AFRL-AFOSR-JP-TR-2022-0020

Compositional Analysis of Autonomous Systems

Xie, Lexing
AUSTRALIAN NATIONAL UNIVERSITY RESEARCH OFFICE ACTON (AUSTRALIA)
10C EAST RD
ACTON, ,
AU

04/24/2022
Final Technical Report

Air Force Research Laboratory
Air Force Office of Scientific Research
Asian Office of Aerospace Research and Development
Unit 45002, APO AP 96338-5002

REPORT DOCUMENTATION PAGE

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE	**2. REPORT TYPE**	**3. DATES COVERED**	
20220424	Final	**START DATE** 20170908	**END DATE** 20210907

4. TITLE AND SUBTITLE
Compositional Analysis of Autonomous Systems

5a. CONTRACT NUMBER	**5b. GRANT NUMBER**	**5c. PROGRAM ELEMENT NUMBER**
FA2386-17-1-4065		61102F
5d. PROJECT NUMBER	**5e. TASK NUMBER**	**5f. WORK UNIT NUMBER**

6. AUTHOR(S)
Lexing Xie

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	**8. PERFORMING ORGANIZATION REPORT NUMBER**
AUSTRALIAN NATIONAL UNIVERSITY RESEARCH OFFICE ACTON (AUSTRALIA) 10C EAST RD ACTON AU	

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSOR/MONITOR'S ACRONYM(S)**	**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**
AOARD UNIT 45002 APO AP 96338-5002	AFRL/AFOSR IOA	AFRL-AFOSR-JP-TR-2022-0020

12. DISTRIBUTION/AVAILABILITY STATEMENT
A Distribution Unlimited: PB Public Release

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Cyber-physical systems (CPS) consist of interacting computational and physical components. Autonomous systems such as autonomous aerial vehicles, cars, trains and factories are prominent examples of CPS. As CPS are becoming continuously larger in size, more complex in functionality, and more safety-critical in their applications, it is vital to guarantee their safety and correctness. This project aims at developing innovative verification techniques to assure safe behavior of cyber-physical systems. Hybrid systems are mathematical models that combine discrete and continuous dynamics, which makes them particularly suitable to model CPS. Although tremendous progress in terms of analysis scalability has been made in the last decade, available hybrid model checkers still lack the scalability to analyze large networked systems, i.e., composite hybrid systems consisting of multiple components. In other words, all available tools do not provide any special treatment for composite systems, whereas industry relevant models, e.g. the ones modelled in MathWorks Simulink, usually consist of multiple components. In this project, we will focus on this problem and develop novel techniques for compositional analysis of hybrid systems, i.e., we will look how to decompose the verification of a system into the verification of its components, which are smaller and therefore easier to verify.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**		
U	U	U	SAR	4

19a. NAME OF RESPONSIBLE PERSON	**19b. PHONE NUMBER** *(Include area code)*
ALAN LIN	227-7009

AOARD Grant FA2386-17-1-4065
Compositional Analysis of Autonomous Systems: Final Report

Sergiy Bogomolov

Newcastle University, UK

Cyber-physical systems (CPS) consist of interacting computational and physical components. This project aims at developing innovative verification techniques to assure safe behaviour of cyber-physical systems. A hybrid system [5] is an expressive mathematical model useful for describing complex dynamic processes involving both continuous and discrete states and their evolution, which makes them particularly suitable to model CPS. In this project, we focus on the development of novel techniques for reachability analysis of hybrid systems, i.e., techniques to automatically explore the state space of a given dynamic system and compute an envelope of system trajectories given boundaries on its uncertain parameters. In order to mitigate the system complexity, we aim at developing compositional methods, i.e. the methods which break the system analysis down to the analysis of its parts. With this overarching goal in mind, our activities within this project can be broadly categorized into the following research thrusts:

Reachability methods for systems featuring linear differential equations. While modern linear algebra packages are efficient for matrices with tens of thousands of dimensions, set-based image computations are limited to a few hundred. In [9], we propose to decompose reach set computations such that set operations are performed in low dimensions, while matrix operations like exponentiation are carried out in the full dimension. Our method is applicable both in dense- and discrete-time settings. For a set of standard benchmarks, it shows a speed-up of up to two orders of magnitude compared to the respective state-of-the-art tools, with only modest losses in accuracy. For the dense-time case, we show an experiment with more than 10,000 variables, roughly two orders of magnitude higher than possible with previous approaches. These algorithms provide a foundation for JuliaReach [10], a toolbox for set-based reachability analysis of dynamical systems. JuliaReach consists of two main packages: Reachability, containing implementations of reachability algorithms for continuous and hybrid systems, and LazySets, a standalone library that implements state-of-the-art algorithms for calculus with convex sets. The library offers both concrete and lazy set representations, where the latter stands for the ability to delay set computations until they are needed. We extend these results in [8] by adding the support of arbitrary-sized partitions and arbitrary low-dimensional set representations. In a related work [11], we extend these results along a different dimension of complexity and namely propose a compositional way to efficiently handle discrete transitions of a hybrid system.

Falsification methods. The falsification of a hybrid system is dual to verification and aims at finding trajectories that violate a given safety property. This is a challenging problem, and the practical applicability of current falsification algorithms still suffers from their high time complexity. In [13], we stive to leverage the power of reachability algorithms we have developed to improve the scalability of falsification techniques. In particular, we start with an existing encoding of the falsificition problem as a nonlinear optimization problem [25], and propose an extension, which reduces the search space of the optimization problem by adding linear state constraints obtained with a reachability algorithm. We showcase the efficiency of our approach on a number of standard hybrid systems benchmarks demonstrating the performance increase in speed and number of falsifiable instances. In [12], we enhance this algorithm by decomposing the nonlinear optimization problem into two simpler optimization problems and solves them in an alternating fashion.

Parallelization methods. As outlined above, reachability analysis techniques are at the core of the current state-of-the-art technology for verifying safety properties of cyber-physical systems. In this thrust, we look at how to scale such techniques by exploiting the powerful parallel multi-core architectures available in modern CPUs. In [18], we address this limitation by presenting for the first time a suite of parallel state-space exploration algorithms that, leveraging multi-core CPUs, enable to scale the reachability analysis for linear

continuous and hybrid automaton models of CPS. To demonstrate the achieved performance speedup on multi-core processors, we provide an empirical evaluation of the proposed parallel algorithms on several benchmarks comparing their key performance indicators.

Koopman operator theory. Reachability analysis of nonlinear dynamical systems is a challenging and computationally expensive task. At the same time, computing the reachable states for linear systems, as discussed above, can often be done efficiently in high dimensions. In [6], we explore verification methods that leverage a connection between these two classes of systems based on the concept of the Koopman operator [23]. The Koopman operator links the behaviors of a nonlinear system to a linear system embedded in a higher dimensional space, with an additional set of so-called observable variables. Although the new dynamical system has linear differential equations, the set of initial states is defined with nonlinear constraints. For this reason, existing approaches for linear systems reachability cannot be used directly. We propose the first reachability algorithm that deals with this unexplored type of reachability problem. Our evaluation examines several optimizations, and shows the proposed workflow is a promising avenue for verifying behaviors of nonlinear systems.

Hybridization methods for reachability analysis. These methods [7] work by approximating nonlinear dynamics with simpler ones (such as constant or affine dynamics). This step makes it possible to leverage the power of existing algorithms for hybrid systems with linear dynamics. In [20], we present improvements to the hybridization approach based on a dynamics scaling model transformation. The transformation aims to reduce the sizes of the linearization domains, and therefore reduces overapproximation error. We showcase the efficiency of our approach on a number of nonlinear benchmark instances.

Online verification. In this research thrust, we aim to apply reachability analysis in the online setting. In other words, we consider a setting where the information provided by reachability analysis is used in real-time to steer the control algorithm of an autonomous system. This in turn imposes particularly tight timing constraints on the efficiency of the performance of reachability analysis. In [14], we propose an approach which utilizes deep neural networks for conservative approximation of reachable sets in bounded time. We provide probabilistic guarantees based on statistical model checking approaches. The approach is evaluated as part of a resilient safety architecture for autonomous vehicles in a simulated environment with several maneuvers. Our evaluation demonstrates that reachability analysis can be done within a fraction of a second and outperforms traditional nonlinear reachability tools by two orders of magnitude. We also propose an alternative approach [1], which performs real-time reachability analysis efficiently by generalizing the computation of barrier certificates [22] to dynamically changing initial conditions and by using the generated safe sets at run-time against previously unknown, possibly time-dependent unsafe sets. These approaches are complemented by [15], where we explore how reachability analysis can be used as part of the model predictive control [17] to support dynamical obstacle avoidance.

