

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, 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>

Rupak Majumdar · Viktor Kunčák (Eds.)

Computer Aided Verification

29th International Conference, CAV 2017
Heidelberg, Germany, July 24–28, 2017
Proceedings, Part II

Editors

Rupak Majumdar
Max Planck Institute for Software Systems
Kaiserslautern, Rheinland-Pfalz
Germany

Viktor Kunčák
School of Computer and Communication
Sciences
EPFL - IC - LARA
Lausanne
Switzerland

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-63389-3 ISBN 978-3-319-63390-9 (eBook)
DOI 10.1007/978-3-319-63390-9

Library of Congress Control Number: 2017946069

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

© Springer International Publishing AG 2017

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.

Printed on acid-free paper

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

Preface

It has been our privilege to serve as the program chairs for CAV 2017, the 29th International Conference on Computer-Aided Verification. CAV 2017 was held in beautiful Heidelberg, Germany, during July 22–28, 2017. The pre-conference workshops took place at the Crowne Plaza Hotel in Heidelberg City Centre. The main conference took place at the Stadthalle by the river Neckar.

The CAV conference series is dedicated to the advancement of the theory and practice of computer-aided formal analysis of hardware and software systems. The conference covers the spectrum from theoretical results to concrete applications, with an emphasis on practical verification tools and the algorithms and techniques that are needed for their implementation. CAV considers it vital to continue spurring advances in hardware and software verification while expanding to new domains such as biological systems and computer security.

Out of 191 submissions to the conference, we chose 50 regular papers and seven tool papers. These papers cover a wide range of topics and techniques, from algorithmic and logical foundations of verification to practical applications in distributed, networked, and cyber-physical systems. One direction of topical interest is the increasingly sophisticated combination of “traditional” techniques for reasoning and search with data-driven techniques. The program featured invited talks by Chris Hawblitzel (Microsoft), Marta Kwiatkowska (Oxford), and Viktor Vafeiadis (MPI-SWS), as well as invited tutorials, by Loris D’Antoni and Mayur Naik. As traditional, one of the winners of the CAV award also gave a presentation. We also had a special workshop to celebrate David Dill’s many contributions to CAV on the occasion of his 60th birthday.

In addition to the main conference, CAV hosted the Verification Mentoring Workshop for junior scientists entering the field and six pre-conference technical workshops: the Workshop on Synthesis (SYNT), Satisfiability Modulo Theories (SMT), Verified Software: Theories, Tools, and Experiments (VSTTE), Design and Analysis of Robust Systems (DARS), Formal Approaches to Explainable Verification (FEVER), and Numerical Software Verification (NSV).

Organizing a conference is a community effort. The Program Committee for CAV consisted of 56 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. In addition, we used 104 external reviewers. All together, the reviewers drafted over 730 reviews and put in enormous effort in ensuring a good-quality program.

This year, we made artifact evaluation mandatory for tool submissions and optional but encouraged for regular submissions. We used an artifact evaluation committee of 26 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 AEC were of help to the developers. Needless to say we were impressed by the quality

of the artifacts and in fact all accepted tools passed artifact evaluation. We are grateful to the reviewers for their outstanding efforts in making sure each paper got a fair chance.

We would like to thank Eva Darulova for chairing the workshop organization process, Barbara Jobstmann and Thomas Wahl for managing sponsorship and student fellowships, respectively, Mikaël Mayer for maintaining the CAV website, and the always helpful Steering Committee members Orna Grumberg, Aarti Gupta, Daniel Kroening, and Kenneth McMillan. We worked closely with Pavithra Prabhakar, Andrey Rybalchenko, and Damien Zufferey, who organized the Verification Mentoring Workshop. Finally, we would like to thank Roslyn Stricker, who helped us tremendously in the administration and organization of CAV.

We hope that you find the proceedings of CAV 2017 thought provoking!

July 2017

Rupak Majumdar
Viktor Kunčák

Organization

Program Chairs

Rupak Majumdar Max Planck Institute for Software Systems, Germany
Viktor Kunčák EPFL, Switzerland

