Cassting

Deliverable D2.3

Thomas Brihaye (UMONS), Kim G. Larsen (AAU)
and Christof Löding (RWTH),
Nicolas Markey (CNRS), Jiří Srba (AAU)

Project	Cassting — Collective Adaptive Systems SynThesIs with Non-zero-sum Games		
Project id.	FP7-601148		
Workpackage	WP2	Nature	R (report)
Deliverable	D2.3	Dissemination	PU (public)
Date submitted	April 2016	Date due	April 2016
Version	1.0		

;

SEVENTH FRAMEWORK PROGRAMME

Algorithms for games played on networks of systems

Thomas Brihaye Kim G. Larsen Christof Löding
Nicolas Markey Jiří Srba

Abstract

This deliverable reports about our recent advances on algorithms for games played on networks of systems. Collective adaptive systems are often composed of a potentially large number of systems that are identical. This number of participants cannot, in general, be bounded *a priori*, which motivates the need for algorithms that can perform *parametric analysis*, that is, to perform verification and possibly synthesise strategy profiles that are valid for all values of the system parameters (in particular, for any number of participants).

Contents

Introduction

Collective adaptive systems are in essence composed of a large number of systems. Often, those systems are identical (or at least use implementations of the same protocols); this is for instance the case of various protocols used over networks (mobile phones, computers, ...). Several techniques have already been proposed for the verification of networks of systems: e.g. using group theory, VASS, Petri Nets, computing invariants , or via statistical model-checking (for Priced Timed Automata). The problem naturally extends to the synthesis of systems: is it possible to synthesise one single process P such that when composing an arbitrary number of copies of P with a central system S, a given property is fulfilled? To the best of our knowledge, this problem has not been addressed in the literature and is of a particular interest when modelling collective adaptive systems.

Similar questions arise when modelling parametrised systems. At the early stages of design, some parameters of the system might not be fixed. This is usually reflected in the model by introducing *non-determinism*. However, it is sometimes more convenient to model those parameters are quantities over unbounded domains (for instance natural numbers). In this case, two natural questions arise. First, determine for which values of the parameters a strategy profile respecting a given property can be computed. Second, compute a family a strategy profiles, one for each possible valuation of the parameters. When the system has good properties (such as monotonicity w.r.t. to a given ordering on the parameters), the set of values for which a suitable strategy profile exists might have a good structure, and those problems might then be decidable.

The main challenge to address here is that the domain of the parameters is often infinite, as it is the case for the unbounded number of players. In the setting of *verification* several approaches have been considered to obtain algorithms able to analyse infinite state systems. A very successful approach can be found in the theory of *well-structured transition systems* (WSTS) [AČJT96, FS01], a very general class of infinite state systems enjoying decidability for certain kinds of safety properties (namely, coverability properties). Among others, WSTS contain VASS, that have been used to

[AČJT96] Parosh Aziz Abdulla, Kārlis Čerāns, Bengt Jonsson, and Yih-Kuen Tsay. General decidability theorems for infinite-state systems. In *Proceedings of the 11th Annual Symposium on Logic in Computer Science (LICS'96)*, pages 313–321. IEEE Comp. Soc. Press, July 1996.

[FS01] Alain Finkel and Philippe Schnoebelen. Well-structured transition systems everywhere! *Theoretical Computer Science*, 256(1-2):63–92, April 2001.

describe *counting abstractions* of systems made up of an unbounded number of identical components [GS92]. Efficient algorithms and data structures to manipulate and analyse those systems have been defined, notably by members of the consortium [GRV10].

1 Algorithms for Timed-Arc Petri Net Games

Background. It is well-known that one can see the Petri net structure as a system component that allows for sequencing of actions, nondetermistic choice between actions and for creating of new instances of processes as well as synchronisation. Each token in the net can then represent a running instance of the process such that the number of tokens in the net can represent the number of processes that run in parallel as a network. As the number of tokens can dynamically change, we can so create new instances of the processes as well as terminate processes. Of course, all such instances of the processes are identical but in a different executing phase. This can be used for example for modelling identical workflow processes with multiple instances running at the same time.

