SAT-BASED BOUNDED MODEL CHECKING FOR TIMED INTERPRETED SYSTEMS AND THE RTECTLK PROPERTIES

BOŻENA WOŻNA-SZCZEŚNIAK, IRENEUSZ SZCZEŚNIAK

ABSTRACT

We define an SAT-based bounded model checking (BMC) method for RTECTLK (the existential fragment of the real-time computation tree logic with knowledge) that is interpreted over timed models generated by timed interpreted systems. Specifically, we translate the model checking problem for RTECTLK to the model checking problem for a variant of branching temporal logic (called $E_y$CTLK) interpreted over an abstract model, and we redefine an SAT-based BMC technique for $E_y$CTLK.

1. Introduction

The Interpreted system (IS) [5] is the formalism, which was designed to model multi-agent systems (MASs) [11], and to reason about the agents’ epistemic and temporal properties. The timed interpreted system (TIS) [14] is the formalism that extends ISs to make feasible reasoning about real-time aspects of MASs. The TIS gives a computationally grounded semantics on which it is feasible to interpret both the time-bounded temporal modalities and the conventional epistemic modalities.

The fundamental thought of the SAT-based bounded model checking (BMC) systems [2, 10] comprises in translating the existential model checking problem for a modal logic and for a Kripke structure to the SAT problem [6], furthermore, exploiting the sophistication of present day SAT-solvers, i.e., programs (tools) that automatically decide whether a propositional formula is satisfiable.

To express the specifications of MASs different extensions of classic temporal logics [3] with epistemic [5], doxastic [7], and deontic (to represent the correct functioning behaviour) [9] modalities have been proposed. In this paper we consider RTCTLK, i.e., an epistemic extension of the existential fragment of the soft real-time CTL (RTECTL) [4], which is a propositional
branching-time temporal logic with bounded operators, and which was introduced to permit specification and reasoning about time-critical correctness properties. We interpret RTECTLK over timed models generated by timed interpreted systems.

A version of the SAT-based BMC method for specifications expressed in RTECTLK has been published in [12, 13]. However, the underlying model for RTECTLK was the interpreted system [5] with the asynchronous semantics (interleaving semantics). Here we use, as the underlying model for RTECTLK, the timed interpreted systems with the synchronous semantics, thus the agents over this semantics perform a joint action at a given time in a global state. Moreover, the RTECTLK properties cannot be expressed using nested applications of the next state operators.

In the paper we make the following contribution. We define the SAT-based BMC method for RTECTLK interpreted over timed models generated by timed interpreted systems. Specifically, we translate the model checking problem for RTECTLK to the model checking problem for a variant of branching temporal logic (called ECTLK) interpreted over an abstract model, and we redefine and improve the SAT-based BMC technique for ECTLK of [8]. The improvement of the SAT-based BMC [8] consists in utilizing the SAT-based BMC method for ECTL [15]. Its main idea is to translate every subformula $\psi$ of the formula $\varphi$ using only $f_k(\psi)$ paths of length $k$. So, our new BMC algorithm uses a reduced number of paths, what results in significantly smaller and less complicated propositional formulae that encode the RTECTLK properties.

The rest of the paper is organised as follows. In Section 2 we introduce the TIS and the RTECTLK logic. In Section 3 we show how to translate the model checking problem for RTECTLK to the model checking problem for ECTLK. In Section 4 we provide a BMC method for ECTLK and for ATIS. Finally in Section 5 we conclude the paper.

2. Preliminaries

Let us start by fixing some notation used through the paper. $\mathbb{N}$ is the set of non-negative integers, $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$, $PV$ is a set of propositional variables, and $X$ is a finite set of non-negative integers variables, called clocks. A clock valuation is a function $v : X \rightarrow \mathbb{N}$ that assigns to each clock $x \in X$ a non-negative integer value $v(x)$. $\mathbb{N}[X]$ is the set of all the clock valuations. For $X' \subseteq X$, the valuation $v' = v|X' := 0$ is defined as: $\forall x \in X', v'(x) = 0$ and $\forall x \in X \setminus X'$, $v'(x) = v(x)$. For $\delta \in \mathbb{N}$, $v + \delta$ denotes the valuation $v'$ such that $\forall x \in X, v'(x) = v(x) + \delta$. 
Let $x \in X$, $c \in \mathbb{N}$, and $\sim \in \{\leq, <, =, >, \geq\}$. The set $\mathcal{C}(X)$ of clock constraints over $X$ is defined by the following grammar:

$$\phi := \text{true} \mid x \sim c \mid \phi \land \phi$$

Let $v$ be a clock valuation, and $\phi \in \mathcal{C}(X)$. The satisfaction relation $v \models \phi$ is defined inductively with the following rules:

$$v \models \text{true},$$

$$v \models x \sim c \text{ iff } v(x) \sim c,$$

$$v \models \phi \land \phi' \text{ iff } v \models \phi \text{ and } v \models \phi'.$$

Finally, by the time successor of $v$ (written $\text{succ}(v)$) we denote the clock valuation $v'$ such that $\forall x \in X, v'(x) = v(x) + 1$.

**Timed Interpreted Systems.** Let $\mathcal{A} = \{1, \ldots, n\}$ be the non-empty and finite set of agents, $\mathcal{E}$ be a special agent that is used to model the environment in which the agents operate, and $\mathcal{PV} = \bigcup_{c \in \mathcal{A}} \mathcal{PV}_c \cup \mathcal{PV}_\mathcal{E}$ be a set of propositional variables such that $\mathcal{PV}_{c_1} \cap \mathcal{PV}_{c_2} = \emptyset$ for all $c_1, c_2 \in \mathcal{A} \cup \{\mathcal{E}\}$. The set of agents $\mathcal{A}$ together with the environment constitute a multi-agent system (MAS), to model which we utilize the formalism of timed interpreted system (TIS).

