Checking EMTLK Properties of Timed Interpreted Systems via Bounded Model Checking [*]

(Extended Abstract)

Bożena Woźna-Szcześniak
Jan Długosz University, IMCS, Armii Krajowej 13/15, 42-200 Częstochowa, Poland
b.wozna@ajd.czest.pl

ABSTRACT

We investigate a SAT-based bounded model checking (BMC) method for EMTLK (the existential fragment of the metric temporal logic with knowledge) that is interpreted over timed models generated by timed interpreted systems. In particular, we translate the existential model checking problem for EMTLK to the existential model checking problem for a linear temporal logic (called HLTLK), and we provide a SAT-based BMC technique for HLTLK.

Categories and Subject Descriptors

D.2.4 [**Software/Program Verification**]: Model checking

Keywords

Metric temporal logic with knowledge; timed interpreted systems; SAT-based bounded model checking; HLTLK.

1. INTRODUCTION

The formalism of *interpreted systems* (IS) [1] was designed to model multi-agent systems (MASs) [6], and to reason about the agents' epistemic and temporal properties. The formalism of *timed interpreted systems* (TIS) extends interpreted systems to make possible reasoning about soft real-time aspects of MASs. TIS provides a computationally grounded semantics on which it is possible to interpret time-bounded temporal modalities as well as traditional epistemic modalities.

To describe the requirements of MASs various extensions of temporal logics with epistemic [1], doxastic [3], and deontic [5] modalities have been proposed. In this paper we consider EMTLK which is an epistemic extension (only existential modalities) of Metric Temporal Logic [2]. We interpret EMTLK over *timed models* generated by TISs.

The main idea of SAT-based bounded model checking (BMC) [4] methods consists in translating the existential model checking problem for a modal language and for a Kripke model to the satisfiability problem (SAT-problem) of a propositional formula, and taking advantage of the power of modern SAT-solvers.

The original contributions of the paper are as follows. First, we define TIS as a model of MASs with the agents that have soft real-time deadlines to achieve intended goals. Second, we introduce two languages: EMTLK and HLTLK (*hard reset* epistemic linear-time temporal logic). Third, we propose a SAT-based BMC technique for TIS and for EMTLK, which is based on a translation of the existential model checking problem from EMTLK to the existential model checking problem for HLTLK; this translation makes use of the translation technique described in [8].

2. TIS, EMTLK, HLTLK, TRANSLATION

TIS. Let $Ag = \{1, \ldots, n, \mathcal{E}\}$ denote the non-empty and finite set of agents with $\mathcal{E}$ being a special agent that is used to model the environment in which the agents operate. We assume knowledge of standard interpreted systems (IS) due to [1]. The *timed interpreted system* (TIS) is a tuple $(\{\iota_{\mathbf{c}}, L_{\mathbf{c}}, Act_{\mathbf{c}}, X_{\mathbf{c}}, P_{\mathbf{c}}, t_{\mathbf{c}}, \mathcal{V}_{\mathbf{c}}, \mathcal{I}_{\mathbf{c}}\}_{\mathbf{c}\in Ag})$, where the elements $\{\iota_{\mathbf{c}}, L_{\mathbf{c}}, Act_{\mathbf{c}}, P_{\mathbf{c}}, \mathcal{V}_{\mathbf{c}}\}_{\mathbf{c}\in Ag}$ are defined as in IS, $X_{\mathbf{c}}$ is a non-empty set of non-negative integers variables (called *clocks*), $t_{\mathbf{c}} : L_{\mathbf{c}} \times \mathcal{C}(X_{\mathbf{c}}) \times 2^{X_{\mathbf{c}}} \times Act \to L_{\mathbf{c}}$ is a (partial) *evolution function* which defines local transitions (each element of $Act = \prod_{\mathbf{c}\in Ag} Act_{\mathbf{c}}$ is called a *joint action*, and each *clock constrain* [4] of $\mathcal{C}(X_{\mathbf{c}})$ is called an *enabling condition*), and $\mathcal{I}_{\mathbf{c}} : L_{\mathbf{c}} \to \mathcal{C}(X_{\mathbf{c}})$ is an *invariant function* which specifies the amount of time agent $\mathbf{c}$ may spent in its local states. We assume that local states and clocks for $\mathcal{E}$ are public. Further, for a given TIS it is possible to define a *timed model* $M = (\iota, S, T, \mathcal{V})$ with $\iota = \prod_{\mathbf{c}\in Ag} \iota_{\mathbf{c}} \times \{0\}^{|X_{\mathbf{c}}|}$, $S = \prod_{\mathbf{c}\in Ag} L_{\mathbf{c}} \times \mathbb{N}^{|X_{\mathbf{c}}|}$, $T \subseteq S \times (Act \cup \mathbb{N}) \times S$ being a total transition relation defined by means of action and time transitions that take into account local evolution functions, $\mathcal{V} : S \to 2^{\mathcal{PV}}$ is the valuation function defined as $\mathcal{V}(s) = \bigcup_{\mathbf{c}\in Ag} \mathcal{V}_{\mathbf{c}}(l_{\mathbf{c}}(s))$; if $s = ((\ell_1, v_1), \ldots, (\ell_n, v_n), (\ell_{\mathcal{E}}, v_{\mathcal{E}}))$ is a global state and $\mathbf{c} \in Ag$, then $l_{\mathbf{c}}(s) = \ell_{\mathbf{c}}$ and $v_{\mathbf{c}}(s) = v_{\mathbf{c}}$.

