Bounded model checking real-time multi-agent systems with clock differences: theory and implementation

Alessio Lomuscio[1], Bożena Woźna[1], and Andrzej Zbrzezny[2]

[1] DCS, University College London. Gower Street, London WC1E6BT, United Kingdom.
email: {A.Lomuscio,B.Wozna}@cs.ucl.ac.uk
[2] IMCS, Jan Długosz University. Al. Armii Krajowej 13/15, 42-200 Częstochowa, Poland.
email: a.zbrzezny@ajd.czest.pl

Abstract. We present a methodology for verifying epistemic and real-time temporal properties of multi-agent systems. We introduce an interpreted systems semantics based on diagonal timed automata and use a real-time temporal epistemic language to describe properties of multi-agent systems. We develop a bounded model checking algorithm for this setting and present experimental results for a real-time version of the alternating bit-transmission problem obtained by means of a preliminary implementation of the technique.

1 Introduction

Reasoning about knowledge has always been a core concern in AI and in multi-agent systems. This is no surprise given that knowledge is a key concept to model intelligent, rational activities, human or artificial. A plethora of formalisms have been proposed and refined over the years, many of them based on logic. One of the most widely studied is based on variants of modal logics and is commonly referred to as epistemic logic [7]. Rather than providing a computational engine for artificial agents' reasoning, epistemic logic, at least in this line, is seen as a specification language for modelling and reasoning about systems, much in common with formal methods in computer science.

Specification languages are most useful when they can be verified automatically. In this effort both theorem proving and model checking techniques and tools have been made available for epistemic logic. In particular, model checking techniques based on BDD [14, 16], bounded model checking [12], unbounded model checking [8] have been developed and their implementation either publicly released [14, 1] or made available via a web-interface [11].

While, given the above, one may be forgiven for thinking that verification via model checking of temporal epistemic logic has now become of age, in many respects the area is still lacking support for many essential functionalities. One of these is *real-time*. While the formalisms above deal with discrete sequence of events, it is often of both theoretical and practical interest to refer to a temporal model that assumes a dense sequence of events and use operators able to represent dense temporal intervals. The only work in this line we are aware of is [17], where a bounded model checking algorithm for TECTLK was suggested. In this paper we aim to extend two key limitations of that work in that: 1) we assume an underlying computationally more expressive semantical model (diagonal timed automata), 2) we report on an in-house implementation of

this technique and discuss experimental results. Further, to exemplify the use of the techniques described in the paper we present a real-time version of the alternating bit transmission problem — a key requirement of this example is the expressive power of a semantics based on diagonal timed automata as the one presented here.

The rest of the paper is organised as follows. In Section2 we present real-time interpreted systems, a semantics for knowledge and real-time, based on diagonal timed automata. In Section 3 we present syntax and semantics for TECTLK, the logic for which the verification method is defined. In Section 4 we define a bounded model checking algorithm for the logic; given the state-spaces in question are infinite the method involves a tailored discretisation process. Finally we test these techniques on a novel real-time variant of the alternating bit protocol.

2 Diagonal real-time interpreted systems

In [17] a semantics for real-time and knowledge based on non-diagonal timed automata was proposed. Automata are given as the finer grained semantics on which real-time interpreted systems are defined. In that framework the only clock conditions that can be used are of the form $x \sim c$ where x is a clock, c a constant and $\sim$ an equality/inequality relation. While this is appropriate for some scenarios (like the "railroad crossing system" discussed in that article), it is well known that in others more expressive tests are required. Crucially, we may need to *compare two clocks of the system as an enabling condition for a transition*. Introducing more expressive clock comparisons is known to generate considerable complications in the verification methodology [3], including a loss of completeness in the resulting bounded model checking technique [10]; aim of this paper is to analyse this setting for the case of real-time and epistemic properties.

To define diagonal real-time interpreted systems we first recall the definitions of diagonal timed automata and their composition. We refer to [15] for discussion and more details.

We assume a finite set X of real variables, called *clocks*, and for $x,\ y \in X$, $\sim \in \{<, \leq, =, >, \geq\}$, $c \in \mathbb{N}$, where $\mathbb{N} = \{0, 1, \ldots\}$ is a set of natural numbers, we define a set of *clock constraints* over X, denoted by $C(X)$, by means of the following grammar:

$$cc ::= \ true \mid x \sim c \mid x - y \sim c \mid cc \wedge cc$$

A *clock valuation* v is a total function from X into the set of non-negative real numbers $\mathbb{R}$. $\mathbb{R}^X$ denotes the set of all the clock valuations, and the satisfaction relation $\models$ for a clock constraint $cc \in X$ and $v \in \mathbb{R}^X$ is defined inductively as follows:

$$\begin{array}{ll} v \models true, & \\ v \models (x \sim c) & \text{iff } v(x) \sim c, \\ v \models (x - y \sim c) & \text{iff } v(x) - v(y) \sim c, \\ v \models (cc \wedge cc') & \text{iff } v \models cc \text{ and } sv \models cc' \end{array}$$

For $cc \in C(X)$, $[\![cc]\!]$ denotes the set of all the clock valuations that satisfy cc. The clock valuation that assigns the value 0 to all clocks is denoted by v^0. For $v \in \mathbb{R}^X$ and $\delta \in \mathbb{R}$, $v + \delta$ is the clock valuation that assigns the value $v(x) + \delta$ to each clock x. For $v \in \mathbb{R}^X$ and $Y \subseteq X$, $v[Y]$ denotes the clock valuation of X that assigns the value 0 to each clock in Y and leaves the values of the other clocks unchanged.

Definition 1 (Diagonal timed automaton). *Let $\mathcal{PV}$ be a set of propositional variables. A* diagonal timed automaton *is a tuple $\mathcal{A} = (\Sigma, L, l^0, X, \mathcal{I}, R, \mathcal{V})$, where*

- *Σ is a nonempty finite set of actions,*
- *L is a nonempty finite set of locations,*
- *$l^0 \in L$ is an initial location,*
- *X is a finite set of clocks,*
- *$\mathcal{I} : L \mapsto C(X)$ is a state invariant function, and*
- *$R \subseteq L \times \Sigma \times C(X) \times 2^X \times L$ is a transition relation,*
- *$\mathcal{V} : L \mapsto 2^{\mathcal{PV}}$ is a function assigning to each location a set of atomic propositions true in that location.*

An element $(l, \sigma, \mathfrak{cc}, Y, l') \in R$ represents a transition from location l to location l' labelled with an action σ. The invariant condition states that the automaton is allowed to remain in location l only as long as the constraint $\mathcal{I}(l)$ is satisfied. The guard $\mathfrak{cc}$ has to be satisfied to enable the transition. The transition resets all clocks in the set Y to the value 0.

As usual, the semantics of diagonal timed automata is defined by associating *dense models* to them.

Definition 2 (Dense Model). *Let $\mathcal{A} = (\Sigma, L, l^0, X, \mathcal{I}, R, \mathcal{V})$ be a diagonal timed automaton, and $C(\mathcal{A}) \subseteq C(X)$ a set of all the clock constrains occurring in any enabling condition used in the transition relation R or in a state invariant of $\mathcal{A}$. A* dense model *for $\mathcal{A}$ is a tuple $\mathcal{G}(\mathcal{A}) = (\Sigma \cup \mathbb{R}, Q, q^0, \rightarrow, \widetilde{\mathcal{V}})$, where*

- *$\Sigma \cup \mathbb{R}$ is a set of labels,*
- *$Q = L \times \mathbb{R}^X$ is a set of states,*
- *$q^0 = (l^0, v^0)$ is an initial state,*
- *$\rightarrow \subseteq Q \times (\Sigma \cup \mathbb{R}) \times Q$ is a time/action transition relation defined by:*
  - *Time transition: $(l, v) \xrightarrow{\delta} (l, v + \delta)$ iff $(\forall 0 \leq \delta' \leq \delta)\ v + \delta' \in [\![\mathcal{I}(l)]\!]$*
  - *Action transition: $(l, v) \xrightarrow{\sigma} (l', v')$ iff $(\exists \mathfrak{cc} \in C(\mathcal{A}))(\exists Y \subseteq X)$ such that $v' = v[Y]$, $(l, \sigma, \mathfrak{cc}, Y, l') \in R$, $v \in [\![\mathfrak{cc}]\!]$, and $v' \in [\![\mathcal{I}(l')]\!]$.*
- *$\widetilde{\mathcal{V}} : Q \mapsto 2^{\mathcal{PV}}$ is a valuation function such that $\widetilde{\mathcal{V}}((l, v)) = \mathcal{V}(l)$*

Lemma 1. *Let $\mathfrak{cc} \in C(X)$, $v \in \mathbb{R}^X$, and $\delta \in \mathbb{R}$. If $v \in [\![\mathfrak{cc}]\!]$ and $v + \delta \in [\![\mathfrak{cc}]\!]$, then for each $(0 \leq \delta' \leq \delta)\ v + \delta' \in [\![\mathfrak{cc}]\!]$.*

Proof Straightforward by induction on clock constraints. □

As the above lemma shows, for the considered set of clock constraints $C(X)$, in the semantics of diagonal timed automata the condition of a time transition $(l, v) \xrightarrow{\delta} (l, v + \delta)$ can be replaced by the following: $v \in [\![\mathfrak{cc}]\!]$ and $v + \delta \in [\![\mathfrak{cc}]\!]$.

In this paper we take diagonal timed automata to provide the lower level, fine-grained description for the agents; the composition of these defines a multi-agent systems. So, in this paper, the computations of a multi-agent system are simply the traces generated by the executions of a network of diagonal timed automata that communicate through shared actions. We model this communication via the standard notion of the parallel composition [15], as defined below.

Consider a network of m diagonal timed automata $\mathcal{A}_i = (\Sigma_i, L_i, l_i^0, X_i, \mathcal{I}_i, R_i, \mathcal{V}_i)$, for $i = 1, \ldots, m$, such that $L_i \cap L_j = \emptyset$ for all $i, j \in \{1, \ldots, m\}$ and $i \neq j$, and denote by $\Sigma(\sigma) = \{1 \leq i \leq m \mid \sigma \in \Sigma_i\}$ the set of indexes of the automata performing action σ. The *parallel composition* of m diagonal timed automata $\mathcal{A}_i$ is a diagonal timed automaton $\mathcal{A} = (\Sigma, L, l^0, X, \mathcal{I}, R, \mathcal{V})$, where $\Sigma = \bigcup_{i=1}^{m} \Sigma_i$, $L = \prod_{i=1}^{m} L_i$, $l^0 = (l_1^0, \ldots, l_m^0)$, $X = \bigcup_{i=1}^{m} X_i$, $\mathcal{I}((l_1, \ldots, l_m)) = \bigwedge_{i=1}^{m} \mathcal{I}_i(l_i)$, $\mathcal{V}((l_1, \ldots, l_m)) = \bigcup_{i=1}^{m} \mathcal{V}_i(l_i)$, and a transition $((l_1, \ldots, l_m), \sigma, \mathfrak{cc}, Y, (l'_1, \ldots, l'_m)) \in R$ iff $(\forall i \in \Sigma(\sigma))\ (l_i, \sigma, \mathfrak{cc}_i, Y_i, l'_i) \in R_i$, $\mathfrak{cc} = \bigwedge_{i \in \Sigma(\sigma)} \mathfrak{cc}_i$, $Y = \bigcup_{i \in \Sigma(\sigma)} Y_i$, and $(\forall j \in \{1, \ldots, m\} \setminus \Sigma(\sigma))\ l'_j = l_j$.

Observe that, given the above, transitions in which actions are not shared are interleaved, whereas the transitions caused by shared action are synchronised.

To give a definition of real-time interpreted systems that supports clock constraints of the form $x - y \sim c$, we define the notion of *weak region equivalence* [19].

Definition 3 (Weak Region Equivalence). *Assume a set of clocks X, and for any $t \in \mathbb{R}$ let $\langle t \rangle$ denote the fractional (respectively integral) part of t (respectively $\lfloor t \rfloor$). The* weak region equivalence *is a relation $\cong \subseteq \mathbb{R}^X \times \mathbb{R}^X$ defined as follows (see Figure 1 for an intuition). For two clock valuations u and v in $\mathbb{R}^X$, $u \cong v$ iff all the following conditions hold:*

E1. $\lfloor u(x) \rfloor = \lfloor v(x) \rfloor$, *for all* $x \in X$,

E2. $\langle u(x) \rangle = 0$ *iff* $\langle v(x) \rangle = 0$, *for all* $x \in X$,

E3. $\langle u(x) \rangle < \langle u(y) \rangle$ *iff* $\langle v(x) \rangle < \langle v(y) \rangle$, *for all* $x, y \in X$.

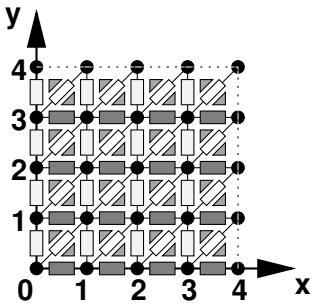

Fig. 1. Weak Region Equivalence of clock valuations for two clocks.

We will use Z, Z', and so on to denote the equivalence classes induced by the relation $\cong$. As customary, we call these classes zones, and the set of all the zones we denote by $Z(|X|)$.

A *diagonal real-time interpreted system* is defined as follows.

