Lecture Notes in Computer Science 11123

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

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

Igor Potapov · Pierre-Alain Reynier (Eds.)

Reachability Problems

12th International Conference, RP 2018
Marseille, France, September 24–26, 2018
Proceedings

Springer

Editors
Igor Potapov
University of Liverpool
Liverpool
UK

Pierre-Alain Reynier
Aix-Marseille University
Marseille
France

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-00249-7 ISBN 978-3-030-00250-3 (eBook)
https://doi.org/10.1007/978-3-030-00250-3

Library of Congress Control Number: 2018953208

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

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

Preface

This volume contains the papers presented at RP 2018, the 12th International Conference on Reachability Problems, organized on September 24–26, 2018 by Aix-Marseille University, Marseille, France. Previous events in the series were located at: Royal Holloway, University of London (2017), 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.

Reachability is a fundamental problem that appears in several different contexts. Typically, for a fixed system description given in some form (rewriting rules, transformations by computable functions, systems of equations, logical formulas, etc.) a reachability problem consists in checking whether a given set of target states can be reached starting from a fixed set of initial states. The set of target states can be represented explicitly or via some implicit representation (e.g., a system of equations, a set of minimal elements with respect to some ordering on the states). Sophisticated quantitative and qualitative properties can often be reduced to basic reachability questions. Decidability and complexity boundaries, algorithmic solutions, and efficient heuristics are all important aspects to be considered in this context. Algorithmic solutions are often based on different combinations of exploration strategies, symbolic manipulations of sets of states, decomposition properties, and reduction to linear programming problems, and they often benefit from approximations, abstractions, accelerations, and extrapolation heurisitics. Ad hoc solutions as well as solutions based on general-purpose constraint solvers and deduction engines are often combined in order to balance efficiency and flexibility.

The invited speakers at the RP 2018 were:

– Olivier Bournez - "On the Computational Complexity of Solving Ordinary Differential Equations"
– Maria Prandini - "Reachability in Cyber-Physical Systems"
– Marcin Jurdzinski - "Universal Ordered Trees and Quasi-polynomial Algorithms for Solving Parity Games"

– Jérémie Chalopin - “A Counterexample to Thiagarajan’s Conjecture on Regular Event Structures”
– Marta Kwiatkowska - “Safety Verification for Deep Neural Networks with Provable Guarantees”

The conference originally received 29 abstracts from which 21 full papers were submitted. Each submission was carefully reviewed by three Program Committee (PC) members. Based on these reviews, the PC decided to accept 11 papers, in addition to the four invited talks (by Olivier Bournez, Maria Prandini, Marcin Jurdzinski, Jérémie Chalopin) and one invited tutorial (by Marta Kwiatkowska). The members of the PC and the list of external reviewers can be found on the next pages. The PC is grateful for the high quality work produced by these external reviewers. Overall this volume contains 11 contributed papers and the conference also provided the opportunity to other young and established researchers to give informal presentations, prepared shortly before the event, informing the participants about current research and work in progress. The informal presentations have not been included at this LNCS proceedings, but may be found on the conference website.

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 conference. Finally, we thank all the authors for their high-quality contributions, and the participants for making RP 2018 a success. We are also very grateful to Alfred Hofmann for the continuous support of the event in the last decade and to LNCS Springer, EATCS, CNRS, Laboratoire d’Excellence Archimède, the LIS Laboratory of Computing and Systems, and Aix-Marseille University for the scientific and financial sponsorship of the event.

September 2018

Igor Potapov
Pierre-Alain Reynier

Organization

Program Committee

S. Akshay	IIT Bombay, India
Christel Baier	TU Dresden, Germany
Paul Bell	Liverpool John Moores University, UK
Nathalie Bertrand	Inria, France
Udi Boker	Interdisciplinary Center (IDC) Herzliya, Israel
Krishnendu Chatterjee	Institute of Science and Technology (IST), Austria
Laure Daviaud	The University of Warwick, UK
Giorgio Delzanno	DIBRIS, Università di Genova, Italy
Emmanuel Filiot	Université Libre de Bruxelles, Belgium
Pierre Ganty	IMDEA Software Institute, Spain
Matthew Hague	Royal Holloway University of London, UK
Vesa Halava	University of Turku, Finland
Petr Jancar	Palacky Univ. Olomouc, Czech Republic
Martin Lange	University of Kassel, Germany
Sławomir Lasota	Warsaw University, Poland
Laurent Fribourg	LSV, France
Benjamin Monmege	Aix-Marseille Université, LIF, CNRS, France
Anca Muscholl	LaBRI, Universite Bordeaux, France
Igor Potapov	University of Liverpool, UK
Pavithra Prabhakar	Kansas State University, USA
Alexander Rabinovich	Tel Aviv University, Israel
Pierre-Alain Reynier	Aix-Marseille Université, France
Thomas Schwentick	Universität Dortmund, Germany
Helmut Seidl	Technical University of Munich, Germany
Mikhail Volkov	Ural Federal University, Russia

