

2010 Formal Methods in Computer-Aided Design

(FMCAD 2010)

**Lugano, Switzerland
20 – 23 October 2010**



IEEE Catalog Number: CFP10FMC-PRT
ISBN: 978-1-4577-0734-6

Table of Contents

Tutorials.

Dimensions in Program Synthesis	1
<i>Sumit Gulwani</i>	

Verifying VIA Nano Microprocessor Components	3
<i>Warren A. Hunt, Jr.</i>	

Session 1. Invited Talk

Embedded Systems Design: Scientific Challenges and Work Directions	11
<i>Joseph Sifakis</i>	

Session 2. Industrial Track – Case Studies

Formal Verification of an ASIC Ethernet Switch Block	13
<i>Balekudru Krishna, Anamaya Sullerey, Alok Jain</i>	

Formal Verification of Arbiters using Property Strengthening and Under-approximations.....	21
<i>Gadiel Auerbach, Fady Copt, Viresh Paruthi</i>	

SAT-Based Semiformal Verification of Hardware	25
<i>Sabih Agbaria, Dan Carmi, Orly Cohen, Dmitry Korchemny, Michael Lifshits, Alexander Nadel</i>	

DFT Logic Verification through Property Based Formal Methods - SOC to IP	33
<i>Lopamudra Sen, Supriya Bhattacharjee, Amit Roy, Bijitendra Mittra, Subir K Roy</i>	

Session 3. Software Verification

SLAM2: Static Driver Verification with Under 4% False Alarms	35
<i>Thomas Ball, Ella Bounimova, Rahul Kumar, Vladimir Levin</i>	

Precise Static Analysis of Untrusted Driver Binaries	43
<i>Johannes Kinder, Helmut Veith</i>	

Verifying SystemC: a Software Model Checking Approach	51
<i>Alessandro Cimatti, Andrea Micheli, Iman Narasamdya, Marco Roveri</i>	

Session 4. Decision Procedures

Coping with Moore's Law (and More): Supporting Arrays in State-of-the-Art Model Checkers	61
<i>Jason Baumgartner, Michael Case, Hari Mony</i>	

CalCS: SMT Solving for Nonlinear Convex Constraints	71
<i>Pierluigi Nuzzo, Alberto Puggelli, Sanjit Seshia, Alberto Sangiovanni-Vincentelli</i>	

Integrating ICP and LRA Solvers for Deciding Nonlinear Real Arithmetic Problems.....	81
<i>Sicun Gao, Malay Ganai, Franjo Ivancic, Aarti Gupta, Sriram Sankaranarayanan, Edmund Clarke</i>	

Session 5. Synthesis

A Halting Algorithm to Determine the Existence of Decoder	91
<i>ShengYu Shen, Ying Qin, Jianmin Zhang, SiKun Li</i>	

Synthesis for Regular Specifications over Unbounded Domains.....	101
<i>Jad Hamza, Barbara Jobstmann, Viktor Kuncak</i>	

Automatic Inference of Memory Fences	111
<i>Michael Kuperstein, Martin Vechev, Eran Yahav</i>	

Session 6. Industrial Track

Applying SMT in Symbolic Execution of Microcode.....	121
<i>Anders Franzen, Alessandro Cimatti, Alexander Nadel, Roberto Sebastiani, Jonathan Shalev</i>	

Automated Formal Verification of Processors Based on Architectural Models .	129
<i>Ulrich Kuehne, Sven Beyer, Joerg Bormann, John Barstow</i>	

Encoding Industrial Hardware Verification Problems into Effectively Propositional Logic.....	137
<i>Zurab Khasidashvili, Moshe Emmer, Konstantin Korovin, Andrei Voronkov</i>	

Session 7. Hardware and Protocol Verification

Combinational Techniques for Sequential Equivalence Checking.....	145
<i>Hamid Savoj, David Berthelot, Alan Mishchenko, Robert Brayton</i>	

Automatic Verification of Estimate Functions with Polynomials of Bounded Functions	151
<i>Jun Sawada</i>	

A Framework for Incremental Modelling and Verification of On-Chip Protocols.....	159
<i>Peter Boehm</i>	

Modular Specification and Verification of Interprocess Communication	167
<i>Eyad Alkassar, Ernie Cohen, Mark Hillebrand, Hristo Pentchev</i>	

Session 8. Invited Talk

Large-scale Formal Application: From Fiction to Fact	175
<i>Viresh Paruthi</i>	

Session 9. Abstraction

A Single-Instance Incremental SAT Formulation of Proof-and Counterexample-Based Abstraction.....	181
<i>Niklas Een, Alan Mishchenko, Nina Amla</i>	

Predicate Abstraction with Adjustable-Block Encoding	189
<i>Dirk Beyer, M. Erkan Keremoglu, Philipp Wendler</i>	

Modular Bug Detection with Inertial Refinement.....	199
<i>Nishant Sinha</i>	

Path Predicate Abstraction by Complete Interval Property Checking	207
<i>Joakim Urdahl, Dominik Stoffel, Jörg Bormann, Markus Wedler, Wolfgang Kunz</i>	

Session 10. SAT and QBF

Relieving Capacity Limits on FPGA-based SAT-solvers	217
<i>Leopold Haller, Satnam Singh</i>	

Boosting Minimal Unsatisfiable Core Extraction	221
<i>Alexander Nadel</i>	

Propelling SAT and SAT-based BMC using Careset.....	231
<i>Malay Ganai</i>	

Efficiently Solving Quantified Bit-Vector Formulas	239
<i>Christoph Wintersteiger, Youssef Hamadi, Leonardo de Moura</i>	

Session 11. Verification of Concurrent Systems

Boosting Multi-Core Reachability Performance with Shared Hash Tables	247
<i>Alfons Laarman, Jaco van de Pol, Michael Weber</i>	

Incremental Component-based Construction and Verification using Invariants.....	257
<i>Saddek Bensalem, Marius Bozga, Axel Legay, Thanh-Hung Nguyen, Joseph Sifakis, Rongjie Yan</i>	

Verifying Shadow Page Table Algorithms	267
<i>Eyad Alkassar, Ernie Cohen, Mark Hillebrand, Mikhail Kovalev, Wolfgang Paul</i>	

Exhibition.

Impacting Verification Closure using Formal Analysis (<i>abstract</i>)	271
<i>Massimo Roselli</i>	

Scalable and Precise Program Analysis at NEC (<i>abstract</i>)	273
<i>Gogul Balakrishnan, Malay Ganai, Aarti Gupta, Franjo Ivancic, Vineet Kahlon, Weihong Li, Naoto Maeda, Nadia Papakonstantinou, Sriram Sankaranarayanan, Nishant Sinha, Chao Wang</i>	

Achieving Earlier Verification Closure Using Advanced Formal Verification (abstract)	275
<i>Michael Siegel</i>	
 PINCETTE - Validating Changes and Upgrades in Networked Software (abstract)	277
<i>Hana Chockler</i>	