

On the Completeness of Model Checking

Francesco Ranzato

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 introduced and studied a novel general temporal specification language, called $\widehat{\mu}$ -calculus, in particular featuring a natural and rich time-symmetric trace-based semantics. The classical state-based model checking of the $\widehat{\mu}$ -calculus is an abstract interpretation of its trace-based semantics, which, surprisingly, turns out to be incomplete, even for finite systems. Cousot and Cousot identified the temporal connectives causing such incompleteness. In this paper, we first characterize the least, i.e. least informative, refinements of the state-based model checking abstraction which are complete relatively to any incomplete temporal connective. On the basis of this analysis, we show that the least refinement of the state-based model checking semantics of (a slight and natural monotone restriction of) the $\widehat{\mu}$ -calculus which is complete w.r.t. the trace-based semantics does exist, and it is essentially the trace-based semantics itself. This result can be read as stating that any model checking algorithm for the $\widehat{\mu}$ -calculus abstracting away from sets of traces will be necessarily incomplete.

1 Introduction

The classical semantics of standard temporal specification languages for model checking, like CTL, μ -calculus and variations thereof, are state-based and time-asymmetric [3, 6, 11, 12]. State-based means that, given a transition system modelling some reactive system, the semantics of a temporal formula ϕ is given by the set of states of the transition system satisfying ϕ , possibly w.r.t. some environment whenever ϕ contains free variables. Time-asymmetry refers to the asymmetric nature of the classical notion of trace in transition systems, since traces are commonly indexed on natural numbers and therefore have a finite past and an infinite future. Recently, Cousot and Cousot [6] introduced a novel general temporal specification language, called $\widehat{\mu}$ -calculus, inspired from Kozen's [9] μ -calculus and featuring a time-symmetric trace-based semantics. In the $\widehat{\mu}$ -calculus semantics, traces are indexed over integer numbers, i.e. both past and future are infinite, and a time reversal operator allows a uniform symmetric treatment of past and future. Traces record the present time, and hence the present state as well, by an integer number, and temporal formulae are therefore interpreted as sets of traces. The generality of the $\widehat{\mu}$ -calculus stems from mixing linear and branching time modalities, and this allows to recover most standard

specification languages like CTL, CTL* and Kozen’s μ -calculus as suitable fragments.

The most relevant feature in Cousot and Cousot’s [6] work is in the application of the abstract interpretation methodology [4, 5] to the μ -calculus. In particular, it is shown how to derive standard state-based model checking by abstract interpretation from the trace-based semantics of the μ -calculus. This is performed exploiting a so-called universal checking abstraction map α_M^\forall : given a model to check M (i.e., the set of traces generated by some transition system), α_M^\forall abstracts a trace-interpreted μ -calculus temporal formula ϕ to the set of present states s of M such that any (here we are considering the universal case: dually, in the existential checking abstraction “any” becomes “some”) execution of M departing from the state s satisfies ϕ . Thus, the abstract domain consists of sets of states, since α_M^\forall abstracts sets of traces to sets of states. In particular, $\alpha_M^\forall(\phi)$ encodes a classical state-based interpretation like $\{s \in States \mid M, s \models \phi\}$, and therefore the state-based local model-checking problem of determining if a given state s in M satisfies ϕ amounts to checking whether $s \in \alpha_M^\forall(\phi)$. This abstraction map from sets of traces to sets of states compositionally induces a state-based abstract semantics $\llbracket \cdot \rrbracket^{state}$ for the μ -calculus, which, by construction through the abstract interpretation technique, is sound w.r.t. the trace-based semantics: for any formula ϕ , $\alpha_M^\forall(\llbracket \phi \rrbracket^{trace}) \supseteq \llbracket \phi \rrbracket^{state}$.

Completeness for the abstract state-based semantics in general does not hold, i.e. the containment above may be strict, even for finite systems (see [6, Counterexample (60)]). This means that trace-based and state-based model checking for the μ -calculus, in general, are not equivalent: there exist some formula ϕ and state s such that $M, s \models_{trace} \phi$, while $M, s \not\models_{state} \phi$. The consequence of such incompleteness is that in order to deal with general temporal specifications of the μ -calculus, model checking algorithms should handle sets of traces instead of sets of states, and this is evidently infeasible. Moreover, Cousot and Cousot single out the sources of such incompleteness, that is, the temporal connectives of the μ -calculus which are incomplete for the universal checking abstraction: these are the predecessor, shifting the present time one step in the past, the disjunction, and the reversal, exchanging past and future w.r.t. the present time.

Giacobazzi et al. [8] observed that completeness for an abstract interpretation, i.e. abstract domains plus abstract operations, only depends on the underlying abstract domains. Hence, this opens up the key question of making an abstract interpretation complete by minimally extending the underlying abstract domain. Following the terminology in [8], we call complete shell of an abstract domain A the most abstract, i.e. containing the least amount of information, domain, when this exists, which extends A and is complete for some operation or (fixpoint) semantics. The relevance of such concept should be clear: the complete shell of an abstract domain A characterizes exactly the least amount of information which must be added to A in order to get completeness, when this can be done. It is shown in [8] that complete shells relative to sets of concrete operations, the so-called absolute complete shells, exist under weak and reasonable hypotheses, and some constructive methods to characterize them are given.

On the other hand, for complete shells relative to fixpoint operators, it is argued that no general result of existence can be given, even under very restrictive hypotheses.

This paper analyzes the incompleteness of state-based model checking within the Cousot and Cousot [6] framework described above from the perspective of minimally making an abstract interpretation complete. We first characterize the absolute complete shells of the universal checking abstraction α_M^\forall — namely, the abstract domain of sets of states approximating the domain of sets of traces — relatively to each incomplete temporal connective, namely predecessor, disjunction and reversal. The results are quite illuminating. Completeness w.r.t. the predecessor leads to an absolute complete shell which refines sets of states to a domain of sequences indexed over natural numbers (intended to represent the past time) of sets of states. The least refinement of α_M^\forall which is complete for the reversal operator is simply a domain consisting of pairs of sets of states, where the meaning is as follows: if $\sim M$ denotes the reversal of the model M , a trace-interpreted formula ϕ is abstracted to the pair $\langle \alpha_M^\forall(\phi), \alpha_{\sim M}^\forall(\phi) \rangle$. Hence, as expected, completeness for the reversal requires an additional component taking into account the universal checking abstraction for the reversed model $\sim M$. Finally, disjunction is, somehow, the more demanding connective: the abstract domain of the corresponding absolute complete shell consists of sets of traces belonging to the model to check M , and therefore this amounts to an abstraction which essentially is the identity. Moreover, this abstraction is complete for the predecessor too, and hence more concrete than its absolute complete shell mentioned above. Globally, we also characterize the absolute complete shell of α_M^\forall relatively to all¹ the temporal connectives involved by the $\hat{\mu}$ -calculus. Hence, this abstract domain must be complete both for disjunction and reversal. Actually, we show that this global absolute complete shell consists of sets of traces belonging to M or to its reversal. Thus, this abstract domain is even more close to the concrete domain of sets of generic traces.

Finally and more importantly, we faced the problem of characterizing the complete shell of the universal checking abstraction relatively to the whole trace-based concrete semantics of the $\hat{\mu}$ -calculus. In other terms, we are seeking to characterize the most abstract domain A^s extending the universal checking abstract domain of sets of states and inducing a complete abstract semantics, i.e., such that for any formula ϕ , $\alpha_{A^s}(\llbracket \phi \rrbracket^{trace}) = \llbracket \phi \rrbracket^{A^s}$. In this case, since the $\hat{\mu}$ -calculus involves (least and greatest) fixpoints, as recalled above, it should be remarked that no general result in [8] ensures the existence of such complete abstract domain. Nevertheless, it turns out that this complete shell does exist, and it coincides with the absolute complete shell relative to all the temporal connectives, namely the identity on sets of traces in M or its reversal. This complete shell therefore induces an abstract semantics which essentially is the trace-based semantics itself. Thus, the intuitive interpretation of this important

¹ There is a technical detail here: abstract interpretation requires concrete operations to be monotone or antitone. Thus, in the paper we consider a standard monotone restriction of the new general universal state quantification introduced in [6].

result is as follows: any semantic refinement of the state-based model checking which aims at being trace-complete for the $\hat{\mu}$ -calculus ineluctably leads to the trace-based semantics itself. Otherwise stated, any model checking algorithm for the $\hat{\mu}$ -calculus abstracting away from sets of traces will be necessarily incomplete.

