A CEGAR approach for stability verification of linear hybrid systems

Miriam García Soto

IMDEA Software Institute & Universidad Politécnica de Madrid, Spain
miriam.garcia@imdea.org

Abstract. This document summarizes results related to an algorithmic approach for stability analysis of hybrid systems. Classical approaches rely on Lyapunov function search and suffer from numerical issues. In addition, an unsuccessful template for the Lyapunov function does not provide insights on the choice of a better template. To overcome these issues, we present a counterexample guided-abstraction refinement (CEGAR) approach which iteratively searches for a stability certification over an abstract system, and provides insights to obtain more accurate abstract systems if needed.

1 Overview

This document summarizes our research on stability analysis in the framework of hybrid systems. The goal of this research is to develop model checking algorithms for stability verification of hybrid systems, where a hybrid system is a proper formalism for modelling cyber-physical systems and stability is a fundamental property in control theory. Stability verification refers to analyse whether the behaviour of a hybrid system approaches to a predefine behaviour or oscillates around it.

The classical approach to stability analysis in control theory is based on Lyapunov functions [8]. For the case of hybrid systems, the existence of a common or a multiple Lyapunov function [22, 5, 9, 4, 6, 10] corresponds to a stability certificate. Automated analysis involves starting with a template which serves as a candidate Lyapunov function and then encodes the conditions of the Lyapunov function in form of a sum-of-squares programming problem over the template. The sum-of-squares programming problem can be efficiently solved using tools such as SOSTOOLS [13, 12, 11]. The major difficulty with this approach is to determine the right template for the candidate Lyapunov function. Furthermore, with the exception of [7], automatically learning the templates is a problem which has not been adequately addressed.

Motivated by these issues, our work introduces a counterexample guided abstraction refinement (CEGAR) approach not based on Lyapunov functions search. This approach introduces a novel quantitative predicate abstraction which outputs an abstract weighted graph, and provides a set of verifiable conditions over the abstract weighted graph for evaluating stability satisfaction. This stability analysis returns either a sound stability certificate or an abstract counterexample. In case of a counterexample detection, this will provide insights either about the reason for instability or to select a more accurate abstraction.

Quantitative predicate abstraction. The core contribution of our research for stability analysis of hybrid systems is the development of a novel quantitative predicate abstraction (QPA) technique. This abstraction technique is a modified predicate abstraction which constructs a finite weighted graph, from a polyhedral hybrid system and from a finite partition of the state space, preserving stability. The output weighted graph is a conservative approximation. The additional element of the QPA with respect to standard predicate abstractions is the quantization over the edges. The weight on the edges traces the distance of the executions from the origin, and its computation is a crucial part of the approach. Weight computation corresponds to solve an optimization problem over a reachability predicate. A formula equivalent to the predicate is constructed. This formula is a boolean combination of linear constraints. Hence, the weight is computed by solving a bunch of linear programming problems.

The theoretical foundations and results related to the abstraction technique are presented in [15, 16]. Next, efficiently verifiable conditions on the graph are presented such that the satisfaction of them implies Lyapunov stability.

Model checking technique. The weighted graph is analysed for the absence of cycles with weight greater than 1, which can be solved by dynamic programming. The absence of these cycles corresponds to a stability certificate for the polyhedral hybrid system. While the existence of a cycle of this kind corresponds to a potential reason for instability, and it is referred to as abstract counterexample. The theoretical foundations and results related to the conditions for stability over the weighted graph are presented in [18].

Counterexample guided abstraction refinement. The existence of an abstract counterexample is due to two different reasons. One reason is the existence of an infinite divergent execution in the hybrid system, which hence refutes stability of this system and is abstracted by the counterexample. The other reason is the fact that the finite weighted graph abstracted from the hybrid system is too coarse. In this second case, the abstract counterexample results to be spurious. Recognition of the reason requires to execute a validation algorithm.

The validation procedure consists of checking the existence of a stability-refuting execution which is expressed in the weighted graph by following the abstract counterexample. The validation problem in the context of stability analysis is not a bounded model checking problem. It consists of checking if there exists an infinite diverging trajectory that follows the counterexample cycle infinitely many times. This property cannot, as is, be encoded as the satisfiability of a formula in a finitary logic. Our work introduces a novel characterization for the existence of an infinite diverging execution in terms of the satisfaction of a first order logic formula, which can be efficiently solved by means of SMT solvers. The validation technique based on such characterization is presented in [20].

