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

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

http://www.springer.de

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:

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

Steering Committee

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

Local Organizer

Jens Christian Godskesen (IT-U of Copenhagen)

Sponsors

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

Referees

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

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

Table of Contents

Compositional/Structural Verification

Timing Analysis

SAT Based Methods

Symbolic Model Checking

Tool Presentations

Infinite State Model Checking

Compositional/Structural Verification

Extended Model Checking

Tool Presentations

Code Verification

Regular Model Checking and Acceleration

Model Reduction