Abstracting Induction by Extrapolation and Interpolation

Patrick Cousot

Courant Institute of Mathematical Sciences, New York University
pcousot@cims.nyu.edu, cims.nyu.edu/~pcousot

Abstract. We introduce a unified view of induction performed by automatic verification tools to prove a given program specification This unification is done in the abstract interpretation framework using extrapolation (widening/dual-widening) and interpolation (narrowing, dual-narrowing, which are equivalent up to the exchange of the parameters). Dual-narrowing generalizes Craig interpolation in First Order Logic pre-ordered by implication to arbitrary abstract domains. An increasing iterative static analysis using extrapolation of successive iterates by widening followed by a decreasing iterative static analysis using interpolation of successive iterates by narrowing (both bounded by the specification) can be further improved by a increasing iterative static analysis using interpolation of iterates with the specification by dual-narrowing until reaching a fixpoint and checking whether it is inductive for the specification.

Keywords: Abstract induction, Abstract interpretation, Dual-narrowing, Dual-widening, Extrapolation, Interpolation, Narrowing, Static analysis, Static checking, Static verification, Widening.

1. Introduction

Program analysis, checking, and verification require some form of induction on program steps [41,62], fixpoints [64], program syntactic structure [47,65], program data [6], or more generally segmentation hierarchies [26]. Whichever form of induction is chosen, the difficulties boil down to the basic case of a proof that $\mathbf{lfp}^{\subseteq} F \subseteq S$ where $S \in \mathscr{D}$ is a specification in a concrete poset $\langle \mathscr{D}, \subseteq, \bot, \cup \rangle$ and $F \in \mathscr{D} \mapsto \mathscr{D}$ is a transformer given by the program semantics, or dually[1,2]. Hypotheses on F like monotony, [co-]continuity, contraction, *etc.* ensure the existence of the least fixpoint $\mathbf{lfp}^{\subseteq} F$ for partial order $\subseteq$.

Since the concrete domain $\mathscr{D}$ is in general not machine-representable, the problem is abstracted in an abstract domain $\overline{\mathscr{D}}$ which is a pre-order[3] $\langle \overline{\mathscr{D}}, \sqsubseteq, \overline{\bot}, \overline{\sqcup} \rangle$ with increasing concretization $\gamma \in \overline{\mathscr{D}} \mapsto \mathscr{D}$. An example is the pre-order $\langle \mathsf{FOL}, \implies, \mathsf{ff}, \vee \rangle$ of first-order formulæ FOL preordered by implication $\implies$. The concretization is the interpretation of formulae in a given set-theoretic structure. This is an abstraction since not all set-theoretic properties are expressible in first order logic, a problem which is at the origin of the incompleteness of Hoare logic [47,17].

The concrete transformer F is abstracted by an abstract transformer $\overline{F} \in \overline{\mathscr{D}} \mapsto \overline{\mathscr{D}}$ satisfying the pointwise semi-commutation property $F \circ \gamma \mathrel{\dot{\subseteq}} \gamma \circ \overline{F}$ (or dually). Abstract iterates $\overline{X}^0 \triangleq \overline{\bot}$, ..., $\overline{X}^{n+1} \triangleq \overline{F}(\overline{X}^n)$, ..., are designed to converge to a limit $\overline{I} \in \overline{\mathscr{D}}$, which is an inductive abstract property, that is $\overline{F}(\overline{I}) \sqsubseteq \overline{I}$ (*e.g.* $\overline{I}$ is an inductive invariant [41,62]).

For abstract specifications $\overline{S} \in \overline{\mathscr{D}}$, the program verification consists in checking that $\overline{I} \sqsubseteq \overline{S}$. By semi-commutation and fixpoint induction [66], this implies $\mathbf{lfp}^{\subseteq} F \subseteq \gamma(\overline{S})$. The abstraction is always meant to be sound (a proof in the abstract is valid in the concrete, $\overline{I} \sqsubseteq \overline{S} \implies \mathbf{lfp}^{\subseteq} F \subseteq$

[1] $\mathbf{lfp}^{\subseteq}_{D} F$ is the $\subseteq$-least fixpoint of F $\subseteq$-greater than or equal D, if any. The least fixpoint of F, if any, is $\mathbf{lfp}^{\subseteq} F \triangleq \mathbf{lfp}^{\subseteq}_{\bot} F$ where $\bot$ is the infimum of $\mathscr{D}$. $\mathbf{gfp}^{\subseteq}_{D} F \triangleq \mathbf{lfp}^{\supseteq}_{D} F$ is dual.

