States vs. Traces in Model Checking by Abstract Interpretation

Roberto Giacobazzi[1] and Francesco Ranzato[2]

[1] Dipartimento di Informatica
Università di Verona
Strada Le Grazie 15, 37134 Verona, Italy
giaco@sci.univr.it
[2] Dipartimento di Matematica Pura ed Applicata
Università di Padova
Via Belzoni 7, 35131 Padova, Italy
franz@math.unipd.it

Abstract. In POPL'00, Cousot and Cousot showed that the classical *state-based* model checking of a very general temporal language called $\overset{\frown}{\mu}$-calculus is an *incomplete* abstract interpretation of its *trace-based* semantics. In ESOP'01, Ranzato showed that the least refinement of the state-based model checking semantics of the $\overset{\frown}{\mu}$-calculus which is *complete* w.r.t. its trace-based semantics exists, and it is essentially the trace-based semantics itself. The analogous problem in the opposite direction is solved by the present paper. First, relatively to any incomplete temporal connective of the $\overset{\frown}{\mu}$-calculus, we characterize the structure of the models, i.e. transition systems, for which the state-based model checking is trace-complete. On this basis, we prove that the unique abstraction of the state-based model checking semantics of the $\overset{\frown}{\mu}$-calculus (actually, of any fragment allowing conjunctions) which is complete w.r.t. the trace-based semantics is the straightforward semantics carrying no information at all. The following consequence can be drawn: there is no way to either refine or abstract sets of states in order to get a model checking algorithm for (any fragment allowing conjunctions of) the $\overset{\frown}{\mu}$-calculus which is trace-complete.

1 Introduction

The standard state-based model checking problem consists in characterizing the set of all the states of a transition system, modelling some reactive system, that satisfy a given temporal specification ϕ. ϕ is defined within some temporal logic language and specifies the required temporal properties of the system to be verified [7, 16]. This model checking procedure must collect all the states s of the model M such that all the possible executions (in the existential checking: "there exists one execution") in M departing from s satisfy ϕ: $\{s \in \mathit{State} \mid M, s \models_{\mathit{state}} \phi\}$, where $\models_{\mathit{state}}$ is used to emphasize the state-based semantics of temporal formulae (i.e., the semantics of a temporal formula is a set of states). Although model checking systems are state-based, i.e. they solve

the above state-based model checking problem, semantics of temporal calculi can be also naturally given in terms of sets of execution traces, i.e. sequences of states distributed along a discrete time-line. Obviously, traces are much richer than states, and, as advocated by Cousot and Cousot [11] in their approach to model checking, the natural semantics of a temporal formula should be a set of execution traces. Nevertheless, for obvious pragmatic reasons of efficiency, model-checkers handle and observe states only, i.e., they abstract away from traces observing states. This abstraction is the subject of this paper. A far more concrete model checking problem can then be formulated for traces: the semantics of a temporal formula is a set of traces, and $M, s \models_{trace} \phi$ means that all the traces in M with present state s satisfy ϕ, i.e. belong to the semantics of ϕ. It should be clear that trace-based model checking is strictly more precise, but it is obviously unfeasible to design a practical model checking algorithm for system verification handling sets of traces. It is not clear however whether it is possible to find some approximation of the trace-based model checking problem which can be solved starting from the state-based model checking with no loss of precision, namely this approximate checking should be logically equivalent to the trace-based checking. More precisely, the paper answers the following question: is it possible to minimally refine or abstract the state-based semantics of a general temporal calculus so that this induces a corresponding model checking which is trace-complete, i.e. logically equivalent to the trace-based model checking? In our approach, refinements and abstractions of a semantics are intended to be expressed by standard abstract interpretation. As far as refinements are concerned, the negative answer has been given by Ranzato [17]: the only semantic refinement of the state-based semantics inducing a trace-complete model checking is the trace-based semantics itself. This paper faces with the remaining question and also in this case reports a negative answer: there exists no trace-complete abstraction of the state-based semantics but for the trivial semantics carrying no information at all. Thus, summing up, this result shows that states are, so to say, "intrinsically trace-incomplete", since there is no way to get a trace-complete model checking by modifying by refinement or by abstraction the state-based semantics.

The Scenario. This result is formulated and shown within the Cousot and Cousot's [11] abstract interpretation approach to model checking. In POPL'00, Cousot and Cousot proposed a general framework, called *temporal abstract interpretation*, introducing an enhanced temporal calculus, called $\overset{\curvearrowright}{\mu}$-calculus and inspired by Kozen's μ-calculus, with a trace-based semantics, and hence featuring a trace-based model checking. The state-based model checking is then specified as an abstract interpretation of the trace-based model checking. The trace-based semantics of the $\overset{\curvearrowright}{\mu}$-calculus is time-symmetric: this means that execution traces have potentially infinite length both in the future and in the past. This time-symmetry is not the only new feature of the $\overset{\curvearrowright}{\mu}$-calculus. The $\overset{\curvearrowright}{\mu}$-calculus also provides a tight combination of linear- and branching-time, allowing to derive classical specification languages like CTL, CTL*, and Kozen's μ-calculus itself, as suitable fragments.

One of the main achievements of Cousot and Cousot's paper [11] is that state-based model checking has been reduced to an abstract interpretation of the trace-based semantics of the $\overset{\frown}{\mu}$-calculus. The semantics $[\![\phi]\!]^{trace}$ of a temporal specification ϕ is the set of traces of a transition system M making ϕ true. Coherently with the state-based model checking problem, the state-abstraction $\alpha^{\forall}_M$ abstracts a set of traces $[\![\phi]\!]^{trace}$ to the set of states of M such that any execution of M departing from s satisfies the formula ϕ: $\alpha^{\forall}_M([\![\phi]\!]^{trace}) = \{s \in \mathit{State} \mid M, s \models_{trace} \phi\}$, where $M, s \models_{trace} \phi$ means that all the traces in M with present state s are in $[\![\phi]\!]^{trace}$. This abstraction $\alpha^{\forall}_M$ induces a state-based semantics $[\![\cdot]\!]^{state}$ for the $\overset{\frown}{\mu}$-calculus which is sound by construction with respect to the trace semantics: for any temporal formula ϕ, $[\![\phi]\!]^{state} \subseteq \alpha^{\forall}_M([\![\phi]\!]^{trace})$. As proved in [11], this inclusion may be strict, namely the state-based model checking of the $\overset{\frown}{\mu}$-calculus is trace-incomplete. This means that there exists some formula ϕ and state s of the system such that $M, s \models_{trace} \phi$ (viz., $s \in \alpha^{\forall}_M([\![\phi]\!]^{trace})$), while $M, s \not\models_{state} \phi$ (viz., $s \notin [\![\phi]\!]^{state}$). This incompleteness means that the semantics $[\![\cdot]\!]^{state}$ used for designing and proving preserving or even strongly preserving properties of most state-based model checking algorithms is incomplete w.r.t. traces. The same holds even for abstract model checking [5, 7, 12, 15], where the abstraction map actually is a state-abstraction and can be modeled as a further abstract interpretation step of $[\![\cdot]\!]^{state}$ [11, 14]. It is therefore important in order to understand the limits of state-based (concrete or abstract) model checking with respect to properties of traces, to investigate whether it is possible to find a semantics $[\![\cdot]\!]^{?}$ as a refinement or abstraction of $[\![\cdot]\!]^{state}$ which is complete for the trace-based semantics $[\![\cdot]\!]^{trace}$.

