Making Abstract Model Checking Strongly Preserving

Francesco Ranzato[1] and Francesco Tapparo[1,2]

[1] Dipartimento di Matematica Pura ed Applicata
Università di Padova
Via Belzoni 7, 35131 Padova, Italy
franz@math.unipd.it

[2] Dipartimento di Matematica
Università di Milano, Milano, Italy
tapparo@math.unipd.it

Abstract. Usually, abstract model checking is not strongly preserving: it may well exist a temporal specification which is not valid on the abstract model but which is instead satisfied by the concrete model. Starting from the standard notion of bisimulation, we introduce a notion of completeness for abstract models: completeness together with a so-called partitioning property for abstract models implies strong preservation for the past μ-calculus. Within a rigorous abstract interpretation framework, we show that the least refinement of a given abstract model, for a suitable ordering on abstract models, which is complete and partitioning always exists, and it can be constructively characterized as a greatest fixpoint. This provides a systematic methodology for minimally refining an abstract model checking in order to get strong preservation.

1 Introduction

Abstract model checking is one practical way to deal with the well-known state explosion problem of model checking [3, 6]. The essence of the abstract model checking approach to system verification is well known and established: the checking of the correctness specification is performed over an abstraction of the system model, called abstract model, which abstracts away from some properties of the system model [4, 5]. Thus, abstract model checking basically consists in applying an abstract interpretation-based approach to the model of the system to check. An abstract state space is considered, where an abstract state approximates some selected properties of a concrete state of the system. An abstract transition relation is defined between abstract states and this gives rise to the abstract model. The check of the temporal specification is performed on the abstract model, and a correctness result, also called preservation result, ensures that if a specification holds on the abstract model then it is also holds on the concrete model. The abstract model checking approach has been very successful, and allowed to verify systems with a tremendous number of states (for instance, a ALU circuit with 10^{1300} reachable states was verified already in early works

[5]), since suitably chosen abstractions can lead to great reductions of the size of the model to verify. The foundations and principles of abstract model checking have been studied and improved in many directions. For instance, it has been shown that an abstract model checking approach can be used for verifying infinite-state systems [1, 11], since the basic idea is substantially the same: an infinite-state model is approximated and then reduced to an abstract model with a finite number of states. Let us point out that abstract model checking can be rigorously specified within standard Cousot and Cousot's [7, 8] abstract interpretation theory [9, 10, 16, 17], and this paper follows this principle as well.

The design of abstract model checking always comes together with a preservation result. *Strong preservation* results are highly desirable: a formula of a suitable specification language is valid on the abstract model if and only if it is valid on the concrete model. Thus, strong preservation allows to draw consequences from negative answers on the abstract side: if a formula is not valid abstractly then it is not valid on the concrete model. It should be clear that strong preservation is related to the idea of *complete abstract interpretation* [8, 15]. Actually, this has been recently noted by Giacobazzi and Quintarelli [13], who studied and related completeness in asbtract interpretation, strongly preserving abstract model checking and the so-called Clarke et al.'s [2] spurious counterexamples of abstract model checking.

The idea of enhancing the precision of abstract interpretations by refining the underlying abstract domains dates back to the early works by Cousot and Cousot [8], and evolved to the systematic design of abstract interpretations by abstract domain refinements [12, 14]. In particular, Giacobazzi et al. [15] thorougly investigated the abstract domain refinement making abstract interpretations complete. They showed that completeness for an abstract interpretation is a property which does not depend on the abstract semantic operations but on the underlying abstract domains only. This opened up the question of making abstract interpretations complete by least refinements of abstract domains. It turns out that this least refinement exist and can be constructively characterized as a fixed point solution of abstract domain equations.

On the model checking side, the idea of systemically refining abstract model checking to enhance its precision is due to Clarke et al. [2]. They introduced the notion of spurious counterexample in abstract model checking: given a temporal formula φ, an abstract execution trace π is a spurious conunterexample for φ if π does not satisfy φ whereas there exists a concrete execution trace whose abstraction is π but which is not a counterexample for φ. Then, they devised a methodology for refining an abstract model checking w.r.t. a given temporal specification φ by using the spurious counterexamples provided by the abstract model checker on φ. Giacobazzi and Quintarelli [13] casted spurious counterexamples as a lack of completeness, in the abstract interpretation sense, for the abstract model checking. Then, by applying the results in [15] for minimally making abstract interpretations complete, they designed a method for systematically refining abstract model checking in order to eliminate spurious counterexamples.

This paper follows the idea of applying systematic refinement operators to abstract model checking in order "to gain precision". However, here the perspective is different from that of [2, 13]: our main goal is that of systematically refining abstract model checking in order to get strong preservation for all the formulae of a suitable temporal specification language.

Firstly, we single out a new (to the best of our knowledge) notion of *complete abstract model*: if (Q, R) and (A, S) are, respectively, the concrete and abstract transition systems and $\rho \subseteq Q \times A$ is the abstraction relation of simulation then (A, S) is complete whenever $R^{-1}\rho = \rho S^{-1}$. Hence, such relation of completeness is, in a sense, dual to the standard bisimulation relation. Strong preservation is related to completeness by the following result: completeness for a so-called *partitioning* abstraction relation implies strong preservation for the past μ-calculus. The partitioning property for the abstraction relation ρ comes from the work of Loiseaux et al. [16] and means that ρ induces a partition of the abstract state space A. Thus, our goal is that of "minimally making an abstract model checking complete and partitioning". Of course, this requires a notion of ordering for the abstract models of a given concrete transition system. This is done by isolating the notions of partitioning and complete closure operators on sets of system states and by defining a bijective correspondence between these closure operators and abstract models which preserves the partitioning and completeness properties. This allows us to move our problem to the standard abstract interpretation framework using closure operators. Closures are a well-known and useful tool for specifying abstract domains in abstract interpretation theory [8], and they are particularly helpful when reasoning on abstract domains independently from the representation of their objects. In this framework, we constructively solve the problem of characterizing the least complete and partitioning refinement of the closure μ_ρ on $\wp(Q)$ associated to the abstraction relation $\rho \subseteq Q \times A$: this is the, necessarily unique, greatest, w.r.t. the standard pointwise ordering, closure μ^*_ρ which is a refinement of μ and which is both partitioning and complete. Analogously to [15], this problem is formulated as a fixpoint equation between abstract domains and hence it is constructively solved. Then, we come back to abstract models by associating to this least refinement μ^*_ρ an abstract model (A^*, R^*): this refined abstract model is related to the concrete model (Q, R) by an abstraction relation ρ^* which is partitioning and induces completeness. We reached our goal: we have systematically designed a strongly preserving abstract model (A^*, R^*) which is a minimal refinement of (A, S) in the following sense: any other complete and partitioning abstract model (B, T) of (Q, R) which is a refinement of (A, S) turns out to be a simulation of (A^*, R^*).

2 Preliminaries

2.1 Abstract Interpretation Basics

The structure $\langle \mathrm{uco}(C), \sqsubseteq, \sqcup, \sqcap, \lambda x.\top, \lambda x.x \rangle$ denotes the complete lattice of all (upper) closure operators on a complete lattice $\langle C, \leq, \vee, \wedge, \top, \bot \rangle$, where $\mu \sqsubseteq \eta$ iff $\forall x \in C.\ \mu(x) \leq \eta(x)$. Throughout the paper, for any $\mu \in \mathrm{uco}(C)$, we follow a

standard notation by denoting the image $\mu(C)$ simply by μ itself: This does not give rise to ambiguity, since one can readily distinguish the use of μ as function or set according to the context. Let us recall that (i) each closure $\mu \in \mathrm{uco}(C)$ is uniquely determined by the set of its fixpoints, which coincides with its image, i.e. $\mu = \{x \in C \mid \mu(x) = x\}$, (ii) $\mu \sqsubseteq \eta$ iff $\eta \subseteq \mu$, and (iii) a subset $X \subseteq C$ is the set of fixpoints of a closure iff $X = \mathcal{M}(X) \stackrel{\text{def}}{=} \{\wedge Y \mid Y \subseteq X\}$ ($\mathcal{M}(X)$ is called the Moore-closure of X; note that $\top = \wedge\varnothing \in \mathcal{M}(X)$). Let us also recall that a closure is additive (i.e., preserves arbitrary lub's, empty set included) iff its set of fixpoints is closed by lub's.

