Completeness of bounded model checking temporal logic of knowledge

Liu Zhifeng[1, 2] Ge Yun[1] Zhang Dong[1] Zhou Conghua[2]

([1] School of Electronic Science and Engineering, Nanjing University, Nanjing 210093, China)
([2] School of Computer Science and Telecommunication Engineering, Jiangsu University, Zhenjiang 212013, China)

Abstract: In order to find the completeness threshold which offers a practical method of making bounded model checking complete, the over-approximation for the complete threshold is presented. First, a linear logic of knowledge is introduced into the past tense operator, and then a new temporal epistemic logic $\mathrm{LTL}_{\mathrm{P}}^{\mathrm{K}}$ is obtained, so that $\mathrm{LTL}_{\mathrm{P}}^{\mathrm{K}}$ can naturally and precisely describe the system's reliability. Secondly, a set of prior algorithms are designed to calculate the maximal reachable depth and the length of the longest of loop free paths in the structure based on the graph structure theory. Finally, some theorems are proposed to show how to approximate the complete threshold with the diameter and recurrence diameter. The proposed work resolves the completeness threshold problem so that the completeness of bounded model checking can be guaranteed.

Key words: bounded model checking; temporal logics of knowledge; multi-agent system

The automatic formal verification of reactive systems model checking[1] is a popular technique which predominantly focuses on system specification expressed in temporal logic-linear temporal logic in the case of SPIN[2–3] and FORSPEC[4] and branching temporal logic in the case of SMV[5] and its relatives. In 1991, Halpern et al. [6] proposed the use of model checking as an alternative to the deduction for logics of knowledge. Since then many researchers have focused on the model checking problem of multi-agent systems (MAS)[7–8]. In the model checking of the MAS, properties are expressed with temporal logics of knowledge, and interpreted systems are used to describe behaviors of the MAS. The state explosion problem is still the main problem in the model checking of the MAS.

Recently, the bounded model checking based on SAT has been introduced as a complementary technique to BDD-based symbolic model checking[5]. Since bounded model checking was introduced, much attention has been paid to the bounded model checking technique for temporal logics of knowledge[9–12]. Some researchers proposed many new temporal logics of knowledge such as CTLK, TECTLK, $\mathrm{CTL}^*\mathrm{K}$. In Ref. [9], authors proposed a temporal logic of knowledge CTLK which combines CTL[13] with knowledge modalities. And they presented that the framework of bounded model checking for ACTL[14] can be extended to the verification of ACTLK. Wozna et al. [11] proposed a new logic called TECTLK, which makes us reason about real time and knowledge in MAS. And they presented a bounded model checking method for TECTLK. Luo et al. [10] extended the temporal logic CTL^* by incorporating epistemic modalities and obtained the so-called temporal epistemic logic $\mathrm{CTL}^*\mathrm{K}$. It is shown that bounded model checking based on SAT is still applicable for the universal fragment of $\mathrm{CTL}^*\mathrm{K}$. Their work is mainly based on the combination of Ref. [15] and Ref. [9]. However, all the above researches did not discuss the complete threshold for bounded model checking of the MAS which is very important for bounded model checking. And their defined temporal logic of knowledge did not include past time which makes us describe many properties very compactly. Their researches show that bounded model checking based on SAT can overcome the state explosion problem efficiently in the model checking of the MAS.

In the bounded model checking of temporal logics of knowledge, in order to make the checking practical, we must find the number k (called the completeness threshold) given a finite system M and a property φ. If there is no counterexample to φ in M of length k or less, then M satisfies φ. However, up to now, to the best of our knowledge, there is no work about the completeness threshold. Therefore, in this paper, our main aim is to find the completeness threshold. Specifically, three contributions are made:

1) We propose a new temporal logic of knowledge called $\mathrm{LTL}_{\mathrm{P}}^{\mathrm{K}}$ which combines linear temporal logic LTL[16] with past operators and knowledge modalities. $\mathrm{LTL}_{\mathrm{P}}^{\mathrm{K}}$ makes us describe many properties more compactly and naturally.

2) We present a framework to the verification of $\mathrm{LTL}_{\mathrm{P}}^{\mathrm{K}}$ properties of the MAS via bounded model checking based on SAT. The SAT-based constraint solution makes very large systems for us.

3) We solve the very important completeness threshold problem[17] for bounded model checking of the MAS. The proposition of the completeness threshold makes bounded model checking complete. To the best of our knowledge, we are the first to discuss the completeness threshold problem.

1 Interpreted System Semantics

Interpreted systems are mainstream semantics for temporal logics of knowledge. We assume that the modeling system is composed of multiple agents, each of which is an independently operating process. Let Ag = {1, 2, …, n} denote the set of agents. We assume that each agent $i \in$ Ag can be any of a set L_i of local states. An agent's local state contains all the information required to completely characterize the state of the agent: the value of each of its local variables,

Received 2009-02-23.
Biographies: Liu Zhifeng (1981—), male, graduate; Zhou Conghua (corresponding author), male, doctor, associate professor, chzhou@ujs.edu.cn.
Foundation items: The National Natural Science Foundation of China (No. 10974093), the Scientific Research Foundation for Senior Personnel of Jiangsu University (No. 07JDG014), the Natural Science Foundation of Higher Education Institutions of Jiangsu Province (No. 08KJD520015).
Citation: Liu Zhifeng, Ge Yun, Zhang Dong, et al. Completeness of bounded model checking temporal logic of knowledge[J]. Journal of Southeast University (English Edition), 2010, 26(3): 399 – 405.

together with the value of its program counter. In particular, the information available to an agent is determined by its local state. The state of a system at any moment can be characterized by a tuple$(l_1, l_2, \ldots, l_n)$, where $l_i \in L_i$ is the local state of agent i at this moment. We let $G \subseteq L_1 \times \ldots \times L_n$ denote the global states of the system. Notice that we have not explicitly introduced environments. For simplicity, we assume that an environment can be modeled as an agent in the system.

Definition 1(models) Given a set of atomic propositions AP and a set of agents $\mathrm{Ag} = \{1, 2, \ldots, n\}$, a temporal knowledge model (simply a model) over AP and Ag is a pair $M = (K, L)$ with $K = (G, S, T, s_0, \sim_1, \ldots, \sim_n)$, where G is the finite set of the global states for the system (simply states); $T \subseteq G \times G$ is a total binary relation on G; S is a set of reachable global states from s_0, i. e., $S = \{s \in G \mid (s_0, s) \in T'\}$. T' denotes the transitive closure of T; $s_0 \in S$ is the initial state; $\sim_i \subseteq G \times G (i \in \mathrm{Ag})$ is a knowledge accessibility relation for each agent $i \in \mathrm{Ag}$ defined $s \sim_i s'$ iff $l_i(s') = l_i(s)$, where the function l_i: $G \to L_i$ returns the local state of agent i from a global state s; L: $G \to 2^{\mathrm{AP}}$ is a function which labels each state with a subset of the atomic propositions set AP.

