Discrete Event Dyn Syst (2017) 27:205–208
DOI 10.1007/s10626-017-0246-9

Guest editorial: special issue on formal methods in control

Necmiye Ozay[1] · Paulo Tabuada[2]

Published online: 20 April 2017

Keywords Formal methods · Control · Synthesis · Verification

1 Introduction

Formal methods are mathematical techniques, originally proposed by the computer science community, to rigorously analyze software systems. In recent years we have witnessed an increase in the use of techniques originating in this area to solve control problems. Similarly, the idea of synthesizing a controller that enforces the desired specifications is becoming an alternative to the verification paradigm prevalent in the formal methods area. There is now a growing body of literature at the intersection of these two disciplines, formal methods and control theory, and the purpose of this special issue is to present the latest developments in this area.

2 Issue at a glance

The call for papers attracted twelve submissions. After a thorough review process, six full papers and two short papers were selected to appear in the special issue. The topics cov-

✉ Necmiye Ozay
necmiye@umich.edu

Paulo Tabuada
tabuada@ucla.edu

[1] Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI, USA

[2] Department of Electrical Engineering, University of California at Los Angeles, Los Angeles, CA, USA

ered include reactive synthesis, abstraction based hierarchical control, synthesis for timed automata, and verification and falsification of linear and hybrid systems.

Reactive synthesis involves the algorithmic generation of systems or controllers that can interact with their environment in the presences of uncontrollable events or adversarial agents. Ehlers et al. compare and contrast supervisory control in discrete event systems and reactive synthesis in formal methods while providing a comprehensive introduction to both topics. They highlight several similarities and differences in the approaches taken by the discrete event systems and the formal methods communities. Schmuck et al. present an algorithm for hierarchical reactive controller synthesis that solves a reactive synthesis problem in a compositional manner. Their modeling formalism provides a means to decompose a reactive synthesis problem into consistent layers of abstractions. They present an example, which involves an autonomous robot in a building environment, demonstrating the scalability of the approach in comparison with a monolithic solution.

Many complex control tasks require discrete (non-smooth) decision making while the underlying dynamics are continuous. A key technique to design and analyze controllers to achieve such complex tasks, in particular those captured by temporal logics, is to create an abstraction of the continuous system to be controlled. The paper by Nilsson et al. proposes a new abstraction structure called augmented finite transition systems that captures transience properties of the underlying dynamics. In addition, they propose an incremental synthesis algorithm, which uses preorders among augmented finite transition systems, for abstraction refinement in order to systematically and adaptively increase the discrete state-space size only when needed based on the specification and dynamics. The paper by Zamani et al. addresses the scalability problem for abstraction based control synthesis for stochastic systems. Instead of discretizing the state-space, they propose to discretize input sequences and characterize several properties of this new type of abstraction. DeCastro et al. address the problem of generating explanations of unrealizability of a high-level mission specification leveraging the information about the abstraction of the dynamics and the assumed behavior of the environment. They further develop a visualization tool to present these unrealizability certificates to a user who can then decide on potential revisions to the specification guided by their algorithm.

Bin Waez et al. revisit the controller synthesis paradigm in the context of timed automata which are finite-state automata equipped with clocks used to describe timing properties of software systems. Through a case study, Bin Waez et al. motivate the use of a variant to timed automata, termed timed process automata, and argue that this model offers two essential features for industrial systems: (i) compositional modeling with reusable designs for different contexts, and (ii) state-space reduction technique. In the context of process timed automata, they show how to reduce the verification of safety and reachability properties to solving timed games. In addition, the authors also discuss the use of compositional reasoning and aggressive abstractions as state-space reduction techniques.

Verification, the task of algorithmically generating correctness certificates, and falsification, the task of automatically identifying bugs, are crucial steps before a safety-critical control system can be deployed. Therefore, scalable verification and falsification techniques are of great potential. The paper by Tran et al. proposes balanced truncation as a means of reducing the dimensionality of high-dimensional linear systems to enable formal verification based on reachability. To this end, they provide methods for the computation of error bounds between the concrete system's output and the reduced-order system's output. These bounds are then used as margins to perform analysis on the reduced order system. The approach is evaluated on a number of computational benchmark problems. The paper by Rawlings and Ydstie focuses on discovering errors in the discrete logic controlling a hybrid plant when the requirements are given in a fragment of computational tree logic containing global safety and existential reachability specifications on the discrete states. For errors in the discrete logic the falsification problem is reduced to a supervisory control problem based on the discrete transition system induced by the discrete states of the overall hybrid system.

Most of the papers also include links to open-source software repositories where the software implementing the proposed algorithms can be accessed.

Acknowledgements The guest editors wish to thank all the authors, for their submissions, and the reviewers, for their timely and careful evaluation of the submitted papers.

Necmiye Ozay received the B.S. degree from Bogazici University, Istanbul in 2004, the M.S. degree from the Pennsylvania State University, University Park in 2006 and the Ph.D. degree from Northeastern University, Boston in 2010, all in electrical engineering. She was a postdoctoral scholar at California Institute of Technology, Pasadena between 2010 and 2013. She is currently an assistant professor of Electrical Engineering and Computer Science, at the University of Michigan, Ann Arbor.

Dr. Ozay's research interests include dynamical systems, control, optimization and formal methods with applications in cyber-physical systems, system identification, verification and validation, and autonomy. Her papers received several awards including an IEEE Control Systems Society Conference on Decision and Control Best Student Paper Award in 2008. She received a DARPA Young Faculty Award in 2014 and an NSF CAREER Award, a NASA Early Career Faculty Award and a DARPA Director's Fellowship in 2016. She is a member of the IEEE and of the IEEE Control Systems Society Technical Committees on Computational Aspects of Control System Design and on Hybrid Systems.

Paulo Tabuada was born in Lisbon, Portugal, one year after the Carnation Revolution. He received his "Licenciatura" degree in Aerospace Engineering from Instituto Superior Tecnico, Lisbon, Portugal in 1998 and his Ph.D. degree in Electrical and Computer Engineering in 2002 from the Institute for Systems and Robotics, a private research institute associated with Instituto Superior Tecnico. Between January 2002 and July 2003 he was a postdoctoral researcher at the University of Pennsylvania. After spending three years at the University of Notre Dame, as an Assistant Professor, he joined the Electrical Engineering Department at the University of California, Los Angeles, where he established and directs the Cyber-Physical Systems Laboratory.

Paulo Tabuada's contributions to cyber-physical systems have been recognized by multiple awards including the NSF CAREER award in 2005, the Donald P. Eckman award in 2009, the George S. Axelby award in 2011, the Antonio Ruberti Prize in 2015, and the grade of fellow awarded by IEEE in 2017. In 2009 he co-chaired the International Conference Hybrid Systems: Computation and Control (HSCC'09) and joined its steering committee in 2015, in 2012 he was program co-chair for the 3rd IFAC Workshop on Distributed Estimation and Control in Networked Systems (NecSys'12), and in 2015 he was program co-chair for the IFAC Conference on Analysis and Design of Hybrid Systems. He also served on the editorial board of the IEEE Embedded Systems Letters and the IEEE Transactions on Automatic Control.