

Lecture Notes in Computer Science

663

Edited by G. Goos and J. Hartmanis

Advisory Board: W. Brauer D. Gries J. Stoer



G. v. Bochmann D. K. Probst (Eds.)

Computer Aided Verification

Fourth International Workshop, CAV '92
Montreal, Canada, June 29 - July 1, 1992
Proceedings

Springer-Verlag

Berlin Heidelberg New York

London Paris Tokyo

Hong Kong Barcelona

Budapest

Series Editors

Gerhard Goos
Universität Karlsruhe
Postfach 69 80
Vincenz-Priessnitz-Straße 1
W-7500 Karlsruhe, FRG

Juris Hartmanis
Cornell University
Department of Computer Science
4130 Upson Hall
Ithaca, NY 14853, USA

Volume Editors

Gregor von Bochmann
Département d'IRO, Université de Montréal
P. O. Box 6128, Station A, Montréal, Québec, H3C 3J7, Canada

David Karl Probst
Department of Computer Science, Concordia University
1455 de Maisonneuve West, Montréal, Québec, H3G 1M8, Canada

CR Subject Classification (1991): F.3, D.2.4, B.7, C.2.2

ISBN 3-540-56496-9 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-56496-9 Springer-Verlag New York Berlin Heidelberg

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 1993
Printed in Germany

Typesetting: Camera ready by author/editor
45/3140-543210 - Printed on acid-free paper

Preface

This is the Proceedings of the Fourth Workshop on Computer-Aided Verification (CAV '92), held in Montreal, June 29 - July 1, 1992. The objective of this series of workshops is to bring together researchers and practitioners interested in the development and use of methods, tools and theories for the computer-aided verification of concurrent systems. The workshops provide an opportunity for comparing various verification methods and practical tools that can be used to assist the applications designer. Emphasis is placed on new research results and the application of existing results to real verification problems.

Of the 75 papers that were submitted, 31 were accepted for presentation. Leslie Lamport gave the invited talk on hierarchical structure in proofs. Amir Pnueli was the banquet speaker. There were sessions devoted to Reduction Techniques, Proof Checking, Symbolic Verification, Timing Verification, Partial-Order Approaches, Case Studies, Model and Proof Checking, and Other Approaches.

Financial support was provided by Concordia University, Computer Research Institute of Montreal (CRIM), Bell Northern Research (BNR), the IDACOM-NSERC-CWARC Industrial Research Chair on Communication Protocols, the Institut National de la Recherche Scientifique (INRS-Telecommunications), the Natural Sciences and Engineering Research Council of Canada (NSERC), and the University of Montreal.

The Program Committee reviewed, managed other reviewers, and helped in the establishment of the program. The Steering Committee, consisting of E.M. Clarke (Carnegie Mellon University), R.P. Kurshan (AT&T Bell Laboratories), A. Pnueli (Weizmann Institute), and J. Sifakis (LGI-IMAG), reviewed and offered council at appropriate moments. This year, the Program Committee members were: R. Alur (AT&T Bell Labs), R. Brayton (UC Berkeley), E. Brinksma (U. Twente), E. Cerny (U. Montreal), C. Courcoubetis (U. Crete), R. de Simone (INRIA), D. Dill (Stanford U.), A. Emerson (UT Austin), O. Grumberg (Technion), H. Hiraishi (Kyoto Sangyo U.), G. Holzmann (AT&T Bell Labs), W.A. Hunt Jr. (CLI), K. Larsen (Aalborg U.), P. Loewenstein (Sun), A. Mazurkiewicz (Polish Acad. Sci.), L. Paulson (Cambridge U.), D.K. Probst (Concordia U.), B. Steffen (TU Aachen), D. Taubner (sd&m GmbH) and P. Wolper (U. Liege). The names of additional reviewers are listed on the following page.

Gregor v. Bochmann was General and Program Chair. David K. Probst was Local Arrangements Chair and much more. Lucie Levesque was Registration Chair and resource person. Anindya Das was Treasurer. Stan Swiercz and Daniel Ouimet provided technical support for tool demonstrations. Most of the articles in this volume were typeset using the \LaTeX document preparation system and Springer-Verlag's LNCS style file, slightly modified.

