Lecture Notes in Computer Science **11652**

More information about this series at http://www.springer.com/series/7407

Majid Zamani · Damien Zufferey (Eds.)

Numerical Software Verification

12th International Workshop, NSV 2019
New York City, NY, USA, July 13–14, 2019
Proceedings

Springer

Editors
Majid Zamani
University of Colorado Boulder
Boulder, CO, USA

Damien Zufferey
Max Planck Institute
for Software Systems
Kaiserslautern, Germany

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-28422-0 ISBN 978-3-030-28423-7 (eBook)
https://doi.org/10.1007/978-3-030-28423-7

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

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

Preface

The 12th International Workshop on Numerical Software Verification (NSV 2019) was held during July 13–14, 2019, in New York, USA. NSV 2019 was co-located with CAV 2019, the 31st International Conference on Computer-Aided Verification.

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 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 the 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 put more emphasis on the challenges related to the automation of driving tasks. This subject was discussed both by invited speakers (from academia and industry) and in contributed papers.

A highlight of NSV 2019 is the presence of high-profile invited speakers from computer science, control theory, and industry: Calin Belta from Boston University, Karl Henrik Johansson from KTH, Jens Oehlerking from Robert Bosch GmbH, and Martin Rinard from MIT. NSV 2019 also added two tutorials, one given by Susmit Jha from SRI International, and the other one by Ashutosh Trivedi from CU Boulder. Regarding the contributed papers, NSV 2019 had 10 submissions which each received 3 reviews, and 7 of them were accepted.

We would like to thank Denso for sponsoring NSV 2019, the CAV organizers for the local organization and support, and the Steering Committee, in particular Sergiy Bogomolov, for allowing us to organize NSV 2019.

July 2019

Majid Zamani
Damien Zufferey

Organization

Program Committee

Matthias Althoff	Technical University of Munich, Germany
Olivier Bouissou	Mathworks, France
Samuel Coogan	Georgia Institute of Technology, USA
Rémi Delmas	ONERA, France
Sicun Gao	University of California San Diego, USA
Alberto Griggio	Fondazione Bruno Kessler, Italy
Ashutosh Gupta	IIT Bombay, India
Ichiro Hasuo	National Institute of Informatics, Japan
Susmit Jha	SRI International, USA
James Kapinski	Toyota, USA
Soonho Kong	Toyota Research Institute, USA
Jun Liu	University of Waterloo, Canada
Manuel Mazo Jr.	Delft University of Technology, The Netherland
Tatjana Petrov	University of Konstanz, Germany
Ruzica Piskac	Yale University, USA
Sylvie Putot	LIX, Ecole Polytechnique, France
Akshay Rajhans	MathWorks, USA
Stefan Ratschan	Institute of Computer Science, Czech Academy of Sciences, Czech Republic
Matthias Rungger	ABB Corporate Research, Germany
Sadra Sadraddini	MIT, USA
Krishna Shankaranarayanan	IIT Bombay, India
Sadegh Soudjani	Newcastle University, UK
Laura Titolo	National Institute of Aerospace, USA
Ashutosh Trivedi	University of Colorado Boulder, USA
Jana Tumova	KTH Royal Institute of Technology, Sweden
Caterina Urban	Inria, France
Xiang Yin	Shanghai Jiao Tong University, China
Majid Zamani	University of Colorado Boulder, USA
Damien Zufferey	Max Planck Institute for Software Systems, Germany

