Lecture Notes in Computer Science 7358

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

P. Madhusudan
Sanjit A. Seshia (Eds.)

Computer Aided Verification

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

Springer

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

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 (LfSA 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 Verication 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
Luchaup, 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

Invited Tutorials

Automata and Synthesis

Inductive Inference and Termination

Abstraction

Concurrency and Software Verification

Biology and Probabilistic Systems

Embedded and Control Systems

SAT/SMT Solving and SMT-based Verification

Timed and Hybrid Systems

Hardware Verification

Security

Verification and Synthesis

Tool Demonstration Papers