Lecture Notes in Computer Science 1954
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

Warren A. Hunt, Jr. Steven D. Johnson (Eds.)

Formal Methods in Computer-Aided Design

Third International Conference, FMCAD 2000
Austin, TX, USA, November 1-3, 2000
Proceedings

Springer

Volume Editors

Warren A. Hunt, Jr.
IBM Corporation, Austin Research Laboratories
Mail Stop 9460, Building 904
11501 Burnet Road, Austin, Texas 78758, USA
E-mail: whunt@austin.ibm.com

Steven D. Johnson
Indiana University, Computer Science Department
Lindley Hall, 150 W. Woodlawn Avenue
Bloomington, Indiana 47405-7104, USA
E-mail: sjohnson@cs.indiana.edu

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Formal methods in computer aided design : third international conference ; proceedings / FMCAD 2000, Austin, Texas, USA, November 1 - 3, 2000. Warren A. Hunt, jr. ; Steven D. Johnson (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 2000
(Lecture notes in computer science ; Vol. 1954)
ISBN 3-540-41219-0

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 3-540-41219-0 Springer-Verlag Berlin Heidelberg New York

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

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Christian Grosche, Hamburg
Printed on acid-free paper SPIN: 10780987 06/3142 5 4 3 2 1 0

Preface

The biannual *Formal Methods in Computer Aided Design* conference (FMCAD 2000) is the third in a series of conferences under that title devoted to the use of discrete mathematical methods for the analysis of computer hardware and software. The work reported in this book describes the use of modeling languages and their associated automated analysis tools to specify and verify computing systems.

Functional verification has become one of the principal costs in a modern computer design effort. In addition, verification of circuit models, timing, power, etc., requires even more effort. FMCAD provides a venue for academic and industrial researchers and practitioners to share their ideas and experiences of using discrete mathematical modeling and verification. It is noted with interest by the conference chairmen how this area has grown from just a few people 15 years ago to a vibrant area of research, development, and deployment. It is clear that these methods are helping reduce the cost of designing computing systems. As an example of this potential cost reduction, we have invited David Russinoff of Advanced Micro Devices, Inc. to describe his verification of floating-point algorithms being used in AMD microprocessors. The program includes 30 regular presentations selected from 63 submitted papers.

The FMCAD conference has a long history dating back to 1984, when the earliest meetings on this topic occurred. A series of workshops sponsored by IFIP WG10.2 were held in Darmstadt (1984, org. Hans Eveking), Edinburgh (1985, org. George J. Milne and P.A. Subrahmanyam), Grenoble (1986, org. Dominique Borrione), Glasgow (1988, org. George J. Milne), Leuven (1989, org. Luc Claessen), and Miami (1990, org. P.A. Subrahmanyam). FMCAD originally had the name *Theorem Provers in Circuit Design*. TPCD meetings were held in Nijmegen (1992, org. Raymond T. Boute, Thomas Melham, and Victoria Stavridou) and Bad Herrenalb (1994, org. Thomas Kropf and Ramayya Kumar). Renamed *Formal Methods in Computer Aided Design*, the venue was changed to San Jose for the next two meetings (1996, org. Albert Camilleri and Mandayam Srivas, and 1998, org. Ganesh Goplakrishan and Phillip J. Windley). FMCAD 2000 was held in Austin. FMCAD alternates with the biannual conference on *Correct Hardware Design and Verification Methods*. CHARME originated with a research presentation of the ESPRIT group "CHARME" at Torino. Subsequent conferences were held at Arles (1993, org. George J. Milne and Laurence Pierre), Frankfort (1995, org. Hans Eveking and Paolo Camurati), Montreal (1997, org. Hon F. Li and David K. Probst), and Bad Herrenalb (1999, org. Thomas Kropf and Laurence Pierre).

The organizers are grateful to Advanced Micro Devices, Inc., Cadence Design Systems, Inc., Compaq Computer Corp., IBM Corp., Intel Corp., Prover Technology AB, Real Intent Corp., Synopsys, Inc., and Xilinx Inc., for their financial sponsorship, which considerably eased the organization of the conference.

Dan Elgin and Jo Moore are to be thanked for their tireless effort; they kept us on an organized and orderly path.

November 2000

Warren A. Hunt, Jr.
Steven D. Johnson

Organization

FMCAD 2000 was organized and held in Austin, Texas, U.S.A., at Austin's Marriott at the Capitol. An ACL2 workshop and a tutorial and workshop on Formal Specification and Verification Methods for Shared Memory Systems were also held in conjunction with FMCAD 2000.

