

Lecture Notes in Computer Science

2725

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer

Berlin

Heidelberg

New York

Hong Kong

London

Milan

Paris

Tokyo

Warren A. Hunt, Jr. Fabio Somenzi (Eds.)

Computer Aided Verification

15th International Conference, CAV 2003
Boulder, CO, USA, July 8-12, 2003
Proceedings



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Warren A. Hunt, Jr.
University of Texas at Austin, Department of Computer Sciences
Taylor Hall, M/S C0500, Austin, TX 78712-1188, USA
E-mail: hunt@cs.utexas.edu

Fabio Somenzi
University of Colorado, Department of Electrical and Computer Engineering
Campus Box 425, Boulder, CO 80309-0425, USA
E-mail: Fabio@Colorado.edu

Cataloging-in-Publication Data applied for

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie;
detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>.

CR Subject Classification (1998): F.3, D.2.4, D.2.2, F.4.1, I.2.3, B.7.2, C.3

ISSN 0302-9743

ISBN 3-540-40524-0 Springer-Verlag Berlin Heidelberg New York

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-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2003
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Markus Richter, Heidelberg
Printed on acid-free paper SPIN: 10929025 06/3142 5 4 3 2 1 0

Preface

This volume contains the proceedings of the conference on *Computer Aided Verification* (CAV 2003) held in Boulder, Colorado, on July 8–12, 2003. CAV 2003 was the 15th in a series of conferences dedicated to the advancement of the theory and practice of computer-assisted formal analysis methods for hardware and software systems. The conference covers the spectrum from theoretical results to applications, with emphasis on practical verification tools, including algorithms and techniques needed for their implementation. The conference has traditionally drawn contributions from researchers as well as practitioners in both academia and industry.

The program of the conference consisted of 32 regular papers, selected from 87 submissions. In addition, the CAV program featured 9 tool presentations and demonstrations selected from 15 submissions. Each submission received an average of 5 referee reviews. The large number of tool submissions and presentations testifies to the liveliness of the field and to its applied flavor.

The CAV 2003 program included a tutorial day with three invited tutorials by Ken McMillan (Cadence) on *SAT-Based Methods for Unbounded Model Checking*, Doron Peled (Warwick) on *Algorithmic Testing Methods*, and Willem Visser (NASA) on *Model Checking Programs with Java PathFinder*. The conference also included two invited talks by Amitabh Srivastava (Microsoft) and Michael Gordon (Cambridge). Five workshops were associated with CAV 2003:

- ACL2 2003: 4th International Workshop on the ACL2 Theorem Prover and Its Applications.
- BMC 2003: 1st International Workshop on Bounded Model Checking.
- PDMC 2003: 2nd International Workshop on Parallel and Distributed Model Checking.
- RV 2003: 3rd Workshop on Runtime Verification.
- SoftMC 2003: 2nd Workshop on Software Model Checking.

The publication of these workshop proceedings was managed by the respective chairs, independently of the present proceedings.

We would like to thank all the Program Committee members and the sub-referees who assisted in the selection of the papers. Our thanks also go to the Steering Committee members and to last year's organizers for their helpful advice. Special thanks go to Virginia Schultz of the Office of Conference Services of the University of Colorado for assisting with the local arrangements; to Robert Krug for installing and managing the START Conference System; and to Erik Reeber for the production of the final proceedings. Finally, we gratefully acknowledge support from IBM, Intel, and Esterel Technologies.

Program Committee

Rajeev Alur (Pennsylvania)	Orna Kupferman (Hebrew University)
George Avrunin (Massachusetts)	Bob Kurshan (Cadence)
Armin Biere (ETH Zürich)	Yassine Lakhnech (IMAG)
Roderick Bloem (Graz)	Kim Guldstrand Larsen (Aalborg)
Ed Clarke (CMU)	Peter Manolios (Georgia Tech)
Matt Dwyer (Kansas State)	Ken McMillan (Cadence)
E. Allen Emerson (Texas)	Tom Melham (Oxford)
Steven German (IBM)	Chris J. Myers (Utah)
Orna Grumberg (Technion)	Kedar Namjoshi (Bell Labs)
Alan Hu (British Columbia)	Doron A. Peled (Warwick)
Warren A. Hunt, Jr. (Texas, co-chair)	Sriram Rajamani (Microsoft)
Robert B. Jones (Intel)	Thomas Shiple (Synopsys)
Bengt Jonsson (Uppsala)	Fabio Somenzi (Colorado, co-chair)
Nils Klarlund (ATT)	Helmut Veith (TU Wien)
Andreas Kuehlmann (Cadence)	Yaron Wolfsthal (IBM)

Steering Committee

Edmund M. Clarke (CMU)	Amir Pnueli (Weizmann)
Robert P. Kurshan (Cadence)	Joseph Sifakis (IMAG)