Additional Reviewers

Balaji, Nikhil
Chillara, Suryajith
Haase, Christoph
Kokkinis, Ioannis
Kwee, Kent
Perez, Guillermo
Totzke, Patrick
Yörük, Lara

Abstracts of Invited Talks

On the Computational Complexity of Solving Ordinary Differential Equations

Olivier Bournez

Ecole Polytechnique, LIX, 91128 Palaiseau Cedex, France

We consider Continuous Ordinary Differential Equations: That is to say x' = f(x) where $f : \mathbb{R}^n \to \mathbb{R}^n$ is a continuous function. When an initial condition $x(0) = x_0$ is added, this is called an Initial Value Problem (IVP), also called a Cauchy's Problem. A trajectory is any solution of the problem, that is to say, any derivable function $\xi : I \subset \mathbb{R}_{\geq 0} \to \mathbb{R}^n$, where I is some interval containing 0 satisfying $\xi(0) = x_0$, and $\xi'(t) = f(\xi(t))$ on its domain. The solution is said to be maximal, if I is maximal (for inclusion) with this property. For f continuous, IVP are known to always have solutions, but possibly non unique, by Peano-Arzelà's Theorem. When in addition f is Lipschitz (in particular if it is $\mathcal{C}^1$) then unicity is guaranteed, by Cauchy-Lipschitz theorem. When f is analytic, solutions are know to be analytic.

In this talk we will survey various results related to the difficulty of computing a or the solutions for various classes of functions f.

In particular, we will discuss the case $y' = p(t, y)$, $y(t_0) = y_0$, where p is a vector of polynomials). In this case, there is a polynomial time algorithm that, given the initial-value problem, the time T at which we want to compute the solution of the IVP, and the maximum allowable error $\varepsilon > 0$, outputs a value $\tilde{y}_T$ such that $\|\tilde{y}_T - y(T)\| \leq \varepsilon$ in time polynomial in T, $-log\varepsilon$, and in several quantities related to the polynomial IVP.

We will relate the discussion to questions related to the computational power of several continuous time analog models such as the General Purpose Analog Computer (GPAC) from Claude Shannon. The GPAC was introduced as a model of famous mechanical, and later-on electronics, analog computers named Differential Analysers.

Reachability in Cyber-Physical Systems

Maria Prandini

Politecnico di Milano, Piazza Leonardo da Vinci 32, 20133 Milan, Italy
maria.prandini@polimi.it

Reachability analysis consists in determining the region of the state space that a given dynamical system will visit starting from some set of initial states, subject to a disturbance input modeling uncertainty in the system dynamics and/or the fact that the system is operating in an uncertain environment that can affect its evolution.

A main application of reachability analysis – that makes it relevant to various application domains – is the automatic verification of the correct behavior of a system, which is typically coded by requiring that all its trajectories remain within some desired range of operation and do not enter any forbidden region of the state space. If the outcome of the verification is negative, then, the system has to be redesigned. The availability of some counter-example showing a violation of the correct behavior can be useful to this purpose.

In reachability analysis, the region of the state space that is visited by the system during its evolution is determined by propagating the set of initial states through the uncertain system dynamics, thus computing the so-call reach sets.

The main issue in reachability analysis is indeed the ability to compute with sets. In systems with a finite state space, sets can be represented by enumeration and reach sets can be computed starting from the given initial set and progressively adding one-step successors. If we consider systems involving a continuous state space, then, representation and propagation of reach sets generally become a challenge. One should in fact choose a class of sets that can be efficiently represented and such that, when one applies to these sets the operations involved in their propagation through the system dynamics, then, sets in the same class are obtained. If this is not possible, some outer-approximation of the obtained sets should be adopted to bring their description back to the same class.