[2] A variant, as found in strictness analysis [61] is $\mathbf{lfp}^{\sqsubseteq} F \subseteq S$ where the computational order $\sqsubseteq$ is different from the approximation order/logical implication $\subseteq$ can be handled in a way similar to that proposed in this paper, see [23].

[3] The pre-order $\sqsubseteq$ is reflexive and transitive. Additionally, a partial order is antisymmetric.

$\gamma(\overline{S})$) and sometimes complete (a valid concrete property $\gamma(\overline{S})$ can be proved in the abstract *i.e.* $\mathbf{lfp}^{\subseteq} F \subseteq \gamma(\overline{S}) \implies \overline{I} \sqsubseteq \overline{S}$). A very simple example of a complete abstraction is the First of a context-free grammar [25].

When using finite domains $|\overline{\mathcal{D}}| \in \mathbb{N}$ (which was shown in [18] to be strictly equivalent to predicate abstraction [43]) or Noetherian domains (*i.e.*, with no infinite ascending and/or descending chain), the induction is done implicitly by repeated joins (or dually meets) in the abstract domain. By the finiteness hypothesis, the abstract iterates always converge in finitely many steps to a fixpoint limit.

This is more difficult for static analysis using infinitary abstract domains not satisfying ascending/descending chain conditions. Successive joins/meets for successive fixpoint iterations may diverge. It is therefore necessary to make an induction on the iterates and to pass to the limit. Under appropriate conditions like [co-]continuity this limit does exist and is unique. Abstract interpretation theory has introduced increasing iterations with widening extrapolation followed by a decreasing iteration with narrowing interpolation (and there duals) to over/under-approximate the limit in finitely many steps [13,20]. When the specification cannot be verified after these two phases, we propose to use a further increasing iteration phase by interpolation with respect to this specification by dual-narrowing. The whole process can be repeated if necessary. In the particular case where the abstract domain $\overline{\mathcal{D}}$ is the set $\langle \mathsf{FOL}, \implies, \mathsf{ff}, \vee \rangle$ of first-order logical sentences over the program variables and symbols, often quantifier-free, pre-ordered by implication, the additional phase is comparable to program verification using Craig interpolants [56].

We recall and show the following results.

- In **Sect. 2.**, we recall known facts on iteration and fixpoints.
- In **Sect. 3.**, we briefly recall basic static analysis methods in infinite abstract domains by extrapolation with widening/dual-widening and interpolation with narrowing/dual-narrowing.
- In **Sect. 4.**, we explain why a terminating [dual-]widening (enforcing the convergence of iterations by extrapolation with [dual-]widening) cannot be increasing in its first parameter. It follows that static analyzers (like Astrée [28]) which proceed by induction on the program syntax cannot assume that the abstract transformers $\overline{F}[\![\mathtt{C}]\!]$ of commands C are increasing since loop components of C may involve non-increasing [dual-]widenings.
- After expressing soundness conditions on widening and its dual with respect to the concrete in **Sect. 5.**, we show in **Sect. 6.** that iteration with widening extrapolation is sound for non-increasing abstract transformers $\overline{F}$ by referring to the concrete fixpoint iterations for an increasing transformer F. Similarly, soundness conditions on narrowing and its dual are expressed in the concrete in **Sect. 7.** In **Sect. 8.**, iterations with narrowing interpolation for non-increasing abstract transformers are shown to be sound with respect to the concrete iterations for a increasing concrete transformer F.
- In **Sect. 9.**, we study dual-narrowing, which is shown to be a narrowing with inverted arguments, and inversely. Graig interpolation [37] in the abstract domain $\langle \mathsf{FOL}, \implies, \mathsf{ff}, \vee \rangle$ of first-order formulæ pre-ordered by logical implication is an example of dual-narrowing. Static analysis based on Graig interpolation and SMT solvers [55] has limitations [1], including to be only applicable to $\langle \mathsf{FOL}, \implies, \mathsf{ff}, \vee \rangle$, that can be circumvented by appropriate generalization to dual-narrowing in arbitrary abstract domains.
- In **Sect. 10.**, we discuss terminating extrapolators and interpolators.
- In **Sect. 11.**, we show that after an increasing abstract iteration using extrapolation of successive iterates by widening which converges to a post-fixpoint followed by a decreasing abstract iteration using interpolation of successive iterates by narrowing to an abstract fixpoint, it is no longer possible to improve this imprecise abstract fixpoint by repeated applications of the abstract transformer. Nevertheless, it is still possible to improve the over-approximation of the concrete fixpoint by an increasing abstract iteration using interpolation of iterates by dual-narrowing with respect to this imprecise abstract fixpoint. This can be repeated until an inductive argument is found implying the specification or no further improvement is possible.

