



Griggio / Rungta (Eds.)

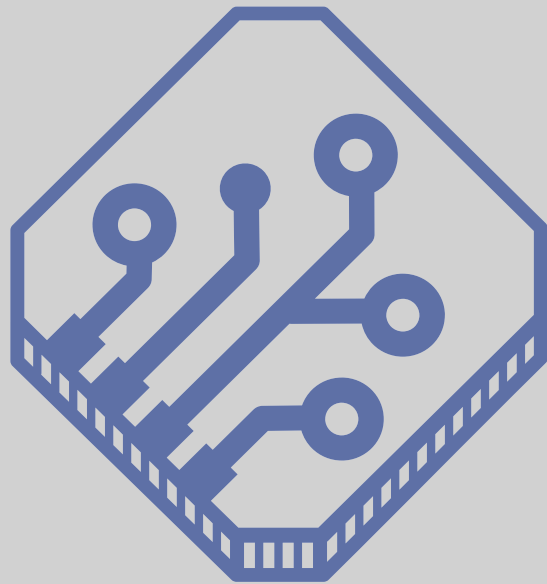
PROCEEDINGS OF THE 22ND CONFERENCE ON FORMAL
METHODS IN COMPUTER-AIDED DESIGN – FMCAD 2022

Alberto Griggio / Neha Rungta (Eds.)

PROCEEDINGS OF THE 22ND CONFERENCE ON FORMAL METHODS IN COMPUTER-AIDED DESIGN – FMCAD 2022



The Conference on Formal Methods in Computer-Aided Design (FMCAD) is an annual conference on the theory and applications of formal methods in hardware and system verification. FMCAD provides a leading forum to researchers in academia and industry for presenting and discussing groundbreaking methods, technologies, theoretical results, and tools for reasoning formally about computing systems. FMCAD covers formal aspects of computer-aided system design including verification, specification, synthesis, and testing.



ISBN 978-3-85448-053-2



www.tuwien.at/academicpress



Alberto Griggio / Neha Rungta (Eds.)
PROCEEDINGS OF THE 22ND CONFERENCE ON FORMAL METHODS IN COMPUTER-AIDED
DESIGN – FMCAD 2022

Conference Series: Formal Methods in Computer-Aided Design

Volume 3

Conference Series: Formal Methods in Computer-Aided Design

Series edited by:

Warren A. Hunt, Jr., The University of Texas at Austin
Austin, TX 78705 | hunt@cs.utexas.edu

Georg Weissenbacher, TU Wien
Karlsplatz 13, 1040 Wien, Austria | georg.weissenbacher@tuwien.ac.at

The Conference on Formal Methods in Computer-Aided Design (FMCAD) is an annual conference on the theory and applications of formal methods in hardware and system verification. FMCAD provides a leading forum to researchers in academia and industry for presenting and discussing groundbreaking methods, technologies, theoretical results, and tools for reasoning formally about computing systems. FMCAD covers formal aspects of computer-aided system design including verification, specification, synthesis, and testing.

Information on this publication series and the volumes published therein is available at www.tuwien.ac.at/academicpress.

Volume 3 edited by:

Alberto Griggio, Fondazione Bruno Kessler
Via Sommarive 18, 38122 Trento, Italy | griggio@fbk.eu

Neha Rungta, Amazon Web Services, Inc.
Seattle, WA, USA | rungta@amazon.com

Alberto Griggio / Neha Rungta (Eds.)

PROCEEDINGS OF THE 22ND CONFERENCE ON FORMAL METHODS IN COMPUTER-AIDED DESIGN – FMCAD 2022

Cite as:

Griggio, A. & Rungta, N. (Eds.). (2022). *Proceedings of the 22nd Conference on Formal Methods in Computer-Aided Design – FMCAD 2022*. TU Wien Academic Press. <https://doi.org/10.34727/2022/isbn.978-3-85448-053-2>

TU Wien Academic Press, 2022

c/o TU Wien Bibliothek
TU Wien
Resselgasse 4, 1040 Wien
academicpress@tuwien.ac.at
www.tuwien.at/academicpress



This work is licensed under a Creative Commons attribution 4.0 international license (CC BY 4.0).
<https://creativecommons.org/licenses/by/4.0/>