In TIS, each agent $c \in \mathcal{A}$ is modelled by:

- $L_c$ - a non-empty and finite set of local states,
- $\text{Act}_c$ - a non-empty and finite set of possible actions such that the special null action $\epsilon_c$ belongs to $\text{Act}_c$; it is assumed that actions are 'public',
- $X_c$ - a non-empty and finite set of clocks,
- $P_c : L_c \to 2^{\text{Act}_c}$ - a protocol function that characterizes rules according to which actions may be performed in every local state,
- $t_c : L_c \times L_c \times \mathcal{C}(X_c) \times 2^{X_c} \times \text{Act} \to L_c$ with $\text{Act} = \prod_{c \in \mathcal{A}} \text{Act}_c \times \text{Act}_\mathcal{E}$ - a (partial) evolution function which defines local transitions; each element of $\text{Act}$ and $\mathcal{C}(X_c)$ is called a joint action and an enabling condition, respectively,
- $\nu_c : L_c \to 2^{\mathcal{PV}}$ - a valuation function which assigns to every local state a set of propositional variables that are assumed to be true at that state,
- $I_c : L_c \to \mathcal{C}(X_c)$ - an invariant function which specifies the amount of time agent $c$ may spend in its local states.

We assume that if $\epsilon_c \in P_c(t_c)$, then $t_c(\epsilon_c, t_c, \phi_c, X_c, (a_1, \ldots, a_n, a_\mathcal{E})) = t_c$ for $a_c = \epsilon_c$, any $\phi_c \in \mathcal{C}(X_c)$, and any $X \in 2^{X_c}$. Finally, we assume that the sets of clocks are pairwise disjoint.

Correspondingly to the other agents, the environment $\mathcal{E}$ is modelled by

- $L_\mathcal{E}$ - a non-empty and finite set of local states,
- $\text{Act}_\mathcal{E}$ - a non-empty and finite set of possible actions,
- $X_\mathcal{E}$ - a non-empty and finite set of clocks,
• \( P_\xi : L_\xi \to 2^{Act_\xi} \) - a protocol function,
• \( t_\xi : L_\xi \times C(X_\xi) \times 2^{X_\xi} \times Act \to L_\xi \) - a (partial) evolution function,
• \( \nu_\xi : L_\xi \to 2^{PV_\xi} \) - a valuation function,
• \( I_\xi : L_\xi \to C(X_\xi) \) - and an invariant function which specifies the amount of time agent \( \xi \) may spend in its local states.

It is assumed that local states, actions and clocks for \( \xi \) are "public".

Let the symbol \( S = \prod_{c \in \mathcal{A} \cup \{ \xi \}} L_c \times \mathbb{N}[\leq |X_c|] \) denote the non-empty set of all global states, and \( s = ((\ell_0, v_1), \ldots, (\ell_n, v_n), (\ell_\xi, v_\xi)) \in S \). Then, the symbols \( l_c(s) = \ell_c \) and \( v_c(s) = v_c \) denote, respectively, the local component and the clocks valuation of agent \( c \in \mathcal{A} \cup \{ \xi \} \) in the global state \( s \). Finally, given a set of agents \( \mathcal{A} \), the environment \( \mathcal{E} \), and a set of initial global states \( \iota \subseteq S \) such that for all \( c \in \mathcal{A} \cup \{ \xi \} \) and for all \( x \in X_c \) it holds \( v_c(x) = 0 \), a timed interpreted system (TIS) is a tuple \( \mathcal{I} = \{ L_c, Act_c, X_c, P_c, t_c, \nu_c, I_\xi \}_{c \in \mathcal{A} \cup \{ \xi \}}, \iota \).

For a given time interpreted system \( \mathcal{I} \) we define a timed model as a tuple \( M = (\Sigma, \iota, S, T, \mathcal{V}) : \)

• \( \Sigma = Act \cup \mathbb{N} \) is the set of labels (i.e., joint actions and natural numbers),
• \( S \) and \( \iota \) are defined as above,
• \( \mathcal{V} : S \to 2^{PV_\xi} \) is the valuation function defined as \( \mathcal{V}(s) = \bigcup_{c \in \mathcal{A}} \nu_c(l_c(s)) \),
• \( T \subseteq S \times (Act \cup \mathbb{N}) \times S \) is a transition relation defined by action and time transitions:
  (1) Action transition: for any \( \overline{a} \in Act \), \( (s, \overline{a}, s') \in T \) iff for all \( c \in \mathcal{A} \), there exists a local transition \( t_c(l_c(s), l_\xi(s), \phi_c, X', \overline{a}) = l_c(s') \) such that \( v_c(s) = \phi_c \wedge I(l_c(s)) \) and \( v_c(s') = v_c(s)[X' := 0] \) and \( v_\xi(s') = I(l_\xi(s')) \), and there exists a local transition \( t_\xi(l_\xi(s), \phi_\xi, X', \overline{a}) = l_\xi(s') \) such that \( v_\xi(s) = \phi_\xi \wedge I(l_\xi(s)) \) and \( v_\xi(s') = v_\xi(s)[X' := 0] \) and \( v_\xi(s') = I(l_\xi(s')) \).
  (2) Time transition: let \( \delta \in \mathbb{N} \), \( (s, \delta, s') \in T \) iff for all \( c \in \mathcal{A} \cup \{ \xi \} \), \( l_c(s) = l_c(s') \) and \( v_c(s) = I(l_c(s)) \) and \( v_c(s') = v_c(s) + \delta \) and \( v_\xi(s') = I(l_\xi(s')) \).