Validation procedure can determine that an infinite diverging execution does not exist in the polyhedral hybrid system. In this case, the finite abstract graph is too coarse. Hence, a tighter abstraction needs to be constructed such that the abstract counterexample is eliminated. A finer abstraction comes out by adding new predicates to the state space partition. This addition can be either an automatic random process or a counterexample based approach. Both approaches are refinement strategies. The automatic random process creates predicates which partition uniformly the state space. The other refinement strategy is an algorithmic technique which constructs predicates based on the counterexample. The extra predicates are added in the quantitative predicate abstraction process to refine the state space partition in order to obtain a more accurate weighted graph. The theoretical foundations and results related to the refinement techniques are presented in [20].

The previous results are further developed in two directions. On one side, a more complex class of hybrid systems is considered, and on the other side, a new stability property is introduced. The stability notions considered in the previous framework are Lyapunov and asymptotic stability, which are local properties. Local properties refer to a particular region in the state space, unlike the new one, global asymptotic stability (GAS), which refers to the full state space. An extension of the previous algorithms is introduced to obtain GAS verification of linear hybrid systems.

Hybridization. The continuous behaviour of linear hybrid systems is determined by linear dynamics which requires a high computational power. An efficient approach to overcome such drawback consists of defining a simpler system based on the linear hybrid system and that is sound with respect to stability satisfaction (stability of the simpler system implies stability of the linear hybrid system). The contribution to this end is to define an abstraction technique for over approximating the behaviour of a linear hybrid system by a polyhedral hybrid system. The abstraction technique is called hybridization and consists of splitting the state space into a finite number of regions and of approximating at each region the linear dynamics by a polyhedral inclusion. We introduce a novel hybridization procedure, where the state space splitting requires to be tuned for stability verification. The computed polyhedral hybrid system enables to define scalable stability verification techniques and ensures stability of the linear hybrid system in case of being stable itself. The theoretical foundations and the results related to this hybridization technique are presented in [21].

Global asymptotic stability verification. The GAS verification is built up in the above-mentioned algorithmic approaches. The main result consists of a decomposition theorem that reduces the GAS verification problem into a region stability (RS) analysis problem and an asymptotic stability (AS) analysis problem. The developed QPA technique is used for AS analysis and also for extracting a stability zone required for the RS analysis. In addition to the decomposition result, the fundamental contributions of the extended procedure are the algorithmic computation of the stability zone and the model checking algorithm for

RS verification. These results are presented in [19] along with a semi-automated proof of GAS for a cruise controller interacting with an automatic gearbox.

Algorithmic verifier of stability. A software tool called AVERIST have been deployed to execute the CEGAR algorithm for Lyapunov stability verification of linear hybrid systems. Details on the architecture and the implementation of AVERIST are presented in [17].

Acknowledgment. This work has been developed in collaboration with Pavithra Prabhakar.

References

1. Rajeev Alur, Thao Dang, and Franjo Ivancic. Counter-Example Guided Predicate Abstraction of Hybrid Systems. In *Tools and Algorithms for the Construction and Analysis of Systems, 9th International Conference, TACAS 2003, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2003, Warsaw, Poland, April 7-11, 2003, Proceedings*, pages 208–223, 2003.
2. Edmund M. Clarke, Ansgar Fehnker, Zhi Han, Bruce H. Krogh, Joël Ouaknine, Olaf Stursberg, and Michael Theobald. Abstraction and Counterexample-Guided Refinement in Model Checking of Hybrid Systems. *Int. J. Found. Comput. Sci.*, 14(4):583–604, 2003.
3. Henning Dierks, Sebastian Kupferschmid, and Kim Guldstrand Larsen. Automatic Abstraction Refinement for Timed Automata. In *Formal Modeling and Analysis of Timed Systems, 5th International Conference, FORMATS 2007, Salzburg, Austria, October 3-5, 2007, Proceedings*, pages 114–129, 2007.
4. José C. Geromel and Patrizio Colaneri. Stability and Stabilization of Continuous-Time Switched Linear Systems. *SIAM Journal on Control and Optimization*, 45(5):1915–1930, 2006.
5. Rafal Goebel, Ricardo G. Sanfelice, and Andrew R. Teel. Hybrid dynamical systems. *IEEE Control Systems*, 29(2):28–93, April 2009.
6. João P. Hespanha. Uniform stability of switched linear systems: extensions of LaSalle's Invariance Principle. *IEEE Transactions on Automatic Control*, 49(4):470–482, April 2004.
7. James Kapinski, Jyotirmoy V. Deshmukh, Sriram Sankaranarayanan, and Nikos Arechiga. Simulation-guided Lyapunov Analysis for Hybrid Dynamical Systems. In *Proceedings of the 17th International Conference on Hybrid Systems: Computation and Control*, HSCC '14, pages 133–142, New York, NY, USA, 2014. ACM.
8. Hassan K. Khalil. *Nonlinear Systems.* Pearson Education. Prentice Hall, Englewood Cliffs, NJ, 3rd edition, 2002.
9. Hai Lin and Panos J. Antsaklis. Stability and Stabilizability of Switched Linear Systems: A Survey of Recent Results. *IEEE Transactions on Automatic Control*, 54(2):308–322, Feb 2009.
10. Paolo Mason, Ugo Boscain, and Yacine Chitour. Common Polynomial Lyapunov Functions for Linear Switched Systems. *SIAM Journal on Control and Optimization*, 45(1):226–245, 2006.
11. Eike Möhlmann and Oliver Theel. Stabhyli: A Tool for Automatic Stability Verification of Non-linear Hybrid Systems. In *Proceedings of the 16th International*

