Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Tokyo
Computer Aided Verification

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

- 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 (FLoC2002), 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  Xioaquin Du
Kamel Barkaoui  Patricia Bouyer  M. Duflot
Sharon Barner  Marius Bozga  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 Herbreuteau
Holger Hermanns
Gerard Holzmann
Hardi Hungar
Radu Iosif
S. Iyer
Damir Jamsek
Somesh Jha
Ranjit Jhala
Hoon Sang 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
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

Invited Talks

Software Analysis and Model Checking .................................1
Gerard J. Holzmann

The Quest for Efficient Boolean Satisfiability Solvers ...............17
Lintao Zhang and Sharad Malik

Invited Tutorials

On Abstraction in Software Verification .................................37
Patrick Cousot and Radhia Cousot

The Symbolic Approach to Hybrid Systems ..............................57
Thomas A. Henzinger

Infinite Games and Verification (Extended Abstract of a Tutorial) ....58
Wolfgang Thomas

Symbolic Model Checking

Symbolic Localization Reduction with Reconstruction Layering and Backtracking .........................65
Sharon Barner, Daniel Geist, and Anna Gringauze

Modeling and Verifying Systems Using a Logic of Counter Arithmetic with Lambda Expressions and Uninterpreted Functions ...............78
Randal E. Bryant, Shuvendu K. Lahiri, and Sanjit A. Seshia

Combining Symmetry Reduction and Under-Approximation for Symbolic Model Checking .........................93
Sharon Barner and Orna Grumberg

Abstraction/Refinement and Model Checking

Liveness with (0, 1, ∞)-Counter Abstraction ............................107
Amir Pnueli, Jessie Xu, and Lenore Zuck

Shared Memory Consistency Protocol Verification Against Weak Memory Models: Refinement via Model-Checking ..........123
Prosenjit Chatterjee, Hemanthkumar Sivaraj, and Ganesh Gopalakrishnan

Automatic Abstraction Using Generalized Model Checking ............137
Patrice Godefroid and Radha Jagadeesan
Compositional/Structural Verification

Property Checking via Structural Analysis .................................151
Jason Baumgartner, Andreas Kuehlmann, and Jacob Abraham

Conformance Checking for Models of Asynchronous Message Passing Software ........................................ 166
Sriram K. Rajamani and Jakob Rehof

A Modular Checker for Multithreaded Programs ...........................180
Cormac Flanagan, Shaz Qadeer, and Sanjit A. Seshia

Timing Analysis

Automatic Derivation of Timing Constraints by Failure Analysis ..........195
Tomohiro Yoneda, Tomoya Kitai, and Chris Myers

Deciding Separation Formulas with SAT .....................................209
Ofer Strichman, Sanjit A. Seshia, and Randal E. Bryant

Probabilistic Verification of Discrete Event Systems Using Acceptance Sampling ..................................223
Håkan L. S. Younes and Reid G. Simmons

SAT Based Methods

Checking Satisfiability of First-Order Formulas by Incremental Translation to SAT ........................................ 236
Clark W. Barrett, David L. Dill, and Aaron Stump

Applying SAT Methods in Unbounded Symbolic Model Checking ........250
Ken L. McMillan

SAT Based Abstraction-Refinement Using ILP and Machine Learning Techniques .......................................265
Edmund Clarke, Anubhav Gupta, James Kukula, and Ofer Strichman

Semi-formal Bounded Model Checking ....................................280
Jesse D. Bingham and Alan J. Hu

Symbolic Model Checking

Algorithmic Verification of Invalidation-Based Protocols .............. 295
Marco Bozzano and Giorgio Delzanno

Formal Verification of Complex Out-of-Order Pipelines by Combining Model-Checking and Theorem-Proving ........................................ 309
Christian Jacobi
Automated Unbounded Verification of Security Protocols ................. 324
Yannick Chevalier and Laurent Vigneron

Tool Presentations

Exploiting Behavioral Hierarchy for Efficient Model Checking ............. 338
Rajeev Alur, Michael McDougall, and Zijiang Yang

IF-2.0: A Validation Environment
for Component-Based Real-Time Systems ................................. 343
Marius Bozga, Susanne Graf, and Laurent Mounier

The AVISS Security Protocol Analysis Tool .............................. 349
Alessandro Armando, David Basin, Mehdi Bouallagui, Yannick Chevalier,
Luca Compagna, Sebastian Mödersheim, Michael Rusinowitch,
Mathieu Turuani, Luca Viganò, and Laurent Vigneron