ISBN (online): 978-3-85448-053-2
ISSN (online): 2708-7824

Available online: <https://doi.org/10.34727/2022/isbn.978-3-85448-053-2>

Media proprietor: TU Wien, Karlsplatz 13, 1040 Wien
Publisher: TU Wien Academic Press
Publication series editor: Warren A. Hunt, Jr. and Georg Weissenbacher
Editors (responsible for the content): Alberto Griggio and Neha Rungta

Preface

These are the proceedings of the twenty-second International Conference on Formal Methods in Computer-Aided Design (FMCAD), which was held in Trento, Italy from October 18 – October 21, 2022. FMCAD was first held in 1996, and was a bi-annual conference until 2006, when the FMCAD and CHARME conferences merged into a single FMCAD conference, and since then has been held annually. FMCAD 2022 is the twenty-second edition in the series, covering formal aspects of computer-aided system design including verification, specification, synthesis, and testing. It provides a leading forum to researchers in academia and industry to present and discuss groundbreaking methods, technologies, theoretical results, and tools for reasoning formally about computing systems.

The program of FMCAD 2022 consists of two tutorials, two invited talks, a student forum, and the main program consisting of presentations of 40 accepted peer-reviewed papers.

The tutorial day featured two presentations:

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

and the main conference featured two invited talks:

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

FMCAD 2022 received 88 submissions out of which the committee decided to accept 40 for publication. Each submission received at least four reviews. The topics of the accepted papers include hardware and software verification, SAT, SMT, learning, synthesis, neural network verification, and others. Among the accepted papers, there are 31 regular papers (28 long and 3 short) and 9 tool/case study papers (6 long and 3 short).

FMCAD 2022 hosted the tenth edition of the Student Forum, which has been held annually since 2013 and provides a platform for graduate students at any career stage to introduce their research to the FMCAD community. The FMCAD Student Forum 2022 was organized by Mathias Preiner and featured short presentations of 21 accepted contributions. The proceedings provide a detailed description of the Student Forum and lists all accepted contributions.

Organizing this event was made possible by the support of a large number of people and our sponsors. The program committee members and additional reviewers, listed on the following pages, did an excellent job providing detailed and insightful reviews. The reviews helped us build a strong program and helped the authors improve their submissions. We thank each and everyone of them for dedicating their time and providing their expertise. We thank Martin Jonáš for acting both as the web master and as the Sponsorship Chair, and Mathias Preiner for organizing this year's FMCAD Student Forum. We thank Georg Weissenbacher both for his exceptional assistance in organizing the event, communicating to us the decisions of the steering committee, as well as being the publication chair.

Holding a conference like FMCAD would not be feasible without the financial support of our sponsors. We would like to express our gratitude to our sponsors (in alphabetical order): Amazon Web Services, Cadence, Intel, Meta, and Synopsys.

The conference proceedings are available as Open Access Proceedings published by TU Wien Academic Press, and through the IEEE Xplore Digital Library. Last but not least, we thank all authors who submitted their papers to FMCAD 2022 (accepted or not), and whose contributions and presentations form the core of the conference. We are grateful to everyone who presented their paper, gave a keynote or gave a tutorial. We thank all attendees of FMCAD for supporting the conference and making FMCAD an engaging and enjoyable event.

October 2022

Alberto Griggio, Fondazione Bruno Kessler
Neha Rungta, Amazon Web Services, Inc.

Organizing Committee

Program Co-Chairs

Alberto Griggio
Neha Rungta

Fondazione Bruno Kessler, Italy
Amazon Web Services, Inc., CA, USA

Student Forum Chair

Mathias Preiner

Stanford University, CA, USA

Sponsorship and Web Chair

Martin Jonáš

Fondazione Bruno Kessler, Italy

Local Organization

Isabella Masè
Annalisa Armani

Fondazione Bruno Kessler, Italy
Fondazione Bruno Kessler, Italy

Publication Chair

Georg Weissenbacher

TU Wien, Austria

FMCAD Steering Committee

Clark Barrett
Armin Biere
Ruzica Piskac
Anna Slobodova
Georg Weissenbacher

Stanford University, CA, USA
University of Freiburg, Germany
Yale University, CT, USA
Intel Corporation, TX, USA
TU Wien, Austria