The Main Result. Ranzato [17] proved that any refinement of the state-based model checking, i.e. which can be obtained by refining the abstraction $\alpha^{\forall}_M$, is still incomplete with respect to the trace-based semantics of the full $\overset{\frown}{\mu}$-calculus. This means that the most abstract semantics which is trace-complete and includes the state-based semantics, is the trace-based semantics itself. This shows that there is no way to enhance state-based model checking to get completeness for traces unless having traces themselves in the model. In this paper we consider the symmetrical situation: instead of refining the state-based model checking abstraction $\alpha^{\forall}_M$, we are interested in isolating those abstractions of $\alpha^{\forall}_M$ which are trace-complete, namely no loss of precision is introduced in the verification by using a state-based model checker with respect to check the same property on the trace-based semantics.

The fact that completeness can be achieved not only by refining abstract domains but also by abstracting them should not be surprising. In this case the abstraction is intended to remove from the abstract domain the source of potential incompleteness in such a way that the resulting domain contains the largest amount of information in order to let completeness be achieved. Consider for instance the abstract domain $\mathit{Sign}^{+} = \{\mathbb{Z}, [0, +\infty], [-\infty, 0], [0, 10], [0]\}$. This domain is not complete for integer multiplication: for example, 2×2 is approximated in Sign^{+} by $[0, 10]$ while the abstract multiplication $\otimes$ in Sign^{+} of the same expression $[0, 10] \otimes [0, 10]$ is $[0 + \infty]$. However, $\mathit{Sign} = \{\mathbb{Z}, [0, +\infty], [-\infty, 0], [0]\}$,

which is an abstraction of $Sign^+$, turns out to be complete for multiplication, i.e. abstract multiplication can be performed with no loss of precision with respect to the approximation of the concrete multiplication. *Sign* is the most concrete domain which abstracts $Sign^+$ and it is complete for multiplication: this is called the *core* of $Sign^+$ (see [13] for details). The core of $Sign^+$ removed the abstract value $[0, 10]$, which was the unique source of incompleteness.

We first characterize the structure of transition systems for which the state-based model checking is complete for the basic modalities predecessor, time-reversal, and conjunction of the $\overset{\curvearrowright}{\mu}$-calculus. In particular, conjunction turns out to be the crucial connective: in fact, the core of the state-based model checking for the conjunction is the straightforward abstraction of states carrying no information at all. On the basis of this fact, we prove that, for any fragment of the $\overset{\curvearrowright}{\mu}$-calculus allowing arbitrary conjunctions, the straightforward abstraction is the unique abstraction of the state-based model checking which induces a corresponding model checking which is complete for the trace-based semantics. This result, together with the one proved by Ranzato [17], shows that there is no way to get a complete approximation of the trace-based semantics by either refining or approximating the state-based model checking, emphasizing the intrinsic limits of the precision of state-based model checking with respect to the trace-based semantics of the $\overset{\curvearrowright}{\mu}$-calculus. This proves that state-based model checking cannot be used as an economic way to prove properties of traces in a complete way. In particular, since abstract model checking can be viewed as abstract interpretation of $[\![\cdot]\!]^{state}$ (cf. [11]), this also implies that there is no abstraction α of states (unless it is the straightforward abstraction) such that no loss of precision occurs by considering the abstract model checking $[\![\cdot]\!]^{\alpha(state)}$ with respect to $\alpha([\![\cdot]\!]^{trace})$. Otherwise stated, any abstract model checking is intrinsically incomplete with respect to the trace-based semantics of the $\overset{\curvearrowright}{\mu}$-calculus.

2 Abstract interpretation and model checking

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 closure operators on a complete lattice $\langle C, \leq, \vee, \wedge, \top, \bot \rangle$, where $\rho \sqsubseteq \eta$ iff $\forall x \in C.\ \rho(x) \leq \eta(x)$. Throughout the paper, for any $\rho \in \mathrm{uco}(C)$, we follow a standard notation by denoting the image $\rho(C)$ simply by ρ itself: This does not give rise to ambiguity, since one can readily distinguish the use of ρ as function or set according to the context. Let us recall that (i) each closure $\rho \in \mathrm{uco}(C)$ is uniquely determined by the set of its fix-points, which coincides with its image, i.e. $\rho = \{x \in C \mid \rho(x) = x\}$ and (ii) $\rho \sqsubseteq \eta$ iff $\eta \subseteq \rho$.

Within the standard Cousot and Cousot framework, abstract domains can be equivalently specified either by Galois connections/insertions (GCs/GIs) or by closure operators [10]. In the first case, concrete and abstract domains C and A — for simplicity, these are assumed to be complete lattices — are related by a pair of adjoint functions $\alpha : C \to A$ 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 (this closure could be also given by means of its set of fix-points). Given a concrete domain C, we will identify $\mathrm{uco}(C)$ with the so-called complete lattice $\mathcal{L}_C$ of abstract interpretations of C (cf. [9, Section 7] and [10, Section 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 $\mathcal{L}_C$ give, respectively, the most precise abstraction and the most abstract concretization of a family of abstract domains.

Complete Abstract Interpretations. Let us succinctly 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, where $A \in \mathcal{L}_C$. 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 $A \in \mathcal{L}_C$ 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 depends on the underlying abstract domain only. Thus, for abstract domains specified by closure operators, an abstract domain $\rho \in \mathcal{L}_C$ is defined to be complete for f if $\rho \circ f = \rho \circ f \circ \rho$. More in general, this definition of completeness can be naturally extended to a set F of semantic functions by requiring completeness for each $f \in F$. Throughout the paper, we will adopt the following notation: $\Gamma(C, f) \stackrel{\text{def}}{=} \{\rho \in \mathcal{L}_C \mid \rho \text{ is complete for } f\}$. Hence, for a set F, $\Gamma(C, F) = \cap_{f \in F} \Gamma(C, f)$.

2.2 Temporal abstract interpretation

Let us recall the basic notions and definitions of Cousot and Cousot's [11] abstract interpretation-based approach to model checking. $\mathbb{S}$ is a given, possibly infinite, set of states. Discrete time is modeled by the whole set of integers and therefore paths of states are time-symmetric, in particular are infinite also in the past. Thus, $\mathbb{P} \stackrel{\text{def}}{=} \mathbb{Z} \to \mathbb{S}$ is the set of paths (an execution path with an initial state s can then be encoded by repeating forever in the past the state s). Of course,

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

traces keep track of the present time, and hence $\mathbb{T} \stackrel{\text{def}}{=} \mathbb{Z} \times \mathbb{P}$ is the set of traces. A (temporal) model is simply a set of traces: $\mathbb{M} \stackrel{\text{def}}{=} \wp(\mathbb{T})$ is the set of temporal models. The semantics of a temporal logical formula ϕ will be a temporal model, that will be the set of all and only those traces making ϕ true.

Models to check will be generated by transition systems, encoding some reactive system. The transition relation $\rightarrow \subseteq \mathbb{S} \times \mathbb{S}$ is assumed to be total, i.e., $\forall s \in \mathbb{S}. \exists s' \in \mathbb{S}.\, s \rightarrow s'$ and $\forall s' \in \mathbb{S}. \exists s \in \mathbb{S}.\, s \rightarrow s'$. This is not restrictive, since any transition relation can be lifted to a total transition relation simply by adding transitions $s \rightarrow s$ for any state s which is not reachable or which cannot reach any state. The model generated by the transition system $\langle \mathbb{S}, \rightarrow \rangle$ is therefore defined as $\mathcal{M}_{\rightarrow} \stackrel{\text{def}}{=} \{\langle i, \sigma \rangle \in \mathbb{T} \mid i \in \mathbb{Z},\ \forall k \in \mathbb{Z}.\, \sigma_k \rightarrow \sigma_{k+1}\}$.

