

*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, Zürich, 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>

Swarat Chaudhuri · Azadeh Farzan (Eds.)

# Computer Aided Verification

28th International Conference, CAV 2016  
Toronto, ON, Canada, July 17–23, 2016  
Proceedings, Part I

*Editors*  
Swarat Chaudhuri  
Rice University  
Houston, TX  
USA

Azadeh Farzan  
University of Toronto  
Toronto, ON  
Canada

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-319-41527-7              ISBN 978-3-319-41528-4 (eBook)  
DOI 10.1007/978-3-319-41528-4

Library of Congress Control Number: 2015943799

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

© Springer International Publishing Switzerland 2016

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.

Printed on acid-free paper

This Springer imprint is published by Springer Nature  
The registered company is Springer International Publishing AG Switzerland

# Preface

It is our pleasure to welcome you to the proceedings of CAV 2016, the 28th International Conference on Computer-Aided Verification, held in Toronto, Ontario, during July 17–23, 2016.

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.

The CAV 2016 program included four invited keynote talks, four invited tutorials, 58 technical papers (consisting of 46 regular papers and 12 tool papers) accepted out of 195 submissions, and briefings from the SYNTCOMP and SYGUS synthesis competitions. The conference was accompanied by six co-located events: VSTTE (Verified Software: Theories, Tools, and Experiments), NSV (Numerical Software Verification), SYNT (Synthesis), EC<sup>2</sup> (Exploiting Concurrency Efficiently and Correctly), HCCV (High-Consequence Control Verification), and VMW (Verification Mentoring Workshop).

Our invited keynote speakers were Gilles Barthe (IMDEA Software Institute), Gerwin Klein (NICTA and University of New South Wales), and Moshe Vardi (Rice University). Parosh Aziz Abdulla (Uppsala University), Vitaly Chipounov (EPFL), Paulo Tabuada (UCLA), and Martin Vechev (ETH Zurich) gave invited tutorials.

We introduced three significant changes to CAV's review process this year. First, CAV 2016 employed a lightweight double-blind reviewing process. This meant that committee members did not have access to the names and affiliations of the authors as they reviewed a paper, and were able to produce an unbiased initial review. However, author names were revealed late in the online discussion process to permit calibration against the authors' prior work. Second, we introduced an External Review Committee, consisting of reviewers committed to producing four to five reviews, and also increased the size of the main Program Committee. These changes significantly reduced the number of papers that a committee had to review. Third, CAV 2016 had a two-phase evaluation process. Each paper received three reviews by the end of the first phase; considering the reviews and accounting for feedback from the reviewers, we solicited up to two additional reviews for papers for which consensus did not exist or further expertise was considered necessary.

Many people worked hard to make CAV 2016 a success. We thank the authors and the invited speakers for providing the excellent technical material, the Program Committee and the External Review Committee for their thorough reviews and the time spent on evaluating all the submissions and discussing them during the online discussion period, and the Steering Committee for their guidance.

We thank Pavol Černý, Sponsorship Chair, for helping to bring much-needed financial support to the conference; Zachary Kincaid, Workshop Chair, and all the organizers of the co-located events for bringing their events to the CAV week; Roopsha Samanta, Publicity Chair, for diligently publicizing the event; and Aws Albarghouthi, Artifact Evaluation Chair, and the Artifact Evaluation Committee for their work on evaluating the artifacts submitted. We gratefully acknowledge NSF for providing financial support for student participants. We sincerely thank the sponsors of CAV 2016 for their generous contributions.

We also thank the University of Toronto and Rice University for their support. Finally, we hope you find the proceedings of CAV 2016 intellectually stimulating and practically valuable.

