Lecture Notes in Computer Science 10506

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

Matthew Hague · Igor Potapov (Eds.)

Reachability Problems

11th International Workshop, RP 2017
London, UK, September 7–9, 2017
Proceedings

Springer

Editors

Matthew Hague
Royal Holloway University of London
London
UK

Igor Potapov
University of Liverpool
Liverpool
UK

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-67088-1 ISBN 978-3-319-67089-8 (eBook)
DOI 10.1007/978-3-319-67089-8

Library of Congress Control Number: 2017951439

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

Printed on acid-free paper

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

Preface

This volume contains the papers presented at the 11th International Workshop on Reachability Problems (RP), held on September 7–9, 2017, at Royal Holloway, University of London, UK. Previous workshops in the series were located at: Aalborg University (2016), the University of Warsaw (2015), the University of Oxford (2014), Uppsala University (2013), the University of Bordeaux (2012), the University of Genoa (2011), Masaryk University Brno (2010), École Polytechnique (2009), the University of Liverpool (2008), and Turku University (2007).

The aim of the conference is to bring together scholars from diverse fields with a shared interest in reachability problems, and to promote the exploration of new approaches for the modelling and analysis of computational processes by combining mathematical, algorithmic, and computational techniques. Topics of interest include (but are not limited to): reachability for infinite state systems; rewriting systems; reachability analysis in counter/timed/cellular/communicating automata; Petri nets; computational aspects of semigroups, groups, and rings; reachability in dynamical and hybrid systems; frontiers between decidable and undecidable reachability problems; complexity and decidability aspects; predictability in iterative maps, and new computational paradigms.

The invited speakers at the 2017 workshop were:

- Hana Chockler, King's College London
- Laurent Doyen, LSV-ENS Cachan
- Raphaël Jungers, Université catholique de Louvain
- Andreas Podelski, University of Freiburg

The workshop received 17 submissions. Each submission was reviewed by three Program Committee (PC) members. The members of the PC and the list of external reviewers can be found on the next two pages. The PC is grateful for the high quality work produced by these external reviewers. Based on these reviews, the PC decided to accept 12 papers, in addition to the four invited talks. Overall this volume contains 12 contributed papers and one paper by an invited speaker. The workshop also provided the opportunity to researchers to give informal presentations, prepared shortly before the event, informing the participants about current research and work in progress.

It is a pleasure to thank the team behind the EasyChair system and the Lecture Notes in Computer Science team at Springer, who together made the production of this volume possible in time for the workshop. Finally, we thank all the authors for their high-quality contributions, and the participants for making RP 2017 a success.

September 2017

Igor Potapov
Matthew Hague

Organization

Program Committee

C. Aiswarya	Chennai Mathematical Institute, India
Paul Bell	Liverpool John Moores University, UK
Patricia Bouyer-Decitre	LSV, CNRS & ENS Cachan, Université Paris Saclay, France
Laura Bozzelli	Technical University of Madrid (UPM), Spain
Giorgio Delzanno	DIBRIS, Università di Genova, Italy
Matthew Hague	Royal Holloway, University of London, UK
Piotrek Hofman	University of Warsaw, Poland
Salvatore La Torre	Università degli studi di Salerno, Italy
Peter Lammich	TU Munich, Germany
Martin Lange	University of Kassel, Germany
Ranko Lazic	University of Warwick, UK
Ondrej Lengal	Brno University of Technology, Czech Republic
Jerome Leroux	CNRS, France
Rupak Majumdar	MPI-SWS, Germany
Igor Potapov	The University of Liverpool, UK
Ahmed Rezine	Linköping University, Sweden
Tachio Terauchi	Japan Advanced Institute of Science and Technology, Japan
Hsu-Chun Yen	National Taiwan University, Taiwan