We assume that the relation \( T \) is total, i.e. for any \( s \in S \) there exists \( s' \in S \) and there exist either a non-empty joint action \( \overline{a} \in Act \) or natural number \( \delta \in \mathbb{N} \) such that it holds \( T(s, \overline{a}, s') \) or \( T(s, \delta, s') \).

Given a time interpreted system \( \mathcal{I} \) one can define the indistinguishability relation \( \sim_c \subseteq S \times S \) for agent \( c \) as follows: \( s \sim_c s' \) iff \( l_c(s') = l_c(s) \) and \( v_c(s') = v_c(s) \).

Let \( M \) be a timed model generated by a TIS \( \mathcal{I} \). A run of \( \mathcal{I} \) is an infinite sequence \( \rho = s_0 \xrightarrow{\delta_0, \overline{a}_0} s_1 \xrightarrow{\delta_1, \overline{a}_1} s_2 \xrightarrow{\delta_2, \overline{a}_2} \ldots \) of global states such that the following conditions hold for all \( i \in \mathbb{N} \): \( s_i \in S \), \( \overline{a}_i \in Act \), \( \delta_i \in \mathbb{N}_+ \), and there exists \( s'_i \in S \) such that \( (s_i, \delta_i, s'_i) \in T \) and \( (s'_i, \overline{a}_i, s_{i+1}) \in T \). Note
that the definition of the run does not allow two consecutive joint actions to be performed one after the other, i.e., between each two joint actions some time must pass.

The symbol $\Pi_I(s)$ denotes the set of all the runs in $I$ that start at the state $s$. $\Pi = \bigcup_{\rho \in \Pi(s^0)}$.

**RTCTLK.** Let $\rho \in \mathcal{P}_\mathcal{V}$, $\epsilon \in \mathcal{A}$, $\Gamma \subseteq \mathcal{A}$, 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 existential fragment of RTCTL with knowledge (RTCTLK) is defined by the following grammar:

$$\varphi := \top | \bot | p | \neg p | \varphi \land \varphi | \varphi \lor \varphi |
E(\varphi U_I \varphi) | EG_I \varphi | K_\epsilon \varphi | E_G \varphi | D_\Gamma \varphi | C_\Gamma \varphi$$

The symbol $E$ (for some path) is the path quantifier. The symbols $U$ (bounded until) and $G_I$ (bounded globally) are temporal modalities. The derived basic temporal modalities for bounded eventually and bounded release are defined as follows: $\text{EF}_I \varphi \overset{\text{def}}{=} E(\top U_I \varphi)$, $\text{EF}_{(\psi \land \varphi)} \overset{\text{def}}{=} E(\psi U_I (\varphi \land \psi)) \lor \text{EG}_I \psi$.

Hereafter, if the interval $I$ is of the form $[0, \infty)$, then we omit it for the simplicity of the presentation. The symbols $\text{K}_\epsilon$ (agent $\epsilon$ considers possible), $\overline{E}_\Gamma$ (possibly everyone in $\Gamma$ knows), $\overline{D}_\Gamma$ (possible distributed knowledge in the group $\Gamma$), and $\overline{C}_\Gamma$ (possible common knowledge among agents in $\Gamma$) are the dualities to standard epistemic modalities.

To define the satisfiability relation for RTCTLK, we define the notion of a discrete path $\lambda_\rho$ corresponding to run $\rho$ (this can be done in a unique way because of the assumption that the runs are strongly monotonic), and we assume the following definitions of epistemic relations:

$$\sim_{\epsilon} \overset{\text{def}}{=} \bigcup_{\epsilon \in \Gamma} \sim_{\epsilon},
\sim_{\epsilon} \overset{\text{def}}{=} (\sim_{\epsilon})^+ \text{ (the transitive closure of } \sim_{\epsilon}),
\sim_{\Gamma} \overset{\text{def}}{=} \bigcap_{\epsilon \in \Gamma} \sim_{\epsilon}, \text{ where } \Gamma \subseteq \mathcal{A}.$$  

Let $\Delta_0 = [b_0, b_1)$, $\Delta_1 = [b_1, b_2)$, $\ldots$ be the sequence of pairwise disjoint intervals, where: $b_0 = 0$ and $b_1 = b_{i-1} + \delta_{i-1}$ if $i > 0$. For each $t \in \mathbb{N}$, let $idx_\rho(t)$ denote the unique index $i$ such that $t \in \Delta_i$. A path $\lambda_\rho$ corresponding to $\rho$ is a mapping $\lambda_\rho : \mathbb{N} \rightarrow S$ such that $\lambda_\rho(t) = ((t_1, v_1 + t - b_1), \ldots, (t_n, v_n + t - b_1), (t_1, v_1 + t - b_1)) = s_i + t - b_i$, where $i = idx_\rho(t)$.

Let $Y \in \{D, E, C\}$. The satisfiability relation $\models$, which indicates truth of a RTCTLK formula in the timed model $M$ at state $s$, is defined inductively with the classical rules for propositional operators and with the following rules for the temporal and epistemic modalities:

$$M, s \models E(\alpha U_I \beta) \text{ iff } (\exists \rho \in \Pi_I(s)) (\forall i \in I) (M, \lambda_\rho(i) \models \beta \text{ and } (\forall 0 \leq j < i) M, \lambda_\rho(j) \models \alpha)$$
$$M, s \models EG_I \alpha \text{ iff } (\exists \rho \in \Pi_I(s)) (\forall i \in I) (M, \lambda_\rho(i) \models \alpha)$$
$$M, s \models K_\epsilon \alpha \text{ iff } (\exists \rho \in \Pi_I(s)) (\exists i \geq 0) (s \sim_\epsilon \lambda_\rho(i) \text{ and } M, \lambda_\rho(i) \models \alpha)$$
$$M, s \models \overline{Y}_\Gamma \alpha \text{ iff } (\exists \rho \in \Pi_I(s)) (\exists i \geq 0) (s \sim_\Gamma \lambda_\rho(i) \text{ and } M, \lambda_\rho(i) \models \alpha)$$
An RTECTLK formula $\phi$ holds in the model $M$ (denoted $M \models \phi$) iff $M, s^0 \models \phi$ for some state $s^0 \in I$. The model checking problem asks whether $M \models \phi$.

