More information about this series at http://www.springer.com/series/7407
Computer Aided Verification

27th International Conference, CAV 2015
San Francisco, CA, USA, July 18–24, 2015
Proceedings, Part II
Preface

It is our great pleasure to welcome you to CAV 2015, the 27th International Conference on Computer-Aided Verification, held in San Francisco, California, during July 18–24, 2015.

The CAV conference series is dedicated to the advancement of the theory and practice of computer-aided formal analysis methods for 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 2015 program included five keynotes, technical papers (58 long and 11 short papers accepted out of 252 submissions), 11 co-located events (VSTTE – Verified Software: Theories, Tools, and Experiments; SMT – Satisfiability Modulo Theories, EC2, IPRA – Interpolation: From Proofs to Applications; SYNT – Synthesis; VeriSure – Verification and Assurance; HCVS – Horn Clauses for Verification and Synthesis; VMW – Verification Mentoring Workshop, REORDER, SNR – Symbolic and Numerical Methods for Reachability Analysis; VEMDP – Verification of Engineered Molecular Devices and Programs), the Artifact Evaluation as well as briefings from the SMT and Synthesis competitions.

The invited keynote speakers were Philippa Gardner (Imperial College London), Leslie Lamport (Microsoft Research), Bob Kurshan (Cadence), William Hung (Synopsys), and Peter O’Hearn (University College London and Facebook).

Many people worked hard to make CAV 2015 a success. We thank the authors and the keynote speakers for providing the excellent technical material, the Program Committee for their thorough reviews and the time spent on evaluating all the submissions and discussing them during the on-line discussion period, and the Steering Committee for their guidance throughout the planning for CAV 2015.

We also thank Temesghen Kahsai, Local Chair, for his dedication and help with CAV 2015 planning and Hana Chockler, Sponsorship Chair, for helping to bring much needed financial support to the conference; Dirk Beyer, Workshop Chair, and all the organizers of the co-located events for bringing their events to the CAV week; Elizabeth Polgreen for the program and proceedings; Arie Gurfinkel, Temesghen Kahsai, Michael Tautschnig, 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 CAV sponsors for their generous contributions:

- Google (Platinum sponsor)
- NASA, Fujitsu, SGT, Facebook, Microsoft (Gold sponsors)
- IBM, Cadence (Silver sponsors)
- Intel, Samsung (Bronze sponsors)
We also thank Carnegie Mellon University Silicon Valley and the University of Oxford for their support.

Finally, we hope you find the proceedings of CAV 2015 intellectually stimulating and practically valuable.

