Bounded Model Checking Knowledge and Branching Time in Synchronous Multi-agent Systems [*]

Xiangyu Luo[1], Kaile Su[1,2], Abdul Sattar[2], Qingliang Chen[1], Guanfeng Lv[1]
[1]Department of Computer Science, Sun Yat-sen University, Guangzhou, P.R. China
[2]Institute for Integrated and Intelligent Systems, Griffith University, Brisbane, Australia
xiang_yu_luo@yahoo.com.cn

ABSTRACT

We present an approach to the verification of temporal epistemic properties in synchronous multi-agent systems (MAS) via bounded model checking (BMC). Based on the semantics of synchronous interpreted system, we extend the temporal logic CTL^* by incorporating epistemic modalities and obtain the so-called temporal epistemic logic CTL^*K. Though CTL^*K is of great expressive power in both temporal and epistemic dimensions, we show that BMC method is still applicable for the universal fragment of CTL^*K. We present in some detail a BMC algorithm by using the semantics of synchronous interpreted system. In our approach, agents' knowledge interpreted in synchronous semantics can be skillfully attained by the state position function, which avoids extending the encoding of the states and the transition relation of the plain temporal epistemic model for time domain.

Categories and Subject Descriptors

I.2.11 [**Artificial Intelligence**]: DAI-Multiagent systems

General Terms

Theory, Verification

Keywords

Bounded model checking, temporal epistemic logic, bounded semantics, translation to SAT

1. INTRODUCTION

Model checking is a popular technique for automatic formal verification of finite state systems. Recently, verification of MAS has become an active field of research. In the multi-agent paradigm, particular emphasis is given to the formal representation of the mental attitudes of agents, such as agents' knowledge, beliefs, desires, intentions and so on. However, the formal specifications of the traditional model checking are most commonly expressed as formula of temporal logics such as CTL and LTL. So, the research of MAS verification has focused on the extension of traditional model checking to incorporate epistemic modalities for describing information and motivation attitudes of agents.

In order to overcome the state explosion problem of the BDD-based symbolic model checking, we adopt *bounded model checking* (BMC) in this paper. The basic idea of BMC is to explore a part of the model sufficient to check a particular formula and translate the existential model checking problem over the part of the model into a test of propositional satisfiability.

The aim of this paper is to develop a BMC method for an expressive logic, called $ACTL^*K$, which incorporates epistemic modalities into $ACTL^*$ (the universal fragment of CTL^*). The significance of $ACTL^*K$ is that the temporal expressive power of $ACTL^*K$ is greater than that of $ACTLK$ [3]. For example, we permit the subformula of an epistemic formula to be a *state* or *path* formula, while $ACTLK$ only subsumes *state* formulas. It is convenient to use $ACTL^*K$ to specify and verify dynamic knowledge of agents in dynamic environments.

2. LOGIC CTL^*K AND ITS SUBSETS

In this paper, we extend the temporal logic CTL^* by incorporating epistemic operators, which include $\mathbf{K}_i$ (knows), $\mathbf{D}_\Gamma$ (distributed knowledge), $\mathbf{E}_\Gamma$ (everyone knows) and $\mathbf{C}_\Gamma$ (common knowledge), where $i \in A$, $\Gamma \subseteq A$ and A is a set of agents. To solve the existential model checking problem, we add four dual epistemic operators related to the operators mentioned above. If $\mathbf{Y} \in \{\mathbf{K}_i, \mathbf{D}_\Gamma, \mathbf{E}_\Gamma, \mathbf{C}_\Gamma\}$ and φ is a formula, then $\overline{\mathbf{Y}}$ is the dual operator of $\mathbf{Y}$ and $\mathbf{Y}\,\varphi \equiv \neg\overline{\mathbf{Y}}\,\neg\varphi$. We call the resulting logic CTL^*K.

Here we adopt the *synchronous* interpreted systems semantics [1], which assumes that the agents have perfect recall or the agents have access to a shared clock and run in synchrony. So each agent always ”knows” the time. Formally, for all agents i and all points (r, n) and (r', n'), if $(r, n) \sim_i (r', n')$, then $n = n'$, where the indistinguishability relation $(r, n) \sim_i (r', n')$ indicates that the i-local state $r_i(n)$ is equal to $r'_i(n')$.

