Abstractions of Multi-Agent Systems

Constantin Enea[1,2] and Catalin Dima[1]

[1] LACL, University Paris 12, 61 av. du Général de Gaulle, 94010 Créteil, France
[2] University "Al. I. Cuza", Str. General Berthlot 16, 740083, Iaşi, Romania

Abstract. With the recent development of many model-checkers for the temporal logic of knowledge, abstraction techniques are necessary to increase the size of the systems that can be verified. In this paper, we introduce several abstraction techniques for interpreted systems and we prove several preservation results. These results consider the temporal logic of knowledge under Kleene's 3-valued interpretation along infinite and maximal finite paths.

1 Introduction

Abstraction techniques, often based on abstract interpretation [2], provide a method for symbolically analyzing systems using the abstract instead of the concrete domain. Familiar data-flow analysis algorithms are examples of abstract interpretation. In particular, abstract interpretation can be used in order to build the abstract state-space of the system.

With the recent development of many model-checkers for the temporal logic of knowledge [5, 8], abstraction techniques are necessary to increase the size of the systems that can be verified. To our knowledge, this is the first attempt to provide abstraction techniques that are useful to prove properties expressed in the temporal logic of knowledge. We include in our logic all the future and past operators [9], paths quantifiers and knowledge operators [4] and we interpret it over infinite paths or maximal finite paths. Moreover, we use Kleene's 3-valued interpretation, whose third truth value $\perp$ is very useful in modeling incomplete observations or malfunctions and performing abstractions. We study three forms of property preservation, the first two being frequently found in the literature [3]: weak-preserving that is preserving the truth value 1, error-preserving that is preserving the truth value 0 and very-weak preserving that is preserving $\{\perp, 1\}$.

The paper is organized as follows. Section 2 fixes the notation and terminology with respect to the temporal logic of knowledge under Kleene's 3-valued interpretation along infinite or maximal finite paths, and 3-valued multi-agent Kripke structures. Section 3 is dedicated to abstractions of multi-agent Kripke structures and the next section deals with preservation results. The paper ends with some concluding remarks.

2 3-valued KCTL*P

The necessity of using multi-valued logics and multi-valued Kripke structures to model and reason about systems with or without knowledge has been pointed

out by many researchers [1, 7]. In this paper we use 3-valued multi-agent Kripke structures and a 3-valued temporal logic of knowledge interpreted on infinite paths or maximal finite paths in order to model and reason about systems.

Let AP be a set of atomic propositions. The syntax of KCTL*P is as follows:

$$\phi = \psi \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \mathbf{X}\ \phi \mid \overline{\mathbf{X}}\ \phi \mid \mathbf{G}\ \phi \mid \mathbf{F}\ \phi \mid \phi\ \mathbf{U}\ \phi \mid \phi\ \mathbf{W}\ \phi \mid \mathbf{Pr}\ \phi \mid$$
$$\mid \mathbf{A}\ \phi \mid \mathbf{O}\ \phi \mid \phi\ \mathbf{S}\ \phi \mid \phi\ \mathbf{B}\ \phi \mid \exists\phi \mid \forall\phi \mid \mathbf{K}_i\phi \mid \mathbf{P}_i\phi,$$

where ψ is a propositional formula over AP and $1 \leq i \leq n$ (n is the number of agents in the system). We use *future time operators* [9]: $\mathbf{X}$ and $\overline{\mathbf{X}}$ are the strong and weak versions of "next-time", $\mathbf{G}$ is "always", $\mathbf{F}$ is "eventually", $\mathbf{U}$ is "until", and $\mathbf{W}$ is "waiting-for"; *past time operators* [9]: $\mathbf{Pr}$ is "previous", $\mathbf{A}$ is "always in the past", $\mathbf{O}$ is "once", $\mathbf{S}$ is "since", and $\mathbf{B}$ is "back to"; *path quantifiers*: $\forall$ and $\exists$; and *knowledge operators* [4]: $\mathbf{K}_i$ means "agent i knows ϕ" and $\mathbf{P}_i$ means "agent i thinks that ϕ is possible". We denote by $\forall$KCTL*P the subset of KCTL*P consisting of formulas that do not contain $\exists$, $\neg$ and $\mathbf{P}_i$, and by $\exists$KCTL*P the subset of formulas that do not contain $\forall$, $\neg$, $\mathbf{K}_i$.

The semantics we choose for KCTL*P is based on *Kleene's 3-valued interpretation* [6] and 3-valued multi-agent Kripke structures. Kleene's 3-valued interpretation consists of the set of truth values $\{0, 1, \perp\}$ ordered as $0 < \perp < 1$ and the interpretation of the propositional operators is defined by $x \vee y = max\{x, y\}$ and $x \wedge y = min\{x, y\}$, for any truth values x and y.