The reversible $\overset{\curvearrowright}{\mu}$-calculus has been introduced by Cousot and Cousot [11] as a generalization of Kozen's μ-calculus, provided with a trace-based semantics. Throughout the paper, $\mathbb{X}$ will denote an infinite set of logical variables.

Definition 2.1 ([11, Definition 13]). Formulae ϕ of the reversible $\overset{\curvearrowright}{\mu}$-calculus are inductively defined as follows:

$$\phi ::= \boldsymbol{\sigma}_S \mid \boldsymbol{\pi}_t \mid X \mid \oplus\, \phi \mid \phi^{\curvearrowleft} \mid \phi_1 \vee \phi_2 \mid \neg\phi \mid \boldsymbol{\mu} X.\phi \mid \boldsymbol{\nu} X.\phi \mid \forall \phi_1 : \phi_2$$

where the quantifications are as follows: $S \in \wp(\mathbb{S})$, $t \in \wp(\mathbb{S} \times \mathbb{S})$, and $X \in \mathbb{X}$. $\mathfrak{L}_{\overset{\curvearrowright}{\mu}}$ denotes the set of $\overset{\curvearrowright}{\mu}$-calculus formulae. □

The intuition is that a closed formula ϕ is interpreted as the set of traces which make ϕ true. The trace-based semantics for the $\overset{\curvearrowright}{\mu}$-calculus goes as follows.

Definition 2.2 ([11, Definition 13]). $\mathbb{E} \stackrel{\text{def}}{=} \mathbb{X} \rightarrow \mathbb{M}$ is the set of environments over $\mathbb{X}$. Given $\xi \in \mathbb{E}$, $X \in \mathbb{X}$ and $N \in \mathbb{M}$, $\xi[X/N] \in \mathbb{E}$ is defined to be the environment acting as ξ in $\mathbb{X} \setminus \{X\}$ and mapping X to N. The $\overset{\curvearrowright}{\mu}$-calculus semantics $[\![\cdot]\!] : \mathfrak{L}_{\overset{\curvearrowright}{\mu}} \rightarrow \mathbb{E} \rightarrow \mathbb{M}$ is inductively and partially (because least or greatest fix-points could not exist) defined as follows:

$$\begin{array}{ll}
[\![\boldsymbol{\sigma}_S]\!]\xi \stackrel{\text{def}}{=} \boldsymbol{\sigma}_{\{\!|S|\!\}} & [\![\phi_1 \vee \phi_2]\!]\xi \stackrel{\text{def}}{=} [\![\phi_1]\!]\xi \cup [\![\phi_2]\!]\xi \\
[\![\boldsymbol{\pi}_t]\!]\xi \stackrel{\text{def}}{=} \boldsymbol{\pi}_{\{\!|t|\!\}} & [\![\neg\phi]\!]\xi \stackrel{\text{def}}{=} \neg([\![\phi]\!]\xi) \\
[\![X]\!]\xi \stackrel{\text{def}}{=} \xi(X) & [\![\boldsymbol{\mu} X.\phi]\!]\xi \stackrel{\text{def}}{=} \mathit{lfp}(\lambda N \in \mathbb{M}.[\![\phi]\!]\xi[X/N]) \\
[\![\oplus\, \phi]\!]\xi \stackrel{\text{def}}{=} \oplus\, ([\![\phi]\!]\xi) & [\![\boldsymbol{\nu} X.\phi]\!]\xi \stackrel{\text{def}}{=} \mathit{gfp}(\lambda N \in \mathbb{M}.[\![\phi]\!]\xi[X/N]) \\
[\![\phi^{\curvearrowleft}]\!]\xi \stackrel{\text{def}}{=} {}^{\curvearrowleft}([\![\phi]\!]\xi) & [\![\forall \phi_1 : \phi_2]\!]\xi \stackrel{\text{def}}{=} \forall([\![\phi_1]\!]\xi, [\![\phi_2]\!]\xi),
\end{array}$$

where the corresponding temporal model transformers are defined as follows:

- For any $S \in \wp(\mathbb{S})$, $\boldsymbol{\sigma}_{\{\!|S|\!\}} \stackrel{\text{def}}{=} \{\langle i, \sigma \rangle \in \mathbb{T} \mid \sigma_i \in S\} \in \mathbb{M}$ is the S-state model, i.e., the set of traces whose current state is in S.
- For any $t \in \wp(\mathbb{S} \times \mathbb{S})$, $\boldsymbol{\pi}_{\{\!|t|\!\}} \stackrel{\text{def}}{=} \{\langle i, \sigma \rangle \in \mathbb{T} \mid (\sigma_i, \sigma_{i+1}) \in t\} \in \mathbb{M}$ is the t-transition model, i.e., the set of traces whose next step is a t-transition.
- $\oplus : \mathbb{M} \rightarrow \mathbb{M}$ is the predecessor transformer: $\oplus(X) \stackrel{\text{def}}{=} \{\langle i-1, \sigma \rangle \in \mathbb{T} \mid \langle i, \sigma \rangle \in X\} = \{\langle i, \sigma \rangle \in \mathbb{T} \mid \langle i+1, \sigma \rangle \in X\}$.

– $\curvearrowleft : \mathbb{M} \to \mathbb{M}$ is the reversal transformer:
$\curvearrowleft(X) \stackrel{\text{def}}{=} \{\langle -i, \lambda k.\sigma_{-k}\rangle \in \mathbb{T} \mid \langle i, \sigma\rangle \in X\}$.
– $\neg : \mathbb{M} \to \mathbb{M}$ is the complement transformer:
$\neg X \stackrel{\text{def}}{=} \mathbb{M} \smallsetminus X$.
– Given $s \in \mathbb{S}$, $(\cdot)_{\downarrow s} : \mathbb{M} \to \mathbb{M}$ is the state projection operator:
$X_{\downarrow s} \stackrel{\text{def}}{=} \{\langle i, \sigma\rangle \in X \mid \sigma_i = s\}$.
– $\forall : \mathbb{M} \times \mathbb{M} \to \mathbb{M}$ is the universal state closure transformer:
$\forall(X, Y) \stackrel{\text{def}}{=} \{\langle i, \sigma\rangle \in X \mid X_{\downarrow \sigma_i} \subseteq Y\}$. □

The successor operator $\ominus$ on traces can be dually defined as follows:

$$\ominus(X) \stackrel{\text{def}}{=} \{\langle i+1, \sigma\rangle \in \mathbb{T} \mid \langle i, \sigma\rangle \in X\} = \{\langle i, \sigma\rangle \in \mathbb{T} \mid \langle i-1, \sigma\rangle \in X\}.$$

Within this trace-based framework the model checking problem is easily formulated as follows. A closed temporal specification $\phi \in \mathfrak{L}_{\widehat{\mu}}$ is identified by its semantics, namely by the temporal model $[\![\phi]\!]\varnothing \in \mathbb{M}$. Thus, the *universal model checking* of a system $\mathcal{M}_{\rightarrow}$ against a specification ϕ amounts to check whether $\mathcal{M}_{\rightarrow} \subseteq [\![\phi]\!]\varnothing$. Dually, in the *existential model checking* the goal is that of checking whether $[\![\phi]\!]\varnothing \cap \mathcal{M}_{\rightarrow} \neq \varnothing$.