Definition 4 (Diagonal real-time interpreted system). *Consider m diagonal timed automata and their parallel composition. A* diagonal real-time interpreted system *(or a* model*) is a tuple $M = (\Sigma \cup \mathbb{R}, Q, q^0, \rightarrow, \sim_1, \ldots, \sim_m, \widetilde{\mathcal{V}})$ such that*

– *$\Sigma \cup \mathbb{R}$, Q, q^0, $\rightarrow$, and $\widetilde{\mathcal{V}}$ are defined as in Definition 2, and*

– *for each agent i, $\sim_i \subseteq Q \times Q$ is a relation defined by: $(l, v) \sim_i (l', v')$ iff $l_i((l, v)) = l_i((l', v'))$ and $v \cong v'$, where $l_i : Q \mapsto L_i$ is a function returning the location of agent i from a global state.*

As in [7] we consider two (global) states to be epistemically indistinguishable for agent i if its local state (i.e., its location) is the same in the two global states. Additionally we assume the agents' clocks to be globally visible, although only privately resettable. For two states to be indistinguishable we further assume the clocks of the states belong to the same zone, i.e., the agents are aware of their own clocks' discretisations. This is not dissimilar from [17].

3 TECTLK

In this section we introduce TECTLK a logic for knowledge and real time. While the logic is the same as the one described in [17], satisfaction is here defined on diagonal real-time interpreted systems.

Syntax. Let $\mathcal{PV}$ be a set of propositional variables containing the symbol $\top$, $\mathcal{AG}$ a set of m agents, and I an interval in $\mathbb{R}$ with integer bounds of the form $[n, n']$, $[n, n')$, $(n, n']$, (n, n'), (n, ∞), and $[n, \infty)$, for $n, n' \in \mathbb{N}$. For $p \in \mathcal{PV}$, $i \in \mathcal{AG}$, and $\Gamma \subseteq \mathcal{AG}$, the *set of* TECTLK *formulas* is defined by the following grammar:

$$\varphi := p \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \mathrm{E}(\varphi \mathrm{U}_I \varphi) \mid \mathrm{E}(\varphi \mathrm{R}_I \varphi) \mid \overline{\mathrm{K}}_i \varphi \mid \overline{\mathrm{D}}_\Gamma \varphi \mid \overline{\mathrm{C}}_\Gamma \varphi \mid \overline{\mathrm{E}}_\Gamma \varphi$$

The other temporal modalities are defined as usual: $\bot \stackrel{def}{=} \neg\top$, $\mathrm{EG}_I\varphi \stackrel{def}{=} \mathrm{E}(\bot \mathrm{R}_I \varphi)$, $\mathrm{EF}_I\varphi \stackrel{def}{=} \mathrm{E}(\top \mathrm{U}_I \varphi)$. Moreover, $\alpha \Rightarrow \beta \stackrel{def}{=} \neg\alpha \vee \beta$.

Semantics. Let $M = (\Sigma \cup \mathbb{R}, Q, q^0, \rightarrow, \sim_1, \ldots, \sim_m, \widetilde{\mathcal{V}})$ be a *model*. We define a q_0-*run* ρ as a sequence of states: $q_0 \xrightarrow{\delta_0} q_0 + \delta_0 \xrightarrow{\sigma_0} q_1 \xrightarrow{\delta_1} q_1 + \delta_1 \xrightarrow{\sigma_1} q_2 \xrightarrow{\delta_2} \ldots$, where $q_i \in Q$, $\sigma_i \in \Sigma$ and $\delta_i \in \mathbb{R}_+$ for each $i \in \mathbb{N}$, and by $f_{\mathcal{A}}(q_0)$ we denote the set of all such q_0-runs.

We say that a state $q \in Q$ is reachable if there is a q^0−run ρ such that there exists a state in ρ equal to q. Finally, in order to give a semantics to TECTLK, we introduce the notation of a *dense path π_ρ corresponding to a run ρ. A dense path π_ρ corresponding to* ρ is a mapping from $\mathbb{R}$ to a set of states Q such that $\pi_\rho(r) = q_i + \delta$ for $r = \Sigma_{j=0}^{i} \delta_j + \delta$ with $i \in \mathbb{N}$ and $0 \leq \delta < \delta_i$. Moreover, we define the following epistemic relations: $\sim_\Gamma^E = \bigcup_{i \in \Gamma} \sim_i$, and $\sim_\Gamma^C = (\sim_\Gamma^E)^+$ (the transitive closure of $\sim_\Gamma^E$), and $\sim_\Gamma^D = \bigcap_{i \in \Gamma} \sim_i$, where $\Gamma \subseteq \mathcal{AG}$.

Definition 5. *Let $M = (\Sigma \cup \mathbb{R}, Q, q^0, \rightarrow, \sim_1, \ldots, \sim_m, \widetilde{\mathcal{V}})$ be a model such that the set Q contains reachable states only. $M, q \models \alpha$ denotes that α is true at state q in M. The satisfaction relation $\models$ is defined inductively as follows:*

$$\begin{array}{ll}
M, q \models p & \text{iff } p \in \widetilde{\mathcal{V}}(q), \\
M, q \models \neg p & \text{iff } p \notin \widetilde{\mathcal{V}}(q), \\
M, q \models \alpha \vee \beta & \text{iff } q \models \alpha \text{ or } q \models \beta, \\
M, q \models \alpha \wedge \beta & \text{iff } q \models \alpha \text{ and } q \models \beta, \\
M, q \models \mathrm{E}(\alpha \mathrm{U}_I \beta) & \text{iff } \exists_{\rho \in f_{\mathcal{A}}(q)} \exists_{r \in I} [M, \pi_\rho(r) \models \beta \text{ and } (\forall_{r' < r}) M, \pi_\rho(r') \models \alpha], \\
M, q \models \mathrm{E}(\alpha \mathrm{R}_I \beta) & \text{iff } \exists_{\rho \in f_{\mathcal{A}}(q)} \forall_{r \in I} [M, \pi_\rho(r) \models \beta \text{ or } (\exists_{r' < r}) M, \pi_\rho(r') \models \alpha], \\
M, q \models \overline{\mathrm{K}}_i \alpha & \text{iff } (\exists q' \in Q)(q \sim_i q' \text{ and } M, q' \models \alpha),
\end{array}$$

$M, q \models \overline{\mathrm{D}}_\Gamma \alpha$ *iff* $(\exists q' \in Q)(q \sim^D_\Gamma q'$ *and* $M, q' \models \alpha)$,
$M, q \models \overline{\mathrm{E}}_\Gamma \alpha$ *iff* $(\exists q' \in Q)(q \sim^E_\Gamma q'$ *and* $M, q' \models \alpha)$,
$M, q \models \overline{\mathrm{C}}_\Gamma \alpha$ *iff* $(\exists q' \in Q)(q \sim^C_\Gamma q'$ *and* $M, q' \models \alpha)$.

We say a TECTLK formula φ is *valid in* M (denoted by $M \models \varphi$) iff $M, q^0 \models \varphi$, i.e., φ is true at the initial state of the model M. In the rest of the paper we are concerned with devising and implementing an automatic model checking algorithm for checking whether a formula φ is valid in a given model M.

4 Bounded Model Checking for TECTLK

Bounded model checking (BMC) is a popular model checking technique for the verification of reactive systems [2, 5]. On discrete-time, it is supported by nuSMV [4] and in its epistemic extension by Verics [11]. Verifying whether a system S satisfies a property P amounts to checking $M_S \models \phi_P$, where M_S is a model capturing S and ϕ_P is a property representing P. In BMC this check is turned into the propositional satisfiability test (ultimately performed by ad-hoc highly-efficient SAT solvers) of $[M_S] \wedge [\phi_P]$, where $[M_S], [\phi_P]$ are appropriate Boolean formulas representing a truncated portion of the model M_S and the modal formula ϕ_P. We refer to [12] for a description of the technique for the case of discrete-time epistemic properties.

To define a BMC method for diagonal real-time interpreted systems, we adapt the BMC technique for TECTLK and non-diagonal automata presented in [17]. We first translate the BMC problem from TECTLK into the BMC problem for ECTLK$_y$ (a discretised version), and then we define BMC for ECTLK$_y$.

4.1 Translation from TECTLK to ECTLK$_y$

When dealing with real-time it is customary to discretise the state space. We use the scheme introduced in [19], which we shortly describe. Let $\mathbb{Q}$ be a set of rational numbers. For every $m \in \mathbb{N}$, we define $D_m = \{d \in \mathbb{Q} \mid (\exists k \in \mathbb{N})\ d \cdot 2^m = k\}$, $E_m = \{e \in \mathbb{Q} \mid (\exists k \in \mathbb{N})\ e \cdot 2^m = k$ and $e > 0\}$, and we choose $D = \bigcup_{m=0}^{\infty} D_m$ as the set of discretised clock's values, and $E = \bigcup_{m=1}^{\infty} E_m$ as the set of labels.

Definition 6 (Discretised model). *Let $\mathcal{A} = (\Sigma, L, l^0, X, \mathcal{I}, R, \mathcal{V})$ be a diagonal timed automaton resulting from the parallel composition of m diagonal timed automata (agents). A* discretised model *for $\mathcal{A}$ is a tuple $M_d = (\Sigma \cup E, S, s^0, \rightarrow_d, \sim^d_1, \ldots, \sim^d_m, \widetilde{\mathcal{V}}_d)$, where $S = L \times D^X$ is a set of states, $s^0 = (l^0, v^0)$ is the initial state, $\sim^d_i \subseteq S \times S$ is an relation defined by $(l, v) \sim^d_i (l', v')$ iff $l_i((l, v)) = l_i((l', v'))$ and $v \cong v'$, for each agent i, $\widetilde{\mathcal{V}}_d : S \mapsto 2^{\mathcal{P}\mathcal{V}}$ is a valuation function defined by $\widetilde{\mathcal{V}}_d((l, v)) = \mathcal{V}(l)$, and $\rightarrow_d \subseteq S \times (\Sigma \cup E) \times S$ is a time/action transition relation defined by:*

- *Time transition: for any $\delta \in E$, $(l, v) \xrightarrow{\delta}_d (l, v + \delta)$ iff $(l, v) \xrightarrow{\delta} (l, v + \delta)$ in $\mathcal{G}(\mathcal{A})$ and $(\forall \delta' \leq \delta)\ v + \delta' \cong v$ or $v + \delta' \cong v + \delta$,*
- *Action transition: for any $\sigma \in \Sigma$, $(l, v) \xrightarrow{\sigma}_d (l', v')$ iff $(\exists \delta)(\exists v'')$ such that $(l, v) \xrightarrow{\delta}_d (l, v'')$ and $(l, v'') \xrightarrow{\sigma} (l', v')$ in $\mathcal{G}(\mathcal{A})$.*

The general idea of the translation is the same as the one in [17], but obviously given the different capabilities there are differences. In particular, the discretised model used here is infinite; so while the procedure in [17] is sound and complete, the one here is only sound[1].

Specifically, given a multi-agent system modelled by a network of diagonal timed automata $\mathcal{A}_i = (\Sigma_i, L_i, l_i^0, X_i, \mathcal{I}_i, R_i, \mathcal{V}_i)$ and a TECTLK formula φ, we extend each automaton $\mathcal{A}_i$ by a new clock y, an action σ_y, and transitions to obtain a new automaton $\mathcal{A}_i^\varphi = (\Sigma_i \cup \{\sigma_y\}, L_i, l_i^0, X_i', \mathcal{I}_i, R_i', \mathcal{V}_i)$ with $X_i' = X_i \cup \{y\}$ and $R_i' = R_i \cup \{(l, \sigma_y, true, \{y\}, l) \mid l \in L\}$. The clock y corresponds to all the timing intervals appearing in φ, and special transitions are used to reset the new clock. We then construct the discretised model for the parallel composition of $\mathcal{A}_i^\varphi$, denoted by $\mathcal{A}_\varphi$, and augment its valuation function with the set of propositional variables containing a new proposition $p_{y\in I}$ for every interval I appearing in φ, and a new proposition p_b representing that a state s is boundary, i.e., the fractional part of the clock's valuation in s is zero. Finally, we translate the TECTLK formula φ into an ECTLK$_y$ formula $\psi = \mathrm{cr}(\varphi)$ such that model checking of φ over the model for the parallel composition of $\mathcal{A}_i$ can be reduced to the model checking of ψ over the discretised model for $\mathcal{A}_\varphi$.

Before we define the final part of the above construction, we will first introduce the syntax and semantics for ECTLK$_y$.

Let $p \in \mathcal{PV}' = \mathcal{PV} \cup \{p_b\} \cup \{p_{y\in I} \mid I \text{ is an interval in } \varphi\}$. Then, the set of ECTLK$_y$ formulae is defined by the following grammar:

$$\alpha := p \mid \neg p \mid \alpha \wedge \alpha \mid \alpha \vee \alpha \mid \mathrm{E}_y(\alpha \mathrm{U} \alpha) \mid \mathrm{E}_y(\alpha \mathrm{R} \alpha) \mid \overline{\mathrm{K}}_i \alpha \mid \overline{\mathrm{D}}_\Gamma \alpha \mid \overline{\mathrm{C}}_\Gamma \alpha \mid \overline{\mathrm{E}}_\Gamma \alpha$$

ECTLK$_y$ is interpreted over the discretised model M_d for $\mathcal{A}_\varphi$.