3. From RTECTLK to $E_\emptyset$CTLK

The translation of the model checking problem for RTECTLK to the model checking problem for $E_\emptyset$CTLK, a language defined below and interpreted over an abstract model for an augmented timed interpreted system is based on [8], where the translation of the model checking problem for the existential part of TCTL [1] augmented with knowledge (TECTLK) with a dense-time semantics defined over timed automata to the model checking problem for $E_\emptyset$CTLK with a semantics defined over the region graph has been introduced.

We start by defining augmented timed interpreted systems (ATIS) for a given timed interpreted system $\mathbb{I} = (\{L_c, Act_c, X_c, P_c, t_c, V_c, I_c\}_{c \in A \cup \{E\}, t})$, and an RTECTLK formula $\phi$.

Let $m$ be the number of intervals appearing in $\phi$. Then, an ATIS $\mathbb{I}_\phi$ is defined as the following tuple

$$(\{L_c, V_c, I_c\}_{c \in A \cup \{E\}}, \{Act_c, X_c, P_c, t_c\}_{c \in A}, Act'_E, X'_E, P'_E, t'_E):$$

- $Act'_E = Act \cup \{a_y\}$, where $a_y$ is a new action corresponding to setting to zero a new clock $y$.
- $X'_E = X \cup \{y\}$, where the new clock $y$ corresponds to all the intervals appearing in $\phi$; one clock is sufficient to perform the BMC algorithm that is presented in the next section.
- $P'_E : L_E \rightarrow 2^{Act'_E}$ such that $\{a_y\} \subseteq P'_E(\ell)$ for all $\ell \in L_E$.
- $t'_E : L_E \times C(X'_E) \times 2^{X'_E} \times Act'_E \rightarrow L_E$ is an extension of $t_E$ such that $Act' = \bigwedge_{i=1}^m Act_i \times Act'_E$ and $t'_E(\ell, true, (a_y), (\epsilon_1, \ldots, \epsilon_n, a_y)) = \ell_E$.

An abstract model for ATIS. Let $\phi$ be an RTECTLK formula, $\mathcal{P}' = \mathcal{P} \cup \{p \in I \mid I \text{ is an interval in } \phi\}$, and $\mathbb{I}_\phi = (\{L_c, Act_c, X_c, P_c, t_c, V_c, I_c\}_{c \in A \cup \{E\}, t})$ be an ATIS. The abstract model for $\mathbb{I}_\phi$ is a tuple $M _\phi = (\Sigma_\phi, t, S_\phi, T_\phi, V_\phi)$, where

- $\Sigma_\phi = Act \cup \{\tau\}$, where $Act = \prod_{c \in A \cup \{E\}} Act_c$.
- $S_\phi = \prod_{c \in A \cup \{E\}} L_c \times \mathbb{N}^{X_c}$ is the set of all possible global states,
- $V_\phi : S_\phi \rightarrow 2^{\mathcal{P}'}$ is the valuation function such that:
  1. $p \in V_\phi(s)$ iff $p \in \bigcup_{c \in A \cup \{E\}} V_c(I_c(s))$ for all $p \in \mathcal{P}'$,
  2. $p_{\phi \in I} \in V_\phi((\ell_1, v_1), \ldots, (\ell_n, v_n), ((\ell_\xi, v_\xi)))$ iff $v_c(y) \in I$.
- $T_\phi \subseteq S_\phi \times \Sigma_\phi \times S_\phi$ is a transition relation defined by action and time transitions. Let $\pi \in Act$: 

\[\text{transitions of } T_\phi\]
1. Action transition: \((s, \overline{a}, s') \in T_\varphi\) iff \((\forall c \in A) (\exists \phi_c \in C(X_c)) (\exists X_c' \subseteq X_c) (v_c(l_c(s), l_c(s), \phi_c, X_c', \overline{a}) = l_c(s') \text{ and } v_c(s) = \phi_c \wedge I(l_c(s)))\) and \(v_c'(s') = v_c(s)[X_c' := 0]\) and \(v_c'(s') = I(l_c(s'))\) and \((\exists \phi_c \in C(X_c)) (\exists X_c' \subseteq X_c) (t_c'(l_c(s), \phi_c, X_c', \overline{a}) = l_c(s') \text{ and } v_c(s) = \phi_c \wedge I(l_c(s)))\) and \(v_c'(s') = v_c(s)[X_c' := 0]\) and \(v_c'(s') = I(l_c(s'))\).

2. Time transition: \((s, \tau, s') \in T_\varphi\) iff \((\forall c \in A \cup \{\epsilon\})(l_c(s) = l_c(s') \text{ and } v_c(s) = I(l_c(s)) \text{ and } v_c'(s') = \text{succ}(v_c(s)) \text{ and } v_c'(s') = I(l_c(s)))\).

Note that each transition is followed by a possible reset of new clocks. This is to ensure that the new clocks can be reset along the evolution of the system any time it is needed.

Given an augmented time interpreted system \(I_\varphi\) one can define the indistinguishability relation \(\sim_e\) of states \(s, s' \in S_\varphi\) for agent \(c\) as follows: \(s \sim_c s'\) iff \(l_c(s) = l_c(s')\) and \(v_c(s) = v_c(s')\).