Additional Reviewers

Haddad, Serge
Kreiker, Joerg
Prianychnykova, Olena
Sorrentino, Loredana

Abstracts of Invited Talks

Trace Abstraction

Andreas Podelski

University of Freiburg, Germany

Abstract. Trace abstraction refers to a new approach to program verification algorithms. Instead of trying to construct a proof for the input program directly, we first construct auxiliary programs from proofs. We construct each auxiliary program (which can be of general form) from the proof for a program in a specific form, namely a program in the form of a trace (i.e., a sequence of statements). A trace is a program (where the statements have a semantics). At the same time, a trace is a word over a finite alphabet (where the semantics of statements is ignored). As a word, a sequence of statements can be read by an automaton. Just as we ask whether there exists an accepting run of a given automaton on a sequence of letters, we can ask whether there exists a correctness proof for a sequence of statements, a correctness proof that can be assembled from a given finite set of Hoare triples. We iteratively construct auxiliary programs from proofs for traces. The iteration stops when the constructed programs together cover all possible behaviors of the input program. A crucial step here is the covering check. This step is based on algorithms for automata (inclusion test, minimization, …). The approach applies to a range of verification problems, for sequential programs with (possibly recursive) procedures and concurrent programs with possibly unboundedly many threads, and even to real-time programs.

How Do We Know That Our System Is Correct?

Hana Chockler

King's College London, UK

Abstract. A negative answer from the model-checking procedure is accompanied by a counterexample – a trace demonstrating what went wrong. On the other hand, when the answer from the model-checker is positive, usually no further information is given. The issue of "suspecting the positive answer" first arose in industry, where positive answers from model-checkers often concealed serious bugs in hardware designs. In this talk, I discuss some reasons why the positive answer from the model-checker may require further investigation and briefly and in broad terms describe algorithms for such investigations, called *sanity checks*.

The talk also (briefly) introduces the theory of causality and counterfactual reasoning and its applications to model-checking, mostly in the context of the subject of this talk, including some recent complexity results and applications of structure-based causality.

The talk then attempts to define the main goal of the sanity checks, explanations, and related algorithms, or at least provide some food for thought regarding the question of the mail goal.

I conclude the talk with outlining some promising future directions.

The talk is based on many papers written by many people, and is not limited to my own research. It is reasonably self-contained.

Path-Complete Lyapunov Techniques: Stability, Safety, and Beyond

Raphaël M. Jungers

ICTEAM Institute, Université catholique de Louvain
raphael.jungers@uclouvain.be

Path-complete Lyapunov Techniques[1] are a family of methods that combine Automata-Theoretic tools with algebraic formulas in order to derive ad hoc criteria for the control of complex systems. These criteria are typically solved with Convex Optimization solvers. They initially appeared in the framework of switched systems, which are dynamical systems for which the state dynamics varies between different operating modes. They take the form

$$x(t+1) = f_{\sigma(t)}(x(t)) \tag{1}$$

where the state $x(t)$ evolves in $\mathbb{R}^n$. The *mode* $\sigma(t)$ of the system at time t takes its value in a set $\{1, \ldots, M\}$ for some integer M, and each mode of the system is described by a continuous map $f_i(x) : \mathbb{R}^n \to \mathbb{R}^n$.

When the functions f_i are linear functions, we say that the system is a *linear switched system.* The *stability problem* is reputedly very hard, even in the restricted case of linear functions (see e.g. [14, Sect. 2.2]). In this case, one can easily obtain a sufficient condition for stability, through the existence of a *common quadratic* Lyapunov function (see e.g. [18, Sect. II-A]). However, such a Lyapunov function may not exist, even when the system is asymptotically stable (see e.g. [17, 18]). Less conservative parameterizations of candidate Lyapunov functions have been proposed, at the cost of greater computational effort (e.g. for linear switching systems, [19] uses sum-of-squares polynomials, [12] uses max-of-quadratics Lyapunov functions, and [4] uses polytopic Lyapunov functions). *Multiple Lyapunov functions* (see [7, 13, 21]) arise as an alternative to common Lyapunov functions. In the case of linear systems, the multiple *quadratic* Lyapunov functions such as those introduced in [6, 8, 9, 16] hold special interest as checking for their existence boils down to solving a set of LMIs. The general framework of *Path-Complete* Lyapunov functions was recently introduced in [1, 15] in this context, for analyzing and unifying these approaches.