Definition 1. *A* 3-valued multi-agent Kripke structure *over a set of atomic propositions AP is a tuple $M = (Q, R, L, (\sim_i \mid 1 \leq i \leq n))$, where Q is the set of states, $R : Q \times Q \to \{0, 1, \perp\}$ is the transition predicate, $L : Q \times AP \to \{0, 1, \perp\}$ is the labeling function which associates to any pair (q, p) the truth value of p in state q, n is the number of agents and $\sim_i$: $Q \times Q \to \{0, 1, \perp\}$, for any $1 \leq i \leq n$, is the similarity relation of agent i (it gives the degree of similarity between two states from the point of view of agent i). Every relation $\sim_i$ is a* 3-valued equivalence*, i.e. it satisfies* reflexivity*: $\sim_i (x, x) = 1$, for any $x \in Q$;* symmetry*: $\sim_i (x, y) = \sim_i (y, x)$, for any $x, y \in Q$;* transitivity*: $\sim_i (x, z) = \sim_i (x, y) \wedge \sim_i (y, z)$, for any $x, y, z \in Q$.*

$\perp$ values in the definition of a 3-valued multi-agent Kripke structure are useful for two main reasons: *modeling systems with incomplete observations or malfunctions* as mentioned also in [1, 7] and *performing abstractions*. The states of an abstract system correspond to sets of states of the original system. The transition between two abstract states depends on the sets of states abstracted by these abstract states. For example, if two disjoint sets of states A and B are abstracted by q_A and q_B, respectively, and for any state in A there exist transitions to all states in B, then we have a definite transition from q_A to q_B; otherwise, we may use a $\perp$-transition from q_A to q_B just to specify that it might be possible to transit from some state in A to some state in B. A similar discussion holds also for the labeling function and the similarity relations.

A *path* of a 3-valued multi-agent Kripke structure is either an infinite sequence of states $\pi = q_0 q_1 \ldots$, such that $R(q_i, q_{i+1}) \in \{\perp, 1\}$, for all $i \geq 0$, or a maximal finite sequence of states $\pi = q_0 q_1 \ldots q_m$, such that $R(q_i, q_{i+1}) \in \{\perp, 1\}$, for all

$0 \leq i < m$, and $R(q_m, q) = 0$, for all $q \in Q$. The *length* of π is ∞, in the first case, and $m+1$, in the second case. $|\pi|$ stands for the length of path π, the ith element of path π is denoted $\pi(i)$, and π^i is the suffix of π starting at q_i, for any $0 \leq i < |\pi|$. We will denote by $\mathsf{Paths}(M)$ the set of paths of the Kripke structure M and by $\mathsf{Paths}(M, q)$ the set of paths of M starting in state q. Also, we will call a *point* any pair (π, m), where $\pi \in \mathsf{Paths}(M)$ and $m \in \mathbb{N}$ with $0 \leq m < |\pi|$. The set of points of the Kripke structure M will be denoted by $\mathsf{Points}(M)$.

The *interpreted system* corresponding to a multi-agent Kripke structure M is a triple $I = (\mathsf{Paths}(M), L^I, (\sim_i^I \mid 1 \leq i \leq n))$, where

$L^I : \mathsf{Points}(M) \times AP \to \{0, 1, \bot\}$ is the interpretation function for the atomic propositions in M defined by $L^I((\pi, m), p) = L(\pi(m), p)$, for any $\pi \in \mathsf{Paths}(M)$ and $0 \leq m < |\pi|$ and $\sim_i^I$: $\mathsf{Points}(M) \times \mathsf{Points}(M) \to \{0, 1, \bot\}$, for any $1 \leq i \leq n$, is the similarity relation defined by $\sim_i^I ((\pi, m), (\pi', m')) = \sim_i (\pi(m), \pi'(m'))$. From now on we will make no distinction between L and its extension to points L^I. The same holds for the similarity relations.

We now give the semantics for the formulas in $\mathsf{KCTL^*P}$, which for the fragment that includes only future time is similar to the multi-valued semantics from [7]. If ϕ is a formula in $\mathsf{KCTL^*P}$ and $I = (\mathsf{Paths}(M), L, (\sim_i \mid 1 \leq i \leq n))$ an interpreted system we define the *truth value of ϕ in the point* (π, m), denoted by $[\phi]^I_{(\pi,m)}$, in the following way (we give only some of the possible cases, the others being similar):

$$
\begin{array}{ll}
[\psi]^I_{(\pi,m)} & = \text{obtained as usual using the interpretation function } L; \\
[\neg\phi]^I_{(\pi,m)} & = \neg[\phi]^I_{(\pi,m)}; \\
[\phi_1 \wedge \phi_2]^I_{(\pi,m)} & = [\phi_1]^I_{(\pi,m)} \wedge [\phi_2]^I_{(\pi,m)}; \\
[\mathbf{X}\ \phi]^I_{(\pi,m)} & = |\pi^m| > 1 \wedge R(\pi(m), \pi(m+1)) \wedge [\phi]^I_{(\pi,m+1)}; \\
[\overline{\mathbf{X}}\ \phi]^I_{(\pi,m)} & = |\pi^m| \leq 1 \vee (R(\pi(m), \pi(m+1)) \wedge [\phi]^I_{(\pi,m+1)}); \\
[\phi_1\ \mathbf{U}\ \phi_2]^I_{(\pi,m)} & = [\phi_2]^I_{(\pi,m)} \vee \bigvee_{0<i<|\pi^m|}([\phi_2]^I_{(\pi,m+i)} \wedge \\
 & \quad \bigwedge_{0\leq j<i}([\phi_1]^I_{(\pi,m+j)} \wedge R(\pi(m+j), \pi(m+j+1)))); \\
[\mathbf{Pr}\ \phi]^I_{(\pi,m)} & = m = 0 \vee (R(\pi(m-1), \pi(m)) \wedge [\phi]^I_{(\pi,m-1)}); \\
[\phi_1\ \mathbf{S}\ \phi_2]^I_{(\pi,m)} & = [\phi_2]^I_{(\pi,m)} \vee \bigvee_{0\leq i<m}([\phi_2]^I_{(\pi,i)} \wedge \\
 & \quad \bigwedge_{i<j\leq m}([\phi_1]^I_{(\pi,j)} \wedge R(\pi(j-1), \pi(j)))); \\
[\exists\phi]^I_{(\pi,m)} & = \bigvee_{\pi'[1..m]=\pi[1..m]}[\phi]^I_{(\pi',m)}; \\
[\forall\phi]^I_{(\pi,m)} & = \bigwedge_{\pi'[1..m]=\pi[1..m]}[\phi]^I_{(\pi',m)}; \\
[\mathbf{K}_i\phi]^I_{(\pi,m)} & = \bigwedge_{\sim_i((\pi,m),(\pi',m'))\neq 0}\big(\sim_i((\pi,m),(\pi',m')) \wedge [\phi]^I_{(\pi',m')}\big); \\
[\mathbf{P}_i\phi]^I_{(\pi,m)} & = \bigvee_{\sim_i((\pi,m),(\pi',m'))\neq 0}\big(\sim_i((\pi,m),(\pi',m')) \wedge [\phi]^I_{(\pi',m')}\big).
\end{array}
$$