– In **Sect. 12.**, we compare static verification, checking, and analysis. In **Sect. 13.**, we discuss different utilizations of extrapolation and interpolation. We conclude in **Sect. 14.**

2. Iteration and fixpoints

We recall results on the iteration of transformers on posets. We let $\mathbb{O}$ be the class of all ordinals. We have [14]:

Lemma 1 (Increasing sequences in posets are ultimately stationary). *Any $\preceq$-increasing[4] transfinite sequence $\langle X^\delta,\ \delta \in \mathbb{O}\rangle$ of elements of a poset $\langle \mathscr{P},\ \preceq\rangle$ is ultimately stationary (i.e. $\exists \epsilon \in \mathbb{O} : \forall \delta \geqslant \epsilon : X^\delta = X^\epsilon$. The smallest such ϵ is the rank of the sequence.).* □

Definition 2 (Upper-bounded iterates). *Let $F \in \mathscr{D} \mapsto \mathscr{D}$ be an transformer on a poset $\langle \mathscr{D},\ \subseteq\rangle$ and $D \in \mathscr{D}$. By* upper-bounded iterates of F from D *we mean a transfinite sequence $\langle X^\delta,\ \delta \in \mathbb{O}\rangle$ of elements of $\mathscr{D}$ such that $X^0 \triangleq D$, $X^{\delta+1} \triangleq F(X^\delta)$, and for limit ordinals λ, $\forall \delta < \lambda : X^\delta \subseteq X^\lambda$.* □

Definition 3 (Least-upper-bounded iterates). *Least-upper-bounded iterates (or lub-iterates) are upper-bounded iterates in* **Def. 2** *such that for limit ordinals λ, X^λ is the least element such that $\forall \delta < \lambda : X^\delta \subseteq X^\lambda$ i.e. $\forall Y : \forall \delta < \lambda : X^\delta \subseteq Y \implies X^\lambda \subseteq Y$.* □

Lemma 4 (Increasing fixpoint iterates). *Let $\langle X^\delta, \delta \in \mathbb{O}\rangle$ be the iterates of a transformer $F \in \mathscr{D} \mapsto \mathscr{D}$ on a poset $\langle \mathscr{D},\ \subseteq\rangle$ from $D \in \mathscr{D}$.*

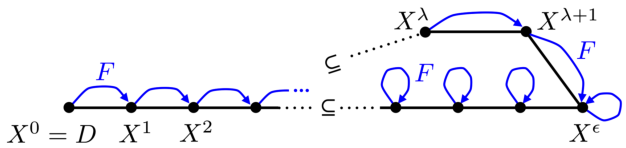
(a) *If F is extensive (i.e. $\forall X \in \mathscr{D} : X \subseteq F(X)$) and the iterates are upper-bounded then they are increasing and F has a fixpoint $\subseteq$-greater than of equal to D.*

(b) *If F is increasing, D a prefix-point of F (i.e. $D \subseteq F(D)$), and the iterates are upper-bounded (resp. least-upper-bounded) then they are increasing and F has a fixpoint $\subseteq$-greater than of equal to D (resp. least fixpoint $\mathit{lfp}^{\subseteq}_D F$).*

(c) *In case* (b) *of lub-iterates, $\forall Y \in \mathscr{D} : (D \subseteq Y \wedge F(Y) \subseteq Y) \implies (\mathit{lfp}^{\subseteq}_D F \subseteq Y)$.* □

Lem. 4.(b)–(c) is often used with the extra assumption that $D = \bot$ is the infimum of a cpo $\langle \mathscr{D}, \subseteq, \bot\rangle$, but the least upper bound (lub) needs only to exist for the iterates, not for all increasing chains (increasing ω-chains when F is assumed to be continuous) of the cpo. For example, $\langle$FOL, $\Longrightarrow$, ff, $\vee\rangle$ has no infinite lubs in general, but specific iterates may or may not have a lub.