2 Abstract Interpretation and Completeness

Notation. Let us first introduce some basic notation that will be used throughout the paper. Conditionals are denoted by $(b \in Bool ? x \dot{\iota} y)$, evaluating to x when b is true and to y when b is false. Let X and Y be sets. $X \setminus Y$ denotes set-difference, $X \subsetneq Y$ denotes strict inclusion, and $X \rightarrow Y$ denotes the set of total functions from X to Y . If X plays the role of some “universe” and $Y \subseteq X$ then $\neg Y \stackrel{\text{def}}{=} X \setminus Y$. Given a sequence $\sigma \in \mathbb{Z} \rightarrow X$, for any $i \in \mathbb{Z}$, $\sigma_i \in X$ stands for $\sigma(i)$. Given $f : X \rightarrow X$, the i -th power of f , where $i \in \mathbb{N}$, is inductively defined as follows: $f^0 \stackrel{\text{def}}{=} \lambda x.x$; $f^{i+1} \stackrel{\text{def}}{=} \lambda x.f(f^i(x))$. $lfp(f)$ and $gfp(f)$ denote, respectively, the least and greatest fixpoint, when they exist, of an operator f on a poset. Sometimes, a poset $\langle P, \leq \rangle$ will be denoted more compactly by P_{\leq} . Given a poset P_{\leq} , the set of functions $X \rightarrow P$ becomes a poset for the pointwise ordering \leq , where $f \leq g$ iff $\forall x \in X. f(x) \leq g(x)$.

Closure Operators. The structure $\langle uco(C), \sqsubseteq, \sqcup, \sqcap, \lambda x.\top, \lambda x.x \rangle$ denotes the complete lattice of all (upper) closure operators (shortly closures) on a complete lattice $\langle C, \leq, \vee, \wedge, \top, \perp \rangle$, where $\rho \sqsubseteq \eta$ iff $\forall x \in C. \rho(x) \leq \eta(x)$. Throughout the paper, for any $\rho \in uco(C)$, 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 $\rho \in uco(C)$ is uniquely determined by the set of its fixpoints, which coincides with its image, i.e. $\rho = \{x \in C \mid \rho(x) = x\}$, (ii) $\rho \sqsubseteq \eta$ iff $\eta \subseteq \rho$, 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 $\top = \wedge \emptyset \in \mathcal{M}(X)$; sometimes, we will write $\mathcal{M}_C(X)$ to emphasize the underlying complete lattice). Hence, note that, given any $X \subseteq C$, $\mathcal{M}(X)$ is the (set of fixpoints of the) greatest (w.r.t. \sqsubseteq) closure whose set of fixpoints contains X .

Abstract Domains. It is well known that within the standard Cousot and Cousot framework, abstract domains can be equivalently specified either by Galois connections/insertions (GCs/GIs) or by closure operators [5]. 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 $\alpha : C \rightarrow A$ and $\gamma : A \rightarrow C$, 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 (and this closure could be also given by means of its set of fixpoints). 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 $uco(C)$ with the so-called

complete lattice \mathcal{L}_C of abstract interpretations of C (cf. [4, Section 7] and [5, Section 8]). The ordering on $uco(C)$ 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 $uco(C)$. 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 $f : C \rightarrow C$ be a monotone or antitone concrete semantic function² occurring in some complex semantic specification, and let $f^\# : A \rightarrow A$ be a corresponding abstract function, where $A \in \mathcal{L}_C$. The concept of soundness is standard and well known: $\langle A, f^\# \rangle$ is a sound abstract interpretation — or $f^\#$ is a correct approximation of f relatively to A — when $\alpha_{C,A} \circ f \dot{\leq}_A f^\# \circ \alpha_{C,A}$. On the other hand, $\langle A, f^\# \rangle$ is complete when equality holds, i.e. $\alpha_{C,A} \circ f = f^\# \circ \alpha_{C,A}$. Thus, in abstract interpretation, completeness means that the abstract semantics equals the abstraction of the concrete semantics, or, otherwise stated, that abstract computations accumulate no loss of information.

Completeness is a Domain Property. Any abstract domain $A \in \mathcal{L}_C$ induces the so-called canonical best correct approximation $f^A : A \rightarrow A$ of $f : C \rightarrow C$, defined by $f^A \stackrel{\text{def}}{=} \alpha_{C,A} \circ f \circ \gamma_{A,C}$. This terminology is justified by the fact that any $f^\# : A \rightarrow A$ is a correct approximation of f iff $f^A \sqsubseteq f^\#$. Consequently, any abstract domain always induces an (automatically) sound abstract interpretation. Of course, this is not in general true for completeness: not every abstract domain induces a complete abstract interpretation. However, whenever a complete abstract operation exists then the best correct approximation is complete as well. This therefore means that completeness is a property which depends on the underlying abstract domain only. As a consequence, whenever abstract domains are specified by closure operators, an abstract domain $\rho \in \mathcal{L}_C$ is defined to be complete for f if $\rho \circ f \circ \rho = \rho \circ f$. 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 useful notation: $\Gamma(C, f) \stackrel{\text{def}}{=} \{\rho \in \mathcal{L}_C \mid \rho \text{ is complete for } f\}$. Hence, for a set F , $\Gamma(C, F) = \cap_{f \in F} \Gamma(C, f)$.

Making Abstract Interpretations Complete. The fact that completeness is an abstract domain property opens the key question of making an abstract interpretation complete by minimally extending (or, dually, restricting: we will not touch this issue here, see [8]) the underlying abstract domain. Following [8], given a concrete interpretation $\langle C, f \rangle$ and an abstract domain $A \in \mathcal{L}_C$, the absolute complete shell³ of A for f , when it exists, is the most abstract domain $A^s \in \mathcal{L}_C$ which extends, viz. is more precise than, A and is complete for f . In other words,

² For simplicity, we consider unary functions with the same domain and co-domain, since the extension to the general case is straightforward.

³ [8] also introduces the concept of relative complete shell, and this explains the use of the adjective absolute.

the absolute complete shell of A characterizes the least amount of information to be added to A in order to get completeness, when this can be done. Let us succinctly recall the solution to this completeness problem recently given in [8].

Let us fix the following standard notation: if $X \subseteq C$ then $\max(X) \stackrel{\text{def}}{=} \{x \in X \mid \forall y \in X. x \leq y \Rightarrow x = y\}$. Given a set of monotone semantic functions $F \subseteq C \rightarrow C$, the abstract domain transformer $R_F : \mathcal{L}_C \rightarrow \mathcal{L}_C$ is defined as follows:

$$R_F(\eta) \stackrel{\text{def}}{=} \mathcal{M}(\cup_{f \in F, y \in \eta} \max(\{x \in C \mid f(x) \leq y\})).$$

Theorem 2.1 ([8, Theorem 5.10, p. 388]). *Let $F \subseteq C \rightarrow C$ and $\rho \in \mathcal{L}_C$. If F is a set of continuous (i.e., preserving lub's of directed subsets) functions then the absolute complete shell of ρ for F exists, and it is given by $\text{gfp}(\lambda \eta \in \text{uco}(C). \rho \sqcap R_F(\eta))$.*

This therefore is a constructive result of existence for absolute complete shells. It turns out that $\lambda \eta. \rho \sqcap R_F(\eta) : \text{uco}(C) \rightarrow \text{uco}(C)$ is itself continuous [8, Lemma 5.11], and therefore its greatest fixpoint can be constructively obtained as ω -limit of the Kleene's iteration sequence.

3 Temporal Abstract Interpretation

In this section, we recall the key notions and definitions of Cousot and Cousot's [6] abstract interpretation-based approach to model checking.

Basic Notions. \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, $\mathbb{P} \stackrel{\text{def}}{=} \mathbb{Z} \rightarrow \mathbb{S}$ is the set of paths. An execution with an initial state s can then be encoded by repeating forever in the past the state s . A trace must keep track of the present time, and hence $\mathbb{T} \stackrel{\text{def}}{=} \mathbb{Z} \times \mathbb{P}$ is the set of traces. Finally, 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 logic formula ϕ will be a temporal model, that, intuitively, will be the set of all and only the traces making ϕ true.

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

3.1 Syntax and Semantics of the $\widehat{\mu}$ -Calculus

The reversible $\widehat{\mu}$ -calculus has been introduced by Cousot and Cousot [6] inspired by Kozen's [9] propositional μ -calculus. Actually, the $\widehat{\mu}$ -calculus is a generalization of the μ -calculus, with new reversal and abstraction modalities and with a trace-based semantics. Throughout the paper, \mathbb{X} will denote an infinite set of logical variables.

Definition 3.1 ([6, Definition 13]). Formulae ϕ of the reversible $\widehat{\mu}$ -calculus are inductively defined as follows:

$$\phi ::= \sigma_S \mid \pi_t \mid X \mid \oplus \phi \mid \phi^\frown \mid \phi_1 \vee \phi_2 \mid \neg\phi \mid \mu X.\phi \mid \nu X.\phi \mid \forall\phi_1 : \phi_2$$

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

In order to give the trace-interpreted semantics of the $\widehat{\mu}$ -calculus, we preliminarily recall the necessary temporal model transformers.

Definition 3.2 ([6, Section 3]).

- For any $S \in \wp(\mathbb{S})$, $\sigma_{\downarrow S} \stackrel{\text{def}}{=} \{\langle i, \sigma \rangle \in \mathbb{T} \mid \sigma_i \in S\} \in \mathbb{M}$ is the S -state model, i.e., the set of traces whose current state is in S .
- For any $t \in \wp(\mathbb{S} \times \mathbb{S})$, $\pi_{\downarrow t} \stackrel{\text{def}}{=} \{\langle i, \sigma \rangle \in \mathbb{T} \mid (\sigma_i, \sigma_{i+1}) \in t\} \in \mathbb{M}$ 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:
 $\oplus(X) \stackrel{\text{def}}{=} \{\langle i-1, \sigma \rangle \in \mathbb{T} \mid \langle i, \sigma \rangle \in X\} = \{\langle i, \sigma \rangle \in \mathbb{T} \mid \langle i+1, \sigma \rangle \in X\}$.
- $\frown : \mathbb{M} \rightarrow \mathbb{M}$ is the reversal transformer:
 $\frown(X) \stackrel{\text{def}}{=} \{\langle -i, \lambda k.\sigma_{-k} \rangle \in \mathbb{T} \mid \langle i, \sigma \rangle \in X\}$.
- $\neg : \mathbb{M} \rightarrow \mathbb{M}$ is the complement transformer:
 $\neg X \stackrel{\text{def}}{=} \mathbb{M} \setminus X$.
- Given $s \in \mathbb{S}$, $(\cdot)_{\downarrow s} : \mathbb{M} \rightarrow \mathbb{M}$ is the state projection operator:
 $X_{\downarrow s} \stackrel{\text{def}}{=} \{\langle i, \sigma \rangle \in X \mid \sigma_i = s\}$.
- $\forall : \mathbb{M} \times \mathbb{M} \rightarrow \mathbb{M}$ is the universal state closure transformer:
 $\forall(X, Y) \stackrel{\text{def}}{=} \{\langle i, \sigma \rangle \in X \mid X_{\downarrow \sigma_i} \subseteq Y\}$. \square

It is worth to recall that reversal and negation allow to define a number of interesting dual transformers. For example, the successor transformer is defined by $\ominus \stackrel{\text{def}}{=} \frown \circ \oplus \circ \frown$, and the existential transformer by $\exists \stackrel{\text{def}}{=} \lambda(X, Y). \neg\forall(X, \neg Y)$.

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

Definition 3.3 ([6, 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 $\widehat{\mu}$ -calculus semantics $\llbracket \cdot \rrbracket : \mathcal{L}_{\widehat{\mu}} \rightarrow \mathbb{E} \rightarrow \mathbb{M}$ is inductively and partially (because least or greatest fixpoints could not exist) defined as follows:

$$\begin{array}{ll} \llbracket \sigma_S \rrbracket \xi \stackrel{\text{def}}{=} \sigma_{\downarrow S} & \llbracket \phi_1 \vee \phi_2 \rrbracket \xi \stackrel{\text{def}}{=} \llbracket \phi_1 \rrbracket \xi \cup \llbracket \phi_2 \rrbracket \xi \\ \llbracket \pi_t \rrbracket \xi \stackrel{\text{def}}{=} \pi_{\downarrow t} & \llbracket \neg\phi \rrbracket \xi \stackrel{\text{def}}{=} \neg(\llbracket \phi \rrbracket \xi) \\ \llbracket X \rrbracket \xi \stackrel{\text{def}}{=} \xi(X) & \llbracket \mu X.\phi \rrbracket \xi \stackrel{\text{def}}{=} \text{lfp}(\lambda N \in \mathbb{M}. \llbracket \phi \rrbracket \xi[X/N]) \\ \llbracket \oplus \phi \rrbracket \xi \stackrel{\text{def}}{=} \oplus(\llbracket \phi \rrbracket \xi) & \llbracket \nu X.\phi \rrbracket \xi \stackrel{\text{def}}{=} \text{gfp}(\lambda N \in \mathbb{M}. \llbracket \phi \rrbracket \xi[X/N]) \\ \llbracket \phi^\frown \rrbracket \xi \stackrel{\text{def}}{=} \frown(\llbracket \phi \rrbracket \xi) & \llbracket \forall\phi_1 : \phi_2 \rrbracket \xi \stackrel{\text{def}}{=} \forall(\llbracket \phi_1 \rrbracket \xi, \llbracket \phi_2 \rrbracket \xi) \end{array} \quad \square$$

Forward/Backward/State-Closed Formulae. Intuitively, a $\widehat{\mu}$ -calculus formula ϕ is defined to be forward/backward/state-closed when the future/past/present only matters, that is, for all $\xi \in \mathbb{E}$, the past/future/past&future of any trace in the semantics $\llbracket \phi \rrbracket \xi$ can be arbitrarily perturbed without affecting the semantics. This is formalized as follows.

Definition 3.4 ([6, Section 7.2]). If $\sigma, \beta \in \mathbb{P}$ and $i \in \mathbb{Z}$, then

- $\beta[_i\sigma \stackrel{\text{def}}{=} \lambda k \in \mathbb{Z}.(k < i ? \beta_k \dot{\iota} \sigma_k)$ is the prolongation of β at time i ;
- $\beta_i] \sigma \stackrel{\text{def}}{=} \lambda k \in \mathbb{Z}.(k \leq i ? \beta_k \dot{\iota} \sigma_k)$ is the prolongation of β after time i .

The following operators of type $\mathbb{M} \rightarrow \mathbb{M}$ are defined:

$Fd \stackrel{\text{def}}{=} \lambda X. \{ \langle i, \beta[_i\sigma \rangle \in \mathbb{T} \mid \langle i, \sigma \rangle \in X, \beta \in \mathbb{P} \}$ is the forward closure;

$Bd \stackrel{\text{def}}{=} \lambda X. \{ \langle i, \beta_i]\sigma \rangle \in \mathbb{T} \mid \langle i, \sigma \rangle \in X, \beta \in \mathbb{P} \}$ is the backward closure;

$St \stackrel{\text{def}}{=} \lambda X. Fd(X) \cup Bd(X) = \lambda X. \{ \langle i, \beta[_i\sigma_i]\beta' \rangle \in \mathbb{T} \mid \langle i, \sigma \rangle \in X, \beta, \beta' \in \mathbb{P} \}$ is the state closure. \square

It is easy to see that these actually are closure operators, i.e., $Fd, Bd, St \in uco(\mathbb{M}_{\subseteq})$. Thus, $\phi \in \mathcal{L}_{\widehat{\mu}}$ is called a forward/backward/state formula whenever, for all $\xi \in \mathbb{E}$, $\llbracket \phi \rrbracket \xi = Fd/Bd/St(\llbracket \phi \rrbracket \xi)$.

The state-closed formulae actually are the classical state-formulae of CTL-like logics [3]. Moreover, path-formulae of CTL-like logics are, in this terminology, forward-closed. Actually, Cousot and Cousot [6] isolate the following fragment of the $\widehat{\mu}$ -calculus called CTL_{+}^* :

$$\phi ::= \sigma_S \mid \pi_t \mid \oplus \phi \mid \phi_1 \vee \phi_2 \mid \neg \phi \mid \phi_1 \mathbf{U} \phi_2 \mid \forall \phi$$

where $\phi_1 \mathbf{U} \phi_2 \stackrel{\text{def}}{=} \mu X. \phi_2 \vee (\phi_1 \wedge \oplus X)$ and $\forall \phi \stackrel{\text{def}}{=} \forall \boxplus (\pi_\tau) : \phi$, with $\llbracket \boxplus (\pi_\tau) \rrbracket \emptyset = \mathcal{M}_\tau$ (see [6, Section 5] for the details). It is then showed [6, Lemma (18)] that any CTL_{+}^* formula is forward-closed, while formulae generated by

$$\psi ::= \sigma_S \mid \psi_1 \vee \psi_2 \mid \neg \psi \mid \forall \psi$$

actually are state-closed.

3.2 Trace-Based Model Checking

It is straightforward to formulate the model checking problem within the trace-based Cousot and Cousot's framework [6]. A closed temporal specification $\phi \in \mathcal{L}_{\widehat{\mu}}$ is identified by its semantics, namely by the temporal model $\llbracket \phi \rrbracket \emptyset \in \mathbb{M}$. Thus, the universal model checking of a system \mathcal{M}_τ against a specification ϕ amounts to check whether $\mathcal{M}_\tau \subseteq \llbracket \phi \rrbracket \emptyset$. It is also useful to distinguish a dual existential model checking, where the goal is that of checking whether $\llbracket \phi \rrbracket \emptyset \cap \mathcal{M}_\tau \neq \emptyset$.

3.3 State-Based Model Checking Abstractions

The classical state-based model checking can then be understood 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 $\alpha_M^\forall : \mathbb{M} \rightarrow \wp(\mathbb{S})$ 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 $\alpha_M^\forall(\phi)$ 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 [6, Definition 45]:

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

Following the terminology by Müller-Olm et al. [12]: (i) the state-based global model checking problem of determining the set of present states in M that satisfy ϕ simply amounts to determining $\alpha_M^\forall(\phi)$, and (ii) the state-based local model checking problem of checking if a given state s in M satisfies ϕ amounts to checking whether $s \in \alpha_M^\forall(\phi)$.

In this context, the superset relation between states provides the right notion of approximation: if $S \subseteq \alpha_M^\forall(\phi)$ then each state in S satisfies ϕ , and therefore if $S \subseteq T$ then T can be thought of as more precise than S . Actually, α_M^\forall gives rise to an adjunction between $\langle \wp(\mathbb{S}), \supseteq \rangle$ and $\langle \mathbb{M}, \supseteq \rangle$, where the concretization map $\gamma_M^\forall : \wp(\mathbb{S}) \rightarrow \mathbb{M}$ is defined by: $\gamma_M^\forall(S) \stackrel{\text{def}}{=} \{\langle i, \sigma \rangle \in \mathbb{T} \mid \langle i, \sigma \rangle \in M, \sigma_i \in S\}$. When dealing with a model \mathcal{M}_τ generated by a transition system, by the totality hypothesis on the transition relation τ , we have that for any $s \in \mathbb{S}$, $\mathcal{M}_{\tau \downarrow s} \neq \emptyset$. This implies that $\gamma_{\mathcal{M}_\tau}^\forall$ is 1-1, and therefore $(\alpha_{\mathcal{M}_\tau}^\forall, \langle \mathbb{M}, \supseteq \rangle, \langle \wp(\mathbb{S}), \supseteq \rangle, \gamma_{\mathcal{M}_\tau}^\forall)$ is a GI [6, (48)]. Thus, this GI induces the following closure operator on models ordered by the superset inclusion.

Definition 3.5. $\rho_M^\forall \stackrel{\text{def}}{=} \gamma_M^\forall \circ \alpha_M^\forall \in \text{uco}(\langle \mathbb{M}, \supseteq \rangle)$ is the *universal checking closure* relative to a model $M \in \mathbb{M}$. Hence, $\rho_M^\forall = \lambda X. \{ \langle i, \sigma \rangle \in M \mid M_{\downarrow \sigma_i} \subseteq X \}$. \square

Notice that for any $X \in \mathbb{M}$, $\rho_M^\forall(X) \subseteq X \cap M$, and that $\rho_M^\forall(X)$ gives the least set of traces whose α_M^\forall -abstraction is $\alpha_M^\forall(X)$. The intuition is that $\rho_M^\forall(X)$ throws away from X all those traces $\langle i, \sigma \rangle$ either which are not in M — these traces “do not matter”, since $\alpha_M^\forall(\neg M) = \emptyset$ — 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 $\alpha_M^\exists : \mathbb{M} \rightarrow \wp(\mathbb{S})$ 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 [6, Definition 49]:

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

In this case, the subset relation formalizes the notion of approximation: if $\alpha_M^\exists(\phi) \subseteq S$ 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 . Thus, it can be roughly said that the existential checking abstraction is ideally useful

for checking so-called safety properties of reactive systems, i.e., “bad things do not happen during executions”. It turns out that α_M^\exists gives rise to an adjunction between $\langle \wp(\mathbb{S}), \subseteq \rangle$ and $\langle \mathbb{M}, \subseteq \rangle$, where the concretization map $\gamma_M^\exists : \wp(\mathbb{S}) \rightarrow \mathbb{M}$ is given by $\gamma_M^\exists(S) \stackrel{\text{def}}{=} \{ \langle i, \sigma \rangle \in \mathbb{T} \mid \langle i, \sigma \rangle \in M \Rightarrow \sigma_i \in S \}$. As above, for a model \mathcal{M}_τ generated by a transition system, by the totality hypothesis, $\alpha_{\mathcal{M}_\tau}^\exists$ is onto, and hence $(\alpha_{\mathcal{M}_\tau}^\exists, \langle \mathbb{M}, \subseteq \rangle, \langle \wp(\mathbb{S}), \subseteq \rangle, \gamma_{\mathcal{M}_\tau}^\exists)$ is a GI [6, (50)]. Here, we get the following closure.

Definition 3.6. $\rho_M^\exists \stackrel{\text{def}}{=} \gamma_M^\exists \circ \alpha_M^\exists \in \text{uco}(\langle \mathbb{M}, \subseteq \rangle)$ is the *existential checking closure* relative to a model $M \in \mathbb{M}$. Hence, $\rho_M^\exists = \lambda X. \{ \langle i, \sigma \rangle \in \mathbb{T} \mid \langle i, \sigma \rangle \in M \Rightarrow M_{\downarrow \sigma_i} \cap X \neq \emptyset \} = \lambda X. \{ \langle i, \sigma \rangle \in M \mid M_{\downarrow \sigma_i} \cap X \neq \emptyset \} \cup \neg M$. \square

Here, we have that, for any $X \in \mathbb{M}$, $X \cup \neg M \subseteq \rho_M^\exists(X)$. The intuition is that ρ_M^\exists 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 $\alpha_M^\exists(\neg M) = \emptyset$ — plus any trace in M whose present state existentially satisfies X .

Classical State-Based (Abstract) Semantics. Given a total transition system $\langle \mathbb{S}, \tau \rangle$ and its associated model \mathcal{M}_τ , the classical state-based semantics of a temporal formula is calculationaly designed as the abstract semantics induced by the model checking abstractions seen above. This is an instance of the very general abstract interpretation scheme introduced by Cousot and Cousot in [6, Section 8] in order to be language-, semantics- and abstraction-independent and to handle monotone and antitone semantic functions simultaneously. Basically, this process amounts to abstract any model transformer of Definition 3.2 by the corresponding best correct approximation induced by the checking abstraction. For example, the predecessor transformer $\oplus : \mathbb{M} \rightarrow \mathbb{M}$ is abstracted to $\alpha_{\mathcal{M}_\tau}^\forall \circ \oplus \circ \gamma_{\mathcal{M}_\tau}^\forall : \wp(\mathbb{S}) \rightarrow \wp(\mathbb{S})$, where $\alpha_{\mathcal{M}_\tau}^\forall \circ \oplus \circ \gamma_{\mathcal{M}_\tau}^\forall = \widetilde{\text{pre}}[\tau] \stackrel{\text{def}}{=} \lambda S \in \wp(\mathbb{S}). \{ s \in \mathbb{S} \mid \forall s' \in \mathbb{S}. (s \xrightarrow{\tau} s') \Rightarrow s' \in S \}$ (cf. [6, Section 11.2]) is the best correct approximation of \oplus for the GI $(\alpha_{\mathcal{M}_\tau}^\forall, \langle \mathbb{M}, \supseteq \rangle, \langle \wp(\mathbb{S}), \supseteq \rangle, \gamma_{\mathcal{M}_\tau}^\forall)$.

