

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

*Lancaster University, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Alfred Kobsa

*University of California, Irvine, CA, USA*

Friedemann Mattern

*ETH Zurich, Switzerland*

John C. Mitchell

*Stanford University, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

Oscar Nierstrasz

*University of Bern, Switzerland*

C. Pandu Rangan

*Indian Institute of Technology, Madras, India*

Bernhard Steffen

*TU Dortmund University, Germany*

Madhu Sudan

*Microsoft Research, Cambridge, MA, USA*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max Planck Institute for Informatics, Saarbruecken, Germany*

P. Madhusudan  
Sanjit A. Seshia (Eds.)

# Computer Aided Verification

24th International Conference, CAV 2012  
Berkeley, CA, USA, July 7-13, 2012  
Proceedings

Volume Editors

P. Madhusudan

University of Illinois at Urbana-Champaign

Dept. of Computer Science

3226 Siebel Center, 201 N. Goodwin Avenue, Urbana, IL 61801-2302, USA

E-mail: madhu@illinois.edu

Sanjit A. Seshia

University of California, Berkeley

Dept. of Electrical Engineering and Computer Science

253 Cory Hall # 1770, Berkeley, CA 94720-1770, USA

E-mail: sseshia@eecs.berkeley.edu

ISSN 0302-9743

e-ISSN 1611-3349

ISBN 978-3-642-31423-0

e-ISBN 978-3-642-31424-7

DOI 10.1007/978-3-642-31424-7

Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012940389

CR Subject Classification (1998): D.2.4-5, I.2.2, F.3, F.1.1-2, F.4, C.3, B.3, D.1

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

© Springer-Verlag Berlin Heidelberg 2012

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, 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.

*Typesetting:* Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

# Preface

This volume contains the proceedings of the 24th International Conference on Computer-Aided Verification (CAV) held in Berkeley, USA, July 7–3, 2012.

The Conference on Computer-Aided Verification (CAV) is dedicated to the advancement of the theory and practice of computer-aided formal methods for the analysis and synthesis of hardware, software, and other computational systems. Its scope ranges from theoretical results to concrete applications, with an emphasis on practical verification tools and the underlying algorithms and techniques.

The conference included two workshop days, a tutorial day, and three and a half days for the main program. We received 185 submissions (140 regular papers and 45 tool papers, a record number) and selected 38 regular and 20 tool papers. We appreciate the diligence of our Program Committee and our external reviewers, and thank them for their hard work; all papers received at least four reviews, and there was intense discussion on papers after the author response period.

This year CAV had four special tracks highlighted in the program: Computer Security, Embedded Systems, Hardware Verification, and SAT & SMT. We thank our Special Track Chairs for their effort in attracting papers in these areas and coordinating the review process for those papers.

The conference was preceded by seven affiliated workshops: The 5th International Workshop on Numerical Software Verification (NSV 2012); The First International Workshop on Memory Consistency Models (REORDER 2012); The 5th International Workshop on Exploiting Concurrency Efficiently and Correctly (EC2 2012); The Second International Workshop on Intermediate Verification Languages (BOOGIE 2012); The First Workshop on Logics for System Analysis (LISA 2012); The First Workshop on Synthesis (SYNT 2012); The First Workshop on Applications of Formal Methods in Systems Biology (AFMSB 2012).

In addition to the presentations for the accepted papers, the conference also featured three invited talks and four invited tutorials.

– Invited talks:

- Wolfgang Thomas (RWTH, Aachen): “Synthesis and Some of Its Challenges”
- David Dill (Stanford University): “Model Checking Cell Biology”
- J. Alex Halderman (University of Michigan): “On Security of Voting Machines”

– Invited tutorials:

- Ras Bodik (University of California, Berkeley): “Synthesizing Programs with Constraint Solvers”
- Aaron Bradley (University of Colorado at Boulder): “IC3 and Beyond: Incremental, Inductive Verification”

- Chris Myers (University of Utah): “Formal Verification of Genetic Circuits”
- Michal Moskal (Microsoft) “From C to Infinity and Back: Unbounded Auto-active Verification with VCC”

We thank all our invited speakers!