Definition 7 (Satisfaction for ECTLK$_y$). *Let α, β be formulae of* ECTLK$_y$*, $M_d = (\Sigma \cup E, S, s^0, \to_d, \sim_1^d, \ldots, \sim_m^d, \widetilde{\mathcal{V}}_d)$ a discretised model for $\mathcal{A}_\varphi$, $\to_{\mathcal{A}}$ denotes the part of $\to_d$, where transitions are labelled with elements of $\Sigma \cup E$, and $\to_y$ denotes the transitions that reset the clock y. A* path *π in M_d is a sequence $(s_0, s_1, \ldots)$ of states such that $s_i \to_{\mathcal{A}} s_{i+1}$ for each $i \in \mathbb{N}$, and $\Pi(s)$ denotes the set of all the paths starting at s in M_d. The satisfaction relation $\models$ is defined inductively as follows:*

$$\begin{aligned}
&M_d, s \models p && \text{iff } p \in \widetilde{\mathcal{V}}_d(s),\\
&M_d, s \models \neg p && \text{iff } p \notin \widetilde{\mathcal{V}}_d(s),\\
&M_d, s \models \alpha \vee \beta && \text{iff } M_d, s \models \alpha \text{ or } M_d, s \models \beta,\\
&M_d, s \models \alpha \wedge \beta && \text{iff } M_d, s \models \alpha \text{ and } M_d, s \models \beta,\\
&M_d, s \models \mathrm{E}_y(\alpha \mathrm{U} \beta) && \text{iff } (\exists s' \in S)(s \to_y s' \text{ and } (\exists \pi \in \Pi(s'))(\exists m \geq 0)\\
&&& \quad [M_d, \pi(m) \models \beta \text{ and } (\forall j < m)\ M_d, \pi(j) \models \alpha]),\\
&M_d, s \models \mathrm{E}_y(\alpha \mathrm{R} \beta) && \text{iff } (\exists s' \in S)(s \to_y s' \text{ and } (\exists \pi \in \Pi(s'))(\forall m \geq 0)\\
&&& \quad [M_d, \pi(m) \models \beta \text{ or } (\exists j \leq m)\ M_d, \pi(j) \models \alpha]),\\
&M_d, s \models \overline{\mathrm{K}}_i \alpha && \text{iff } \exists_{\pi \in \Pi(s^0)} \exists_{j \geq 0} (M_d, \pi(j) \models \alpha \text{ and } s \sim_i \pi(j)),\\
&M_d, s \models \overline{\mathrm{D}}_\Gamma \alpha && \text{iff } \exists_{\pi \in \Pi(s^0)} \exists_{j \geq 0} (M_d, \pi(j) \models \alpha \text{ and } s \sim_\Gamma^D \pi(j)),
\end{aligned}$$

[1] Note though that because of the complexity in the SAT translation and satisfiability checks, BMC is never complete in practice when the system is sufficiently complex, so this is not a real concern.

$$M_d, s \models \overline{\mathrm{E}}_\Gamma \alpha \qquad \textit{iff } \exists_{\pi \in \Pi(s^0)} \exists_{j \geq 0} (M_d, \pi(j) \models \alpha \text{ and } s \sim_\Gamma^E \pi(j)),$$
$$M_d, s \models \overline{\mathrm{C}}_\Gamma \alpha \qquad \textit{iff } \exists_{\pi \in \Pi(s^0)} \exists_{j \geq 0} (M_d, \pi(j) \models \alpha \text{ and } s \sim_\Gamma^C \pi(j)).$$

Definition 8 (Validity). *An* ECTLK$_y$ *formula* φ *is* valid in M_d *(denoted* $M_d \models \varphi$*) iff* $M_d, s^0 \models \varphi$*, i.e.,* φ *is true at the initial state of* M_d*.*

We can now translate inductively a TECTLK formula φ into the ECTLK$_y$ formula $\mathrm{cr}(\varphi)$. The translation is defined inductively as follows:

- $\mathrm{cr}(p) = p$ for $p \in \mathcal{PV}'$,
- $cr(\neg p) = \neg cr(p)$ for $p \in \mathcal{PV}'$,
- $\mathrm{cr}(\alpha \vee \beta) = \mathrm{cr}(\alpha) \vee \mathrm{cr}(\beta)$,
- $\mathrm{cr}(\alpha \wedge \beta) = \mathrm{cr}(\alpha) \wedge \mathrm{cr}(\beta)$,
- $\mathrm{cr}(\mathrm{E}(\alpha \mathrm{U}_I \beta)) = \mathrm{E}_y(\mathrm{cr}(\alpha)\mathrm{U}(\mathrm{cr}(\beta) \wedge p_{y \in I} \wedge (p_b \vee \mathrm{cr}(\alpha))))$,
- $\mathrm{cr}(\mathrm{E}(\alpha \mathrm{R}_{I_i} \beta)) = \mathrm{E}_y(\mathrm{cr}(\alpha)\mathrm{R}(\neg p_{y \in I_i} \vee (\mathrm{cr}(\beta) \wedge (p_b \vee \mathrm{cr}(\alpha)))))$.
- $\mathrm{cr}(\overline{\mathrm{K}}_i \alpha) = \overline{\mathrm{K}}_i \mathrm{cr}(\alpha)$,
- $\mathrm{cr}(\overline{\mathrm{D}}_\Gamma \alpha) = \overline{\mathrm{D}}_\Gamma \mathrm{cr}(\alpha)$,
- $\mathrm{cr}(\overline{\mathrm{E}}_\Gamma \alpha) = \overline{\mathrm{E}}_\Gamma \mathrm{cr}(\alpha)$,
- $\mathrm{cr}(\overline{\mathrm{C}}_\Gamma \alpha) = \overline{\mathrm{C}}_\Gamma \mathrm{cr}(\alpha)$.

4.2 Correctness of the translation from TECTLK to ECTLK$_y$

In the section we will show that validity of a TECTLK formula φ over the model for $\mathcal{A} = (\Sigma, L, l^0, X, \mathcal{I}, R, \mathcal{V})$ is equivalent to the validity of $\mathrm{cr}(\varphi)$ over the discretised model for $\mathcal{A}_\varphi$ with the extended valuation function.

We begin by proving the fact that states belonging to the same *region*, i.e., to the pair (l, Z) with $l \in L$ and $Z \in Z(|X|)$, satisfies the same set of TECTLK formulae. To do this, we will first prove Lemmas 2-5.

Lemma 2. *Let* X *be a set of clocks, and* $u, v \in \mathbb{R}^X$ *be clock valuations such that* $u \cong v$*. For any clock constraint* $\mathrm{cc} \in C(X)$*,* $u \in [\![\mathrm{cc}]\!]$ *iff* $v \in [\![\mathrm{cc}]\!]$*.*

Proof Straightforward induction on clock constraints. □

Lemma 3. *Let* u*,* v *be clock valuations such that* $u \cong v$*. For every* $\delta \in \mathbb{R}$ *there exists* $\delta' \in \mathbb{R}$ *such that* $u + \delta \cong v + \delta'$*.*

Proof We omit the proof as it is analogous to the proof of the Lemma 4.3 of [18] □

Further, we extend the equivalence relation $\cong$ to an equivalence relation over the set of states of the model $M = (\Sigma \cup \mathbb{R}, Q, q^0, \rightarrow, \sim_1, \ldots, \sim_m, \widetilde{\mathcal{V}})$. Namely, for any (l, u) and (l', u') in Q, $(l, u) \cong (l', u')$ iff $l = l'$ and $u \cong u'$. Then, we can prove the following lemmas.

Lemma 4. *Let* $\sigma \in \Sigma$*, and let* q_1*,* q_2 *be states such that* $q_1 \cong q_2$*. Then, for each state* q_3 *such that* $q_1 \xrightarrow{\sigma} q_3$*, there exists a state* q_4 *such that* $q_2 \xrightarrow{\sigma} q_4$ *and* $q_3 \cong q_4$*.*

Proof Straightforward, by using Lemma 2. □

Lemma 5. *Let q_0, q'_0 be two states such that $q_0 \cong q'_0$. Moreover, let ρ be a run $q_0 \xrightarrow{\delta_0} q_0 + \delta_0 \xrightarrow{\sigma_0} q_1 \xrightarrow{\delta_1} q_1 + \delta_1 \xrightarrow{\sigma_1} q_2 \xrightarrow{\delta_2} \dots$ of M. There exists a run ρ' such that $\pi_{\rho'}(0) = q'_0$, and for every $r \in \mathbb{R}$, $\pi_\rho(r) \cong \pi_{\rho'}(r)$).*

Proof Straightforward, by using Lemmas 3 and 4. □

We can now prove the lemma showing that states belonging to the same region satisfies the same set of TECTLK formulae.

Lemma 6. *Let M be a model, φ a* TECTLK *formula, and $q = (l, u)$ and $q' = (l, v)$ states of M such that $u \cong v$. Then, $M, (l, u) \models \varphi$ iff $M, (l, v) \models \varphi$*

Proof [Induction on the length of TECTLK formulae]

It is easy to see that the thesis holds for all the propositional variables and for all the negations of propositional variables. If φ is of the form $\alpha \vee \beta$ or $\alpha \wedge \beta$, then the proof of the thesis is straightforward. If φ is of the form $\overline{\mathrm{K}}_i\alpha$, $\overline{\mathrm{D}}_\Gamma\alpha$, $\overline{\mathrm{C}}_\Gamma\alpha$, and $\overline{\mathrm{E}}_\Gamma\alpha$, then the proof of the thesis follows directly from Definition 5 and the definition of the relations $\sim_i$, $\sim^D_\Gamma$, $\sim^C_\Gamma$, and $\sim^E_\Gamma$ respectively.

It remains to prove that the thesis holds for formulas of the form $\mathrm{E}(\alpha \mathrm{U}_I \beta)$, and $\mathrm{E}(\alpha \mathrm{R}_I \beta)$.

Consider a formula of the form $\mathrm{E}(\alpha \mathrm{U}_I \beta)$ and suppose that $M, q \models \mathrm{E}(\alpha \mathrm{U}_I \beta)$. By Definition 5 we have that for some run $\rho \in f_{\mathcal{A}}(q)$ there exists $r \in I$ such that

$$M, \pi_\rho(r) \models \beta \text{ and } (\forall r' < r)\ M, \pi_\rho(r') \models \alpha$$

By Lemma 5 there exists a run $\rho' \in f_{\mathcal{A}}(q')$ such that for every $r \in \mathbb{R}$, $\pi_\rho(r) \cong \pi_{\rho'}(r)$. Thus, by the induction hypotheses $M, \pi_{\rho'}(r) \models \beta$ and $(\forall r' < r)\ M, \pi_{\rho'}(r') \models \alpha$. Hence it follows that $M, q' \models \mathrm{E}(\alpha \mathrm{U}_I \beta)$.

The proof of the case $\mathrm{E}(\alpha \mathrm{R}_I \beta)$ is analogous. □

Lemma 7 ([19]). *For every state (l, v) in M with $v \in \mathbb{R}^X$ there exists at least one state (l, u) in M_d with $u \in D^X$ such that $u \cong v$.*

The following two lemmas guarantee that for each run in M we can construct an equivalent run (path) in M_d.

Lemma 8 ([19]). *Let $v \in \mathbb{R}^X$ be a clock valuation, $\delta \in \mathbb{R}$, and $m \in \mathbb{N}$. Then for each $u \in D^X_m$ such that $u \cong v$ there exists $\delta' \in E_{m+1}$ such that $v + \delta \cong u + \delta'$. Moreover, $u + \delta' \in D^X_{m+1}$.*

We are now ready to show that validity of the TECTLK formula φ over the model for $\mathcal{A}$ is equivalent to the validity of $\mathrm{cr}(\varphi)$ over the discretised model for $\mathcal{A}_\varphi$ with the extended valuation function.

Lemma 9. *Let φ be a* TECTLK *formula, M a model, and M_d the discretised version of M. Further, let $(l,v)\lfloor X \stackrel{def}{=} (l, v\lfloor X)$. For any state $q = (l,v) \in Q$ there exists $s = (l,v') \in S$ such that $(l,v')\lfloor X \cong (l,v)$ and $M, q \models \varphi$ iff $M_d, s \models \mathrm{cr}(\varphi)$.*

Proof [Induction on the length of formulae]
("Left-to-right") It is obvious that the thesis holds for all the propositional variables and their negations. Next, assume that the hypothesis holds for all the proper sub-formulae of φ. If φ is equal to either $\alpha \wedge \beta$ or $\alpha \vee \beta$, then it is easy to check that the lemma holds. Consider φ to be of the following forms:

- $\varphi = \mathrm{E}(\alpha \mathrm{U}_I \beta)$. By Definition 5, we have that $M, q \models \mathrm{E}(\alpha \mathrm{U}_I \beta)$ if

$$(\exists\, \rho \in f_{\mathcal{A}}(q))(\exists r \in I)[M, \pi_\rho(r) \models \beta \text{ and } (\forall r' < r)\ M, \pi_\rho(r') \models \alpha] \tag{1}$$