In the area of model checking, symbolic continuous-time on-the-fly methods were ensuring the success of tools such as Kronos, UPPAAL, Tina and Romeo, utilizing the zone abstraction approach via the data structure DBM. These symbolic techniques were recently employed in on-the-fly algorithms [LS98] for synthesis of controllers for timed games [BCD$^+$07,

[GS92] Steven M. German and A. Prasad Sistla. Reasoning about systems with many processes. *Journal of the ACM*, 39(3):675–735, July 1992.

[GRV10] Gilles Geeraerts, Jean-François Raskin, and Laurent Van Begin. On the efficient computation of the minimal coverability set of Petri nets. *International Journal of Foundations of Computer Science*, 21(2):135–165, April 2010.

[LS98] X. Liu and S. A. Smolka. Simple linear-time algorithms for minimal fixed points (extended abstract). In *Automata, Languages and Programming: 25th International Colloquium*, volume 1443 of *LNCS*, pages 53–66. Springer, 1998.

[BCD$^+$07] G. Behrmann, A. Cougnard, A. David, E. Fleury, K. G. Larsen, and D. Lime. Uppaal-tiga: Time for playing games! In *Computer Aided Verification: 19th International Conference*, volume 4590 of *LNCS*, pages 121–125. Springer, 2007.

CDF$^+$05, PAMS98]. While these methods scale well for classical reachability, the limitation of symbolic techniques is more apparent when used for liveness properties and for solving timed games. We have shown that for reachability and liveness properties, the discrete-time methods performing point-wise exploration of the state-space can prove competitive on a wide range of problems [ALS$^+$13], in particular in combination with additional techniques as time-darts [JLS12], constant-reducing approximation techniques [BJJ$^+$14] and memory-preserving data structures as PTrie [JLS$^+$14].

Our contribution. For this contribution, we benefit from the recent advances in the discrete-time verification of timed systems and suggest an on-the-fly point-wise algorithm for the synthesis of timed controllers relative to safety objectives (avoiding undesirable behaviour). The algorithm is described for a novel game extension of the well-studied timed-arc Petri net formalism [BLT90, Han93] and we show that in the general setting the ex-

---

[CDF$^+$05] F. Cassez, A. David, E. Fleury, K. G. Larsen, and D. Lime. Efficient on-the-fly algorithms for the analysis of timed games. In *Concurrency Theory: 16th International Conference*, volume 3653 of *LNCS*, pages 66–80. Springer, 2005.

[PAMS98] A. Pnueli, E. Asarin, O. Maler, and J. Sifakis. Controller synthesis for timed automata. In *System Structure and Control*. Elsevier, 1998.

[ALS$^+$13] M. Andersen, H.G. Larsen, J. Srba, M.G. Sørensen, and J.H. Taankvist. Verification of liveness properties on closed timed-arc Petri nets. In *Mathematical and Engineering Methods in Computer Science: 8th International Doctoral Workshop*, volume 7721 of *LNCS*, pages 69–81. Springer, 2013.

[JLS12] K.Y. Jørgensen, K. G. Larsen, and J. Srba. Time-darts: A data structure for verification of closed timed automata. In *Proceedings Seventh Conference on Systems Software Verification*, volume 102 of *EPTCS*, pages 141–155. Open Publishing Association, 2012.

[BJJ$^+$14] S.V. Birch, T.S. Jacobsen, J.J. Jensen, Ch. Moesgaard, N.N. Samuelsen, and J. Srba. Interval abstraction refinement for model checking of timed-arc Petri nets. In *Formal Modeling and Analysis of Timed Systems: 12th International Conference*, volume 8711 of *LNCS*, pages 237–251. Springer, 2014.

[JLS$^+$14] P. G. Jensen, K. G. Larsen, J. Srba, M. G. Sørensen, and J. H. Taankvist. Memory efficient data structures for explicit verification of timed systems. In *NASA Formal Methods: 6th International Symposium*, volume 8430 of *LNCS*, pages 307–312. Springer, 2014.

[BLT90] T. Bolognesi, F. Lucidi, and S. Trigila. From Timed Petri Nets to Timed LOTOS. In *Protocol Specification, Testing and Verification X, Proceedings of the IFIP WG6.1 Tenth International Symposium on Protocol Specification*, pages 395–408. North-Holland, 1990.

