Model-Checking Timed ATL for Durational Concurrent Game Structures*

François Laroussinie, Nicolas Markey, and Ghassan Oreiby**

Lab. Spécification & Vérification
ENS de Cachan & CNRS UMR 8643
61, av. Pdt. Wilson, 94235 Cachan Cedex, France
{fl, markey, oreiby}@lsv.ens-cachan.fr

Abstract. We extend the framework of ATL model-checking to "simply timed" concurrent game structures, *i.e.*, multi-agent structures where each transition carry an integral duration (or interval thereof). While the case of single durations is easily handled from the semantics point of view, intervals of durations raise several interesting questions. Moreover subtle algorithmic problems have to be handled when dealing with model checking. We propose a semantics for which we develop efficient (PTIME) algorithms for timed ATL without equality constraints, while the general case is shown to be EXPTIME-complete.

1 Introduction

Verification and model-checking. The development of embedded reactive systems is impressive (both in terms of their number and of their complexity), and their formal verification can't be ignored. Model-checking [12,7] is a well-established technique for verifying that (an automaton representing) such a system satisfies a given property. Following [21,11,22], temporal logics have been used for specifying those properties: *Linear time* temporal logics (*e.g.* LTL) expresses properties on each single execution of the model, while *branching time* temporal logics (*e.g.* CTL) deal with the computation tree of the model.

The model-checking technique has been extended to also handle quantitative measurement of time. In that framework, automata are equipped with real-valued clocks [2], and temporal logics are extended to also express quantitative constraints on the flow of time [1]. Again, this framework is now well understood, but the algorithms are noticeably more complex.

In order to lower the complexity of those algorithms, less expressive models and logics have been developed [14,9,17]. Those models are less expressive, but can be handled very efficiently, especially through symbolic model-checking algorithms using BDD techniques [8,20,9,19].

* This work is partly supported by ACI Sécurité & Informatique CORTOS, a program of the French ministry of research.

** This author is supported by a PhD grant from Région Ile-de-France.

E. Asarin and P. Bouyer (Eds.): FORMATS 2006, LNCS 4202, pp. 245–259, 2006.

Verification and control. In the late 80's, a new framework has been developed in the field of verification: control (and controller synthesis) [23]. The goal is now to build a controller that should prevent the (model of the) system from having unwanted behaviors.

This problem is closely related to (multi-player) games: solving such a game amounts to compute a strategy (if it exists) for a player so that he surely reaches a state where he is declared the winner. In that case, the underlying model is not a simple automaton, but rather a "concurrent game structure" (CGSs) [5], in which several agents concurrently decide on the behavior of the system. In order to reason with strategies, a new flavor of temporal logics has been defined: *alternating time* temporal logics (ATL) [4,5]. This logic allows to express, for instance, that a coalition of agents has a strategy in order to always reach a winning location, or to always avoid reaching a bad locations. When the concurrent game structure is defined explicitly, ATL enjoys polynomial-time model-checking algorithms.

Our contribution. The goal of this paper is to extend the framework of ATL to (simply) timed systems. To that aim, we introduce *durational* CGSs (DCGSs), in which each transition is labeled with an interval of possible (integer) durations. Those durations are assumed to be atomic, *i.e.*, there are no intermediate state, and the complete duration elapses in one step.

We propose a semantics for DCGSs where we assume that each transition is associated with an extra agent, who is in charge of selecting the duration of that transition within the interval it is labeled with. We believe that this semantics is really interesting, as it allows to finely select which durations can be controlled by a coalition. Moreover, we show that it still enjoys polynomial-time quantitative model-checking algorithms in the case when no equality constraint is involved.

Related work. Our discrete-time extension of CGSs to DCGSs is inspired by that of [17], where efficient quantitative model-checking algorithms are proposed. Several other extensions of games with time have been proposed in the recent literature, *e.g.* [18,3,6,10]. The semantics assumed there uses dense-time where players choose either to wait for a delay or to fire an action-transition. In [13], another dense-time semantics is proposed, working (roughly) as follows: each player chooses a (strictly positive) delay and a transition, and the game follows the player with the shortest delay. With this semantics, each player can take the others by surprise.

Those papers only deal with qualitative control objectives. In [24], Schobbens proposes a quantitative extension of ATL over timed CGSs (with a semantics of time similar to that of [13]). The resulting logic, ARTL*, a mixture of ATL and MITL, is shown decidable.

2 Definitions

2.1 Tight Durational CGS (TDCGS)

We extend the model of CGSs, see [5,16].