It is obvious that in the system model M, the relation $\sim_i$ is an equivalence relation. Let $\Gamma \subseteq \mathrm{Ag}$. Given the knowledge relations for the agents in Γ, the union of Γ's accessibility relations defines the knowledge relation corresponding to the modality everybody knows: $\sim_\Gamma^{\mathrm{E}} = \bigcup_{i \in \Gamma} \sim_i$, $\sim_\Gamma^{\mathrm{C}}$ denotes the transitive closure of $\sim_\Gamma^{\mathrm{E}}$, and corresponds to the relation used to interpret the modality of common knowledge. The intersection of Γ's accessibility relations defines the knowledge relation corresponding to the modality of distributed knowledge: $\sim_\Gamma^{\mathrm{D}} = \bigcup_{i \in \Gamma} \sim_i$.

A path in system model M is an infinite sequence of states $\pi = s_0, s_1, \ldots$ such that $(s_i, s_{i+1}) \in T$ for each $i \geqslant 0$. For a path $\pi = s_0, s_1, \ldots$, let $\pi(k) = s_k$ and π^k denote the suffix of π starting from the k-th state.

Definition 2 A path π is a (k, l)-loop, with $l < k$, if $(\pi(k), \pi(l)) \in T$ and $\pi = uv^\omega$, where $u = \pi(0), \ldots, \pi(l-1)$ and $v = \pi(l), \ldots, \pi(k)$. We call π simply a k-loop if there is an integer l with $0 \leqslant l \leqslant k$ for which π is a (k, l)-loop.

2 $\mathrm{LTL}_\mathrm{P}^\mathrm{K}$: Linear Temporal Logic of Knowledge with Past

We use LTL as our basic temporal language and add an epistemic and past component to it. We call the resulting logic linear temporal logic of knowledge with past ($\mathrm{LTL}_\mathrm{P}^\mathrm{K}$). The introduction of past operators can be used to describe more natural formulation of the wide properties of MAS, compared with traditional pure future temporal logics.

Definition 3(syntax of $\mathrm{LTL}_\mathrm{P}^\mathrm{K}$) Let AP be a set of propositions and Ag be a set of agents. The set of $\mathrm{LTL}_\mathrm{P}^\mathrm{K}$ is defined as follows:

- If $p \in \mathrm{AP}$ then $p, \neg p$ are the $\mathrm{LTL}_\mathrm{P}^\mathrm{K}$ formulae;
- If f is an $\mathrm{LTL}_\mathrm{P}^\mathrm{K}$ formula, then Xf, Ff, Gf, Yf, Zf, Of, Hf are the $\mathrm{LTL}_\mathrm{P}^\mathrm{K}$ formulae;
- If f, g are $\mathrm{LTL}_\mathrm{P}^\mathrm{K}$ formulae then $f \vee g$, $f \wedge g$, $f \cup g$, fRg, fSg, fTg are $\mathrm{LTL}_\mathrm{P}^\mathrm{K}$ formulae;
- If f is an $\mathrm{LTL}_\mathrm{P}^\mathrm{K}$ formula then $\overline{K}_i f$, $\overline{D}_\Gamma f$, $\overline{E}_\Gamma f$, $\overline{C}_\Gamma f$ are $\mathrm{LTL}_\mathrm{P}^\mathrm{K}$ formulae, where $\Gamma \subseteq \mathrm{Ag}$.

Definition 4(unbounded semantics) Let AP be a set of propositions, Ag be a set of agents, M be a system model over AP and Ag, π be a path in M starting from the initial state s_0 of M, and f be an $\mathrm{LTL}_\mathrm{P}^\mathrm{K}$ formula. We define $\pi \vDash f$ iff $\pi^0 \vDash f$, where

- $\pi^i \vDash p \Leftrightarrow p \in L(s_i)$ for $p \in \mathrm{AP}$; $\pi^i \vDash f \vee g \Leftrightarrow \pi^i \vDash$ for $\pi^i \vDash g$;
- $\pi^i \vDash f \wedge g \Leftrightarrow \pi^i \vDash f$ and $\pi^i \vDash g$; $\pi^i \vDash Xf \Leftrightarrow \pi^{i+1} \vDash f$;
- $\pi^i \vDash Gf \Leftrightarrow \forall n \geqslant i, \pi^n \vDash f$;
- $\pi^i \vDash f \cup g \Leftrightarrow \exists n \geqslant i$ such that $\pi^n \vDash g$ and $\pi^j \vDash f$ for all $i \leqslant j < n$;
- $\pi^i \vDash fRg \Leftrightarrow \exists n \geqslant i, \pi^n \vDash g$ or $\pi^j \vDash f$ for some $i \leqslant j < n$;
- $\pi^i \vDash Yf \Leftrightarrow i > 0$ and $\pi^{i-1} \vDash f$; $\pi^i \vDash Zf \Leftrightarrow i = 0$ or $\pi^{i-1} \vDash f$;
- $\pi^i \vDash Of \Leftrightarrow \pi^j \vDash f$ for some $0 \leqslant j \leqslant i$; $\pi^i \vDash Hf \Leftrightarrow \pi^j \vDash f$ for all $0 \leqslant j \leqslant i$;
- $\pi^i \vDash fSg \Leftrightarrow \pi^j \vDash g$ for some $0 \leqslant j \leqslant i$ and $\pi^n \vDash f$ for all $j < n \leqslant i$;
- $\pi^i \vDash fTg \Leftrightarrow$for all $0 \leqslant j \leqslant i$: $\pi^j \vDash g$ or $\pi^n \vDash f$ for some $j < n \leqslant i$;
- $\pi^i \vDash \overline{K}_j f \Leftrightarrow$there is a path π' starting from s_0 and a natural number $n \geqslant 0$ such that $\pi(i) \sim_j \pi'(n)$ and $\pi'^n \vDash f$;
- $\pi^i \vDash \overline{D}_\Gamma f \Leftrightarrow$there is a path π' starting from s_0 and a natural number $n \geqslant 0$ such that $\pi(i) \sim_\Gamma^{\mathrm{D}} \pi'(n)$ and $\pi'^n \vDash f$;
- $\pi^i \vDash \overline{E}_\Gamma f \Leftrightarrow$there is a path π' starting from s_0 and a natural number $n \geqslant 0$ such that $\pi(i) \sim_\Gamma^{\mathrm{E}} \pi'(n)$ and $\pi'^n \vDash f$;
- $\pi^i \vDash \overline{C}_\Gamma f \Leftrightarrow$there is a path π' starting from s_0 and a natural number $n \geqslant 0$ such that $\pi(i) \sim_\Gamma^{\mathrm{C}} \pi'(n)$ and $\pi'^n \vDash f$.

We call f is existentially valid in a model M(in symbols $M \vDash Ef$) if and only if there exists a path π in M starting from the initial state such that $\pi \vDash f$.