May 2015

Corina S. Păsăreanu
Daniel Kroening
Organization

Program Committee

Aws Al barghouthi University of Toronto, Canada
Jade Alglave University College London, UK
Domagoj Babic Google
Armin Biere Johannes Kepler University, Austria
Roderick Bloem Graz University of Technology, Austria
Ahmed Bouajjani LIAFA, University of Paris Diderot, France
Marius Bozga Verimag/CNRS, France
Aaron Bradley Mentor Graphics
David Brumley Carnegie Mellon University, USA
Tevfik Bultan University of California at Santa Barbara, USA
Krishnendu Chatterjee Institute of Science and Technology (IST)
Swarat Chaudhuri Rice University, USA
Marsha Chechik University of Toronto, Canada
Hana Chockler King’s College London, UK
Byron Cook Microsoft Research
Isil Dillig Stanford University, USA
Dino Distefano Facebook
Alastair Donaldson Imperial College London, UK
Azadeh Farzan University of Toronto, Canada
Antonio Filieri University of Stuttgart, Germany
Jasmin Fisher Microsoft Research
Indradeep Ghosh Fujitsu Labs of America
Patrice Godefroid Microsoft Research
Aarti Gupta Princeton University, USA
Arie Gurfinkel Software Engineering Institute, CMU, USA
Gerard Holzmann NASA/JPL, USA
Warren Hunt University of Texas, USA
Ranjit Jhala University of California San Diego, USA
Barbara Jobstmann EPFL, Jasper DA, and CNRS-Verimag, Switzerland/France
Joost-Pieter Katoen RWTH Aachen University, Germany
Daniel Kroening University of Oxford, UK
Marta Kwiatkowska University of Oxford, UK
Akash Lal Microsoft Research, India
Darko Marinov University of Illinois at Urbana-Champaign, USA
Ken McMillan Microsoft Research
Kedar Namjoshi Bell Labs
David Parker University of Birmingham, UK
Corina Pasareanu CMU/NASA Ames Research Center, USA
André Platzer Carnegie Mellon University, USA
Zvonimir Rakamaric University of Utah, USA
Grigore Rosu University of Illinois at Urbana-Champaign, USA
Philipp Ruemmer Uppsala University, Sweden
Mooly Sagiv Tel Aviv University, Israel
Sriram Sankaranarayanan University of Colorado, Boulder, USA
Koushik Sen University of California, Berkeley, USA
Natarajan Shankar SRI International
Natasha Sharygina Università della Svizzera Italiana, Italy
Sharon Shoham Technion, Israel
Nishant Sinha IBM Research Labs
Fabio Sommelli University of Colorado at Boulder, USA
Manu Sridharan Samsung Research America
Ofer Strichman Technion, Israel
Zhendong Su UC Davis, USA
Cesare Tinelli The University of Iowa, USA
Emina Torlak U.C. Berkeley, USA
Tayssir Touili LIAFA, CNRS and University Paris Diderot, France
Thomas Wahl Northeastern University, USA
Georg Weissenbacher Vienna University of Technology, Austria
Eran Yahav Technion, Israel

Additional Reviewers

Abdelkader, Karam Bartocci, Ezio Calcagno, Cristiano
Abdullah, Syed Md. Basset, Nicolas Ceska, Milan
Jakaria Ben Sassi, Chakarov, Aleksandar
Abraham, Erika Mohamed Amin Chakravarthy, Venkat
Aiswarya, C. Ben-David, Shoham Chan, May T.M.
Akshay, S. Benes, Nikola Chapman, Martin
Alberti, Francesco Berdine, Josh Chau, Cuong
Alt, Leonardo Bertrand, Nathalie Chen, Xin
André, Etienne Bhatt, Devesh Chen, Yuting
Arechiga, Nikos Blackshear, Sam Cherini, Renato
Asarin, Eugene Bocić, Ivan Chiang, Wei-Fan
Astefanoaei, Lacramioara Bogomolov, Sergiy Chmelik, Martin
Athanasiou, Konstantinos Bornholt, James Choi, Wontae
Aydin, Abdulbaki Bortz, David Cimatti, Alessandro
Backman, Peter Brain, Martin Ciobaca, Stefan
Balakrishnan, Gogul Brockschmidt, Marc Clancy, Kevin
Bang, Lucas Brotherston, James Combez, Jacques
Barbot, Benoît Bruns, Glenn Cox, Arlen
Barrett, Clark Bushnell, David D’Antoni, Loris
D’Silva, Vijay
Dan, Andrei Marian
Dang, Thao
Darulova, Eva
David, Cristina
De Niz, Dionisio
Degorre, Aldric
Dehnert, Christian
Dhok, Monika
Diaz, Marcio
Dimjascevic, Marko
Dor, Nurit
Doyen, Laurent
Dragoi, Cezara
Dutertre, Bruno
Dutra, Rafael
Ebtекar, Aram
Ehlers, Rudiger
Eide, Eric
Eisner, Cindy
Enea, Constantin
Fainekos, Georgios
Falcone, Ylies
Fedynukovich, Grigory
Feret, Jerome
Ferrere, Thomas
Fisman, Dana
Forejt, Vojtech
Fraer, Ranan
Frehse, Goran
Fu, Xiang
Fu, Zhoulai
Fuhs, Carsten
Fulton, Nathan
Gao, Sicun
Garg, Pranav
Garroche, Pierre-Loic
Gascon, Adria
Gerard, Leonard
Ghorbal, Khalil
Giacobbe, Mirco
Girard, Antoine
Gligoric, Milos
Goel, Shilpi
Gong, Liang
Gordon, Colin S.

