

LNCS 13466

Omri Isac
Radoslav Ivanov
Guy Katz
Nina Narodytska
Laura Nenzi (Eds.)

Software Verification and Formal Methods for ML-Enabled Autonomous Systems

5th International Workshop, FoMLAS 2022
and 15th International Workshop, NSV 2022
Haifa, Israel, July 31 – August 1, and August 11, 2022
Proceedings



Springer

Founding Editors

Gerhard Goos

Karlsruhe Institute of Technology, Karlsruhe, Germany

Juris Hartmanis

Cornell University, Ithaca, NY, USA


Editorial Board Members

Elisa Bertino

Purdue University, West Lafayette, IN, USA

Wen Gao

Peking University, Beijing, China

Bernhard Steffen 

TU Dortmund University, Dortmund, Germany

Moti Yung 

Columbia University, New York, NY, USA

More information about this series at <https://link.springer.com/bookseries/558>

Omri Isac · Radoslav Ivanov · Guy Katz ·
Nina Narodytska · Laura Nenzi (Eds.)

Software Verification and Formal Methods for ML-Enabled Autonomous Systems


5th International Workshop, FoMLAS 2022
and 15th International Workshop, NSV 2022
Haifa, Israel, July 31 – August 1, and August 11, 2022
Proceedings

Editors

Omri Isac
The Hebrew University of Jerusalem
Jerusalem, Israel

Radoslav Ivanov 
Rensselaer Polytechnic Institute
New York, NY, USA

Guy Katz 
The Hebrew University of Jerusalem
Jerusalem, Israel

Nina Narodytska 
VMware Research
Palo Alto, CA, USA

Laura Nenzi 
University of Trieste
Trieste, Italy

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-031-21221-5

ISBN 978-3-031-21222-2 (eBook)

<https://doi.org/10.1007/978-3-031-21222-2>

© The Editor(s) (if applicable) and The Author(s), under exclusive license
to Springer Nature Switzerland AG 2022

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

FoMLAS 2022 Preface

This volume contains the contributed papers presented at the 5th International Workshop on Formal Methods for ML-Enabled Autonomous Systems (FoMLAS 2022), which was held in Haifa (Israel) during July 31 – August 1, 2022. FoMLAS 2022 was co-located with the 34th International Conference on Computer-Aided Verification (CAV 2022).

Machine learning has emerged as a highly effective way for creating real-world software, and is revolutionizing the way complex systems are being designed all across the board. For example, deep learning is being applied to autonomous systems, like autonomous cars and aircraft, achieving exciting results that are beyond the reach of manually created software. However, these significant changes have created new challenges when it comes to explainability, predictability, and correctness of these systems. We believe that a promising avenue for tackling these difficulties is by developing formal methods capable of analyzing and verifying these new kinds of systems.

The FoMLAS workshop is dedicated to the development of novel formal methods techniques to address these challenges. Our mission is to create an international forum for researchers and developers in the field to discuss how formal methods can be used to increase predictability, explainability, and accountability of ML-enabled autonomous systems.

This volume contains eight of the 17 papers presented at FoMLAS 2022. These papers contain original research contributions that have not been published before. Each submission was reviewed by at least two Program Committee members in a XX blind process. The committee decided to accept all papers. This edition of FoMLAS had strong emphasis on the challenges in the verification of neural networks, including scalability and reliability of verification tools for solving these verification problems. These topics were featured both in invited talks and in contributed papers.

The workshop program also featured two invited talks, one by Suman Jana on “Efficient Neural Network Verification using Branch and Bound”, and the second by Mark Müller and Christopher Brix on the results of the “Verification of Neural Networks Competition’ (VNN-COMP’22)”. VNN-COMP’22 was organized by Stanley Bak, Changliu Liu, Taylor T. Johnson, Mark Müller, and Christopher Brix.

August 2022

Omri Isac
Guy Katz
Nina Narodytska

FoMLAS 2022 Organization

Program Committee Chairs

Omri Isac	The Hebrew University of Jerusalem, Israel
Guy Katz	The Hebrew University of Jerusalem, Israel
Nina Narodytska	VMware Research, USA

Program Committee

Clark Barrett	Stanford University, USA
Chih-Hong Cheng	Fraunhofer IKS, Germany
Suman Jana	Columbia University, USA
Susmit Jha	SRI International, USA
Ekaterina Komendantskaya	Heriot-Watt University, UK
Alessio Lomuscio	Imperial College London, UK
Corina Pasareanu	CMU and NASA, USA
Luca Pulina	University of Sassari, Italy
Gagandeep Singh	UIUC, USA
Armando Tacchella	Università di Genova, Italy
Hoang Dung Tran	University of Nebraska-Lincoln, USA
Aleksandar Zeljić	Stanford University, USA
Min Zhang	East China Normal University, China
Yuhao Zhang	University of Wisconsin-Madison, USA
Zhen Zhang	Utah State University, USA

NSV 2022 Preface

This volume contains the contributed papers presented at the 15th International Workshop on Numerical Software Verification (NSV 2022), which was held in Haifa (Israel) on August 11, 2022. NSV 2022 was co-located with the 34th International Conference on Computer-Aided Verification (CAV 2022).