3 Bounded Model Checking for $\mathrm{LTL}_\mathrm{P}^\mathrm{K}$

Bounded model checking based on SAT methods has been introduced as a complementary technique to BDD-based symbolic model checking. The main idea of bounded model checking is to search for an execution of the system of some length k, which constitutes a counterexample for a verified property. To perform bounded model checking on $\mathrm{LTL}_\mathrm{P}^\mathrm{K}$, we first define a bounded semantics for $\mathrm{LTL}_\mathrm{P}^\mathrm{K}$, which is an approximation to the unbounded semantics. Secondly, we reduce bounded model checking to propositional satisfiability. Thirdly, we discuss the completeness threshold for bounded model checking on $\mathrm{LTL}_\mathrm{P}^\mathrm{K}$.

3.1 Bounded semantics for $\mathrm{LTL}_\mathrm{P}^\mathrm{K}$

In bounded model checking, a crucial observation is that the prefix of a path is finite. It still might represent an infinite path if there is a back loop from the last state of the prefix to any of the previous states. If there is no such back loop, then the prefix does not mean anything about the infinite behavior of the path. Thus when we define bounded semantics for $\mathrm{LTL}_\mathrm{P}^\mathrm{K}$, we must consider whether a finite path represents an infinite behavior.

Definition 5(bounded semantics for a loop) Let π be a

k-loop path. Then an LTL$_{\mathrm{P}}^{\mathrm{K}}$ formula f is valid along π with bound k(in symbols $\pi \models_k f$) iff $\pi \models f$.

Definition 6(bounded semantics for a loop) Let π be a path that is not k-loop. Then an LTL$_{\mathrm{P}}^{\mathrm{K}}$ formula f is valid along π with bound k(in symbols $\pi \models_k f$) iff $\pi \models_k^0 f$, where

- $\pi \models_k^i p$ iff $p \in L(\pi(i))$; $\pi \models_k^i \neg p$ iff $p \notin L(\pi(i))$;
- $\pi \models_k^i f \wedge g$ iff $\pi \models_k^i f$ and $\pi \models_k^i g$; $\pi \models_k^i f \vee g$ iff $\pi \models_k^i$ for $\pi \models_k^i g$;
- $\pi \models_k^i Gf$ is always false. $\pi \models_k^i Ff$ iff $\exists j, i \leqslant j \leqslant k, \pi \models_k^j f$;
- $\pi \models_k^i Xf$ iff $i \leqslant k$ and $\pi \models_k^{i+1} f$;
- $\pi \models_k^i fUg$ iff $\exists j, i \leqslant j \leqslant k[\pi \models_k^j g$ and $\forall n, i \leqslant n < j, \pi \models_k^n f]$;
- $\pi \models_k^i fRg$ iff $\exists j, i \leqslant j \leqslant k[\pi \models_k^j f$ and $\forall n, i \leqslant n \leqslant j, \pi \models_k^n g]$;
- $\pi \models_k^i Yf$ iff $i > 0$ and $\pi \models_k^{i-1} f$; $\pi \models_k^i Zf$ iff $i = 0$ or $\pi \models_k^{i-1} f$;
- $\pi \models_k^i Hf$ iff f or all $0 \leqslant j \leqslant \mathrm{i}$, $\pi \models_k^i f$;
- $\pi \models_k^i f\, Sg$ iff $\pi \models_k^j g$ for some $0 \leqslant j \leqslant i$ and $\pi \models_k^n f$ for all $j < n \leqslant i$;
- $\pi \models_k^i f\, Tg$ iff $\forall j \in [0, i]: \pi \models_k^j g$ or $\pi \models_k^n f$ for some $j < n \leqslant i$;
- $\pi \models_k^i \overline{K}_j f$ iff there is a path π'starting from s_0 and exists $0 \leqslant n \leqslant k$ such that $\pi(i) \sim_i \pi'(n)$ and $\pi' \models_k^n f$;
- $\pi \models_k^i \overline{D}_\Gamma f$ iff there is a path π' starting from s_0 and exists $0 \leqslant n \leqslant k$ such that $\pi(i) \sim_\Gamma^{\mathrm{D}} \pi'(n)$ and $\pi' \models_k^n f$;
- $\pi \models_k^i \overline{E}_\Gamma f$ iff there is a path π' starting from s_0 and exists $0 \leqslant n \leqslant k$ such that $\pi(i) \sim_\Gamma^{\mathrm{E}} \pi'(n)$ and $\pi' \models_k^n f$;
- $\pi \models_k^i \overline{C}_\Gamma f$ iff there is a path π' starting from s_0 and exists $0 \leqslant n \leqslant k$ such that $(\pi(i), \pi'(n)) \in (\overline{E}_\Gamma)^k$ and $\pi' \models_k^n f$.

f is said to be bounded existentially valid in a model M with the bound k(in symbols $M \models_k Ef$) if and only if there exists a path π in M starting from the initial state such that $\pi \models_k f$. Now we describe how the existential model checking problem ($M \models Ef$) can be reduced to a bounded existential model checking problem.

Theorem 1 Let AP be a set of propositions, Ag be a set of agents, and M a system model over AP and Ag. And let π be a path in M starting from the initial state s_0 of M, and f an LTL$_{\mathrm{P}}^{\mathrm{K}}$ formula, and k be a bound. Then $\pi \models_k f$ implies that $\pi \models f$.

Theorem 2 Let AP be a set of propositions, Ag be a set of agents, and M be a system model over AP and Ag. Then $M \models Ef$ implies that there exists a bound $k \leqslant |M| \times 2^{|f|}$ such that $M \models_k Ef$.

Theorems 1 and 2 can be proved by induction on the length of the LTL$_{\mathrm{P}}^{\mathrm{K}}$ formula. Limited by space, we omit the proofs.

3.2 Translation

In the previous sections, the semantics is defined for bounded model checking on LTL$_{\mathrm{P}}^{\mathrm{K}}$. We now reduce bounded model checking to propositional satisfiability. This reduction enables us to use efficient propositional decision procedures to perform model checking.

Definition 7(unfolding transition relation) For two integers k and n, we define Path$_n^k$: $= I(\pi_n(0)) \wedge \bigwedge_{i=0}^{k-1} T(\pi_n(i), \pi_n(i+1))$, where if $I(\pi_n(0))$ is true then $\pi_n(0)$ is the initial state.

Definition 8(loop condition) For two integers k, l with $k \geqslant l \geqslant 0$ and the path π_i, let ${}_lL_K^{\pi_i}$: $= T(\pi_i(k), \pi_i(l))$. We notice that if Path$_n^k$ is satisfiable then the state sequence $\pi_n(0)$, …, $\pi_n(k)$ is a finite path. And if ${}_lL_K^{\pi_i}$ is satisfiable then there is a loop from $\pi_i(k)$ to $\pi_i(l)$. For temporal operators, our translation method is the same as Ref. [18]. For knowledge modalities, such as $\overline{K}_i f$, what we want is to construct a new finite path π_{n+1} starting from the initial state such that f is valid along π_{n+1} where n is a global variable used to compute the number of new finite paths. Initially $n = 0$.

Definition 9 (translation of an LTL$_{\mathrm{P}}^{\mathrm{K}}$ formula without a loop)

- $[p]_k^{i,m}$: $= p \in L(\pi_m(i))$, $[f \wedge g]_k^{i,m}$: $= [f]_k^{i,m} \wedge [g]_k^{i,m}$;
- $[\neg p]_k^{i,m}$: $= p \notin L(\pi_m(i))$, $[f \vee g]_k^{i,m}$: $= [f]_k^{i,m} \vee [g]_k^{i,m}$;
- $[Xf]_k^{i,m}$: $=$ if $i < k$ then $[f]_k^{i+1,m}$ else false;
- $[Ff]_k^{i,m}$: $= \bigvee_{j=\mathrm{i}}^{k} [f]_k^{j,m}$, $[Gf]_k^{i,m}$: $=$ false;
- $[fUg]_k^{i,m}$: $= \bigvee_{j=\mathrm{i}}^{k} ([g]_k^{j,m} \wedge \bigwedge_{h=\mathrm{i}}^{j-1} [f]_k^{h,m})$, $[fRg]_k^{i,m}$: $= \bigwedge_{j=\mathrm{i}}^{k} ([g]_k^{j,m} \vee \bigvee_{h=\mathrm{i}}^{j-1} [f]_k^{h,m})$;
- $[Yf]_k^{i,m}$: $=$ if $i > 0$ then $[f]_k^{i-1,m}$ else false;
- $[Zf]_k^{i,m}$: $=$ if $i > 0$ then $[f]_k^{i-1,m}$ else true;
- $[Of]_k^{i,m}$: $= \bigvee_{j=0}^{i} [f]_k^{j,m}$, $[Hf]_k^{i,m}$: $= \bigwedge_{j=0}^{i} [f]_k^{j,m}$;
- $[fSg]_k^{i,m}$: $= \bigvee_{j=0}^{i} ([g]_k^{j,m} \wedge \bigwedge_{h=j+1}^{i} [f]_k^{h,m})$, $[fTg]_k^{i,m}$: $= \bigwedge_{j=0}^{i} ([g]_k^{j,m} \vee \bigvee_{h=j+1}^{i} [f]_k^{h,m})$;
- $[\overline{K}_\omega f]_k^{i,m}$: $=$ Path$_{n+1}^k \wedge (\bigvee_{j=0}^{k} (l_\omega(\pi_m(i)) = l_\omega(\pi_{n+1}(j)) \wedge ([f]_k^{j,n+1} \vee \bigvee_{l=0}^{k} ({}_lL_k^{\pi_{n+1}} \wedge {}_l[f]_k^{j,n+1}))))$, and let $n = n+1$;
- $[\overline{D}_\Gamma f]_k^{i,m}$: $=$ Path$_{n+1}^k \wedge (\bigvee_{j=0}^{k} (\bigwedge_{\omega \in \Gamma} l_\omega(\pi_m(i)) = l_\omega(\pi_{n+1}(j)) \wedge ([f]_k^{j,n+1} \vee \bigvee_{l=0}^{k} ({}_lL_k^{\pi_{n+1}} \wedge {}_l[f]_k^{j,n+1}))))$, and let $n = n+1$;
- $[\overline{E}_\Gamma f]_k^{i,m}$: $=$ Path$_{n+1}^k \wedge (\bigvee_{j=0}^{k} (\bigvee_{\omega \in \Gamma} l_\omega(\pi_m(i)) = l_\omega(\pi_{n+1}(j)) \wedge ([f]_k^{j,n+1} \vee \bigvee_{1=0}^{k} ({}_lL_k^{\pi_{n+1}} \wedge {}_l[f]_k^{j,n+1}))))$, and let $n = n+1$;
- $[\overline{C}_\Gamma f]_k^{i,m}$: $=$ Path$_{n+1}^k \wedge (\bigvee_{j=0}^{k} (\bigwedge_{v=1}^{k} (\pi_{n+1}(k+v), \pi_{n+1}(k+v+1)) \in \overline{E}_\Gamma \wedge \bigvee_{v=1}^{k} (\pi_{n+1}(k+v) = \pi_m(i)) \wedge \bigvee_{v=1}^{k} (\pi_{n+1}(k+v) = (\pi_{n+1}(j)) \wedge ([f]_k^{j,n+1} \vee \bigvee_{l=0}^{k} ({}_lL_k^{\pi_{n+1}} \wedge {}_l[f]_k^{j,n+1}))))$, and let $n = n+1$.

Definition 10 (translation of an LTL$_{\mathrm{P}}^{\mathrm{K}}$ formula f on a (k, l)-loop)

- ${}_l[p]_k^{i,m}$: $= p \in L(\pi_m(i))$, ${}_l[f \wedge g]_k^{i,m}$: $= {}_l[f]_k^{i,m} \wedge {}_l[g]_k^{i,m}$;
- ${}_l[\neg p]_k^{i,m}$: $= p \notin L(\pi_m(i))$, ${}_l[f \vee g]_k^{i,m}$: $= {}_l[f]_k^{i,m} \vee {}_l[g]_k^{i,m}$;
- ${}_l[Xf]_k^{i,m}$: $=$ if $i < k$ then $[f]_k^{i+1,m}$ else $[Xf]_k^{l,m}$;
- ${}_l[Ff]_k^{i,m}$: $= \bigvee_{j=\min(i,l)}^{k} {}_l[f]_k^{j,m}$, ${}_l[Gf]_k^{i,m}$: $= \bigwedge_{j=\min(i,l)}^{k} {}_l[f]_k^{j,m}$;
- ${}_l[fUg]_k^{i,m}$: $= \bigvee_{j=i}^{k} ({}_l[g]_k^{j,m} \wedge \bigwedge_{h=i}^{j-1} [f]_k^{h,m}) \vee \bigvee_{j=l}^{i-1} ({}_l[g]_k^{j,m} \wedge \bigwedge_{h=i}^{k} {}_l[f]_k^{h,m} \wedge \bigwedge_{h=l}^{j-1} {}_l[f]_k^{h,m})$;