Workshop Chair

Eva Darulova Max Planck Institute for Software Systems, Germany

Sponsorship Chair

Barbara Jobstmann EPFL, Switzerland and Cadence Design Systems

Fellowship Chair

Thomas Wahl Northeastern University, USA

Program Committee

Aws Albarghouthi	University of Wisconsin, USA
Christel Baier	TU Dresden, Germany
Per Bjesse	Synopsys, USA
Jasmin Blanchette	Inria Nancy – Grand Est, France
Sergiy Bogomolov	Australian National University, Australia
Ahmed Bouajjani	IRIF, Paris Diderot University, France
Rohit Chadha	University of Missouri, USA
Bor-Yuh Evan Chang	University of Colorado at Boulder, 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
Isil Dilig	University of Texas at Austin, USA
Dino Distefano	Facebook and Queen Mary University of London, UK
Michael Emmi	Nokia Bell Labs, USA
Javier Esparza	TU Munich, Germany
Georgios Fainekos	Arizona State University, USA
Azadeh Farzan	University of Toronto, Canada
Aarti Gupta	Princeton University, USA
Gerard Holzmann	Nimble Research, USA
Marieke Huisman	University of Twente, The Netherlands
Radu Iosif	Verimag, France

Franjo Ivančić	Google, USA
Stefan Kiefer	Oxford University, UK
Zachary Kincaid	Princeton University, USA
Barbara König	University of Duisburg-Essen, Germany
Daniel Kroening	Oxford University, UK
Rustan Leino	Microsoft Research, USA
Kenneth McMillan	Microsoft Research, Redmond, USA
Alexander Nadel	Intel, USA
Madhusudan	University of Illinois at Urbana Champaign, USA
Parthasarathy	
Corina Pasareanu	NASA Ames and Carnegie Mellon University, USA
Nadia Polikarpova	MIT, USA
Pavithra Prabhakar	Kansas State University, USA
Arjun Radhakrishna	University of Pennsylvania, USA
Zvonimir Rakamaric	University of Utah, USA
Andrey Rybalchenko	Microsoft Research, Cambridge, UK
Roopsha Samanta	Purdue University, USA
Rahul Sharma	Microsoft Research, India
Anna Slobodova	Centaur Technology, USA
Ana Sokolova	University of Salzburg, Austria
Zhendong Su	University of California at Davis, USA
Serdar Tasiran	Amazon Web Services, USA
Emina Torlak	University of Washington, USA
Willem Visser	Stellenbosch University, South Africa
Mahesh Viswanathan	University of Illinois at Urbana Champaign, USA
Yakir Vizel	Princeton University, USA
Tomas Vojnar	Brno University of Technology, Czechia
Thomas Wahl	Northeastern University, USA
Bow-Yaw Wang	Academia Sinica, Taiwan
Georg Weissenbacher	Vienna University of Technology, Austria
Verena Wolf	Saarland University, Germany
Lenore Zuck	University of Illinois at Chicago, USA
Damien Zufferey	Max Planck Institute for Software Systems, Germany

Artifact Evaluation Committee

Ayca Balkan	University of California, Los Angeles, USA
Stephanie Balzer	Carnegie Mellon University, USA
James Bornholt	University of Washington, USA
Simon Cruanes	Inria Nancy, France
Matthias Dangel	University of Passau, Germany
Marko Doko	Max Planck Institute for Software Systems, Germany
Chuchu Fan	University of Illinois, Urbana-Champaign, USA
Pietro Ferrara	Julia Software, Italy
Johannes Hoelzl	TU Munich, Germany
Lars Hupel	TU Munich, Germany

Swen Jacobs	Saarland University, Germany
Moa Johansson	Chalmers, Sweden
Dejan Jovanovic	SRI International, USA
Ralf Jung	Max Planck Institute for Software Systems, Germany
Ivan Kuraj	MIT, USA
Andreas Lochbihler	ETH Zurich, Switzerland
Jose Morales	IMDEA Software, Spain
Van Chan Ngo	Carnegie Mellon University, USA
Zvonimir Pavlinovic	New York University, USA
Markus Rabe	University of California, Berkeley, USA
Mukund Raghothaman	University of Pennsylvania, USA
Andrew Reynolds	University of Iowa, USA
Nima Roohi	University of Illinois, Urbana-Champaign, USA
Christian Schilling	University of Freiburg, Germany
Muralidaran Vijayaraghavan	MIT, USA
Nicolas Voirol	EPFL, Switzerland