Numerical computations are ubiquitous in digital systems: supervision, prediction, simulation, and signal processing rely heavily on numerical calculus to achieve desired goals. Design and verification of numerical algorithms has a unique set of challenges, which set it apart from the rest of software verification. To achieve the verification and validation of global properties, numerical techniques need to precisely represent local behaviors of each component. The implementation of numerical techniques on modern hardware adds another layer of approximation because of the use of finite representations of infinite precision numbers that usually lack basic arithmetic properties, such as commutativity and associativity. Finally, the development and analysis of cyber-physical systems (CPS), which involve interacting continuous and discrete components, pose a further challenge. It is hence imperative to develop logical and mathematical techniques for the reasoning about programmability and reliability. The NSV workshop is dedicated to the development of such techniques.

This edition of NSV had strong emphasis on the challenges of the verification of cyber-physical systems with machine learning components. This topic was featured both in invited presentations and in contributed papers.

NSV 2022 had very high-profile invited speakers from computer science and from control theory, who gave the following talks:

- Erika Ábrahám (RWTH Aachen University, Germany): “Recent advances for hybrid systems verification with HyPro”
- Jyotirmoy Deshmukh (University of Southern California, USA): “Combining learning-based methods and temporal logic specifications for designing controllers for unknown environments”
- Jana Tumova (KTH Royal Institute of Technology, Sweden): “Motion planning with temporal logic constraints and preferences environments”
- Georgios Fainekos (Toyota North America, USA): “Statistical Verification of Hyperproperties for Cyber-Physical Systems”

Regarding the contributed papers, NSV 2022 received four submissions, each of which received two or three XX blind reviews, and three were accepted. We would like to thank the NSV Steering Committee, in particular Sergiy Bogomolov, for giving us the opportunity to organize NSV 2022.

July 2022

Radoslav Ivanov
Lauraenzi

NSV 2022 Organization

Program Committee Chairs

Laura Nenzi	University of Trieste, Italy
Radoslav Ivanov	Rensselaer Polytechnic Institute, USA

Steering Committee

Sergiy Bogomolov	Newcastle University, UK
Radu Grosu	TU Vienna, Austria
Matthieu Martel	Université de Perpignan, France
Pavithra Prabhakar	Kansas State University, USA
Sriram Sankaranarayanan	UC Boulder, USA

Program Committee

Xin Chen	University of Dayton, USA
Souradeep Dutta	University of Pennsylvania, USA
Ylies Falcone	Université Grenoble Alpes, CNRS, Inria, France
Taylor T Johnson	Vanderbilt University, USA
Michele Loreti	University of Camerino, Italy
Anna Lukina	TU Delft, The Netherlands
Nicola Paoletti	Royal Holloway, University of London, UK
Tatjana Petrov	University of Konstanz, Germany
Yasser Shoukry	University of California, Irvine, USA
Miriam Garcia Soto	IST Austria, Austria
Sadegh Soudjani	Newcastle University, UK
Hoang-Dung Tran	Vanderbilt University, USA
Tichakorn (Nok) Wongpiromsarn	Iowa State University, USA
Huafeng Yu	TOYOTA InfoTechnology Center, USA
Paolo Zuliani	Newcastle University, UK

Contents

FoMLAS 2022

VPN: Verification of Poisoning in Neural Networks	3
<i>Youcheng Sun, Muhammad Usman, Divya Gopinath, and Corina S. Păsăreanu</i>	
A Cascade of Checkers for Run-time Certification of Local Robustness	15
<i>Ravi Mangal and Corina Păsăreanu</i>	
CEG4N: Counter-Example Guided Neural Network Quantization Refinement	29
<i>João Batista P. Matos Jr., Iury Bessa, Edoardo Manino, Xidan Song, and Lucas C. Cordeiro</i>	
Minimal Multi-Layer Modifications of Deep Neural Networks	46
<i>Idan Rejaeli and Guy Katz</i>	
Differentiable Logics for Neural Network Training and Verification	67
<i>Natalia Ślusarz, Ekaterina Komendantskaya, Matthew L. Daggitt, and Robert Stewart</i>	
Neural Networks in Imandra: Matrix Representation as a Verification Choice	78
<i>Remi Desmartin, Grant Passmore, and Ekaterina Kommendantskaya</i>	
Self-correcting Neural Networks for Safe Classification	96
<i>Klas Leino, Aymeric Fromherz, Ravi Mangal, Matt Fredrikson, Bryan Parno, and Corina Păsăreanu</i>	
Formal Specification for Learning-Enabled Autonomous Systems	131
<i>Saddek Bensalem, Chih-Hong Cheng, Xiaowei Huang, Panagiotis Katsaros, Adam Molin, Dejan Nickovic, and Doron Peled</i>	

NSV 2022

Verified Numerical Methods for Ordinary Differential Equations	147
<i>Ariel E. Kellison and Andrew W. Appel</i>	
Neural Network Precision Tuning Using Stochastic Arithmetic	164
<i>Quentin Ferro, Stef Graillat, Thibault Hilaire, Fabienne Jézéquel, and Basile Lewandowski</i>	

**MLTL Multi-type (MLTLM): A Logic for Reasoning About Signals
of Different Types** 187
*Gokul Hariharan, Brian Kempa, Tichakorn Wongpiromsarn,
Phillip H. Jones, and Kristin Y. Rozier*

Author Index 205