

Non-Zero-Sum-Games and Control

Edited by

Krishnendu Chatterjee¹, Stéphane Lafortune², Nicolas Markey³,
and Wolfgang Thomas⁴

1 IST Austria – Klosterneuburg, AT, Krishnendu.Chatterjee@ist.ac.at

2 University of Michigan – Ann Arbor, US, stephane@umich.edu

3 ENS – Cachan, FR, markey@lsv.ens-cachan.fr

4 RWTH Aachen, DE, thomas@cs.rwth-aachen.de

Abstract

In this report, the program, research issues, and results of Dagstuhl Seminar 15061 “Non-Zero-Sum-Games and Control” are described. The area of non-zero-sum games is addressed in a wide range of topics: multi-player games, partial-observation games, quantitative game models, and – as a special focus – connections with control engineering (supervisory control).

Seminar February 1–6, 2015 – <http://www.dagstuhl.de/15061>

1998 ACM Subject Classification B.6.3 Design Aids, F.1.2 Modes of Computation, I.2.2 Automatic Programming, I.2.8 Problem Solving, Control Methods, and Search

Keywords and phrases non-zero-sum games, infinite games, multi-player games, partial-observation games, quantitative games, controller synthesis, supervisory control

Digital Object Identifier 10.4230/DagRep.5.2.1

Edited in cooperation with Benedikt Brütsch


1 Executive Summary

Krishnendu Chatterjee

Stéphane Lafortune

Nicolas Markey

Wolfgang Thomas

License  Creative Commons BY 3.0 Unported license
© Krishnendu Chatterjee, Stéphane Lafortune, Nicolas Markey, and Wolfgang Thomas

Games played on graphs provide the framework to study a wide range of problems that are central in computer science, for example, reactive synthesis, well-formedness of systems, checking compatibility of behavioral type systems, etc. The traditional study of games has been for two-player zero-sum perfect-information deterministic games with Boolean objectives (where a win of one player coincides with a loss by the other player). Fundamental results of this theory are contributions of automata theory that go back to the 1960’s (Büchi, McNaughton, Rabin).

Significant progress has been achieved in the last few decades both in terms of theoretical results (understanding the complexity of such games, developing efficient algorithms) as well as their practical applicability (in reactive synthesis and controller synthesis). The current research directions explore several important extensions of the traditional study, namely, multi-player games, games with partial-observation, quantitative aspects in games, as well as application of game results in other domains. In this regard, the connection to control theory is important: The methodology of “supervisory control” has developed in parallel



Except where otherwise noted, content of this report is licensed under a Creative Commons BY 3.0 Unported license

Non-Zero-Sum-Games and Control, *Dagstuhl Reports*, Vol. 5, Issue 2, pp. 1–25

Editors: Krishnendu Chatterjee, Stéphane Lafortune, Nicolas Markey, and Wolfgang Thomas



DAGSTUHL
REPORTS

Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

to the emergence of the game-theoretic approach, and a joint and integrating view of these closely related branches of research seemed overdue.

The Dagstuhl Seminar “Non-Zero Sum Games and Control” addressed these developments, with a particular emphasis on the connections to control theory. The response to the call for participation was very positive, and the 42 scientists joining the seminar represented the full range of topics mentioned above. There was a very good mixture between young and “established” researchers, and the participation of female researchers (making a quarter) was high (in the context of computer science). In order to support the understanding between the different research branches, it was decided to have on each half-day at least one survey talk, outlining a field and describing general challenges; some of these talks were contributed by young researchers. The speakers of the survey talks were Rüdiger Ehlers, Tom Henzinger, Barbara Jobstmann, Stéphane Lafortune, Kim Larsen, Peter Bro Miltersen, Jean-François Raskin, Armando Solar-Lezama, John Thistle, and Ufuk Topcu. Furthermore, a special evening session was organized on challenges in supervisory control. Besides the aim of joining and integrating different tracks of research in the area, an important objective of the seminar was to bring together (at least some) members of two large research communities in the area, namely the community of automata, logic, and games in Europe and the U.S. research network EXCAPE (Expeditions in Computer Augmented Program Engineering).

During the seminar, several small circles of participants started or continued joint work. As a general result of the seminar, confirmed by many positive and even enthusiastic comments of participants after the seminar, one may say that a much better understanding and appreciation between the various research branches was established. As one of the participants put it, the seminar was “eye-opening”.

As an overview of the areas covered in the talks, we give a short description of the topics studied in the seminar.

Multi-player games

The study of multi-player games is an important extension of the two-player setting. In terms of theoretical study it gives rise to a rich class of questions related to different notions of equilibria, studying computability and complexity results for them, as well as different logics to express them. In terms of practical applicability, various notions of synthesis such as rational synthesis, secure equilibria, assume-guarantee synthesis, assume-admissible synthesis, etc. have been developed to apply the results of multi-player games for synthesis of component-based systems.

Partial-observation games

Partial-observation games extend perfect-information games where players do not have perfect knowledge about the game. This is particularly relevant in control theory, where the controller does not have access to private variables of the plant. The results of partial-observation games have been recently extended to the stochastic setting, as well as for finite-memory strategies, leading to a new framework which can potentially solve interesting applications from the control domain.

Quantitative game models

These are a prominent class of game models for applications to verification and synthesis. In particular, taking real-time constraints into account is especially important for such applications. Timed automata and timed games have already played an important role, as

they are a convenient and expressive model enjoying efficient algorithms. Statistical model checking in particular offers a very effective technique for strategy optimization. Robustness analysis of timed models makes the verification process even more faithful.

- Weighted timed games extend timed games with the ability of modeling other quantitative aspects of cyber-physical systems. While the expressive power is greatly improved, the verification and synthesis problems get much more complex than for plain timed automata. Still, algorithms sometimes exist for *approximating* the optimal cost, which in most practical situations is sufficient.
- Timed automata have now reached maturity. Powerful data-structures and efficient symbolic algorithms have been designed to develop efficient algorithms. Statistical model checking is now also used in tools for efficiently optimizing strategies. These tools can now be applied on real-life scenarios, e.g. in home automation and motion planning.
- Probabilistic models form another important class of models of particular interest for representing and reasoning about e.g. systems involving stochastic behaviors. Efficient algorithms have recently been developed for diagnosing probabilistic automata, or for synthesizing strategies that guarantee good performance level with sufficient probability in Markov Decision Processes.

In the quantitative setting, the range of objectives is large; there are mean-payoff objectives, energy objectives, mean-payoff of energy objectives, their Boolean combinations, and combinations of quantitative (e.g., stochastic) semantics with adversarial semantics.

Other domains

Theoretical results developed for games have been generalized to problems in other settings as well. A prime example is that the lower bound for strategy improvement algorithms for parity games was modified to obtain lower bounds for linear-programming solutions, and recent results show that exploiting structures of Markov decision processes it can be established that several classical rules for linear-programming algorithms solve PSPACE-complete problems.

Control engineering

In the field of control engineering, research on supervisory control of discrete event systems and on formal methods in feedback control has recently emphasized distributed and decentralized control architectures that more accurately capture the physical constraints arising in cyber-physical and networked control systems. In these architectures, a set of controllers, possibly with different run-time information about the system, cooperate as a team in order to achieve a specification (either qualitative or quantitative objective) on the entire system behavior, in the presence of a reactive environment. For instance, costly sensors and actuators, as well as costly communication, lead to challenging synthesis problems, both conceptually (e.g., characterization of the information structure) and computationally (e.g., distributed synthesis of the controllers). Another important consideration is to ensure robustness of the synthesized implementation with respect to classes of disturbances on the controlled system.

