

2022 Formal Methods in Computer-Aided Design (FMCAD 2022)

**Trento, Italy
17-21 October 2022**



**IEEE Catalog Number: CFP22FMC-POD
ISBN: 978-1-6654-8040-6**

**Copyright © 2022, The FMCAD Association and the authors
All Rights Reserved**

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP22FMC-POD
ISBN (Print-On-Demand):	978-1-6654-8040-6
ISBN (Online):	978-3-85448-053-2
ISSN:	2641-8177

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

Table of Contents

Invited Talks

- The seL4 Verification Journey: How Have the Challenges and Opportunities Evolved 1
June Andronick
- Why Do Things Go Wrong (or Right)? Applications of Causal Reasoning to Verification 2
Hana Chockler

Tutorials

- On Applying Model Checking in Formal Verification 3
Håkan Hjort
- Verification of Distributed Protocols: Decidable Modeling and Invariant Inference 4
Oded Padon

Student Forum

- The FMCAD 2022 Student Forum 5
Matthias Preiner

Verification in Machine Learning

- Proving Robustness of KNN Against Adversarial Data Poisoning 7
Yannan Li, Jingbo Wang and Chao Wang
- On Optimizing Back-Substitution Methods for Neural Network Verification 17
Tom Zelazny, Haoze Wu, Clark Barrett and Guy Katz
- Verification-Aided Deep Ensemble Selection 27
Guy Amir, Tom Zelazny, Guy Katz and Michael Schapira
- Neural Network Verification with Proof Production 38
Omri Isac, Clark Barrett, Min Zhang and Guy Katz

Proofs

- TBUDDY: A Proof-Generating BDD Package 49
Randal Bryant
- Stratified Certification for k-Induction 59
Emily Yu, Nils Frolyeks, Armin Biere and Keijo Heljanko
- Reconstructing Fine-Grained Proofs of Complex Rewrites Using a Domain-Specific Language 65
Andres Noetzli, Haniel Barbosa, Aina Niemetz, Mathias Preiner, Andrew Reynolds, Cesare Tinelli and Clark Barrett
- Small Proofs from Congruence Closure 75
Oliver Flatt, Samuel Coward, Max Willsey, Zachary Tatlock and Pavel Panchekha

Proof-Stitch: Proof Combination for Divide-and-Conquer SAT Solvers	84
<i>Abhishek Nair, Saranyu Chattopadhyay, Haoze Wu, Alex Ozdemir and Clark Barrett</i>	

Hardware and RTL

Reconciling Verified-Circuit Development and Verilog Development	89
<i>Andreas Lööw</i>	
Timed Causal Fanin Analysis for Symbolic Circuit Simulation	99
<i>Roope Kaivola and Neta Bar Kama</i>	
Divider Verification Using Symbolic Computer Algebra and Delayed Don't Care Optimization	108
<i>Alexander Konrad, Christoph Scholl, Alireza Mahzoon, Daniel Große and Rolf Drechsler</i>	
Formally Verified Isolation of DMA	118
<i>Jonas Haglund and Roberto Guanciale</i>	
Foundations and Tools in HOL4 for Analysis of Microarchitectural Out-of-Order Execution	129
<i>Karl Palmskog, Xiaomo Yao, Ning Dong, Roberto Guanciale and Mads Dam</i>	
Synthesizing Instruction Selection Rewrite Rules from RTL using SMT	139
<i>Ross Daly, Caleb Donovan, Jack Melchert, Raj Setaluri, Nestan Tsiskaridze, Priyanka Raina, Clark Barrett and Pat Hanrahan</i>	
Error Correction Code Algorithm and Implementation Verification using Symbolic Representations .	151
<i>Aarti Gupta, Roope Kaivola, Mihir Parang Mehta and Vaibhav Singh</i>	

