Scientific Issues
Jan Długosz University
in Częstochowa
Mathematics XXI (2016)
161–187
DOI http://dx.doi.org/10.16926/m.2016.21.14

ON THE SMT-BASED VERIFICATION OF COMMUNICATIVE COMMITMENTS

BOŻENA WOŹNA-SZCZEŚNIAK AND IRENEUSZ SZCZEŚNIAK

Abstract

We propose an SMT-based bounded model checking (BMC) technique for the existential fragments of CCTL*K – an epistemic temporal logic extended to include modalities for different social commitments – and for multi-agent systems modelled by Communication Interpreted Systems (CIS). Furthermore, we exemplify the use of the technique by means of the NetBill protocol, a popular example in the MAS literature related to the modelling of business processes.

1. Introduction

Agents are autonomous and sophisticated entities that act autonomously on behalf of their users, across open and distributed environments, to solve a growing number of complex problems. A multi-agent system (MAS) [16] is a loosely united network of agents that interact to solve problems that are beyond the capacities or knowledge of a single agent. In particular, multi-agent systems can model an artificial society that mainly evolves through communication among participating entities.

In order to model formally communication between agents of an artificial society, an adequate agent communication language (ACL) is needed. Such an ACL should have computationally grounded semantics that provides capabilities to verify, for example, whether or not agent behaviours comply with the protocol. Moreover, according to recent advances in the ACL field, an ACL semantics should be based on *social approaches* [14, 5, 6] that allow to overcome the shortcomings and inconveniences incorporated with *mental approaches* [19]; the mental semantics is defined in terms of the agents' internal mental states such as believes, goals, desires and intentions.

Following [6, 18], in the paper we consider CCTL*K, which is an agent communication language that extends CTL* [4] with epistemic [8], commitments [6], and group commitment [18] modalities. The CCTL*K language allows for reasoning about temporal, epistemic and social properties

of MASs. Its semantics is defined by Kripke models that are generated by *communication interpreted systems* (CIS) [6] - a social extension of standard *interpreted systems* (IS) [8].

Automatic verification of commitment properties and commitment-based protocols, performed by the analysis of their models, is a very important subject of research. This is highly motivated by an increasing demand to help protocol inventors either find undesirable and faulty agents' behaviours to eliminate them or implement desirable agents' behaviours so that such protocols conform to given specifications at design time.

Verifying a correctness property of a system by means of model checking techniques [4] amounts to checking whether a logical formula (expressing the property) is valid in a model of the system representing all its possible computations. So far several model checking approaches for commitment properties and commitment-based protocols have been developed. Among others, in [12] the CTLC logic, which extends CTL with modalities for reasoning about social commitments, their fulfillment and violation, has been introduced. Moreover, the model checking problem for CTLC has been translated into the model checking problem for CTLK (the combination of CTL with the logic of knowledge), in which the commitment modality is represented by the knowledge modality. The proposed translation has been implemented as a BDD-based symbolic model-checking algorithm for CTLC on the top of MCMAS [9]. In [6] the authors introduced the CTLC$^+$ logic that slightly modifies CTLC, and proposed verification technique, which is based on a translation of the model checking problem for CTLC$^+$ into the model checking problem for ARCTL (the combination of CTL with action formulae) and into the model checking problem for GCTL* (a generalized version of CTL* with action formulae), and then using, respectively, NuSMV [3] and the CWB-NC automata-based model checker [21]. Finally, in [18] a SAT-based bounded model checking (BMC) [13] for communication deontic interpreted systems (CDIS) and for ECDCTL*K, which is the existential fragment of CDCTL*K (a branching time temporal logic extended to knowledge, correct functioning behaviour, and different social commitments modalities) has been proposed.

BMC is, in general, a method of performing verification using only a fragment of the considered model that is truncated up to some specific depth. It exploits the observation that we can infer some properties of the model using only its fragments. To be applicable in practice, this approach can be combined with a technique which involves translation of the verification problem to the boolean satisfiability problem (SAT), or to the satisfiability modulo theories (SMT) problem. The aim of this paper is to report on recent progress on the application of the SMT-based BMC that employs

SMT-solvers (i.e., tools for deciding the satisfiability of formulae in a number of theories [1]) to verifying no just temporal and epistemic, but also social properties of MAS. In particular, we define an SMT-based BMC for CIS and for ECCTL*K, which is the existential fragment of CCTL*K, and we prove its correctness and completeness.

The rest of the paper is organised as follows. In Section 2 we introduce CIS together with its Kripke model, and we provide syntax and semantics of the CCTL*K language together with its existential (ECCTL*K) and universal (ACCTL*K) fragments. In Section 3 we define a bounded semantics for the ECCTL*K subset, we prove the equivalence of the bounded and unbounded semantics, we provide a SMT-based BMC method for ECCTL*K, and we prove the correctness and completeness of the BMC method. In Section 4 we apply the BMC technique to the NetBill protocol. In the last section we conclude the paper with a short discussion and an outline of our future work.

2. Preliminaries

Let us begin by setting some notations utilized through the paper. Let $\mathbb{A} = \{1, \ldots, n\}$ be the non-empty and finite set of agents, $\mathcal{E}$ a special agent that is used to model the environment in which the agents operate, $\mathcal{PV} = \bigcup_{\mathbf{c} \in \mathbb{A}} \mathcal{PV}_{\mathbf{c}} \cup \mathcal{PV}_{\mathcal{E}}$ a set of propositional variables such that $\mathcal{PV}_{\mathbf{c}_1} \cap \mathcal{PV}_{\mathbf{c}_2} = \emptyset$ for all $\mathbf{c}_1, \mathbf{c}_2 \in \mathbb{A} \cup \{\mathcal{E}\}$, and $\mathbb{Z}$ the set of integers.

2.1. **CIS.** The set $\mathbb{A}$ of agents together with the environment constitute a multi-agent system (MAS), to model which we use the formalism of *communication interpreted system* (CIS). In CIS, each agent $\mathbf{c} \in \mathbb{A}$ is modelled by:

- $L_{\mathbf{c}}$ - a non-empty and finite set of *local states*, which models the instantaneous configuration of the agent $\mathbf{c}$ in MAS. The content varies according to what we need to model, e.g. it may be the values of some (local) variables.
- $Var_{\mathbf{c}}$ - a finite set of *local non-negative integer variables*. These variables are used to represent communication channels through which messages are sent and received, and then to define the *social accessibility* relation, which in turn will be used to define the computationally grounded semantics of *communication commitments*.
- $Act_{\mathbf{c}}$ - a non-empty and finite set of *possible actions* such that the special *null* action $\epsilon_{\mathbf{c}}$ belongs to $Act_{\mathbf{c}}$; it is assumed that actions are "public".
- $P_{\mathbf{c}} : L_{\mathbf{c}} \to 2^{Act_{\mathbf{c}}}$ - a *protocol function* defining the action selection mechanism.

- $t_{\mathbf{c}} : L_{\mathbf{c}} \times L_{\mathcal{E}} \times Act \to L_{\mathbf{c}}$ (each element of $Act = \prod_{\mathbf{c}\in\mathbb{A}} Act_{\mathbf{c}}$, as usually, is called *joint action*) is a (partial) *evolution function*. We assume that if $\epsilon_{\mathbf{c}} \in P_{\mathbf{c}}(\ell_{\mathbf{c}})$, then $t_{\mathbf{c}}(\ell_{\mathbf{c}}, \ell_{\mathcal{E}}, (a_1, \ldots, a_n, a_{\mathcal{E}})) = \ell_{\mathbf{c}}$ for $a_{\mathbf{c}} = \epsilon_{\mathbf{c}}$.
- $\mathcal{V}_{\mathbf{c}} : L_{\mathbf{c}} \to 2^{\mathcal{PV}}$ - a *valuation function* which assigns to every local state a set of propositional variables that are assumed to be true at that state.

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

- $L_{\mathcal{E}}$ - a non-empty and finite set of *local states*,
- $Var_{\mathcal{E}}$ - a finite set of *local non-negative integer variables*.
- $Act_{\mathcal{E}}$ - a non-empty and finite set of *possible actions*,
- $P_{\mathcal{E}} : L_{\mathcal{E}} \to 2^{Act_{\mathcal{E}}}$ - a protocol function,
- $t_{\mathcal{E}} : L_{\mathcal{E}} \times Act \to L_{\mathcal{E}}$ - a (partial) *evolution function*,
- $\mathcal{V}_{\mathcal{E}} : L_{\mathcal{E}} \to 2^{\mathcal{PV}_{\mathcal{E}}}$ - a *valuation function*.

The environment $\mathcal{E}$ captures relevant information that is not specific to any individual agent, e.g. messages in transit in a communication channel. Moreover, it is assumed that local states, and actions for $\mathcal{E}$ are "public".

A set of all *global states* is defined as $S = L_1 \times \ldots \times L_n \times L_{\mathcal{E}}$ [8], and each element $s \in S$ represents the instantaneous snapshot of MAS at a given time. Furthermore, given a set of agents $\mathbb{A}$, the environment $\mathcal{E}$, and a set of initial global states $\iota \subseteq S$, a *communication interpreted system* (CIS) is a tuple:

$$\mathcal{C} = (\{L_{\mathbf{c}}, Var_{\mathbf{c}}, Act_{\mathbf{c}}, P_{\mathbf{c}}, t_{\mathbf{c}}, \mathcal{V}_{\mathbf{c}}\}_{\mathbf{c}\in\mathbb{A}\cup\{\mathcal{E}\}}, \iota)$$

Let $s = (\ell_1, \ldots, \ell_n, \ell_{\mathcal{E}})$ be a global state. We write $l_{\mathbf{c}}(s)$ to denote the local state of agent $\mathbf{c} \in \mathbb{A}$. Next, for each agent $\mathbf{c} \in \mathbb{A}$ we define a standard indistinguishability relation $\sim_{\mathbf{c}} \subseteq S \times S$ as: $s \sim_{\mathbf{c}} s'$ iff $l_{\mathbf{c}}(s') = l_{\mathbf{c}}(s)$. This relation is used to give the computationally grounded semantics for standard epistemic properties of MAS. Moreover, we define a *global evolution function* $t : S \times Act \to S$ as follows: $t(s, a) = s'$ iff $t_{\mathbf{c}}(l_{\mathbf{c}}(s), l_{\mathcal{E}}(s), a) = l_{\mathbf{c}}(s')$ for all $\mathbf{c} \in \mathbb{A}$ and $t_{\mathcal{E}}(l_{\mathcal{E}}(s), a) = l_{\mathcal{E}}(s')$. In brief we write the above as $s \xrightarrow{a} s'$. Furthermore, as in [6], we denote the value of a variable $x \in Var_{\mathbf{c}}$ at local state $l_{\mathbf{c}}(s)$ by $l^x_{\mathbf{c}}(s)$, and we assume that if $l_{\mathbf{c}}(s) = l_{\mathbf{c}}(s')$, then $l^x_{\mathbf{c}}(s) = l^x_{\mathbf{c}}(s')$ for all $x \in Var_{\mathbf{c}}$. Next, for each pair $(\mathbf{c}_1, \mathbf{c}_2)$ of agents in $\mathbb{A}$ we define a *social accessibility* relation $\sim_{\mathbf{c}_1\to\mathbf{c}_2} \subseteq S \times S$ as:

$$s \sim_{\mathbf{c}_1\to\mathbf{c}_2} s' \text{ iff } l_{\mathbf{c}_1}(s) = l_{\mathbf{c}_1}(s') \text{ and } Var_{\mathbf{c}_1} \cap Var_{\mathbf{c}_2} \neq \emptyset \text{ such that}$$
$$\forall_{x\in Var_{\mathbf{c}_1}\cap Var_{\mathbf{c}_2}}\ (l^x_{\mathbf{c}_1}(s) = l^x_{\mathbf{c}_2}(s')) \text{ and } \forall_{y\in Var_{\mathbf{c}_2}-Var_{\mathbf{c}_1}}\ (l^y_{\mathbf{c}_2}(s) = l^y_{\mathbf{c}_2}(s')).$$

The intuition behind the definition of the social accessibility relation $\sim_{\mathbf{c}_1\to\mathbf{c}_2}$ is the following. The states s and s' are indistinguishable for $\mathbf{c}_1$ ($l_{\mathbf{c}_1}(s) = l_{\mathbf{c}_1}(s')$), since $\mathbf{c}_1$ initiates the communication and it does not learn any new information. There is a communication channel between $\mathbf{c}_1$ and $\mathbf{c}_2$ ($Var_{\mathbf{c}_1} \cap Var_{\mathbf{c}_2} \neq \emptyset$). The channel is filled in by $\mathbf{c}_1$ in state s, and in state s' $\mathbf{c}_2$ receives the information, which makes the value of the shared

variable the same for $\mathbf{c}_1$ and $\mathbf{c}_2$ ($l^x_{\mathbf{c}_1}(s) = l^x_{\mathbf{c}_2}(s')$). The states s and s' are indistinguishable for $\mathbf{c}_2$ with regard to the variables that have not been communicated by $\mathbf{c}_1$, i.e., unshared variables $\forall_{y \in Var_{\mathbf{c}_2} - Var_{\mathbf{c}_1}} l^y_{\mathbf{c}_2}(s) = l^y_{\mathbf{c}_2}(s')$.

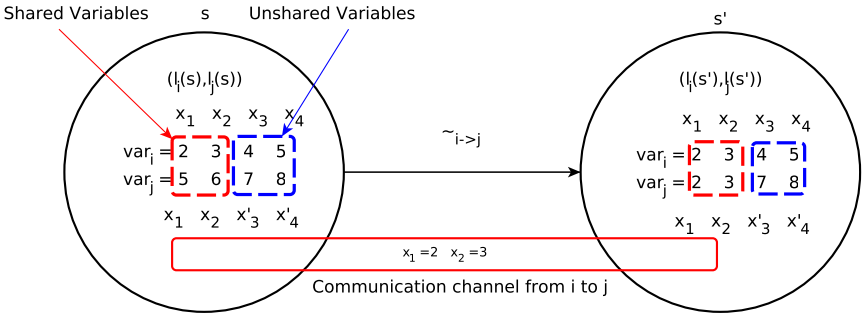

FIGURE 1. An example of the social accessibility relation $\sim_{i \to j}$.

