

2023 Formal Methods in Computer-Aided Design (FMCAD 2023)

**Ames, Iowa, USA
24-27 October 2023**



**IEEE Catalog Number: CFP23FMC-POD
ISBN: 979-8-3503-4889-7**

**Copyright © 2023, FMCAD Association
All Rights Reserved**

**Copyright for individual papers remains with the authors and is licensed under a
Creative Commons attribution 4.0 international license (CC BY 4.0).
<https://creativecommons.org/licenses/by/4.0/>**

****** 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): | 979-8-3503-4889-7 |
| ISBN (Online): | 978-3-85448-060-0 |
| 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

| | |
|--|---|
| Reasoning about Quantifiers in SMT: The QSMA Algorithm..... | 1 |
| <i>Maria Paola Bonacina</i> | |
| Distribution Testing: The New Frontier for Formal Methods..... | 2 |
| <i>Kuldeep Meel</i> | |
| Formal Methods for Trusted AI..... | 3 |
| <i>Bettina Könighofer</i> | |

Tutorials

| | |
|--|---|
| Developing an Open-Source, State-of-the-Art Symbolic Model-Checking Framework for the Model-Checking Research Community..... | 4 |
| <i>Kristin Y. Rozier, Natarajan Shankar, Cesare Tinelli, Moshe Vardi</i> | |
| MiniZinc for Formal Methods..... | 5 |
| <i>Peter J. Stuckey</i> | |
| Local Search and Its Application in CDCL/CDCL(T) solvers for SAT/SMT..... | 6 |
| <i>Shaowei Cai</i> | |
| NASA's core Flight System Framework Overview..... | 7 |
| <i>David Swartwout</i> | |

Student Forum

| | |
|--|---|
| The FMCAD 2022 Student Forum..... | 8 |
| <i>Mikoláš Janota, Nina Narodytska</i> | |

Neural Networks and Machine Learning

| | |
|---|----|
| Formally Explaining Neural Networks within Reactive Systems..... | 10 |
| <i>Shahaf Bassan, Guy Amir, Davide Corsi, Idan Refaeli, and Guy Katz</i> | |
| Lightweight Online Learning for Sets of Related Problems in Automated Reasoning..... | 23 |
| <i>Haoze Wu, Christopher Hahn, Florian Lonsing, Makai Mann, Raghuram Ramanujan, and Clark Barrett</i> | |
| DelBugV: Delta-Debugging Neural Network Verifiers..... | 34 |
| <i>Raya Elsaleh and Guy Katz</i> | |

Model Checking

| | |
|--|----|
| Towards Compositional Hardware Model Checking Certification..... | 44 |
| <i>Emily Yu, Nils Froylyks, Armin Biere, and Keijo Heljanko</i> | |