[Han93] H. Hanisch. Analysis of Place/Transition Nets with Timed Arcs and its Application to Batch Process Control. In *Application and Theory of Petri* istence of a controller for a safety objective in the discrete-time setting does not imply the existence of such a controller in the continuous-time setting and vice versa, not even for systems with closed guards—contrary to the fact that continuous-time and discrete-time reachability problems coincide for timed models [BMT99], in particular also for timed-arc Petri nets [MSS15]. However, if we restrict ourselves to the practically relevant subclass of urgent controllers that either react immediately to the environmental events or simply wait for another occurrence of such an event, then we can use the discrete-time methods for checking the existence of a continuous-time safety controller on closed timed-arc Petri nets. The algorithm for controller synthesis is implemented in the tool TAPAAL [DJJ+12], including the memory optimization technique via PTrie [JLS+14], and the experimental data show a promising performance on a large data-set of infinite job scheduling problems as well as on other examples.

Participants: Jonas F. Jensen (AAU)
Kim G. Larsen (AAU)
Jiri Srba (AAU)
References: [JLS16]

Nets 1993: 14th International Conference, volume 691 of *LNCS*, pages 282–299. Springer, 1993.

[BMT99] M. Bozga, O. Maler, and S. Tripakis. Efficient verification of timed automata using dense and discrete time semantics. In *Correct Hardware Design and Verification Methods: 10th IFIP WG10.5 Advanced Research Working Conference*, volume 1703 of *LNCS*, pages 125–141. Springer, 1999.

[MSS15] J.A. Mateo, J. Srba, and M.G. Sørensen. Soundness of timed-arc workflow nets in discrete and continuous-time semantics. *Fundamenta Informaticae*, 140(1):89–121, 2015.

[DJJ+12] A. David, L. Jacobsen, M. Jacobsen, K.Y. Jørgensen, M.H. Møller, and J. Srba. TAPAAL 2.0: Integrated development environment for timed-arc Petri nets. In *Tools and Algorithms for the Construction and Analysis of Systems: 18th International Conference*, volume 7214 of *LNCS*, pages 492–497. Springer, 2012.

[JLS+14] P. G. Jensen, K. G. Larsen, J. Srba, M. G. Sørensen, and J. H. Taankvist. Memory efficient data structures for explicit verification of timed systems. In *NASA Formal Methods: 6th International Symposium*, volume 8430 of *LNCS*, pages 307–312. Springer, 2014.

2 Stable Routing in Dynamic Networks

In this joint work of the RWTH Aachen team with J. Gross (KTH, Sweden), we study stability and delay in dynamic networks under adversarial conditions. The network is modeled as an undirected graph in which the nodes are connected by communication links. A list of source and destination pairs determines the desired traffic that has to be routed through the network. We assume that there is a primary user that can block parts of the communication links (subject to some constraints). Such a network is called stable if there is a strategy for routing the traffic from the sources to the destinations such that the number of packets in the network remains bounded, no matter how the primary user blocks the communication links.

As already reported in the deliverable D2.2 "Algorithms for games on evolving structures", we have given a characterization of the stability region of such a network in terms of multi-commodity flows (MCF) published in [TLRG14]. This characterization states that the network is stable if there is an MCF with throughput 1 (the commodities corresponding the the individual source and destination pairs for the traffic). The routing strategy that we construct in [TLRG14] guarantees to keep the network stable whenever such an MCF exists, and if there is no such MCF, then the primary user has a way to block the network such that over time the number of packets grows unboundedly. This analysis has been carried out under the view of a two player game, in which one player modifies the structure (the primary user who is blocking connections), and the other player is in charge of routing the packets. However, this means that the routing player controls all the nodes of the network and has global knowledge on the current network structure for making the routing decisions.

