Project no.:	**ICT-FP7-STREP-214755**
Project full title:	**Quantitative System Properties in Model-Driven Design**
Project Acronym:	**QUASIMODO**

Deliverable no.: D3.3

Title of Deliverable: Model-checking of controllability properties

Contractual Date of Delivery to the CEC:	**Month 12**
Actual Date of Delivery to the CEC:	**Month 12 (february 1, 2009)**
Organisation name of lead contractor for this deliverable:	**Université Libre de Bruxelles (CFV)**
Author(s):	**Jean-François Raskin**
Participants(s):	**P04 RWTH, CNRS, CFV, SU, AAU**
Work package contributing to the deliverable:	**WP 3**
Nature:	**R**
Version:	**1.0**
Total number of pages:	**6**
Start date of project:	1 Jan. 2008 **Duration:** 36 month

Project co-funded by the European Commission within the Seventh Framework Programme (2007-2013)

Dissemination Level

PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Abstract:

Model-checking of controllability properties is a central problem when considering realistic models for reactive systems. Reactive systems are open systems where we must distinguish events (or actions) that are controlled by the system to develop (usually called a controller), and events (or actions) that are not controlled by the system to develop and are controlled by the environment. Those events of the environment are usually called *uncontrollable events* (or uncontrollable actions). With this view, games are natural models for reactive systems. To reason about those games, we have to develop adequate logics and algorithms able to formalize and answer questions about *strategies*. Indeed, *Winning strategies* in those games are action plans (sequence of events) that the system to develop has to produce in order to control the environment, i.e. to meet its specification.

Keyword list: Alternating time temporal logic, multi-agent games structures, winning strategies, imperfect information, timed games, stochastic games.

Contents

Abbreviations

AAU: Aalborg University, DK

CFV: Centre Fèdèrè en Vèrification, B

CNRS: National Center for Scientific Research, FR

ESI: Embedded Systems Institute, NL

ESI/RU: Radboud University Nijmegen, NL

RWTH: RWTH Aachen University, D

SU: Saarland University, D

1 Introduction

In this deliverable, we report on the progresses that we have made in the domain of model-checking controllability properties of reactive systems. The specifications that must meet a reactive system must distinguish between events that are *controllable*, i.e. under the control of the system to build, and events that are *uncontrollable*, i.e. under the control of the environment into which the reactive system is embedded. When this distinction between controllable and uncontrollable events is done, it is natural to see a model for a reactive system as a game between the system to build and the environment to control. Models and logics for those games have to be defined and algorithms have to be developed.

During 2008, the teams of our consortium have worked on three different topics in this area. The topics are:

1. foundations of the Alternating-time Temporal Logic (ATL for short);
2. game of imperfect information;
3. Markov decision processes.

2 ATL

2.1 Participants

2.2 Participants

- Thomas Brihaye (CNRS et CFV)
- Nicolas Markey, Patricia Bouyer, François Laroussinie, Arnaud Da Costa, and Ghassan Oreiby (CNRS).

2.3 Contribution

The logic ATL has been proposed ten years ago as a temporal logic in which controllability properties can be directly formulated. Formulas of that logic are evaluated in state of concurrent game structures that are models that allow to distinguish between actions that are controllable and actions that are uncontrollable. In those game structures, actions are controlled by players and the logic allow us to express properties like "Players A and B (the system) can collaborate against C (the environment) so that on all resulting behaviors, the property p is eventually satisfied". While there is a growing literature about concurrent games and the logic ATL, there is still a large number of fundamental research questions to be settled before being able to offer industrial strength model-checking tools for concurrent game structure and ATL. In line with this research goals, we have revisited the complexity and expressiveness questions for the logic ATL, and we have established that

- the original definition of ATL is not as expressive as expected. Contrary to other classical temporal logics, some classical equivalences do not hold in the case of ATL.
- while the logic was defined in the setting of multi-player games, the P-completeness of the model-checking problem only holds for the case of games with a fixed number of players. We precisely studied the complexity of this problem in the general setting, proving that it was much more difficult than expected (harder than NP) when the games is described symbolically.

We also defined a new seantics for ATL where strategy quantification keeps the earlier strategies in a context. This provides us with a much more expressive logic, containing the classical logics ATL and ATL*. Unfortunately, our algorithm for model checking this logic is non-elementary. Still, we defined and studied the case of bounded-memory strategies, and proved that the complexity then lowered to EXPSPACE.

Details about those progresses can be found in [5, 4].

3 Games of imperfect information

3.1 Participants

- Jean-François Raskin and Pierre-Alain Reynier (CFV)
- Franck Cassez (CNRS)
- Laurent Doyen (CFV and EPFL) and Tom Henzinger (EPFL)
- Krishnendu Chatterjee (UC Berkeley)
- Kim Larsen, Alexandre David, and Jesper Jensens (AAU),

3.2 Contributions

Classical models for reactive systems make the hypothesis that the controller has a perfect knowledge of the state of the environment that it is controlling. In practice, this assumption is usually not realistic. In fact, most often a controller will acquire information about the state of the environment using sensors of finite precision. For example, if a controller has to control the temperature into a tank, it will sense this temperature with a thermometer of finite precision. To reflect this important aspect of control, we must develop models and algorithms that handle this *imperfect information*.

In collaboration with EPFL and Berkeley, CFV has recently studied new algorithms for the synthesis of controller with imperfect information. The algorithms are in the form fixed points. The fixed point theory is defined on the lattice of antichains of sets of states. Contrary to the classical solution proposed by Reif in the early 80's, the new solution does not involve determinization. As a consequence, it is readily applicable to classes of systems that do not admit

determinization. Notable examples of such systems are timed and hybrid automata. As an application, we have shown that the discrete control problem for games of imperfect information defined by rectangular automata is decidable. This result extends former results by Henzinger and Kopke on discrete time control. Those results are summarized in [2].

