Efficient Model Checking of Causal-Knowledge Protocols

Wojciech Penczek

Institute of Computer Science
Polish Academy of Sciences, Warsaw, Poland
and Akademia Podlaska
Institute of Informatics, Siedlce, Poland
penczek@ipipan.waw.pl

Abstract. A model checking algorithm for proving correctness of causal knowledge protocols for multi-agent systems is given. Protocols are specified in an extension of the temporal logic of causal knowledge \[18\]. The temporal language is interpreted over labelled prime event structures. The epistemic operators correspond to knowledge and goals, whereas the temporal modalities correspond to the immediate causality and causality. The model checking algorithm is translated to the model checking problem for LTL or ACTL. This enables a further translation to the SAT-problem, using the technique of the bounded model checking.

1 Introduction

The classical definition of knowledge and semantics of knowledge-based programs are built on global states and global time, see \[6,5\]. The consequence of that definition is logical omniscience of the agents, which is frequently regarded as a drawback, especially if the agents are modeled to take decisions in real time. An alternative proposal to the classical notion of knowledge \[19,17,18\] is based on partial order structures of local states, called event structures \[20,16\]. Knowledge is acquired by the agents via communication with local interactions. Each agent has (causal) knowledge about the most recent events of the other agents. This approach captures the changes in state due to actions, which is crucial for successful modeling of knowledge, but quite rarely incorporated by global state logical formalisms (due to undecidability \[19\]). In addition to the advantage of having a very intuitive and “practical” notion of knowledge, there are two more important reasons for investigating knowledge in the framework of partial order models of local states. Firstly, there is no distinction between computations that are equivalent with respect to the ordering of independent operations, which makes it a natural framework. Secondly, local state based interpretations allow for using efficient methods of alleviating the state explosion problem in verification \[17\].

$\star$ Partly supported by the State Committee for Scientific Research under the grant No. 7T11C 006 20
Model checking is one of the most successful methods of automatic verification of program properties. A model-checking algorithm decides whether a finite-state distributed system satisfies its specification, given as a formula of a temporal logic \([3,8]\). In this paper we address a model checking problem for an extension of the temporal logic of causal knowledge on local states, suggested in \([18]\). The logics is used to specify causal knowledge based protocols for multi-agent systems. The agents acquire their knowledge gradually by getting informations from other agents during execution of synchronization actions and take decisions depending on their knowledge.

We start with defining labelled prime event structures (lpes) to represent behaviours of multi agent systems in terms of executed events and their relationships. Since our modal language is to be interpreted over local state occurrences (lso’s) rather than over events, for each lpes we define the corresponding iso-structure, which serves as a frame. Iso-structures (typically infinite) are generated by finite deterministic asynchronous automata \(A\) using trace semantics.

In order to define a model checking algorithm over an iso-structure, we need to find its finite quotient structure, which preserves the formulas of our language. This problem is solved by using a gossip automaton, which keeps track about the latest information the agents have about each other. The global state space of the product of the gossip automaton and the automaton \(A\) is a required finite quotient structure.

The main contribution of this paper relies on defining a model checking algorithm for proving correctness of causal knowledge protocols w.r.t. the goals of the agents. Moreover, our algorithm is defined in such a way that it can be translated to the model checking problem for LTL or ACTL \([3,8]\). This enables a further translation to the SAT-problem using a very promising technique of the bounded model checking \([1,21]\). The rest of the paper is organized as follows. In section 2 labelled branching synchronization structures are introduced. Modal logic of causal knowledge is defined in section 3. Model checking is explained in section 4. Translation to the SAT-problem is discussed in section 5. In section 6 we discuss a related work.

2 Labelled Branching Synchronization Structures

Our formal theory of Multi Agent Systems (MASs) uses an event-based approach. Event structures have been successfully applied in the theory of distributed systems \([20]\) and several temporal logics have adopted them as frames \([9,16,18]\). Next, we present a formal definition of an event structure.

Definition 1. A labelled prime event structure (lpes, for short) is a 5-tuple \(\mathcal{ES} = (E, A, \rightarrow, \#, l)\), where

1. \(E\) is a finite set, called the set of events or action occurrences,
2. \(A\) is a finite set, called the set of actions,
3. \(\rightarrow \subseteq E \times E\) is an irreflexive, acyclic relation, called the immediate causality relation between the events such that \(\downarrow e \overset{df}{=} \{ e' \in E \mid e' \rightarrow^* e \}\) is finite for each \(e \in E\), where \(\rightarrow^*\) is the reflexive and transitive closure of \(\rightarrow\).