

Lecture Notes in Computer Science

1522

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

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Singapore

Tokyo

Ganesh Gopalakrishnan Phillip Windley (Eds.)

Formal Methods in Computer-Aided Design

Second International Conference, FMCAD '98
Palo Alto, CA, USA, November 4-6, 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

Ganesh Gopalakrishnan
University of Utah, Department of Computer Science
50 S Central Campus, Salt Lake City, UT 84112-9205, USA
E-mail: ganesh@cs.utah.edu

Phillip Windley
Brigham Young University, Department of Computer Science
3361 TMCB, Provo, UT 84602-6576, USA
E-mail: windley@cs.byu.edu

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Formal methods in computer-aided design : second international conference ; proceedings / FMCAD '98, Palo Alto, CA, USA, November 4 - 6, 1998. Ganesh Gopalakrishnan ; Philip Windley (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 1998 (Lecture notes in computer science ; Vol. 1522)
ISBN 3-540-65191-8

CR Subject Classification (1998): B.1.2, B.1.4, B.2.2-3, B.6.2-3, B.7.2-3, F.3.1, F.4.1, I.2.3, D.2.4, J.6

ISSN 0302-9743

ISBN 3-540-65191-8 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 1998
Printed in Germany

Typesetting: Camera-ready by author
SPIN 10692817 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

Preface

This volume contains the proceedings of the Second International Conference on *Formal Methods in Computer-Aided Design (FMCAD'98)*, organized November 4-6, in Palo Alto, California, USA. The first event of this series was organized by Mandayam Srivas and Albert Camilleri in 1996 in Palo Alto. FMCAD, which evolved from the series *Theorem Provers in Circuit Design (TPCD)*, strives to be a premier forum for disseminating research in Formal Verification (FV) methods for digital circuits and systems, including processors, custom VLSI circuits, microcode, and reactive software. In addition to significant case-studies and verification approaches, FMCAD also endeavors to represent advances in the driving technologies for verification, including binary decision diagrams, model checking, symbolic reasoning (theorem proving), symbolic simulation, and abstraction methods.

The conference included four invited lectures. The invited lectures were given by Kenneth McMillan (Cadence Berkeley Labs) on *Minimalist proof assistants: interactions of technology and methodology in formal system level verification*, by Carl-Johan Seger on *Formal methods in CAD from an industrial perspective*, by Randal E. Bryant and Bwolen Yang on *A performance study of BDD-based model checking*, and by Amir Pnueli on *Verification of data-insensitive circuits: an in-order-retirement case study*. Of the 55 regular paper submissions received, 27 were selected by the technical program committee for presentation at the conference. All four tools papers received were also selected.

We gratefully acknowledge the services of the technical program committee of FMCAD'98, which consisted of Adnan Aziz (Univ. of Texas at Austin, USA), Alan Hu (Univ. of British Columbia, Canada), Albert Camilleri (Hewlett-Packard, USA), Carl Pixley (Motorola, USA), Carlos Delgado Kloos (Univ. Carlos III de Madrid, Spain), Ching-Tsun Chou (Intel, USA), Eduard Cerny (Univ. of Montreal, Canada), Francisco Corella (Hewlett-Packard, USA), Jens (Stanford University, USA), Jerry Burch (Cadence Labs, USA), John van Tassel (Texas Instruments, USA), Limor Fix (Intel, Israel), Mandayam Srivas (SRI International, USA), Mark Aagaard (Intel, USA), Mary Sheeran (Chalmers University, Sweden), Masahiro Fujita (Fujitsu, USA), Ramin Hojati (HDAC, and UC Berkeley, USA), Randy Bryant (Carnegie-Mellon, USA), Ranga Vemuri (Univ. of Cincinnati, USA), Shiu-kai Chin (Syracuse Univ., USA), Steven German (IBM, USA), Steven Johnson (Indiana Univ., USA), Thomas Kropf (Univ. Karlsruhe, Germany), Tim Leonard (Compaq, USA), Tom Henzinger (UC Berkeley, USA), Tom Melham (Univ. of Glasgow, UK), Tom Shiple (Synopsys, USA), and Warren Hunt (IBM, USA).