Planning via verification. In our earlier work [16], we have made a first step in bridging the gap between the areas of planning and verification of hybrid automata by providing a translation scheme from PDDL+, a formalism to describe planning domains, to hybrid systems. This enables application of model-checking tools in the hybrid planning domain. In this way, we can address PDDL+ domains that are out of the scope of state-of-the-art planners. In this project, we adapt these ideas in [19] to temporal planning, as well as incorporate our approach into a refinement cycle. We also propose an abstraction-based relaxation [21] for reasoning about linear numeric planning problems.

Event-B for hybrid systems. In this line of research, we consider the synergies between Event-B [2] and hybrid systems. Our results in this space include the development of a generic hybrid railway signalling system model [3] which can be further refined to capture a specific railway signalling system. Also, in [4], we present a multifaceted development methodology of cyber-physical systems which is built upon a refinement and proof based modelling language Event-B and its extension for modelling hybrid systems. To improve a low

deductive verification automation of the resulting Event-B models within the methodology, this work describes a novel approach of integrating reachability analysis in the proof process. Furthermore, to provide a more comprehensive cyber-physical system development and simulation-based validation, we describe mechanism for translating cyber-physical systems Event-B models to Simulink.

Random ordinary differential equations (RODEs). As their name suggests, these are ordinary differential equations (ODEs) that contain a stochastic process in their vector field functions. They have been used for many years in a wide range of applications, but have been a shadow existence to stochastic differential equations (SDEs) despite being able to model a wider and often physically more adequate range of disturbances. In [24], we study the safety verification problem over both finite time horizons and the infinite time horizon for RODEs incorporating Wiener processes. In more detail, we investigate the p-safety problem, where we identify the set of initial states from which the probability to satisfy safety specifications is at least p. Based on identifying a set of sample paths whose probability measure is larger than p, we propose a method of reducing stochastic reachability to adversary reachability of ODEs for solving the p-safety problem over finite time horizons. This method permits an efficient lifting of reachset computation methods for perturbed ODEs to RODEs. In this method, the p-safety problem over finite time horizons is reduced to the problem of inner-approximating robust backward reachable sets for ODEs with time-varying perturbation inputs. We then extend the method to the p-safety problem over the infinite time horizon. Finally, we demonstrate our method on several examples.

References

[1] A. Abate, S. Bogomolov, A. Edwards, K. Potomkin, S. Soudjani, and P. Zuliani. Safe reach set computation via neural barrier certificates. Submitted to the *13th ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS 2022)*.

[2] J.-R. Abrial. *Modeling in Event-B: system and software engineering*. Cambridge University Press, 2010.

[3] Y. Aït-Ameur, S. Bogomolov, G. Dupont, A. Iliasov, A. Romanovsky, and P. Stankaitis. A refinement-based development of cyber-physical railway signalling systems. Submitted to the *Formal Aspects of Computing*.

[4] Y. Aït-Ameur, S. Bogomolov, G. Dupont, N. K. Singh, and P. Stankaitis. Reachability analysis and simulation for hybridised event-b models. Submitted to the *25th ACM International Conference on Hybrid Systems: Computation and Control (HSCC 2022)*.

[5] R. Alur, C. Courcoubetis, N. Halbwachs, T. A. Henzinger, P.-H. Ho, X. Nicollin, A. Olivero, J. Sifakis, and S. Yovine. The algorithmic analysis of hybrid systems. *Theoretical Computer Science*, 138(1):3–34, 1995.

[6] S. Bak, S. Bogomolov, P. S. Duggirala, A. Gerlach, and K. Potomkin. Reachability of black-box nonlinear systems after Koopman operator linearization. Accepted to *7th IFAC Conference on Analysis and Design of Hybrid Systems (ADHS 2021)*.

[7] S. Bak, S. Bogomolov, T. A. Henzinger, T. T. Johnson, and P. Prakash. Scalable static hybridization methods for analysis of nonlinear systems. In *19th International Conference on Hybrid Systems: Computation and Control (HSCC 2016)*, pages 155–164. ACM.

[8] S. Bogomolov, M. Forets, G. Frehse, A. Podelski, and C. Schilling. Decomposing reach set computations with low-dimensional sets and high-dimensional matrices (extended version). Submitted to *Information and Computation)*.