Also, we say that a property $\phi \in \mathsf{KCTL^*P}$ is *valid* in some interpreted system I if $[\phi]^I_{(\pi,m)} = 1$, for all $(\pi, m) \in \mathsf{Points}(M)$. If there exists some point (π, m) such that $[\phi]^I_{(\pi,m)} = 0$, we will say that ϕ is *false* in I.

Running Example Consider the system from Figure 1. It consists of two agents H and L asynchronously composed (the $\wedge$ symbol means that the instructions are executed in one atomic transition). H continuously increases x by 2 but, when it receives a signal from L (L sets z to 1) it increases x only by 1. The agent L also uses y to count the number of signals it sends.

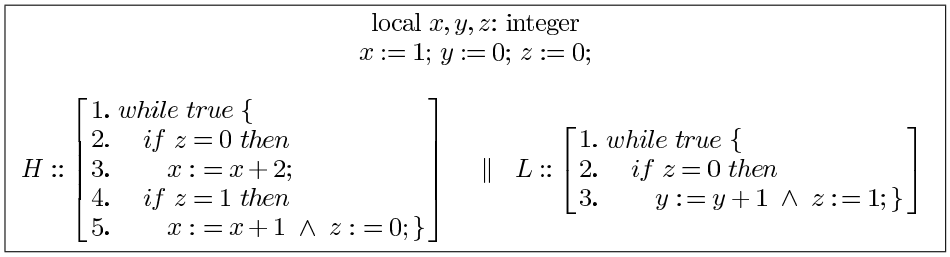

Fig. 1. A system with two processes

Suppose that L can not read x. We would be interested in checking whether the low-level user L can deduce something about the parity of x.

We model this system by a multi-agent Kripke structure $M = (Q, R, L, (\sim_H, \sim_L))$, whose states are triples (x, y, z), where x, y and z are the variables from Figure 1. We consider that $(x, y, z) \sim_H (x', y', z')$ if $x = x'$ and $z = z'$ and $(x, y, z) \sim_L (x', y', z')$ if $y = y'$ and $z = z'$.

An instance of the question above is the formula

$$\phi = P_L \ \mathbf{O} \ \big((even(y) \wedge z = 1) \Rightarrow \mathbf{P} \ \neg(even(x) \ \ \mathbf{S} \ \ z = 1)\big),$$

where *even* is a predicate that it is 1 for even numbers and 0 otherwise. If this property is false then, the fact that y is even implies that x is even in all the states since the last time z was 1. Consequently, if y is even the low-level user knows the parity of x for some of the past states.

Such a property is an instance of information flow w.r.t *run-based secrecy* [10]. In fact, the falsity of ϕ would prove also that agent H does not maintain run-based secrecy with respect to agent L, i.e. there exists an H-local and satisfiable formula ϕ such that $P_L \ \mathbf{O} \ \phi$ is false.

3 Abstractions of multi-agent Kripke structures

In this section we will investigate several types of abstractions that can be applied to multi-agent Kripke structures. Let $M_1 = (Q_1, R_1, L_1, (\sim_i^1 | \ 1 \leq i \leq n))$ be a multi-agent Kripke structure over a set AP of atomic propositions. An abstraction of M_1 is based on some equivalence relation ρ on Q_1 that it is used to create *abstract states*. Hence, an abstract state is any equivalence class on Q_1 (we denote $[q]$ the equivalence class of q with respect to ρ). However, this is not sufficient to create an abstract Kripke structure: we still need a definition for the transition predicate, for the labeling function and for the similarity relations. Let $M_2 = (Q_2, R_2, L_2, (\sim_i^2 | \ 1 \leq i \leq n))$ be a multi-agent Kripke structure with $Q_2 = Q_1/\rho$. Following [11], we say that R_2 is defined in a $\forall\exists$ *manner from* R_1 if