July 2016

Swarat Chaudhuri  
Azadeh Farzan

# Organization

## Program Committee

Rajeev Alur	University of Pennsylvania, USA
Christel Baier	Technische Universität Dresden, Germany
Clark Barrett	New York University, USA
Roderick Bloem	Graz University of Technology, Austria
Pavol Cerny	University of Colorado, Boulder, USA
Adam Chlipala	MIT, USA
Swarat Chaudhuri	Rice University, Houston, USA
Alessandro Cimatti	Fondazione Bruno Kessler, Italy
Loris D'Antoni	University of Wisconsin, Madison, USA
Constantin Enea	University of Paris Diderot (Paris 7), France
Javier Esparza	Technische Universität München, Germany
Kousha Etessami	University of Edinburgh, UK
Azadeh Farzan	University of Toronto, Toronto, Canada
Susanne Graf	VERIMAG, France
Orna Grumberg	Technion, Israel
Franjo Ivancic	Google, USA
Somesh Jha	University of Wisconsin, Madison, USA
Ranjit Jhala	University of California, San Diego, USA
Joost-Pieter Katoen	RWTH Aachen University, Germany
Zachary Kincaid	University of Toronto, Canada
Laura Kovacs	Chalmers University of Technology, Sweden
Viktor Kuncak	EPFL, Switzerland
Marta Kwiatkowska	Oxford University, UK
Shuvendu Lahiri	Microsoft Research, Redmond, USA
Akash Lal	Microsoft Research, Bangalore, India
Pete Manolios	Northeastern University, USA
Kenneth McMillan	Microsoft Research, Redmond, USA
David Monniaux	VERIMAG, France
Kedar Namjoshi	Bell Labs, Alcatel-Lucent, USA
David Parker	University of Birmingham, UK
Corina Pasareanu	Carnegie Mellon Silicon Valley; NASA Ames, USA
Ruzica Piskac	Yale University, USA
Andreas Podelski	University of Freiburg, Germany
Shaz Qadeer	Microsoft Research, Redmond, USA
Andrey Rybalchenko	Microsoft Research, Cambridge, UK
Mooly Sagiv	Tel Aviv University, Israel
Sriram Sankaranarayanan	University of Colorado, Boulder, USA

Sanjit Seshia	University of California, Berkeley, USA
Natasha Sharygina	University of Lugano, Switzerland
Sharon Shoham	Academic College of Tel Aviv-Yaffo, Israel
Fabio Somenzi	University of Colorado, Boulder, USA
Serdar Tasiran	Koç University, Turkey
Mahesh Viswanathan	University of Illinois, Urbana-Champaign, USA
Bow-Yaw Wang	Academia Sinica, Taiwan
Thomas Wies	New York University, USA
Lenore Zuck	University of Illinois, Chicago, USA

## External Review Committee

Aws Albarghouthi	University of Wisconsin, Madison, USA
Jade Alglave	Microsoft Research Cambridge; University College London, UK
Sagar Chaki	Software Engineering Institute, Carnegie Mellon University, USA
Hana Chockler	King's College London, UK
Byron Cook	University College London; Amazon, UK
Deepak D'Souza	Indian Institute of Science, India
Thao Dang	CNRS, France
Cezara Dragoi	Inria, France
Pierre Ganty	IMDEA, Spain
Ganesh Gopalakrishnan	University of Utah, USA
Arie Gurfinkel	Software Engineering Institute, Carnegie Mellon University, USA
Jan Hoffmann	Carnegie Mellon University, USA
William Hung	Synopsys, USA
Joxan Jaffer	National University of Singapore
Naoki Kobayashi	University of Tokyo, Japan
Igor Konnov	Vienna University of Technology, Austria
Hillel Kugler	Bar-Ilan University, Israel
Rupak Majumdar	Max Planck Institute for Software Systems, Germany
Sayan Mitra	University of Illinois at Urbana Champaign, USA
Peter Mueller	ETH Zurich, Switzerland
Tim Nelson	Brown University, USA
Jan Otop	University of Wroclaw, Poland
Gennaro Parlato	University of Southampton, UK
Madhusudan Parthasarathy	University of Illinois at Urbana Champaign, USA
Doron Peled	Bar Ilan University, Israel
Pavithra Prabhakar	Kansas State University, USA
Arjun Radhakrishna	University of Pennsylvania, USA
Zvonimir Rakamaric	University of Utah, USA
Nishant Sinha	IBM Research, Bangalore, India
Ana Sokolova	University of Salzburg, Austria
Armando Solar-Lezama	MIT, USA