Additional Reviewers

Alireza Abyaneh	Constantin Enea	K. Narayan Kumar
Mahmudul Faisal	Chuchu Fan	Sebastian Küpper
Al Ameen	Samira Farahani	Axel Legay
Sebastian Arming	Grigory Fedyukovich	Sorin Lerner
Konstantinos Athanasiou	Pierre Flener	Peizin Liu
Mohamed Faouzi Atig	Matthias Fleury	Le Quang Loc
Domagoj Babic	Wan Fokkink	Andreas Lochbihler
Michael Backenköhler	Zhoulai Fu	Alexander Lück
Gogul Balakrishnan	Nils Gesbert	Ravichandran Madhavan
Clark Barrett	Shilpi Goel	Victor Magron
Matthew Bauer	Yijia Gu	Assaf Marron
Ryan Beckett	Arie Gurfinkel	Umang Mathur
Harsh Beohar	Vahid Hashemi	Todd Millstein
Olaf Beyersdorff	Bardh Hoxha	Sergio Mover
Pavol Bielik	Johannes Hölzl	Suvam Mukherjee
Armin Biere	Catalin Hritcu	Daniel Neider
Jesse Bingham	Mens Irini-Eleftheria	Dennis Nolte
Stefan Blom	Himanshu Jain	Peter O'Hearn
Stefan Bucur	Chuan Jiang	Wytse Oortwijn
Dario Cattaruzza	George Karpenkov	Gustavo Petri
Ed Cerny	Dileep Kini	Lauren Pick
Le Ton Chanh	Hui Kong	Markus Rabe
Dmitry Chistikov	Aamod Kore	Jaideep Ramachandran
Andreea Costea	Jan Křetínský	Rajarshi Ray
Eva Darulova	Thilo Krüger	Andrew Reynolds

Nima Roohi	Ofer Strichman	Mike Whalen
Philipp Ruemmer	Kausik Subramanian	Christoph Wintersteiger
Sarah Sallinger	Rob Sumners	Xiao Xu
Anne-Kathrin Schmuck	Sol Swords	Shakiba Yaghoubi
Peter Schrammel	Michael Tautschnig	Eugen Zalinescu
Daniel Schwartz-Narbonne	Nguyen Toan Thanh	Qirun Zhang
Cristina Serban	Dmitriy Traytel	Yiji Zhang
Alexey Solovyev	Nikos Tzevelekos	Cai Zhouhong
Sadegh Soudjani	Viktor Vafeiadis	Florian Zuleger
Benno Stein	Freak van der Berg	
	Jules Villard	

Steering Committee

Orna Grumberg	Technion, Israel
Aarti Gupta	Princeton University, USA
Daniel Kroening	Oxford University, UK
Kenneth McMillan	Microsoft Research, USA

CAV Award Committee

Tom Ball (Chair)	Microsoft Research, USA
Kim G. Larsen	Aalborg University, Denmark
Natarajan Shankar	SRI International, USA
Pierre Wolper	Liege University, Belgium

Verification Mentoring Workshop

Pavithra Prabhakar	Kansas State University, USA
Andrey Rybalchenko	Microsoft Research, UK
Damien Zufferey	Max Planck Institute for Software Systems, Germany

Publicity Chair

Mikaël Mayer	EPFL, Switzerland
--------------	-------------------

Contents – Part II

Analysis of Software and Hardware

Verified Compilation of Space-Efficient Reversible Circuits	3
<i>Matthew Amy, Martin Roetteler, and Krysta M. Svore</i>	
Ascertaining Uncertainty for Efficient Exact Cache Analysis	22
<i>Valentin Touzeau, Claire Maïza, David Monniaux, and Jan Reineke</i>	
Non-polynomial Worst-Case Analysis of Recursive Programs	41
<i>Krishnendu Chatterjee, Hongfei Fu, and Amir Kafshdar Goharshady</i>	
Automated Resource Analysis with Coq Proof Objects	64
<i>Quentin Carbonneaux, Jan Hoffmann, Thomas Reps, and Zhong Shao</i>	
Look for the Proof to Find the Program: Decorated-Component-Based Program Synthesis.	86
<i>Adrià Gascón, Ashish Tiwari, Brent Carmer, and Umang Mathur</i>	
E-QED: Electrical Bug Localization During Post-silicon Validation Enabled by Quick Error Detection and Formal Methods.	104
<i>Eshan Singh, Clark Barrett, and Subhasish Mitra</i>	
SMTCoq: A Plug-In for Integrating SMT Solvers into Coq	126
<i>Burak Ekici, Alain Mebsout, Cesare Tinelli, Chantal Keller, Guy Katz, Andrew Reynolds, and Clark Barrett</i>	

Foundations of Verification

Efficient Parallel Strategy Improvement for Parity Games	137
<i>John Fearnley</i>	
Model-Checking Linear-Time Properties of Parametrized Asynchronous Shared-Memory Pushdown Systems	155
<i>Marie Fortin, Anca Muscholl, and Igor Walukiewicz</i>	
Minimization of Symbolic Transducers	176
<i>Olli Saarikivi and Margus Veanes</i>	
Abstract Interpretation with Unfoldings	197
<i>Marcelo Sousa, César Rodríguez, Vijay D'Silva, and Daniel Kroening</i>	
Cutoff Bounds for Consensus Algorithms.	217
<i>Ognjen Marić, Christoph Sprenger, and David Basin</i>	