| | |
|--|-----|
| Btor2MLIR: A Format and Toolchain for Hardware Verification | 55 |
| <i>Joseph Tafese, Isabel Garcia-Contreras, and Arie Gurfinkel</i> | |
| Data-Driven Learning of Strong Conjunctive Invariants | 64 |
| <i>Arkesh Thakkar and Deepak D’Souza</i> | |
| Automating Cutoff-based Verification of Distributed Protocols | 75 |
| <i>Shreesha G. Bhat and Kartik Nagar</i> | |
| Optimal Bounded Partial Order Reduction | 86 |
| <i>Iason Marmanis and Viktor Vafeiadis</i> | |
| Hardware | |
| Datapath Verification via Word-Level E-Graph Rewriting | 92 |
| <i>Samuel Coward, Emiliano Morini, Bryan Tan, Theo Drane, and George A. Constantinides</i> | |
| μ ArchiFI: Formal Modeling and Verification Strategies for Microarchitectural Fault Injections | 101 |
| <i>Simon Tollec, Mihail Asavoae, Damien Couroussé, Karine Heydemann, and Mathieu Jan</i> | |
| Sylvia: Countering the Path Explosion Problem in the Symbolic Execution of Hardware Designs ... | 110 |
| <i>Kaki Ryan and Cynthia Sturton</i> | |
| Binary decision diagrams on modern hardware | 122 |
| <i>Samuel Pastva and Thomas Henzinger</i> | |
| SAT | |
| Proofs for Incremental SAT with Inprocessing | 132 |
| <i>Benjamin Kiesl-Reiter and Michael W. Whalen</i> | |
| Verified Encodings for SAT Solvers | 141 |
| <i>Cayden R. Codel, Jeremy Avigad, and Marijn J. H. Heule</i> | |
| SAT-Based Quantified Symmetric Minimization of the Reachable States of Distributed Protocols ... | 152 |
| <i>Katalin Fazekas, Aman Goel, and Karem A. Sakallah</i> | |
| BIG Backbones | 162 |
| <i>Nils Froleys, Emily Yu, and Armin Biere</i> | |
| SMT | |
| Local Search For SMT On Linear and Multilinear Real Arithmetic | 168 |
| <i>Bohan Li and Shaowei Cai</i> | |
| Mariposa: Measuring SMT Instability in Automated Program Verification | 178 |
| <i>Yi Zhou, Jay Bosamiya, Yoshiki Takashima, Jessica Li, Marijn J. H. Heule, and Bryan Parno</i> | |
| A Procedure for SyGuS Solution Fitting via Matching and Rewrite Rule Discovery | 189 |
| <i>Abdalrhman Mohamed, Andrew Reynolds, Clark Barrett, and Cesare Tinelli</i> | |
| Partitioning Strategies for Distributed SMT Solving | 199 |
| <i>Amalee Wilson, Andres Noetzli, Andrew Reynolds, Byron Cook, Cesare Tinelli, and Clark Barrett</i> | |

Avionics

- CRV: An Automated Resiliency Reasoner for System Design Models 209
Daniel Larraz, Robert Lorch, Moosa Yahyazadeh, M. Fareed Arif, Omar Chowdhury, and Cesare Tinelli
- Towards a Correct-by-Construction Design of Integrated Modular Avionics 221
Baoluo Meng, Joyanta Debnath, Sarat Chandra Varanasi, Emmanuel Manolios, Michael Durling, Saswata Paul, Daniel Prince, Saif Alsabbagh, Richard Haadsma, Craig McMillan, Chi Zhang, and Tim Oates
- Fortis: A Tool for Analysis and Repair of Robust Software Systems 228
Changjian Zhang, Ian Dardik, Rômulo Meira-Góes, David Garlan, and Eunsuk Kang
- A provably correct floating-point implementation of Well Clear Avionics Concepts 237
Nikson Bernardes Fernandes Ferreira, Mariano M. Moscato, Laura Titolo, and Mauricio Ayala-Rincón

Security and Synthesis

- Formal Verification of Correctness and Information Flow Security for an In-Order Pipelined Processor 247
Ning Dong, Roberto Guanciale, Mads Dam, and Andreas Lööw
- Modular System Synthesis 257
Kanghee Park, Keith J. C. Johnson, Loris D'Antoni, and Thomas Reps
- Modelling and Verification of Security-Oriented Resource Partitioning Schemes 268
Adwait Godbole, Leiqi Ye, Yatin A. Manerkar, and Sanjit A. Seshia

Cyber-Physical Systems

- Lift-off: Trustworthy ARMv8 semantics from formal specifications 274
Kait Lam and Nicholas Coughlin
- Cycle and Commute: Rare-Event Probability Verification for Chemical Reaction Networks 284
Landon Taylor, Bryant Israelsen, and Zhen Zhang
- Conformance Testing for Stochastic Cyber-Physical Systems 294
Xin Qin, Navid Hashemi, Lars Lindemann, Jyotirmoy V. Deshmukh
- MediK: Towards Safe Guideline-based Clinical Decision Support 306
Manasvi Saxena, Shuang Song, and Lui Sha