The general scenario is as follows. $\mathbb{E}^s \stackrel{\text{def}}{=} \mathbb{X} \rightarrow \wp(\mathbb{S})$ is the set of state environments. The checking abstractions α_M^\forall and α_M^\exists are extended pointwise to environments: $\hat{\alpha}_M^\forall, \hat{\alpha}_M^\exists : \mathbb{E} \rightarrow \mathbb{E}^s$, where, e.g., $\hat{\alpha}_M^\forall(\xi) \stackrel{\text{def}}{=} \lambda X \in \mathbb{X}. \alpha_M^\forall(\xi(X))$. The process of abstraction then compositionally leads to the following abstract state-based semantics for the $\hat{\mu}$ -calculus: $\llbracket \cdot \rrbracket_\tau^\forall, \llbracket \cdot \rrbracket_\tau^\exists : \mathcal{L}_{\hat{\mu}} \rightarrow \mathbb{E}^s \rightarrow \wp(\mathbb{S})$. These are inductively defined as one expects, following the lines of Definition 3.3. Thus, $\llbracket \phi \rrbracket_\tau^\forall$ corresponds to the classical state interpretation of a temporal formula ϕ .

Soundness of the abstract state-based semantics is by construction: for any $\phi \in \mathcal{L}_{\hat{\mu}}$ and $\xi \in \mathbb{E}$, $\alpha_{\mathcal{M}_\tau}^\forall(\llbracket \phi \rrbracket_\tau^\forall \xi) \supseteq \llbracket \phi \rrbracket_\tau^\forall \hat{\alpha}_{\mathcal{M}_\tau}^\forall(\xi)$ and $\alpha_{\mathcal{M}_\tau}^\exists(\llbracket \phi \rrbracket_\tau^\exists \xi) \subseteq \llbracket \phi \rrbracket_\tau^\exists \hat{\alpha}_{\mathcal{M}_\tau}^\exists(\xi)$.

3.4 Completeness Issues

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 [6, Counterexample (60)]). This means, for example, that there exist a closed formula $\phi \in \mathcal{L}_{\hat{\mu}}$ and a state $s \in \mathbb{S}$ such that $s \in \alpha_{\mathcal{M}_\tau}^\forall(\llbracket \phi \rrbracket_\tau^\forall \emptyset) \setminus \llbracket \phi \rrbracket_\tau^\forall \emptyset$, and therefore trace-based and state-based model checking for ϕ are not equivalent:

$\mathcal{M}_\tau, s \models_{trace} \phi$ (viz., $\mathcal{M}_{\tau \downarrow s} \subseteq \llbracket \phi \rrbracket \emptyset$), while $\mathcal{M}_\tau, s \not\models_{state} \phi$ (viz., $s \notin \llbracket \phi \rrbracket^\forall \emptyset$). Intuitively, incompleteness states that in order to deal with temporal specifications of the $\hat{\mu}$ -calculus, model checking algorithms should handle sets of traces instead that sets of traces, and this is evidently infeasible.

Cousot and Cousot [6] identified the model transformers causing such incompleteness and provided some sufficient conditions ensuring completeness. In view of Section 2, in the following, we will mostly adopt the convenient closure operator approach to abstract domains.

The first incomplete transformer for the universal checking abstraction is the predecessor operator \oplus , as shown in [6, Section 11.2]. In this case, the following sufficient condition holds: for all $X \in \mathbb{M}$, if $X = Fd(X)$ then $\rho_{\mathcal{M}_\tau}^\forall(\oplus(\rho_{\mathcal{M}_\tau}^\forall(X))) = \rho_{\mathcal{M}_\tau}^\forall(\oplus(X))$. In other words, the predecessor transformer is complete for any forward-closed formula to check. Of course, dually, the successor model transformer \ominus is incomplete as well.

Disjunction, namely set union, is the second incomplete model transformer, as observed in [6, Section 11.6]. Here, we have that for any $X, Y \in \mathbb{M}$, if $X = St(X)$ or $Y = St(Y)$ then $\rho_{\mathcal{M}_\tau}^\forall(\rho_{\mathcal{M}_\tau}^\forall(X) \cup \rho_{\mathcal{M}_\tau}^\forall(Y)) = \rho_{\mathcal{M}_\tau}^\forall(X \cup Y)$. This means that disjunction on at least one state-closed formula turns out to be complete.

The above sufficient conditions allow to identify some meaningful complete fragments of the $\hat{\mu}$ -calculus. This is the case, for example, of the μ_+^\forall -calculus considered in [6, Section 13], which is complete for the universal checking abstraction and subsumes the classical \forall CTL logic.

Finally, the reversal model transformer \frown is also incomplete, as shown by the following example, although this is not explicitly mentioned in [6, Section 11].

Example 3.7. We follow the lines of [6, Counterexample (56)]. Let $\mathbb{S} \stackrel{\text{def}}{=} \{o, \bullet\}$ and $\tau \stackrel{\text{def}}{=} \{(o, o), \langle \bullet, \bullet \rangle, \langle \bullet, o \rangle\}$. We have that $\mathcal{M}_\tau = \{\langle i, \lambda k.o \rangle\}_{i \in \mathbb{Z}} \cup \{\langle i, \lambda k.\bullet \rangle\}_{i \in \mathbb{Z}} \cup \{\langle i, \lambda k.(k < m ? \bullet : i.o) \rangle\}_{i, m \in \mathbb{Z}}$. Let $X \stackrel{\text{def}}{=} \{\langle i, \sigma \rangle \mid \forall k \geq i. \sigma_k = \bullet\}$, and therefore $\frown(X) = \{\langle i, \sigma \rangle \mid \forall k \leq i. \sigma_k = \bullet\}$. Since $\mathcal{M}_{\tau \downarrow o} \not\subseteq X$ and $\mathcal{M}_{\tau \downarrow \bullet} = \{\langle i, \lambda k.\bullet \rangle\}_{i \in \mathbb{Z}} \cup \{\langle i, \lambda k.(k < m ? \bullet : i.o) \rangle\}_{i, m \in \mathbb{Z}, i < m} \not\subseteq X$, we have that $\rho_{\mathcal{M}_\tau}^\forall(X) = \emptyset$, and hence $\rho_{\mathcal{M}_\tau}^\forall(\frown(\rho_{\mathcal{M}_\tau}^\forall(X))) = \emptyset$. Instead, it turns out that $\rho_{\mathcal{M}_\tau}^\forall(\frown(X)) = \mathcal{M}_{\tau \downarrow \bullet}$. \square

Of course, a dual reasoning can be made for the existential checking abstraction: here, the incomplete model transformers are predecessor, successor, conjunction and reversal.

4 Absolute Complete Shells for Model Transformers

In this section we characterize the absolute complete shells of the checking closures for the incomplete model transformers identified in Section 3.4.

In the following, we will consider checking closures parameterized w.r.t. a generic model $M \in \mathbb{M}$ satisfying the following hypothesis.

Hypothesis 4.1. *For any universal and existential state closure, respectively ρ_M^\forall and ρ_M^\exists , the model $M \in \mathbb{M}$ is such that $\oplus(M) = M = \ominus(M)$ and $\oplus(\frown(M)) = \frown(M) = \ominus(\frown(M))$.*

This therefore means that M and its reversal $\smile M$ are closed for forward and backward time progresses. This is obviously satisfied by any model generated by a transition system.

Remark 4.2. Any model $\mathcal{M}_\tau \in \mathbb{M}$ generated by a transition system $\langle \mathbb{S}, \tau \rangle$ satisfies the Hypothesis 4.1.

Predecessor. Let us first characterize the absolute complete shell of the universal checking closure for the predecessor model transformer. Since the predecessor operator is additive, this complete shell actually exists in view of Theorem 2.1, and its set of fixpoints turns out to be as follows.

Theorem 4.3. The absolute complete shell $S_{\check{V}_M}^\oplus$ of $\rho_M^\check{V}$ for \oplus exists and it is characterized by the following set of fixpoints: $\mathcal{M}_{\mathbb{M}_\supseteq}(\{\ominus^n(X) \mid n \in \mathbb{N}, X \in \rho_M^\check{V}\})$.

Thus, each arbitrary union (that is Moore-closure in $\langle \mathbb{M}, \supseteq \rangle$) of arbitrary powers of the successor transformer applied to fixpoints of the universal checking closure turns out to be a fixpoint of the closure $S_{\check{V}_M}^\oplus \in \text{uco}(\langle \mathbb{M}, \supseteq \rangle)$. In other terms, in order to minimally refine the checking closure $\rho_M^\check{V}$ to a complete closure for the predecessor transformer, one must close the image of $\rho_M^\check{V}$ under the application of the inverse of the predecessor transformer, i.e., the successor.

We also provide an interesting characterization of the absolute complete shell $S_{\check{V}_M}^\oplus$ as a mapping on models. First, we need to introduce the following notion.

Definition 4.4. Given $\langle i, \sigma \rangle \in \mathbb{T}$, $M \in \mathbb{M}$ and $k \in \mathbb{N}$, the projection $M_{\downarrow \langle i, \sigma \rangle}^{-k}$ of M at the k -th past state of $\langle i, \sigma \rangle$ is defined as follows:

$$M_{\downarrow \langle i, \sigma \rangle}^{-k} \stackrel{\text{def}}{=} \{(j, \beta) \in M \mid \beta_{j-k} = \sigma_{i-k}\}. \quad \square$$

The k -th past state projection of a model is therefore a generalization of the (current) state projection, since $M_{\downarrow \sigma_i} = M_{\downarrow \langle i, \sigma \rangle}^0$. The following result holds.

Theorem 4.5. The absolute complete shell $S_{\check{V}_M}^\oplus$ of $\rho_M^\check{V}$ for \oplus can be characterized as follows: $S_{\check{V}_M}^\oplus = \lambda X. \{(i, \sigma) \in M \mid \exists k \in \mathbb{N}. M_{\downarrow \langle i, \sigma \rangle}^{-k} \subseteq X\}$.

Thus, for any $X \in \mathbb{M}$, $S_{\check{V}_M}^\oplus(X)$ throws away from X all those traces either which are not in M or which are in M but any past or current state of the trace does not universally satisfy X . $S_{\check{V}_M}^\oplus(X)$ is actually a refinement of $\rho_M^\check{V}(X)$, since $\rho_M^\check{V}(X) \subseteq S_{\check{V}_M}^\oplus(X) \subseteq X \cap M$, and it characterizes exactly the least amount of information that must be added to $\rho_M^\check{V}(X)$ in order to be complete for the predecessor. The intuition is that while $\rho_M^\check{V}$ considers present states only (i.e., $M_{\downarrow \sigma_i} \subseteq X$), as expected, completeness for the predecessor forces to take into account any past state (i.e., $\exists k \in \mathbb{N}. M_{\downarrow \langle i, \sigma \rangle}^{-k} \subseteq X$). Thus, the basic idea is “to prolong the abstract domain $\wp(\mathbb{S})$ in the past”. This leads to design the following abstract domain.

Definition 4.6. Define $\wp(\mathbb{S})^\triangleleft \stackrel{\text{def}}{=} \mathbb{Z}_{\leq 0} \rightarrow \wp(\mathbb{S})$, where $\mathbb{Z}_{\leq 0}$ is the set of nonpositive integers. $\wp(\mathbb{S})^\triangleleft$ is endowed with standard pointwise orderings \subseteq and \supseteq , making it a complete lattice.

Given $z \in \mathbb{Z}_{\leq 0}$, $s \in \mathbb{S}$ and $M \in \mathbb{M}$, define $M_{\downarrow s}^z \stackrel{\text{def}}{=} \{\langle i, \sigma \rangle \in M \mid \sigma_{i+z} = s\}$.
The mappings $\alpha_{\mathbb{V}_M}^\oplus : \mathbb{M} \rightarrow \wp(\mathbb{S})^\triangleleft$ and $\gamma_{\mathbb{V}_M}^\oplus : \wp(\mathbb{S})^\triangleleft \rightarrow \mathbb{M}$ are defined as follows:

$$\alpha_{\mathbb{V}_M}^\oplus(X) \stackrel{\text{def}}{=} \lambda z \in \mathbb{Z}_{\leq 0}. \{s \in \mathbb{S} \mid M_{\downarrow s}^z \subseteq X\};$$

$$\gamma_{\mathbb{V}_M}^\oplus(\Sigma) \stackrel{\text{def}}{=} \{\langle i, \sigma \rangle \in M \mid \exists k \in \mathbb{N}. \sigma_{i-k} \in \Sigma_{-k}\}. \quad \square$$

Corollary 4.7. $(\alpha_{\mathbb{V}_M}^\oplus, \mathbb{M}_{\supseteq}, \wp(\mathbb{S})_{\supseteq}^\triangleleft, \gamma_{\mathbb{V}_M}^\oplus)$ is a GC, and additionally a GI when $M = \mathcal{M}_\tau$ for some transition system $\langle \mathbb{S}, \tau \rangle$, inducing the closure $S_{\mathbb{V}_M}^\oplus \in \text{uco}(\mathbb{M}_{\supseteq})$.

Hence, the above result provides a concrete representation for one possible and simple abstract domain for the closure $S_{\mathbb{V}_M}^\oplus$. The abstract domain $\wp(\mathbb{S})_{\supseteq}^\triangleleft$ of the universal checking abstraction α_M^\forall is refined to a domain of infinite sequences of sets of states. Such sequences are indexed over $\mathbb{Z}_{\leq 0}$, and this aims at recalling that for any $\Sigma \in \wp(\mathbb{S})^\triangleleft$ and $i \in \mathbb{N}$, $\Sigma_{-i} \in \wp(\mathbb{S})$ is a set of states at time $-i \in \mathbb{Z}_{\leq 0}$. Basically, $\alpha_{\mathbb{V}_M}^\oplus$ can be viewed as the most natural ‘‘prolongation’’ of α_M^\forall in the past.

Example 4.8. The example [6, Counterexample (56)] has been used to show that, in general, α_M^\forall is not complete for \oplus . The setting has been already recalled in Example 3.7. Let $X \stackrel{\text{def}}{=} \{\langle i, \sigma \rangle \mid i \in \mathbb{Z}, \forall j < i. \sigma_j = \bullet\}$. It is observed in [6, Counterexample (56)] that $\emptyset = \rho_{\mathcal{M}_\tau}^\forall(\oplus(\rho_{\mathcal{M}_\tau}^\forall(X))) \subsetneq \rho_{\mathcal{M}_\tau}^\forall(\oplus(X))$. Instead, it is not hard to check that for $S_{\mathbb{V}_{\mathcal{M}_\tau}}^\oplus$ completeness does hold:

$$\begin{aligned} S_{\mathbb{V}_{\mathcal{M}_\tau}}^\oplus(\oplus(X)) &= \\ &= \mathcal{M}_{\tau \downarrow \bullet} = \{\langle i, \lambda k. \bullet \rangle \mid i \in \mathbb{Z}\} \cup \{\langle i, \lambda k. (k < m ? \bullet : \circ) \rangle \mid i, m \in \mathbb{Z}, i < m\} = \\ &= S_{\mathbb{V}_{\mathcal{M}_\tau}}^\oplus(\oplus(S_{\mathbb{V}_{\mathcal{M}_\tau}}^\oplus(X))). \quad \square \end{aligned}$$

Disjunction. Let us turn to disjunction, i.e. union \cup , the second incomplete model transformer. Here again, the absolute complete shell of ρ_M^\forall for (finite) disjunction exists by Theorem 2.1, because union on \mathbb{M}_{\supseteq} is trivially additive.

Theorem 4.9. *The absolute complete shell $S_{\mathbb{V}_M}^\cup$ of ρ_M^\forall for \cup exists and it is characterized as follows:*

- (1) *The set of fixpoints of $S_{\mathbb{V}_M}^\cup$ is $\{X \in \mathbb{M} \mid X \subseteq M\}$;*
- (2) $S_{\mathbb{V}_M}^\cup = \lambda X. X \cap M$;
- (3) $S_{\mathbb{V}_M}^\cup$ is the closure induced by the GI $(\alpha_{\mathbb{V}_M}^\cup, \mathbb{M}_{\supseteq}, \wp(M)_{\supseteq}, \gamma_{\mathbb{V}_M}^\cup)$, where $\alpha_{\mathbb{V}_M}^\cup \stackrel{\text{def}}{=} \lambda X. X \cap M$ and $\gamma_{\mathbb{V}_M}^\cup \stackrel{\text{def}}{=} \lambda X. X$.

Thus, this shows that the absolute complete shell $S_{\mathbb{V}_M}^\cup$ of the universal checking closure for the union of models is essentially the identity mapping. More precisely, given the model to check M , one simple (actually, in a natural sense, it could be termed the simplest) abstract domain equivalent to the closure $S_{\mathbb{V}_M}^\cup$ is $\wp(M)_{\supseteq}$ endowed with the abstraction map $\lambda X. X \cap M$ which merely removes those traces which are not in M . This can be read as stating that completeness for disjunction requires all the traces in M .