Conference on Hybrid Systems: Computation and Control, HSCC '13, pages 107–112, New York, NY, USA, 2013. ACM.

12. Antonis Papachristodoulou and Stephen Prajna. On the construction of Lyapunov functions using the sum of squares decomposition. In *Proceedings of the 41st IEEE Conference on Decision and Control, 2002.*, volume 3, pages 3482–3487 vol.3, Dec 2002.
13. Pablo A. Parrilo. Structured Semidefinite Programs and Semialgebraic Geometry Methods in Robustness and Optimization. Technical report, California Institute of Technology, Pasadena, CA, USA, 2000.
14. Pavithra Prabhakar, Parasara Sridhar Duggirala, Sayan Mitra, and Mahesh Viswanathan. Hybrid Automata-Based CEGAR for Rectangular Hybrid Systems. In *Verification, Model Checking, and Abstract Interpretation, 14th International Conference, VMCAI 2013, Rome, Italy, January 20-22, 2013. Proceedings*, pages 48–67, 2013.
15. Pavithra Prabhakar and Miriam García Soto. Abstraction Based Model-Checking of Stability of Hybrid Systems. In *Computer Aided Verification - 25th International Conference, CAV 2013, Saint Petersburg, Russia, July 13-19, 2013. Proceedings*, pages 280–295, 2013.
16. Pavithra Prabhakar and Miriam García Soto. An algorithmic approach to stability verification of polyhedral switched systems. In *American Control Conference, ACC 2014, Portland, OR, USA, June 4-6, 2014*, pages 2318–2323, 2014.
17. Pavithra Prabhakar and Miriam García Soto. AVERIST: An Algorithmic Verifier for Stability. *Electr. Notes Theor. Comput. Sci.*, 317:133–139, 2015.
18. Pavithra Prabhakar and Miriam García Soto. Foundations of quantitative predicate abstraction for stability analysis of hybrid systems. In *Verification, Model Checking, and Abstract Interpretation - 16th International Conference, VMCAI 2015, Mumbai, India, January 12-14, 2015. Proceedings*, pages 318–335, 2015.
19. Pavithra Prabhakar and Miriam García Soto. An algorithmic approach to global asymptotic stability verification of hybrid systems. In *2016 International Conference on Embedded Software, EMSOFT 2016, Pittsburgh, Pennsylvania, USA, October 1-7, 2016*, pages 9:1–9:10, 2016.
20. Pavithra Prabhakar and Miriam García Soto. Counterexample guided abstraction refinement for stability analysis. In *Computer Aided Verification - 28th International Conference, CAV 2016, Toronto, ON, Canada, July 17-23, 2016, Proceedings, Part I*, pages 495–512, 2016.
21. Pavithra Prabhakar and Miriam García Soto. Hybridization for Stability Analysis of Switched Linear Systems. In *Proceedings of the 19th International Conference on Hybrid Systems: Computation and Control, HSCC 2016, Vienna, Austria, April 12-14, 2016*, pages 71–80, 2016.
22. Eduardo D. Sontag. Input to state stability: Basic concepts and results. In *Nonlinear and Optimal Control Theory*, pages 163–220. Springer, 2006.