In this talk, we first present these criteria guaranteeing that the system (1) is stable under *arbitrary switching*, i.e. where the function $\sigma(\cdot)$ is not constrained, and one is

R.J. is supported by the Communauté française de Belgique - Actions de Recherche Concertées, and by the Belgian Programme on Interuniversity Attraction Poles initiated by the Belgian Federal Science Policy Office. He is a Fulbright Fellow and a FNRS Fellow, currently visiting the Dept. of Electrical Engineering at UCLA.

[1] Path-complete techniques are implemented in the JSR toolbox [22].

interested in the worst-case stability. We then show how this very natural idea can be leveraged for much more general purposes: we present recent works were the same idea has been applied to more general systems than the ones described above [20], or for proving different properties than stability [10].

These techniques give rise to many natural questions: First, they essentially provide algebraic criteria, that is, equations and inequations, that can be solved numerically in order to (hopefully) conclude stability, if a solution is found. But what do they mean in terms of control systems? Do they have a geometric interpretation in the state space? Second, among the different criteria in this framework, which one should an engineer pick in practice? Do these criteria compare with each other (in terms of conservativeness)? How to algorithmically choose the good criterion, when one is given a particular problem? While recent progress has been done to provide a geometric interpretation of these criteria [3], several problems remain open, like the one of comparing two given path-complete criteria [2].

Finally, we draw connections with other recent works in Control and Computer Science, which bear similarities with path-complete techniques, in safety analysis of computer programs [5], or in connection with tropical Kraus maps [11].

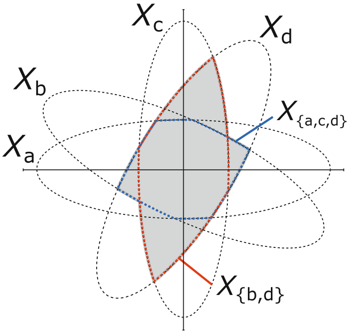

Fig. 1. Graphical illustration of the level set of a path-complete Lyapunov function.We will show in the talk that these level sets can always be expressed as unions of intersections of Ellipsoids.

References

1. Ahmadi, A.A., Jungers, R.M., Parrilo, P.A., Roozbehani, M.: Joint spectral radius and path-complete graph lyapunov functions. SIAM J. Control Optim. **52**(1), 687–717 (2014)
2. Angeli, D., Athanasopoulos, N., Jungers, R.M., Philippe, M.: A linear program to compare path-complete lyapunov functions (2017, submitted)
3. Angeli, D., Athanasopoulos, N., Jungers, R.M., Philippe, M.: Path-complete graphs and common lyapunov functions. In: Proceedings of the 20th International Conference on Hybrid Systems: Computation and Control, pp. 81–90. ACM (2017)
4. Athanasopoulos, N., Lazar, M.: Alternative stability conditions for switched discrete time linear systems. In: IFAC World Congress, pp. 6007–6012 (2014)
5. Balakrishnan, G., Sankaranarayanan, S., Ivančić, F., Gupta, A.: Refining the control structure of loops using static analysis. In: Proceedings of the Seventh ACM International Conference on Embedded Software, pp. 49–58. ACM (2009)