Example 4.10. [6, Counterexample (58)] shows that, in general, α_M^\forall is not complete for \cup . The setting is still that of Example 3.7. Let $X_1 \stackrel{\text{def}}{=} \{\langle i, \sigma \rangle \mid i \in \mathbb{Z}, \exists k \geq$

$i.\forall j \geq k.\sigma_j = \circ$ and $X_2 \stackrel{\text{def}}{=} \{\langle i, \sigma \rangle \mid i \in \mathbb{Z}, \forall k \geq i.\sigma_k = \bullet\}$. [6, Counterexample (58)] observes incompleteness: $\rho_{\mathcal{M}_\tau}^\forall (\rho_{\mathcal{M}_\tau}^\forall (X_1) \cup \rho_{\mathcal{M}_\tau}^\forall (X_2)) \subsetneq \rho_{\mathcal{M}_\tau}^\forall (X_1 \cup X_2)$. For the absolute complete shell $S_{\forall \mathcal{M}_\tau}^\cup$, instead, we have that:

$$S_{\forall \mathcal{M}_\tau}^\cup (X_1) = X_1 \cap \mathcal{M}_\tau = \{\langle i, \lambda k.\circ \rangle \mid i \in \mathbb{Z}\} \cup \{\langle i, \lambda k.(k < m ? \bullet : \circ) \rangle \mid i, m \in \mathbb{Z}, i \leq m\},$$

$$S_{\forall \mathcal{M}_\tau}^\cup (X_2) = X_2 \cap \mathcal{M}_\tau = \{\langle i, \lambda k.\bullet \rangle \mid i \in \mathbb{Z}\},$$

$$S_{\forall \mathcal{M}_\tau}^\cup (X_1 \cup X_2) = S_{\forall \mathcal{M}_\tau}^\cup (X_1) \cup S_{\forall \mathcal{M}_\tau}^\cup (X_2),$$

and this easily implies that $S_{\forall \mathcal{M}_\tau}^\cup (S_{\forall \mathcal{M}_\tau}^\cup (X_1) \cup S_{\forall \mathcal{M}_\tau}^\cup (X_2)) = S_{\forall \mathcal{M}_\tau}^\cup (X_1 \cup X_2)$. \square

Reversal. Let us consider reversal, the last incomplete model transformer. Again, the absolute complete shell of ρ_M^\forall for the reversal exists by Theorem 2.1, because the reversal operator \frown on \mathbb{M}_\supseteq is obviously additive.

Theorem 4.11. *The absolute complete shell $S_{\forall M}^\frown$ of ρ_M^\forall for \frown exists and it is characterized as follows:*

- (1) *The set of fixpoints of $S_{\forall M}^\frown$ is $\mathcal{M}_{\mathbb{M}_\supseteq}(\rho_M^\forall \cup \{\frown(X) \in \mathbb{M} \mid X \in \rho_M^\forall\})$;*
- (2) $S_{\forall M}^\frown = \lambda X.\rho_M^\forall(X) \cup \frown(\rho_M^\forall(\frown(X)))$;
- (3) $S_{\forall M}^\frown$ *is the closure operator induced by the GC $(\alpha_{\forall M}^\frown, \mathbb{M}_\supseteq, \wp(\mathbb{S})_\supseteq^2, \gamma_{\forall M}^\frown)$, where $\alpha_{\forall M}^\frown \stackrel{\text{def}}{=} \lambda X.\langle \alpha_M^\forall(X), \alpha_M^\forall(X) \rangle$ and $\gamma_{\forall M}^\frown \stackrel{\text{def}}{=} \lambda(X_1, X_2).\gamma_M^\forall(X_1) \cup \gamma_M^\forall(X_2)$.*

The above result tells us that the complete shell $S_{\forall M}^\frown$ simply refines $\wp(\mathbb{S})$ to $\wp(\mathbb{S})^2$, where a model X is abstracted to the pair $\langle \alpha_M^\forall(X), \alpha_M^\forall(X) \rangle$. Hence, completeness for the reversal requires an additional component taking into account the universal checking abstraction for the reversed model $\frown(M)$. Also, notice that the GC $(\alpha_{\forall M}^\frown, \mathbb{M}_\supseteq, \wp(\mathbb{S})_\supseteq^2, \gamma_{\forall M}^\frown)$ can be also viewed as the direct (not reduced) product (see [5]) of $(\alpha_M^\forall, \mathbb{M}_\supseteq, \wp(\mathbb{S})_\supseteq, \gamma_M^\forall)$ and $(\alpha_M^\forall, \mathbb{M}_\supseteq, \wp(\mathbb{S})_\supseteq, \gamma_M^\forall)$.

All the Model Transformers. To conclude our analysis, we characterize the absolute complete shell of ρ_M^\forall for the set of all the model transformers of Definition 3.2. This exists by Theorem 2.1 because all the operations are continuous, taking 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 $\lambda X.\forall(N, X) : \mathbb{M} \rightarrow \mathbb{M}$, where $N \subseteq M \cup \frown(M)$, of the universal state closure transformer, because from the abstract interpretation viewpoint the binary transformer $\forall : \mathbb{M} \times \mathbb{M} \rightarrow \mathbb{M}$ is problematic. In fact, the binary operation \forall 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 seen at the end of Section 3.1, this is enough to recover the standard universal state quantification. In the sequel, we will use the following compact notation: $M^* \stackrel{\text{def}}{=} M \cup \frown(M)$. We have the following result.

Theorem 4.12. *The absolute complete shell $S_{\forall M}$ of ρ_M^\forall for $\{\sigma_S\}_{S \in \wp(\mathbb{S})} \cup \{\pi_t\}_{t \in \wp(\mathbb{S}^2)} \cup \{\oplus, \cap, \cup, \neg, \frown\} \cup \{\lambda X.\forall(N, X)\}_{N \subseteq M^*}$ exists and it is characterized as follows:*

- (1) *The set of fixpoints of $S_{\forall M}$ is $\{X \in \mathbb{M} \mid X \subseteq M^*\}$;*
- (2) $S_{\forall M} = \lambda X. X \cap M^*$;
- (3) $S_{\forall M}$ *is the closure induced by the GI $(\alpha_{\forall M}, \mathbb{M}_{\supseteq}, \wp(M^*)_{\supseteq}, \gamma_{\forall M})$, where $\alpha_{\forall M} \stackrel{\text{def}}{=} \lambda X. X \cap M^*$ and $\gamma_{\forall M} \stackrel{\text{def}}{=} \lambda X. X$;*
- (4) $S_{\forall M} = S_{\forall M}^{\cup} \sqcap S_{\forall M}^{\cap}$.

This shell must be complete both for disjunction and reversal, and therefore $S_{\forall M}$ results to be more concrete than the corresponding shells $S_{\forall M}^{\cup}$ and $S_{\forall M}^{\cap}$ seen above. Actually, it turns out that $S_{\forall M}$ is precisely the glb in $uco(\mathbb{M}_{\supseteq})$ of these two shells. Thus, this globally complete abstract domain is even more close to the concrete domain of sets of generic traces, since the corresponding abstraction is just “something less” than the identity.

It is also interesting to observe that when we leave out the reversal operator, as expected, the complete shell becomes $S_{\forall M}^{\cup}$, as stated by the following result.

Theorem 4.13. $S_{\forall M}^{\cup}$ *is the absolute complete shell of ρ_M^{\forall} for $\{\sigma_S\}_{S \in \wp(\mathbb{S})} \cup \{\pi_t\}_{t \in \wp(\mathbb{S}^2)} \cup \{\oplus, \cap, \cup, \neg\} \cup \{\lambda X. \forall(N, X)\}_{N \subseteq M}$.*

Existential Checking Closure. The scenario for the existential checking closure is dual to the universal case. The following statement collects the most important characterizations.

Theorem 4.14.