- ${}_l[fRg]_k^{i,m} := \bigwedge_{j=\min(i,l)}^{k} {}_l[g]_k^{j,m} \vee \bigvee_{j=i}^{k} ({}_l[f]_k^{j,m} \wedge \bigwedge_{h=i}^{j} {}_l[g]_k^{h,m} \vee \bigvee_{j=l}^{i-1} ({}_l[f]_k^{j,m} \wedge \bigwedge_{h=i}^{k} {}_l[g]_k^{h,m} \wedge \bigwedge_{h=l}^{j} {}_l[g]_k^{h,m})$;
- ${}_l[Yf]_k^{i,m} :=$ if $i > 0$ then ${}_l[f]_k^{i-1,m}$ else false;
- ${}_l[Zf]_k^{i,m} :=$ if $i > 0$ then ${}_l[f]_k^{i-1,m}$ else true;
- ${}_l[Of]_k^{i,m} := \bigvee_{j=0}^{i} {}_l[f]_k^{j,m}$, ${}_l[Hf]_k^{i,m} := \bigwedge_{j=0}^{i} {}_l[f]_k^{j,m}$;
- ${}_l[fSg]_k^{i,m} := \bigvee_{j=0}^{i} ({}_l[g]_k^{j,m} \wedge \bigwedge_{h=j+1}^{i} {}_l[f]_k^{h,m})$, ${}_l[fTg]_k^{i,m} := \bigwedge_{j=0}^{i} ({}_l[g]_k^{j,m} \vee \bigvee_{h=j+1}^{i} {}_l[f]_k^{h,m})$;
- ${}_l[\overline{K}_\omega f]_k^{i,m} := \mathrm{Path}_{n+1}^{k} \wedge (\bigvee_{j=0}^{k} (l_\omega(\pi_m(i)) = l_\omega(\pi_{n+1}(j)) \wedge ([f]_k^{j,n+1} \vee \bigvee_{l=0}^{k} ({}_lL_k^{\pi_{n+1}} \wedge {}_l[f]_k^{j,n+1}))))$, and let $n = n+1$;
- ${}_l[\overline{D}_\Gamma f]_k^{i,m} := \mathrm{Path}_{n+1}^{k} \wedge (\bigvee_{j=0}^{k} (\bigwedge_{\omega\in\Gamma} l_\omega(\pi_m(i)) = l_\omega(\pi_{n+1}(j)) \wedge ([f]_k^{j,n+1} \vee \bigvee_{l=0}^{k} ({}_lL_k^{\pi_{n+1}} \wedge {}_l[f]_k^{j,n+1}))))$, and let $n = n+1$;
- ${}_l[\overline{E}_\Gamma f]_k^{i,m} := \mathrm{Path}_{n+1}^{k} \wedge (\bigvee_{j=0}^{k} (\bigvee_{\omega\in\Gamma} l_\omega(\pi_m(i)) = l_\omega(\pi_{n+1}(j)) \wedge ([f]_k^{j,n+1} \vee \bigvee_{l=0}^{k} ({}_lL_k^{\pi_{n+1}} \wedge {}_l[f]_k^{j,n+1}))))$, and let $n = n+1$;
- ${}_l[\overline{C}_\Gamma f]_k^{i,m} := \mathrm{Path}_{n+1}^{k} \wedge (\bigvee_{j=0}^{k} (\bigwedge_{v=1}^{k} (\pi_{n+1}(k+v), \pi_{n+1}(k+v+1)) \in \overline{E_\Gamma} \wedge \bigvee_{v=1}^{k} (\pi_{n+1}(k+v) = \pi_m(i)) \wedge \bigvee_{v=1}^{k} (\pi_{n+1}(k+v) = (\pi_{n+1}(j)) \wedge ([f]_k^{j,n+1} \vee \bigvee_{l=0}^{k} ({}_lL_k^{\pi_{n+1}} \wedge {}_l[f]_k^{j,n+1}))))$, and let $n = n+1$.

Definition 11 (general translation) Let AP be a set of propositions, Ag a set of agents, M a system model over AP and Ag, f an $\mathrm{LTL}_\mathrm{P}^\mathrm{K}$ formula, and k a bound.

$$[M,f]_k := I(\pi_0(0)) \wedge \bigwedge_{i=0}^{k-1} T(\pi_0(i), (\pi_0(i+1)) \wedge ([f]_k^{0,0} \vee \bigvee_{l=0}^{k} ({}_lL_k^{\pi_0} \wedge {}_l[f]_k^{0,0}))$$

Theorem 3 Let AP be a set of propositions, Ag be a set of agents, M a system model over AP and Ag, f an $\mathrm{LTL}_\mathrm{P}^\mathrm{K}$ formula, and k a bound. Then $[M,f]_k$ is satisfiable if and only if $M \vDash_k Ef$.

Corollary 1 Let AP be a set of propositions, Ag a set of agents, M a system model over AP and Ag, f an $\mathrm{LTL}_\mathrm{P}^\mathrm{K}$ formula. $M \vDash Ef$ if and only if there exists an integer $k \leqslant |M| \times 2^{|f|}$ such that $[M,f]_k$ is satisfiable.

Theorem 3 and corollary 1 can be proved by induction on the length of the $\mathrm{LTL}_\mathrm{P}^\mathrm{K}$ formula. Limited by space, we omit the proofs.

3.3 Determining completeness threshold

It has been shown that the unbounded semantics is equivalent to the bounded semantics if we take all the possible bounds into account. This equivalence leads to a straightforward $\mathrm{LTL}_\mathrm{P}^\mathrm{K}$ model checking procedure. To check whether $M \vDash Ef$, the procedure checks $M \vDash_k Ef$ for $k = 0, 1, 2, \ldots$. If $M \vDash_k Ef$, then the procedure proves that $M \vDash Ef$ and produces a witness of length k. If $M \nvDash_k Ef$, we have to increase the value of k indefinitely, and the procedure does not terminate. In this section, we establish several bounds on k which we call completeness thresholds of f in M. If $M \nvDash_k Ef$ for all k within the bound, we conclude that $M \nvDash_k Ef$.

Definition 12 (diameter) The diameter of a model M, denoted by $d(M)$, is the longest shortest path between any two reachable states. $d^\mathrm{I}(M)$ is the longest shortest path between the initial state and any reachable states.

Definition 13[14] (recurrence diameter) The recurrence diameter of a model M, denoted by $\mathrm{rd}(M)$, is the longest loop-free path between any two reachable states. $\mathrm{rd}^\mathrm{I}(M)$ is the longest loop-free path between the initial state and any reachable state, where a finite path is loop-free if and only if there are not two same states in the path.

Notice that there exist the relationships of $d^\mathrm{I}(M) \leqslant d(M) \leqslant \mathrm{rd}(M)$ and $d^\mathrm{I}(M) \leqslant \mathrm{rd}^\mathrm{I}(M) \leqslant \mathrm{rd}(M)$ in the model M. For example, Fig. 1 is a simple model M, where $d(M) = 2$, $d^\mathrm{I}(M) = 1$, $\mathrm{rd}(M) = 3$, $\mathrm{rd}^\mathrm{I}(M) = 3$.

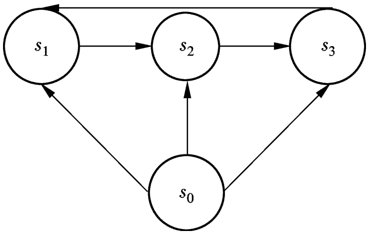

Fig. 1 A simple model M

Lemma 1[19] Given an LTL formula Fp, where p is an atomic proposition, and a system model M, $M \vDash Ef$ if there exists $k \leqslant d^\mathrm{I}(M)$ with $M \vDash_k Ef$.

We notice that since reachability can be reduced to an LTL formula Fp, one of completeness thresholds for reachability analysis is $d^\mathrm{I}(M)$.

Lemma 2[19] Given an LTL formula Gp, where p is an atomic proposition, and a system model M, $M \vDash Ef$ iff there exists $k \leqslant \mathrm{rd}^\mathrm{I}(M)$ with $M \vDash_k Ef$.

For the convenience of proofs, we define $\pi^j \vDash \sim_i s$ iff $\pi(j) \sim_i s$, $\pi^j \vDash \sim_\Gamma^\mathrm{C} s$ iff $\pi(j) \sim_\Gamma^\mathrm{C} s$.