Within the standard Cousot and Cousot framework, abstract domains can be equivalently specified either by Galois connections/insertions (GCs/GIs) or by closure operators [8]. In the first case, concrete and abstract domains C and A — for simplicity, let C and A be complete lattices — are related by a pair of adjoint maps $\alpha : C \to A$ and $\gamma : A \to C$, compactly denoted by (α, C, A, γ), and therefore C and A may consist of objects having different representations. In the second case, instead, an abstract domain is specified as a closure operator on the concrete domain C. Thus, the closure operator approach is particularly convenient when reasoning about properties of abstract domains independently from the representation of their objects. Given a concrete domain C, we will identify $\mathrm{uco}(C)$ with the so-called complete lattice of abstract interpretations of C (cf. [7, 8]). The ordering on $\mathrm{uco}(C)$ corresponds precisely to the standard order used in abstract interpretation to compare abstract domains with regard to their precision: A_1 is more precise (or concrete) than A_2 iff $A_1 \sqsubseteq A_2$ in $\mathrm{uco}(C)$. Thus, lub's $\sqcup$ and glb's $\sqcap$ on $\mathrm{uco}(C)$ give, respectively, the most precise abstraction and the most abstract concretization of a family of abstract domains.

Complete Abstract Interpretations. Let us briefly recall the basic notions concerning completeness in abstract interpretation. Let $f : C \to C$ be a monotone or antitone concrete semantic function[1] occurring in some complex semantic specification, and let $f^\sharp : A \to A$ be a corresponding abstract function on the abstract domain A. Then, $\langle A, f^\sharp \rangle$ is a sound abstract interpretation — or $f^\sharp$ is a correct approximation of f relatively to A — when $\forall c \in C.\, \alpha(f(c)) \leq_A f^\sharp(\alpha(c))$. On the other hand, $\langle A, f^\sharp \rangle$ is complete when equality holds, i.e. $\alpha \circ f = f^\sharp \circ \alpha$. Thus, completeness means that abstract computations accumulate no loss of information.

Any abstract domain A induces the so-called canonical best correct approximation $f^A : A \to A$ of $f : C \to C$, defined by $f^A \stackrel{\text{def}}{=} \alpha \circ f \circ \gamma$. This terminology is justified by the fact that any $f^\sharp : A \to A$ is a correct approximation of f iff $f^A \sqsubseteq f^\sharp$. Consequently, any abstract domain always induces an (automatically) sound abstract interpretation. However, not all abstract domains induce a complete abstract interpretation. It turns out that whenever a complete abstract function exists then this actually is the best correct approximation. This therefore means that completeness for an abstract function is a property which

[1] For simplicity, we consider unary functions with the same domain and co-domain; the extension to the general case is conceptually straightforward.

depends on the underlying abstract domain only. Consequently, for abstract domains specified by closure operators, an abstract domain $\mu \in \mathrm{uco}(C)$ is defined to be complete for f if $\mu \circ f = \mu \circ f \circ \mu$ (see [15] for more details).

We call abstract domain refinement any operator performing an action of refinement on abstract domains, with respect to their standard ordering of precision $\sqsubseteq$ [8, 14]. In particular, the concepts of shell and shell refinement with respect to a given property of abstract domains, namely a given subclass of $\mathrm{uco}(C)$, are as follows.

Definition 2.1. Let C be a complete lattice and $\mathcal{P} \subseteq \mathrm{uco}(C)$ be an abstract domain property. Let $\mu, \sigma \in \mathrm{uco}(C)$. Then, σ is the $\mathcal{P}$-*shell* of μ if:

1. $\sigma \in \mathcal{P}$,
2. $\sigma \sqsubseteq \mu$,
3. if $\eta \in \mathcal{P}$ and $\eta \sqsubseteq \mu$ then $\eta \sqsubseteq \sigma$.

An operator $\mathcal{F} : \mathrm{uco}(C) \to \mathrm{uco}(C)$ is called the $\mathcal{P}$-*shell refinement* if for any $\mu \in \mathrm{uco}(C)$, $\mathcal{F}(\mu)$ is the $\mathcal{P}$-shell of μ. □

Thus, the $\mathcal{P}$-shell of an abstract domain A, if this exists, is the most abstract among the domains which satisfy $\mathcal{P}$ and are more precise than A. Complete shells with respect to a concrete interpretation $f : C \to C$ are particularly important. They have been studied by Giacobazzi et al. in [15], where the authors characterized through fixpoints the complete shell refinement under the weak hypothesis that f is a continuous function.

2.2 Abstract Model Checking

We follow a general approach to abstract model checking [16]. If $R \subseteq X \times Y$ and $S \subseteq Y \times Z$ are relations then $R^{-1} \subseteq Y \times X$ denotes the reverse relation of R and $RS \subseteq X \times Z$ denotes the composition of the two relations. We deal with generic transition systems (Q, R), where Q is any (finite or infinite) set of system states and $R \subseteq Q \times Q$ is the transition relation. Let us recall the well-known notions of simulation and bisimulation between transition systems. Let $\mathcal{T} = (Q, R)$ and $\mathcal{T}' = (A, S)$ be transition systems and $\rho \subseteq Q \times A$ be a *relation of abstraction* (also called *abstraction relation*). Then (i) $\mathcal{T}'$ is a ρ-*abstraction* of $\mathcal{T}$, or $\mathcal{T}$ ρ-simulates $\mathcal{T}'$, denoted by $\mathcal{T} \sqsubseteq_\rho \mathcal{T}'$, if $R^{-1}\rho \subseteq \rho S^{-1}$; (ii) $\mathcal{T}$ ρ-*bisimulates* $\mathcal{T}'$, denoted by $\mathcal{T} \simeq_\rho \mathcal{T}'$, if $\mathcal{T} \sqsubseteq_\rho \mathcal{T}'$ and $\mathcal{T}' \sqsubseteq_{\rho^{-1}} \mathcal{T}$. $\mathcal{T}$ and $\mathcal{T}'$ are called, respectively, the concrete and abstract model.

Definition 2.2. Let (Q, R) be a transition system. An *abstraction* (of Q) is simply a triple $\langle Q, \rho, A \rangle$ where A is any set and $\rho \subseteq Q \times A$. □

An abstraction $\langle Q, \rho, A \rangle$ induces the usual pre/post transformers:

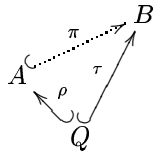
- $\mathrm{pre}[\rho] \stackrel{\mathrm{def}}{=} \lambda Y.\{a \in Q \mid \exists b \in Y.\ a\rho b\} : \wp(A) \to \wp(Q)$
- $\widetilde{\mathrm{pre}}[\rho] \stackrel{\mathrm{def}}{=} \lambda Y.\{a \in Q \mid \forall b \in A.(a\rho b \Rightarrow b \in Y)\} : \wp(A) \to \wp(Q)$
- $\mathrm{post}[\rho] \stackrel{\mathrm{def}}{=} \lambda X.\{b \in A \mid \exists a \in X.\ a\rho b\} : \wp(Q) \to \wp(A)$
- $\widetilde{\mathrm{post}}[\rho] \stackrel{\mathrm{def}}{=} \lambda X.\{b \in A \mid \forall a \in Q.(a\rho b \Rightarrow a \in X\} : \wp(Q) \to \wp(A)$

Moreover, $\mathrm{dom}(\rho) \stackrel{\text{def}}{=} \{q \in Q \mid \exists a \in A.\, q\rho a\}$ and $\mathrm{img}(\rho) \stackrel{\text{def}}{=} \{a \in A \mid \exists q \in Q.\, q\rho a\}$. The relation ρ is *total* when $\mathrm{dom}(\rho) = Q$ and *surjective* when $\mathrm{img}(\rho) = A$.