Scalability of reach set computations arises as an issue, and calls for abstraction of models through simulation or approximate simulation relations. In the case of a simulation relation, the abstracted model can be used for verifying the correct behavior of the original system since all trajectories of the original system can be generated by simulating the abstracted model (but not vice-versa). For instance, a nonlinear continuous system with smooth dynamics can be reduced to a piecewise affine system that satisfies a simulation relation if the abstraction procedure appropriately accounts for the modeling error through a (fictitious) disturbance input.

We shall consider reachability analysis for cyber-physical systems that represent engineering systems where communication, computation, and control (the cyber part)

Supported by the European Commission under the project UnCoVerCPS with grant number 643921.

are integrated within natural and/or human-made systems (the physical part) governed by the laws of physics. Hybrid models are used to describe this class of systems, since the interleaved discrete and continuous state components of a hybrid model can represent the cyber and physical parts integrated in a cyber-physical system.

Reachability analysis of hybrid systems is challenging since their hybrid state has a continuous component and the propagation of the reach sets in the continuous state space depends on the value taken by the hybrid state. Typically, a reach set in the continuous state space can split in subsets that propagate according to different continuous dynamics, thus growing the effort in reach set computations.

In this invited talk, we shall focus on discrete time piecewise affine systems, which often arise as a model for cyber-physical systems and have also some potential as a unifying modeling framework for automatic verification of nonlinear continuous systems. More specifically, we address verification of discrete time piecewise affine systems based on reach set computations, including the generation of counter-examples, and the use of abstraction and invariant sets to improve scalability. We also address the case when a control input is available to impose the correct system behavior via disturbance compensation, and describe a set-based approach to feedback control design integrating reach set computations.

Universal Trees and Quasi-Polynomial Algorithms for Solving Parity Games

Marcin Jurdziński

Department of Computer Science, University of Warwick, UK

Parity games have played a fundamental role in automata theory, logic, and their applications to verification and synthesis since early 1990's. Solving parity games is polynomial-time equivalent to checking *emptiness of automata on infinite trees* and to the *modal mu-calculus model checking*. It is a long-standing open question whether there is a polynomial-time algorithm for solving parity games. The quest for a polynomial-time algorithm has not only brought diverse algorithmic techniques to the theory and practice of verification and synthesis, but it has also significantly contributed to resolving long-standing open problems in other research areas, such as Markov Decision Processes and Linear Programming.

All algorithms for solving parity games that were known until 2016 required time that was exponential in the most important parameter of a parity game—the number of distinct *priorities*. The major breakthrough was achieved by Calude, Jain, Khoussainov, Li, and Stephan in 2017, who have given the first quasi-polynomial algorithm and established that parity games are in FPT (fixed-parameter tractable). Two other quasi-polynomial algorithms for solving parity games were subsequently devised by Jurdziński and Lazić, 2017, and by Lehtinen, 2018, and a space-efficient version of Calude et al.'s algorithm was given by Fearnley, Jain, Schewe, Stephan, and Wojtczak, 2017. The conceptual and technical toolkits used by all the three algorithms seem rather distinct: the breakthrough result of Calude et al. was based on computing *play summaries* by *succinct counting*, Jurdziński and Lazić have devised a *succinct coding* of *ordered trees* and applied it to the *progress measure lifting* algorithm, and Lehtinen has developed novel concepts of *register games* and the *register index*.

In this talk we first focus on presenting the technical insights of the quasi-polynomial algorithm for solving parity games that is based on progress measure lifting and succinct coding of ordered trees. Following Czerwiński, Daviaud, Fijalkow, Jurdziński, Lazić, and Parys, 2018, we then argue that *universal ordered trees*—implicit in the succinct tree-coding result of Jurdziński and Lazić—offer a unifying perspective on the three distinct quasi-polynomial algorithms. Moreover, the analysis of universal trees leads to an automata-theoretic quasi-polynomial lower bound that forms a barrier that all the existing approaches, as well as other possible techniques that follow the separation approach, must overcome in the quest for a polynomial-time algorithm for solving parity games.