A more realistic view is to see each node of the network as an individual player who can only act based on some local knowledge. In this setting, we have a network of players, all with the same objective. The task is now to identify or synthesize local strategies for the individual players such that the combined behavior ensures stability of the network. For this purpose,

[TLRG14] Simon Tenbusch, Christof Löding, Frank G. Radmacher, and James Gross. Guaranteeing stability and delay in dynamic networks based on infinite games. In *11th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2014, Philadelphia, PA, USA, October 28-30, 2014*, pages 461–469. IEEE, 2014.

we have studied the behavior of the backpressure routing scheme [TE92] in our setting. Backpressure routing is a routing scheme that only requires local information for the forwarding decisions in each node of the network. Roughly, the packets are forwarded to the neighbors which currently have the smallest queue sizes (the queues are storing the packets that have to be forwarded at a node). Based on the results published in [TLRG14], we can show that backpressure routing is stable under almost the same conditions as the general stability criterion. The existence of an MCF with throughput 1 has to be strengthened to the existence of an MCF with throughput strictly greater than 1. The algorithm from [TLRG14] that checks for a given network whether there exists an MCF with throughput one computes an MCF with maximal throughput, and thus can also be used to check for this new criterion. These results provide interesting insights on how the existence of a global strategy can be used to reason about combinations of local strategies.

Participants: Simon Tenbusch (RWTH)
Christof Löding (RWTH)
Frank Radmacher (RWTH)
James Gross (KTH, Sweden)

3 Reachability in Networks of Register Protocols under Stochastic Schedulers

Background. Networks of processes may use various kinds of communications. In a recent work involving CNRS and ULB, we considered a communication model where the processes asynchronously access a shared register, and where read and write operations on this register are performed

[TE92] L. Tassiulas and A. Ephremides. Stability Properties of Constrained Queueing Systems and Scheduling Policies for Maximum Throughput in Multihop Radio Networks. *IEEE Transactions on Automatic Control*, 37(12):1936–1948, dec 1992.

[TLRG14] Simon Tenbusch, Christof Löding, Frank G. Radmacher, and James Gross. Guaranteeing stability and delay in dynamic networks based on infinite games. In *11th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2014, Philadelphia, PA, USA, October 28-30, 2014*, pages 461–469. IEEE, 2014.

non-atomically. A similar model has been proposed by Hague in [Hag11], where the behavior of processes is defined by a pushdown automaton. The complexity of some reachability and liveness problems for shared-memory models have then been established in [EGM13] and [DEGM15], respectively. These works consider networks in which a specific process, called the leader, runs a different program, and address the problem whether, for some number of processes, the leader can satisfy a given reachability or liveness property. In the case where there is no leader, and where processes are finite-state, the parameterized control-state reachability problem (asking whether one of the processes can reach a given control state) can be solved in polynomial time, by adapting the approach of [DSTZ12] for lossy broadcast protocols.

In our work, we further insert fairness assumptions in the model of parameterized networks with asynchronous shared memory, and consider reachability problems in this setting. There are different ways to include fairness in parameterized models. One approach is to enforce fairness expressed as a temporal-logic property on the executions (e.g., any action that is available infinitely often must be performed infinitely often); this is the option chosen for parameterized networks with rendez-vous [GS92] and for

---

[Hag11] Matthew Hague. Parameterised pushdown systems with non-atomic writes. In Supratik Chakraborty and Amit Kumar, editors, *Proceedings of the 31st Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'11)*, volume 13 of *Leibniz International Proceedings in Informatics*, pages 457–468. Leibniz-Zentrum für Informatik, December 2011.

[EGM13] Javier Esparza, Pierre Ganty, and Rupak Majumdar. Parameterized verification of asynchronous shared-memory systems. In Natasha Sharygina and Helmut Veith, editors, *Proceedings of the 25th International Conference on Computer Aided Verification (CAV'13)*, volume 8044 of *Lecture Notes in Computer Science*, pages 124–140. Springer-Verlag, July 2013.

[DEGM15] Antoine Durand-Gasselin, Javier Esparza, Pierre Ganty, and Rupak Majumdar. Model checking parameterized asynchronous shared-memory systems. In Daniel Kroening and Corina S. Pasareanu, editors, *Proceedings of the 27th International Conference on Computer Aided Verification (CAV'15)*, volume 9206 of *Lecture Notes in Computer Science*, pages 67–84. Springer-Verlag, July 2015.