We also thank the members of the CAV Steering Committee—Michael Gordon, Orna Grumberg, Bob Kurshan, and Ken McMillan—for their advice on various organizational matters. Shuvendu Lahiri, our Workshop Chair, smoothly handled the organization of the workshops. Miyoko Tsubamoto played an invaluable role in handling local arrangements. We thank Bryan Brady for his service as Publicity Chair and Edgar Pek for maintaining the website. Special thanks go to the Past Chairs, Ganesh Gopalakrishnan and Shaz Qadeer, for their advice and guidance throughout the process. We thank Alfred Hofmann and Anna Kramer of Springer for publishing the paper and USB proceedings for CAV 2012. We are grateful to Andrei Voronkov and his team for the use of the EasyChair system for tracking reviews and preparing the final camera-ready version. We gratefully acknowledge the donations provided by our corporate sponsors—Microsoft Research, IBM Research, Coverity, NEC Labs, and Intel. And last, but not the least, we thank the office staff of EECS Department at the University of California, Berkeley, and the Department of Computer Science at the University of Illinois at Urbana-Champaign, for providing critical administrative assistance in organizing the conference.

May 2012

P. Madhusudan  
Sanjit A. Seshia

# Organization

## Program Committee

Rajeev Alur	University of Pennsylvania, USA
Roderick Bloem	Graz University of Technology, Austria
Supratik Chakraborty	IIT Bombay, India
Swarat Chaudhuri	Rice University, USA
Adam Chlipala	MIT, USA
Vincent Danos	University of Edinburgh, UK
Thomas Dillig	College of William and Mary, USA
Andy Gordon	Microsoft Research
Mike Gordon	University of Cambridge, UK
Orna Grumberg	Technion - Israel Institute of Technology, Israel
Aarti Gupta	NEC Labs America, USA
William Hung	Synopsys Inc.
Somesh Jha	University of Wisconsin, Madison, USA
Ranjit Jhala	University of California, San Diego, USA
Bengt Jonsson	Uppsala University, Sweden
Rajeev Joshi	NASA JPL
Daniel Kroening	Oxford University, UK
Andreas Kuehlmann	Coverity
Viktor Kuncak	EPFL, Switzerland
Shuvendu Lahiri	Microsoft Research
P. Madhusudan	University of Illinois, Urbana-Champaign, USA
Rupak Majumdar	MPI-SWS
Ken Mcmillan	Microsoft Research
David Molnar	Microsoft Research
Kedar Namjoshi	Bell Labs
Albert Oliveras	Technical University of Catalonia, Spain
Joel Ouaknine	Oxford University, UK
Gennaro Parlato	University of Southampton, UK
Nir Piterman	University of Leicester, UK
Andreas Podelski	University of Freiburg, Germany
Shaz Qadeer	Microsoft Research
Zvonimir Rakamaric	University of Utah, USA
Sriram Sankaranarayanan	University of Colorado, Boulder, USA
Sanjit A. Seshia	University of California, Berkeley, USA
Natasha Sharygina	University of Lugano, Switzerland
Stavros Tripakis	University of California, Berkeley, USA
Helmut Veith	Vienna University of Technology, Austria
Mahesh Viswanathan	University of Illinois, Urbana-Champaign, USA
Jin Yang	Intel Corporation
Karen Yorav	IBM Haifa Research Lab, Israel