Viktor Vafeiadis	Max Planck Institute for Software Systems, Germany
Martin Vechev	ETH Zurich, Switzerland
Willem Visser	Stellenbosch University, South Africa
Tomas Vojnar	Brno University of Technology, Czech Republic
Thomas Wahl	Northeastern University, USA
Eran Yahav	Technion, Israel
Karen Yorav	IBM Haifa Research Lab, Israel
Florian Zuleger	Vienna University of Technology, Austria

## **Additional Reviewers**

Houssam Abbas	University of Pennsylvania, USA
Stavros Aronis	Uppsala University, Sweden
Amir Ben-Amram	The Academic College of Tel Aviv-Yaffo, Israel
Dirk Beyer	University of Passau, Germany
Armin Biere	Johannes Kepler University, Austria
David Binkley	Loyola University, USA
James Brotherston	University College London, UK
Domenico Cantone	University of Catania, Italy
Ernie Cohen	Amazon, USA
Sylvain Conchon	LRI, Université Paris-Sud 11, France
Chris Hawblitzel	Microsoft Research, Redmond, USA
Jean-François Raskin	Université Libre de Bruxelles, Belgium
Antoine Miné	UPMC University, France
Anders Møller	Aarhus University, Denmark
Andrew Reynolds	University of Iowa, USA
Ulrich Schmid	Vienna University of Technology, Austria
Margus Veanes	Microsoft Research, Redmond, USA

# Contents – Part I

## Probabilistic Systems

Termination Analysis of Probabilistic Programs Through Positivstellensatz's. . . . .	3
<i>Krishnendu Chatterjee, Hongfei Fu, and Amir Kafshdar Goharshady</i>	
Markov Chains and Unambiguous Büchi Automata. . . . .	23
<i>Christel Baier, Stefan Kiefer, Joachim Klein, Sascha Klüppelholz, David Müller, and James Worrell</i>	
Synthesizing Probabilistic Invariants via Doob's Decomposition . . . . .	43
<i>Gilles Barthe, Thomas Espitau, Luis María Ferrer Fioriti, and Justin Hsu</i>	
PSI: Exact Symbolic Inference for Probabilistic Programs . . . . .	62
<i>Timon Gehr, Sasa Misailovic, and Martin Vechev</i>	
PSCV: A Runtime Verification Tool for Probabilistic SystemC Models . . . . .	84
<i>Van Chan Ngo, Axel Legay, and Vania Joloboff</i>	

## Synthesis I

Structural Synthesis for GXW Specifications . . . . .	95
<i>Chih-Hong Cheng, Yassine Hamza, and Harald Ruess</i>	
Bounded Cycle Synthesis. . . . .	118
<i>Bernd Finkbeiner and Felix Klein</i>	
Fast, Flexible, and Minimal CTL Synthesis via SMT. . . . .	136
<i>Tobias Klenze, Sam Bayless, and Alan J. Hu</i>	
Synthesis of Self-Stabilising and Byzantine-Resilient Distributed Systems . . .	157
<i>Roderick Bloem, Nicolas Braud-Santoni, and Swen Jacobs</i>	

## Constraint Solving I

A Decision Procedure for Sets, Binary Relations and Partial Functions . . . . .	179
<i>Maximiliano Cristiá and Gianfranco Rossi</i>	
Precise and Complete Propagation Based Local Search for Satisfiability Modulo Theories. . . . .	199
<i>Aina Niemetz, Mathias Preiner, and Armin Biere</i>	