Let $(Q, R) \sqsubseteq_\rho (A, S)$ and $(Q, R) \sqsubseteq_\tau (B, T)$. Simulation takes into account the transition relations. Instead, we need a way to compare the underlying abstractions of Q only.

Definition 2.3. The abstraction $\langle Q, \rho, A\rangle$ is more precise than $\langle Q, \tau, B\rangle$, denoted by $\langle Q, \rho, A\rangle \leq \langle Q, \tau, B\rangle$, iff there exists $\pi \subseteq A \times B$ such that $\tau = \rho\pi$. □

This general definition formalizes the following diagram and therefore it is the right one.



The following key notion of partitioning relation is taken from [16, Section 4].

Definition 2.4. Let $\langle Q, \rho, A\rangle$ be an abstraction. The relation ρ is called *partitioning* when $\rho = \rho\rho^{-1}\rho$. □

Hence, ρ is partitioning whenever any two states of Q which are abstracted by ρ to a common abstract state actually are abstracted by ρ exactly to the same set of abstract states. The terminology "partitioning" is justified by the following fact.

Lemma 2.5. *ρ is partitioning iff $\{\mathrm{post}[\rho](\{q\}) \mid q \in Q\}$ is a partition of A.*

Abstractions of Q can be related to closure operators on $\wp(Q)$ as follows.

Definition 2.6.

(i) Given an abstraction $\langle Q, \rho, A\rangle$, $\mu_\rho \stackrel{\text{def}}{=} \widetilde{\mathrm{pre}}[\rho] \circ \mathrm{post}[\rho] \in \mathrm{uco}(\langle \wp(Q), \subseteq\rangle)$ is the closure operator associated to $\langle Q, \rho, A\rangle$.

(ii) Let Q be a set and $\mu \in \mathrm{uco}(\wp(Q))$. Then, the abstraction $\langle Q, \rho_\mu, A_\mu\rangle$ associated to μ is defined as follows: $A_\mu \stackrel{\text{def}}{=} \{\mu(\{q\}) \in \wp(Q) \mid q \in Q\}$; $\langle q_1, \mu(\{q_2\})\rangle \in \rho_\mu \stackrel{\text{def}}{\Leftrightarrow} \mu(\{q_1\}) = \mu(\{q_2\})$. □

The fact that $\widetilde{\mathrm{pre}}[\rho] \circ \mathrm{post}[\rho] \in \mathrm{uco}(\wp(Q))$ is a consequence of the well-known fact that $(\mathrm{post}[\rho], \wp(Q), \wp(A), \widetilde{\mathrm{pre}}[\rho])$ is a Galois connection (see e.g. [16, Section 2]). Actually, the correspondences of Definition 2.6 give rise to a bijection between total, surjective and partitioning abstractions and closure operators on $\wp(Q)$, as stated by the following result.

Lemma 2.7. *If Q is a set and $\mu \in \mathrm{uco}(\wp(Q))$, then ρ_μ is total, surjective and partitioning, and $\mu_{\rho_\mu} = \mu$. On the other hand, if $\langle Q, \rho, A\rangle$ is a total, surjective and partitioning abstraction then $\langle Q, \rho, A\rangle$ is isomorphic to $\langle Q, \rho_{\mu_\rho}, A_{\mu_\rho}\rangle$ (i.e., they are the same relation up to bijections).*

The adequacy of Definitions 2.3 and 2.6 is shown by the following result: it turns out that the preordering on abstractions is equivalent to the standard ordering between the associated closures.

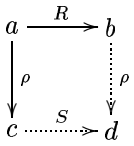
Lemma 2.8. *Let* $\langle Q, \rho, A\rangle$ *and* $\langle Q, \tau, B\rangle$ *be abstractions. Then,* $\langle Q, \rho, A\rangle \leq \langle Q, \tau, B\rangle$ *iff* $\mu_\rho \sqsubseteq_{\mathrm{uco}(\wp(Q))} \mu_\tau$.

3 Complete Abstract Models

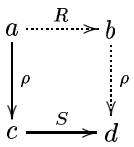
Let us consider the bisimulation property:

$$(Q, R) \simeq_\rho (A, S) \text{ iff } R^{-1}\rho \subseteq \rho S^{-1} \text{ and } S^{-1}\rho^{-1} \subseteq \rho^{-1}R^{-1}.$$

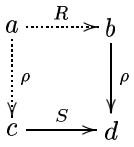
The condition of ρ-abstraction $R^{-1}\rho \subseteq \rho S^{-1}$ means that for all a, b, c there exists some d such that the following diagram commutes:



On the other hand, the condition of ρ-bisimulation $S^{-1}\rho^{-1} \subseteq \rho^{-1}R^{-1}$ is equivalent to $\rho S \subseteq R\rho$, and this latter means that for all a, c, d there exists some b such that the following diagram commutes:



While the relation of ρ-abstraction provides the standard order of comparison between transition systems, on the other side it is natural to consider the following diagram dual to the bisimulation diagram above:



Thus, this diagram corresponds to the inclusion $\rho S^{-1} \subseteq R^{-1}\rho$. This leads us to the following definition of completeness between transition systems.

Definition 3.1. Let $\mathcal{T} = (Q, R)$ and $\mathcal{T}' = (A, S)$ be transition systems and $\rho \subseteq Q \times A$. Then, $\mathcal{T}'$ is a *complete ρ-abstraction* of $\mathcal{T}$, denoted by $\mathcal{T} \preccurlyeq_\rho \mathcal{T}'$, if $R^{-1}\rho = \rho S^{-1}$. □

The following simple example shows that completeness and bisimulation are orthogonal notions.

Example 3.2. Let us consider the transition systems $(\mathbb{Z}, \mathrm{succ})$ and $(A, \mathrm{succ}^\sharp)$, where $\langle m, n\rangle \in \mathrm{succ} \stackrel{\text{def}}{\Leftrightarrow} n = m+1$, $A \stackrel{\text{def}}{=} \{\mathrm{ev}, \mathrm{od}\}$ and $\mathrm{succ}^\sharp \stackrel{\text{def}}{=} \{\langle \mathrm{ev}, \mathrm{od}\rangle, \langle \mathrm{od}, \mathrm{ev}\rangle\}$. Let $\rho \subseteq \mathbb{Z} \times A$ be the function mapping any integer to its parity. Then, it is easily seen that $(\mathbb{Z}, \mathrm{succ}) \simeq_\rho (A, \mathrm{succ}^\sharp)$ and $(\mathbb{Z}, \mathrm{succ}) \preccurlyeq_\rho (A, \mathrm{succ}^\sharp)$. Instead, we have that $(\mathbb{N}, \mathrm{succ}) \simeq_\rho (A, \mathrm{succ}^\sharp)$ but $(\mathbb{N}, \mathrm{succ}) \not\preccurlyeq_\rho (A, \mathrm{succ}^\sharp)$. Finally, it turns out that $(\mathbb{Z} \smallsetminus \mathbb{N}, \mathrm{succ}) \preccurlyeq_\rho (A, \mathrm{succ}^\sharp)$ but $(\mathbb{Z} \smallsetminus \mathbb{N}, \mathrm{succ}) \not\simeq_\rho (A, \mathrm{succ}^\sharp)$. □

Completeness for an abstract model w.r.t. a given concrete model, of course, depends on the abstract transition relation. However, when the abstraction relation is partitioning, it turns out that all the possible complete abstract models are bisimilar, as stated by the following result.