Gotsman, Alexey
Gretz, Friedrich
Griesmayer, Andreas
Grinchtein, Olga
Grumberg, Orna
Gu, Yijia
Guck, Dennis
Gupta, Ashutosh
Gvero, Tihomir
Gyori, Alex
Günther, Henning
Haase, Christoph
Hadarean, Liana
Hahn, Ernst Moritz
Hall, Ben
Hall, Benjamin
Hallé, Sylvain
Hamza, Jad
He, Shaobo
Heizmann, Matthias
Henriques, David
Henry, Julien
Heule, Marijn
Hofferek, Georg
Horn, Alexander
Hyvärinen, Antti
Ivancic, Franjo
Ivrii, Alexander
Jain, Mitesh
Jansen, Nils
Jeannin, Jean-Baptiste
Ji, Ran
Jovanovic, Aleksandra
Jovanović, Dejan
Kafle, Bishoksan
Kahsai, Temesghen
Kahveci, Tuba
Kaminski, Benjamin
Lucien
Kannan, Jayanthkumar
Kapinski, James
Karbyshev, Aleksandr
Karimi, Derrick
Keidar-Barner, Sharon
Keller, Chantal
Kennedy, Andrew

Khalimov, Ayrat
Khlaaf, Heidy
Kiefer, Stefan
Kim, Chang Hwan Peter
Kincaid, Zachary
King, Andy
King, Tim
Kini, Keshav
Koenighofer, Robert
Komuravelli, Anvesh
Konnov, Igor
Koskinen, Eric
Kretinsky, Jan
Kugler, Hilfel
Kuncak, Viktor
Laarman, Alons
Lahav, Ori
Lahiri, Shuvendu
Lampka, Kai
Lange, Martin
Lano, Kevin
Lawford, Mark
Le, Vu
Legay, Axel
Li, Goudong
Li, Guodong
Li, Peng
Li, Wenchao
Li, Yi
Liang, Tianyi
Lin, Yu
Liu, Peizun
Loos, Sarah
Luo, Qingzhou
Maler, Oded
Marescotti, Matteo
Martins, João G.
Martins, Ruben
Meel, Kuldeep
Mehne, Ben
Meller, Yoel
Merseccre, Alexandru
Meshman, Yuri
Miné, Antoine
Misailovic, Sasa
Mitra, Sayan
Contents – Part II

SMT Techniques and Applications

POLING: SMT Aided Linearizability Proofs ........................................ 3
He Zhu, Gustavo Petri, and Suresh Jagannathan

Finding Bounded Path in Graph Using SMT for Automatic Clock Routing . . . 20
Amit Erez and Alexander Nadel

Cutting the Mix ............................................................... 37
Jürgen Christ and Jochen Hoenicke

The Inez Mathematical Programming Modulo Theories Framework ........ 53
Panagiotis Manolios, Jorge Pais, and Vasilis Papavasileiou

Using Minimal Correction Sets to More Efficiently Compute Minimal Unsatisfiable Sets .................................................. 70
Fahiem Bacchus and George Katsirelos

Deciding Local Theory Extensions via E-matching ......................... 87
Kshitij Bansal, Andrew Reynolds, Tim King, Clark Barrett, and Thomas Wies

HW Verification

Modular Deductive Verification of Multiprocessor Hardware Designs .... 109
Muralidaran Vijayaraghavan, Adam Chlipala, Arvind, and Nirav Dave

