Strong Preservation of Temporal Fixpoint-Based Operators by Abstract Interpretation

Francesco Ranzato and Francesco Tapparo

Dipartimento di Matematica Pura ed Applicata,
Università di Padova, Italy

Abstract. Standard abstract model checking relies on abstract Kripke structures which approximate the concrete model by gluing together indistinguishable states. Strong preservation for a specification language $\mathcal{L}$ encodes the equivalence of concrete and abstract model checking of formulas in $\mathcal{L}$. Abstract interpretation allows to design abstract models which are more general than abstract Kripke structures. In this paper we show how abstract interpretation-based models can be exploited in order to specify a general strongly preserving abstract model checking framework. This is shown in particular for specification languages including standard temporal operators which admit a characterization as least/greatest fixpoints, as e.g. standard "Finally", "Globally", "Until" and "Release" modalities.

1 Introduction

Abstract model checking is one successful and practical way to deal with the well-known state explosion problem of model checking in system verification [1, 3]. Standard abstract model checking [2] relies on abstract models which are based on partitions of the state space. Given a concrete model as a Kripke structure $\mathcal{K} = (\Sigma, \rightarrow)$, a standard abstract model is specified by an abstract Kripke structure $\mathcal{A} = (A, \rightarrow^\sharp)$ where the set A of abstract states is defined by a surjective map $h : \Sigma \rightarrow A$ and $\rightarrow^\sharp$ is an abstract transition relation on A. Thus, A determines a partition P_A of Σ and vice versa. A weak preservation result for some temporal language $\mathcal{L}$ guarantees that for any formula $\varphi \in \mathcal{L}$, if φ holds on the abstract model $\mathcal{A}$ then φ also holds on the concrete model $\mathcal{K}$. On the other hand, strong preservation means that any formula of $\mathcal{L}$ holds on $\mathcal{A}$ if and only if it holds on $\mathcal{K}$. Strong preservation is highly desirable since it allows to draw consequences from negative answers on the abstract side [3]. Thus, in order to design a standard abstract model we need both an appropriate partition of the space state and a suitable abstract transition relation.

The relationship between abstract interpretation and abstract model checking has been the subject of a number of works (see e.g. [2, 6, 7, 9, 10, 11, 15, 16, 19, 18]). We introduced in [17] an abstract interpretation-based framework for specifying generic strongly preserving abstract models, where a partition of the state space Σ is viewed as a particular abstract domain of the powerset $\wp(\Sigma)$, where $\wp(\Sigma)$ plays the role of concrete semantic domain. This generalized approach leads to a precise correspondence between forward complete abstract interpretations and strongly preserving abstract models. We deal with generic (temporal) languages $\mathcal{L}$ of state formulas which are inductively generated by a set AP of atomic propositions p and a set Op of operators f, i.e. $\mathcal{L} \ni \varphi ::= p \mid f(\varphi_1, ..., \varphi_n)$. A semantic interpretation $\boldsymbol{p} \subseteq \Sigma$ of atomic

E.A. Emerson and K.S. Namjoshi (Eds.): VMCAI 2006, LNCS 3855, pp. 332–347, 2006.

propositions and of operators $\boldsymbol{f} : \wp(\Sigma)^n \to \wp(\Sigma)$ determines a concrete semantic function $[\![\cdot]\!] : \mathcal{L} \to \wp(\Sigma)$ where $[\![p]\!] = \boldsymbol{p}$ and $[\![f(\varphi_1, ..., \varphi_n)]\!] = \boldsymbol{f}([\![\varphi_1]\!], ..., [\![\varphi_n]\!])$. Thus, any abstract domain A of $\wp(\Sigma)$ and corresponding abstract interpretation $\boldsymbol{p}^\sharp \in A$ and $\boldsymbol{f}^\sharp : A^n \to A$ for constants/operators, denoted by $I^\sharp$, induce an abstract semantic function $[\![\cdot]\!]^A : \mathcal{L} \to A$ where $[\![p]\!]^A = \boldsymbol{p}^\sharp$ and $[\![f(\varphi_1, ..., \varphi_n)]\!]^A = \boldsymbol{f}^\sharp([\![\varphi_1]\!]^A, ..., [\![\varphi_n]\!]^A)$. In particular, the abstract interpretation of $\boldsymbol{p}$ and $\boldsymbol{f}$ can be given as their best correct approximations on A, i.e. $\boldsymbol{p}^A \stackrel{\text{def}}{=} \alpha(\boldsymbol{p})$ and $\boldsymbol{f}^A \stackrel{\text{def}}{=} \alpha \circ \boldsymbol{f} \circ \gamma$ where α and γ are the abstraction and concretization maps relating A to $\wp(\Sigma)$. In this generalized setting, strong preservation goes as follows: the abstract interpretation $(A, I^\sharp)$ is strongly preserving for $\mathcal{L}$ when for any $S \subseteq \Sigma$ and $\varphi \in \mathcal{L}$, $S \subseteq [\![\varphi]\!] \Leftrightarrow \alpha(S) \leq [\![\varphi]\!]^A$. When A is an abstract domain representing a partition of Σ, this boils down to standard strong preservation for abstract Kripke structures, where different choices for the abstract transition relation $\to^\sharp$ correspond to different abstract interpretations of the operators $\boldsymbol{f}$.

It turns out that forward completeness implies strong preservation, i.e. if the abstract domain A is forward complete for the concrete constants/operators of $\mathcal{L}$ — this means that no loss of precision occurs by approximating each $\boldsymbol{p}$ and $\boldsymbol{f}$ on the abstract domain A — then A is strongly preserving for $\mathcal{L}$. The converse is in general not true. However, we show that when A is $\mathcal{L}$-covered — meaning that each abstract value $a \in A$ corresponds to some formula $\varphi \in \mathcal{L}$, i.e. $\gamma(a) = [\![\varphi]\!]$ — forward completeness and strong preservation are indeed equivalent notions and consequently the abstract interpretation of constants/operators of $\mathcal{L}$ as best correct approximations on A is the only possible choice in order to have strong preservation. One interesting point to remark is that when the abstract domain is a state partition P, an abstract transition relation $\to^\sharp$ on P such that the abstract Kripke structure $(P, \to^\sharp)$ strongly preserves $\mathcal{L}$ might not exist, while, in contrast, a strongly preserving abstract semantics on the partition P viewed as an abstract domain always exists.

The abstract semantics is therefore defined by approximating the interpretation of logical/temporal operators of $\mathcal{L}$ through their best correct approximations on the abstract domain A. In principle, this can be done for any logical/temporal operator. However, when a temporal operator $\boldsymbol{f}$ can be expressed as a least/greatest fixpoint of another temporal operator $\boldsymbol{g}$, e.g. $\boldsymbol{f} = \lambda X.\, \mathrm{lfp}(\lambda Y.\boldsymbol{g}(X, Y))$, the best correct approximation $\alpha \circ \boldsymbol{f} \circ \gamma$ might not be characterizable as a least/greatest fixpoint. For example, the existential "Finally" operator can be characterized as a least fixpoint by $\mathbf{EF}(X) = \mathrm{lfp}(\lambda Y.X \cup \mathbf{EX}(Y))$, where $\mathbf{EX} = \mathrm{pre}_{\to}$ is the standard predecessor transformer on the concrete Kripke structure. The best correct approximation of $\mathbf{EF}$ on an abstract domain A is therefore the abstract function $\alpha \circ \mathbf{EF} \circ \gamma : A \to A$. However, this definition gives us no clue for computing $\alpha \circ \mathbf{EF} \circ \gamma$ as a least fixpoint. By contrast, in standard abstract model checking the abstract interpretation of language operators is based on an abstract Kripke structure $\mathcal{A} = (P, \to^\sharp)$, so that it is enough to compute the least fixpoint $\mathrm{lfp}(\lambda Y^\sharp.X^\sharp \cup \mathbf{EX}^\sharp(Y^\sharp))$ on the abstract state space P, namely $X^\sharp$ and $Y^\sharp$ are sets of blocks in P, $\cup$ is union of sets of blocks and $\mathbf{EX}^\sharp = \mathrm{pre}_{\to^\sharp}$ is the predecessor transformer on $\mathcal{A}$. For example, for the language $\mathcal{L} \ni \varphi ::= p \mid \varphi_1 \wedge \varphi_2 \mid \mathrm{EF}\varphi$ if one can define a strongly preserving abstract Kripke structure $(P, \to^\sharp)$, where P is some partition of Σ, then the abstract Kripke structure $(P, \to^{\exists\exists})$ strongly preserves $\mathcal{L}$ as well, where $B_1 \to^{\exists\exists} B_2$ iff $\exists s_1 \in B_1.\exists s_2 \in B_2.s_1 \to s_2$.

In this case, while the concrete fixpoint is given by $\mathbf{EF}(X) = \mathrm{lfp}(\lambda Y.X \cup \mathrm{pre}_{\rightarrow}(Y))$, the abstract fixpoint is $\mathbf{EX}^{\sharp}(X^{\sharp}) = \mathrm{lfp}(\lambda Y^{\sharp}.X^{\sharp} \cup \mathrm{pre}_{\rightarrow^{\exists\exists}}(Y^{\sharp}))$. The key point here is that the best correct approximation of the concrete function $\lambda\langle X, Y\rangle.\ X \cup \mathrm{pre}_{\rightarrow}(Y)$ on the partition P viewed as an abstract domain is indeed $\lambda\langle X^{\sharp}, Y^{\sharp}\rangle.\ X^{\sharp} \cup \mathrm{pre}_{\rightarrow^{\exists\exists}}(Y^{\sharp})$. In other terms, the best correct approximation of $\lambda X.\,\mathrm{lfp}(\lambda Y.X \cup \mathrm{pre}_{\rightarrow}(Y))$ can be expressed as $\lambda X^{\sharp}.\,\mathrm{lfp}(\lambda Y^{\sharp}.X^{\sharp} \cup \mathrm{pre}_{\rightarrow^{\exists\exists}}(Y^{\sharp}))$ and thus preserves the same "template" of the concrete fixpoint function. We generalized this phenomenon to generic functions and abstract domains and then applied to standard temporal operators which can be expressed as fixpoints, that is, "Finally", "Globally", "Until" and "Release" modalities. We applied our results both to partitions, namely standard abstract models, and to disjunctive abstract domains, namely domains which are able to represent precisely logical disjunction. As far as partitions are concerned, we obtained new results of strong preservation on standard abstract Kripke structures. On the other hand, applications to disjunctive abstract domains provide a new procedure to perform a strongly preserving abstract model checking. This latter approach seems especially interesting because examples hint that efficient implementations are feasible.

