audience and has become a regular highlight at CAV. This year’s LogicLounge took place at the Oxford Union and was on the topic of “Ethics and Morality of Robotics,” moderated by Judy Wajcman and featuring a panel of experts on the topic: Luciano Floridi, Ben Kuipers, Francesca Rossi, Matthias Scheutz, Sandra Wachter, and Jeannette Wing. We thank May Chan, Katherine Fletcher, and Marta Kwiatkowska for organizing this event, and the Vienna Center of Logic and Algorithms for their support.

In addition, CAV attendees enjoyed a number of FLoC plenary talks and events targeting the broad FLoC community.

In addition to the main conference, CAV hosted the Verification Mentoring Workshop for junior scientists entering the field and a high number of pre- and post-conference technical workshops: the Workshop on Formal Reasoning in Distributed Algorithms (FRIDA), the workshop on Runtime Verification for Rigorous Systems Engineering (RV4RISE), the 5th Workshop on Horn Clauses for Verification and Synthesis (HCVS), the 7th Workshop on Synthesis (SYNT), the First International Workshop on Parallel Logical Reasoning (PLR), the 10th Working Conference on Verified Software: Theories, Tools and Experiments (VSTTE), the Workshop on Machine Learning for Programming (MLP), the 11th International Workshop on Numerical Software Verification (NSV), the Workshop on Verification of Engineered Molecular Devices and Programs (VEMDP), the Third Workshop on Fun With Formal Methods (FWFM), the Workshop on Robots, Morality, and Trust through the Verification Lens, and the IFAC Conference on Analysis and Design of Hybrid Systems (ADHS).

The Program Committee (PC) for CAV consisted of 80 members; we kept the number large to ensure each PC member would have a reasonable number of papers to review and be able to provide thorough reviews. As the review process for CAV is double-blind, we kept the number of external reviewers to a minimum, to avoid accidental disclosures and conflicts of interest. Altogether, the reviewers drafted over 860 reviews and made an enormous effort to ensure a high-quality program. Following the tradition of CAV in recent years, the artifact evaluation was mandatory for tool submissions and optional but encouraged for regular submissions. We used an Artifact Evaluation Committee of 25 members. Our goal for artifact evaluation was to provide friendly “beta-testing” to tool developers; we recognize that developing a stable tool on a cutting-edge research topic is certainly not easy and we hope the constructive comments provided by the Artifact Evaluation Committee (AEC) were of help to the developers. As a result of the evaluation, the AEC accepted 25 of 31 artifacts accompanying regular papers; moreover, all 13 accepted tool papers passed the evaluation. We are grateful to the reviewers for their outstanding efforts in making sure each paper was fairly assessed. We would like to thank our artifact evaluation chair,

Igor Konnov, and the AEC for evaluating all artifacts submitted with tool papers as well as optional artifacts submitted with regular papers.

Of course, without the tremendous effort put into the review process by our PC members this conference would not have been possible. We would like to thank the PC members for their effort and thorough reviews.

We would like to thank the FLoC chairs, Moshe Vardi, Daniel Kroening, and Marta Kwiatkowska, for the support provided, Thanh Hai Tran for maintaining the CAV website, and the always helpful Steering Committee members Orna Grumberg, Aarti Gupta, Daniel Kroening, and Kenneth McMillan. Finally, we would like to thank the team at the University of Oxford, who took care of the administration and organization of FLoC, thus making our jobs as CAV chairs much easier.