$$R_2([q], [q']) = \begin{cases} 1, & \text{if } (\forall q_1 \in [q])(\forall q_2 \in [q'])(R(q_1, q_2) = 1) \\ 0, & \text{if } (\exists q_1 \in [q])(\exists q_2 \in [q'])(R(q_1, q_2) = 0) \\ \perp, & \text{otherwise,} \end{cases}$$

for any $q, q' \in Q_1$. Defining R_2 in a $\exists\forall$ or $\forall\forall$ manner from R_1 can be done similarly by changing the quantifiers that specify how elements from equivalence

classes are chosen. We also consider the three cases for the definition of L_2. For example, L_2 is defined in a $\exists\forall$ *manner from* L_1 if

$$L_2([q],p) = \begin{cases} 1, & \text{if } (\exists q_1 \in [q])(L_1(q_1,p) = 1) \\ 0, & \text{if } (\forall q_1 \in [q])(L_1(q_1,p) = 0) \\ \bot, & \text{otherwise,} \end{cases}$$

for any $q \in Q_1$ and $p \in AP$.

Trying to adopt a similar approach for the similarity relations $\sim_i^2$, we have to ensure that these relations remain three-valued equivalences. The relations between the different possible definitions for $\sim_i^2$ and the properties of a three-valued equivalence are enumerated in the next proposition.

Proposition 1. *Let M_1 be a multi-agent Kripke structure like above, ρ an equivalence relation on Q_1 and $\delta : Q_1/\rho \times Q_1/\rho \to \{0,1,\bot\}$ a function. We have that:*

1. *if δ is defined in a $\forall\exists$-manner from $\sim_i^1$ then it is symmetric and transitive;*
2. *if δ is defined in a $\exists\forall$-manner from $\sim_i^1$ then it is reflexive and symmetric;*
3. *if δ is defined in a $\forall\forall$-manner from $\sim_i^1$ then it is symmetric;*

The above proposition mentions all the properties of a 3-valued equivalence that are always satisfied by a $\forall\exists$, $\exists\forall$ or $\forall\forall$ definition of $\sim_i^1$. Consequently, when trying to redefine the similarity relations in the abstract system we have to apply some closures to obtain three-valued equivalences.

Definition 2. *Let M_1, ρ and M_2 be as above. M_2 is called a (T_1,T_2,T_3)-*abstraction of M_1 by ρ, *for any $T_1, T_2, T_3 \in \{\forall\forall, \forall\exists, \exists\forall\}$, if R_2 is defined in a T_1 manner from R_1, L_2 is defined in a T_2 manner from L_1 and:*
– if $T_3 = \forall\exists$, $\sim_i^2$ is the reflexive closure of the $\forall\exists$ definition of $\sim_i^1$;
– if $T_3 = \exists\forall$, $\sim_i^2$ is the transitive closure of the $\exists\forall$ definition of $\sim_i^1$;
– if $T_3 = \forall\forall$, $\sim_i^2$ is the reflexive and transitive closure of the $\forall\forall$ definition of $\sim_i^1$.

Running Example We define on the set of states of M the equivalence relation ρ as follows: $(x,y,z)\ \rho\ (x',y',z')$ if $even(|x-x'|) \wedge even(|y-y'|) \wedge z = z'$. The $(\exists\forall,\exists\forall,\exists\forall)$-abstraction of M by ρ is depicted in Figure 2. We have denoted the abstract states by triples, where the first two elements specify the parity of x and y, respectively, while the third component gives the value of z.

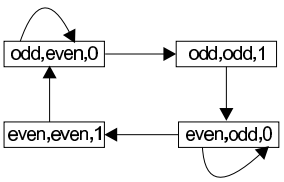

Fig. 2. An $(\exists\forall,\exists\forall,\exists\forall)$-abstraction of M

Notice that the abstract system has only 4 reachable states and it is very easy to verify it. We will investigate in the next section the cases in which the truth value of a property is preserved in the concrete system.

4 Preservation results

This section is dedicated to proving the utility of the types of abstraction presented in the previous section. In general, abstractions are useful when they offer preservation results with respect to a specific set of properties. We will study three forms of property preserving, the first two being frequently found in the literature [3]:

- *weak-preservation with respect to a set of properties* P: an abstraction is weakly preserving with respect to P if for any $\phi \in P$, ϕ is evaluated to 1 in the abstract system implies that ϕ is evaluated to 1 in the concrete system;
- *error-preservation with respect to a set of properties* P: an abstraction is error preserving with respect to P if for any $\phi \in P$, ϕ is evaluated to 0 in the abstract system implies that ϕ is evaluated to 0 in the concrete system;
- *very weak-preservation with respect to a set of properties* P: an abstraction is very weak-preserving with respect to P if for any $\phi \in P$, ϕ is evaluated to 1 or $\perp$ in the abstract system implies that ϕ is evaluated to 1 or $\perp$ in the concrete system.

4.1 Weak and very weak preservation results

We will study in this subsection the weak and very weak preservation results that hold for the types of abstraction presented in the previous section. We will give first two technical lemmas that will identify the basic conditions that must be satisfied by the abstraction in order to be weak or very weak preserving with respect to $\forall$KCTL*P or $\exists$KCTL*P.

Let $M_1 = (Q_1, R_1, L_1, (\sim_i^1 |\ 1 \leq i \leq n))$ and $M_2 = (Q_2, R_2, L_2, (\sim_i^2 |\ 1 \leq i \leq n))$ be two 3-valued multi-agent Kripke structures over some set AP of atomic propositions and ρ an equivalence relation on Q_1 such that $Q_2 = Q_1/\rho$. We say that M_2 *preserves the paths of* M_1 if for each path π_1 in M_1 there exists a path π_2 in M_2 with the same length as π_1 such that $\pi_2(m) = [\pi_1(m)]$, for any $0 \leq m < |\pi_2|$ (we say that π_2 *corresponds* to π_1). Also, we say that M_1 *preserves the paths of* M_2 if for each path π_2 in M_2 there exists a path π_1 in M_1 with the same length such that $\pi_1(m) \in \pi_2(m)$, for any $0 \leq m < |\pi_1|$ (again, we say that π_1 *corresponds* to π_2). We say that R_2 (R_1) *preserves the set of truth values* B if $R_2([q],[q']) \in B$ ($R_1(q,q') \in B$) implies $R_1(q,q') \in B$ ($R_2([q],[q']) \in B$), for any $q, q' \in Q_1$. In the same way we define the facts that L_2, L_1, $\sim_i^2$ and $\sim_i^1$ preserve some set of truth values.

Lemma 1. *Let M_1 and M_2 be as above. For any formula ϕ in $\forall$KCTL*P:*

1. *if M_2 preserves the paths of M_1 and L_2, $\sim_i^1$ preserve $\{\perp, 1\}$, then $[\phi]^{I_2}_{(\pi_2,m)} \in \{\perp, 1\}$ implies $[\phi]^{I_1}_{(\pi_1,m)} \in \{\perp, 1\}$, for any $(\pi_1, m) \in$ Points(M_1) (π_2 is the path in M_2 that corresponds to π_1 and I_1, I_2 are the interpreted systems corresponding to M_1, M_2).*
2. *if M_2 preserves the paths of M_1, $\sim_i^1$ preserves $\{\perp, 1\}$ and R_2, L_2, $\sim_i^2$ preserve 1, then $[\phi]^{I_2}_{(\pi_2,m)} = 1$ implies $[\phi]^{M_1}_{(\pi_1,m)} = 1$, for any $(\pi_1, m) \in$ Points(M_1). The same holds even if the requirements that R_2 and $\sim_i^2$ preserve 1 are replaced by $R_1(q,q') \in \{0,1\}$ and $\sim_i^1$ $(q,q') \in \{0,1\}$, for any $q, q' \in Q_1$.*

Proof. All claims can be proved by structural induction on ϕ. We will exhibit only the interesting cases of the first proof, the others being obtained in a similar manner:

- $\phi = p \in AP$. Then, $[\phi]^{I_2}_{(\pi_2,m)} = L_2(\pi_2(m), p) \in \{\bot, 1\}$. By the definition of π_2 and the fact that L_2 preserves $\{\bot, 1\}$, we obtain that $L_1(\pi_1(m), p) \in \{\bot, 1\}$. Therefore, $[\phi]^{I_1}_{(\pi_1,m)} \in \{\bot, 1\}$;
- $\phi = \overline{\mathbf{X}}\ \phi_1$. Assume that ϕ_1 satisfies the property. Then, $[\overline{\mathbf{X}}\ \phi_1]^{I_2}_{(\pi_2,m)} = |\pi_2^m| \leq 1 \vee \left([\phi_1]^{I_2}_{(\pi_2,m+1)} \wedge R_2(\pi_2(m), \pi_2(m+1))\right) \in \{\bot, 1\}$. If $|\pi_2^m| \leq 1$, then $|\pi_1^m| \leq 1$ which leads to $[\overline{\mathbf{X}}\ \phi_1]^{I_1}_{(\pi_1,m)} = 1$. Otherwise, $[\phi_1]^{I_2}_{(\pi_2,m+1)} \wedge R_2(\pi_2(m), \pi_2(m+1)) \in \{\bot, 1\}$. By the definition of π_2 we obtain $|\pi_1^m| > 1$ and $R_1(\pi_1(m), \pi_1(m+1)) \in \{\bot, 1\}$, and by the induction hypothesis, $[\phi_1]^{I_1}_{(\pi_1,m+1)} \in \{\bot, 1\}$. Consequently, $[\overline{\mathbf{X}}\ \phi_1]^{I_1}_{(\pi_1,m)} \in \{\bot, 1\}$;
- $\phi = \forall\phi_1$. Assume that ϕ_1 satisfies the property. Consequently, $[\forall\phi_1]^{I_2}_{(\pi_2,m)} = \bigwedge_{\pi[1..m]=\pi_2[1..m]} [\phi_1]^{I_2}_{(\pi,m)} \in \{\bot, 1\}$ which implies $[\phi_1]^{I_2}_{(\pi,m)} \in \{\bot, 1\}$, for all paths π such that $\pi[1..m] = \pi_2[1..m]$. Since M_2 preserves the paths of M_1, for each path σ of M_1 with $\sigma[1..m] = \pi_1[1..m]$ there exists a path σ' of M_2 such that $\sigma'[1..m] = \pi_2[1..m]$. Moreover, $[\phi_1]^{I_2}_{(\sigma',m)} \in \{\bot, 1\}$, for each path σ' as above. Applying the induction hypothesis we get $[\phi_1]^{I_1}_{(\sigma,m)} \in \{\bot, 1\}$, for each path σ with $\sigma[1..m] = \pi_1[1..m]$. Hence, $[\forall\phi_1]^{I_1}_{(\pi_1,m)} \in \{\bot, 1\}$.
- $\phi = K_i\phi_1$. Assume that ϕ_1 satisfies the property. The hypothesis will imply that $\bigwedge_{\sim_i^2((\pi_2,m),(\pi_2'',m'))\neq 0} \sim_i^2 ((\pi_2, m), (\pi_2'', m')) \wedge [\phi]^{I_2}_{(\pi_2'',m')} \in \{\bot, 1\}$, and we have to prove $\bigwedge_{\sim_i^1((\pi_1,m),(\pi_1',m''))\neq 0} \sim_i^1 ((\pi_1, m), (\pi_1', m'')) \wedge [\phi]^{I_1}_{(\pi_1',m'')} \in \{\bot, 1\}$. Let (π_1', m'') be a point of M_1 such that $\sim_i^1 ((\pi_1, m), (\pi_1', m'')) \neq 0$. Since M_2 preserves the paths of M_1, there exists a corresponding path for π_1', denote it π_2' such that $\pi_2'(m'') = [\pi_1'(m'')]$. Moreover, because $\sim_i^1$ preserves $\{\bot, 1\}$ we obtain that $\sim_i^2 ((\pi_2, m), (\pi_2', m'')) \in \{\bot, 1\}$. From above we obtain that $[\phi_1]^{I_2}_{(\pi_2',m'')} \in \{\bot, 1\}$ which, by the induction hypothesis, implies $[\phi_1]^{I_1}_{(\pi_1',m'')} \in \{\bot, 1\}$. □