The following researchers also helped in the evaluation of the submissions, and we are grateful for their efforts: Abdel Mokkedem, Mike Jones, and Rajnish Ghughal (University of Utah), Rob Shaw (Hewlett-Packard), Armin Biere, Bwolen Yang, and Yirng-An Chen (CMU), Andres Marin Lopez, Franz Josef

Stewing, and Peter T. Breuer (Univ. Carlos III, Madrid), Abdelkader Dekdouk, E. Mostapha Aboulhamid, and Otmane AIT MOHAMED (Univ. of Montreal, Canada), Chuck Yount, Marten van Hulst, and John Mark Bouler (Intel), Koichiro Takayama and Vamsi Boppana (Fujitsu), Orna Kupferman, Luca de Alfaro, Sriram K. Rajamani, and Shaz Qadeer (Berkeley), Jun Sawada (U. of Texas), Howard Wong-Toi (Cadence), Supratik Chakraborty, Clark Barrett, and Jeffrey Su (Stanford), Michaela Huhn, Ralf Reetz, Klaus Schneider, and Jürgen Ruf (Karlsruhe), Justin Chien and Jun Yuan (Compaq), Nazanin Mansouri, Naren Narasimhan, Elena Teica, and Rajesh Radhakrishnan (Univ. of Cincinnati). We also thank Ratan Nalumasu, PhD student at the Department of Computer Science, University of Utah, for helping us with the tool demo session in his capacity as the *Tools Chair* of FMCAD'98.

We thank Judith Burgess of SRI International, Menlo Park, CA, for her help and advice in organizing FMCAD'98. We gratefully acknowledge the services of Conferences and Institutes, University of Utah, notably of Jacqueline Brakey, Cathy Cunningham, and Linda Williams, for their work on registration, publicity, and conference facilities. We also gratefully acknowledge the services of the Springer-Verlag LNCS department, especially Alfred Hofmann and Anna Kramer, for their prompt help and communication. We thank the IFIP Working Group 10.5 for granting us the *in co-operation* status.

Last, *but not least*, FMCAD'98 has received financial support from Hewlett-Packard Company, Intel, Synopsys Inc., and Cadence Berkeley Labs. We thank all sponsors for their generosity.

Salt Lake City, UT
Provo, UT

Ganesh C. Gopalakrishnan
Phillip J. Windley

August 1998

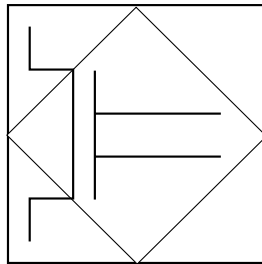


Table of Contents

Minimalist Proof Assistants: Interactions of Technology and Methodology in Formal System Level Verification <i>Kenneth L. McMillan</i>	1
Reducing Manual Abstraction in Formal Verification of Out-of-Order Execution <i>Robert B. Jones, Jens U. Skakkebak, and David L. Dill</i>	2
Bit-Level Abstraction in the Verification of Pipelined Microprocessors by Correspondence Checking <i>Miroslav N. Velev and Randal E. Bryant</i>	18
Solving Bit-Vector Equations <i>M. Oliver Möller and Harald Rueß</i>	36
The Formal Design of 1M-Gate ASICs <i>Ásgeir Þór Eiríksson</i>	49
Design of Experiments for Evaluation of BDD Packages Using Controlled Circuit Mutations <i>Justin E. Harlow III and Franc Brglez</i>	64
A Tutorial on Stålmarck's Proof Procedure for Propositional Logic <i>Mary Sheeran and Gunnar Stålmarck</i>	82
Almana: A BDD Minimization Tool Integrating Heuristic and Rewriting Methods <i>Macha Nikolskaia, Antoine Rauzy, and David James Sherman</i>	100
Bisimulation Minimization in an Automata-Theoretic Verification Framework <i>Kathi Fisler and Moshe Y. Vardi</i>	115
Automatic Verification of Mixed-Level Logic Circuits <i>Keith Hanna</i>	133
A Timed Automaton-Based Method for Accurate Computation of Circuit Delay in the Presence of Cross-Talk <i>S. Taşiran, S.P. Khatri, S. Yovine, R.K. Brayton, and A. Sangiovanni-Vincentelli</i>	149
Maximum Time Separation of Events in Cyclic Systems with Linear and Latest Timing Constraints <i>Fen Jin, Henrik Hulgaard, and Eduard Cerny</i>	167
Using MTBDDs for Composition and Model Checking of Real-Time Systems <i>Jürgen Ruf and Thomas Kropf</i>	185
Formal Methods in CAD from an Industrial Perspective <i>Carl-Johan H. Seger</i>	203