Program Committee

Conference Chairs: Warren A. Hunt, Jr. (IBM Austin Research Lab, USA)
Steven D. Johnson (Indiana University, USA)
Mark Aagaard (Intel Corporation, USA)
Dominique Borrione (Laboratoire TIMA and Université Joseph Fourier, France)
Randy Bryant (Carnegie Mellon University, USA)
Albert Camilleri (Hewlett-Packard Co., USA)
Eduard Cerny (Université de Montréal, Canada)
Shiu-Kai Chin (Syracuse University, USA)
Luc Claesen (LCI SMARTpen N.V. & K.U.Leuven, Belgium)
Edmund Clarke (Carnegie Mellon University, USA)
David L. Dill (Stanford University, USA)
Hans Eveking (Darmstadt University of Technology, Germany)
Limor Fix (Intel Corporation, Israel)
Masahiro Fujita (University of Toyko, Japan)
Steven German (IBM T.J. Watson Research Center, USA)
Ganesh Gopalakrishnan (University of Utah, USA)
Mike Gordon (Cambridge University, UK)
Yuri Gurevich (Microsoft Research, USA)
Kieth Hanna (University of Kent, Great Britian)
Alan Hu (University of British Columbia, Canada)
Damir Jamsek (IBM Austin Research Lab, USA)
Matt Kaufmann (Advanced Micro Devices, Inc., USA)
Thomas Kropf (Robert Bosch GmbH and University of Tübingen, Germany)
Andreas Kuehlmann (Cadence Design Systems, Inc., USA)
John Launchbury (Oregon Graduate Institute, USA)
Tim Leonard (Compaq Computer Corp., USA)
Ken McMillan (Cadence Berkeley Labs, USA)
Tom Melham (University of Glasgow, Scotland)
Paul Miner (NASA Langley Research Center, USA)
John O'Leary (Intel Corp., USA)
Laurence Pierre (Université de Provence, France)
Carl Pixley (Motorola, Inc., USA)
Amir Pnueli (Technion, Israel)
Rajeev Ranjan (Real Intent Corp., USA)

David Russinoff (Advanced Micro Devices, Inc., USA)
Mary Sheeran (Chalmers Univ. of Technology and Prover Technology, Sweden)
Anna Slobodova (Compaq Computer Corp., USA)
Mandayam Srivas (SRI International, USA)
Victoria Stavridou (SRI International, USA)
Ranga Vemuri (University of Cincinnati, USA)
Matthew Wilding (Rockwell Collins, Inc., USA)
Phillip J. Windley (Brigham Young University, USA)

Additional Referees

Tamarah Arons
Annette Bunker
Venkatesh Choppella
Bruno Dutertre
Dana Fisman
Rob Gerth
David Greve
Dirk Hoffmann
Ravi Hosabettu
Michael D. Jones
Nazanin Mansouri
Nir Piterman
Rajesh Radhakrishnan
Sriram Rajamani
Vanderlei Rodrigues
Hassen Saidi
Elad Shahar
Robert Shaw
Kanna Shimizu
Robert Sumners
Elena Teica
Margus Veanes

FMCAD'00 Bibliography

[1] Warren A. Hunt, Jr. and Steven D. Johnson, editors. *Formal Methods in Computer-Aided Design, Third International Conference, FMCAD 2000, Austin, TX, USA, November 1-3, 2000, Proceedings*, volume 1954 of *Lecture Notes in Computer Science*. Springer-Verlag, Heidelberg Berlin, 2000.

[2] David M. Russinoff. A case study in formal verification of register-transfer logic with ACL2: The floating point adder of the AMD Athlon^{TM} processor. In Warren A. Hunt, Jr. and Steven D. Johnson, editors, *Formal Methods in Computer-Aided Design, Third International Conference, FMCAD 2000, Austin, TX, USA, November 1-3, 2000, Proceedings*, volume 1954 of *Lecture Notes in Computer Science*, pages 3–37, Heidelberg Berlin, 2000. Springer-Verlag.

[3] Roderick Bloem, Harold N. Gabow, and Fabio Somenzi. An algorithm for strongly connected component analysis in $n \log n$ symbolic steps. In Warren A. Hunt, Jr. and Steven D. Johnson, editors, *Formal Methods in Computer-Aided Design, Third International Conference, FMCAD 2000, Austin, TX, USA, November 1-3, 2000, Proceedings*, volume 1954 of *Lecture Notes in Computer Science*, pages 38–55, Heidelberg Berlin, 2000. Springer-Verlag.

[4] David Basin, Stefan Friedrich, and Sebastian Mödersheim. B2M: A semantic based tool for BLIF hardware descriptions. In Warren A. Hunt, Jr. and Steven D. Johnson, editors, *Formal Methods in Computer-Aided Design, Third International Conference, FMCAD 2000, Austin, TX, USA, November 1-3, 2000, Proceedings*, volume 1954 of *Lecture Notes in Computer Science*, pages 56–73, Heidelberg Berlin, 2000. Springer-Verlag.

[5] Mary Sheeran, Satnam Singh, and Gunnar Stålmarck. Checking safety properties using induction and a SAT-solver. In Warren A. Hunt, Jr. and Steven D. Johnson, editors, *Formal Methods in Computer-Aided Design, Third International Conference, FMCAD 2000, Austin, TX, USA, November 1-3, 2000, Proceedings*, volume 1954 of *Lecture Notes in Computer Science*, pages 74–91, Heidelberg Berlin, 2000. Springer-Verlag.