2.3 State-based model checking abstractions

The classical state-based model checking can be formulated as an abstract interpretation, roughly abstracting traces to states.

Universal Checking Abstraction. Given a model (to check) $M \in \mathbb{M}$, the universal checking abstraction map $\alpha^{\forall}_M : \mathbb{M} \to \wp(\mathbb{S})$ abstracts a trace-interpreted temporal specification $\phi \in \mathbb{M}$ to the set of possible (present) states s of M which universally satisfy ϕ, that is, such that if the present state of M is s then ϕ holds. The intuition is that $\alpha^{\forall}_M(\phi)$ encodes a standard state-based interpretation like $\{s \in \mathbb{S} \mid M, s \models \phi\}$. The universal checking abstraction is therefore encoded by the following definition [11, Definition 45]:

$$\alpha^{\forall}_M(\phi) \stackrel{\text{def}}{=} \{s \in \mathbb{S} \mid M_{\downarrow s} \subseteq \phi\}.$$

Following the terminology by Müller-Olm et al. [16]: (i) the state-based global model checking problem of determining the set of present states in M that satisfy ϕ simply amounts to determining $\alpha^{\forall}_M(\phi)$, and (ii) the state-based local model checking problem of checking if a given state s in M satisfies ϕ amounts to checking whether $s \in \alpha^{\forall}_M(\phi)$.

In this case, the superset relation between states provides the notion of approximation. Actually, $\alpha^{\forall}_M$ gives rise to an adjunction between $\langle \mathbb{M}, \supseteq\rangle$ and $\langle \wp(\mathbb{S}), \supseteq\rangle$, and, together with its adjoint $\gamma^{\forall}_M$, induces the following closure operator on models.

Definition 2.3. The *universal checking closure* relative to a model $M \in \mathbb{M}$ is $\rho^{\forall}_M \stackrel{\text{def}}{=} \gamma^{\forall}_M \circ \alpha^{\forall}_M \in \mathrm{uco}(\langle \mathbb{M}, \supseteq\rangle)$ defined by $\rho^{\forall}_M = \lambda X.\{\langle i, \sigma\rangle \in M \mid M_{\downarrow \sigma_i} \subseteq X\}$. □

The intuition is that $\rho^{\forall}_M(X)$ throws away from X all those traces $\langle i, \sigma\rangle$ either which are not in M — these traces "do not matter", since $\alpha^{\forall}_M(\neg M) = \varnothing$ — or which are in M but whose present state σ_i does not universally satisfy X.

Existential Checking Abstraction. Dually, the existential checking abstraction map $\alpha^{\exists}_M : \mathbb{M} \to \wp(\mathbb{S})$ abstracts a given trace-interpreted temporal specification $\phi \in \mathbb{M}$ to the set of possible (present) states s of the model M which existentially satisfy ϕ, that is, for which there exists at least a trace of M which satisfies ϕ and whose present state is s. This leads to the following definition [11, Definition 49]:

$$\alpha^{\exists}_M(\phi) \stackrel{\text{def}}{=} \{s \in \mathbb{S} \mid M_{\downarrow s} \cap \phi \neq \varnothing\}.$$

It can be roughly said that the existential checking abstraction is useful for checking so-called safety properties of reactive systems, i.e., "bad things do not happen during executions". In fact, the subset relation formalizes the notion of approximation: if $\alpha^{\exists}_M(\phi) \subseteq S$ then each $s \notin S$ is such that if M is in state s then ϕ surely does not hold, and therefore any $T \supseteq S$ has to be understood as less precise than S. It turns out that $\alpha^{\exists}_M$ gives rise to an adjunction between $\langle \mathbb{M}, \subseteq\rangle$ and $\langle \wp(\mathbb{S}), \subseteq\rangle$, and hence to the following closure ($\gamma^{\exists}_M$ is the adjoint map).

Definition 2.4. The *existential checking closure* relative to a model $M \in \mathbb{M}$ is $\rho^{\exists}_M \stackrel{\text{def}}{=} \gamma^{\exists}_M \circ \alpha^{\exists}_M \in \text{uco}(\langle \mathbb{M}, \subseteq\rangle)$ defined by $\rho^{\exists}_M = \lambda X.\{\langle i, \sigma\rangle \in \mathbb{T} \mid \langle i, \sigma\rangle \in M \Rightarrow M_{\downarrow \sigma_i} \cap X \neq \varnothing\} = \lambda X.\{\langle i, \sigma\rangle \in M \mid M_{\downarrow \sigma_i} \cap X \neq \varnothing\} \cup \neg M$. □

Here, the intuition is that $\rho^{\exists}_M$ adds to X any trace which is not in M — these can be considered meaningless as far as the existential checking of M is concerned, since $\alpha^{\exists}_M(\neg M) = \varnothing$ — and any trace in M whose present state existentially satisfies X.

State-Based (Abstract) Semantics. Given a total transition system $\langle \mathbb{S}, \rightarrow\rangle$ and its associated model $\mathcal{M}_{\rightarrow}$, the classical state-based semantics on $\wp(\mathbb{S})$ of a temporal formula is calculationally designed as the abstract semantics induced by the model checking abstractions seen above. This is an instance of the standard abstract interpretation methodology (as recalled in general terms by Cousot and Cousot in [11, Section 8]): basically, this amounts to abstract any model transformer of Definition 2.2 by the corresponding best correct approximation induced by the checking abstraction. For example, the predecessor transformer $\ominus : \mathbb{M} \to \mathbb{M}$ is abstracted to $\alpha^{\forall}_{\mathcal{M}_{\rightarrow}} \circ \ominus \circ \gamma^{\forall}_{\mathcal{M}_{\rightarrow}} : \wp(\mathbb{S}) \to \wp(\mathbb{S})$.

The general scenario is as follows. $\mathbb{E}^s \stackrel{\text{def}}{=} \mathbb{X} \to \wp(\mathbb{S})$ is the set of state environments. The checking abstractions $\alpha^{\forall}_M$ and $\alpha^{\exists}_M$ are extended pointwise to environments: $\dot{\alpha}^{\forall}_M$, $\dot{\alpha}^{\exists}_M : \mathbb{E} \to \mathbb{E}^s$, where, e.g., $\dot{\alpha}^{\forall}_M(\xi) \stackrel{\text{def}}{=} \lambda X \in \mathbb{X}.\alpha^{\forall}_M(\xi(X))$. The process of abstraction then compositionally leads to the following abstract state-based semantics for the $\overset{\curvearrowright}{\mu}$-calculus: $[\![\cdot]\!]^{\forall}_{\rightarrow}$, $[\![\cdot]\!]^{\exists}_{\rightarrow} : \mathfrak{L}_{\overset{\curvearrowright}{\mu}} \to \mathbb{E}^s \to \wp(\mathbb{S})$. These are inductively defined as one expects, following the lines of Definition 2.2. Thus, $[\![\phi]\!]^{\forall}_{\rightarrow}$ and $[\![\phi]\!]^{\exists}_{\rightarrow}$ correspond to the classical state interpretations of a temporal formula ϕ.

Soundness of the abstract state-based semantics is by construction: for any $\phi \in \mathfrak{L}_{\widehat{\mu}}$ and $\xi \in \mathbb{E}$, $\alpha^{\forall}_{\mathcal{M}_{\rightarrow}}([\![\phi]\!]\xi) \supseteq [\![\phi]\!]^{\forall}_{\rightarrow}\dot{\alpha}^{\forall}_{\mathcal{M}_{\rightarrow}}(\xi)$ and $\alpha^{\exists}_{\mathcal{M}_{\rightarrow}}([\![\phi]\!]\xi) \subseteq [\![\phi]\!]^{\forall}_{\rightarrow}\dot{\alpha}^{\exists}_{\mathcal{M}_{\rightarrow}}(\xi)$.