Sponsors

IBM
Esterel Technologies
Intel

Referees

Mark Aagaard	Gadiel Auerbach	Ritwik Bhattacharya
Parosh Abdulla	Mohammad Awedh	Jesse D. Bingham
Cyril Allauzen	Christel Baier	Per Bjesse
Nina Amla	Thomas Ball	Rastislav Bodik
Torben Amtoft	Jason Baumgartner	Ahmed Bouajjani
Konstantine Arkoudas	Gerd Behrmann	Patricia Bouyer
Cyrille Artho	Shoham Ben-David	Marius Bozga
Eugene Asarin	Johan Bengtsson	Donald Chai
Hossein S. Attar	Sergey Berezin	Sagar Chaki

Ching-Tsun Chou	Charanjit Jutla	Shaz Qadeer
David Dagon	Vineet Kahlon	Ishai Rabinovitz
Anat Dahan	Gila Kamhi	Venkatesh Prasad Ran-
Weizhen Dai	Joost-Pieter Katoen	ganath
Dennis Dams	Sagi Katz	Kavita Ravi
Thao Dang	Shmuel Katz	Sandip Ray
Ashish Darbari	Stefan Katzenbeisser	Erik Reeber
Alexandre David	Sharon Keidar-Barner	Robby
David Deharbe	Mike Kishinevsky	Marco Roveri
William Deng	Daniel Kroening	Sitvanit Ruah
J. Deshmukh	Robert Krug	Hassen Saidi
Rolf Drechsler	Antonin Kucera	Marko Samer
Xiaoqun Du	Jim Kukula	Jun Sawada
Stefan Edelkamp	Ranko Lazic	Karsten Schmidt
Cindy Eisner	Tim Leonard	Viktor Schuppan
Cristian Ene	Flavio Lerda	Assaf Schuster
Kousha Etessami	Martin Leucker	Stefan Schwoon
Eitan Farchi	Bing Li	Bikram Sengupta
Ansgar Fehnker	Yuan Lu	Ohad Shacham
Elena Fersman	Hanbing Lui	Vitaly Shmatikov
Görschwin Fey	Yoad Lustig	Sharon Shoham
Dana Fisman	Tony Ma	Eli Singerman
Emmanuel Fleury	P. Madhusudan	Nishant Sinha
Ruben Gamboa	Monika Maidl	Prasad Sistla
Blaise Genest	Oded Maler	Christian Stangier
Rob Gerth	Freddy Mang	Ofer Strichman
Dimitra Giannakopoulou	S. Manley	Rob Summers
Alain Girault	Rupak Majumdar	Matyas Sustik
Ganesh Gopalakrishnan	Alexander Medvedev	Bassam Tabbara
Susanne Graf	Todd Millstein	Paulo Tabuada
Alan Hartman	Marius Minea	Murali Talupur
John Hatcliff	Laurent Mounier	Oksana Tkachuk
Klaus Havelund	Anca Muscholl	Richard Treffer
Holger Hermanns	Naren Narasimhan	Stavros Tripakis
Tamir Heyman	Ziv Nevo	Ken Turner
Stefan Höreth	Matthew Nichols	Rachel Tzoref
Neil Immerman	Marcus Nilsson	Serita Van Groningen
Radu Iosif	John O'Leary	Moshe Vardi
S. Iyer	Arlindo Oliveira	Miroslav Velev
Ranjit Jhala	Joel Ouaknine	Bjorn Victor
Wei Jiang	Viresh Paruthi	Catalin Visinescu
HoonSang Jin	Corina Pasareanu	Willem Visser
Rajeev Joshi	Paul Pettersson	Vinod Viswanath
Alma Lizbeth Juarez-	Nir Piterman	Daron Vroon
Dominguez	Mitra Purandare	T. Wahl

VIII Organization

Chao Wang

Farn Wang

Rafael Wisniewski

Jin Yang

Karen Yorav

Yunshan Zhu

David Zook

Table of Contents

Extending Bounded Model Checking

Interpolation and SAT-Based Model Checking	1
<i>K.L. McMillan</i>	

Bounded Model Checking and Induction: From Refutation to Verification	14
<i>Leonardo de Moura, Harald Rueß, Maria Sorea</i>	

Symbolic Model Checking

Reasoning with Temporal Logic on Truncated Paths	27
<i>Cindy Eisner, Dana Fisman, John Havlicek, Yoad Lustig, Anthony McIsaac, David Van Campenhout</i>	

Structural Symbolic CTL Model Checking of Asynchronous Systems	40
<i>Gianfranco Ciardo, Radu Siminiceanu</i>	

A Work-Efficient Distributed Algorithm for Reachability Analysis	54
<i>Orna Grumberg, Tamir Heyman, Assaf Schuster</i>	

Games, Trees, and Counters

Modular Strategies for Infinite Games on Recursive Graphs	67
<i>Rajeev Alur, Salvatore La Torre, P. Madhusudan</i>	

Fast Mu-Calculus Model Checking when Tree-Width Is Bounded	80
<i>Jan Obdržálek</i>	

Dense Counter Machines and Verification Problems	93
<i>Gaoyan Xie, Zhe Dang, Oscar H. Ibarra, Pierluigi San Pietro</i>	

Tool Presentations I

TRIM: A Tool for Triggered Message Sequence Charts	106
<i>Bikram Sengupta, Rance Cleaveland</i>	