2 Background

Notation. The standard pointwise ordering between functions will be denoted by $\sqsubseteq$. For a set $S \in \wp(\wp(X))$, we write the sets in S in a compact form like in $\{[1], [12], [123]\} \in \wp(\wp(\{1, 2, 3\}))$. We denote by $\complement$ the complement operator w.r.t. some universe set. $\mathrm{Part}(\Sigma)$ denotes the set of partitions of Σ. We consider transition systems (Σ, R) where the relation $R \subseteq \Sigma \times \Sigma$ (also denoted by $\xrightarrow{R}$) is total. A Kripke structure $\mathcal{K} = (\Sigma, R, AP, \ell)$ consists of a transition system (Σ, R) together with a set AP of atomic propositions and a labelling function $\ell : \Sigma \to \wp(AP)$. Paths in $\mathcal{K}$ are defined by $\mathrm{Path}(\mathcal{K}) \stackrel{\mathrm{def}}{=} \{\pi : \mathbb{N} \to \Sigma \mid \forall i \in \mathbb{N}.\ \pi_i \xrightarrow{R} \pi_{i+1}\}$. A transition relation $R \subseteq \Sigma \times \Sigma$ defines the usual pre/post transformers on $\wp(\Sigma)$: pre_R, post_R, $\widetilde{\mathrm{pre}}_R$, $\widetilde{\mathrm{post}}_R$. When clear from the context, subscripts R are sometimes omitted. The relations $R^{\exists\exists}, R^{\forall\exists} \subseteq \wp(\Sigma) \times \wp(\Sigma)$ are defined as follows: $(S_1, S_2) \in R^{\exists\exists}$ (respectively, $R^{\forall\exists}$) iff $\exists s_1 \in S_1.$ (respectively, $\forall s_1 \in S_1.$) $\exists s_2 \in S_2.\ (s_1, s_2) \in R$.

Abstract Interpretation and Completeness. As usual in standard abstract interpretation, abstract domains are specified by Galois connections/insertions (GCs/GIs) [4, 5]. A GC/GI of the abstract domain A into the concrete domain C through the abstraction and concretization maps $\alpha : C \to A$ and $\gamma : A \to C$ will be denoted by (C, α, γ, A). GIs of a common concrete domain C are pre-ordered w.r.t. precision as usual: $\mathcal{G}_1 = (C, \alpha_1, \gamma_1, A_1) \sqsubseteq \mathcal{G}_2 = (C, \alpha_2, \gamma_2, A_2)$ (i.e., A_1 is more precise than A_2) iff $\gamma_1 \circ \alpha_1 \sqsubseteq \gamma_2 \circ \alpha_2$. Moreover, $\mathcal{G}_1$ and $\mathcal{G}_2$ are equivalent when $\mathcal{G}_1 \sqsubseteq \mathcal{G}_2$ and $\mathcal{G}_2 \sqsubseteq \mathcal{G}_1$. Let $\mathcal{G} = (C, \alpha, \gamma, A)$ be a GI, $f : C \to C$ be some concrete semantic function — for simplicity, we consider here 1-ary functions — and $f^{\sharp} : A \to A$ be a corresponding abstract function. $\langle A, f^{\sharp}\rangle$ is a sound abstract interpretation 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 corresponds to require the following strengthening of soundness: $\alpha \circ f = f^{\sharp} \circ \alpha$. This is called *backward* completeness because an orthogonal notion of *forward* completeness may be considered: in fact, the

soundness condition $\alpha \circ f \sqsubseteq f^\sharp \circ \alpha$ is equivalent to $f \circ \gamma \sqsubseteq \gamma \circ f^\sharp$, so that forward completeness for $f^\sharp$ corresponds to strengthen soundness by requiring: $f \circ \gamma = \gamma \circ f^\sharp$. Giacobazzi et al. [12] observed that both backward and forward completeness uniquely depend upon the abstraction map, namely they are abstract domain properties. In fact, it turns out that there exists $f^\sharp : A \to A$ such that $\langle A, f^\sharp \rangle$ is backward (forward) complete iff $\gamma \circ \alpha \circ f \circ \gamma \circ \alpha = \gamma \circ \alpha \circ f$ ($\gamma \circ \alpha \circ f \circ \gamma \circ \alpha = f \circ \gamma \circ \alpha$). Thus, we say that a GI $\mathcal{G}$ is backward (forward) complete for f when $\gamma \circ \alpha \circ f \circ \gamma \circ \alpha = \gamma \circ \alpha \circ f$ ($\gamma \circ \alpha \circ f \circ \gamma \circ \alpha = f \circ \gamma \circ \alpha$). Note that $\mathcal{G}$ is forward complete for f iff f maps elements in $\mathrm{img}(\gamma)$ to elements in $\mathrm{img}(\gamma)$.

If $[\![\cdot]\!] : \mathcal{L} \to C$ and $[\![\cdot]\!]^\sharp : \mathcal{L} \to A$ are, respectively, a concrete and an abstract semantics of a generic language $\mathcal{L}$, then soundness and completeness for the abstract semantics $[\![\cdot]\!]^\sharp$ are defined as follows: $\langle A, [\![\cdot]\!]^\sharp \rangle$ is sound (respectively, backward complete, forward complete) if for any $\varphi \in \mathcal{L}$, $\alpha([\![\varphi]\!]) \leq_A [\![\varphi]\!]^\sharp$ (respectively, $\alpha([\![\varphi]\!]) = [\![\varphi]\!]^\sharp$, $[\![\varphi]\!] = \gamma([\![\varphi]\!]^\sharp)$).

Recall that a GI $\mathcal{G} = (C, \alpha, \gamma, A)$ is disjunctive (or additive) when γ is additive, i.e. when γ preserves arbitrary least upper bounds. It turns out that $\mathcal{G}$ is disjunctive iff $\mathrm{img}(\gamma) \subseteq C$ is join-closed, i.e. closed under arbitrary lub's. Disjunctive GIs can be "inverted" as follows and such inversion preserves forward completeness.

Proposition 2.1. *Let $\mathcal{G} = (C_\leq, \alpha, \gamma, A_\leq)$ be a disjunctive GI and $f : C \to C$.*
(i) *Let $\alpha^\triangledown(c) \stackrel{\text{def}}{=} \vee \{a \in A \mid \gamma(a) \leq c\}$. Then, $\mathcal{G}^\triangledown \stackrel{\text{def}}{=} (C_\geq, \alpha^\triangledown, \gamma, A_\geq)$ is a GI.*
(ii) *$\mathcal{G}^\triangledown$ is forward complete for f iff $\mathcal{G}$ is forward complete for f. In this case, the two best correct approximations of f w.r.t. $\mathcal{G}^\triangledown$ and $\mathcal{G}$ coincide.*

3 Abstract Models

3.1 Abstract Semantics

We consider (temporal) specification languages $\mathcal{L}$ whose state formulas φ are inductively defined by: $\mathcal{L} \ni \varphi ::= p \mid f(\varphi_1, ..., \varphi_n)$, where $p \in AP$ ranges over a set of atomic propositions while f ranges over a finite set Op of operators. AP and Op are also denoted, respectively, by $AP_\mathcal{L}$ and $Op_\mathcal{L}$. Each $f \in Op$ has an arity $\mathrm{ar}(f) > 0$. The interpretation of formulas in $\mathcal{L}$ is determined by a *semantic structure* $\mathcal{S} = (\Sigma, I)$ where Σ is a set of states and I is an interpretation function which maps $p \in AP$ to $I(p) \in \wp(\Sigma)$ and $f \in Op$ to $I(f) : \wp(\Sigma)^{\mathrm{ar}(f)} \to \wp(\Sigma)$. We also use $\boldsymbol{p}$ and $\boldsymbol{f}$ to denote, respectively, $I(p)$ and $I(f)$. Also, $\boldsymbol{AP} \stackrel{\text{def}}{=} \{\boldsymbol{p} \in \wp(\Sigma) \mid p \in AP\}$ and $\boldsymbol{Op} \stackrel{\text{def}}{=} \{\boldsymbol{f} : \wp(\Sigma)^{\mathrm{ar}(f)} \to \wp(\Sigma) \mid f \in Op\}$. The *concrete state semantic function* $[\![\cdot]\!]_\mathcal{S} : \mathcal{L} \to \wp(\Sigma)$ evaluates a formula $\varphi \in \mathcal{L}$ to the set of states making φ true w.r.t. the semantic structure $\mathcal{S}$:

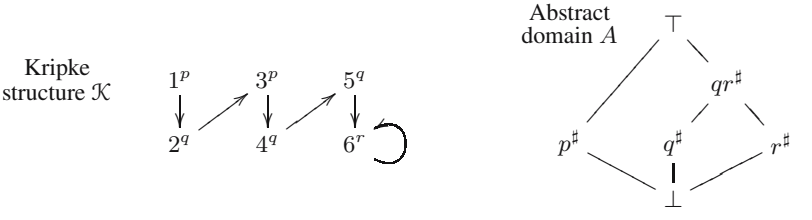
$$[\![p]\!]_\mathcal{S} = \boldsymbol{p} \quad \text{and} \quad [\![f(\varphi_1, ..., \varphi_n)]\!]_\mathcal{S} = \boldsymbol{f}([\![\varphi_1]\!]_\mathcal{S}, ..., [\![\varphi_n]\!]_\mathcal{S}).$$

Semantic structures generalize the role of Kripke structures. In fact, in standard model checking [3], a semantic structure is usually defined through a Kripke structure $\mathcal{K}$ so that the interpretation of operators in Op is defined in terms of paths in $\mathcal{K}$ and of standard logical operators. In the following, we will freely use standard logical and temporal operators together with their corresponding usual interpretations: for example, $I(\wedge) = \cap$, $I(\neg) = \complement$, $I(\mathrm{EX}) = \mathrm{pre}_R$, etc.

Following the abstract interpretation approach, an *abstract semantic structure* is given by $\mathcal{S}^\sharp = (A, I^\sharp)$ where (C, α, γ, A) is a GI and for any $p \in AP$ and $f \in Op$, $I(p) \in A$ and $I^\sharp(f) : A^{\mathrm{ar}(f)} \to A$. Thus, an abstract semantic structure $\mathcal{S}^\sharp$ defines an *abstract semantics* $[\![\cdot]\!]_{\mathcal{S}^\sharp} : \mathcal{L} \to A$ for the language $\mathcal{L}$.

