

2013 Formal Methods in Computer-Aided Design

(FMCAD 2013)

**Portland, Oregon, USA
20-23 October 2013**



**IEEE Catalog Number: CFP13FMC-POD
ISBN: 978-1-4799-2684-8**

Table of Contents

Preface	iv
<i>Barbara Jobstmann, Sandip Ray</i>	
Conference Organization	v
<i>Tutorials</i>	
Syntax-Guided Synthesis	1
<i>Rajeev Alur, Rastislav Bodik, Garvit Juniwal, Milo M. K. Martin, Mukund Raghothaman, Sanjit A. Seshia, Rishabh Singh, Armando Solar-Lezama, Emina Torlak, Abhishek Udupa</i>	
Network Programming in Frenetic	9
<i>Nate Foster, Arjun Guha, Mark Reitblatt, Cole Schlesinger</i>	
Firmware Validation: Challenges and Opportunities	11
<i>Jim Grundy</i>	
Secure Programs via Game-based Synthesis	12
<i>Somesh Jha, Tom Reps, Bill Harris</i>	
<i>Keynotes and Special Events</i>	
Using Process Modeling and Analysis Techniques to Reduce Errors in Healthcare	14
<i>Lori A. Clarke</i>	
Static Verification Based Signoff - A Key Enabler for Managing Verification Complexity in the Modern SoC	15
<i>Pranav Ashar</i>	
Student Forum	16
<i>Thomas Wahl</i>	
Panel	17
<i>Panagiotis Manolios</i>	
<i>Session 1: Synthesis</i>	
Distributed Synthesis for LTL Fragments	18
<i>Krishnendu Chatterjee, Thomas Henzinger, Jan Otop and Andreas Pavlogiannis</i>	
Counter-Strategy Guided Refinement of GR(1) Temporal Logic Specifications	26
<i>Rajeev Alur, Salar Moarref and Ufuk Topcu</i>	
Efficient Handling of Obligation Constraints in Synthesis from Omega-Regular Specifications	34
<i>Saqib Sohail and Fabio Somenzi</i>	

On the Feasibility of Automation for Bandwidth Allocation Problems in Data Centers	42
<i>Yifei Yuan, Anduo Wang, Rajeev Alur and Boon Loo</i>	

Session 2: Decision Procedure Enhancements

Computing prime implicants	46
<i>David Deharbe, Pascal Fontaine, Daniel Le Berre and Bertrand Mazure</i>	
A Circuit Approach to LTL Model Checking.....	53
<i>Niklas Een, Baruch Sterin and Koen Claessen</i>	
Invariants for Finite Instances and Beyond	61
<i>Sylvain Conchon, Amit Goel, Sava Krstic, Alain Mebsout and Fatiha Zaidi</i>	

Session 3: Interpolation, Quantifier Elimination, Synthesis

Exploring Interpolants	69
<i>Philipp Ruemmer and Pavle Subotic</i>	
Synthesizing Multiple Boolean Functions using Interpolation on a Single Proof.....	77
<i>Georg Hofferek, Ashutosh Gupta, Bettina Könighofer, Jie-Hong Roland Jiang and Roderick Bloem</i>	
Quantifier Elimination via Clause Redundancy	85
<i>Eugene Goldberg and Panagiotis Manolios</i>	
Interpolation for Synthesis on Unbounded Domains.....	93
<i>Viktor Kuncak and Régis Blanc</i>	

Session 4: Verification of Digital, Hybrid, and Analog Systems

Relational STE and Theorem Proving for Formal Verification of Industrial Circuit Designs	97
<i>John O'Leary, Roope Kaivola and Tom Melham</i>	
Satisfiability Modulo ODEs	105
<i>Sicun Gao, Soonho Kong and Edmund Clarke</i>	
Verifying Global Convergence for a Digital Phase-Locked Loop.....	113
<i>Jijie Wei, Mark Greenstreet, Yan Peng and Ge Yu</i>	

Session 5: Embedded Software Verification

Formal Co-Validation of Low-Level Hardware/Software Interfaces	121
<i>Alex Horn, Michael Tautschnig, Celina Val, Lihao Liang, Tom Melham, Jim Grundy and Daniel Kroening</i>	
An SMT Based Method for Optimizing Arithmetic Computations in Embedded Software Code	129
<i>Hassan Eldib and Chao Wang</i>	
Verifying Periodic Programs with Priority Inheritance Locks	137
<i>Sagar Chaki, Arie Gurfinkel and Ofer Strichman</i>	

Abstractions for Model Checking SDN Controllers.....	145
<i>Divyot Sethi, Srinivas Narayana and Sharad Malik</i>	
Session 6: IC3 and Debugging	
Efficient Modular SAT Solving for IC3.....	149
<i>Sam Bayless, Celina Val, Thomas Ball, Holger Hoos and Alan Hu</i>	
Better Generalization in IC3.....	157
<i>Zyad Hassan, Aaron Bradley and Fabio Somenzi</i>	
Parameter Synthesis with IC3.....	165
<i>Alessandro Cimatti, Alberto Griggio, Sergio Mover and Stefano Tonetta</i>	
Generalized Counter-Examples to Liveness Properties.....	169
<i>Gadi Aleksandrowicz, Jason Baumgartner, Alexander Ivrii and Ziv Nevo</i>	
Session 7: SAT/SMT	
The Design and Implementation of the Model Constructing Satisfiability Calculus.....	173
<i>Dejan Jovanović, Clark Barrett and Leonardo De Moura</i>	
Trimming while Checking Clausal Proofs.....	181
<i>Marijn Heule, Warren Hunt and Nathan Wetzler</i>	
Sum of Infeasibility Simplex for SMT.....	189
<i>Timothy King, Clark Barrett and Bruno Dutertre</i>	
Efficient MUS Extraction with Resolution.....	197
<i>Alexander Nadel, Vadim Ryvchin and Ofer Strichman</i>	
Session 8: Software Verification	
Parameterized Model Checking of Fault-tolerant Distributed Algorithms by Abstraction.....	201
<i>Annu John, Igor Konnov, Ulrich Schmid, Helmut Veith and Josef Widder</i>	
Verifying Multithreaded Software with Impact.....	210
<i>Björn Wachter, Daniel Kroening and Joel Ouaknine</i>	
Proving Termination of Imperative Programs Using Max-SMT.....	218
<i>Daniel Larráz, Albert Oliveras, Enric Rodríguez Carbonell and Albert Rubio</i>	
On the Concept of Variable Roles and its Use in Software Analysis (Short Paper).....	226
<i>Yulia Demyanova, Helmut Veith and Florian Zuleger</i>	
Author index.....	251