Researchers are still trying to establish the precise boundary between decidable and undecidable problems in this research domain. It is known that synthesis for both safety and a form of liveness termed non-blockingness, well-understood in a centralized-information setting, becomes undecidable in a decentralized-information setting. But the decidability of special classes of this problem is still an open issue. Establishing concrete bridges between the theory of partial-observation games and such decentralized/distributed control problems for

discrete abstractions of cyber-physical systems is an important research issue, both in terms of answering open undecidability questions and in terms of developing efficient synthesis procedures for decidable problems. Similarly, problems of intrusion by malicious agents into control architectures (e.g., taking over actuators or sensors) also lead to new classes of problems where the theory of games with quantitative objectives can be leveraged.

Recently-developed synthesis techniques for “correct-by-construction” controllers in engineering systems have exploited game formulations between the set of controllers on the one hand and the system/environment on the other hand. Related approaches have considered synthesis of the “complete” controller implementation from a “partial” implementation and a sample set of desired behaviors in the reactive environment under consideration.

2 Table of Contents

Executive Summary

Krishnendu Chatterjee, Stéphane Lafortune, Nicolas Markey, and Wolfgang Thomas 1

Overview of Talks

Diagnosis of probabilistic systems <i>Nathalie Bertrand</i>	7
Infinite games with finite knowledge gaps <i>Dietmar Berwanger</i>	7
On the value problem in weighted timed games <i>Patricia Bouyer-Decitre</i>	8
The Complexity of Admissibility in Omega-Regular Games <i>Romain Brenguier</i>	8
Weak subgame perfect equilibria in quantitative multiplayer games <i>Véronique Bruyère</i>	8
Robustness and Cooperation <i>Rüdiger Ehlers</i>	9
The Complexity of the Simplex Method <i>John Fearnley</i>	9
Two-Player Perfect-Information Zero-Sum Shift-Invariant Submixing Stochastic Games Are Half-Positional <i>Hugo Gimbert</i>	10
Quantitative Sabotage Games <i>Axel Haddad</i>	10
Games Everywhere <i>Thomas Anton Henzinger</i>	11
The Big Match in small space <i>Rasmus Ibsen-Jensen</i>	11
Quantitative Objectives In Reactive Synthesis <i>Barbara Jobstmann</i>	12
Distributed Synthesis in Continuous Time <i>Jan Krčál</i>	12
Fast learning of small strategies <i>Jan Křetínský</i>	13
Open Problems in Supervisory Control of Partially-Observed Discrete Event Systems <i>Stéphane Lafortune</i>	13
From Timed Games to Stochastic Hybrid Games <i>Kim Guldstrand Larsen</i>	13
Average Energy in Weighted Games <i>Simon B. Laursen</i>	14
Temporal logics for non-zero-sum games <i>Nicolas Markey</i>	15

Computer Poker and Computational Game Theory <i>Peter Bro Miltersen</i>	15
Why Negatively-Priced Timed Games Are Hard <i>Benjamin Monmege</i>	15
Correct-by-construction controller synthesis for highly dynamic systems: an application in automotive safety systems <i>Necmiye Ozay</i>	16
Fun with funnels <i>Nicolas Perrin</i>	17
Percentile Queries in Multi-Dimensional Markov Decision Processes <i>Mickael Randour</i>	17
Beyond Two-Player Zero-sum Games. Motivations and Highlights of Recent Results <i>Jean-François Raskin</i>	17
Synthesis for Human-in-the-Loop Control Systems <i>Dorsa Sadigh</i>	19
Symbolic Quantitative Robustness Analysis of Timed Automata <i>Ocan Sankur</i>	19
Quantitative Verification in Rational Environments <i>Sven Schewe</i>	19
Supervisory Control Synthesis for Deterministic Context Free Specification Languages – Enforcing Controllability Least Restrictively <i>Anne-Kathrin Schmuck</i>	20
Program Synthesis for Games and Control <i>Armando Solar-Lezama</i>	20
Home Automation Synthesis: From Toy Examples to Realistic Scenarios <i>Jiří Srba</i>	21
Games among arbitrarily many players <i>John G. Thistle</i>	21
Correct-by-construction control protocol synthesis for autonomous systems <i>Ufuk Topcu</i>	22
Refinement Calculus for Reactive Systems <i>Stavros Tripakis</i>	22
Synthesizing Finite-state Protocols from Scenarios and Requirements <i>Stavros Tripakis</i>	23
Omega-regular and Max-regular Delay Games <i>Martin Zimmermann</i>	23
Working Groups	
Discussion on Supervisory Control and Reactive Synthesis <i>Stéphane Lafortune</i>	24
Participants	25

3 Overview of Talks

3.1 Diagnosis of probabilistic systems

Nathalie Bertrand (INRIA Rennes – Bretagne Atlantique, FR)

License © Creative Commons BY 3.0 Unported license
© Nathalie Bertrand

Fault diagnosis aims at detecting the occurrence of faulty events in partially observable systems. When it comes to probabilistic models, one can relax the notion of diagnosability by requiring a set of ambiguous sequences of null measure. In our talk, we answered the following questions: How to check for diagnosability of a probabilistic system? And in case it is not diagnosable, can one control a system so that it is?

References

- 1 N. Bertrand, S. Haddad and E. Lefaucheu. Foundation of Diagnosis and Predictability in Probabilistic Systems. In *Proc. of FSTTCS'14*, LIPIcs, Schloss Dagstuhl, 2014. DOI: 10.4230/LIPIcs.FSTTCS.2014.417
- 2 N. Bertrand, E. Fabre, S. Haar, S. Haddad and L. Helouet. Active diagnosis for probabilistic systems. In *Proc. of FoSSaCS'14*, LNCS, Springer, 2014. DOI: 10.1007/978-3-642-54830-7_2

3.2 Infinite games with finite knowledge gaps

Dietmar Berwanger (ENS – Cachan, FR)

License © Creative Commons BY 3.0 Unported license
© Dietmar Berwanger

Joint work of Berwanger, Dietmar; Mathew, Anup Basil

Main reference D. Berwanger, A. B. Mathew, “Infinite games with finite knowledge gaps,” arXiv:1411.5820v1 [cs.GT], 2014.

URL <http://arxiv.org/abs/1411.5820v1>

Infinite games where several players seek to coordinate under imperfect information are known to be intractable, unless the information flow is severely restricted. Examples of undecidable cases typically feature a situation where players become uncertain about the current state of the game, and this uncertainty lasts forever.

In contrast, we consider games where the players attain certainty about the current state over and over again, along every play. This leads to a new class on which the distributed synthesis problem is solvable. We show that the question of whether a game belongs to the class is NLOGSPACE-complete, and in that case, it is NEXPTIME-complete to decide whether a joint winning strategy exists.

3.3 On the value problem in weighted timed games

Patricia Bouyer-Decitre (CNRS, FR)

License © Creative Commons BY 3.0 Unported license
© Patricia Bouyer-Decitre

Joint work of Bouyer, Patricia; Jaziri, Samy; Markey, Nicolas

Main reference P. Bouyer, S. Jaziri, N. Markey, “On the Value Problem in Weighted Timed Games,” Research Report LSV-14-12, Laboratoire Spécification et Vérification, ENS Cachan, France, 2014.

URL <http://www.lsv.ens-cachan.fr/~bouyer/mes-publis.php?l=fr&onlykey=rr-lsv-14-12>

In this talk, I present the model of weighted timed games. I give an overview of rather old results about the value problem in such games, and then present our new results, that concern the approximability of the value in weighted timed games, under a slight restriction on the weight.