Let $\mathcal{S}$ be a (concrete) semantic structure for $\mathcal{L}$. A GI (C, α, γ, A) always induces an abstract semantic structure $\mathcal{S}^A = (A, I^A)$ where I^A provides the best correct approximations on A of the concrete interpretation of constants/operators: $I^A(p) \stackrel{\mathrm{def}}{=} \alpha(I(p))$ for $p \in AP$ and $I^A(f) \stackrel{\mathrm{def}}{=} (I(f))^A$ for $f \in Op$. If the (concrete) interpretation $\boldsymbol{Op}_{\mathcal{L}}$ consists of monotone functions then the abstract semantics $[\![\cdot]\!]_{\mathcal{S}^A}$ induced by $\mathcal{S}^A$ is always automatically sound. This *induced abstract semantics* will be denoted by $[\![\cdot]\!]^A_{\mathcal{S}}$.

Example 3.1. Let us consider the following Kripke structure $\mathcal{K}$, where superscripts denote the labelling function.



Let $\mathcal{L} \ni \varphi ::= p \mid \varphi_1 \wedge \varphi_2 \mid \mathrm{EX}\varphi$. Let $\mathcal{S}$ be the semantic structure for $\mathcal{L}$ induced by the Kripke structure $\mathcal{K}$ so that $\mathbf{EX} = \mathrm{pre}_\rightarrow$. Let A be the lattice depicted above. We consider the abstraction map $\alpha : \wp(\Sigma)_\subseteq \to A$ where $\alpha(\{n\})$, i.e. on singletons, is defined by $\alpha(\{1\}) = \alpha(\{3\}) \stackrel{\mathrm{def}}{=} p^\sharp$, $\alpha(\{2\}) = \alpha(\{4\}) = \alpha(\{5\}) \stackrel{\mathrm{def}}{=} q^\sharp$ and $\alpha(\{6\}) \stackrel{\mathrm{def}}{=} r^\sharp$, while for any $S \in \wp(\Sigma)$, $\alpha(S) \stackrel{\mathrm{def}}{=} \vee_{s \in S}\, \alpha(\{s\})$. Hence, we have that:

$$[\![\mathrm{EX}r]\!]^A_{\mathcal{S}} = \mathbf{EX}^A([\![r]\!]^A_{\mathcal{S}}) = \mathbf{EX}^A(\alpha(\boldsymbol{r})) = \mathbf{EX}^A(\alpha(\{6\})) = \mathbf{EX}^A(r^\sharp) = \alpha(\mathbf{EX}(\gamma(r^\sharp))) = \alpha(\mathbf{EX}(\{6\})) = \alpha(\{5,6\}) = \alpha(\{5\}) \vee \alpha(\{6\}) = q^\sharp \vee r^\sharp = qr^\sharp.$$

Since $\gamma(qr^\sharp) = \{2,4,5,6\}$, as expected, observe that the abstract semantics $[\![\mathrm{EX}r]\!]^A_{\mathcal{S}}$ is a proper over-approximation in A of the concrete semantics $[\![\mathrm{EX}r]\!]_{\mathcal{S}} = \{5,6\}$. □

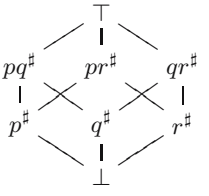
3.2 Partitioning Abstractions

As shown in [17], standard partition-based abstract model checking [2, 3] can be viewed as a particular instance of abstract semantics as defined in Section 3.1, where: (i) given some state partition $P \in \mathrm{Part}(\Sigma)$, the abstract domain is $\wp(P)_\subseteq$, where the abstraction map is the "covering" function $\alpha_P : \wp(\Sigma)_\subseteq \to \wp(P)_\subseteq$ such that $\alpha_P(S) \stackrel{\mathrm{def}}{=} \{B \in P \mid B \cap S \neq \varnothing\}$, while $\gamma_P : \wp(P)_\subseteq \to \wp(\Sigma)_\subseteq$ is given by $\gamma_P(X) = \cup_{B \in X} B$; (ii) if the concrete interpretation function I is based on a concrete Krike structure $\mathcal{K}$, then the abstract interpretation function $I^\sharp$ is simply given by the evaluation of I on an abstract Kripke structure $\mathcal{A} = (P, R^\sharp, AP, \ell^\sharp)$ which replaces $\mathcal{K}$, where $R^\sharp \subseteq P \times P$ is the abstract transition relation on the abstract state space P. Thus, in this sense, an abstract Kripke structure always induces an abstract semantics for a language.

Any GI $\mathcal{G} = (\wp(\Sigma)_\subseteq, \alpha, \gamma, A)$ which is equivalent to a GI $(\wp(\Sigma)_\subseteq, \alpha_P, \gamma_P, \wp(P)_\subseteq)$, for some partition $P \in \mathrm{Part}(\Sigma)$, is called *partitioning*. It turns out (see [17]) that $\mathcal{G}$

is partitioning iff $\gamma(A)$ is closed under complementation. Of course, not every abstraction of $\wp(\Sigma)_\subseteq$ is partitioning. For instance, if $\bar{s} \in \Sigma$, $A = \{\bot, \top\}$, $\gamma(\bot) = \{\bar{s}\}$ and $\gamma(\top) = \Sigma$ then $(\wp(\Sigma)_\subseteq, \alpha, \gamma, A)$ is a disjunctive GI, where α denotes the left adjoint to γ, which is not partitioning because $\gamma(A) = \{\{\bar{s}\}, \Sigma\}$ is not closed under complementation. This opens the question whether it is possible to minimally refine a given abstract domain in order to make it partitioning. Given a GI $\mathcal{G} = (\wp(\Sigma)_\subseteq, \alpha, \gamma, A)$, we define an equivalence relation $\sim_\mathcal{G}$ on Σ by identifying those states that are blurred by the abstraction α: $s \sim_\mathcal{G} t$ iff $\alpha(\{s\}) = \alpha(\{t\})$. This is an equivalence relation, namely a partition in $\mathrm{Part}(\Sigma)$, and therefore it induces a partitioning abstraction that we denote by $\mathbb{P}(\mathcal{G})$. As shown in [17], it turns out that $\mathbb{P}(\mathcal{G})$ is the least partitioning refinement of $\mathcal{G}$, that is: $\mathbb{P}(\mathcal{G}) \sqsubseteq \mathcal{G}$ and for any partitioning $\mathcal{G}' \sqsubseteq \mathcal{G}$, $\mathcal{G}' \sqsubseteq \mathbb{P}(\mathcal{G})$.

Example 3.2. Let us consider the abstraction $\mathcal{G}$ in Example 3.1. From the definition of α, we have that $\alpha(\{s\}) = \alpha(\{t\})$ iff s and t belong to the same block of the partition $P = \{[13], [245], [6]\}$, so that $\mathbb{P}(\mathcal{G})$ is given by the GI $(\wp(\Sigma), \alpha_P, \gamma_P, \wp(P))$. The abstract domain $\wp(P)_\subseteq$ can be therefore represented by the lattice depicted on the right. □



3.3 Strong Preservation

As recalled above, standard abstract model checking [2, 3] is based on state partitions and abstract Kripke structures. Strong preservation for some language $\mathcal{L}$ encodes the equivalence of abstract and concrete validity for formulas in $\mathcal{L}$. Given a partition $P \in \mathrm{Part}(\Sigma)$, let $[\![\cdot]\!]^P : \mathcal{L} \to \wp(P)$ denote an abstract semantics defined on $\wp(P)$. For example, but not necessarily, this can be the abstract semantics induced by an abstract Kripke structure $(P, R^\sharp, AP, \ell^\sharp)$. A partition $P \in \mathrm{Part}(\Sigma)$ is *strongly preserving* (s.p. for short) for $\mathcal{L}$ when for any $s \in \Sigma$ and $\varphi \in \mathcal{L}$, $s \in [\![\varphi]\!]$ iff $\alpha_P(\{s\}) \in [\![\varphi]\!]^P$. It is known [8, 9, 17] that the coarsest s.p. partition $P_\mathcal{L}$ for $\mathcal{L}$ is given by the following state equivalence $\sim_\mathcal{L}$ induced by $\mathcal{L}$: $s_1 \sim_\mathcal{L} s_2$ iff $\forall \varphi \in \mathcal{L}.\ s_1 \in [\![\varphi]\!] \Leftrightarrow s_2 \in [\![\varphi]\!]$. Obviously, the definition of an abstract Kripke structure which induces a s.p. abstract semantics depends on the language $\mathcal{L}$. Let us recall some well-known examples [2, 3, 13]. Let $\mathcal{K} = (\Sigma, R, AP, \ell)$ be a concrete Kripke structure and let $P_{\mathrm{sim}}, P_{\mathrm{bis}} \in \mathrm{Part}(\Sigma)$ denote, respectively, simulation and bisimulation equivalence on $\mathcal{K}$. Then, the abstract semantics induced by the abstract Kripke structure $(P_{\mathrm{sim}}, R^{\forall\exists}, AP, \ell^\sharp)$ (where $\ell^\sharp(B) = \cup_{s \in B} \ell(s)$) is s.p. for ACTL^*, while that induced by $(P_{\mathrm{bis}}, R^{\exists\exists}, AP, \ell^\sharp)$ is s.p. for CTL^*.

Strong preservation was generalized in [17] to abstract domains as follows.

Definition 3.3. Let $\mathcal{S} = (\Sigma, I)$ and $\mathcal{S}^\sharp = (A, I^\sharp)$ be, respectively, concrete and abstract semantic structures for $\mathcal{L}$. Let $[\![\cdot]\!]_{\mathcal{S}^\sharp} : \mathcal{L} \to A$ be the corresponding abstract semantics. $\mathcal{S}^\sharp$ (or $[\![\cdot]\!]_{\mathcal{S}^\sharp}$) is *strongly preserving* for $\mathcal{L}$ (w.r.t. $\mathcal{S}$) when for any $S \in \wp(\Sigma)$ and $\varphi \in \mathcal{L}$, $S \subseteq [\![\varphi]\!]_\mathcal{S} \Leftrightarrow \alpha(S) \leq_A [\![\varphi]\!]_{\mathcal{S}^\sharp}$. □

The following simple but key result shows that strong preservation amounts to forward completeness.

Theorem 3.4. *$\mathcal{S}^\sharp$ is s.p. for $\mathcal{L}$ iff the abstract semantics $\langle A, [\![\cdot]\!]_{\mathcal{S}^\sharp} \rangle$ is forward complete.*

It turns out (cf. [17]) that if a s.p. abstract semantics on the abstract domain A exists then the abstract semantics $[\![\cdot]\!]^A_{\mathcal{S}}$ induced by A is s.p. as well, so that strong preservation is an *abstract domain property*. Hence, we say that the GI $\mathcal{G} = (\wp(\Sigma)_{\subseteq}, \alpha, \gamma, A)$ (or simply A when the GI is clear from the context) is s.p. for $\mathcal{L}$ if $\mathcal{S}^A$ is s.p. for $\mathcal{L}$ (or, equivalently, if a s.p. abstract semantics on A exists). In this case, by Theorem 3.4, we also say that the abstract domain A is *language forward complete* for $\mathcal{L}$.