The following lemma can be proved in a similar way to Lemma 1.

Lemma 2. *Let M_1 and M_2 be as above. For any formula ϕ in* ∃KCTL*P*:

1. *if M_1 preserves the paths of M_2 and L_2, $\sim_i^2$ preserve $\{\bot, 1\}$, then $[\phi]^{I_2}_{(\pi_2,m)} \in \{\bot, 1\}$ implies $[\phi]^{M_1}_{(\pi_1,m)} \in \{\bot, 1\}$, for any $(\pi_2, m) \in \mathsf{Points}(M_2)$ (π_1 is the path in M_1 that corresponds to π_2).*
2. *if M_1 preserves the paths of M_2 and R_2, L_2, $\sim_i^2$ preserve 1, then $[\phi]^{I_2}_{(\pi_2,m)} = 1$ implies $[\phi]^{M_1}_{(\pi_1,m)} = 1$, for any $(\pi_2, m) \in \mathsf{Points}(M_2)$.*

We will enumerate now the weak and very weak preservation results that hold for all the possible types of abstraction.

Theorem 1. *Let M_1 and M_2 be as above, where R_2 and $\sim_i^2$, for any $1 \leq i \leq n$, are $\exists\forall$ defined. Then, for any $\phi \in \forall\mathsf{KCTL}^*\mathsf{P}$ we have the following:*

1. *If L_2 is $\forall\exists$ defined, then $[\phi]^{I_2}_{(\pi_2,m)} \in \{\bot, 1\}$ implies $[\phi]^{I_1}_{(\pi_1,m)} \in \{\bot, 1\}$, for any $(\pi_1, m) \in \mathsf{Points}(M_1)$ (π_2 is a path in M_2 corresponding to π_1). Moreover, if $R_1(q, q') \in \{0, 1\}$ and $\sim_i^1 (q, q') \in \{0, 1\}$, for all $q, q' \in Q_1$ and $1 \leq i \leq n$, then $[\phi]^{I_2}_{(\pi_2,m)} = 1$ implies $[\phi]^{I_1}_{(\pi_1,m)} = 1$, for any $(\pi_1, m) \in \mathsf{Points}(M_1)$.*
2. *If L_2 is $\forall\forall$ defined, $R_1(q, q') \in \{0, 1\}$ and $\sim_i^1 (q, q') \in \{0, 1\}$, for all $q, q' \in Q_1$ and $1 \leq i \leq n$, then $[\phi]^{I_2}_{(\pi_2,m)} = 1$ implies $[\phi]^{I_1}_{(\pi_1,m)} = 1$, for any $(\pi_1, m) \in \mathsf{Points}(M_1)$.*

Proof. Directly from Lemma 1. □

Next, we try to give a weak and a very weak preservation result for abstractions of type $(\forall\exists, T, \forall\exists)$, for some T, with respect to $\exists\mathsf{KCTL}^*\mathsf{P}$. By Lemma 2 we need that $\sim_i^2$ preserves $\{\bot, 1\}$ and since we use the reflexive closure of the $\forall\exists$ definition of $\sim_i^1$, this may not happen. Consequently, the preservation results will hold only for equivalences relations ρ that ensure that the $\forall\exists$ definition of $\sim_i^1$ is already reflexive. If M_1 and M_2 are as above, we say that ρ *is compatible with* $\sim_i^1$ if whenever $q\ \rho\ q'$ we have $\sim_i^1 (q, q') = 1$. Clearly, this compatibility implies that the $\forall\exists$ definition of $\sim_i^1$ is reflexive.