3.4 The Complexity of Admissibility in Omega-Regular Games

Romain Brenguier (Free University of Brussels, BE)

License © Creative Commons BY 3.0 Unported license
© Romain Brenguier

Joint work of Brenguier, Romain; Raskin, Jean-François; Sassolas, Mathieu

Main reference R. Brenguier, J. Raskin, M. Sassolas, “The complexity of admissibility in Omega-regular games,” in Proc. of the Joint Meeting of the 23rd EACSL Annual Conf. on Computer Science Logic (CSL’14) and the 29th Annual ACM/IEEE Symp. on Logic in Computer Science (LICS’14), pp. 21:1–23:10, ACM, 2014; pre-print available as arXiv:1304.1682v3 [cs.GT].

URL <http://dx.doi.org/10.1145/2603088.2603143>

URL <http://arxiv.org/abs/1304.1682v3>

Iterated admissibility is a well-known and important concept in classical game theory, e.g. to determine *rational* behaviors in multi-player matrix games. As recently shown by Berwanger, this concept can be soundly extended to infinite games played on graphs with ω -regular objectives. In this paper, we study the algorithmic properties of this concept for such games. We settle the exact complexity of natural decision problems on the set of strategies that survive iterated elimination of dominated strategies. As a byproduct of our construction, we obtain automata which recognize all the possible outcomes of such strategies.

3.5 Weak subgame perfect equilibria in quantitative multiplayer games

Véronique Bruyère (University of Mons, BE)

License © Creative Commons BY 3.0 Unported license
© Véronique Bruyère

We study subgame perfect equilibria (SPE), and variants (weak SPE and very weak SPE), in quantitative multiplayer turn-based games played on graphs. We give a characterization of the outcomes of such equilibria (as a Folk theorem for Nash equilibria). This characterization allows us to construct finite-memory SPE in quantitative reachability games.

3.6 Robustness and Cooperation

Rüdiger Ehlers (Universität Bremen, DE)

License © Creative Commons BY 3.0 Unported license
© Rüdiger Ehlers

Joint work of Roderick Bloem; Rüdiger Ehlers; Gangyuan Jing; Robert Könighofer; Hadas Kress-Gazit; Ufuk Topcu; Kai Weng Wong

In reactive synthesis, a correct-by-construction system is computed from a specification and an environment model. The synthesized system is guaranteed to satisfy its specification if the environment’s behavior is covered by the model. Unfortunately, when theory meets practice, synthesized controllers often exhibit unsuitable behavior. Environment assumptions may sometimes be violated temporarily in the field, and there is no requirement for the controller to behave correctly in such a case. Equally problematic are controllers that try to force the environment to violate its assumptions or needlessly rely on liveness assumptions to hold, which leads to bad performance of controllers in practice. Yet, such controllers are possible solutions to the standard synthesis problem.

The talk addresses these issues and discusses results on synthesizing controllers that are robust, eager, and cooperative. Games with quantitative objectives are mostly avoided along the way, so the approaches leave room for further combination with other quantitative or qualitative optimization objectives.

3.7 The Complexity of the Simplex Method

John Fearnley (University of Liverpool, GB)

License © Creative Commons BY 3.0 Unported license
© John Fearnley

Joint work of Fearnley, John; Savani, Rahul

Main reference J. Fearnley, R. Savani, “The Complexity of the Simplex Method,” arXiv:1404.0605v2 [cs.DS], 2014.

URL <http://arxiv.org/abs/1404.0605v2>

The simplex method is a well-studied and widely-used pivoting method for solving linear programs. When Dantzig originally formulated the simplex method, he gave a natural pivot rule that pivots into the basis a variable with the most violated reduced cost. In their seminal work, Klee and Minty showed that this pivot rule takes exponential time in the worst case. We prove two main results on the simplex method. Firstly, we show that it is PSPACE-complete to find the solution that is computed by the simplex method using Dantzig’s pivot rule. Secondly, we prove that deciding whether Dantzig’s rule ever chooses a specific variable to enter the basis is PSPACE-complete. We use the known connection between Markov decision processes (MDPs) and linear programming, and an equivalence between Dantzig’s pivot rule and a natural variant of policy iteration for average-reward MDPs. We construct MDPs and show PSPACE-completeness results for single-switch policy iteration, which in turn imply our main results for the simplex method.

3.8 Two-Player Perfect-Information Zero-Sum Shift-Invariant Submixing Stochastic Games Are Half-Positional

Hugo Gimbert (University of Bordeaux, FR)

License © Creative Commons BY 3.0 Unported license
© Hugo Gimbert

Joint work of Gimbert, Hugo; Kelmendi, Edon

Main reference H. Gimbert, E. Kelmendi, “Two-Player Perfect-Information Shift-Invariant Submixing Stochastic Games Are Half-Positional,” arXiv:1401.6575v1 [cs.GT], 2014.

URL <http://arxiv.org/abs/1401.6575v1>

We consider zero-sum stochastic games with perfect information and finitely many states and actions. The payoff is computed by a payoff function which associates to each infinite sequence of states and actions a real number. We prove that if the the payoff function is both shift-invariant and submixing, then the game is half-positional, i.e., the first player has an optimal strategy which is both deterministic and stationary. This result relies on the existence of epsilon-subgame-perfect equilibria in shift-invariant games, a second contribution of the paper.

3.9 Quantitative Sabotage Games

Axel Haddad (Free University of Brussels, BE)

License © Creative Commons BY 3.0 Unported license
© Axel Haddad

Joint work of Brihaye, Thomas; Geeraerts, Gilles; Haddad, Axel; Monmege, Benjamin; Perez, Guillermo; Renault, Gabriel

We study a model of evolving environment systems called quantitative sabotage games. Sabotage games have been introduced in an essay by Johan van Benthem [1] as special games on evolving arenas: whereas one player (Walker) moves from vertex to vertex following the topology of a finite graph, trying to reach a special target vertex, the other player (Saboteur) takes out an edge after each step. Hence, this game is naturally finite, and stops after a bounded number of steps. It has been shown to be PSPACE-complete to solve these games [2] as well as a randomized variant of it [3]. Our aim is to extend the study of sabotage games to deal with behavior of infinite lengths. To that purpose, the process of sabotage has to be changed to incorporate possibly unbounded behaviors. Our choice is to handle this by introducing quantities. Whereas Walker continues to move along the edges, Saboteur has now a budget of tokens that he puts on vertices of the graphs, and is allowed to move one token at every step. The first player wants to minimize its average number of tokens he sees during the whole play.

If the budget is fixed a priori, the problem of knowing whether the first player has a strategy to obtain an average value below a given threshold seems to be solvable in polynomial time. The static version of this problem, where the second player simply drops his tokens on the graph and leaves them as they are forever, is coNP-complete. In the general case, we show that the problem is EXPTIME-complete (we did not have the EXPTIME-hardness at the moment of the talk).

An EXPTIME algorithm can be obtained by studying the configuration graph of this game and solving the induced Mean-Payoff game. The EXPTIME-hardness is obtained by studying a variant of those games where Walker wants to never see a token. We show that such safety games can be encoded into quantitative sabotage games, and furthermore we

reduce an EXPTIME-complete problem, finding the winner in a two-player version of the SAT problem [4], into this variant.