Given a TIS one can define the indistinguishability relation $\sim_{\mathbf{c}} \subseteq S \times S$ for agent $\mathbf{c}$ as follows: $s \sim_{\mathbf{c}} s'$ iff $l_{\mathbf{c}}(s') = l_{\mathbf{c}}(s)$ and $v_{\mathbf{c}}(s') \simeq v_{\mathbf{c}}(s)$, where $\simeq$ is an equivalence relation on clock valuations. A *run* of TIS is an infinite sequence $\rho = s_0, s_1, s_2, \ldots$ of global states such that the following conditions hold for all $i \in \mathbb{N}$: $s_i \in S$, $a_i \in Act$, $\delta_i \in \mathbb{N}_+$, and there exists $s'_i \in S$ such that $(s_i, \delta, s'_i) \in T$ and $(s'_i, a, s_{i+1}) \in T$.

EMTLK. Let $p \in \mathcal{PV}$, $\mathbf{c} \in Ag$, $\Gamma \subseteq Ag$, and I be an interval in $\mathbb{N}$ of the form: $[a, b)$ or $[a, \infty)$, for $a, b \in \mathbb{N}$ and $a \neq b$. The EMTLK formulae are defined by the following grammar: $\varphi ::= \mathbf{true} \mid \mathbf{false} \mid p \mid \neg p \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \varphi \mathrm{U}_I \varphi \mid \varphi \mathrm{R}_I \varphi \mid \overline{\mathrm{K}}_{\mathbf{c}}\varphi \mid \overline{\mathrm{E}}_{\Gamma}\varphi \mid \overline{\mathrm{D}}_{\Gamma}\varphi \mid \overline{\mathrm{C}}_{\Gamma}\varphi$. The modalities U_I and R_I are read as the *bounded until* and the *bounded release*, respectively. The existential epistemic modalities are read as standard.

[*] Partly supported by National Science Center under the grant No. 2011/01/B/ST6/05317.