Model Checking Multi-Agent Programs with CASP	110
<i>Rafael H. Bordini, Michael Fisher, Carmen Pardavila, Willem Visser, Michael Wooldridge</i>	

Monitoring Temporal Rules Combined with Time Series	114
<i>Doron Drusinsky</i>	

FAST: Fast Acceleration of Symbolic Transition Systems	118
<i>Sébastien Bardin, Alain Finkel, Jérôme Leroux, Laure Petrucci</i>	

Rabbit: A Tool for BDD-Based Verification of Real-Time Systems	122
<i>Dirk Beyer, Claus Lewerentz, Andreas Noack</i>	

Abstraction I

Making Predicate Abstraction Efficient: How to Eliminate Redundant Predicates	126
<i>Edmund Clarke, Orna Grumberg, Muralidhar Talupur, Dong Wang</i>	
A Symbolic Approach to Predicate Abstraction	141
<i>Shuvendu K. Lahiri, Randal E. Bryant, Byron Cook</i>	
Unbounded, Fully Symbolic Model Checking of Timed Automata Using Boolean Methods	154
<i>Sanjit A. Seshia, Randal E. Bryant</i>	

Dense Time

Digitizing Interval Duration Logic	167
<i>Gaurav Chakravorty, Paritosh K. Pandya</i>	
Timed Control with Partial Observability	180
<i>Patricia Bouyer, Deepak D’Souza, P. Madhusudan, Antoine Petit</i>	
Hybrid Acceleration Using Real Vector Automata	193
<i>Bernard Boigelot, Frédéric Herbreteau, Sébastien Jodogne</i>	

Tool Presentations II

Abstraction and BDDs Complement SAT-Based BMC in <i>DiVer</i>	206
<i>Aarti Gupta, Malay Ganai, Chao Wang, Zijiang Yang, Pranav Ashar</i>	
TLQSolver: A Temporal Logic Query Checker	210
<i>Marsha Chechik, Arie Gurfinkel</i>	
Evidence Explorer: A Tool for Exploring Model-Checking Proofs	215
<i>Yifei Dong, C.R. Ramakrishnan, Scott A. Smolka</i>	
HERMES: An Automatic Tool for Verification of Secrecy in Security Protocols	219
<i>Liana Bozga, Yassine Lakhnech, Michaël Périn</i>	

Infinite State Systems

Iterating Transducers in the Large	223
<i>Bernard Boigelot, Axel Legay, Pierre Wolper</i>	
Algorithmic Improvements in Regular Model Checking	236
<i>Parosh Aziz Abdulla, Bengt Jonsson, Marcus Nilsson, Julien d’Orso</i>	

Efficient Image Computation in Infinite State Model Checking	249
<i>Constantinos Bartzis, Tevfik Bultan</i>	

Abstraction II

Thread-Modular Abstraction Refinement	262
<i>Thomas A. Henzinger, Ranjit Jhala, Rupak Majumdar, Shaz Qadeer</i>	
A Game-Based Framework for CTL Counterexamples and 3-Valued Abstraction-Refinement	275
<i>Sharon Shoham, Orna Grumberg</i>	
Abstraction for Branching Time Properties	288
<i>Kedar S. Namjoshi</i>	

Applications

Certifying Optimality of State Estimation Programs	301
<i>Grigore Roşu, Ram Prasad Venkatesan, Jon Whittle, Laurenţiu Leuştean</i>	
Domain-Specific Optimization in Automata Learning	315
<i>Hardi Hungar, Oliver Niese, Bernhard Steffen</i>	
Model Checking Conformance with Scenario-Based Specifications	328
<i>Marcelo Glusman, Shmuel Katz</i>	

Theorem Proving

Deductive Verification of Advanced Out-of-Order Microprocessors	341
<i>Shuvendu K. Lahiri, Randal E. Bryant</i>	
Theorem Proving Using Lazy Proof Explication	355
<i>Cormac Flanagan, Rajeev Joshi, Xinming Ou, James B. Saxe</i>	

Automata-Based Verification

Enhanced Vacuity Detection in Linear Temporal Logic	368
<i>Roy Armoni, Limor Fix, Alon Flaisher, Orna Grumberg, Nir Piterman, Andreas Tiemeyer, Moshe Y. Vardi</i>	
Bridging the Gap between Fair Simulation and Trace Inclusion	381
<i>Yonit Kesten, Nir Piterman, Amir Pnueli</i>	
An Improved On-the-Fly Tableau Construction for a Real-Time Temporal Logic	394
<i>Marc Geilen</i>	

Invariants

Strengthening Invariants by Symbolic Consistency Testing	407
<i>Husam Abu-Haimed, Sergey Berezin, David L. Dill</i>	

Linear Invariant Generation Using Non-linear Constraint Solving	420
<i>Michael A. Colón, Sriram Sankaranarayanan, Henny B. Sipma</i>	

Explicit Model Checking

To Store or Not to Store	433
<i>Gerd Behrmann, Kim G. Larsen, Radek Pelánek</i>	

Calculating τ -Confluence Compositionally	446
<i>Gordon J. Pace, Frédéric Lang, Radu Mateescu</i>	

Author Index	461
-------------------------------	-----