References

- 1 Johan van Benthem. An essay on sabotage and obstruction. In *Mechanizing Mathematical Reasoning, Essays in Honor of Jörg H. Siekmann on the Occasion of His 60th Birthday*, vol. 2605 of *LNCS*, pp. 268–276, Springer, 2005. DOI: 10.1007/978-3-540-32254-2_16
- 2 Christof Löding and Philipp Rohde. Solving the Sabotage Game Is PSPACE-Hard. In *Proc. of MFCS'03*, vol. 2747 of *LNCS*, pp. 531–540, Springer, 2003. DOI: 10.1007/978-3-540-45138-9_47
- 3 Dominik Klein, Frank G. Radmacher, and Wolfgang Thomas. Moving in a network under random failures: A complexity analysis. *Science of Computer Programming*, 77(7-8):940–954, 2012. DOI: 10.1016/j.scico.2010.05.009
- 4 Larry J. Stockmeyer and Ashok K. Chandra. Provably Difficult Combinatorial Games. *SIAM Journal on Computing*, 8(2):151–174, 1979. DOI: 10.1137/0208013

3.10 Games Everywhere

Thomas Anton Henzinger (IST Austria – Klosterneuburg, AT)

License  Creative Commons BY 3.0 Unported license
© Thomas Anton Henzinger

We survey some uses of graph games with qualitative and quantitative, zero-sum and non-zero-sum objectives for specifying and verifying reactive systems (game logics), defining and checking the well-formedness and compatibility of reactive systems (receptiveness and interface theories), refining and synthesizing reactive systems (simulation games and supervisory control).

3.11 The Big Match in small space

Rasmus Ibsen-Jensen (IST Austria – Klosterneuburg, AT)

License  Creative Commons BY 3.0 Unported license
© Rasmus Ibsen-Jensen

Joint work of Ibsen-Jensen, Rasmus; Koucky, Michal; Hansen, Kristoffer Arnsfelt

The talk will be on the well-studied game the Big Match, a concurrent, zero-sum, two-player, mean-payoff game. It is known that no finite memory strategy exists that achieves anything non-trivial. All previously known ε -optimal strategies uses space $\Omega(\log T)$ in round T . The talk will be about an ε -optimal strategy, in the limsup sense, that uses space $O(s(T))$ in round T whp., for any unbounded, nondecreasing function s . The talk will also describe an ε -optimal strategy, in the liminf sense, that uses space $O(\log \log T)$ in round T whp.

The talk will then consider the open problem of generalising the result to arbitrary concurrent, zero-sum, two-player, mean-payoff games and the problems encountered while trying to do so.

3.12 Quantitative Objectives In Reactive Synthesis

Barbara Jobstmann (EPFL Lausanne, CH)

License © Creative Commons BY 3.0 Unported license
© Barbara Jobstmann

Joint work of Bloem, Roderick; Chatterjee, Krishnendu; Henzinger, Thomas; Singh, Rohit; Greimel, Karin; von Essen, Christian

Reactive Synthesis aims to automatically construct a reactive system from a temporal specification that describes the desired functional behavior of the system. Graph-based games are at the heart of many synthesizers for reactive systems. In the classical approach a synthesizer can produce any system that satisfies the specification. However, in many settings users prefer one correct system over another, e.g., among two correct systems, one might prefer the more robust or more efficient system.

In this talk I will first give a short introduction to Reactive Synthesis. Then, I will present quantitative objectives to express default behavior, robustness, and efficiency, and discuss the games that result from these objectives. Finally, I will present an approach to select repairs for a faulty program, a problem that can be solved using reactive synthesis. The novelty of this approach is that it requires a repair to keep all the correct behaviors of the faulty program, which enables us to synthesize meaningful repairs, even for incomplete specifications.

3.13 Distributed Synthesis in Continuous Time

Jan Krčál (Universität des Saarlandes, DE)

License © Creative Commons BY 3.0 Unported license
© Jan Krčál

Joint work of Hermanns, Holger; Krčál, Jan; Vester, Steen

Distributed synthesis has been studied for more than 25 years. Various forms of communication of distributed agents have been discussed. However, the focus of previous foundational approaches to distributed synthesis has abstracted the flow of time to a discrete setting. In this paper, we introduce a formalism modelling communication of distributed agents strictly in continuous-time. Within this framework, we study the problem of synthesizing local strategies for individual agents such that a specified set of goal states is reached, or reached with at least a given probability. The flow of time is modelled explicitly based on continuous-time randomness, with two natural implications: First, the non-determinism stemming from interleaving of communication steps disappears. Second, when we restrict to a subclass of non-urgent models, both the qualitative and quantitative reachability problem can be solved in EXPTIME. The crucial observation is that explicit continuous time enables the players to communicate their states by delaying synchronization, turning it into full-observation setting. In general, the quantitative problem is undecidable for two or more players and the qualitative problem is EXPTIME-hard for two players and undecidable for three or more players.

3.14 Fast learning of small strategies

Jan Křetínský (*IST Austria – Klosterneuburg, AT*)

License  Creative Commons BY 3.0 Unported license
© Jan Křetínský

Joint work of Brázdil, Tomáš; Chatterjee, Krishnendu; Chmelík, Martin; Fellner, Andreas; Forejt, Vojtěch; Křetínský, Jan; Kwiatkowska, Marta; Parker, David; Ujma, Mateusz

In verification, precise analysis is required, but the algorithms usually suffer from scalability issues. In machine learning, scalability is achieved, but with only very weak guarantees. We show how to merge the two philosophies and profit from both. In this talk, we focus on $1\frac{1}{2}$ -player games (Markov decision processes). We show how to learn ε -optimal strategies fast and how to represent them concisely so that some understanding of the behaviour and debugging information can be extracted.

References

- 1 Tomáš Brázdil, Krishnendu Chatterjee, Martin Chmelík, Andreas Fellner, and Jan Křetínský. Counterexample Explanation by Learning Small Strategies in Markov Decision Processes. *CoRR*, 2015. <http://arxiv.org/abs/1502.02834>
- 2 Tomáš Brázdil, Krishnendu Chatterjee, Martin Chmelík, Vojtěch Forejt, Jan Křetínský, Marta Z. Kwiatkowska, David Parker, and Mateusz Ujma. Verification of Markov Decision Processes Using Learning Algorithms. In *Proc. of ATVA '14*, vol. 8837 of *LNCS*, pp. 98–114, Springer, 2014. DOI: 10.1007/978-3-319-11936-6_8

3.15 Open Problems in Supervisory Control of Partially-Observed Discrete Event Systems

Stéphane Lafortune (*University of Michigan – Ann Arbor, US*)

License  Creative Commons BY 3.0 Unported license
© Stéphane Lafortune

Joint work of Lafortune, Stéphane; Yin, Xiang

We present a set of unsolved problems in the area of supervisory control of discrete event systems in control engineering. We consider systems with partial observation and limited controllability, representing the limited sensing and actuation capabilities of the engineering system to be controlled. We wish to address safety and nonblocking specifications in a maximally permissive manner. We also wish to consider a specification on the minimum required behavior for the controlled system. We list open problems in centralized and decentralized control architectures in the context of the above requirements.

3.16 From Timed Games to Stochastic Hybrid Games

Kim Guldstrand Larsen (*Aalborg University, DK*)

License  Creative Commons BY 3.0 Unported license
© Kim Guldstrand Larsen

In this talk the focus is on extensions of the well-established formalism of timed automata towards games. The formalism of (stochastic) timed automata has been extensively used for modelling several real-time controllers and communication protocols with efficient algorithms

as found in the tool UPPAAL and its branch UPPAAL SMC allowing for automatic (statistical) model checking of a range of desired correctness and performance properties of these complex systems.


Moving to the setting of games marks a paradigm shift, where control programs that are correct-by-construction are automatically synthesized from the desired properties (objectives). The talk provides insight into the symbolic on-the-fly algorithm used in the tool UPPAAL TIGA for efficient construction of winning control strategies with respect to reachability, safety, time-bounded reachability as well as Büchi conditions. In fact the tool has previously been applied to the synthesis of control strategies for a number of industrial cases (including control for pig stables, and control for hydraulic pumps) that exhibit performance significantly better than the (at the time) current industrial solution.