Example 1. *Consider the example shown in Figure 1. We can observe that the shared and unshared variables for agents are the following:* $Var_i = \{x_1, x_2, x_3, x_4\}$ *for agent* i*, and* $Var_j = \{x_1, x_2, x'_3, x'_4\}$ *for agent* j*. More precisely,* x_1 *and* x_2 *are shared variables (i.e., they represent the communication channel), and* x_3 *,* x_4*,* x'_3*, and* x'_4 *are unshared variables, which may represent communication channels with other agents. Notice that the values of the variables* x_1 *and* x_2 *for* j *in the state* s' *are changed to be equal to the values of these variables for agent* i*, which illustrates the massage passing through the channel. On the other hand, the values of the variables in* Var_i *are unchanged as* $l_i(s) = l_i(s')$*.*

2.2. **Model.** For a given CIS we define a *model* as a tuple

$$M = (Act, S, \iota, T, \mathcal{V}, \sim_{\mathbf{c}}, \sim_{\mathbf{c}_1 \to \mathbf{c}_2}), \text{ where}$$

- Act is the set of labels (i.e., joint actions),
- S and $\iota \subseteq S$ are defined as above,
- $T \subseteq S \times S$ is a total transition relation on S defined by: $(s, s') \in T$ iff there exists an action $a \in Act$ such that $s \xrightarrow{a} s'$,
- $\mathcal{V} : S \to 2^{\mathcal{PV}}$ is the valuation function defined as $\mathcal{V}(s) = \bigcup_{\mathbf{c} \in \mathbb{A}} \mathcal{V}_{\mathbf{c}}(l_{\mathbf{c}}(s))$,
- $\sim_{\mathbf{c}} \subseteq S \times S$ is the indistinguishability relation, for $\mathbf{c} \in \mathbb{A}$,
- $\sim_{\mathbf{c}_1 \to \mathbf{c}_2} \subseteq S \times S$ is the social accessibility relation for, $\mathbf{c} \in \mathbb{A}$.

A *path* in M is an infinite sequence $\pi = (s_0, s_1, \ldots)$ of states such that $(s_m, s_{m+1}) \in T$ for each $m \in \mathbb{N}$. Let $m \in \mathbb{N}$. Then, the m-th state of

π is defnied as $\pi(m) = s_m$, and the m-th suffix of π is defnied as $\pi^m = (s_m, s_{m+1}, \ldots)$. $\Pi(s)$ denotes the set of all the paths starting at $s \in S$, and $\Pi = \bigcup_{s^0 \in \iota} \Pi(s^0)$ is the set of all the paths starting at initial states.

2.3. **Syntax of** CCTL*K**.** Let $p \in \mathcal{PV}$ be a propositional variable, $\mathbf{c}_1, \mathbf{c}_2 \in \mathbb{A}$, $\Gamma \subseteq \mathbb{A}$. The syntax of CCTL*K, which is a combination of branching time CTL* [7] with standard epistemic modalities, the social commitments modality [6], and the group social commitments modality [18], is defined as follows:

$$\begin{aligned}\varphi ::=& \text{true} \mid \text{false} \mid p \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \mathrm{A}\phi \mid \\ & \mathrm{K}_{\mathbf{c}}\phi \mid \mathrm{E}_\Gamma\phi \mid \mathrm{D}_\Gamma\phi \mid \mathrm{C}_\Gamma\phi \mid \mathrm{C}_{i\to j}\phi \mid \mathrm{C}_{i\to\Gamma}\phi \\ \phi ::=& \varphi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \mathrm{X}\phi \mid \phi\mathrm{U}\phi \mid \phi\mathrm{R}\phi\end{aligned}$$

where φ is a *state formula* and ϕ is a *path formula*, A is the universal quantifier on paths, X, U, and R are CTL* path temporal modalities standing for *next*, *until* and *release*, respectively. The modalities $\mathrm{K}_{\mathbf{c}}, \mathrm{D}_\Gamma, \mathrm{E}_\Gamma$, and C_Γ represent *knowledge of agent* $\mathbf{c}$, *distributed knowledge in the group* Γ, *everyone in* Γ *knows*, and *common knowledge among agents in* Γ, respectively. Finally, the modalities $\mathrm{C}_{i\to j}$ and $\mathrm{C}_{i\to\Gamma}$ represent *commitment* and *group commitment*, respectively.

> CCTL*K consists of the set of state formulae generated by the above grammar.

In this logic, $\mathrm{C}_{i\to j}\phi$ is read as *agent* i *commits towards agent* j *that* ϕ, or equivalently as ϕ *is committed to by* i *towards* j. $\mathrm{C}_{i\to\Gamma}\phi$ is read as *agent* i *commits towards group of agent* Γ *that* ϕ, or equivalently as ϕ *is committed to by* i *towards group of agent* Γ.

For more details on commitment modality $\mathrm{C}_{i\to j}$ and on group commitment modality $\mathrm{C}_{i\to\Gamma}$ we refer to [6] and [18], respectively.

Other temporal, epistemic and commitment modalities are given by their usual abbreviations, i.e. $\mathrm{F}\phi \stackrel{def}{=} \text{true}\mathrm{U}\phi$, $\mathrm{G}\phi \stackrel{def}{=} \text{false}\mathrm{R}\phi$, $\overline{\mathrm{K}}_{\mathbf{c}}\phi \stackrel{def}{=} \neg\mathrm{K}_{\mathbf{c}}\neg\phi$, $\overline{\mathrm{D}}_\Gamma\phi \stackrel{def}{=} \neg\mathrm{D}_\Gamma\neg\phi$, $\overline{\mathrm{E}}_\Gamma\phi \stackrel{def}{=} \neg\mathrm{E}_\Gamma\neg\phi$, $\overline{\mathrm{C}}_\Gamma\phi \stackrel{def}{=} \neg\mathrm{C}_\Gamma\neg\phi$, $\overline{\mathrm{C}}_{i\to j}\phi \stackrel{def}{=} \neg\mathrm{C}_{i\to j}\neg\phi$, $\overline{\mathrm{C}}_{i\to\Gamma}\phi \stackrel{def}{=} \neg\mathrm{C}_{i\to\Gamma}\neg\phi$.

We define several sublogics of CCTL*K including variants of linear-time temporal logic as well as branching-time temporal logic. In particular we find it usefull to consider the following fragments of CCTL*K:

ACCTL*K is defined by the following grammar: $\varphi ::= \text{true} \mid \text{false} \mid p \mid \neg p \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \mathrm{A}\phi \mid \mathrm{K}_{\mathbf{c}}\phi \mid \mathrm{E}_\Gamma\phi \mid \mathrm{D}_\Gamma\phi \mid \mathrm{C}_\Gamma\phi \mid \mathrm{C}_{i\to j}\phi \mid \mathrm{C}_{i\to\Gamma}\phi$; $\phi ::= \varphi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \mathrm{X}\phi \mid \phi\mathrm{U}\phi \mid \phi\mathrm{R}\phi$.

ECCTL*K is defined by the following grammar: $\varphi ::= \text{true} \mid \text{false} \mid p \mid \neg p \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \mathrm{E}\phi \mid \overline{\mathrm{K}}_{\mathbf{c}}\phi \mid \overline{\mathrm{E}}_{\Gamma}\phi \mid \overline{\mathrm{D}}_{\Gamma}\phi \mid \overline{\mathrm{C}}_{\Gamma}\phi \mid \overline{\mathrm{C}}_{i\to j}\phi \mid \overline{\mathrm{C}}_{i\to\Gamma}\phi$; $\phi ::= \varphi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \mathrm{X}\phi \mid \phi \mathrm{U} \phi \mid \phi \mathrm{R} \phi$.
ECLTLK is defined by the following grammar: $\varphi ::= \text{true} \mid \text{false} \mid p \mid \neg p \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \mathrm{X}\varphi \mid \varphi \mathrm{U} \varphi \mid \varphi \mathrm{R} \varphi \mid \overline{\mathrm{K}}_{\mathbf{c}}\varphi \mid \overline{\mathrm{E}}_{\Gamma}\varphi \mid \overline{\mathrm{D}}_{\Gamma}\varphi \mid \overline{\mathrm{C}}_{\Gamma}\varphi \mid \overline{\mathrm{C}}_{\mathbf{c}_1\to\mathbf{c}_2}\varphi \mid \overline{\mathrm{C}}_{\mathbf{c}_1\to\Gamma}\varphi$;
LTL is defined by the following grammar: $\varphi ::= \text{true} \mid \text{false} \mid p \mid \neg p \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \mathrm{X}\varphi \mid \varphi \mathrm{U} \varphi \mid \varphi \mathrm{R} \varphi$.

We use the universal fragment (i.e., ACCTL*K) to express properties of a system in question, and we use the existential fragment (i.e., ECCTL*K) to verify these properties by means of the SMT-based bounded model checking method, which is presented in the next section. Fragments ECLTLK and LTL are used to prove equivalence of the bounded and unbounded semantics.

2.4. **Semantics of** CCTL*K**.** The semantics of CCTL*K formulae is defined with respect to the model $M = (Act, S, \iota, T, \mathcal{V}, \sim_{\mathbf{c}}, \sim_{\mathbf{c}_1\to\mathbf{c}_2})$. In the semantics we assume the following definitions of epistemic relations: $\sim_{\Gamma}^{E} \stackrel{def}{=} \bigcup_{\mathbf{c}\in\Gamma} \sim_{\mathbf{c}}$, $\sim_{\Gamma}^{C} \stackrel{def}{=} (\sim_{\Gamma}^{E})^{+}$ (the transitive closure of $\sim_{\Gamma}^{E}$), $\sim_{\Gamma}^{D} \stackrel{def}{=} \bigcap_{\mathbf{c}\in\Gamma} \sim_{\mathbf{c}}$, where $\Gamma \subseteq \mathbb{A}$.

Let M be a model, s a state of M, π a path in M, $m \in \mathbb{N}$, $p \in \mathcal{PV}$ a propositional variable, α and β state formulae of CCTL*K, and φ and ψ path formulae of CCTL*K. For a state formula α over $\mathcal{PV}$, the notation $M, s \models \alpha$ means that α holds at the state s in the model M. Similarly, for a path formula φ over $\mathcal{PV}$, the notation $M, \pi \models \varphi$ means that φ holds along the path π in the model M. The relation $\models$ is defined inductively as follows:

$M, s \models \text{true}$, $M, s \not\models \text{false}$, $M, s \models p$ iff $p \in \mathcal{V}(s)$, $M, s \models \neg\alpha$ iff $M, s \not\models \alpha$,
$M, s \models \alpha \wedge \beta$ iff $M, s \models \alpha$ and $M, s \models \beta$,
$M, s \models \alpha \vee \beta$ iff $M, s \models \alpha$ or $M, s \models \beta$,
$M, s \models \mathrm{K}_{\mathbf{c}}\alpha$ iff $(\forall \pi \in \Pi)(\forall i \geqslant 0)(s \sim_{\mathbf{c}} \pi(i)$ implies $M, \pi^i \models \alpha)$,
$M, s \models Y_{\Gamma}\alpha$ iff $(\forall \pi \in \Pi)(\forall i \geqslant 0)(s \sim_{\Gamma}^{Y} \pi(i)$ implies $M, \pi^i \models \alpha)$, with $Y \in \{\mathrm{D}, \mathrm{E}, \mathrm{C}\}$,
$M, s \models \mathrm{C}_{\mathbf{c}_1\to\mathbf{c}_2}\alpha$ iff $(\forall \pi \in \Pi)(\forall i \geqslant 0)(s \sim_{\mathbf{c}_1\to\mathbf{c}_2} \pi(i)$ implies $M, \pi^i \models \alpha)$
$M, s \models \mathrm{C}_{\mathbf{c}_1\to\Gamma}\alpha$ iff $(\forall \pi \in \Pi)(\forall i \geqslant 0)(\forall \mathbf{c}_2 \in \Gamma)(s \sim_{\mathbf{c}_1\to\mathbf{c}_2} \pi(i)$ implies $M, \pi^i \models \alpha)$,
$M, s \models \mathrm{A}\varphi$ iff $(\forall \pi \in \Pi(s))(M, \pi^0 \models \varphi)$,
$M, \pi^m \models \alpha$ iff $M, \pi(m) \models \alpha$,
$M, \pi^m \models \varphi \wedge \psi$ iff $M, \pi^m \models \varphi$ and $M, \pi^m \models \psi$,
$M, \pi^m \models \varphi \vee \psi$ iff $M, \pi^m \models \varphi$ or $M, \pi^m \models \psi$,
$M, \pi^m \models \mathrm{X}\varphi$ iff $M, \pi^{m+1} \models \varphi$,

$$\begin{array}{ll} M,\pi^m \models \varphi \mathrm{U} \psi & \text{iff } (\exists j \geqslant m)\big(M,\pi^j \models \psi \text{ and } (\forall m \leqslant i < j) M,\pi^i \models \varphi\big), \\ M,\pi^m \models \varphi \mathrm{R} \psi & \text{iff } (\exists j \geqslant m)\big(M,\pi^j \models \varphi \text{ and } (\forall m \leqslant i \leqslant j) M,\pi^i \models \psi\big) \\ & \quad \text{or } (\forall j \geqslant m)(M,\pi^j \models \psi). \end{array}$$

- A CCTL*K state formula α is *universally valid* in M, denoted by $M \models^\forall \alpha$, iff for each $s \in \iota$, $M, s \models \alpha$, i.e., α holds at every initial state of M.
- A CCTL*K state formula α is *existentially valid* in M, denoted by $M \models \alpha$, iff for some $s \in \iota$, $M, s \models \alpha$, i.e., α holds at some initial state of M.
- Determining whether a CCTL*K state formula α is existentially (resp. universally) valid in the model M is called an *existential* (resp. *universal*) model checking problem. In other words, the *universal model checking problem* asks whether $M \models^\forall \alpha$, and the *existential model checking problem* asks whether $M \models \alpha$.

In order to solve the universal model checking problem, one can negate the formula and show that the existential model checking problem for the negated formula has no solution. Intuitively, we are attempting to discover a counterexample, and if we do not succeed, then the formula is universally valid. Now, since bounded model checking is intended for finding a solution to an existential model checking problem, in the paper we only consider the properties expressible in ECCTL*K.

3. SMT- based Bounded Model Checking

The main idea of the SMT-based bounded model checking (BMC) method consists of translating the existential model checking problem for a modal logic and for a (Kripke like) model to the SMT satisfiability problem [1]. More precisely, SMT-based BMC consists in representing a counterexample-trace of bounded length by a quantifier-free first-order formula and checking the resulting quantifier-free first-order formula with a specialised SMT-solver, i.e., programs (tools) that automatically decide whether a quantifier-free first-order formula is satisfiable. If the formula in question is satisfiable, then a satisfying assignment returned by the SMT-solver can be converted into a concrete counterexample that shows that the property is violated. Otherwise, the bound is increased and the process repeated.

