CONFERENCE SERIES: FORMAL METHODS IN COMPUTER-AIDED DESIGN 5

Nina Narodytska / Philipp Rümmer (Eds.)

PROCEEDINGS OF THE 24TH CONFERENCE ON FORMAL METHODS IN COMPUTER-AIDED DESIGN – FMCAD 2024

TU WIEN Academic Press

fmcad.24

Nina Narodytska / Philipp Rümmer (Eds.)
PROCEEDINGS OF THE 24TH CONFERENCE ON FORMAL METHODS IN COMPUTER-AIDED DESIGN – FMCAD 2024

Conference Series: Formal Methods in Computer-Aided Design
Volume 5

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 Vienna, 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 4 edited by:
Nina Narodytska, VMware by Broadcom, Palo Alto, USA | n.narodytska@gmail.com
Philipp Rümmer, University of Regensburg, Germany and Uppsala University, Sweden | philipp.ruemmer@ur.de

Nina Narodytska / Philipp Rümmer (Eds.)

PROCEEDINGS OF THE 24TH CONFERENCE ON FORMAL METHODS IN COMPUTER-AIDED DESIGN – FMCAD 2024

TU WIEN Academic Press

Cite as:
Narodytska, N., & Rümmer, P. (Eds.). (2024). *Proceedings of the 24th Conference on Formal Methods in Computer-Aided Design – FMCAD 2024*. TU Wien Academic Press. https://doi.org/10.34727/2024/isbn.978-3-85448-065-5

TU Wien Academic Press, 2024

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

ISBN (online): 978-3-85448-065-5
ISSN (online): 2708-7824

Available online: https://doi.org/10.34727/2024/isbn.978-3-85448-065-5

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): Nina Narodytska and Philipp Rümmer

Preface

These are the proceedings of the twenty-fourth International Conference on Formal Methods in Computer-Aided Design (FMCAD), which was held in Prague, Czech Republic, October 14–18, 2024. The first FMCAD was organized in 1996, and FMCAD was a bi-annual conference until 2006, when the FMCAD and CHARME conferences merged into a single FMCAD. Since then, FMCAD has been an annual event. FMCAD 2024 was the twenty-fourth edition in the series, covering formal aspects of computer-aided system design including verification, specification, synthesis, and testing. It provided 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 2024 consisted of one tutorial, three invited talks, the presentation of the Hardware Model Checking Competition HWMCC'24, a student forum, and the main program consisting of presentations of 29 accepted peer-reviewed papers. FMCAD 2024 was co-located with the VSTTE 2024 conference, when took place on October 14–15.

The joint VSTTE/FMCAD tutorial day (October 15) featured two tutorials:

- The VSTTE tutorial: *The Lean Programming Language and Theorem Prover,* given by Sebastian Ullrich and Joachim Breitner;
- The FMCAD tutorial: *Writing proofs in Dafny,* given by Rustan Leino.

The main FMCAD conference (October 16–18) featured three invited talks:

- *Tackling Scalability Issues in Bit-Vector Reasoning* by Aina Niemetz;
- *Some Adventures in Learning Proving, Instantiation and Synthesis* by Josef Urban;
- *Harnessing SMT Solvers for Reasoning about DeFi Protocols* by Mooly Sagiv.

FMCAD 2024 received 56 submissions, out of which the committee decided to accept 29 for publication. Each submission received at least four reviews. The topics of the accepted papers include machine learning, model checking, hardware and software validation, SAT&SMT solving and proofs generation. Among the accepted papers, there are 26 regular papers (23 long and 3 short) and 3 tool/case study papers (all short). FMCAD 2024 hosted the twelfth edition of the FMCAD 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 2024 was organized by Martin Blicha and Nestan Tsiskaridze and featured short presentations of 23 accepted contributions. The proceedings provide a detailed description of the Student Forum and lists all accepted contributions.