Example 3.5. Let us consider again Example 3.1. It turns out that A is not s.p. preserving for $\mathcal{L}$ because $\gamma([\![\mathrm{EX}r]\!]^A_{\mathcal{S}}) = \gamma(qr^\sharp) = \{2,4,5,6\}$, while $[\![\mathrm{EX}r]\!]_{\mathcal{S}} = \{5,6\}$. Therefore, for instance, $2 \in \gamma([\![\mathrm{EX}p]\!]^A_{\mathcal{S}}) \smallsetminus [\![\mathrm{EX}r]\!]_{\mathcal{S}}$, or, equivalently, $\alpha(\{2\}) \leq [\![\mathrm{EX}r]\!]^A_{\mathcal{S}}$ whilst $2 \notin [\![\mathrm{EX}r]\!]_{\mathcal{S}}$. □

4 Abstract Semantics

It is known (see e.g. [7]) that if an abstract domain A is forward complete for all the constants/operators of $\boldsymbol{AP} \cup \boldsymbol{Op}$ (where atomic propositions are viewed as 0-ary operators) — here also called *operator-wise forward completeness* — of some concrete interpretation of some language $\mathcal{L}$ then A is language forward complete for $\mathcal{L}$ (i.e., for all $\varphi \in \mathcal{L}$, $[\![\varphi]\!]_{\mathcal{S}} = \gamma([\![\varphi]\!]^A_{\mathcal{S}})$). The converse in general is not true, as shown by the following example.

Example 4.1. Let us consider the following Kripke structure $\mathcal{K}$ and the partitioning abstract domain A induced by the partition $P = \{[12],[3]\}$, i.e. $A = \wp(P)_{\subseteq}$.

Let us consider the language $\mathcal{L} \ni \varphi ::= p \mid \mathrm{EX}\varphi$. The Kripke structure $\mathcal{K}$ induces the semantic structure $\mathcal{S} = (\{1,2,3\}, I)$ such that $I(p) = \{1,2,3\}$ and $I(\mathrm{EX}) = \mathrm{pre}_{\rightarrow}$. Hence, we have that $[\![p]\!]_{\mathcal{S}} = \{1,2,3\}$, $[\![\mathrm{EX}p]\!]_{\mathcal{S}} = \{1,2,3\}$ and, for $k > 1$, $[\![\mathrm{EX}^k p]\!]_{\mathcal{S}} = \{1,2,3\}$. On the abstract side we have that $[\![p]\!]^A_{\mathcal{S}} = \{[12],[3]\}$, $[\![\mathrm{EX}p]\!]^A_{\mathcal{S}} = \{[12],[3]\}$ and, for $k > 1$, $[\![\mathrm{EX}^k p]\!]^A_{\mathcal{S}} = \{[12],[3]\}$. Thus, for any $\varphi \in \mathcal{L}$, $[\![\varphi]\!]_{\mathcal{S}} = \gamma_P([\![\varphi]\!]^A_{\mathcal{S}})$, i.e. the abstract domain A is language forward complete for $\mathcal{L}$. On the other hand, $\mathrm{pre}_{\rightarrow}(\gamma_P(\alpha_P(\{3\}))) = \mathrm{pre}_{\rightarrow}(\{3\}) = \{2,3\}$ while $\gamma_P(\alpha_P(\mathrm{pre}_{\rightarrow}(\gamma_P(\alpha_P(\{3\}))))) = \gamma_P(\alpha_P(\{2,3\})) = \{1,2,3\}$, so that A is not forward complete for $\mathrm{pre}_{\rightarrow}$. □

Operator-wise forward completeness is easier to check than language forward completeness. Moreover, the problem of refining an abstract domain in order to make it forward (or backward) complete for a given set of operators admits constructive fixpoint solutions [12, 18]. It is thus interesting to determine conditions on abstract domains which guarantee the equivalence of operator-wise and language forward completeness.

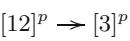
Definition 4.2. Let $\mathcal{S} = (\Sigma, I)$ be a semantic structure for $\mathcal{L}$ and $(\wp(\Sigma)_{\subseteq}, \alpha, \gamma, A)$ be a GI. The abstract domain A is $\mathcal{L}$*-covered* by the concrete semantics $[\![\cdot]\!]_{\mathcal{S}}$ (or simply by $\mathcal{S}$) when for any $a \in A$ there exists $\varphi \in \mathcal{L}$ such that $\gamma(a) = [\![\varphi]\!]_{\mathcal{S}}$. □

It turns out that this notion of covering ensures the equivalence of operator-wise and language forward completeness.

Theorem 4.3. *Let A be $\mathcal{L}$-covered by $\mathcal{S}$. Then, A is language forward complete for $\mathcal{L}$ iff A is forward complete for all the constants/operators in $\boldsymbol{AP}_{\mathcal{L}} \cup \boldsymbol{Op}_{\mathcal{L}}$.*

As recalled above, given an abstract domain A, if an abstract semantic structure $\mathcal{S}^\sharp = (A, I^\sharp)$ is s.p. for $\mathcal{L}$ then the abstract structure $\mathcal{S}^A = (A, I^A)$ induced by A is s.p. for $\mathcal{L}$ as well. However, the interpretation functions $I^\sharp$ and I^A may differ.

Example 4.4. Let us consider again Example 4.1. Let us first note that A is not $\mathcal{L}$-covered by $\mathcal{S}$ because $\{[\![\varphi]\!]_{\mathcal{S}} \mid \varphi \in \mathcal{L}\} = \{\{1,2,3\}\}$. Let us consider the abstract semantic structure $\mathcal{S}^\sharp = (A, I^\sharp)$ induced by the following abstract Kripke structure:



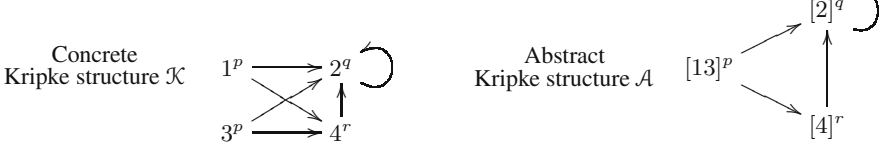
Hence, $I^\sharp(\mathrm{EX}) = \mathrm{pre}_{R^\sharp}$ where $\mathrm{pre}_{R^\sharp}(\varnothing) = \varnothing$, $\mathrm{pre}_{R^\sharp}(\{[12]\}) = \varnothing$, $\mathrm{pre}_{R^\sharp}(\{[3]\}) = \{[12],[3]\}$, $\mathrm{pre}_{R^\sharp}(\{[12],[3]\}) = \{[12],[3]\}$. It is easy to see that $\mathcal{S}^\sharp$ is s.p. for $\mathcal{L}$. In fact, we have that $\gamma_P([\![p]\!]_{\mathcal{S}^\sharp}) = \gamma_P(\{[12],[3]\}) = \{1,2,3\} = [\![p]\!]_{\mathcal{S}}$ and $\gamma_P([\![\mathrm{EX}p]\!]_{\mathcal{S}^\sharp}) = \gamma_P(\mathrm{pre}_{R^\sharp}(\{[12],[3]\})) = \gamma_P(\{[12],[3]\}) = \{1,2,3\} = [\![\mathrm{EX}p]\!]_{\mathcal{S}}$, so that by Theorem 3.4, $\mathcal{S}^\sharp$ is s.p. for $\mathcal{L}$. However, it turns out that $I^\sharp(\mathrm{EX}) \neq I^A(\mathrm{EX}) = \alpha_P \circ \mathrm{pre}_\to \circ \gamma_P$. In fact, $\mathrm{pre}_{R^\sharp}(\{[12]\}) = \varnothing$ while $\alpha_P(\mathrm{pre}_\to(\gamma_P(\{[12]\}))) = \alpha_P(\mathrm{pre}_\to(\{1,2\})) = \alpha_P(\{1\}) = \{[12]\}$. Thus, $\mathcal{S}^\sharp$ and $\mathcal{S}^A$ are two different abstract semantic structures which are both s.p. for $\mathcal{L}$. □

Thus, in general, for a given abstract domain A, there may be different s.p. abstract semantic structures defined over A. However, if A is $\mathcal{L}$-covered by the concrete semantic structure then a unique s.p. abstract semantic structure may exist.

Corollary 4.5. *If A is $\mathcal{L}$-covered by $\mathcal{S}$ and $\mathcal{S}^\sharp = (A, I^\sharp)$ is s.p. for $\mathcal{L}$ then $I^\sharp = I^A$.*

Thus, when A is $\mathcal{L}$-covered by $\mathcal{S}$, we have that a *unique interpretation* of constants/functions on A which is s.p. for $\mathcal{L}$ may exist, namely their best correct approximations on A.

Example 4.6. Let us consider the language $\mathcal{L} \ni \varphi ::= p \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi \mid \mathrm{EX}\varphi$ and the following Kripke structure $\mathcal{K}$ with transition relation R.



This induces a concrete semantic structure $\mathcal{S} = (\{1,2,3,4\}, I)$ where $I(p) = \{1,3\}$, $I(q) = \{2\}$, $I(r) = \{4\}$, $I(\neg) = \complement$, $I(\wedge) = \cap$ and $I(\mathrm{EX}) = \mathrm{pre}_R$. Let us consider the state partition $P = \{13, 2, 4\}$ and the corresponding abstract Kripke structure $\mathcal{A}$ depicted above where the transition relation is given by $R^{\exists\exists}$. Let us consider the abstract semantic structure $\mathcal{S}^\sharp = (A, I^\sharp)$ induced by $\mathcal{A}$, i.e. $A = \wp(P)_\subseteq$ and $I^\sharp(p) = \{13\}$, $I^\sharp(q) = \{2\}$, $I^\sharp(r) = \{4\}$, $I^\sharp(\neg) = \complement$, $I^\sharp(\wedge) = \cap$ and $I^\sharp(\mathrm{EX}) = \mathrm{pre}_{R^{\exists\exists}}$.

It is easy to check that $I^\sharp(\neg)$, $I^\sharp(\wedge)$ and $I^\sharp(\mathrm{EX})$ are indeed the best correct approximations on A of, respectively, the concrete operations of set complementation $\complement = I(\neg)$, set interesection $\cap = I(\wedge)$ and $\mathrm{pre}_R = I(\mathrm{EX})$. Hence, $I^\sharp = I^A$, namely $\mathcal{S}^\sharp = \mathcal{S}^A$.

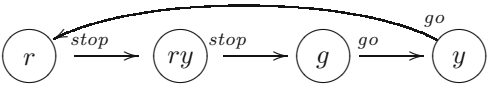
It turns out that A is $\mathcal{L}$-covered by $\mathbb{S}$. In fact, since the set of concrete semantics of formulas in $\mathcal{L}$ is closed under set complementation we have that any union of blocks of P belongs to $\{[\![\varphi]\!]_{\mathbb{S}} \mid \varphi \in \mathcal{L}\}$, so that $\mathrm{img}(\gamma_P) \subseteq \{[\![\varphi]\!]_{\mathbb{S}} \mid \varphi \in \mathcal{L}\}$.

We also have that $\mathbb{S}^A$ is s.p. for $\mathcal{L}$. This happens because A is forward complete for the constants/operations of $\mathcal{L}$. In fact, all the concrete operations $\complement$, $\cap$ and pre_R map unions of blocks in $\wp(P)$ into unions of blocks in $\wp(P)$ and therefore the abstract domain $A = \wp(P)$ is forward complete for them. For example, let us observe that this holds for pre_R because $\mathrm{pre}_R(\{1,3\}) = \varnothing$, $\mathrm{pre}_R(\{2\}) = \{1,3,4\}$ and $\mathrm{pre}_R(\{4\}) = \{1,3\}$. Hence, since A is operator-wise forward complete we have that A is language forward complete for $\mathcal{L}$ as well and therefore, by Theorem 3.4, $\mathbb{S}^A$ is s.p. for $\mathcal{L}$.

Consequently, by Corollary 4.5, $\mathbb{S}^A$ is the unique abstract semantic structure on the abstract domain A which is s.p. for $\mathcal{L}$. □

It may also happen that one can define a s.p. abstract semantics on some partition P although this abstract semantics cannot be derived from an abstract Kripke structure on P, as shown by the following example.

Example 4.7. Consider the following simple language $\mathcal{L} \ni \varphi ::= p \mid \mathrm{AXX}\varphi$ and the following Kripke structure $\mathcal{K}$ where R is the transition relation.



This models a four-state traffic light controller (like in the U.K. and in Germany). This gives rise to a concrete semantic structure $\mathbb{S} = (\{r, ry, g, y\}, I)$ where $I(stop) = \{r, ry\}$, $I(go) = \{g, y\}$ and $I(\mathrm{AXX}) = \widetilde{\mathrm{pre}}_{R^2}$. Hence, according to the standard interpretation $I(\mathrm{AXX}) = \widetilde{\mathrm{pre}}_{R^2}$, we have that $s \in [\![\mathrm{AXX}\varphi]\!]_{\mathbb{S}}$ iff for any path $\pi_0\pi_1\pi_2\ldots$ in $\mathcal{K}$ starting from $s = \pi_0$, we have that $\pi_2 \in [\![\varphi]\!]_{\mathbb{S}}$. Observe that $[\![\mathrm{AXX}stop]\!]_{\mathbb{S}} = \{g, y\}$ and $[\![\mathrm{AXX}go]\!]_{\mathbb{S}} = \{r, ry\}$. Consider the partition $P = \{[r, ry], [g, y]\}$ and the corresponding partitioning abstract domain $A = \wp(P)_{\subseteq}$. Hence, for the corresponding abstract semantic structure $\mathbb{S}^A = (A, I^A)$ we have that $I^A(stop) = \{[r, ry]\}$, $I^A(go) = \{[g, y]\}$ and $I^A(\mathrm{AXX}) = \alpha_P \circ \widetilde{\mathrm{pre}}_{R^2} \circ \gamma_P$, so that

$$
\begin{array}{l}
I^A(\mathrm{AXX})(\varnothing) = \varnothing; \\
I^A(\mathrm{AXX})(\{[r, ry]\}) = \{[g, y]\}; \quad I^A(\mathrm{AXX})(\{[g, y]\}) = \{[r, ry]\}; \\
I^A(\mathrm{AXX})(\{[r, ry], [g, y]\}) = \{[r, ry], [g, y]\}.
\end{array}
$$

By Theorem 3.4, it turns out that $\mathbb{S}^A$ is s.p. for $\mathcal{L}$ because A is forward complete for $\widetilde{\mathrm{pre}}_{R^2}$. In fact, it turns out that $\widetilde{\mathrm{pre}}_{R^2}$ maps unions of blocks in P to unions of blocks in P because: $\widetilde{\mathrm{pre}}_{R^2}(\varnothing) = \varnothing$, $\widetilde{\mathrm{pre}}_{R^2}(\{r, ry\}) = \{g, y\}$, $\widetilde{\mathrm{pre}}_{R^2}(\{g, y\}) = \{r, ry\}$ and $\widetilde{\mathrm{pre}}_{R^2}(\{r, ry, g, y\}) = \{r, ry, g, y\}$.

However, let us show that there exists no abstract transition relation $R^\sharp \subseteq P \times P$ on the partition P such that the abstract Kripke structure $\mathcal{A} = (P, R^\sharp, AP, \ell^\sharp)$ induces an abstract semantic structure which is s.p. for $\mathcal{L}$. Assume by contradiction that such an abstract Kripke structure $\mathcal{A}$ exists and let $\mathbb{S}^\sharp$ be the corresponding induced abstract semantic structure. Let $B_1 = [r, ry] \in P$ and $B_2 = [g, y] \in P$. Since $r \in [\![\mathrm{AXX}go]\!]_{\mathbb{S}}$ and $g \in [\![\mathrm{AXX}stop]\!]_{\mathbb{S}}$, by strong preservation, it must be that $B_1 \in [\![\mathrm{AXX}go]\!]_{\mathbb{S}^\sharp}$ and $B_2 \in [\![\mathrm{AXX}stop]\!]_{\mathbb{S}^\sharp}$. Thus, necessarily, $(B_1, B_2), (B_2, B_1) \in R^\sharp$. This leads to the

contradiction $B_1 \notin [\![\mathrm{AXX}go]\!]_{\mathbb{S}^\sharp}$. In fact, if $R^\sharp = \{(B_1, B_2), (B_2, B_1)\}$ then we would have that $B_1 \notin [\![\mathrm{AXX}go]\!]_{\mathbb{S}^\sharp}$. Moreover, if, instead, $(B_1, B_1) \in R^\sharp$ (the case (B_2, B_2) is analogous), then we would still have that $B_1 \notin [\![\mathrm{AXX}go]\!]_{\mathbb{S}^\sharp}$. Even more, along the same lines it is not difficult to show that no proper abstract Kripke structure induces an abstract semantic structure which strongly preserves $\mathcal{L}$, because even if we split one of the two blocks B_1 or B_2 we still cannot define an abstract transition relation ensuring strong preservation for $\mathcal{L}$. □

5 Fixpoints in Abstract Semantics

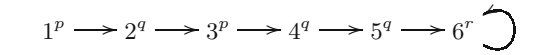
The above abstract interpretation-based approach to abstract model checking systematically defines the abstract semantics by approximating the interpretation of logical/temporal operators through their best correct approximations on the abstract domain. In principle, this can be done for any logical/temporal operator. However, when a temporal operator $\boldsymbol{f}$ can be expressed as a least/greatest fixpoint of another temporal operator $\boldsymbol{g}$, e.g. $\boldsymbol{f}(S) = \mathrm{lfp}(\lambda X.\boldsymbol{g}(X, S))$, the best correct approximation $\alpha \circ \boldsymbol{f} \circ \gamma$ might not be characterizable as a least/greatest fixpoint. Ideally, we would aim at approximating $\boldsymbol{g}$ through some abstract operator $\boldsymbol{g}^\sharp$ in order to be able to characterize $\alpha \circ \boldsymbol{f} \circ \gamma$ as the abstract least fixpoint of $\boldsymbol{g}^\sharp$. Let us illustrate this through the case of the "Finally" operator EF, whose standard interpretation can be characterized as a fixpoint: $\mathbf{EF}(S) = \mathrm{lfp}(\lambda X.S \cup \mathbf{EX}(X))$. The best correct approximation of $\mathbf{EF}$ w.r.t. a Galois insertion $(\wp(\Sigma)_\subseteq, \alpha, \gamma, A)$ is the abstract function $\alpha \circ \mathbf{EF} \circ \gamma : A \to A$. However, this definition gives us no clue for computing $\alpha \circ \mathbf{EF} \circ \gamma$ as a least fixpoint. By contrast, in standard abstract model checking the abstract interpretation of the language operators is based on an abstract transition relation defined on the abstract state space, i.e. an abstract Kripke structure, so that it is enough to compute the least fixpoint $\mathrm{lfp}(\lambda X.S \cup \mathbf{EX}(X))$ on the abstract Kripke structure. For example, consider the language $\mathcal{L} \ni \varphi ::= p \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi \mid \mathrm{EF}\varphi$. Let $\mathcal{K} = (\Sigma, R, AP, \ell)$ be a concrete Kripke structure. One can easily see that if $P \in \mathrm{Part}(\Sigma)$ is s.p. for $\mathcal{L}$ then the abstract Kripke structure on P with abstract transition relation $R^{\exists\exists} \subseteq P \times P$ is s.p. for $\mathcal{L}$. In this case, while the concrete fixpoint is given by $\mathbf{EF}(S) = \mathrm{lfp}(\lambda X.S \cup \mathrm{pre}_R(X))$, for any $S \subseteq \Sigma$, the abstract fixpoint is $\mathrm{lfp}(\lambda X^\sharp.S^\sharp \cup_P \mathrm{pre}_{R^{\exists\exists}}(X^\sharp))$, for any $S^\sharp \subseteq P$, where $\cup_P$ is union of blocks in P, namely the least upper bound of the abstract domain $\wp(P)_\subseteq$. Recall that the abstract domain $\wp(P)_\subseteq$ is related to the concrete domain $\wp(\Sigma)_\subseteq$ by the GI $\mathcal{G}_P = (\wp(\Sigma)_\subseteq, \alpha_P, \gamma_P, \wp(P)_\subseteq)$. The key point to note here is that $\lambda\langle X^\sharp, Y^\sharp\rangle.\ X^\sharp \cup^A \mathrm{pre}^A_R(Y^\sharp)$ is indeed the best correct approximation of the concrete operation $\lambda\langle X, Y\rangle.\ X \cup \mathrm{pre}_R(Y)$ through the GI $\mathcal{G}_P$. These observations lead us to the following generalization.

Theorem 5.1. *Let C be a complete lattice, (C, α, γ, A) be a GI and $f : C^{n+1} \to C$ be monotone. Let $F \stackrel{\mathrm{def}}{=} \lambda\vec{c} \in C^n.\, \mathrm{lfp}(\lambda x.f(c_1, ..., x, ..., c_n))$. If A is forward complete for F then $F^A = \lambda\vec{a} \in A^n.\mathrm{lfp}(\lambda x.f^A(a_1, ..., x, ..., a_n))$.*

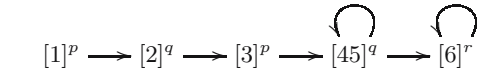
Let us remark that the above result can be also stated by duality for greatest fixpoints as follows: if $(C_\geq, \alpha, \gamma, A_\geq)$ is a GI, $F \stackrel{\mathrm{def}}{=} \lambda\vec{c} \in C^n.\, \mathrm{gfp}(\lambda x.f(c_1, ..., x, ..., c_n))$ and A is forward complete for F then $F^A = \lambda\vec{a} \in A^n.\mathrm{gfp}(\lambda x.f^A(a_1, ..., x, ..., a_n))$.

By Theorems 3.4 and 4.3, given a language $\mathcal{L}$ and a semantic structure $\mathcal{S}$ for $\mathcal{L}$, if A is $\mathcal{L}$-covered by $\mathcal{S}$ then A is forward complete for the constants/operators in $\boldsymbol{AP}_{\mathcal{L}} \cup \boldsymbol{Op}_{\mathcal{L}}$ iff $\mathcal{S}^A$ is s.p. for $\mathcal{L}$. Thus, in this case, by Theorem 5.1, if $\mathcal{S}^A$ is s.p. for $\mathcal{L}$ and $\boldsymbol{Op}_{\mathcal{L}}$ includes an operator $\boldsymbol{f}$ which can be expressed as a least/greatest fixpoint of some operation $\boldsymbol{g}$ then the best correct approximation of $\boldsymbol{f}$ on A can be obtained as the abstract least/greatest fixpoint of the best correct approximation of $\boldsymbol{g}$ on A.

Example 5.2. Let us consider $\mathcal{L} \ni \varphi ::= p \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi \mid \mathrm{EF}\varphi$ and the following Kripke structure $\mathcal{K}$ with transition relation R which induces a concrete semantic structure $\mathcal{S}$.



Let us consider the partition $P = \{[1], [2], [3], [45], [6]\}$ and the corresponding abstract Kripke structure $\mathcal{A}$ depicted below where the transition relation is given by $R^{\exists\exists}$.



Let $\mathcal{S}^A$ be the abstract semantic structure induced by the abstract domain $A = \wp(P)_{\subseteq}$. It turns out that $\mathcal{S}^A$ is s.p. for $\mathcal{L}$ because A is forward complete for ($\boldsymbol{AP}_{\mathcal{L}}$ and) $\boldsymbol{Op}_{\mathcal{L}} = \{\cap, \complement, \mathbf{EF}\}$: in fact, it is easy to check that A is forward complete for $\mathbf{EF}$ because $\mathbf{EF}$ maps unions of blocks in P to unions of blocks in P. Since A is forward complete for $\mathbf{EF}$ and $\mathbf{EF}(S) = \mathrm{lfp}(\lambda X.f(S, X))$, where $f(S, X) \stackrel{\mathrm{def}}{=} S \cup \mathrm{pre}_R(X)$, by Theorem 5.1 we have that $\mathbf{EF}^A = \lambda S^\sharp.\mathrm{lfp}(\lambda X^\sharp.f^A(S^\sharp, X^\sharp)) : \wp(P) \to \wp(P)$. Moreover, as discussed above, $f^A(S^\sharp, X^\sharp) = \alpha_P(f(\gamma_P(S^\sharp), \gamma_P(X^\sharp))) = S^\sharp \cup_P \mathrm{pre}_{R^{\exists\exists}}(X^\sharp)$ so that $\mathbf{EF}^A = \lambda S^\sharp.\,\mathrm{lfp}(\lambda X^\sharp.S^\sharp \cup \mathrm{pre}_{R^{\exists\exists}}(X^\sharp))$, namely the best correct approximation $\mathbf{EF}^A$ can be computed as the least fixpoint characterization of the "finally" operator on the above abstract Kripke structure $\mathcal{A}$. □

6 Applications

We are mainly interested in applying Theorem 5.1 to standard fixpoint-based operators of well known temporal languages (cf. [3]), as recalled in Table 1.

Table 1. Temporal operators in fixpoint form

"Finally"	$\mathbf{AF}(S) = \mathrm{lfp}(\lambda X.S \cup \mathbf{AX}(X))$
	$\mathbf{EF}(S) = \mathrm{lfp}(\lambda X.S \cup \mathbf{EX}(X))$
"Globally"	$\mathbf{AG}(S) = \mathrm{gfp}(\lambda X.S \cap \mathbf{AX}(X))$
	$\mathbf{EG}(S) = \mathrm{gfp}(\lambda X.S \cap \mathbf{EX}(X))$
"(Strong) Until"	$\mathbf{AU}(S, T) = \mathrm{lfp}(\lambda X.T \cup (S \cap \mathbf{AX}(X)))$
	$\mathbf{EU}(S, T) = \mathrm{lfp}(\lambda X.T \cup (S \cap \mathbf{EX}(X)))$
"Weak Until"	$\mathbf{AU}_{\boldsymbol{w}}(S, T) = \mathrm{gfp}(\lambda X.T \cup (S \cap \mathbf{AX}(X)))$
	$\mathbf{EU}_{\boldsymbol{w}}(S, T) = \mathrm{gfp}(\lambda X.T \cup (S \cap \mathbf{EX}(X)))$
"(Weak) Release"	$\mathbf{AR}(S, T) = \mathrm{gfp}(\lambda X.T \cap (S \cup \mathbf{AX}(X)))$
	$\mathbf{ER}(S, T) = \mathrm{gfp}(\lambda X.T \cap (S \cup \mathbf{EX}(X)))$
"Strong Release"	$\mathbf{AR}_{\boldsymbol{s}}(S, T) = \mathrm{lfp}(\lambda X.T \cap (S \cup \mathbf{AX}(X)))$
	$\mathbf{ER}_{\boldsymbol{s}}(S, T) = \mathrm{lfp}(\lambda X.T \cap (S \cup \mathbf{EX}(X)))$

6.1 Partitioning Abstractions

Let $P \in \mathrm{Part}(\Sigma)$ be any partition and let $\mathcal{G} = (\wp(\Sigma)_{\subseteq}, \alpha_P, \gamma_P, \wp(P)_{\subseteq})$ be the corresponding partitioning GI. By Proposition 2.1 (i), $\mathcal{G}^{\triangledown} = (\wp(\Sigma)_{\supseteq}, \alpha_P^{\triangledown}, \gamma_P, \wp(P)_{\supseteq})$ is a GI where $\alpha_P^{\triangledown}(S) = \{B \in P \mid B \subseteq S\}$. Hence, while $\mathcal{G}$ over-approximates a set S by the set of blocks in P which have a nonempty intersection with S, $\mathcal{G}^{\triangledown}$ under-approximates S by the set of blocks in P which are contained in S. Thus, we can apply Theorem 5.1 to $\mathcal{G}$ for least fixpoints and to $\mathcal{G}^{\triangledown}$ for greatest fixpoints. Since $\mathcal{G}$ is disjunctive, Let us note that by Proposition 2.1 (ii), $\mathcal{G}$ is forward complete for some function F iff $\mathcal{G}^{\triangledown}$ is forward complete for F. Hence, the hypotheses of Theorem 5.1 for least and greatest fixpoints actually coincide. Furthermore, in this case, the best correct approximations of F w.r.t. $\mathcal{G}$ and $\mathcal{G}^{\triangledown}$ coincide. In order to distinguish which GI has been applied, we use f^A to denote the best correct approximation of some concrete function f w.r.t. $\mathcal{G}$ while $f^{\triangledown A}$ denotes the best correct approximation of f w.r.t. $\mathcal{G}^{\triangledown}$.

For the standard temporal fixpoint-based operators in Table 1, the following result shows that their best correct approximations on a s.p. partitioning abstract domain preserve their characterizations as least/greatest fixpoints.

Corollary 6.1. *Let $P \in \mathrm{Part}(\Sigma)$ and $\mathcal{G} = (\wp(\Sigma)_{\subseteq}, \alpha_P, \gamma_P, A = \wp(P)_{\subseteq})$ be the corresponding partitioning GI. Assume that $\mathcal{G}$ is forward complete for some fixpoint-based operator F in Table 1. Then, the corresponding best correct approximations of F w.r.t. $\mathcal{G}$ are as follows:*

$$
\begin{array}{l}
\mathbf{AF}^A(S^\sharp) = \mathrm{lfp}(\lambda X^\sharp.S^\sharp \cup_P \widetilde{\mathrm{pre}}_R^A(X^\sharp)) \\
\mathbf{EF}^A(S^\sharp) = \mathrm{lfp}(\lambda X^\sharp.S^\sharp \cup_P \mathrm{pre}_R^A(X^\sharp)) \\
\mathbf{AG}^A(S^\sharp) = \mathrm{gfp}(\lambda X^\sharp.S^\sharp \cap_P \widetilde{\mathrm{pre}}_R^{\triangledown A}(X^\sharp)) \\
\mathbf{EG}^A(S^\sharp) = \mathrm{gfp}(\lambda X^\sharp.S^\sharp \cap_P \mathrm{pre}_R^{\triangledown A}(X^\sharp)) \\
\mathbf{AU}^A(S^\sharp, T^\sharp) = \mathrm{lfp}(\lambda X^\sharp.T^\sharp \cup_P (S^\sharp \cap_P \widetilde{\mathrm{pre}}_R^A(X^\sharp))) \\
\mathbf{EU}^A(S^\sharp, T^\sharp) = \mathrm{lfp}(\lambda X^\sharp.T^\sharp \cup_P (S^\sharp \cap_P \mathrm{pre}_R^A(X^\sharp))) \\
\mathbf{AU}_{\boldsymbol{w}}^A(S^\sharp, T^\sharp) = \mathrm{gfp}(\lambda X^\sharp.T^\sharp \cup_P (S^\sharp \cap_P \widetilde{\mathrm{pre}}_R^{\triangledown A}(X^\sharp))) \\
\mathbf{EU}_{\boldsymbol{w}}^A(S^\sharp, T^\sharp) = \mathrm{gfp}(\lambda X^\sharp.T^\sharp \cup_P (S^\sharp \cap_P \mathrm{pre}_R^{\triangledown A}(X^\sharp))) \\
\mathbf{AR}^A(S^\sharp, T^\sharp) = \mathrm{gfp}(\lambda X^\sharp.T^\sharp \cap_P (S^\sharp \cup_P \widetilde{\mathrm{pre}}_R^{\triangledown A}(X^\sharp))) \\
\mathbf{ER}^A(S^\sharp, T^\sharp) = \mathrm{gfp}(\lambda X^\sharp.T^\sharp \cap_P (S^\sharp \cup_P \mathrm{pre}_R^{\triangledown A}(X^\sharp))) \\
\mathbf{AR}_{\boldsymbol{s}}^A(S^\sharp, T^\sharp) = \mathrm{lfp}(\lambda X^\sharp.T^\sharp \cap_P (S^\sharp \cup_P \widetilde{\mathrm{pre}}_R^A(X^\sharp))) \\
\mathbf{ER}_{\boldsymbol{s}}^A(S^\sharp, T^\sharp) = \mathrm{lfp}(\lambda X^\sharp.T^\sharp \cap_P (S^\sharp \cup_P \mathrm{pre}_R^A(X^\sharp)))
\end{array}
$$

It turns out that the best correct approximations pre_R^A and $\widetilde{\mathrm{pre}}_R^{\triangledown A}$ can be characterized through the abstract transition relation $R^{\exists\exists} \subseteq P \times P$ as follows.