Theorem 4 Let M be a system model. For the $\mathrm{LTL}_\mathrm{P}^\mathrm{K}$ property $f = \overline{K}_i p, \overline{E}_\Gamma p, \overline{D}_\Gamma p$, where p is an atomic proposition, if $M \vDash Ef$ then there exists an integer k with $k \leqslant d^\mathrm{I}(M)$ such that $M \vDash_k Ef$.

Proof Without loss of generality, we only consider $f = \overline{K}_i p$. By the definition of unbounded semantics of $\mathrm{LTL}_\mathrm{P}^\mathrm{K}$, $M \vDash Ef$ means there is a path π starting from s_0 such that $\pi \vDash F(p \wedge \sim_i s_0)$. By lemma 1, there is an integer k with $k \leqslant d^\mathrm{I}(M)$ such that $\pi \vDash_k F(p \wedge \sim_i s_0)$, that is $M \vDash_k Ef$.

Since $\pi \vDash OFp \Leftrightarrow \pi \vDash fp$, $\pi \vDash O\overline{K}_i p \Leftrightarrow \pi \vDash \overline{K}_i p$, $\pi \vDash O\overline{E}_\Gamma p \Leftrightarrow \pi \vDash \overline{E}_\Gamma p$, $\pi \vDash O\overline{D}_\Gamma p \Leftrightarrow \pi \vDash \overline{D}_\Gamma p$, the following corollary is clear.

Corollary 2 Let M be a system model. For the $\mathrm{LTL}_\mathrm{P}^\mathrm{K}$ property $f = OFp$, $O\overline{K}_i p$, $O\overline{E}_\Gamma p$, $O\overline{D}_\Gamma p$, where p is an atomic proposition, if $M \vDash Ef$ then there exists an integer k with $k \leqslant d^\mathrm{I}(M)$ such that $M \vDash_k Ef$.

Lemma 3 Given a system model M, $(s_0, s) \in \overline{C}_\Gamma$ if and only if there exists k with $k \leqslant |M|$ such that $(s_0, s) \in (\overline{E}_\Gamma)^k$, where $|M|$ is the number of states in M.

Proof It is obvious from right to left. We assume that there is an integer v with $v > |M|$, such that $(s_0, s) \in (\overline{E}_\Gamma)^v$, that is there is a state sequence $s_1, s_2 \ldots, s_{v-1}$ such that for all $0 \leqslant i \leqslant v-1$, $(s_i, s_{i+1}) \in \overline{E}_\Gamma$ (let $s = s_v$). Since $v > |M|$, there must exist two integers i, j with $0 \leqslant i < j \leqslant v$

such that $s_i = s_j$. Therefore, $(s_0, s) \in (\overline{E}_\Gamma)^{v-j+i}$. Then if $v-j+i > |M|$, we can continue as above until there is an integer $v' \leqslant |M|$ such that $(s_0, s) \in (\overline{E}_\Gamma)^{v'}$.

Theorem 5 Let M be a system model. For the LTL$^{\mathrm{K}}_{\mathrm{P}}$ property $f = \overline{C}_\Gamma p$, where p is an atomic proposition, if $M \models Ef$ then there exists an integer k with $k \leqslant |M|$ such that $M \models_k Ef$.

Proof By the definition of unbounded semantics of LTL$^{\mathrm{K}}_{\mathrm{P}}$, $M \models Ef$ means that there is a path π starting from s_0 such that $\pi \models F(p \wedge \sim^{\mathrm{C}}_{\Gamma} s_0)$. Again by the definition of unbounded semantics of LTL$^{\mathrm{K}}_{\mathrm{P}}$ and lemma 1, there is an integer j with $j \leqslant d^{\mathrm{I}}(M)$ such that $p \in L(\pi(j))$ and $\pi(j) \sim^{\mathrm{C}}_{\Gamma} s_0$. By lemma 2, there exists an integer k with $k \leqslant |M|$ such that $(s_0, s) \in (\overline{E}_\Gamma)^k$. Therefore, by the definition of bounded semantics of LTL$^{\mathrm{K}}_{\mathrm{P}}$, there exists an integer k with $k \leqslant |M|$ such that $M \models_k Ef$.

Corollary 3 Let M be a system model. For the LTL$^{\mathrm{K}}_{\mathrm{P}}$ property $f = O\overline{C}_\Gamma p$, where p is an atomic proposition, if $M \models Ef$ then there exists an integer k with $k \leqslant |M|$ such that $M \models_k Ef$. Since $\pi \models O\overline{C}_\Gamma p$ if and only if $\pi \models \overline{C}_\Gamma p$, corollary 4 is clear.

Theorem 6 Let M be a system model. For the LTL$^{\mathrm{K}}_{\mathrm{P}}$ property $f = F\overline{K}_i p$, $F\overline{E}_\Gamma p$, $F\overline{D}_\Gamma p$, where p is an atomic proposition, if $M \models Ef$ then there exists an integer k with $k \leqslant d^{\mathrm{I}}(M)$ such that $M \models_k Ef$.

Proof Without loss of generality, we only consider $f = F\overline{K}_i p$. By the definition of unbounded semantics of LTL$^{\mathrm{K}}_{\mathrm{P}}$, there are two states s, s' which are reachable from s_0 such that $s \sim_i s'$ and $p \in L(s')$. By lemma 1, s, s' are reachable from s_0 in $d^{\mathrm{I}}(M)$ steps. Therefore, there exists an integer k with $k \leqslant d^{\mathrm{I}}(M)$ such that $M \models_k EF\overline{K}_i p$.

Theorem 7 Let M be a system model. For the LTL$^{\mathrm{K}}_{\mathrm{P}}$ property $f = \overline{K}_i Fp$, $\overline{E}_\Gamma Fp$, $\overline{D}_\Gamma Fp$, where p is an atomic proposition, if $M \models Ef$ then there exists an integer k with $k \leqslant d(M)$ such that $M \models_k Ef$.

Proof Without loss of generality, we only consider $f = \overline{K}_i Fp$. By the definition of unbounded semantics of LTL$^{\mathrm{K}}_{\mathrm{P}}$, there are two states s, s'such that s is reachable from s_0, and $s'$is reachable from s, $s \sim_i s_0$ and $p \in L(s')$. By lemma 1, s is reachable from s_0 in $d^{\mathrm{I}}(M)$ steps, s' is reachable from s in $d(M)$ steps. Therefore there exists an integer k with $k \leqslant d(M)$ such that $M \models_k E\overline{K}_i Fp$.

Theorem 8 Let M be a system model. For the LTL$^{\mathrm{K}}_{\mathrm{P}}$ property $f = \overline{K}_i Op$, $\overline{E}_\Gamma Op$, $\overline{D}_\Gamma Op$, where p is an atomic proposition, if $M \models Ef$ then there exists an integer k with $k \leqslant d(M) + d^{\mathrm{I}}(M)$ such that $M \models_k Ef$.

