

Verification of Multi-agent Systems via Bounded Model Checking ^{*}

Xiangyu Luo¹, Kaile Su^{2,4***}, Abdul Sattar², and Mark Reynolds³

¹ Department of Computer Science, Guilin University of Electronic Technology, Guilin, China
shiangyuluo@gmail.com

² Institute for Integrated and Intelligent Systems, Griffith University, Brisbane, Australia
{k.su, a.sattar}@griffith.edu.au

³ School of CSSE, The University of Western Australia, Perth, Australia
mark@csse.uwa.edu.au

⁴ Department of Computer Science, Sun Yat-sen University, Guangzhou, 510275, China

Abstract. We present a bounded model checking (BMC) approach to the verification of temporal epistemic properties of multi-agent systems. We extend the temporal logic CTL^* by incorporating epistemic modalities and obtain a temporal epistemic logic that we call CTL^*K . CTL^*K logic is interpreted under the semantics of synchronous interpreted systems. 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 and prove its correctness. 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 relations of the plain temporal epistemic model for time domain.

Key words: bounded model checking, multi-agent systems, temporal epistemic logic, bounded semantics

1 Introduction

Model checking is a technique for automatic formal verification of finite state systems. There are many practical applications of the technique for hardware and software verification. Recently, verification of multi-agent systems (MAS) has become an active field of research. Verification of MAS has mainly focused on extending the existing model checking techniques usually used for verification of reactive systems. 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

*** Corresponding author

* This paper is an alternative version of a paper published in Proceedings of Australian Conference on Artificial Intelligence 2006. This work was partially supported by the Australian Research Council grant DP0452628, National Basic Research 973 Program of China under grant 2005CB321902, National Natural Science Foundation of China grants 60496327, 10410638 and 60473004, and Guangdong Provincial Natural Science Foundation grants 04205407 and 06023195.

so on. However, the formal specifications used in the traditional model checking are most commonly expressed as formulas of temporal logics [?] such as *CTL* and *LTL*. So, the research of MAS verification has focused on the extension of traditional model checking techniques to incorporate epistemic modalities for describing information and motivation attitudes of agents [?].

The application of model checking within the context of the logic of knowledge was first proposed by Halpern and Vardi [?] in 1991. In [?,?], van der Hoek and Wooldridge analyzed the application of SPIN and MOCHA respectively to model checking of *LTL* and *ATL* extended by epistemic modalities. In 2004 Meyden and Su took a promising step towards model checking of anonymity properties in formulas involving knowledge [?], and then based on the semantics of interpreted systems with local propositions, Su developed an approach to the BDD-based symbolic model checking for *CKL_n* [?].

Unfortunately, the main bottleneck of BDD-based symbolic model checking is the state explosion problem. One of complementary techniques to BDD-based model checking is *Bounded Model Checking* (BMC). 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 (the problem that decides whether there is a path in a system satisfying a given formula) over the part of the model into a test of propositional satisfiability.

BMC for *LTL* was first introduced by Biere *et al.* [?]. Then, Penczek *et al.* developed a BMC method for *ACTL* (the universal fragment of *CTL*) [?]. In addition, Penczek and Lomuscio presented a BMC method for *ACTLK* in [?], which incorporates epistemic modalities to *ACTL* logic. Further, in [?], Woźna proposed a BMC method for *ACTL**, the universal fragment of *CTL**, which subsumes both *ACTL* and *LTL*. Naturally, it is meaningful to develop a BMC method for those languages that incorporate epistemic modalities into *ACTL**.

In computer science, many protocols are designed so that their actions take place in rounds or steps (where no agent starts round $m + 1$ before all agents finish round m), and agents know what round it is now at all times. Therefore, we restrict MAS to a *synchronous* one, in which agents have access to a shared clock and run in synchrony.

This paper is the extension version of our previous work [?]. The aim of this paper is to develop a BMC method for an expressive branching time logic of knowledge that we call *ACTL*K*, which incorporates epistemic modalities into *ACTL**. We adopt the *synchronous* interpreted systems semantics [?]. Moreover, in order to avoid extending the encoding of the states and the transition relations of the *plain* temporal epistemic model for the time domain of synchronous interpreted systems, we introduce a *state position function* to attain agents' knowledge.

The significance of *ACTL*K* is that the temporal expressive power of *ACTL*K* is greater than that of *ACTLK* extended from *ACTL*. For example, we permit the subformula of an epistemic formula (its main operator is an epistemic one) 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 the dynamic environment of a MAS.

The rest of this paper is organized as follows. Section 2 introduces synchronous semantics of multi-agent interpreted systems. Section 3 defines the syntax and the synchronous semantics of *CTL*K*, and Section 4 defines the bounded semantics of

*ECTL*K*. In Section 5, the equivalence between the synchronous semantics and the bounded one is to be proven. Section 6 describes the BMC method for *ECTL*K*. Finally, we conclude this paper in Section 7.

2 Synchronous Temporal Epistemic Model

We begin with a short discussion about a set of agents $A = \{1, \dots, n\}$ and their environment e . Let L_e be a set of possible states for the environment and L_i a set of possible local states for each agent $i \in A$. We take $G = L_e \times L_1 \times \dots \times L_n$ to be the set of global states and define function $l_i: G \rightarrow L_i$, which returns the local state of agent i from a global state $s \in G$. A *run* over G is a function from the time domain (natural numbers) to G , it can be identified with a sequence of global states in G . A *point* is a pair (r, m) consisting of a run r and time m . The global state at the point (r, m) is defined as $r(m) = (s_e, s_1, \dots, s_n)$, where $s_e \in L_e$ and $s_i \in L_i$ for all $i \in A$. So $r(0)$ is the initial state. Further we define $r_e(m) = s_e$ and $r_i(m) = s_i$ for all $i \in A$. Thus, $r_i(m)$ is agent i 's local state at the point (r, m) . We define a *system* \mathcal{R} over G as a set of runs over G . (r, m) is a point in system \mathcal{R} if $r \in \mathcal{R}$. An *interpreted system* \mathcal{I} is a structure $(\mathcal{R}, \mathcal{V})$, where \mathcal{R} is a system over G and \mathcal{V} assigns truth values to the primitive propositions at the global states in G .

We introduce the indistinguishability relation \sim_i for each agent $i \in A$ as follows. Let s and s' be two global states in G , $s \sim_i s'$ denotes that s and s' are indistinguishable to agent i , i.e., i has the same local state in both s and s' . If $r(n) = s$ and $r'(n') = s'$, we use $(r, n) \sim_i (r', n')$ to denote $s \sim_i s'$. Let $i \in A$ and $\Gamma \subseteq A$, we introduce four epistemic modalities \mathbf{K}_i (knows), \mathbf{D}_Γ (distributed knowledge), \mathbf{E}_Γ (everyone knows) and \mathbf{C}_Γ (common knowledge) to our logic *CTL*K*. Their epistemic relations are defined as $\sim_i, \sim_{\frac{D}{\Gamma}} = \bigcap_{i \in \Gamma} \sim_i, \sim_{\frac{E}{\Gamma}} = \bigcup_{i \in \Gamma} \sim_i$ and $\sim_{\frac{C}{\Gamma}}$, respectively, where $\sim_{\frac{C}{\Gamma}}$ is the transitive closure of $\sim_{\frac{E}{\Gamma}}$ [?]. By modifying the epistemic accessibility relation in Def. 2.1 in [?] to a synchronous one, we get the following definition:

Definition 1. *Given an interpreted system $\mathcal{I} = (\mathcal{R}, \mathcal{V})$ and a set of agents $A = \{1, \dots, n\}$, we associate with \mathcal{I} a Synchronous Temporal Epistemic Model $M = (S, s_0, T, \overset{\mathcal{T}}{\sim}_1, \dots, \overset{\mathcal{T}}{\sim}_n, \mathcal{V})$, where (1) S is a finite set of global states of \mathcal{I} ; (2) s_0 is the initial state of \mathcal{I} ; (3) $T \subseteq S \times S$ is a total binary (successor) relation on S such that $r(m)Tr(m+1)$ for each $r \in \mathcal{R}$ and natural number $m \geq 0$; (4) $\overset{\mathcal{T}}{\sim}_i$ is a synchronous epistemic accessibility relation on the points of \mathcal{I} for agent $i \in A$. Let (r, m) and (r', m') be two points of \mathcal{I} , then $(r, m) \overset{\mathcal{T}}{\sim}_i (r', m')$ iff $r_i(m) = r'_i(m')$ and $m = m'$; (5) $\mathcal{V}: S \times \mathcal{PV} \rightarrow \{\text{true}, \text{false}\}$ is a truth assignment function for a set of propositional variables \mathcal{PV} such that $\mathcal{V}(s)(p) \in \{\text{true}, \text{false}\}$ for all $s \in S$ and $p \in \mathcal{PV}$.*

Thus, given a synchronous temporal epistemic model M , each run of M can be obtained by infinitely unfolding T of M from the initial state s_0 . In addition, let $i \in A$ and $\Gamma \subseteq A$, the epistemic relations used by $\mathbf{K}_i, \mathbf{D}_\Gamma, \mathbf{E}_\Gamma$ and \mathbf{C}_Γ are defined as $\overset{\mathcal{T}}{\sim}_i, \overset{\mathcal{T}}{\sim}_{\frac{D}{\Gamma}} = \bigcap_{i \in \Gamma} \overset{\mathcal{T}}{\sim}_i, \overset{\mathcal{T}}{\sim}_{\frac{E}{\Gamma}} = \bigcup_{i \in \Gamma} \overset{\mathcal{T}}{\sim}_i$, and $\overset{\mathcal{T}}{\sim}_{\frac{C}{\Gamma}}$, respectively, where $\overset{\mathcal{T}}{\sim}_{\frac{C}{\Gamma}}$ is the transitive closure of $\overset{\mathcal{T}}{\sim}_{\frac{E}{\Gamma}}$. It is easy to prove that for any points (r, n) and (r', n') of a synchronous system, $(r, n) \overset{\mathcal{T}}{\sim}_Y (r', n')$ iff $(r, n) \sim_Y (r', n')$ and $n = n'$, where $Y \in \{\mathbf{D}, \mathbf{E}, \mathbf{C}\}$. Hereafter, we use "model" to denote *synchronous temporal epistemic model*.

3 CTL^*K Logic and its Subsets

Here we extend the temporal logic CTL^* [?] by incorporating epistemic modalities, which include \mathbf{K}_i , \mathbf{D}_Γ , \mathbf{E}_Γ and \mathbf{C}_Γ , where $i \in A$ and $\Gamma \subseteq A$. In order to solve the existential model checking problem, we add four dual epistemic modalities related to the modalities mentioned above. If $\mathbf{Y} \in \{\mathbf{K}_i, \mathbf{D}_\Gamma, \mathbf{E}_\Gamma, \mathbf{C}_\Gamma\}$ and φ is a formula, then $\bar{\mathbf{Y}}$ is the dual modalities of \mathbf{Y} and $\mathbf{Y}\varphi \equiv \neg\bar{\mathbf{Y}}\neg\varphi$. We call the resulting logic CTL^*K . Assume the familiarity with the syntax of CTL^* , we refer to [?] for more details. The only thing about CTL^*K mentioned here is that if α is a *path* formula, then epistemic formula $\bar{\mathbf{Y}}\alpha$ is a *state* formula. Note that any state formula is also a path formula.

We define the $ECTL^*K$ logic as the restriction of CTL^*K such that the negation can be applied only to propositions and the operators are restricted to \mathbf{E} (in some path), $\bar{\mathbf{K}}_i$, $\bar{\mathbf{D}}_\Gamma$, $\bar{\mathbf{E}}_\Gamma$ and $\bar{\mathbf{C}}_\Gamma$. The $ACTL^*K$ logic is also the restriction of CTL^*K such that its language is defined as $\{\neg\varphi \mid \varphi \in ECTL^*K\}$, in which the path quantifier \mathbf{A} (in all paths) is defined as $\mathbf{A}\varphi \equiv \neg\mathbf{E}\neg\varphi$.

Definition 2 (Synchronous Semantics of CTL^*K). Let M be a model, (r, n) a point of M and α, β be CTL^*K formulas. $(M, r, n) \models \alpha$ denotes that α is true at point (r, n) . M is omitted if it is implicitly understood. The relation \models is defined as follows:

$(r, n) \models p$ iff $\mathcal{V}(r(n))(p) = \text{true}$, $(r, n) \models \neg p$ iff $(r, n) \not\models p$,
 $(r, n) \models \alpha \wedge \beta \mid \alpha \vee \beta$ iff $(r, n) \models \alpha$ and (or) $(r, n) \models \beta$, $(r, n) \models \mathbf{X}\alpha$ iff $(r, n+1) \models \alpha$,
 $(r, n) \models \mathbf{F}\alpha$ iff $\exists_{n' \geq n} (r, n') \models \alpha$, $(r, n) \models \mathbf{G}\alpha$ iff $\forall_{n' \geq n} (r, n') \models \alpha$,
 $(r, n) \models \alpha \mathbf{U} \beta$ iff $\exists_{n' \geq n} ((r, n') \models \beta$ and $\forall_{n \leq i < n'} (r, i) \models \alpha)$,
 $(r, n) \models \mathbf{E}\alpha$ iff there is a run r' and time n' with $r(n) = r'(n')$ such that $(r', n') \models \alpha$,
 $(r, n) \models \mathbf{Y}\alpha$ iff there is a run r' and time n' with $(r, n) \stackrel{\mathbf{Y}}{\sim} (r', n')$ and $n = n'$ such that $(r', n') \models \alpha$, where $(\mathbf{Y}, \stackrel{\mathbf{Y}}{\sim}) \in \{(\bar{\mathbf{K}}_i, \sim_i), (\bar{\mathbf{D}}_\Gamma, \sim_\Gamma^D), (\bar{\mathbf{E}}_\Gamma, \sim_\Gamma^E), (\bar{\mathbf{C}}_\Gamma, \sim_\Gamma^C)\}$.

As for modality \mathbf{K}_i , here we capture the intuition that agent i knows formula φ at point (r, n) of M exactly if at all points with the same time n that i considers possible at (r, n) , φ is true. For the modality $\bar{\mathbf{K}}_i$, conversely, $(M, r, n) \models \bar{\mathbf{K}}_i\varphi$ if and only if φ is true at some point with the same time n that i considers possible at (r, n) . So with such a synchronous semantics, only one point with time n should be considered in a run.

Definition 3 (Validity). A CTL^*K formula φ is valid in M (denoted $M \models \varphi$) iff $(M, r, 0) \models \varphi$ for all run r in M , i.e., φ is true in the initial state of M .

4 Bounded Semantics of $ECTL^*K$

In this section we combine the bounded semantics for $ECTL^*$ [?] 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 $\pi_k = \{s_0, \dots, s_k\}$ of states such that $(s_i, s_{i+1}) \in T$ for all $0 \leq i < k$, and state s_i of π_k can be denoted by $\pi_k(i)$. A finite k -path can also represent an infinite path if there is a *back loop* from the last state to a certain previous state of the k -path. So, a k -path π_k is a (k, l) -loop if $(\pi_k(k), \pi_k(l)) \in T$ for some $0 \leq l < k$.

Given a model M , in order to translate the existential model checking into bounded model checking and the SAT problem, we only consider a part of the model M , i.e., the compact model consists of all the k -paths of M and is defined as follows.

Definition 4 (k -model). Let $M = (S, s_0, T, \tilde{\tau}_1, \dots, \tilde{\tau}_n, \mathcal{V})$ be a model and k a positive natural number. A k -model of M is a tuple $M_k = (S, s_0, P_k, \tilde{\tau}_1, \dots, \tilde{\tau}_n), \mathcal{V}$, where s_0 is the initial state of M and P_k is the set of all the k -paths of M .

Since the bounded semantics for temporal operators depends on whether the considered k -path π_k of the k -model M_k is a loop or not, we define a function $loop(\pi_k) = \{l \mid 0 \leq l \leq k \text{ and } (\pi_k(k), \pi_k(l)) \in T\}$ so as to distinguish whether π_k is a loop.

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 onto a k -path π_k . Let $r(n) = \pi_k(m)$ for some $n \geq 0$ and $0 \leq m \leq k$, by Def. ??, we can calculate the position $i \in \{0, \dots, k\}$ of the state of π_k such that $\pi_k(i) = r(c)$ for some time $c \geq n$, i.e., state $\pi_k(i)$ of M_k represents state $r(c)$ of M .

Definition 5 (State Position Function). Let M be a model and M_k a k -model of M . Assume that r is a run in M and the corresponding π_k is a k -path of M_k such that $r(n) = \pi_k(m)$ for some $n \geq 0$ and $m \leq k$, then, for time $c \geq n$ and $l \leq k$, function

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

returns the position of the state of π_k such that $\pi_k(pos(n, m, k, l, c)) = r(c)$, where $\%$ is modular arithmetic. Further define State Position Function $f_I(k, l, c) := pos(0, 0, k, l, c)$ for epistemic operators.

Thus, a part of an infinite run of M may be represented by a (k, l) -loop of M_k by means of the state position function. Next, we extend Def. 4.3 in [?] to Def. ??, the bounded semantics of $ECTL^*K$, by incorporating the time domain and epistemic operators.

Definition 6 (Bounded Semantics of $ECTL^*K$). Let M_k be a k -model and α, β $ECTL^*K$ formulas. Given a natural number $l \in \{0, \dots, k\}$, if α is a state formula, then $[M_k, \pi_k, l, m, c] \models \alpha$ denotes that α is true at the state $\pi_k(m)$ of M_k and time c . If α is a path formula, then $[M_k, \pi_k, l, m, c] \models \alpha$ denotes that α is true along the suffix of the k -path π_k of M_k , which starts at the position m and time c . M_k is omitted if it is implicitly understood. The relation \models is defined inductively as follows:

$$[\pi_k, l, m, c] \models p \text{ iff } \mathcal{V}(\pi_k(m))(p) = \text{true}. \quad [\pi_k, l, m, c] \models \neg p \text{ iff } \mathcal{V}(\pi_k(m))(p) = \text{false}.$$

$$[\pi_k, l, m, c] \models \alpha \wedge \beta \mid \alpha \vee \beta \text{ iff } [\pi_k, l, m, c] \models \alpha \text{ and (or) } [\pi_k, l, m, c] \models \beta.$$

$$[\pi_k, l, m, c] \models \mathbf{E}\alpha \text{ iff } \exists \pi'_k \in P_k \left(\pi'_k(0) = \pi_k(m) \text{ and } \exists 0 \leq l' \leq k [\pi'_k, l', 0, c] \models \alpha \right).$$

$$[\pi_k, l, m, c] \models \mathbf{X}\alpha \text{ iff}$$

$$\begin{cases} \text{if } m \geq k \text{ then false else } [\pi_k, l, m + 1, c + 1] \models \alpha, & \text{if } l \notin loop(\pi_k); \\ \text{if } m \geq k \text{ then } [\pi_k, l, l, c + 1] \models \alpha \text{ else } [\pi_k, l, m + 1, c + 1] \models \alpha, & \text{otherwise.} \end{cases}$$

$$[\pi_k, l, m, c] \models \mathbf{F}\alpha \text{ iff } \begin{cases} \exists m \leq i \leq k [\pi_k, l, i, c + i - m] \models \alpha, & \text{if } l \notin loop(\pi_k); \\ \exists m \leq i \leq k [\pi_k, l, i, c + i - m] \models \alpha \text{ or} \\ \exists l \leq i < m [\pi_k, l, i, c + k - m + 1 + i - l] \models \alpha, & \text{otherwise.} \end{cases}$$

$$[\pi_k, l, m, c] \models \mathbf{G}\alpha \text{ iff } \begin{cases} \text{false,} & \text{if } l \notin loop(\pi_k); \\ \forall m \leq i \leq k [\pi_k, l, i, c + i - m] \models \alpha, & \text{if } l \in loop(\pi_k) \text{ and } l \geq m; \\ \forall l \leq i < m [\pi_k, l, i, c + k - m + 1 + i - l] \models \alpha \text{ and} \\ \forall m \leq i \leq k [\pi_k, l, i, c + i - m] \models \alpha, & \text{if } l \in loop(\pi_k) \text{ and } l < m. \end{cases}$$

$$\begin{aligned}
& [\pi_k, l, m, c] \models \alpha \mathbf{U} \beta \text{ iff} \\
& \left\{ \begin{array}{l} \exists_{m \leq i \leq k} \left([\pi_k, l, i, c + i - m] \models \beta \text{ and } \forall_{m \leq j < i} [\pi_k, l, j, c + j - m] \models \alpha \right), \text{ if } l \notin \text{loop}(\pi_k); \\ \exists_{m \leq i \leq k} \left([\pi_k, l, i, c + i - m] \models \beta \text{ and } \forall_{m \leq j < i} [\pi_k, l, j, c + j - m] \models \alpha \right) \text{ or} \\ \exists_{l \leq i < m} \left([\pi_k, l, i, c + k - m + 1 + i - l] \models \beta \text{ and } \forall_{m \leq j \leq k} [\pi_k, l, j, c + j - m] \models \alpha \text{ and} \right. \\ \left. \forall_{l \leq j < i} [\pi_k, l, j, c + k - m + 1 + j - l] \models \alpha \right), \text{ otherwise.} \end{array} \right. \\
& [\pi_k, l, m, c] \models \mathbf{Y} \alpha \text{ iff } \exists \pi'_k \in P_k \text{ such that } \pi'_k(0) = s_0 \text{ and, if } c \leq k, \text{ then } \pi_k(m) \overset{\mathcal{Y}}{\sim} \pi'_k(c) \text{ and} \\
& \exists_{0 \leq l' \leq k} [\pi'_k, l', c, c] \models \alpha; \text{ else } \exists_{0 \leq l' \leq k} (l' \in \text{loop}(\pi'_k) \text{ and } \pi_k(m) \overset{\mathcal{Y}}{\sim} \pi'_k(f_I(k, l', c)) \text{ and} \\
& [\pi'_k, l', f_I(k, l', c), c] \models \alpha), \text{ where } (\mathbf{Y}, \overset{\mathcal{Y}}{\sim}) \in \{(\overline{\mathbf{K}}_i, \sim_i), (\overline{\mathbf{D}}_\Gamma, \sim^D_\Gamma), (\overline{\mathbf{E}}_\Gamma, \sim^E_\Gamma)\}. \\
& [\pi_k, l, m, c] \models \overline{\mathbf{C}}_\Gamma \alpha \Leftrightarrow [\pi_k, l, m, c] \models \bigvee_{i=1}^k (\overline{\mathbf{E}}_\Gamma)^i \alpha.
\end{aligned}$$

From the above bounded semantics, we can see that when checking a temporal formula at the state $\pi_k(m)$ and time c , the time domain c' corresponding to the i -th state of π_k can be calculated as follows: $c' := c + i - m$ if $i \geq m$, or else if $l \in \text{loop}(\pi_k)$, then $c' := c + k - m + 1 + i - l$, where i is the position of the current state under consideration in π_k . It assures that the time c' always increases.

As for the knowledge modality \mathbf{K}_i , we consider whether or not there is a k -path π'_k from the *initial* state (the first state $\pi_k(0)$ of π_k is equal to the initial state of M) that results in a state s' that agent i consider possible in $\pi_k(m)$ and the current time in s' is equal to c . Note that the position of s' should be calculated by the state position function $f_I(k, l, c)$ only if the time $c > k$.

Definition 7 (Validity for Bounded Semantics). An $ECTL^*K$ formula φ is valid in a k -model M_k (denoted $M \models_k \varphi$) iff $[M_k, \pi_k, l, 0, 0] \models \varphi$ for some $0 \leq l \leq k$, where $\pi_k(0)$ is the initial state of M_k .

5 Correctness of the Bounded Semantics

In this section we will prove that the $ECTL^*K$ model checking problem ($M \models \varphi$) can be reduced to the $ECTL^*K$ BMC problem ($M \models_k \varphi$). Some proofs similar to [?] or [?] are omitted for the limited space. Note that the bounded semantics of $ECTL^*K$ differs from those of other papers because we add time to it. Firstly, we define the length of a formula φ (denoted by $|\varphi|$) as the number of operators (exclude \neg) in φ . Then, by Lemma ??, ?? and ??, we can determine the maximum bound k (called Diameter of M) that an $ECTL^*K$ formula should be checked with to guarantee that the property holds.

Lemma 1. Let M be a model and α an LTL formula, the following implication holds: if $M \models \mathbf{E} \alpha$, then there exists $k \leq |M| \cdot |\alpha| \cdot 2^{|\alpha|}$ with $M \models_k \mathbf{E} \alpha$, where $|M|$ is the sum of the number of reachable states and transitions of M (Lemma 4.3 of [?]).

Lemma 2. Let M be a model, α an LTL formula and $\mathbf{Y} \in \{\mathbf{E}, \overline{\mathbf{K}}_i, \overline{\mathbf{D}}_\Gamma\}$, then, if $(M, r, 0) \models \mathbf{Y} \alpha$ then there exists $k \leq |M| \cdot |\alpha| \cdot 2^{|\alpha|}$ with $[M_k, \pi_k, l, 0, 0] \models \mathbf{Y} \alpha$ for some $0 \leq l \leq k$, where $r(0)$ and $\pi_k(0)$ are equal to the initial state of M .

Proof. (1) Let $\mathbf{Y} = \mathbf{E}$. The case can be easily proven by Lemma ?? when time domain is added to it. (2) Let $\mathbf{Y} = \overline{\mathbf{K}}_i$ and $(r, 0)$ be an initial point of M . By Def. ??,

$(M, r, 0) \models \bar{\mathbf{K}}_i \alpha$ iff there is a run r' and time c' with $(r, 0) \sim_i (r', c')$ and $c' = 0$ such that $(M, r', c') \models \alpha$. Since $r'(0)$ is also the initial state of M , it can be viewed as an existential model checking problem [?] for the *LTL* formula α in M . So the case holds by Lemma ??.

(3) Let $\mathbf{Y} = \bar{\mathbf{D}}_\Gamma$. Straightforward by definition from the case $\mathbf{Y} = \bar{\mathbf{K}}_i$. \square

Lemma 3. *Let M be a model, φ be an *ECTL** K formula and (r, c) be a point of M . If $(M, r, c) \models \varphi$, then there exists $k \leq |M| \cdot |\varphi| \cdot 2^{|\varphi|}$ and a k -path π_k of M_k with $r(c) = \pi_k(m)$ such that $[M_k, \pi_k, l, m, c] \models \varphi$ for some $0 \leq l \leq k$.*

Proof. By induction on the length of φ . The lemma follows directly when φ is a propositional variable or its negation. Assume that the hypothesis holds for all the proper subformulas of φ . The lemma is easily proven when $\varphi = \alpha \vee \beta \mid \alpha \wedge \beta$. Consider case 1) and 2):

1) Assume that α is an *LTL* formula. Let $\varphi = \bar{\mathbf{E}}_\Gamma \alpha$. Since $\bar{\mathbf{E}}_\Gamma \alpha = \bigvee_{i \in A} \bar{\mathbf{K}}_i \alpha$, by induction the lemma follows from the case of $\mathbf{Y} = \bar{\mathbf{K}}_i$ in Lemma ?? for some $i \in A$ and the case for the boolean connectives. Let $\varphi = \bar{\mathbf{C}}_\Gamma \alpha$. Because $(M, r, c) \models \bar{\mathbf{C}}_\Gamma \alpha$ iff $(M, r, c) \models \bigvee_{i \leq |S|} (\bar{\mathbf{E}}_\Gamma)^i \alpha$, where $|S|$ is the number of reachable states in M , the lemma holds by induction on the former cases. Because the state under consideration may be the subsequent one of the initial state, the existential model checking problem here is not harder than that of Lemma ??, so Lemma ?? can be applied in the former cases.

2) Assume that α is not a "pure" *LTL* formula, we extend the state labelling technique of [?] to epistemic operators. Let $\varphi = \mathbf{Y} \alpha$ and $\mathbf{Y}, \mathbf{Y}_i, \mathbf{Z} \in \{\mathbf{E}, \bar{\mathbf{K}}_i, \bar{\mathbf{D}}_\Gamma, \bar{\mathbf{E}}_\Gamma, \bar{\mathbf{C}}_\Gamma\}$ for $i = 1, \dots, n$. Let $\mathbf{Y}_1 \alpha_1, \dots, \mathbf{Y}_n \alpha_n$ be the list of all maximal subformulas of α (i.e., each $\mathbf{Y}_i \alpha_i$ is a state subformula of $\mathbf{Y} \alpha$, but not a subformula of any subformula $\mathbf{Z} \beta$ of $\mathbf{Y} \alpha$, where $\mathbf{Z} \beta$ is different from $\mathbf{Y} \alpha$ and $\mathbf{Y}_i \alpha_i$ for $i = 1, \dots, n$).

Next, we introduce for each $\mathbf{Y}_i \alpha_i$ a fresh atomic proposition p_i , where $1 \leq i \leq n$, and augment the labelling of each state s of M_k with p_i iff $\mathbf{Y}_i \alpha_i$ holds at state s , then we replace each subformula $\mathbf{Y}_i \alpha_i$ by p_i and obtains a new formula α' , which is a "pure" *LTL* formula. Furthermore, by the definition of synchronous semantics, we have that verifying $(M, r, c) \models \bar{\mathbf{E}}_\Gamma \alpha' \mid \bar{\mathbf{C}}_\Gamma \alpha'$ can also be viewed as an existential model checking problem for the *LTL* formula α' in M . The proof is similar to that in the case of $\mathbf{Y} = \bar{\mathbf{K}}_i$ in Lemma ??.

Hence, by Lemma ?? and the cases above, we have that $(M, r, c) \models \mathbf{Y} \alpha$ implies $[M_k, \pi_k, l, m, c] \models \mathbf{Y} \alpha$. \square

The condition $r(c) = \pi_k(m)$ in Lemma ?? expresses that the state $\pi_k(m)$ of M_k is the same as the state $r(c)$ of M .

Theorem 1. *Let M be a model and φ an *ECTL** K formula. Then $M \models \varphi$ iff $M \models_k \varphi$ for some $k \leq |M| \cdot |\varphi| \cdot 2^{|\varphi|}$.*

Proof. (\Rightarrow) Follows directly from Lemma ?? with $m = c = 0$.

(\Leftarrow) By induction on the length of φ , the following implication holds: $[M_k, \pi_k, l, 0, 0] \models \varphi$ implies $(M, r, 0) \models \varphi$, where $r(0)$ and $\pi_k(0)$ are equal to the initial state of M . \square

Theorem ?? shows that the satisfiability of an *ECTL** K formula φ in the bounded semantics is equivalent to the unbounded one with the diameter $|M| \cdot |\varphi| \cdot 2^{|\varphi|}$.

6 Bounded Model Checking 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 [?].

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 (the *submodel* of M_k), which consists of a part of valid k -paths in M_k . Def. ?? determines the number of those k -paths that 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 . The bound $f_k(\varphi)$ can be obtained by structural induction on the translation of φ in Def. ??.

Definition 8. Define a function f_k from the set of formulas to natural number:

$$\begin{aligned} f_k(p) = f_k(\neg p) = 0, \text{ where } p \in \mathcal{PV}, \quad & f_k(\alpha \vee \beta) = \max(f_k(\alpha), f_k(\beta)), \\ f_k(\alpha \wedge \beta) = f_k(\alpha) + f_k(\beta), \quad & f_k(\mathbf{X}\alpha) = f_k(\mathbf{F}\alpha) = f_k(\alpha), \\ f_k(\mathbf{G}\alpha) = (k+1) \cdot f_k(\alpha), \quad & f_k(\alpha \mathbf{U}\beta) = k \cdot f_k(\alpha) + f_k(\beta), \\ f_k(\mathbf{C}_\Gamma\alpha) = f_k(\alpha) + k, \quad & f_k(\mathbf{Y}\alpha) = f_k(\alpha) + 1, \text{ where } \mathbf{Y} \in \{\mathbf{E}, \bar{\mathbf{K}}_i, \bar{\mathbf{D}}_\Gamma, \bar{\mathbf{E}}_\Gamma\}. \end{aligned}$$

Once $[M, \varphi]_k$ is constructed, the validity of formula φ over M_k can be determined by checking the satisfiability of $[M, \varphi]_k$ via a SAT solver. We give the BMC algorithm for $ACTL^*K$ as follows: Let φ be an $ACTL^*K$ formula. Then, start with $k := 1$, test the satisfiability of $[M, \neg\varphi]_k$ via a SAT solver, and increase k by one either until $[M, \neg\varphi]_k$ becomes satisfiable or k reaches $|M| \cdot |\neg\varphi| \cdot 2^{|\neg\varphi|}$. If $[M, \neg\varphi]_k$ is satisfiable with some k , then returns " $M \not\models \varphi$ ", returns " $M \models \varphi$ " otherwise.

We now give details of the translations for the propositional formulas $[M^{\varphi, s_0}]_k$ and $[\varphi]_{M_k}$. Because the synchronous model is identical with the model in [?] except that the synchronous epistemic accessibility relation, the technical details of translation are similar to that of [?], from which we only 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 ; $T(w, v)$ encodes $(s, s') \in T$; $p(w)$ represents $p \in \mathcal{V}(s)$; $H(w, v)$ 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 [?] for more details.

The propositional formula $[M^{\varphi, s_0}]_k$ represents the transitions in the k -model M_k , its definition is given as below.

Definition 9 (Unfolding of Transition Relation). Let $M_k = (S, s_0, P_k, \tau_1, \dots, \tau_n, \mathcal{V})$ be a k -model of M , $s \in S$, and φ an $ECTL^*K$ formula. Define formula

$$[M^{\varphi, s}]_k := I_s(w_{0,0}) \wedge \bigwedge_{1 \leq j \leq f_k(\varphi)} \bigwedge_{0 \leq i \leq k-1} T(w_{i,j}, w_{i+1,j}),$$

where $w_{0,0}$ and $w_{i,j}$ are global state variables for $i = 0, \dots, k$ and $j = 1, \dots, f_k(\varphi)$. $w_{i,j}$ also represents the i^{th} state of the j^{th} symbolic k -path.

According to the bounded semantics of $ECTL^*K$, we make the following definition for translating an $ECTL^*K$ formula φ into a propositional formula.

Definition 10. Given a k -model M_k and $ECTL^*K$ formulas α, β and let $L_{k,i} := \bigvee_{l'=0}^k L_{k,i}(l')$, $x \in \{k, (k, l)\}$, 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 φ is defined inductively as follows:

$$\begin{aligned}
[p]_x^{[m,n,c]} &:= p(w_{m,n}), \quad [\neg p]_x^{[m,n,c]} := \neg p(w_{m,n}), \quad [\alpha \wedge \beta]_x^{[m,n,c]} := [\alpha]_x^{[m,n,c]} \wedge [\beta]_x^{[m,n,c]}, \\
[X\alpha]_k^{[m,n,c]} &:= \text{if } m < k \text{ then } [\alpha]_k^{[m+1,n,c+1]} \text{ else false}, \quad [\alpha \vee \beta]_x^{[m,n,c]} := [\alpha]_x^{[m,n,c]} \vee [\beta]_x^{[m,n,c]}, \\
[X\alpha]_{k,l}^{[m,n,c]} &:= \text{if } m < k \text{ then } [\alpha]_{k,l}^{[m+1,n,c+1]} \text{ else } [\alpha]_{k,l}^{[l,n,c+1]}, \quad [F\alpha]_k^{[m,n,c]} := \bigvee_{i=m}^k [\alpha]_k^{[i,n,c+i-m]}, \\
[F\alpha]_{k,l}^{[m,n,c]} &:= \bigvee_{i=m}^k [\alpha]_{k,l}^{[i,n,c+i-m]} \vee \bigvee_{i=l}^{m-1} [\alpha]_{k,l}^{[i,n,c+k-m+1+i-l]}, \quad [G\alpha]_k^{[m,n,c]} := \text{false}, \\
[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]} \\
&\quad \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]}, \\
[\alpha U \beta]_k^{[m,n,c]} &:= \bigvee_{i=m}^k ([\beta]_k^{[i,n,c+i-m]} \wedge \bigwedge_{j=m}^{i-1} [\alpha]_k^{[j,n,c+j-m]}), \\
[\alpha U \beta]_{k,l}^{[m,n,c]} &:= \bigvee_{i=m}^k ([\beta]_{k,l}^{[i,n,c+i-m]} \wedge \bigwedge_{j=m}^{i-1} [\alpha]_{k,l}^{[j,n,c+j-m]}) \\
&\quad \vee \bigvee_{i=l}^{m-1} ([\beta]_{k,l}^{[i,n,c+k-m+1+i-l]} \wedge \bigwedge_{j=m}^k [\alpha]_{k,l}^{[j,n,c+j-m]} \wedge \bigwedge_{j=l}^{i-1} [\alpha]_{k,l}^{[j,n,c+k-m+1+j-l]}), \\
[E\alpha]_x^{[m,n,c]} &:= \bigvee_{i=1}^{f_k(\varphi)} (H(w_{m,n}, w_{0,i}) \wedge ((\neg L_{k,i} \wedge [\alpha]_k^{[0,i,c]}) \vee \bigvee_{l'=0}^k (L_{k,i}(l') \wedge [\alpha]_{k,l'}^{[0,i,c]}))), \\
[Y\alpha]_x^{[m,n,c]} &:= \\
&\quad \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})) \\ \quad \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 \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} \\
&\quad \text{where } (\mathbf{Y}, \mathbf{Z}) \in \{(\bar{\mathbf{K}}_a, \epsilon), (\bar{\mathbf{D}}_\Gamma, \bigwedge_{a \in \Gamma}), (\bar{\mathbf{E}}_\Gamma, \bigvee_{a \in \Gamma})\} \text{ and } \epsilon \text{ denotes that } \mathbf{Z} \text{ is empty.} \\
[\bar{C}\Gamma\alpha]_x^{[m,n,c]} &:= [\bigvee_{1 \leq i \leq k} (\bar{\mathbf{E}}_\Gamma)^i \alpha]_x^{[m,n,c]}.
\end{aligned}$$

Lemma 4. Let M_k be a k -model, φ be an $ECTL^*K$ formula, $m, l \leq k$ and $c \geq 0$. Then, $[M_k, \pi_k, l, m, c] \models \varphi$ iff there is a submodel M'_k of M_k with $|P'_k| \leq f_k(\varphi)$ such that $[M'_k, \pi_k, l, m, c] \models \varphi$.

Lemma 5. Let M_k be a k -model of M , φ an $ECTL^*K$ formula, and $l \leq k$. For each point (r, c) of M , if there is a submodel M'_k of M_k with $|P'_k| \leq f_k(\varphi)$, where P'_k is the set of all the k -paths of M'_k , and there is a k -path $\pi_k \in P'_k$ with $\pi_k(m) = r(c)$ ($m \leq k$), then $M'_k, [(\pi_k, l), m, c] \models \varphi$ if and only if the following conditions holds:

1. $[M^{\varphi, \pi_k(m)}]_k \wedge [\varphi]_k^{[0,0,c]}$ is satisfiable, if φ is a state formula;
2. $[M^{\varphi, \pi_k(m)}]_k \wedge [\varphi]_k^{[m,0,c]}$ is satisfiable, if φ is a path formula and π_k is not a (k,l) -loop;
3. $[M^{\varphi, \pi_k(m)}]_k \wedge [\varphi]_{k,l}^{[m,0,c]}$ is satisfiable, if φ is a path formula and π_k is a (k,l) -loop.