Additional Reviewers

P. Attie (UT Austin), A. Aziz (UC Berkeley), W. Baker (UC Berkeley), F. Balarin (UC Berkeley), D. Barnard (TU Munich), H. Baumer (U Twente), R. Bayardo (UT Austin), O. Bernholtz (Technion), A. Borjesson (Aalborg U), B. Botma (U Twente), A. Bouajjani (LGI-IMAG), A. Bouali (INRIA), G. Boudol (INRIA), O. Burkart (RWTH Aachen), I. Castellani (INRIA), A. Claen (RWTH Aachen), H. Eertink (U Twente), P. Eijk (U Twente), U. Engberg (Aarhus U), T. Filkorn (Siemens), N. Francez (Technion), M. Fujita (Fujitsu), H. Garavel (Verilog), P. Godefroid (U Liege), C. Godskesen (Aalborg U), M. Gordon (Cambridge), S. Graf (LGI-IMAG), P. Gutwin (UC Berkeley), N. Halbwachs (LGI-IMAG), K. Hamaguchi (Kyoto U), T. Henzinger (Cornell U), R. Hojati (UC Berkeley), A. Hu (Stanford U), H. Huttel (Aalborg U), C. Jard (IRISA), T. Jeron (Alcatel), C. Jutla (IBM), M. Kaltenbach (UT Austin), T. Kam (UC Berkeley), P. Kars (U Twente), S. Katz (Technion), S. Kimura (Kobe U), A. Kindler (RWTH Aachen), M. Klein (RWTH Aachen), J. Knoop (Kiel), S. Krishnan (UC Berkeley), W. Lam (UC Berkeley), R. Langerak (U Twente), L. Lavagno (UC Berkeley), C. Loiseaux (LGI-IMAG), A. Mader (TU Munich), J. Makowsky (Technion), A. Mendelson (Technion), F. Mignard (INRIA), C. Moon (UC Berkeley), D. Ouimet (U Montreal), R. Rajaraman (UT Austin), C. Ratel (LGI-IMAG), D. Russinoff (CLI), S. Sagiv (Haifa), A. Scholz (Siemens), M. Sekine (UC Berkeley), N. Shankar (SRI), T. Shiple (UC Berkeley), M. Sinderen (U Twente), A. Skou (Aalborg U), P. Stephan (UC Berkeley), J. Tretmans (U Twente), F. Vaandrager (INRIA), J. Vaucher (U Montreal), T. Villa (UC Berkeley), H. Wang (UC Berkeley), C. Weise (RWTH Aachen), G. Whitcomb (UC Berkeley), H. Wong-Toi (Stanford U), W. Yi (Aalborg U), M. Yoeli (Technion), G. York (UC Berkeley), S. Yovine (LGI-IMAG).

Table of Contents

Invited Lecture:

Computer-Hindered Verification (Humans Can Do It Too) <i>Leslie Lamport (DEC SRC)</i>	1
--	---

Session: Reduction Techniques I

Modular Abstractions for Verifying Real-Time Distributed Systems <i>Hana De-Leon and Orna Grumberg (Technion)</i>	2
Layering Techniques for Development of Parallel Systems <i>Mannes Poel and Job Zwiers (U. Twente)</i>	16
Efficient Local Correctness Checking <i>Kim Larsen (Aalborg U.)</i>	30

Session: Proof Checking

Mechanical Verification of Concurrent Systems with TLA <i>Urban Engberg (Aarhus U.), Peter Grønning (TU Denmark) and Leslie Lamport (DEC SRC)</i>	44
Using a Theorem Prover for Reasoning about Concurrent Algorithms <i>Joakim von Wright and Thomas Långbacka (Åbo Akademi U.)</i>	56
Verifying a Logic Synthesis Tool in Nuprl: A Case Study in Software Verification <i>Mark Aagaard and Miriam Leeser (Cornell U.)</i>	69

Session: Symbolic Verification I

Higher-Level Specification and Verification with BDDs <i>Alan Hu, David Dill, Andreas Drezler and Han Yang (Stanford U.)</i>	82
Symbolic Bisimulation Minimisation <i>Amar Bouali (ENSMP) and Robert de Simone (INRIA)</i>	96
Towards a Verification Technique for Large Synchronous Circuits <i>Prabhat Jain, Prabhakar Kudva and Ganesh Gopalakrishnan (U. Utah)</i>	109

