

Alan J. Hu Moshe Y. Vardi (Eds.)

Computer Aided Verification

10th International Conference, CAV'98
Vancouver, BC, Canada, June 28 – July 2, 1998
Proceedings



Springer

Series Editors

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

Volume Editors

Alan J. Hu
The University of British Columbia, Department of Computer Science
2366 Main Hall, Vancouver, BC, V6T 1Z4, Canada
E-mail: ajh@cs.ubc.ca

Moshe Y. Vardi
Rice University, Department of Computer Science
P.O. Box 1892, Houston, TX 77251-1892, USA
E-mail: vardi@cs.rice.edu

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Computer aided verification : 10th international conference ;
proceedings / CAV '98, Vancouver, BC, Canada, June 28 - July 2,
1998. Alan J. Hu ; Moshe Y. Vardi (ed.). - Berlin ; Heidelberg ; New
York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ;
Santa Clara ; Singapore ; Tokyo : Springer, 1998
(Lecture notes in computer science ; Vol. 1427)
ISBN 3-540-64608-6

CR Subject Classification (1991): F3, D.2.4, D.2.2, F4.1, B.7.2, C.3, I.2.3

ISSN 0302-9743

ISBN 3-540-64608-6 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 1998
Printed in Germany

Typesetting: Camera-ready by author
SPIN 10637540 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

Preface

This volume contains the proceedings of the Tenth International Conference on Computer-Aided Verification (CAV'98), held June 28 – July 2 at the University of British Columbia. The CAV conferences are 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 and has traditionally drawn contributions from both researchers and practitioners in both academia and industry. This year is no exception. We accepted 33 research papers out of 98 submissions and 10 short tool papers out of 19 submissions. Rounding out the program are a set of invited papers.

Given the practical and industrial aspects of CAV, we are very proud of the support we receive from industry. We would like to thank the following generous and forward-looking companies for their sponsorship of CAV'98:

Cadence Design Systems	NEC USA
Chrysalis Symbolic Design	Prover Technology (Logikkonsult)
Dassault Aviation	Rockwell Collins
Fujitsu Ltd.	SGS-Thomson Microelectronics
Hewlett-Packard	Siemens
IBM Research	Sun Microsystems
Intel	Synopsys
Lucent Technologies	Verisity
Mentor Graphics	Verysys
Motorola	

The conference program was selected by the program committee: Martin Abadi (DEC SRC, USA), Rajeev Alur (Univ. of Pennsylvania, USA), Ahmed Bouajjani (VERIMAG, France), Jerry Burch (Cadence Labs, USA), Olivier Coudert (Synopsys, USA), Werner Damm (Oldenburg University, Germany), David Dill (Stanford University, USA), Limor Fix (Intel, Israel), Patrice Godefroid (Bell Labs, USA), Mike Gordon (Cambridge University, Great Britain), Orna Grumberg (The Technion, Israel), Alan Hu, co-chair (Univ. of British Columbia, Canada), Daniel Jackson (MIT, USA), Bengt Jonsson (Uppsala University, Sweden), Kim Larsen (Aalborg University, Denmark), Ken McMillan (Cadence Labs, USA), Doron Peled (Bell Labs, USA), Carl Pixley (Motorola, USA), Amir Pnueli (Weizmann Institute, Israel), Carl Seger (Intel, USA), Natarajan Shankar (SRI International, USA), Joseph Sifakis (VERIMAG, France), Prasad Sistla (Univ. of Illinois, Chicago, USA), Fabio Somenzi (Univ. of Colorado, Boulder, USA), Moshe Vardi, co-chair (Rice University, USA), and Yaron Wolfsthal (IBM, Israel).

The following additional reviewers also helped in the evaluation of submitted papers: Parosh Abdulla, Roy Armoni, Tamarah Arons, Eugene Asarin,

