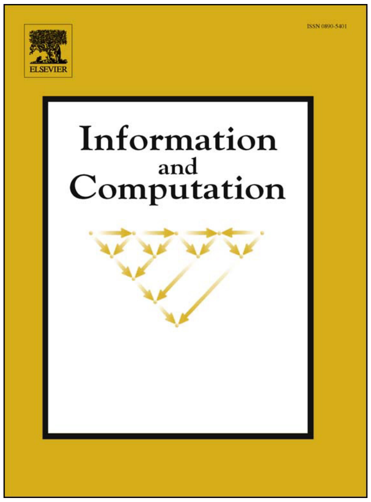

Special Issue: Formal Verification of Cyber-Physical Systems

Luca Geretti, Alessandro Abate, Pierluigi Nuzzo and Tiziano Villa

PII: S0890-5401(22)00134-1
DOI: https://doi.org/10.1016/j.ic.2022.104979
Reference: YINCO 104979

To appear in: *Information and Computation*

Received date: 23 October 2022
Accepted date: 27 October 2022

Please cite this article as: L. Geretti, A. Abate, P. Nuzzo et al., Special Issue: Formal Verification of Cyber-Physical Systems, *Information and Computation*, 104979, doi: https://doi.org/10.1016/j.ic.2022.104979.

Special Issue:
Formal Verification of Cyber-Physical Systems
Preface

Guest Editors:

Luca Geretti[1,3], Alessandro Abate[2], Pierluigi Nuzzo[3], and Tiziano Villa[1]

[1] Università di Verona, Italy, {luca.geretti,tiziano.villa}@univr.it
[2] University of Oxford, UK, alessandro.abate@cs.ox.ac.uk
[3] University of Southern California, CA, USA, {nuzzo,geretti}@usc.edu

In June 2019, a group of leading scholars lectured during a week-long Ph.D. school for researchers, students, and practitioners, which was entitled "Numerical and Symbolic Methods for Reachability Analysis of Hybrid Systems." The event was the Second Summer School on Formal Methods for Cyber-Physical Systems, organized at the University of Verona. The speakers, including the guest editors of this Special Issue, surveyed the field and highlighted future research directions for this area, which provides an enabling technology for the design and verification of cyber-physical systems.

Given the success of the event, the timeliness of the topic, and its growing importance, the lecturers recognized that it would have been of enduring value to prepare a scholarly publication, providing surveys on some of the aspects of the field and updates on the state of the art and open challenges to a larger academic and professional audience. The guest editors were tasked to explore the feasibility of such a publication.

This Special Issue provides an overview of recent contributions to the area of continuous and hybrid system models and methods for the specification and verification of cyber-physical systems. Verification is increasing in importance as a way to enhance design-time and runtime assurance due to the ubiquitous presence of cyber-physical systems that are safety- or mission-critical. A special attention is devoted to reachability analysis techniques, and to the transfer from theory to practice. Hybrid systems are complex dynamical systems that combine discrete and continuous components. As such, they represent a rich model for describing cyber-physical systems. Reachability questions, regarding whether a system can reach a certain subset of its state space, stand at the core of verification problems for hybrid systems.

Several methods have shown to be effective in the verification of hybrid systems based on reachability analysis. Some methods explicitly construct flowpipes that approximate the set of reachable states over time. In that case, proper control of the numerical error is a particularly important aspect, possibly suggesting the use of symbolic representations to achieve efficient and effective computation of the resulting over-approximations. Methods based on satisfiability checking technologies symbolically encode reachability properties as logical formulas, whose solution increasingly requires a combination of Boolean satisfiability solving with numerically-driven decision procedures and optimization methods. On the other hand, automated deduction by means of theorem provers can lead to effective analysis approaches that avoid the numerical criticalities mentioned above. This Special Issue presents different techniques for reachability analysis and verification of hybrid systems, including both deterministic and probabilistic approaches, aiming to also promote synergies among them.

In the following, we offer a short description of the seven contributions.

The paper *Survey on Mining Signal Temporal Logic Specifications* by Dejan Nickovic, Ezio Bartocci, Cristinel Mateis, and Eleonora Nesterini overviews methods for mining Signal Temporal Logic (STL) specifications from cyber-physical system behaviors. Specification mining is the process of learning likely system properties from the observation of the system behaviors and its interactions with the environment; such activity is crucial because formal specifications are only partially (if at all) available. STL is a popular formalism for expressing properties of cyber-physical systems. This survey presents in an intuitive and didactic manner the most influential techniques and aspects of specification mining: template-based vs. template-free, model-based vs. model-free, passive vs. active, and supervised vs. unsupervised learning.

The paper *Parameter Synthesis of Polynomial Dynamical Systems* by Carla Piazza, Alberto Casagrande, Thao Dang, Luca Dorigo, Tommaso Dreossi, and Eleonora Pippia deals with discrete-time parametric polynomial dynamical systems, for which the task of tuning parameters represents a challenge, usually tackled using simulation. This work instead proposes a formal approach driven by an STL specification. It leverages a state representation based on Bernstein polynomials, which have different numerical properties compared to the more common Taylor polynomials. The approach is implemented and tested in the C++ library Sapo, showing results from an epidemiological model and an application to neural networks.

