Bounded Model Checking Real-Time Multi-agent Systems with Clock Differences: Theory and Implementation

Alessio Lomuscio\textsuperscript{1,*}, Bożena Woźna\textsuperscript{2,**}, and Andrzej Zbrzezny\textsuperscript{2,**}\textsuperscript{***}

\textsuperscript{1} Department of Computing, Imperial College London, London SW72BZ, UK
\texttt{A.Lomuscio@doc.imperial.ac.uk}

\textsuperscript{2} IMCS, Jan Długosz University. Al. Armii Krajowej 13/15, 42-200 Częstochowa, Poland
\{b.wozna,a.zbrzezny\}@ajd.czest.pl

Abstract. We present a methodology for verifying epistemic and real-time temporal properties of multi-agent systems. We introduce an interpreted systems semantics based on diagonal timed automata and use a real-time temporal epistemic language to describe properties of multi-agent systems. We develop a bounded model checking algorithm for this setting and present experimental results for a real-time version of the alternating bit-transmission problem obtained by means of a preliminary implementation of the technique.

1 Introduction

Reasoning about knowledge has always been a core concern in AI and in multi-agent systems. This is no surprise given that knowledge is a key concept to model intelligent, rational activities, human or artificial. A plethora of formalisms have been proposed and refined over the years, many of them based on logic. One of the most widely studied is based on variants of modal logics and is commonly referred to as epistemic logic \cite{10}. Rather than providing a computational engine for artificial agents’ reasoning, epistemic logic, at least in this line, is seen as a specification language for modelling and reasoning about systems, much in common with formal methods in computer science.

Specification languages are most useful when they can be verified automatically. In this effort both theorem proving and model checking techniques and tools have been made available for epistemic logic. In particular, model checking techniques based on BDD \cite{18,20}, bounded model checking \cite{16}, unbounded model checking \cite{11} have been developed and their implementation either publicly released \cite{18,12} or made available via a web-interface \cite{15}.

\* The author acknowledge support from the EPSRC (grant GR/S49353).
\** The research presented here was conducted while B. Woźna was at University College London supported by EPSRC (grant GR/S49353). The author also acknowledges support from the Ministry of Science and Information Society Technologies under grant number 3 T11C 011 28.
\*** The author acknowledges partial support from the Ministry of Science and Information Society Technologies under grant number 3 T11C 011 28.

© Springer-Verlag Berlin Heidelberg 2007
Given the above, one may be forgiven for thinking that verification via model checking of temporal epistemic logic has now become of age; however, in many respects the area is still lacking support for many essential functionalities. One of these is real-time. While the formalisms above deal with discrete sequence of events, it is often of both theoretical and practical interest to refer to a temporal model that assumes a dense sequence of events and use operators able to represent dense temporal intervals. The only work in this line we are aware of is [21], where a bounded model checking algorithm for TECTLK was suggested. In this paper we aim to extend two key limitations of that work in that: 1) we assume a computationally more expressive underlying semantical model (diagonal timed automata), 2) we report on an in-house implementation of this technique and discuss experimental results. Further, to exemplify the use of the techniques described in the paper we present a real-time version of the alternating bit transmission problem — a key requirement of this example is the expressive power of a semantics based on diagonal timed automata as the one presented here.

The rest of the paper is organised as follows. In Section 2 we present real-time interpreted systems, a semantics for knowledge and real-time, based on diagonal timed automata. In Section 3 we present syntax and semantics for TECTLK, the logic for which the verification method is defined. In Section 4 we define a bounded model checking algorithm for the logic; given the state-spaces in question are infinite the method involves a tailored discretisation process. Finally we test these techniques on a novel real-time variant of the alternating bit protocol.

2 Diagonal Real-Time Interpreted Systems

In [21] a semantics for real-time and knowledge based on non-diagonal timed automata was proposed. Automata are given as the finer grained semantics on which real-time interpreted systems are defined. In that framework the only clock conditions that can be used are of the form $x \sim c$, where $x$ is a clock, $c$ a constant and $\sim$ an equality/inequality relation. While this is appropriate for some scenarios (like the “railroad crossing system”), it is known that in others more expressive tests are required. Crucially, we may need to compare two clocks of the system as an enabling condition for a transition. Aim of this paper is to analyse this setting for the case of real-time and epistemic properties by means of diagonal automata.

Of course from a theoretical point of view, every diagonal timed automaton can be transformed into non-diagonal timed automaton [3], but the transformation suffers from an exponential blow up in the size of the automaton’s clocks. However the approach presented here is known to generate considerable complications in the verification methodology [5] and results in a loss of completeness in the resulting bounded model checking technique [14].

To define diagonal real-time interpreted systems we first recall the definitions of diagonal timed automata and their composition. We refer to [19] for discussion and more details.

We assume a finite set $X$ of real variables, called clocks, and for $x, y \in X$, $\sim \in \{<, \leq, =, >, \geq\}, c \in \mathbb{N}$, where $\mathbb{N} = \{0, 1, \ldots\}$ is a set of natural numbers, we