Towards Verifying Nonlinear Integer Arithmetic	238
<i>Paul Beame and Vincent Liew</i>	

Distributed and Networked Systems

Network-Wide Configuration Synthesis	261
<i>Ahmed El-Hassany, Petar Tsankov, Laurent Vanbever, and Martin Vechev</i>	
Verifying Equivalence of Spark Programs	282
<i>Shelly Grossman, Sara Cohen, Shachar Itzhaky, Noam Rinetzkyy, and Mooly Sagiv</i>	
Synchronization Synthesis for Network Programs	301
<i>Jedidiah McClurg, Hossein Hojjat, and Pavol Černý</i>	

Synthesis

BoSy: An Experimentation Framework for Bounded Synthesis	325
<i>Peter Faymonville, Bernd Finkbeiner, and Leander Tenstrup</i>	
Bounded Synthesis for Streett, Rabin, and CTL*	333
<i>Ayrat Khalimov and Roderick Bloem</i>	
Quantitative Assume Guarantee Synthesis	353
<i>Shaull Almagor, Orna Kupferman, Jan Oliver Ringert, and Yaron Velner</i>	
Syntax-Guided Optimal Synthesis for Chemical Reaction Networks.	375
<i>Luca Cardelli, Milan Češka, Martin Fränzle, Marta Kwiatkowska, Luca Laurenti, Nicola Paoletti, and Max Whitby</i>	

Decision Procedures and Their Applications

Model Counting for Recursively-Defined Strings	399
<i>Minh-Thai Trinh, Duc-Hiep Chu, and Joxan Jaffar</i>	
A Three-Tier Strategy for Reasoning About Floating-Point Numbers in SMT	419
<i>Sylvain Conchon, Mohamed Iguernlala, Kailiang Ji, Guillaume Melquiond, and Clément Fumex</i>	
A Correct-by-Decision Solution for Simultaneous Place and Route	436
<i>Alexander Nadel</i>	
Scaling Up DPLL(T) String Solvers Using Context-Dependent Simplification	453
<i>Andrew Reynolds, Maverick Woo, Clark Barrett, David Brumley, Tianyi Liang, and Cesare Tinelli</i>	

On Expansion and Resolution in CEGAR Based QBF Solving 475
Leander Tentrup

A Decidable Fragment in Separation Logic with Inductive Predicates
and Arithmetic 495
Quang Loc Le, Makoto Tatsuta, Jun Sun, and Wei-Ngan Chin

Software Analysis

Finding Fix Locations for CFL-Reachability Analyses via Minimum Cuts . . . 521
*Andrei Marian Dan, Manu Sridharan, Satish Chandra,
Jean-Baptiste Jeannin, and Martin Vechev*

Proving Linearizability Using Forward Simulations 542
*Ahmed Bouajjani, Michael Emmi, Constantin Enea,
and Suha Orhun Mutluergil*

EAHyper: Satisfiability, Implication, and Equivalence Checking
of Hyperproperties 564
Bernd Finkbeiner, Christopher Hahn, and Marvin Stenger

Automating Induction for Solving Horn Clauses 571
Hiroshi Unno, Sho Torii, and Hiroki Sakamoto

A **STORM** is Coming: A Modern Probabilistic Model Checker. 592
*Christian Dehnert, Sebastian Junges, Joost-Pieter Katoen,
and Matthias Volk*

On Multiphase-Linear Ranking Functions. 601
Amir M. Ben-Amram and Samir Genaim

Author Index 621

Contents – Part I

Invited Contributions

Safety Verification of Deep Neural Networks	3
<i>Xiaowei Huang, Marta Kwiatkowska, Sen Wang, and Min Wu</i>	
Program Verification Under Weak Memory Consistency Using Separation Logic	30
<i>Viktor Vafeiadis</i>	
The Power of Symbolic Automata and Transducers	47
<i>Loris D’Antoni and Margus Veanes</i>	
Maximum Satisfiability in Software Analysis: Applications and Techniques	68
<i>Ujje Si, Xin Zhang, Radu Grigore, and Mayur Naik</i>	

