Incompleteness of States w.r.t. Traces in Model Checking

Roberto Giacobazzi [a] and Francesco Ranzato [b]

[a] *Dipartimento di Informatica, Università di Verona, Italy*

[b] *Dipartimento di Matematica Pura ed Applicata, Università di Padova, Italy*

Abstract

Cousot and Cousot introduced and studied a general past/future-time specification language, called $\widehat{\mu}^{\star}$-calculus, featuring a natural time-symmetric *trace-based* semantics. The standard *state-based* semantics of the $\widehat{\mu}^{\star}$-calculus is an *abstract interpretation* of its trace-based semantics, which turns out to be *incomplete*, that is trace-incomplete, even for finite systems. As a consequence, standard state-based model checking of the $\widehat{\mu}^{\star}$-calculus is incomplete w.r.t. trace-based model checking. This paper shows that any refinement or abstraction of the domain of sets of states induces a corresponding semantics which is still trace-incomplete for any propositional fragment of the $\widehat{\mu}^{\star}$-calculus. This derives from a number of results, one for each incomplete logical/temporal connective of the $\widehat{\mu}^{\star}$-calculus, that characterize the structure of models, i.e. transition systems, whose corresponding state-based semantics of the $\widehat{\mu}^{\star}$-calculus is trace-complete.

1 Introduction

Temporal specification languages used in automatic verification by model checking can be classified in two broad classes: linear and branching time languages. Linear time languages allow to express properties of computation paths of the model, called traces, while specifications in branching time languages describe properties that depend on the branching structure of the model. LTL and CTL are the most commonly used languages for, respectively, linear and branching time model checking. The relationship between linear and branching time languages has been the subject of thorough investigation since the 1980s (see [26] for a survey). In particular, it is well known that LTL and CTL have incomparable expressive powers [2,11,18].

Email addresses: roberto.giacobazzi@univr.it (Roberto Giacobazzi), francesco.ranzato@unipd.it (Francesco Ranzato).

Given a linear specification ϕ, the standard universal model checking problem consists in characterizing the set $\mathrm{MC}^{\forall}_{M}(\phi)$ of states s of a model M, i.e. a transition system (or a Kripke structure), such that any trace in M whose present time is s satisfies ϕ. Hence, if $[\![\phi]\!] = \{\langle i, \sigma\rangle \in \mathit{Traces}_M \mid \langle i, \sigma\rangle \models \phi\}$ denotes the trace semantics of ϕ, where in a trace $\langle i, \sigma\rangle$, σ is a $\mathbb{Z}$-indexed sequence of states and $i \in \mathbb{Z}$ denotes present time, then $\mathrm{MC}^{\forall}_{M}(\phi) = \{s \in \mathit{States} \mid \forall\langle i, \sigma\rangle \in \mathit{Traces}_M \,.\, (\sigma_i = s) \Rightarrow \langle i, \sigma\rangle \in [\![\phi]\!]\}$. Cousot and Cousot showed in their POPL'00 paper [10] that this can be formalized as a step of abstraction within the standard abstract interpretation framework [8,9]. In fact, Cousot and Cousot [10] consider the universal path quantifier $\alpha^{\forall}_{M} : \wp(\mathit{Traces}) \to \wp(\mathit{States})$ which maps any set T of traces to the set of states s such that any trace in M with present state s belongs to T and show that $\alpha^{\forall}_{M}$ is an approximation map in the abstract interpretation sense. Hence, $\alpha^{\forall}_{M}$ is called the *universal model checking abstraction* because $\mathrm{MC}^{\forall}_{M}(\phi) = \alpha^{\forall}_{M}([\![\phi]\!])$. Dually, one can define an *existential* model checking abstraction $\alpha^{\exists}_{M} : \wp(\mathit{Traces}) \to \wp(\mathit{States})$ that formalizes the standard existential model checking problem: $\alpha^{\exists}_{M}(T)$ provides the set of states s such that there exists a trace in M with present state s which belongs to T. According to the standard abstract interpretation methodology, this universal abstraction gives rise to an abstract state semantics of a linear language and thus transforms the trace-based universal model checking problem to a state-based universal model checking problem. The universal state-based semantics $[\![\phi]\!]^{\forall}_{\mathrm{state}}$ of a linear formula ϕ is obtained by abstracting each linear temporal operator appearing in ϕ, like next-time or sometime operators, to its *best correct approximation* on $\wp(\mathit{States})$ through the abstraction map $\alpha^{\forall}_{M}$. This abstract semantics $[\![\phi]\!]^{\forall}_{\mathrm{state}}$ of ϕ coincides with the state semantics of the branching time formula $\phi_{\forall}$ obtained from ϕ by preceding each linear temporal operator occurring in ϕ by the universal path quantifier. Hence, this allows to transform the trace-based model checking problem $M, s \models_{\mathrm{trace}} \phi$, i.e. $s \in \alpha^{\forall}_{M}([\![\phi]\!])$, to a state-based model checking problem $M, s \models_{\mathrm{state}} \phi$, i.e. $s \in [\![\phi]\!]^{\forall}_{\mathrm{state}}$.

It should be clear that state-based model checking is a *sound* approximation of trace-based model checking, namely:

$$M, s \models_{\mathrm{state}} \phi \;\Rightarrow\; M, s \models_{\mathrm{trace}} \phi.$$

It should be noted that in abstract interpretation soundness is guaranteed by construction, namely $[\![\phi]\!]^{\forall}_{\mathrm{state}} \subseteq \alpha^{\forall}_{M}([\![\phi]\!])$ holds by abstract interpretation. However, it turns out that this approximation is *incomplete*, that is, the reverse direction does not hold, even for finite-state systems. We will provide later an example for this phenomenon. Let us remark that when $[\![\phi]\!]^{\forall}_{\mathrm{state}} = \alpha^{\forall}_{M}([\![\phi]\!])$ holds for some linear formula ϕ, Kupferman and Vardi [17,25] say that the formula ϕ is *branchable*. Branchable formulae have been used by Kupferman and Vardi for studying how model checking of a LTL formula ϕ can be reduced to an equivalent model checking of the corresponding CTL formula $\phi_{\forall}$.

The above incompleteness means that universal model checking of linear formulae

cannot be reduced with no loss of precision to universal model checking on states through the universal abstraction. This also means that standard state-based model checking algorithms (e.g. for CTL) do not provide exact information w.r.t. a trace-based interpretation. This opens the question whether it is possible to find some different approximation $\mathcal{A}$ of the trace-based model checking problem which (1) is still related to states, namely $\mathcal{A}$ refines or abstracts from sets of states, and (2) induces an approximated model checking which is instead equivalent to trace-based model checking: for any $s \in States$ and any linear formula ϕ,

$$M, s \models_{\mathcal{A}} \phi \;\Leftrightarrow\; M, s \models_{\mathrm{trace}} \phi. \qquad (*)$$

It is important to remark that we do not consider generic approximations of traces, but only approximations that can be obtained by refinements or simplifications of sets of states, namely of the domain $\wp(States)$. Let us notice that the trivial abstraction $\mathrm{Trivial} \stackrel{\mathrm{def}}{=} \{\bot\}$, i.e. the abstraction carrying no information at all by confusing all the traces, i.e. $\alpha_{\mathrm{Trivial}}(T) = \bot$ for any set T of traces, satisfies the above equivalence because we always have that $[\![\phi]\!]_{\mathrm{Trivial}} = \bot = \alpha_{\mathrm{Trivial}}([\![\phi]\!])$. More precisely, the paper answers the following question: is it possible to minimally refine/abstract the state-based semantics of a general temporal languages so that this refinement/abstraction induces a corresponding approximated model checking which is trace-complete, i.e. equivalent to trace-based model checking? In our approach, refinements and abstractions of a semantics are intended to be specified by *standard abstract interpretation* [8,9]. This paper provides the following results:

(i) the only refinement of the state-based semantics that induces a trace-complete model checking is the trace-based semantics itself;
(ii) on the opposite direction, the only abstraction of the state-based semantics that induces a trace-complete model checking is the trivial semantics carrying no information at all;
(iii) for each basic temporal/logical operator of a past- and future-time extension of Kozen's μ-calculus we characterize the least refinements and abstractions of the state-based semantics which are trace-complete.

Points (i) and (ii) prove that states are, so to say, "intrinsically trace-incomplete", since there is no way to obtain a trace-complete model checking by modifying, through refinements or abstractions, the state-based semantics.

The Scenario. As mentioned above, our results are formulated and shown within the Cousot and Cousot's [10] abstract interpretation-based approach to model checking called *temporal abstract interpretation*. Cousot and Cousot [10] introduced an enhanced past- and future-time temporal calculus, called $\widehat{\mu}$-calculus, which is inspired by Kozen's μ-calculus [16]. The trace-based semantics of the $\widehat{\mu}$-calculus is time-symmetric: this means that execution traces have potentially infinite length both in the future and in the past. Time symmetry is not the only feature of the $\widehat{\mu}$-

calculus. The $\widehat{\mu}$-calculus also provides a tight combination of linear and branching time, allowing to derive classical specification languages like LTL, CTL, CTL* and Kozen's μ-calculus itself, as suitable fragments.

One main achievement in [10] is that state-based model checking of transition systems (or Kripke structures) can be viewed as an abstract interpretation of the trace-based semantics. It is worth mentioning that this abstract interpretation-based approach has been applied to a number of temporal languages by Schmidt [24] and also to modal Kripke transition systems by Schmidt [24] and Huth et al. [15]. The semantics $[\![\phi]\!]_{\mathrm{trace}}$ of a temporal specification $\phi \in \widehat{\mu}$ is the set of traces in the model M making ϕ true. States are viewed as a universal abstract interpretation of traces through the universal concretization $\gamma^{\forall}_M : \wp(States) \longrightarrow \wp(Traces)$ defined by

$$\gamma^{\forall}_M(S) = \{\langle i, \sigma\rangle \in Traces_M \mid \sigma_i \in S\}.$$

This maps $\gamma^{\forall}_M$ induces an abstract interpretation together with its adjoint universal abstraction $\alpha^{\forall}_M : \wp(Traces) \longrightarrow \wp(States)$ defined by

$$\alpha^{\forall}_M(T) = \{s \in S \mid \text{ for any trace } \langle i, \sigma\rangle \in Traces_M, \text{ if } \sigma_i = s \text{ then } \langle i, \sigma\rangle \in T\}.$$

This abstract interpretation systematically induces a state-based semantics $[\![\cdot]\!]^{\forall}_{\mathrm{state}} : \widehat{\mu} \longrightarrow \wp(States)$. For example, for an atomic proposition p,

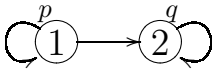
$$\begin{aligned} [\![p]\!]^{\forall}_{\mathrm{state}} &\stackrel{\mathrm{def}}{=} \alpha^{\forall}_M([\![p]\!]_{\mathrm{trace}}) \\ [\![\mathrm{AX}p]\!]^{\forall}_{\mathrm{state}} &\stackrel{\mathrm{def}}{=} \alpha^{\forall}_M \circ \mathbf{X} \circ \gamma^{\forall}_M([\![p]\!]^{\forall}_{\mathrm{state}}) = \widetilde{\mathrm{pre}}_{\rightarrow}([\![p]\!]^{\forall}_{\mathrm{state}}) \end{aligned}$$

where $\mathbf{X}$ is the next-time transformer on traces and $\widetilde{\mathrm{pre}}_{\rightarrow}$ is the standard "universal pre" transformer of states w.r.t. the transition relation $\rightarrow$ of the model M. The abstract interpretation approach ensures that $[\![\cdot]\!]^{\forall}_{\mathrm{state}}$ is sound by construction with respect to the trace semantics: for any $\phi \in \widehat{\mu}$,

$$[\![\phi]\!]^{\forall}_{\mathrm{state}} \subseteq \alpha^{\forall}_M([\![\phi]\!]_{\mathrm{trace}}).$$

However, as proved in [10], this inclusion may be strict meaning that state-based model checking of the $\widehat{\mu}$-calculus is trace-incomplete, namely the above equivalence $(*)$ does not hold. Let us recall an example of incompleteness from [10].

Example 1.1 Consider the following minimal transition system M:



and consider the linear formula $\phi = \mathrm{G}p \vee \mathrm{FG}q$. We have that:

$$\begin{aligned}
[\![\mathrm{G}p]\!]_{\mathrm{trace}} &= \{\langle i,\sigma\rangle \in \mathit{Traces}_M \mid \forall j \geq i.\, \langle j,\sigma\rangle \in [\![p]\!]_{\mathrm{trace}}\} \\
&= \{\langle i, \cdots 1\,1\,1\,\cdots\rangle \in \mathit{Traces}_M \mid i \in \mathbb{Z}\} \\
[\![\mathrm{FG}q]\!]_{\mathrm{trace}} &= \{\langle i,\sigma\rangle \in \mathit{Traces}_M \mid \exists j \geq i.\, \forall k \geq j.\, \langle k,\sigma\rangle \in [\![p]\!]_{\mathrm{trace}}\} \\
&= \{\langle i, \cdots 1\,1\,1\,2\,2\,2\cdots\rangle \in \mathit{Traces}_M \mid i \in \mathbb{Z}\} \\
&\quad \cup \{\langle i, \cdots 2\,2\,2\,\cdots\rangle \in \mathit{Traces}_M \mid i \in \mathbb{Z}\}.
\end{aligned}$$

Thus, $[\![\phi]\!]_{\mathrm{trace}} = \mathit{Traces}_M$, so that $\alpha^{\forall}_M([\![\phi]\!]_{\mathrm{trace}}) = \{1,2\}$. On the other hand, we have that the state semantics $[\![\phi]\!]^{\forall}_{\mathrm{state}}$ is given by the state semantics of the CTL formula $\phi_\forall = \mathrm{AG}p \vee \mathrm{AFAG}q$. Thus, it turns out that $[\![\phi]\!]^{\forall}_{\mathrm{state}} = \{2\}$ because in M: (i) it is possible to jump from state 1 to state 2 so that $[\![\mathrm{AG}p]\!]_{\mathrm{state}} = \varnothing$ and (ii) it is possible to stay forever in state 1 so that $[\![\mathrm{AFAG}q]\!]_{\mathrm{state}} = \{2\}$. Hence,

$$M, 1 \models_{\mathrm{trace}} \phi \quad \text{while} \quad M, 1 \not\models_{\mathrm{state}} \phi$$

that is, universal state-based model checking for ϕ is trace-incomplete. □

The same phenomenon holds even for standard, i.e. partition-based [6,7], or generic, i.e. abstract domain-based [10,13,21,22], abstract model checking where the abstraction map actually is a state-abstraction and can be modeled as a further abstract interpretation step of $[\![\cdot]\!]_{\mathrm{state}}$. 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 $[\![\cdot]\!]_{\mathrm{state}}$ which is complete for the trace-based semantics $[\![\cdot]\!]_{\mathrm{trace}}$.

Complete Core and Shell. Our main goal is that of isolating the least refinements and abstractions of state-based model checking, i.e. of $\wp(\mathit{States})$ viewed as abstract domain of $\wp(\mathit{Traces})$ through the universal abstraction $\alpha^{\forall}_M$, which are trace-complete.

Let us recall that an abstract domain $A = \alpha(\mathit{Concrete})$ together with an abstract semantics $f^\sharp : A \to A$ is *complete* for a semantic function $f : \mathit{Concrete} \to \mathit{Concrete}$ when $\alpha(f(c)) = f^\sharp(\alpha(c))$ holds for any concrete c. Thus, completeness means that abstract computations by $f^\sharp$ are as precise as possible in the abstract domain A. Giacobazzi et al. [12] observed that completeness actually depends on the abstract domain A only, because it is enough to consider the best correct approximation $\alpha \circ f \circ \gamma$ of f as abstract semantics. Thus, it turns out that completeness is an abstract domain property: A is complete for f iff the equation $\alpha \circ f = \alpha \circ f \circ \gamma \circ \alpha$ holds. Hence, this opens up the key question of making an abstract interpretation complete by minimally extending or restricting the underlying abstract domain. Following the terminology in [12], we call *complete shell/core* of A the most abstract/concrete domain, when this exists, which refines/abstracts A and is complete for f. Thus, complete shells add to an abstract domain the *minimal* amount of information in order to make it complete, while

complete cores act in the opposite direction by removing the minimal amount of information in order to achieve completeness. As shown in [12], complete cores always exist, while complete shells exist under the weak hypothesis that the concrete semantics f is Scott-continuous. Furthermore, complete cores and shells enjoy a constructive fixpoint characterization. While it should be clear that completeness could be achieved by refining abstract domains, perhaps it is somehow surprising that also by removing information from an abstract domain one could obtain the completeness property. In this case the abstraction is intended to remove from an incomplete abstract domain exactly the source of incompleteness. Let us consider a simple example to illustrate this. Consider the following abstract domain of signs $\mathit{Sign}^+ \stackrel{\text{def}}{=} \{\mathbb{Z}, [0,+\infty], [-\infty,0], [0,9], [0]\}$, which additionally to sign information also represents precisely the interval $[0,9]$. It turns out that Sign^+ is not complete for integer multiplication: for example, 2×3 is approximated in Sign^+ by $[0,9]$ while the abstract multiplication $\alpha_{\mathit{Sign}^+}(2) \times^{\mathit{Sign}^+} \alpha_{\mathit{Sign}^+}(3)$ gives $[0,+\infty]$. However, $\mathit{Sign} = \{\mathbb{Z}, [0,+\infty], [-\infty,0], [0]\}$, which is an abstraction of Sign^+, turns out to be complete for multiplication. Even more, Sign is the most concrete domain which abstracts Sign^+ and is complete for multiplication, namely Sign is the complete core of Sign^+ for multiplication. Hence, the complete core isolated and removed from Sign^+ the abstract value $[0,9]$, which was the unique source of incompleteness for integer multiplication.

Main Results. We characterize the complete core and shell of the universal state domain $\wp(\mathit{States})$ for all the trace transformers of the $\widehat{\mu}$-calculus which are sources of incompleteness: negation, next-time, time-reversal and disjunction. We also characterize the structure of transition systems such that universal state-based model checking is complete for next-time and time-reversal. In particular, disjunction turns out to be the crucial connective. In fact, the trace-complete shell of the universal state domain for the disjunction operation is (essentially) the domain of traces itself, while the trace-complete core is the trivial abstraction of states carrying no information at all. Let us point out that one remarkable feature of our abstract interpretation-based approach lies in the fact that it is fully constructive, namely we exploit general abstract interpretation results that always provide complete cores and shells in fixpoint form.

On the basis of this analysis, we show that for the $\widehat{\mu}$-calculus:

(1) The most abstract refinement of the domain of states that induces a trace-complete model checking results to be the domain of traces itself.
(2) The straightforward abstraction to a noninformative singleton is the unique abstraction of the domain of states (and hence of the domain of traces) which induces a trace-complete model checking.
(3) For each basic temporal/logical operator of the $\widehat{\mu}$-calculus we constructively characterize the complete core and shell of the state abstraction for traces. These

results provide the basis for isolating fragments of the $\widehat{\mu}$-calculus which have nonstraightforward trace-complete shells and cores of states.

These results prove 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 for the entire $\widehat{\mu}$-calculus, emphasizing the intrinsic limits of precision of state-based model checking with respect to the trace-based semantics. Moreover, since abstract model checking can be viewed as abstract interpretation of $[\![\cdot]\!]_{\mathrm{state}}$ (cf. [10]), this also implies that any abstract model checking is intrinsically incomplete with respect to the trace-semantics of the $\widehat{\mu}$-calculus.

2 Abstract Interpretation and Model Checking

2.1 Notation

If X is any set then $\mathrm{Cl}^{\cap}, \mathrm{Cl}^{\cup} : \wp(\wp(X)) \to \wp(\wp(X))$ denote, respectively, the operators that close any subset $Y \in \wp(\wp(X))$ under arbitrary intersections and unions, e.g. $\mathrm{Cl}^{\cap}(Y) \stackrel{\mathrm{def}}{=} \{\cap S \mid S \subseteq Y\}$. Note that $X \in \mathrm{Cl}^{\cap}(Y)$ and $\varnothing \in \mathrm{Cl}^{\cup}(Y)$ because $X = \cap\varnothing$ and $\varnothing = \cup\varnothing$. If $S \subseteq X$ then $\neg S$ denotes the complement of S in X.

A poset P w.r.t. a partial ordering $\leq$ is denoted by $\langle P, \leq\rangle$ or $P_{\leq}$. We use the symbol $\sqsubseteq$ to denote pointwise ordering between functions: if X is any set, $P_{\leq}$ a poset, and $f, g : X \to P$ then $f \sqsubseteq g$ if for all $x \in X$, $f(x) \leq g(x)$. If P is a poset and $X \subseteq P$ then $\max(X) \stackrel{\mathrm{def}}{=} \{x \in X \mid \forall y \in X.\, x \leq y \Rightarrow x = y\}$. We denote by $\mathrm{lfp}(f)$ and $\mathrm{gfp}(f)$ (or by $\mathrm{lfp}^{\leq}(f)$ and $\mathrm{gfp}^{\leq}(f)$ to emphasize the partial ordering $\leq$), respectively, the least and greatest fixpoints, when they exist, of an operator $f : P \to P$ on a poset $P_{\leq}$. It is well known that if $\langle C, \leq, \vee, \wedge, \top, \bot\rangle$ is a complete lattice (actually, a CPO would be enough) and $f : C \to C$ is monotone then both $\mathrm{lfp}(f)$ and $\mathrm{gfp}(f)$ exist and the following characterizations hold:

$$\mathrm{lfp}(f) = \wedge\{x \in C \mid f(x) \leq x\}, \qquad \mathrm{gfp}(f) = \vee\{x \in C \mid x \leq f(x)\}.$$

It also well known that if f is continuous — i.e. f preserves lub's of directed subsets or, equivalently, of ascending chains — then $\mathrm{lfp}(f) = \vee_{i\in\mathbb{N}} f^i(\bot)$, where the sequence $\{f^i(x)\}_{i\in\mathbb{N}}$, for any $x \in C$, is inductively defined by $f^0(x) \stackrel{\mathrm{def}}{=} x$ and $f^{i+1}(x) \stackrel{\mathrm{def}}{=} f(f^i(x))$. Dually, if f is co-continuous then $\mathrm{gfp}(f) = \wedge_{i\in\mathbb{N}} f^i(\top)$. A function $f : C \to C$ is (finitely) additive when f preserves lub's of (finite) arbitrary subsets of C, while co-additivity is dually defined.