Theorem 2. *Let M_1 and M_2 be as above, where R_2 and $\sim_i^2$ are $\forall\exists$ defined and ρ is compatible with $\sim_i^1$, for any $1 \leq i \leq n$. Then, for any $\phi \in \exists\mathsf{KCTL}^*\mathsf{P}$ we have the following:*

1. *If L_2 is $\forall\exists$ or $\forall\forall$ defined, then $[\phi]^{I_2}_{(\pi_2,m)} = 1$ implies $[\phi]^{I_1}_{(\pi_1,m)} = 1$, for any $(\pi_2, m) \in \mathsf{Points}(M_2)$ (π_1 is a path in M_1 corresponding to π_2).*
2. *If L_2 is $\forall\exists$ defined, then $[\phi]^{I_2}_{(\pi_2,m)} = \bot$ implies $[\phi]^{I_1}_{(\pi_1,m)} \in \{\bot, 1\}$, for any $(\pi_2, m) \in \mathsf{Points}(M_2)$.*

Proof. Directly from Lemma 2. □

Theorem 3. *Let M_1 and M_2 be as above, where R_2 and $\sim_i^2$, for any $1 \leq i \leq n$, are $\forall\forall$ defined. Then, for any formula ϕ in $\forall\mathsf{KCTL}^*\mathsf{P}$ we have the following:*

1. *If L_2 is $\forall\exists$ defined, then $[\phi]^{I_2}_{(\pi_2,m)} = 1$ implies $[\phi]^{I_1}_{(\pi_1,m)} = 1$, for any $(\pi_1, m) \in \mathsf{Points}(M_1)$ (π_2 is a path in M_2 corresponding to π_1).*
2. *If L_2 is $\forall\forall$ defined, then $[\phi]^{I_2}_{(\pi_2,m)} = 1$ implies $[\phi]^{I_1}_{(\pi_1,m)} = 1$, for any $(\pi_1, m) \in \mathsf{Points}(M_1)$.*

Proof. Directly from Lemma 1. □

4.2 Error preservation results

We will study in this section the error preservation results that hold for the types of abstraction we have introduced in Section 3. As before, we first give two technical lemmas that identify basic conditions that must be satisfied by an abstraction in order to be error-preserving.

Lemma 3. *Let M_1 and M_2 be as above. If M_2 preserves the paths of M_1, L_2 preserves 0 and $\sim_i^1$ preserves $\{\bot, 1\}$, then $[\phi]^{I_2}_{(\pi_2,m)} = 0$ implies $[\phi]^{M_1}_{(\pi_1,m)} = 0$, for any $\phi \in \exists\mathsf{KCTL^*P}$ and $(\pi_1, m) \in \mathsf{Points}(M_1)$ (π_2 is the path in M_2 that corresponds to π_1).*

Proof. The claim is proved by structural induction on ϕ. We will enumerate only the interesting cases, the others can be obtained similarly:

- $\phi = \exists\phi_1$. Assume that ϕ_1 satisfies the property. We obtain that $[\exists\phi_1]^{I_2}_{(\pi_2,m)} = \bigvee_{\pi[1..m]=\pi_2[1..m]} [\phi_1]^{I_2}_{(\pi,m)} = 0$ implies that $[\phi_1]^{I_2}_{(\pi,m)} = 0$, for all paths π such that $\pi[1..m] = \pi_2[1..m]$. Since M_2 preserves the paths of M_1, for each path σ of M_1 with $\sigma[1..m] = \pi_1[1..m]$ there exists a path σ' of M_2 such that $\sigma'[1..m] = \pi_2[1..m]$. Moreover, $[\phi_1]^{I_2}_{(\sigma',m)} = 0$, for each path σ' as above. Applying the induction hypothesis we get $[\phi_1]^{I_1}_{(\sigma,m)} = 0$, for each path σ with $\sigma[1..m] = \pi_1[1..m]$. Hence, $[\exists\phi_1]^{I_1}_{(\pi_1,m)} = 0$
- $\phi = P_i\phi_1$. Assume that ϕ_1 satisfies the property. The hypothesis will imply that $\bigvee_{\sim_i^2((\pi_2,m),(\pi_2'',m'))\neq 0} \left(\sim_i^2 ((\pi_2, m), (\pi_2'', m')) \wedge [\phi]^{I_2}_{(\pi_2'',m')}\right) = 0$ and we have to prove $\bigvee_{\sim_i^1((\pi_1,m),(\pi_1',m''))\neq 0} \sim_i^1 ((\pi_1, m), (\pi_1', m'')) \wedge [\phi]^{I_1}_{(\pi_1',m'')} = 0$. Let (π_1', m'') be a point of M_1 such that $\sim_i^1 ((\pi_1, m), (\pi_1', m'')) \neq 0$. Since M_2 preserves the paths of M_1, there exists a corresponding path for π_1', denote it π_2' such that $\pi_2'(m'') = [\pi_1'(m'')]$. By the fact that $\sim_i^1$ preserves $\{\bot, 1\}$, we obtain $\sim_i^2 ((\pi_2, m), (\pi_2', m'')) \in \{\bot, 1\}$. From above, $[\phi_1]^{I_2}_{(\pi_2',m'')} = 0$ and by the induction hypothesis we get $[\phi_1]^{I_1}_{(\pi_1',m'')} = 0$. □

The following lemma can be proved in a similar way to Lemma 3.