The paper *Recent Developments in Theory and Tool Support for Hybrid Systems Verification with HyPro* by Stephan Schupp, Erika Abraham, and Tristan Ebert focuses on the HyPro C++ library for linear hybrid systems, an effort towards providing different state set representations and allowing them to be easily interchangeable. The features of the library are described, both in terms of data structures and algorithms for efficient handling of reachability analysis for linear hybrid systems.

The paper *Hierarchical Identification of Nonlinear Hybrid Systems in a Bayesian Framework* by Ahmad Madary, Hamid Reza Momeni, Alessandro Abate, and Kim Guldstrand Larsen presents a hierarchical framework for the identification of nonlinear hybrid systems in the form of Switched Nonlinear AutoRegressive models with eXogenous variables (SNARX). The identification is done via three levels of inference, using Bayes' rule. In the first level, model parameters are computed via a Maximum a Posteriori (MAP) estimator. The posterior distribution therein involved depends on hyper-parameters that are tuned in the second level of inference. Such terms determine the model complexity, and the Bayesian framework is key in returning values that trade complexity with accuracy by automatically embodying the Occam's razor principle. Lastly, the third level compares different model structures by means of a quality measure that encompasses data fitness, model complexity, and data classification. The proposed framework is compared with existing relevant methods and is tested on different numerical models, showing promising performance.

The paper *Decomposing Reach Set Computations with Low-Dimensional Sets and High-Dimensional Matrices* by Sergiy Bogomolov, Marcelo Forets, Goran Frehse, Andreas Podelski, and Christian Schilling deals with the problem of scalability for dense- and discrete-time linear time invariant systems with non-deterministic inputs, by decomposing sets while keeping full matrix complexity. The main result is in terms of efficiency, where the authors demonstrate a speedup of two orders of magnitude with respect to non-decomposed solutions, with limited overapproximation error.

The paper *Encoding Inductive Invariants as Barrier Certificates: Synthesis via Difference-of-Convex Programming* by Qiuye Wang, Mingshuai Chen, Bai Xue, Naijun Zhan, and Joost-Pieter Katoen presents a novel condition on barrier certificates, termed the invariant barrier-certificate condition, which witnesses unbounded-time safety of differential dynamical systems and is the weakest possible one to attain inductive invariance. A barrier certificate often serves as an inductive invariant that isolates an unsafe region from the reachable set of states, and hence is widely used in proving safety of hybrid systems, possibly over an infinite time horizon. The authors present a weak completeness result, namely, a barrier certificate is guaranteed to be found (under some mild assumptions) whenever there exists an inductive invariant (in the form of a given template) that suffices to certify safety of the system. Experimental results on benchmarks demonstrate the effectiveness and efficiency of the approach.

The paper *LTL Falsification in Infinite-State Systems* by Alessandro Cimatti, Alberto Griggio, and Enrico Magnago addresses the problem that, differently from finite-state systems, infinite-state systems do not enjoy the property that, if an LTL formula is false, then there is always a counterexample path for it, i.e., a witness, that is ultimately periodic, i.e., in a lasso-shaped form. To circumvent this problem, the authors propose an automatic approach that presents witnesses in an indirect way. The approach is based on two key insights. First, they leverage the notion of well-founded funnel, showing that, under suitable conditions, a sequence of funnels ensures the existence of a fair path. Second, they adopt a compositional approach to partition the original system into projections that result in a non-empty under-approximation of the original system that only contains fair paths. Finally, they describe an algorithm whose implementation outperforms various competitor tools on examples from software, timed, and hybrid systems.

We hope that you will enjoy reading the proposed papers.

We would like to thank all the reviewers: Julien Alexandre Dit Sandretto, Calin Belta, Davide Bresolin, Xin Chen, Parasara Duggirala, Laurent Fribourg, Khalil Ghorbal, Mirko Giacobbe, Taylor Johnson, Dhruva Kartik Mokhasunavisu, Sergio Mover, Ameneh Nejati, Andrea Peruffo, Giordano Pola, Stephan Ratschan, Anna Scampicchio, Guido Sciavicco, Stefan Schupp, Enrico Tronci, Abraham Vinod, Mark Wetzlinger, and Yuriy Zacchia Lun, for their invaluable work in refereeing the contributions.

Finally, we acknowledge the efforts of the Applied Verification for Continuous and Hybrid Systems (ARCH) group,[4] from which many of the collaborations between editors, authors, and reviewers that made this Special Issue possible originated. The group holds an annual friendly competition between verification tools in distinct categories which stimulates collaboration and dissemination of progress from the current state of the art. Two of the guest editors for this Issue act as category leads, namely Luca Geretti for Nonlinear Dynamics and Alessandro Abate for Stochastic Models. Results of the competition are presented, along with contributed scientific papers, in a workshop attached to conferences in the formal verification field.

[4] https://cps-vo.org/group/ARCH

Declaration of interests

☒ The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

☐The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: