
Final accepted version (with author's formatting)
Available from Middlesex University's Research Repository at http://eprints.mdx.ac.uk/19691/

Copyright:

Middlesex University Research Repository makes the University's research available electronically.

Copyright and moral rights to this thesis/research project are retained by the author and/or other copyright owners. The work is supplied on the understanding that any use for commercial gain is strictly forbidden. A copy may be downloaded for personal, non-commercial, research or study without prior permission and without charge. Any use of the thesis/research project for private study or research must be properly acknowledged with reference to the work's full bibliographic details.

This thesis/research project may not be reproduced in any format or medium, or extensive quotations taken from it, or its content changed in any way, without first obtaining permission in writing from the copyright holder(s).

If you believe that any material held in the repository infringes copyright law, please contact the Repository Team at Middlesex University via the following email address:

eprints@mdx.ac.uk

The item will be removed from the repository while any claim is being investigated.
Using multi-agent systems to go beyond temporal patterns verification

Franco Raimondi, Department of Computer Science
Middlesex University, London
Email: f.raimondi@mdx.ac.uk

A key step in formal verification is the translation of requirements into logic formulae. Various flavours of temporal logic are commonly used in academia and in industry to capture, among others, liveness and safety requirements. In the past two decades there has been a substantial amount of work in the area of verification of extensions of temporal logic. In this column I will provide a high level overview of some work in this area, focussing in particular on the verification of temporal-epistemic properties, showing how temporal-epistemic logics can be used to capture requirements that are common in many concrete systems, and describing a model checker for multi-agent systems called MCMAS.

1. INTRODUCTION

Expressing properties such as mutual exclusion and deadlock freeness using temporal logics such as LTL or CTL [Baier and Katoen 2008] is nowadays considered a standard skill for software engineers and computer science graduates, especially when they are working on safety- and mission-critical projects. Several model checking tools, such as Spin [Holzmann 2003] and NuSMV [Cimatti et al. 2002], support the verification of temporal properties and are now mature enough to be incorporated into the development lifecycle of industrial products. A detailed study of property specifications [Dwyer et al. 1999] has built a repository of patterns, encoding desired behaviours of systems in the most common temporal logics.

Temporal logics belong to the more general class of modal logics [Hughes and Cresswell 1996], which extend propositional logic with modalities. In addition to temporal logics, other examples of modal logics include doxastic logic with modalities to reason about beliefs, deontic logic to reason about obligations, and epistemic logic to reason about knowledge. The proposal of using temporal logic to reason about the correctness of programs has been put forward in [Pnueli 1977] and since then temporal logic has gained wide acceptance in software engineering. However, other modalities have not “transitioned” in a similar way outside the more theoretical venues in Computer Science.

Modal logics have been used routinely in artificial intelligence and multi-agent systems. In particular, there has been a substantial amount of work in the past 20 years in the area of verification for multi-agent systems. On the other hand, the software engineering community and the certification authorities seem to have focussed mainly on temporal specifications. The current trend in integrating automation and humans, for instance in creating autonomous cars and a mixed airspace with autonomous and human-controlled aircraft, gives rise to systems whose requirements can be easily captured by multi-modal logics [Gabbay et al. 2003] that extend temporal-only logic.

In this paper I will focus mainly on temporal-epistemic logic with the aim of showing that the tools and the techniques available can capture in a natural and efficient way several patterns that require reasoning about knowledge and its temporal evolution in a system composed of multiple components. I will show how multi-agent systems (MAS) provide a suitable abstraction for this kind of reasoning and I will provide an overview of MCMAS [Lomuscio et al. 2015], a model checker dedicated to extensions of temporal logic.

The rest of the paper is organised as follows: I discuss Kripke semantics for extensions of temporal logic in Section 2. I will then present a computationally grounded
formalism for multi-agent systems in Section 3, describe the tool MCMAS in Section 4 and introduce some examples in Section 5.

2. KRIPKE SEMANTICS FOR TEMPORAL-EPISTEMIC LOGICS

In this section I introduce the syntax and the semantics of temporal-epistemic logic. I start with a quick overview of temporal logics and then I introduce epistemic logic, discussing the notions of knowledge, group knowledge, distributed and common knowledge.