Then, the epistemic relations used by $\mathbf{K}_i$, $\mathbf{D}_\Gamma$, $\mathbf{E}_\Gamma$ and $\mathbf{C}_\Gamma$ are defined as $\sim_i$, $\sim^{D}_{\Gamma} = \bigcap_{i\in\Gamma} \sim_i$, $\sim^{E}_{\Gamma} = \bigcup_{i\in\Gamma} \sim_i$, and $\sim^{C}_{\Gamma} =$ the transitive closure of $\sim^{E}_{\Gamma}$, respectively. We only define the synchronous semantics of epistemic operators as follows:

$(r, n) \models \mathbf{Y}\,\varphi$ iff there is a run r' and time n' with $(r, n) \overset{Y}{\sim} (r', n')$
and $n = n'$ such that $(r', n') \models \varphi$,

where $(\mathbf{Y}, \overset{Y}{\sim}) \in \{(\overline{\mathbf{K}}_i, \sim_i), (\overline{\mathbf{D}}_\Gamma, \sim^{D}_{\Gamma}), (\overline{\mathbf{E}}_\Gamma, \sim^{E}_{\Gamma}), (\overline{\mathbf{C}}_\Gamma, \sim^{C}_{\Gamma})\}$.

The $ECTL^*K$ logic is the restriction of CTL^*K such that the negation can be applied only to propositions. The $ACTL^*K$ logic is also the restriction of CTL^*K such that its language is defined as $\{\neg\varphi | \varphi \in ECTL^*K\}$.

[*]Supported by the Australian Research Council grant DP0452628, and partially by the NSFC grants 60496327 and 60473004.

AAMAS'05, July 25-29, 2005, Utrecht, Netherlands.
Copyright 2005 ACM 1-59593-094-9/05/0007 ...$5.00.

3. BOUNDED SEMANTICS OF $ECTL^*K$

In this section we combine the bounded semantics for $ECTL^*$ [2] with epistemic modalities so that the BMC problem for $ECTL^*K$ can be translated into a propositional satisfiability problem.

Let M be a model and k a positive natural number. A *k-path* is a path of length k, i.e. *k-path* is a finite sequence $\pi_k = \{s_0, \ldots, s_k\}$ of states such that $(s_i, s_{i+1}) \in T$ (T is the transition relation of M) for all $0 \leq i < k$, and s_i can be denoted by $\pi_k(i)$. A *k-path* π_k is called a *(k,l)-loop* if $(\pi_k(k), \pi_k(l)) \in T$ for some $0 \leq l \leq k$. To translate the existential model checking into the BMC and SAT problem, we only consider a part of the model M, called k-model (M_k), which consists of all the *k-paths* of M.

A k-path π_k in M_k can be viewed as a part of a *run* r in M. So, we can project a partial r into a k-path π_k. Let $r(n) = \pi_k(m)$ for some $n \geq 0$ and $0 \leq m \leq k$, and let time $c \geq n$ and $0 \leq l \leq k$. We introduce a function $pos(n, m, k, l, c) :=$

$$\begin{cases} m + c - n, & \text{if } c \leq n + k - m; \\ l + (c - n - l + m)\%(k - l + 1), & \text{else if } l \in loop(\pi_k). \end{cases}$$

which returns the position of a state of π_k such that $\pi_k(pos(n, m, k, l, c)) = r(c)$, i.e. the state $\pi_k(pos(n, m, k, l, c))$ of M_k represents the state $r(c)$ of M, where $\%$ is modular arithmetic and $loop(\pi_k) = \{l | 0 \leq l \leq k \text{ and } (\pi_k(k), \pi_k(l)) \in T\}$. Thus, we can use a (k, l)-loop of M_k to represent a part of an *infinite* run of M by the function. Further we define *state position function* $f_I(k, l, c) := pos(0, 0, k, l, c)$ for epistemic operators.

Next, we define the bounded synchronous semantics of $ECTL^*K$, which is a revision of [2], whereas time domain and epistemic operators are added to it. Note that when checking a temporal formula at the state $\pi_k(m)$ and time c, let i be the position of the current state under consideration and c' the corresponding time of the i-th state of the k-path π_k, then $c' = c + i - m$ if $i \geq m$, or else if $l \in loop(\pi_k)$, then $c' = c + k - m + 1 + i - l$, which assures that the time c' always increases. For example, let α be an $ECTL^*K$ formula, the bounded synchronous semantics for the temporal operator **G** (always) is defined as follows:

$$[(\pi_k, l), m, c] \models \mathbf{G}\,\alpha \quad \Leftrightarrow$$
$$\begin{cases} l \notin loop(\pi_k) : false, \\ l \in loop(\pi_k) \text{ and } l \geq m : \forall_{m \leq i \leq k}\, [(\pi_k, l), i, c + i - m] \models \alpha, \\ l \in loop(\pi_k) \text{ and } l < m : \forall_{m \leq i \leq k}\, [(\pi_k, l), i, c + i - m] \models \alpha \\ \qquad\qquad \text{and } \forall_{l \leq i < m}\, [(\pi_k, l), i, c + k - m + 1 + i - l] \models \alpha. \end{cases}$$

