2008 Formal Methods in Computer-Aided Design

Portland, Oregon, USA
17-20 November 2008

ISBN: 978-1-4244-2735-2

Library of Congress: 2008906093

TABLE OF CONTENTS

Invited Tutorial: Considerations in the Design and Verification of Microprocessors for Safety-Critical and Security-Critical Applications 1
David S. Hardin

Invariant-Strengthened Elimination of Dependent State Elements..9
Michael L. Case, Alan Mishchenko, Robert K. Brayton, Jason Baumgartner, Hari Mony

Optimal Constraint-Preserving Netlist Simplification..18
Jason Baumgartner, Hari Mony, Adnan Aziz

Recording Synthesis History for Sequential Verification 27
Alan Mishchenko, Robert Brayton

BackSpace: Formal Analysis for Post-Silicon Debug..35
Flavio M. De Paula, Marcel Gort, Alan J. Hu, Steven J. E. Wilton, Jin Yang

Automatic Formal Verification of Block Cipher Implementations 45
Eric Smith, David L. Dill

Verifying an Arbiter Circuit 52
Chao Yan, Mark R. Greenstreet

Formal Verification of Hardware Support for Advanced Encryption Standard......................................61
Anna Slobodová

BACH : Bounded ReAchability CHecker for Linear Hybrid Automata 65
Lei Bu, You Li, Linzhang Wang, Xuandong Li

Going with the Flow: Parameterized Verification Using Message Flows..69
Murali Talupur, Mark R. Tuttle

Automatic Non-Interference Lemmas for Parameterized Model Checking 77
Jesse Bingham

Model Checking Nash Equilibria in MAD Distributed Systems..85
Federico Mari, Igor Melatti, Ivano Salvo, Enrico Tronci, Lorenzo Alvisi, Allen Clement, Harry Li

A Theory-Based Decision Heuristic for DPLL(T) 93
Dan Goldwasser, Ofer Strichman, Shai Fine

A Write-Based Solver for SAT Modulo the Theory of Arrays...101
Miquel Bofill, Robert Nieuwenhuis, Albert Oliveras, Enric Rodríguez-Carbonell, Albert Rubio

Scaling Up the Formal Verification of Lustre Programs with SMT-Based Techniques..........................109
George Hagen, Cesare Tinelli

Word-Level Sequential Memory Abstraction for Model Checking..118
Per Bjesse

Combining Predicate and Numeric Abstraction for Software Model Checking 127
Arie Gurfinkel, Sagar Chaki

A Refinement Approach to Design and Verification of On-Chip Communication Protocols 136
Peter Böhm, Tom Melham

Symbolic Program Analysis Using Term Rewriting and Generalization...144
Nishant Sinha

Machine-Code Verification for Multiple Architectures - An Application of Decompilation into Logic 153
Magnus O. Myreen, Michael J. C. Gordon, Konrad Slind

Scheduling Optimisations for SPIN to Minimise Buffer Requirements in Synchronous Data Flow 161
Pieter H. Hartel, Theo C. Ruys, Marc C. W. Geilen

A Temporal Language for SystemC 171
Deian Tabakov, Gila Kamhi, Moshe Y. Vardi, Eli Singerman

Augmenting a Regular Expression-Based Temporal Logic with Local Variables 180
Cindy Eisner, Dana Fisman

Beyond Vacuity: Towards the Strongest Passing Formula 188
Hana Chockler, Arie Gurfinkel, Ofer Strichman

A Theory of Mutations with Applications to Vacuity, Coverage, and Fault Tolerance 196
Orna Kupferman, Wenchao Li, Sanjit A. Seshia

Trading-Off SAT Search and Variable Quantifications for Effective Unbounded Model Checking 205
G. Cabodi, P. Camurati, L. Garcia, M. Murciano, S. Nocco, S. Quer

Automatic Generation of Local Repairs for Boolean Programs 213
Roopsha Samanta, Jyotirmoy V. Deshmukh, E. Allen Emerson

Consistency Checking of All Different Constraints over Bit-Vectors within a SAT Solver 223
Armin Biere, Robert Brummayer

Mechanized Information Flow Analysis through Inductive Assertions 227
Warren A. Hunt Jr., Robert Bellarmine Krug, Sandip Ray, William D. Young

Author Index