[9] S. Bogomolov, M. Forets, G. Frehse, A. Podelski, C. Schilling, and F. Viry. Reach set approximation through decomposition with low-dimensional sets and high-dimensional matrices. In *21th International Conference on Hybrid Systems: Computation and Control (HSCC 2018)*, pages 41–50. ACM, 2018.

[10] S. Bogomolov, M. Forets, G. Frehse, K. Potomkin, and C. Schilling. JuliaReach: a toolbox for set-based reachability. In *22nd ACM International Conference on Hybrid Systems: Computation and Control (HSCC 2019)*, pages 39–44. ACM, 2019.

[11] S. Bogomolov, M. Forets, G. Frehse, K. Potomkin, and C. Schilling. Reachability analysis of linear hybrid systems via block decomposition. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)*, 39(11):4018–4029, 2020. Special Issue from EMSOFT 2020.

[12] S. Bogomolov, G. Frehse, A. Gurung, D. Li, G. Martius, and R. Ray. Falsification of hybrid systems with symbolic reachability analysis and trajectory splicing. Accepted to *Nonlinear Analysis: Hybrid Systems (NAHS)*, 2021.

[13] S. Bogomolov, G. Frehse, A. Gurung, D. Li, G. Martius, and R. Ray. Falsification of hybrid systems using symbolic reachability and trajectory splicing. In *22nd ACM International Conference on Hybrid Systems: Computation and Control (HSCC 2019)*, pages 1–10. ACM, 2019.

[14] S. Bogomolov, A. Hekal, B. Hoxha, and T. Yamaguchi. Reachability analysis with deep neural networks. Submitted to the *25th ACM International Conference on Hybrid Systems: Computation and Control (HSCC 2022)*.

[15] S. Bogomolov, T. T. Johnson, D. Manzanas Lopez, P. Musau, and P. Stankaitis. Combining model predictive control and reachability analysis for dynamical obstacle avoidance. In preparation for the *NASA Formal Methods 2022 (NFM 2022)*.

[16] S. Bogomolov, D. Magazzeni, S. Minopoli, and M. Wehrle. PDDL+ planning with hybrid automata: Foundations of translating must behavior. In *25th International Conference on Automated Planning and Scheduling (ICAPS 2015)*, pages 42–46. AAAI Press, 2015.

[17] E. F. Camacho and C. B. Alba. *Model predictive control*. Springer science & business media, 2013.

[18] A. Gurung, R. Ray, E. Bartocci, S. Bogomolov, and R. Grosu. Parallel reachability analysis of hybrid systems in XSpeed. *International Journal on Software Tools for Technology Transfer (STTT)*, pages 1–23, 2018.

[19] A. Heinz, M. Wehrle, S. Bogomolov, D. Magazzeni, M. Greitschus, and A. Podelski. Temporal planning as refinement-based model checking. In *29th International Conference on Automated Planning and Scheduling (ICAPS 2019)*, pages 195–199. AAAI Press, 2019.

[20] D. Li, S. Bak, and S. Bogomolov. Reachability analysis of nonlinear systems using hybridization and dynamics scaling. In *18th International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS 2020)*, volume 12288 of *LNCS*, pages 265–282. Springer, 2020.

[21] D. Li, E. Scala, P. Haslum, and S. Bogomolov. Effect-abstraction based relaxation for linear numeric planning. In *27th International Joint Conference on Artificial Intelligence (IJCAI 2018)*, pages 4787–4793. International Joint Conferences on Artificial Intelligence Organization, 2018.

[22] S. Prajna and A. Jadbabaie. Safety verification of hybrid systems using barrier certificates. In *International Workshop on Hybrid Systems: Computation and Control*, pages 477–492. Springer, 2004.

[23] Y. Susuki, I. Mezic, F. Raak, and T. Hikihara. Applied koopman operator theory for power systems technology. *Nonlinear Theory and Its Applications, IEICE*, 7(4):430–459, 2016.

[24] B. Xue, M. Fränzle, N. Zhan, S. Bogomolov, and B. Xia. Safety verification for random ordinary differential equations. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)*, 39(11):4090–4101, 2020. Special Issue from EMSOFT 2020.

[25] A. Zutshi, S. Sankaranarayanan, J. V. Deshmukh, and J. Kapinski. A trajectory splicing approach to concretizing counterexamples for hybrid systems. In *Proceedings of the 52nd IEEE Conference on Decision and Control, CDC 2013, December 10-13, 2013*, pages 3918–3925, 2013.