

# Table of Contents

## Tutorials and Invited Papers

|                                                                                 |    |
|---------------------------------------------------------------------------------|----|
| Alternative Approaches to Hardware Verification .....                           | 1  |
| <i>D. L. Dill</i>                                                               |    |
| The Compositional Specification of Timed Systems – A Tutorial .....             | 2  |
| <i>J. Sifakis</i>                                                               |    |
| Timed Automata .....                                                            | 8  |
| <i>R. Alur</i>                                                                  |    |
| Stålmarck’s Method with Extensions to Quantified Boolean Formulas .             | 23 |
| <i>G. Stålmarck</i>                                                             |    |
| Verification of Parameterized Systems by Dynamic Induction<br>on Diagrams ..... | 25 |
| <i>Z. Manna and H. B. Sipma</i>                                                 |    |
| Formal Methods for Conformance Testing:<br>Theory Can Be Practical! .....       | 44 |
| <i>E. Brinksma</i>                                                              |    |

## Processor Verification

|                                                                                                             |    |
|-------------------------------------------------------------------------------------------------------------|----|
| Proof of Correctness of a Processor with Reorder Buffer Using<br>the Completion Functions Approach .....    | 47 |
| <i>R. Hosabettu, M. Srivas, G. Gopalakrishnan</i>                                                           |    |
| Verifying Safety Properties of a PowerPCMicroprocessor<br>Using Symbolic Model Checking without BDDs .....  | 60 |
| <i>A. Biere, E. Clarke, R. Raimi, Y. Zhu</i>                                                                |    |
| Model Checking the IBM Gigahertz Processor: An Abstraction<br>Algorithm for High-Performance Netlists ..... | 72 |
| <i>J. Baumgartner, T. Heyman, V. Singhal, A. Aziz</i>                                                       |    |
| Validation of Pipelined Processor Designs Using Esterel Tools:<br>A Case Study .....                        | 84 |
| <i>S. Ramesh, P. Bhaduri</i>                                                                                |    |

## Protocol Verification and Testing

|                                                                                                 |    |
|-------------------------------------------------------------------------------------------------|----|
| Automated Verification of a Parametric Real-Time Program:<br>The ABR Conformance Protocol ..... | 96 |
| <i>B. Bérard, L. Fribourg</i>                                                                   |    |

|                                                                                                    |     |
|----------------------------------------------------------------------------------------------------|-----|
| Test Generation Derived from Model-Checking .....                                                  | 108 |
| <i>T. Jeron, P. Morel</i>                                                                          |     |
| Latency Insensitive Protocols .....                                                                | 123 |
| <i>L. P. Carloni, K. L. McMillan, A. L. Sangiovanni-Vincentelli</i>                                |     |
| <b>Infinite State Space</b>                                                                        |     |
| Handling Global Conditions in Parametrized System Verification .....                               | 134 |
| <i>P. A. Abdulla, A. Bouajjani, B. Jonsson, M. Nilsson</i>                                         |     |
| Verification of Infinite-State Systems by Combining Abstraction and<br>Reachability Analysis ..... | 146 |
| <i>P. A. Abdulla, A. Annichini, S. Bensalem, A. Bouajjani,<br/>P. Habermehl, Y. Lakhnech</i>       |     |
| Experience with Predicate Abstraction .....                                                        | 160 |
| <i>S. Das, D. L. Dill, S. Park</i>                                                                 |     |
| <b>Theory of Verification</b>                                                                      |     |
| Model Checking of Safety Properties .....                                                          | 172 |
| <i>O. Kupferman, M. Y. Vardi</i>                                                                   |     |
| A Complete Finite Prefix for Process Algebra .....                                                 | 184 |
| <i>R. Langerak, E. Brinksma</i>                                                                    |     |
| The Mathematical Foundation of Symbolic Trajectory Evaluation ....                                 | 196 |
| <i>C.-T. Chou</i>                                                                                  |     |
| Assume-Guarantee Refinement between Different Time Scales .....                                    | 208 |
| <i>T. A. Henzinger, S. Qadeer, S. K. Rajamani</i>                                                  |     |
| <b>Linear Temporal Logic</b>                                                                       |     |
| Efficient Decision Procedures for Model Checking of Linear Time Logic<br>Properties .....          | 222 |
| <i>R. Bloem, K. Ravi, F. Somenzi</i>                                                               |     |
| Stutter-Invariant Languages, $\omega$ -Automata, and Temporal Logic .....                          | 236 |
| <i>K. Etessami</i>                                                                                 |     |
| Improved Automata Generation for Linear Temporal Logic .....                                       | 249 |
| <i>M. Daniele, F. Giunchiglia, M. Y. Vardi</i>                                                     |     |
| <b>Modeling of Systems</b>                                                                         |     |
| On the Representation of Probabilities over Structured Domains .....                               | 261 |
| <i>M. Bozga, O. Maler</i>                                                                          |     |