FMCAD 2024 was made possible by the support of a large number of people, as well as 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 would like to thank the local organization chair, Mikoláš Janota, and the registration chair, Milena Zeithamlová, who did an amazing job taking care of the organization and all practical matters. We thank our web master Julie Cailler, our sponsorship chair Guy Amir, and the Student Forum organizers Martin Blicha and Nestan Tsiskaridze. We thank the organizers of the HWMCC competition, Armin Biere, Nils Froleyks, and Mathias Preiner. 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 the sponsors, given here in alphabetical order: AWS, Cadence, General Electric Aerospace, Intel, NSF, Toyota, and VMware by Broadcom.

Last but not least, we thank all authors who submitted their papers to FMCAD 2024, and whose contributions and presentations form the core of the conference. The conference proceedings are available as Open Access Proceedings published by TU Wien Academic Press, and through the IEEE Xplore Digital Library.

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 2024

Nina Narodytska VMware by Broadcom, USA
Philipp Rümmer University of Regensburg, Germany and Uppsala University, Sweden

Organizing Committee

Program Co-Chairs

Nina Narodytska	VMware Research by Broadcom, CA, USA
Philipp Rümmer	University of Regensburg, Germany, and Uppsala University, Sweden

Local Organization Chair

Mikoláš Janota	Czech Technical University in Prague, Czech Republic

Registration Chair

Milena Zeithamlová	Action M Agency, Prague, Czech Republic

Student Forum Chairs

Martin Blicha	Università della Svizzera italiana, Switzerland
Nestan Tsiskaridze	Stanford University, CA, USA

Sponsorship Chair

Guy Amir	Cornell University, NY, USA

Web Chair

Julie Cailler	University of Regensburg, Germany

Publication Chair

Georg Weissenbacher	TU Wien, Austria

FMCAD Steering Committee

Clark Barrett	Stanford University, CA, USA
Armin Biere	University of Freiburg, Germany
Ruzica Piskac	Yale University, CT, USA
Anna Slobodova	Intel Corporation, TX, USA
Georg Weissenbacher	TU Wien, Austria

Board of the FMCAD Association

Armin Biere	University of Freiburg, Germany
Roderick Bloem	Graz University of Technology, Austria
Georg Weissenbacher	TU Wien, Austria
Florian Zuleger	TU Wien, Austria

Program Committee

FMCAD 2024 Program Committee

Nina Narodytska (co-chair)	VMware Research by Broadcom
Philipp Rümmer (co-chair)	University of Regensburg
Guy Amir	Cornell University
Mohamed Faouzi Atig	Uppsala University
Jaroslav Bendík	Certora
Armin Biere	University of Freiburg
Per Bjesse	Synopsys Inc.
Nikolaj Bjørner	Microsoft
Roderick Bloem	Graz University of Technology
Shaowei Cai	Chinese Academy of Sciences
Rayna Dimitrova	CISPA Helmholtz Center for Information Security
Rohit Dureja	Advanced Micro Devices, Inc.
Gabriel Ebner	Microsoft Research
Grigory Fedyukovich	Florida State University
Alberto Griggio	Fondazione Bruno Kessler
Arie Gurfinkel	University of Waterloo
Liana Hadarean	Amazon Web Services
William Harrison	Idaho National Laboratory
Bo-Yuan Huang	Intel Corporation
William Hung	Cadence
Warren Hunt	The University of Texas at Austin
Ahmed Irfan	SRI International
Mikoláš Janota	Czech Technical University in Prague
Daniela Kaufmann	TU Wien
Tim King	Google
Anna Lukina	TU Delft
Andreas Lööw	Imperial College London
Ravi Mangal	Colorado State University
Ken McMillan	UT Austin
Baoluo Meng	GE Aerospace Research
David Monniaux	CNRS / VERIMAG
Alexander Nadel	Technion & Intel
Ruzica Piskac	Yale University
Mathias Preiner	Stanford University
Mohammad Rahmani Fadiheh	Stanford University
Andrew Reynolds	University of Iowa
Kristin Yvonne Rozier	Iowa State University
Christoph Scholl	University of Freiburg
Natasha Sharygina	University of Lugano, Switzerland
Aditya A. Shrotri	Siemens Digital Industries Software
Carsten Sinz	Karlsruhe University of Applied Sciences
Christoph Sticksel	The MathWorks