The SMT encoding of the BMC problem for ECCTL*K and for CIS, which we present here, is based on the SAT encoding of the same BMC problem introduced in [18].

3.1. Bounded Semantics of ECCTL*K.

Let M be a model, $k \in \mathbb{N}$, and $0 \leqslant l \leqslant k$.

- A *k-path* π_l is a pair (π, l) where π is a finite sequence $\pi = (s_0, \ldots, s_k)$ of states such that $(s_j, s_{j+1}) \in T$ for each $0 \leqslant j < k$.

- A k-path π_l is a *loop* if $l < k$ and $\pi(k) = \pi(l)$. If a k-path π_l is a loop it represents the infinite path of the form uv^ω, where $u = (\pi(0), \ldots, \pi(l))$ and $v = (\pi(l+1), \ldots, \pi(k))$. We denote this unique path by $\varrho(\pi_l)$. Note that for each $j \in \mathbb{N}$, $\varrho(\pi_l)^{l+j} = \varrho(\pi_l)^{k+j}$.

Let $\Pi_k(s)$ denote the set of all the k-paths starting at $s \in S$, $\Pi_k = \bigcup_{s^0 \in \iota} \Pi_k(s^0)$ denote the set of all the paths starting at initial states, s be a state of M, and π_l a k-path in Π_k. For a state formula α over $\mathcal{PV}$, the notation $M, s \models_k \alpha$ means that α is k-true at the state s in the model M. Similarly, for a path formula φ over $\mathcal{PV}$, the notation $M, \pi_l^m \models_k \varphi$, where $0 \leqslant m \leqslant k$, means that φ is k-true along the suffix $(\pi(m), \ldots, \pi(k))$ of π. The relation $\models_k$ is defined inductively as follows:

- $M, s \models_k \text{true}$, $M, s \not\models_k \text{false}$,
- $M, s \models_k p$ iff $p \in \mathcal{V}(s)$,
- $M, s \models_k \neg\alpha$ iff $M, s \not\models_k \alpha$,
- $M, s \models_k \alpha \wedge \beta$ iff $M, s \models_k \alpha$ and $M, s \models_k \beta$,
- $M, s \models_k \alpha \vee \beta$ iff $M, s \models_k \alpha$ or $M, s \models_k \beta$,
- $M, s \models_k \overline{\mathrm{K}}_{\mathbf{c}}\alpha$ iff $(\exists \pi_l \in \Pi_k)(\exists 0 \leqslant i \leqslant k)(s \sim_{\mathbf{c}} \pi(i)$ and $M, \pi_l^i \models_k \alpha)$,
- $M, s \models_k \overline{Y}_{\Gamma}\alpha$ iff $(\exists \pi_l \in \Pi_k)(\exists 0 \leqslant i \leqslant k)(s \sim_{\Gamma}^{Y} \pi(i)$ and $M, \pi_l^i \models_k \alpha)$, where $Y \in \{\mathrm{D}, \mathrm{E}, \mathrm{C}\}$,
- $M, s \models_k \overline{\mathrm{C}}_{\mathbf{c}_1 \to \mathbf{c}_2}\alpha$ iff $(\exists \pi_l \in \Pi_k)(\exists 0 \leqslant i \leqslant k)(s \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \pi(i)$ and $M, \pi_l^i \models_k \alpha)$,
- $M, s \models_k \overline{\mathrm{C}}_{\mathbf{c}_1 \to \Gamma}\alpha$ iff $(\exists \pi_l \in \Pi_k)(\exists 0 \leqslant i \leqslant k)(\forall \mathbf{c}_2 \in \Gamma)(s \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \pi(i)$ and $M, \pi_l^i \models_k \alpha)$,
- $M, s \models_k \mathrm{E}\varphi$ iff $(\exists \pi_l \in \Pi_k(s))(M, \pi_l^0 \models_k \varphi)$,
- $M, \pi_l^m \models_k \alpha$ iff $M, \pi(m) \models_k \alpha$,
- $M, \pi_l^m \models_k \varphi \wedge \psi$ iff $M, \pi_l^m \models_k \varphi$ and $M, \pi_l^m \models_k \psi$,
- $M, \pi_l^m \models_k \varphi \vee \psi$ iff $M, \pi_l^m \models_k \varphi$ or $M, \pi_l^m \models_k \psi$,
- $M, \pi_l^m \models_k \mathrm{X}\varphi$ iff ($m < k$ and $M, \pi_l^{m+1} \models_k \varphi$) or ($m = k$ and $l < k$ and $\pi(k) = \pi(l)$ and $M, \pi_l^{l+1} \models_k \varphi$),
- $M, \pi_l^m \models_k \varphi \mathrm{U} \psi$ iff $(\exists m \leqslant j \leqslant k)(M, \pi_l^j \models_k \psi$ and $(\forall m \leqslant i < j)\ M, \pi_l^i \models_k \varphi)$ or ($l < m$ and $\pi(k) = \pi(l)$ and $(\exists l < j < m)(M, \pi_l^j \models_k \psi$ and $(\forall l < i < j) M, \pi_l^i \models \varphi$ and $(\forall m \leqslant i \leqslant k) M, \pi_l^i \models_k \varphi))$,
- $M, \pi_l^m \models_k \varphi \mathrm{R} \psi$ iff $(\exists m \leqslant j \leqslant k)(M, \pi_l^j \models_k \varphi$ and $(\forall m \leqslant i \leqslant j) M, \pi_l^i \models_k \psi)$ or ($l < m$ and $\pi(k) = \pi(l)$ and $(\exists l < j < m)(M, \pi_l^j \models_k \varphi$ and $(\forall l < i \leqslant j) M, \pi_l^i \models \psi$ and $(\forall m \leqslant i \leqslant k) M, \pi_l^i \models_k \psi)$ or ($l < k$ and $\pi(k) = \pi(l)$ and $(\forall j \leqslant k)(j \geqslant min(m, l)$ implies $M, \pi_l^j \models_k \psi)$.

An ECCTL*K state formula α is k-valid (true) in M, denoted $M \models_k \varphi$, iff for each $s \in \iota$, $M, s \models_k \varphi$. The *bounded model checking problem* asks whether there exists $k \in \mathbb{N}$ such that $M \models_k \varphi$.

3.2. **Equivalence of the bounded and unbounded semantics.** The following theorem states that for a given model M and an ECCTL*K formula α there exists a bound such that the model checking problem can be reduced to the bounded model checking problem.

Theorem 1. *Let M be a model and α an* ECCTL*K *state formula. Then, for each $s \in \iota$, $M, s \models \alpha$ iff $M, s \models_k \alpha$ for some $k \in \mathbb{N}$.*

Proof. The theorem follows from Lemmas 2 and 6. □

Let us start by proving Lemma 1 showing that if an ECCTL*K path formula is k-true along the suffix $(\pi(m), \ldots, \pi(k))$ of a k-path π in the model M, then the formula is also true along any extension of the suffix in the model M. Next, we prove Lemma 2 showing that if a ECCTL*K state formula is k-true at the state s in the model M, then the formula is true at the state s in the model M. In the next lemmas we prove that if a ECCTL*K formula is true in the model M, then the formula is also k-true in the model M, for some $k > 0$.

Lemma 1. *Let M be a model. For every* ECCTL*K *path formula φ, every k-path π_l in M, and every $0 \leqslant m \leqslant k$, if $M, \pi_l^m \models_k \varphi$, then*

(1) if π_l is not a loop, then $M, \rho^m \models \varphi$ holds for each path $\rho \in M$ such that $\rho[0..k] = \pi$.
(2) if π_l is a loop, then $M, \varrho(\pi_l)^m \models \varphi$.

Proof. Assume that $M, \pi_l^m \models_k \varphi$ and consider the following cases:

(1) φ is a state formula. Then, let ρ be any path in M such that $\rho[0..k] = \pi$.
- If φ is not of the form $\mathrm{E}\psi$ or $\overline{\mathrm{K}}_{\mathbf{c}}\psi$ or $\overline{\mathrm{D}}_{\Gamma}\psi$ or $\overline{\mathrm{E}}_{\Gamma}\psi$ or $\overline{\mathrm{C}}_{\Gamma}\psi$ or $\overline{\mathrm{C}}_{\mathbf{c}_1 \to \mathbf{c}_2}\psi$ or $\overline{\mathrm{C}}_{\mathbf{c} \to \Gamma}\psi$, then the thesis of the lemma follows immediately from the fact that $\pi(m) = \rho(m)$.
- $\varphi = E\psi$. By induction hypothesis - see Lemma 2.10 of [20].
- $\varphi = Y\psi$ with $Y \in \{\overline{\mathrm{K}}_{\mathbf{c}}, \overline{\mathrm{D}}_{\Gamma}, \overline{\mathrm{E}}_{\Gamma}, \overline{\mathrm{C}}_{\Gamma}\}$. By induction hypothesis - see Lemma 3.1 of [17].
- If φ is of the form $\overline{\mathrm{C}}_{\mathbf{c}_1 \to \mathbf{c}_2}\psi$, then it follows from $M, \pi_l^m \models_k \varphi$ that there exists $\widetilde{\pi} \in \Pi_k$ and there exists j such that $0 \leqslant j \leqslant k$ and $\pi(m) \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \widetilde{\pi}(j)$ and $M, \widetilde{\pi}_l^j \models_k \psi$. By the inductive hypothesis $M, \widehat{\rho}^j \models \psi$ holds for every path $\widehat{\rho} \in M$ such that $\widehat{\rho}[0..k] = \widetilde{\pi}$. Moreover, $\widehat{\rho}(j) = \widetilde{\pi}(j)$ and $\pi(m) = \rho(m)$ and $\rho(m) \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \widehat{\rho}(j)$. Hence, $M, \rho^m \models \overline{\mathrm{C}}_{\mathbf{c}_1 \to \mathbf{c}_2}\psi$.
- If φ is of the form $\overline{\mathrm{C}}_{\mathbf{c}_1 \to \Gamma}\psi$, then it follows from $M, \pi_l^m \models_k \varphi$ that there exists $\widetilde{\pi} \in \Pi_k$ and there exists j such that $0 \leqslant j \leqslant k$ and $(\forall \mathbf{c}_2 \in \Gamma)$ $(\pi(m) \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \widetilde{\pi}(j)$ and $M, \widetilde{\pi}_l^j \models_k \psi)$. By the inductive hypothesis $M, \widehat{\rho}^j \models \psi$ holds for every path $\widehat{\rho} \in M$ such that $\widehat{\rho}[0..k] =$

$\widetilde{\pi}$. Moreover, $\widehat{\rho}(j) = \widetilde{\pi}(j)$ and $\pi(m) = \rho(m)$ and $\rho(m) \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \widehat{\rho}(j)$ for all $\mathbf{c}_2 \in \Gamma$. Hence, $M, \rho^m \models \overline{\mathrm{C}}_{\mathbf{c}_1 \to \mathbf{c}_2} \psi$.

- $\varphi = \psi_1 \wedge \psi_2 \mid \psi_1 \vee \psi_2 \mid \mathrm{X}\psi \mid \psi_1 \mathrm{U} \psi_2 \mid \psi_1 \mathrm{R} \psi_2$ - see Lemma 2.10 of [20].

□

Lemma 2. *Let M be a model and s be a state of M. For every* ECCTL*K *state formula α, if $M, s \models_k \alpha$, then $M, s \models \alpha$.*

Proof. The lemma follows directly for the propositional variables and their negations. Assume that the hypothesis holds for all the proper state subformulae of α.

(1) Let $\alpha = \alpha_1 \wedge \alpha_2 \mid \alpha_1 \vee \alpha_2 \mid \mathrm{E}\psi \mid Y\psi$, where α_1 and α_2 are state formulae, and ψ is a path formula, and $Y \in \{\overline{\mathrm{K}}_{\mathbf{c}}, \overline{\mathrm{D}}_{\Gamma}, \overline{\mathrm{E}}_{\Gamma}, \overline{\mathrm{C}}_{\Gamma}\}$ - see Lemma 3.2 of [17].

(2) Let $\alpha = \overline{\mathrm{C}}_{\mathbf{c}_1 \to \mathbf{c}_2} \psi$, where ψ is a path formula. By the definition of the bounded semantics we have that there exists a k-path $\pi_l \in \Pi_k$ and there exists j such that $0 \leqslant j \leqslant k$ and $M, \pi_l^j \models \psi$ and $s \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \pi(j)$. Thus, by Lemma 1 we have:
   (a) if π_l is not a loop, then $M, \rho \models \psi$ for each path ρ of M such that $\rho[0..k] = \pi$.
   (b) if π_l is a loop, then $M, \varrho(\pi_l) \models \psi$.

   Furthermore, if π_l is not a loop, then $s \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \rho(j)$. Otherwise, i.e., if π_l is a loop, then $s \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \varrho(\pi_l)(j)$. Therefore, by the definition of the unbounded semantics it follows that $M, s \models \overline{\mathrm{C}}_{\mathbf{c}_1 \to \mathbf{c}_2} \psi$.

(3) Let $\alpha = \overline{\mathrm{C}}_{\mathbf{c}_1 \to \Gamma} \psi$, where ψ is a path formula. By the definition of the bounded semantics we have that there exists a k-path $\pi_l \in \Pi_k$ and there exists j such that $0 \leqslant j \leqslant k$ and $M, \pi_l^j \models \psi$ and $s \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \pi(j)$ for all $\mathbf{c}_2 \in \Gamma$. Thus, by Lemma 1 we have:
   (a) if π_l is not a loop, then $M, \rho \models \psi$ for each path ρ of M such that $\rho[0..k] = \pi$.
   (b) if π_l is a loop, then $M, \varrho(\pi_l) \models \psi$.

   Furthermore, if π_l is not a loop, then $s \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \rho(j)$ for all $\mathbf{c}_2 \in \Gamma$. Otherwise, i.e., if π_l is a loop, then $s \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \varrho(\pi_l)(j)$ for all $\mathbf{c}_2 \in \Gamma$. Therefore, by the definition of the unbounded semantics it follows that $M, s \models \overline{\mathrm{C}}_{\mathbf{c}_1 \to \mathbf{c}_2} \psi$.