2.2 Abstract interpretation and completeness

2.2.1 The lattice of abstract domains

In standard abstract interpretation [8,9], abstract domains can be equivalently specified either by Galois connections/insertions (GCs/GIs) or by (upper) closure operators (uco's). These two approaches are equivalent, modulo isomorphic representations of domain's objects. The closure operator approach enjoys the advantage of being independent from the representation of domain's objects because an abstract domain is given as a function on the concrete domain of computation. This feature makes closures appropriate for reasoning on abstract domains independently from their representation. Given a complete lattice $C_{\leq}$, playing the role of concrete domain, recall that $\rho : C \to C$ is a uco when ρ is monotone, idempotent and extensive (viz. $x \leq \rho(x)$). We denote by $\mathrm{uco}(C)$ the set of uco's on C. Let us recall that each $\rho \in \mathrm{uco}(C)$ is uniquely determined by the set of its fixpoints, which is its image, i.e. $\mathrm{img}(\rho) = \{x \in C \mid \rho(x) = x\}$, because $\rho = \lambda x. \wedge \{y \in C \mid y \in \mathrm{img}(\rho),\, x \leq y\}$. Moreover, a subset $X \subseteq C$ is the set of fixpoints of some uco on C iff X is meet-closed, i.e. $X = \mathcal{M}(X) \stackrel{\text{def}}{=} \{\wedge Y \mid Y \subseteq X\}$ (note that $\top_C = \wedge\varnothing \in \mathcal{M}(X)$). Note that when $C = \wp(S)_{\subseteq/\supseteq}$, for some set S, then $\mathcal{M} = \mathrm{Cl}^{\cap}/\mathrm{Cl}^{\cup}$. Often, we will identify closures with their sets of fixpoints. This does not give rise to ambiguity, since one can distinguish their use as functions or sets according to the context. It is well known that $\mathrm{uco}(C)$ endowed with the pointwise ordering $\sqsubseteq$ gives rise to the complete lattice $\langle \mathrm{uco}(C), \sqsubseteq, \sqcup, \sqcap, \lambda x.\top, \mathrm{id}\rangle$. It turns out that the pointwise ordering between uco's corresponds to superset ordering of the corresponding sets of fixpoints, i.e., $\rho \sqsubseteq \mu$ iff $\mathrm{img}(\mu) \subseteq \mathrm{img}(\rho)$. Let us also recall that for any $\rho \in \mathrm{uco}(C)$ and $X \subseteq C$, $\rho(\vee X) = \rho(\vee_{x\in X}\rho(x))$, and for any set of closures $\{\rho_i\}_{i\in I} \subseteq \mathrm{uco}(C)$:

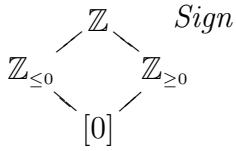
$$\sqcup_{i\in I}\rho_i = \cap_{i\in I}\rho_i; \qquad \sqcap_{i\in I}\rho_i = \mathcal{M}(\cup_{i\in I}\rho_i); \qquad \sqcap_{i\in I}\rho_i = \lambda x.\, \wedge_{i\in I}\, \rho_i(x).$$

We denote by (α, C, A, γ) a GC/GI of the abstract domain A into the concrete domain C through the abstraction and concretization maps $\alpha : C \to A$ and $\gamma : A \to C$. Thus, it is required that α and γ form an adjunction between C and A: $\alpha(c) \leq_C a \Leftrightarrow a \leq_A \gamma(a)$. The map α (γ) is called the left (right) adjoint of γ (α). Let us recall that it is enough to specify either the abstraction or the concretization map because in any GC the left/right adjoint map uniquely determines the right/left adjoint map: on the one hand, any $\alpha : C \to A$ admits a necessarily unique right adjoint $\gamma : A \to C$ defined by $\gamma(a) = \vee_C\{c \in C \mid \alpha(c) \leq_A a\}$ iff α is additive; on the other hand, any $\gamma : A \to C$ admits a necessarily unique left adjoint $\alpha : C \to A$ defined by $\alpha(c) = \wedge_A\{a \in A \mid c \leq_C \gamma(a)\}$ iff γ is co-additive. Recall that a GC is a GI when α is onto or, equivalently, γ is 1-1. In abstract interpretation terms, this means that A does not contain useless abstract values, namely objects in A which are not abstractions of some concrete object in C. Let us recall that $\rho_A \stackrel{\text{def}}{=} \gamma\circ\alpha$ is the uco corresponding to the GC (α, C, A, γ) and, conversely, any $\rho \in \mathrm{uco}(C)$ induces a GI $(\rho, C, \mathrm{img}(\rho), \mathrm{id})$. Moreover, these two constructions are one the inverse of

each other. By this equivalence, throughout the paper, $\langle \mathrm{uco}(C), \sqsubseteq \rangle$ will play the role of the (complete) lattice of abstract domains of the concrete domain C. The pointwise ordering on $\mathrm{uco}(C)$ corresponds to the standard order used to compare abstract domains with regard to their precision: $A_1 \sqsubseteq A_2$ in $\mathrm{uco}(C)$ encodes the fact that A_1 is more precise or concrete than A_2 or, equivalently, A_2 is less precise or more abstract than A_1; in this case, we also say that A_1 is a refinement of A_2 and A_2 is a simplification or abstraction of A_1. Lub's and glb's on $\mathrm{uco}(C)$ have therefore the following reading as operators on abstract domains. Let $\{A_i\}_{i \in I} \subseteq \mathrm{uco}(C)$: (i) $\sqcup_{i \in I} A_i$ is the most concrete among the domains which are abstractions of all the A_i's; (ii) $\sqcap_{i \in I} A_i$ is the most abstract among the domains which are more concrete than every A_i — this domain is also known as reduced product of all the A_i's.

2.2.2 Complete abstract domains

Let (α, C, A, γ) be a GI, $f : C \to C$ be some concrete semantic function — for simplicity of notation, we consider here unary functions — and $f^\sharp : A \to A$ be a corresponding abstract semantic function. Then, $\langle A, f^\sharp \rangle$ is a sound abstract interpretation, or $f^\sharp$ is a correct approximation of f on A, when $\alpha \circ f \sqsubseteq f^\sharp \circ \alpha$. The abstract function $f^A \stackrel{\mathrm{def}}{=} \alpha \circ f \circ \gamma : A \to A$ is called the best correct approximation of f in A. Completeness in abstract interpretation [8,12] corresponds to require the following strengthening of soundness: $\alpha \circ f = f^\sharp \circ \alpha$. Hence, in addition to soundness, completeness corresponds to require that no loss of precision is introduced by the abstract function $f^\sharp$ on an approximation $\alpha(c)$ of a concrete object $c \in C$ with respect to approximating by α the concrete computation $f(c)$. As a very simple example, let us consider again the following abstract domain $Sign$ representing the sign of an integer variable.



Let us also consider the binary concrete operations of integer addition and multiplication, pointwise lifted to sets of integers in $\wp(\mathbb{Z})$, e.g., $X + Y = \{x + y \mid x \in X,\, y \in Y\}$. Hence, it turns out that the best correct approximation $+^{Sign}$ on $Sign$ of integer addition is sound but not complete because $\alpha(\{-1\} + \{1\}) = \alpha(\{0\}) = [0] <_{Sign} \mathbb{Z} = \mathbb{Z}_{\leq 0} +^{Sign} \mathbb{Z}_{\geq 0} = \alpha(\{-1\}) +^{Sign} \alpha(\{1\})$. On the other hand, it is immediate to note that the best correct approximation of integer multiplication is instead complete.

Let us also recall that, by a well-known result (see, e.g., [9, Theorem 7.1.0.4] and [10, Section 6]) completeness lifts to least fixpoints, i.e., if $\langle A, f^\sharp \rangle$ is complete then $\alpha(\mathrm{lfp}(f)) = \mathrm{lfp}(f^\sharp)$. Completeness is an abstract domain property because it only depends on the abstract domain: in fact, it turns out that $\langle A, f^\sharp \rangle$ is complete iff

$\langle A, f^A\rangle$ is complete. Thus, completeness can be equivalently stated as a property of closures: A is complete iff $\alpha \circ f = f^A \circ \alpha$ iff $\gamma \circ \alpha \circ f = \gamma \circ \alpha \circ f \circ \gamma \circ \alpha$. Thus, for abstract domains specified as closure operators, an abstract domain $\rho \in \mathrm{uco}(C)$ is defined to be complete for f if $\rho \circ f = \rho \circ f \circ \rho$. More in general, the definition of completeness is extended to any set F of semantic functions by requiring completeness for each $f \in F$. Throughout the paper, we will adopt the following notation: $\Gamma(C, f) \stackrel{\mathrm{def}}{=} \{\rho \in \mathrm{uco}(C) \mid \rho \text{ is complete for } f\}$, so that for a set F, $\Gamma(C, F) = \cap_{f\in F}\Gamma(C, f)$. The following property will be useful later on.

$$\rho \in \Gamma(C, f) \quad \text{iff} \quad \rho \in \Gamma(C, \{f^n\}_{n\in\mathbb{N}}) \tag{$*$}$$

In fact, let us show by induction on $n \in \mathbb{N}$ that if $\rho \in \Gamma(C, f)$ then for any $n \in \mathbb{N}$, $\rho \in \Gamma(C, f^n)$. The case $n = 0$ amounts to $\rho \in \Gamma(C, \lambda x.x)$ which is trivially true. For $n+1$ we have that: $\rho\circ f^{n+1} =$ (since $\rho \in \Gamma(C, f)$) $= \rho\circ f\circ\rho\circ f^n =$ (by inductive hypothesis) $= \rho\circ f\circ\rho\circ f^n\circ\rho =$ (since $\rho \in \Gamma(C, f)$) $= \rho\circ f\circ f^n\circ\rho = \rho\circ f^{n+1}\circ\rho$.

Let us also recall how completeness lifts to least/greatest fixpoints for abstract domains specified by uco's. If $\rho \in \Gamma(C, f)$, where f is monotone, then $\mathrm{lfp}(\rho \circ f) = \rho(\mathrm{lfp}(f))$. Moreover, if either ρ does not contain infinite descending chains or ρ is co-continuous then this also holds for greatest fixpoints, namely $\mathrm{gfp}(\rho \circ f) = \rho(\mathrm{gfp}(f))$.

2.2.3 Complete core and shell

The fact that completeness is an abstract domain property opens the question of making an abstract interpretation complete by minimally extending or, dually, restricting the underlying abstract domain. Following [12], given a set of concrete semantic functions $F \subseteq C \to C$ and an abstract domain $A \in \mathrm{uco}(C)$, the *complete shell* (respectively, *core*) of A for F, when it exists, is the most abstract (respectively, concrete) domain $A^s \in \mathrm{uco}(C)$ (respectively, $A^c \in \mathrm{uco}(C)$) which extends (respectively, restricts) A and is complete for F. In other terms, the 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. Complete shell and core of A for F are denoted, respectively, by $\mathrm{Shell}_F(A)$ and $\mathrm{Core}_F(A)$. Thus, a complete shell $\mathrm{Shell}_F(A)$ exists when $\sqcup\{A' \in \mathrm{uco}(C) \mid A' \sqsubseteq A,\ A' \in \Gamma(C, F)\} \in \Gamma(C, F)$, while a complete core $\mathrm{Core}_F(A)$ exists when $\sqcap\{A' \in \mathrm{uco}(C) \mid A \sqsubseteq A',\ A' \in \Gamma(C, F)\} \in \Gamma(C, F)$.

These problems were solved by Giacobazzi et al. [12] who gave a constructive characterization of complete shells and cores. Given a set of functions $F \subseteq C \to C$, the abstract domain transformers $L_F, R_F : \mathrm{uco}(C) \to \mathrm{uco}(C)$ are defined as

follows:

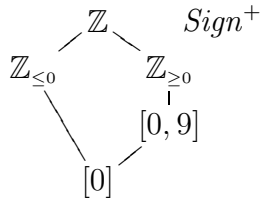
$$L_F(\eta) \stackrel{\text{def}}{=} \{y \in C \mid \cup_{f\in F} \max(\{x \in C \mid f(x) \leq y\}) \subseteq \eta\}$$
$$R_F(\eta) \stackrel{\text{def}}{=} \mathcal{M}(\cup_{f\in F, y\in\eta} \max(\{x \in C \mid f(x) \leq y\})).$$

Theorem 2.1 (Giacobazzi et al. [12]) *Let F be a set of continuous functions and $\rho \in \mathrm{uco}(C)$. Then, $\rho \in \Gamma(C, F)$ iff $L_F(\rho) \sqsubseteq \rho$ iff $\rho \sqsubseteq R_F(\rho)$. Moreover, the complete shell and core of ρ for F exist and are constructively characterized as follows:*

$$\mathrm{Shell}_F(\rho) = \sqcap_{i\in\mathbb{N}} R_F^i(\rho), \qquad \mathrm{Core}_F(\rho) = \sqcup_{i\in\mathbb{N}} L_F^i(\rho).$$

Thus, the complete shell of ρ for F can be obtained by iteratively adding to ρ the image of the transformer R_F on the current domain, while the complete core can be obtained by iteratively removing from ρ the elements that are not in the image of the transformer L_F on the current domain.

Example 2.2 Let us consider again the abstract domain $Sign^+$ which abstracts $\wp(\mathbb{Z})_\subseteq$ and the square operation on sets of integers $sq : \wp(\mathbb{Z}) \to \wp(\mathbb{Z})$ defined by $sq(X) = \{x^2 \mid x \in X\}$.



It turns out that $Sign^+$ is not complete for sq: in fact, $\rho_{Sign^+}(sq(\rho_{Sign^+}([0, 3]))) = \rho_{Sign^+}(sq([0, 9])) = \mathbb{Z}$, while $\rho_{Sign^+}(sq([0, 3])) = \rho_{Sign^+}(\{0, 1, 4, 9\}) = [0, 9]$. Theorem 2.1 tells us that the abstract element $[0, 9]$ is a source of incompleteness: in fact, we have that $\max(\{X \in \wp(\mathbb{Z}) \mid sq(X) \subseteq [0, 9]\}) = [-3, 3] \notin \rho_{Sign^+}$ so that $R_{sq}(\rho_{Sign^+}) \not\subseteq \rho_{Sign^+}$. Moreover, $[0, 9]$ is the unique source of incompleteness in $Sign^+$ because:

$$\max(\{X \in \wp(\mathbb{Z}) \mid sq(X) \subseteq \mathbb{Z}\}) = \mathbb{Z} \in \rho_{Sign^+}$$
$$\max(\{X \in \wp(\mathbb{Z}) \mid sq(X) \subseteq \mathbb{Z}_{\leq 0}\}) = \{0\} \in \rho_{Sign^+}$$
$$\max(\{X \in \wp(\mathbb{Z}) \mid sq(X) \subseteq \mathbb{Z}_{\geq 0}\}) = \mathbb{Z} \in \rho_{Sign^+}$$
$$\max(\{X \in \wp(\mathbb{Z}) \mid sq(X) \subseteq \{0\}\}) = \{0\} \in \rho_{Sign^+}$$

Thus, by Theorem 2.1, we have that $\mathrm{Core}_{sq}(Sign^+) = Sign$. □

When $f : C \to C$ is merely monotone, in general the complete shell of an abstract domain for f may not exist, while the complete core of an abstract domain for f

always exists even if it cannot be constructively characterized by Theorem 2.1.

Remark 2.3 Let F be a set of additive functions. Then, any $F \ni f : C \to C$ admits a right adjoint $f^r : C \to C$ defined by $f^r(y) = \vee\{x \in C \mid f(x) \leq y\}$. In this case, the above operators L_F and R_F can be simplified as follows:

$$L_F(\eta) = \{y \in C \mid \{f^r(y) \mid f \in F\} \subseteq \eta\}; \quad R_F(\eta) = \mathfrak{M}(\{f^r(y) \mid y \in \eta,\ f \in F\}).$$

2.3 Temporal abstract interpretation

Let us recall the basic notions and definitions of Cousot and Cousot's [10] temporal abstract interpretation framework (see also Schimdt's paper [24]). $\mathbb{S}$ is any 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: $\mathbb{P} \stackrel{\text{def}}{=} \mathbb{Z} \to \mathbb{S}$ is the set of paths. As usual, an execution path with an initial state s can be encoded by repeating forever in the past the state s. Traces keep track of present time, so that $\mathbb{T} \stackrel{\text{def}}{=} \mathbb{Z} \times \mathbb{P}$ is defined to be the set of traces. We denote by $\sigma_i \in \mathbb{S}$ the present state of a trace $\langle i, \sigma\rangle \in \mathbb{T}$. The trace-semantics of a temporal formula ϕ will be a temporal model, namely the set of traces making ϕ true.

Temporal models will be generated by transition systems or Kripke structures, encoding some reactive system. The transition relation $\to \subseteq \mathbb{S} \times \mathbb{S}$ is assumed to be (backward and forward) total, i.e., $\forall s \in \mathbb{S}.\exists s' \in \mathbb{S}.\, s \to s'$ and $\forall s' \in \mathbb{S}.\exists s \in \mathbb{S}.\, s \to s'$. This is not restrictive, since any transition relation can be lifted to a total transition relation by adding transitions $s \to s$ for any state s which is not reachable (i.e., an initial state) or which cannot reach any state (i.e., a final state). The model generated by a transition system $\langle \mathbb{S}, \to\rangle$ is therefore defined as $\mathscr{M}_\to \stackrel{\text{def}}{=} \{\langle i, \sigma\rangle \in \mathbb{T} \mid i \in \mathbb{Z},\ \forall k \in \mathbb{Z}.\ \sigma_k \to \sigma_{k+1}\}$. The pre/post transformers on $\wp(\mathbb{S})$ induced by $\langle \mathbb{S}, \to\rangle$ are defined as usual:

- $\mathrm{pre}_\to(Y) \stackrel{\text{def}}{=} \{a \in \mathbb{S} \mid \exists b \in Y.\ a \to b\}$;
- $\widetilde{\mathrm{pre}}_\to(Y) \stackrel{\text{def}}{=} \neg(\mathrm{pre}_\to(\neg Y)) = \{a \in \mathbb{S} \mid \forall b \in \mathbb{S}.(a \to b \Rightarrow b \in Y)\}$;
- $\mathrm{post}_\to(Y) \stackrel{\text{def}}{=} \{b \in \mathbb{S} \mid \exists a \in Y.\ a \to b\}$;
- $\widetilde{\mathrm{post}}_\to(Y) \stackrel{\text{def}}{=} \neg(\mathrm{post}_\to(\neg Y)) = \{b \in \mathbb{S} \mid \forall a \in \mathbb{S}.(a \to b \Rightarrow a \in Y)\}$.

The forward closure $\mathrm{Fd} : \wp(\mathbb{T}) \to \wp(\mathbb{T})$ is defined as $\mathrm{Fd}(X) \stackrel{\text{def}}{=} \{\langle i, \sigma\rangle \in \mathbb{T} \mid \exists \langle i, \tau\rangle \in X.\forall j \geq i.\, \sigma_j = \tau_j\}$. Dually, $\mathrm{Bd}(X) \stackrel{\text{def}}{=} \{\langle i, \sigma\rangle \in \mathbb{T} \mid \exists \langle i, \tau\rangle \in X.\forall j \leq i.\, \sigma_j = \tau_j\}$ is the backward closure of $X \in \wp(\mathbb{T})$. A set of traces X is forward (backward) closed when $\mathrm{Fd}(X) = X$ ($\mathrm{Bd}(X) = X$), while X is state closed when X is both forward and backward closed. Thus, X is forward (backward) closed when the past (future) does not matter, while X is state closed when the present only matters.

The reversible $\widehat{\mu t}$-calculus was introduced by Cousot and Cousot [10] as a past and future time-symmetric generalization of the μ-calculus, with a trace-based semantics. Formulae ϕ of the reversible $\widehat{\mu t}$-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 $S \in \wp(\mathbb{S})$, $t \in \wp(\mathbb{S} \times \mathbb{S})$ and $X \in \mathbb{X}$, for an infinite set $\mathbb{X}$ of logical variables. The set of $\widehat{\mu t}$-calculus formulae is denoted by $\mathfrak{L}_{\widehat{\mu}}$.

Let us give the intuition for the operators of the $\widehat{\mu t}$-calculus. $\boldsymbol{\sigma}_S$ stands for a state atomic proposition which holds in traces whose present state is in S. $\boldsymbol{\pi}_t$ stands for a transition atomic proposition which holds in traces whose next step is a transition in t. $\curvearrowleft$ is time-reversal that allows to express past/future time modalities from corresponding future/past time modalities. $\oplus$ is the linear temporal next operator (usually denoted by X). Finally, $\forall$ is a generalized universal quantification with two arguments.