## Additional Reviewers

Abio, Ignasi  
Adir, Allon  
Akshay, S.  
Alberti, Francesco  
Atig, Mohamed Faouzi  
Bennett, Huxley  
Bing, Liu  
Bingham, Jesse  
Bogomolov, Sergiy  
Boigelot, Bernard  
Bruttomesso, Roberto  
Bustan, Doron  
Calin, Georgel  
Chadha, Rohit  
Chatterjee, Debapriya  
Chen, Yu-Fang  
Chockler, Hana  
Cimatti, Alessandro  
D'Solva, Vijay  
Dang, Thao  
Darulova, Eva  
Davidson, Drew  
Demyanova, Yulia  
Donaldson, Alastair  
Duggirala, Parasara Sridhar  
Eisner, Cindy  
Emmi, Michael  
Enea, Constantin  
Esmaeilsabzali, Shahram  
Faouzi, Mohamed  
Farzan, Azadeh  
Fedyukovich, Grigory  
Finkbeiner, Bernd  
Fischer, Bernd  
Florian, Mihai  
Fredrikson, Matt  
Frehse, Goran  
Ganty, Pierre  
Garg, Pranav  
Gay, Simon  
Geilen, Marc  
German, Steven  
Giannakopoulou, Dimitra

Goubault, Eric  
Griesmayer, Andreas  
Grinchtein, Olga  
Groce, Alex  
Guan, Nan  
Gurfinkel, Arie  
Habermehl, Peter  
Hariharan, Ramesh  
Harris, William  
Harrison, John  
Hofferek, Georg  
Holcomb, Daniel  
Holzer, Andreas  
Holzmann, Gerard  
Iosif, Radu  
Ivrii, Alexander  
Jacobs, Swen  
Jha, Sumit Kumar  
Jha, Susmit  
Jhala, Ranjit  
Jobstmann, Barbara  
John, Annu  
Keidar Barner, Sharon  
Khalimov, Ayrat  
Kini, Dileep  
Kneuss, Etienne  
Koenighofer, Robert  
Konnov, Igor  
Korchemny, Dmitry  
Krstic, Sava  
Kumar, Pratyush  
La Torre, Salvatore  
Lal, Akash  
Legay, Axel  
Leonardsson, Carl  
Leroux, Jerome  
Lewis, Matt  
Li, Wenchao  
Lodaya, Kamal  
Logozzo, Francesco  
Luchangco, Victor  
Lucaup, Daniel  
Matsliah, Arie

Miné, Antoine  
Monniaux, David  
Nadel, Alexander  
Narayanaswamy, Ganesh  
Nevo, Ziv  
Nickovic, Dejan  
Orni, Avigail  
Pandav, Sudhindra  
Parker, David  
Parkinson, Matthew  
Persson, Magnus  
Pill, Ingo  
Piskac, Ruzica  
Platzer, André  
Prabhu, Prathmesh  
Qian, Kairong  
Rajamani, Sriram  
Rajan, Ajitha  
Raskin, Jean-Francois  
Ray, Sandip  
Rezine, Othmane  
Riener, Heinz  
Rodriguez-Carbonell, Enric  
Rollini, Simone Fulvio  
Ruah, Sitvanit  
Rubio, Albert  
Ruemmer, Philipp  
Rungta, Neha  
Rybalchenko, Andrey  
Sadrzadeh, Mehrnoosh  
Samanta, Roopsha  
Sangnier, Arnaud  
Schewe, Sven  
Sery, Ondrej  
Shashidhar, K.C.  
Sheinvald, Sarai  
Shoham, Sharon  
Shurek, Gil  
Sighireanu, Mihaela  
Sinha, Rohit  
Sinn, Moritz  
Sosnovich, Adi  
Spielmann, Andrej  
Srivastava, Saurabh  
Stenman, Jari  
Stigge, Martin  
Strichman, Ofer  
Suter, Philippe  
Talupur, Murali  
Tautschnig, Michael  
Terauchi, Tachio  
Tiwari, Ashish  
Tristan, Jean-Baptiste  
Tsitovich, Aliaksei  
Tuerk, Thomas  
Vizel, Yakir  
Wahl, Thomas  
Wang, Bow-Yaw  
Wang, Chao  
Wasson, Zach  
Weissenbacher, Georg  
Welp, Tobias  
Widder, Josef  
Wintersteiger, Christoph  
Worrell, James  
Yi, Wang  
Yu, Andy  
Zamfir, Cristian  
Zuleger, Florian  
Zuliani, Paolo