[6] Nancy A. Day, Mark D. Aagaard, and Byron Cook. Combining stream-based and state-based verification techniques for microarchitectures. In Warren A. Hunt, Jr. and Steven D. Johnson, editors, *Formal Methods in Computer-Aided Design, Third International Conference, FMCAD 2000, Austin, TX, USA, November 1-3, 2000, Proceedings*, volume 1954 of *Lecture Notes in Computer Science*, pages 92–108, Heidelberg Berlin, 2000. Springer-Verlag.

[7] Kavita Ravi, Roderick Bloem, and Fabio Somenzi. A comparative study of symbolic algorithms for the computation of fair cycles. In Warren A. Hunt, Jr. and Steven D. Johnson, editors, *Formal Methods in Computer-Aided*

Table of Contents

Invited Talk

Trends in Computing 1
Mark E. Dean

Invited Paper

A Case Study in Formal Verification of Register-Transfer Logic with ACL2: The Floating Point Adder of the AMD Athlon^{TM} Processor 3
David M. Russinoff

Contributed Papers

An Algorithm for Strongly Connected Component Analysis in $n \log n$ Symbolic Steps 37
Roderick Bloem, Harold N. Gabow, Fabio Somenzi

Automated Refinement Checking for Asynchronous Processes 55
Rajeev Alur, Radu Grosu, Bow-Yaw Wang

Border-Block Triangular Form and Conjunction Schedule in Image Computation 73
In-Ho Moon, Gary D. Hachtel, Fabio Somenzi

B2M: A Semantic Based Tool for BLIF Hardware Descriptions 91
David Basin, Stefan Friedrich, Sebastian Mödersheim

Checking Safety Properties Using Induction and a SAT-Solver 108
Mary Sheeran, Satnam Singh, Gunnar Stålmarck

Combining Stream-Based and State-Based Verification Techniques 126
Nancy A. Day, Mark D. Aagaard, Byron Cook

A Comparative Study of Symbolic Algorithms for the Computation of Fair Cycles 143
Kavita Ravi, Roderick Bloem, Fabio Somenzi

Correctness of Pipelined Machines 161
Panagiotis Manolios

Do You Trust Your Model Checker? 179
Wolfgang Reif, Jürgen Ruf, Gerhard Schellhorn, Tobias Vollmer

Executable Protocol Specification in **ESL** 197
Edmund M. Clarke, S. German, Y. Lu, Helmuth Veith, D. Wang

Formal Verification of Floating Point Trigonometric Functions 217
John Harrison

Hardware Modeling Using Function Encapsulation 234
Jun Sawada, Warren A. Hunt, Jr.

A Methodology for the Formal Analysis of Asynchronous Micropipelines . . 246
Antonio Cerone, George J. Milne

A Methodology for Large-Scale Hardware Verification 263
Mark D. Aagaard, Robert B. Jones, Thomas F. Melham, John W. O'Leary, Carl-Johan H. Seger

Model Checking Synchronous Timing Diagrams 283
Nina Amla, E. Allen Emerson, Robert P. Kurshan, Kedar S. Namjoshi

Model Reductions and a Case Study 299
Jin Hou, Eduard Cerny

Modeling and Parameters Synthesis for an Air Traffic Management System 316
Adilson Luiz Bonifácio, Arnaldo Vieira Moura

Monitor-Based Formal Specification of PCI 335
Kanna Shimizu, David L. Dill, Alan J. Hu

SAT-Based Image Computation with Application in Reachability Analysis 354
Aarti Gupta, Zijiang Yang, Pranav Ashar, Anubhav Gupta

SAT-Based Verification without State Space Traversal 372
Per Bjesse, Koen Claessen

Scalable Distributed On-the-Fly Symbolic Model Checking 390
Shoham Ben-David, Tamir Heyman, Orna Grumberg, Assaf Schuster

The Semantics of Verilog Using Transition System Combinators 405
Gordon J. Pace

Sequential Equivalence Checking by Symbolic Simulation 423
Gerd Ritter

Speeding Up Image Computation by Using RTL Information 443
Christoph Meinel, Christian Stangier

Symbolic Checking of Signal-Transition Consistency for Verifying High-Level Designs 455
Kiyoharu Hamaguchi, Hidekazu Urushihara, Toshinobu Kashiwabara

Symbolic Simulation with Approximate Values 470
Chris Wilson, David L. Dill, Randal E. Bryant

A Theory of Consistency for Modular Synchronous Systems 486
Randal E. Bryant, Pankaj Chauhan, Edmund M. Clarke, Amit Goel

Verifying Transaction Ordering Properties in Unbounded Bus Networks through Combined Deductive/Algorithmic Methods 505
Michael Jones, Ganesh Gopalakrishnan

Visualizing System Factorizations with Behavior Tables 520
Alex Tsow, Steven D. Johnson

Author Index 539