Andrea Asperti, Adnan Aziz, Clark Barrett, Ilan Beer, Shoham Ben-David, Sergey Berezin, Roderick Bloem, Juergen Bohn, Bernard Boigelot, Dragan Bosjatski, Olivier Bournez, Alex Brodsky, Stephen Brookes, Glenn Bruns, Paul Caspi, Judy Crow, David Cyrluk, Mads Dam, Dennis Dams, Juergen Dingel, Cindy Eisner, Henrik Ejersbo Jensen, Amy Felty, Martin Fraenzle, Ranan Fraer, Danny Geist, Boris Ginsburg, Leonid Glukhovski, Susanne Graf, Efim Gukovsky, Viktor Gyuris, Gary Hachtel, Alan Hartman, Henrik Huldgaard, Hardi Hungar, Norris Ip, Amitai Irron, Radhakrishnan Jagadeesan, Jae-Young Jang, Somesh Jha, Bernhard Josko, Gila Kamhi, Sagi Katz, Shmuel Katz, Yonit Kesten, Kaare Kristoffersen, Andreas Kuehlmann, Orna Kupferman, Yassine Lakhnech, Avner Landver, Karen Laster, Jorn Lind-Nielsen, Sela Mador-Haim, Bozga Maler, Monica Marcus, Will Marrero, Stephan Melzer, Stephan Merz, Kim Milvang-Jensen, Marius Minea, Faron Moller, In-Ho Moon, Laurent Mounier, David Notkin, Sam Owre, Paul Pettersson, Sriram Rajamony, Rajeev Ranjan, Kavita Ravi, Michel Raynal, Yoav Rodeh, Roni Rosner, Sitvanit Ruah, John Rushby, Mark Sauer, Elad Shahar, Dafna Sheinwald, Tom Shiple, Ze'ev Shtadler, Ofer Shtrichman, Michael Siegel, Vigyan Singhal, Gal Siton, Jens Skakkebaek, Arne Skou, Mandayam Srivas, Martin Steffen, Ulrich Stern, Jeffrey Su, Serdar Tasiran, Gadi Taubenfeld, Stavros Tripakis, Shmuel Ur, Koen van Eijk, Carsten Weise, Derek Williams, Gunnar Wittich, Pierre Wolper, Howard Wong-Toi, Han Yang, Wang Yi, Sergio Yovine. We would like to thank all of the reviewers for their time and expertise.

The steering committee consists of the founders of the conference: Edmund Clarke (Carnegie Mellon University, USA), Robert Kurshan (Bell Labs, USA), Amir Pnueli (Weizmann Institute, Israel), and Joseph Sifakis (VERIMAG, France). We thank them and last year's conference chair Orna Grumberg (Technion, Israel) for their helpful advice.

Finally, on the logistical side, the conference was held at UBC with the co-operation of the Computer Science Department and the Center for Integrated Computer Systems Research (CICSR). We thank CICSR Director Rabab Ward for sanctioning UBC's hosting of the conference. Computing Facilities Manager John Demco orchestrated computer access for the conference. The UBC Conference Center staff Melanie Kelleher, Brenda Kiernan, and Karen Read were invaluable in planning local arrangements. Holly Mitchell provided indispensable secretarial support. We thank them for their time and energy.

Vancouver, British Columbia
Houston, Texas

Alan J. Hu
Moshe Y. Vardi

April 1998

Table of Contents

Invited Papers

Synchronous Programming of Reactive Systems	
<i>N. Halbwachs</i>	1
Ten Years of Partial Order Reduction	
<i>D. Peled</i>	17
An ACL2 Proof of Write Invalidate Cache Coherence	
<i>J. S. Moore</i>	29
Transforming the Theorem Prover into a Digital Design Tool: From Concept Car to Off-Road Vehicle	
<i>D. Hardin, M. Wilding, D. Greve</i>	39
A Role for Theorem Proving in Multi-Processor Design	
<i>A. J. Camilleri</i>	45
A Formal Method Experience at Secure Computing Corporation	
<i>J. Hoffman, C. Payne</i>	49
Formal Methods in an Industrial Environment	
<i>J. R. Cuéllar</i>	57
On Checking Model Checkers	
<i>G. J. Holzmann</i>	61
Finite-State Analysis of Security Protocols	
<i>J. C. Mitchell</i>	71
Integrating Proof-Based and Model-Checking Techniques for the Formal Verification of Cryptographic Protocols	
<i>D. Bolognani</i>	77
Verifying Systems with Infinite but Regular State Spaces	
<i>P. Wolper, B. Boigelot</i>	88

Regular Papers

Formal Verification of Out-of-Order Execution Using Incremental Flushing	
<i>J. U. Skakkebæk, R. B. Jones, D. L. Dill</i>	98
Verification of an Implementation of Tomasulo's Algorithm by Compositional Model Checking	
<i>K. L. McMillan</i>	110
Decomposing the Proof of Correctness of Pipelined Microprocessors	
<i>R. Hosabettu, M. Srivas, G. Gopalakrishnan</i>	122
Processor Verification with Precise Exceptions and Speculative Execution	
<i>J. Sawada, W. A. Hunt, Jr.</i>	135
Symmetry Reductions in Model Checking	
<i>E. M. Clarke, E. A. Emerson, S. Jha, A. P. Sistla</i>	147

Structural Symmetry and Model Checking	
<i>G. S. Manku, R. Hojati, R. Brayton</i>	159
Using Magnetic Disk Instead of Main Memory in the Mur ϕ Verifier	
<i>U. Stern, D. L. Dill</i>	172
On-the-Fly Model Checking of RCTL Formulas	
<i>I. Beer, S. Ben-David, A. Landver</i>	184
From Pre-historic to Post-modern Symbolic Model Checking	
<i>T. A. Henzinger, O. Kupferman, S. Qadeer</i>	195
Model Checking LTL Using Net Unfoldings	
<i>F. Wallner</i>	207
Model Checking for a First-Order Temporal Logic Using Multiway Decision Graphs	
<i>Y. Xu, E. Cerny, X. Song, F. Corella, O. Aït Mohamed</i>	219
On the Limitations of Ordered Representations of Functions	
<i>J. S. Thathachar</i>	232
BDD Based Procedures for a Theory of Equality with Uninterpreted Functions	
<i>A. Goel, K. Sajid, H. Zhou, A. Aziz, V. Singhal</i>	244
Computing Reachable Control States of Systems Modeled with Uninterpreted Functions and Infinite Memory	
<i>A. J. Isles, R. Hojati, R. K. Brayton</i>	256
Multiple Counters Automata, Safety Analysis, and Presburger Arithmetic	
<i>H. Comon, Y. Jurski</i>	268
A Comparison of Presburger Engines for EFSM Reachability	
<i>T. R. Shiple, J. H. Kukula, R. K. Ranjan</i>	280
Generating Finite-State Abstractions of Reactive Systems Using Decision Procedures	
<i>M. A. Colón, T. E. Uribe</i>	293
On-the-Fly Analysis of Systems with Unbounded, Lossy FIFO Channels	
<i>P. A. Abdulla, A. Bouajjani, B. Jonsson</i>	305
Computing Abstractions of Infinite State Systems Compositionally and Automatically	
<i>S. Bensalem, Y. Lakhnech, S. Owre</i>	319
Normed Simulations	
<i>D. Griffioen, F. Vaandrager</i>	332
An Experiment in Parallelizing an Application Using Formal Methods	
<i>R. Couturier, D. Méry</i>	345
Efficient Symbolic Detection of Global Properties in Distributed Systems	
<i>S. D. Stoller, Y. A. Liu</i>	357
A Machine-Checked Proof of the Optimality of a Real-Time Scheduling Policy	
<i>M. Wilding</i>	369
A General Approach to Partial Order Reductions in Symbolic Verification	
<i>P. A. Abdulla, B. Jonsson, M. Kindahl, D. Peled</i>	379
Correctness of the Concurrent Approach to Symbolic Verification of Interleaved Models	
<i>F. Balarin</i>	391

Verification of Timed Systems Using POSETs	
<i>W. Belluomini, C. J. Myers</i>	403
Mechanising BAN Kerberos by the Inductive Method	
<i>G. Bella, L. C. Paulson</i>	416
Protocol Verification in Nuprl	
<i>A. P. Felty, D. J. Howe, F. A. Stomp</i>	428
You Assume, We Guarantee: Methodology and Case Studies	
<i>T. A. Henzinger, S. Qadeer, S. K. Rajamani</i>	440
Verification of a Parameterized Bus Arbitration Protocol	
<i>E. A. Emerson, K. S. Namjoshi</i>	452
The ‘Test Model-Checking’ Approach to the Verification of Formal Memory Models of Multiprocessors	
<i>R. Nalumasu, R. Ghughal, A. Mokkedem, G. Gopalakrishnan</i>	464
Design Constraints in Symbolic Model Checking	
<i>M. Kaufmann, A. Martin, C. Pixley</i>	477
Verification of Floating-Point Adders	
<i>Y.-A. Chen, R. E. Bryant</i>	488

Tool Papers

Xeve: An Esterel Verification Environment	
<i>A. Bouali</i>	500
InVeSt: A Tool for the Verification of Invariants	
<i>S. Bensalem, Y. Lakhnech, S. Owre</i>	505
Verifying Mobile Processes in the HAL Environment	
<i>G. Ferrari, S. Gnesi, U. Montanari, M. Pistore, G. Ristori</i>	511
Mona 1.x: New Techniques for WS1S and WS2S	
<i>J. Elgaard, N. Klarlund, A. Møller</i>	516
MOCHA: Modularity in Model Checking	
<i>R. Alur, T. A. Henzinger, F. Y. C. Mang, S. Qadeer, S. K. Rajamani, S. Tasiran</i>	521
SCR*: A Toolset for Specifying and Analyzing Software Requirements	
<i>C. Heitmeyer, J. Kirby, B. Labaw, R. Bharadwaj</i>	526
A Toolset for Message Sequence Charts	
<i>D. A. Peled</i>	532
Real-Time Verification of Statemate Designs	
<i>U. Brockmeyer, G. Wittich</i>	537
Optikron: A Tool Suite for Enhancing Model-Checking of Real-Time Systems	
<i>C. Daws</i>	542
Kronos: A Model-Checking Tool for Real-Time Systems	
<i>M. Bozga, C. Daws, O. Maler, A. Olivero, S. Tripakis, S. Yovine</i>	546
Author Index	551