

Lecture Notes in Computer Science

2404

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

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Tokyo

Ed Brinksma Kim Guldstrand Larsen (Eds.)

Computer Aided Verification

14th International Conference, CAV 2002
Copenhagen, Denmark, July 27-31, 2002
Proceedings



Springer

Series Editors

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

Volume Editors

Ed Brinksma
University of Twente, Department of Computer Science
P. O. Box 217, 7500 AE Enschede, The Netherlands
E-mail: brinksma@cs.utwente.nl

Kim Guldstrand Larsen
Aalborg University, Department of Computer Science
Fredrik Bajers Vej 7, 9220, Aalborg Ø, Denmark
E-mail: kgl@cs.auc.dk

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Computer aided verification : 14th international conference ; proceedings /
CAV 2002, Copenhagen, Denmark, July 27 - 31, 2002. Ed Brinksma ;
Kim Guldstrand Larsen (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ;
Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 2002
(Lecture notes in computer science ; Vol. 2404)
ISBN 3-540-43997-8

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 3-540-43997-8 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 2002
Printed in Germany

Typesetting: Camera-ready by author, data conversion by DA-TeX Gerd Blumenstein
Printed on acid-free paper SPIN 10873641 06/3142 5 4 3 2 1 0

Preface

This volume contains the proceedings of the conference on *Computer Aided Verification* (CAV 2002), held in Copenhagen, Denmark on July 27-31, 2002. CAV 2002 was the 14th in a series of conferences dedicated to the advancement of the theory and practice of computer-assisted formal analysis methods for software and hardware systems. The conference covers the spectrum from theoretical results to concrete applications, with an 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.

This year we received 94 regular paper submissions out of which 35 were selected. Each submission received an average of 4 referee reviews. In addition, the CAV program contained 11 tool presentations selected from 16 submissions. For each tool presentation, a demo was given at the conference. The large number of tool submissions and presentations testifies to the liveliness of the field and its applied flavor.

The CAV 2002 program included a tutorial day with three invited tutorials by Wolfgang Thomas (Aachen) on *Infinite Games and Verification*, Patrick Cousot (ENS Paris) on *Abstraction in Software Verification* and Thomas A. Henzinger (Berkeley) on *The Symbolic Approach to Hybrid Systems*. The conference also included two invited talks by Sharad Malik (Princeton) on *The Quest for Efficient Boolean Satisfiability Solvers* and Gerard J. Holzmann (Bell Labs) on *Software Analysis and Model Checking*. In addition, there were three workshops associated with CAV 2002:

- PAMP-PROBMIV: Process Algebras and Performance Modeling/Probabilistic Methods in Verification.
- RT-TOOLS: Workshop on Real-Time Tools.
- RV: Run-Time Verification.

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

We would like to thank all the Program Committee members and the sub-referees who assisted in their work. Our thanks also go to the Steering Committee members and last year's organizers for their helpful advice. The Local Organization Chair, Jens Christian Godskesen, deserves our gratitude for his contributions throughout the preparations. We would also like to thank the invited speakers and invited tutorial speakers, the authors of submitted papers, and all the participants of the conference. Special thanks go to Brian Nielsen for installing and managing the START Conference system and to Ole Høgh Jensen for the production of the final proceedings.

This year, CAV was part of the Federated Logic Conference (FLoC 2002), and was organized jointly with CADE (Conference on Automated Deduction),

FME (Formal Methods Europe), ICL (International Conference on Logic Programming), LICS (Logic in Computer Science), RTA (Rewriting Techniques and Applications), and TABLEAUX (Automated Reasoning with Analytic Tableaux and Related Methods). In particular, the invited talk given by Sharad Malik was joint with CADE 2002, and the paper also appears, in identical form, in the proceedings of CADE 2002. In addition, FLoC included 31 workshops associated with the different conferences. We would like to acknowledge the help of the FLoC 2002 steering committee Moshe Y. Vardi (General Chair), Neil D. Jones (Conference Chair), Ulrich Firbach (CADE), Edmund M. Clarke (CAV), Dines Bjørner (CAV), Catuscia Palamidessi (ICLP), Samson Abramsky (LICS), Nachum Dershowitz (RTA), Reiner Hähnle (TABLEAUX), Harald Ganzinger (Associate General Chair), and Dana Scott (IFCOLOG).

Finally, we gratefully acknowledge support from IBM, Esterel Technologies, IT-U of Copenhagen, the Department of Computer Science at Aalborg University, Twente University, and BRICS.