□

Lemma 3. (Theorem 3.1 of[2]) *Let M be a model, α an LTL formula, and ρ a path. Then, the following implication holds: $M, \rho \models \alpha$ implies that for some $k \geqslant 0$ and $0 \leqslant l \leqslant k$, $M, \pi_l \models_k \alpha$ with $\rho[0..k] = \pi$.*

Lemma 4. *Let M be a model, α an LTL formula, $Y \in \{\overline{\mathrm{K}}_{\mathbf{c}}, \overline{\mathrm{D}}_{\Gamma}, \overline{\mathrm{E}}_{\Gamma}, \overline{\mathrm{C}}_{\Gamma}, \overline{\mathrm{C}}_{\mathbf{c}_1 \to \mathbf{c}_2}, \overline{\mathrm{C}}_{\mathbf{c}_1 \to \Gamma}\}$, and ρ a path. Then, the following implication holds:*

$M, \rho(0) \models Y\alpha$ implies that for some $k \geqslant 0$ and $0 \leqslant l \leqslant k$, $M, \pi_l(0) \models_k Y\alpha$ with $\rho[0..k] = \pi$.

Proof. Let X^j denote the next-time operator applied j-times.

(1) $Y = \overline{\mathrm{K}}_{\mathbf{c}} \mid \overline{\mathrm{D}}_{\Gamma} \mid \overline{\mathrm{E}}_{\Gamma} \mid \overline{\mathrm{C}}_{\Gamma}$ - see Lemma 4 of [11].

(2) Let $Y = \overline{\mathrm{C}}_{\mathbf{c}_1 \to \mathbf{c}_2}$. Then $M, \rho(0) \models Y\alpha$ iff $(\exists \rho' \in \Pi)\ (\exists j \geqslant 0)(\rho(0) \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \rho'(j)$ and $M, \rho'^j \models \alpha)$. Since $\rho'(j)$ is reachable from an initial state of M, the checking of $M, \rho'^j \models \alpha$ is equivalent to the checking of $M, \rho'^0 \models X^j\alpha$. Now since $\mathrm{X}^j\alpha$ is a pure LTL formula, by Lemma 3 we have that for some $k \geqslant 0$ and $0 \leqslant l \leqslant k$, $M, \pi'^0_l \models_k \mathrm{X}^j\alpha$ with $\rho'[0..k] = \pi'$. This implies that $M, \pi'^j_l \models_k \alpha$ with $\rho'[0..k] = \pi'$, for some $k \geqslant 0$ and $0 \leqslant l \leqslant k$. Now, since $\rho(0) \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \rho'(j)$, we have $\pi(0) \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \pi'(j)$. Thus, by the bounded semantics we have that for some $k \geqslant 0$ and $0 \leqslant l \leqslant k$, $M, \pi_l(0) \models_k Y\alpha$ with $\rho[0..k] = \pi$.

(3) Let $Y = \overline{\mathrm{C}}_{\mathbf{c}_1 \to \Gamma}$. Then $M, \rho(0) \models Y\alpha$ iff $(\exists \rho' \in \Pi)\ (\exists j \geqslant 0)(\forall \mathbf{c}_2 \in \Gamma)(\rho(0) \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \rho'(j)$ and $M, \rho'^j \models \alpha)$. Since $\rho'(j)$ is reachable from an initial state of M, the checking of $M, \rho'^j \models \alpha$ is equivalent to the checking of $M, \rho'^0 \models X^j\alpha$. Now since $\mathrm{X}^j\alpha$ is a pure LTL formula, by Lemma 3 we have that for some $k \geqslant 0$ and $0 \leqslant l \leqslant k$, $M, \pi'^0_l \models_k \mathrm{X}^j\alpha$ with $\rho'[0..k] = \pi'$. This implies that $M, \pi'^j_l \models_k \alpha$ with $\rho'[0..k] = \pi'$, for some $k \geqslant 0$ and $0 \leqslant l \leqslant k$. Now, since $\rho(0) \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \rho'(j)$ for all $\mathbf{c}_2 \in \Gamma$, we have $\pi(0) \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \pi'(j)$. Thus, by the bounded semantics we have that for some $k \geqslant 0$ and $0 \leqslant l \leqslant k$, $M, \pi_l(0) \models_k Y\alpha$ with $\rho[0..k] = \pi$. □

Lemma 5. *Let M be a model, φ a ECLTLK formula, and ρ a run. Then, the following implication holds: $M, \rho \models \varphi$ implies that for some $k \geqslant 0$ and $0 \leqslant l \leqslant k$, $M, \pi_l \models_k \varphi$ with $\rho[0..k] = \pi$.*

Proof. (Induction on the length of φ) The lemma follows directly for the propositional variables and their negations. Assume that the hypothesis holds for all the proper subformulae of φ and consider φ to be of the following form:

(1) $\varphi = \psi_1 \vee \psi_2 \mid \psi_1 \wedge \psi_2 \mid \mathrm{X}\psi \mid \psi_1 \mathrm{U} \psi_2 \mid \psi_1 \mathrm{R} \psi_2$. Straightforward by the induction hypothesis and Lemma 3.

(2) Let $\varphi = Y\alpha$, and $Y, Y_1, \ldots, Y_n, Z \in \{\overline{\mathrm{K}}_{\mathbf{c}}, \overline{\mathrm{D}}_{\Gamma}, \overline{\mathrm{E}}_{\Gamma}, \overline{\mathrm{C}}_{\Gamma}, \overline{\mathrm{C}}_{\mathbf{c}_1 \to \mathbf{c}_2}, \overline{\mathrm{C}}_{\mathbf{c}_1 \to \Gamma}\}$, and $Y_1\alpha_1, \ldots, Y_n\alpha_n$ be the list of all "top level" proper Y-subformulae of α (i.e., each $Y_i\alpha_i$ is a subformula of $Y\alpha$, but it is not a subformula of any subformula $Z\beta$ of $Y\alpha$, where $Z\beta$ is different from $Y\alpha$ and from $Y\alpha_i$ for $i = 1, \ldots, n$). If this list is empty, then α is a "pure" LTL formula with no nested epistemic and commitment modalities. Hence, by Lemma 4 we

have $M, \rho \models \varphi$ implies that for some $k \geqslant 0$ and $0 \leqslant l \leqslant k$, $M, \pi_l \models_k \varphi$ with $\rho[0..k] = \pi$.

Otherwise, introduce for each $Y_i\alpha_i$ a new proposition q_i, where $i = 1, \ldots, n$. It is easy to show that we can augment with q_i the labelling of each state s of M initialising some path along which the epistemic or commitment formula $Y_i\alpha_i$ holds, and then translate the formula α to the formula α', which instead of each subformula $Y_i\alpha_i$ contains adequate propositions q_i. Therefore, we can obtain "pure" LTL formula. Hence, by Lemma 4 we have $M, \rho \models \varphi$ implies that for some $k \geqslant 0$ and $0 \leqslant l \leqslant k$, $M, \pi_l \models_k \varphi$ with $\rho[0..k] = \pi$.

□

Lemma 6. *Let M be a model, s a state of M, and α a* ECCTL*K *state formula. If $M, s \models \alpha$, then $M, s \models_k \alpha$ for some $k \in \mathbb{N}$.*

Proof. The lemma follows directly for the propositional variables and their negations. Assume that the hypothesis holds for all the proper state subformulae of α.

(1) Let $\alpha = \alpha_1 \wedge \alpha_2 \mid \alpha_1 \vee \alpha_2$. The proof is straightforward.
(2) Let $\alpha = Y\beta$ and $Y \in \{\mathrm{E}, \overline{\mathrm{K}}_{\mathbf{c}}, \overline{\mathrm{D}}_{\Gamma}, \overline{\mathrm{E}}_{\Gamma}, \overline{\mathrm{C}}_{\Gamma}\}$ – see Lemma 3.7 of [17].
(3) Let $\alpha = \overline{\mathrm{C}}_{\mathbf{c}_1 \to \mathbf{c}_2}\beta$. By the definition of the unbounded semantics we have $(\exists \pi \in \Pi)(\exists i \geqslant 0)(s \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \pi(i)$ and $M, \pi^i \models \beta)$. next, by the same definition we have $M, \pi(i) \models \beta$. Thus, by the inductive assumption we have $M, \pi(i) \models_k \beta$. Hence, by the definition of the bounded semantics we get $M, \pi^i_l \models_k \beta$. Further, since $s \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \pi(i)$, we can conclude that $M, s \models_k \overline{\mathrm{C}}_{\mathbf{c}_1 \to \mathbf{c}_2}\beta$.
(4) Let $\alpha = \overline{\mathrm{C}}_{\mathbf{c}_1 \to \Gamma}\beta$. By the definition of the unbounded semantics we have $(\exists \pi \in \Pi)(\exists i \geqslant 0)(\forall \mathbf{c}_2 \in \Gamma)(s \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \pi(i)$ and $M, \pi^i \models \beta)$. Next, by the same definition we have $M, \pi(i) \models \beta$. Thus, by the inductive assumption we have $M, \pi(i) \models_k \beta$. Hence, by the definition of the bounded semantics we get $M, \pi^i_l \models_k \beta$. Further, since $s \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \pi(i)$ for all $\mathbf{c}_2 \in \Gamma$, we can conclude that $M, s \models_k \overline{\mathrm{C}}_{\mathbf{c}_1 \to \Gamma}\beta$.

□

3.3. **Translation to quantifier-free first-order formulae.** Let $M = (Act, S, \iota, T, \mathcal{V}, \sim_{\mathbf{c}}, \sim_{\mathbf{c}_1 \to \mathbf{c}_2})$ be a model, α an ECCTL*K state formula, and $k \in \mathbb{N}$ a bound. We define the quantifier-free first-order formula:

$$[M, \alpha]_k := [M^{\alpha,\iota}]_k \wedge [\alpha]_{M,k} \tag{1}$$

which is satisfiable if and only if $M \models_k \alpha$ holds. More precisely, let $\mathbf{c} \in \mathbb{A} \cup \{\mathcal{E}\}$. The definition of the formula $[M, \alpha]_k$ assumes that:

- each state $s \in S$ is represented by a valuation of a *symbolic state* $\mathbf{w} = (\mathtt{w}_1, \ldots, \mathtt{w}_n, \mathtt{w}_{\mathcal{E}})$ that consists of *symbolic local states* and each symbolic local

state $\mathtt{w}_{\mathbf{c}}$ is a vector of individual variables ranging over the non-negative integer numbers,
- each joint action $a \in Act$ is represented by a valuation of a *symbolic action* $\overline{a} = (\mathtt{a}_1, \ldots, \mathtt{a}_n, \mathtt{a}_{\mathcal{E}})$ that consists of *symbolic local actions* and each symbolic local action $\mathtt{a}_{\mathbf{c}}$ is an individual variables ranging over the non-negative integer numbers,
- each non-negative integer number from the set $\{0, \ldots, k\}$ is represented by a valuation of a *symbolic number* $\mathbf{u}$, which is an individual variables ranging over the non-negative integer numbers.

Furthermore, the definition of the formula $[M, \alpha]_k$ uses the auxiliary function $f_k : \mathrm{ECCTL}^\star\mathrm{K} \to \mathbb{N}$ that returns the number of k-paths of the model M that are sufficient to validate an ECCTL*K formula. The formal definition of the function is the following. Let $p \in \mathcal{PV}$. The function is defined as:

- $f_k(\mathrm{true}) = f_k(\mathrm{false}) = f_k(p) = f_k(\neg p) = 0$,
- $f_k(\varphi \wedge \phi) = f_k(\varphi) + f_k(\phi)$,
- $f_k(\varphi \vee \phi) = max\{f_k(\varphi), f_k(\phi)\}$,
- $f_k(\mathrm{X}\varphi) = f_k(\varphi)$,
- $f_k(\varphi \mathrm{U} \phi) = k \cdot f_k(\varphi) + f_k(\phi)$,
- $f_k(\varphi \mathrm{R} \phi) = (k+1) \cdot f_k(\phi) + f_k(\varphi)$,
- $f_k(\overline{\mathrm{C}}_\Gamma \varphi) = f_k(\varphi) + k$,
- $f_k(Y\varphi) = f_k(\varphi) + 1$, for $Y \in \{\overline{\mathrm{K}}_{\mathbf{c}}, \overline{\mathrm{D}}_\Gamma, \overline{\mathrm{E}}_\Gamma, \overline{\mathrm{C}}_{\mathbf{c}_1 \to \mathbf{c}_2}, \overline{\mathrm{C}}_{\mathbf{c}_1 \to \Gamma}\}$.

Finally, the definition of $[M, \varphi]_k$ uses the following auxiliary quantifier-free first-order formulae:

- $p(\mathbf{w})$ - encodes a set of states of M in which proposition variable $p \in \mathcal{PV}$ holds.
- $I_s(\mathbf{w})$ - encodes the state s of the model M.
- $H(\mathbf{w}, \mathbf{w}')$ - encodes equality of two symbolic states.
- $H_{\mathbf{c}}(\mathbf{w}, \mathbf{w}')$ - encodes that the local states of agent $\mathbf{c} \in \mathbb{A}$ are the same in the symbolic states $\mathbf{w}$ and $\mathbf{w}'$.
- $\mathcal{S}_{\mathbf{c}_1 \to \mathbf{c}_2}(\mathbf{w}, \mathbf{w}')$ - encodes the social accessibility relation for agents $\mathbf{c}_1, \mathbf{c}_2 \in \mathbb{A}$.
- $\mathcal{A}(\overline{a})$ - encodes that each symbolic local action $\mathtt{a}_{\mathbf{c}}$ of $\overline{a}$ has to be executed by each agent in which it appears.
- $\mathcal{T}_{\mathbf{c}}(\mathtt{w}_{\mathbf{c}}, \mathtt{w}_{\mathcal{E}}, \overline{a}, \mathtt{w}'_{\mathbf{c}})$ - encodes the local evolution function of agent $\mathbf{c} \in \mathbb{A}$.
- $\mathcal{T}_{\mathcal{E}}(\mathtt{w}_{\mathcal{E}}, \overline{a}, \mathtt{w}'_{\mathcal{E}})$ - encodes the local evolution function of the environment $\mathcal{E}$.
- $\mathcal{T}(\mathbf{w}, \overline{a}, \mathbf{w}') := \bigwedge_{\mathbf{c} \in \mathbb{A}} \mathcal{T}_{\mathbf{c}}(\mathtt{w}_{\mathbf{c}}, \overline{a}, \mathtt{w}'_{\mathbf{c}}) \wedge \mathcal{T}_{\mathcal{E}}(\mathtt{w}_{\mathcal{E}}, \overline{a}, \mathtt{w}'_{\mathcal{E}}) \wedge \mathcal{A}(\overline{a})$ - encodes the transition relation of the model M.
- $\mathcal{N}_j^{\sim}(\mathbf{u})$ - encodes that the value j is in the arithmetic relation $\sim \in \{<, >, \leqslant, =, \geqslant\}$ with the value represented by the symbolic number $\mathbf{u}$.

- $\boldsymbol{\pi}_j := (\mathbf{w}_{0,j} \xrightarrow{\overline{a}_{1,j}} \mathbf{w}_{1,j} \xrightarrow{\overline{a}_{2,j}} \ldots \xrightarrow{\overline{a}_{k,j}} \mathbf{w}_{k,j}, \mathbf{u})$, where $\mathbf{u}$ is the symbolic number, $\mathbf{w}_{i,j}$ are symbolic states, $\overline{a}_{i,j}$ are symbolic actions, $0 \leqslant i \leqslant k$, and $1 \leqslant j \leqslant f_k(\alpha)$ - encodes the j-th k-path.
- $\mathcal{L}_k^l(\boldsymbol{\pi}_j) := \mathcal{N}_l^{=}(\mathbf{u}_j) \wedge H(\mathbf{w}_{k,j}, \mathbf{w}_{l,j})$, where $l < k$ and $k \in \mathbb{N}$ - encodes that the j-th k-path is a loop.

Let $\mathbf{w}_{i,j}$, $\overline{a}_{i,j}$, and $\mathbf{u}_j$ are, respectively, symbolic states, symbolic actions, and symbolic numbers, for $0 \leqslant i \leqslant k$ and $1 \leqslant j \leqslant f_k(\alpha)$. The formula $[M^{\alpha,\iota}]_k$, which encodes a rooted tree of $k-$paths of the model M, is defined as follows:

$$[M^{\alpha,\iota}]_k := \bigvee_{s \in \iota} I_s(\mathbf{w}_{0,0}) \wedge \bigwedge_{j=1}^{f_k(\alpha)} \bigvee_{l=0}^{k} \mathcal{N}_l^{=}(\mathbf{u}_j) \wedge \bigwedge_{j=1}^{f_k(\alpha)} \bigwedge_{i=0}^{k-1} \mathcal{T}(\mathbf{w}_{i,j}, \overline{a}_{i+1,j}, \mathbf{w}_{i+1,j})$$

We shall now proceed to define the quantifier-free first-order formula $[\alpha]_{M,k}$, which encodes the bounded semantics of a ECCTL*K state formula α. The main idea of this translation consists in translating every subformula φ of α using only $f_k(\varphi)$ k-paths. To be clear, given a formula α and a set $F_k(\alpha) = \{j \in \mathbb{N} \mid 1 \leqslant j \leqslant f_k(\alpha)\}$ of indices of k-paths, following [20], we divide the set $F_k(\alpha) \subset \mathbb{N}$ into subsets needed for translating the subformulae of α. The partition process is based on the relation $\prec$ that is defined on the power set of $\mathcal{N}$ as: $A \prec B$ iff for all natural numbers x and y, if $x \in A$ and $y \in B$, then $x < y$. Furthermore, it employs the following auxiliary functions of [20]. Let $A \subset \mathbb{N}$ be a finite non-empty set, and $n, m \in \mathcal{N}$, where $m \leqslant |A|$. Then,

- $g_l(A, m)$ denotes the subset B of A such that $|B| = m$ and $B \prec A \setminus B$.
- $g_r(A, m)$ denotes the subset C of A such that $|C| = m$ and $A \setminus C \prec C$.
- $g_s(A)$ denotes the set $A \setminus \{min(A)\}$.
- if n divides $|A| - m$, then $hp(A, m, n)$ denotes the sequence $(B_0, \ldots, B_n)$ of subsets of A such that $\bigcup_{j=0}^{n} B_j = A$, $|B_0| = \ldots = |B_{n-1}|$, $|B_n| = m$, and $B_i \prec B_j$ for every $0 \leqslant i < j \leqslant n$.

We assume that $h_k^{\mathrm{U}}(A, m) \stackrel{df}{=} hp(A, m, k)$, and $h_k^{\mathrm{R}}(A, m) \stackrel{df}{=} hp(A, m, k+1)$. Thus, if $h_k^{\mathrm{U}}(A, m) = (B_0, \ldots, B_k)$, then $h_k^{\mathrm{U}}(A, m)(j)$ denotes the set B_j, for every $0 \leqslant j \leqslant k$. Similarly, if $h_k^{\mathrm{R}}(A, m) = (B_0, \ldots, B_{k+1})$, then $h_k^{\mathrm{R}}(A, m)(j)$ denotes the set B_j, for every $0 \leqslant j \leqslant k+1$. For more details we refer to [20].

In the definition of $[\alpha]_{M,k}$ we assume the fundamental notation, the crucial auxiliary quantifier-free first-order formulae and the auxiliary partition functions which have been introduced above. Next, we assume that $\langle\alpha\rangle_k^{[m,n,A]}$ denotes the translation of a ECCTL*K state formula α at the symbolic state $\mathbf{w}_{m,n}$ by using the set A, and by $[\varphi]_k^{[m,n,A]}$ we denote the

translation of a ECCTL*K path formula φ along the n-th symbolic k-path $\boldsymbol{\pi}_n$ with starting point m by using the set A.

The quantifier-free first-order formula $[\alpha]_{M,k}$ is defined as $\langle\alpha\rangle_k^{[0,0,F_k(\alpha)]}$, where $F_k(\alpha) = \{j \in \mathbb{N} \mid 1 \leqslant j \leqslant f_k(\alpha)\}$, and:

- $\langle \mathrm{true}\rangle_k^{[m,n,A]} := \mathrm{true}$, • $\langle \mathrm{false}\rangle_k^{[m,n,A]} := \mathrm{false}$,
- $\langle p\rangle_k^{[m,n,A]} := p(\mathbf{w}_{m,n})$, • $\langle \neg p\rangle_k^{[m,n,A]} := \neg p(\mathbf{w}_{m,n})$,
- $\langle \alpha \wedge \beta\rangle_k^{[m,n,A]} := \langle\alpha\rangle_k^{[m,n,g_l(A,f_k(\alpha))]} \wedge \langle\beta\rangle_k^{[m,n,g_r(A,f_k(\beta))]}$,
- $\langle \alpha \vee \beta\rangle_k^{[m,n,A]} := \langle\alpha\rangle_k^{[m,n,g_l(A,f_k(\alpha))]} \vee \langle\beta\rangle_k^{[m,n,g_l(A,f_k(\beta))]}$,
- $\left\langle \overline{\mathrm{K}}_{\mathbf{c}}\alpha\right\rangle_k^{[m,n,A]} := I_s \wedge \bigvee_{j=0}^{k}([\alpha]_k^{[j,n',g_s(A)]} \wedge H_{\mathbf{c}}(\mathbf{w}_{m,n}, \mathbf{w}_{j,n'}))$,
- $\left\langle \overline{\mathrm{D}}_{\Gamma}\alpha\right\rangle_k^{[m,n,A]} := I_s \wedge \bigvee_{j=0}^{k}([\alpha]_k^{[j,n',g_s(A)]} \wedge \bigwedge_{\mathbf{c}\in\Gamma} H_{\mathbf{c}}(\mathbf{w}_{m,n}, \mathbf{w}_{j,n'}))$,
- $\left\langle \overline{\mathrm{E}}_{\Gamma}\alpha\right\rangle_k^{[m,n,A]} := I_s \wedge \bigvee_{j=0}^{k}([\alpha]_k^{[j,n',g_s(A)]} \wedge \bigvee_{\mathbf{c}\in\Gamma} H_{\mathbf{c}}(\mathbf{w}_{m,n}, \mathbf{w}_{j,n'}))$,
- $\left\langle \overline{\mathrm{C}}_{\Gamma}\alpha\right\rangle_k^{[m,n,A]} := \left\langle \bigvee_{j=1}^{k}(\overline{\mathrm{E}}_{\Gamma})^j\alpha\right\rangle_k^{[m,n,A]}$,
- $\left\langle \overline{\mathrm{C}}_{\mathbf{c}_1\to\mathbf{c}_2}\alpha\right\rangle_k^{[m,n,A]} := I_s \wedge \bigvee_{j=0}^{k}([\alpha]_k^{[j,n',g_s(A)]} \wedge \mathcal{S}_{\mathbf{c}_1\to\mathbf{c}_2}(\mathbf{w}_{m,n}, \mathbf{w}_{j,n'}))$,
- $\left\langle \overline{\mathrm{C}}_{\mathbf{c}_1\to\Gamma}\alpha\right\rangle_k^{[m,n,A]} := I_s \wedge \bigvee_{j=0}^{k}([\alpha]_k^{[j,n',g_s(A)]} \wedge \bigwedge_{\mathbf{c}_2\in\Gamma} \mathcal{S}_{\mathbf{c}_1\to\mathbf{c}_2}(\mathbf{w}_{m,n}, \mathbf{w}_{j,n'}))$,
- $\langle \mathrm{E}\varphi\rangle_k^{[m,n,A]} := H(\mathbf{w}_{m,n}, \mathbf{w}_{0,n'}) \wedge [\varphi]_k^{[0,n',g_s(A)]}$,
- $[\alpha]_k^{[m,n,A]} := \langle\alpha\rangle_k^{[m,n,A]}$,
- $[\varphi \wedge \psi]_k^{[m,n,A]} := [\varphi]_k^{[m,n,g_l(A,f_k(\varphi))]} \wedge [\psi]_k^{[m,n,g_r(A,f_k(\psi))]}$,
- $[\varphi \vee \psi]_k^{[m,n,A]} := [\varphi]_k^{[m,n,g_l(A,f_k(\varphi))]} \vee [\psi]_k^{[m,n,g_l(A,f_k(\psi))]}$,
- $[\mathrm{X}\varphi]_k^{[m,n,A]} := \begin{cases} [\varphi]_k^{[m+1,n,A]}, & \text{if } m < k \\ \bigvee_{l=0}^{k-1}(\mathcal{L}_k^l(\boldsymbol{\pi}_n) \wedge [\varphi]_k^{[l+1,n,A]}), & \text{if } m = k \end{cases}$
- $[\varphi\mathrm{U}\psi]_k^{[m,n,A]} := \bigvee_{j=m}^{k}([\psi]_k^{[j,n,h_k^{\mathrm{U}}(A,f_k(\psi))(k)]} \wedge \bigwedge_{i=m}^{j-1}[\varphi]_k^{[i,n,h_k^{\mathrm{U}}(A,f_k(\psi))(i)]}) \vee \Big(\bigvee_{l=0}^{m-1}\left(\mathcal{L}_k^l(\boldsymbol{\pi}_n)\right) \wedge \bigwedge_{i=m}^{k}[\varphi]_k^{[i,n,h_k^{\mathrm{U}}(A,f_k(\psi))(i)]} \wedge \bigvee_{j=0}^{m-1}\left(\mathcal{N}_j^{>}(\mathbf{u}_n) \wedge [\psi]_k^{[j,n,h_k^{\mathrm{U}}(A,f_k(\psi))(k)]} \wedge \bigwedge_{i=0}^{j-1}(\mathcal{N}_i^{>}(\mathbf{u}_n) \to [\varphi]_k^{[i,n,h_k^{\mathrm{U}}(A,f_k(\psi))(i)]})\right)\Big)$,
- $[\varphi\mathrm{R}\psi]_k^{[m,n,A]} := \bigvee_{j=m}^{k}\Big([\varphi]_k^{[j,n,h_k^{\mathrm{R}}(A,f_k(\varphi))(k+1)]} \wedge \bigwedge_{i=m}^{j}[\psi]_k^{[i,n,h_k^{\mathrm{R}}(A,f_k(\varphi))(i)]}\Big) \vee \Big(\bigvee_{l=0}^{m-1}(\mathcal{L}_k^l(\boldsymbol{\pi}_n)) \wedge \bigvee_{j=0}^{m}\left(\mathcal{N}_j^{>}(\mathbf{u}_n) \wedge [\varphi]_k^{[j,n,h_k^{\mathrm{R}}(A,f_k(\varphi))(k+1)]} \wedge \bigwedge_{i=0}^{j-1}(\mathcal{N}_i^{>}(\mathbf{u}_n) \to [\psi]_k^{[i,n,h_k^{\mathrm{R}}(A,f_k(\varphi))(i)]}) \wedge \bigwedge_{i=m}^{k}[\psi]_k^{[i,n,h_k^{\mathrm{R}}(A,f_k(\varphi))(i)]}\right)\Big) \vee \Big(\bigvee_{l=0}^{k-1}\left(\mathcal{L}_k^l(\boldsymbol{\pi}_n)\right) \wedge \bigwedge_{j=0}^{m-1}\left(\mathcal{N}_j^{\geqslant}(\mathbf{u}_n) \to [\psi]_k^{[j,n,h_k^{\mathrm{R}}(A,f_k(\varphi))(j)]}\right) \wedge \bigwedge_{j=m}^{k}[\psi]_k^{[j,n,h_k^{\mathrm{R}}(A,f_k(\varphi))(j)]}\Big)$.

where $n' = min(A)$, and I_s denotes the formula $\bigvee_{s\in\iota} I_s(\mathbf{w}_{0,min(A)})$.

3.4. **Correctness and completeness of the translation.** Let $V : PV \to \mathbb{N}$ be a *valuation of individual variables ranging over the non-negative integer numbers* (a *valuation* for short). To prove the correctness of the translation we have to show that for each valuation V, if V satisfies the translation of a ECCTL*K formula for some $k \in \mathbb{N}$, then this formula is k-true along the k-path corresponding to the valuation V.