Appears in: *Alessio Lomuscio, Paul Scerri, Ana Bazzan, and Michael Huhns (eds.), Proceedings of the 13th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2014), May 5-9, 2014, Paris, France.*

The *satisfiability* relation $\models$, which indicates truth of a EMTLK formula in the timed model M along a *discrete path* λ_ρ *corresponding to run* ρ [8] at time t, is defined inductively with the classical rules for propositional and epistemic operators and with the following rules for the temporal modalities: (•) $M, \lambda_\rho^t \models \alpha \mathrm{U}_I \beta$ iff $(\exists i \in I)(M, \lambda_\rho^{t+i} \models \beta$ and $(\forall 0 \leq j < i)\ M, \lambda_\rho^{t+j} \models \alpha)$; (•) $M, \lambda_\rho^t \models \alpha \mathrm{R}_I \beta$ iff $(\forall i \in I)(M, \lambda_\rho^{t+i} \models \alpha$ or $(\exists 0 \leq j < i)$ $M, \lambda_\rho^{t+j} \models \beta)$. An EMTLK formula φ *existentially holds* in the model M (denoted $M \models \varphi$) iff $M, \lambda_\rho^0 \models \varphi$ for some path λ_ρ of M. The *existential model checking problem* asks whether $M \models \varphi$.

HLTLK. Let φ be an EMTLK formula, m the number of intervals in φ, $Y = \{y_1, \ldots, y_m\}$ a set of new clocks that corresponds to all the time intervals appearing in φ, $p \in \mathcal{PV}' = \mathcal{PV} \cup \{q_{y_h \in I_h} \mid h = 1, \ldots, m\}$, $\mathbf{c} \in Ag$ and $\Gamma \subseteq Ag$. The HLTLK formulae are given by the following grammar: $\psi ::= \mathbf{true} \mid \mathbf{false} \mid p \mid \neg p \mid \psi \wedge \psi \mid \psi \vee \psi \mid \mathrm{H}_h(\psi \mathrm{U} \psi) \mid \mathrm{H}_h(\psi \mathrm{R} \psi) \mid \overline{\mathrm{K}}_{\mathbf{c}} \psi \mid \overline{\mathrm{E}}_\Gamma \psi \mid \overline{\mathrm{D}}_\Gamma \psi \mid \overline{\mathrm{C}}_\Gamma \psi$. The meaning of temporal and epistemic symbols is standard. The indexed symbol H_h denotes the *reset* modality representing setting to zero the clock number h that belongs to Y.

We assume a definition of an *augmented timed interpreted systems* (ATIS) that is like TIS, but we extend the set of original clocks of the environment $\mathcal{E}$, and we modify accordingly the set of actions, the local protocol and the local evolution function of $\mathcal{E}$. Further, let $\mathbb{D}_{\mathbf{c}} = \{0, \ldots, c_{\mathbf{c}} + 1\}$ with $c_{\mathbf{c}}$ being the largest constant appearing in any enabling condition or state invariants of agent $\mathbf{c}$ and in intervals appearing in φ, and $\mathbb{D} = \bigcup_{\mathbf{c} \in Ag} \mathbb{D}_{\mathbf{c}}^{|X_{\mathbf{c}}|}$. The HLTLK formulae are interpreted over the *abstract model* $M_\varphi = (\iota_\varphi, S_\varphi, T_\varphi, \mathcal{V}_\varphi)$ for an ATIS, where $\iota_\varphi = \iota$, $S_\varphi = \prod_{\mathbf{c} \in Ag} L_{\mathbf{c}} \times \mathbb{D}_{\mathbf{c}}^{|X_{\mathbf{c}}|}$, $T_\varphi \subseteq S_\varphi \times ((\{\tau\} \cup Act) \times 2^Y) \times S_\varphi$ is a total transition relation defined by means of action and time transitions such that each transition is followed by a possible rest of new clocks from Y, $\mathcal{V}_\varphi : S_\varphi \rightarrow 2^{\mathcal{PV}'}$ is the valuation function such that (1) $p \in \mathcal{V}_\varphi(s)$ iff $p \in \bigcup_{\mathbf{c} \in Ag} \mathcal{V}_{\mathbf{c}}(l_{\mathbf{c}}(s))$ for all $p \in \mathcal{PV}$; (2) $q_{y_h \in I_h} \in \mathcal{V}_\varphi(((\ell_1, v_1), \ldots, (\ell_n, v_n), (\ell_\mathcal{E}, v_\mathcal{E})))$ iff $v_\mathcal{E}(y_h) \in I_h$.