SAT and SMT

First-Order Subsumption via SAT Solving	160
<i>Jakob Rath, Armin Biere and Laura Kovacs</i>	
BaxMC: a CEGAR approach to MAX#SAT	170
<i>Thomas Vigouroux, Cristian Ene, David Monniaux, Laurent Mounier and Marie-Laure Potet</i>	
Compact Symmetry Breaking for Tournaments	179
<i>Evan Lohn, Chris Lambert and Marijn Heule</i>	
Enumerative Data Types with Constraints	189
<i>Andrew T Walter, David Greve and Panagiotis Manolios</i>	
Reducing NEXP-complete problems to DQBF	199
<i>Fa-Hsun Chen, Shen-Chang Huang, Yu-Cheng Lu and Tony Tan</i>	
INC: A Scalable Incremental Weighted Sampler	205
<i>Suwei Yang, Victor Liang and Kuldeep S. Meel</i>	
Bounded Model Checking for LLVM	214
<i>Siddharth Priya, Xiang Zhou, Yusen Su, Yakir Vizel, Yuyan Bao and Arie Gurfinkel</i>	

Parameterized Systems and Quantified Reasoning

Automatic Repair and Deadlock Detection for Parameterized Systems	225
<i>Swen Jacobs, Mouhammad Sakr and Marcus Völz</i>	
Synthesizing Locally Symmetric Parameterized Protocols from Temporal Specifications	235
<i>Ruoxi Zhang, Richard Trefler and Kedar Namjoshi</i>	

Synthesizing Self-Stabilizing Parameterized Protocols with Unbounded Variables	245
<i>Ali Ebneenasir</i>	
The Rapid Software Verification Framework	255
<i>Pamina Georgiou, Bernhard Gleiss, Ahmed Bhayat, Michael Rawson, Laura Kovacs and Giles Reger</i>	
Distributed Systems	
ACORN: Network Control Plane Abstraction using Route Nondeterminism	261
<i>Divya Raghunathan, Ryan Beckett, Aarti Gupta and David Walker</i>	
Plain and Simple Inductive Invariant Inference for Distributed Protocols in TLA+	273
<i>William Schultz, Ian Dardik and Stavros Tripakis</i>	
Awaiting for Godot: Stateless Model Checking that Avoids Executions where Nothing Happens	284
<i>Bengt Jonsson, Magnus Lång and Kostis Sagonas</i>	
Synthesis	
Synthesizing Transducers from Complex Specifications	294
<i>Anway Grover, Rüdiger Ehlers and Loris D'Antoni</i>	
Synthesis of Semantic Actions in Attribute Grammars	304
<i>Pankaj Kumar Kalita, Miriyala Jeevan Kumar and Subhajit Roy</i>	
Reactive Synthesis Modulo Theories using Abstraction Refinement	315
<i>Benedikt Maderbacher and Roderick Bloem</i>	
Learning Deterministic Finite Automata Decompositions from Examples and Demonstrations	325
<i>Niklas Lauffer, Beyazit Yalcinkaya, Marcell Vazquez-Chanlatte, Ameesh Shah and Sanjit A. Seshia</i>	
Reachability and Safety Verification	
Automated Conversion of Axiomatic to Operational Models: Theoretical and Practical Results	331
<i>Adwait Godbole, Yatin A. Manerkar and Sanjit A. Seshia</i>	
Formally Verified Quite OK Image Format	343
<i>Mario Bucev and Viktor Kunčak</i>	
Split Transition Power Abstraction for Unbounded Safety	349
<i>Martin Blicha, Grigory Fedukovich, Antti Hyvärinen and Natasha Sharygina</i>	
Automating Geometric Proofs of Collision Avoidance with Active Corners	359
<i>Nishant Kheterpal, Elanor Tang and Jean-Baptiste Jeannin</i>	
Differential Testing of Pushdown Reachability with a Formally Verified Oracle	369
<i>Anders Schlichtkrull, Morten Konggaard Schou, Jiri Srba and Dmitriy Traytel</i>	
TriCera: Verifying C Programs Using the Theory of Heaps	380
<i>Zafer Esen and Philipp Ruemmer</i>	