Word-Level Symbolic Trajectory Evaluation. ............................... 128
Supratik Chakraborty, Zurab Khasidashvili, Carl-Johan H. Seger,
Rajkumar Gajavelly, Tanmay Haldankar, Dinesh Chhatani,
and Rakesh Mistry

Verifying Linearizability of Intel® Software Guard Extensions ............ 144
Rebekah Leslie-Hurd, Dror Caspi, and Matthew Fernandez

Synthesis

Synthesis Through Unification .................................................. 163
Rajeev Alur, Pavol Černý, and Arjun Radhakrishna
From Non-preemptive to Preemptive Scheduling
Using Synchronization Synthesis
Pavol Černý, Edmund M. Clarke, Thomas A. Henzinger,
Arjun Radhakrishna, Leonid Ryzhyk, Roopsha Samanta,
and Thorsten Tarrach

Countercexample-Guided Quantifier Instantiation for Synthesis in SMT
Andrew Reynolds, Morgan Deters, Viktor Kuncak, Cesare Tinelli,
and Clark Barrett

Deductive Program Repair
Etienne Kneuss, Manos Koukoutos, and Viktor Kuncak

Quantifying Conformance Using the Skorokhod Metric
Jyotirmoy V. Deshmukh, Rupak Majumdar, and Vinayak S. Prabhu

Pareto Curves of Multidimensional Mean-Payoff Games
Romain Brenguier and Jean-François Raskin

Termination
Conflict-Driven Conditional Termination
Vijay D’Silva and Caterina Urban

Predicate Abstraction and CEGAR for Disproving Termination
of Higher-Order Functional Programs
Takuya Kuwahara, Ryosuke Sato, Hiroshi Unno, and Naoki Kobayashi

Complexity of Bradley-Manna-Sipma Lexicographic Ranking Functions
Amir M. Ben-Amram and Samir Genaim

Measuring with Timed Patterns
Thomas Ferrère, Oded Maler, Dejan Ničković, and Dogan Ulus

Automatic Verification of Stability and Safety for Delay Differential
Equations
Liang Zou, Martin Fränzle, Naijun Zhan, and Peter Nazier Mosaad

Time Robustness in MTL and Expressivity in Hybrid System Falsification
Takumi Akazaki and Ichiro Hasuo

Concurrency
Adaptive Concretization for Parallel Program Synthesis
Jinseong Jeon, Xiaokang Qiu, Armando Solar-Lezama,
and Jeffrey S. Foster
Automatic Completion of Distributed Protocols with Symmetry 395
   Rajeev Alur, Mukund Raghothaman, Christos Stergiou, Stavros Tripakis,
   and Abhishek Udupa

An Axiomatic Specification for Sequential Memory Models 413
   William Mansky, Dmitri Garbuzov, and Steve Zdancewic

Approximate Synchrony: An Abstraction for Distributed
Almost-Synchronous Systems 429
   Ankush Desai, Sanjit A. Seshia, Shaz Qadeer, David Broman,
   and John C. Eidson

Automated and Modular Refinement Reasoning for Concurrent Programs 449
   Chris Hawblitzel, Erez Petrank, Shaz Qadeer, and Serdar Tasiran

Author Index 467
Contents – Part I

Invited Paper

A Trusted Mechanised Specification of JavaScript: One Year On ................. 3  
Philioppa Gardner, Gareth Smith, Conrad Watt, and Thomas Wood

Model Checking and Refinements

On Automation of CTL* Verification for Infinite-State Systems .................. 13  
Byron Cook, Heidy Khlaaf, and Nir Piterman

Algorithms for Model Checking HyperLTL and HyperCTL* ....................... 30  
Bernd Finkbeiner, Markus N. Rabe, and César Sánchez

Fairness Modulo Theory: A New Approach to LTL Software  
Model Checking .............................................................. 49  
Daniel Dietsch, Matthias Heizmann, Vincent Langenfeld,  
and Andreas Podelski

