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

August 1998
# Table of Contents

Minimalist Proof Assistants: Interactions of Technology an Methodology in Formal System Level Verification  
*Kenneth L. McMillan* .......................................................... 1

Reducing Manual Abstraction in Formal Verification of Out-of-Order Execution  
*Robert B. Jones, Jens U. Skakkebæk, and David L. Dill* .................. 2

Bit-Level Abstraction in the Verification of Pipelined Microprocessors by Correspondence Checking  
*Miroslav N. Velev and Randal E. Bryant* ................................. 18

Solving Bit-Vector Equations  
*M. Oliver Möller and Harald Rueß* ........................................... 36

The Formal Design of 1M-Gate ASICs  
*Ásgeir Pór Eiríksson* .......................................................... 49

Design of Experiments for Evaluation of BDD Packages Using Controlled Circuit Mutations  
*Justin E. Harlow III and Franc Brglez* .................................... 64

A Tutorial on Stålmarck’s Proof Procedure for Propositional Logic  
*Mary Sheeran and Gunnar Stålmarck* ...................................... 82

Almana: A BDD Minimization Tool Integrating Heuristic and Rewriting Methods  
*Macha Nikolskaïa, Antoine Rauzy, and David James Sherman* .......... 100

Bisimulation Minimization in an Automata-Theoretic Verification Framework  
*Kathi Fisler and Moshe Y. Vardi* ............................................ 115

Automatic Verification of Mixed-Level Logic Circuits  
*Keith Hanna* .................................................................. 133

A Timed Automaton-Based Method for Accurate Computation of Circuit Delay in the Presence of Cross-Talk  
*S. Taşrın, S.P. Khatri, S. Yovine, R.K. Brayton, and A. Sangiovanni-Vincentelli* .................................................. 149

Maximum Time Separation of Events in Cyclic Systems with Linear and Latest Timing Constraints  
*Fen Jin, Henrik Hulgaard, and Eduard Cerny* ............................. 167

Using MTBDDs for Composition and Model Checking of Real-Time Systems  
*Jürgen Ruf and Thomas Kropf* .............................................. 185

Formal Methods in CAD from an Industrial Perspective  
*Carl-Johan H. Seger* .......................................................... 203
A Methodology for Automatic Verification of Synthesized RTL Designs and Its Integration with a High-Level Synthesis Tool
*Nazanin Mansouri and Ranga Vemuri* .............................................................. 204

Combined Formal Post- and Presynthesis Verification in High Level Synthesis
*Thomas Lock, Michael Mendler, and Matthias Mutz* ............................... 222

Formalization and Proof of a Solution to the PCI 2.1 Bus Transaction Ordering Problem
*Abdel Mokkedem, Ravi Hosabettu, and Ganesh Gopalakrishnan* ............ 237

A Performance Study of BDD-Based Model Checking
*Buwlon Yang, Randal E. Bryant, David R. O’Hallaron, Armin Biere, Olivier Coudert, Geert Janssen, Rajeev K. Ranjan, and Fabio Somenzi* .. . 255

Symbolic Model Checking Visualization
*Gila Kamhi, Limor Fix, and Ziv Bingamini* .............................................. 290

Input Elimination and Abstraction in Model-Checking
*Sela Mador-Haim and Limor Fix* ................................................................. 304

Symbolic Simulation of the JEM1 Microprocessor
*David A. Greve* ............................................................................................... 321

Symbolic Simulation: An ACL2 Approach
*J. Strother Moore* ......................................................................................... 334

Verification of Data-Insensitive Circuits: An In-Order-Retirement Case Study
*Amir Pnueli and T. Arons* ............................................................................. 351

Combining Symbolic Model Checking with Uninterpreted Functions for Out-of-Order Processor Verification
*Sergey Berezin, Armin Biere, Edmund Clarke, and Yunshan Zhu* .......... 369

Formally Verifying Data and Control with Weak Reachability Invariants
*Jeffrey Su, David L. Dill, and Jens U. Skakkebæk* ........................................ 387

Generalized Reversible Rules
*C. Norris Ip* .................................................................................................. 403

An Assume-Guarantee Rule for Checking Simulation
*Thomas A. Henzinger, Shaz Qadeer, Sriram K. Rajamani, and Serdar Taşiran* .................................................................................................................. 421

Three Approaches to Hardware Verification: HOL, MDG, and VIS Compared
*Sofiène Tahar, Paul Curzon, and Jianping Lu* ............................................. 433

An Instruction Set Process Calculus
*Shiu-Kai Chin and Jang Dae Kim* ............................................................... 451

Techniques for Implicit State Enumeration of EFSMs
*James H. Kukula, Tom R. Shiple, and Adnan Aziz* .................................. 469

Model Checking on Product Structures
*Klaus Schneider* ............................................................................................ 483
<table>
<thead>
<tr>
<th>Title</th>
<th>Authors</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>BDDNOW: A Parallel BDD Package</td>
<td>Kim Milvang-Jensen and Alan J. Hu</td>
<td>501</td>
</tr>
<tr>
<td>Model-Checking VHDL with CV</td>
<td>David Déharbe, Subash Shankar, and Edmund M. Clarke</td>
<td>508</td>
</tr>
<tr>
<td>Alexandria: A Tool for Hierarchical Verification</td>
<td>Annette Bunker, Trent N. Larson, Michael D. Jones, and Phillip J. Windley</td>
<td>515</td>
</tr>
<tr>
<td>PV: An Explicit Enumeration Model-Checker</td>
<td>Ratan Nalumasu and Ganesh Gopalakrishnan</td>
<td>523</td>
</tr>
<tr>
<td>Author Index</td>
<td></td>
<td>529</td>
</tr>
</tbody>
</table>