[DSTZ12] Giorgio Delzanno, Arnaud Sangnier, Riccardo Traverso, and Gianluigi Zavattaro. On the complexity of parameterized reachability in reconfigurable broadcast networks. In Deepak D'Souza, Telikepalli Kavitha, and Jaikumar Radhakrishnan, editors, *Proceedings of the 32nd Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'12)*, volume 18 of *Leibniz International Proceedings in Informatics*, pages 289–300. Leibniz-Zentrum für Informatik, December 2012.

[GS92] Steven M. German and A. Prasad Sistla. Reasoning about systems with many

systems with disjunctive guards (where processes can query the states of other processes) in [AJK16]. We follow another choice, by equipping our networks with a stochastic scheduler that, at each step of the execution, assigns the same probability to the available actions of all the processes. From a high-level perspective, both forms of fairness are similar. However, expressing fairness via temporal logic allows for very regular patterns (e.g., round-robin execution of the processes), whereas the stochastic approach leads to consider all possible interleavings with probability 1. Under this stochastic scheduler assumption, we focus on almost-sure reachability of a given control state by one of the processes of the system. More specifically, as in [AJK16], we are interested in determining the existence of a cut-off, i.e., an integer k such that networks with more than k processes almost-surely reach the target state. Deciding the existence and computing such cut-offs is important for at least two aspects: first, it ensures that the system is correct for arbitrarily large networks; second, if we are able to derive a bound on the cut-off, then using classical verification techniques we can find the exact value of the cut-off and exactly characterize the sizes of the networks for which the behavior is correct.

Our contributions. We prove that for finite-state asynchronous shared-memory protocols with a stochastic scheduler, and for almost-sure reachability of some control state by some process of the network, there always exists a positive or negative cut-off; positive cut-offs are those above which the target state is reached with probability 1, while negative cut-offs are those above which the target state is reached with probability strictly less than 1. Notice that both cut-offs are not complement of one another, so that our result is not trivial. We then prove that the "sign" (positive or

processes. *Journal of the ACM*, 39(3):675–735, July 1992.

[AJK16] Simon Außerlechner, Swen Jacobs, and Ayrat Khalimov. Tight cutoffs for guarded protocols with fairness. In Barbara Jobstmann and K. Rustan M. Leino, editors, *Proceedings of the 17th International Workshop on Verification, Model Checking, and Abstract Interpretation (VMCAI'16)*, volume 9583 of *Lecture Notes in Computer Science*, pages 476–494. Springer-Verlag, January 2016.

[AJK16] Simon Außerlechner, Swen Jacobs, and Ayrat Khalimov. Tight cutoffs for guarded protocols with fairness. In Barbara Jobstmann and K. Rustan M. Leino, editors, *Proceedings of the 17th International Workshop on Verification, Model Checking, and Abstract Interpretation (VMCAI'16)*, volume 9583 of *Lecture Notes in Computer Science*, pages 476–494. Springer-Verlag, January 2016.

negative) of a cut-off can be decided in EXPSPACE, and that this problem is PSPACE-hard. Finally, we provide lower and upper bounds on the values of the cut-offs, exhibiting in particular protocols with exponential (negative) cut-off. Notice how these results contrast with classical results in related areas: in the absence of fairness, reachability can be decided in polynomial time, and in most settings, when cut-offs exist, they generally have polynomial size [AJK16, EN03, EK00].

These results will appear as [BMR+16]. A direct corollary of this work is that we can perform bounded-memory strategy synthesis for reachability objectives in this context. The directions for extending this work are numerous: in particular, we will extend our study to other winning conditions, and will focus more closely on strategy synthesis in order to obtain better algorithms.

Participants: Patricia Bouyer (CNRS)
Nicolas Markey (CNRS)
Mickael Randour (CNRS/ULB)
Arnaud Sangnier (U. Paris Diderot)
Daniel Stan (CNRS)
References: [BMR+16]

[AJK16] Simon Außerlechner, Swen Jacobs, and Ayrat Khalimov. Tight cutoffs for guarded protocols with fairness. In Barbara Jobstmann and K. Rustan M. Leino, editors, *Proceedings of the 17th International Workshop on Verification, Model Checking, and Abstract Interpretation (VMCAI'16)*, volume 9583 of *Lecture Notes in Computer Science*, pages 476–494. Springer-Verlag, January 2016.