July 2018

Hana Chockler
Georg Weissenbacher

Organization

Program Committee

Aws Albarghouthi	University of Wisconsin-Madison, USA
Christel Baier	TU Dresden, Germany
Clark Barrett	Stanford University, USA
Ezio Bartocci	TU Wien, Austria
Dirk Beyer	LMU Munich, Germany
Per Bjesse	Synopsys Inc., USA
Jasmin Christian Blanchette	Vrije Universiteit Amsterdam, Netherlands
Roderick Bloem	Graz University of Technology, Austria
Ahmed Bouajjani	IRIF, University Paris Diderot, France
Pavol Cerny	University of Colorado Boulder, USA
Rohit Chadha	University of Missouri, USA
Swarat Chaudhuri	Rice University, USA
Wei-Ngan Chin	National University of Singapore, Singapore
Hana Chockler	King's College London, UK
Alessandro Cimatti	Fondazione Bruno Kessler, Italy
Loris D'Antoni	University of Wisconsin-Madison, USA
Vijay D'Silva	Google, USA
Cristina David	University of Cambridge, UK
Jyotirmoy Deshmukh	University of Southern California, USA
Isil Dillig	The University of Texas at Austin, USA
Cezara Dragoi	Inria Paris, ENS, France
Kerstin Eder	University of Bristol, UK
Michael Emmi	Nokia Bell Labs, USA
Georgios Fainekos	Arizona State University, USA
Dana Fisman	University of Pennsylvania, USA
Vijay Ganesh	University of Waterloo, Canada
Sicun Gao	University of California San Diego, USA
Alberto Griggio	Fondazione Bruno Kessler, Italy
Orna Grumberg	Technion - Israel Institute of Technology, Israel
Arie Gurfinkel	University of Waterloo, Canada
William Harrison	Department of CS, University of Missouri, Columbia, USA
Gerard Holzmann	Nimble Research, USA
Alan J. Hu	The University of British Columbia, Canada
Franjo Ivancic	Google, USA
Alexander Ivrii	IBM, Israel
Himanshu Jain	Synopsys, USA
Somesh Jha	University of Wisconsin-Madison, USA

Susmit Jha	SRI International, USA
Ranjit Jhala	University of California San Diego, USA
Barbara Jobstmann	EPFL and Cadence Design Systems, Switzerland
Stefan Kiefer	University of Oxford, UK
Zachary Kincaid	Princeton University, USA
Laura Kovacs	TU Wien, Austria
Viktor Kuncak	Ecole Polytechnique Fédérale de Lausanne, Switzerland
Orna Kupferman	Hebrew University, Israel
Shuvendu Lahiri	Microsoft, USA
Rupak Majumdar	MPI-SWS, Germany
Ken McMillan	Microsoft, USA
Alexander Nadel	Intel, Israel
Mayur Naik	Intel, USA
Kedar Namjoshi	Nokia Bell Labs, USA
Dejan Nickovic	Austrian Institute of Technology AIT, Austria
Corina Pasareanu	CMU/NASA Ames Research Center, USA
Nir Piterman	University of Leicester, UK
Pavithra Prabhakar	Kansas State University, USA
Mitra Purandare	IBM Research Laboratory Zurich, Switzerland
Shaz Qadeer	Microsoft, USA
Arjun Radhakrishna	Microsoft, USA
Noam Rinetzky	Tel Aviv University, Israel
Philipp Ruemmer	Uppsala University, Sweden
Roopsha Samanta	Purdue University, USA
Sriram Sankaranarayanan	University of Colorado, Boulder, USA
Martina Seidl	Johannes Kepler University Linz, Austria
Koushik Sen	University of California, Berkeley, USA
Sanjit A. Seshia	University of California, Berkeley, USA
Natasha Sharygina	Università della Svizzera Italiana, Lugano, Switzerland
Sharon Shoham	Tel Aviv University, Israel
Anna Slobodova	Centaur Technology, USA
Armando Solar-Lezama	MIT, USA
Ofer Strichman	Technion, Israel
Serdar Tasiran	Amazon Web Services, USA
Caterina Urban	ETH Zurich, Switzerland
Yakir VizeI	Technion, Israel
Tomas Vojnar	Brno University of Technology, Czechia
Thomas Wahl	Northeastern University, USA
Bow-Yaw Wang	Academia Sinica, Taiwan
Georg Weissenbacher	TU Wien, Austria
Thomas Wies	New York University, USA
Karen Yorav	IBM Research Laboratory Haifa, Israel
Lenore Zuck	University of Illinois in Chicago, USA
Damien Zufferey	MPI-SWS, Germany
Florian Zuleger	TU Wien, Austria