In general, completeness does not hold, even when the set of states is finite, i.e., the containments above may well be strict (see the finite counterexample given in [11, Counterexample (60)]). This means, for example, that there exist a closed formula $\phi \in \mathfrak{L}_{\widehat{\mu}}$ and a state $s \in \mathbb{S}$ such that trace-based and state-based model checking for ϕ in s are not equivalent: $\mathcal{M}_{\rightarrow}, s \models_{trace} \phi$ (viz., $(\mathcal{M}_{\rightarrow})_{\downarrow s} \subseteq [\![\phi]\!]\varnothing$), while $\mathcal{M}_{\rightarrow}, s \not\models_{state} \phi$ (viz., $s \notin [\![\phi]\!]^{\forall}_{\rightarrow}\varnothing$). Intuitively, incompleteness states that in order to deal with temporal specifications of the $\widehat{\mu}$-calculus, model checking algorithms should handle sets of traces instead that sets of states, and clearly this is unfeasible.

Cousot and Cousot [11] identified the model transformers causing such incompleteness and provided some sufficient conditions ensuring completeness. The first incomplete transformer for the universal checking abstraction is the predecessor operator $\oplus$, as shown in [11, Section 11.2]. Disjunction, namely set union, is the second incomplete model transformer, as observed in [11, Section 11.6]. The aforementioned sufficient conditions allow to identify some meaningful complete fragments of the $\widehat{\mu}$-calculus. This is the case, for example, of the $\mu^{\forall}_{+}$-calculus considered in [11, Section 13], which is complete for the universal checking abstraction and subsumes the classical $\forall$CTL logic. Finally, the reversal model transformer $\curvearrowleft$ is also incomplete, as shown by the example given in [17], although this is not explicitly mentioned in [11]. Of course, a dual reasoning can be made for the existential checking abstraction: here, the incomplete model transformers are predecessor, conjunction and reversal.

3 Making state-based model checking complete for traces

We have seen that the possibility of defining a complete abstract operation on a given abstract domain A depends on A only. This means that completeness is an abstract domain property and therefore opens the relevant question of making an abstract interpretation complete by minimally extending or, dually, restricting the underlying abstract domain. Following [13], given a concrete interpretation $f : C \rightarrow C$ and an abstract domain $A \in \mathcal{L}_C$, the *absolute complete shell*[2] (resp., *core*) of A for f, when it exists, is the most abstract (resp., concrete) domain $A^s \in \mathcal{L}_C$ (resp., $A^c \in \mathcal{L}_C$) which extends (resp., restricts), viz. is more (resp., less) precise than A, and is complete for f. In other words, the absolute complete shell, respectively core, of A characterizes the least amount of information to be added to, respectively removed from, A in order to get completeness, when this can be done. These completeness problems have been solved in a constructive way by Giacobazzi et al. in [13].

Theorem 3.1 ([13, Theorem 5.10]). *Let $F \subseteq C \rightarrow C$ and $A \in \mathcal{L}_C$. If F is a set of continuous (i.e., preserving lub's of directed subsets) functions then the*

[2] [13] also introduces the concepts of relative complete shell and core, and this explains the use of the adjective absolute.

absolute complete shell and core of A for F exist, and they can be characterized, respectively, as greatest and least fix-points.

In the following, we study the problem of making state-based model checking complete with respect to the trace semantics of the $\overset{\frown}{\mu}$-calculus by minimally reducing the abstract domain of states $\wp(\mathbb{S})$. We will make the following assumption.

Hypothesis 3.2. *For any universal and existential checking closure, respectively $\rho^{\forall}_M$ and $\rho^{\exists}_M$, the model $M \in \mathbb{M}$ is such that for any $s \in \mathbb{S}$, $|M_{\downarrow s}| > 1$.*

This means that for any state s, $M_{\downarrow s}$ contains at least two traces, i.e., for any trace in the model M there exists at least one more trace in M with the same present state. This hypothesis is satisfied by any model generated by a total transition system. In fact, let $\mathcal{M}_{\rightarrow}$ be generated by a total transition system $\langle \mathbb{S}, \rightarrow \rangle$. Thus, if $s \in \mathbb{S}$ then, by the totality of the transition relation, there exists at least a trace in $\mathcal{M}_{\rightarrow}$ with present state s, i.e., there exists $\langle i, \sigma \rangle \in (\mathcal{M}_{\rightarrow})_{\downarrow s}$. If $\sigma_{i+1} = s = \sigma_i$ then we simply consider the trace $\langle i+1, \sigma \rangle \in (\mathcal{M}_{\rightarrow})_{\downarrow s}$. Otherwise, $\sigma_{i+1} \neq \sigma_i$, and therefore it is enough to consider, for example, the shifted path $\sigma^{+1} \stackrel{\text{def}}{=} \lambda j.\, \sigma_{j+1}$, which is different from the path σ, and the trace $\langle i-1, \sigma^{+1} \rangle$, which belongs to $(\mathcal{M}_{\rightarrow})_{\downarrow s}$.

We have chosen to present our results for the case of the existential checking closure $\rho^{\exists}_M$. The existential closure $\rho^{\exists}_M$ is defined on the concrete domain $\langle \mathbb{M}, \subseteq \rangle$ of models ordered by the subset relation, and therefore this simplifies both the technical approach and the intuition.

3.1 Absolute complete core for the predecessor

As recalled in Section 2.3, the predecessor model transformer of Definition 2.2 is a source of incompleteness. Since $\oplus$ is clearly continuous, by Theorem 3.1, we know that the absolute core of the existential checking closure for $\oplus$ exists. The following results characterize this core.

Definition 3.3. Given $n \in \mathbb{N}$, define $\eta^n_{\exists_M} \stackrel{\text{def}}{=} \oplus^n \circ \rho^{\exists}_M \circ \ominus^n$. □

Note that $\eta^n_{\exists_M} \in \mathrm{uco}(\langle \mathbb{M}, \subseteq \rangle)$. Monotonicity follows by composition, while $\eta^n_{\exists_M}$ is extensive because $Y \subseteq \eta^n_{\exists_M}(Y) \Leftrightarrow \ominus^n Y \subseteq \rho^{\exists}_M(\ominus^n(Y))$. Idempotence is as follows: $\eta^n_{\exists_M}(\eta^n_{\exists_M}(Y)) = \oplus^n(\rho^{\exists}_M(\ominus^n(\oplus^n(\rho^{\exists}_M(\ominus^n(Y)))))) = \oplus^n(\rho^{\exists}_M(\rho^{\exists}_M(\ominus^n(Y)))) = \oplus^n(\rho^{\exists}_M(\ominus^n(Y))) = \eta^n_{\exists_M}(Y)$.

Theorem 3.4. *The absolute complete core $C^{\oplus}_{\exists_M}$ of $\rho^{\exists}_M$ for $\oplus$ exists and it is characterized as follows:*
(1) *The set of fix-points of $C^{\oplus}_{\exists_M}$ is $\{Y \in \mathbb{M} \mid \forall k \in \mathbb{N}.\ \ominus^k Y = \rho^{\exists}_M(\ominus^k Y)\}$.*
(2) $C^{\oplus}_{\exists_M} = \sqcup_{n \in \mathbb{N}} \eta^n_{\exists_M}$.