May 2002

Ed Brinksma and Kim Guldstrand Larsen

Program Committee

Thomas Ball (Microsoft Research)	Kim G. Larsen (Aalborg, co-chair)
David Basin (Freiburg)	Tim Leonard (Compaq)
Armin Biere (ETH Zürich)	Ken McMillan (Cadence)
Ed Brinksma (Twente, co-chair)	Kedar Namjoshi (Bell Labs)
Werner Damm (Oldenburg)	Doron A. Peled (Austin)
E. Allen Emerson (Austin)	Amir Pnueli (Weizmann Inst.)
Alain Finkel (Cachan)	Natarajan Shankar (SRI)
Nicolas Halbwachs (IMAG Grenoble)	Joseph Sifakis (IMAG Grenoble)
John Hatcliff (Kansas State)	Fabio Somenzi (Boulder)
Klaus Havelund (NASA)	Bernhard Steffen (Dortmund)
Thomas A. Henzinger (Berkeley)	Yaron Wolfsthal (IBM)
Andreas Kuehlmann (Cadence)	Wang Yi (Uppsala)
Orna Kupferman (Jerusalem)	

Steering Committee

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

Local Organizer

Jens Christian Godskesen (IT-U of Copenhagen)

Sponsors

IBM	Dept. of CS, Aalborg University
Esterel Technologies	Twente University
IT-U of Copenhagen	BRICS

Referees

Parosh Abdulla	Gerd Behrmann	Ionut Buricea
Nina Amla	Shoham Ben-David	Franck Cassez
Pablo Argon	Johan Bengtsson	Pavol Cerny
Tamarah Arons	Sergey Berezin	Hana Chockler
Cyrille Artho	Roderick Bloem	Thomas Colcombet
Evgueni Asarin	Bernard Boigelot	Dennis Dams
Gadiel Auerbach	Michele Boreale	Alexandre David
Abdelwaheb Ayari	Ahmed Bouajjani	Xiaoqun Du
Kamel Barkaoui	Patricia Bouyer	M. Dufлот
Sharon Barner	Marius Bozga	Bruno Dutertre

VIII Organization

Matthew Dwyer	Robert P. Kurshan	Grigore Rosu
Niklas Een	Yassine Lakhnech	Sitvanit Ruah
Cindy Eisner	Rom Langerak	Harald Ruess
Kousha Etessami	Jim Larus	John Rushby
Monica Farkash	Jerome Leroux	Oliver R��thing
Jean-Claude Fernandez	Xavier Leroy	Theo Ruys
D. Fink	Bing Li	Hassen Saidi
Dana Fisman	Angelika Mader	Jun Sawada
Emmanuel Fleury	Monika Maidl	Viktor Schuppan
Martin Fr��nzle	Rupak Majumdar	Helmut Seidl
Carl Chr. Frederiksen	Oded Maler	Ohad Shaham
L. Fribourg	Freddy Mang	Elad Shahar
Dimitra Giannakopoulou	Panagiotis Manolios	Gil Shurek
Patrice Godefroid	Nicolas Markey	Maria Sorea
Jean Goubault-Larrecq	Ken McMillan	Robert Staerk
Susanne Graf	Jon Millen	Christian Stehno
Claudia G��ttberger	Mark Minas	M. Sustik
Elsa Gunter	Sebastian Moedersheim	Gregoire Sutre
Alan Hartman	Oliver M��ller	Ashish Tiwari
Frederic Herbreteau	In-Ho Moon	Richard J. Tre��ler
Holger Hermanns	Remi Morin	Jan Tretmans
Gerard Holzmann	Laurent Mounier	Stavros Tripakis
Hardi Hungar	Leonardo de Moura	Tomas Uribe
Radu Iosif	Markus M��ller-Olm	Moshe Vardi
S. Iyer	Uwe Nestmann	Miroslav Velev
Damir Jamsek	Juergen Niehaus	Luca Vigano
Somesh Jha	Oliver Niese	S. Vinod
Ranjit Jhala	Thomas Noll	Willem Visser
HoonSang Jin	Abelardo Pardo	T. Wahl
Damien Joly	Corina Pasareanu	Chao Wang
Bengt Jonsson	Charles Pecheur	Farn Wang
Bernhard Josko	Wojciech Penczek	Ingo Wegener
Marcin Jurszinski	Paul Pettersson	Jon Whittle
Vineet Kahlon	Claudine Picaronny	Thomas Wilke
M. Kaltenbach	Nir Piterman	Harro Wimmel
Joost-Pieter Katoen	Shaz Qadeer	Burkhart Wolff
Felix Klaedtke	Sriram K. Rajamani	Heisung Yoo
Nils Klarlund	Kavita Ravi	Emmanuel Zarpas
Jens Knoop	S. Ray	Wenhui Zhang
Olga Kouchnarenko	E. Reeber	C. Zhou
Hillel Kugler	Iris Reuveni	Lenore Zuck