Artifact Evaluation Committee

Thibaut Balabonski	Université Paris-Sud, France
Sergiy Bogomolov	The Australian National University, Australia
Simon Cruanes	Aesthetic Integration, USA
Matthias Dangl	LMU Munich, Germany
Eva Darulova	Max Planck Institute for Software Systems, Germany
Ramiro Demasi	Universidad Nacional de Córdoba, Argentina
Grigory Fedyukovich	Princeton University, USA
Johannes Hölzl	Vrije Universiteit Amsterdam, The Netherlands
Jochen Hoenicke	University of Freiburg, Germany
Antti Hyvärinen	Università della Svizzera Italiana, Lugano, Switzerland
Swen Jacobs	Saarland University, Germany
Saurabh Joshi	IIT Hyderabad, India
Dejan Jovanovic	SRI International, USA
Ayrat Khalimov	The Hebrew University, Israel
Igor Konnov (Chair)	Inria Nancy (LORIA), France
Jan Kretínský	Technical University of Munich, Germany
Alfons Laarman	Leiden University, The Netherlands
Ravichandhran Kandhadai Madhavan	Ecole Polytechnique Fédérale de Lausanne, Switzerland
Andrea Micheli	Fondazione Bruno Kessler, Italy
Sergio Mover	University of Colorado Boulder, USA
Aina Niemetz	Stanford University, USA
Burcu Kulahcioglu Ozkan	MPI-SWS, Germany
Markus N. Rabe	University of California, Berkeley, USA
Andrew Reynolds	University of Iowa, USA
Martin Suda	TU Wien, Austria
Mitra Tabaei	TU Wien, Austria

Additional Reviewers

Alpernas, Kalev	Cohen, Ernie	Friedberger, Karlheinz
Asadi, Sepideh	Costea, Andreea	Ghorbani, Soudeh
Athanasίου, Konstantinos	Dangl, Matthias	Ghosh, Shromona
Bauer, Matthew	Doko, Marko	Goel, Shilpi
Bavishi, Rohan	Drachsler Cohen, Dana	Gong, Liang
Bayless, Sam	Dreossi, Tommaso	Govind, Hari
Berzish, Murphy	Dutra, Rafael	Gu, Yijia
Blich, Martin	Ebrahimi, Masoud	Habermehl, Peter
Bui, Phi Diep	Eisner, Cindy	Hamza, Jad
Cauderlier, Raphaël	Fedyukovich, Grigory	He, Paul
Cauli, Claudia	Fremont, Daniel	Heo, Kihong
Ceska, Milan	Freund, Stephen	Holik, Lukas

Humenberger, Andreas	Maffei, Matteo	Reynolds, Andrew
Hyvärinen, Antti	Marescotti, Matteo	Reynolds, Thomas
Hözl, Johannes	Mathur, Umang	Ritirc, Daniela
Iusupov, Rinat	Miné, Antoine	Rogalewicz, Adam
Jacobs, Swen	Mora, Federico	Scott, Joe
Jain, Mitesh	Nevo, Ziv	Shacham, Ohad
Jaroschek, Maximilian	Ochoa, Martin	Song, Yahui
Jha, Sumit Kumar	Orni, Avigail	Sosnovich, Adi
Keidar-Barner, Sharon	Ouaknine, Joel	Sousa, Marcelo
Khalimov, Ayrat	Padhye, Rohan	Subramanian, Kausik
Kiesl, Benjamin	Padon, Oded	Sumners, Rob
Koenighofer, Bettina	Partush, Nimrod	Swords, Sol
Krstic, Srdjan	Pavlinovic, Zvonimir	Ta, Quang Trung
Laeufer, Kevin	Pavlogiannis, Andreas	Tautschnig, Michael
Lee, Woosuk	Peled, Doron	Traytel, Dmitriy
Lemberger, Thomas	Pendharkar, Ishan	Trivedi, Ashutosh
Lemieux, Caroline	Peng, Yan	Udupa, Abhishek
Lewis, Robert	Petri, Gustavo	van Dijk, Tom
Liang, Jia	Polozov, Oleksandr	Wendler, Philipp
Liang, Jimmy	Popescu, Andrei	Zdancewic, Steve
Liu, Peizun	Potomkin, Kostiantyn	Zulkoski, Ed
Lång, Magnus	Raghothaman, Mukund	