Theorem 3.3. *Let $\mathcal{T} = (Q, R)$ be a transition system and $\rho \subseteq Q \times A$ be surjective and partitioning. If $\mathcal{T} \preccurlyeq_\rho \mathcal{T}_1 = (A, S_1)$ and $\mathcal{T} \preccurlyeq_\rho \mathcal{T}_2 = (A, S_2)$ then $\mathcal{T}_1 \simeq_{\rho^{-1}\rho} \mathcal{T}_2$.*

It is then natural to give the following existential notion of completeness for mere state abstractions of concrete transition systems, i.e., which takes into account $\langle Q, \rho, A\rangle$ and R only, and does not depend on a specific abstract transition relation.

Definition 3.4. Let (Q, R) be a transition system. The abstraction $\langle Q, \rho, A\rangle$ is *complete* for (Q, R) if there exists $S \subseteq A \times A$ such that $(Q, R) \preccurlyeq_\rho (A, S)$. □

Example 3.5. Consider the Example 3.2. Then, as shown by Example 3.2, the abstraction $\langle \mathbb{Z}, \rho, \{\mathrm{ev}, \mathrm{od}\}\rangle$ is complete for the concrete model $(\mathbb{Z}, \mathrm{succ})$. On the other hand, let $B \stackrel{\text{def}}{=} \{\bullet, \circ\}$ and consider the abstraction $\langle \mathbb{Z}, \zeta, B\rangle$, where $\zeta \stackrel{\text{def}}{=} \{\langle 1, \bullet\rangle, \langle 2, \bullet\rangle\} \cup \{\langle z, \circ\rangle \mid z \in \mathbb{Z} \smallsetminus \{1, 2\}\}$. Assume that $S \subseteq B \times B$ is an abstract transition relation such that $(\mathbb{Z}, \mathrm{succ}) \sqsubseteq_\zeta (B, S)$. Then, we have that $\langle \bullet, \circ\rangle \in S$: in fact, $\langle 2, \bullet\rangle \in \zeta$ and $\langle 2, 3\rangle \in \mathrm{succ}$ and therefore, by simulation, there exists $x \in B$ such that $\langle 3, x\rangle \in \zeta$ and $\langle \bullet, x\rangle \in S$; thus, $\langle 3, x\rangle \in \zeta$ implies $x = \circ$, and therefore $\langle \bullet, \circ\rangle \in S$. Similarly, one can show that S must be the greatest relation $B \times B$, and this transition relation does not give rise to completeness. Thus, this means that the abstraction $\langle \mathbb{Z}, \zeta, B\rangle$ is not complete for $(\mathbb{Z}, \mathrm{succ})$. □

It turns out that if an abstraction is complete and partitioning then the abstract transition relation $\rho^{-1}R\rho$ induces a complete abstract model.

Theorem 3.6. *Let $\langle Q, \rho, A\rangle$ be a complete abstraction of (Q, R), where ρ is total and partitioning. Then, $(Q, R) \preccurlyeq_\rho (A, \rho^{-1}R\rho)$.*

$(A, \rho^{-1}R\rho)$ is called the *canonical complete abstract model* induced by a complete abstraction $\langle Q, \rho, A\rangle$.

Example 3.7. Let us go on with Example 3.5. We observed that the abstraction $\langle \mathbb{Z}, \rho, \{\mathrm{ev}, \mathrm{od}\}\rangle$ is complete for the concrete model $(\mathbb{Z}, \mathrm{succ})$ by considering the abstract transition relation $\mathrm{succ}^\sharp$. Actually, let us point out that $\rho^{-1}\,\mathrm{succ}\,\rho = \{\langle \mathrm{ev}, \mathrm{od}\rangle, \langle \mathrm{od}, \mathrm{ev}\rangle\} = \mathrm{succ}^\sharp$, i.e., $(\{\mathrm{ev}, \mathrm{od}\}, \mathrm{succ}^\sharp)$ is the canonical complete abstract model induced by the abstraction ρ. □

4 Strong Preservation of Temporal Calculi

Preservation and strong preservation of temporal specifications in abstract model checking are well known. Let us recall these notions in our framework. Let $\mathcal{T} = (Q, R)$ and $\mathcal{A} = (A, S)$ be transition systems. Let $\mathcal{P}$ be a set of atomic propositions used in some temporal language L. Let $\mathcal{I} : \mathcal{P} \to \wp(Q)$ be an interpretation function and $\alpha : \wp(Q) \to \wp(A)$ be any function mapping "concrete properties" to "abstract properties". In particular, α induces the abstract interpretation function $\alpha \circ \mathcal{I} : \mathcal{P} \to \wp(A)$. α is called *consistent* with $\mathcal{I}$ when for all $P \in \mathcal{P}$, $\alpha(Q \smallsetminus \mathcal{I}(P)) \cap \alpha(\mathcal{I}(P)) = \varnothing$. Then, any formula φ of L is semantically interpreted as a set $|\varphi|_{\mathcal{T},\mathcal{I}}$ of concrete states for the interpretation $\mathcal{I}$ and abstractly as a set $|\varphi|_{\mathcal{A},\alpha\circ\mathcal{I}}$ of abstract states for the interpretation $\alpha \circ \mathcal{I}$. For a subset of states $Z \subseteq Q$, the abstraction map α *preserves* a formula φ on Z for $\mathcal{I}$ whenever for any $q \in Z$,

$$q \in |\varphi|_{\mathcal{T},\mathcal{I}} \;\Rightarrow\; \alpha(\{q\}) \subseteq |\varphi|_{\mathcal{A},\alpha\circ\mathcal{I}},$$

while α *strongly preserves* φ on Z when $\Leftrightarrow$ holds. Whenever the subset Z is omitted we refer to (strong) preservation on all Q.

In this paper we deal with temporal formulae expressed within a standard μ-calculus. Let $\mathcal{X}$ be a set of variables. The formulae φ of the μ-calculus are inductively defined as follows:

$$\varphi ::= \top \mid P \in \mathcal{P} \mid X \in \mathcal{X} \mid \Diamond\varphi \mid \varphi_1 \vee \varphi_2 \mid \neg\varphi \mid \mu X.\varphi$$

where any occurrence of a propositional variable X in φ is under an even number of negations. L_μ denotes the set of μ-calculus formulae. The remaining standard connectives of the μ-calculus, namely $\bot$, $\wedge$, $\to$, ν and $\Box$, can be defined as usual by abbreviations. $\Diamond^p$ and $\Box^p$ denote, respectively, the *past* existential and universal operators. $L_\mu^{\leftarrow}$ denotes the set of formulae of the calculus obtained by replacing $\Diamond$ with $\Diamond^p$ in the above definition of the μ-calculus: this is called the past μ-calculus.

The semantics $|\varphi|_{\mathcal{T},\mathcal{I}} \in \wp(Q)$ of a closed (i.e., without free variables) formula φ is therefore defined w.r.t. a given transition system $\mathcal{T} = (Q, R)$ and an interpretation $\mathcal{I}$. This semantics is defined as usual (see e.g. [16]). For example, let us recall that $|\Diamond\varphi|_{\mathcal{T},\mathcal{I}} \stackrel{\text{def}}{=} \text{pre}[R](|\varphi|_{\mathcal{T},\mathcal{I}})$ and $|\Diamond^p\varphi|_{\mathcal{T},\mathcal{I}} \stackrel{\text{def}}{=} \text{post}[R](|\varphi|_{\mathcal{T},\mathcal{I}})$.

We will use the following fragments of the μ-calculus.