Abstracts of Invited Talks

Correctness and Optimality for Control Systems

Calin Belta

Boston University, Boston, USA

Abstract. In control theory, complicated dynamics such as systems of (nonlinear) differential equations are mostly controlled to achieve stability. This fundamental property is often linked with optimality, which requires minimization of a certain cost along the trajectories of a stable system. In formal synthesis, simple systems such as finite state transition graphs modeling computer programs or digital circuits are controlled from specifications such as safety, liveness, or richer requirements expressed as formulas of temporal logics. With the development and integration of cyber physical and safety critical systems, there is an increasing need for computational tools for controlling complex systems from rich, temporal logic specifications. In this talk, I will introduce some recent results on the connection between optimal control and formal synthesis. Specifically, I will focus on the following problem: given a cost and a correctness temporal logic specification for a dynamical system, generate an optimal control strategy that satisfies the specification. I will first talk about automata-based methods, in which the dynamics of the system are mapped to a finite abstraction that is then controlled using an automaton corresponding to the specification. I will then focus on optimization-based methods, which rely on mapping the specification and the dynamics to constraints of an optimization problem. I will illustrate the usefulness of these approaches with examples from robotics and traffic control.

Modeling, Control, and Verification of an Automated Transport System

Karl H. Johansson

KTH Royal Institute of Technology, Sweden

Abstract. Freight transportation is of utmost importance for our society. It accounts for a significant amount of all energy consumption and greenhouse gas emissions. In this talk, we will discuss the potential future of road goods transportation and how it can be made more robust and efficient, from the automation of individual long-haulage trucks to the optimisation of fleet management and logistics. Such an integrated transportation system benefits from having trucks travelling together in vehicle platoons. From the reduced air drag, platooning trucks travelling close together can save more than 10% of their fuel consumption. In addition, by automating the driving, it is possible to change driver regulations and thereby increase the efficiency even more. Control and optimization problems on various level of this transportation system will be presented. It will be argued that a system architecture utilising vehicle-to-vehicle and vehicle-to-infrastructure communication enable robust and safe control of individual trucks as well as optimised vehicle fleet collaborations and new market opportunities. Extensive experiments done on European highways will illustrate system performance and safety requirements. The presentation will mainly be based on joint work over the last ten years with collaborators at KTH and with the truck manufacturers Scania and Volvo.

Formal Methods for Highly Automated Driving Applications

Jens Oehlerking

Robert Bosch GmbH, Stuttgart, Germany

Abstract. In highly automated driving (HAD), the complexity of the environment leads to challenges in perception, planning, and control that go beyond those encountered in classical cyber-physical systems. These include the need to certify systems including artificial neural networks for perception, the need to predict human behavior in complex situations and the need to give safety guarantees without a human driver as a fallback.

Coming from concepts that are heavily used in the design of HAD system, such as criticality metrics, this talk gives perspectives on the applicability of formal methods. Formal methods of interest include hybrid systems, reachability computations, control invariants and the formal analysis of neural networks. Drawing from this discussion, a case is made for new specification languages that are tailored to the domain of autonomous systems.

Contents

Tutorials

Trust, Resilience and Interpretability of AI Models 3
Susmit Jha

Reinforcement Learning and Formal Requirements 26
Fabio Somenzi and Ashutosh Trivedi

Contributed Papers

An Evaluation of Monte-Carlo Tree Search for Property Falsification on Hybrid Flight Control Laws 45
Rémi Delmas, Thomas Loquen, Josep Boada-Bauxell, and Mathieu Carton

Rigorous Continuous Evolution of Uncertain Systems 60
Luca Geretti, Sanja Živanović Gonzalez, Pieter Collins, Davide Bresolin, and Tiziano Villa

Stochastic Local Search for Solving Floating-Point Constraints 76
Shaobo He, Marek Baranowski, and Zvonimir Rakamarić

Evaluating Branching Heuristics in Interval Constraint Propagation for Satisfiability 85
Calvin Huang, Soonho Kong, Sicun Gao, and Damien Zufferey

Approximate Probabilistic Relations for Compositional Abstractions of Stochastic Systems 101
Abolfazl Lavaei, Sadegh Soudjani, and Majid Zamani

Polytopic Trees for Verification of Learning-Based Controllers 110
Sadra Sadraddini, Shen Shen, and Osbert Bastani

Mutant Accuracy Testing for Assessing the Implementation of Numerical Algorithms 128
Ruining (Ray) Wu and Ian M. Mitchell

Author Index 145