  By the definition of run we have that ρ must be of the following form:

$$(l_0, v_0) \xrightarrow{\delta_0} (l_0, v_0) + \delta_0 \xrightarrow{\sigma_0} (l_1, v_1) \xrightarrow{\delta_1} (l_1, v_1) + \delta_1 \xrightarrow{\sigma_1} (l_2, v_2) \xrightarrow{\delta_2} \dots \tag{2}$$

  where $(l_0, v_0) = q$, $\delta_i \in \mathbb{R}_+$, for all $i \geq 0$. Since ρ is progressive, we have that $r = \sum_{j=0}^{i-1} \delta_j + \delta$ for some $0 \leq \delta < \delta_i$ and $i \geq 0$. Consider the following "augmented run" ρ^*:

$$(l_0, v_0^*) \xrightarrow{\delta_0} (l_0, v_0^*) + \delta_0 \xrightarrow{\sigma_0} (l_1, v_1^*) \xrightarrow{\delta_1} (l_1, v_1^*) + \delta_1 \xrightarrow{\sigma_1} (l_2, v_2^*) \xrightarrow{\delta_2} \dots \tag{3}$$

  where $(\forall i \geq 0)(\forall x \in X' \setminus \{y\})\ v_i^*(x) = v_i(x)$, and $v_0^*(y) = 0$ and $(\forall i > 0)$, $v_i^*(y) = \sum_{j=0}^{i-1} \delta_j$. ρ^* is a run of $\mathcal{A}_\varphi$ (i.e., a run of the model for $\mathcal{A}_\varphi$). Further, since the clock y cannot be reset along ρ^*, it is easy to observe that $r = v_i^*(y) + \delta$ for some $0 \leq \delta < \delta_i$ and $i \geq 0$, which implies that $p_{y \in I} \in \widetilde{\mathcal{V}}(\pi_{\rho^*}(r))$.
  By lemma 8 and lemma 4 we have that there exists run ρ'

$$(l_0, v_0') \xrightarrow{\delta_0'} (l_0, v_0') + \delta_0' \xrightarrow{\sigma_0} (l_1, v_1') \xrightarrow{\delta_1'} (l_1, v_1') + \delta_1' \xrightarrow{\sigma_1} (l_2, v_2') \xrightarrow{\delta_2'} \dots \tag{4}$$

  equivalent to ρ^* such that for each $i \geq 0$, $v_i' \cong v_i^*$, $v_i' + \delta_i' \cong v_i^* + \delta_i$, and (l_i, v_i') and $(l_i, v_i') + \delta_i'$ are states in M_d. This implies that for $r' = \sum_{j=0}^{i-1} \delta_j' + \delta'$, where $0 \leq \delta' < \delta_i'$ and $\delta' \in E$, we have $\pi_{\rho^*}(r) \cong \pi_{\rho'}(r')$. Further, by Lemma 6 and (1) we have that $p_{y \in I} \in \widetilde{\mathcal{V}}(\pi_{\rho'}(r'))$, $M, \pi_{\rho'}(r') \models \beta$ and $(\forall r'' < r')\ M, \pi_{\rho'}(r'') \models \alpha$.
  Take now the following path π:

$$\begin{gathered}
(l_0, v_0'), (l_0, v_0') + {\delta'}_0^1, \dots, (l_0, v_0') + {\delta'}_0^{n_0}, (l_1, v_1'), \\
(l_1, v_1') + {\delta'}_1^1, \dots, (l_1, v_1') + {\delta'}_1^{n_1}, (l_2, v_2'), \dots, \\
\dots \\
(l_{i-1}, v_{i-1}') + {\delta'}_{i-1}^1, \dots, (l_{i-1}, v_{i-1}') + {\delta'}_{i-1}^{n_{i-1}}, (l_i, v_i'), \dots, \\
(l_i, v_i') + {\delta'}_i^1, \dots, (l_i, v_i') + {\delta'}_i^{n_{\delta'}}, \dots, (l_i, v_i') + {\delta'}_i^{n_i}, (l_{i+1}, v_{i+1}'), \dots
\end{gathered} \tag{5}$$

with $\delta'_i = \sum_{j=0}^{n_i} {\delta'}_i^j$, ${\delta'}_i^j \in (0,1)$, and for all $j \in \{0,\ldots,n_i-1\}$ either $(l_i, v'_i + {\delta'}_i^j) \cong (l_i, v'_i + {\delta'}_i^{j+1})$ or $(l_i, v'_i + \delta_i^j) \overset{{\delta'}_i^{j+1}-{\delta'}_i^j}{\rightarrow}_d (l_i, v'_i + {\delta'}_i^{j+1})$, and $\pi(k) = \pi_{\rho'}(r')$ for

$$k = \begin{cases} \sum_{j=0}^{i-1} n_j, & \delta' = 0 \\ \sum_{j=0}^{i-1} n_j + n_{\delta'}, & \delta' > 0 \end{cases}$$

By the construction of the path π, we have that π is a valid path of M_d and $p_{y\in I} \in \widetilde{\mathcal{V}}_d(\pi(k))$ (note that $p_{y\in I} \in \widetilde{\mathcal{V}}(\pi_{\rho'}(r'))$). Now consider two cases: $\pi_\rho(r')$ is boundary and $\pi_{\rho'}(r)$ is not.

Let first assume that $\pi_{\rho'}(r')$ is boundary. Then, by the definition of the valuation function $\widetilde{\mathcal{V}}_d$ we have that $p_b \in \widetilde{\mathcal{V}}_d(\pi(k))$. Further, since (1) holds, by the induction assumption, the construction of π and Lemma 6, we have that $M_d, \pi(k) \models \mathrm{cr}(\beta)$ and $M_d, \pi(j) \models \mathrm{cr}(\alpha)$ for all $j < k$. We have to now show that there exists state $s \in S$ such that $s \rightarrow_y \pi(0)$. It is enough to take $s = (l_0, v')$ such that $v' \restriction X = v'_0 \restriction X$. Therefore, by the definition of the satisfaction relation for ECTLK$_y$ formulae, we conclude that $M_d, s \models \mathrm{cr}(\varphi)$.

Assume now that $\pi_{\rho'}(r')$ is not boundary. Since interval I is of the form $[a,b]$, $[a,b)$, $(a,b]$, (a,b), $[a,\infty)$, or (a,∞) for $a,\ b \in \mathbb{N}$, we have that there exists $r'' < r'$ such that $\pi_{\rho'}(r'') \cong \pi_{\rho'}(r')$. Further, since (1) holds, by Lemma 6 we have that $M, \pi_{\rho'}(r') \models \alpha$. Further, by the induction assumption and the construction of π we have that $M_d, \pi(k) \models \mathrm{cr}(\beta)$ and $M_d, \pi(j) \models \mathrm{cr}(\alpha)$ for all $j \leq k$. We have to now show that there exists state $s \in S$ such that $s \rightarrow_y \pi(0)$. It is enough to take $s = (l_0, v')$ such that $v' \restriction X = v'_0 \restriction X$. Therefore, by the definition of the satisfaction relation for ECTLK$_y$ formulae, we conclude that $M_d, s \models \mathrm{cr}(\varphi)$.

- $\varphi = \mathrm{E}(\alpha \mathrm{R}_I \beta)$. The proof is similar to the above case.
- $\varphi = \overline{\mathrm{K}}_i \alpha$. By Definition 5, we have that $M, q \models \overline{\mathrm{K}}_i \alpha$ iff

$$(\exists q' \in Q)(q \sim_i q' \text{ and } M, q' \models \alpha) \tag{6}$$

Let $s' = (l, v') \in S$ be a state such that $s' \restriction X \cong q'$. By Lemma 6 and (6) we have that $M, s' \restriction X \models \alpha$. Thus, by induction we have that

$$M_d, s' \models \mathrm{cr}(\alpha) \tag{7}$$

Now, let $s = (l, v) \in S$ be a state such that $s \restriction X \cong q$ and $v(y) = v'(y)$. It is easy to see that $s \sim_i s'$. Thus by Definition 7, the definition of cr, and (7) we have that $M_d, s \models \mathrm{cr}(\overline{\mathrm{K}}_i \alpha)$.

- $\varphi = \overline{\mathrm{D}}_I \alpha$. The proof is similar to the case for $\overline{\mathrm{K}}_i$.
- $\varphi = \overline{\mathrm{E}}_I \alpha$. The proof is similar to the case for $\overline{\mathrm{K}}_i$.
- $\varphi = \overline{\mathrm{C}}_I \alpha$. The proof is similar to the case for $\overline{\mathrm{K}}_i$.

("Right-to-left") It is obvious that the thesis holds for all the propositional variables and their negations. Next, assume that the hypothesis holds for all the proper sub-formulae of φ. If φ is equal to either $\alpha \wedge \beta$ or $\alpha \vee \beta$, then it is easy to check that the lemma holds. Consider φ to be of the following forms:

- $\varphi = \mathrm{cr}(\mathrm{E}(\alpha \mathrm{U}_I \beta))$. Let $q = (l, v) \in Q$ and $s = (l, v') \in S$ and $(l, v') \downharpoonright X \cong (l, v)$. Let assume that $M_d, s \models \mathrm{E}_y(\mathrm{cr}(\alpha)\mathrm{U}(\mathrm{cr}(\beta) \wedge p_{y \in I_i} \wedge (p_b \vee \mathrm{cr}(\alpha))))$. By the definition of the satisfaction relation for ECTLK$_y$ formulae, we have that

$$(\exists s' \in S)(s \rightarrow_y s' \text{ and } (\exists \pi \in \Pi(s'))(\exists m \geq 0) \tag{8}$$
$$[M_d, \pi(m) \models (\mathrm{cr}(\beta) \wedge p_{y \in I} \wedge (p_b \vee \mathrm{cr}(\alpha)))\text{and } (\forall j < m)\ M_d, \pi(j) \models \mathrm{cr}(\alpha)])$$

Observe that π is of the following form:

$$\begin{gathered}(l_0, v'_0), (l_0, v'_0) + {\delta'}_0^1, \ldots, (l_0, v'_0) + {\delta'}_0^{n_0}, (l_1, v'_1), \\ (l_1, v'_1) + {\delta'}_1^1, \ldots, (l_1, v'_1) + {\delta'}_1^{n_1}, (l_2, v'_2), \ldots, \\ \ldots \\ (l_{i-1}, v'_{i-1}) + {\delta'}_{i-1}^1, \ldots, (l_{i-1}, v'_{i-1}) + {\delta'}_{i-1}^{n_{i-1}}, (l_i, v'_i), \ldots, \\ (l_i, v'_i) + {\delta'}_i^1, \ldots, (l_i, v'_i) + {\delta'}_i^{n_{\delta'}}, \ldots, (l_i, v'_i) + {\delta'}_i^{n_i}, (l_{i+1}, v'_{i+1}), \ldots\end{gathered} \tag{9}$$

such that ${\delta'}_i^j \in (0, 1)$, for all $j \in \{0, \ldots, n_i - 1\}$ either $(l_i, v'_i + {\delta'}_i^j) \cong (l_i, v'_i + {\delta'}_i^{j+1})$ or $(l_i, v'_i + \delta_i^j) \overset{{\delta'}_i^{j+1} - {\delta'}_i^j}{\rightarrow}_d (l_i, v'_i + {\delta'}_i^{j+1})$, $v'_0(y) = 0$, $(\forall i > 0)$, $v'_i(y) = \sum_{j=0}^{i-1} \sum_{t=1}^{n_i} \delta_j^t$.
Consider the following "augmented" run ρ':

$$(l_0, v'_0) \overset{\delta'_0}{\rightarrow} (l_0, v'_0) + \delta'_0 \overset{\sigma_0}{\rightarrow} (l_1, v'_1) \overset{\delta'_1}{\rightarrow} (l_1, v'_1) + \delta'_1 \overset{\sigma_1}{\rightarrow} (l_2, v'_2) \overset{\delta'_2}{\rightarrow} \ldots \tag{10}$$

where $\delta'_i = \sum_{j=0}^{n_i} {\delta'}_i^j$ for $i \geq 0$. Next, take the following run ρ:

$$(l_0, v_0) \overset{\delta'_0}{\rightarrow} (l_0, v_0) + \delta'_0 \overset{\sigma_0}{\rightarrow} (l_1, v_1) \overset{\delta'_1}{\rightarrow} (l_1, v_1) + \delta'_1 \overset{\sigma_1}{\rightarrow} (l_2, v_2) \overset{\delta'_2}{\rightarrow} \ldots \tag{11}$$

where for all $i \geq 0$, $v_i = v'_i \downharpoonright X$, and associate with ρ a dense path $\pi_\rho : \mathbb{R} \rightarrow Q$ such that $\pi_\rho(r) = (l_i, v_i) + \delta$, $0 \leq \delta \leq \delta'_i$, and $r = \sum_{j=0}^{i-1} \delta'_j + \delta$.
Moreover, assume that $\pi(m) \cong \pi_\rho(r_m)$ for some $r_m = \sum_{j=0}^{i-1} \delta'_j + \delta$ and $0 \leq \delta \leq \delta'_i$. Since (8) holds, by the construction of the run ρ, the inductive assumption, and Lemma 6 we have that

$$M, \pi_\rho(r_m) \models \beta \wedge p_{y \in I} \wedge (p_b \vee \alpha) \tag{12}$$

and for all $r' \leq r_{m-1}$ with $\pi_\rho(r_{m-1}) \cong \pi(m-1)$

$$M, \pi_\rho(r') \models \alpha \tag{13}$$

Since (12) holds, we have that $p_{y \in I} \in \widetilde{V}(\pi_\rho(r_m))$. This implies that $r_m \in I$. So, to conclude that $M, q \models \mathrm{E}(\alpha \mathrm{U}_I \beta)$, it remains to show that for all $r_{m-1} < r'' < r_m$, $M, \pi_\rho(r'') \models \alpha$ holds.
Consider the following two cases:

- Let $M, \pi_\rho(r_m) \models \alpha$. Then, by the construction of the run ρ, we have that for all $r_{m-1} < r'' < r_m$ either $\pi_\rho(r_m) \cong \pi_\rho(r'')$ or $\pi_\rho(r_{m-1}) \cong \pi_\rho(r'')$. Since $M, \pi_\rho(r_m) \models \alpha$ and Condition (13) and Lemma 6 hold, we have that for all $r_{m-1} < r'' < r_m$, $M, \pi_\rho(r'') \models \alpha$.

– Let $M, \pi_\rho(r_m) \models p_b$. Then, by the construction of the run ρ, we have that for all $r_{m-1} < r'' < r_m$, $\pi_\rho(r_{m-1}) \cong \pi_\rho(r'')$. Since Condition (13) and Lemma 6 hold, we have that for all $r_{m-1} < r'' < r_m$, $M, \pi_\rho(r'') \models \alpha$.

Therefore, we conclude that $M, q \models \mathrm{E}(\alpha \mathrm{U}_I \beta)$.

