

2024 Formal Methods in Computer-Aided Design (FMCAD 2024)

**Prague, Czech Republic
15-18 October 2024**



**IEEE Catalog Number: CFP24FMC-POD
ISBN: 979-8-3315-2478-4**

**Copyright © 2024, FMCAD Association (and 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:	CFP24FMC-POD
ISBN (Print-On-Demand):	979-8-3315-2478-4
ISBN (Online):	978-3-8544-8065-5
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



Table of Contents

Tutorial

Writing Proofs in Dafny	1
<i>K. Rustan M. Leino</i>	

Invited Talks

Tackling Scalability Issues in Bit-Vector Reasoning	2
<i>Aina Niemetz</i>	
Some Adventures in Learning Proving, Instantiation and Synthesis	3
<i>Josef Urban</i>	
Harnessing SMT Solvers for Reasoning about DeFi Protocols	4
<i>Mooly Sagiv</i>	

Student Forum

The FMCAD 2024 Student Forum	5
<i>Martin Blicha and Nestan Tsiskaridze</i>	

Hardware Model Checking Competition

Hardware Model Checking Competition 2024	7
<i>Armin Biere and Nils Froleys and Mathias Preiner</i>	

SMT Solving and Applications

Efficiently Synthesizing Lowest Cost Rewrite Rules for Instruction Selection	8
<i>Ross Daly, Caleb Donovick, Caleb Terrill, Jackson Melchert, Priyanka Raina, Clark Barrett, and Pat Hanrahan</i>	
Extending DRAT to SMT	18
<i>S Hitarth, Cayden R. Codel, Hanna Lachnitt, and Bruno Dutertre</i>	
Solving String Constraints with Concatenation Using SAT	29
<i>Kevin Lotz, Amit Goel, Bruno Dutertre, Benjamin Kiesl-Reiter, Soonho Kong, and Dirk Nowotka</i>	
SMT-D: New Strategies for Portfolio-Based SMT Solving	39
<i>Clark Barrett, Pei-Wei Chen, Byron Cook, Bruno Dutertre, Robert B. Jones, Nham Le, Andrew Reynolds, Kunal Sheth, and Mike W. Whalen</i>	
Modernizing SMT-Based Type Error Localization	49
<i>Max Kopinsky, Brigitte Pientka, and Xujie Si</i>	

Static Analysis

Context Pruning for More Robust SMT-based Program Verification	59
<i>Yi Zhou, Jay Bosamiya, Jessica Li, Marijn J. H. Heule, and Bryan Parno</i>	
Easter Egg: Equality Reasoning Based on E-Graphs with Multiple Assumptions	70
<i>Eytan Singher and Shachar Itzhaky</i>	
Word Equations as Abstract Domain for String Manipulating Programs	84
<i>Antonina Nepeivoda</i>	

Machine Learning in Verification

Formally Verifying Deep Reinforcement Learning Controllers with Lyapunov Barrier Certificates . . .	95
<i>Udayan Mandal, Guy Amir, Haoze Wu, Ieva Daukantas, Fletcher Lee Newell, Umberto J. Ravaioli, Baoluo Meng, Michael Durling, Milan Ganai, Tobey Shim, Guy Katz, and Clark Barrett</i>	
Leveraging LLMs for Program Verification	107
<i>Adharsh Kamath, Nausheen Mohammed, Aditya Senthilnathan, Saikat Chakraborty, Pantazis Deligiannis, Shuvendu K. Lahiri, Akash Lal, Aseem Rastogi, Subhajit Roy, and Rahul Sharma</i>	
Translating Natural Language to Temporal Logics with Large Language Models and Model Checkers	119
<i>Daniel Mendoza, Christopher Hahn, and Caroline Trippel</i>	

Verification I

Recomposition: A New Technique for Efficient Compositional Verification	130
<i>Ian Dardik, April Porter, and Eunsuk Kang</i>	
Evaluating LLM-driven User-Intent Formalization for Verification-Aware Languages	142
<i>Shuvendu Lahiri</i>	
Towards Verification Modulo Theories of asynchronous systems via abstraction refinement	148
<i>Gianluca Redondi, Alessandro Cimatti, and Alberto Griggio</i>	

Hardware

Semi-open-state testing for in-silicon coherent interconnects	153
<i>Jasmin Schult, Ben Fiedler, David Cock, and Timothy Roscoe</i>	
Memory Consistency Model-Aware Cache Coherence for Heterogeneous Hardware	163
<i>Rachel Cleaveland and Caroline Trippel</i>	

Proofs and Certificates

Translating Pseudo-Boolean Proofs into Boolean Clausal Proofs	175
<i>Karthik Nukala, Soumyaditya Choudhuri, Randal E. Bryant, and Marijn J. H. Heule</i>	
Verified Substitution Redundancy Checking	186
<i>Cayden R. Codel, Jeremy Avigad, and Marijn J. H. Heule</i>	

Satisfiability Solving and Applications

2-DQBF Solving and Certification via Property-Directed Reachability Analysis	197
<i>Long-Hin Fung, Che Cheng, Yu-Wei Fan, Tony Tan, and Jie-Hong Roland Jiang</i>	

Projective Model Counting for IP Addresses in Access Control Policies	208
<i>Loris D’Antoni, Andrew Gacek, Amit Goel, Dejan Jovanović, Rami Gökhan Kıcı, Dan Peebles, Neha Rungta, Yasmine Sharoda, and Chungha Sung</i>	
Toward Exhaustive Sequential Redundancy Removal	217
<i>Rohit Dureja, Jason Baumgartner, Raj Kumar Gajavelly, Robert Kanzelman, and Kristin Y. Rozier</i>	
DAG-Based Compositional Approaches for LTLf to DFA Conversions	227
<i>Yash Kankariya, Yong Li, and Suguman Bansal</i>	
Clausal Equivalence Sweeping	236
<i>Armin Biere, Katalin Fazekas, Mathias Fleury, and Nils Froleyks</i>	
Algorithms and Arithmetic	
Automatic Verification of Right-greedy Numerical Linear Algebra Algorithms	242
<i>Carl Kwan and Warren A. Hunt, Jr.</i>	
Formally Verified Rounding Errors of the Logarithm-Sum-Exponential Function	251
<i>Paul Bonnot, Benoît Boyer, Florian Faissolle, Claude Marché, and Raphaël Rieu-Helft</i>	
Symbolic Computer Algebra for Multipliers Revisited – It’s All About Orders and Phases	261
<i>Alexander Konrad and Christoph Scholl</i>	
Verification II	
Combining Symbolic Execution with Predicate Abstraction and CEGAR	272
<i>Martin Jonáš, Jan Strejček, and Alberto Griggio</i>	
Efficient Synthesis of Symbolic Distributed Protocols by Sketching	281
<i>Derek Egoal, William Schultz, and Stavros Tripakis</i>	
Ownership in low-level intermediate representation	292
<i>Siddharth Priya and Arie Gurfinkel</i>	