Model Checking Parameterized Asynchronous Shared-Memory Systems ........ 67  
Antoine Durand-Gasselin, Javier Esparza, Pierre Ganty,  
and Rupak Majumdar

SMT and POR Beat Counter Abstraction: Parameterized Model Checking  
of Threshold-Based Distributed Algorithms ...................................... 85  
Igor Konnov, Helmut Veith, and Josef Widder

Skipping Refinement ............................................................. 103  
Mitesh Jain and Panagiotis Manolios

Quantitative Reasoning

Percentile Queries in Multi-dimensional Markov Decision Processes ........... 123  
Mickael Randour, Jean-François Raskin, and Ocan Sankur

Faster Algorithms for Quantitative Verification in Constant  
Treewidth Graphs ....................................................................... 140  
Krishnendu Chatterjee, Rasmus Ibsen-Jensen,  
and Andreas Pavlogiannis

Counterexample Explanation by Learning Small Strategies in Markov  
Decision Processes ................................................................. 158  
Tomáš Brázdil, Krishnendu Chatterjee, Martin Chmelík,  
Andreas Fellner, and Jan Krčetinský
Symbolic Polytopes for Quantitative Interpolation and Verification
Klaus von Gleissenthall, Boris Köpf, and Andrey Rybalchenko

Adaptive Aggregation of Markov Chains: Quantitative Analysis of Chemical Reaction Networks
Alessandro Abate, Luboš Brim, Milan Češka, and Marta Kwiatkowska

PROPhESY: A PRObabilistic ParamEter SYnthesis Tool
Christian Dehnert, Sebastian Junges, Nils Jansen, Florian Corzilius, Matthias Volk, Harold Bruintjes, Joost- Pieter Katoen, and Erika Ábrahám

Software Analysis

Effective Search-Space Pruning for Solvers of String Equations, Regular Expressions and Length Constraints
Yunhui Zheng, Vijay Ganesh, Sanu Subramanian, Omer Tripp, Julian Dolby, and Xiangyu Zhang

Automata-Based Model Counting for String Constraints
Abdulbaki Aydin, Lucas Bang, and Tevfik Bultan

OpenJDK’s Java.utils.Collection.sort() Is Broken: The Good, the Bad and the Worst Case
Stijn de Gouw, Jurriaan Rot, Frank S. de Boer, Richard Bubel, and Reiner Hähnle

Tree Buffers
Radu Grigore and Stefan Kiefer

Learning Commutativity Specifications
Timon Gehr, Dimitar Dimitrov, and Martin Vechev

Angelic Verification: Precise Verification Modulo Unknowns
Ankush Das, Shuvendu K. Lahiri, Akash Lal, and Yi Li

The SeaHorn Verification Framework
Arie Gurfinkel, Temesghen Kahsai, Anvesh Komuravelli, and Jorge A. Navas

Automatic Rootcausing for Program Equivalence Failures in Binaries
Shuvendu K. Lahiri, Rohit Sinha, and Chris Hawblitzel

Fine-Grained Caching of Verification Results
K. Rustan M. Leino and Valentin Wüstholz

Predicting a Correct Program in Programming by Example
Rishabh Singh and Sumit Gulwani
Abstract Interpretation with Higher-Dimensional Ellipsoids
and Conic Extrapolation .................................................. 415
   Mendes Oulamara and Arnaud J. Venet

Lightning Talks

ADAM: Causality-Based Synthesis of Distributed Systems ............... 433
   Bernd Finkbeiner, Manuel Gieseking, and Ernst-Rüdiger Olderog

Alchemist: Learning Guarded Affine Functions .............................. 440
   Shambwaditya Saha, Pranav Garg, and P. Madhusudan

OptiMathSAT: A Tool for Optimization Modulo Theories ..................... 447
   Roberto Sebastiani and Patrick Trentin