$\Box^p L_\mu$ (past universal fragment):
$\varphi ::= \top \mid \bot \mid P \mid \neg P \mid X \mid \Box^p\varphi \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \wedge \varphi_2 \mid \mu X.\varphi \mid \nu X.\varphi$

$\Diamond L_\mu$ (existential fragment):
$\varphi ::= \top \mid \bot \mid P \mid \neg P \mid X \mid \Diamond\varphi \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \wedge \varphi_2 \mid \mu X.\varphi \mid \nu X.\varphi$

$\Diamond L_\mu^+$ (positive existential fragment):
$\varphi ::= \top \mid \bot \mid P \mid X \mid \Diamond\varphi \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \wedge \varphi_2 \mid \mu X.\varphi \mid \nu X.\varphi$

The plain preservation result basically states that simulation implies preservation.

Theorem 4.1 ([16, Theorem 2]). *Let $\rho \subseteq Q \times A$ and $(Q,R) \sqsubseteq_\rho (A,S)$. Let $\mathcal{I} : \mathcal{P} \to \wp(Q)$ be an interpretation. Then,* $\mathrm{post}[\rho] : \wp(Q) \to \wp(A)$ *preserves the formulae of $\Diamond L_\mu^+$, and if* $\mathrm{post}[\rho]$ *is consistent with $\mathcal{I}$ then* $\mathrm{post}[\rho]$ *preserves $\Diamond L_\mu$.*

As far as strong preservation is concerned, it is well known that bisimulation implies strong preservation. In our framework, this corresponds to the following result.

Theorem 4.2 ([16, Theorem 4]). *Let $\rho \subseteq Q \times A$ be a partitioning relation and $(Q,R) \simeq_\rho (A,S)$. Then, for any interpretation $\mathcal{I} : \mathcal{P} \to \mathrm{img}(\mathrm{pre}[\rho])$,* $\mathrm{post}[\rho]$ *strongly preserves L_μ on $\bigcup \mathrm{img}(\mathrm{pre}[\rho])$.*

We investigated the impact of complete and partitioning abstract models on strong preservation. Basically, we obtained that completeness implies strong preservation for the past universal fragment of the μ-calculus. Moreover, for the canonical complete abstract model, we are able to prove strong preservation for the full past μ-calculus. This is stated by the following result.

Theorem 4.3. *Let $\rho \subseteq Q \times A$ be total and partitioning and $(Q,R) \preccurlyeq_\rho (A,S)$. Let $\mathcal{I} : \mathcal{P} \to \mathrm{img}(\mathrm{pre}[\rho])$ be an interpretation. Then:*

1. $\mathrm{post}[\rho]$ *strongly preserves $\Box^p L_\mu$ for $\mathcal{I}$ on $\bigcup \mathrm{img}(\mathrm{pre}[\rho])$.*
2. *For the canonical complete abstract model $(A, \rho^{-1}R\rho)$,* $\mathrm{post}[\rho]$ *strongly preserves $L_\mu^{\leftarrow}$ for $\mathcal{I}$ on $\bigcup \mathrm{img}(\mathrm{pre}[\rho])$.*

5 Partitioning and Complete Closures

The aim of this section is to set up a closure operator-based framework to reason about abstract models, as far as their precision is concerned. One main advantage of handling closures is that they allow to reason about properties of abstract models independently from the representation of abstract states. Of course, this setting must be equivalent to the relation-based approach introduced above. Our first result provides a characterization of the closures associated, by Definition 2.6, to (total and) partitioning abstraction relations.

Lemma 5.1. *Let Q be a set and $\mu \in \mathrm{uco}(\wp(Q))$. Then, μ is additive and $\{\mu(\{q\})\}_{q \in Q}$ is a partition of Q iff there exists a set X and a total and partitioning $\rho \subseteq Q \times X$ such that $\mu_\rho = \mu$.*

Thus, this enables us to introduce the following notion.

Definition 5.2. Let Q be a set and $\mu \in \mathrm{uco}(\wp(Q))$. Then, μ is *partitioning* if μ is additive and $\{\mu(\{q\})\}_{q \in Q}$ is a partition of Q. □

Let us now turn to completeness. The following result shows that an abstraction $\langle Q, \rho, A \rangle$ is complete, namely there exists an abstract transition relation S such that $(Q,R) \preccurlyeq_\rho (A,S)$, if and only if the associated closure μ_ρ is complete for $\mathrm{post}[R^{-1}]$ in the classical abstract interpretation sense of Section 2.1. Observe that this is somehow surprising, since completeness for relation-based abstractions (Definition 3.4) is an existential property.

Lemma 5.3. *Let (Q, R) be a transition system and $\langle Q, \rho, A\rangle$ be an abstraction. Then, $\langle Q, \rho, A\rangle$ is complete for (Q, R) iff $\mu_\rho \circ \mathrm{post}[R^{-1}] = \mu_\rho \circ \mathrm{post}[R^{-1}] \circ \mu_\rho$.*

Thus, analogously to Definiton 5.2, this characterization justifies the following notion of completeness for closures w.r.t. a concrete model.

Definition 5.4. Let (Q, R) be a transition system and $\mu \in \mathrm{uco}(\wp(Q))$. Then, μ is *complete* for (Q, R) when $\mu \circ \mathrm{post}[R^{-1}] = \mu \circ \mathrm{post}[R^{-1}] \circ \mu$. □

Consider a closure μ which is simultaneously partitioning and complete. Then, by Definition 2.6 and Lemma 2.7, μ gives rise to a partitioning abstraction $\langle Q, \rho_\mu, A_\mu\rangle$. The following key result shows that the canonical abstract model induced by ρ_μ, as defined at the end of Section 3, actually turns out to be complete.

Theorem 5.5. *Let (Q, R) be a transition system and $\mu \in \wp(Q)$ be partitioning and complete. Then, $(Q, R) \preccurlyeq_{\rho_\mu} (A_\mu, \rho_\mu^{-1} R \rho_\mu)$.*

6 Making Abstract Models Partitioning and Complete

In the previous section we set up a closure-based framework characterizing complete and partitioning abstract model checking. As recalled in Section 2.1, closures, i.e. abstract domains, can be compared w.r.t. their precision simply by their standard pointwise ordering $\sqsubseteq$. On the other hand, we have shown in Section 4 that a complete and partitioning abstract model checking is strongly preserving. Thus, following the general approach of Definition 2.1, in this section we aim at minimally making abstract models complete and partitioning by a least refinement, so that we get a strongly preserving abstract model checking. Following the terminology of Definition 2.1, we have to show that the partitioning and complete shell of any given closure on sets of concrete states actually exists. In order to accomplish this task, first we study separately partitioning shells and complete shells, and then a combination of these solutions will solve our problem.

Definition 6.1. Given any set of states Q, define $\mathbb{P} : \mathrm{uco}(\wp(Q)) \to \mathrm{uco}(\wp(Q))$ as follows:

$$\mathbb{P}(\mu) \stackrel{\text{def}}{=} \lambda Y \in \wp(Q).\{x \in Q \mid \exists y \in Y.\, \mu(\{x\}) = \mu(\{y\})\}.$$ □

It is easy to show that the operator $\mathbb{P}$ is well-defined, i.e., for any $\mu \in \wp(Q)$, $\mathbb{P}(\mu)$ is a closure. Additionally, it turns out that $\mathbb{P}(\mu)$ is an additive closure. More than this can be proved. Actually, it turns out that $\mathbb{P}$ is the right operator refining any closure to its partitioning shell.

Lemma 6.2. *$\mathbb{P}$ is the partitioning shell refinement.*

Example 6.3. Consider $Q = \{1,2,3\}$ and $\mu \in \mathrm{uco}(\wp(Q))$ as given by $\mu = \{\varnothing, \{1\}, \{2\}, \{1,2,3\}\}$. Then, μ is not partitioning, since neither $\{\mu(\{q\})\}_{q \in Q} = \{\{1\}, \{2\}, \{1,2,3\}\}$ is a partition of Q nor μ is additive, namely closed by set union. Then, $\mathbb{P}(\mu) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$, i.e., the least closure, turns out to be the partitioning shell of μ. □

Let us turn to complete closures.