The talk also presents the newest branch of the UPPAAL tool suit, namely UPPAAL STRATEGO. In STRATEGO strategies are first-class citizens that may be named and used to constrain any existing type of model checking query of UPPAAL and UPPAAL SMC; i.e. additional (performance) properties of a game under a synthesized strategy may be performed. In addition, given a (most permissive) strategy ensuring given (hard real-time) safety constraints – and obtained by symbolic methods from UPPAAL TIGA – the tool may synthesize sub-strategies that (near-) optimize the expectation of additional performance measures – e.g. total energy consumed, waiting time of given component. This optimization is made using reinforcement learning, a well-established technique from machine learning.

The methods of performance analysis (using UPPAAL SMC) and optimization (using UPPAAL STRATEGO) has been extended to stochastic hybrid automata/games. Future work includes strategy learning under partial observability, thus addressing the need for compact control programs. Also, the use of statistical methods for rare event estimation of stochastic timed automata, as well as data structures for more general classes of strategies are work to be dealt with in near future.

3.17 Average Energy in Weighted Games

Simon B. Laursen (Aalborg University, DK)

License  Creative Commons BY 3.0 Unported license

© Simon B. Laursen

Joint work of Laursen, Simon; Bouyer, Patricia; Larsen, Kim G.; Markey, Nicolas; Randour, Mickael

We consider a two player game on a weighted graph, where the goal for Player 1 is to keep the average accumulated weight under a given threshold, we name this objective average energy. We describe how this objective relates to the mean-payoff and total-payoff objectives. Our results include complexity and memory analyses of problems related to average energy games combined with lower and upper bound energy constraints.

3.18 Temporal logics for non-zero-sum games

Nicolas Markey (*ENS – Cachan, FR*)

License © Creative Commons BY 3.0 Unported license
© Nicolas Markey

Joint work of Brihaye, Thomas; Da Costa-Lopes, Arnaud; Laroussinie, François; Markey, Nicolas

Several extensions of the temporal logics CTL have been proposed in the recent years to express properties of multi-player games. In this talk I develop one such extension, ATL with strategy contexts, and propose a generic technique for dealing with it. I then show how this technique is also applicable to Strategy Logic. I conclude with a list of directions for further research.

References

- 1 François Laroussinie and Nicolas Markey. Quantified CTL: Expressiveness and Complexity. *Logical Methods in Computer Science* 10(4:17), 2014.
- 2 François Laroussinie and Nicolas Markey. Augmenting ATL with strategy contexts. *Information and Computation*, 2015. To appear.

3.19 Computer Poker and Computational Game Theory

Peter Bro Miltersen (*Aarhus University, DK*)

License © Creative Commons BY 3.0 Unported license
© Peter Bro Miltersen

We survey recent work by the computer poker community on computational game theory, focusing (we hope), on work relevant for the formal methods community in general and the non-zero-sum-games-for-controller-synthesis subcommunity in particular.

3.20 Why Negatively-Priced Timed Games Are Hard

Benjamin Monmege (*Free University of Brussels, BE*)

License © Creative Commons BY 3.0 Unported license
© Benjamin Monmege

Joint work of Brihaye, Thomas; Geeraerts, Gilles; Krishna, Shankara Narayanan; Lefauchaux, Engel; Manasa, Lakshmi; Monmege, Benjamin; Trivedi, Ashutosh

Main reference T. Brihaye, G. Geeraerts, S. N. Krishna, L. Manasa, B. Monmege, A. Trivedi, “Adding negative prices to priced timed games,” in Proc. of the 25th Int’l Conf. on Concurrency Theory (CONCUR’14), LNCS, Vol. 8704, pp. 560–575, Springer, 2014.

URL http://dx.doi.org/10.1007/978-3-662-44584-6_38

Priced timed games (PTGs) are two-player zero-sum games played on the infinite graph of configurations of priced timed automata where two players take turns to choose transitions in order to optimize cost to reach target states. Bouyer et al. [2] and Alur, Bernadsky, and Madhusudan [1] independently proposed algorithms to solve PTGs with non-negative prices under certain divergence restriction over prices. Brihaye, Bruyère, and Raskin [4] later provided a justification for such a restriction by showing the undecidability of the optimal strategy synthesis problem in the absence of this divergence restriction. This problem for PTGs with one clock has long been conjectured to be in polynomial time, however the current best known algorithms are exponential, like the one by Rutkowski [6] (adapted from

a previous attempt from by Bouyer, Larsen, Markey, and Rasmussen [3]), or by Hansen, Ibsen- Jensen, and Miltersen [5].

In this talk, we study the extension of PTGs with both negative and positive prices. I will summarize the results we previously obtained: some new undecidability results, and the identification of a subclass (one-clock, bi-valued price-rates) for which we designed a pseudo-polynomial time algorithm (and even polynomial time if non-negative bi-valued price-rates) to partially answer the conjecture on the complexity of one-clock PTGs. The rest of my talk will show some examples of PTGs not in the latter subclass with interesting phenomena, showing some strong features of PTGs, and our hopes to obtain a decidability result for a large class of one-clock PTGs with negative prices.

References

- 1 Rajeev Alur, Mikhail Bernadsky, and P. Madhusudan. Optimal reachability for weighted timed games. In *Proc. of the 31st Int'l Colloquium on Automata, Languages and Programming (ICALP'04)*, vol. 3142 of *LNCS*, pp. 122–133, Springer, 2004. DOI: 10.1007/978-3-540-27836-8_13
- 2 Patricia Bouyer, Franck Cassez, Emmanuel Fleury, and Kim G. Larsen. Optimal strategies in priced timed game automata. In *Proc. of the 24th Conf. on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'04)*, vol. 3328 of *LNCS*, pp. 148–160, Springer, 2005. DOI: 10.1007/978-3-540-30538-5_13
- 3 Patricia Bouyer, Kim G. Larsen, Nicolas Markey, and Jacob Illum Rasmussen. Almost optimal strategies in one-clock priced timed games. In *Proc. of the 26th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'06)*, vol. 4337 of *LNCS*, pp. 345–356, Springer, 2006. DOI: 10.1007/11944836_32
- 4 Thomas Brihaye, Véronique Bruyère, and Jean-François Raskin. On optimal timed strategies. In *Proc. of the 3rd Int'l Conf. on Formal Modeling and Analysis of Timed Systems (FORMATS'05)*, vol. 3829 of *LNCS*, pp. 49–64, Springer, 2005. DOI: 10.1007/11603009_5
- 5 Thomas Dueholm Hansen, Rasmus Ibsen-Jensen, and Peter Bro Miltersen. A faster algorithm for solving one-clock priced timed games. In *Proc. of the 24th Int'l Conf. on Concurrency Theory (CONCUR'13)*, vol. 8052 of *LNCS*, pp. 531–545, Springer, 2013. DOI: 10.1007/978-3-642-40184-8_37
- 6 Michał Rutkowski. Two-player reachability-price games on single-clock timed automata. In *Proc. of the 9th Workshop on Quantitative Aspects of Programming Languages (QAPL'11)*, vol. 57 of *EPTCS*, pp. 31–46, 2011. DOI: 10.4204/EPTCS.57.3

3.21 Correct-by-construction controller synthesis for highly dynamic systems: an application in automotive safety systems

Necmiye Ozay (University of Michigan – Ann Arbor, US)

License  Creative Commons BY 3.0 Unported license
© Necmiye Ozay

Joint work of Ozay, Necmiye; Nilsson, Petter; Liu, Jun; Grizzle, Jessy; Chen, Yuxiao; Peng, Huei

A plethora of driver convenience and safety automation systems are being introduced into production vehicles, such as electronic stability control, adaptive cruise control, lane keeping, and obstacle avoidance. Assuring the seamless and safe integration of each new automation function with existing control functions is a major challenge for vehicle manufacturers. In this talk, I will present some preliminary results to address this problem through the use of

formal methods and correct-by-construction controller synthesis techniques. Mechanisms for handling implementation, perception or model imperfections will be discussed. I will conclude the talk with some open problems and directions for future research.