6. Bliman, P.-A., Ferrari-Trecate, G.: Stability analysis of discrete-time switched systems through lyapunov functions with nonminimal state. In: Proceedings of IFAC Conference on the Analysis and Design of Hybrid Systems, pp. 325–330 (2003)
7. Branicky, M.S.: Multiple lyapunov functions and other analysis tools for switched and hybrid systems. IEEE Trans. Autom. Control **43**(4), 475–482 (1998)
8. Daafouz, J., Riedinger, P., Iung, C.: Stability analysis and control synthesis for switched systems: a switched lyapunov function approach. IEEE Trans. Autom. Control **47**(11), 1883–1887 (2002)
9. Essick, R., Lee, J.-W., Dullerud, G.E.: Control of linear switched systems with receding horizon modal information. IEEE Trans. Autom. Control **59**(9), 2340–2352 (2014)
10. Forni, F., Jungers, R.M., Sepulchre, R.: Path-complete positivity of switching systems (2016). arXiv preprint, arXiv:1611.02603
11. Gaubert, S., Stott, N.: Tropical kraus maps for optimal control of switched systems (2017). arXiv preprint, arXiv:1706.04471
12. Goebel, R., Hu, T., Teel, A.R.: Dual matrix inequalities in stability and performance analysis of linear differential/difference inclusions. In: Current Trends in Nonlinear Systems and Control, pp. 103–122. Springer (2006)
13. Johansson, M., Rantzer, A., et al.: Computation of piecewise quadratic lyapunov functions for hybrid systems. IEEE Trans. Autom. Control **43**(4), 555–559 (1998)
14. Jungers, R.: The joint spectral radius. Lect. Notes Control Inf. Sci. **385** (2009)
15. Jungers, R.M., Ahmadi, A.A., Parrilo, P.A., Roozbehani, M.: A characterization of lyapunov inequalities for stability of switched systems. IEEE Trans. Autom. Control **62**(6), 3062–3067 (2017)
16. Lee, J.-W., Dullerud, G.E.: Uniform stabilization of discrete-time switched and markovian jump linear systems. Automatica **42**(2), 205–218 (2006)
17. Liberzon, D., Morse, A.S.: Basic problems in stability and design of switched systems. IEEE Control Syst. Mag. **19**(5), 59–70 (1999)
18. Lin, H., Antsaklis, P.J.: Stability and stabilizability of switched linear systems: a survey of recent results. IEEE Trans. Autom. Control **54**(2), 308–322 (2009)
19. Parrilo, P.A., Jadbabaie, A.: Approximation of the joint spectral radius using sum of squares. Linear Algebra Appl. **428**(10), 2385–2402 (2008)
20. Philippe, M., Essick, R., Dullerud, G.E., Jungers, R.M.: Stability of discrete-time switching systems with constrained switching sequences. Automatica **72**, 242–250 (2016)
21. Shorten, R., Wirth, F., Mason, O., Wulff, K., King, C.: Stability criteria for switched and hybrid systems. SIAM Rev. **49**(4), 545–592 (2007)
22. Vankeerberghen, G., Hendrickx, J., Jungers, R.M.: JSR: a toolbox to compute the joint spectral radius. In: Proceedings of the 17th International Conference on Hybrid Systems: Computation and Control, pp. 151–156. ACM (2014)

The Multiple Dimensions of Mean-Payoff Games

Laurent Doyen

LSV, ENS Paris-Saclay & CNRS

Abstract. We consider quantitative game models for the design of reactive systems working in resource-constrained environment. The game is played on a finite weighted graph where some resource (e.g., battery) can be consumed or recharged along the edges of the graph.

In mean-payoff games, the resource usage is computed as the long-run average resource consumption. In energy games, the resource usage is the initial amount of resource necessary to maintain the resource level always positive.

We review fundamental results about mean-payoff games that show the existence of memoryless optimal strategies, and the equivalence of mean-payoff games with finite-duration reachability games, as well as with energy games (which can also be viewed as safety games). These results provide conceptually simple backward-induction algorithms for solving mean-payoff games, and for constructing memoryless optimal strategies. It follows that mean-payoff games can be solved in NP $\cap$ coNP.

Then we consider games with multiple mean-payoff conditions for systems using multiple resources. In multi-dimension mean-payoff games, memory is necessary for optimal strategies, and the previous equivalence results with reachability and energy (safety) games no longer hold. First, infinite memory is necessary in general for optimal strategies. With infinite memory, the limit of the long-run average resource consumption may not exist, and it is necessary to distinguish between the limsup and the liminf of the long-run average resource consumption. Second, the equivalence with a multi-dimensional version of energy games holds only if the players are restricted to use finite-memory strategies, and in that case the limsup- and the liminf-value coincide.

The complexity of solving multi-dimension mean-payoff games is as follows, depending on which class of strategies is given to the player: NP-complete for memoryless strategies, coNP-complete for finite-memory strategies, NP $\cap$ coNP for infinite-memory strategies and a conjunction of limsup objectives, and coNP-complete for infinite-memory strategies and a conjunction of liminf objectives.

Contents