Contents – Part I

Invited Papers

Semantic Adversarial Deep Learning	3
<i>Tommaso Dreossi, Somesh Jha, and Sanjit A. Seshia</i>	
From Programs to Interpretable Deep Models and Back.	27
<i>Eran Yahav</i>	
Formal Reasoning About the Security of Amazon Web Services.	38
<i>Byron Cook</i>	

Tutorials

Foundations and Tools for the Static Analysis of Ethereum Smart Contracts. . .	51
<i>Ilya Grishchenko, Matteo Maffei, and Clara Schneidewind</i>	
Layered Concurrent Programs.	79
<i>Bernhard Kragl and Shaz Qadeer</i>	

Model Checking

Propositional Dynamic Logic for Higher-Order Functional Programs.	105
<i>Yuki Satake and Hiroshi Unno</i>	
Syntax-Guided Termination Analysis.	124
<i>Grigory Fedyukovich, Yueling Zhang, and Aarti Gupta</i>	
Model Checking Quantitative Hyperproperties	144
<i>Bernd Finkbeiner, Christopher Hahn, and Hazem Torfah</i>	
Exploiting Synchrony and Symmetry in Relational Verification	164
<i>Lauren Pick, Grigory Fedyukovich, and Aarti Gupta</i>	
JBMC: A Bounded Model Checking Tool for Verifying Java Bytecode.	183
<i>Lucas Cordeiro, Pascal Kesseli, Daniel Kroening, Peter Schrammel, and Marek Trtik</i>	
Eager Abstraction for Symbolic Model Checking	191
<i>Kenneth L. McMillan</i>	

Program Analysis Using Polyhedra

Fast Numerical Program Analysis with Reinforcement Learning 211
Gagandeep Singh, Markus Püschel, and Martin Vechev

A Direct Encoding for NNC Polyhedra 230
Anna Becchi and Enea Zaffanella

Synthesis

What’s Hard About Boolean Functional Synthesis? 251
S. Akshay, Supratik Chakraborty, Shubham Goel, Sumith Kulal, and Shetal Shah

Counterexample Guided Inductive Synthesis Modulo Theories 270
Alessandro Abate, Cristina David, Pascal Kesseli, Daniel Kroening, and Elizabeth Polgreen

Synthesizing Reactive Systems from Hyperproperties 289
Bernd Finkbeiner, Christopher Hahn, Philip Lukert, Marvin Stenger, and Leander Tentrup

Reactive Control Improvisation 307
Daniel J. Fremont and Sanjit A. Seshia

Constraint-Based Synthesis of Coupling Proofs 327
Aws Albarghouthi and Justin Hsu

Controller Synthesis Made Real: Reach-Avoid Specifications and Linear Dynamics 347
Chuchu Fan, Umang Mathur, Sayan Mitra, and Mahesh Viswanathan

Synthesis of Asynchronous Reactive Programs from Temporal Specifications 367
Suguman Bansal, Kedar S. Namjoshi, and Yaniv Sa’ar

Syntax-Guided Synthesis with Quantitative Syntactic Objectives 386
Qinheping Hu and Loris D’Antoni

Learning

Learning Abstractions for Program Synthesis 407
Xinyu Wang, Greg Anderson, Isil Dillig, and K. L. McMillan

The Learnability of Symbolic Automata 427
George Argyros and Loris D’Antoni

Runtime Verification, Hybrid and Timed Systems

Reachable Set Over-Approximation for Nonlinear Systems Using Piecewise Barrier Tubes	449
<i>Hui Kong, Ezio Bartocci, and Thomas A. Henzinger</i>	
Space-Time Interpolants.	468
<i>Goran Frehse, Mirco Giacobbe, and Thomas A. Henzinger</i>	
Monitoring Weak Consistency	487
<i>Michael Emmi and Constantin Enea</i>	
Monitoring CTMCs by Multi-clock Timed Automata.	507
<i>Yijun Feng, Joost-Pieter Katoen, Haokun Li, Bican Xia, and Naijun Zhan</i>	
Start Pruning When Time Gets Urgent: Partial Order Reduction for Timed Systems	527
<i>Frederik M. Bønneland, Peter Gjør Jensen, Kim Guldstrand Larsen, Marco Muñoz, and Jiří Srba</i>	
A Counting Semantics for Monitoring LTL Specifications over Finite Traces	547
<i>Ezio Bartocci, Roderick Bloem, Dejan Nickovic, and Franz Roeck</i>	

