

2011 Formal Methods in Computer-Aided Design

(FMCAD 2011)

Austin, Texas, USA
30 October – 2 November 2011



IEEE Catalog Number: CFP11FMC-PRT
ISBN: 978-1-4673-0896-0

TABLE OF CONTENTS	i
Preface – Per Bjesse and Anna Slobodová	iii
<i>Verifying Concurrent Programs</i> (Invited Tutorial) – Aarti Gupta	1
<i>Self-Timing: a Step Beyond Synchrony</i> (Invited Tutorial) – Ivan Sutherland	2
<i>IC3: Where Monolithic and Incremental Meet</i> (Invited Tutorial) – Fabio Somenzi and Aaron Bradley	3
<i>Planning for End-to-End Formal using Simulation-based Coverage</i> (Invited Tutorial) – Prashant Aggarwal, Darrow Chu, Vijay Kadamby and Vigyan Singhal	9
<i>Specification Based Testing with QuickCheck</i> (Invited Tutorial) – John Hughes	17
<i>Theorem Proving for Verification: The Early Days</i> (Keynote) – J Strother Moore	18
Interpolants from Z3 Proofs – Kenneth Mcmillan	19
Effective Word-Level Interpolation for Software Verification – Alberto Griggio	28
Accelerating MUS Extraction with Recursive Model Rotation (Short Paper) – Anton Belov and Joao Marques-Silva	37
Pseudo-Boolean Solving by Incremental Translation to SAT (Short Paper) – Panagiotis Manolios and Vasilis Papavasileiou	41
Automated Specification Analysis Using an Interactive Theorem Prover – Harsh Raju Chamarthi and Panagiotis Manolios	46
Proving and Explaining the Unfeasibility of Message Sequence Charts for Hybrid Systems – Alessandro Cimatti, Sergio Mover and Stefano Tonetta	54
Post-Silicon Fault Localisation Using Maximum Satisfiability and Backbones (Short Paper) – Charlie Shucheng Zhu, Georg Weissenbacher and Sharad Malik	63
Algebraic Approach to Arithmetic Design Verification (Short Paper) – Mohamed Basith, Tariq Ahmad, Andre Rossi and Maciej Ciesielski	67
Time-Bounded Analysis of Real-Time Systems – Sagar Chaki, Arie Gurfinkel and Ofer Strichman	72
Timing Analysis of Interrupt-Driven Programs under Context Bounds – Jonathan Kotker, Dorsa Sadigh and Sanjit A. Seshia	81
Automated Error Localization and Correction for Imperative Programs – Robert Koenighofer and Roderick Bloem	91
Optimal Redundancy Removal without Fixedpoint Computation – Mike Case, Jason Baumgartner, Hari Mony and Bob Kanzelman	101

Approximate Reachability With Combined Symbolic And Ternary Simulation – Michael Case, Jason Baumgartner, Hari Mony and Robert Kanzelman	109
Learning Conditional Abstractions – Bryan Brady, Randal Bryant and Sanjit A. Seshia	116
Efficient Implementation of Property Directed Reachability – Niklas Een, Alan Mishchenko and Robert Brayton	125
Incremental Formal Verification of Hardware – Hana Chockler, Alexander Ivrii, Arie Matsliah, Shiri Moran and Ziv Nevo	135
An Incremental Approach to Model Checking Progress Properties – Aaron Bradley, Fabio Somenzi, Zyad Hassan and Yan Zhang	144
Hardware Model Checking: Status, Challenges, and Opportunities (Discussion Panel) – Muralidhar Talupur	154
Realtime Regular Expressions for Analog and Mixed-Signal Assertions – John Havlicek and Scott Little	155
Formal Analysis of Fractional Order Systems in HOL – Umair Siddique and Osman Hasan	163
Static Scheduling of Latency Insensitive Designs with Lucy-n (Short Paper) – Louis Mandel, Florence Plateau and Marc Pouzet	171
A Theory of Abstraction for Arrays – Steven German	176
Parameterized Verification of Deadlock Freedom in Symmetric Cache Coherence Protocols – Brad Bingham, Jesse Bingham and Mark Greenstreet	186
Scaling Probabilistic Timing Verification of Hardware Using Abstractions in Design Source Code – Jayanand Asok Kumar, Lingyi Liu and Shobha Vasudevan	196
Pervasive Formal Verification in Control System Design (Discussion Panel) – Lee Pike	206
Hybrid Verification of a Hardware Modular Reduction Engine – Jun Sawada, Peter Sandon, Viresh Paruthi, Jason Baumgartner, Michael Case and Hari Mony	207
Desynchronization: Design For Verification – Sudarshan Srinivasan and Raj Katti	215
Hunting deadlocks efficiently in microarchitectural models of communication fabrics – Freek Verbeek and Julien Schmaltz	223
Author Index	232