- $\varphi = \mathrm{cr}(\underline{\mathrm{E}}(\alpha \mathrm{R}_I \beta))$. The proof is similar to the EU_I case.
- $\varphi = \mathrm{cr}(\overline{\mathrm{K}}_i \alpha)$. Let $q = (l, v) \in Q$ and $s = (l, v') \in S$ and $(l, v') \downharpoonright X \cong (l, v)$. Let assume that $M_d, s \models \mathrm{cr}(\overline{\mathrm{K}}_i \alpha)$. By the definition of the satisfaction relation for ECTLK_y formulae, we have that

$$(\exists \pi \in \Pi(s^0))(\exists j \geq 0)(M_d, \pi(j) \models \mathrm{cr}(\alpha) \text{ and } s \sim_i^d \pi(j)), \tag{14}$$

  By induction we have that $M, \pi(j) \downharpoonright X \models \alpha$. Since $s \sim_i^d \pi(j)$, we have that $s \downharpoonright X \sim_i \pi(j) \downharpoonright X$. Next, since $s \downharpoonright X \cong q$, we have that $s \downharpoonright X \sim_i q$. Therefore, we have that $q \sim_i \pi(j) \downharpoonright X$. Thus, we conclude that $M, q \models \overline{\mathrm{K}}_i \alpha$.
- The cases for $\varphi = \mathrm{cr}(\overline{\mathrm{D}}_\Gamma \alpha)$, $\varphi = \mathrm{cr}(\overline{\mathrm{E}}_\Gamma \alpha)$, and $\varphi = \mathrm{cr}(\overline{\mathrm{C}}_\Gamma \alpha)$ can be proven similarly to the case $\overline{\mathrm{K}}_i$.

□

4.3 ECTLK_y Bounded Model Checking

All the known BMC techniques are based on so called $k-$bounded semantics. In particular, BMC for ECTLK_y is based on the $k-$bounded semantics for ECTLK_y, the definition of which we present below.

Bounded Semantics We start with some auxiliary notions. Let $M_d = (\Sigma \cup E, S, s^0, \rightarrow_d, \sim_1^d, \ldots, \sim_m^d, \widetilde{\mathcal{V}}_d)$ be a discretised model, and $k \in \mathbb{N}_+$ a bound. As before, we denote by $\rightarrow_{\mathcal{A}}$ the part of $\rightarrow_d$, where transitions are labelled with elements of $\Sigma \cup E$, and by $\rightarrow_y$ the transitions that reset the clock y. A *$k-$path* π in M_d is a finite sequence of states $(s_0, \ldots, s_k)$ such that $s_i \rightarrow_{\mathcal{A}} s_{i+1}$ for each $0 \leq i < k$, and $\Pi_k(s)$ denotes the set of all the k-paths starting at s in M_d. A *k-model* for M_d is a structure $M_k = (\Sigma \cup E, S, s^0, P_k, P_y, \sim_1^d, \ldots, \sim_m^d, \widetilde{\mathcal{V}}_d)$, where $P_k = \bigcup_{s \in S} \Pi_k(s)$ and $P_y = \{(s, s') \mid s \rightarrow_y s' \text{ and } s, s' \in S\}$.

The satisfaction of the temporal operator $\mathrm{E}_y \mathrm{R}$ on a k-path in the bounded case depends on whether or not π represents a loop. To indicate k-paths that can simulate loops, we define a function $loop : P_k \mapsto 2^{\mathbb{N}}$ by $loop(\pi) = \{i \mid 0 \leq i \leq k \text{ and } \pi(k) \rightarrow_{\mathcal{A}} \pi(i)\}$.

We can now define a bounded semantics for ECTLK_y formulae. Let $k \in \mathbb{N}_+$, M_d be a discretised model, M_k its k-model, and α, β ECTLK_y formulae. Further, let $M_k, s \models \alpha$ denote that α is true at the state s of M_k. The (bounded) satisfaction relation $\models$ is defined as follows:

$$\begin{array}{ll}
M_k, s \models p & \text{iff } p \in \widetilde{\mathcal{V}}_d(s), \\
M_k, s \models \neg p & \text{iff } p \notin \widetilde{\mathcal{V}}_d(s), \\
M_k, s \models \alpha \vee \beta & \text{iff } M_k, s \models \alpha \text{ or } M_k, s \models \beta, \\
M_k, s \models \alpha \wedge \beta & \text{iff } M_k, s \models \alpha \text{ and } M_k, s \models \beta, \\
M_k, s \models \overline{\mathrm{K}}_i \alpha & \text{iff } (\exists_{\pi \in \Pi_k(s^0)})(\exists_{0 \leq j \leq k})(M_k, \pi(j) \models \alpha \text{ and } s \sim_i \pi(j)),
\end{array}$$

$M_k, s \models \overline{\mathrm{D}}_\Gamma \alpha$ iff $(\exists_{\pi \in Pi_k(s^0)})(\exists_{0 \le j \le k})(M_k, \pi(j) \models \alpha$ and $s \sim^D_\Gamma \pi(j))$,
$M_k, s \models \overline{\mathrm{E}}_\Gamma \alpha$ iff $(\exists_{\pi \in \Pi_k(s^0)})(\exists_{0 \le j \le k})(M_k, \pi(j) \models \alpha$ and $s \sim^E_\Gamma \pi(j))$,
$M_k, s \models \overline{\mathrm{C}}_\Gamma \alpha$ iff $(\exists_{\pi \in \Pi_k(s^0)})(\exists_{0 \le j \le k})(M_k, \pi(j) \models \alpha$ and $s \sim^C_\Gamma \pi(j))$,
$M_k, s \models \mathrm{E}_y(\alpha \mathrm{U} \beta)$ iff $(\exists s' \in S)((s, s') \in P_y$ and $(\exists \pi \in \Pi_k(s'))(\exists_{0 \le j \le k})$
$(M_k, \pi(j) \models \beta$ and $(\forall_{0 \le i < j})\ M_k, \pi(i) \models \alpha))$,
$M_k, s \models \mathrm{E}_y(\alpha \mathrm{R} \beta)$ iff $(\exists s' \in S)((s, s') \in P_y$ and $(\exists \pi \in \Pi_k(s'))[(\exists_{0 \le j \le k})$
$(M_k, \pi(j) \models \alpha$ and $(\forall_{0 \le i \le j}) M_k, \pi(i) \models \beta)$ or
$(\forall_{0 \le j \le k})(M_k, \pi(j) \models \beta$ and $loop(\pi) \neq \emptyset)])$.

Definition 9. *An* ECTLK$_y$ *formula* φ *is* valid in a k-model M_k *(denoted* $M_d \models_k \varphi$*) iff* $M_k, s^0 \models \varphi$*, i.e.,* φ *is true at the initial state of the k-model* M_k*.*

We can now describe how the model checking problem ($M_d \models \varphi$) can be reduced to the bounded model checking problem ($M_d \models_k \varphi$).

Theorem 1. *Let* $k \in \mathbb{N}_+$*,* M_d *be a discretised model,* M_k *its k-model, and* φ *an* ECTLK$_y$ *formula. For any s in* M_d*,* $M_k, s \models \varphi$ *implies* $M_d, s \models \varphi$*.*
Proof By straightforward induction on the length of φ. □

Note that both the discretised model and its k-model are infinite. So, to perform bounded model checking we have to consider a finite submodels of a k-model such that an ECTLK$_y$ formula ψ holds in M_d if and only if ψ holds in a finite submodel of M_k.

Definition 10. *A* s-submodel *of k-model* $M_k = (\Sigma \cup E, S, s^0, P_k, P_y, \sim^d_1, \ldots, \sim^d_m, \widetilde{\mathcal{V}}_d)$ *is a tuple* $M'(s) = (\Sigma \cup E, S', s, P'_k, P'_y, \sim'_1, \ldots, \sim'_m, \widetilde{\mathcal{V}}'_d)$*, such that* $P'_k \subseteq P_k$*,* $S' = \{r \in S \mid (\exists \pi \in P'_k)(\exists i \le k)\pi(i) = r\} \cup \{s\}$*,* $P'_y \subseteq P_y \cap (S' \times S')$*,* $\sim'_i = \sim^d_i \cap (S' \times S')$ *for each* $i \in \{1, \ldots, m\}$*, and* $\widetilde{\mathcal{V}}'_d = \widetilde{\mathcal{V}}_d \downharpoonright S'$*.*

The bounded semantics for ECTLK$_y$ over a submodel $M'(s)$ is defined as for M_k. Moreover, the following theorem holds.

We will now introduce a definition of a function f_k that gives a bound on the number of k-paths in the submodel $M'(s)$, and a function $f_{k,y}$ that gives a bound on the number of elements of the set P'_y in the submodel $M'(s)$. We will show later that these bound guarantee that the validity of ψ in $M'(s)$ is equivalent to the validity of ψ in M_k. The function f_k : ECTLK$_y \to \mathbb{N}$ is defined by:

- $f_k(p) = f_k(\neg p) = 0$, where $p \in \mathcal{PV}'$,
- $f_k(\alpha \vee \beta) = max\{f_k(\alpha), f_k(\beta)\}$,
- $f_k(\alpha \wedge \beta) = f_k(\alpha) + f_k(\beta)$,
- $f_k(\mathrm{E}_y(\alpha \mathrm{U} \beta)) = k \cdot f_k(\alpha) + f_k(\beta) + 1$,
- $f_k(\mathrm{E}_y(\alpha \mathrm{R} \beta)) = (k+1) \cdot f_k(\beta) + f_k(\alpha) + 1$,
- $f_k(Y\alpha) = f_k(\alpha) + 1$, for $Y \in \{\overline{\mathrm{K}}_i, \overline{\mathrm{D}}_\Gamma, \overline{\mathrm{E}}_\Gamma\}$,
- $f_k(\overline{\mathrm{C}}_\Gamma \alpha) = f_k(\alpha) + k$.

The function $f_{k,y}$: ECTLK$_y \to \mathbb{N}$ is defined by:

- $f_{k,y}(p) = f_{k,y}(\neg p) = 0$, where $p \in \mathcal{PV}'$,
- $f_{k,y}(\alpha \vee \beta) = max\{f_{k,y}(\alpha),\ f_{k,y}(\beta)\}$,

- $f_{k,y}(\alpha \wedge \beta) = f_{k,y}(\alpha) + f_{k,y}(\beta)$,
- $f_{k,y}(\mathrm{E}_y(\alpha \mathrm{U} \beta)) = k \cdot f_{k,y}(\alpha) + f_{k,y}(\beta) + 1$,
- $f_{k,y}(\mathrm{E}_y(\alpha \mathrm{R} \beta)) = (k+1) \cdot f_{k,y}(\beta) + f_{k,y}(\alpha) + 1$,
- $f_{k,y}(Y\alpha) = f_{k,y}(\alpha)$, for $Y \in \{\overline{\mathrm{K}}_i, \overline{\mathrm{D}}_\Gamma, \overline{\mathrm{E}}_\Gamma, \overline{\mathrm{C}}_\Gamma\}$.

Lemma 10. *Let $M'(s)$ and $M''(s)$ be two submodels of M_k with $P'_k \subseteq P''_k$, $P'_y \subseteq P''_y$, and ψ an* ECTLK$_y$ *formula. If $M'(s) \models_k \psi$, then $M''(s) \models_k \psi$.*

Proof By straightforward induction on the length of ψ. □

Lemma 11. *$M_k, s \models \psi$ iff there is a submodel $M'(s)$ of M_k with $|P'_k| \leq f_k(\psi)$ and $|P'_y| \leq f_{k,y}(\psi)$ such that $M'(s), s \models \psi$.*

Proof The 'right-to-left' implication is straightforward. To prove 'left-to-right' implication, we will use induction on the length of ψ.