Table of Contents

Invited Talks

Software Analysis and Model Checking	1
<i>Gerard J. Holzmann</i>	
The Quest for Efficient Boolean Satisfiability Solvers	17
<i>Lintao Zhang and Sharad Malik</i>	

Invited Tutorials

On Abstraction in Software Verification	37
<i>Patrick Cousot and Radhia Cousot</i>	
The Symbolic Approach to Hybrid Systems	57
<i>Thomas A. Henzinger</i>	
Infinite Games and Verification (Extended Abstract of a Tutorial)	58
<i>Wolfgang Thomas</i>	

Symbolic Model Checking

Symbolic Localization Reduction with Reconstruction Layering and Backtracking	65
<i>Sharon Barner, Daniel Geist, and Anna Gringauze</i>	
Modeling and Verifying Systems Using a Logic of Counter Arithmetic with Lambda Expressions and Uninterpreted Functions	78
<i>Randal E. Bryant, Shuvendu K. Lahiri, and Sanjit A. Seshia</i>	
Combining Symmetry Reduction and Under-Approximation for Symbolic Model Checking	93
<i>Sharon Barner and Orna Grumberg</i>	

Abstraction/Refinement and Model Checking

Liveness with $(0, 1, \infty)$ -Counter Abstraction	107
<i>Amir Pnueli, Jessie Xu, and Lenore Zuck</i>	
Shared Memory Consistency Protocol Verification Against Weak Memory Models: Refinement via Model-Checking	123
<i>Prosenjit Chatterjee, Hemanthkumar Sivaraj, and Ganesh Gopalakrishnan</i>	
Automatic Abstraction Using Generalized Model Checking	137
<i>Patrice Godefroid and Radha Jagadeesan</i>	

Compositional/Structural Verification

Property Checking via Structural Analysis	151
<i>Jason Baumgartner, Andreas Kuehlmann, and Jacob Abraham</i>	
Conformance Checking for Models of Asynchronous Message Passing Software	166
<i>Sriram K. Rajamani and Jakob Rehof</i>	
A Modular Checker for Multithreaded Programs	180
<i>Cormac Flanagan, Shaz Qadeer, and Sanjit A. Seshia</i>	

Timing Analysis

Automatic Derivation of Timing Constraints by Failure Analysis	195
<i>Tomohiro Yoneda, Tomoya Kitai, and Chris Myers</i>	
Deciding Separation Formulas with SAT	209
<i>Ofer Strichman, Sanjit A. Seshia, and Randal E. Bryant</i>	
Probabilistic Verification of Discrete Event Systems Using Acceptance Sampling	223
<i>Håkan L. S. Younes and Reid G. Simmons</i>	

SAT Based Methods

Checking Satisfiability of First-Order Formulas by Incremental Translation to SAT	236
<i>Clark W. Barrett, David L. Dill, and Aaron Stump</i>	
Applying SAT Methods in Unbounded Symbolic Model Checking	250
<i>Ken L. McMillan</i>	
SAT Based Abstraction-Refinement Using ILP and Machine Learning Techniques	265
<i>Edmund Clarke, Anubhav Gupta, James Kukula, and Ofer Strichman</i>	
Semi-formal Bounded Model Checking	280
<i>Jesse D. Bingham and Alan J. Hu</i>	

Symbolic Model Checking

Algorithmic Verification of Invalidation-Based Protocols	295
<i>Marco Bozzano and Giorgio Delzanno</i>	
Formal Verification of Complex Out-of-Order Pipelines by Combining Model-Checking and Theorem-Proving	309
<i>Christian Jacobi</i>	

Automated Unbounded Verification of Security Protocols	324
<i>Yannick Chevalier and Laurent Vigneron</i>	