Those theoretical results have been extended to stuttering invariant and observation based strategies for the control of timed automata. This work has been done in collaboration with U Aalborg and EC Nantes and have been published in [1]. Those results should soon be integrated into the tool UppAal-Tiga. In this line of research, during 2008, we have also:

- started to study algorithms that are able to synthesize automatically a set of observations that is sufficient to control a system. This collaboration is ongoing and we hope to submit first results on those algorithms at the beginning of 2009.
- applied the current techniques that we have implemented in UppAal-Tiga to a case study proposed by Hydac that we manage to solve with a methodology that make intensive use of our new synthesis algorithms. This work has been reported in a paper to appear next spring in HSCC'09, see [3] for the details.

4 Markov decision processes

4.1 Participants

- Christel Baier (TU Dresden),
- Boudewijn R. Haverkort (ESI/RU),
- Holger Hermanns (SU),
- Joost-Pieter Katoen (RWTH).

4.2 Contribution

Having their roots in economics, Markov decision processes (MDPs, for short) in computer science are used in application areas such as randomised distributed algorithms and security protocols. The discrete probabilities are used to model random phenomena in such algorithms, like flipping a coin or choosing an identity from a fixed range according to a uniform distribution, whereas the nondeterminism in MDPs is used to specify unknown or underspecified behaviour, e.g., concurrency (interleaving) or the unknown malicious behavior of an attacker.

MDPs – also considered as turn-based $1\frac{1}{2}$-player stochastic games – consist of decision epochs, states, actions, and transition probabilities. On entering a state, an action, α, say, is nondeterministically selected and the next state is determined randomly by a probability distribution that depends on α. Actions may incur a reward, interpreted as gain, or dually, as cost. Schedulers or strategies prescribe which actions to choose in a state. One of the simplest schedulers, the so-called memoryless (or positional) ones, base their decision solely on the current

state and not on the further history. A plethora of results for MDPs are known that mainly focus on finding an optimal scheduler for a certain objective. For, e.g., reachability objectives – find a scheduler, possibly the simplest one, maximises the probability to reach a set of states – memoryless schedulers suffice and can be determined in polynomial time. For step-bounded reachability, finite memory schedulers are sufficient. These schedulers perform the selection process on the basis of a finite piece of information, typically encoded as a finite-state automaton that runs in parallel to the MDP at hand.

We consider turn-based $1\frac{1}{2}$-player stochastically timed games, also known as *continuous-time* Markov decision processes (CTMDPs). They behave as MDPs but in addition their timing behaviour is random. The probability to stay at most t time units in a state is determined by a negative exponential distribution of which the rate depends on α. A reward is obtained which is linearly dependent on the time t spent in state s, as well as on a factor $rew(s, \alpha)$, the state- and action-dependent reward rate.

In contrast to MDPs, CTMDPs have received far less attention; a reason for this might be the increased complexity when moving to continuous time. We study reachability objectives for CTMDPs, in particular time-bounded reachability – what is the optimal policy to reach a set of states within a certain deadline – reward-bounded reachability, and their combination. We survey the results in this field, and show that reward-bounded and time-bounded reachability are interchangeable. As a result, counting schedulers are shown to be optimal for reward-bounded reachability in CTMDPs, and can be computed in polynomial time using a greedy backward algorithm.

The presented reachability objectives are for instance relevant for job-shop scheduling problems where individual jobs have a random exponential duration. The problem of finding a schedule for a fixed number of such (preemptable) jobs on a given set of identical machines such that the probability to meet a given deadline is maximised, is, in fact, an instance of timed reachability on CTMDPs. Optimal memoryless strategies exists for minimising the sum of the job completion times, but, as is shown, this is not the case for maximising the probability to reach the deadline. The same applies for maximising the probability to complete all jobs within a fixed cost.

Details about this work can be found in [6].

Bibliography

[1] Franck Cassez, Alexandre David, Kim Guldstrand Larsen, Didier Lime, and Jean-François Raskin, **Timed Control with Observation Based and Stuttering Invariant Strategies**, *ATVA*, LNCS **4762**, 192-206, Springer, 2007

[2] Krishnendu Chatterjee, Laurent Doyen, Thomas A. Henzinger, and Jean-François Raskin, **Algorithms for Omega-Regular Games with Imperfect Information**, *Logical Methods in Computer Science*(3):3, 1-25, 2007.

[3] F. Cassez, J. J. Jessen, K. G. Larsen, J.-F. Raskin and P.-A. Reynier Automatic Synthesis of **Robust and Optimal Controllers – An Industrial Case Study**. To appear in *HSCC'09*, 2009.

[4] Laroussinie, François, Markey, Nicolas and Oreiby, Ghassan **On the Expressiveness and Complexity of ATL** *Logical Methods in Computer Science*(7):2, 2008.

[5] Brihaye, Thomas, Da Costa, Arnaud, Laroussinie, François and Markey, Nicolas, **ATL with Strategy Contexts and Bounded Memory**, *Proceedings of the Symposium on Logical Foundations of Computer Science (LFCS'09)*, LNCS **5407**, pp. 92-106, Springer, 2009.

[6] Christel Baier, Boudewijn R. Haverkort, Holger Hermanns, and Joost-Pieter Katoen. **Reachability in continuous-time Markov reward decision processes**. In Erich Graedel, Joerg Flum, and Thomas Wilke, editors, Logic and Automata: History and Perspectives. pages 53-72. Volume 2 of Texts in Logics and Games. Amsterdam University Press, 2008.