The 'left-to-right' implication follows directly for the propositional variables and their negations. Assume that the hypothesis holds for all the proper sub-formulae of ψ, and consider the following cases:

- Let $\psi = \alpha \vee \beta$ and $M_k, s \models \alpha \vee \beta$. By the definition of the bounded semantics we have that $M_k, s \models \alpha$ or $M_k, s \models \beta$. Hence, by induction we have that there is a submodel $M'(s)$ of M_k such that $M'(s), s \models \alpha$ and $|P'_k| \leq f_k(\alpha)$ and $|P'_y| \leq f_{k,y}(\alpha)$, or there is a submodel $M''(s)$ of M_k such that $M''(s), s \models \beta$ and $|P''_k| \leq f_k(\beta)$ and $|P''_y| \leq f_{k,y}(\beta)$. Now, consider a submodel $M'''(s)$ of M_k such that $P'''_k = P'_k$ and $P'''_y = P'_y$ if $M'(s), s \models \alpha$, $P'''_k = P''_k$ and $P'''_y = P''_y$ otherwise. Thus, $|P'''_k| \leq max\{f_k(\alpha), f_k(\beta)\}$ and $|P'''_y| \leq max\{f_{k,y}(\alpha), f_{k,y}(\beta)\}$. It is obvious that $M'''(s), s \models \alpha$ or $M'''(s), s \models \beta$. Therefore, by the definition of the bounded semantics we have that $M'''(s), s \models \alpha \vee \beta$.
- Let $\psi = \alpha \wedge \beta$ and $M_k, s \models \alpha \wedge \beta$. By the definition of the bounded semantics we have that $M_k, s \models \alpha$ and $M_k, s \models \beta$. Hence, by induction we have that there is a submodel $M'(s)$ of M_k such that $M'(s), s \models \alpha$ and $|P'_k| \leq f_k(\alpha)$ and $|P'_y| \leq f_{k,y}(\alpha)$, and there is a submodel $M''(s)$ of M_k such that $M''(s), s \models \beta$ and $|P''_k| \leq f_k(\beta)$ and $|P''_y| \leq f_{k,y}(\beta)$. Now, consider the submodel $M'''(s)$ of M_k such that $P'''_k = P'_k \cup P''_k$ and $P'''_y = P'_y \cup P''_y$. It is easy to observe that $|P'''_k| \leq f_k(\alpha) + f_k(\beta)$ and $|P'''_y| \leq f_{k,y}(\alpha) + f_{k,y}(\beta)$. So, by Lemma 10, we have that $M'''(s), s \models \alpha$ and $M'''(s), s \models \beta$. Therefore, by the definition of the bounded semantics we have that $M'''(s), s \models \alpha \wedge \beta$.
- Let $\psi = \mathrm{E}_y(\alpha \mathrm{U} \beta)$ and $M_k, s \models \mathrm{E}_y(\alpha \mathrm{U} \beta)$. By the definition of the bounded semantics, there is a state $s' \in S$ such that $(s, s') \in P_y$ and there is a $k-$path $\pi \in \Pi_k(s')$ such that

$$(\exists 0 \leq m \leq k)(M_k, \pi(m) \models \beta \text{ and } (\forall 0 \leq i < m) M_k, \pi(i) \models \alpha) \tag{15}$$

  Hence, by the inductive assumption, for all i such that $0 \leq i < m$ there are submodels $M^i(\pi(i))$ of M_k with $|P^i_k| \leq f_k(\alpha)$ and $|P^i_y| \leq f_{k,y}(\alpha)$ and

$$M^i(\pi(i)), \pi(i) \models \alpha \tag{16}$$

  and there is a submodel $M^m(\pi(m))$ of M_k with $|P^m_k| \leq f_k(\beta)$ and $|P^m_y| \leq f_{k,y}(\beta)$ and

$$M^m(\pi(m)), \pi(m) \models \beta \tag{17}$$

Consider a submodel $M'(s)$ of M_k such that $P'_k = \bigcup_{i=0}^{m} P^i_k \cup \{\pi\}$ and $P'_y = \bigcup_{i=0}^{m} P^i_y \cup \{(s, s')\}$. Thus, by the construction of $M'(s)$, we have that $(s, s') \in P'_y$ and $\pi \in P'_k$. Therefore, since conditions (15), (16), and (17) hold, by the definition of the bounded semantics, we have that $M', s \models \mathrm{E}_y(\alpha \mathrm{U} \beta)$ and $|P'_k| \leq k \cdot f_k(\alpha) + f_k(\beta) + 1$ and $|P'_y| \leq k \cdot f_{k,y}(\alpha) + f_{k,y}(\beta) + 1$.

- Let $\psi = \mathrm{E}_y(\alpha \mathrm{R} \beta)$ and $M_k, s \models \mathrm{E}_y(\alpha \mathrm{R} \beta)$. By the definition of the bounded semantics, there is a state $s' \in S$ such that $(s, s') \in P_y$ and there is a $k-$path $\pi \in \Pi_k(s')$ such that

$$(\exists 0 \leq j \leq k)(M_k, \pi(j) \models \alpha \text{ and } (\forall 0 \leq i \leq j) M_k, \pi(i) \models \beta) \text{ or} \tag{18}$$

$$(\forall 0 \leq j \leq k)(M_k, \pi(j) \models \beta \text{ and } loop(\pi) \neq \emptyset) \tag{19}$$

Let us consider the two cases. First, assume that condition (18) holds. Then, by the inductive assumption, for all i such that $0 \leq i \leq j$ there are submodels $M^i(\pi(i))$ of M_k with $|P^i_k| \leq f_k(\beta)$ and $|P^i_y| \leq f_{k,y}(\beta)$ and

$$M^i(\pi(i)), \pi(i) \models \beta \tag{20}$$

and there is a submodel $M^{''}(\pi(m))$ of M_k with $|P^{''}_k| \leq f_k(\alpha)$ and $|P^{''}_y| \leq f_{k,y}(\alpha)$ and

$$M^{''}(\pi(m)), \pi(m) \models \alpha \tag{21}$$

Consider the submodel $M'(s)$ of M_k such that $P'_k = \bigcup_{i=0}^{j} P^i_k \cup P^{''}_k \cup \{\pi\}$ and $P'_y = \bigcup_{i=0}^{j} P^i_y \cup P''_y \cup \{(s, s')\}$. Thus, by the construction of $M'(s)$, we have that $(s, s') \in P'_y$ and $\pi \in P'_k$. Therefore, since the conditions (18), (20) and (21) hold, by the definition of the bounded semantics we have that $M'(s), s \models \mathrm{E}_y(\alpha \mathrm{R} \beta)$ and $|P'_k| \leq (k+1) \cdot f_k(\beta) + f_k(\alpha) + 1$ and $|P'_y| \leq (k+1) \cdot f_{k,y}(\beta) + f_{k,y}(\alpha) + 1$.
Assume now that condition (19) holds. Then, by the inductive assumption, for all j such that $0 \leq j \leq k$ there are submodels $M^j(\pi(j))$ of M_k with $|P^j_k| \leq f_k(\beta)$ and $|P^j_y| \leq f_{k,y}(\beta)$ and

$$(M^j(\pi(j)), \pi(j) \models \beta) \tag{22}$$

Consider the submodel $M'(s)$ of M_k such that $P'_k = \bigcup_{j=0}^{k} P^j_k \cup \{\pi\}$ and $P'_y = \bigcup_{i=0}^{k} P^i_y \cup \{(s, s')\}$. Thus, by the construction of $M'(s)$, we have that $(s, s') \in P'_y$ and $\pi \in P'_k$. Therefore, since conditions (18) and (22) hold, by the definition of the bounded semantics we have that $M'(s), s \models \mathrm{E}_y(\alpha \mathrm{R} \beta)$ and $|P'_k| \leq (k+1) \cdot f_k(\beta) + f_k(\alpha) + 1$ and $|P'_y| \leq (k+1) \cdot f_{k,y}(\beta) + f_{k,y}(\alpha) + 1$.

- Let $\psi = \overline{\mathrm{K}}_i \alpha$ and $M_k, s \models \overline{\mathrm{K}}_i \alpha$. By the definition of the bounded semantics, we have that there exists $\pi \in \Pi_k(s^0)$ such that

$$(\exists 0 \leq j \leq k)(s \sim_i \pi(j) \text{ and } \pi(j) \models \alpha) \tag{23}$$

By the inductive assumption there is a submodel $M'(\pi(j))$ of M_k with $|P'_k| \leq f_k(\alpha)$ and $|P'_y| \leq f_{k,y}(\alpha)$ such that $M'(\pi(j)), \pi(j) \models \alpha$. Consider a submodel $M''(s)$ of M_k such that $P''_k = P'_k \cup \{\pi\}$ and $P''_y = P'_y$. Since $\pi \in P''_k$, $s \in S''$, and condition (23) holds, by the construction of $M''(s)$ and the definition of the bounded semantics, we have that $M'', s \models \overline{\mathrm{K}}_i \alpha$ and $|P''_k| \leq f_k(\alpha) + 1$ and $|P''_y| \leq f_{k,y}(\alpha)$.

- Let $\psi = \overline{\mathrm{E}}_\Gamma\alpha$ and $M_k, s \models \overline{\mathrm{E}}_\Gamma\alpha$. By the definition of the bounded semantics, we have that there exists $\pi \in \Pi_k(s^0)$ such that

$$(\exists 0 \leq j \leq k)(M_k, \pi(j) \models \alpha \text{ and } s \sim^E_\Gamma \pi(j)) \tag{24}$$

  By the inductive assumption there is a submodel $M'(\pi(j))$ of M_k with $|P'_k| \leq f_k(\alpha)$ and $|P'_y| \leq f_{k,y}(\alpha)$ such that $M'(\pi(j)), \pi(j) \models \alpha$. Consider a submodel $M''(s)$ of M_k such that $P''_k = P'_k \cup \{\pi\}$ and $P''_y = P'_y$. Since $\pi \in P''_k$, $s \in S''$, and condition (24) holds, by the construction of $M''(s)$ and the definition of the bounded semantics, we have that $M''(s), s \models \overline{\mathrm{E}}_\Gamma\alpha$ and $|P''_k| \leq f_k(\alpha) + 1$ and $|P''_y| \leq f_{k,y}(\alpha)$.
- Let $\psi = \overline{\mathrm{D}}_\Gamma\alpha$ and $M_k, s \models \overline{\mathrm{D}}_\Gamma\alpha$. This case can be proven similarly to the two above.
- Let $\psi = \overline{\mathrm{C}}_\Gamma\alpha$ and $M_k, s \models \overline{\mathrm{C}}_\Gamma\alpha$. Below, we only prove that $f_k(\overline{\mathrm{C}}_\Gamma\alpha) = f_k(\alpha) + k$ is a sufficient number of paths in a submodel $M'(s)$ validating φ and that $f_{k,y}(\overline{\mathrm{C}}_\Gamma\alpha) = f_{k,y}(\alpha)$. The actual construction of $M'(s)$ can be given similarly to the case $\psi = \overline{\mathrm{K}}_i\alpha$ and $\psi = \alpha \vee \beta$.
  Note that $\overline{\mathrm{C}}_\Gamma\alpha = \bigvee_{1\leq i\leq k}(\overline{\mathrm{E}}_\Gamma)^i\alpha$, $f_k((\overline{\mathrm{E}}_\Gamma)^1\alpha) = f_k(\overline{\mathrm{E}}_\Gamma\alpha) = f_k(\alpha)+1$, and $f_{k,y}((\overline{\mathrm{E}}_\Gamma)^1\alpha) = f_{k,y}(\overline{\mathrm{E}}_\Gamma\alpha) = f_{k,y}(\alpha)$. It is easy to show, by induction on i, that $f_k((\overline{\mathrm{E}}_\Gamma)^i\alpha) = f_k(\alpha) + i$ and $f_{k,y}((\overline{\mathrm{E}}_\Gamma)^i\alpha) = f_{k,y}(\alpha)$, for $i \in \{1, \ldots, k\}$. Therefore, $f_k(\psi) = f_k(\bigvee_{1\leq i\leq k}(\overline{\mathrm{E}}_\Gamma)^i\alpha) = max\{f_k((\overline{\mathrm{E}}_\Gamma)^1\alpha), \ldots, f_k((\overline{\mathrm{E}}_\Gamma)^k\alpha)\} = f_k((\overline{\mathrm{E}}_\Gamma)^k\alpha) = f_k(\alpha) + k$, and
  $f_{k,y}(\psi) = f_{k,y}(\bigvee_{1\leq i\leq k}(\overline{\mathrm{E}}_\Gamma)^i\alpha) = max\{f_{k,y}((\overline{\mathrm{E}}_\Gamma)^1\alpha), \ldots, f_{k,y}((\overline{\mathrm{E}}_\Gamma)^k\alpha)\} = f_{k,y}((\overline{\mathrm{E}}_\Gamma)^k\alpha) = f_{k,y}(\alpha)$.

□

From Lemma 11 we can now derive the following.

Corollary 1. *$M_k, s^0 \models \psi$ iff there is a submodel $M'(s^0)$ of M_k with $|P'_k| \leq f_k(\psi)$ and $|P'_y| \leq f_{k,y}(\psi)$ such that $M'(s^0), s^0 \models \psi$.*

Proof It follows from the definition of bounded semantics and Lemma 11, by using $s = s^0$. □

Theorem 2. *Let M_d be a discretised model, and ψ an* ECTLK$_y$ *formula. If there exist $k \in \mathbb{N}_+$ and s^0-submodel $M'(s^0)$ of k-model M_k with $P'_k \leq f_k(\psi)$ and $|P'_{k,y}| \leq f_{k,y}(\psi)$ such that $M'(s^0) \models_k \psi$, then $M_d \models \psi$.*

Proof Follows from Theorem 1 and Lemma 11. □

Having defined the bounded semantics, we can easily translate the model checking problem for ECTLK$_y$ to the problem of satisfiability of a Boolean formula that encodes all the discretised model for an ECTLK$_y$ formula under consideration and an appropriate fragments of the considered discretised models. The translation is presented in the next section.

4.4 Translation to Boolean formulae

The main idea of BMC for ECTLK$_y$ consists in translating the model checking problem for ECTLK$_y$ into the satisfiability problem of a propositional formula. Namely, given an ECTLK$_y$ formula ψ, a discretised model M_d, and a bound $k \in \mathbb{N}_+$, this proposition formula, denoted by $[M_d, \psi]_k$, if of the form: $[M_d^{\psi,s^0}]_k \wedge [\psi]_{M_k}$. The first conjunct represents possible s^0-submodels of M_d that consist of $f_k(\psi)$ $k-$paths of M_d, whereas the second conjunct encodes a number of constraints that must hold on these submodels for ψ to be satisfied. Once this translation is defined, checking satisfiability of an ECTLK$_y$ formula can be done by means of a SAT-checker. In order to define $[M_d, \psi]_k$, we proceed as follows.