Definition 6.4. Given (Q,R), define $\mathbb{C}_R : \mathrm{uco}(\wp(Q)) \to \mathrm{uco}(\wp(Q))$ as follows:

$$\mathbb{C}_R(\mu) \stackrel{\text{def}}{=} \lambda X \in \wp(Q).\{q \in Q \mid \mu(\mathrm{post}[R^{-1}](\{q\})) \subseteq \mu(\mathrm{post}[R^{-1}](X))\}.$$

Also, for any $\mu \in \mathrm{uco}(\wp(Q))$, define $\mathbb{C}^{\mu}_R : \mathrm{uco}(\wp(Q)) \to \mathrm{uco}(\wp(Q))$ as follows:

$$\mathbb{C}^{\mu}_R(\eta) \stackrel{\text{def}}{=} \mu \sqcap \mathbb{C}_R(\eta).$$ □

It is not hard to show that $\mathbb{C}_R$ is well-defined, i.e., for any $\mu \in \wp(Q)$, $\mathbb{C}_R(\mu)$ is a closure. It turns out that $\mathbb{C}_R$ allows to characterize complete closures. As a consequence, given a closure μ the greatest fixpoint of the operator $\mathbb{C}^{\mu}_R$ provides the complete shell of μ.

Theorem 6.5. *Let (Q,R) be a transition system. Then, for any $\eta \in \mathrm{uco}(\wp(Q))$, η is complete iff $\eta \sqsubseteq \mathbb{C}_R(\eta)$. Moreover, $\lambda\mu.\,\mathrm{gfp}(\mathbb{C}^{\mu}_R)$ is the complete shell refinement.*

Finally, let us combine these separate shell refinements in an operator which simultaneously minimally refines a closure for the partitioning and complete properties. The idea is simple: basically, we consider the glb, i.e. the reduced product, of the single shell refinements. In general, it can be shown that this works for any two properties. Here, we only face with our specific case of interest.

Definition 6.6. Given a transition system (Q,R), for any $\mu \in \mathrm{uco}(\wp(Q))$, define $\mathcal{F}^{\mu}_R : \mathrm{uco}(\wp(Q)) \to \mathrm{uco}(\wp(Q))$ as follows:

$$\mathcal{F}^{\mu}_R(\eta) \stackrel{\text{def}}{=} \mu \sqcap \mathbb{C}_R(\eta) \sqcap \mathbb{P}(\eta).$$ □

Corollary 6.7. *Let (Q,R) be a transition system. Then, $\lambda\mu.\,\mathrm{gfp}(\mathcal{F}^{\mu}_R)$ is the partitioning and complete shell refinement.*

Actually, the above operator $\mathcal{F}^{\mu}_R$ can be simplified as follows.

Lemma 6.8. *Let (Q,R) be a transition system.*
(1) *Define $\mathbb{C}^s_R \stackrel{\text{def}}{=} \mathbb{P} \circ \mathbb{C}_R$. Then, for any $\mu \in \mathrm{uco}(\wp(Q))$,*

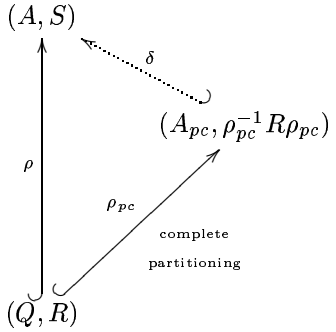
$$\mathbb{C}^s_R(\mu) = \lambda X \in \wp(Q).\{q \in Q \mid \exists x \in X.\, \mu(\mathrm{post}[R^{-1}](\{q\})) = \mu(\mathrm{post}[R^{-1}](\{x\}))\}.$$

(2) *For any $\mu \in \mathrm{uco}(\wp(Q))$, $\mathrm{gfp}(\mathcal{F}^{\mu}_R) = \mathrm{gfp}(\lambda\eta.\,\mu \sqcap \mathbb{C}^s_R(\eta) \sqcap \mathbb{P}(\eta))$.*

Note that for any $\mu \in \mathrm{uco}(\wp(Q))$, $\mathbb{C}^s_R(\mu)$ is a partitioning closure and therefore it is additive. Later on, we will illustrate how this methodology applies to a simple but significant example.

6.1 Refinements and Simulations

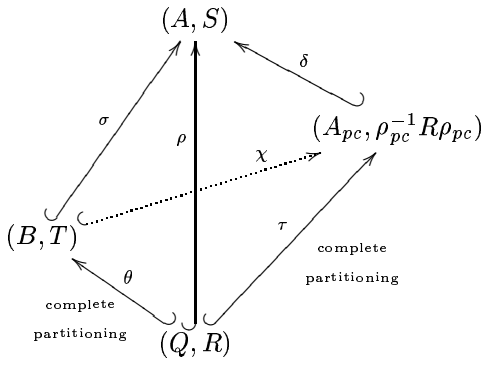
Let (Q, R) and (A, S) be transition systems such that $(Q, R) \sqsubseteq_\rho (A, S)$. Consider the associated closure $\mu_\rho \in \mathrm{uco}(\wp(Q))$, and let $\mu_\rho^{pc} \in \mathrm{uco}(\wp(Q))$ be the partitioning and complete shell of μ_ρ as given by Corollary 6.7. Let $\langle Q, \rho_{pc}, A_{pc} \rangle$ be the abstraction of Q canonically associated to μ_ρ^{pc} by Definition 2.6. Then, by Theorem 3.6, the canonical complete abstract model induced by the complete and partitioning abstraction relation ρ_{pc} is complete, i.e., $(Q, R) \preccurlyeq_{\rho_{pc}} (A_{pc}, \rho_{pc}^{-1} R \rho_{pc})$. It can be shown that the initial abstract model is an abstraction of its complete and partitioning refinement, i.e., there exists $\delta \subseteq A_{pc} \times A$ such that $(A_{pc}, \rho_{pc}^{-1} R \rho_{pc}) \sqsubseteq_\delta (A, S)$ where, additionally, $\rho = \rho_{pc}\delta$. The scenario is depicted by the following commuting diagram.



We show that $(A_{pc}, \rho_{pc}^{-1} R \rho_{pc})$ actually is the least complete and partitioning refinement of (A, S) with respect to (Q, R) for the canonical simulation preordering between transition systems. This is formalized by the following result.

Theorem 6.9. *Let (B, T) be a transition system such that: (1) $(B, T) \sqsubseteq_\sigma (A, S)$ for some $\sigma \subseteq B \times A$; (2) $(Q, R) \preccurlyeq_\theta (B, T)$ for some $\theta \subseteq Q \times B$; (3) θ is partitioning and surjective; (4) $\rho = \theta\sigma$. Then, there exists $\chi \subseteq B \times A_{pc}$ such that $(B, T) \sqsubseteq_\chi (A_{pc}, \rho_{pc}^{-1} R \rho_{pc})$.*

Thus, the closure-based methodology of refinement given in Section 6 actually is coherent with the standard simulation-based approach. Graphically, this means that the following diagram commutes.



6.2 An Example

Consider the transition systems $\mathcal{T} = (Q, R)$ and $\mathcal{A} = (A, S)$ depicted in Fig. 1. $\mathcal{A}$ is designed as the abstract model where all the concrete states except the state 5 collapse to a single abstract state. Dotted arrows from states of $\mathcal{T}$ to states of $\mathcal{A}$ formally define the abstraction relation $\rho \subseteq Q \times A$. Observe that ρ is partitioning (e.g. use Lemma 2.5).