Let us recall the trace-semantics for the $\widehat{\mu t}$-calculus. $\mathbb{E} \stackrel{\text{def}}{=} \mathbb{X} \to \wp(\mathbb{T})$ denotes the set of environments over $\mathbb{X}$. Given $\xi \in \mathbb{E}$, $X \in \mathbb{X}$ and $N \in \wp(\mathbb{T})$, $\xi[X/N] \in \mathbb{E}$ is the environment that acts as ξ in $\mathbb{X} \smallsetminus \{X\}$ and maps X to N. The $\widehat{\mu t}$-calculus semantics $[\![\cdot]\!] : \mathfrak{L}_{\widehat{\mu}} \to \mathbb{E} \to \wp(\mathbb{T})$ is inductively and partially — because least or greatest fixpoints could not exist — defined as follows:

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

where the corresponding temporal transformers are defined as follows:

- For any $S \in \wp(\mathbb{S})$, $\boldsymbol{\sigma}_{\{\!|S|\!\}} \stackrel{\text{def}}{=} \{\langle i, \sigma\rangle \in \mathbb{T} \mid \sigma_i \in S\}$ is the S-state model, i.e., the set of traces whose current state belongs to S.
- For any $t \in \wp(\mathbb{S} \times \mathbb{S})$, $\boldsymbol{\pi}_{\{\!|t|\!\}} \stackrel{\text{def}}{=} \{\langle i, \sigma\rangle \in \mathbb{T} \mid (\sigma_i, \sigma_{i+1}) \in t\}$ is the t-transition model, i.e., the set of traces whose next step is a t-transition.
- $\oplus : \wp(\mathbb{T}) \to \wp(\mathbb{T})$ is the next-time or predecessor transformer:
  $\oplus(X) \stackrel{\text{def}}{=} \{\langle i-1, \sigma\rangle \in \mathbb{T} \mid \langle i, \sigma\rangle \in X\} = \{\langle i, \sigma\rangle \in \mathbb{T} \mid \langle i+1, \sigma\rangle \in X\}$.
- ${\curvearrowleft} : \wp(\mathbb{T}) \to \wp(\mathbb{T})$ is the reversal transformer:
  ${\curvearrowleft}(X) \stackrel{\text{def}}{=} \{\langle -i, \lambda k.\sigma_{-k}\rangle \in \mathbb{T} \mid \langle i, \sigma\rangle \in X\}$.
- $\neg : \wp(\mathbb{T}) \to \wp(\mathbb{T})$ is the complement:
  $\neg X \stackrel{\text{def}}{=} \mathbb{T} \smallsetminus X$.
- Given $s \in \mathbb{S}$, $(\cdot)_{\downarrow s} : \wp(\mathbb{T}) \to \wp(\mathbb{T})$ is the state projection operator:
  $X_{\downarrow s} \stackrel{\text{def}}{=} \{\langle i, \sigma\rangle \in X \mid \sigma_i = s\}$.

– $\forall : \wp(\mathbb{T}) \times \wp(\mathbb{T}) \to \wp(\mathbb{T})$ is the universal quantifier:
$\forall(X, Y) \stackrel{\text{def}}{=} \{\langle i, \sigma\rangle \in X \mid X_{\downarrow\sigma_i} \subseteq Y\}$.

If $\phi \in \mathfrak{L}_{\overset{\frown}{\mu}}$ is a closed formula then the semantics $[\![\phi]\!]\xi$ is independent from the environment ξ and thus we simply write $[\![\phi]\!]$.

The time-reversal operator of the $\overset{\frown}{\mu}$-calculus allows to express both backward and forward time modalities. Standard linear and branching temporal specification languages like (past and future) LTL, linear μ-calculus, CTL*, CTL, etc., can all be expressed as suitable fragments of the $\overset{\frown}{\mu}$-calculus, since the standard missing operators can be defined as derived operators. Let us see some examples.

– Previous-time (or successor) $\ominus$: $\ominus(X) \stackrel{\text{def}}{=} \curvearrowleft(\oplus(\curvearrowright(X))) = \{\langle i{+}1, \sigma\rangle \in \mathbb{T} \mid \langle i, \sigma\rangle \in X\} = \{\langle i, \sigma\rangle \in \mathbb{T} \mid \langle i-1, \sigma\rangle \in X\}$.

– Forward sometime (or finally) F: $\mathbf{F}(X) \stackrel{\text{def}}{=} \text{lfp}(\lambda Y \in \wp(\mathbb{T}).X \cup \oplus(Y)) = \cup_{n\in\mathbb{N}}\oplus^n(X)$.

– Forward globally G: $\mathbf{G}(X) \stackrel{\text{def}}{=} \text{gfp}(\lambda Y \in \wp(\mathbb{T}).X \cap \oplus(Y)) = \cap_{n\in\mathbb{N}}\oplus^n(X)$.

– Backward sometime F$_-$: $\mathbf{F}_-(X) \stackrel{\text{def}}{=} \curvearrowleft(\mathbf{F}(\curvearrowright(X))) = \cup_{n\in\mathbb{N}}\ominus^n(X)$.

– Backward globally G$_-$: $\mathbf{G}_-(X) \stackrel{\text{def}}{=} \curvearrowleft(\mathbf{G}(\curvearrowright(X))) = \cap_{n\in\mathbb{N}}\ominus^n(X)$.

Thus, traces in a model $\mathscr{M}_{\rightarrow}$ can be defined as $\boxplus\boldsymbol{\pi}_{\rightarrow} \stackrel{\text{def}}{=} \mathrm{G}(\boldsymbol{\pi}_{\rightarrow}) \wedge \mathrm{G}_-(\boldsymbol{\pi}_{\rightarrow})$, so that $\mathscr{M}_{\rightarrow} = [\![\boxplus\boldsymbol{\pi}_{\rightarrow}]\!]$. Therefore, standard universal quantification in $\mathscr{M}_{\rightarrow}$ can be defined as $\forall\phi \stackrel{\text{def}}{=} \forall\,(\boxplus\boldsymbol{\pi}_{\rightarrow}) : \phi$, while generalized existential quantification is dually defined by $\exists\phi_1 : \phi_2 \stackrel{\text{def}}{=} \neg(\forall\phi_1 : \neg\phi_2)$.

In this framework, the trace-based model checking problem is as follows. Let $\mathscr{M}_{\rightarrow}$ be a model and $\phi \in \mathfrak{L}_{\overset{\frown}{\mu}}$ be a closed temporal specification. Then, the universal (existential) model checking problem consists in determining whether $\mathscr{M}_{\rightarrow} \subseteq [\![\phi]\!]$ ($\mathscr{M}_{\rightarrow} \cap [\![\phi]\!] \neq \varnothing$).

2.4 State-based model checking abstraction

Cousot and Cousot [10] show how states can be viewed as an abstract interpretation of traces through universal or existential checking abstractions. This abstraction from traces to states induces a corresponding state-based model checking problem which is a sound approximation of the concrete trace-based problem.

2.4.1 Universal checking abstraction

For the universal model checking problem, the right notion of approximation is encoded by the superset relation. In fact, if $[\![\cdot]\!]^\sharp$ is an approximated semantics such that

$[\![\phi]\!]^\sharp \subseteq [\![\phi]\!]$ for any ϕ, then the universal abstract verification $\mathscr{M}_\rightarrow \subseteq [\![\phi]\!]^\sharp$ entails the concrete one $\mathscr{M}_\rightarrow \subseteq [\![\phi]\!]$. Thus, $[\![\cdot]\!]^\sharp_1 \subseteq [\![\cdot]\!]^\sharp_2$ means that $[\![\cdot]\!]^\sharp_2$ is a better approximation than $[\![\cdot]\!]^\sharp_1$, so that sets of traces and states are ordered w.r.t. the superset relation: $\langle \wp(\mathbb{T}), \supseteq \rangle$ and $\langle \wp(\mathbb{S}), \supseteq \rangle$ play, respectively, the role of concrete and abstract domain. Let $M \subseteq \mathbb{T}$ be any given model, e.g. generated by a total transition system $\langle \mathbb{S}, \rightarrow \rangle$. Traces can be abstracted to states through the universal quantifier: a set of traces $X \subseteq \mathbb{T}$ is abstracted to the set of states $s \in \mathbb{S}$ such that any trace in the model M whose present state is s belongs to X. Formally, the universal checking abstraction $\alpha^\forall_M : \wp(\mathbb{T}) \rightarrow \wp(\mathbb{S})$ is defined as follows:

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

Thus, $\alpha^\forall_M$ abstracts the trace-semantics $[\![\phi]\!]$ of some temporal specification $\phi \in \hat{\mu t}$ to the set of (present) states s which universally satisfy ϕ, that is, such that any trace of M with present state s satisfies ϕ. This map is onto (by totality of $\rightarrow$) and preserves arbitrary intersections, therefore it induces a a Galois insertion $(\alpha^\forall_M, \wp(\mathbb{T})_\supseteq, \wp(\mathbb{S})_\supseteq, \gamma^\forall_M)$ where $\gamma^\forall_M$ is the right adjoint to $\alpha^\forall_M$. A set of states $S \in \wp(\mathbb{S})$ is viewed through the concretization map $\gamma^\forall_M$ as an abstract representation for the set of traces in M whose present state belongs to S. Hence, the universal concretization $\gamma^\forall_M : \wp(\mathbb{S}) \rightarrow \wp(\mathbb{T})$ is defined as follows:

$$\gamma^\forall_M(S) \stackrel{\text{def}}{=} \{\langle i, \sigma \rangle \in M \mid \sigma_i \in S\}.$$

For our purposes it is helpful to view the universal abstraction $(\alpha^\forall_M, \wp(\mathbb{T})_\supseteq, \wp(\mathbb{S})_\supseteq, \gamma^\forall_M)$ as a closure operator in order to make our analysis independent from specific representations of abstract domains of $\wp(\mathbb{T})$.

Definition 2.4 The *universal checking closure* (or simply universal closure) relative to a model $M \in \wp(\mathbb{T})$ is given by $\rho^\forall_M \stackrel{\text{def}}{=} \gamma^\forall_M \circ \alpha^\forall_M \in \mathrm{uco}(\wp(\mathbb{T})_\supseteq)$. Thus, $\rho^\forall_M = \lambda X.\{\langle i, \sigma \rangle \in M \mid M_{\downarrow \sigma_i} \subseteq X\}$. $\square$

Notice that, due to the superset relation, $\rho^\forall_M(X) \subseteq X$. 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.

Let us observe that, for any $S \in \wp(\mathbb{S})$, $\gamma^\forall_M(S) = \cup_{s \in S} M_{\downarrow s}$ and that the set of fixpoints of $\rho^\forall_M$ can be also characterized as follows:

$$\rho^\forall_M = \{\gamma^\forall_M(S) \mid S \subseteq \mathbb{S}\} \qquad (\ddagger)$$

because $\rho^\forall_M = \{\gamma^\forall_M(\alpha^\forall_M(T)) \mid T \in \mathbb{T}\} = \{\gamma^\forall_M(S) \mid S \in \mathbb{S}\}$.

Example 2.5 Consider the two states transition system in Example 1.1 generating the model $\mathscr{M}_\rightarrow$. Consider the set of traces depicted below where arrows point to

present states:

$$
\begin{aligned}
a = \ & \cdots 1\,1\,1\,\overset{\downarrow}{1}\,1\,1\cdots \\
b = \ & \cdots 1\,1\,1\,\overset{\downarrow}{1}\,1\,1\,1\,2\,2\,2\cdots \\
c = \ & \cdots 1\,1\,1\,2\,2\,2\,\overset{\downarrow}{2}\,2\,2\,2\cdots \\
d = \ & \cdots 2\,2\,2\,\overset{\downarrow}{2}\,2\,2\,2\,1\,1\,1\cdots
\end{aligned}
$$

For the set of traces a and b the arrow moves over 1 while in c and d the arrow moves over 2. Let $X = a \cup b \cup c \cup d$. It turns out that $\rho^{\forall}_{\mathscr{M}_{\rightarrow}}(X) = a \cup b$ because:

– the trace $\cdots\ 2\ 2\ 2\ \overset{\downarrow}{2}\ 2\ 2\ \cdots$ belongs to $(\mathscr{M}_{\rightarrow})_{\downarrow 2}$ but it does not belong to X, so that $c \cap \rho^{\forall}_{\mathscr{M}_{\rightarrow}}(X) = \varnothing$;
– the traces in d do not belong to $\mathscr{M}_{\rightarrow}$, so that $d \cap \rho^{\forall}_{\mathscr{M}_{\rightarrow}}(X) = \varnothing$.

As a further example, let us consider the formula $\oplus p \in \mathfrak{L}_{\overset{\frown}{\mu}}$, where $p = \boldsymbol{\sigma}_1$. We have that $[\![\oplus p]\!] = \bigoplus(\mathscr{M}_{\rightarrow})_{\downarrow 1} = (\mathscr{M}_{\rightarrow})_{\downarrow 1} \smallsetminus \{\langle i, \sigma\rangle \in (\mathscr{M}_{\rightarrow})_{\downarrow 1} \,\big|\, \sigma_{i+1} = 2\}$. Therefore, it turns out that $\rho^{\forall}_{\mathscr{M}_{\rightarrow}}([\![\oplus p]\!]) = \varnothing$. $\square$

In the paper, we will make the following weak assumption on the universal closure.

Hypothesis 2.6 For any universal checking closure $\rho^{\forall}_{M}$, the model $M \in \wp(\mathbb{T})$ is such that (i) for any $s \in \mathbb{S}$, $|M_{\downarrow s}| > 1$ and (ii) $\bigoplus(M) = M = \bigominus(M)$ and $\bigoplus(\curvearrowleft(M)) = \curvearrowleft(M) = \bigominus(\curvearrowleft(M))$. $\square$

Hypothesis (i) means that for any state s, there exist at least two traces in M with present state s, while hypothesis (ii) means that M and its reversal $\curvearrowleft(M)$ are closed for forward and backward time progresses. These conditions are obviously satisfied by any model $\mathscr{M}_{\rightarrow}$ generated by a total transition system $\langle \mathbb{S}, \rightarrow \rangle$.

2.4.2 Existential checking abstraction

The existential checking abstraction is defined by duality. In this case, the relation of approximation is set inclusion, because $[\![\phi]\!] \subseteq [\![\phi]\!]^{\sharp}_1 \subseteq [\![\phi]\!]^{\sharp}_2$ and $[\![\phi]\!]^{\sharp}_1 \cap M \neq \varnothing$ imply $[\![\phi]\!]^{\sharp}_2 \cap M \neq \varnothing$. The Galois insertion $(\alpha^{\exists}_M, \wp(\mathbb{T})_{\subseteq}, \wp(\mathbb{S})_{\subseteq}, \gamma^{\exists}_M)$ is defined by duality as follows:

$$
\begin{aligned}
\alpha^{\exists}_M(X) &\stackrel{\text{def}}{=} \neg(\alpha^{\forall}_M(\neg(X))) = \{s \in \mathbb{S} \mid M_{\downarrow s} \cap X \neq \varnothing\} \\
\gamma^{\exists}_M(S) &\stackrel{\text{def}}{=} \neg(\gamma^{\forall}_M(\neg(X))) = \{\langle i, \sigma\rangle \in \mathbb{T} \mid (\langle i, \sigma\rangle \in M) \Rightarrow (\sigma_i \in S)\}.
\end{aligned}
$$

The intuition is that $\alpha^{\exists}_M$ abstracts a given trace-semantics $[\![\phi]\!]$ to the set of states which existentially satisfy ϕ. In this case, the *existential checking closure* relative

to a model M is $\rho^{\exists}_M \stackrel{\text{def}}{=} \gamma^{\exists}_M \circ \alpha^{\exists}_M \in \mathrm{uco}(\wp(\mathbb{T})_{\subseteq})$, that is,

$$\begin{aligned}\rho^{\exists}_M(X) &= \{\langle i,\sigma\rangle \in \mathbb{T} \mid (\langle i,\sigma\rangle \in M) \Rightarrow M_{\downarrow\sigma_i} \cap X \neq \varnothing\}\\ &= \{\langle i,\sigma\rangle \in M \mid M_{\downarrow\sigma_i} \cap X \neq \varnothing\} \cup \neg M.\end{aligned}$$

Hence, $\rho^{\exists}_M(X)$ adds to X any trace which is not in M — these are meaningless because $\alpha^{\exists}_M(\neg M) = \varnothing$ — and any trace in M whose present state existentially satisfies X. $\rho^{\exists}_M$ is dual to $\rho^{\forall}_M$ since $\rho^{\exists}_M = \neg \circ \rho^{\forall}_M \circ \neg$. In the following, we will consider the universal abstraction only, since all the results can be stated and proved by duality in the existential case.

2.4.3 State-based abstract semantics

The universal abstraction for some model M (typically $M = \mathscr{M}_{\rightarrow}$ for some total transition system $\langle \mathbb{S}, \rightarrow\rangle$) induces a state-based abstract semantics on $\wp(\mathbb{S})$ of the $\widehat{\mu t}$-calculus which is obtained by applying standard abstract interpretation. Basically, this amounts to abstract any trace transformer on $\wp(\mathbb{T})$ by its corresponding best correct approximation on $\wp(\mathbb{S})$ induced by the universal abstraction $\alpha^{\forall}_M/\gamma^{\forall}_M$. For example, the next-time transformer $\bigoplus : \wp(\mathbb{T}) \to \wp(\mathbb{T})$ is abstracted to $\alpha^{\forall}_M \circ \bigoplus \circ \gamma^{\forall}_M : \wp(\mathbb{S}) \to \wp(\mathbb{S})$.

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 state-based abstract semantics $[\![\cdot]\!]^{\forall}_M : \mathfrak{L}_{\widehat{\mu}} \to \mathbb{E}^s \to \wp(\mathbb{S})$ is inductively defined by replacing each trace transformer $Tr : \wp(\mathbb{T}) \to \wp(\mathbb{T})$ with its corresponding best correct approximation on states $\alpha^{\forall}_M \circ Tr \circ \gamma^{\forall}_M : \wp(\mathbb{S}) \to \wp(\mathbb{S})$. The following lemma characterizes these best correct approximations.

Lemma 2.7

(1) $\alpha^{\forall}_M(\boldsymbol{\sigma}_{\{\!|S|\!\}}) = S$;

(2) $\alpha^{\forall}_{\mathscr{M}_{\rightarrow}}(\boldsymbol{\pi}_{\{\!|t|\!\}}) = \{s \in \mathbb{S} \mid \forall s' \in \mathbb{S}.\ s \to s' \Rightarrow (s,s') \in t\}$;

(3) $\alpha^{\forall}_M(\gamma^{\forall}_M(S_1) \cup \gamma^{\forall}_M(S_2)) = S_1 \cup S_2$;

(4) $\alpha^{\forall}_M \circ \neg \circ \gamma^{\forall}_M = \neg$;

(5) $\alpha^{\forall}_M \circ \bigoplus \circ \gamma^{\forall}_M = \widetilde{\mathrm{pre}}_{\rightarrow}$

(6) $\alpha^{\forall}_M(\curvearrowleft(\gamma^{\forall}_M(S))) = \{s \in S \mid M_{\downarrow s} = (\curvearrowleft M)_{\downarrow s}\}$;

(7) $\alpha^{\forall}_M(\forall(\gamma^{\forall}_M(S_1), \gamma^{\forall}_M(S_2))) = S_1 \cap S_2$.

PROOF. Point (1) is as follows: $\alpha^{\forall}_M(\boldsymbol{\sigma}_{\{\!|S|\!\}}) = \{s \in \mathbb{S} \mid M_{\downarrow s} \subseteq \{\langle i,\sigma\rangle \in \mathbb{T} \mid \sigma_i \in S\}\} = \{s \in \mathbb{S} \mid (\langle i,\sigma\rangle \in M \,\&\, \sigma_i = s) \Rightarrow \sigma_i \in S\}$. Since, by Hypothesis 2.6, $|M_{\downarrow s}| > 1$ for any s, we obtain that $\{s \in \mathbb{S} \mid (\langle i,\sigma\rangle \in M \,\&\, \sigma_i = s) \Rightarrow \sigma_i \in S\} = S$.

Point (2) is as follows: $\alpha^{\forall}_{\mathscr{M}_{\rightarrow}}(\boldsymbol{\pi}_{\{\!|t|\!\}}) = \{s \in \mathbb{S} \mid (\mathscr{M}_{\rightarrow})_{\downarrow s} \subseteq \{\langle i, \sigma\rangle \in \mathbb{T} \mid (\sigma_i, \sigma_{i+1}) \in t\}\} = \{s \in \mathbb{S} \mid (\langle i, \sigma\rangle \in \mathscr{M}_{\rightarrow} \,\&\, \sigma_i = s) \;\Rightarrow\; (\sigma_i, \sigma_{i+1}) \in t\} = \{s \in \mathbb{S} \mid \forall s' \in \mathbb{S}.\, s \rightarrow s' \;\Rightarrow\; (s, s') \in t\}$.
Point (3) is as follows: $\alpha^{\forall}_M(\gamma^{\forall}_M(S_1) \cup \gamma^{\forall}_M(S_2)) = \alpha^{\forall}_M(\gamma^{\forall}_M(S_1 \cup S_2)) = S_1 \cup S_2$.
Let us consider point (4) and let us show that $\neg\alpha^{\forall}_M(\neg\gamma^{\forall}_M(S)) = S$. By [10, Section 11.7], $\neg \circ \alpha^{\forall}_M = \alpha^{\exists}_M \circ \neg$ so that we have that $\neg\alpha^{\forall}_M(\neg\gamma^{\forall}_M(S)) = \alpha^{\exists}_M(\gamma^{\forall}_M(S)) = \{s \in \mathbb{S} \mid M_{\downarrow s} \cap \gamma^{\forall}_M(S) \neq \varnothing\}$. By exploiting Hypothesis 2.6 which guarantees that $|M_{\downarrow s}| > 1$ for any s, it is immediate to prove that $\{s \in \mathbb{S} \mid M_{\downarrow s} \cap \gamma^{\forall}_M(S) \neq \varnothing\} = S$.
Point (5) is shown in [10, Section 11.2].
Point (6) is as follows. By [10, Section 11.7], $\alpha^{\forall}_M \circ \curvearrowleft = \alpha^{\forall}_{\curvearrowleft M}$. Thus, $\alpha^{\forall}_M(\curvearrowleft(\gamma^{\forall}_M(S))) = \{t \in \mathbb{S} \mid (\curvearrowleft M)_{\downarrow t} \subseteq \gamma^{\forall}_M(S)\} = \{t \in \mathbb{S} \mid \curvearrowleft(M_{\downarrow t}) \subseteq \cup_{s \in S} M_{\downarrow s}\}$. Since $\curvearrowleft(M_{\downarrow t}) \subseteq M_{\downarrow t}$ iff $\curvearrowleft(M_{\downarrow t}) = M_{\downarrow t}$, we obtain that $\alpha^{\forall}_M(\curvearrowleft(\gamma^{\forall}_M(S))) = \{s \in S \mid M_{\downarrow s} = (\curvearrowleft M)_{\downarrow s}\}$.
Finally, point (7) is as follows. Observe that $\alpha^{\forall}_M(\forall(\gamma^{\forall}_M(S_1), \gamma^{\forall}_M(S_2))) = \{s \in \mathbb{S} \mid M_{\downarrow s} \subseteq \{\langle i, \sigma\rangle \in \gamma^{\forall}_M(S_1) \mid (\gamma^{\forall}_M(S_1))_{\downarrow \sigma_i} \subseteq \gamma^{\forall}_M(S_2)\}\}$. On the one hand, it is easy to check that $S_1 \cap S_2 \subseteq \alpha^{\forall}_M(\forall(\gamma^{\forall}_M(S_1), \gamma^{\forall}_M(S_2)))$. The reverse inclusion follows easily by noting that Hypothesis 2.6 ensures that for any $s \in \mathbb{S}$ there exists some $\langle i, \sigma\rangle \in M_{\downarrow s}$. $\square$

By the above lemma, the abstract semantics $[\![\cdot]\!]^{\forall}_{\mathscr{M}_{\rightarrow}} : \mathfrak{L}_{\overset{\frown}{\mu}} \rightarrow \mathbb{E}^s \rightarrow \wp(\mathbb{S})$ is inductively defined as follows:

$$
\begin{aligned}
&[\![\boldsymbol{\sigma}_S]\!]^{\forall}_{\mathscr{M}_{\rightarrow}}\chi = S\\
&[\![\boldsymbol{\pi}_t]\!]^{\forall}_{\mathscr{M}_{\rightarrow}}\chi = \{s \in \mathbb{S} \mid \forall s' \in \mathbb{S}.\, s \rightarrow s' \;\Rightarrow\; (s, s') \in t\}\\
&[\![X]\!]^{\forall}_{\mathscr{M}_{\rightarrow}}\chi = \chi(X)\\
&[\![\phi_1 \vee \phi_2]\!]^{\forall}_{\mathscr{M}_{\rightarrow}}\chi = [\![\phi_1]\!]^{\forall}_{\mathscr{M}_{\rightarrow}}\chi \cup [\![\phi_2]\!]^{\forall}_{\mathscr{M}_{\rightarrow}}\chi\\
&[\![\neg\phi]\!]^{\forall}_{\mathscr{M}_{\rightarrow}}\chi = \neg[\![\phi]\!]^{\forall}_{\mathscr{M}_{\rightarrow}}\chi\\
&[\![\oplus\,\phi]\!]^{\forall}_{\mathscr{M}_{\rightarrow}}\chi = \widetilde{\mathrm{pre}}_{\rightarrow}([\![\phi]\!]^{\forall}_{\mathscr{M}_{\rightarrow}}\chi)\\
&[\![\phi\curvearrowleft]\!]^{\forall}_{\mathscr{M}_{\rightarrow}}\chi = \alpha^{\forall}_{\mathscr{M}_{\rightarrow}}(\curvearrowleft(\gamma^{\forall}_{\mathscr{M}_{\rightarrow}}([\![\phi]\!]^{\forall}_{\mathscr{M}_{\rightarrow}}\chi)))\\
&[\![\boldsymbol{\mu}X.\phi]\!]^{\forall}_{\mathscr{M}_{\rightarrow}}\chi = \mathrm{lfp}(\lambda S \in \wp(\mathbb{S}).[\![\phi]\!]^{\forall}_{\mathscr{M}_{\rightarrow}}\chi[X/S])\\
&[\![\boldsymbol{\nu}X.\phi]\!]^{\forall}_{\mathscr{M}_{\rightarrow}}\chi = \mathrm{gfp}(\lambda S \in \wp(\mathbb{S}).[\![\phi]\!]^{\forall}_{\mathscr{M}_{\rightarrow}}\chi[X/S])\\
&[\![\forall\phi_1 : \phi_2]\!]^{\forall}_{\mathscr{M}_{\rightarrow}}\chi = [\![\phi_1]\!]^{\forall}_{\mathscr{M}_{\rightarrow}}\chi \cap [\![\phi_2]\!]^{\forall}_{\mathscr{M}_{\rightarrow}}\chi
\end{aligned}
$$

Thus, for any linear formula ϕ, namely a formula ϕ with no quantifier, $[\![\phi]\!]^{\forall}_{\mathscr{M}_{\rightarrow}}$ provides the state-semantics of the state formula $\phi^{\forall}$ which is obtained from ϕ by preceding each linear temporal operator, i.e. next-time $\oplus$ and time-reversal $\curvearrowleft$, occurring in ϕ by the universal path quantifier $\forall$.

The universal abstraction $\alpha^{\forall}_{M}$ is extended pointwise to environments $\dot{\alpha}^{\forall}_{M} : \mathbb{E} \to \mathbb{E}^{s}$ as follows: $\dot{\alpha}^{\forall}_{M}(\xi) \stackrel{\text{def}}{=} \lambda X \in \mathbb{X}.\alpha^{\forall}_{M}(\xi(X))$. The correctness of the state-based semantics $[\![\cdot]\!]^{\forall}_{\mathscr{M}_{\rightarrow}}$ is a consequence of its abstract interpretation-based definition:

$$\text{For any } \phi \in \mathfrak{L}_{\widehat{\mu}} \text{ and } \xi \in \mathbb{E},\ \alpha^{\forall}_{M}([\![\phi]\!]\xi) \supseteq [\![\phi]\!]^{\forall}_{M}\dot{\alpha}^{\forall}_{M}(\xi).$$

This means that given any state $s \in [\![\phi]\!]^{\forall}_{M}\dot{\alpha}^{\forall}_{M}(\xi)$, it turns out that any trace $\langle i, \sigma\rangle$ in M whose present state is s satisfies ϕ. Following the terminology by Kupferman and Vardi [17,25], when $\alpha^{\forall}_{M}([\![\phi]\!]\xi) = [\![\phi]\!]^{\forall}_{M}\dot{\alpha}^{\forall}_{M}(\xi)$ holds for some $\phi \in \mathfrak{L}_{\widehat{\mu}}$, the formula ϕ is called *branchable*. In general, completeness does not hold for all the formulae of the $\widehat{\mu}$-calculus, i.e. the above containment may be strict, as shown in the Introduction. This intuitively means that universal model checking of linear formulae cannot be reduced with no loss of precision to universal model checking on states through the universal quantifier abstraction. Consequently, it turns out that the universal abstraction is incomplete for some trace operators of the $\widehat{\mu}$-calculus. Cousot and Cousot [10, Section 11] identified the sources of this incompleteness, namely those operators Op of the $\widehat{\mu}$-calculus such that $\rho^{\forall}_{M}$ is incomplete for Op: next-time, disjunction, negation and time-reversal. Incompleteness of $\rho^{\forall}_{M}$ w.r.t. time-reversal and negation is not explicitly mentioned in [10] and is shown by the following example.

Example 2.8 Let us consider the two states transition system in Example 1.1. Let $X \stackrel{\text{def}}{=} \{\langle i, \sigma\rangle \in \mathbb{T} \mid \forall k \geq i.\, \sigma_k = 1\}$, so that $\overset{\frown}{}(X) = \{\langle i, \sigma\rangle \mid \forall k \leq i.\, \sigma_k = 1\}$. Since $(\mathscr{M}_{\rightarrow})_{\downarrow 1} \not\subseteq X$ and $(\mathscr{M}_{\rightarrow})_{\downarrow 2} \not\subseteq X$, we have that $\rho^{\forall}_{\mathscr{M}_{\rightarrow}}(X) = \varnothing$ and therefore $\rho^{\forall}_{\mathscr{M}_{\rightarrow}}(\overset{\frown}{}(\rho^{\forall}_{\mathscr{M}_{\rightarrow}}(X))) = \varnothing$. Instead, it turns out that $\rho^{\forall}_{\mathscr{M}_{\rightarrow}}(\overset{\frown}{}(X)) = (\mathscr{M}_{\rightarrow})_{\downarrow 1}$. This means that $\rho^{\forall}_{\mathscr{M}_{\rightarrow}}$ is not complete for $\overset{\frown}{}$.
As far as negation is concerned, consider any $\langle i, \sigma\rangle \in (\mathscr{M}_{\rightarrow})_{\downarrow 1}$ (e.g., $\langle 0, \lambda k \in \mathbb{Z}.1\rangle$) and $\langle j, \tau\rangle \in (\mathscr{M}_{\rightarrow})_{\downarrow 2}$ (e.g., $\langle 0, \lambda k \in \mathbb{Z}.2\rangle$), and let $X \stackrel{\text{def}}{=} \neg\{\langle i, \sigma\rangle, \langle j, \tau\rangle\}$. It turns out that $\rho^{\forall}_{\mathscr{M}_{\rightarrow}}(\neg X) = \rho^{\forall}_{\mathscr{M}_{\rightarrow}}(\{\langle i, \sigma\rangle, \langle j, \tau\rangle\}) = \varnothing$, while $\rho^{\forall}_{\mathscr{M}_{\rightarrow}}(\neg\rho^{\forall}_{\mathscr{M}_{\rightarrow}}(X)) = \rho^{\forall}_{\mathscr{M}_{\rightarrow}}(\neg\varnothing) = \rho^{\forall}_{\mathscr{M}_{\rightarrow}}(\mathbb{T}) = \mathscr{M}_{\rightarrow}$, so that completeness does not hold. □

Cousot and Cousot [10] provide some conditions on the incomplete trace operators that ensure completeness of $\rho^{\forall}_{M}$. As far as next-time is concerned, Cousot and Cousot show that completeness of $\rho^{\forall}_{M}$ for $\oplus$ holds when the linear operator $\oplus$ is restricted to forward closed (i.e. future-time) formulae, namely formulae of the $\widehat{\mu}$-calculus without time-reversal. On the other hand, when disjunction is restricted to have at least one state formula, i.e. a universally quantified formula, it turns out that $\rho^{\forall}_{M}$ is complete. These sufficient conditions allow to identify some complete fragments of the $\widehat{\mu}$-calculus. This is the case, for example, of the $\mu^{\forall}_{+}$-calculus considered by Cousot and Cousot in [10, Section 13], where time-reversal is disallowed and disjunction is restricted to at least one state formulae.

Completeness of $\rho^{\forall}_{M}$ is related to Maidl's [19] characterization of the maximum

common fragment $\mathrm{LTL}_{\mathrm{det}}$ of LTL and ACTL, which is defined as follows:

$$\mathrm{LTL}_{\mathrm{det}} \ni \phi ::= \boldsymbol{\sigma}_S \mid \neg\boldsymbol{\sigma}_S \mid \phi_1 \wedge \phi_2 \mid (\boldsymbol{\sigma}_S \wedge \phi_1) \vee (\neg\boldsymbol{\sigma}_S \wedge \phi_2) \mid \\ \oplus\phi \mid \mathrm{U}(\boldsymbol{\sigma}_S \wedge \phi_1, \neg\boldsymbol{\sigma}_S \wedge \phi_2) \mid \mathrm{W}(\boldsymbol{\sigma}_S \wedge \phi_1, \neg\boldsymbol{\sigma}_S \wedge \phi_2)$$

where U and W denote, respectively, standard until and weak-until, i.e. $\mathrm{W}(\phi_1, \phi_2) = \mathrm{G}\phi_1 \vee \mathrm{U}(\phi_1, \phi_2)$, operators. Obviously, $\mathrm{LTL}_{\mathrm{det}}$ is a fragment of the $\widehat{\mu}$-calculus. Maidl [19] shows that $\mathrm{LTL}_{\mathrm{det}} = \mathrm{LTL} \cap \mathrm{ACTL}$, namely that for any $\phi \in \mathrm{LTL}$, there exists some $\psi \in \mathrm{ACTL}$ such that $\alpha^{\forall}_M(\llbracket\phi\rrbracket) = \llbracket\psi\rrbracket$ iff there exists some $\zeta \in \mathrm{LTL}_{\mathrm{det}}$ such that $\llbracket\phi\rrbracket = \llbracket\zeta\rrbracket$.

Ranzato and Tapparo [23] show that the universal abstraction is complete for all the formulae of $\mathrm{LTL}_{\mathrm{det}}$, namely for any $\phi \in \mathrm{LTL}_{\mathrm{det}}$, $\alpha^{\forall}_M(\llbracket\phi\rrbracket) = \llbracket\phi\rrbracket^{\forall}_M$. Let $\mathrm{LTL}_{\forall} = \{\phi \in \mathrm{LTL} \mid \alpha^{\forall}_M(\llbracket\phi\rrbracket) = \llbracket\phi\rrbracket^{\forall}_M\}$ denote the set of branchable LTL formulae. Thus, we have that $\mathrm{LTL}_{\mathrm{det}} \subseteq \mathrm{LTL}_{\forall}$. Furthermore, the following converse holds: any branchable LTL formula is equivalent to some formula in $\mathrm{LTL}_{\mathrm{det}}$. In fact, if $\phi \in \mathrm{LTL}$ is branchable then, by Maidl's [19, Corollary 1] result, there exists some $\psi \in \mathrm{LTL}_{\mathrm{det}}$ such that $\llbracket\phi\rrbracket = \llbracket\psi\rrbracket$. As a consequence, we obtain the following characterization of branchability for LTL formulae.

Theorem 2.9 *Let $\phi \in \mathrm{LTL}$. Then, there exists $\zeta \in \mathrm{LTL}_{\forall}$ such that $\llbracket\phi\rrbracket = \llbracket\zeta\rrbracket$ if and only if there exists $\psi \in \mathrm{LTL}_{\mathrm{det}}$ such that $\llbracket\phi\rrbracket = \llbracket\psi\rrbracket$.*

Thus, $\mathrm{LTL}_{\mathrm{det}}$ also provides a synctatic characterization for the set of branchable LTL formulae.

3 Complete Cores and Shells for Temporal Connectives

In the following, we will characterize the complete cores and shells of the universal abstraction $\rho^{\forall}_M$ for the following trace operators which are sources of incompleteness: next-time, disjunction and time-reversal. These complete cores and shells do exist because $\oplus$, $\cup$ and $^{\frown}$ are trivially continuous functions on the concrete domain $\wp(\mathbb{T})_{\supseteq}$ so that we can exploit Theorem 2.1 in order to characterize them. As recalled in Section 2.2.3, complete shells may not exist and we show that this is indeed the case of negation. Let us observe that Theorem 2.1 cannot be applied in this case because negation is not continuous on $\wp(\mathbb{T})_{\supseteq}$. On the other hand, the complete core for negation does exist.

One remarkable feature of our approach lies in the fact that it is fully constructive, namely Theorem 2.1 always provides complete cores and shells in fixpoint form so that we do not need to conjecture some abstract domain and successively to prove that it is indeed a complete core or shell.

Theorem 3.1 *The complete shell of $\rho^{\forall}_M$ for $\neg$ does not exist.*

PROOF. Let us consider the simplest transition system $\langle\{\bullet\}, \{\bullet \to \bullet\}\rangle$ consisting of a single state $\bullet$ and of a single transition $\bullet \to \bullet$. The only possible path is $\lambda n \in \mathbb{Z}.\bullet$ so that the model M generated by this transition system coincides with the set of traces, namely $M = \{\langle i, \lambda n.\bullet\rangle \mid i \in \mathbb{Z}\}$. Thus, any set of traces can be simply represented by the corresponding set of present times, namely by a corresponding set of integers, so that the concrete domain $\wp(\mathbb{T})_{\supseteq}$ can be represented by $\wp(\mathbb{Z})_{\supseteq}$ and in particular $M = \mathbb{Z}$. We also have that $\rho^{\forall}_M = \{\varnothing, \mathbb{Z}\}$.
Let $\mathbb{Z}_{\mathrm{ev}}$ and $\mathbb{Z}_{\mathrm{od}}$ denote, respectively, the set of even and odd intergers and consider the following two closures: for any $X \in \wp(\mathbb{Z})$,

$$\rho_{\mathrm{ev}}(X) = \begin{cases} \mathbb{Z} & \text{if } X = \mathbb{Z} \\ X \cap \mathbb{Z}_{\mathrm{ev}} & \text{otherwise} \end{cases} \qquad \rho_{\mathrm{od}}(X) = \begin{cases} \mathbb{Z} & \text{if } X = \mathbb{Z} \\ X \cap \mathbb{Z}_{\mathrm{od}} & \text{otherwise} \end{cases}$$

Let us note that $\rho_{\mathrm{ev}}, \rho_{\mathrm{od}} \in \mathrm{uco}(\wp(\mathbb{Z})_{\supseteq})$, because their images are closed under arbitrary unions, and that $\rho_{\mathrm{ev}}, \rho_{\mathrm{od}} \sqsubseteq \rho^{\forall}_M$. Let us show that ρ_{ev} is complete for $\neg$ (the case of ρ_{od} is analogous). If $X \in \{\mathbb{Z}, \varnothing\}$ then $\rho_{\mathrm{ev}}(\neg X) = \rho_{\mathrm{ev}}(\neg\rho_{\mathrm{ev}}(X))$ trivially holds. If $X \in \wp(\mathbb{Z})$ and $X \notin \{\mathbb{Z}, \varnothing\}$ then

$$\rho_{\mathrm{ev}}(\neg\rho_{\mathrm{ev}}(X)) = \rho_{\mathrm{ev}}(\neg(\mathbb{Z}_{\mathrm{ev}} \cap X)) = \rho_{\mathrm{ev}}(\mathbb{Z}_{\mathrm{od}} \cup \neg X) =$$
$$\mathbb{Z}_{\mathrm{ev}} \cap (\mathbb{Z}_{\mathrm{od}} \cup \neg X) = \mathbb{Z}_{\mathrm{ev}} \cap \neg X = \rho_{\mathrm{ev}}(\neg X).$$

If $\mathrm{Shell}_{\neg}(\rho^{\forall}_M)$ would exist then we would have that $\rho_{\mathrm{ev}}, \rho_{\mathrm{od}} \sqsubseteq \mathrm{Shell}_{\neg}(\rho^{\forall}_M)$, so that $\rho_{\mathrm{ev}} \sqcup \rho_{\mathrm{od}} \sqsubseteq \mathrm{Shell}_{\neg}(\rho^{\forall}_M)$. But $\rho_{\mathrm{ev}} \sqcup \rho_{\mathrm{od}} = \rho^{\forall}_M$, so that we would have that $\mathrm{Shell}_{\neg}(\rho^{\forall}_M) = \rho^{\forall}_M$ which is a contradiction because $\rho^{\forall}_M$ is not complete for $\neg$. □

Negation is antimonotone, however this is not the reason why the corresponding complete shell does not exist. In fact, as a further remarkable example, we show that this is also the case of the "sometime" operator F, which is instead monotone.

Theorem 3.2 *The complete shell of $\rho^{\forall}_M$ for* $\mathbf{F}$ *does not exist.*

PROOF. Let us consider again the transition system $\langle\{\bullet\}, \{\bullet \to \bullet\}\rangle$ used in the proof of Theorem 3.1 so that the concrete domain $\wp(\mathbb{T})_{\supseteq}$ can be represented by $\wp(\mathbb{Z})_{\supseteq}$ and in particular $M = \mathbb{Z}$. We also have that $\rho^{\forall}_M = \{\varnothing, \mathbb{Z}\}$, namely $\rho^{\forall}_M(\mathbb{Z}) = \mathbb{Z}$, while if $X \subsetneq \mathbb{Z}$ then $\rho^{\forall}_M(X) = \varnothing$. Let us observe that for any $k \in \mathbb{Z}$, $\mathbf{F}([k, +\infty)) = \mathbb{Z}$, because for any $i \in \mathbb{Z}$ there exists some $m \geq i$ and $m \in [k, +\infty)$.