SPeeDI – A Verification Tool for Polygonal Hybrid Systems ............... 354
Eugene Asarin, Gordon Pace, Gerardo Schneider, and Sergio Yovine

NuSMV 2: An OpenSource Tool for Symbolic Model Checking .............. 359
Alessandro Cimatti, Edmund Clarke, Enrico Giunchiglia,
Fausto Giunchiglia, Marco Pistore, Marco Roveri, Roberto Sebastiani,
and Armando Tacchella

The d/dt Tool for Verification of Hybrid Systems ....................... 365
Eugene Asarin, Thao Dang, and Oded Maler

Infinite State Model Checking

Model Checking Linear Properties of Prefix-Recognizable Systems ....... 371
Orna Kupferman, Nir Piterman, and Moshe Y. Vardi

Using Canonical Representations of Solutions
to Speed Up Infinite-State Model Checking ............................. 386
Tatiana Rybina and Andrei Voronkov

On Discrete Modeling and Model Checking
for Nonlinear Analog Systems ........................................... 401
Walter Hartong, Lars Hedrich, and Erich Barke

Compositional/Structural Verification

Synchronous and Bidirectional Component Interfaces ..................... 414
Arindam Chakrabarti, Luca de Alfaro, Thomas A. Henzinger,
and Freddy Y. C. Mang
Interface Compatibility Checking for Software Modules ............... 428
Arindam Chakrabarti, Luca de Alfaro, Thomas A. Henzinger,
Marcin Jurdziński, and Freddy Y.C. Mang

Practical Methods for Proving Program Termination ................. 442
Michael A. Colón and Henny B. Sipma

Extended Model Checking

Evidence-Based Model Checking ........................................... 455
Li Tan and Rance Cleaveland

Mixing Forward and Backward Traversals
in Guided-Prioritized BDD-Based Verification ......................... 471
Gianpiero Cabodi, Sergio Nocco, and Stefano Quer

Vacuum Cleaning CTL Formulae ....................................... 485
Mitra Purandare and Fabio Somenzi

Tool Presentations

CVC: A Cooperating Validity Checker ................................. 500
Aaron Stump, Clark W. Barrett, and David L. Dill

χChek: A Multi-valued Model-Checker .................................. 505
Marsha Chechik, Arie Gurfinkel, and Benet Devereux

PathFinder: A Tool for Design Exploration ............................... 510
Shoham Ben-David, Anna Gringauze, Baruch Sterin,
and Yaron Wolfsthal

Abstracting C with abC .................................................. 515
Dennis Dams, William Hesse, and Gerard Holzmann

AMC: An Adaptive Model Checker .................................... 521
Alex Groce, Doron Peled, and Mihalis Yannakakis

Code Verification

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

Regular Model Checking and Acceleration

Extrapolating Tree Transformations .................................. 539
Ahmed Bouajjani and Tayssir Touili
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regular Tree Model Checking</td>
<td>555</td>
</tr>
<tr>
<td><em>Parosh Aziz Abdulla, Bengt Jonsson, Pritha Mahata, and Julien d'Orso</em></td>
<td></td>
</tr>
<tr>
<td>Compressing Transitions for Model Checking</td>
<td>569</td>
</tr>
<tr>
<td><em>Robert Kurshan, Vladimír Levin, and Hüsnü Yenigün</em></td>
<td></td>
</tr>
<tr>
<td><strong>Model Reduction</strong></td>
<td></td>
</tr>
<tr>
<td>Canonical Prefixes of Petri Net Unfoldings</td>
<td>582</td>
</tr>
<tr>
<td><em>Victor Khomenko, Maciej Koutny, and Walter Vogler</em></td>
<td></td>
</tr>
<tr>
<td>State Space Reduction by Proving Confluence</td>
<td>596</td>
</tr>
<tr>
<td><em>Stefan Blom and Jaco van de Pol</em></td>
<td></td>
</tr>
<tr>
<td>Fair Simulation Minimization</td>
<td>610</td>
</tr>
<tr>
<td><em>Sankar Gurumurthy, Roderick Bloem, and Fabio Somenzi</em></td>
<td></td>
</tr>
<tr>
<td><strong>Author Index</strong></td>
<td>625</td>
</tr>
</tbody>
</table>