Lemma 6.2. $\mathrm{pre}_R^A = \mathrm{pre}_{R^{\exists\exists}}$ *and* $\widetilde{\mathrm{pre}}_R^{\triangledown A} = \widetilde{\mathrm{pre}}_{R^{\exists\exists}}$.

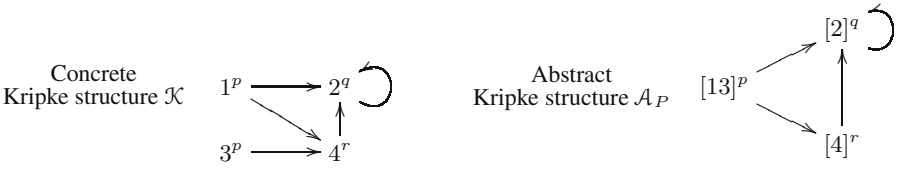
Let $Op \subseteq \{\mathrm{EX}, \mathrm{AX}, \mathrm{EF}, \mathrm{AG}, \mathrm{EU}, \mathrm{AU}_w, \mathrm{AR}, \mathrm{ER}_s\}$ be a set of temporal fixpoint-based operators and let $\mathcal{L} \ni \varphi ::= p \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi \mid f(\varphi_1, \ldots, \varphi_{\mathrm{ar}(f)})$, where $f \in Op$, be the corresponding language. Let $\mathcal{K} = (\Sigma, R, AP, \ell)$ be a concrete Kripke structure and $\mathcal{S}$ be the concrete semantic structure for $\mathcal{L}$ induced by $\mathcal{K}$. Consider now a partition $P \in \mathrm{Part}(\Sigma)$ and the corresponding abstract semantic structure $\mathcal{S}^P = (\wp(P), I^P)$.

Assume that $\mathcal{S}^P$ is s.p. for $\mathcal{L}$. As a consequence of the above results, it turns out that one can define an abstract Kripke structure on P whose abstract transition relation is $R^{\exists\exists}$ which induces precisely $\mathcal{S}^P$.

Corollary 6.3. *If $\mathcal{S}^P$ is s.p. for $\mathcal{L}$ then $\mathcal{S}^P$ is induced by the abstract Kripke structure $\mathcal{A}_P = (P, R^{\exists\exists}, AP, \ell_P)$, where $\ell_P \stackrel{\text{def}}{=} \lambda B \in P.\{p \in AP \mid B \in I^P(p)\}$.*

Thus, a strongly preserving abstract model checking of the language $\mathcal{L}$ can be performed on the abstract Kripke structure $\mathcal{A}_P$.

Example 6.4. Let us consider $\mathcal{L} \ni \varphi ::= p \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi \mid \mathrm{AG}\varphi$ and the following Kripke structure $\mathcal{K}$ and let $\mathcal{S}$ be the concrete semantic structure for $\mathcal{L}$ induced by $\mathcal{K}$.

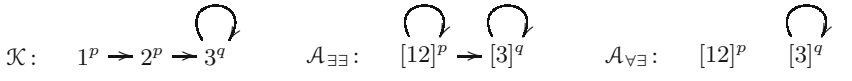


Let us consider the partition $P = \{[13], [2], [4]\}$ and the corresponding abstract semantic structure $\mathcal{S}^P = (\wp(P), I^P)$. It turns out that $\mathcal{S}^P$ is s.p. for $\mathcal{L}$. This is a consequence of the fact that the abstract domain $\wp(P)$ is operator-wise forward complete for $\mathcal{L}$ hence $\wp(P)$ is language forward complete for $\mathcal{L}$ and in turn, by Theorem 3.4, $\mathcal{S}^P$ is s.p. for $\mathcal{L}$. In fact, the following equalities show that $\wp(P)$ is forward complete for $\mathbf{AG}$, because $\mathbf{AG}$ maps unions of blocks in P to unions of blocks in P:

$$\mathbf{AG}(\varnothing) = \mathbf{AG}(\{4\}) = \mathbf{AG}(\{1,3\}) = \mathbf{AG}(\{1,3,4\}) = \varnothing;$$
$$\mathbf{AG}(\{2\}) = \mathbf{AG}(\{1,2,3\}) = \{2\};$$
$$\mathbf{AG}(\{2,4\}) = \{2,4\};$$
$$\mathbf{AG}(\{1,2,3,4\}) = \{1,2,3,4\}.$$

Thus, by Corollary 6.3, it turns out that $\mathcal{S}^P$ is induced by the abstract Kripke structure $\mathcal{A}_P = (P, R^{\exists\exists}, AP_P, \ell_P)$ which is depicted above. Let us notice that P is not a bisimulation on $\mathcal{K}$ because the states 1 and 3 belong to the same block $[13]$ and $1 \to 2$ while $3 \not\to 2$. Thus, strong preservation of $\mathcal{L}$ on the abstract Kripke structure $\mathcal{A}_P$, with abstract transition relation $R^{\exists\exists}$, cannot be obtained as a consequence of standard strong preservation results [2, 3, 13]. □

Example 6.5. Let us consider $\mathcal{L} \ni \varphi ::= p \mid \varphi \wedge \varphi_2 \mid \neg\varphi \mid \mathrm{EG}\varphi$ and the following Kripke structure $\mathcal{K}$ and let $\mathcal{S}$ be the concrete semantic structure for $\mathcal{L}$ induced by $\mathcal{K}$.



In this case, EG is not included among the operators of Corollary 6.3. Let us consider the partition $P = \{[13], [2], [4]\}$, the abstract domain $A = \wp(P)$ and the corresponding abstract semantic structure $\mathcal{S}^A = (A, I^A)$. It turns out that $\mathcal{S}^A$ is s.p. for $\mathcal{L}$. As in Example 6.4, by Theorem 3.4, this derives from the following equalities which show

that A is forward complete for $\mathbf{EG}$, because $\mathbf{EG}$ maps unions of blocks in P to unions of blocks in P:

$$\mathbf{EG}(\varnothing) = \mathbf{EG}(\{1,2\}) = \varnothing; \quad \mathbf{EG}(\{3\}) = \{3\}; \quad \mathbf{EG}(\{1,2,3\}) = \{1,2,3\}.$$

Let us point out here that both the abstract Kripke structures $\mathcal{A}_{\exists\exists}$ and $\mathcal{A}_{\forall\exists}$ on P depicted above, whose abstract transition relations are, respectively, $R^{\exists\exists}$ and $R^{\forall\exists}$, are not s.p. for $\mathcal{L}$. This is shown by the following counterexamples:

$$[1,2] \models^{\mathcal{A}_{\exists\exists}} \mathrm{EG}p \text{ while } 1 \not\models^{\mathcal{K}} \mathrm{EG}p; \quad [1,2] \not\models^{\mathcal{A}_{\forall\exists}} \mathrm{EG}(p \vee q) \text{ while } 1 \models^{\mathcal{K}} \mathrm{EG}(p \vee q).$$

On the other hand, we can exploit Corollary 6.1 so that $\mathbf{EG}^A(S^\sharp) = \mathrm{gfp}(\lambda X^\sharp.S^\sharp \cap_P \mathrm{pre}_R^{\forall A}(X^\sharp))$, where $\mathrm{pre}_R^{\forall A} = \alpha_P^\forall \circ \mathrm{pre}_R \circ \gamma_P$. For instance, we have that

$$\mathrm{pre}_R^{\forall A}(\{[3]\}) = \alpha_P^\forall(\mathrm{pre}_R(\gamma_P(\{[3]\}))) = \alpha_P^\forall(\mathrm{pre}_R(\{3\})) = \alpha_P^\forall(\{2,3\}) = \{[3]\}.$$

Likewise, $\mathrm{pre}_R^{\forall A}(\varnothing) = \mathrm{pre}_R^{\forall A}(\{[12]\}) = \varnothing$ and $\mathrm{pre}_R^{\forall A}(\{[12],[3]\}) = \{[12],[3]\}$. As an example, we have that $\mathbf{EG}^A(\{[3]\}) = \mathrm{gfp}(\lambda X^\sharp.\{[3]\} \cap \mathrm{pre}_R^{\forall A}(X^\sharp)) = \{[3]\}$. □

6.2 Disjunctive Abstractions

In model checking, disjunctive abstract domains have been implicitely used by Henzinger et al.'s [14] algorithm for computing simulation equivalence: in fact, this algorithm maintains, for any state $s \in \Sigma$, a set of states $\mathrm{sim}(s) \subseteq \Sigma$ which represents exactly a disjunctive abstract domain. As observed in Section 3.2, any partitioning abstract domain is disjunctive while the converse is not true.

Let $\mathcal{G} = (\wp(\Sigma)_\subseteq, \alpha, \gamma, A)$ be a disjunctive GI. By Proposition 2.1 (i), $\mathcal{G}^\nabla = (\wp(\Sigma)_\supseteq, \alpha^\nabla, \gamma, A_\geq)$ is a GI where $\alpha^\nabla(S) = \vee\{a \in A \mid \gamma(a) \subseteq S\}$. Thus, we can apply Theorem 5.1 to $\mathcal{G}$ for least fixpoints and Theorem 5.1 to $\mathcal{G}^\nabla$ for greatest fixpoints. Also, as already observed in Section 6.1, the hypotheses of Theorem 5.1 for least and greatest fixpoints coincide and, in this case, the best correct approximations of some concrete function w.r.t. $\mathcal{G}$ and $\mathcal{G}^\nabla$ coincide. We use f^A to denote the best correct approximation of some concrete function f w.r.t. $\mathcal{G}$ while $f^{\nabla A}$ denotes the best correct approximation of f w.r.t. $\mathcal{G}^\nabla$. Here, we can generalize Corollary 6.1 to disjunctive abstract domains for the case of "finally" and "globally" operators.