Even when X^λ is chosen to be a minimal upper bound of the previous iterates for limit ordinals λ (*i.e.* $\forall \delta < \lambda : X^\delta \subseteq X^\lambda \wedge \forall Y \in \mathscr{D} : (\forall \delta < \lambda : X^\delta \subseteq Y) \implies Y \not\subseteq X^\lambda$), F may have no minimal fixpoint, as shown by the following counter-example



3. Iterative static analysis by extrapolation and interpolation

3.1 Mathematical iteration with induction

To calculate a solution $\overline{I}$ to a system of constraints $\overline{F}(X) \sqsubseteq X$ on a poset $\langle \overline{\mathscr{D}}, \sqsubseteq\rangle$, a mathematician (i) will start from an initial approximation $\overline{I}^0 = \overline{D}$ for some initial guess $\overline{D}$, (ii) calculate the first iterates $\overline{I}^1 = \overline{F}(\overline{I}^0)$, $\overline{I}^2 = \overline{F}(\overline{I}^1)$, *etc.* to help her guess a recurrence hypothesis $\overline{I}^n = \mathcal{I}(\overline{I}^0, \overline{F}, \overline{S}, \sqsubseteq, n)$, (iii) prove that the recurrence hypothesis is inductive $\overline{I}^{n+1} = \overline{F}(\overline{I}^n) = \overline{F}(\mathcal{I}(\overline{I}^0, \overline{F}, \overline{S}, \sqsubseteq, n)) =$

[4] A map $f \in P \mapsto Q$ of pre-order $\langle P, \sqsubseteq\rangle$ into pre-order $\langle Q, \leqslant\rangle$ is *increasing* if and only if $\forall x, y \in P : x \sqsubseteq y \implies f(x) \leqslant f(y)$. In particular, a sequence $\langle X^\delta, \delta \in \mathbb{O}\rangle$, considered as a map $X \in \mathbb{O} \mapsto \mathscr{D}$ where $X^\delta \triangleq X(\delta)$, is *increasing* when $\beta \leqslant \delta \implies X^\beta \subseteq X^\delta$. It is then called an increasing chain.

$\mathcal{J}(\overline{I}^0, \overline{F}, \overline{S}, \sqsubseteq, n+1)$ so that, by recurrence, $\forall n \in \mathbb{N} : \overline{I}^n = \mathcal{J}(\overline{I}^0, \overline{F}, \overline{S}, \sqsubseteq, n))$, and (iv) pass to the limit $\overline{I} = \lim_{n\to\infty} \mathcal{J}(\overline{I}^0, \overline{F}, \overline{S}, \sqsubseteq, n)$. Static analysis must do a similar induction in the abstract.

3.2 Abstract iteration in Noetherian domains

In abstract interpretation with finite abstract domains (which has been shown to be strictly equivalent to predicate abstraction [18]) and, more generally, with Noetherian domains, the induction, which consists in joining/(dually intersecting) the successive abstract properties $\mathcal{J}(\overline{I}^0, \overline{F}, \overline{S}, \sqsubseteq, n+1) = \bigsqcup_{k\leqslant n}(\mathcal{J}(\overline{I}^0, \overline{F}, \overline{S}, \sqsubseteq, k))$, is pre-encoded in the join/(dually meet) operations of the abstract domain. They are ensured to converge in finitely many steps to a fixpoint limit.

3.3 Abstract iteration in non-Noetherian domains with convergence acceleration

In abstract interpretation with infinitary non-Noetherian abstract domains extra machinery is needed to discover inductive hypotheses and pass to the limit. For example extrapolators like terminating widening [12] and dual-widening [20] can enforce convergence of increasing iterations after finitely many steps as illustrated in **Fig. 1**. Instead of applying the function as in **Def. 2**

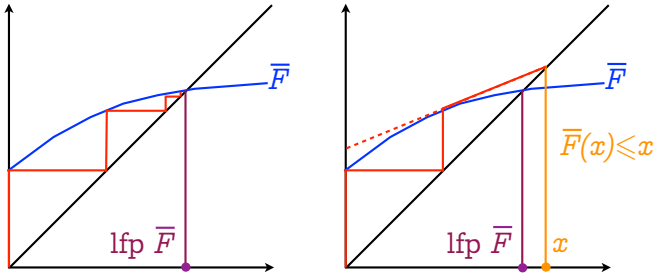


Fig. 1. Convergence acceleration by extrapolation with widening

or 3, its derivative is used to accelerate convergence and ultimately reach a post-fixpoint which over-approximates the least fixpoint [66]. A similar widening is implicitly used in [36].