2.1. Temporal logics

The two most common flavours of temporal logic are LTL (Linear Temporal Logic) and CTL (Computation Tree Logic). The syntax of LTL is as follows:

\[ \phi ::= p \mid \neg \phi \mid \phi \lor \phi \mid X\phi \mid G\phi \mid F\phi \mid \phi U \psi \]

where the other propositional connectives for conjunction and implication can be derived as usual. The temporal operators `X`, `G`, `F` express, respectively, that something is true in the next state, globally, and at some point in the future. The binary operator `U` requires that the second formula `\psi` must become true at some point in the future, and until that point `\phi` has to remain true. The syntax of CTL is similar, but it prefixes each temporal operator with a path quantifier:

\[ \phi ::= p \mid \neg \phi \mid \phi \lor \phi \mid EX\phi \mid EG\phi \mid EF\phi \mid E[\phi U \psi] \]

(There the dual quantifier `A` for “All paths” can be obtained in a standard way).

Given a set of atomic propositions `AP`, temporal logic formulae are interpreted in Kripke structures `M = (S, t, L, I)`, where `S` is a set of states, `t \subseteq S \times S` is a temporal transition relation, `L : S \rightarrow 2^{AP}` is a labelling function for states, and `I \subseteq S` is a set of initial states. In the reminder, I will use the term Kripke structure and model interchangeably. A path `π` is a sequence of states `π = (s_0, s_1, \ldots)` such that `(s_i, s_{i+1}) \in t` for all `i \geq 0`. A state `s_i` in a path `π` is denoted by `π(i)`. CTL formulae are evaluated in a state of a model, while LTL formulae are evaluated over paths. In particular, the semantics of temporal CTL operators is defined in terms of paths, as follows:

\[ M, s \models EX\phi \iff \text{there exists a path } \pi \text{ s.t. } s = \pi(0) \text{ and } M, \pi(1) \models \phi \]

\[ M, s \models EG\phi \iff \text{there exists a path } \pi \text{ s.t. } s = \pi(0) \text{ and } M, \pi(i) \models \phi \text{ for all } i \geq 0 \]

\[ M, s \models E[\phi U \psi] \iff \text{there exists a path } \pi \text{ s.t. } s = \pi(0) \text{ and there exists a } j \text{ s.t. } M, \pi(j) \models \psi \text{ and for all } 0 \leq i \leq j, M, \pi(i) \models \phi \]

The semantics of LTL operators is defined in terms of paths, as follows:

\[ M, s \models X\phi \iff M, \pi[i] \models \phi \]

\[ M, s \models G\phi \iff M, \pi[i] \models \phi \text{ for all } i \geq 0 \]

\[ M, s \models [\phi U \psi] \iff \text{there exists a } j \text{ s.t. } M, \pi[j] \models \psi \text{ and for all } 0 \leq i \leq j, M, \pi[i] \models \phi \]

(where `\pi[i]` is the suffix path of `\pi` starting at state `i`).

2.2. Epistemic and temporal-epistemic logics

The syntax of single-agent epistemic logic is given by the following grammar:

\[ \phi ::= p \mid \neg \phi \mid \phi \lor \phi \mid K\phi \]

\footnote{The semantics of EF can be defined in term of EU, as $EF\phi \equiv E[\top U \phi]$.}
in which propositional logic operators are extended with the operator $K$. The formula $K\phi$ is read as “knows that $\phi$” and is normally used to express the epistemic state of an agent (more on this later).

Epistemic formulae are interpreted in Kripke structures $M = (S, \sim, L)$ in which, as in the previous section, $S$ is a set of states, $L$ is a labelling function and $\sim \subseteq S \times S$ is an accessibility relation that is serial, transitive and symmetric. The accessibility relation $\sim$ is thus an equivalence relation encoding the set of states that are indistinguishable for an agent. The semantics of the $K$ operator is given in terms of $\sim$, as follows:

$$M, s \models K\phi \text{ iff } M, s' \models \phi \text{ for all } s' \text{ s.t. } (s, s') \in \sim$$

Intuitively, an agent consider $K\phi$ true in a state $s$ if and only if $\phi$ is true in all the states that the agent cannot distinguish from $s$. This is a very strong notion of “knowledge”: not only it implies that an agent knows all tautologies, it also implies positive and negative introspection, in the sense that, if the agents knows something, then it knows that it knows it, and if an agent does not know something, then the agent knows that it does not know it. Nevertheless, this characterisation of knowledge is appropriate for a range of scenarios [Fagin et al. 2003], such as when reasoning about security properties and other epistemic states of agents.