|                                                                                                                                        |     |
|----------------------------------------------------------------------------------------------------------------------------------------|-----|
| Model Checking Partial State Spaces with 3-Valued Temporal Logics .<br><i>G. Bruns, P. Godefroid</i>                                   | 274 |
| Elementary Microarchitecture Algebra .....<br><i>J. Matthews, J. Launchbury</i>                                                        | 288 |
| Verifying Sequential Consistency on Shared-Memory Multiprocessor<br>Systems .....<br><i>T. A. Henzinger, S. Qadeer, S. K. Rajamani</i> | 301 |
| <b>Symbolic Model-Checking</b>                                                                                                         |     |
| Stepwise CTL Model Checking of State/Event Systems .....<br><i>J. Lind-Nielsen, H. R. Andersen</i>                                     | 316 |
| Optimizing Symbolic Model Checking for Constraint-Rich Models ....<br><i>B. Yang, R. Simmons, R. E. Bryant, D. R. O'Hallaron</i>       | 328 |
| Efficient Timed Reachability Analysis Using Clock Difference Diagrams<br><i>G. Behrmann, K. G. Larsen, J. Pearson, C. Weise, W. Yi</i> | 341 |
| <b>Theorem Proving</b>                                                                                                                 |     |
| Mechanizing Proofs of Computation Equivalence .....<br><i>M. Glusman, S. Katz</i>                                                      | 354 |
| Linking Theorem Proving and Model-Checking with Well-Founded<br>Bisimulation .....<br><i>P. Manolios, K. S. Namjoshi, R. Sumners</i>   | 369 |
| Automatic Verification of Combinational and Pipelined FFT Circuits .<br><i>P. Bjesse</i>                                               | 380 |
| <b>Automata-Theoretic Methods</b>                                                                                                      |     |
| Efficient Analysis of Cyclic Definitions .....<br><i>K. S. Namjoshi, R. P. Kurshan</i>                                                 | 394 |
| A Theory of Restrictions for Logics and Automata .....<br><i>N. Klarlund</i>                                                           | 406 |
| Model Checking Based on Sequential ATPG .....<br><i>V. Boppana, S. P. Rajan, K. Takayama, M. Fujita</i>                                | 418 |
| Automatic Verification of Abstract State Machines .....<br><i>M. Spielmann</i>                                                         | 431 |

**Abstraction**

|                                                                                           |     |
|-------------------------------------------------------------------------------------------|-----|
| Abstract and Model Check while You Prove .....                                            | 443 |
| <i>H. Saïdi, N. Shankar</i>                                                               |     |
| Deciding Equality Formulas by Small Domains Instantiations .....                          | 455 |
| <i>A. Pnueli, Y. Rodeh, O. Shtrichman, M. Siegel</i>                                      |     |
| Exploiting Positive Equality in a Logic of Equality with<br>Uninterpreted Functions ..... | 470 |
| <i>R. E. Bryant, S. German, M. N. Velez</i>                                               |     |

**Tool Presentations**

|                                                                                             |     |
|---------------------------------------------------------------------------------------------|-----|
| A Toolbox for the Analysis of Discrete Event Dynamic Systems .....                          | 483 |
| <i>P. Buchholz, P. Kemper</i>                                                               |     |
| TIPPtool: Compositional Specification and Analysis of Markovian<br>Performance Models ..... | 487 |
| <i>H. Hermanns, V. Mertsiotakis, M. Siegle</i>                                              |     |
| Java Bytecode Verification by Model Checking .....                                          | 491 |
| <i>D. Basin, S. Friedrich, J. Posegga, H. Vogt</i>                                          |     |
| NuSMV: A New Symbolic Model Verifier .....                                                  | 495 |
| <i>A. Cimatti, E. Clarke, F. Giunchiglia, M. Roveri</i>                                     |     |
| PIL/SETHEO: A Tool for the Automatic Analysis of Authentication<br>Protocols .....          | 500 |
| <i>J. Schumann</i>                                                                          |     |
| <b>Author Index</b> .....                                                                   | 505 |