It is simple to observe that $\rho_M^\forall$ is not complete for $\mathbf{F}$. In fact, for any $k \in \mathbb{Z}$, we have that $\rho_M^\forall(\mathbf{F}([k,+\infty))) = \rho_M^\forall(\mathbb{Z}) = \mathbb{Z}$, while $\rho_M^\forall(\mathbf{F}(\rho_M^\forall([k,+\infty)))) = \rho_M^\forall(\mathbf{F}(\varnothing)) = \rho_M^\forall(\varnothing) = \varnothing$. It is also easy to note that $\mathbf{F}$ is not continuous on $\wp(\mathbb{T})_\supseteq$: in fact, $\bigcap_{k\in\mathbb{Z}} \mathbf{F}([k,+\infty)) = \mathbb{Z}$, whereas $\mathbf{F}(\bigcap_{k\in\mathbb{Z}}[k,+\infty)) = \mathbf{F}(\varnothing) = \varnothing$. Hence, noncontinuity of $\mathbf{F}$ is consistent with Theorem 2.1.

Let us now consider the following family of closures: for any $k \in \mathbb{Z}$ and $X \in \wp(\mathbb{Z})$,

$$\rho_k(X) = \begin{cases} \mathbb{Z} & \text{if } X = \mathbb{Z} \\ X \cap [k,+\infty) & \text{otherwise} \end{cases}$$

Let us note that $\rho_k \in \mathrm{uco}(\wp(\mathbb{Z})_\supseteq)$, because $\mathrm{img}(\rho_k) = \{\mathbb{Z}\} \cup \{X \in \wp(\mathbb{Z}) \mid X \subseteq [k,+\infty)\}$ is closed under arbitrary unions, and that $\rho_k \sqsubseteq \rho_M^\forall$. Let us show that ρ_k is complete for $\mathbf{F}$. Let $X \in \wp(\mathbb{Z})$. If $X = \mathbb{Z}$ then $\rho_k(\mathbf{F}(X)) = \rho_k(\mathbf{F}(\rho_k(X)))$ trivially holds because $X = \mathbb{Z} \in \rho_k$. Thus, consider $X \subsetneq \mathbb{Z}$. We distinguish the following two cases.
Case (i). Assume that for any $j \in \mathbb{Z}$, $X \cap [j,+\infty) \neq \varnothing$. Then, we have that $\mathbf{F}(X) = \mathbb{Z}$ because, by hypothesis on X, for any $i \in \mathbb{Z}$ there exists some $k \in X$ such that $i \leq k$. Moreover, $\mathbf{F}(\rho_k(X)) = \mathbf{F}(X \cap [k,+\infty)) = \mathbb{Z}$ because for any $i \in \mathbb{Z}$, $X \cap [k,+\infty) \cap [i,+\infty) \neq \varnothing$. Thus, in this case, $\mathbf{F}(X) = \mathbf{F}(\rho_k(X))$, so that $\rho_k(\mathbf{F}(X)) = \rho_k(\mathbf{F}(\rho_k(X))) = \mathbb{Z}$.
Case (ii). On the other hand, assume that there exists some $i \in \mathbb{Z}$ such that $X \cap [i,+\infty) = \varnothing$. Therefore, $\max(X) = n \in \mathbb{Z}$ so that $\mathbf{F}(X) = (-\infty, n]$. Let us distinguish two cases: $n < k$ and $n \geq k$. If $n < k$ then $\rho_k(\mathbf{F}(X)) = (-\infty, n] \cap [k,+\infty) = \varnothing$, $\rho_k(X) = X \cap [k,+\infty) = \varnothing$, so that $\rho_k(\mathbf{F}(\rho_k(X))) = \varnothing$. If, instead, $n \geq k$ then $\rho_k(\mathbf{F}(X)) = (-\infty, n] \cap [k,+\infty) = [k,n]$, $\rho_k(X) = X \cap [k,+\infty)$ so that $\max(\rho_k(X)) = n$ and this implies $\mathbf{F}(\rho_k(X)) = (-\infty, n]$, from which $\rho_k(\mathbf{F}(\rho_k(X))) = (-\infty, n] \cap [k,+\infty) = [k,n]$.
Hence, summing up, we have shown that for any $k \in \mathbb{Z}$ and $X \in \wp(\mathbb{Z})$, $\rho_k(\mathbf{F}(X)) = \rho_k(\mathbf{F}(\rho_k(X)))$, i.e. any ρ_k is complete for $\mathbf{F}$. If $\mathrm{Shell}_\mathbf{F}(\rho_M^\forall)$ would exist then we would have that for any k, $\rho_k \sqsubseteq \mathrm{Shell}_\mathbf{F}(\rho_M^\forall)$, so that $\sqcup_{k\in\mathbb{Z}}\rho_k \sqsubseteq \mathrm{Shell}_\mathbf{F}(\rho_M^\forall)$. But $\mathrm{img}(\sqcup_{k\in\mathbb{Z}}\rho_k) = \bigcap_{k\in\mathbb{Z}} \mathrm{img}(\rho_k) = \{\varnothing, \mathbb{Z}\} = \mathrm{img}(\rho_M^\forall)$, so that we would have that $\mathrm{Shell}_\mathbf{F}(\rho_M^\forall) = \rho_M^\forall$ which is a contradiction because $\rho_M^\forall$ is not complete for $\mathbf{F}$. □

The above proof also shows that $\mathbf{F}$ is not continuous on $\wp(\mathbb{T})_\supseteq$, so that noncontinuity of $\mathbf{F}$ is consistent with Theorem 2.1.

Although negation is not monotone, it turns out that the core of $\rho_M^\forall$ for $\neg$ exists even if we cannot exploit Theorem 2.1 in order to obtain a constructive characterization of it. This core results to be the greatest totally uninformative closure.

Theorem 3.3 $\mathrm{Core}_\neg(\rho_M^\forall) = \lambda X.\varnothing$.

PROOF. Let $\eta \in \mathrm{uco}(\wp(\mathbb{T})_{\supseteq})$ such that $\rho^{\forall}_M \sqsubseteq \eta$, so that, for any X, $\rho^{\forall}_M(X) \supseteq \eta(X)$. By Hypothesis 2.6, for any $s \in \mathbb{S}$, we consider some $\langle i, \sigma_s \rangle \in M_{\downarrow s}$, so that $|M_{\downarrow s} \smallsetminus \{\langle i, \sigma_s \rangle\}| \geq 1$. Consider $Y \stackrel{\mathrm{def}}{=} \{\langle i, \sigma_s \rangle \in \mathbb{T} \mid s \in \mathbb{S}\}$. Then, we have that $\eta(\neg Y) \subseteq \rho^{\forall}_M(\neg Y) = \varnothing$, so that $\eta(\neg Y) = \varnothing$. On the other hand, $\eta(Y) \subseteq \rho^{\forall}_M(Y) = \varnothing$, so that $\eta(Y) = \varnothing$ and in turn $\eta(\neg\eta(Y)) = \eta(\neg\varnothing) = \eta(\mathbb{T})$. Thus, if η is complete for $\neg$ then $\eta(\mathbb{T}) = \varnothing$ so that for any $X \subseteq \mathbb{T}$, $\eta(X) \subseteq \eta(\mathbb{T}) = \varnothing$. Hence, $\lambda X.\varnothing$ is the unique closure which is greater than $\rho^{\forall}_M$ and complete for $\neg$, i.e., $\mathrm{Core}_{\neg}(\rho^{\forall}_M) = \lambda X.\varnothing$. □

3.2 Next-time

Let us first show the following easy properties of the predecessor and successor trace operators.

Lemma 3.4
(1) $\oplus : \wp(\mathbb{T}) \to \wp(\mathbb{T})$ *and* $\ominus : \wp(\mathbb{T}) \to \wp(\mathbb{T})$ *preserve arbitrary unions and intersections, and* $\oplus^{-1} = \ominus$ *and* $\ominus^{-1} = \oplus$.
Let $\rho \in \mathrm{uco}(\wp(\mathbb{T})_{\supseteq})$. *Then,*
(2) $\rho \in \Gamma(\wp(\mathbb{T})_{\supseteq}, \oplus)$ *iff for all* $n \in \mathbb{N}$ *and* $X \in \wp(\mathbb{T})$, $\ominus^n(\rho(X)) = \rho(\ominus^n(\rho(X)))$*;*
(3) $\rho \in \Gamma(\wp(\mathbb{T})_{\supseteq}, \ominus)$ *iff for all* $n \in \mathbb{N}$ *and* $X \in \wp(\mathbb{T})$, $\oplus^n(\rho(X)) = \rho(\oplus^n(\rho(X)))$.

PROOF. (1): Clear.
(2) and (3): Let us check that $\rho \in \Gamma(\wp(\mathbb{T})_{\supseteq}, \oplus)$ iff for all $n \in \mathbb{N}$ and $X \in \wp(\mathbb{T})$, $\ominus^n(\rho(X)) = \rho(\ominus^n(\rho(X)))$ (the remaining proof is analogous). Because, by (1), $\oplus$ is additive on $\wp(\mathbb{T})_{\supseteq}$, by Theorem 2.1 and Remark 2.3, we have that $\rho \in \Gamma(\wp(\mathbb{T})_{\supseteq}, \oplus)$ iff $\{\cap\{X \in \wp(\mathbb{T}) \mid \oplus(X) \supseteq Y\}\}_{Y \in \rho} \subseteq \rho$. By (1), $\oplus(X) \supseteq Y$ iff $X \supseteq \ominus(Y)$, and therefore $\rho \in \Gamma(\wp(\mathbb{T})_{\supseteq}, \oplus)$ iff $\{\ominus(Y) \mid Y \in \rho\} \subseteq \rho$, and therefore, iff $\{\ominus(\rho(X)) \mid X \in \wp(\mathbb{T})\} \subseteq \rho$. Analogously, we get that, for any $n \in \mathbb{N}$, $\rho \in \Gamma(\wp(\mathbb{T})_{\supseteq}, \oplus^n)$ iff $\{\ominus^n(\rho(X)) \mid X \in \wp(\mathbb{T})\} \subseteq \rho$. Thus, property $(*)$ in Section 2.2.2 closes the proof. □

Let us recall from [10] that $\rho^{\forall}_M$ is complete for $\oplus$ when $\oplus$ is restricted to forward closed set of traces, namely if $X \in \wp(\mathbb{T})$ is such that $X = \mathrm{Fd}(X)$ then $\rho^{\forall}_M(\oplus(X)) = \rho^{\forall}_M(\oplus(\rho^{\forall}_M(X)))$. This implies that for forward or state closed specification languages, namely languages with no past-time modality like LTL and CTL*, the universal abstraction is already complete for the next-time trace transformer. The situation changes in the general case of the $\widehat{\mu}$-calculus, where $\rho^{\forall}_M$ is incomplete for next-time.

3.2.1 Complete core

By exploiting the constructive method provided by Theorem 2.1, the set of fixpoints of the complete core $\mathrm{Core}_{\oplus}(\rho^{\forall}_{M})$ is first characterized as follows.

Theorem 3.5 *The set of fixpoints of* $\mathrm{Core}_{\oplus}(\rho^{\forall}_{M})$ *is* $\{Y \in \wp(\mathbb{T}) \mid \forall k \in \mathbb{N}.\, \ominus^{k} Y = \rho^{\forall}_{M}(\ominus^{k} Y)\}$.

PROOF. By Theorem 2.1 and Remark 2.3, $\mathrm{Core}_{\oplus}(\rho^{\forall}_{M}) = \sqcup_{i\in\mathbb{N}} L^{i}_{F}(\rho^{\forall}_{M})$. Thus, $Y \in \mathrm{Core}_{\oplus}(\rho^{\forall}_{M}) \Leftrightarrow \forall i \in \mathbb{N}.\, Y \in L^{i}_{\oplus}(\rho^{\forall}_{M})$. Moreover, by Lemma 3.4, we have that $L_{\oplus}(\eta) = \{Y \in \wp(\mathbb{T}) \mid \cap \{X \in \wp(\mathbb{T}) \mid X \supseteq \ominus Y\} \in \eta\} = \{Y \in \wp(\mathbb{T}) \mid \ominus Y \in \eta\} = \{Y \in \wp(\mathbb{T}) \mid \ominus Y = \eta(\ominus Y)\}$, and therefore, for any $i \in \mathbb{N}$, $Y \in L^{i}_{\oplus}(\rho^{\forall}_{M}) \Leftrightarrow \ominus^{i} Y = \rho^{\forall}_{M}(\ominus^{i} Y)$. Therefore, the thesis follows. □

The following result provides a further useful characterization of the complete core based on the structure of the 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 $k > 0$, $r \xrightarrow{k} s$ iff $r = r_0 \rightarrow r_1 \rightarrow r_2 \rightarrow \ldots \rightarrow r_k = s$, where $\{r_1, ..., r_{k-1}\} \subseteq \mathbb{S}$. Moreover, we consider the following property $P_{\rightarrow}$ for any $S \subseteq \mathbb{S}$:

$$P_{\rightarrow}(S) \quad \text{iff} \quad \exists k > 0, q \in S, r \in \mathbb{S} \smallsetminus S, t \in \mathbb{S}.\ q \xrightarrow{k} t \text{ and } r \xrightarrow{k} t.$$

Theorem 3.6 *Let* $M = \mathscr{M}_{\rightarrow}$*, for some total transition system* $\langle \mathbb{S}, \rightarrow \rangle$*. Then, for any* $S \subseteq \mathbb{S}$*,* $\gamma^{\forall}_{M}(S) \notin \mathrm{Core}_{\oplus}(\rho^{\forall}_{M})$ *iff* $P_{\rightarrow}(S)$.

PROOF. ($\Leftarrow$) Assume that there exist $k > 0$, $q \in S$, $r \in \mathbb{S} \smallsetminus S$, $t \in \mathbb{S}$ such that $q \xrightarrow{k} t$ and $r \xrightarrow{k} t$. By Theorem 3.5, it is enough to show that $\ominus^{k}(\cup_{s\in S} M_{\downarrow s}) \supsetneq \rho^{\forall}_{M}(\ominus^{k}(\cup_{s\in S} M_{\downarrow s}))$. Since $q \xrightarrow{k} t$ and $\langle \mathbb{S}, \rightarrow \rangle$ is total, there exists $\langle j, \pi \rangle \in M$ such that $\pi_j = q$ and $\pi_{j+k} = t$. Since $q \in S$, we have that $\langle j, \pi \rangle \in \cup_{s\in S} M_{\downarrow s}$ and therefore $\langle j + k, \pi \rangle \in \ominus^{k}(\cup_{s\in S} M_{\downarrow s})$. On the other hand, since $r \xrightarrow{k} t$ and $\langle \mathbb{S}, \rightarrow \rangle$ is total, there exists $\langle l, \tau \rangle \in M$ such that $\tau_l = r$ and $\tau_{l+k} = t = \pi_{j+k}$. Thus, $\langle l + k, \tau \rangle \in M_{\downarrow \pi_{j+k}}$, while $\langle l + k, \tau \rangle \notin \ominus^{k}(\cup_{s\in S} M_{\downarrow s})$ because $\tau_l = r \notin S$. Thus, by definition of $\rho^{\forall}_{M}$, this means that $\langle j + k, \pi \rangle \notin \rho^{\forall}_{M}(\ominus^{k}(\cup_{s\in S} M_{\downarrow s}))$.
($\Rightarrow$) By Theorem 3.5, there exist $k > 0$ and $\langle j, \beta \rangle$ such that (i) $\langle j, \beta \rangle \in \ominus^{k}(\cup_{s\in S} M_{\downarrow s})$ and (ii) $\langle j, \beta \rangle \notin \rho^{\forall}_{M}(\ominus^{k}(\bigcup_{s\in S} M_{\downarrow s}))$. Thus, by (i), $\langle j - k, \beta \rangle \in \cup_{s\in S} M_{\downarrow s}$, i.e., $\beta_{j-k} \in S$. Moreover, by (ii), $M_{\downarrow \beta_j} \not\subseteq \ominus^{k}(\bigcup_{s\in S} M_{\downarrow s})$, so that there exists $\langle l, \tau \rangle \in M$ such that $\pi_l = \beta_j$ and $\langle l - k, \pi \rangle \notin \cup_{s\in S} M_{\downarrow s}$, i.e., $\pi_{l-k} \notin S$. Summing up, we have that $\pi_{l-k} \xrightarrow{k} \pi_l$, $\beta_{j-k} \xrightarrow{k} \pi_l$, $\pi_{l-k} \notin S$ and $\beta_{j-k} \in S$, that is $P_{\rightarrow}(S)$. □

Thus, by the characterization ($\ddagger$) in Section 2.4.1 of $\rho^{\forall}_{M}$ stating that $\{\gamma^{\forall}_{M}(S)\}_{S\subseteq\mathbb{S}}$ is the set of fixpoints of $\rho^{\forall}_{M}$, the above result characterizes exactly the fixpoints which must be removed from $\rho^{\forall}_{M}$ in order to get the complete core $\mathrm{Core}_{\oplus}(\rho^{\forall}_{M})$. As an

immediate consequence of Theorem 3.6, observe that $M \in \mathrm{Core}_{\oplus}(\rho^{\forall}_M)$: in fact, by Theorem 3.6, $M = \gamma^{\forall}_M(\mathbb{S})$ and $P_{\rightarrow}(\mathbb{S})$ is not satisfied. Let us also observe that $P_{\rightarrow}(S)$ holds iff $P_{\rightarrow}(\neg S)$ holds, so that $\gamma^{\forall}_M(S) \notin \mathrm{Core}_{\oplus}(\rho^{\forall}_M) \Leftrightarrow \gamma^{\forall}_M(\neg S) \notin \mathrm{Core}_{\oplus}(\rho^{\forall}_M)$.

Example 3.7 Consider the transition system in Example 1.1. We know that $\rho^{\forall}_M = \{\gamma^{\forall}_M(\varnothing), \gamma^{\forall}_M(\{1\}), \gamma^{\forall}_M(\{2\}), \gamma^{\forall}_M(\{1,2\})\}$. Which elements are in $\mathrm{Core}_{\oplus}(\rho^{\forall}_M)$? We have that $\gamma^{\forall}_M(\varnothing)$ and $\gamma^{\forall}_M(\{1,2\})$ always belong to $\mathrm{Core}_{\oplus}(\rho^{\forall}_M)$. Moreover, note that $1 \xrightarrow{1} 2$ and $2 \xrightarrow{1} 2$ so that $P_{\rightarrow}(\{1\})$ holds. Hence, by Theorem 3.6, $\gamma^{\forall}_M(\{1\})$ and $\gamma^{\forall}_M(\{2\})$ do not belong to $\mathrm{Core}_{\oplus}(\rho^{\forall}_M)$. $\square$

By exploiting the above constructive result, we are also able to characterize the structure of transition systems whose models induce a universal closure which is complete for next-time. These are the transition systems $\langle \mathbb{S}, \rightarrow \rangle$ such that $\rightarrow$ is injective. A transition relation $\rightarrow$ is *injective* when

$$\forall r, s, t \in \mathbb{S}.\, (r \rightarrow t \ \ \& \ \ s \rightarrow t) \Rightarrow r = s.$$

Theorem 3.8 *Let $M = \mathscr{M}_{\rightarrow}$, for some total transition system $\langle \mathbb{S}, \rightarrow \rangle$. Then, $\rho^{\forall}_M$ is complete for $\oplus$ if and only if $\rightarrow$ is injective.*

PROOF. $\rho^{\forall}_M$ is complete for $\oplus$ iff $\mathrm{Core}_{\oplus}(\rho^{\forall}_M) = \rho^{\forall}_M$ iff $\mathrm{Core}_{\oplus}(\rho^{\forall}_M) \sqsubseteq \rho^{\forall}_M$ iff $\rho^{\forall}_M \subseteq \mathrm{Core}_{\oplus}(\rho^{\forall}_M)$. Thus:
($\Rightarrow$) By hypothesis, for any $s \in \mathbb{S}$, $\gamma^{\forall}_M(\{s\}) \in \mathrm{Core}_{\oplus}(\rho^{\forall}_M)$. Thus, by Theorem 3.6, for any $r, s, t \in \mathbb{S}$ such that $r \neq s$, we have that for any $k > 0$, $s \xrightarrow{k} t$ implies $\neg(r \xrightarrow{k} t)$. Hence, for any $r, s, t \in \mathbb{S}$ and for any $k > 0$, $r \xrightarrow{k} t$ and $s \xrightarrow{k} t$ imply $s = r$. Therefore, for $k = 1$, this implies that $\rightarrow$ is injective.
($\Leftarrow$) Let $\rightarrow$ be injective. Let $r, s, t \in \mathbb{S}$ and $k > 0$ such that $r \xrightarrow{k} t$ and $s \xrightarrow{k} t$, i.e., $r \rightarrow r_1 \rightarrow \ldots \rightarrow r_{k-1} \rightarrow t$ and $s \rightarrow s_1 \rightarrow \ldots \rightarrow s_{k-1} \rightarrow t$. Then, by injectivity, $r_{k-1} = s_{k-1}$, and in turn, still by injectivity, $r_{k-2} = s_{k-2}$, and so on, so that we get $r = s$. Hence, for any $r, s, t \in \mathbb{S}$, for any $k > 0$, $s \xrightarrow{k} t$ and $r \xrightarrow{k} t$ imply $r = s$. This means that, for any $s \in \mathbb{S}$, $P_{\rightarrow}(\{s\})$ does not hold. Thus, by Theorem 3.6, $\gamma^{\forall}_M(\{s\}) \in \mathrm{Core}_{\oplus}(\rho^{\forall}_M)$. Since $\mathrm{Core}_{\oplus}(\rho^{\forall}_M)$ is a uco on $\wp(\mathbb{T})_{\supseteq}$, its set of fixpoints is closed under arbitrary set-unions. Moreover, since $\gamma^{\forall}_M$ is co-additive on $\wp(\mathbb{S})_{\supseteq}$, we have that $\gamma^{\forall}_M$ preserves arbitrary set-unions. Thus, for any $S \subseteq \mathbb{S}$, $\gamma^{\forall}_M(S) = \cup_{s \in S} \gamma^{\forall}_M(\{s\}) \in \mathrm{Core}_{\oplus}(\rho^{\forall}_M)$. Thus, since $\rho^{\forall}_M = \{\gamma^{\forall}_M(S)\}_{S \subseteq \mathbb{S}}$, it turns out that $\rho^{\forall}_M \subseteq \mathrm{Core}_{\oplus}(\rho^{\forall}_M)$. $\square$

It is worth noting that injectivity means that each computation step is reversible, i.e. the reversed transition system $\langle \mathbb{S}, \leftarrow \rangle$ obtained by reversing the transition relation is deterministic. This is the case of Bennett's reversible computations [1], i.e. computations whose output uniquely defines the input, which have been extensively studied by many authors in different contexts. 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

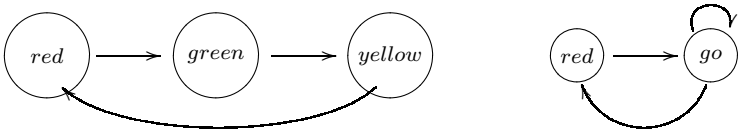


Figure 1. A traffic light controller and its abstract version.

requires that $t \not\rightarrow s$ for any $t \neq s$, i.e., s cannot be reached by any other state so that s must necessarily be an initial system state.