Tools

Rabinizer 4: From LTL to Your Favourite Deterministic Automaton	567
<i>Jan Křetínský, Tobias Meggendorfer, Salomon Sickert, and Christopher Ziegler</i>	
Strix: Explicit Reactive Synthesis Strikes Back!	578
<i>Philipp J. Meyer, Salomon Sickert, and Michael Luttenberger</i>	
Btor2 , BtorMC and Boolector 3.0	587
<i>Aina Niemetz, Mathias Preiner, Clifford Wolf, and Armin Biere</i>	
Nagini: A Static Verifier for Python	596
<i>Marco Eilers and Peter Müller</i>	
PEREGRINE: A Tool for the Analysis of Population Protocols	604
<i>Michael Blondin, Javier Esparza, and Stefan Jaax</i>	
ADAC: Automated Design of Approximate Circuits	612
<i>Milan Češka, Jiří Matyáš, Vojtech Mrazek, Lukas Sekanina, Zdenek Vasicek, and Tomáš Vojnar</i>	

Probabilistic Systems

Value Iteration for Simple Stochastic Games: Stopping Criterion and Learning Algorithm.	623
<i>Edon Kelmendi, Julia Krämer, Jan Křetínský, and Maximilian Weininger</i>	
Sound Value Iteration	643
<i>Tim Quatmann and Joost-Pieter Katoen</i>	
Safety-Aware Apprenticeship Learning	662
<i>Weichao Zhou and Wenchao Li</i>	
Deciding Probabilistic Bisimilarity Distance One for Labelled Markov Chains	681
<i>Qiyi Tang and Franck van Breugel</i>	
Author Index	701

Contents – Part II

Tools

Let this Graph Be Your Witness! An Attestor for Verifying Java Pointer Programs.	3
<i>Hannah Arndt, Christina Jansen, Joost-Pieter Katoen, Christoph Matheja, and Thomas Noll</i>	
MaxSMT-Based Type Inference for Python 3.	12
<i>Mostafa Hassan, Caterina Urban, Marco Eilers, and Peter Müller</i>	
The JKIND Model Checker	20
<i>Andrew Gacek, John Backes, Mike Whalen, Lucas Wagner, and Elaheh Ghassabani</i>	
The DEEPSEC Prover.	28
<i>Vincent Cheval, Steve Kremer, and Itsaka Rakotonirina</i>	
SimpleCAR: An Efficient Bug-Finding Tool Based on Approximate Reachability	37
<i>Jianwen Li, Rohit Dureja, Geguang Pu, Kristin Yvonne Rozier, and Moshe Y. Vardi</i>	
StringFuzz: A Fuzzer for String Solvers.	45
<i>Dmitry Blotsky, Federico Mora, Murphy Berzish, Yunhui Zheng, Ifaz Kabir, and Vijay Ganesh</i>	

Static Analysis

Permission Inference for Array Programs	55
<i>Jérôme Dohrau, Alexander J. Summers, Caterina Urban, Severin Münger, and Peter Müller</i>	
Program Analysis Is Harder Than Verification: A Computability Perspective	75
<i>Patrick Cousot, Roberto Giacobazzi, and Francesco Ranzato</i>	

Theory and Security

Automata vs Linear-Programming Discounted-Sum Inclusion	99
<i>Suguman Bansal, Swarat Chaudhuri, and Moshe Y. Vardi</i>	