Proof Without loss of generality, we only consider $f = \overline{K}_i Op$. By the definition of unbounded semantics of LTL$^{\mathrm{K}}_{\mathrm{P}}$, there are two states s, s' such that $s'$is reachable from s_0, and s is reachable from s', $p \in L(s')$, and $s_0 \sim_i s$. By lemma 1, s' is reachable from s_0 in $d^{\mathrm{I}}(M)$ steps, and s is reachable from s' in $d(M)$ steps. Therefore, there exists an integer k with $k \leqslant d(M) + d^{\mathrm{I}}(M)$ such that $M \models_k E\overline{K}_i Op$.

Theorem 9 Let M be a system model. For the LTL$^{\mathrm{K}}_{\mathrm{P}}$ property $f = G\overline{K}_i p$, $G\overline{E}_\Gamma p$, $G\overline{D}_\Gamma p$, where p is an atomic proposition, $M \models Ef$ if and only if there exists an integer k with $k \leqslant \mathrm{rd}^{\mathrm{I}}(M)$ such that $M \models_k Ef$.

Proof Without loss of generality, we only consider $f = G\overline{K}_i p$. By lemma 2, there is a k-loop path π with $k \leqslant \mathrm{rd}^{\mathrm{I}}(M)$ such that for each $j \leqslant k$, $\pi^j \models \overline{K}_i p$. For each $j \leqslant k$, By the unbounded semantics of $\pi^j \models \overline{K}_i p$, there is a state s reachable from s_0 such that $s \sim_i \pi(j)$ and $p \in L(s)$. By lemma 1, s is reachable from s_0 in $\mathrm{d}^{\mathrm{I}}(M)$ steps. Therefore, there exists an integer k with $k \leqslant \mathrm{rd}^{\mathrm{I}}(M)$ such that $M \models_k EG\overline{K}_i p$.

Theorem 10 Let M be a system model. For the LTL$^{\mathrm{K}}_{\mathrm{P}}$ property $f = \overline{K}_i Gp$, $\overline{E}_\Gamma Gp$, $\overline{D}_\Gamma Gp$, where p is an atomic proposition, if $M \models Ef$ then there exists an integer k with $k \leqslant \mathrm{rd}(M)$ such that $M \models_k Ef$.

Proof Without loss of generality, we only consider $f = \overline{K}_i Gp$. By the unbounded semantics of $\overline{K}_i Gp$, there is a state s reachable from s_0 such that there is an infinite path π starting from s with $\pi \models Gp$. By lemmas 1 and 2, s is reachable from s_0 in $\mathrm{d}^{\mathrm{I}}(M)$ steps and there is a k-loop path π with $k \leqslant \mathrm{rd}(M)$ such that $\pi \models Gp$. Therefore, there exists an integer k with $k \leqslant \mathrm{rd}(M)$ such is $M \models_k E\overline{K}_i Gp$.

Theorem 11 Let M be a system model. For the LTL$^{\mathrm{K}}_{\mathrm{P}}$ property $f = \overline{K}_i Hp$, $\overline{E}_\Gamma Hp$, $\overline{D}_\Gamma Hp$, where p is an atomic proposition, $M \models Ef$ if and only if there exists an integer k with $k \leqslant \mathrm{rd}^{\mathrm{I}}(M)$ such that $M \models_k Ef$.

Proof Without loss of generality, we only consider $f = \overline{K}_i Hp$. By the unbounded semantics of $\overline{K}_i Hp$, there is a state s reachable from s_0 in $d^{\mathrm{I}}(M)$ steps and between s and s_0, and there is a finite path π_k such that for each $0 \leqslant j \leqslant k$, $p \in L(\pi_k(j))$. By the definition of $\mathrm{rd}^{\mathrm{I}}(M)$, if $k > \mathrm{rd}^{\mathrm{I}}(M)$ there exists two integers m, n with $m < n \leqslant k$ such that $\pi_k(m) = \pi_k(n)$. Thus we can construct a new finite path $\pi'_{k+m-n} = \pi_k(0), \ldots, \pi_k(m), \pi_k(n+1), \ldots, \pi_k(k)$ such that for each $j \leqslant k+m-n$, $p \in L(\pi'_{k+m-n}(j))$. If $k+m-n > \mathrm{rd}^{\mathrm{I}}(M)$, we continue as above until we obtain a finite path π_x'' such that $x \leqslant \mathrm{rd}^{\mathrm{I}}(M)$ and for each $j \leqslant x$, $p \in L(\pi_x''(j))$. Therefore, there exists an integer k with $k \leqslant \mathrm{rd}^{\mathrm{I}}(M)$ such that $M \models_k E\overline{K}_i Hp$.

Theorem 12 Let M be a system model. For the LTL$^{\mathrm{K}}_{\mathrm{P}}$ property $f = F\overline{C}_\Gamma p$, $\overline{C}_\Gamma Fp$, $G\overline{C}_\Gamma p$, $\overline{C}_\Gamma Gp$, $\overline{C}_\Gamma Hp$, $\overline{C}_\Gamma Op$ where p is an atomic proposition, $M \models Ef$ if and only if there exists an integer k with $k \leqslant |M|$ such that $M \models_k Ef$.

Proof Without loss of generality, we only consider $f = F\overline{C}_\Gamma p$. By the unbounded semantics of $F\overline{C}_\Gamma p$, there are two states s, s' reachable from s_0 in $d^{\mathrm{I}}(M)$ steps and $s \sim^{\mathrm{C}}_{\Gamma} s'$. By lemma 3, $(s, s') \in \overline{C}_\Gamma$ if and only if there exists k with $k \leqslant |M|$ such that $(s, s') \in (\overline{E}_\Gamma)^k$. Therefore, there exists an integer k with $k \leqslant |M|$ such that $M \models_k EF\overline{C}_\Gamma p$.

In this section, for some simple LTL$^{\mathrm{K}}_{\mathrm{P}}$ formulae we find their completeness threshold. Since finding the longest loop-free path between two states is NP-complete in the size of the graph, we believe that determining completeness thresholds for general LTL$^{\mathrm{K}}_{\mathrm{P}}$ properties is at least NP-complete in the size of the model.

4 Case Study

We now present a short case study, illustrating why we introduced past operators. The system we considered is a train controller adopted from Ref. [20]. The system contains three agents: two trains and a controller. The trains, one is Eastbound, the other is Westbound, each occupy their own circular track. At one point, both tracks pass through a narrow tunnel *l*. There is not room for both trains in the tunnel at the same time. There are traffic lights on both sides of the tunnel, which can be either red or green. Both trains are equipped with a signaller, with which they can send signals to the controller. The idea is that they send a signal when they approach the tunnel. The controller can receive signals from both trains and control the color of the traffic lights. The task of the controller is, first and foremost, to ensure that the trains are never both in the tunnel at the same time; the secondary task is to ensure the smooth running of the system (e. g., the trains can always move through the tunnel, they cannot be forced into the tunnel, and so on).