Let us assume that each state s of the discretised model M_d is encoded by a bit-vector whose length, say b, depends on the number of locations, the number of clocks, and the bound $k \in \mathbb{N}_+$. So, each state s of M_d can be represented by a vector $w = (w[1], \ldots, w[b])$ (called *global state variable*), where each $w[i]$, for $i = 1, \ldots, b$, is a propositional variable (called state variable). Notice that we distinguish between states s encoded as sequences of 0's and 1's and their representations in terms of propositional variables $w[i]$. A finite sequence $(w_0, \ldots, w_k)$ of global state variables is called a *symbolic k-path*. In general, we need to consider not just one but a number of symbolic k-paths. This number depends on the formula ψ under investigation, and it is returned as the value $f_k(\psi)$ of the function f_k. The j-th symbolic k-path is denoted by $w_{0,j}, \ldots, w_{k,j}$, where $w_{i,j}$ are global state variables for $1 \leq j \leq f_k(\psi)$, $0 \leq i \leq k$. For two global state variables w, w', we define the following propositional formulae:

- $I_s(w)$ is a formula over w, which is true for a valuation s_w of w iff $s_w = s$.
- $p(w)$ is a formula over w, which is true for a valuation s_w of w iff $p \in \mathcal{V}_d(s_w)$, where $p \in \mathcal{PV}'$,
- $H_i(w, w')$ is a formula over two global state variables $w = (\mathfrak{l}, \mathfrak{v})$, $w' = (\mathfrak{l}', \mathfrak{v}')$, which is true for valuations $s_\mathfrak{l}$ of $\mathfrak{l}$, $s_{\mathfrak{l}'}$ of $\mathfrak{l}'$, $s_\mathfrak{v}$ of $\mathfrak{v}$, and $s_{\mathfrak{v}'}$ of $\mathfrak{v}'$ iff $l_i(s_\mathfrak{l}) = l_i(s_{\mathfrak{l}'})$ and $s_\mathfrak{v} \cong s_{\mathfrak{v}'}$ (encodes equivalence of local states of agent i).
- $\mathcal{R}(w, w')$ is a formula over w, w', which is true for two valuations s_w of w and $s_{w'}$ of w' iff $s_w \rightarrow_\mathcal{A} s_{w'}$ (encodes the non-resetting transition relation of M_d),
- $R_y(w, w')$ is a formula over w, w', which is true for two valuations s_w of w and $s_{w'}$ of w' iff $s_w \rightarrow_y s_{w'}$ (encodes the transitions resetting the clock y).

The propositional formula $[M_d, \psi]_k$ is defined over state variables $w_{0,0}$, $w_{n,m}$, for $0 \leq m \leq k$ and $1 \leq n \leq f_k(\psi)$. We start off with a definition of its first conjunct, i.e., $[M_d^{\psi,s^0}]_k$, which constrains the $f_k(\psi)$ symbolic k-paths to be valid k-path of M_k. Namely,

$$[M_d^{\psi,s^0}]_k := I_{s^0}(w_{0,0}) \wedge \bigwedge_{n=1}^{f_k(\psi)} \bigwedge_{m=0}^{k-1} \mathcal{R}(w_{m,n}, w_{m+1,n})$$

The second conjunct, i.e., the formula $[\psi]_{M_k} = [\psi]_k^{[0,0]}$, is inductively defined as follows:

$$
\begin{array}{ll}
[p]_k^{[m,n]} & := p(w_{m,n}),\\
[\neg p]_k^{[m,n]} & := \neg p(w_{m,n}),\\
[\alpha \wedge \beta]_k^{[m,n]} & := [\alpha]_k^{[m,n]} \wedge [\beta]_k^{[m,n]},\\
[\alpha \vee \beta]_k^{[m,n]} & := [\alpha]_k^{[m,n]} \vee [\beta]_k^{[m,n]},\\
[\mathrm{E}_y(\alpha \mathrm{U} \beta)]_k^{[m,n]} & := \bigvee_{i=1}^{f_k(\psi)} (R_y(w_{m,n}, w_{0,i}) \wedge \bigvee_{j=0}^{k} ([\beta]_k^{[j,i]} \wedge \bigwedge_{l=0}^{j-1} [\alpha]_k^{[l,i]})),\\
[\mathrm{E}_y(\alpha \mathrm{R} \beta)]_k^{[m,n]} & := \bigvee_{i=1}^{f_k(\psi)} (R_y(w_{m,n}, w_{0,i}) \wedge (\bigvee_{j=0}^{k} ([\alpha]_k^{[j,i]} \wedge \bigwedge_{l=0}^{j} [\beta]_k^{[l,i]})\\
& \qquad \vee \bigwedge_{j=0}^{k} [\beta]_k^{[j,i]} \wedge \bigvee_{l=0}^{k} \mathcal{R}(w_{k,i}, w_{l,i}))),\\
[\overline{\mathrm{K}}_l \alpha]_k^{[m,n]} & := \bigvee_{i=1}^{f_k(\psi)} (I_{s^0}(w_{0,i}) \wedge \bigvee_{j=0}^{k} ([\alpha]_k^{[j,i]} \wedge H_l(w_{m,n}, w_{j,i}))),\\
[\overline{\mathrm{D}}_\Gamma \alpha]_k^{[m,n]} & := \bigvee_{i=1}^{f_k(\psi)} (I_{s^0}(w_{0,i}) \wedge \bigvee_{j=0}^{k} ([\alpha]_k^{[j,i]} \wedge \bigwedge_{l \in \Gamma} H_l(w_{m,n}, w_{j,i}))),\\
[\overline{\mathrm{E}}_\Gamma \alpha]_k^{[m,n]} & := \bigvee_{i=1}^{f_k(\psi)} (I_{s^0}(w_{0,i}) \wedge \bigvee_{j=0}^{k} ([\alpha]_k^{[j,i]} \wedge \bigvee_{l \in \Gamma} H_l(w_{m,n}, w_{j,i}))),\\
[\overline{\mathrm{C}}_\Gamma \alpha]_k^{[m,n]} & := [\bigvee_{i=1}^{k} (\overline{\mathrm{E}}_\Gamma)^i \alpha]_k^{[m,n]}.
\end{array}
$$

Lemma 12. *Let M_d be discretised model, M_k its k-model, and ψ an* ECTLK$_y$ *formula. For each state s of M_d, the following holds: $[M_d^{\psi,s}]_k \wedge [\psi]_{M_k}$ is satisfiable iff there is a submodel $M'(s)$ of M_k with $|P'_k| \leq f_k(\psi)$ and $|P'_y| \leq f_{k,y}(\psi)$ such that $M'(s), s \models \psi$.*

Proof (=>) Let $[M_d^{\psi,s}]_k \wedge [\psi]_{M_k}$ be satisfiable. By the definition of the translation, the propositional formula $[\psi]_{M_k}$ encodes all the sets of $k-$paths of size $f_k(\psi)$ which satisfy the formula ψ and all the sets of transitions resetting the clock y of size $f_{k,y}(\psi)$. By the definition of the unfolding of the transition relation, the propositional formula $[M^{\psi,s}]_k$ encodes $f_k(\psi)$ symbolic k-paths to be valid $k-$paths of M_k. Hence, there is a set of $k-$paths in M_k, which satisfies the formula ψ of size smaller or equal to $f_k(\psi)$, and there is a set of transitions resetting the clock y of size $f_{k,y}(\psi)$. Thus, we conclude that there is a submodel $M'(s)$ of M_k with $|P'_k| \leq f_k(\psi)$ and $|P'_y| \leq f_{k,y}(\psi)$ such that $M'(s), s \models \psi$.

(<=) The proof is by induction on the length of ψ. The lemma follows directly for the propositional variables and their negations. Consider the following cases:

- For $\psi = \alpha \vee \beta, \alpha \wedge \beta$, or the temporal operators the proof is like in [13].
- Let $\psi = \overline{\mathrm{K}}_l \alpha$. If $M'(s), s \models \overline{\mathrm{K}}_l \alpha$ with $|P'_k| \leq f_k(\overline{\mathrm{K}}_l \alpha)$ and $|P'_y| \leq f_{k,y}(\overline{\mathrm{K}}_l \alpha)$, then by the definition of bounded semantics we have that there is a $k-$path π such that $\pi(0) = s^0$ and $(\exists j \leq k)\ s \sim_l \pi(j))$ and $M'(s), \pi(j) \models \alpha$. Hence, by induction we obtain that for some $j \leq k$ the propositional formula $[\alpha]_k^{[0,0]} \wedge [M^{\alpha,\pi(j)}]_k$ is satisfiable. Let $ii = f_k(\alpha) + 1$ be the index of a new symbolic $k-$path which satisfies the formula $I_{s^0}(w_{0,ii})$. Therefore, by the construction above, it follows that the propositional formula $I_{s^0}(w_{0,ii}) \ \wedge \ \bigvee_{j=0}^{k} \left([\alpha]_k^{[j,ii]} \wedge H_l(w_{0,0}, w_{j,ii})\right) \wedge [M^{\overline{\mathrm{K}}_l \alpha, s}]_k$ is satisfiable. Therefore, the following propositional formula is satisfiable:

$$
\bigvee_{1 \leq i \leq f_k(\overline{\mathrm{K}}_l \alpha)} \left(I_{s^0}(w_{0,i}) \ \wedge \ \bigvee_{j=0}^{k} \left([\alpha]_k^{[j,i]} \wedge H_l(w_{0,0}, w_{j,i})\right) \wedge [M^{\overline{\mathrm{K}}_l \alpha, s}]_k \right).
$$

  Hence, by the definition of the translation of an ECTLK$_y$ formula, the above formula is equal to the propositional formula $[\overline{\mathrm{K}}_l \alpha]_k^{[0,0]} \wedge [M^{\overline{\mathrm{K}}_l \alpha, s}]_k$.
- The other proofs are similar.

□

Theorem 3. *Let M_d be a discretised model, and ψ an* ECTLK$_y$ *formula. If there exists $k \in \mathbb{N}_+$ such that $[\psi]_{M_k} \wedge [M^{\psi,s^0}]_k$ is satisfiable, then $M_d \models \psi$.*

Proof Follows from Theorem 2 and Lemma 12. □

5 A real-time alternating bit transmission problem

To exemplify the theoretical concepts of the previous sections we analyse a real-time version of one of the variants of the alternating bit protocol. In the original formulation [7] two agents attempt to transmit information over an unreliable communication channel, which they have access to. Sender $\mathcal{S}$ starts sending the bit to receiver $\mathcal{R}$. $\mathcal{R}$ is initially silent but as soon as it receives the bit from $\mathcal{S}$, it starts sending acknowledgments back to $\mathcal{S}$. As soon as $\mathcal{S}$ receives one of these acknowledgments, it stops sending the bit, the system is reset and a new bit is sent. Under these conditions it can be checked automatically [14] that whenever $\mathcal{S}$ receives an acknowledgment it then knows (in the formal epistemic sense) that $\mathcal{R}$ knows the value of the bit. Consider now one of the variants analysed in [9] where $\mathcal{R}$ may (erroneously) send acknowledgments without having received the bit first. Intuitively in this case, given that the protocol of execution is commonly known in interpreted systems, the property above will no longer hold; indeed this can also be checked automatically [14].

We extend the scenario above by adding the clock expressions. Assume that each agent has two possibly faulty communication channels to choose from to send bits or acknowledgments. In order to optimise the performance of the transmission both agents concurrently run a channel monitoring service in the background. To this aim they regularly send each other control bits and keep track of the time elapsed since the receipt of a control bit from the other party. The agents send the information bit on the channel that has demonstrated to be in the better working condition, i.e., the one that has recently been able to transmit the control bit from the other party.

To formalise the above we use a network of diagonal timed automata consisting of an automaton for $\mathcal{S}$ (see Figure 2) and an automaton for $\mathcal{R}$ (see Figure 3). $\mathcal{S}$ can be in 11 different local states: *Decide* ("$\mathcal{S}$ selects which bit will be sent"), 0-*ctr-bit* and 1-*ctr-bit* ("$\mathcal{S}$ sends a control bit and listens to $\mathcal{R}$'s control bit"), 0-*select* and 1-*select* ("$\mathcal{S}$ selects the channel to use to send bit 0 (1), or he sends a control bit"), 0-*channel*-1 and 0-*channel*-2 ("$\mathcal{S}$ sends bit 0 through channel 1 (2)"), 1-*channel*-1 and 1-*channel*-2, ("$\mathcal{S}$ sends bit 1 through channel 1 (2)"), 0-*ack* and 1-*ack* ("$\mathcal{S}$ has received an acknowledgement"). $\mathcal{S}$ can perform independently the following actions: 0-*bit*, 1-*bit* ("bit 0 (1) is sent"), *scbs*-1-*fail*, *scbs*-2-*fail* ("a control bit is sent to a faulty channel 1 (2)"), *s-send-fail* ("bit 0 or 1 is sent to a faulty channel"), *nothing*, and *next-bit* whose interpretation is obvious. The remaining actions are synchronised with $\mathcal{R}$.