As for epistemic conditions, we consider whether or not there is a k-path π_k from the initial state that results in a state s' that is indistinguishable to agent i from the considered global state and the current clock at state s' is equal to the time under consideration. The position of state s' can be obtained by the above method for calculating state position. The bounded synchronous semantics for epistemic operators are defined as follows:

$$[(\pi_k, l), m, c] \models \mathbf{Y}\alpha \quad \Leftrightarrow \quad \exists \pi'_k \in P_k \text{ such that } \pi'_k(0) = s_0 \text{ and}$$
$$\begin{cases} \text{if } c \leq k \text{ then } \pi_k(m) \stackrel{Y}{\sim} \pi'_k(c) \text{ and } \exists_{0 \leq l' \leq k}\, [(\pi'_k, l'), c, c] \models \alpha \\ \text{else } \exists_{0 \leq l' \leq k} \;\; l' \in loop(\pi'_k) \text{ and } \pi_k(m) \stackrel{Y}{\sim} \pi'_k(f_I(k, l', c)) \\ \qquad\qquad \text{and } [(\pi'_k, l'), f_I(k, l', c), c] \models \alpha \;\;, \end{cases}$$

where $(\mathbf{Y}, \stackrel{Y}{\sim}) \in \{(\overline{\mathbf{K}}_i\,, \sim_i), (\overline{\mathbf{D}}_\Gamma\,, \sim^D_\Gamma), (\overline{\mathbf{E}}_\Gamma\,, \sim^E_\Gamma)\}$.
$[(\pi_k, l), m, c] \models \overline{\mathbf{C}}_\Gamma\,\alpha \Leftrightarrow [(\pi_k, l), m, c] \models \bigvee_{i=1}^{k} (\overline{\mathbf{E}}_\Gamma\,)^i \alpha.$

4. BMC FOR $ECTL^*K$

In this section we present a BMC method for $ECTL^*K$ in synchronous interpreted systems. It is an extension of the method presented in [2]. The main idea of the BMC method is that the validity of an $ECTL^*K$ formula φ can be determined by checking the satisfiability of a propositional formula $[M, \varphi]_k = [M^{\varphi, s_0}]_k \wedge [\varphi]_{M_k}$, where $[\varphi]_{M_k}$ is a number of constraints that must be satisfied on M_k for φ to be satisfied, and $[M^{\varphi, s_0}]_k$ represents the (partial) k-model M_k under consideration, which consists of a part of valid k-paths in M_k. Definition 4.7 of [2] plus the following functions determine the number of those k-paths is sufficient for checking formula φ, such that the validity of φ in M_k is equivalent to the validity of φ in the part of M_k.
$f_k(\overline{\mathbf{C}}_\Gamma\,\alpha) = f_k(\alpha) + k,\; f_k(\mathbf{Y}\,\alpha) = f_k(\alpha) + 1$, where $\mathbf{Y} \in \{\overline{\mathbf{K}}_i\,, \overline{\mathbf{D}}_\Gamma\,, \overline{\mathbf{E}}_\Gamma\,\}$.

Once $[M, \varphi]_k$ is constructed, the validity of formula φ over M_k can be determined by checking the satisfiability of the propositional formula $[M, \varphi]_k$ via a SAT solver. Thus, the BMC problem for $ECTL^*K$ ($M \models_k \varphi$) is translated into a propositional satisfiability problem. We give the BMC algorithm for $ECTL^*K$ as follows: let $\varphi = \neg\psi$ if ψ is an $ACTL^*K$ formula. Then, start with $k := 1$, test the satisfiability of $[M, \varphi]_k = [M^{\varphi, s_0}]_k \wedge [\varphi]_{M_k}$ via a SAT solver, and increase k by one either until $[M, \varphi]_k$ becomes satisfiable or k reaches $|M| \cdot |\varphi| \cdot 2^{|\varphi|}$.