Martin Suda	Czech Technical University in Prague
Tachio Terauchi	Waseda University
Yakir Vizel	The Technion
Tomáš Vojnar	Brno University of Technology
Mike Whalen	AWS
Thomas Wies	New York University
Hongce Zhang	Hong Kong University of Science and Technology (Guangzhou)
Shufang Zhu	University of Liverpool
Florian Zuleger	TU Wien
Ivana Černá	Masaryk University

FMCAD 2024 Student Forum Committee

Martin Blicha (co-chair)	Università della Svizzera italiana
Nestan Tsiskaridze (co-chair)	Stanford University
Guy Amir	Cornell University
Haniel Barbosa	Universidade Federal de Minas Gerais
Armin Biere	University of Freiburg
Nikolaj Bjørner	Microsoft
William Eiers	Stevens Institute of Technology
Katalin Fazekas	TU Wien
Alberto Griggio	Fondazione Bruno Kessler
Arie Gurfinkel	University of Waterloo
Petra Hozzová	Czech Technical University in Prague
Antti Hyvärinen	Certora
Ahmed Irfan	SRI International
Konstantin Korovin	University of Manchester
Daniel Larraz	University of Iowa
Ondřej Lengál	Brno University of Technology
Alexander Nadel	Technion & Intel
Andres Noetzli	Stanford University
Rodrigo Otoni	Università della Svizzera italiana
Sophie Rain	TU Wien
Mark Santolucito	Barnard College, Columbia University
Christoph Sticksel	The MathWorks
Hari Govind V. K.	University of Waterloo & Microsoft
Yoni Zohar	Bar Ilan University

Additional Reviewers

Barbosa, Haniel
Bogaerts, Bart
Britikov, Konstantin
Brown, Chad

Cailler, Julie
Chadha, Rohit
Chvalovský, Karel

Dewes, Rafael

Esen, Zafer

Fazekas, Katalin
Feng, Jincao
Fleury, Mathias

Gauthier, Thibault
Govind, R

Hamza, Ameer
He, Fei
Herrmann, Roland
Hinnerichs, Tilman
Holík, Lukáš
Hu, Guangyu

Isac, Omri

Kern, Philipp
Kolárik, Tomáš
Konrad, Alexander

Labbaf, Faezeh
Lengal, Ondrej
Li, Elaine
Lipparini, Enrico
Lutz, Sterre

Maderbacher, Benedikt
Mony, Hari

Paul, Saswata

Rao, Vikas
Rebola Pardo, Adrian
Riley, Daniel
Rodriguez, Andoni
Rogalewicz, Adam

Saivasan, Prakash
Seufert, Tobias
Sextl, Florian
Sindoni, Giulia

Temel, Mertcan

Varanasi, Sarat Chandra

Zavalia, Lucas

Table of Contents

Static Analysis

Machine Learning in Verification

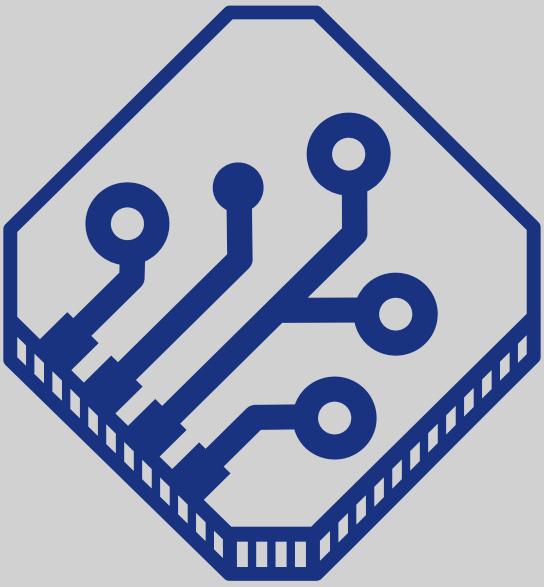
Verification I

Hardware

Proofs and Certificates

Satisfiability Solving and Applications

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 978-3-85448-065-5

9 783854 480655

www.tuwien.at/academicpress