Example 3.9 Consider a traffic light controller modeled by the transition system $\langle \mathbb{S}, \rightarrow \rangle$ depicted in Figure 1 that generates the model M. Then, $\langle \mathbb{S}, \rightarrow \rangle$ is total and injective, and therefore, by Theorem 3.8, the corresponding universal closure is complete for next-time, so that $\mathrm{Core}_{\oplus}(\rho^{\forall}_{M}) = \rho^{\forall}_{M}$.
Consider instead the abstract transition system $\langle \mathbb{S}^{\sharp} = \{red, go\}, \rightarrow^{\sharp} \rangle$ induced by the state partition $\{\{red\}, \{green, yellow\}\}$ (see [7] for an introduction to abstract model checking) and still depicted in Figure 1. In this case, $\langle \mathbb{S}^{\sharp}, \rightarrow^{\sharp} \rangle$ is total but it is not injective. Let $M^{\sharp}$ be the model generated by $\langle \mathbb{S}^{\sharp}, \rightarrow^{\sharp} \rangle$. We exploit Theorem 3.6 in order to compute the complete core in this case. It turns out that $red \rightarrow^{\sharp} go$ and $go \rightarrow^{\sharp} go$, so that $P_{\rightarrow^{\sharp}}(red)$ and $P_{\rightarrow^{\sharp}}(go)$ do not hold. Thus, in this case it turns out that the complete core is trivial, i.e., $\mathrm{Core}_{\oplus}(\rho^{\forall}_{M^{\sharp}}) = \{\varnothing, M^{\sharp}\}$.
Let us also observe that any abstraction with at least two states of $\langle \mathbb{S}, \rightarrow \rangle$ induces an abstract transition system for which the universal closure is not complete for next-time. This is not always the case for abstract transition systems. For example, in the case of an infinite counter modeled by a concrete transition system $\langle \mathbb{S}, \rightarrow \rangle$ where $\mathbb{S} = \mathbb{Z}$ 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 even/odd partition of integer numbers, are such that the corresponding universal closures are complete for $\oplus$: in fact, both transition relations are injective and therefore Theorem 3.8 applies. □

3.2.2 Complete shell

By applying again Theorem 2.1, let us now characterize the set of fixpoints of the complete shell of the universal closure for next-time.

Theorem 3.10 *The set of fixpoints of* $\mathrm{Shell}_{\oplus}(\rho^{\forall}_{M})$ *is* $\mathrm{Cl}^{\cup}(\{\ominus^{n}(X) \mid n \in \mathbb{N}, X \in \rho^{\forall}_{M}\})$.

PROOF. By Theorem 2.1 and Remark 2.3, $\mathrm{Shell}_{\oplus}(\rho^{\forall}_{M}) = \sqcap_{i \in \mathbb{N}} R^{i}_{\oplus}(\eta)$, where $R_{\oplus}(\eta) = \mathrm{Cl}^{\cup}(\{\cap\{X \in \wp(\mathbb{T}) \mid \oplus X \supseteq Y\} \mid Y \in \eta\}) = \mathrm{Cl}^{\cup}(\{\ominus(Y) \mid Y \in \eta\})$.

Moreover, for any $i \in \mathbb{N}$, $R^i_{\oplus}(\eta) = \mathrm{Cl}^{\cup}(\{\ominus^i(Y) \mid Y \in \eta\})$. Thus, it turns out that

$$\begin{aligned}\mathrm{Shell}_{\oplus}(\rho^{\forall}_M) &= \sqcap_{i\in\mathbb{N}} R^i_{\oplus}(\rho^{\forall}_M)\\ &= \mathrm{Cl}^{\cup}(\cup_{i\in\mathbb{N}}\, \mathrm{Cl}^{\cup}(\{\ominus^i(Y) \mid Y \in \rho^{\forall}_M\}))\\ &= \mathrm{Cl}^{\cup}(\cup_{i\in\mathbb{N}}\{\ominus^i(Y) \mid Y \in \rho^{\forall}_M\})\\ &= \mathrm{Cl}^{\cup}(\{\ominus^i(Y) \mid i \in \mathbb{N},\, Y \in \rho^{\forall}_M\}). \qquad \Box\end{aligned}$$

Thus, in order to minimally refine the universal closure $\rho^{\forall}_M$ to a complete closure for the next-time $\oplus$, one must close the image of $\rho^{\forall}_M$ under the application of the inverse of $\oplus$, i.e., the previous-time trace operator $\ominus$.

As a consequence of Theorem 3.10, we can also provide a characterization of $\mathrm{Shell}_{\oplus}(\rho^{\forall}_M)$ as a function. Given $\langle i, \sigma\rangle \in \mathbb{T}$, $M \in \wp(\mathbb{T})$ and $k \in \mathbb{Z}$, let us define:

$$M^k_{\downarrow\langle i,\sigma\rangle} \stackrel{\mathrm{def}}{=} \{\langle j, \tau\rangle \in M \mid \tau_{j+k} = \sigma_{i+k}\}.$$

This is a generalization of the (current) state projection, since $M_{\downarrow\sigma_i} = M^0_{\downarrow\langle i,\sigma\rangle}$. In particular, if $k \in \mathbb{N}$, $M^{-k}_{\downarrow\langle i,\sigma\rangle}$ can be thought of as the k-th past state projection of M.

Theorem 3.11 $\mathrm{Shell}_{\oplus}(\rho^{\forall}_M) = \lambda X.\{\langle i, \sigma\rangle \in M \mid \exists k \in \mathbb{N}.\ M^{-k}_{\downarrow\langle i,\sigma\rangle} \subseteq X\}$.

PROOF. By Theorem 3.10, we have that $\mathrm{Shell}_{\oplus}(\rho^{\forall}_M) = \lambda X.\cup\{\ominus^n(Z) \mid n \in \mathbb{N},\, Z \in \rho^{\forall}_M, \ominus^n(Z) \subseteq X\}$. Thus, let us show that for any $X \subseteq \mathbb{T}$,

$$\cup\{\ominus^n(Z) \mid n \in \mathbb{N},\, Z \in \rho^{\forall}_M,\, \ominus^n(Z) \subseteq X\} = \{\langle i, \sigma\rangle \in M \mid \exists k \in \mathbb{N}.\ M^{-k}_{\downarrow\langle i,\sigma\rangle} \subseteq X\}.$$

($\subseteq$): Let $\langle i, \sigma\rangle \in \ominus^n(Z)$, for some $n \in \mathbb{N}$ and $Z \in \rho^{\forall}_M$ such that $\ominus^n(Z) \subseteq X$. Then, $\langle i - n, \sigma\rangle \in Z$ and, since $Z \in \rho^{\forall}_M$, $\langle i - n, \sigma\rangle \in M$. Let us show that $M^{-n}_{\downarrow\langle i,\sigma\rangle} \subseteq X$. Consider $\langle j, \tau\rangle \in M$ such that $\tau_{j-n} = \sigma_{i-n}$. Since $\langle i-n, \sigma\rangle \in Z$ and $Z \in \rho^{\forall}_M$, we have that $\langle j-n, \tau\rangle \in Z$, so that $\langle j, \tau\rangle \in \ominus^n(Z)$. Hence, $\ominus^n(Z) \subseteq X$ implies $\langle j, \tau\rangle \in X$.
($\supseteq$): Consider $\langle i, \sigma\rangle \in M$ such that $M^{-k}_{\downarrow\langle i,\sigma\rangle} \subseteq X$ for some $k \geq 0$. We consider $M_{\downarrow\sigma_{i-k}} \in \rho^{\forall}_M$ and we observe that $\langle i, \sigma\rangle \in \ominus^k(M_{\downarrow\sigma_{i-k}})$. In order to conclude, let us check that $\ominus^k(M_{\downarrow\sigma_{i-k}}) \subseteq X$. Consider $\langle j, \tau\rangle \in \ominus^k(M_{\downarrow\sigma_{i-k}})$, so that $\langle j - k, \tau\rangle \in M_{\downarrow\sigma_{i-k}}$. Hence, $\tau_{j-k} = \sigma_{i-k}$, so that $\langle j, \tau\rangle \in M^{-k}_{\downarrow\langle i,\sigma\rangle} \subseteq X$, and therefore $\langle j, \tau\rangle \in X$. $\Box$

Thus, for any $X \in \wp(\mathbb{T})$, $\mathrm{Shell}_{\oplus}(\rho^{\forall}_M)(X)$ 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. The intuition is that while the universal closure $\rho^{\forall}_M$

considers present states only (i.e., $M_{\downarrow\sigma_i} \subseteq X$), as expected, completeness for next-time forces to take into account any past state (i.e., $\exists k \in \mathbb{N}.\ M^{-k}_{\downarrow\langle i,\sigma\rangle} \subseteq X$). Therefore, in order to design a suitable abstract domain for representing $\mathrm{Shell}_{\oplus}(\rho^{\forall}_M)$ we need "to prolong the abstract domain $\wp(\mathbb{S})_{\supseteq}$ in the past" as follows.

Definition 3.12 Define $\wp(\mathbb{S})^{\overleftarrow{\omega}} \stackrel{\text{def}}{=} \mathbb{Z}_{\leq 0} \to \wp(\mathbb{S})$, where $\mathbb{Z}_{\leq 0}$ is the set of nonpositive integers. Observe that $\wp(\mathbb{S})^{\overleftarrow{\omega}}$ is a complete lattice w.r.t. the standard pointwise ordering $\dot{\supseteq}$.
Given $z \in \mathbb{Z}_{\leq 0}$, $s \in \mathbb{S}$ and $M \in \wp(\mathbb{T})$, define $M^z_{\downarrow s} \stackrel{\text{def}}{=} \{\langle i, \sigma\rangle \in M \mid \sigma_{i+z} = s\}$.
The mappings $\alpha^{\oplus}_{\forall_M} : \wp(\mathbb{T}) \to \wp(\mathbb{S})^{\overleftarrow{\omega}}$ and $\gamma^{\oplus}_{\forall_M} : \wp(\mathbb{S})^{\overleftarrow{\omega}} \to \wp(\mathbb{T})$ are defined as follows:

$$\alpha^{\oplus}_{\forall_M}(X) \stackrel{\text{def}}{=} \lambda z \in \mathbb{Z}_{\leq 0}.\ \{s \in \mathbb{S} \mid M^z_{\downarrow s} \subseteq X\};$$
$$\gamma^{\oplus}_{\forall_M}(\Sigma) \stackrel{\text{def}}{=} \{\langle i, \sigma\rangle \in M \mid \exists k \in \mathbb{N}.\ \sigma_{i-k} \in \Sigma(-k)\}. \quad \square$$

Corollary 3.13 *$(\alpha^{\oplus}_{\forall_M}, \wp(\mathbb{T})_{\supseteq}, \wp(\mathbb{S})^{\overleftarrow{\omega}}_{\dot{\supseteq}}, \gamma^{\oplus}_{\forall_M})$ is a GC, and additionally a GI when $M = \mathscr{M}_{\rightarrow}$, for some total transition system $\langle \mathbb{S}, \rightarrow\rangle$, which induces the closure $\mathrm{Shell}_{\oplus}(\rho^{\forall}_M)$.*

PROOF. The fact that $(\alpha^{\oplus}_{\forall_M}, \wp(\mathbb{T})_{\supseteq}, \wp(\mathbb{S})^{\overleftarrow{\omega}}_{\dot{\supseteq}}, \gamma^{\oplus}_{\forall_M})$ is a GC/GI follows easily from the GC/GI $(\alpha^{\forall}_M, \wp(\mathbb{T})_{\supseteq}, \wp(\mathbb{S})_{\supseteq}, \gamma^{\forall}_M)$. Moreover, observe that $\gamma^{\oplus}_{\forall_M} \circ \alpha^{\oplus}_{\forall_M}$ coincides with the characterization of $\mathrm{Shell}_{\oplus}(\rho^{\forall}_M)$ given by Theorem 3.11. $\square$

Hence, the state abstract domain $\wp(\mathbb{S})_{\supseteq}$ needs to be refined to a domain of infinite sequences of sets of states, namely the "prolongation" of $\gamma^{\forall}_M$ in the past. We index the sequences $\Sigma \in \wp(\mathbb{S})^{\overleftarrow{\omega}}$ over $\mathbb{Z}_{\leq 0}$, so that for any and $i \in \mathbb{N}$, $\Sigma(-i) \in \wp(\mathbb{S})$ is reminiscent of a set of states at time $-i \in \mathbb{Z}_{\leq 0}$.

As a consequence, it is easy to design an abstract domain for representing the complete shell of the universal closure for both next- and previous-time. In fact, the prolongation of $\wp(\mathbb{S})_{\supseteq}$ both in the past and in the future leads to the Galois insertion $(\alpha^{\pm}_{\forall_M}, \wp(\mathbb{T})_{\supseteq}, \wp(\mathbb{S})^{\omega}_{\dot{\supseteq}}, \gamma^{\pm}_{\forall_M})$, where:

$$\alpha^{\pm}_{\forall_M}(X) \stackrel{\text{def}}{=} \lambda z \in \mathbb{Z}.\ \{s \in \mathbb{S} \mid M^z_{\downarrow s} \subseteq X\};$$
$$\gamma^{\pm}_{\forall_M}(\Sigma) \stackrel{\text{def}}{=} \{\langle i, \sigma\rangle \in M \mid \exists k \in \mathbb{Z}.\ \sigma_{i+k} \in \Sigma(k)\}.$$

Example 3.14 Let us consider again the two states transition system in Example 1.1 and the formula $\oplus\ominus p \in \mathfrak{L}_{\overset{\rightarrow}{\mu}}$, where $p = \boldsymbol{\sigma}_1$. Observe that $[\![\oplus\ominus p]\!] = [\![p]\!] = M_{\downarrow 1}$. The formula $\oplus\ominus p$ is not branchable, namely the abstract semantics of $\oplus\ominus p$ induced by $\rho^{\forall}_M$ is not complete. In fact, $\alpha^{\forall}_M([\![\oplus\ominus p]\!]) = \{1\}$ while $[\![\oplus\ominus p]\!]^{\forall}_M = \widetilde{\mathrm{pre}}_{\rightarrow}(\widetilde{\mathrm{post}}_{\rightarrow}(\alpha^{\forall}_M(M_{\downarrow 1}))) = \widetilde{\mathrm{pre}}_{\rightarrow}(\widetilde{\mathrm{post}}_{\rightarrow}(\{1\})) = \widetilde{\mathrm{pre}}_{\rightarrow}(\{1\}) = \varnothing$.
Let us check that for the above abstract domain $\wp(\mathbb{S})^{\omega}$ completeness does hold. In this case, the abstract semantics is as follows: $[\![\oplus \ominus p]\!]^{\pm}_M = \alpha^{\pm}_{\forall_M} \circ \bigoplus \circ \gamma^{\pm}_{\forall_M} \circ \alpha^{\pm}_{\forall_M} \circ$

$\ominus \circ \gamma^{\pm}_{\forall_M} \circ \alpha^{\pm}_{\forall_M}(M_{\downarrow 1})$. Hence, we have the following equalities:

$$\alpha^{\pm}_{\forall_M}(M_{\downarrow 1})(z) = \begin{cases} \varnothing & \text{if } z < 0 \\ \{1\} & \text{if } z \geq 0 \end{cases}$$

$$\gamma^{\pm}_{\forall_M}(\alpha^{\pm}_{\forall_M}(M_{\downarrow 1})) = M_{\downarrow 1}$$

$$\ominus(\gamma^{\pm}_{\forall_M}(\alpha^{\pm}_{\forall_M}(M_{\downarrow 1}))) = M_{\downarrow 1} \cup \{\langle i, \sigma\rangle \in M \mid \sigma_i = 2,\, \sigma_{i-1} = 1\}$$

$$\alpha^{\pm}_{\forall_M}(\ominus(\gamma^{\pm}_{\forall_M}(\alpha^{\pm}_{\forall_M}(M_{\downarrow 1}))))(z) = \begin{cases} \varnothing & \text{if } z < -1 \\ \{1\} & \text{if } z \geq -1 \end{cases}$$

$$\gamma^{\pm}_{\forall_M}(\alpha^{\pm}_{\forall_M}(\ominus(\gamma^{\pm}_{\forall_M}(\alpha^{\pm}_{\forall_M}(M_{\downarrow 1}))))) = M_{\downarrow 1} \cup \{\langle i, \sigma\rangle \in M \mid \sigma_i = 2,\, \sigma_{i-1} = 1\}$$

$$\oplus(\gamma^{\pm}_{\forall_M}(\alpha^{\pm}_{\forall_M}(\ominus(\gamma^{\pm}_{\forall_M}(\alpha^{\pm}_{\forall_M}(M_{\downarrow 1})))))) = M_{\downarrow 1}$$

As a consequence, it turns out that

$$\begin{aligned} \alpha^{\pm}_{\forall_M}([\![\oplus\ominus p]\!]) &= \alpha^{\pm}_{\forall_M}(M_{\downarrow 1}) \\ &= \alpha^{\pm}_{\forall_M}(\oplus(\gamma^{\pm}_{\forall_M}(\alpha^{\pm}_{\forall_M}(\ominus(\gamma^{\pm}_{\forall_M}(\alpha^{\pm}_{\forall_M}(M_{\downarrow 1}))))))) = [\![\oplus\ominus p]\!]^{\pm}_M \end{aligned}$$

namely completeness holds for this abstract domain. □

3.3 Time reversal

Let us now analyze the time reversal operator. The universal abstraction for the reversed model $\curvearrowleft M$ is characterized as follows. Of course, notice that if M is generated by a transition system $\langle \mathbb{S}, \rightarrow\rangle$ then $\curvearrowleft M$ is the model generated by the reversed transition system $\langle \mathbb{S}, \leftarrow\rangle$.

Lemma 3.15 $\rho^{\forall}_{\curvearrowleft M} = \curvearrowleft \circ \rho^{\forall}_M \circ \curvearrowleft$.

PROOF. Let us show that $\curvearrowleft(\rho^{\forall}_M(\curvearrowleft X)) = \rho^{\forall}_{\curvearrowleft M}(X)$. Let $\langle i, \sigma\rangle \in \curvearrowleft(\rho^{\forall}_M(\curvearrowleft X))$. We have that $\curvearrowleft\langle i, \sigma\rangle \in \rho^{\forall}_M(\curvearrowleft X)$, and therefore $\curvearrowleft\langle i, \sigma\rangle \in M$ and $M_{\downarrow\sigma_i} \subseteq \curvearrowleft X$. This implies $\langle i, \sigma\rangle \in \curvearrowleft M$ and $\curvearrowleft(M_{\downarrow\sigma_i}) \subseteq X$. Since $\curvearrowleft(M_{\downarrow\sigma_i}) = (\curvearrowleft M)_{\downarrow\sigma_i}$, this means that $\langle i, \sigma\rangle \in \rho^{\forall}_{\curvearrowleft M}(X)$. On the other hand, the previous implications actually are equivalences, and thus the reverse inclusion simply follows by going backward. □

3.3.1 Complete core

Theorem 2.1 allows us here to show that the complete core is given by those fixpoints of $\rho^{\forall}_M$ which also belong to the universal closure $\rho^{\forall}_{\curvearrowleft M}$ relative to the reversed model $\curvearrowleft M$.

Theorem 3.16 *The set of fixpoints of* $\mathrm{Core}_{\curvearrowleft}(\rho^{\forall}_M)$ *is* $\{Y \in \wp(\mathbb{T}) \mid Y, \curvearrowleft Y \in \rho^{\forall}_M\}$. *Moreover,* $\mathrm{Core}_{\curvearrowleft}(\rho^{\forall}_M) = \rho^{\forall}_M \sqcup \rho^{\forall}_{\curvearrowleft M}$.