Corollary 6.6. *Let $\mathcal{G} = (\wp(\Sigma)_\subseteq, \alpha, \gamma, A)$ be a disjunctive GI .Assume that $\mathcal{G}$ is forward complete for some operator $F \in \{\mathbf{AF}, \mathbf{EF}, \mathbf{AG}, \mathbf{EG}\}$. Then, the corresponding best correct approximations of F w.r.t. $\mathcal{G}$ are as follows:*

$$\mathbf{AF}^A(S^\sharp) = \mathrm{lfp}(\lambda X^\sharp.S^\sharp \cup \widetilde{\mathrm{pre}}_R^A(X^\sharp)); \quad \mathbf{EF}^A(S^\sharp) = \mathrm{lfp}(\lambda X^\sharp.S^\sharp \cup \mathrm{pre}_R^A(X^\sharp));$$
$$\mathbf{AG}^A(S^\sharp) = \mathrm{gfp}(\lambda X^\sharp.S^\sharp \cap \widetilde{\mathrm{pre}}_R^{\nabla A}(X^\sharp)); \quad \mathbf{EG}^A(S^\sharp) = \mathrm{gfp}(\lambda X^\sharp.S^\sharp \cap \mathrm{pre}_R^{\nabla A}(X^\sharp)).$$

Example 6.7. Let us consider the concrete Kripke structure $\mathcal{K}$ of Example 5.2 and the language $\mathcal{L} \ni \varphi ::= p \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \vee \varphi_2 \mid \mathrm{EF}\varphi$. Let $\mathrm{Atoms} \stackrel{\mathrm{def}}{=} \{[1],[2],[3],[6],[245]\}$ and let A be the closure under arbitrary unions of Atoms. Let $(\wp(\Sigma)_\subseteq, \alpha, \mathrm{id}, A_\subseteq)$ be the corresponding disjunctive GI where α on singletons in $\wp(\Sigma)$ is as follows:

$$\alpha(\{1\}) = [1]; \quad \alpha(\{2\}) = [2]; \quad \alpha(\{3\}) = [3];$$
$$\alpha(\{4\}) = [245]; \quad \alpha(\{5\}) = [245]; \quad \alpha(\{6\}) = [6].$$

It turns out that A is forward complete for $\mathbf{EF}$ because $\mathbf{EF}$ maps atoms to unions of atoms and $\mathbf{EF}$ is additive:

$$\mathbf{EF}(\{1\}) = \{1\};\ \ \mathbf{EF}(\{2\}) = \{1,2\};\ \ \mathbf{EF}(\{3\}) = \{1,2,3\};$$
$$\mathbf{EF}(\{6\}) = \{1,2,3,4,5,6\};\ \ \mathbf{EF}(\{2,4,5\}) = \{1,2,3,4,5\}.$$

Thus, we can apply Corollary 6.6 so that $\mathbf{EF}^A(S^\sharp) = \mathrm{lfp}(\lambda X^\sharp.S^\sharp \cup \mathrm{pre}^A_R(X^\sharp))$, where $\mathrm{pre}^A_R = \alpha \circ \mathrm{pre}_R \circ \mathrm{id}$. For instance, pre^A_R on the atom $[245]$ is as follows:

$$\mathrm{pre}^A_R([245]) = \alpha(\mathrm{pre}_R(\{2,4,5\})) = \alpha(\{1,3,4\}) = [12345].$$

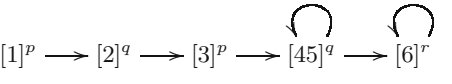
Likewise, we have that pre^A_R on Atoms is as follows:

$$\mathrm{pre}^A_R([1]) = \varnothing;\ \ \mathrm{pre}^A_R([2]) = [1];\ \ \mathrm{pre}^A_R([3]) = [2];\ \ \mathrm{pre}^A_R([6]) = [2456].$$

As an example, $\mathbf{EF}^A([6]) = \mathrm{lfp}(\lambda X^\sharp.[6] \cup \mathrm{pre}^A_R(X^\sharp))$ is computed as follows:

$$\begin{aligned}
&X^\sharp_0 = \varnothing;\\
&X^\sharp_1 = [6] \cup \mathrm{pre}^A_R(\varnothing) = [6] \cup \varnothing = [6];\\
&X^\sharp_2 = [6] \cup \mathrm{pre}^A_R([6]) = [6] \cup [2456] = [2456];\\
&X^\sharp_3 = [6] \cup \mathrm{pre}^A_R([2456]) = [6] \cup [123456] = [123456] \quad \text{(fixpoint)}
\end{aligned}$$

How to obtain an abstract Kripke structure which is s.p. for $\mathcal{L}$? This can be obtained from the coarsest s.p. partition $P_{\mathcal{L}}$ for $\mathcal{L}$ (cf. Section 3.3). As a consequence of results in [17], it turns out that $P_{\mathcal{L}} = \{[1],[2],[3],[6],[45]\}$ because $\wp(P_{\mathcal{L}})$ is exactly the least partitioning refinement of A (cf. Section 3.2). One can define a s.p. abstract Kripke structure $\mathcal{A}$ on $P_{\mathcal{L}}$ by considering $R^{\exists\exists}$ as abstract transition relation:



For the abstract Kripke structure $\mathcal{A}$, $\mathbf{EF}^\sharp([6]) = \mathrm{lfp}(\lambda X^\sharp.\{[6]\} \cup \mathrm{pre}_{R^{\exists\exists}}(X^\sharp))$ is computed as follows:

$$\begin{aligned}
&X^\sharp_0 = \varnothing;\\
&X^\sharp_1 = \{[6]\} \cup \mathrm{pre}_{R^{\exists\exists}}(\varnothing) = \{[6]\};\\
&X^\sharp_2 = \{[6]\} \cup \mathrm{pre}_{R^{\exists\exists}}(\{[6]\}) = \{[6]\} \cup \{[6],[45]\} = \{[6],[45]\};\\
&X^\sharp_3 = \{[6]\} \cup \mathrm{pre}_{R^{\exists\exists}}(\{[6],[45]\}) = \{[6]\} \cup \{[6],[45],[3]\} = \{[6],[45],[3]\};\\
&X^\sharp_4 = \{[6]\} \cup \mathrm{pre}_{R^{\exists\exists}}(\{[6],[45],[3]\}) = \{[6]\} \cup \{[6],[45],[3],[2]\} = \{[6],[45],[3],[2]\};\\
&X^\sharp_5 = \{[6]\} \cup \mathrm{pre}_{R^{\exists\exists}}(\{[6],[45],[3],[2]\}) = \{[6]\} \cup \{[6],[45],[3],[2],[1]\}\\
&\quad = \{[6],[45],[3],[2],[1]\} \quad \text{(fixpoint)}
\end{aligned}$$

The point to observe here is that this standard approach needs a greater number of iterations than our abstract interpretation-based approach to reach the fixpoint. □

Acknowledgements. This work was partially supported by the FIRB Project "Abstract interpretation and model checking for the verification of embedded systems" and by the COFIN2004 Project "AIDA: Abstract Interpretation Design and Applications".

References

1. E.M. Clarke, O. Grumberg, S. Jha, Y. Lu, H. Veith. Progress on the state explosion problem in model checking. In *Informatics - 10 Years Back, 10 Years Ahead*. LNCS 2000, pp. 176-194, 2001.
2. E.M. Clarke, O. Grumberg and D. Long. Model checking and abstraction. *ACM Trans. Program. Lang. Syst.*, 16(5):1512-1542, 1994.
3. E.M. Clarke, O. Grumberg and D.A. Peled. *Model Checking*. The MIT Press, 1999.
4. P. Cousot and R. Cousot. Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *Proc. 4^{th} ACM POPL*, 238-252, 1977.
5. P. Cousot and R. Cousot. Systematic design of program analysis frameworks. In *Proc. 6^{th} ACM POPL*, 269-282, 1979.
6. P. Cousot and R. Cousot. Refining model checking by abstract interpretation. *Automated Software Engineering Journal*, 6(1):69-95, 1999.
7. P. Cousot and R. Cousot. Temporal abstract interpretation. In *Proc. 27^{th} ACM POPL*, pp. 12-25, 2000.
8. D. Dams. *Abstract Interpretation and Partition Refinement for Model Checking*. PhD Thesis, Eindhoven Univ., 1996.
9. D. Dams. Flat fragments of CTL and CTL*: separating the expressive and distinguishing powers. *Logic J. of the IGPL*, 7(1):55-78, 1999.
10. D. Dams, O. Grumberg and R. Gerth. Abstract interpretation of reactive systems. *ACM Trans. Program. Lang. Syst.*, 16(5):1512-1542, 1997.
11. R. Giacobazzi and E. Quintarelli. Incompleteness, counterexamples and refinements in abstract model checking. In *Proc. 8^{th} SAS*, LNCS 2126, pp. 356-373, 2001.
12. R. Giacobazzi, F. Ranzato and F. Scozzari. Making abstract interpretations complete. *J. ACM*, 47(2):361-416, 2000.
13. O. Grumberg and D.E. Long. Model checking and modular verification. *ACM Trans. Program. Lang. Syst.*, 16(3):843-871, 1994.
14. M.R. Henzinger, T.A. Henzinger and P.W. Kopke. Computing simulations on finite and infinite graphs. In *Proc. 36^{th} FOCS*, pp. 453-462, 1995.
15. C. Loiseaux, S. Graf, J. Sifakis, A. Bouajjani and S. Bensalem. Property preserving abstractions for the verification of concurrent systems. *Formal Methods in System Design*, 6:1-36, 1995.
16. D. Massé. Semantics for abstract interpretation-based static analyzes of temporal properties. In *Proc. 9^{th} SAS*, LNCS 2477, pp. 428-443, 2002.
17. F. Ranzato and F. Tapparo. Strong preservation as completeness in abstract interpretation. In *Proc. 13^{th} ESOP*, LNCS 2986, pp. 18-32, 2004.
18. F. Ranzato and F. Tapparo. An abstract interpretation-based refinement algorithm for strong preservation. In *Proc. 11^{th} TACAS*, LNCS 3440, pp. 140-156, 2005.
19. D.A. Schmidt. Closed and logical relations for over- and under-approximation of powersets. In *Proc. 11^{th} SAS*, LNCS 3148, pp. 22-37, 2004.