**The \(E_y\) CTLK language.** In order to translate a RTECTLK formula \(\varphi\) into the corresponding \(E_y\) CTLK formula \(\psi\) we map the RTECTLK language into \(E_y\) CTLK by reinterpreting the temporal operators, denoted by \(E_yU\) and \(E_yG\). Formally, for \(p \in P_\varphi', c \in A, \text{ and } \Gamma \subseteq A\), the \(E_y\) CTLK formulae are defined by the following grammar:

\[
\varphi := T \mid \bot \mid \neg p \mid \varphi \land \psi \mid \varphi \lor \psi \mid E_y(gU) \mid E_yG \mid \text{release} \mid \text{eventually}.
\]

In addition, we introduce some useful derived temporal modalities:

- \(E_y(gU) \equiv E_y(\psi U \land \psi) \lor E_yG \psi \text{ (release)},\)
- \(E_y \text{eventually} \equiv E_y(\text{eventually}) \text{ (eventually)}\).

The \(E_y\) CTLK formulae are interpreted over the abstract model \(M_\varphi\). Let \(T_1\) denote the part of \(T_\varphi\), where transitions are labelled with elements of \(Act \cup \{\tau\}\), and \(T_y\) denotes the transitions that reset the clock \(y\).

**Definition 1.** A path \(\pi\) in \(M_\varphi\) is a sequence \(\pi = (s_0, s_1, \ldots)\) of states such that \((s_0, \tau, s_1) \in T_1\), and for each \(i > 0\), either \((s_i, \overline{a}_i, s_{i+1}) \in T_1\) or \((s_i, \tau, s_{i+1}) \in T_1\), and if \((s_i, \overline{a}_i, s_{i+1}) \in T_1\) holds, then \((s_{i+1}, \tau, s_{i+2}) \in T_1\) holds, and \(\overline{a}_i \in Act\) for each \(i \geq 0\).

Observe that the above definition of the path ensures that the first transition is the time one, and between each two action transitions at least one time transition appears.

For a path \(\pi\), \(\pi(i)\) denotes the \(i\)-th state \(s_i\) of \(\pi\). \(\Pi_\varphi(s)\) denotes the set of all the paths starting at \(s \in S_\varphi\), and \(\Pi_\varphi = \bigcup_{s' \in E_y} \Pi_\varphi(s')\).

The satisfiability relation \(\models\), which indicates truth of \(\psi\) in \(M_\varphi\) at state \(s\) (in symbols \(M_\varphi, s \models \psi\)), is defined inductively with the classical rules for
Theorem 1.

An RTECTL formula \( M \) Let \( \phi \) (\( s, \epsilon_1, ..., \epsilon_n, a_y \), \( s' \)) \( \in T_y \) and 
(\( \exists \pi \in \Pi_\varphi(s') \)(\( \exists m \geq 0 \) [\( M, \pi(m) \models \beta \) and (\( \forall j < m \)\( M, \pi(j) \models \alpha \)]),

M, s \models E_\varphi \alpha \) if (\( \exists s' \in S_\varphi \))((\( s, \epsilon_1, ..., \epsilon_n, a_y \), \( s' \)) \( \in T_y \) and 
(\( \exists \pi \in \Pi_\varphi(s') \)(\( \forall m \geq 0 \) \( M, \pi(m) \models \alpha \)),

M, s \models K_\varphi \alpha \) if (\( \exists \pi \in \Pi_\varphi \)(\( \exists m \geq 0 \) \( s \sim_\varphi \pi(m) \) and \( M, \pi(m) \models \alpha \)),

M, s \models \forall \varphi \alpha \) if (\( \exists \pi \in \Pi_\varphi \)(\( \exists m \geq 0 \) \( s \sim_\varphi \pi(m) \) and \( M, \pi(m) \models \alpha \)).

An E_\varphi CTLK formula \( \varphi \) is valid on \( M_\varphi \) (denoted \( M_\varphi \models \varphi \)) iff \( M_\varphi, s^0 \models \varphi \) for some \( s^0 \) \( \in \) \( \epsilon \), i.e., \( \varphi \) is true at some initial state of the model \( M_\varphi \).

Having defined syntax and semantics of the E_\varphi CTLK logic, we can now introduce the translation mentioned above. An RTECTL formula \( \varphi \) is translated inductively into the E_\varphi CTLK formula \( \mathcal{H}(\varphi) \) as follows:

- \( \mathcal{H}(p) = p \) if \( p \in P \forall \), \( \mathcal{H}(\neg p) = \neg p \) if \( p \in P \forall \),
- \( \mathcal{H}(\alpha \vee \beta) = \mathcal{H}(\alpha) \vee \mathcal{H}(\beta) \), \( \mathcal{H}(\alpha \land \beta) = \mathcal{H}(\alpha) \land \mathcal{H}(\beta) \),
- \( \mathcal{H}(E_\Gamma \alpha) = E_\varphi \mathcal{H}(\neg p \in I \vee \mathcal{H}(\alpha)) \),
- \( \mathcal{H}(E(\alpha U_\beta)) = E_\varphi \mathcal{H}(\alpha U (\beta) \land p \in I) \),
- \( \mathcal{H}(K_\varphi \alpha) = K_\varphi \mathcal{H}(\alpha) \), \( \mathcal{H}(\forall \Gamma \alpha) = \forall \Gamma \mathcal{H}(\alpha) \), where \( \Gamma \in \{D, E, C\} \).

The main theorem of the section states that the validity of the RTECTL formula \( \varphi \) over the timed model is equivalent to the validity of the corresponding E_\varphi CTLK formula \( \mathcal{H}(\varphi) \) over the abstract model. The proof of the theorem can be completed by an induction of the formula \( \varphi \).