3.4 Extrapolators (widening, dual-widening) and interpolators (narrowing, dual-narrowing)

The convergence acceleration operators used in abstract interpretation are of two distinct kinds. The widening [12] and dual-widening [20] are extrapolators. They are used to find abstract properties outside the range of known abstract properties. The narrowing [13] and dual-narrowing [20] are interpolators. They are used to find abstract properties within the range of known abstract properties. The objective is to over-approximate or under-approximate the limit of increasing or decreasing fixpoint iterations, so that the various possibilities of using the convergence acceleration operators of **Table 1** are illustrated in **Fig. 2**. Notice that their are four distinct notions since widening and narrowing (as well as dual-widening and dual-narrowing) are definitely *not* order-dual concepts. Of course widening and dual-widening (as well as narrowing and dual-narrowing) *are* order-dual concepts. In [11], the approximation properties of extrapolators are considered

	Convergence above the limit	Convergence below the limit
Increasing iteration	Widening ∇	Dual-narrowing $\widetilde{\Delta}$
Decreasing iteration	Narrowing Δ	Dual-widening $\widetilde{\nabla}$

Table 1. Extrapolators (∇, $\widetilde{\nabla}$) and interpolators (Δ, $\widetilde{\Delta}$)

separately from their convergence properties. For example, their approximation properties are useful to approximate missing or costly lattice join/meet operations. Independently, their convergence properties are useful to ensure termination of iterations for fixpoint approximation.

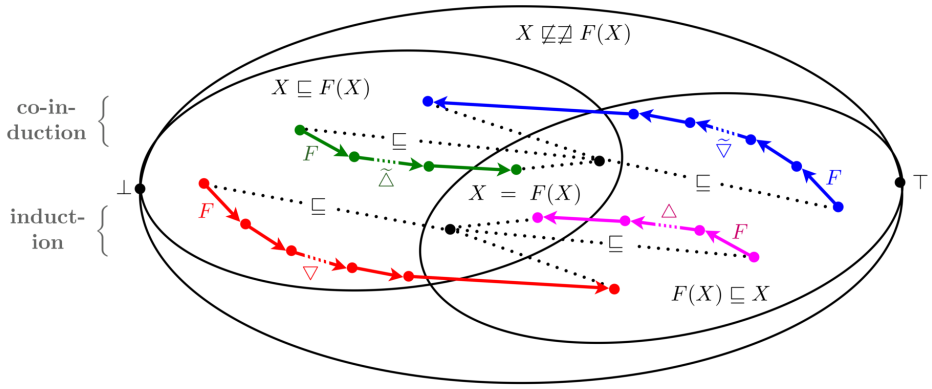


Fig. 2. Fixpoint iteration approximation

4. Terminating (dual) widenings are not increasing

An iteration sequence with widening in a poset $\langle \overline{\mathcal{D}}, \sqsubseteq \rangle$ has the form $\overline{X}^0 \triangleq \overline{D}$, where $\overline{D} \in \overline{\mathcal{D}}$ is some initial approximation, and $\overline{X}^{k+1} \triangleq \overline{X}^k \nabla \overline{F}(\overline{X}^k)$, $k \in \mathbb{N}$ where $\overline{F}$ can be assumed to be extensive on the iterates[5]. It follows that the iterates $\langle \overline{X}^k, k \in \mathbb{N} \rangle$ form a $\sqsubseteq$-increasing chain[6].

The widening $\nabla \in \overline{\mathcal{D}} \times \overline{\mathcal{D}} \mapsto \overline{\mathcal{D}}$ should have the following properties.

(∇.a) $\quad \forall \overline{X}, \overline{Y} \in \overline{\mathcal{D}} : \overline{Y} \sqsubseteq \overline{X} \nabla \overline{Y}$.

Requiring the widening to be extensive in its second parameter, that is an extrapolator, ensures that $\overline{F}(\overline{X}^k) \sqsubseteq \overline{X}^{k+1}$, which guarantees convergence to an over-approximation of the limit $\lim_{k \to +\infty} \overline{F}^k(D)$ of the exact iterates $\overline{F}^0(\overline{X}) = \overline{X}$ and $\overline{F}^{n+1}(\overline{X}) = \overline{F}(\overline{F}^n(\overline{X}))$.[7]

(∇.b) $\quad \forall \overline{X}, \overline{Y} \in \overline{\mathcal{D}} : (\overline{Y} \sqsubseteq \overline{X}) \implies (\overline{X} \nabla \overline{Y} = \overline{X})$.