Lemma 4. *Let M_1 and M_2 be as above. If M_1 preserves the paths of M_2, L_2 preserves 0 and $\sim_i^2$ preserves $\{\bot, 1\}$, then $[\phi]^{I_2}_{(\pi_2,m)} = 0$ implies $[\phi]^{M_1}_{(\pi_1,m)} = 0$, for any $\phi \in \forall\mathsf{KCTL^*P}$ and $(\pi_2, m) \in \mathsf{Points}(M_2)$ ($\pi_1 \in \mathsf{Paths}(M_1)$ corresponds to π_2).*

We can now state the error preservation results.

Theorem 4. *Let M_1 and M_2 be as above, where R_2 and $\sim_i^2$ are $\exists\forall$ defined. If L_2 is $\exists\forall$ or $\forall\forall$ defined, then $[\phi]^{I_2}_{(\pi_2,m)} = 0$ implies $[\phi]^{I_1}_{(\pi_1,m)} = 0$, for any $\phi \in \exists\mathsf{KCTL^*P}$ and $(\pi_1, m) \in \mathsf{Points}(M_1)$ ($\pi_2 \in \mathsf{Paths}(M_2)$ corresponds to π_1).*

Proof. Directly from Lemma 3. □

Next, we prove that the $(\forall\exists, T, \forall\exists)$-abstractions, for some T, are error preserving with respect to $\forall\mathsf{KCTL^*P}$. Again, ρ must be compatible with $\sim_i^1$.

Theorem 5. *Let M_1 and M_2 be as above, where R_2 and $\sim_i^2$ are $\forall\exists$ defined and ρ is compatible with $\sim_i^1$, for any $1 \leq i \leq n$. If L_2 is $\exists\forall$ or $\forall\forall$ defined, then $[\phi]^{I_2}_{(\pi_2,m)} = 0$ implies $[\phi]^{I_1}_{(\pi_1,m)} = 0$, for any $\phi \in \forall\mathsf{KCTL^*P}$ and $(\pi_2, m) \in \mathsf{Points}(M_2)$ (π_1 is the path in M_1 corresponding to π_2).*

Proof. Directly from Lemma 4. □

Theorem 6. *Let M_1 and M_2 be as above, where R_2 and $\sim_i^2$, for any $1 \leq i \leq n$, are $\forall\forall$ defined. For any ϕ in $\exists$KCTL*P we have that:*

1. *If L_2 is $\exists\forall$ defined, then $[\phi]^{I_2}_{(\pi_2,m)} = 0$ implies $[\phi]^{I_1}_{(\pi_1,m)} = 0$, for any $(\pi_1, m) \in$ Points(M_1) (π_2 is a path in M_2 that corresponds to π_1).*
2. *If L_2 is $\forall\forall$ defined, then $[\phi]^{I_2}_{(\pi_2,m)} = 0$ implies $[\phi]^{I_1}_{(\pi_1,m)} = 0$, for any $(\pi_1, m) \in$ Points(M_1).*

Proof. Directly from Lemma 3. □

Running Example Using the predicate $odd(x)$, which is 1 for odd numbers and 0 otherwise, we transform ϕ into an equivalent formula which is in $\exists$KCTL*P. The abstract system from Figure 2 has only 4 reachable states and we can easily prove that the formula ϕ is false. Since $\phi \in \exists$KCTL*P we apply the error preservation result from Theorem 4 and obtain that it is false also in the concrete system I_1.

5 Conclusions

We have introduced in this paper abstraction techniques that are useful to prove properties expressed in the temporal logic of knowledge. We have used a very general logic under Kleene's 3-valued interpretation and we have offered weak, very weak and error preservation results. These techniques can be used to increase the size of the systems that can be verified.

References

1. Marsha Chechik, Steve M. Easterbrook, and Victor Petrovykh. Model-checking over multi-valued logics. In *Proceedings of FME, LNCS 2021*, pages 72–98, 2001.
2. P. Cousot and R. Cousot. Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *Proceedings of POPL*, pages 238–252, 1977.
3. D. Dams. *Abstract Interpretation and Partial Refinement for Model Checking*. PhD thesis, Technische Universität Eindhoven, 1996.
4. R. Fagin, J.Y. Halpern, Y. Moses, and M.Y. Vardi. *Reasoning about Knowledge*. MIT Press, 1995.
5. Peter Gammie and Ron van der Meyden. MCK: Model checking the logic of knowledge. In *Proceedings of CAV, LNCS 3114*, pages 479–483, 2004.
6. M. Ginsberg. Multivalued logics. *A* uniform approach to inference in artificial intelligence. *Computational Intelligence*, 4:265–316, 1988.
7. Beata Konikowska and Wojciech Penczek. Model checking for multivalued logic of knowledge and time. In *Proceedings of AAMAS*, pages 169–176, 2006.
8. Alessio Lomuscio and Franco Raimondi. MCMAS: A model checker for multi-agent systems. In *Proceedings of TACAS, LNCS 3920*, pages 450–454, 2006.
9. Z. Manna and A. Pnueli. *The Temporal Logic of Reactive and Concurrent Systems. Specification*. Springer-Verlag, 1992.
10. Kevin R. O'Neill and Joseph Y. Halpern. Secrecy in multiagent systems. *CoRR*, cs.CR/0307057, 2003.
11. F.L. Tiplea and C. Enea. Abstractions of data types. *Acta Informatica*, 42(8-9):639–671, 2006.