Given the abstract model M_φ, one can define the indistinguishability relation $\sim_{\mathbf{c}} \subseteq S_\varphi \times S_\varphi$ for agent $\mathbf{c}$ as follows: $s \sim_{\mathbf{c}} s'$ iff $l_{\mathbf{c}}(s') = l_{\mathbf{c}}(s)$ and $v_{\mathbf{c}}(s') = v_{\mathbf{c}}(s)$.

In this short paper we do not provide the semantics for the HLTLK formulae ψ, we only say that $M_\varphi \models \psi$ iff $M_\varphi, \pi \models \psi$ for some path π of M_φ that start at an initial state. The *existential model checking problem* consists in finding out whether $M_\varphi \models \psi$.

From EMTLK to HLTLK. Having defined EMTLK and HLTLK, we can now introduce a translation (”connection”) of the EMTLK formula φ into an HLTLK formula $\psi = \mathcal{H}(\varphi)$. Formally, let φ be an EMTLK formula and $p \in \mathcal{PV}'$. We translate the formula φ inductively into the HLTLK formula $\mathcal{H}(\varphi)$ in the following way: $\mathcal{H}(\mathbf{true}) = \mathbf{true}$, $\mathcal{H}(\mathbf{false}) = \mathbf{false}$, $\mathcal{H}(p) = p$, $\mathcal{H}(\neg p) = \neg p$, $\mathcal{H}(\alpha \vee \beta) = \mathcal{H}(\alpha) \vee \mathcal{H}(\beta)$, $\mathcal{H}(\alpha \wedge \beta) = \mathcal{H}(\alpha) \wedge \mathcal{H}(\beta)$, $\mathcal{H}(\alpha \mathrm{U}_{I_h} \beta) = \mathrm{H}_h(\mathcal{H}(\alpha) \mathrm{U}(\mathcal{H}(\underline{\beta}) \wedge p_{y_h \in \underline{I_h}}))$, $\mathcal{H}(\alpha \mathrm{R}_{\underline{I_h}} \beta))$ $= \mathrm{H}_h(\mathcal{H}(\alpha) \mathrm{R}(\neg p_{y_h \in I_h} \vee \mathcal{H}(\beta)))$, $\mathcal{H}(\overline{\mathrm{K}}_{\mathbf{c}} \alpha) = \overline{\mathrm{K}}_{\mathbf{c}} \mathcal{H}(\alpha)$, $\mathcal{H}(\overline{Y}_\Gamma \alpha)$ $= \overline{Y}_\Gamma \mathcal{H}(\alpha)$, where $Y \in \{\mathrm{D}, \mathrm{E}, \mathrm{C}\}$.

THEOREM 1. *Let M be a timed model for TIS, φ an EMTLK formula, and M_φ the abstract model for ATIS. Then, $M \models \varphi$ iff $M_\varphi \models \mathcal{H}(\varphi)$.*

3. SAT-BASED BMC FOR HLTLK

We assume knowledge of basic SAT-based BMC techniques for temporal and epistemic logics, and knowledge of the paper [7]. Let φ be an EMTLK formula, $\psi = \mathcal{H}(\varphi)$ a corresponding HLTLK formula, M_φ an abstract model, and $k \geq 0$ a bound. The *BMC problem* consists in finding out whether there exists a bound $k \in \mathbb{N}$ such that $M_\varphi \models_k \psi$. We can show that the following equivalence holds: $M_\varphi \models \psi$ iff there exists $k \geq 0$ such that $M_\varphi \models_k \psi$, i.e., the existential model checking problem can be reduced to the bounded model checking problem.

The presented propositional encoding of the BMC problem for HLTLK is based on the BMC encoding of [9], and it relies on defining the propositional formula $[M_\varphi, \psi]_k := [M_\varphi^{\psi, \iota_\varphi}]_k \wedge [\psi]_{M_\varphi, k}$, which is satisfiable if and only if $M_\varphi \models_k \psi$ holds.