The following result provides a useful characterization of the absolute complete core $C^{\oplus}_{\exists_M}$ based on the structure of the underlying transition system. We use the following notation: given a transition system $\langle \mathbb{S}, \rightarrow \rangle$ and states $r, s \in \mathbb{S}$, for any $k > 0$, $r \overset{k}{\rightarrow} s$ iff $r = r_0 \rightarrow r_1 \rightarrow r_2 \rightarrow \ldots \rightarrow r_k = s$, where $\{r_1, ..., r_{k-1}\} \subseteq \mathbb{S}$.

Lemma 3.5. $\rho^{\exists}_M = \{(\bigcup_{s\in S} M_{\downarrow s}) \cup \neg M \mid S \subseteq \mathbb{S}\}$.

Theorem 3.6. *Let $M = \mathcal{M}_{\rightarrow}$, for some total transition system $\langle \mathbb{S}, \rightarrow\rangle$. Then, for any $S \subseteq \mathbb{S}$, $(\bigcup_{s\in S} M_{\downarrow s}) \cup \neg M \notin C^{\oplus}_{\exists_M}$ iff there exist $k > 0$, $q \in S$, $r \in \mathbb{S} \smallsetminus S$ and $t \in \mathbb{S}$ such that $q \xrightarrow{k} t$ and $r \xrightarrow{k} t$.*

Hence, by Lemma 3.5, Theorem 3.6 characterizes exactly all the fix-points of the closure $\rho^{\exists}_M$ which must be removed in order to get the absolute complete core $C^{\oplus}_{\exists_M}$. As a consequence, observe that it always holds that $\mathbb{T}, \neg M \in C^{\oplus}_{\exists_M}$: in fact, by Theorem 3.6, $\mathbb{T} = (\bigcup_{s\in\mathbb{S}} M_{\downarrow s}) \cup \neg M$ and $\neg M = (\bigcup_{s\in\varnothing} M_{\downarrow s}) \cup \neg M$.

By exploiting the constructive results above, we are also able to characterize the structure of transition systems whose models induce an existential checking closure which is complete for the predecessor. These are the transition systems $\langle \mathbb{S}, \rightarrow\rangle$ for which the transition relation $\rightarrow$ is injective: the relation $\rightarrow$ is *injective* whenever $\forall r, s, t \in \mathbb{S}.\, (r \rightarrow t \;\&\; s \rightarrow t) \Rightarrow r = s$.

Theorem 3.7. *Let $M = \mathcal{M}_{\rightarrow}$, for some total transition system $\langle \mathbb{S}, \rightarrow\rangle$. Then, $\rho^{\exists}_M$ is complete for $\oplus$ if and only if $\rightarrow$ is injective.*

It is worth noting that injectivity means that each computation step is reversible, i.e. the reverse transition system $\langle \mathbb{S}, \leftarrow\rangle$ obtained by reversing the transition relation is deterministic. This is the case of *reversible computations*, i.e. computations whose output uniquely defines the input [2]. Let us also observe that if $s \in \mathbb{S}$ is a stalling state, i.e. such that $s \rightarrow s$, then the injectivity of the transition relation requires that $t \not\rightarrow s$ for any $t \neq s$, i.e., s cannot be reached by any other state.

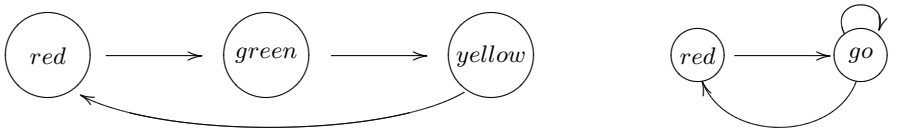

Fig. 1. A traffic light controller and its abstract version.

Example 3.8. Consider a traffic light controller as in Figure 1 with three states, i.e., $\mathbb{S} \stackrel{\text{def}}{=} \{red, green, yellow\}$ and $\rightarrow \stackrel{\text{def}}{=} \{red \rightarrow green, green \rightarrow yellow, yellow \rightarrow red\}$. Then, $\langle \mathbb{S}, \rightarrow\rangle$ is total and injective, and therefore, by Theorem 3.7, the corresponding existential checking closure is complete for the predecessor, i.e. $C^{\oplus}_{\exists_M} = \rho^{\exists}_M$.
Consider instead the abstraction induced by the following state partition: $h(red) = red$ and $h(green) = h(yellow) = go$ (cf. [6]). The resulting abstract transition system $\mathbb{S}^\sharp \stackrel{\text{def}}{=} \{red, go\}$ and $\rightarrow^\sharp \stackrel{\text{def}}{=} \{red \rightarrow^\sharp go, go \rightarrow^\sharp go, go \rightarrow^\sharp red\}$ is systematically derived from h as usual (cf. [6], see Figure 1). $\langle \mathbb{S}^\sharp, \rightarrow^\sharp\rangle$ is total but it is not injective. Let $M^\sharp$ be the model generated by $\langle \mathbb{S}^\sharp, \rightarrow^\sharp\rangle$. In order to compute the absolute complete core of $\rho^{\exists}_{M^\sharp}$ for $\oplus$ we exploit Theorem 3.6. Then, it is easy to

verify that for any $\varnothing \neq S \subsetneq \mathbb{S}^\sharp$, i.e. either $S = \{go\}$ or $S = \{red\}$, the condition of Theorem 3.6 is satisfied. For example, for $S = \{go\}$, we have that $red \rightarrow^\sharp go$ and $go \rightarrow^\sharp go$, with $go \in S$ and $red \notin S$. Thus, the absolute complete core of $\rho^\exists_M$ for $\oplus$ is $C^\oplus_{\exists_M} = \{\mathbb{T}, \neg M\}$.
Actually, it is not difficult to show that any abstraction with at least two states of $\langle \mathbb{S}, \rightarrow \rangle$ induces an abstract transition system for which the existential closure is not complete for the predecessor. Of course, this is not always the case for abstract transition systems. In the case of an infinite counter modelled by a concrete transition system $\langle \mathbb{S}, \rightarrow \rangle$ where $\mathbb{S} = \mathbb{N}$ and $x \rightarrow y$ iff $y = x + 1$, it turns out that both $\langle \mathbb{S}, \rightarrow \rangle$ and the abstract transition system $\langle \{even,\ odd\}, \rightarrow^p \rangle$ with $\rightarrow^p \stackrel{\text{def}}{=} \{odd \rightarrow even, even \rightarrow odd\}$, obtained by the straightforward abstraction partitioning states in even and odd numbers, are such that the existential checking closure is complete for the predecessor: in fact, both transition relations are injective and therefore Theorem 3.7 can be applied. □

3.2 Absolute complete core for time reversal

Let us now analyze the time reversal operator $^\frown$. Also in this case $^\frown$ is trivially continuous on $\langle \mathbb{M}, \subseteq \rangle$, and therefore Theorem 3.1 guarantees the existence of the absolute core of the existential checking closure for $^\frown$. Then, let us characterize the existential checking closure for the reversed model.

Lemma 3.9. $\rho^\exists_{^\frown M} = {}^\frown \circ \rho^\exists_M \circ {}^\frown$.

The following characterization proves that the absolute complete core is given by those fix-points of $\rho^\exists_M$ which also belong to the existential checking closure $\rho^\exists_{^\frown M}$ relative to the reversed model $^\frown M$.