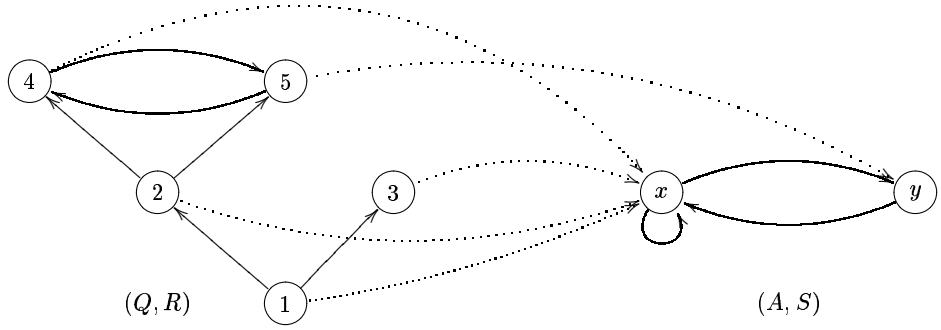


Fig. 1. The concrete and abstract models, and the abstraction relation.

Obviously, we have that $\mathcal{T} \sqsubseteq_\rho \mathcal{A}$. On the other hand, neither ρ-bisimulation nor ρ-completeness hold. In fact, we have that $\mathcal{T} \not\simeq_\rho \mathcal{A}$: $\langle y, 3\rangle \in S^{-1}\rho^{-1}$ whereas $\langle y, 3\rangle \notin \rho^{-1}R^{-1}$. Also, $\mathcal{T} \not\preceq_\rho \mathcal{A}$: $\langle 1, y\rangle \in \rho S^{-1}$ whereas $\langle 1, y\rangle \notin R^{-1}\rho$.

Consider the following temporal specification φ: "at present state there exists an execution trace which visited the state 5", namely, "the present state may be reached from the state 5". Of course, for the concrete model $\mathcal{T}$ we have that $|\varphi|_\mathcal{T} = \{4, 5\}$ and therefore, for example, $2 \notin |\varphi|_\mathcal{T}$. Let p be the atomic proposition "the present state is 5" so that the corresponding interpretation $\mathcal{I}$ is $\mathcal{I}(p) = \{5\}$. The induced interpretation on $\wp(A)$ is therefore $\mathcal{I}^\sharp \stackrel{\text{def}}{=} \text{post}[\rho] \circ \mathcal{I}$ such that $\mathcal{I}^\sharp(p) = \{y\}$. Then, φ can be specified in the past μ-calculus by the formula $\varphi \stackrel{\text{def}}{=} \mu x.(p \vee \Diamond^p x) \in L_\mu^{\leftarrow}$.

Our aim is to perform an abstract check of $2 \notin |\varphi|_\mathcal{T}$. Preservation given by Theorem 4.1 is not enough: we need strong preservation and Theorem 4.2 cannot be applied. Thus, we refine the abstract model checking $\mathcal{A}$ using our methodology in order to get an enhanced abstract model which satisfies the hypotheses of Theorem 4.3. Note that in order to be able to apply Theorem 4.3, we will need that the interpretation of the atomic proposition p belongs to $\text{img}(\text{pre}[\rho])$: this is already true for $\mathcal{A}$ and hence it will be still true for the refinement of $\mathcal{A}$.

Let $\mu_\rho \stackrel{\text{def}}{=} \widetilde{\text{pre}}[\rho] \circ \text{post}[\rho]$. Thus, the set of fixpoints of μ_ρ is as follows:

$$\mu_\rho = \{\varnothing, \{1, 2, 3, 4\}, \{5\}, \{1, 2, 3, 4, 5\}\}.$$

It is immediate to observe that μ_ρ is already partitioning, and therefore, by Lemma 6.2, $\mathbb{P}(\mu_\rho) = \mu_\rho$.

By Lemma 6.8, let us now compute $\mathbb{C}^s_R(\mu_\rho)$. Since $\mathbb{C}^s_R(\mu_\rho)$ is an additive closure, it is enough to compute $\mathbb{C}^s_R(\mu_\rho)(\{q\})$ for any singleton $\{q\}$. By Lemma 6.8, let us recall that $\mathbb{C}^s_R(\mu_\rho)(\{q\}) = \{x \in Q \mid \mu(\mathrm{post}[R^{-1}](\{x\})) = \mu(\mathrm{post}[R^{-1}](\{q\}))\}$. $\mathrm{post}[R^{-1}]$ works as follows:

$$\begin{aligned}\mathrm{post}[R^{-1}](\{1\}) &= \varnothing,\\ \mathrm{post}[R^{-1}](\{2\}) &= \{1\},\\ \mathrm{post}[R^{-1}](\{3\}) &= \{1\},\\ \mathrm{post}[R^{-1}](\{4\}) &= \{2,5\},\\ \mathrm{post}[R^{-1}](\{5\}) &= \{2,4\}.\end{aligned}$$

Hence, we have:

$$\begin{aligned}\mathbb{C}^s_R(\mu_\rho)(\{1\}) &= \{1\},\\ \mathbb{C}^s_R(\mu_\rho)(\{2\}) &= \{2,3,5\},\\ \mathbb{C}^s_R(\mu_\rho)(\{3\}) &= \{2,3,5\},\\ \mathbb{C}^s_R(\mu_\rho)(\{4\}) &= \{4\},\\ \mathbb{C}^s_R(\mu_\rho)(\{5\}) &= \{2,3,5\}.\end{aligned}$$

and therefore

$$\mathbb{C}^s_R(\mu_\rho) = \{\varnothing, \{1\}, \{4\}, \{1,4\}, \{2,3,5\}, \{1,2,3,5\}, \{2,3,4,5\}, \{1,2,3,4,5\}\}.$$

By Definition 6.6 and Lemma 6.8, we have that

$$\mu_1 = \mu_\rho \sqcap \mathbb{P}(\mu_\rho) \sqcap \mathbb{C}^s_R(\mu_\rho) = \mu_\rho \sqcap \mathbb{C}^s_R(\mu_\rho) =$$

$$= \{\varnothing, \{1\}, \{4\}, \{5\}, \{1,4\}, \{2,3\}, \{1,2,3\}, \{2,3,4\}, \{2,3,5\},$$
$$\{1,2,3,4\}, \{1,2,3,5\}, \{2,3,4,5\}, \{1,2,3,4,5\}\}.$$

Let us now go on with the second iteration, i.e., $\mu_2 = \mu \sqcap \mathbb{P}(\mu_1) \sqcap \mathbb{C}^s_R(\mu_1)$. Observe that μ_1 is not partitioning, because it is not additive: hence,

$$\mathbb{P}(\mu_1) = \{\varnothing, \{1\}, \{4\}, \{5\}, \{1,4\}, \{1,5\}, \{2,3\}, \{4,5\},$$
$$\{1,2,3\}, \{1,4,5\}, \{2,3,4\}, \{2,3,5\},$$
$$\{1,2,3,4\}, \{1,2,3,5\}, \{2,3,4,5\}, \{1,2,3,4,5\}\}.$$

Let us compute $\mathbb{C}^s_R(\mu_1)$. As before, it is enough to compute $\mathbb{C}^s_R(\mu_1)(\{q\})$ for any singleton $\{q\}$. We have:

$$\begin{aligned}\mathbb{C}^s_R(\mu_1)(\{1\}) &= \{1\},\\ \mathbb{C}^s_R(\mu_1)(\{2\}) = \mathbb{C}^s_R(\mu_1)(\{3\}) &= \{2,3\},\\ \mathbb{C}^s_R(\mu_1)(\{4\}) &= \{4\},\\ \mathbb{C}^s_R(\mu_1)(\{4\}) &= \{5\},\end{aligned}$$

and therefore, $\mathbb{C}^s_R(\mu_1) = \mu_1$. Thus, $\mu_2 = \mathbb{P}(\mu_1) \sqcap \mathbb{C}^s_R(\mu_1) = \mathbb{P}(\mu_1) \sqcap \mu_1 = \mathbb{P}(\mu_1)$.