Temporal and epistemic logics can be fused (in a technical sense, see [Gabbay et al. 2003]), resulting in a multi-dimensional modal logic in which the temporal and epistemic components are evaluated separately. In fact, one could consider multiple agents, each of them with their own epistemic accessibility relation. Consider $n$ agents: a temporal-epistemic Kripke structure is defined as

$$M = (S, t, \{\sim_i\}_{1 \leq i \leq n}, L)$$

This Kripke structure has $n + 1$ relations: a temporal one and $n$ epistemic accessibility relations, one for each agent. This model allows the interpretation of formulae defined by the following syntax, in addition to propositional and temporal operators:

$$\phi ::= K_i\phi \mid E_{\Gamma}\phi \mid D_{\Gamma}\phi \mid C_{\Gamma}\phi$$

where $i$ is an index ranging from 1 to $n$, $\Gamma \subseteq \{1, \ldots, n\}$ is a group of agents, $E_{\Gamma}\phi$ denotes that everybody in a group knows $\phi$, $D_{\Gamma}\phi$ denotes that $\phi$ is distributed knowledge in the group, and $C_{\Gamma}\phi$ denotes that $\phi$ is common knowledge in the group. To clarify the difference between these three group operators, consider the following example: Alice is the teenage daughter of Bob. Alice smokes cigarettes but she has always kept this secret from her father, so she thinks that he does not know that she smokes. However, one day Bob could see Alice smoking in a corner, without being noticed by her. Additionally, Alice keeps cigarettes in a drawer in her bedroom, and Bob does not know about this. In this situation, everybody knows that Alice smokes. Also, the location of the cigarettes is distributed knowledge between Alice and Bob (this is the knowledge that could be achieved if epistemic states where shared). However, the fact that Alice smokes is not common knowledge because Alice does not know that her father knows that she smokes. Suppose now that one day Bob enters Alice’s room while she is smoking: at this point the fact that Alice smokes is common knowledge between Alice and Bob. I refer to [Fagin et al. 2003] for the formal semantics of epistemic group operators in terms of the epistemic accessibility relations of each agent.

3. MULTI-AGENT SYSTEMS

One of the reasons for temporal patterns to be more widely used than epistemic or other modalities is probably the clear link between the temporal evolution of a program
and the temporal relation $t$ defined in the previous section. A possible execution of a program path is a possible path in a model, and the set of all possible executions is the model. To make verification of temporal-epistemic properties viable it is necessary to make clear the link between “real” executions and Kripke structures. This is exactly the notion of *computationally grounded semantics* introduced in [Wooldridge 2000].

### 3.1. Interpreted systems

In this section I describe the formalism of interpreted systems [Fagin et al. 2003], showing how they link both to executions of “real” systems and to Kripke structures. For a given set of $n$ agents $Agt = \{Ag_1, Ag_2, \ldots, Ag_n\}$, an interpreted system is a tuple:

$$IS = (\{L_i, Act_i, P_i, t_i\}_{i \in Agt}, I, h)$$

where $L_i$ is a finite set of local states for agent $Ag_i$, $Act_i$ is a finite set of actions that agent $Ag_i$ can perform, $P_i : L_i \rightarrow 2^{Act_i}$ is a function, called a protocol, that specifies which actions are enabled in each local state for agent $Ag_i$, and $t_i : (L_i \times Act_1 \times \cdots \times Act_n) \rightarrow L_i$ is a local temporal relation that describes the evolution of the local states of $Ag_i$ in terms of its current local states and of the actions of all the other agents. This implies that agents can only “see” the actions of the other agents, but not their local states. The characterisation of an interpreted system is completed by a set of initial states $I \subseteq L_1 \times \cdots \times L_n$ and by an evaluation function $h : (L_1 \times \cdots \times L_n) \rightarrow 2^{AP}$, where $AP$ is a set of atomic propositions.

Each interpreted system gives rise to an *induced* multi-dimensional Kripke structure $M_{IS} = (S, t, \{\sim_i\}_{i \in Agt}, L)$, as follows:

- The set $S$ is the set of of *reachable global states*: this is the set of states $S \subseteq (L_1 \times \cdots \times L_n)$ that are reachable from $I$ according to the local temporal relations.
- The temporal relation $t$ is defined by the composition of the temporal relations $t_i$ that, in turn, take into account the protocols of each agent.
- The epistemic accessibility relations are defined by equivalence of local states. Formally, two global states $g = (l_1, \ldots, l_n)$ and $g' = (l'_1, \ldots, l'_n)$ are epistemically equivalent for agent $i$ iff $l_i = l'_i$. This is a key point, as it allows to define epistemic accessibility relations as the byproduct of the temporal evolution and the structure of the overall system, thereby providing a *computationally grounded semantics*.
- The evaluation function $L$ is identical to the evaluation function $h$.

As a result, it is possible to use all the known results for standard Kripke structures in interpreted systems. In particular, traditional model checking algorithms can be employed for the verification of temporal-epistemic formulae in interpreted systems, as discussed in the next section.