A Methodology for Automatic Verification of Synthesized RTL Designs and Its Integration with a High-Level Synthesis Tool <i>Nazanin Mansouri and Ranga Vemuri</i>	204
Combined Formal Post- and Presynthesis Verification in High Level Synthesis <i>Thomas Lock, Michael Mendler, and Matthias Mutz</i>	222
Formalization and Proof of a Solution to the PCI 2.1 Bus Transaction Ordering Problem <i>Abdel Mokkedem, Ravi Hosabettu, and Ganesh Gopalakrishnan</i>	237
A Performance Study of BDD-Based Model Checking <i>Bwolen Yang, Randal E. Bryant, David R. O'Hallaron, Armin Biere, Olivier Coudert, Geert Janssen, Rajeev K. Ranjan, and Fabio Somenzi</i> ...	255
Symbolic Model Checking Visualization <i>Gila Kamhi, Limor Fix, and Ziv Binyamini</i>	290
Input Elimination and Abstraction in Model-Checking <i>Sela Mador-Haim and Limor Fix</i>	304
Symbolic Simulation of the JEM1 Microprocessor <i>David A. Greve</i>	321
Symbolic Simulation: An ACL2 Approach <i>J. Strother Moore</i>	334
Verification of Data-Insensitive Circuits: An In-Order-Retirement Case Study <i>Amir Pnueli and T. Arons</i>	351
Combining Symbolic Model Checking with Uninterpreted Functions for Out-of-Order Processor Verification <i>Sergey Berezin, Armin Biere, Edmund Clarke, and Yunshan Zhu</i>	369
Formally Verifying Data and Control with Weak Reachability Invariants <i>Jeffrey Su, David L. Dill, and Jens U. Skakkebak</i>	387
Generalized Reversible Rules <i>C. Norris Ip</i>	403
An Assume-Guarantee Rule for Checking Simulation <i>Thomas A. Henzinger, Shaz Qadeer, Sriram K. Rajamani, and Serdar Tas̄van</i>	421
Three Approaches to Hardware Verification: HOL, MDG, and VIS Compared <i>Softène Tahar, Paul Curzon, and Jianping Lu</i>	433
An Instruction Set Process Calculus <i>Shiu-Kai Chin and Jang Dae Kim</i>	451
Techniques for Implicit State Enumeration of EFSMs <i>James H. Kukula, Tom R. Shiple, and Adnan Aziz</i>	469
Model Checking on Product Structures <i>Klaus Schneider</i>	483

BDDNOW: A Parallel BDD Package <i>Kim Milvang-Jensen and Alan J. Hu</i>	501
Model-Checking VHDL with CV <i>David Déharbe, Subash Shankar, and Edmund M. Clarke</i>	508
Alexandria: A Tool for Hierarchical Verification <i>Annette Bunker, Trent N. Larson, Michael D. Jones, and Phillip J. Windley</i>	515
PV: An Explicit Enumeration Model-Checker <i>Ratan Nalumasu and Ganesh Gopalakrishnan</i>	523
Author Index	529