We can model the example above with the interpreted system as follows. The local states for the agents are

$$L_{\mathrm{train}_1} = \{\mathrm{away}_1, \mathrm{wait}_1, \mathrm{tunnel}_1\}$$
$$L_{\mathrm{controller}} = \{\mathrm{red, green}\}$$
$$L_{\mathrm{train}_2} = \{\mathrm{away}_2, \mathrm{wait}_2, \mathrm{tunnel}_2\}$$

The set of global states is defined as $G = L_{\mathrm{train}_1} \times L_{\mathrm{controller}} \times L_{\mathrm{train}_2}$. Let $s_0 = (\mathrm{away}_1, \mathrm{green}, \mathrm{away}_2)$. Consider the following formula:

$$f = G((\mathrm{tunnel}_1 \vee \mathrm{tunnel}_2) \rightarrow Y(\neg\ (\mathrm{tunnel}_1 \vee \mathrm{tunnel}_2)\ S\ \mathrm{green}))$$

The formula *f* states that between the coterminous two trains going through the tunnel, the color of the traffic lights must be green once. If we use the pure future temporal logics, the above property will be described as follows. It is clear that f' is more complex than *f*.

$$f' = (\mathrm{green}R\neg\ (\mathrm{tunnel}_1 \vee \mathrm{tunnel}_2)) \wedge ((\mathrm{tunnel}_1 \vee \mathrm{tunnel}_2) \rightarrow (\mathrm{green} \vee (X(\mathrm{green}R\neg\ (\mathrm{tunnel}_1 \vee \mathrm{tunnel}_2)))))$$

5 Conclusion and Future Work

In the model checking of MAS, the main difficulty is the state explosion problem. In this paper, we propose a new temporal logic of knowledge called $\mathrm{LTL}_{\mathrm{P}}^{\mathrm{K}}$, which combines linear temporal logic with past operators and knowledge modalities. $\mathrm{LTL}_{\mathrm{P}}^{\mathrm{K}}$ allows us to describe many properties compactly and naturally. The bounded model checking for LTL based on SAT is a very efficient method to overcome the state explosion. We present a framework to verify $\mathrm{LTL}_{\mathrm{P}}^{\mathrm{K}}$ properties of multi-agents by the bounded model checking based on SAT. And we are the first to discuss the complete threshold problem for bounded model checking of temporal logics of knowledge.

To evaluate the effectiveness of our approach in practical application, a tool, currently, is being developed, and then an experiment will be conducted on the tool. The SAT-based verification method depends on the size of formulae produced in the translation. How to reduce the size of the formulae produced in the translation is future work.

References

[1] Clarke E M, Grumberg O, Peled D. *Model checking*[M]. Massachusetts: MIT Press, 2000.

[2] Nguyen V Y, Ruys T C. Incremental hashing for spin[C]// *Lecture Notes in Computer Science*. Berlin: Springer-Verlag, 2008, **5156**: 232 - 249.

[3] Zaks A, Joshi R. Verfying multi-threaded C programs with SPIN[C]//*Lecture Notes in Computer Science*. Berlin: Springer-Verlag, 2008, **5156**: 325 - 342.

[4] Vardi M Y. Branching vs. linear time: final showdown [C]//*Proceedings of the Conference on Tools and Algorithms for the Construction and Analysis of Systems*. Berlin: Springer-Verlag, 2001: 1 - 22.

[5] McMillan K L. *Symbolic model checking*[M]. Boston, MA, USA: Kluwer Academic Publishers, 1993.

[6] Fagin R, Halpern J, Vardi M Y. A model-theoretic analysis of knowledge[J]. *Journal of the ACM*, 1991, **38**(2): 382 - 428.

[7] Fagiu R, Halperu J Y, Moses Y, et al. *Reasoning about knowledge*[M]. Massachusetts: MIT Press, 1995.

[8] Jamroga W, Dix J. Model checking abilities of agents: a closer look[J]. *Theory of Computing Systems*, 2008, **42** (3): 366 - 410.

[9] Penczek W, Lomuscio A. Verifying epistemic properties of multi-agent systems via bounded model checking[J]. *Fundamenta Informaticae*, 2003, **55**(2):167 - 185.

[10] Luo Xiangyu, Su Kaile, Sattar A, et al. Bounded model checking knowledge and branching time in synchronous multi-agent systems[C]//*Proc of the 4th Intl Joint Conf on Autonomous Agents and Multiagent Systems*. New York: ACM Press, 2005: 1129 - 1130.

[11] Wozna B, Lomuscio A, Penczek W. Bounded model checking for knowledge and real time[C]//*Proc of the 4th Intl Joint Conf on Autonomous Agents and Multiagent Systems*. New York: ACM Press, 2005:165 - 172.

[12] Wozna B, Lomuscio A, Penczek W. Bounded model checking for deontic interpreted systems [C]//*Proc of LCMAS'04*. The Netherlands: Elsevier, 2004, **126**: 93 - 114.

[13] Ben-Ari M, Manna Z, Pnueli A. The temporal logic of branching time[J]. *Acta Information*, 1983, **20**: 207 - 226.

[14] Penczek W, Wozna B, Zbrzezny A. Bounded model checking for the universal fragment of CTL[J]. *Fundamenta Informaticae*, 2002, **51**(1): 135 - 156.

[15] Wozna B. ACTL* properties and bounded model checking [J]. *Fundamenta Informaticae*, 2004, **63**(1):65 - 87.

[16] Pnueli A. A temporal logic of concurrent programs[J]. *Theoretical Computer Science*, 1983, **13**(1): 45 - 60.

[17] Clarke E, Kroening D, Ouaknine J, et al. Completeness and complexity of bounded model checking[C]//*Lecture Notes in Computer Science*. Berlin: Springer-Verlag, 2004, **2937**: 85 - 96.

[18] Benedetti M, Cimatti A. Bounded model checking for past LTL[C]//*Lecture Notes in Computer Science*. Berlin: Springer-Verlag, 2003, **2619**: 18 - 33.

[19] Biere A, Cimatti A, Clarke E M, et al. Symbolic model checking without BDDs[C]//*Lecture Notes in Computer Science*. Berlin: Springer-Verlag, 1999, **1579**: 193 - 207.

[20] Hoek W V D, Wooldridge M. Tractable multiagent planning for epistemic goals[C]//*Proc of the First International Conference on Autonomous Agents and Multi-Agent Systems*. New York: ACM, 2002:1167 - 1174.

知识时态逻辑有界模型检测中的完备性

刘志锋[1,2] 葛 云[1] 章 东[1] 周从华[2]

([1] 南京大学电子科学与工程学院,南京 210093)
([2] 江苏大学计算机科学与通信工程学院,镇江 212013)

摘要:为解决限界模型检测的完备性问题,研究了完全界的计算问题,给出了完全界的上近似计算.首先,在线性时态认知逻辑中引入过去时态算子,得到新的时态认知逻辑 $\mathrm{LTL}_{\mathrm{P}}^{\mathrm{K}}$,从而可以紧凑自然地描述系统的可靠性规范;其次,依据图结构理论,设计了一套深度优先算法计算出系统的最大可达深度和最长无循环路径的长度;最后,以定理的形式给出了最大可达深度和最长无循环路径的长度与完全界的关系,得出了完全界的一种上近似估算.所做工作有效地解决了限界模型检测中的完全界计算问题,从而保证了限界模型检测的完备性.

关键词:有界模型检测;知识时态逻辑;多智体系统

中图分类号:TP311