Theorem 3.10. *The absolute complete core $C^{^\frown}_{\exists_M}$ of $\rho^\exists_M$ for $^\frown$ exists and it is characterized as follows:*
(1) *The set of fix-points of $C^{^\frown}_{\exists_M}$ is $\{Y \in \mathbb{M} \mid Y, {}^\frown Y \in \rho^\exists_M\}$.*
(2) $C^{^\frown}_{\exists_M} = \rho^\exists_M \sqcup \rho^\exists_{^\frown M}$.

This result allows us to give a characterization of the structure of transition systems inducing an existential checking closure complete for time reversal. These are the transition systems with a symmetric transition relation ($\rightarrow$ is symmetric whenever $\forall r, s \in \mathbb{S}.\, r \rightarrow s \ \Rightarrow\ s \rightarrow r$), i.e. which allow both a computation and its reverse.

Corollary 3.11. *Let $M = \mathcal{M}_\rightarrow$, for some total transition system $\langle \mathbb{S}, \rightarrow \rangle$. Then, $\rho^\exists_M$ is complete for $^\frown$ if and only if $\rightarrow$ is symmetric.*

Thus, in practice, the existential checking closure is rarely complete for time reversal, since symmetry is not a realistic condition for most concrete transition systems.

Example 3.12. Consider the abstract transition systems of Example 3.8, namely the abstract counter and the abstract traffic light controller. For both systems, since the transition relations are symmetric, by Corollary 3.11, the existential checking closure is complete for time reversal. Instead, this is not the case for the concrete three-state traffic light controller, since the transition relation is not symmetric. □

3.3 Absolute complete core for conjunction

Finally, let us consider conjunction, namely set intersection of models. Again, Theorem 3.1 ensures us that the absolute complete core does exist.

Theorem 3.13. *The absolute complete core* $C^{\cap}_{\exists_M}$ *of* $\rho^{\exists}_M$ *for* $\cap$ *exists and it is the top closure operator* $\lambda X.\mathbb{T}$.

Recall that the top closure operator corresponds to a straightforward and totally uninformative abstract domain consisting of a unique abstract value which is the abstraction of any concrete value. Hence, this is a "striking" result: in general, the top closure operator is always trivially complete (see [13]), and in our case this is the unique abstraction of $\rho^{\exists}_M$ which is complete for the conjunction. The intuition, that will be formally proved later on, is that any abstraction, but for the straightforward top closure, of the state-based model checking for a temporal calculus including an unrestricted connective of conjunction is incomplete for the trace-based semantics. This allows to state that state-based model checking is intrinsically incomplete for temporal calculi including conjunction, such as Kozen's μ-calculus, CTL, and CTL*.

3.4 Absolute complete core for all the connectives

Finally, let us characterize the absolute complete core of $\rho^{\exists}_M$ for all the connectives of the $\widehat{\mu}$-calculus, i.e., the set of all the model transformers of Definition 2.2. This core exists by Theorem 3.1 because all the operations are continuous. However, as noted by Ranzato [17], we must take care of the following technicality. As far as the universal state closure transformer $\forall$ is concerned, the following restriction is needed. We just consider the unary restrictions $\lambda X.\forall(N, X) : \mathbb{M} \to \mathbb{M}$, where $N \subseteq M \cup \curvearrowleft(M)$, of the universal state closure transformer, because the binary transformer $\forall : \mathbb{M} \times \mathbb{M} \to \mathbb{M}$ is neither monotone nor antitone in its first argument, and therefore it does not give rise to a concrete binary operation suitable to abstract interpretation. On the other hand, given any $N \in \mathbb{M}$, the unary restriction $\lambda X.\forall(N, X)$ is monotone. As observed in [11, Section 5] and [17, Section 3.1], this slight restriction still allows to recover the standard universal state quantification. In the sequel, we will use the following compact notation: $M^* \stackrel{\text{def}}{=} M \cup \curvearrowleft(M)$. As a simple consequence of Theorem 3.13, we get the following result.

Theorem 3.14. *The top closure operator* $\lambda X.\mathbb{T}$ *is the absolute complete core* $C_{\exists_M}$ *of* $\rho^{\exists}_M$ *for* $\{\boldsymbol{\sigma}_S\}_{S\in\wp(\mathbb{S})} \cup \{\boldsymbol{\pi}_t\}_{t\in\wp(\mathbb{S}^2)} \cup \{\oplus, \cap, \cup, \neg, \curvearrowleft\} \cup \{\lambda X.\forall(N, X)\}_{N\subseteq M^*}$.

The proof simply consists in observing that (1) the top closure $\lambda X.\mathbb{T}$ is trivially complete for any operation [13, Proposition 3.5 (i)], and (2) the absolute complete core of conjunction $\lambda X.\mathbb{T}$ is less than or equal to $C_{\exists_M}$, i.e., $C_{\exists_M} = \lambda X.\mathbb{T}$.

4 Completeness of temporal calculi

As observed above, from the abstract interpretation viewpoint, the universal state closure connective $\forall$ of the full $\overset{\frown}{\mu}$-calculus is somehow problematic, because, according to Cousot and Cousot's [11] Definition 2.1, the binary connective $\forall$ can be applied without any restriction, while its semantic counterpart, the universal state closure transformer $\forall : \mathbb{M} \times \mathbb{M} \to \mathbb{M}$, is neither monotone nor antitone in its first argument. On the other hand, given any $N \in \mathbb{M}$, the unary restriction $\lambda X.\forall(N, X) : \mathbb{M} \to \mathbb{M}$ is monotone, and this is enough in order to have the standard universal state quantification: $\forall\phi \stackrel{\text{def}}{=} \forall \boxplus (\boldsymbol{\pi}_\tau) : \phi$, where $[\![\boxplus (\boldsymbol{\pi}_\tau)]\!]\varnothing = \mathcal{M}_\tau$ (see [11, Section 5] for the details). Following Ranzato [17], this naturally leads to the following slight "monotone" restriction, which we call $\overset{\frown}{\mu}^-$-calculus, of the $\overset{\frown}{\mu}$-calculus.

Definition 4.1. Formulae ϕ of the $\overset{\frown}{\mu}^-$-calculus are inductively defined as follows:

$$\phi ::= \boldsymbol{\sigma}_S \mid \boldsymbol{\pi}_t \mid X \mid \oplus\, \phi \mid \phi^{\curvearrowleft} \mid \phi_1 \vee \phi_2 \mid \neg\phi \mid \boldsymbol{\mu} X.\phi \mid \boldsymbol{\nu} X.\phi \mid \forall\phi$$

where $S \in \wp(\mathbb{S})$, $t \in \wp(\mathbb{S} \times \mathbb{S})$, and $X \in \mathbb{X}$. $\mathfrak{L}_{\overset{\frown}{\mu}^-}$ denotes the set of $\overset{\frown}{\mu}^-$-calculus formulae. □

Of course, the trace-semantics for the $\overset{\frown}{\mu}^-$-calculus is completely identical to that of the $\overset{\frown}{\mu}$-calculus given in Definition 2.2, but for the universal connective: $[\![\forall\phi]\!]\xi \stackrel{\text{def}}{=} \forall(\mathcal{M}_\tau, [\![\phi]\!]\xi)$.