3.22 Fun with funnels

Nicolas Perrin (UPMC – Paris, FR)

License © Creative Commons BY 3.0 Unported license
© Nicolas Perrin

Related to the notion of Lyapunov stability, funnels are regions of finite time invariance that can help to reason about dynamical systems whose differential equations are too difficult to handle directly. We explain how finite libraries of funnels could be used to construct variants of timed automata with potentially interesting applications to switching controller synthesis with collision avoidance objectives.

3.23 Percentile Queries in Multi-Dimensional Markov Decision Processes

Mickael Randour (ENS – Cachan, FR)

License © Creative Commons BY 3.0 Unported license
© Mickael Randour

Joint work of Randour, Mickael; Raskin, Jean-François; Sankur, Ocan

Main reference M. Randour, J.-F. Raskin, O. Sankur, “Percentile queries in multi-dimensional Markov decision processes,” arXiv:1410.4801v1 [cs.LO], 2014.

URL <http://arxiv.org/abs/1410.4801v1>

Markov decision processes (MDPs) with multi-dimensional weights are useful to analyze systems with multiple objectives that may be conflicting and require the analysis of trade-offs. In this work, we study the complexity of percentile queries in such MDPs and give algorithms to synthesize strategies that enforce such constraints. Given a multi-dimensional weighted MDP and a quantitative payoff function f , thresholds v_i (one per dimension), and probability thresholds α_i , we show how to compute a single strategy to enforce that for all dimensions i , the probability of outcomes ρ satisfying $f_i(\rho) \geq v_i$ is at least α_i . We consider classical quantitative payoffs from the literature (sup, inf, lim sup, lim inf, mean-payoff, truncated sum, discounted sum). Our work extends to the quantitative case the multi-objective model checking problem studied by Etessami et al. in unweighted MDPs.

3.24 Beyond Two-Player Zero-sum Games. Motivations and Highlights of Recent Results

Jean-François Raskin (Free University of Brussels, BE)

License © Creative Commons BY 3.0 Unported license
© Jean-François Raskin

We motivate and review three recent results that we have obtained about non-zero sum games:

1. *Doomsday Equilibria for Omega-Regular Games* (Krishnendu Chatterjee, Laurent Doyen, Emmanuel Filiot, Jean-François Raskin)

Two-player games on graphs provide the theoretical framework for many important problems such as reactive synthesis. While the traditional study of two-player zero-sum games has been extended to multi-player games with several notions of equilibria, they are decidable only for perfect-information games, whereas several applications require imperfect-information games. In this paper we propose a new notion of equilibria, called doomsday equilibria, which is a strategy profile such that all players satisfy their own objective, and if any coalition of players deviates and violates even one of the players objective, then the objective of every player is violated. We present algorithms and complexity results for deciding the existence of doomsday equilibria for various classes of omega-regular objectives, both for imperfect-information games, and for perfect-information games. We provide optimal complexity bounds for imperfect-information games, and in most cases for perfect-information games.

2. *The Complexity of Admissibility in Omega-Regular Games* (Romain Brenguier, Jean-François Raskin, Mathieu Sassolas)

Iterated admissibility is a well-known and important concept in classical game theory, e.g. to determine rational behaviors in multi-player matrix games. As recently shown by Berwanger, this concept can be soundly extended to infinite games played on graphs with omega-regular objectives. In this paper, we study the algorithmic properties of this concept for such games. We settle the exact complexity of natural decision problems on the set of strategies that survive iterated elimination of dominated strategies. As a byproduct of our construction, we obtain automata which recognize all the possible outcomes of such strategies.

3. *Meet Your Expectations With Guarantees: Beyond Worst-Case Synthesis in Quantitative Games* (Véronique Bruyère, Emmanuel Filiot, Mickael Randour, Jean-François Raskin)

We extend the quantitative synthesis framework by going beyond the worst-case. On the one hand, classical analysis of two-player games involves an adversary (modeling the environment of the system) which is purely antagonistic and asks for strict guarantees. On the other hand, stochastic models like Markov decision processes represent situations where the system is faced to a purely randomized environment: the aim is then to optimize the expected payoff, with no guarantee on individual outcomes. We introduce the beyond worst-case synthesis problem, which is to construct strategies that guarantee some quantitative requirement in the worst-case while providing an higher expected value against a particular stochastic model of the environment given as input. This problem is relevant to produce system controllers that provide nice expected performance in the everyday situation while ensuring a strict (but relaxed) performance threshold even in the event of very bad (while unlikely) circumstances. We study the beyond worst-case synthesis problem for two important quantitative settings: the mean-payoff and the shortest path. In both cases, we show how to decide the existence of finite-memory strategies satisfying the problem and how to synthesize one if one exists. We establish algorithms and we study complexity bounds and memory requirements.

3.25 Synthesis for Human-in-the-Loop Control Systems

Dorsa Sadigh (University of California – Berkeley, US)

License © Creative Commons BY 3.0 Unported license
© Dorsa Sadigh

Joint work of Sadigh, Dorsa; Li, Wenchao; Seshia, Sanjit; Sastry, Shankar

Main reference W. Li, D. Sadigh, S. A. Seshia, S. S. Sastry, “Synthesis for Human-in-the-Loop Control Systems,” in Proc. of the 20th Int’l Conf. on Tools and Algorithms for the Construction and Analysis of Systems (TACAS’14), LNCS, Vol. 8413, pp. 470–484, 2014.

URL http://dx.doi.org/10.1007/978-3-642-54862-8_40

Several control systems in safety-critical applications involve the interaction of an autonomous controller with one or more human operators. Examples include pilots interacting with an autopilot system in an aircraft, and a driver interacting with automated driver-assistance features in an automobile. The correctness of such systems depends not only on the autonomous controller, but also on the actions of the human controller. In this paper, we present a formalism for human-in-the-loop (HuLL) control systems. Particularly, we focus on the problem of synthesizing a semi-autonomous controller from high-level temporal specifications that expect occasional human intervention for correct operation. We present an algorithm for this problem, and demonstrate its operation on problems related to driver assistance in automobiles.

3.26 Symbolic Quantitative Robustness Analysis of Timed Automata

Ocan Sankur (Free University of Brussels, BE)

License © Creative Commons BY 3.0 Unported license
© Ocan Sankur

Main reference O. Sankur, “Symbolic Quantitative Robustness Analysis of Timed Automata,” in Proc. of the 21st Int’l Conf. on Tools and Algorithms for the Construction and Analysis of Systems (TACAS’15), LNCS, Vol. 9035, pp. 484–498, Springer, 2015.

URL http://dx.doi.org/10.1007/978-3-662-46681-0_48

We consider the robustness analysis of real-time systems modeled by timed automata, where the goal is to compute a bound on the timing imprecisions so that the model satisfies a given specification. We give a semi-algorithm for infinitesimal analysis, which consists in finding a safe bound on imprecisions (rather than the maximal bound). Our algorithm uses parameterized zones, and exact zone approximations, and performs LTL model checking. The implemented tool is shown to perform well on several standard benchmarks.