**Theorem 1.** Let \( M \) be the timed model, \( \varphi \) an RTECTL formula, and \( M_\varphi \) the abstract model. Then, \( M \models \varphi \) iff \( M_\varphi \models \mathcal{H}(\varphi) \).

4. AN SAT-BASED BMC METHOD FOR E_\varphi CTLK

**Bounded semantics.** Let \( M_\varphi = (\Sigma_\varphi, l, S_\varphi, T_\varphi, V_\varphi) \) be an abstract model, \( k \in \mathbb{N} \), and \( 0 \leq l \leq k \). As before, we denote by \( T_1 \) the subset of \( T_\varphi \), where transitions are labelled with elements of \( Act \cup \{\tau\} \), and by \( T_\varphi \) the set of transitions resetting the clock \( y \).

**Definition 2.** A k-path \( \pi \) is a finite sequence \( \pi = (s_0, ..., s_k) \) of states such that \( (s_0, \tau, s_1) \in T_1 \), and for each \( 0 < i < k \), either \( (s_i, \tau, s_{i+1}) \in T_1 \) or \( (s_i, \tau, s_{i+1}) \in T_\varphi \), and if \( (s_i, \tau, s_{i+1}) \in T_1 \) holds, then \( (s_{i+1}, \tau, s_{i+2}) \in T_1 \) holds, and \( \pi_i \in Act \) for each \( 0 \leq i < k \).

The symbol \( \Pi_k(s) \) denotes the set of all the k-paths starting at \( s \) in \( M_\varphi \), and \( \Pi_k = \bigcup_{s_0 \in \varphi} \Pi_k(s_0) \).

**Definition 3.** Let \( \pi(i) = ((l_1, v_1'), ..., (l_n, v_n'), (l_k, v_k')) \) for all \( i \leq k \). A k-path \( \pi = (\pi(0), ..., \pi(k)) \) is a loop if there exists \( 0 \leq l < k \) and (\( \forall c \in A \cup \{\epsilon\}\)\( (v_c^k = v_c') \) and \( (\forall c \in A)\)\( v_c^k = v_c \) and \( v_c^k \downarrow X_\epsilon = v_c' \downarrow X_\epsilon \), where \( \downarrow X_\epsilon \).
denoted the projection of the clock valuation \( v_\mathcal{E} : X_\mathcal{E} \cup \{ y \} \rightarrow \mathbb{N} \) on the clock valuation \( v_\mathcal{E}' : X_\mathcal{E} \rightarrow \mathbb{N} \).

Satisfaction of the temporal operator \( \mathcal{E}_y \mathcal{G} \) on a \( k \)-path \( \pi \) in the bounded case depends on whether or not \( \pi \) is a loop. Therefore, we assume a function \( \text{loop} : \Pi_k \mapsto 2^{\mathbb{N}} \) which returns the set of all the indices of the states for which there is a transition from the last state of a \( k \)-path \( \pi \). Note that if a \( k \)-path is a loop, then it represents an infinite path.

The bounded satisfiability relation \( \models_k \), which indicates truth of \( \psi \) in \( M_\varphi \) at state \( s \) (denoted \( M_\varphi, s \models_k \psi \)) is defined inductively with the classical rules for propositional operators and with the following rules for the temporal and epistemic modalities:

- \( M_\varphi, s \models_k \mathcal{E}_y (\alpha \cup \beta) \) iff \( (\exists s' \in S_\varphi)((s, (\epsilon_1, \ldots, \epsilon_n, a_y), s') \in T_y \) and \( (\exists \pi \in \Pi_k(s'))(\exists 0 \leq m \leq k) (M_\varphi, \pi(m) \models_k \beta \) and \( (\forall j < m)M_\varphi, \pi(j) \models \alpha) \),
- \( M_\varphi, s \models_k \mathcal{E}_y \mathcal{G} \alpha \) iff \( (\exists s' \in S_\varphi)((s, (\epsilon_1, \ldots, \epsilon_n, a_y), s') \in T_y \) and \( (\exists \pi \in \Pi_k(s'))(\forall 0 \leq j \leq k) (M_\varphi, \pi(j) \models \alpha \) and \( \text{loop}(\pi) \neq \emptyset) \),
- \( M_\varphi, s \models_k \mathcal{K}_y \alpha \) iff \( (\exists \pi \in \Pi_k)(\exists 0 \leq m \leq k)(s \sim_c \pi(m) \) and \( M_\varphi, \pi(m) \models \alpha) \),
- \( M_\varphi, s \models_k \mathcal{Y}_y \alpha \) iff \( (\exists \pi \in \Pi_k)(\exists 0 \leq m \leq k)(s \sim_k \pi(m) \) and \( M, \pi(m) \models \alpha) \),

where \( Y \in \{ \mathcal{D}, \mathcal{E}, \mathcal{C} \} \).

We use the following notation \( M_\varphi \models_k \psi \) if \( M_\varphi, s^0 \models_k \psi \) for some \( s^0 \in \iota_\varphi \).

The bounded model checking problem consists in finding out whether there exists \( k \in \mathbb{N} \) such that \( M_\varphi \models_k \psi \).

The following theorem shows that for some particular bound the bounded and unbounded semantics are equivalent.

**Theorem 2.** Let \( \varphi \) be an RTCTLK formula, \( M_\varphi \) an abstract model, and \( \psi = \mathcal{H}(\varphi) \) an \( \mathcal{E}_y \text{CTL}K \) formula. The following equivalence holds: \( M_\varphi \models \varphi \iff \text{there exists } k \geq 0 \text{ such that } M_\varphi \models_k \psi \).