The main result is stated for this $\overset{\frown}{\mu}^-$-calculus. The scenario is as follows. Any abstraction of the concrete domain $\mathbb{M}$ of temporal models, ordered by the superset or subset relation, induces an abstract semantics for the $\overset{\frown}{\mu}$-calculus, and therefore for the $\overset{\frown}{\mu}^-$-calculus. As seen in Section 2.3, the checking abstractions are an example: $[\![\cdot]\!]^\forall_\to$ and $[\![\cdot]\!]^\exists_\to$ are the abstract semantics induced, respectively, by $\rho^\forall_M$ and $\rho^\exists_M$. More in general, for the existential case of our interest, given a model to check $M \in \mathbb{M}$ — which is supposed to be generated by a transition system $\langle \mathbb{S}, \to \rangle$ — any closure operator, i.e. abstract domain, $\rho \in \mathrm{uco}(\mathbb{M}_\subseteq)$, induces the set of abstract environments $\mathbb{E}^\rho \stackrel{\text{def}}{=} \mathbb{X} \to \rho$, and the corresponding abstract semantics $[\![\cdot]\!]^\rho : \mathfrak{L}_{\overset{\frown}{\mu}^-} \to \mathbb{E}^\rho \to \rho$. Given an environment $\xi \in \mathbb{E}$, $\dot\rho(\xi) \stackrel{\text{def}}{=} \lambda X.\rho(\xi(X)) \in \mathbb{E}^\rho$ is the corresponding abstract environment induced by ρ. Soundness, i.e., $\forall\phi \in \mathfrak{L}_{\overset{\frown}{\mu}^-}.\forall\xi \in \mathbb{E}.\ \rho([\![\phi]\!]\xi) \supseteq [\![\phi]\!]^\rho\dot\rho(\xi)$, holds by construction (cf. [11, Theorem (40)]), while completeness for ρ means that equality always holds.

Theorem 4.2. *Let $\delta_\wedge$ be any fragment of the $\overset{\frown}{\mu}^-$-calculus which allows arbitrary conjunctions of formulae. The top closure operator $\lambda X.\mathbb{T} \in \mathrm{uco}(\mathbb{M}_\subseteq)$ is the*

greatest (w.r.t. subset image containment) closure operator on $\mathbb{M}_{\subseteq}$ (1) *complete for* $\delta_\wedge$ *and* (2) *contained in the existential checking closure* $\rho^{\exists}_M$.

This result exactly formalizes the intuition described above: for any temporal language allowing unrestricted conjunctions of formulae, the top closure is the unique abstraction of the existential state-based checking closure which induces a corresponding model checking which is complete for the trace-based semantics.

To conclude, let us mention that, dually, for the universal case, one gets the greatest closure operator on $\langle \mathbb{M}, \supseteq \rangle$, i.e. $\lambda X.\varnothing$.

5 Conclusion

This paper completed the study started by Ranzato [17] on the completeness of state-based model checking w.r.t. trace-based model checking. Both results show that abstract interpretation provides a powerful body of techniques to study the relation between computational models at different levels of abstraction. By using a slogan, this study showed that "*the state checking is intrinsically incomplete w.r.t. trace checking*", since no refinement or abstraction of the classical state-based model checking can lead to a semantics inducing a model checking which is complete for the trace semantics of the temporal language. This is not only a negative result concerning completeness of states vs. traces. This result opens new interesting research directions. In particular, in view of Theorem 3.7 and Corollary 3.11, it is possible to isolate fragments of μ-calculi which are complete for particular classes of transition systems. An important issue in this context is how completeness of state-based abstractions interacts with the presence of spurious counterexamples, when the transition systems are derived by abstract interpretation [1, 6, 14]. Completeness of states w.r.t. traces can also be studied from a different viewpoint. The idea is that of modifying the underlying temporal language in order to get completeness of states w.r.t. traces, where the modifications of the temporal language should be *minimal*. This means that temporal languages should be somehow ordered w.r.t. their expressive power, and this order should allow to define syntactically the minimal simplifications of the language. Further applications of our results could be obtained for temporal databases. Temporal logic has been proposed as the core language for specifying integrity constraints and triggers in temporal databases [3, 18]. Since the time-point-indexed sequences (i.e. traces) of database states cannot be efficiently handled, several more efficient models have been obtained by abstraction. The problem of characterizing completeness in database abstractions has been attacked by several authors (e.g. see the notion of weak completeness in [8]), in particular for comparing different data-models. However, to the best of our knowledge, none of them have been considered as an abstract interpretation problem. In the case of temporal databases, temporal abstractions, such as the interval abstraction which induces the notion of period or temporal element [19], are particularly relevant. In view of recent results encoding temporal query languages as fragments of temporal logic [4], we believe that our results can help in

comparing abstractions of temporal databases with the expressivity of temporal query languages, in particular for aspects concerning completeness with respect to a concrete temporal time-point-indexed database.

Acknowledgements. This work has been partially supported by the Italian MIUR Cofin2000 project "Abstract interpretation, type systems and control-flow analysis".

References

1. T. Ball, A. Podelski, and S.K. Rajamani. Relative Completeness of Abstraction Refinement for Software Model Checking. In *Proc. of TACAS'02*, LNCS 2280, pp. 158-172, Springer, 2002.
2. C.H. Bennett. Logical reversibility of computation. *IBM J. Research Dev.*, 21:905-940, 1981.
3. J. Chomicki. Temporal query languages: A survey. In *Proc. 1st Int. Conf. on Temporal Logic*, LNAI 827, pp. 506-534, Springer, 1994.
4. J. Chomicki, D. Toman, and M.H. Böhlen. Quering ATSQL databases with temporal logic. *ACM Trans. Database Syst.*, 26(2):145-1178, 2001.
5. E.M. Clarke, O. Grumberg, and D. E. Long. Model checking and abstraction. *ACM Trans. Program. Lang. Syst.*, 19(5):1512-1542, 1994.
6. 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.
7. E.M. Clarke, O. Grumberg, and D. Peled. *Model checking.* The MIT Press, 1999.
8. J. Clifford, A. Croker, and A. Tuzhilin. On completeness of historical relational query languages. *ACM Trans. Database Syst.*, 19(1):64-116, 1994.
9. 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. ACM Press, 1977.
10. P. Cousot and R. Cousot. Systematic design of program analysis frameworks. In *Proc. ACM POPL'79*, pp. 269–282. ACM Press, 1979.
11. P. Cousot and R. Cousot. Temporal abstract interpretation. In *Proc. ACM POPL'00*, pp. 12–25. ACM Press, 2000.
12. D. Dams, R. Gerth, and O. Grumberg. Abstract interpretation of reactive systems. *ACM Trans. Program. Lang. Syst.*, 19(2):253–291, 1997.
13. R. Giacobazzi, F. Ranzato, and F. Scozzari. Making abstract interpretations complete. *J. ACM*, 47(2):361–416, 2000.
14. R. Giacobazzi and E. Quintarelli. Incompleteness, counterexamples and refinements in abstract model checking. In *Proc. SAS'01*, LNCS 2126, pp. 356-373, Springer, 2001.
15. C. Loiseaux, S. Graf, J. Sifakis, A. Bouajjani, and S. Bensalem. Property preserving abstractions for the verification of concurrent systems. *Formal Methods Syst. Des.*, 6:1–36, 1995.
16. M. Müller-Olm, D. Schmidt, and B. Steffen. Model checking: A tutorial introduction. In *Proc. SAS'99*, LNCS 1694, pp. 330–354. Springer, 1999.
17. F. Ranzato. On the completeness of model checking. In *Proc. ESOP'01*, LNCS 2028, pp. 137-154, Springer, 2001.
18. A.P. Sistla and O. Wolfson. Temporal triggers in active databases. *IEEE Trans. Knowl. Data. Eng.*, 7(3):471-486, 1995.
19. A.U. Tansel. Adding time dimension to relational model and extending relational algebra. *Information Systems*, 11(4):343-355, 1986.