Before we formulate the appropriate lemmas, let us first introduce the following auxiliary notations:

- For every $m, a, b \in \mathbb{N}_+$, each valuation V induces the following functions:
  - $\mathbf{S} : SV^m \to \mathbb{N}^m$ defined as: $\mathbf{S}((\mathtt{w}_1, \ldots, \mathtt{w}_m)) = ((V(\mathtt{w}_{1_1}), \ldots, V(\mathtt{w}_{1_a})), \ldots, (V(\mathtt{w}_{m_1}), \ldots, V(\mathtt{w}_{m_b}))$,
  - $\mathbf{A} : AV^m \to \mathbb{N}^m$ defined as: $\mathbf{A}((\mathtt{a}_1, \ldots, \mathtt{a}_m)) = (V(\mathtt{a}_1), \ldots, V(\mathtt{a}_m))$.
- Let $A = \{j \in \mathbb{N} \mid 1 \leqslant j \leqslant n\}$ be a finite set of indexes of symbolic k-paths, for some $n \in \mathbb{N}$. The *unfolding of the transition relation*, denoted $[M]_k^A$, is defined as:

$$[M]_k^A := \bigwedge_{j \in A} \bigvee_{l=0}^{k} \mathcal{N}_l^{=}(\mathbf{u}_j) \wedge \bigwedge_{j \in A} \bigwedge_{i=0}^{k-1} \mathcal{T}(\mathbf{w}_{i,j}, \overline{a}_{i+1,j}, \mathbf{w}_{i+1,j})$$

  Thus, for an ECCTL*K state formula α, and $F_k(\alpha) = \{j \in \mathbb{N} \mid 1 \leqslant j \leqslant f_k(\alpha)\}$, we have $[M^{\alpha,\iota}]_k = \bigvee_{s \in \iota} I_s(\mathbf{w}_{0,0}) \wedge [M]_k^{F_k(\alpha)}$.
- For every ECCTL*K state subformula β of α, the symbol $\langle\beta\rangle_k^{[\alpha,m,n,A]}$ denotes the quantifier-free first-order formula $[M]_k^{F_k(\alpha)} \wedge \langle\beta\rangle_k^{[m,n,A]}$.
- For every ECCTL*K path subformula φ of α, the symbol $[\varphi]_k^{[\alpha,m,n,A]}$ denotes the quantifier-free first-order formula $[M]_k^{F_k(\alpha)} \wedge [\varphi]_k^{[m,n,A]}$.
- The notation $V \Vdash \xi$ means that the valuation V satisfies the quantifier-free first-order formula ξ.

Taking into account the above, we write $s \models_k \alpha$ instead of $M, s \models_k \alpha$, $\pi_l^m \models_k \varphi$ instead of $M, \pi_l^m \models_k \varphi$, $s_{i,j}$ instead of $\mathbf{S}(\mathbf{w}_{i,j})$, $a_{i,j}$ instead of $\mathbf{A}(\overline{a}_{i,j})$, and l_j instead of $V(\mathbf{u}_j)$.

Lemma 7 (Correctness of the translation)**.** *Let M be a model, α be a* ECCTL*K *state formula and $k \in \mathbb{N}$. For every subformula φ of the formula α, every $(m, n) \in \{0, \ldots, k\} \times F_k(\alpha)$, every $A \subseteq F_k(\alpha) \setminus \{n\}$ such that $|A| = f_k(\varphi)$, and every valuation V, the following condition holds: $V \Vdash [\varphi]_k^{[\alpha,m,n,A]}$ implies $((s_{0,n}, \ldots, s_{k,n}), l_n)^m \models_k \varphi$.*

Proof. For convenience, by π_l we denote the k-path $((s_{0,n}, \ldots, s_{k,n}), l_n)$.

A. $\varphi = \text{true} \mid \text{false} \mid p \mid \neg p \mid \psi_1 \wedge \psi_2 \mid \psi_1 \vee \psi_2 \mid \mathrm{E}\psi \mid \mathrm{X}\psi \mid \psi_1 \mathrm{U} \psi_2 \mid \psi_1 \mathrm{R} \psi_2$, where $p \in \mathcal{PV}$ – see Lemma 3.3 of [20].

B. $\varphi = \overline{\mathrm{K}}_{\mathbf{c}}\psi \mid \overline{\mathrm{D}}_\Gamma\psi \mid \overline{\mathrm{E}}_\Gamma\psi \mid \overline{\mathrm{C}}_\Gamma\psi$ – see Lemma 4.1 of [17]

C. $\varphi = \overline{\mathrm{C}}_{\mathbf{c}_1\to\mathbf{c}_2}\psi$. Let $n' = \min(A)$, and $\widetilde{\pi}_{l'} = ((s_{0,n'},\ldots,s_{k,n'}),l_{n'})$ such that $s_{0,n'} \in \iota$. From $V \Vdash [\overline{\mathrm{C}}_{\mathbf{c}_1\to\mathbf{c}_2}\psi]_k^{[\alpha,m,n,A]}$, we obtain that $V \Vdash \langle\overline{\mathrm{C}}_{\mathbf{c}_1\to\mathbf{c}_2}\psi\rangle_k^{[\alpha,m,n,A]}$. Thus, we have

$$V \Vdash \bigvee_{s\in\iota} I_s(\mathbf{w}_{0,n'}) \wedge \bigvee_{j=0}^{k}([\psi]_k^{[\alpha,j,n',g_s(A)]} \wedge \mathcal{S}_{\mathbf{c}_1\to\mathbf{c}_2}(\mathbf{w}_{m,n},\mathbf{w}_{j,n'})).$$

Since $V \Vdash \mathcal{S}_{\mathbf{c}_1\to\mathbf{c}_2}(\mathbf{w}_{m,n},\mathbf{w}_{j,n'})$ holds, we have $s_{m,n} \sim_{\mathbf{c}_1\to\mathbf{c}_2} s_{j,n'}$, for some $0 \leqslant j \leqslant k$. Next, by inductive hypotheses, we have $\widetilde{\pi}_{l'}^{j} \models_k \psi$ for some $0 \leqslant j \leqslant k$. Therefore, we get $s_{m,n} \models \overline{\mathrm{C}}_{\mathbf{c}_1\to\mathbf{c}_2}\psi$. Thus, $\pi_l^m \models_k \overline{\mathrm{C}}_{\mathbf{c}_1\to\mathbf{c}_2}\psi$, for $s_{m,n} = \pi(m)$.

D. $\varphi = \overline{\mathrm{C}}_{\mathbf{c}_1\to\Gamma}\psi$. Let $n' = \min(A)$, and $\widetilde{\pi}_{l'} = ((s_{0,n'},\ldots,s_{k,n'}),l_{n'})$ such that $s_{0,n'} \in \iota$. From $V \Vdash [\overline{\mathrm{C}}_{\mathbf{c}_1\to\Gamma}\psi]_k^{[\alpha,m,n,A]}$, we obtain that $V \Vdash \langle\overline{\mathrm{C}}_{\mathbf{c}_1\to\Gamma}\psi\rangle_k^{[\alpha,m,n,A]}$. Thus, we have

$$V \Vdash \bigvee_{s\in\iota} I_s(\mathbf{w}_{0,n'}) \wedge \bigvee_{j=0}^{k}([\psi]_k^{[\alpha,j,n',g_s(A)]} \wedge \bigwedge_{\mathbf{c}_2\in\Gamma} \mathcal{S}_{\mathbf{c}_1\to\Gamma}(\mathbf{w}_{m,n},\mathbf{w}_{j,n'})).$$

Since $V \Vdash \mathcal{S}_{\mathbf{c}_1\to\mathbf{c}_2}(\mathbf{w}_{m,n},\mathbf{w}_{j,n'})$ holds for all $\mathbf{c}_2 \in \Gamma$, we have $s_{m,n} \sim_{\mathbf{c}_1\to\mathbf{c}_2} s_{j,n'}$, for some $0 \leqslant j \leqslant k$ and for all $\mathbf{c}_2 \in \Gamma$. Next, by inductive hypotheses, we have $\widetilde{\pi}_{l'}^{j} \models_k \psi$ for some $0 \leqslant j \leqslant k$. Therefore, we get $s_{m,n} \models \overline{\mathrm{C}}_{\mathbf{c}_1\to\Gamma}\psi$. Thus, $\pi_l^m \models_k \overline{\mathrm{C}}_{\mathbf{c}_1\to\Gamma}\psi$, for $s_{m,n} = \pi(m)$.

□

Lemma 8 (Correctness of the translation of state formulae)**.** *Let M be a model, α be an* ECCTL⋆K *state formula and $k \in \mathbb{N}$. For every subformula β of the formula α, every $A \subseteq F_k(\alpha)$ such that $|A| = f_k(\beta)$, and every valuation V, the following condition holds: $V \Vdash \langle\beta\rangle_k^{[\alpha,m,n,A]}$ implies $\mathbf{S}(\mathbf{w}_{m,m}) \models_k \beta$.*

Proof. We omit the proof since it is analogous to the proof of Lemma 7. □

Let $Var(B)$ denotes the set of all the individual variables appearing in all the symbolic states of all the symbolic k-paths whose indices are taken from the set B. Notice that if $B \cap C = \emptyset$, then $Var(B) \cap Var(C) = \emptyset$. This property is used in the proof of the following lemma. Moreover, for every valuation V and every set of indices B, by $V \restriction B$ we denote the restriction of the valuation V to the set $Var(B)$.

Lemma 9 (Completeness of the translation)**.** *Let M be a model, $k \in \mathbb{N}$, and α be an* ECCTL⋆K *state formula such that $f_k(\alpha) > 0$. For every subformula φ of the formula α, every $(m,n) \in \{(0,0)\} \cup \{0,\ldots,k\} \times F_k(\alpha)$, every $A \subseteq F_k(\alpha) \setminus \{n\}$ such that $|A| = f_k(\varphi)$, and every k-path π_l, the following condition holds: $\pi_l^m \models_k \varphi$ implies that there exists a valuation V such that $\pi_l = ((s_{0,n},\ldots,s_{k,n}),l_n)$ and $V \Vdash [\varphi]_k^{[\alpha,m,n,A]}$.*

Proof. First, let us note that given an ECCTL*K state formula α, and non-negative integer numbers k, m, n with $0 \leqslant m \leqslant k$ and $n \in F_k(\alpha)$, there exist a valuation V such $V \Vdash [M]_k^{F_k(\alpha)}$, since M has no terminal states. Now we proceed by induction on the complexity of φ. Let $n \in F_k(\alpha)$, A be a set such that $A \subseteq F_k(\alpha) \setminus \{n\}$ and $|A| = f_k(\varphi)$, π_l be a k-path in M, and m be a non-negative integer number such that $0 \leqslant m \leqslant k$. Suppose that $M, \pi_l^m \models_k \varphi$ and consider the following cases:

A. $\varphi = \text{true} \mid \text{false} \mid p \mid \neg p \mid \psi_1 \wedge \psi_2 \mid \psi_1 \vee \psi_2 \mid \mathrm{E}\psi \mid \mathrm{X}\psi \mid \psi_1 \mathrm{U} \psi_2 \mid \psi_1 \mathrm{R} \psi_2$, where $p \in \mathcal{PV}$ – see Lemma 3.5 of [20].

B. $\varphi = \overline{\mathrm{K}}_{\mathbf{c}}\psi$. Since $M, \pi_l^m \models_k \overline{\mathrm{K}}_{\mathbf{c}}\psi$, we have $M, \pi(m) \models_k \overline{\mathrm{K}}_{\mathbf{c}}\psi$. Thus, there exists a k-path $\pi'_{l'}$ and there exists $0 \leqslant i \leqslant k$ such that $\pi(m) \sim_{\mathbf{c}} \pi'(i)$ and $M, \pi'^i_{l'} \models_k \psi$. By inductive hypothesis and the definition of formula $\mathcal{H}_{\mathbf{c}}$, there exists a valuation V' such that $V' \Vdash [M]_k^{F_k(\alpha)}$ and $V' \Vdash [\psi]_k^{[i,min(A),g_s(A)]} \wedge H_{\mathbf{c}}(\mathbf{w}_{m,n}, \mathbf{w}_{i,min(A)})$ for some $0 \leqslant i \leqslant k$. Thus, we have

$$V' \Vdash \bigvee_{i=0}^{k} \big([\psi]_k^{[i,min(A),g_s(A)]} \wedge H_{\mathbf{c}}(\mathbf{w}_{m,n}, \mathbf{w}_{i,min(A)})\big).$$

Further, since $\pi'_{l'} \in \bigcup_{s^0 \in \iota} \Pi_k(s^0)$, we have $\pi'_{l'}(0) = s^0$ for some $s^0 \in \iota$. By the definition of the formula I, we get $V' \Vdash \bigvee_{s^0 \in \iota} I_{s^0}(\mathbf{w}_{0,min(A)})$. Therefore, we have $V' \Vdash \bigvee_{s^0 \in \iota} I_{s^0}(\mathbf{w}_{0,min(A)}) \wedge \bigvee_{i=0}^{k} \big([\psi]_k^{[i,min(A),g_s(A)]} \wedge H_{\mathbf{c}}(\mathbf{w}_{m,n}, \mathbf{w}_{i,min(A)})\big)$, which implies that $V' \Vdash [\overline{\mathrm{K}}_{\mathbf{c}}\psi]_k^{[m,n,A]}$. Since $min(A) \notin g_s(A)$ and $n \notin A$, there exists a valuation V such that $V \uparrow g_s(A) = V' \uparrow g_s(A)$ and moreover $V \Vdash [M]_k^{F_k(\alpha)}$ and $V \Vdash [\overline{\mathrm{K}}_{\mathbf{c}}\psi]_k^{[m,n,A]}$. Therefore we get, $V \Vdash [\overline{\mathrm{K}}_{\mathbf{c}}\psi]_k^{[\alpha,m,n,A]}$.

C. $\varphi = \overline{\mathrm{C}}_{\Gamma}\psi \mid \overline{\mathrm{D}}_{\Gamma}\psi \mid \overline{\mathrm{E}}_{\Gamma}\psi$. This can be proven analogously to the above case.

D. $\varphi = \overline{\mathrm{C}}_{\mathbf{c}_1 \to \mathbf{c}_2}\psi$. Since $M, \pi_l^m \models_k \overline{\mathrm{C}}_{\mathbf{c}_1 \to \mathbf{c}_2}\psi$, we have $M, \pi(m) \models_k \overline{\mathrm{C}}_{\mathbf{c}_1 \to \mathbf{c}_2}\psi$. Thus, there exists a k-path $\pi'_{l'}$ and there exists $0 \leqslant i \leqslant k$ such that $\pi(m) \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \pi'(i)$ and $M, \pi'^i_{l'} \models_k \psi$. By inductive hypothesis and the definition of formula $\mathcal{S}_{\mathbf{c}_1 \to \mathbf{c}_2}$, there exists a valuation V' such that $V' \Vdash [M]_k^{F_k(\alpha)}$ and $V' \Vdash [\psi]_k^{[i,min(A),g_s(A)]} \wedge \mathcal{S}_{\mathbf{c}_1 \to \mathbf{c}_2}(\mathbf{w}_{m,n}, \mathbf{w}_{i,min(A)})$ for some $0 \leqslant i \leqslant k$. Thus, we have

$$V' \Vdash \bigvee_{i=0}^{k} \big([\psi]_k^{[i,min(A),g_s(A)]} \wedge \mathcal{S}_{\mathbf{c}_1 \to \mathbf{c}_2}(\mathbf{w}_{m,n}, \mathbf{w}_{i,min(A)})\big).$$

Further, since $\pi'_{l'} \in \bigcup_{s^0 \in \iota} \Pi_k(s^0)$, we have $\pi'_{l'}(0) = s^0$ for some $s^0 \in \iota$. By the definition of the formula I, we get $V' \Vdash \bigvee_{s^0 \in \iota} I_{s^0}(\mathbf{w}_{0,min(A)})$.

