# Lecture Notes in Computer Science 9779

*Commenced Publication in 1973*
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

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

Springer

*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



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), $EC^2$ (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 reivew. 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, Univesité 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

# Contents – Part II

**Constraint Solving II**



**Automata and Games**



**Synthesis II**

**Model Checking II**