PROOF. By Theorem 2.1 and Remark 2.3, $\mathrm{Core}_{\curvearrowleft}(\rho^{\forall}_M) = \sqcup_{i\in\mathbb{N}} L^i_{\curvearrowleft}(\rho^{\forall}_M)$, where $L_{\curvearrowleft}(\eta) = \{Y \in \wp(\mathbb{T}) \mid \cap\{X \in \wp(\mathbb{T}) \mid \curvearrowleft X \supseteq Y\} \in \eta\}$. Since $\curvearrowleft X \supseteq Y \Leftrightarrow X \supseteq \curvearrowleft Y$, we have that $L_{\curvearrowleft}(\eta) = \{Y \in \wp(\mathbb{T}) \mid \curvearrowleft Y \in \eta\}$. Thus, for any $j > 0$, $L^{2j}_{\curvearrowleft}(\rho^{\forall}_M) = \rho^{\forall}_M$ and $L^{2j+1}_{\curvearrowleft}(\rho^{\forall}_M) = L_{\curvearrowleft}(\rho^{\forall}_M)$. Hence, $\sqcup_{i\in\mathbb{N}} L^i_{\curvearrowleft}(\rho^{\forall}_M) = \rho^{\forall}_M \sqcup L_{\curvearrowleft}(\rho^{\forall}_M) = \{Y \in \wp(\mathbb{T}) \mid Y, \curvearrowleft Y \in \rho^{\forall}_M\}$. Moreover, let us observe that $\curvearrowleft Y \in \rho^{\forall}_M \Leftrightarrow \rho^{\forall}_M(\curvearrowleft Y) = \curvearrowleft Y \Leftrightarrow \curvearrowleft(\rho^{\forall}_M(\curvearrowleft Y)) = Y$. Therefore, by Lemma 3.15, we have that $\curvearrowleft Y \in \rho^{\forall}_M \Leftrightarrow Y \in \rho^{\forall}_{\curvearrowleft M}$, and thus $\mathrm{Core}_{\curvearrowleft}(\rho^{\forall}_M) = \rho^{\forall}_M \sqcup \rho^{\forall}_{\curvearrowleft M}$. □

This allows us to give a characterization of transition systems that induce universal closures which are complete for time reversal. It turns out that these are the symmetric transition systems: a relation $\rightarrow$ is symmetric when $\forall r, s \in \mathbb{S}.\, r \rightarrow s \;\Rightarrow\; s \rightarrow r$. This means that in symmetric transition systems any computation step is reversibile.

Corollary 3.17 *Let* $M = \mathscr{M}_{\rightarrow}$ *for some total transition system* $\langle \mathbb{S}, \rightarrow \rangle$. *Then,* $\rho^{\forall}_M$ *is complete for* $\curvearrowleft$ *if and only if* $\rightarrow$ *is symmetric.*

PROOF. Let us first observe that $\rightarrow$ is symmetric iff $M = \curvearrowleft M$. Let us show that $\rho^{\forall}_{\curvearrowleft M} \sqsubseteq \rho^{\forall}_M \;\Rightarrow\; M = \curvearrowleft M$: we have that $\curvearrowleft M = \rho^{\forall}_{\curvearrowleft M}(\mathbb{T}) \supseteq \rho^{\forall}_M(\mathbb{T}) = M$, and in turn, by applying $\curvearrowleft$, $M \supseteq \curvearrowleft M$, that is $\curvearrowleft M = M$. Thus, $\rho^{\forall}_{\curvearrowleft M} \sqsubseteq \rho^{\forall}_M \;\Leftrightarrow\; M = \curvearrowleft M$. Moreover, by Theorem 3.16, $\rho^{\forall}_M$ is complete for $\curvearrowleft$ iff $\mathrm{Core}_{\curvearrowleft}(\rho^{\forall}_M) = \rho^{\forall}_M$ iff $\rho^{\forall}_{\curvearrowleft M} \sqsubseteq \rho^{\forall}_M$. Hence, this closes the proof. □

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

Example 3.18 Consider the abstract counter and the abstract traffic light controller in Example 3.9. The transition relations of both systems are symmetric, so that, by Corollary 3.17, the universal closure is complete for time reversal. This is not the case of the concrete three-state traffic light controller, since the transition relation is not symmetric. Observe that the model generated by this transition system is as follows:

$$M = \{\langle i, \cdots \mathit{red\ green\ yellow\ red\ green\ yellow} \cdots \rangle \mid i \in \mathbb{Z}\}.$$

Thus, for any $Y \subseteq M$, $Y, \curvearrowleft Y \in \rho^{\forall}_M$ holds if and only if $Y = \varnothing$. Therefore, by Theorem 3.16, $\mathrm{Core}_{\curvearrowleft}(\rho^{\forall}_M) = \{\varnothing\}$, i.e., the complete core is the trivial abstract domain representing no information. □

3.3.2 Complete shell

Let us now apply our constructive approach to characterize the complete shell.

Theorem 3.19 *The set of fixpoints of* $\mathrm{Shell}_{\curvearrowleft}(\rho^{\forall}_M)$ *is* $\mathrm{Cl}^{\cup}(\rho^{\forall}_M \cup \{Y \in \wp(\mathbb{T}) \mid \curvearrowleft Y \in \rho^{\forall}_M\})$. *Moreover,* $\mathrm{Shell}_{\curvearrowleft}(\rho^{\forall}_M) = \rho^{\forall}_M \sqcap \rho^{\forall}_{\curvearrowleft M}$.

PROOF. By Theorem 2.1 and Remark 2.3, $\mathrm{Shell}_{\curvearrowleft}(\rho^{\forall}_M) = \sqcap_{i\in\mathbb{N}} R^i_{\curvearrowleft}(\rho^{\forall}_M)$, where $R_{\curvearrowleft}(\eta) = \mathrm{Cl}^{\cup}(\{\cap\{X \in \wp(\mathbb{T}) \mid \curvearrowleft X \supseteq Y\} \mid Y \in \eta\}) = \mathrm{Cl}^{\cup}(\{\curvearrowleft Y \mid Y \in \eta\}) = \mathrm{Cl}^{\cup}(\{Y \mid \curvearrowleft Y \in \eta\})$. Since $\curvearrowleft$ preserves arbitrary unions, for any $j > 0$, $R^{2j}_{\curvearrowleft}(\rho^{\forall}_M) = \rho^{\forall}_M$ and $R^{2j+1}_{\curvearrowleft}(\rho^{\forall}_M) = R_{\curvearrowleft}(\rho^{\forall}_M)$. Hence, we have that $\sqcap_{i\in\mathbb{N}} R^i_{\curvearrowleft}(\rho^{\forall}_M) = \rho^{\forall}_M \sqcap R_{\curvearrowleft}(\rho^{\forall}_M) = \mathrm{Cl}^{\cup}(\rho^{\forall}_M \cup \{Y \mid \curvearrowleft(Y) \in \rho^{\forall}_M\})$. Moreover, as observed in the proof of Theorem 3.16, $\curvearrowleft Y \in \rho^{\forall}_M \Leftrightarrow \curvearrowleft(\rho^{\forall}_M(\curvearrowleft Y)) = Y$, and therefore, by Lemma 3.15, $R_{\curvearrowleft}(\rho^{\forall}_M) = \rho^{\forall}_{\curvearrowleft M}$, so that we obtain that $\mathrm{Shell}_{\curvearrowleft}(\rho^{\forall}_M) = \rho^{\forall}_M \sqcap \rho^{\forall}_{\curvearrowleft M}$. □

It is therefore simple to design an abstract domain for representing this complete shell. We consider the abstract domain $\wp(\mathbb{S})^2_{\supseteq}$ as related to the concrete domain $\wp(\mathbb{T})_{\supseteq}$ by the following abstraction and concretization maps:

$$\alpha^{\curvearrowleft}_{\forall_M} \stackrel{\text{def}}{=} \lambda X.\langle \alpha^{\forall}_M(X), \alpha^{\forall}_{\curvearrowleft M}(X)\rangle;$$
$$\gamma^{\curvearrowleft}_{\forall_M} \stackrel{\text{def}}{=} \lambda\langle X_1, X_2\rangle.\gamma^{\forall}_M(X_1) \cup \gamma^{\forall}_{\curvearrowleft M}(X_2).$$

As a consequence of Theorem 3.19, it turns out $\mathrm{Shell}_{\curvearrowleft}(\rho^{\forall}_M)$ is the closure induced by the GI $(\alpha^{\curvearrowleft}_{\forall_M}, \wp(\mathbb{T})_{\supseteq}, \wp(\mathbb{S})^2_{\supseteq}, \gamma^{\curvearrowleft}_{\forall_M})$. Thus, the above result tells us that completeness for time reversal requires an additional component taking into account the universal abstraction for the reversed model $\curvearrowleft M$.

3.4 Disjunction

Finally, let us consider disjunction, namely set-union in the concrete domain $\wp(\mathbb{T})$.

3.4.1 Complete core

Theorem 3.20 $\mathrm{Core}_{\cup}(\rho^{\forall}_M) = \lambda X.\varnothing$.

PROOF. By Theorem 2.1 and Remark 2.3, $\mathrm{Core}_{\cup}(\rho^{\forall}_M) = \sqcup_{i\in\mathbb{N}} L^i_{\cup}(\rho^{\forall}_M)$, where $L_{\cup}(\eta) = \{Y \in \wp(\mathbb{T}) \mid \{\cap\{Z \in \wp(\mathbb{T}) \mid Z \cup X \supseteq Y\}\}_{X\in\wp(\mathbb{T})} \subseteq \eta\}$. Note that, for any $X, Y \in \wp(\mathbb{T})$, $\cap\{Z \in \wp(\mathbb{T}) \mid Z \cup X \supseteq Y\} = Y \cap \neg X$ and $\downarrow Y \stackrel{\text{def}}{=} \{Z \in \wp(\mathbb{T}) \mid Z \subseteq Y\} = \{Y \cap \neg X \mid X \in \wp(\mathbb{T})\}$. Thus, $L_{\cup}(\eta) = \{Y \in \wp(\mathbb{T}) \mid \downarrow Y \subseteq \eta\}$. Also, let us observe that $L_{\cup}(\eta) \subseteq \eta$ and $\downarrow L_{\cup}(\eta) = L_{\cup}(\eta)$, so that, for any $i \geq 2$,

$L^i_\cup(\rho^\forall_M) = L_\cup(\rho^\forall_M)$, and therefore $\sqcup_{i\in\mathbb{N}} L^i_\cup(\rho^\forall_M) = \{Y \in \wp(\mathbb{T}) \mid \downarrow Y \subseteq \rho^\forall_M\}$. Consider now some $Y \in \wp(\mathbb{T})$ such that $\downarrow Y \subseteq \rho^\forall_M$. Then, $Y \in \rho^\forall_M$, so that there exists some $S \subseteq \mathbb{S}$ such that $Y = \gamma^\forall_M(S)$. If $s \in S$ then there exists some $\langle i, \sigma\rangle \in M_{\downarrow s} \subseteq \gamma^\forall_M(S)$, so that $\{\langle i, \sigma\rangle\} \subseteq Y$. It turns out that $\{\langle i, \sigma\rangle\} \notin \rho^\forall_M$ because $\gamma^\forall_M(\{\sigma_i\}) = M_{\downarrow\sigma_i}$ and, by Hypothesis 2.6 (i), $|M_{\downarrow\sigma_i}| > 1$. This means that if $S \neq \varnothing$ then $\downarrow Y \not\subseteq \rho^\forall_M$. Thus, $\mathrm{Core}_\cup(\rho^\forall_M) = \{\varnothing\}$, i.e., the core is the greatest closure $\lambda X.\varnothing$. □

The greatest closure $\lambda X.\varnothing$ represents the straightforward uninformative abstract domain consisting of a unique abstract value which is the abstraction of any concrete value. The above result states that there is no further abstraction, but for the straightforward abstraction, of the universal abstraction which is complete for disjunction. As a consequence, we will prove later that any abstraction, but for the straightforward one, of the state-based model checking for a temporal calculus that includes an unrestricted connective of disjunction is incomplete for the trace-based semantics.

3.4.2 Complete shell

Theorem 3.21 $\mathrm{Shell}_\cup(\rho^\forall_M) = \lambda X.X \cap M$*, so that the set of fixpoints of* $\mathrm{Shell}_\cup(\rho^\forall_M)$ *is* $\{X \in \wp(\mathbb{T}) \mid X \subseteq M\}$.

PROOF. By Theorem 2.1 and Remark 2.3, $\mathrm{Shell}_\cup(\rho^\forall_M) = \sqcap_{i\in\mathbb{N}} R^i_\cup(\rho^\forall_M)$, where $R_\cup(\eta) = \mathrm{Cl}^\cup(\{\cap\{X \in \wp(\mathbb{T}) \mid X \cup Y \supseteq Z\}\}_{Y\in\wp(\mathbb{T}),\, Z\in\eta}) = \mathrm{Cl}^\cup(\{Z \cap \neg Y \mid Y \in \wp(\mathbb{T}),\ Z \in \eta\}) = \mathrm{Cl}^\cup(\{Z \cap Y \mid Y \in \wp(\mathbb{T}),\ Z \in \eta\})$. Thus, we have that $\sqcap_{i\in\mathbb{N}} R^i_\cup(\rho^\forall_M) = R_\cup(\rho^\forall_M)$. It remains to observe that $\mathrm{Cl}^\cup(\{Z \cap Y \mid Y \in \wp(\mathbb{T}),\ Z \in \eta\}) = \{X \in \wp(\mathbb{T}) \mid X \subseteq M\}$: this is an immediate set-theoretic consequence of the fact that $M \in \rho^\forall_M$ and that if $Z \in \rho^\forall_M$ then $Z \subseteq M$. Moreover, let us also note that the set of fixpoints of $\lambda X.X \cap M$ is $\{X \in \wp(\mathbb{T}) \mid X \subseteq M\}$. □

As a consequence, let us also notice that $\mathrm{Shell}_\cup(\rho^\forall_M)$ is the closure induced by the GI $(\alpha^\cup_{\forall_M}, \wp(\mathbb{T})_\supseteq, \wp(M)_\supseteq, \gamma^\cup_{\forall_M})$, where $\alpha^\cup_{\forall_M} \stackrel{\text{def}}{=} \lambda X.X \cap M$ and $\gamma^\cup_{\forall_M} \stackrel{\text{def}}{=} \lambda X.X$. Hence, the complete shell of the universal abstraction for the union is "essentially" the identity mapping. More precisely, for a given model M, the closure $\mathrm{Shell}_\cup(\rho^\forall_M)$ can be represented by the abstract domain $\wp(M)_\supseteq$ endowed with the abstraction map $\lambda X.X \cap M$ which simply removes those traces which are not in M. This means that completeness for disjunction indeed requires all the traces in M.

Once again the above complete shell was characterized by exploiting the constructive method in Section 2.2.3. This complete shell can be also obtained in a noncon-

structive way [1] .

Lemma 3.22 *Let X be any set and $\rho \in \mathrm{uco}(\wp(X)_{\supseteq})$ such that $\rho(M) = M$. If ρ is finitely additive then for any $Z \subseteq M$, $\rho(Z) = Z$.*

PROOF. Assume by contradiction that $Z \subseteq M$ is such that $\rho(Z) \subsetneq Z$, and let $x \in Z \smallsetminus \rho(Z)$. Then, $x \notin M \smallsetminus Z$, so that $x \notin \rho(M \smallsetminus Z)$. Moreover, since $\rho(M \cap Z) \subseteq \rho(Z)$, we also have that $x \notin \rho(M \cap Z)$. On the other hand, $x \in M = \rho(M) = \rho((M \cap Z) \cup M \smallsetminus Z)$, so that $\rho(M \cap Z) \cup \rho(M \smallsetminus Z) \subsetneq \rho((M \cap Z) \cup (M \smallsetminus Z))$, i.e., ρ is not additive, a contradiction. □

Let us observe that $\rho \in \mathrm{uco}(\wp(\mathbb{T})_{\supseteq})$ is complete for finite set-union when for any $X, Y \in \wp(\mathbb{T})$, $\rho(X \cup Y) = \rho(\rho(X) \cup \rho(Y)) = \rho(X) \cup \rho(Y)$, that is, when ρ is finitely additive. This observation allows us to show that $\mathrm{Shell}_{\cup}(\rho^{\forall}_M) = \lambda X.X \cap M$ in a nonconstructive way: by Lemma 3.22, since $M \in \rho^{\forall}_M \subseteq \mathrm{Shell}_{\cup}(\rho^{\forall}_M)$, it turns out that for any $X \subseteq M$, $X \in \mathrm{Shell}_{\cup}(\rho^{\forall}_M)$; hence, $\{X \in \wp(\mathbb{T}) \mid X \subseteq M\} \subseteq \mathrm{Shell}_{\cup}(\rho^{\forall}_M)$, and since $\{X \in \wp(\mathbb{T}) \mid X \subseteq M\}$ is (the set of fixpoints of) the closure $\lambda X.X \cap M$ which is finitely additive, i.e. complete for set-union, we have that $\mathrm{Shell}_{\cup}(\rho^{\forall}_M) = \lambda X.X \cap M$. Let us remark that in this easy nonconstructive proof one first needs to guess some abstract domain and then to prove that this is indeed the complete shell. By contrast, our proof (of Theorem 3.21) is easy as well and, more importantly, constructive so that it is enough to apply the methodology in Section 2.2.3 to characterize the complete shell.

3.5 All the connectives

To conclude our analysis, let us characterize the complete core and shell of the universal checking closure for all the connectives of the $\widehat{\mu t}$-calculus, i.e., the set TT of all the trace transformers. We need to take care of the following technicality. As far as the universal quantifier is concerned, the following restriction is needed. We just consider the unary restrictions $\lambda X.\forall(N, X) : \wp(\mathbb{T}) \to \wp(\mathbb{T})$, where $N \subseteq M \cup \curvearrowleft M$, because the binary trace transformer $\forall : \wp(\mathbb{T}) \times \wp(\mathbb{T}) \to \wp(\mathbb{T})$ is neither monotone nor antitone in its first argument, while given any $N \in \wp(\mathbb{T})$, the unary restriction $\lambda X.\forall(N, X)$ is instead monotone. Standard universal quantification can be expressed, because, as recalled in Section 2.3, $\forall\phi \stackrel{\text{def}}{=} \forall\,(\boxplus\boldsymbol{\pi}_{\to}) : \phi$, where $[\![\,\boxplus(\boldsymbol{\pi}_{\to})]\!] = \mathscr{M}_{\to}$. In the sequel, we will use the following compact notation: $M^* \stackrel{\text{def}}{=} M \cup \curvearrowleft M$. Hence, the set of trace transformers of the $\widehat{\mu t}$-calculus is $\mathrm{TT} \stackrel{\text{def}}{=} \{\boldsymbol{\sigma}_S\}_{S \in \wp(\mathbb{S})} \cup \{\boldsymbol{\pi}_t\}_{t \in \wp(\mathbb{S}^2)} \cup \{\oplus, \cup, \neg, \curvearrowleft\} \cup \{\lambda X.\forall(N, X)\}_{N \subseteq M^*}$. As TT

[1] This has been suggested by one anonymous referee.

includes negation which is antimonotone, observe that the existence of the complete core and shell of the universal closure for all the connectives is not guaranteed. However, since the complete core of $\rho^{\forall}_M$ for negation and disjunction is the greatest closure $\lambda X.\varnothing$ (by Theorems 3.3 and 3.20), as a straight consequence we obtain that $\lambda X.\varnothing$ is also the complete core of $\rho^{\forall}_M$ for the set TT of trace transformers, that is $\mathrm{Core}_{\mathrm{TT}}(\rho^{\forall}_M) = \lambda X.\varnothing$. On the other hand, the complete shell for all the connectives does exist and is as follows.

Theorem 3.23 $\mathrm{Shell}_{\mathrm{TT}}(\rho^{\forall}_M) = \lambda X.X \cap M^*$*, so that the set of fixpoints of* $\mathrm{Shell}_{\mathrm{TT}}(\rho^{\forall}_M)$ *is* $\{X \in \wp(\mathbb{T}) \mid X \subseteq M^*\}$.