Progressive Reasoning over Recursively-Defined Strings . . . . .	218
<i>Minh-Thai Trinh, Duc-Hiep Chu, and Joxan Jaffar</i>	
String Analysis via Automata Manipulation with Logic Circuit Representation . . . . .	241
<i>Hung-En Wang, Tzung-Lin Tsai, Chun-Han Lin, Fang Yu, and Jie-Hong R. Jiang</i>	
RAHFT: A Tool for Verifying Horn Clauses Using Abstract Interpretation and Finite Tree Automata. . . . .	261
<i>Bishoksan Kafle, John P. Gallagher, and José F. Morales</i>	
<b>Model Checking I</b>	
Infinite-State Liveness-to-Safety via Implicit Abstraction and Well-Founded Relations. . . . .	271
<i>Jakub Daniel, Alessandro Cimatti, Alberto Griggio, Stefano Tonetta, and Sergio Mover</i>	
Proving Parameterized Systems Safe by Generalizing Clausal Proofs of Small Instances. . . . .	292
<i>Michael Dooley and Fabio Somenzi</i>	
Learning-Based Assume-Guarantee Regression Verification . . . . .	310
<i>Fei He, Shu Mao, and Bow-Yaw Wang</i>	
Automated Circular Assume-Guarantee Reasoning with N-way Decomposition and Alphabet Refinement. . . . .	329
<i>Karam Abd Elkader, Orna Grumberg, Corina S. Păsăreanu, and Sharon Shoham</i>	
JayHorn: A Framework for Verifying Java programs . . . . .	352
<i>Temesghen Kahsai, Philipp Rümmer, Huascar Sanchez, and Martin Schäf</i>	
<b>Program Analysis</b>	
Trigger Selection Strategies to Stabilize Program Verifiers . . . . .	361
<i>K.R.M. Leino and Clément Pit-Claudel</i>	
Satisfiability Modulo Heap-Based Programs . . . . .	382
<i>Quang Loc Le, Jun Sun, and Wei-Ngan Chin</i>	
Automatic Verification of Iterated Separating Conjunctions Using Symbolic Execution. . . . .	405
<i>Peter Müller, Malte Schwerhoff, and Alexander J. Summers</i>	

From Shape Analysis to Termination Analysis in Linear Time . . . . . 426  
*Roman Manevich, Boris Dogadov, and Noam Rinetzký*

RV-Match: Practical Semantics-Based Program Analysis . . . . . 447  
*Dwight Guth, Chris Hathhorn, Manasvi Saxena, and Grigore Roşu*

**Timed and Hybrid Systems**

Under-Approximating Backward Reachable Sets by Polytopes . . . . . 457  
*Bai Xue, Zhikun She, and Arvind Easwaran*

Parsimonious, Simulation Based Verification of Linear Systems . . . . . 477  
*Parasara Sridhar Duggirala and Mahesh Viswanathan*

Counterexample Guided Abstraction Refinement for Stability Analysis . . . . . 495  
*Pavithra Prabhakar and Miriam García Soto*

Symbolic Optimal Reachability in Weighted Timed Automata . . . . . 513  
*Patricia Bouyer, Maximilien Colange, and Nicolas Markey*

Automatic Reachability Analysis for Nonlinear Hybrid Models with C2E2. . . 531  
*Chuchu Fan, Bolun Qi, Sayan Mitra, Mahesh Viswanathan,  
and Parasara Sridhar Duggirala*

**Author Index** . . . . . 539

## Contents – Part II

### Verification in Practice

Model Checking at Scale: Automated Air Traffic Control Design Space Exploration . . . . .	3
<i>Marco Gario, Alessandro Cimatti, Cristian Mattarei, Stefano Tonetta, and Kristin Yvonne Rozier</i>	
Investigating Safety of a Radiotherapy Machine Using System Models with Pluggable Checkers . . . . .	23
<i>Stuart Pernsteiner, Calvin Loncaric, Emina Torlak, Zachary Tatlock, Xi Wang, Michael D. Ernst, and Jonathan Jacky</i>	
End-to-End Verification of ARM <sup>®</sup> Processors with ISA-Formal . . . . .	42
<i>Alastair Reid, Rick Chen, Anastasios Deligiannis, David Gilday, David Hoyes, Will Keen, Ashan Pathirane, Owen Shepherd, Peter Vrabel, and Ali Zaidi</i>	
A Practical Verification Framework for Preemptive OS Kernels . . . . .	59
<i>Fengwei Xu, Ming Fu, Xinyu Feng, Xiaoran Zhang, Hui Zhang, and Zhaohui Li</i>	
Probabilistic Automated Language Learning for Configuration Files . . . . .	80
<i>Mark Santolucito, Ennan Zhai, and Ruzica Piskac</i>	