Model Checking Indistinguishability of Randomized Security Protocols	117
<i>Matthew S. Bauer, Rohit Chadha, A. Prasad Sista, and Mahesh Viswanathan</i>	
Lazy Self-composition for Security Verification	136
<i>Weikun Yang, Yakir Vizel, Pramod Subramanyan, Aarti Gupta, and Sharad Malik</i>	
SCINFER: Refinement-Based Verification of Software Countermeasures Against Side-Channel Attacks.	157
<i>Jun Zhang, Pengfei Gao, Fu Song, and Chao Wang</i>	
Symbolic Algorithms for Graphs and Markov Decision Processes with Fairness Objectives	178
<i>Krishnendu Chatterjee, Monika Henzinger, Veronika Loitzenbauer, Simin Oraee, and Viktor Toman</i>	
Attracting Tangles to Solve Parity Games	198
<i>Tom van Dijk</i>	
SAT, SMT and Decision Procedures	
Delta-Decision Procedures for Exists-Forall Problems over the Reals.	219
<i>Soonho Kong, Armando Solar-Lezama, and Sicun Gao</i>	
Solving Quantified Bit-Vectors Using Invertibility Conditions.	236
<i>Aina Niemetz, Mathias Preiner, Andrew Reynolds, Clark Barrett, and Cesare Tinelli</i>	
Understanding and Extending Incremental Determinization for 2QBF	256
<i>Markus N. Rabe, Leander Tentrup, Cameron Rasmussen, and Sanjit A. Seshia</i>	
The Proof Complexity of SMT Solvers	275
<i>Robert Robere, Antonina Kolokolova, and Vijay Ganesh</i>	
Model Generation for Quantified Formulas: A Taint-Based Approach	294
<i>Benjamin Farinier, Sébastien Bardin, Richard Bonichon, and Marie-Laure Potet</i>	
Concurrency	
Partial Order Aware Concurrency Sampling	317
<i>Xinhao Yuan, Junfeng Yang, and Ronghui Gu</i>	
Reasoning About TSO Programs Using Reduction and Abstraction	336
<i>Ahmed Bouajjani, Constantin Enea, Suha Orhun Mutluergil, and Serdar Tasiran</i>	

Quasi-Optimal Partial Order Reduction	354
<i>Huyen T. T. Nguyen, César Rodríguez, Marcelo Sousa, Camille Coti, and Laure Petrucci</i>	
On the Completeness of Verifying Message Passing Programs Under Bounded Asynchrony	372
<i>Ahmed Bouajjani, Constantin Enea, Kailiang Ji, and Shaz Qadeer</i>	
Constrained Dynamic Partial Order Reduction	392
<i>Elvira Albert, Miguel Gómez-Zamalloa, Miguel Isabel, and Albert Rubio</i>	
CPS, Hardware, Industrial Applications	
Formal Verification of a Vehicle-to-Vehicle (V2V) Messaging System	413
<i>Mark Tullsen, Lee Pike, Nathan Collins, and Aaron Tomb</i>	
Continuous Formal Verification of Amazon s2n	430
<i>Andrey Chudnov, Nathan Collins, Byron Cook, Joey Dodds, Brian Huffman, Colm MacCárthaigh, Stephen Magill, Eric Mertens, Eric Mullen, Serdar Tasiran, Aaron Tomb, and Eddy Westbrook</i>	
Symbolic Liveness Analysis of Real-World Software.	447
<i>Daniel Schemmel, Julian Bünig, Oscar Soria Dustmann, Thomas Noll, and Klaus Wehrle</i>	
Model Checking Boot Code from AWS Data Centers	467
<i>Byron Cook, Kareem Khazem, Daniel Kroening, Serdar Tasiran, Michael Tautschnig, and Mark R. Tuttle</i>	
Android Stack Machine	487
<i>Taolue Chen, Jinlong He, Fu Song, Guozhen Wang, Zhilin Wu, and Jun Yan</i>	
Formally Verified Montgomery Multiplication	505
<i>Christoph Walther</i>	
Inner and Outer Approximating Flowpipes for Delay Differential Equations . . .	523
<i>Eric Goubault, Sylvie Putot, and Lorenz Sahlmann</i>	
Author Index	543