Program Committees

FMCAD 2022 Program Committee

Erika Abraham	RWTH Aachen University
Josh Berdine	Meta
Per Bjesse	Synopsys, Inc.
Nikolaj Bjørner	Microsoft
Roderick Bloem	Graz University of Technology
Supratik Chakraborty	IIT Bombay
Sylvain Conchon	Universite Paris-Sud
Vijay D'Silva	Google
Rayna Dimitrova	CISPA Helmholtz Center for Information Security
Rohit Dureja	IBM Corporation
Grigory Fedyukovich	Florida State University
Arie Gurfinkel	University of Waterloo
Fei He	Tsinghua University
Ahmed Irfan	Amazon Web Services
Alexander Ivrii	IBM
Barbara Jobstmann	EPFL and Cadence Design Systems
Tim King	Google
Kuldeep S. Meel	National University of Singapore
Sergio Mover	Ecole Polytechnique
Alexander Nadel	Intel
Aina Niemetz	Stanford University
Elizabeth Polgreen	University of California, Berkeley
Rahul Purandare	Indraprastha Institute of Information Technology Delhi
Andrew Reynolds	University of Iowa
Marco Roveri	University of Trento
Kristin Yvonne Rozier	Iowa State University
Philipp Ruemmer	University of Regensburg
Christoph Scholl	University of Freiburg
Natasha Sharygina	Università della Svizzera Italiana
Elena Sherman	Boise State University
Sharon Shoham	Tel Aviv University
Anna Slobodova	Intel
Christoph Stickel	The MathWorks
Michael Tautschnig	Queen Mary University of London
Nestan Tsiskaridze	Stanford University
Yakir Vizel	The Technion
Georg Weissenbacher	TU Wien
Michael Whalen	Amazon Web Services

FMCAD 2022 Student Forum Committee

Armin Biere	University of Freiburg
Martin Blicha	University of Lugano
Rayna Dimitrova	CISPA Helmholtz Center for Information Security
Rohit Dureja	IBM Corporation
Mathias Fleury	University of Freiburg
Aman Goel	Amazon Web Services
Stéphane Graham-Lengrand	SRI International
Antti Hyvärinen	Università della Svizzera Italiana
Ahmed Irfan	Amazon Web Services
Martin Jonáš	Fondazione Bruno Kessler, Italy
Daniela Kaufmann	Software Competence Center Hagenberg
Daniel Larraz	University of Iowa
Makai Mann	MIT Lincoln Laboratory
Alexander Nadel	Intel
Nina Narodytska	VMware Research
Andres Noetzli	Stanford University
Mark Santolucito	Barnard College
Nestan Tsiskaridze	Stanford University
Tom van Dijk	University of Twente
Florian Zuleger	TU Wien

Additional Reviewers

Andraus, Zaher
Asadi, Sepideh

Barrett, Clark
Becchi, Anna
Biere, Armin
Blich, Martin
Bourgeat, Thomas
Britikov, Konstantin

Cano, Filip

De Masellis, Riccardo
Debrestian, Darin

Eiers, William
Esen, Zafer

Fan, Hongyu
Fazekas, Katalin
Feldman, Yotam M. Y.
Fleury, Mathias

Gamboa Guzman, Laura P.
Garcia-Contreras, Isabel
Geatti, Luca
Gidon, Ernst
Goel, Aman
Golia, Priyanka

Hadarean, Liana
Hadzic, Vedad
Hamza, Ameer
Hamza, Jad
Hyvärinen, Antti

Itzhaky, Shachar

Jain, Himanshu
Jain, Mitesh
Johannsen, Chris
Jovanović, Dejan
Junges, Sebastian

Kaivola, Roope
Kapoor, Ashish
Kaufmann, Daniela
Khasidashvili, Zurab
Koenig, Jason
Könighofer, Bettina
Korneva, Alexandrina
Kroening, Daniel
Kuncak, Viktor

Larrauri, Alberto
Larraz, Daniel
Leslie-Hurd, Joe
Liang, Chencheng
Lonsing, Florian
Luppen, Zachary

Maderbacher, Benedikt
Magnago, Enrico
Martins, Ruben
Mohajerani, Sahar
Mony, Hari
Mora, Federico

O’Leary, John
Otoni, Rodrigo

Parsert, Julian
Peled, Doron
Prabhu, Sumanth
Preiner, Mathias
Priya, Siddharth

Rao, Vikas
Rappaport, Omer
Riley, Daniel
Rosner, Nicolás

Soos, Mate
Sosnovich, Adi
Strichman, Ofer
Su, Yusen
Sumners, Rob
Swords, Sol

Torfah, Hazem

Vediramana Krishnan,
Hari Govind

Weiss, Gail

Yu, Qianshan

Zohar, Yoni
Zuleger, Florian

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 Völpl</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>	