### Concurrency

The Commutativity Problem of the MapReduce Framework: A Transducer-Based Approach . . . . .	91
<i>Yu-Fang Chen, Lei Song, and Zhilin Wu</i>	
Liveness of Randomised Parameterised Systems under Arbitrary Schedulers . . .	112
<i>Anthony W. Lin and Philipp Rümmer</i>	
Stateless Model Checking for POWER . . . . .	134
<i>Parosh Aziz Abdulla, Mohamed Faouzi Atig, Bengt Jonsson, and Carl Leonardsson</i>	
Hitting Families of Schedules for Asynchronous Programs . . . . .	157
<i>Dmitry Chistikov, Rupak Majumdar, and Filip Nikić</i>	
ParCoSS: Efficient Parallelized Compiled Symbolic Simulation . . . . .	177
<i>Vladimir Herdt, Hoang M. Le, Daniel Große, and Rolf Drechsler</i>	

**Constraint Solving II**

XSat: A Fast Floating-Point Satisfiability Solver . . . . .	187
<i>Zhoulai Fu and Zhendong Su</i>	
Effectively Propositional Interpolants . . . . .	210
<i>Samuel Drews and Aws Albarghouthi</i>	
Array Folds Logic . . . . .	230
<i>Przemysław Daga, Thomas A. Henzinger, and Andrey Kupriyanov</i>	

**Automata and Games**

Compositional Synthesis of Reactive Controllers for Multi-agent Systems . . .	251
<i>Rajeev Alur, Salar Moarref, and Ufuk Topcu</i>	
Solving Parity Games via Priority Promotion . . . . .	270
<i>Massimo Benerecetti, Daniele Dell'Erba, and Fabio Mogavero</i>	
A Simple Algorithm for Solving Qualitative Probabilistic Parity Games . . . . .	291
<i>Ernst Moritz Hahn, Sven Schewe, Andrea Turrini, and Lijun Zhang</i>	
Limit-Deterministic Büchi Automata for Linear Temporal Logic . . . . .	312
<i>Salomon Sickert, Javier Esparza, Stefan Jaax, and Jan Křetínský</i>	
Slugs: Extensible GR(1) Synthesis . . . . .	333
<i>Rüdiger Ehlers and Vasumathi Raman</i>	

**Synthesis II**

Synthesis of Fault-Attack Countermeasures for Cryptographic Circuits . . . . .	343
<i>Hassan Eldib, Meng Wu, and Chao Wang</i>	
A SAT-Based Counterexample Guided Method for Unbounded Synthesis . . .	364
<i>Alexander Legg, Nina Narodytska, and Leonid Ryzhyk</i>	
QLOSE: Program Repair with Quantitative Objectives . . . . .	383
<i>Loris D'Antoni, Roopsha Samanta, and Rishabh Singh</i>	
BDD-Based Boolean Functional Synthesis . . . . .	402
<i>Dror Fried, Lucas M. Tabajara, and Moshe Y. Vardi</i>	
SOUFFLÉ: On Synthesis of Program Analyzers . . . . .	422
<i>Herbert Jordan, Bernhard Scholz, and Pavle Subotić</i>	

**Model Checking II**

Property Directed Equivalence via Abstract Simulation . . . . .	433
<i>Grigory Fedyukovich, Arie Gurfinkel, and Natasha Sharygina</i>	
Combining Model Learning and Model Checking to Analyze TCP Implementations . . . . .	454
<i>Paul Fiterău-Broștean, Ramon Janssen, and Frits Vaandrager</i>	
BFS-Based Model Checking of Linear-Time Properties with an Application on GPUs . . . . .	472
<i>Anton Wijs</i>	
BigraphER: Rewriting and Analysis Engine for Bigraphs . . . . .	494
<i>Michele Sevegnani and Muffy Calder</i>	
Verification-Aided Debugging: An Interactive Web-Service for Exploring Error Witnesses . . . . .	502
<i>Dirk Beyer and Matthias Dangel</i>	
The KIND 2 Model Checker . . . . .	510
<i>Adrien Champion, Alain Mebsout, Christoph Stickse, and Cesare Tinelli</i>	
<b>Author Index</b> . . . . .	519