It is now easy to check that $\mathbb{P}(\mu_2) = \mu_2$ and $\mathbb{C}^s_R(\mu_2) = \mu_2$. We have reached the fixpoint. Thus, by Corollary 6.7 and Lemma 6.8, μ_2 is the partitioning and complete shell of μ_ρ.

Following Definition 2.6, let us give the abstraction associated to μ_2. We have that $A_{\mu_2} = \{a \stackrel{\text{def}}{=} \mu_2(\{1\}) = \{1\}, b \stackrel{\text{def}}{=} \mu_2(\{2\}) = \mu_2(\{3\}) = \{2,3\}, c \stackrel{\text{def}}{=} \mu_2(\{4\}) = \{4\}, d \stackrel{\text{def}}{=} \mu_2(\{5\}) = \{5\}\}$. The corresponding abstraction $\rho_{\mu_2} \subseteq Q \times A_{\mu_2}$ is depicted in Fig. 2, where the abstract model is equipped with the canonical abstract transition relation $\rho_{\mu_2}^{-1} R \rho_{\mu_2}$. Let $\mathcal{A}_{pc} \stackrel{\text{def}}{=} (A_{\mu_2}, \rho_{\mu_2}^{-1} R \rho_{\mu_2})$.

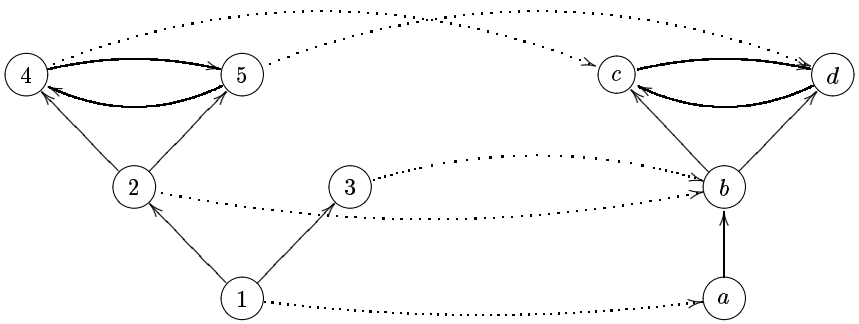


Fig. 2. The refined abstract model $\mathcal{A}_{pc}$.

By Theorem 5.5, $\mathcal{T} \preccurlyeq_{\rho_{\mu_2}} \mathcal{A}_{pc}$. Note that $\mathrm{img}(\mathrm{pre}[\rho_{\mu_2}]) = \{\{1\}, \{2,3\}, \{4\}, \{5\}\}$, and therefore $\mathcal{I}(p) \in \mathrm{img}(\mathrm{pre}[\rho_{\mu_2}])$. The interpretation $\mathcal{I}^\natural$ associated to $\mathcal{A}_{pc}$ is defined as $\mathrm{post}[\rho_{\mu_2}] \circ \mathcal{I}$. Thus, now we can exploit strong preservation as given by Theorem 4.3. We have that $2 \in |\varphi|_{\mathcal{T},\mathcal{I}}$ iff $\mathrm{post}[\rho_{\mu_2}](\{2\}) \subseteq |\varphi|_{\mathcal{A}_{pc},\mathcal{I}^\natural}$. Since $b \notin |\varphi|_{\mathcal{A}_{pc},\mathcal{I}^\natural}$, by strong preservation we conclude that $2 \notin |\varphi|_{\mathcal{T},\mathcal{I}}$, as desired.

7 Future Work

As recalled in Section 4, it is well known that bisimulation for the abstract model is a sufficient condition for strong preservation. It is then natural to ask whether it is possible to apply the methodological ideas of this paper for minimally refining an abstract model in order to get bisimulation. Unfortunately, our preliminary results seem to indicate that this cannot be done under reasonable hypotheses. Let us also cite a recent related work by Schmidt [18], who studied some notions of refinement for binary relations and simulations in connection with the strong preservation property. The possible relationship between Schmidt's work and ours is subject for future work.

Acknowledgements. We wish to thank Gilberto Filé who contributed to the early stages of this work. This work has been partially supported by the Italian MIUR Cofin projects "Abstract interpretation, type systems and control-flow analysis" (Cofin2000) and "MEFISTO" (Cofin2001).

References

1. S. Bensalem, Y. Lakhnech, S. Owre. Computing Abstractions of Infinite State Systems Compositionally and Automatically. In *Proc. CAV'98*, LNCS 1427, pp. 319–331, Springer, 1998.
2. E.M. Clarke, O. Grumberg, S. Jha, Y. Lu, and H. Veith. Counterexample-guided abstraction refinement. In *Proc. CAV'00*, LNCS 1855, pp. 154–169, Springer, 2000.
3. E.M. Clarke, O. Grumberg, S. Jha, Y. Lu, H. Veith. Progress on the State Explosion Problem in Model Checking. In *Informatics - 10 Years Back, 10 Years Ahead.* LNCS 2000, pp. 176–194, Springer, 2001.
4. E.M. Clarke, O. Grumberg, D.E. Long. Model checking and abstraction. In *Proc. ACM POPL'92*, pp. 342–354, 1992.
5. E.M. Clarke, O. Grumberg and D. Long. Model checking and abstraction. *ACM TOPLAS*, 16(5):1512–1542, 1994.
6. E.M. Clarke, O. Grumberg and D.A. Peled. *Model checking.* The MIT Press, 1999.
7. P. Cousot and R. Cousot. Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *Proc. ACM POPL'77*, pp. 238–252, 1977.
8. P. Cousot and R. Cousot. Systematic design of program analysis frameworks. In *Proc. ACM POPL'79*, pp. 269–282, 1979.
9. P. Cousot and R. Cousot. Temporal abstract interpretation. In *Proc. ACM POPL'00*, pp. 12–25, 2000.
10. D. Dams, O. Grumberg, and R. Gerth. Abstract interpretation of reactive systems. *ACM TOPLAS*, 16(5):1512–1542, 1997.
11. J. Dingel and T. Filkorn. Model checking for infinite state systems using data abstraction, assumption-commitment style reasoning and theorem proving. In *Proc. CAV'95*, LNCS 939, pp. 54–69, Springer, 1995.
12. G. Filé, R. Giacobazzi, and F. Ranzato. A unifying view of abstract domain design. *ACM Comput. Surv.*, 28(2):333–336, 1996.
13. R. Giacobazzi and E. Quintarelli. Incompleteness, counterexamples and refinements in abstract model checking. In *Proc. SAS'01*, LNCS 2126, pp. 356–373, Springer, 2001.
14. R. Giacobazzi and F. Ranzato. Refining and compressing abstract domains. In *Proc. ICALP'97*, LNCS 1256, pp. 771–781, Springer, 1997.
15. R. Giacobazzi, F. Ranzato, and F. Scozzari. Making abstract interpretations complete. *J. ACM*, 47(2):361–416, 2000.
16. C. Loiseaux, S. Graf, J. Sifakis, A. Bouajjani, and S. Bensalem. Property preserving abstractions for the verification of concurrent systems. *Formal Methods in System Design*, 6:1–36, 1995.
17. F. Ranzato. On the completeness of model checking. In *Proc. ESOP'01*, LNCS 2028, pp. 137–154, Springer, 2001.
18. D.A. Schmidt. Binary relations for abstraction and refinement. In *Proc. Workshop on Refinement and Abstraction*, Japan 1999. To appear in Elsevier Electronic Notes in Computer Science.