**Translation to SAT.** Let \( M_\varphi \) be an abstract model, \( \psi \) an \( \mathcal{E}_y \text{CTL}K \) formula, and \( k \geq 0 \) a bound. The presented propositional encoding of the BMC problem for \( \mathcal{E}_y \text{CTL}K \) improves the BMC encoding of [8] and it is based on the BMC encoding of [16]. It relies on defining the propositional formula \([M_\varphi, \psi]_k := [M_\varphi^0]_k \wedge [\psi]_M, k\), which is satisfiable if and only if \( M_\varphi \models_k \psi \) holds.

The definition of \([M_\varphi, \psi]_k\) assumes that both the states and the joint actions of \( M_\varphi \) are encoded symbolically. This is possible, since both the set of states and the set of joint actions are finite. Also, since we work with a set of \( k \)-paths, we can bound the clocks valuation to the set \( \mathbb{D} = \{0, \ldots, c + 1\} \) with \( c \) being the largest constant appearing in any enabling condition or state invariants of all the agents and in intervals appearing in \( \varphi \). Moreover, this definition assumes knowledge of the number of \( k \)-paths of \( M_\varphi \) that are sufficient to validate \( \psi \). To this aim, as usually, we define the auxiliary
function $f_k : E_p CTLK \to \mathbb{N}$: $f_k(\top) = f_k(\bot) = f_k(p) = f_k(\lnot p) = 0,$ where $p \in \mathcal{PV}$; $f_k(\alpha \land \beta) = f_k(\alpha) + f_k(\beta); f_k(\alpha \lor \beta) = \max\{f_k(\alpha), f_k(\beta)\}; f_k(E_c(\alpha \lor \beta)) = k \cdot f_k(\alpha) + f_k(\beta) + 1$; $f_k(\text{E}_p \alpha) = (k + 1) \cdot f_k(\alpha) + 1;$ $f_k(\text{G}_p \alpha) = f_k(\alpha) + k; f_k(Y \alpha) = f_k(\alpha) + 1$ for $Y \in \{\text{F}_c, \text{D}_p, \text{G}_p\}.$

Formally, let $c \in \mathcal{A}$. We assume that each state $s \in S_c$ is represented by a symbolic state $w = ((w_1, v_1), \ldots, (w_n, v_n), (w_{\mathcal{E}}, v_{\mathcal{E}}))$, where each symbolic local state $(w_c, v_c)$ is a pair of vectors of propositional variables; the first element encodes local states of $L_c$ and the second element encodes the clock valuations over $D$. Next, we assume that each join action $a \in \text{Act}$ is represented by a symbolic action $a = (a_1, \ldots, a_n, a_{\mathcal{E}})$, where each symbolic local action $a_c$ is a vector of propositional variables. Moreover, we assume that the time action $\tau$ is represented by a proposition variable $\varphi_{\tau}$. Finally, we assume a symbolic representation of a $k$-path $\pi$, the number of which is $j$, and we call it the $j$-th symbolic $k$-path $\pi_j = (w_{0,j}, \ldots, w_{k,j})$, where $0 \leq j < f_k(\varphi_{\tau})$. We assume that each symbolic state $\psi$ of $\pi_j = (w_{0,j}, \varphi_{\tau}, s_{\mathcal{E}}), s_{\mathcal{E}}$ is $\varphi_{\tau}$.

Let $w$ and $w'$ be two different symbolic states, and $a$ a symbolic action. We assume definitions of the following auxiliary propositional formulæ:

- $p(w)$ - encodes the set of states of $M_\varphi$ in which $p \in \mathcal{PV}$ holds.
- $L_s(w)$ - encodes the state $s$ of $M_\varphi$.
- $H_c(w, w')$ - encodes the equality of two local states and two local clock valuations of agent $c \in \mathcal{A}$.
- $H(w, w', a, \mathcal{E}) := \bigwedge_{c \in \mathcal{A}, \{c\}} H_c(w, w')$ - encodes equality of two global states.
- $T(a, w, w')$ is a formula over $w, w'$, and $a$, which is true for valuations $s_w$ of $w, s_{w'}$ of $w'$, and $s_a$ of $a$ iff either $(s_w, s_a, s_{\mathcal{E}}) \in T_1$ or $(s_w, \varphi_{\tau}, s_{\mathcal{E}}) \in T_2$ (encodes non-resetting transitions of $M_\varphi$).
- $T_y(a, w, w')$ is a formula over $w$ and $w'$, which is true for two valuations $s_w$ of $w$ and $s_{w'}$ of $w'$ iff $(s_w, (\epsilon_1, \ldots, \epsilon_n, a_{\mathcal{E}}), s_{w'}) \in T_y$ (encodes transitions resetting the clock $y$).

Let $F_k(\psi) = \{j \in \mathbb{N} \mid 1 \leq j \leq f_k(\psi)\}$, $w_j$ and $a_j$ be, respectively, symbolic states and symbolic actions, for $0 \leq j \leq k$ and $j \in F_k(\psi)$. The formula $[M_\varphi^w]_{k}$, which encodes the unfolding of the transition relation of $M_\varphi$, $f_k(\psi)$-times to the depth $k$, is defined as follows:

$$[M_\varphi^w]_{k} := \bigwedge_{s \in \mathcal{A}} L_s(w_{0,0}) \land \bigwedge_{n=1}^{f_k(\psi) - 1} \bigwedge_{m=0}^{k - 1} T(w_n, m, a_{m,n}, w_{m+1,n}).$$

The next step is a translation of a $E_p CTLK$ formula $\psi$ to a propositional formula $[\psi]_{M_{\varphi,k}} := [\psi]^{0,0,F_k(\psi)}$, where $[\alpha]^{m,n,A}_{k}$ denotes the translation of $\alpha$ at the symbolic state $w_{m,n}$ by using the set $A \subseteq F_k(\psi)$. To define $[\psi]^{0,0,F_k(\psi)}$, we have to know how to divide the set $F_k(\psi)$ into subsets
needed for translating the subformulae of $\psi$. To accomplish this goal we use some auxiliary functions $(g_t, g_r, g_s, h^U_k, h^G_k)$ that were defined in [16].