Tool Presentations

Exploiting Behavioral Hierarchy for Efficient Model Checking	338
<i>Rajeev Alur, Michael McDougall, and Zijiang Yang</i>	
IF-2.0: A Validation Environment for Component-Based Real-Time Systems	343
<i>Marius Bozga, Susanne Graf, and Laurent Mounier</i>	
The AVISS Security Protocol Analysis Tool	349
<i>Alessandro Armando, David Basin, Mehdi Bouallagui, Yannick Chevalier, Luca Compagna, Sebastian Mödersheim, Michael Rusinowitch, Mathieu Turuani, Luca Viganò, and Laurent Vigneron</i>	
SPeeDI – A Verification Tool for Polygonal Hybrid Systems	354
<i>Eugene Asarin, Gordon Pace, Gerardo Schneider, and Sergio Yovine</i>	
NuSMV 2: An OpenSource Tool for Symbolic Model Checking	359
<i>Alessandro Cimatti, Edmund Clarke, Enrico Giunchiglia, Fausto Giunchiglia, Marco Pistore, Marco Roveri, Roberto Sebastiani, and Armando Tacchella</i>	
The d/dt Tool for Verification of Hybrid Systems	365
<i>Eugene Asarin, Thao Dang, and Oded Maler</i>	

Infinite State Model Checking

Model Checking Linear Properties of Prefix-Recognizable Systems	371
<i>Orna Kupferman, Nir Piterman, and Moshe Y. Vardi</i>	
Using Canonical Representations of Solutions to Speed Up Infinite-State Model Checking	386
<i>Tatiana Rybina and Andrei Voronkov</i>	
On Discrete Modeling and Model Checking for Nonlinear Analog Systems	401
<i>Walter Hartong, Lars Hedrich, and Erich Barke</i>	

Compositional/Structural Verification

Synchronous and Bidirectional Component Interfaces	414
<i>Arindam Chakrabarti, Luca de Alfaro, Thomas A. Henzinger, and Freddy Y. C. Mang</i>	

Interface Compatibility Checking for Software Modules	428
<i>Arindam Chakrabarti, Luca de Alfaro, Thomas A. Henzinger,</i> <i>Marcin Jurdziński, and Freddy Y.C. Mang</i>	
Practical Methods for Proving Program Termination	442
<i>Michael A. Colón and Henny B. Sipma</i>	

Extended Model Checking

Evidence-Based Model Checking	455
<i>Li Tan and Rance Cleaveland</i>	
Mixing Forward and Backward Traversals in Guided-Prioritized BDD-Based Verification	471
<i>Gianpiero Cabodi, Sergio Nocco, and Stefano Quer</i>	
Vacuum Cleaning CTL Formulae	485
<i>Mitra Purandare and Fabio Somenzi</i>	

Tool Presentations

CVC: A Cooperating Validity Checker	500
<i>Aaron Stump, Clark W. Barrett, and David L. Dill</i>	
χ Chek: A Multi-valued Model-Checker	505
<i>Marsha Chechik, Arie Gurfinkel, and Benet Devereux</i>	
PathFinder: A Tool for Design Exploration	510
<i>Shoham Ben-David, Anna Gringauze, Baruch Sterin,</i> <i>and Yaron Wolfsthal</i>	
Abstracting C with abC	515
<i>Dennis Dams, William Hesse, and Gerard Holzmann</i>	
AMC: An Adaptive Model Checker	521
<i>Alex Groce, Doron Peled, and Mihalis Yannakakis</i>	

Code Verification

Temporal-Safety Proofs for Systems Code	526
<i>Thomas A. Henzinger, Ranjit Jhala, Rupak Majumdar,</i> <i>George C. Necula, Grégoire Sutre, and Westley Weimer</i>	

Regular Model Checking and Acceleration

Extrapolating Tree Transformations	539
<i>Ahmed Bouajjani and Tayssir Touili</i>	

Regular Tree Model Checking	555
<i>Parosh Aziz Abdulla, Bengt Jonsson, Pritha Mahata, and Julien d’Orso</i>	

Compressing Transitions for Model Checking	569
<i>Robert Kurshan, Vladimir Levin, and Hüsni Yenigün</i>	

Model Reduction

Canonical Prefixes of Petri Net Unfoldings	582
<i>Victor Khomenko, Maciej Koutny, and Walter Vogler</i>	

State Space Reduction by Proving Confluence	596
<i>Stefan Blom and Jaco van de Pol</i>	

Fair Simulation Minimization	610
<i>Sankar Gurumurthy, Roderick Bloem, and Fabio Somenzi</i>	

Author Index	625
---------------------------	-----