- (1) $S_{\exists M}^{\oplus} \stackrel{\text{def}}{=} \lambda X. \{\langle i, \sigma \rangle \in \mathbb{T} \mid \langle i, \sigma \rangle \in M \Rightarrow (\forall k \in \mathbb{N}. M_{\downarrow \langle i, \sigma \rangle}^{-k} \cap X \neq \emptyset)\}$ *is the absolute complete shell of ρ_M^{\exists} for \oplus ;*
- (2) $S_{\exists M}^{\cap} \stackrel{\text{def}}{=} \lambda X. X \cup \neg M$ *is the absolute complete shell of ρ_M^{\exists} for \cap ;*
- (3) $S_{\exists M}^{\cap} \stackrel{\text{def}}{=} \lambda X. \rho_M^{\exists}(X) \cup \cap(\rho_M^{\exists}(\cap X))$ *is the absolute complete shell of ρ_M^{\exists} for \cap ;*
- (4) $S_{\exists M}^{\cup} \stackrel{\text{def}}{=} \lambda X. X \cup \neg M^*$ *is the absolute complete shell of ρ_M^{\exists} for $\{\sigma_S\}_{S \in \wp(\mathbb{S})} \cup \{\pi_t\}_{t \in \wp(\mathbb{S}^2)} \cup \{\oplus, \cap, \cup, \neg, \cap\} \cup \{\lambda X. \forall(N, X)\}_{N \subseteq M^*}$.*

5 Completeness of Temporal Calculi

As already observed in Section 4, from the abstract interpretation viewpoint, the universal state closure connective \forall of the full $\widehat{\mu}$ -calculus is somehow problematic, because, according to Cousot and Cousot’s [6] Definition 3.1, the binary connective \forall can be applied without any restriction, while its semantic counterpart, the universal state closure transformer $\forall : \mathbb{M} \times \mathbb{M} \rightarrow \mathbb{M}$, is neither monotone nor antitone in its first argument. On the other hand, given any $N \in \mathbb{M}$, the unary restriction $\lambda X. \forall(N, X) : \mathbb{M} \rightarrow \mathbb{M}$ is monotone, and this is enough in order to have the standard universal state quantification: $\forall \phi \stackrel{\text{def}}{=} \forall \boxtimes (\pi_{\tau}) : \phi$. This naturally leads to the following slight “monotone” restriction, which we call $\widehat{\mu}^-$ -calculus, of the $\widehat{\mu}$ -calculus.

Definition 5.1. Formulae ϕ of the $\widehat{\mu}^-$ -calculus are inductively defined as follows:

$$\phi ::= \sigma_S \mid \pi_t \mid X \mid \oplus \phi \mid \phi^{\cap} \mid \phi_1 \vee \phi_2 \mid \neg \phi \mid \mu X. \phi \mid \nu X. \phi \mid \forall \phi$$

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

Of course, the trace-semantics for the $\widehat{\mu}^-$ -calculus is completely identical to that of the $\widehat{\mu}$ -calculus given in Definition 3.3, but for the universal connective: $\llbracket \forall \phi \rrbracket \xi \stackrel{\text{def}}{=} \forall (\mathcal{M}_\tau, \llbracket \phi \rrbracket \xi)$.

The main result of this section is then stated for the $\widehat{\mu}^-$ -calculus. The scenario is as follows. As seen in Section 3.3 for the universal and existential checking abstractions, any abstraction of the domain \mathbb{M} of concrete temporal models, ordered by the superset or subset relation, induces an abstract semantics for the $\widehat{\mu}$ -calculus, and therefore for the $\widehat{\mu}^-$ -calculus. More in detail, for the universal case, given a model to check $M \in \mathbb{M}$ — which is supposed to be generated by a transition system $\langle \mathbb{S}, \tau \rangle$ — any closure operator, i.e. abstract domain, $\rho \in \text{uco}(\mathbb{M}_\supseteq)$, induces the set of abstract environments $\mathbb{E}^\rho \stackrel{\text{def}}{=} \mathbb{X} \rightarrow \rho$, and the corresponding abstract semantics $\llbracket \cdot \rrbracket^\rho : \mathcal{L}_{\widehat{\mu}^-} \rightarrow \mathbb{E}^\rho \rightarrow \rho$. 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., $\forall \phi \in \mathcal{L}_{\widehat{\mu}^-}. \forall \xi \in \mathbb{E}. \rho(\llbracket \phi \rrbracket \xi) \supseteq \llbracket \phi \rrbracket^\rho \dot{\rho}(\xi)$, holds by construction (cf. [6, Theorem (40)]), while completeness for ρ means that equality always holds. We therefore have the following theorem.

Theorem 5.2. S_{\forall_M} is the least (w.r.t. subset image containment) closure operator on \mathbb{M}_\supseteq (1) complete for the $\widehat{\mu}^-$ -calculus and (2) containing the universal checking closure ρ_M^\forall .

It is important to stress that since the $\widehat{\mu}^-$ -calculus involves (least and greatest) fixpoints, no general result in [8] ensures the existence of the above complete abstract domain. Nevertheless, the above result shows that this complete shell does exist, and it coincides with the absolute complete shell S_{\forall_M} relative to all the temporal connectives seen in Theorem 4.12, namely the identity on sets of traces in M or its reversal. Hence, in this case, fixpoints do not affect the outcome. This complete shell induces an abstract semantics which essentially is the trace-based semantics itself. Thus, this key result can be interpreted as follows: if we want to refine the state-based model checking — i.e., the classical domain of sets of states — in order to be trace-complete for the $\widehat{\mu}$ -calculus, we ineluctably get the trace-based semantics itself.

When the reversal connective is not included, analogously to Theorem 4.13 we get the following characterization.

Definition 5.3. Formulae ϕ of the $\widehat{\mu}^-$ -calculus are defined as follows:

$$\phi ::= \sigma_S \mid \pi_t \mid X \mid \oplus \phi \mid \phi_1 \vee \phi_2 \mid \neg \phi \mid \mu X. \phi \mid \nu X. \phi \mid \forall \phi$$

where $S \in \wp(\mathbb{S})$, $t \in \wp(\mathbb{S} \times \mathbb{S})$, and $X \in \mathbb{X}$. □

Theorem 5.4. $S_{\forall_M}^\cup$ is the least (w.r.t. subset image containment) closure operator on \mathbb{M}_\supseteq (1) complete for the $\widehat{\mu}^-$ -calculus and (2) containing the universal checking closure ρ_M^\forall .

The Existential Case. The situation is fully dual: we simply state the result.

Theorem 5.5. S_{\exists_M} and $S_{\exists_M}^\cup$ are, respectively, the least (w.r.t. subset image containment) closures on \mathbb{M}_\subseteq (1) complete, respectively, for the $\widehat{\mu}^-$ -calculus and for the $\widehat{\mu}^-$ -calculus, and (2) containing the existential checking closure ρ_M^\exists .

6 Conclusion

In the context of a novel and rich temporal specification language called $\widehat{\mu}$ -calculus, Cousot and Cousot [6] showed that classical state-based model checking is an abstract interpretation of the trace-based semantics for the $\widehat{\mu}$ -calculus, which is incomplete. In this paper, we have characterized the least, i.e. least informative, refinement of the state-based model checking semantics of the $\widehat{\mu}$ -calculus which is complete w.r.t. the trace-based semantics, and this turns out to be essentially the trace-based semantics itself.

Cousot and Cousot [6, Section 14] also showed that standard abstract model checking [2, 3, 7, 10] using a surjective mapping from concrete states to a set of abstract states can be understood as a further step of abstraction over the state-based model checking semantics. Analogously to what has been studied in this paper, this opens the question of minimally refining abstract model checking in order to get completeness, which is a very desirable property when performing model checking for abstract models. Some recent results in this direction for ACTL* are given by Clarke et al. in [1].

Acknowledgements. I wish to thank Roberto Giacobazzi for the many helpful discussions we had on May 2000 in Place des Vosges, and Radhia Cousot for hosting me at LIX, École Polytechnique, Palaiseau, on May 2000. Special thanks to Maddie Hayes. This work has been partly supported by the Italian MURST project “Automatic program certification by abstract interpretation”.

References

1. 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, 2000.
2. E.M. Clarke, O. Grumberg and D. Long. Model checking and abstraction. *ACM TOPLAS*, 16(5):1512–1542, 1994.
3. E.M. Clarke, O. Grumberg and D.A. Peled. *Model checking*. The MIT Press, 1999.
4. P. Cousot and R. Cousot. Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *Proc. 4th ACM POPL*, pp. 238–252, 1977.
5. P. Cousot and R. Cousot. Systematic design of program analysis frameworks. In *Proc. 6th ACM POPL*, pp. 269–282, 1979.
6. P. Cousot and R. Cousot. Temporal abstract interpretation. In *Proc. 27th ACM POPL*, pp. 12–25, 2000.
7. D. Dams, O. Grumberg, and R. Gerth. Abstract interpretation of reactive systems. *ACM TOPLAS*, 16(5):1512–1542, 1997.
8. R. Giacobazzi, F. Ranzato, and F. Scozzari. Making abstract interpretations complete. *J. ACM*, 47(2):361–416, 2000.
9. D. Kozen. Results on the propositional μ -calculus. *TCS*, 27:333–354, 1983.
10. 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.
11. Z. Manna and A. Pnueli. *The Temporal Logic of Reactive and Concurrent Systems Specification*. Springer-Verlag, 1992.
12. M. Müller-Olm, D. Schmidt, and B. Steffen. Model-checking: a tutorial introduction. In *Proc. SAS'99*, LNCS 1694, pp. 330–354, 1999.