Therefore, we have $V' \Vdash \bigvee_{s^0 \in \iota} I_{s^0}(\mathbf{w}_{0,min(A)}) \wedge \bigvee_{i=0}^{k} \big([\psi]_k^{[i,min(A),g_s(A)]} \wedge \mathcal{S}_{\mathbf{c}_1 \to \mathbf{c}_2}(\mathbf{w}_{m,n}, \mathbf{w}_{i,min(A)})\big)$, which implies that $V' \Vdash [\overline{\mathrm{C}}_{\mathbf{c}_1 \to \mathbf{c}_2} \psi]_k^{[m,n,A]}$. Since $min(A) \notin g_s(A)$ and $n \notin A$, there exists a valuation V such that $V{\uparrow}g_s(A) = V'{\uparrow}g_s(A)$ and $V \Vdash [M]_k^{F_k(\alpha)}$ and $V \Vdash [\overline{\mathrm{C}}_{\mathbf{c}_1 \to \mathbf{c}_2} \psi]_k^{[m,n,A]}$. Therefore we get, $V \Vdash [\overline{\mathrm{C}}_{\mathbf{c}_1 \to \mathbf{c}_2} \psi]_k^{[\alpha,m,n,A]}$.

E. $\varphi = \overline{\mathrm{C}}_{\mathbf{c}_1 \to \Gamma} \psi$. This can be proven analogously to the above case.

□

Lemma 10 (Completeness of the translation of state formulae)**.** *Let M be a model, s a state of M, $k \in \mathbb{N}$, and α an* ECCTL*K *state formula. For every state subformula β of the formula α, and every $A \subseteq F_k(\alpha)$ such that $|A| = f_k(\beta)$, the following condition holds: if $M, s \models_k \beta$, then there exists a valuation V such that $\mathbf{S}(\mathbf{w}_{0,0}) = s$ and $V \Vdash \langle \beta \rangle_k^{[\alpha,0,0,A]}$.*

Proof. We proceed by induction on the complexity of α.

A. $\beta = \mathrm{true} \mid \mathrm{false} \mid p \mid \neg p \mid \beta_1 \wedge \beta_2 \mid \beta_1 \vee \beta_2 \mid \mathrm{E}\beta_1$, where $p \in \mathcal{PV}$ – see Lemma 3.6 of [20].

B. $\beta = \overline{\mathrm{K}}_{\mathbf{c}} \beta_2 \mid \overline{\mathrm{C}}_{\Gamma} \beta_2 \mid \overline{\mathrm{D}}_{\Gamma} \beta_2 \mid \overline{\mathrm{E}}_{\Gamma} \beta_2$ – see Lemma 4.4 of [17].

C. $\beta = \overline{\mathrm{C}}_{\mathbf{c}_1 \to \mathbf{c}_2} \psi$. Let $A \subseteq F_k(\alpha)$ be a set such that $|A| = f_k(\beta)$, $n' \in F_k(\alpha)$, $n' \notin A$, and let $\pi_l' = ((\mathbf{S}'(\mathbf{w}_{0,n'}), \ldots, \mathbf{S}'(\mathbf{w}_{k,n'})), V(\mathbf{u}_{n'}))$ be a k-path such that $\mathbf{S}'(\mathbf{w}_{0,n'}) = s$ for some valuation V' and $0 \leqslant i \leqslant k$. The assumption that $M, s \models_k \overline{\mathrm{C}}_{\mathbf{c}_1 \to \mathbf{c}_2} \psi$ means that there exists a k-path $\pi_l \in \Pi_k$ and there exists $0 \leqslant j \leqslant k$ such that $M, \pi_l^j \models_k \psi$ and $s \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \pi(j)$. Now, let $n = \min(A)$. By Lemma 9 and the definition of the translation it follows that there exists a valuation V'' such that $\pi_l = ((\mathbf{S}''(\mathbf{w}_{0,n}), \ldots, \mathbf{S}''(\mathbf{w}_{k,n})), V''(\mathbf{u}_n))$, and $V'' \Vdash [\psi]_k^{[\alpha,j,n,g_s(A)]}$ for some $0 \leqslant j \leqslant k$. Since $n \neq 0$, $n' \neq 0$, $n \neq n'$, $s \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \pi(j)$, and $\pi_l \in \Pi_k$, there exists a valuation V such that $\mathbf{S}(\mathbf{w}_{0,n'}) \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \mathbf{S}(\mathbf{w}_{j,n})$, $\mathbf{S}(\mathbf{w}_{0,0}) = \mathbf{S}(\mathbf{w}_{0,n'})$, $\mathbf{S}(\mathbf{w}_{0,n}) \in \iota$, $\pi_l = ((\mathbf{S}(\mathbf{w}_{0,n}), \ldots, \mathbf{S}(\mathbf{w}_{k,n})), V(\mathbf{u}_n))$, and $V \Vdash [\psi]_k^{[\alpha,j,n,g_s(A)]}$ for some $0 \leqslant j \leqslant k$. From $\mathbf{S}(\mathbf{w}_{0,n'}) \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \mathbf{S}(\mathbf{w}_{j,n})$, we have $V \Vdash \mathcal{S}_{\mathbf{c}_1 \to \mathbf{c}_2}(\mathbf{w}_{0,n'}, \mathbf{w}_{j,n})$ for $0 \leqslant j \leqslant k$. From $\mathbf{S}(\mathbf{w}_{0,n}) \in \iota$, we have $V \Vdash I_{\mathbf{S}(\mathbf{w}_{0,n})}(\mathbf{w}_{0,n})$, which implies that $V \Vdash \bigvee_{s \in \iota} I_s(\mathbf{w}_{0,n})$. Therefore, we have

$$V \Vdash \bigvee_{s \in \iota} I_s(\mathbf{w}_{0,n}) \wedge \bigvee_{j=0}^{k} (S_{\mathbf{c}_1 \to \mathbf{c}_2}(\mathbf{w}_{0,n'}, \mathbf{w}_{j,n}) \wedge [\psi]_k^{[\alpha,j,n,g_s(A)]})$$

Thus, $V \Vdash \big\langle \overline{\mathrm{C}}_{\mathbf{c}_1 \to \mathbf{c}_2} \psi \big\rangle_k^{[\alpha,0,n',g_s(A)]}$. Since $\mathbf{S}(\mathbf{w}_{0,0}) = \mathbf{S}(\mathbf{w}_{0,n'}) = s$, we have $V \Vdash \big\langle \overline{\mathrm{C}}_{\mathbf{c}_1 \to \mathbf{c}_2} \psi \big\rangle_k^{[\alpha,0,0,g_s(A)]}$.

D. $\beta = \overline{\mathrm{C}}_{\mathbf{c}_1 \to \Gamma} \psi$. Let $A \subseteq F_k(\alpha)$ be a set such that $|A| = f_k(\beta)$, $n' \in F_k(\alpha)$, $n' \notin A$, and let $\pi_l' = ((\mathbf{S}'(\mathbf{w}_{0,n'}), \ldots, \mathbf{S}'(\mathbf{w}_{k,n'})), V(\mathbf{u}_{n'}))$ be a k-path

such that $\mathbf{S}'(\mathbf{w}_{0,n'}) = s$ for some valuation V' and $0 \leqslant i \leqslant k$. The assumption that $M, s \models_k \overline{\mathrm{C}}_{\mathbf{c}_1 \to \Gamma} \psi$ means that there exists a k-path $\pi_l \in \Pi_k$ and there exists $0 \leqslant j \leqslant k$ such that $M, \pi_l^j \models_k \psi$ and $s \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \pi(j)$ for all $\mathbf{c}_2 \in \Gamma$. Now, let $n = \min(A)$. By Lemma 9 and the definition of the translation it follows that there exists a valuation V'' such that $\pi_l = ((\mathbf{S}''(\mathbf{w}_{0,n}), \ldots, \mathbf{S}''(\mathbf{w}_{k,n})), V''(\mathbf{u}_n))$, and $V'' \Vdash [\psi]_k^{[\alpha,j,n,g_s(A)]}$ for some $0 \leqslant j \leqslant k$. Since $n \neq 0$, $n' \neq 0$, $n \neq n'$, $s \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \pi(j)$ for all $\mathbf{c}_2 \in \Gamma$, and $\pi_l \in \Pi_k$, there exists a valuation V such that $\mathbf{S}(\mathbf{w}_{0,n'}) \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \mathbf{S}(\mathbf{w}_{j,n})$ for all $\mathbf{c}_2 \in \Gamma$, $\mathbf{S}(\mathbf{w}_{0,0}) = \mathbf{S}(\mathbf{w}_{0,n'})$, $\mathbf{S}(\mathbf{w}_{0,n}) \in \iota$, $\pi_l = ((\mathbf{S}(\mathbf{w}_{0,n}), \ldots, \mathbf{S}(\mathbf{w}_{k,n})), V(\mathbf{u}_n))$, and $V \Vdash [\psi]_k^{[\alpha,j,n,g_s(A)]}$ for some $0 \leqslant j \leqslant k$. From $\mathbf{S}(\mathbf{w}_{0,n'}) \sim_{\mathbf{c}_1 \to \mathbf{c}_2} \mathbf{S}(\mathbf{w}_{j,n})$ for all $\mathbf{c}_2 \in \Gamma$, we have $V \Vdash \bigwedge_{\mathbf{c}_2 \in \Gamma} \mathcal{S}_{\mathbf{c}_1 \to \mathbf{c}_2}(\mathbf{w}_{0,n'}, \mathbf{w}_{j,n})$ for $0 \leqslant j \leqslant k$. From $\mathbf{S}(\mathbf{w}_{0,n}) \in \iota$, we have $V \Vdash I_{\mathbf{S}(\mathbf{w}_{0,n})}(\mathbf{w}_{0,n})$, which implies that $V \Vdash \bigvee_{s \in \iota} I_s(\mathbf{w}_{0,n})$. Therefore, we have

$$V \Vdash \bigvee_{s \in \iota} I_s(\mathbf{w}_{0,n}) \wedge \bigvee_{j=0}^{k} \Big(\bigwedge_{\mathbf{c}_2 \in \Gamma} S_{\mathbf{c}_1 \to \mathbf{c}_2}(\mathbf{w}_{0,n'}, \mathbf{w}_{j,n}) \wedge [\psi]_k^{[\alpha,j,n,g_s(A)]} \Big)$$

Thus, $V \Vdash \big\langle \overline{\mathrm{C}}_{\mathbf{c}_1 \to \Gamma} \psi \big\rangle_k^{[\alpha,0,n',g_s(A)]}$. Since $\mathbf{S}(\mathbf{w}_{0,0}) = \mathbf{S}(\mathbf{w}_{0,n'}) = s$, we have $V \Vdash \big\langle \overline{\mathrm{C}}_{\mathbf{c}_1 \to \Gamma} \psi \big\rangle_k^{[\alpha,0,0,g_s(A)]}$.

□

The correctness of the SMT-based translation scheme for ECCTL*K is guaranteed by the following theorem.

Theorem 2. *Let M be a model and α be an* ECCTL*K *state formula. Then for every $k \in \mathbb{N}$ and for every $s \in \iota$, $M, s \models_k \alpha$ if, and only if, the quantifier-free first-order formula $[M, \alpha]_k$ is satisfiable.*

Proof. ($\Longrightarrow$) Let $k \in \mathbb{N}$, $s \in \iota$ and $M, s \models_k \alpha$. By Lemma 10 it follows that there exists a valuation V such that $\mathbf{S}(\mathbf{w}_{0,0}) = s$ and $V \Vdash \langle \alpha \rangle_k^{[\alpha,0,0,F_k(\alpha)]}$. Hence, $V \Vdash \bigvee_{s \in \iota} I_s(\mathbf{w}_{0,0})$ and $V \Vdash \langle \alpha \rangle_k^{[\alpha,0,0,F_k(\alpha)]}$. Thus $V \Vdash [M, \alpha]_k$.
($\Longleftarrow$) Let $k \in \mathbb{N}$ and $[M, \alpha]_k$ is satisfiable. Thus, there exists a valuation V such that $V \Vdash [M, \alpha]_k$. So, $V \Vdash \bigvee_{s \in \iota} I_s(\mathbf{w}_{0,0})$ and $V \Vdash [M]_k^{F_k(\alpha)} \wedge \langle \alpha \rangle_k^{[0,0,F_k(\alpha)]}$. Hence, $\mathbf{S}(\mathbf{w}_{0,0})$ is an initial state of M. Moreover, by Lemma 8 it follows that $M, \mathbf{S}(\mathbf{w}_{0,0}) \models_k \alpha$. Thus, $M, s \models_k \alpha$ and $s \in \iota$. □

4. Example - the NB protocol

The NetBill (NB) protocol [15] is an electronic commerce protocol for buying and selling of goods on the Internet. There are three active components in the scenario: the customer, the merchant, and the communication

channel [10]. Specifically, the protocol begins with the customer requesting a price for some desired goods (e.g. lego bricks). This request is followed by the merchant's reply with sending an offer (the price quote), which means creating a commitment. The customer can then either reject the offer and the protocol moves to the initial state after passing through a releasing offer state, or accept the offer, which means creating a payment commitment in relation to the merchant. At this state, the customer has two possibilities: (1) to fulfill his commitment by sending the payment to the merchant; (2) to withdraw his commitment and the protocol will move to the initial state after passing through a releasing offer state. When the merchant receives the payment, he has two possibilities: (1) he commits to deliver the requested goods to the customer. The merchant can fulfill his commitment by delivering the requested goods to the customer, and then sending the receipt to the customer. After that the protocol moves to the initial state; (2) he withdraws his offer. In this case, the merchant violates his commitment, and then the protocol moves to the initial state after sending the refund to the customer.