### 3.2. Model checking multi-agent systems

Several approaches have been developed to verify multi-agent systems using model checking. In general, and at a very high level, most of the model checking techniques [Baier and Katoen 2008] for temporal logics transfer to model checking multi-agent systems. Examples of model checkers for multi-agent systems include:

- VerICS [Kaczprzak et al. 2008; Meski et al. 2011]: this is a model checker that supports the verification of CTL and LTL extended with knowledge. It implements model checking techniques based on Ordered Binary Decision Diagrams (OBDDs [Bryant 1986]) and reduction to SAT for bounded model checking.
- MCK [Gammie and van der Meyden 2004; MCK 2016]: this is a model checker that supports the verification of epistemic and CTL* properties, including support for *per-
Agent SampleAgent

Vars:
  v1 : {a, b, c}; — This is a comment
  v2 : boolean;
end Vars

Actions = {action1, action2, action3};

Protocol:
  v1=a and v2=false : {action1};
  v1=b : {action2, action3};
  Other : {action3};
end Protocol

Evolution:
  (v2=true) if (v2=false) and
  (AnotherAgent.Action=someAction);
end Evolution
end Agent

Fig. 1. A minimal ISPL example: an Agent.

exact recall semantics [van der Meyden and Shilov 1999] for some specific patterns of
formulae.

— Other approaches have reduced the model checking problem for multi-agent system
to a temporal-only model checking problem using NuSVM [Su et al. 2007; Lomuscio
et al. 2007].

In this column I will focus mainly on the model checker MCMAS [Lomuscio et al.
2015]. This model checker supports the verification of CTL properties extended with
epistemic operators (both for individual and for group of agents), in addition to ATL
operators [Alur et al. 2002], implementing OBDD-based verification. MCMAS
implements the standard model checking algorithm for CTL, which is based on the fix-point
characterisation of temporal operators [Baier and Katoen 2008]. This algorithm is ex-
tended to epistemic operators for individual agents by taking into account that the
K operator behaves like the AX operator, but over the epistemic transition. The op-
erator for common knowledge, instead, is computed as a fix-point of the operator for
“everybody knows” $E_\Gamma \phi$, building on the observation that $C_\Gamma \phi \equiv E_\Gamma (\phi \land C_\Gamma \phi)$.

4. THE MODEL CHECKER MCMAS

MCMAS [Lomuscio et al. 2015] is a Model Checker for Multi-Agent Systems, released
for the first time in 2004. It allows the verification of CTL formulae extended with epis-
temic modalities (both individual and groups), the verification of ATL properties [Alur
et al. 2002] and it supports fairness conditions and counter-example/witness genera-
tion. In its default configuration MCMAS implements the standard labelling algorithm
for CTL extended to epistemic and strategic operators. The verification engine makes
use of OBDDs [Bryant 1986] to represent states and transitions symbolically.

MCMAS semantics is based on interpreted systems and its input language is called
ISPL (Interpreted Systems Programming Language). Figure 1 provides an example to
encode an agent called SimpleAgent. The local states of an agent are defined by the
variables it controls: in this example, two variables are declared, an enumeration and
a boolean variable, for a total of 6 possible local states. The data types supported by
MCMAS are boolean, enumerations, and bounded numeric ranges. Actions are defined
as a simple list of labels, while the protocol section allows the introduction of non-
determinism in the model (see the protocol line assigning two possible actions to the
case $v1 = b$). The evolution function is encoded using a NuSMV-like syntax: the evolu-
tion line in Figure 1 is read as “The next value of $v2$ is true if the current value is false
and the action of AnotherAgent is someAction.”
MCMAS is available for download from http://vas.doc.ic.ac.uk/software/mcmas/. The tool is released as open source and it includes a graphical interface based on an Eclipse plug-in. A screenshot of the editor window is shown in Figure 2. Formulae to be verified are listed at the end of the ISPL file and the tool can generate a witness/counter-example for temporal and epistemic/strategic formulae. These are displayed as a tree and can be exported as an image. The tool is built using standard C/C++, Flex and Bison and it has been compiled on Windows, Mac, and Linux. I refer to [Lomuscio et al. 2015] for a more detailed description and for performance considerations.

5. EXAMPLES

As mentioned at the beginning of this column, the key feature of temporal-epistemic logic is that it allows the encoding of several requirements that may be difficult to express using temporal-only formulae. Examples of domains in which temporal-epistemic logic have been employed are the verification of authentication protocols [Boureanu et al. 2009], the verification of BPEL web-service composition [A. Lomuscio 2012], the verification of a confidential conference management system [Kanav et al. 2014], etc.