Session: Timing Verification I

Verifying Timed Behavior Automata with Nonbinary Delay Constraints <i>David Probst and Hon Li (Concordia U.)</i>	123
Timing Verification by Successive Approximation <i>Rajeev Alur, Alon Itai, Robert Kurshan and Mihalis Yannakakis (AT&T Bell Labs)</i>	137
A Verification Strategy for Timing-Constrained Systems <i>Felice Balarin and Alberto Sangiovanni-Vincentelli (UC Berkeley)</i>	151

Session: Partial-Order Approaches

- Using Unfoldings to Avoid the State Explosion Problem in the Verification of Asynchronous Circuits
Kenneth McMillan (Carnegie Mellon U.)..... 164
- State-Space Caching Revisited
Patrice Godefroid (U. Liège), Gerard Holzmann (AT&T Bell Labs) and Didier Pirottin (U. Liège)..... 178

Session: Case Studies

- Verification in Process Algebra of the Distributed Control of Track Vehicles - A Case Study (Extended Abstract)
Siegfried Fischer, Andreas Scholz and Dirk Taubner (Siemens AG)..... 192
- Design Verification of a Microprocessor Using Branching Time Regular Temporal Logic
Kiyoharu Hamaguchi (Kyoto U.), Hiromi Hiraishi (Kyoto Sangyo U.) and Shuzo Yajima (Kyoto U.)..... 206
- A Case Study in Safety-Critical Design
Glenn Bruns (U. Edinburgh)..... 220

Session: Reduction Techniques II

- Automatic Reduction in CTL Compositional Model Checking
Thomas Shiple (UC Berkeley), Massimiliano Chiodo (Magnetis Marelli), Alberto Sangiovanni-Vincentelli and Robert Brayton (UC Berkeley)..... 234
- Compositional Model Checking for Linear-Time Temporal Logic
Roope Kaivola (U. Helsinki)..... 248
- Property Preserving Simulations
Saddek Bensalem, Ahmed Bouajjani, Claire Loiseaux and Joseph Sifakis (IMAG-LGI)..... 260

Session: Timing Verification II

- Verification with Real-Time COSPAN
Costas Courcoubetis (U. Crete), David Dill (Stanford U.), Magda Chatzaki and Panagiotis Tzounakis (U. Crete)..... 274
- Model-Checking for Real-Time Systems Specified in Lotos
Nathalie Rico, Gregor von Bochmann (U. Montreal) and Omar Cherkaoui (UQAM)..... 288
- Decidability of Bisimulation Equivalences for Parallel Timer Processes
Kārlis Čerāns (U. Latvia)..... 302

Session: Model and Proof Checking

A Proof Assistant for Symbolic Model-Checking

Julian Bradfield (U. Edinburgh) 316

Tableau Recycling

Angelika Mader (TU Munich) 330

CrocOS: An Integrated Environment for Interactive Verification of SDL Specifications

Dominique Méry and Abdelillah Mokkedem (CRIN and INRIA) 343**Session: Other Approaches**

Verifying General Safety and Liveness Properties with Integer Programming

James Corbett (U. Massachusetts) 357

Generating Diagnostic Information for Behavioral Preorders

Ufuk Celikkan and Rance Cleaveland (North Carolina State U.) 370

A Verification Procedure via Invariant for Extended Communicating Finite-State Machines

Masahiro Higuchi, Osamu Shirakawa, Hiroyuki Seki, Mamoru Fujii (Osaka U.) and Tadao Kasami (AIST, Nara) 384**Session: Symbolic Verification II**Efficient ω -Regular Language Containment*Ramin Hojati (UC Berkeley), Hervé Touati (DEC PRL), Robert Kurshan (AT&T Bell Labs) and Robert Brayton (UC Berkeley)* 396

Faster Model Checking for the Modal Mu-Calculus

Rance Cleaveland (North Carolina State U.), Marion Klein and Bernhard Steffen (RWTH Aachen) 410