# Table of Contents

## Invited Talks

Synthesis and Some of Its Challenges . . . . .	1
<i>Wolfgang Thomas</i>	
Model Checking Cell Biology . . . . .	2
<i>David L. Dill</i>	

## Invited Tutorials

Synthesizing Programs with Constraint Solvers . . . . .	3
<i>Rastislav Bodik and Emina Torlak</i>	
IC3 and beyond: Incremental, Inductive Verification . . . . .	4
<i>Aaron R. Bradley</i>	
Formal Verification of Genetic Circuits . . . . .	5
<i>Chris J. Myers</i>	
From C to Infinity and Back: Unbounded Auto-active Verification with VCC . . . . .	6
<i>Michał Moskal</i>	

## Automata and Synthesis

Deterministic Automata for the (F,G)-Fragment of LTL . . . . .	7
<i>Jan Křetínský and Javier Esparza</i>	
Efficient Controller Synthesis for Consumption Games with Multiple Resource Types . . . . .	23
<i>Tomáš Brázdil, Krishnendu Chatterjee, Antonín Kučera, and Petr Novotný</i>	
ACTL $\cap$ LTL Synthesis . . . . .	39
<i>Rüdiger Ehlers</i>	

## Inductive Inference and Termination

Learning Boolean Functions Incrementally . . . . .	55
<i>Yu-Fang Chen and Bow-Yaw Wang</i>	
Interpolants as Classifiers . . . . .	71
<i>Rahul Sharma, Aditya V. Nori, and Alex Aiken</i>	

Termination Analysis with Algorithmic Learning . . . . . 88  
*Wonchan Lee, Bow-Yaw Wang, and Kwangkeun Yi*

Automated Termination Proofs for Java Programs with Cyclic Data . . . . 105  
*Marc Brockschmidt, Richard Musiol, Carsten Otto, and Jürgen Giesl*

Proving Termination of Probabilistic Programs Using Patterns . . . . . 123  
*Javier Esparza, Andreas Gaiser, and Stefan Kiefer*

**Abstraction**

The Gauge Domain: Scalable Analysis of Linear Inequality Invariants . . . 139  
*Arnaud J. Venet*

Diagnosing Abstraction Failure for Separation Logic-Based Analyses . . . 155  
*Josh Berdine, Arlen Cox, Samin Ishtiaq, and  
 Christoph M. Wintersteiger*

A Method for Symbolic Computation of Abstract Operations . . . . . 174  
*Aditya Thakur and Thomas Reps*

Leveraging Interpolant Strength in Model Checking . . . . . 193  
*Simone Fulvio Rollini, Ondrej Sery, and Natasha Sharygina*

**Concurrency and Software Verification**

Detecting Fair Non-termination in Multithreaded Programs . . . . . 210  
*Mohamed Faouzi Atig, Ahmed Bouajjani, Michael Emmi, and  
 Akash Lal*

Lock Removal for Concurrent Trace Programs . . . . . 227  
*Vineet Kahlon and Chao Wang*

How to Prove Algorithms Linearisable . . . . . 243  
*Gerhard Schellhorn, Heike Wehrheim, and John Derrick*

Synchronisation- and Reversal-Bounded Analysis of Multithreaded  
 Programs with Counters . . . . . 260  
*Matthew Hague and Anthony Widjaja Lin*

Software Model Checking via IC3 . . . . . 277  
*Alessandro Cimatti and Alberto Griggio*

**Biology and Probabilistic Systems**

Delayed Continuous-Time Markov Chains for Genetic Regulatory  
 Circuits . . . . . 294  
*Călin C. Guet, Ashutosh Gupta, Thomas A. Henzinger,  
 Maria Mateescu, and Ali Sezgin*

Assume-Guarantee Abstraction Refinement for Probabilistic Systems . . .	310
<i>Anvesh Komuravelli, Corina S. Păsăreanu, and Edmund M. Clarke</i>	