In this section I provide two simple examples to show how temporal-epistemic logic can express the key properties of two systems in a compact and intuitive form: the protocol of the dining cryptographers [Chaum 1988] and a characterisation of situational awareness using a temporal-epistemic pattern [Chen et al. 2015].

5.1. The protocol of the Dining Cryptographers

The original wording of this example is as follows:

"Three cryptographers are sitting down to dinner at their favourite three-star restaurant. Their waiter informs them that arrangements have been made with the maître d’hotel for the bill to be paid anonymously. One of the cryptographers might be paying for the dinner, or it might have been NSA (U.S. National Security Agency). The three cryptographers respect each other’s right to make an anonymous payment, but they won-
der if NSA is paying. They resolve their uncertainty fairly by carrying out the following protocol:

Each cryptographer flips an unbiased coin behind his menu, between him and the cryptographer on his right, so that only the two of them can see the outcome. Each cryptographer then states aloud whether the two coins he can see – the one he flipped and the one his left-hand neighbour flipped – fell on the same side or on different sides. If one of the cryptographers is the payer, he states the opposite of what he sees. An odd number of differences uttered at the table indicates that a cryptographer is paying; an even number indicates that NSA is paying (assuming that the dinner was paid for only once). Yet if a cryptographer is paying, neither of the other two learns anything from the utterances about which cryptographer it is. [Chaum 1988]

This protocol is the basic building block for the definition of more complex infrastructures enabling anonymous communication over public networks; moreover, notice that the protocol works for any number of cryptographers greater or equal to three.

The key property of this example can be formalised by the following formula

\[ \text{AG} \left( \bigwedge_{i=1}^{n} c_i \text{announced} \land \neg c_1 \text{paid} \implies \left( K_{c_1} \left( \bigwedge_{i=1}^{n} \neg c_i \text{paid} \right) \lor \left( K_{c_1} \left( \bigvee_{i=2}^{n} c_i \text{paid} \right) \land \bigwedge_{i=2}^{n} \neg K_{c_1} (c_i \text{paid}) \right) \right) \right) \]

where AG is the CTL temporal operator expressing that the formula is true in all states, \( n \) is the number of cryptographers, \( c_i \text{announced} \) represents the announcement made by cryptographer \( i \), and \( c_i \text{paid} \) encodes the fact that cryptographer \( i \) paid the bill. Anonymity is captured by the fact that, if a cryptographer did not pay and there is an odd number of “different” utterances, then the cryptographer knows that someone paid for the dinner (expressed as a disjunction), but the cryptographer does not know who actually paid.

5.2. Situational awareness as a temporal-epistemic formula

As stated in [Chen et al. 2015], “Informally, situational awareness is the ability of an agent (typically human) to determine the correct internal state of some component (or some other agent) based on his/her current beliefs. Situational awareness is a key factor for decision makers in safety-critical situations, such as airplane pilots, medical doctors, firemen, etc”.

The work in [Chen et al. 2015] introduces an extension of epistemic logic that allows to count the number of states of an epistemic equivalence class in which a given formula is true. In turn, this allows for the definition of a doxastic operator \( B_{<\delta} \phi \), which is true if the ratio of states in an equivalence class in which \( \phi \) is true is \( < \delta \). The work in [Chen et al. 2015] models an avionic scenario and it defines the lack of situational awareness of a situation \( \phi \) if there exists a state in which \( \phi \) is true, but an agent believes it to be true with certainty less than 5% (this limit is arbitrary and can be modified). Specifically, consider a stall situation characterised by the proposition actualStall, and consider that a Pilot can be represented by an agent. Then, the fact that it is possible for a pilot to have lack of situational awareness of a stall can be characterised by the following formula:

\[ \text{EF} \left( \text{actualStall} \land B_{<0.05} \text{actualStall} \right) \]
A tool like MCMAS can be used to verify whether this formula is true in a model of the cockpit of an airplane, thus enabling the detection of potentially dangerous flaws very early in the design stages of a project.

6. CONCLUSION

In this column I have discussed how the extension of temporal logic with epistemic operators enables the formalisation of requirements from a range of domains. After introducing some basic concepts, I have discussed the notion of computationally grounded semantics for multi-agent systems and I have presented MCMAS, a tool that supports the verification of extensions of the temporal logic CTL in multi-agent systems.

My opinion is that an understanding of extensions of temporal logic should be part of the skills of everyone involved in verification of critical systems, as these extensions enable the formalisation of a range of requirements that may be difficult to express otherwise. I have only sketched some of the research in this area and I refer the interested reader to the proceedings of conferences such as AAMAS and IJCAI for more in-depth results.

Acknowledgements

I gratefully acknowledge Giuseppe Primiero for his comments and feedback.

REFERENCES


