

2009 Formal Methods in Computer-Aided Design

(FMCAD 2009)

Austin, Texas, USA
15-18 November 2009



IEEE Catalog Number: CFP09FMC-PRT
ISBN: 978-1-4244-4965-1

Table of Contents

Panels

Session 1. Model Checking

Interpolation-Sequence Based Model Checking	1
<i>Yakir VizeI, Orna Grumberg</i>	

Structure-Aware Computation of Predicate Abstraction	9
<i>Alessandro Cimatti, Jori Dubrovin, Tommi Junttila, Marco Roveri</i>	

Enhanced Verification By Temporal Decomposition	17
<i>Michael Case, Hari Mony, Jason Baumgartner, Robert Kanzelman</i>	

Session 2. Software Verification

Software Model Checking via Large-Block Encoding	25
<i>Dirk Beyer, Alessandro Cimatti, Alberto Griggio, M. Erkan Keremoglu, Roberto Sebastiani</i>	

Verification of Recursive Methods on Tree-like Data Structures	33
<i>Jyotirmoy Deshmukh, E. Allen Emerson</i>	

MCC: A runtime verification tool for MCAPI user applications	41
<i>Subodh Sharma, Ganesh Gopalakrishnan, Eric Mercer, Jim Holt</i>	

Session 3. Satisfiability Modulo Theory

Generalized and Efficient Array Decision Procedures	45
<i>Leonardo de Moura, Nikolaj Bjorner</i>	

Decision Diagrams for Linear Arithmetic	53
<i>Sagar Chaki, Arie Gurfinkel, Ofer Strichman</i>	

Efficient Decision Procedure for Non-linear Arithmetic Constraints using CORDIC	61
<i>Malay Ganai, Franjo Ivancic</i>	

Mixed Abstractions for Floating-Point Arithmetic	69
<i>Angelo Brillout, Daniel Kroening, Thomas Wahl</i>	

Session 4. Games

Safety First: A Two-Stage Algorithm for LTL Games	77
<i>Saqib Sohail, Fabio Somenzi</i>	

Synthesizing Robust Systems	85
<i>Roderick Bloem, Karin Greimel, Thomas Henzinger, Barbara Jobstmann</i>	

Session 5. Quantitative Reasoning

Formal Verification of Analog Designs using MetiTarski	93
<i>William Denman, Behzad Akbarpour, Sofiene Tahar, Mohamed H. Zaki, Lawrence Paulson</i>	
Formal Verification of Correctness and Performance of Random Priority-based Arbiters	101
<i>Krishnan Kailas, Viresh Paruthi, Brian Monwai</i>	

Session 6. Assume Guarantee Reasoning

Assume-Guarantee Validation for STE Properties within an SVA Environment	108
<i>Zurab Khasidashvili, Gavriel Gavrielov, Tom Melham</i>	
Data Mining based Decomposition for Assume-Guarantee Reasoning	116
<i>He Zhu, Fei He, William N. N. Hung, Xiaoyu Song, Ming Gu</i>	

Session 7. Equivalence Checking

Scalable Conditional Equivalence Checking: An Automated Invariant-Generation Based Approach	120
<i>Jason Baumgartner, Hari Mony, Michael Case, Jun Sawada, Karen Yorav</i>	
Verifying Equivalence of Memories Using a First Order Logic Theorem Prover	128
<i>Zurab Khasidashvili, Mahmoud Kinanah, Andrei Voronkov</i>	
A Compositional Theory for Post-Reboot Observational Equivalence Checking of Hardware	136
<i>Zurab Khasidashvili, Daher Kaiss, Doron Bustan</i>	

Session 8. Debugging

Scaling VLSI Design Debugging with Interpolation	144
<i>Brian Keng, Andreas Veneris</i>	
Debugging Formal Specifications Using Simple Counterstrategies	152
<i>Robert Koenighofer, Georg Hofferek, Roderick Bloem</i>	
Connecting Pre-silicon and Post-silicon Verification	160
<i>Sandip Ray, Warren Hunt</i>	

Session 9. Case Studies and Verification in the Large

A Verified Platform for a Gate-Level Electronic Control Unit	164
<i>Sergey Tverdyshev</i>	
Protocol verification using Flows: An Industrial Experience	172
<i>John O'Leary, Murali Talupur, Mark Tuttle</i>	
Industrial Strength Refinement Checking	180
<i>Jesse Bingham, Flemming Andersen, John Erickson, Gaurav Singh</i>	
Towards a Formally Verified Network-on-Chip	184
<i>Tom van den Broek, Julien Schmaltz</i>	
Hardware/Software Co-verification of Cryptographic Algorithms using Cryptol	188
<i>Levent Erkok, Magnus Carlsson, Adam Wick</i>	

Session 10. Synthesis

Retiming and Resynthesis With Sweep Are Complete for Sequential Transformations	192
<i>Hai Zhou</i>	
SAT-based Synthesis of Clock Gating Functions Using 3-Valued Abstraction	198
<i>Eli Arbel, Oleg Rokhlenko, Karen Yorav</i>	
Finding heap-bounds for hardware synthesis	205
<i>Byron Cook, Ashutosh Gupta, Stephen Magill, Andrey Rybalchenko, Jiri Simsa, Satnam Singh, Viktor Vafeiadis</i>	

Author Index