3.27 Quantitative Verification in Rational Environments

Sven Schewe (University of Liverpool, GB)

License © Creative Commons BY 3.0 Unported license
© Sven Schewe

Joint work of Gupta, Anshul; Schewe, Sven

Main reference A. Gupta, S. Schewe, “Quantitative Verification in Rational Environments,” in Proc. of the 21st Int’l Symp. on Temporal Representation and Reasoning (TIME’14), pp. 123–131, IEEE Computer Society, 2014.

URL <http://dx.doi.org/10.1109/TIME.2014.9>

We provide a motivation for and discuss the complexity of finding optimal leader / Stackelberg equilibria for non-zero-sum mean payoff games. In this setting, a clever leader trespasses on

the Nash-y rationality of her followers, using their goals to increase her overall return. We show that this quantitative verification problem is NP-complete, and in PTIME with a (two player zero-sum) MPG oracle for a bounded number of players.

3.28 Supervisory Control Synthesis for Deterministic Context Free Specification Languages – Enforcing Controllability Least Restrictively

Anne-Kathrin Schmuck (TU Berlin, DE)

License © Creative Commons BY 3.0 Unported license

© Anne-Kathrin Schmuck

Joint work of Schmuck, Anne-Kathrin; Schneider, Sven; Raisch, Joerg; Nestmann, Uwe

Main reference A. K. Schmuck, S. Schneider, J. Raisch, U. Nestmann, “Extending Supervisory Controller Synthesis to Deterministic Pushdown Automata – Enforcing Controllability Least Restrictively,” in Proc. of the 12th Int’l Workshop on Discrete Event Systems, pp. 286–293, 2014.

URL <http://dx.doi.org/10.3182/20140514-3-FR-4046.00058>

Supervisory Control Theory (SCT) was established by Ramadge and Wonham in the early 80’s for the purpose of controller synthesis on formal languages using their finite automaton realizations. This implies that this synthesis can only be applied to regular plant and specification languages, as only regular languages can be realized by deterministic finite automata (DFA). While the plant can typically be realized by a DFA, requiring that the specification can also be realized by a DFA is rather restrictive.

After introducing the original synthesis for regular languages, we have discussed an extension of SCT to a larger class of specifications, namely specifications that can be written as deterministic context free languages.

3.29 Program Synthesis for Games and Control

Armando Solar-Lezama (MIT - Cambridge, US)

License © Creative Commons BY 3.0 Unported license

© Armando Solar-Lezama

Joint work of Solar-Lezama, Armando; Chaudhuri, Swarat

Main reference A. Solar-Lezama, S. Chaudhuri, “Smooth Interpretation,” in Proc. of the 2010 ACM SIGPLAN Conf. on Programming Language Design and Implementation (PLDI’10), pp. 279–291, ACM, 2010.

URL <http://dx.doi.org/10.1145/1809028.1806629>

This talk described how recent work on constraint based synthesis via sketches can be applied to solve for winning strategies for two player games. The talk used the example of the “Cinderella Game” to illustrate the approach and to show some of its limitations. The talk also described how the ideas of encoding a synthesis problem as a sketch can be leveraged in the context of controller synthesis. Specifically I described some joint work with Swarat Chaudhuri on the use of smooth interpretation together with sketches to facilitate the search of optimal controllers.

3.30 Home Automation Synthesis: From Toy Examples to Realistic Scenarios

Jiří Srba (Aalborg University, DK)

License © Creative Commons BY 3.0 Unported license
© Jiří Srba

Joint work of Jiří Srba; Mathias Grund Sørensen; Kim G. Larsen; David Junker; Lasse E. Nielsen; Mads Mikkelsen; Martin Lykke; Martin Z. Kristensen; Søren B. Andersen

The synthesis of a controller for a home automation systems is a complex task. In this talk we shall present an if-this-then-that rule format for the description of intended behaviour of a smart house and discuss the different approaches for automatic controller synthesis. We discuss their limitations and demonstrate a prototype implementation on a scaled model of a real house.

3.31 Games among arbitrarily many players

John G. Thistle (University of Waterloo, CA)

License © Creative Commons BY 3.0 Unported license
© John G. Thistle

Joint work of M. Hadi Zibaeenejad; Thistle, John G.

Main reference M. H. Zibaeenejad, J. G. Thistle, “Weak invariant simulation and its application to analysis of parameterized networks,” *IEEE Transactions on Automatic Control*, 59(8):2024–2037, 2014.

URL <http://dx.doi.org/10.1109/TAC.2014.2315311>

Distributed control of manufacturing networks, transportation networks, groups of mobile robots and the like, is a form of strategy design for nonzero-sum games. In many of these applications, the number of players may vary with time; it may be large, making explicit modelling cumbersome; or indeed it may be unknown. For such reasons it may be of interest to study games involving arbitrary numbers of players. Control design – or strategy design – can be seen as involving alternating phases of synthesis and verification: for example, disabling of a state transition or a move may give rise to livelocks or deadlocks, requiring further design iterations. This talk will focus on verification of the existence of reachable deadlock states of a game.

The literature – specifically the literature on “parameterized systems” – contains a number of decidability results for verification of relatively simple games among arbitrary numbers of players (where the allowed sequences of moves of each player are defined by an isomorphism to a given template process, and where the players’ strategies are likewise isomorphic). For instance, players may be assumed to form a ring network, in which they interact directly only with their immediate neighbours, and only through the passing of tokens that carry no data. This talk asks whether there exist more complex games that still admit decision procedures for deadlock. It submits as an answer a somewhat tentative “yes”. Our “existence proof” is based on a novel, and unconventional, process-algebraic simulation relation that allows the formulation of less restrictive assumptions about modes of interaction. In the case of ring networks, these assumptions allow the set of reachable deadlocked states to be characterized as those involving circular waits – and such states can be represented as the language accepted by a finite automaton over the alphabet of state symbols of the template process. For a more general class of network topologies featuring branching, we can similarly characterize the set of suitably generalized circular waits as the language accepted by a finite automaton on finite trees. Under some additional assumptions, we can show that the deadlocked network states are exactly those containing generalized circular waits.

3.32 Correct-by-construction control protocol synthesis for autonomous systems

Ufuk Topcu (University of Pennsylvania, US)

License © Creative Commons BY 3.0 Unported license
© Ufuk Topcu

How can we affordably build trustworthy autonomous, networked systems? Partly motivated by this question, I describe a shift from the traditional “design+verify” approach to “specify+synthesize” in model-based development of autonomous systems. I then discuss our recent results on automated synthesis of correct-by-construction, hierarchical control protocols. These results account for hybrid dynamics that are subject to rich temporal logic specifications and heterogeneous uncertainties, and that operate in adversarial environments. They combine ideas from control theory with those from computer science, and exploit underlying system-theoretic interpretations to suppress the inherent computational complexity. The expressivity of the resulting design methodology enables us to formally investigate a number of emerging issues in autonomous, networked systems. I conclude my talk with a brief overview of several such issues from my ongoing projects: (i) compositional synthesis for the so-called fractionated systems; (ii) effects of perception imperfections on protocol synthesis; (iii) interfaces between learning modules and reactive controllers with provable guarantees of correctness; and (iv) human-embedded autonomy.

3.33 Refinement Calculus for Reactive Systems

Stavros Tripakis (University of California – Berkeley, US)

License © Creative Commons BY 3.0 Unported license
© Stavros Tripakis

Joint work of Preoteasa, Viorel; Tripakis, Stavros

Main reference V. Preoteasa, S. Tripakis, “Refinement Calculus of Reactive Systems,” in Proc. of the 14th Int’l Conf. on Embedded Software (EMSOFT’14), pp. 2:1–2:10, ACM, 2014; pre-print available as arXiv:1406.6035v1 [cs.SE].