The definition of $[M_\varphi^{\psi, \iota_\varphi}]_k$ assumes that the states, the joint actions (also these representing clock actions) of M_φ, are encoded symbolically, which is possible, since both the set of states and the set of joint actions are finite. Thus, let $\mathbf{w}_{i,j}$, $\mathbf{a}_{i,j}$, $\mathbf{y}_{i,j}$ and $\mathbf{u}_j$ be, respectively, symbolic states, symbolic actions, symbolic clock actions, and symbolic numbers, for $0 \leq i \leq k$ and $1 \leq j \leq \widehat{f}_k(\varphi)$. The formula $[M_\varphi^{\psi, \iota_\varphi}]_k$, which encodes the unfolding of the transition relation of M_φ $\widehat{f}_k(\psi)$-times to the depth k, is defined as follows: $\bigvee_{s \in \iota_\varphi} I_s(\mathbf{w}_{0,0}) \wedge \bigvee_{j=1}^{\widehat{f}_k(\psi)} H(\mathbf{w}_{0,0}, \mathbf{w}_{0,j}) \wedge \bigwedge_{j=1}^{\widehat{f}_k(\psi)} \bigvee_{l=0}^{k} \mathcal{N}_l^{=}(\mathbf{u}_j) \wedge \bigwedge_{j=1}^{\widehat{f}_k(\psi)} \bigwedge_{i=0}^{k-1} \mathcal{T}(\mathbf{w}_{i,j}, (\mathbf{a}_{i,j}, \mathbf{y}_{i,j}), \mathbf{w}_{i+1,j})$, where $\widehat{f}_k(\psi)$ is the function which specifies the number of k-paths of M_φ that are sufficient to validate ψ, the formulae I_s, H, and $\mathcal{N}_l^{=}$ can be defined as in [9], and the formula $\mathcal{T}$ encodes the transition relation of M_φ.

The definition of $[\psi]_{M_\varphi, k}$, which is not presented here because of the space limit, defines an encoding of the bounded semantics of ψ along a set of k-paths of M_φ.

The following theorem guarantees that the BMC problem for HLTLK and for ATIS can be reduced to the SAT-problem.

THEOREM 2. *Let M_φ be an abstract model, and ψ a HLTLK formula. For every $k \in \mathbb{N}$, $M_\varphi \models_k \psi$ if, and only if, the propositional formula $[M_\varphi, \psi]_k$ is satisfiable.*

4. REFERENCES

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

[2] C. A. Furia and P. Spoletini. Tomorrow and all our yesterdays: MTL satisfiability over the integers. In *Proceedings of the Theoretical Aspects of Computing*, volume 5160 of *LNCS*, pp. 253–264. Springer-Verlag, 2008.

[3] H. Levesque. A logic of implicit and explicit belief. In *Proceedings of the 6th National Conference of the AAAI*, pp. 198–202. Morgan Kaufman, 1984.

[4] A. Lomuscio, W. Penczek, and B. Woźna. Bounded model checking for knowledge and real time. *Artificial Intelligence*, 171:1011–1038, 2007.

[5] A. Lomuscio and M. Sergot. Deontic interpreted systems. *Studia Logica*, 75(1):63–92, 2003.

[6] M. Wooldridge. *An introduction to multi-agent systems-Second Edition*. John Wiley & Sons, 2009.

[7] B. Woźna-Szcześniak and A. Zbrzezny. Checking MTL Properties of Discrete Timed Automata via Bounded Model Checking (Extended Abstract). In *Proceedings of CS&P 2013*, pp. 469-477, volume 1032 of CEUR-WP, 2013.

[8] B. Woźna-Szcześniak and A. Zbrzezny. A translation of the existential model checking problem from MITL to HLTL. *Fundamenta Informaticae*, 122(4):401–420, 2013.

[9] A. Zbrzezny. A new translation from ECTL* to SAT. *Fundamenta Informaticae*, 120(3-4):377–397, 2012.