More specifically, we argue that the techniques underlying all the three quasi-polynomial algorithms can be interpreted as constructions of automata on infinite words that are of quasi-polynomial size and that facilitate solving parity games by the *separation approach* formalized by Bojańczyk and Czerwiński, 2018, and implicit in

the work of Bernet, Janin, and Walukiewicz, 2002. In particular, we point out how such *separating automata* arise in a very natural way from universal ordered trees. Then we present two lower bounds: one is a quasi-polynomial lower bound on the size of universal trees that nearly matches (up to a small polynomial factor) the succinct tree-coding upper bound of Jurdziński and Lazić, and the other establishes that the set of states in every separating automaton contains leaves of some universal tree, which implies that every separating automaton is of at least quasi-polynomial size.

Keywords: Parity games · Quasi-polynomial algorithms · Progress measures
Universal ordered trees · Separating automata · Lower bounds

A Counterexample to Thiagarajan's Conjecture on Regular Event Structures

Jérémie Chalopin

LIS, CNRS, Aix-Marseille Université, and Universit de Toulon
jeremie.chalopin@lis-lab.fr

We provide a counterexample to a conjecture by Thiagarajan [8, 9] that regular event structures correspond exactly to event structures obtained as unfoldings of finite 1-safe Petri nets. Event structures, trace automata, and Petri nets are fundamental models in concurrency theory. There exist nice interpretations of these structures as combinatorial and geometric objects and both conjectures can be reformulated in this framework. Namely, from a graph theoretical point of view, the domains of prime event structures correspond exactly to median graphs; from a geometric point of view, these domains are in bijection with CAT(0) cube complexes.

A necessary condition for the conjecture to be true is that domains of regular event structures admit a regular nice labeling (which corresponds to a special coloring of the hyperplanes of the associated CAT(0) cube complex). To disprove these conjectures, we describe a regular event domain that does not admit a regular nice labeling. Our counterexample is derived from an example by Wise [10, 11] of a nonpositively curved square complex $\mathbf{X}$ with six squares, whose edges are colored in five colors, and whose universal cover $\widetilde{\mathbf{X}}$ is a CAT(0) square complex containing a particular plane with an aperiodic tiling. We prove that other counterexamples to Thiagarajan's conjecture arise from aperiodic 4-way deterministic tile sets of Kari and Papasoglu [6] and Lukkarila [7].

On the positive side, we show that event structures obtained as unfoldings of finite 1-safe Petri nets correspond to the finite special cube complexes. This subclass of nonpositively curved cube complexes was introduced by Haglund and Wise [4, 5] in geometric group theory and is characterized by simple combinatorial properties satisfied by the hyperplanes. Using the breakthrough results by Agol [1] based on special cube complexes, we prove that Thiagarajan's conjecture is true for regular event structures whose domains occur as principal filters of hyperbolic CAT(0) cube complexes which are universal covers of finite nonpositively curved cube complexes.

Joint work with Victor Chepoi.

The full version of this paper is available on ArXiv [2], an extended abstract appeared in the proceedings of ICALP 2017 [3].

References

1. Agol, I.: The virtual Haken conjecture. Doc. Math. **18**, 1045–1087 (2013). with an appendix by Ian Agol, Daniel Groves, and Jason Manning
2. Chalopin, J., Chepoi, V.: A counterexample to Thiagarajan's conjecture on regular event structures. arXiv preprint (2016)
3. Chalopin, J., Chepoi, V.: A counterexample to Thiagarajan's conjecture on regular event structures. In: ICALP. LIPIcs, vol. 80, pp. 101:1–101:14. Schloss Dagstuhl -Leibniz-Zentrum für Informatik (2017)
4. Haglund, F., Wise, D.: Special cube complexes. Geom. Funct. Anal. **17**(5), 1551–1620 (2008)
5. Haglund, F., Wise, D.: A combination theorem for special cube complexes. Annals Math. **176** (3), 1427–1482 (2012)
6. Kari, J., Papasoglu, P.: Deterministic aperiodic tile sets. GAFA, Geom. Funct. Anal. **9**(2), 353–369 (1999)
7. Lukkarila, V.: The 4-way deterministic tiling problem is undecidable. Theor. Comput. Sci. **410**(16), 1516–1533 (2009)
8. Thiagarajan, P.: Regular trace event structures. Technical report BRICS RS-96-32, Computer Science Department, Aarhus University, Aarhus, Denmark (1996)
9. Thiagarajan, P.: Regular event structures and finite petri nets: a conjecture. In: Brauer, W., Ehrig, H., Karhumäki, J., Salomaa, A. (eds.) Formal and Natural Computing. LNCS, vol. 2300, pp. 244–256. Springer, Heidelberg (2002)
10. Wise, D.: Non-positively curved squared complexes, aperiodic tilings, and non-residually finite groups. Ph.D. thesis, Princeton University (1996)
11. Wise, D.: Complete square complexes. Comment. Math. Helv **82**(4), 683–724 (2007)