Lemma ?? and ?? can be proven by structural induction on the length of φ . These proofs are omitted here for the limited space. Then, from the two Lemmas we immediately have Theorem ??, which guarantee the correctness of the translation.

Theorem 2. Let M be a model, φ be an $ECTL^*K$ formula, and k be a bound. Then, $M \models \varphi$ iff $[M^{\varphi, s_0}]_k \wedge [\varphi]_{M_k}$ is satisfiable, where $[\varphi]_{M_k} = [\varphi]_k^{[0,0,0]}$.

7 Conclusions

Formal verification methods in multi-agent systems have traditionally been associated with specifications. In this paper we present the BMC method for branching time logic of knowledge $ACTL^*K$ in synchronous multi-agent systems. We define synchronous

interpreted system semantics via revising epistemic accessibility relations of interpreted system semantics of [?] to synchronous ones. On the other hand, in order to obtain more expressive power in temporal dimension, we adopt $ACTL^*$ [?] as the underlying temporal logic and incorporate epistemic modalities to it. So, the resulting logic $ACTL^*K$ is different from $ACTLK$.

After construction of the model of a MAS, we can use the proposed BMC algorithm for $ACTL^*K$ to check (1) agents' knowledge about the dynamic world, (2) agents' knowledge about other agents' knowledge, (3) the temporal evolution of the above knowledge, and (4) any combination of (1), (2), and (3). For example, consider a typical synchronous multi-agent system, the well-known Muddy Children Puzzle with n children [?], the $ACTL^*K$ formula $AGC_{\Gamma}(\bigwedge_{i=1}^n (m_i \Rightarrow FK_i m_i))$ says that in any situation, all children have the common knowledge that the child whose forehead is muddy will eventually know his/her forehead has mud, where $m_i = true$ represents that child i 's forehead is muddy. Note that the subformula $\bigwedge_{i=1}^n (m_i \Rightarrow FK_i m_i)$ is a *path* subformula. Obviously, the $ACTL^*K$ formula cannot be expressed in $ACTLK$ [?]. In addition, if an $ACTL^*K$ ($ECTL^*K$) specification is $false(true)$, then we can get a counterexample (witness) of *minimal length*. This feature helps the users to analyze a MAS for faults more easily.

We are also keen to explore how to develop a security protocol verifier using our BMC method, which can automatically construct the synchronous temporal epistemic model of security protocols and check various security properties such as privacy, anonymity and nonrepudiation. In addition, in order to overcome the intrinsic limitation of BMC techniques, we will extend our BMC method to *Unbounded Model Checking* (UMC) [?] for the full CTL^*K language.

References

1. E.M. Clark, O., Peled, D.: Model Checking. The MIT Press, Cambridge, MA (2000)
2. Bordini, R.H., Fisher, M., Pardavila, C., Wooldridge, M.: Model checking agentspeak. In: Proceedings of the second international joint conference on Autonomous agents and multiagent systems, ACM Press (2003) 409–416
3. Halpern, J.Y., Vardi, M.Y.: Model checking vs. theorem proving: A manifesto. In: KR. (1991) 325–334
4. van der Hoek, W., Wooldridge, M.: Model checking knowledge and time. In: Proc. 19th Workshop on SPIN, Grenoble (2002)
5. van der Hoek, W., Wooldridge, M.: Tractable multiagent planning for epistemic goals. In: Proc. of the 1st Int. Conf. on Autonomous Agents and Multi-Agent Systems (AAMAS02). Volume III., ACM (2002) 1167–1174
6. van der Meyden, R., Su, K.: Symbolic model checking the knowledge of the dining cryptographers. In: Proc of 17th IEEE Computer Security Foundations Workshop. (2004) 280–291
7. Su, K.: Model checking temporal logics of knowledge in distributed systems. In McGuinness, D.L., Ferguson, G., eds.: AAI, AAI Press / The MIT Press (2004) 98–103
8. Biere, A., Cimatti, A., Clarke, E., Zhu, Y.: Symbolic model checking without BDDs. In: Proc. of TACAS99. Volume 1579 of LNCS., Springer-Verlag (1999) 193–207
9. Penczek, W., Woźna, B., Zbrzezny, A.: Bounded model checking for the universal fragment of CTL. Fundamenta Informaticae **51** (2002) 135–156

10. W.Penczek, A.Lomuscio: Verifying epistemic properties of multi-agent systems via bounded model checking. *Fundamenta Informaticae* **55** (2003)
11. Woźna, B.: ACTL* properties and Bounded Model Checking. *Fundamenta Informaticae* **63**(1) (2004) 65–87
12. Luo, X., Su, K., Sattar, A., Chen, Q., Lv, G.: Bounded model checking knowledge and branching time in synchronous multi-agent systems. In Dignum, F., Dignum, V., Koenig, S., Kraus, S., Singh, M.P., Wooldridge, M., eds.: *AAMAS, ACM* (2005) 1129–1130
13. Fagin, R., Halpern, J., Moses, Y., Vardi, M.: *Reasoning about knowledge*. MIT Press, Cambridge, MA (1995)
14. Kacprzak, M., Lomuscio, A., Penczek, W.: From bounded to unbounded model checking for temporal epistemic logic. *Fundamenta Informaticae* **62** (2004) 1–20