4.1. **Modelling the NB protocol.** In line with the spirit of the interpreted systems formalism, it is convenient to see the customer (Cus) and the merchant (Mer) as agents, and the communication channel as the environment $\mathcal{E}$. Thus $\mathbb{A} = \{Mer, Cus\}$ is the set of agents of the NB protocol. Each agent of the NB protocol can be modelled by considering its finite set of local states, finite set of local non-negative integer variables, finite set of local actions, local protocol, local evolution function, and local valuation function, i.e., the associated commitment interpreted system is the following:

$$\mathcal{C} = (\{L_{\mathbf{c}}, Var_{\mathbf{c}}, Act_{\mathbf{c}}, P_{\mathbf{c}}, t_{\mathbf{c}}, \mathcal{V}_{\mathbf{c}}\}_{\mathbf{c}\in\mathbb{A}\cup\{\mathcal{E}\}}, \iota)$$

where

- $L_{Cus} = \{c_0, \ldots, c_9\}$, $L_{Mer} = \{m_0, \ldots, m_9\}$. The meaning of local states is the following:
  - c_0 - initiate the contract by placing the price request
  - c_1 - wait for the merchant's offer
  - c_2 - make a decision on the acceptance or on the rejection of the offer
  - c_3 - make a decision on the payment or on the non-payment
  - c_4 - the offer is rejected and the contract is violated
  - c_5 - wait for the merchant to deliver offered goods
  - c_6 - wait for the merchant to send the receipt
  - c_7 - the contract is fulfilled successfully
  - c_8 - wait for the merchant to send the refund
  - c_9 - receive the refund from the merchant; the contract is violated by the merchant

  - m_0 - wait for the price request from the Customer
  - m_1 - make an offer
  - m_2 - wait for the Customer to send back the notification about the acceptance or the rejection of the offer
  - m_3 - wait for the payment
  - m_4 - the offer is rejected and the contract is violated by the customer
  - m_5 - make a decision on the delivering or on non-delivering goods
  - m_6 - send the receipt to the Customer
  - m_7 - the contract is fulfilled successfully
  - m_8 - violate the contract and send the refund
  - m_9 - end of the transaction violated by the merchant
- For simplicity, we shall take the local states of the environment to be just a singleton: $L_{\mathcal{E}} = \{\cdot\}$. This is to simplify the presentation.
- the sets of natural (non-negative) variables available to the agents are: $Var_{Cus} = \{x_1\}$, $Var_{Mer} = \{x_1\}$. The variable x_1 represents the communication channel between Cus and Mer.
- the sets of local actions are:
  - $Act_{Cus} = \{PriceRequest,\ Payment,\ notPayment,\ Accept,\ Reject,\ terminate_C,\ \epsilon_C\}$, where ϵ_C stands for the null action.
  - $Act_{Mer} = \{Offer, notDeliver, Refund, Deliver, Receipt, terminate_M,\ \epsilon_M\}$, where ϵ_M stands for the null action.
  - $Act_{\mathcal{E}} = \{\leftrightarrows\}$, where $\leftrightarrows$ represents the action in which the channel transmits any message successfully in both directions. For simplicity, we assume that the channel always works properly.

  Thus, $Act = Act_{Cus} \times Act_{Mer} \times Act_{\mathcal{E}}$.
- the local protocols of the agents are:
  - $P_{Cus}(c_0) = \{PriceRequest\}$, $P_{Cus}(c_2) = \{Accept, Reject\}$; $P_{Cus}(c_3) = \{Payment, notPayment\}$; $P_{Cus}(c_4) = \{terminate_C\}$; $P_{Cus}(c_i) = \{\epsilon_C\}$ with $i = 1, 5, 6, 7, 8, 9$;
  - $P_{Mer}(m_1) = \{Offer\}$; $P_{Mer}(m_5) = \{Deliver, notDeliver\}$; $P_{Mer}(m_6) = \{Receipt\}$; $P_{Mer}(m_7) = \{terminate_M\}$; $P_{Mer}(m_8) = \{Refund\}$; $P_{Mer}(m_i) = \{\epsilon_M\}$ with $i = 0, 2, 3, 4, 9$;
- the local protocol of the environment is: $P_{Mer}(\cdot) = \{\leftrightarrows\}$;
- Let $\bar{\epsilon}$ be the joint null action (i.e., the action composed of the null actions only), $state$ denote a local state of an agent, $a \in Act$, $act_C(a)$ denote an action of Cus, $act_M(a)$ denote an action of Mer, and $act_{nb}(a)$ denote an action of NB. We assume the following local evolution functions.
  The customer:
  - $t_{Cus}(state, \cdot, a) = state$ if $a \neq \bar{\epsilon}$ and $act_C(a) = \epsilon_C$, and $\cdot \in L_{NB}$.
  - $t_{Cus}(c_0, \cdot, a) = c_1$ if and $act_C(a) = priceReques$.
  - $t_{Cus}(c_1, \cdot, a) = c_2$ if and $act_M(a) = Offer$.

- $t_{Cus}(c_2, \cdot, a) = c_3$ if and $act_C(a) = Accept$.
- $t_{Cus}(c_2, \cdot, a) = c_4$ if and $act_C(a) = Reject$.
- $t_{Cus}(c_3, \cdot, a) = c_5$ if and $act_C(a) = Paymen$.
- $t_{Cus}(c_5, \cdot, a) = c_6$ if and $act_M(a) = Deliver$.
- $t_{Cus}(c_6, \cdot, a) = c_7$ if and $act_M(a) = Receipt$.
- $t_{Cus}(c_5, \cdot, a) = c_8$ if and $act_M(a) = notDeliver$.
- $t_{Cus}(c_8, \cdot, a) = c_9$ if and $act_M(a) = Refund$.
- $t_{Cus}(c_4, \cdot, a) = c_0$ if and $act_C(a) = terminate_C$.
- $t_{Cus}(c_7, \cdot, a) = c_0$ if and $act_M(a) = terminate_M$.
- $t_{Cus}(c_9, \cdot, a) = c_0$ if and $act_M(a) = terminate_M$.

The merchant:

- $t_{Mer}(state, \cdot, a) = state$ if $a \neq \overline{\epsilon}$ and $act_M(a) = \epsilon_C$, and $\cdot \in L_{NB}$.
- $t_{Mer}(m_7, \cdot, a) = m_0$ if $act_M(a) = terminate_M$.
- $t_{Mer}(m_4, \cdot, a) = m_0$ if $act_C(a) = terminate_C$.
- $t_{Mer}(m_0, \cdot, a) = m_1$ if $act_C(a) = priceRequest$.
- $t_{Mer}(m_1, \cdot, a) = m_2$ if $act_M(a) = Offer$.
- $t_{Mer}(m_2, \cdot, a) = m_3$ if $act_C(a) = Accept$.
- $t_{Mer}(m_2, \cdot, a) = m_4$ if $act_C(a) = Reject$.
- $t_{Mer}(m_3, \cdot, a) = m_5$ if $act_C(a) = Payment$.
- $t_{Mer}(m_5, \cdot, a) = m_6$ if $act_M(a) = Deliver$.
- $t_{Mer}(m_6, \cdot, a) = m_7$ if $act_M(a) = Receipt$.
- $t_{Mer}(m_5, \cdot, a) = m_8$ if $act_M(a) = notDeliver$.
- $t_{Mer}(m_8, \cdot, a) = m_9$ if $act_M(a) = Refund$.

The environment:

- $t_{\mathcal{E}}(\cdot, a) = \cdot$ if $a \neq \overline{\epsilon}$ and $act_{nb}(a) = \leftrightarrows$.

The set of possible global states S for the NB protocol is defined as the product $L_{Cus} \times L_{Mer} \times L_{\mathcal{E}}$. Moreover, we consider the following set of initial states $\iota = \{(c_0, m_0, \cdot)\}$.

Furthermore, in the Kripke model of the NB protocol, we assume the following set of proposition variables:

$$\mathcal{PV} = \{Payed, Deliver, Accept\}$$

with the following interpretation:

$(M, s) \models Accept$ if $l_{Cus}(s) = c_3$ and $l_{Mer} = m_3$
$(M, s) \models Payed$ if $l_{Cus}(s) = c_5$ and $l_{Mer} = m_5$,
$(M, s) \models Deliver$ if $l_{Cus}(s) = c_6$ and $l_{Mer} = m_6$.

Some temporal and social properties we may be interested in checking for the example above are the following:

(1) $\varphi_1 = \mathrm{AG}(Payed \rightarrow \mathrm{F}Deliver)$ - whenever Cus pays for the goods, then the goods will eventually be delivered.

(2) $\varphi_2 = \mathrm{AG}(\mathrm{C}_{Cus \to Mer} Accept \to \mathrm{F} Payed)$ - whenever Cus commits towards Mer that he accept the offer, then Cus will eventually pay for the offer.

(3) $\varphi_3 = \mathrm{AG}(\mathrm{C}_{Cus \to Mer} Payed \to \mathrm{F} Deliver)$ - whenever Cus commits towards Mer that he pays for the goods then Cus will eventually receive the goods.

Note that we specify each property for the considered NB protocol in the universal form by an ACCTL*K formula, for which we verify the corresponding counterexample formula, i.e., the negated universal formula in ECCTL*K which is interpreted existentially. Moreover, for every specification given, there exists a counterexample, i.e., the ECCTL*K formula specifying the counterexample holds in the model of the scenario.

Having the above modelling of the NB protocol, we can easily infer the quantifier-free first-order formulae that encode both the model and all the properties mentioned above. Further, checking that the NB satisfies the properties 1–3 can now be done by feeding a SMT solver with the propositional formulae generated in the way explained above.

5. Conclusions

Bounded model checking to be applicable in practice can be combined with a translation of the model checking problem to the SAT problem, or to the SMT problem. In [18] the authors proposed a SAT-based BMC for ECCTL*K and for CIS, however they did not show its correctness and completeness. In this paper we introduced the SMT-based BMC for ECCTL*K and for CIS, and we proved its correctness and completeness. The proof can be easily adapted to the SAT settings. Therefore, this work should also be considered as a supplement of the corresponding BMC methods that is based on SAT.

Our future work include an implementation of both BMC algorithms (i.e., based on SAT and SMT), a careful evaluation of experimental results to be obtained, and a comparison of the both methods.

References

[1] Clark Barrett, Roberto Sebastiani, Sanjit Seshia, and Cesare Tinelli. Satisfiability modulo theories. In *Handbook of Satisfiability*, volume 185 of *Frontiers in Artificial Intelligence and Applications*, chapter 26, pages 825–885. IOS Press, 2009. DOI:10.3233/978-1-58603-929-5-825.

[2] A. Biere, K. Heljanko, T. Junttila, T. Latvala, and V. Schuppan. Linear encodings of bounded LTL model checking. *Logical Methods in Computer Science*, 2(5:5):1–64, 2006. DOI:10.2168/LMCS-2(5:5)2006.

[3] A. Cimatti, E. Clarke, F. Giunchiglia, and M. Roveri. NuSMV: a new symbolic model checker. *International Journal on Software Tools for Technology Transfer*, 2:2000, 2000. DOI:10.1.1.19.4520.

[4] E. M. Clarke, O. Grumberg, and D. A. Peled. *Model Checking*. The MIT Press, Cambridge, Massachusetts, 1999. ISBN: 0-262-03270-8.

[5] M. El-Menshawy, J. Bentahar, and R. Dssouli. Verifiable semantic model for agent interactions using social commitments. In *Proceedings of the 2nd International Conference on Languages, Methodologies, and Development Tools for Multi-Agent Systems (LADS'2009)*, volume 6039 of *LNAI*, pages 128–152. Springer-Verlag, 2010. DOI:10.1007/978-3-642-13338-1_8.

[6] M. El-Menshawy, J. Bentahar, W. El Kholy, and R. Dssouli. Reducing model checking commitments for agent communication to model checking arctl and GCTL*. *Autonomous Agents and Multi-Agent Systems*, 27(3):375–418, 2013. DOI: 10.1007/s10458-012-9208-7.

[7] E. A. Emerson and J. Y. Halpern. "Sometimes" and "not never" revisited: on branching versus linear time temporal logic. *Journal of ACM*, 33(1):151–178, 1986. DOI:10.1145/4904.4999.

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

[9] A. Lomuscio, H. Qu, and F. Raimondi. MCMAS: A model checker for the verification of multi-agent systems. In *Proceedings of the 21st International Conference on Computer Aided Verification (CAV'2009)*, volume 5643 of *LNCS*, pages 682–688. Springer-Verlag, 2009. DOI:10.1007/978-3-642-02658-4_55.

[10] A.U. Mallya and M.P. Singh. An algebra for commitment protocols. *Autonomous Agents and Multi-Agent Systems*, 14(2):143–163, 2007. DOI: 10.1007/s10458-006-7232-1.

[11] Artur Męski, W. Penczek, M.Szreter, B. Woźna-Szcześniak, and A. Zbrzezny. BDD-versus SAT-based bounded model checking for the existential fragment of linear temporal logic with knowledge: algorithms and their performance. *Autonomous Agents and Multi-Agent Systems*, 28(4):558–604, 2014. DOI: 10.1007/s10458-013-9232-2.

[12] M. El Menshawy, J. Benthar, H. Qu, and R. Dssouli. On the verification of social commitments and time. In *Proceedings of the 10th International Conference on Autonomous Agents and Multiaagent Systems (AAMAS'2011)*, pages 483–490. IFAAMAS, 2011.

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

[14] M. P. Singh. A social semantics for agent communication languages. In *Issues in Agent Communication*, volume 1916 of *LNCS*, pages 31–45. Springer-Verlag, 2000. DOI:10.1007/10722777_3.

[15] Marvin A. Sirbu. Credits and debits on the internet. *IEEE Spectrum*, 34(2):23–29, 1997.

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

[17] B. Woźna-Szcześniak. Sat-based bounded model checking for weighted deontic interpreted systems. *Fundamenta Informaticae*, 143(1-2):173–205, 2016. DOI: 10.3233/FI-2016-1310.

[18] Bożena Woźna-Szcześniak. *Trends in Contemporary Computer Science*, chapter Formal Methods and Data Mining. On the SAT-based Verification of Communicative Commitments, pages 175–186. Białystok University of Technology Publishing Office, 2014.

[19] L. Wu, J. Su, K. Su, X. Luo, and Z. Yang. A concurrent dynamic logic of knowledge, belief and certainty for multi-agent systems. *Knowledge-Based Systems*, 23(2):162–168, 2010. DOI:10.1007/978-3-642-01818-3_16.

[20] A. Zbrzezny. A new translation from ECTL* to SAT. *Fundamenta Informaticae*, 120(3-4):377–397, 2012. DOI: 10.3233/FI-2012-768.

[21] D. Zhang, R. Cleaveland, and E. W. Stark. The integrated cwb-nc/pioatool for functional verification and performance analysis of concurrent systems. In *Proceedings of the 9th International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, TACAS'03, pages 431–436. Springer-Verlag, 2003. DOI:10.1007/3-540-36577-X_31.

Received: May 2016

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@ajd.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