Cross-Entropy Optimisation of Importance Sampling Parameters for Statistical Model Checking . . . . .	327
<i>Cyrille Jegourel, Axel Legay, and Sean Sedwards</i>	

## Embedded and Control Systems

Timed Relational Abstractions for Sampled Data Control Systems . . . . .	343
<i>Aditya Zutshi, Sriram Sankaranarayanan, and Ashish Tiwari</i>	

Approximately Bisimilar Symbolic Models for Digital Control Systems . . . . .	362
<i>Rupak Majumdar and Majid Zamani</i>	

Formal Verification and Validation of ERTMS Industrial Railway Train Spacing System . . . . .	378
<i>Alessandro Cimatti, Raffaele Corvino, Armando Lazzaro, Iman Narasamdya, Tiziana Rizzo, Marco Roveri, Angela Sansevieri, and Andrei Tchaltsev</i>	

## SAT/SMT Solving and SMT-based Verification

Minimum Satisfying Assignments for SMT . . . . .	394
<i>Isil Dillig, Thomas Dillig, Kenneth L. McMillan, and Alex Aiken</i>	

When Boolean Satisfiability Meets Gaussian Elimination in a Simplex Way . . . . .	410
<i>Cheng-Shen Han and Jie-Hong Roland Jiang</i>	

A Solver for Reachability Modulo Theories . . . . .	427
<i>Akash Lal, Shaz Qadeer, and Shuvendu K. Lahiri</i>	

## Timed and Hybrid Systems

On Decidability of Prebisimulation for Timed Automata . . . . .	444
<i>Shibashis Guha, Chinmay Narayan, and S. Arun-Kumar</i>	

Exercises in <i>Nonstandard Static Analysis</i> of Hybrid Systems . . . . .	462
<i>Ichiro Hasuo and Kohei Suenaga</i>	

A Box-Based Distance between Regions for Guiding the Reachability Analysis of SpaceEx . . . . .	479
<i>Sergiy Bogomolov, Goran Frehse, Radu Grosu, Hamed Ladan, Andreas Podelski, and Martin Wehrle</i>	

## Hardware Verification

An Axiomatic Memory Model for POWER Multiprocessors . . . . .	495
<i>Sela Mador-Haim, Luc Maranget, Susmit Sarkar, Kayvan Memarian, Jade Alglave, Scott Owens, Rajeev Alur, Milo M.K. Martin, Peter Sewell, and Derek Williams</i>	
nuTAB-BackSpace: Rewriting to Normalize Non-determinism in Post-silicon Debug Traces . . . . .	513
<i>Flavio M. De Paula, Alan J. Hu, and Amir Nahir</i>	
Incremental, Inductive CTL Model Checking . . . . .	532
<i>Zyad Hassan, Aaron R. Bradley, and Fabio Somenzi</i>	

## Security

Efficient Runtime Policy Enforcement Using Counterexample-Guided Abstraction Refinement . . . . .	548
<i>Matthew Fredrikson, Richard Joiner, Somesh Jha, Thomas Reps, Phillip Porras, Hassen Saïdi, and Vinod Yegneswaran</i>	
Automatic Quantification of Cache Side-Channels . . . . .	564
<i>Boris Köpf, Laurent Mauborgne, and Martín Ochoa</i>	
Secure Programming via Visibly Pushdown Safety Games . . . . .	581
<i>William R. Harris, Somesh Jha, and Thomas Reps</i>	

## Verification and Synthesis

Alternate and Learn: Finding Witnesses without Looking All over . . . . .	599
<i>Nishant Sinha, Nimit Singhania, Satish Chandra, and Manu Sridharan</i>	
A Complete Method for Symmetry Reduction in Safety Verification . . . .	616
<i>Duc-Hiep Chu and Joxan Jaffar</i>	
Synthesizing Number Transformations from Input-Output Examples . . . .	634
<i>Rishabh Singh and Sumit Gulwani</i>	