Probabilistic Systems

Reluplex: An Efficient SMT Solver for Verifying Deep Neural Networks . . .	97
<i>Guy Katz, Clark Barrett, David L. Dill, Kyle Julian, and Mykel J. Kochenderfer</i>	
Automated Recurrence Analysis for Almost-Linear Expected-Runtime Bounds	118
<i>Krishnendu Chatterjee, Hongfei Fu, and Aniket Murhekar</i>	
Markov Automata with Multiple Objectives	140
<i>Tim Quatmann, Sebastian Junges, and Joost-Pieter Katoen</i>	
Ensuring the Reliability of Your Model Checker: Interval Iteration for Markov Decision Processes	160
<i>Christel Baier, Joachim Klein, Linda Leuschner, David Parker, and Sascha Wunderlich</i>	
Repairing Decision-Making Programs Under Uncertainty	181
<i>Aws Albarghouthi, Loris D’Antoni, and Samuel Drews</i>	
Value Iteration for Long-Run Average Reward in Markov Decision Processes	201
<i>Pranav Ashok, Krishnendu Chatterjee, Przemyslaw Daca, Jan Křetínský, and Tobias Megendorfer</i>	

Data Driven Techniques

STLInspector: STL Validation with Guarantees.	225
<i>Hendrik Roehm, Thomas Heinz, and Eva Charlotte Mayer</i>	
Learning a Static Analyzer from Data	233
<i>Pavol Bielik, Veselin Raychev, and Martin Vechev</i>	
Synthesis with Abstract Examples.	254
<i>Dana Drachler-Cohen, Sharon Shoham, and Eran Yahav</i>	
Data-Driven Synthesis of Full Probabilistic Programs	279
<i>Sarah Chasins and Phitchaya Mangpo Phothilimthana</i>	
Logical Clustering and Learning for Time-Series Data	305
<i>Marcell Vazquez-Chanlatte, Jyotirmoy V. Deshmukh, Xiaoqing Jin, and Sanjit A. Seshia</i>	

Runtime Verification

MONTRE: A Tool for Monitoring Timed Regular Expressions	329
<i>Dogan Ulus</i>	
Runtime Monitoring with Recovery of the SENT Communication Protocol . . .	336
<i>Konstantin Selyunin, Stefan Jaksic, Thang Nguyen, Christian Reidl, Udo Hafner, Ezio Bartocci, Dejan Nickovic, and Radu Grosu</i>	
Runtime Verification of Temporal Properties over Out-of-Order Data Streams	356
<i>David Basin, Felix Klaedtke, and Eugen Zălinescu</i>	

Cyber-Physical Systems

Lagrangian Reachability	379
<i>Jacek Cyranka, Md. Ariful Islam, Greg Byrne, Paul Jones, Scott A. Smolka, and Radu Grosu</i>	
Simulation-Equivalent Reachability of Large Linear Systems with Inputs	401
<i>Stanley Bak and Parasara Sridhar Duggirala</i>	
MIGHTYL: A Compositional Translation from MITL to Timed Automata	421
<i>Thomas Brihaye, Gilles Geeraerts, Hsi-Ming Ho, and Benjamin Monmege</i>	
DRYVR: Data-Driven Verification and Compositional Reasoning for Automotive Systems.	441
<i>Chuchu Fan, Bolun Qi, Sayan Mitra, and Mahesh Viswanathan</i>	

Automated Formal Synthesis of Digital Controllers for State-Space Physical Plants	462
<i>Alessandro Abate, Iury Bessa, Dario Cattaruzza, Lucas Cordeiro, Cristina David, Pascal Kesseli, Daniel Kroening, and Elizabeth Polgreen</i>	
Classification and Coverage-Based Falsification for Embedded Control Systems	483
<i>Arvind Adimoolam, Thao Dang, Alexandre Donzé, James Kapinski, and Xiaoqing Jin</i>	
Concurrency	
GPUdrano: Detecting Uncoalesced Accesses in GPU Programs	507
<i>Rajeev Alur, Joseph Devietti, Omar S. Navarro Leija, and Nimit Singhania</i>	
Context-Sensitive Dynamic Partial Order Reduction	526
<i>Elvira Albert, Puri Arenas, María García de la Banda, Miguel Gómez-Zamalloa, and Peter J. Stuckey</i>	
Starling: Lightweight Concurrency Verification with Views	544
<i>Matt Windsor, Mike Dodds, Ben Simner, and Matthew J. Parkinson</i>	
Compositional Model Checking with Incremental Counter-Example Construction	570
<i>Anton Wijs and Thomas Neele</i>	
Pithya: A Parallel Tool for Parameter Synthesis of Piecewise Multi-affine Dynamical Systems	591
<i>Nikola Beneš, Luboš Brim, Martin Demko, Samuel Pastva, and David Šafránek</i>	
Author Index	599