[EN03] E. Allen Emerson and Kedar Namjoshi. On reasoning about rings. *International Journal of Foundations of Computer Science*, 14(4):527–550, August 2003.

[EK00] E. Allen Emerson and Vineet Kahlon. Reducing model checking of the many to the few. In David McAllester, editor, *Proceedings of the 17th International Conference on Automated Deduction (CADE'00)*, volume 1831 of *Lecture Notes in Artificial Intelligence*, pages 236–254. Springer-Verlag, June 2000.

4 Nash Equilibria in Symmetric Graph Games with Partial Observation

Background. In this work, we propose a model for representing large interacting systems, which we call a *game network*. A game network is made of multiple copies of a single arena; each player plays on his own copy of the arena. Here, the players have (imperfect) information about the global state of the game. For instance, they may have a perfect view on some of their "neighbours", but may be blind to some other players. In *symmetric* game networks, we additionally require that any two players are in similar situations: for every pair of players (A, B), we are able to map each player C to a corresponding player D with the informal meaning that 'player D is to B what player C is to A'. Of course, winning conditions and imperfect information should respect that symmetry. In these systems, we are interested in so-called symmetric pure Nash equilibria, which are special Nash equilibria where all players follow the same deterministic strategy.

Our contributions. In [BMV14], we showed several undecidability results, in particular that the parameterized synthesis problem (aiming to obtain one policy that forms a Nash equilibrium when applied to any number of participants) is undecidable. We then characterize the complexity of computing constrained pure symmetric Nash equilibria in symmetric game networks, when objectives are given as LTL formulas, and when restricting to memoryless and bounded-memory strategies. This problem with no memory bound is then proven undecidable.

In a recent extension of this work, which will appear as [BMV16], we studied *succinct game networks*, which are parametrized models similar to the ones in the previous section. Communication between components are by direct observation of some of the neighbours, and partial information about the whole network (e.g. for modelling a situation where each component can measure the *global noise* of the whole system).

The synthesis of symmetric Nash equilibria for an arbitrary number of players was one of our target applications in this work: we study the problem whether a succinct symmetric game network admits a symmetric Nash equilibrium when the number of players is large enough. More precisely, we aim at deciding the existence of a one-player strategy σ_0, and of an integer n_0, such that the strategy profile obtained by making all n_0 players follow strategy σ_0 (each player having its own observation) is a Nash equilibrium. We show that deciding the existence of such an equilibrium is undecidable, even when considering only memoryless strategies.

For the case where the number of players is fixed, bounded-memory symmetric Nash equilibria can be computed in EXPSPACE (and that the problem is actually EXPSPACE-complete). Notice that the naive approach of enumerating memoryless strategies would require doubly-exponential space.

5 List of publications

[BMR+16] Patricia Bouyer, Nicolas Markey, Mickael Randour, Arnaud Sangnier, and Daniel Stan. Reachability in networks of register protocols under stochastic schedulers. In *Proceedings of the 43rd International Colloquium on Automata, Languages and Programming (ICALP'16)*, Leibniz International Proceedings in Informatics, Rome, Italy, July 2016. Leibniz-Zentrum für Informatik. To appear.

[BMV14] Patricia Bouyer, Nicolas Markey, and Steen Vester. Nash equilibria in symmetric games with partial observation. In Fabio Mogavero and Aniello Murano, editors, *Proceedings of the 2nd International Workshop on Strategic Reasoning (SR'14)*, volume 146 of *Electronic Proceedings in Theoretical Computer Science*, pages 49–55, Grenoble, France, April 2014.

[BMV16] Patricia Bouyer, Nicolas Markey, and Steen Vester. Nash equilibria in symmetric graph games with partial observation. *Information & Computation*, 2016. To appear.

[JLS16] Jonas F. Jensen, Kim G. Larsen, and Jiří Srba. Real-time strategy synthesis for timed-arc Petri net games via discretization. In Dragan Bosnacki and Anton Wijs, editors, *Proceedings of the 23rd International Symposium on Model-Cherking Software (SPIN'16)*, volume 9641 of *Lecture Notes in Computer Science*, pages 129–146, Eindhoven, The Netherlands, April 2016. Springer.