The translation for $[M^{\varphi, s_0}]_k$ is omitted here because it is similar to that of [2]. Now we give some details of the translations for $[\varphi]_{M_k}$, i.e. $[\varphi]_k^{[0,0,0]}$. Firstly, we introduce some propositional formulas. Let w, v be two global state variables, s and s' two states encoded by w and v respectively. $I_s(w)$ encodes state s of the model by global state variable w; $H(w, v)$ represents the fact that w, v represent the same state; $H_i(w, v)$ represents that the i-local state in s and s' is the same; $L_{k,j}(l) := T(w_{k,j}, w_{l,j})$ represents that the j-th k-path is a (k, l)-loop. See [3] for more details.

Next, given a k-model M_k and an $ECTL^*K$ formula α. Let $L_{k,i} := \bigvee_{l'=0}^{k} L_{k,i}(l')$ and $x \in \{k, (k, l)\}$. We use $[\alpha]_k^{[m,n,c]}$ to denote the translation of α at state $w_{m,n}$ and time c into a propositional formula based on the bounded semantics of a non-loop k-path, whereas the translation of $[\alpha]_{k,l}^{[m,n,c]}$ depends on the bounded semantics of a (k, l)-loop. The translation of $\mathbf{G}\,\alpha$ and epistemic formulas are defined inductively as follows: $[\mathbf{G}\,\alpha]_k^{[m,n,c]} := false$,

$$[\mathbf{G}\,\alpha]_{k,l}^{[m,n,c]} := \text{if } l \geq m \text{ then } \bigwedge_{i=m}^{k} [\alpha]_{k,l}^{[i,n,c+i-m]}$$
$$\qquad \text{else } \bigwedge_{i=m}^{k} [\alpha]_{k,l}^{[i,n,c+i-m]} \wedge \bigwedge_{i=l}^{m-1} [\alpha]_{k,l}^{[i,n,c+k-m+1+i-l]},$$

$$[\mathbf{Y}\,\alpha]_x^{[m,n,c]} :=$$
$$\begin{cases} \text{if } c \leq k \text{ then } \bigvee_{i=1}^{f_k(\varphi)} (I_{s_0}(w_{0,i}) \wedge \mathbf{Z}(H_a(w_{m,n}, w_{c,i})) \\ \qquad \wedge((\neg L_{k,i} \wedge [\alpha]_k^{[c,i,c]}) \vee \bigvee_{l'=0}^{k} (L_{k,i}(l') \wedge [\alpha]_{k,l'}^{[c,i,c]}))) \\ \text{else } \bigvee_{i=1}^{f_k(\varphi)} (I_{s_0}(w_{0,i}) \wedge \bigvee_{l'=0}^{k} (L_{k,i}(l') \wedge \\ \qquad \mathbf{Z}(H_a(w_{m,n}, w_{f_I(k,l',c),i})) \wedge [\alpha]_{k,l'}^{[f_I(k,l',c),i,c]})), \end{cases}$$

where $(\mathbf{Y}, \mathbf{Z}) \in \{(\overline{\mathbf{K}}_a\,, \epsilon), (\overline{\mathbf{D}}_\Gamma\,, \bigwedge_{a \in \Gamma}), (\overline{\mathbf{E}}_\Gamma\,, \bigvee_{a \in \Gamma})\}$
and ϵ denotes that $\mathbf{Z}$ is empty.
$[\overline{\mathbf{C}}_\Gamma\,\alpha]_x^{[m,n,c]} := [\bigvee_{1 \leq i \leq k} (\overline{\mathbf{E}}_\Gamma\,)^i\,\alpha]_x^{[m,n,c]}.$

5. CONCLUSIONS

According to our BMC method, we are currently implementing the $ACTL^*K$ bounded model checker (MCTK), which is an extension of the LTL BMC modules in NuSMV. We are keen to explore how sophisticatedly SAT solvers developed in constraint satisfaction community can be used for BMC. In addition, we are also interested in the extension of our approach to permit agents to have *perfect recall* [1]. Furthermore, in order to overcome the intrinsic limitation of BMC techniques, we will extend our BMC method to *unbounded model checking* for the full CTL^*K language.

6. REFERENCES

[1] R. Fagin, J. Halpern, Y. Moses, and M. Vardi. *Reasoning about knowledge*. MIT Press, Cambridge, MA, 1995.

[2] B. Woźna. ACTL* properties and Bounded Model Checking. *Fundamenta Informaticae*, 63(1):65–87, 2004.

[3] W.Penczek and A.Lomuscio. Verifying epistemic properties of multi-agent systems via bounded model checking. *Fundamenta Informaticae*, 55, 2003.