URL <http://dx.doi.org/10.1145/2656045.2656068>

URL <http://arxiv.org/abs/1406.6035v1>

Refinement calculus is a powerful and expressive tool for reasoning about sequential programs in a compositional manner. In this talk I present an extension of refinement calculus for reactive systems. Refinement calculus is based on monotonic predicate transformers, which transform sets of post-states into sets of pre-states. To model reactive systems, we introduce monotonic property transformers, which transform sets of output traces into sets of input traces. This semantics can model refinement, sequential composition, demonic choice, and other semantic operations on reactive systems. Syntactically, monotonic property transformers can be described in higher order logic, but also using other formalisms more amenable to automation, such as linear temporal logic (suitable for specifications) and symbolic transition systems (suitable for implementations). This framework generalizes previous work on relational interfaces so as to be able to express systems with infinite behaviors and liveness properties.

3.34 Synthesizing Finite-state Protocols from Scenarios and Requirements

Stavros Tripakis (University of California – Berkeley, US)

- License** © Creative Commons BY 3.0 Unported license
© Stavros Tripakis
- Joint work of** Alur, Rajeev; Martin, Milo; Raghothaman, Mukund; Stergiou, Christos; Tripakis, Stavros; Udupa, Abhishek
- Main reference** R. Alur, M. M. K. Martin, M. Raghothaman, C. Stergiou, S. Tripakis, A. Udupa, “Synthesizing Finite-state Protocols from Scenarios and Requirements,” in Proc. of the 10th Int’l Haifa Verification Conf. (HVC’14), LNCS, Vol. 8855, pp. 75–91, Springer, 2014; pre-print available as arXiv:1402.7150v1 [cs.FL].
- URL** http://dx.doi.org/10.1007/978-3-319-13338-6_7
- URL** <http://arxiv.org/abs/1402.7150v1>

Scenarios, or Message Sequence Charts, offer an intuitive way of describing the desired behaviors of a distributed protocol. In this paper we propose a new way of specifying finite-state protocols using scenarios: we show that it is possible to automatically derive a distributed implementation from a set of scenarios augmented with a set of safety and liveness requirements, provided the given scenarios adequately *cover* all the states of the desired implementation. We first derive incomplete state machines from the given scenarios, and then synthesis corresponds to completing the transition relation of individual processes so that the global product meets the specified requirements. This completion problem, in general, has the same complexity, PSPACE, as the verification problem, but unlike the verification problem, is NP-complete for a constant number of processes. We present two algorithms for solving the completion problem, one based on a heuristic search in the space of possible completions and one based on OBDD-based symbolic fixpoint computation. We evaluate the proposed methodology for protocol specification and the effectiveness of the synthesis algorithms using the classical alternating-bit protocol.

3.35 Omega-regular and Max-regular Delay Games

Martin Zimmermann (Universität des Saarlandes, DE)

- License** © Creative Commons BY 3.0 Unported license
© Martin Zimmermann
- Joint work of** Zimmermann, Martin; Klein, Felix
- Main reference** F. Klein, M. Zimmermann, “How Much Lookahead is Needed to Win Infinite Games?” arXiv:1412.3701v1 [cs.GT], 2014.
- URL** <http://arxiv.org/abs/1412.3701v1>

In delay games, one of the players is able to delay her moves to obtain a lookahead on her opponent’s moves. Recently, we showed that exponential lookahead is sufficient for omega-regular games with delay, gave a matching lower bound, and showed solving such games to be EXPTIME-complete.

Similar techniques are also applicable to quantitative extensions of the omega-regular languages, e.g., max-regular languages. These are the languages definable in weak MSO with the unbounding quantifier. We showed that max-regular delay games with respect to bounded lookahead are decidable and gave a doubly-exponential upper bound on the necessary lookahead. On the other hand, we showed that bounded delay is not always sufficient to win such a game.

I will present these results and discuss open problems, mainly on quantitative winning conditions, e.g., there is no matching lower bound in the max-regular case and the exact complexity is open.

This is (partially) joint work with Felix Klein (Saarland University).

4 Working Groups

4.1 Discussion on Supervisory Control and Reactive Synthesis

Stéphane Lafortune (University of Michigan – Ann Arbor, US)

License  Creative Commons BY 3.0 Unported license
© Stéphane Lafortune

We discussed how to approach open problems in supervisory control of discrete event systems using reactive synthesis techniques. We considered in particular the range problem in supervisory control under partial observations, where in addition to the safety and non-blocking specifications, a minimum required behavior is imposed on the controlled system. We also discussed how to establish the decidability, or lack thereof, of special cases of the decentralized supervisory control problem where non-blockingness (for which undecidability is known) is replaced by the weaker condition of deadlock-freeness or by a condition on local maximality of the solution. The participants exchanged several ideas on these problems that led to conjectures that will be pursued in future investigations.

Participants

- Nathalie Bertrand
INRIA Rennes – Bretagne
Atlantique, FR
- Dietmar Berwanger
ENS – Cachan, FR
- Patricia Bouyer-Decitre
CNRS, FR
- Romain Brenguier
Free University of Brussels, BE
- Benedikt Brütch
RWTH Aachen, DE
- Véronique Bruyère
University of Mons, BE
- Krishnendu Chatterjee
IST Austria –
Klosterneuburg, AT
- Laurent Doyen
ENS – Cachan, FR
- Rüdiger Ehlers
Universität Bremen, DE
- John Fearnley
University of Liverpool, GB
- Gilles Geeraerts
Free University of Brussels, BE
- Hugo Gimbert
University of Bordeaux, FR
- Alessandro Giua
University of Aix-Marseille, FR
& University of Cagliari, IT
- Axel Haddad
Free University of Brussels, BE
- Thomas Anton Henzinger
IST Austria –
Klosterneuburg, AT
- Rasmus Ibsen-Jensen
IST Austria –
Klosterneuburg, AT
- Barbara Jobstmann
EPFL Lausanne, CH
- Jan Krčál
Universität des Saarlandes, DE
- Jan Křetínský
IST Austria –
Klosterneuburg, AT
- Stéphane Lafortune
University of Michigan –
Ann Arbor, US
- Kim Guldstrand Larsen
Aalborg University, DK
- Simon B. Laursen
Aalborg University, DK
- Christof Löding
RWTH Aachen, DE
- Nicolas Markey
ENS – Cachan, FR
- Peter Bro Miltersen
Aarhus University, DK
- Benjamin Monmege
Free University of Brussels, BE
- Necmiye Ozay
University of Michigan – Ann
Arbor, US
- Nicolas Perrin
UPMC – Paris, FR
- Sophie Pinchinat
IRISA – Rennes, FR
- Mickael Randour
ENS – Cachan, FR
- Jean-François Raskin
Free University of Brussels, BE
- Dorsa Sadigh
University of California –
Berkeley, US
- Ocan Sankur
Free University of Brussels, BE
- Sven Schewe
University of Liverpool, GB
- Anne-Kathrin Schmuck
TU Berlin, DE
- Armando Solar-Lezama
MIT – Cambridge, US
- Jiří Srba
Aalborg University, DK
- John G. Thistle
University of Waterloo, CA
- Wolfgang Thomas
RWTH Aachen, DE
- Ufuk Topcu
University of Pennsylvania, US
- Stavros Tripakis
University of California –
Berkeley, US
- Martin Zimmermann
Universität des Saarlandes, DE