Systematic Asynchrony Bug Exploration for Android Apps .................... 455
   Burcu Kulahcioglu Ozkan, Michael Emmi, and Serdar Tasiran

Norn: An SMT Solver for String Constraints ................................ 462
   Parosh Aziz Abdulla, Mohamed Faouzi Atig, Yu-Fang Chen,
   Lukáš Holík, Ahmed Rezine, Philipp Rümmer, and Jari Stenman

PVSio-web 2.0: Joining PVS to HCI ........................................ 470
   Paolo Masci, Patrick Oladimeji, Yi Zhang, Paul Jones, Paul Curzon,
   and Harold Thimbleby

The Hanoi Omega-Automata Format .......................................... 479
   Tomáš Babiak, František Blahoudek, Alexandre Duret-Lutz,
   Joachim Klein, Jan Křetínský, David Müller, David Parker,
   and Jan Strejček

The Open-Source LearnLib: A Framework for Active Automata Learning ... 487
   Malte Isberner, Falk Howar, and Bernhard Steffen

Bbs: A Phase-Bounded Model Checker for Asynchronous Programs ........... 496
   Rupak Majumdar and Zilong Wang

Time-Aware Abstractions in HybridSal ...................................... 504
   Ashish Tiwari

A Type-Directed Approach to Program Repair ................................. 511
   Alex Reinking and Ruzica Piskac

Formal Design and Safety Analysis of AIR6110 Wheel Brake System ........ 518
   M. Bozzano, A. Cimatti, A. Fernandes Pires, D. Jones, G. Kimberly,
   T. Petri, R. Robinson, and S. Tonetta
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meeting a Powertrain Verification Challenge</td>
<td>536</td>
</tr>
<tr>
<td>Parasara Sridhar Duggirala, Chuchu Fan, Sayan Mitra, and Mahesh Viswanathan</td>
<td></td>
</tr>
<tr>
<td>Synthesising Executable Gene Regulatory Networks from Single-Cell Gene Expression Data</td>
<td>544</td>
</tr>
<tr>
<td>Jasmin Fisher, Ali Sinan Köksal, Nir Piterman, and Steven Woodhouse</td>
<td></td>
</tr>
<tr>
<td>Empirical Software Metrics for Benchmarking of Verification Tools</td>
<td>561</td>
</tr>
<tr>
<td>Yulia Demyanova, Thomas Pani, Helmut Veith, and Florian Zuleger</td>
<td></td>
</tr>
</tbody>
</table>

**Interpolation, IC3/PDR, and Invariants**

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property-Directed Inference of Universal Invariants or Proving Their Absence</td>
<td>583</td>
</tr>
<tr>
<td>A. Karbyshev, N. Björner, S. Itzhaky, N. Rinetzky, and S. Shoham</td>
<td></td>
</tr>
<tr>
<td>Efficient Anytime Techniques for Model-Based Safety Analysis</td>
<td>603</td>
</tr>
<tr>
<td>Marco Bozzano, Alessandro Cimatti, Alberto Griggio, and Cristian Mattarei</td>
<td></td>
</tr>
<tr>
<td>Boosting k-Induction with Continuously-Refined Invariants</td>
<td>622</td>
</tr>
<tr>
<td>Dirk Beyer, Matthias Dangl, and Philipp Wendler</td>
<td></td>
</tr>
<tr>
<td>Fast Interpolating BMC</td>
<td>641</td>
</tr>
<tr>
<td>Yakir Vizel, Arie Gurfinkel, and Sharad Malik</td>
<td></td>
</tr>
<tr>
<td>Counterexample-Guided Polynomial Loop Invariant Generation by Lagrange Interpolation</td>
<td>658</td>
</tr>
<tr>
<td>Yu-Fang Chen, Chih-Duo Hong, Bow-Yaw Wang, and Lijun Zhang</td>
<td></td>
</tr>
<tr>
<td>Author Index</td>
<td>675</td>
</tr>
</tbody>
</table>