$\mathcal{R}$ can be in 10 different local states: *wait* ("$\mathcal{R}$ is listening to the channels"), *ctr-bit* ("$\mathcal{R}$ sends a control bit, or he sends a faulty acknowledgement"), $r0$ and $r1$ ("$\mathcal{R}$

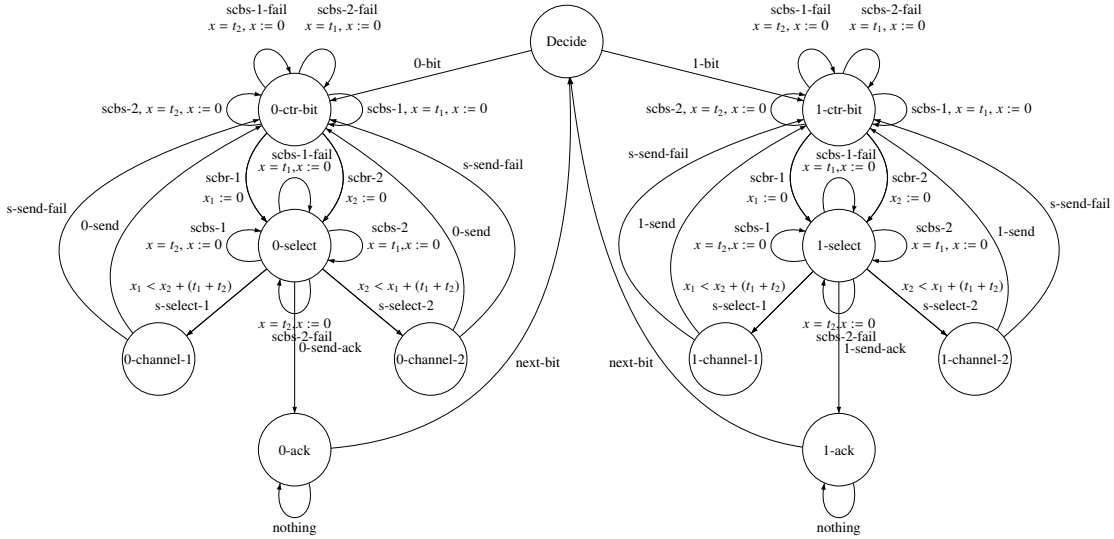

Fig. 2. An automaton for Sender

has received bit 0 (1)"), 0-*select* and 1-*select* ("$\mathcal{R}$ selects the channel for the ack"), 0-*channel*-1, 0-*channel*-2, 1-*channel*-1 and 1-*channel*-2, ("$\mathcal{R}$ sends an ack on channel 1 (2)."). $\mathcal{R}$ can perform independently the following actions: *scbr*-1-$fail$, *scbr*-2-$fail$ ("a control bit is sent to a faulty channel 1 (2)"), *r-send-fail* ("an ack is sent to a faulty channel"). We refer to Figures 2, 3 for a pictorial representation.

Further, $\mathcal{S}$ uses 3 clocks $(x, x_1, x_2,)$, and $\mathcal{R}$ three more (y, y_1, y_2). Control bits are sent at regular intervals: t_1 for channel 1 and t_2 for channel 2; the clocks x and y are used for this purpose. Clocks x_i and y_i measure the time since a control bit has been received; x_i gets reset when $\mathcal{S}$ receives a control bit on channel i, likewise for y_i for $\mathcal{R}$. When sending bits (either information bits of acknowledgments) each agent evaluates the following two clock expressions $z_1 - z_2 < (t_1 + t_2)$ and $z_2 - z_1 < (t_1 + t_2)$ for $z \in \{x, y\}$. When the former expression is true, channel 1 is chosen, when the latter is true, channel 2 is chosen. Intuitively the above guarantees that the channel that has been demonstrated to be alive more recently gets selected. Using the threshold $t_1 + t_2$ enables an agent not to switch channel unnecessarily often (for instance simply because they are desynchronised). Note that ease with which the use of a clock difference allows us to implement real-time channel selection without having a large state space for the automata in question.

The automata run in parallel and synchronise through the actions: *scbs*-1, *scbs*-2, *scbr*-1, and *scbr*-2 ("send a control bit via channel 1 (2)"), 0-*send*, and 1-*send* ("send bit 0 (1)"), 0-*send-ack*, and 1-*send-ack* (" send an acknowledgement to bit 0 (1)").

Given the above, one can construct the automaton $\mathcal{A}_{BTP}$ that describes the whole alternating bit protocol running in real time as well as the set of traces generated by it. In our approach this is done automatically by the bounded model checking implementation.

Now, assume the following set of propositional variables: $\mathcal{PV} = \{\mathbf{recack}, \mathbf{bit0}\}$, and the following usual interpretation for the proposition variables in $\mathcal{PV}$: $\mathcal{V}_{\mathcal{S}}(0\text{-}channel\text{-}1) = \mathcal{V}_{\mathcal{S}}(0\text{-}channel\text{-}2) = \mathcal{V}_{\mathcal{S}}(0\text{-}ack) = \mathbf{bit0}$, and $\mathcal{V}_{\mathcal{S}}(0\text{-}ack) = \mathcal{V}_{\mathcal{S}}(1\text{-}ack) = \mathbf{recack}$.

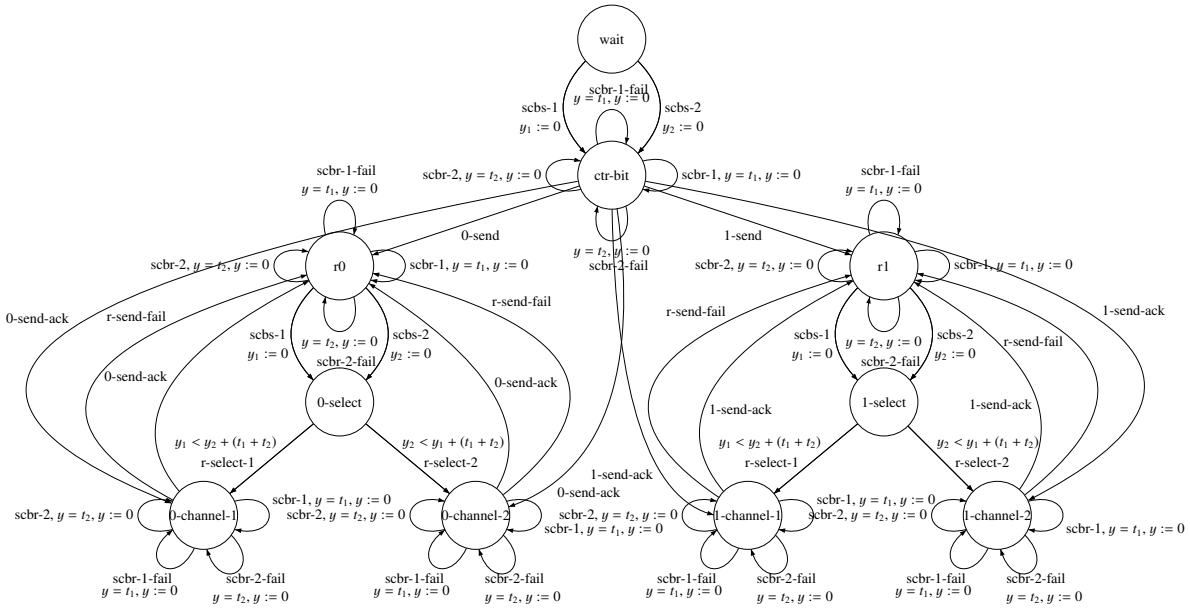

Fig. 3. An automaton for Receiver

The typical specification properties that one may be interested in checking for the example above are the following: 1) "forever in the future from t_1 if an ack has been received by $\mathcal{S}$ and the value of the bit is 0, then $\mathcal{R}$ knows the bit is equal to 0" and 2) "forever in the future from t_1 if an ack has been received by $\mathcal{S}$ and the value of the bit is 0, then $\mathcal{S}$ knows that $\mathcal{R}$ knows the bit is equal to 0."

By means of an implementation of the technique above we were able to check that the properties above are not satisfied (as intuitively is the case given $\mathcal{R}$'s possible behaviour). More precisely, we can check that the negations of the properties above are true, i.e., the following formulas are satisfied on the model for $\mathcal{A}_{BTP}$:

$$\varphi_1 = \mathrm{EF}_{[t_1,\infty]}(\mathbf{reckack} \wedge \mathbf{bit0} \wedge \overline{\mathrm{K}}_{\mathcal{R}}(\mathbf{bit0})), \text{ and}$$
$$\varphi_2 = \mathrm{EF}_{[t_1,\infty]}(\mathbf{reckack} \wedge \mathbf{bit0} \wedge \overline{\mathrm{K}}_{\mathcal{S}}\overline{\mathrm{K}}_{\mathcal{R}}(\mathbf{bit0})).$$

To verify satisfaction of φ_1 over the model for $\mathcal{A}_{BTP}$, 2 paths of length 11 were required. To do this we checked satisfaction of a Boolean formula that encoded the translation of the formula φ_1 and an appropriate fragments of the model for $\mathcal{A}_{BTP}$ as described in [10]. The formula in question consists of 125260 variables and 258821 clauses; our implementation needed 19.6 second and 18.7 MB memory to produce it. Satisfaction itself was checked by MiniSat [6], a mainstream SAT solver, that required 4.0 seconds and 19.9 MB memory to return satisfiable as the answer.

Similarly satisfaction of φ_2 required 3 paths of the length 11. The Boolean formula representing the bounded model checking test consists of 213034 variables and 471494 clauses; our implementation needed 1364.4 second and 31.4 MB memory to produce it. Given the formula MiniSat needed 320.0 seconds and 81.8 MB memory to return satisfiable as the answer; for reference the experiments were performed on an AMD Athlon XP 1800 (1544 MHz), 768 MB main memory, running Linux with Kernel 2.6.15.

We are not able to compare these results to other tools as we are not aware of any other implementation available that is capable of a real-time epistemic check for (diagonal and non-diagonal) automata.

6 Conclusions

Model checking real-time in AI and MAS is still in its infancy. In [17] a first proposal was made for a bounded model checking algorithm for real-time epistemic properties based on non-diagonal automata semantics. In this paper we have tried to extend that work by allowing the expressivity of clock differences. We have proposed a syntax, semantics for the logic, as well as a bounded model checking method, and showed experimental results of a preliminary implementation for a real-time version of the alternating bit protocol.

References

1. MCK: Model checking knowledge. http://www.cse.unsw.edu.au/~mck.
2. A. Biere, A. Cimatti, E. Clarke, and Y. Zhu. Symbolic model checking without BDDs. In *Proc. of TACAS'99*, volume 1579 of *LNCS*, pages 193–207. Springer-Verlag, 1999.
3. P. Bouyer, F. Laroussinie, and P. Reynier. Diagonal constraints in timed automata: Forward analysis of timed systems. In Paul Pettersson and Wang Yi, editors, *Proceedings of the 3rd International Conference on Formal Modelling and Analysis of Timed Systems (FORMATS'05)*, volume 3829 of *LNCS*, pages 112–126, Uppsala, Sweden, November 2005. Springer.
4. A. Cimatti, E. M. Clarke, E. Giunchiglia, F. Giunchiglia, M. Pistore, M. Roveri, R. Sebastiani, and A. Tacchella. NuSMV2: An open-source tool for symbolic model checking. In *Proceedings of the 14th International Conference on Computer Aided Verification (CAV'02)*, volume 2404 of *LNCS*, pages 359–364. Springer-Verlag, 2002.
5. P. Dembiński, A. Janowska, P. Janowski, W. Penczek, A. Pólrola, M. Szreter, B. Woźna, and A. Zbrzezny. VerICS: A tool for verifying Timed Automata and Estelle specifications. In *Proc. of the 9th Int. Conf. on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'03)*, volume 2619 of *LNCS*, pages 278–283. Springer-Verlag, 2003.
6. N. Eén and N. Sörensson. MiniSat. http://www.cs.chalmers.se/Cs/Research/FormalMethods/MiniSat/.
7. R. Fagin, J. Y. Halpern, Y. Moses, and M. Y. Vardi. *Reasoning about Knowledge*. MIT Press, Cambridge, 1995.

8. M. Kacprzak, A. Lomuscio, and W. Penczek. Verification of multiagent systems via unbounded model checking. In N. R. Jennings, C. Sierra, L. Sonenberg, and M. Tambe, editors, *Proceedings of the Third International Conference on Autonomous Agents and Multiagent Systems (AAMAS'04)*, volume II, pages 638–645. ACM, July 2004.
9. A. Lomuscio and M. Sergot. A formalisation of violation, error recovery, and enforcement in the bit transmission problem. *Journal of Applied Logic*, 2(1):93–116, March 2004.
10. A. Lomuscio, B. Wozna, and A. Zbrzezny. Bounded model checking real-time multi-agent systems with clock differences: theory and implementation. Technical Report RN/06/03, Department of Computer Science, University College London, Gower Street, London WC1E 6BT, United Kingdom, 2006.
11. W. Nabialek, A. Niewiadomski, W. Penczek, A. Pólrola, and M. Szreter. VerICS 2004: A model checker for real time and multi-agent systems. In *Proceedings of the International Workshop on Concurrency, Specification and Programming (CS&P'04)*, volume 170 of *Informatik-Berichte*, pages 88–99. Humboldt University, 2004.
12. W. Penczek and A. Lomuscio. Verifying epistemic properties of multi-agent systems via bounded model checking. *Fundamenta Informaticae*, 55(2):167–185, 2003.
13. W. Penczek, B. Woźna, and A. Zbrzezny. Bounded model checking for the universal fragment of CTL. *Fundamenta Informaticae*, 51(1-2):135–156, 2002.
14. F. Raimondi and A. Lomuscio. Automatic verification of multi-agent systems by model checking via OBDDs. *Journal of Applied Logic*, 2005. To appear in Special issue on Logic-based agent verification.
15. S. Tripakis and S. Yovine. Analysis of timed systems using time-abstracting bisimulations. *Formal Methods in System Design*, 18(1):25–68, 2001.
16. R. van der Meyden and Kaile Su. Symbolic model checking the knowledge of the dining cryptographers. In *Proceedings of the 17th IEEE Computer Security Foundations Workshop (CSFW'04)*, pages 280–291, Washington, DC, USA, 2004. IEEE Computer Society.
17. B. Woźna, A. Lomuscio, and W. Penczek. Bounded model checking for knowledge over real time. In *Proceedings of the 4st International Conference on Autonomous Agents and Multi-Agent Systems (AAMAS'05)*, volume I, pages 165–172. ACM Press, July 2005.
18. A. Zbrzezny. Improvements in SAT-based reachability analysis for timed automata. *Fundamenta Informaticae*, 60(1-4):417–434, 2004.
19. A. Zbrzezny. SAT-based reachability checking for timed automata with diagonal constraints. *Fundamenta Informaticae*, 67(1-3):303–322, 2005.