Let $M_\varphi$ be a model, $\psi$ a $E_\gamma\text{CTL}K$ formula, and $k \geq 0$ a bound. The formula $[\psi]_k^{[0,0, F_k(\psi)]}$ that encodes the bounded semantics for $E_\gamma\text{CTL}K$ is inductively defined as shown below.

Namely, let $0 \leq n < f_k(\psi)$, $m \leq k$, $n' = \min(A)$, $h^U_k = h^U_k(g_s(A), f_k(\beta))$, and $h^G_k = h^G_k(g_s(A), f_k(\alpha))$.

\[
\begin{align*}
\phi_k[m,n,A] &= \top, \\

\neg \phi_k[m,n,A] &= \bot, \\

[p]_k[m,n,A] &= p(w_{m,n}), \\

\neg [p]_k[m,n,A] &= \neg p(w_{m,n}), \\

[\alpha \land \beta]_k[m,n,A] &= [\alpha]_k[m,n,g_t(A,f_k(\alpha))] \land [\beta]_k[m,n,g_t(A,f_k(\beta))], \\

[\alpha \lor \beta]_k[m,n,A] &= [\alpha]_k[m,n,g_t(A,f_k(\alpha))] \lor [\beta]_k[m,n,g_t(A,f_k(\beta))], \\

[E_\gamma(\alpha \land \beta)]_k[m,n,A] &= \mathcal{T}_\psi(w_{m,n}, w_{0,n'}) \land \bigwedge_{i=0}^{k-1} \bigwedge_{j=0}^{\infty} \bigwedge_{\alpha}^1 [\beta]_{\alpha}^i [\gamma]_{\alpha}^i (m', n, \gamma^i (\gamma)), \\

[E_\gamma \land E_\gamma]_k[m,n,A] &= \mathcal{T}_\psi(w_{m,n}, w_{0,n'}) \land \bigwedge_{i=0}^{k-1} \bigwedge_{j=0}^{\infty} \bigwedge_{\alpha}^1 [\beta]_{\alpha}^i [\gamma]_{\alpha}^i (m', n, \gamma^i (\gamma)), \\

[K_c \alpha]_k[m,n,A] &= (\bigwedge_{s \in e} I_s(w_{0,n'})) \land (\bigwedge_{\alpha}^1 [\beta]_{\alpha}^i [\gamma]_{\alpha}^i (m', n, \gamma^i (\gamma)) \land H_c(w_{m,n}, w_{j,n'})), \\

[D_\Gamma \alpha]_k[m,n,A] &= (\bigwedge_{s \in e} I_s(w_{0,n'})) \land (\bigwedge_{\alpha}^1 [\beta]_{\alpha}^i [\gamma]_{\alpha}^i (m', n, \gamma^i (\gamma)) \land H_c(w_{m,n}, w_{j,n'})), \\

[E_\Gamma \alpha]_k[m,n,A] &= (\bigwedge_{s \in e} I_s(w_{0,n'})) \land (\bigwedge_{\alpha}^1 [\beta]_{\alpha}^i [\gamma]_{\alpha}^i (m', n, \gamma^i (\gamma)) \land H_c(w_{m,n}, w_{j,n'})), \\

[C_\Gamma \alpha]_k[m,n,A] &= (\bigwedge_{j=1}^\infty (E_\Gamma^j \alpha)]_k[m,n,A].
\end{align*}
\]

The following theorem guarantees that the BMC problem for $E_\gamma\text{CTL}K$ and for an augmented timed interpreted system can be reduced to the SAT-problem. The theorem can be proven by induction on the length of the formula $\psi$.

**Theorem 3.** Let $M_\varphi$ be an abstract model, and $\psi$ an $E_\gamma\text{CTL}K$ 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.

5. Conclusions

We have defined an SAT-based BMC for timed interpreted system and for properties expressed in RTCTLK. The method is based on a translation of the model checking problem for RTCTLK to the model checking problem
for $\text{E}_\gamma\text{CTLK}$, and then on the translation of the model checking problem for $\text{E}_\gamma\text{CTLK}$ to the SAT-problem.

In [8] a formalism of real time interpreted systems (RTIS) has been defined to model MASs with hard real-time deadlines and an SAT-based BMC for the existential version of the timed CTLK (TECTLK) has been defined. However, in contrast to the semantics adopted in this work, the semantics of the RTIS model is asynchronous, the agents are just pure timed automata, and the $\text{E}_\gamma\text{CTLK}$ logic is interpreted on the region graph for timed automata.

In the future, we plan to implement and experimentally evaluate the proposed SAT-based BMC. Next, we plan to define SMT-based BMC for TIS and for RTECTLK, and compare it with the SAT-based one.

REFERENCES


Received: September 2015

Bożena Woźna-Szcześniak
Jan Długosz University in Częstochowa
Institute of Mathematics and Computer Science
Al. Armii Krajowej 13/15, 42-200 Częstochowa, Poland
E-mail address: b.wozna@ujd.czest.pl

Ireneusz Szcześniak
Częstochowa University of Technology
Institute of Computer and Information Sciences
ul. Dąbrowskiego 69, 42-201 Częstochowa, Poland
E-mail address: iszczesniak@icis.pcz.pl