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), EC² (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  ŃNRS, 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 Veenes  
Microsoft Research, Redmond, USA
## Contents – Part I

### Probabilistic Systems

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

### Synthesis I

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

### Constraint Solving I

<table>
<thead>
<tr>
<th>Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Decision Procedure for Sets, Binary Relations and Partial Functions</td>
<td>179</td>
</tr>
<tr>
<td>Maximiliano Cristià and Gianfranco Rossi</td>
<td></td>
</tr>
<tr>
<td>Precise and Complete Propagation Based Local Search for Satisfiability Modulo Theories</td>
<td>199</td>
</tr>
<tr>
<td>Aina Niemetz, Mathias Preiner, and Armin Biere</td>
<td></td>
</tr>
</tbody>
</table>
Progressive Reasoning over Recursively-Defined Strings .......................... 218
  Minh-Thai Trinh, Duc-Hiep Chu, and Joxan Jaffar

String Analysis via Automata Manipulation with Logic Circuit
  Representation .............................................. 241
  Hung-En Wang, Tzung-Lin Tsai, Chun-Han Lin, Fang Yu,
  and Jie-Hong R. Jiang

RAHFT: A Tool for Verifying Horn Clauses Using Abstract Interpretation
  and Finite Tree Automata........................................ 261
  Bishoksan Kafle, John P. Gallagher, and José F. Morales

Model Checking I

Infinite-State Liveness-to-Safety via Implicit Abstraction
  and Well-Founded Relations..................................... 271
  Jakub Daniel, Alessandro Cimatti, Alberto Griggio, Stefano Tonetta,
  and Sergio Mover

Proving Parameterized Systems Safe by Generalizing Clausal Proofs of Small Instances........................................ 292
  Michael Dooley and Fabio Somenzi

Learning-Based Assume-Guarantee Regression Verification .................... 310
  Fei He, Shu Mao, and Bow-Yaw Wang

Automated Circular Assume-Guarantee Reasoning with N-way Decomposition and Alphabet Refinement ............................. 329
  Karam Abd Elkader, Orna Grumberg, Corina S. Păslăreanu,
  and Sharon Shoham

JayHorn: A Framework for Verifying Java programs ................................ 352
  Temesghen Kahsai, Philipp Rümmer, Huascar Sanchez,
  and Martin Schäf

Program Analysis

Trigger Selection Strategies to Stabilize Program Verifiers .................... 361
  K.R.M. Leino and Clément Pit-Claudel

Satisfiability Modulo Heap-Based Programs ..................................... 382
  Quang Loc Le, Jun Sun, and Wei-Ngan Chin

Automatic Verification of Iterated Separating Conjunctions Using Symbolic Execution .................................................. 405
  Peter Müller, Malte Schwerhoff, and Alexander J. Summers
From Shape Analysis to Termination Analysis in Linear Time .................. 426
Roman Manevich, Boris Dogadov, and Noam Rinetzky

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
  Marco Gario, Alessandro Cimatti, Cristian Mattarei, Stefano Tonetta,
  and Kristin Yvonne Rozier

Investigating Safety of a Radiotherapy Machine Using System Models with
Pluggable Checkers ............................................................. 23
  Stuart Pernsteiner, Calvin Loncaric, Emina Torlak, Zachary Tatlock,
  Xi Wang, Michael D. Ernst, and Jonathan Jacky

End-to-End Verification of ARM® Processors with ISA-Formal .............. 42
  Alastair Reid, Rick Chen, Anastasios Deligiannis, David Gilday,
  David Hoyes, Will Keen, Ashan Pathirane, Owen Shepherd,
  Peter Vrabel, and Ali Zaidi

A Practical Verification Framework for Preemptive OS Kernels ............ 59
  Fengwei Xu, Ming Fu, Xinyu Feng, Xiaoran Zhang, Hui Zhang,
  and Zhaohui Li

Probabilistic Automated Language Learning for Configuration Files ....... 80
  Mark Santolucito, Ennan Zhai, and Ruzica Piskac

Concurrency

The Commutativity Problem of the MapReduce Framework:
A Transducer-Based Approach ............................................. 91
  Yu-Fang Chen, Lei Song, and Zhilin Wu

Liveness of Randomised Parameterised Systems under Arbitrary Schedulers...
  Anthony W. Lin and Philipp Rümmer

Stateless Model Checking for POWER ...................................... 134
  Parosh Aziz Abdulla, Mohamed Faouzi Atig, Bengt Jonsson,
  and Carl Leonardsson

Hitting Families of Schedules for Asynchronous Programs .................. 157
  Dmitry Chistikov, Rupak Majumdar, and Filip Niksic

ParCoSS: Efficient Parallelized Compiled Symbolic Simulation ............ 177
  Vladimir Herdt, Hoang M. Le, Daniel Große, and Rolf Drechsler
Constraint Solving II

XSat: A Fast Floating-Point Satisfiability Solver ........................................ 187
Zhoulai Fu and Zhendong Su

Effectively Propositional Interpolants ....................................................... 210
Samuel Drews and Aws Albarghouthi

Array Folds Logic ...................................................................................... 230
Przemyslaw Daca, Thomas A. Henzinger, and Andrey Kupriyanov

Automata and Games

Compositional Synthesis of Reactive Controllers for Multi-agent Systems ... 251
Rajeev Alur, Salar Moarref, and Ufuk Topcu

Solving Parity Games via Priority Promotion ............................................. 270
Massimo Benerecetti, Daniele Dell’Erba, and Fabio Mogavero

A Simple Algorithm for Solving Qualitative Probabilistic Parity Games ... 291
Ernst Moritz Hahn, Sven Schewe, Andrea Turrini, and Lijun Zhang

Limit-Deterministic Büchi Automata for Linear Temporal Logic .............. 312
Salomon Sickert, Javier Esparza, Stefan Jaax, and Jan Křetínský

Slugs: Extensible GR(1) Synthesis .......................................................... 333
Rüdiger Ehlers and Vasumathi Raman

Synthesis II

Synthesis of Fault-Attack Countermeasures for Cryptographic Circuits ... 343
Hassan Eldib, Meng Wu, and Chao Wang

A SAT-Based Counterexample Guided Method for Unbounded Synthesis ... 364
Alexander Legg, Nina Narodytska, and Leonid Ryzhyk

QLOSE: Program Repair with Quantitative Objectives ............................. 383
Loris D’Antoni, Roopsha Samanta, and Rishabh Singh

BDD-Based Boolean Functional Synthesis ............................................... 402
Dror Fried, Lucas M. Tabajara, and Moshe Y. Vardi

SOUFFLÉ: On Synthesis of Program Analyzers ....................................... 422
Herbert Jordan, Bernhard Scholz, and Pavle Subotić
Model Checking II

Property Directed Equivalence via Abstract Simulation ........................................ 433
  Grigory Fedyukovich, Arie Gurfinkel, and Natasha Sharygina

Combining Model Learning and Model Checking to Analyze TCP Implementations ........................................ 454
  Paul Fiterău-Broștean, Ramon Janssen, and Frits Vaandrager

BFS-Based Model Checking of Linear-Time Properties with an Application on GPUs ........................................ 472
  Anton Wijs

BigraphER: Rewriting and Analysis Engine for Bigraphs ........................................ 494
  Michele Sevegnani and Muffy Calder

Verification-Aided Debugging: An Interactive Web-Service for Exploring Error Witnesses ........................................ 502
  Dirk Beyer and Matthias Dangl

The KIND 2 Model Checker ........................................ 510
  Adrien Champion, Alain Mebsout, Christoph Sticksel, and Cesare Tinelli

Author Index ........................................ 519