Safety Verification for Deep Neural Networks with Provable Guarantees (Extended Abstract)

Marta Kwiatkowska

Department of Computing Science, University of Oxford, UK

Deep neural networks have achieved impressive experimental results in image classification, but can surprisingly be unstable with respect to adversarial perturbations, that is, minimal changes to the input image that cause the network to misclassify it. With potential applications including perception modules and end-to-end controllers for self-driving cars, this raises concerns about their safety. This lecture will describe progress with developing automated verification techniques for deep neural networks to ensure safety of their classification decisions with respect to image manipulations, for example scratches or changes to camera angle or lighting conditions, that should not affect the classification. The techniques exploit Lipschitz continuity of the networks and aim to approximate, for a given set of inputs, the reachable set of network outputs in terms of lower and upper bounds, in anytime manner, with provable guarantees. We develop novel algorithms based on games and global optimisation, and evaluate them on state-of-the-art networks.

Robustness of neural networks is an active topic of investigation and a number of approaches have been proposed to search for adversarial examples. They are based on computing the gradients [1, 3], computing a Jacobian-based saliency map [6], transforming the existence of adversarial examples into an optimisation problem [2], and transforming the existence of adversarial examples into a constraint solving problem [5]. In contrast, this lecture reports on research that aims to rule out the existence of adversarial examples, which approaches based on heuristic search are not able to achieve. In particular, we will adopt the definition of safety based on pointwise robustness introduced in [4], where the first practical automated verification method was developed, based on discretising the neighbourhood and searching it exhaustively in a layer-by-layer manner. A brief overview will also be given of two approaches that utilise Lipschitz continuity, one based on global optimisation [7], and capable of expressing the safety of [4] as well as reachability, and the other [8, 9] on reducing dimensionality by working with black or grey box feature extraction and searching for adversarial examples using a two-player game, where the first player targets the features and the second targets pixels within the feature. The game tree is traversed using Monte Carlo tree search and variants of A* and Alpha-Beta pruning, which produces successive lower and upper bounds on the maximum safe radius with asymptotic convergence guarantees.

References

1. Biggio, B., et al.: Evasion attacks against machine learning at test time. In: Blockeel, H., Kersting, K., Nijssen, S., Železný, F. (eds.) ECML PKDD 2013. LNCS, vol. 8190, pp. 387–402. Springer, Heidelberg (2013)
2. Nicholas, C., David, W.: Towards evaluating the robustness of neural networks. In: 2017 IEEE Symposium on Security and Privacy (SP), pp. 39–57. IEEE (2017)
3. Goodfellow, I.J., Shlens, J., Szegedy, C.: Explaining and harnessing adversarial examples. CoRR
4. Huang, X., Kwiatkowska, M., Wang, S., Wu, M.: Safety verification of deep neural networks. In: Majumdar, R., Kunčak, V. (eds.) CAV 2017. LNCS, vol. 10426, pp. 3–29. Springer, Cham (2017)
5. Katz, G., Barrett, C., Dill, D.L., Julian, K., Kochenderfer, M.J.: Reluplex: an efficient SMT solver for verifying deep neural networks. In: Majumdar, R., Kunčak, V. (eds.) CAV 2017. LNCS, vol. 10426, pp. 97–117. Springer, Cham (2017)
6. Papernot, N., McDaniel, P., Jha, S., Fredrikson, M., Celik, Z.B., Swami, A: The limitations of deep learning in adversarial settings. In: 2016 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 372–387. IEEE (2016)
7. Ruan, W., Huang, X., Kwiatkowska, M.: Reachability analysis of deep neural networks with provable guarantees. In: International Joint Conference on Artificial Intelligence (2018)
8. Wicker, M., Huang, X., Kwiatkowska, M.: Feature-guided black-box safety testing of deep neural networks. In: Beyer, D., Huisman, M. (eds.) TACAS 2018. LNCS, vol. 10805, pp. 408–426. Springer, Cham (2018)
9. Wu, M., Wicker, M., Ruan, W., Huang, X., Kwiatkowska, M.: A game-based approximate verification of deep neural networks with provable guarantees. CoRR, abs/1807.03571 (2018)

Contents