## Tool Demonstration Papers

Acacia+, a Tool for LTL Synthesis . . . . .	652
<i>Aaron Bohy, Véronique Bruyère, Emmanuel Filiot, Naiyong Jin, and Jean-François Raskin</i>	
MGSyn: Automatic Synthesis for Industrial Automation . . . . .	658
<i>Chih-Hong Cheng, Michael Geisinger, Harald Ruess, Christian Buckl, and Alois Knoll</i>	

OpenNWA: A Nested-Word Automaton Library . . . . .	665
<i>Evan Driscoll, Aditya Thakur, and Thomas Reps</i>	
UFO: A Framework for Abstraction- and Interpolation-Based Software Verification . . . . .	672
<i>Aws Albarghouthi, Yi Li, Arie Gurfinkel, and Marsha Chechik</i>	
SAFARI: SMT-Based Abstraction for Arrays with Interpolants . . . . .	679
<i>Francesco Alberti, Roberto Bruttomesso, Silvio Ghilardi, Silvio Ranise, and Natasha Sharygina</i>	
BMA: Visual Tool for Modeling and Analyzing Biological Networks . . . . .	686
<i>David Benque, Sam Bourton, Caitlin Cockerton, Byron Cook, Jasmin Fisher, Samin Ishtiaq, Nir Piterman, Alex Taylor, and Moshe Y. Vardi</i>	
APEX: An Analyzer for Open Probabilistic Programs . . . . .	693
<i>Stefan Kiefer, Andrzej S. Murawski, Joël Ouaknine, Björn Wachter, and James Worrell</i>	
Recent Developments in FDR . . . . .	699
<i>Philip Armstrong, Michael Goldsmith, Gavin Lowe, Joël Ouaknine, Hristina Palikareva, A. W. Roscoe, and James Worrell</i>	
A Model Checker for Hierarchical Probabilistic Real-Time Systems . . . . .	705
<i>Songzheng Song, Jun Sun, Yang Liu, and Jin Song Dong</i>	
SYMDIFF: A Language-Agnostic Semantic Diff Tool for Imperative Programs . . . . .	712
<i>Shuvendu K. Lahiri, Chris Hawblitzel, Ming Kawaguchi, and Henrique Rebêlo</i>	
Cubicle: A Parallel SMT-Based Model Checker for Parameterized Systems: Tool Paper . . . . .	718
<i>Sylvain Conchon, Amit Goel, Sava Krstić, Alain Mésout, and Fatiha Zaïdi</i>	
HybridSAL Relational Abstracter . . . . .	725
<i>Ashish Tiwari</i>	
EULER: A System for Numerical Optimization of Programs . . . . .	732
<i>Swarat Chaudhuri and Armando Solar-Lezama</i>	
SPT: Storyboard Programming Tool . . . . .	738
<i>Rishabh Singh and Armando Solar-Lezama</i>	
CSolve: Verifying C with Liquid Types . . . . .	744
<i>Patrick Rondon, Alexander Bakst, Ming Kawaguchi, and Ranjit Jhala</i>	

PASSERT: A Tool for Debugging Parallel Programs . . . . .	751
<i>Daniel Schwartz-Narbonne, Feng Liu, David August, and Sharad Malik</i>	
TRACER: A Symbolic Execution Tool for Verification . . . . .	758
<i>Joxan Jaffar, Vijayaraghavan Murali, Jorge A. Navas, and Andrew E. Santosa</i>	
Joogie: Infeasible Code Detection for Java . . . . .	767
<i>Stephan Arlt and Martin Schäf</i>	
HECTOR: An Equivalence Checker for a Higher-Order Fragment of ML . . . . .	774
<i>David Hopkins, Andrzej S. Murawski, and C.-H. Luke Ong</i>	
Resource Aware ML . . . . .	781
<i>Jan Hoffmann, Klaus Aehlig, and Martin Hofmann</i>	
<b>Author Index</b> . . . . .	<b>787</b>