PROOF. Let $\rho = \lambda X.X \cap M^*$ and note that this is a closure on $\wp(\mathbb{T})_{\supseteq}$. The following points show that $\rho \in \Gamma(\wp(\mathbb{T})_{\supseteq}, \mathrm{TT})$.
(1) $\rho \in \Gamma(\wp(\mathbb{T})_{\supseteq}, \{\boldsymbol{\sigma}_S\}_{S\in\wp(\mathbb{S})} \cup \{\boldsymbol{\pi}_t\}_{t\in\wp(\mathbb{S}^2)})$ because $\boldsymbol{\sigma}_S$ and $\boldsymbol{\pi}_t$ are 0-ary operators.
(2) $\rho \in \Gamma(\wp(\mathbb{T})_{\supseteq}, \oplus)$. Since $\oplus$ preserves unions and intersections, given $X \in \wp(\mathbb{T})$, $\rho(\oplus(\rho(X))) = \rho(\oplus(X) \cap (\oplus(M) \cup \oplus(\curvearrowleft(M)))) = \oplus(X) \cap (\oplus(M) \cup \oplus(\curvearrowleft(M)))\cap(M\cup\curvearrowleft(M))$. Also, by Hypothesis 2.6 (ii), $\oplus(M) = M$ and $\oplus(\curvearrowleft(M)) = \curvearrowleft(M)$, and therefore $\rho(\oplus(\rho(X))) = \oplus(X) \cap (M \cup \curvearrowleft(M)) = \rho(\oplus(X))$.
(3) $\rho \in \Gamma(\wp(\mathbb{T})_{\supseteq}, \cup)$. In fact, $\rho(\rho(X) \cup \rho(Y)) = \rho((X \cap M^*) \cup (Y \cap M^*)) = \rho((X \cup Y) \cap M^*) = (X \cup Y) \cap M^* = \rho(X \cup Y)$.
(4) $\rho \in \Gamma(\wp(\mathbb{T})_{\supseteq}, \neg)$. In fact, $\rho(\neg\rho(X)) = (\neg(X \cap M^*)) \cap M^* = ((\neg X) \cap M^*) \cup ((\neg M^*) \cap M^*) = (\neg X) \cap M^* = \rho(\neg X)$.
(5) $\rho \in \Gamma(\wp(\mathbb{T})_{\supseteq}, \curvearrowleft)$. As $\curvearrowleft$ preserves intersections and, by Hypothesis 2.6 (ii), $\curvearrowleft(M^*) = M^*$, we have that $\rho(\curvearrowleft(\rho(X))) = \rho(\curvearrowleft(X \cap M^*)) = \rho(\curvearrowleft(X) \cap M^*) = \curvearrowleft(X) \cap M^* = \rho(\curvearrowleft(X))$.
(6) $\rho \in \Gamma(\wp(\mathbb{T})_{\supseteq}, \{\lambda X.\forall(N, X)\}_{N\subseteq M})$. Let $N \subseteq M$ and $X \in \wp(\mathbb{T})$, and observe that for any $\langle i, \sigma\rangle \in N$, we have that $N_{\downarrow\sigma_i} \subseteq X \cap (M^*) \Leftrightarrow (N_{\downarrow\sigma_i} \subseteq X)$. Thus, $\rho(\forall(N, \rho(X))) = \{\langle i, \sigma\rangle \in N \mid N_{\downarrow\sigma_i} \subseteq X \cap M^*\} \cap M^* = \{\langle i, \sigma\rangle \in N \mid N_{\downarrow\sigma_i} \subseteq X\} \cap M^* = \rho(\forall(N, X))$.
To conclude, consider any $\eta \in \mathrm{uco}(\wp(\mathbb{T})_{\supseteq})$ such that $\eta \in \Gamma(\wp(\mathbb{T})_{\supseteq}, \mathrm{TT})$ and $\eta \sqsubseteq \rho^{\forall}_M$. Since $\eta \in \Gamma(\wp(\mathbb{T})_{\supseteq}, \cup)$, by Theorem 3.21, we have that $\eta \sqsubseteq \mathrm{Shell}_{\cup}(\rho^{\forall}_M) = \lambda X.X \cap M$. Moreover, $\eta \in \Gamma(\wp(\mathbb{T})_{\supseteq}, \curvearrowleft)$, and hence, by Theorem 3.19, $\eta \sqsubseteq \mathrm{Shell}_{\curvearrowleft}(\rho^{\forall}_M) = \rho^{\forall}_M \sqcap \rho^{\forall}_{\curvearrowleft M} \sqsubseteq \rho^{\forall}_{\curvearrowleft M}$. Thus, because $\eta \sqsubseteq \rho^{\forall}_{\curvearrowleft M}$ and $\eta \in \Gamma(\wp(\mathbb{T})_{\supseteq}, \curvearrowleft)$, we have that $\eta \sqsubseteq \mathrm{Shell}_{\cup}(\rho^{\forall}_{\curvearrowleft M})$. By Theorem 3.21, $\mathrm{Shell}_{\cup}(\rho^{\forall}_{\curvearrowleft M}) = \lambda X.X \cap \curvearrowleft(M)$, so that $\eta \sqsubseteq \lambda X.X \cap \curvearrowleft(M)$. Hence, we obtained that $\eta \sqsubseteq (\lambda X.X \cap M) \sqcap (\lambda X.X \cap \curvearrowleft(M)) = \rho$. Thus, $\mathrm{Shell}_{\mathrm{TT}}(\rho^{\forall}_M) = \rho$. $\square$

Let us observe that $\wp(M^*)_{\supseteq}$ is a suitable abstract domain for representing this complete shell because the GI $(\alpha_{\forall_M}, \wp(\mathbb{T})_{\supseteq}, \wp(M^*)_{\supseteq}, \gamma_{\forall_M})$, where $\alpha_{\forall_M} \stackrel{\mathrm{def}}{=} \lambda X.X \cap M^*$ and $\gamma_{\forall_M} \stackrel{\mathrm{def}}{=} \lambda X.X$, induces the closure $\lambda X.X \cap M^*$. The abstract domain $\wp(M^*)$ therefore represents the traces both of the system $\langle \mathbb{S}, \rightarrow\rangle$ and of the reversed system $\langle \mathbb{S}, \leftarrow\rangle$.

Let us remark that by exploiting the above results in Sections 3.1-3.4, it is not hard to characterize the complete shell of the universal abstraction for any subset of trace transformers. For example, when we leave out the reversal operator from TT, as one expects, it is easy to show that in this case $\mathrm{Shell}_{\mathrm{TT}}(\rho^{\forall}_{M}) = \lambda X.X \cap M$.

4 Completeness of Temporal Languages

Let Op be any set of temporal connectives, where each $op \in Op$ has a corresponding arity $\sharp(op) \geq 0$ so that constants are viewed as connectives whose arity is 0. Following Cousot and Cousot [10, Section 8], Op induces a corresponding fixpoint temporal language $\mathfrak{L}_{Op}$ which is inductively defined as follows:

$$\mathfrak{L}_{Op} \ni \phi ::= X \mid op(\phi_1, ..., \phi_n) \mid \boldsymbol{\mu} X.\phi \mid \boldsymbol{\nu} X.\phi$$

where $X \in \mathbb{X}$ and $op \in Op$. Given any set $\mathbb{S}$ of states which determines a corresponding set $\mathbb{T}$ of traces, the semantics of any connective op with arity $n \geq 0$ is given by a corresponding trace transformer $\boldsymbol{op} : \wp(\mathbb{T})^n \to \wp(\mathbb{T})$. The set of trace transformers that provide the semantics of connectives in Op is denoted by $\boldsymbol{Op}$. Hence, this determines a trace semantics of $\mathfrak{L}_{Op}$, namely $[\![\cdot]\!] : \mathfrak{L}_{Op} \to \mathbb{E} \to \wp(\mathbb{T})$, which is inductively (and, due to fixpoints, possibly partially) defined as follows:

$$[\![X]\!]\xi = \xi(X)$$
$$[\![op(\phi_1, ..., \phi_n)]\!]\xi = \boldsymbol{op}([\![\phi_1]\!]\xi, ..., [\![\phi_n]\!]\xi)$$
$$[\![\boldsymbol{\mu} X.\phi]\!]\xi = \mathrm{lfp}(\lambda N \in \wp(\mathbb{T}).[\![\phi]\!]\xi[X/N])$$
$$[\![\boldsymbol{\nu} X.\phi]\!]\xi = \mathrm{gfp}(\lambda N \in \wp(\mathbb{T}).[\![\phi]\!]\xi[X/N])$$

Thus, any abstraction of the concrete domain $\wp(\mathbb{T})$ induces an abstract semantics for $\mathfrak{L}_{Op}$. As described in Section 2.4.3, the universal abstraction provides an example: the state semantics $[\![\cdot]\!]^{\forall}_{M}$ is the abstract semantics induced by $\rho^{\forall}_{M} \in \mathrm{uco}(\wp(\mathbb{T}_{\supseteq}))$. In general, any abstract domain $\rho \in \mathrm{uco}(\wp(\mathbb{T})_{\supseteq})$ induces the set of abstract environments $\mathbb{E}^{\rho} \stackrel{\mathrm{def}}{=} \mathbb{X} \to \rho$. Hence, the abstract semantics $[\![\cdot]\!]^{\rho} : \mathfrak{L}_{Op} \to \mathbb{E}^{\rho} \to \rho$ is defined as follows:

$$[\![X]\!]^{\rho}\chi = \chi(X)$$
$$[\![op(\phi_1, ..., \phi_n)]\!]^{\rho}\chi = \rho(\boldsymbol{op}([\![\phi_1]\!]^{\rho}\chi, ..., [\![\phi_n]\!]^{\rho}\chi))$$
$$[\![\boldsymbol{\mu} X.\phi]\!]^{\rho}\chi = \mathrm{lfp}(\lambda N \in \rho.[\![\phi]\!]^{\rho}\chi[X/N])$$
$$[\![\boldsymbol{\nu} X.\phi]\!]^{\rho}\chi = \mathrm{gfp}(\lambda N \in \rho.[\![\phi]\!]^{\rho}\chi[X/N])$$

Given a concrete environment $\xi \in \mathbb{E}$, $\dot{\rho}(\xi) \stackrel{\mathrm{def}}{=} \lambda X.\rho(\xi(X)) \in \mathbb{E}^{\rho}$ is the corresponding abstract environment induced by ρ. Soundness of ρ for the language $\mathfrak{L}_{Op}$ means

that the abstract semantics $[\![\cdot]\!]^\rho$ is sound, namely for any $\phi \in \mathfrak{L}_{Op}$ and $\xi \in \mathbb{E}$, $\rho([\![\phi]\!]\xi) \subseteq [\![\phi]\!]^\rho \dot{\rho}(\xi)$. Completeness of ρ for $\mathfrak{L}_{Op}$ means that equality always holds. As usual, the abstract interpretation approach always ensures soundness, while completeness in general does not hold.

Given $\rho \in \mathrm{uco}(\wp(\mathbb{T})_{\supseteq})$, the complete shell of ρ for $\mathfrak{L}_{Op}$, when it exists, is the most abstract domain $\mathrm{Shell}_{\mathfrak{L}_{Op}}(\rho) \in \mathrm{uco}(\wp(\mathbb{T})_{\supseteq})$ such that $\mathrm{Shell}_{\mathfrak{L}_{Op}}(\rho) \sqsubseteq \rho$ and $\mathrm{Shell}_{\mathfrak{L}_{Op}}(\rho)$ is complete for $\mathfrak{L}_{Op}$. Complete cores for $\mathfrak{L}_{Op}$ are defined dually.

As recalled in Section 2.2.2, it turns out that if ρ is complete for some function f then ρ is also fixpoint complete for f. Thus, as a straight consequence we obtain that if $\rho \in \mathrm{uco}(\wp(\mathbb{T})_{\supseteq})$ is complete for $\boldsymbol{Op}$ and either ρ does not contain infinite descending chains or ρ is co-continuous then ρ is complete for $\mathfrak{L}_{Op}$. Moreover, it turns out that complete shells and cores for a temporal language $\mathfrak{L}_{Op}$ coincide with complete shells and cores for the corresponding set $\boldsymbol{Op}$ of trace transformers.

Theorem 4.1 *Let $\rho \in \mathrm{uco}(\wp(\mathbb{T})_{\supseteq})$. If $\mathrm{Shell}_{\boldsymbol{Op}}(\rho)$ exists and either it does not contain infinite descending chains or it is co-continuous then $\mathrm{Shell}_{\mathfrak{L}_{Op}}(\rho) = \mathrm{Shell}_{\boldsymbol{Op}}(\rho)$.*

PROOF. As recalled above, since $\mathrm{Shell}_{\boldsymbol{Op}}(\rho)$ is complete for $\boldsymbol{Op}$, we have that $\mathrm{Shell}_{\boldsymbol{Op}}(\rho)$ is complete for $\mathfrak{L}_{Op}$. Moreover, $\mathrm{Shell}_{\boldsymbol{Op}}(\rho) \sqsubseteq \rho$. Let us consider any $\eta \in \mathrm{uco}(\wp(\mathbb{T})_{\supseteq})$ such that $\eta \sqsubseteq \rho$ and η is complete for $\mathfrak{L}_{Op}$. Let us check that η is complete for $\boldsymbol{Op}$. Consider $\boldsymbol{op} \in \boldsymbol{Op}$ and, for simplicity, assume that $\boldsymbol{op}$ is unary. Given $T \in \wp(\mathbb{T})$, we consider an environment $\xi \in \mathbb{E}$ such that $\xi(X) = T$. Hence, by completeness of η for $\mathfrak{L}_{Op}$, we have that $\eta(\boldsymbol{op}(T)) = \eta(\boldsymbol{op}(\xi(X))) = \eta([\![op(X)]\!]\xi) = [\![op(X)]\!]^\eta \dot{\eta}(\xi) = \eta(\boldsymbol{op}(\eta(\xi(X)))) = \eta(\boldsymbol{op}(\eta(T)))$. Therefore, $\eta \sqsubseteq \mathrm{Shell}_{\boldsymbol{Op}}(\rho)$. As a consequence, it turns out that $\mathrm{Shell}_{\mathfrak{L}_{Op}}(\rho)$ exists and that $\mathrm{Shell}_{\mathfrak{L}_{Op}}(\rho) = \mathrm{Shell}_{\boldsymbol{Op}}(\rho)$. $\square$

Obviously, an analogous result holds for complete cores as well. This general result can be applied to the $\widehat{\mu}$-calculus. Recall that TT denotes the set of trace transformers of the $\widehat{\mu}$-calculus, where the universal quantifier is restricted to a unary operator. Let us denote by TT the corresponding set of temporal connectives of the $\widehat{\mu}$-calculus so that $\mathfrak{L}_{TT} \subseteq \mathfrak{L}_{\widehat{\mu}}$ is a slight restriction of the $\widehat{\mu}$-calculus where universal quantifications are unary. Consider any set $Op \subseteq TT$ of temporal connectives, that gives rise to the language $\mathfrak{L}_{Op} \subseteq \mathfrak{L}_{TT}$, and assume that the complete shell $\mathrm{Shell}_{\boldsymbol{Op}}(\rho^\forall_M)$ of the universal closure $\rho^\forall_M$ for the trace transformers in $\boldsymbol{Op}$ exists. Then, by Theorem 4.1, it turns out that $\mathrm{Shell}_{\mathfrak{L}_{Op}}(\rho^\forall_M) = \mathrm{Shell}_{\boldsymbol{Op}}(\rho^\forall_M)$. Analogously, this also holds for complete cores. Consequently, as far as the core is concerned, we have that

$$\mathrm{Core}_{\mathfrak{L}_{TT}}(\rho^\forall_M) = \lambda X.\varnothing.$$

On the other hand, by Theorem 3.23, it turns out that

$$\mathrm{Shell}_{\mathfrak{L}_{TT}}(\rho^\forall_M) = \lambda X.X \cap M^*.$$

Thus, in general, in order to obtain the complete shell/core of the universal closure for some fragment $\mathfrak{L}_{Op}$ of the $\hat{\mu}$-calculus it is enough to characterize the complete shell/core for the corresponding set $\boldsymbol{Op}$ of trace transformers. For example, if Op includes arbitrary disjunction but does not include time reversal, so that $\mathfrak{L}_{Op}$ is a future-time language, by the result mentioned at the end of Section 3.5, we have that $\mathrm{Shell}_{\mathfrak{L}_{Op}}(\rho^{\forall}_{M}) = \lambda X.X \cap M$.

5 Conclusion

This paper studied the completeness of state-based w.r.t. trace-based model checking by using a body of techniques based on abstract interpretation. By using a slogan, this study showed that "*the state-based model checking is intrinsically incomplete w.r.t. trace-based model checking*", since no refinement or abstraction of the standard state-based semantics for model checking induced by the universal/existential abstraction of past- and future-time specification languages can lead to a semantics whose corresponding model checking is complete for the trace semantics of the specification language.

The results of this paper suggest some research directions. An abstract interpretation-based approach to model checking for modal Kripke transition systems has been studied by Huth et al. [15]. It is then interesting to investigate whether the framework of modal transition systems based on three-valued logics affects the incompleteness of states w.r.t. traces. In view of the characterizations of transition systems provided by Theorem 3.8 and Corollary 3.17, it is also interesting to determine fragments of μ-calculi and classes of transition systems such that the universal/existential abstraction results to be complete. Finally, it is certainly interesting to investigate how completeness of state-based abstractions interacts with the presence of spurious counterexamples in abstract model checking. The works by Clarke et al. [3,4,5] on spurious counterexamples originated from the idea of systemically refining abstract models in order to enhance their precision. A spurious counterexample is an abstract trace which is an artificial counterexample generated by the approximation of the abstract model checker, namely there exists a concrete trace approximated by the spurious counterexample which is not a real counterexample. Clarke et al. devised a methodology for refining an partition-based abstract model relatively to a given temporal specification ϕ by using the spurious counterexamples provided by the abstract model checker on ϕ. The relationship between spurious counterexamples and the trace-semantics of temporal calculi has not been investigated from an abstract interpretation-based perspective and we believe that the results of this paper might shed some light on these issues.

Acknowledgements. We are grateful to the anonymous referees for their helpful comments. This work is an extended and revised version of two conference papers

[14,20] and was partially supported by the FIRB Project RBAU018RCZ "Abstract interpretation and model checking for the verification of embedded systems" and by the COFIN2004 Project "AIDA: Abstract Interpretation Design and Applications".

References

[1] C.H. Bennett. Logical reversibility of computation. *IBM J. Research Dev.*, 21:905-940, 1981.

[2] E.M. Clarke and I.A. Draghicescu. Expressibility results for linear time and branching time logics. In *Linear Time, Branching Time and Partial Order in Logics and Models for Concurrency*, LNCS 354, pp. 428–437, Springer, 1988.

[3] E.M. Clarke, O. Grumberg, S. Jha, Y. Lu, and H. Veith. Counterexample-guided abstraction refinement. In *Proc. of the 12th Internat. Conf. on Computer Aided Verification (CAV'00)*, LNCS 1855, pp. 154–169, Springer, 2000.

[4] E.M. Clarke, O. Grumberg, S. Jha, Y. Lu, and H. Veith. Counterexample-guided abstraction refinement for symbolic model checking. *J. ACM*, 50(5):752–794, 2003.

[5] E.M. Clarke, S. Jha, Y. Lu and H. Veith. Tree-like counterexamples in model checking. In *Proc. of the 17th IEEE Symp. on Logic in Computer Science (LICS'02)*, pp. 19–29, IEEE Press, 2002.

[6] E.M. Clarke, O. Grumberg, and D. E. Long. Model checking and abstraction. *ACM Trans. Program. Lang. Syst.*, 19(5):1512-1542, 1994.

[7] E.M. Clarke, O. Grumberg, and D. Peled. *Model checking*. The MIT Press, 1999.

[8] 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 Symp. on Principles of Programming Languages (POPL'77)*, pp. 238–252. ACM Press, 1977.

[9] P. Cousot and R. Cousot. Systematic design of program analysis frameworks. In *Proc. ACM Symp. on Principles of Programming Languages (POPL'79)*, pp. 269–282. ACM Press, 1979.

[10] P. Cousot and R. Cousot. Temporal abstract interpretation. In *Proc. ACM Symp. on Principles of Programming Languages (POPL'00)*, pp. 12–25. ACM Press, 2000.

[11] E.A. Emerson and J.Y. Halpern. "Sometimes" and "Not Never" revisited: on branching versus linear time temporal logic. *J. ACM*, 33(1): 151-178, 1986.

[12] R. Giacobazzi, F. Ranzato, and F. Scozzari. Making abstract interpretations complete. *J. ACM*, 47(2):361–416, 2000.

[13] R. Giacobazzi and E. Quintarelli. Incompleteness, counterexamples and refinements in abstract model checking. In *Proc. 8th Internat. Static Analysis Symposium (SAS'01)*, LNCS 2126, pp. 356-373, Springer, 2001.

[14] R. Giacobazzi and F. Ranzato. States vs. traces in model checking. In *Proc. 9th Internat. Static Analysis Symposium (SAS'02)*, LNCS 2477, pp. 461–476, 2002.

[15] M. Huth, R. Jagadeesan, and D. Schmidt. Modal transition systems: a foundation for three-valued program analysis. In *Proc. 10th European Symposium on Programming (ESOP'01)*, LNCS 2028, pp. 155-169, Springer, 2001.

[16] D. Kozen. Results on the propositional μ-calculus. *Theoret. Comput. Sci.*, 27:333-354, 1983.

[17] O. Kupferman and M. Vardi. Relating linear and branching model checking. In *Proc. IFIP Working Conference on Programming Concepts and Methods*, pp. 304–326, Chapman & Hall, 1998.

[18] L. Lamport. Sometimes is sometimes "not never" – on the temporal logic of programs. In *Proc. 7th ACM POPL*, pp. 174–185, 1980.

[19] M. Maidl. The common fragment of CTL and LTL. In *Proc. 41st IEEE Symposium on Foundations of Computer Science, FOCS'00*, pp. 643-652, IEEE Press, 2000.

[20] F. Ranzato. On the completeness of model checking. In *Proc. Proc. 10th European Symposium on Programming (ESOP'01)*, LNCS 2028, pp. 137-154, Springer, 2001.

[21] F. Ranzato and F. Tapparo. Strong preservation as completeness in abstract interpretation. In *Proc. Proc. 13th European Symposium on Programming (ESOP'04)*, LNCS 2986, pp. 18–32, Springer, 2004.

[22] F. Ranzato and F. Tapparo. An abstract interpretation-based refinement algorithm for strong preservation. In *Proc. 11th Internat. Conf. on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'05)*, LNCS 3440, pp. 140–156, Springer, 2005.

[23] F. Ranzato and F. Tapparo. An abstract interpretation perspective on linear vs branching time. In *Proc. 3rd Asian Symposium on Programming Languages and Systems (APLAS'05)*, LNCS 3780, pp. 69–85, Springer, 2005.

[24] D. Schmidt. From trace sets to modal transition systems by stepwise abstract interpretation. In *Proc. Workshop on Structure Preserving Relations*, Amagasaaki, Japan, 2001.

[25] M. Vardi. Sometimes and not never re-revisited: on branching versus linear time. In *Proc. 9th Internat. Conf. on Concurrence Theory (CONCUR'98)*, LNCS 1466, pp. 1-17, Springer, 1998.

[26] M. Vardi. Branching vs. linear time: final showdown. In *Proc. 7th Internat. Conf. on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'01)*, LNCS 2031, pp. 1-22, 2001.