This condition (∇.b) guarantees that the iterations with widening do stop as soon as a solution $\overline{X}^n$ to the constraint problem of finding $\overline{X}$ such that $\overline{F}(\overline{X}) \sqsubseteq \overline{X}$ has been found. If $\overline{F}(\overline{X}^n) \sqsubseteq \overline{X}^n$, then ($\nabla$.b) ensures that the next iterate is $\overline{X}^{n+1} \triangleq \overline{X}^n \nabla \overline{F}(\overline{X}^n) = \overline{X}^n$.

(∇.c) $\quad \nabla$ is *terminating* that is for any increasing chain $\langle \overline{X}^k \in \overline{\mathcal{D}}, k \in \mathbb{N} \rangle$ and arbitrary sequence $\langle \overline{Y}^k \in \overline{\mathcal{D}}, k \in \mathbb{N} \rangle$ such that $\forall k \in \mathbb{N} : \overline{X}^k \sqsubseteq \overline{Y}^k$, the sequence $\langle \overline{X}^k \nabla \overline{Y}^k, k \in \mathbb{N} \rangle$ is ultimately stationary (*i.e.* $\exists n \in \mathbb{N} : \forall k \geqslant n : \overline{X}^k \nabla \overline{Y}^k = \overline{X}^n$).

This condition (∇.c) guarantees the convergence of the iterates with widening where $\langle \overline{Y}^k, k \in \mathbb{N} \rangle$ stands for $\langle \overline{F}(\overline{X}^k), k \in \mathbb{N} \rangle$ so that $\forall k \in \mathbb{N} : \overline{X}^k \sqsubseteq \overline{Y}^k$ since $\overline{F} \in \overline{\mathcal{D}} \mapsto \overline{\mathcal{D}}$ is extensive but is otherwise unknown. Because $\overline{X}^k \sqsubseteq \overline{F}(\overline{X}^k) \sqsubseteq \overline{X}^k \nabla \overline{F}(\overline{X}^k) \triangleq \overline{X}^{k+1}$, $\langle \overline{X}^k, k \in \mathbb{N} \rangle$ is a $\sqsubseteq$-increasing chain.

---

[5] *i.e.*, $\forall k \in \mathbb{N} : \overline{X}^k \sqsubseteq \overline{F}(\overline{X}^k)$. This is also the case when $\overline{D} \sqsubseteq \overline{F}(\overline{D})$ and $\overline{F}$ is increasing, *i.e.*, $\forall \overline{X}, \overline{Y} \in \overline{\mathcal{D}} : (\overline{X} \sqsubseteq \overline{Y}) \implies \overline{F}(\overline{X}) \sqsubseteq \overline{F}(\overline{Y})$. It is always possible to use $\boldsymbol{\lambda}\, \overline{X} \cdot \overline{X} \sqcup \overline{F}(\overline{X})$ when the join $\sqcup$ exists in the abstract domain $\overline{\mathcal{D}}$.

[6] If $\overline{F}$ is not extensive, one can assume that $\forall \overline{X}, \overline{Y} \in \overline{\mathcal{D}} : \overline{X} \sqsubseteq \overline{X} \nabla \overline{Y}$ in which case $\forall i \in \mathbb{N} : \overline{X}^i \sqsubseteq \overline{X}^{i+1}$.

[7] Besides extrapolation, widenings are also as an over-approximation/upper-bound in posets missing least upper bounds. In that case, in addition to (∇.a), it is also required $\forall \overline{X}, \overline{Y} \in \overline{\mathcal{D}} : \overline{X} \sqsubseteq \overline{X} \nabla \overline{Y}$. Such widenings can be generalized to sets of infinitely many parameters $\nabla \in \wp(\overline{\mathcal{D}}) \mapsto \overline{\mathcal{D}}$ such that $\forall \mathfrak{X} \in \wp(\overline{\mathcal{D}}) : \forall P \in \mathfrak{X} : P \sqsubseteq \nabla \mathfrak{X}$.

Example 5 (Interval widenings). The basic widening on the abstract domain of integer intervals $\mathbb{I} \triangleq \{\emptyset\} \cup \{[a,b] \mid -\infty \leqslant a \leqslant b \leqslant +\infty \wedge a \neq +\infty \wedge b \neq -\infty\}$ was defined in [19] as $\emptyset \nabla X = X \nabla \emptyset \triangleq X$, $[a,b] \nabla [c,d] \triangleq [\!(c < a \,?\, -\infty : a)\!], [\!(d > b \,?\, +\infty : b)\!]$[8]. This basic widening may yield static analyzes which are less precise than the sign analysis. For example $[2,+\infty] \nabla [1, +\infty] = [-\infty,+\infty]$ whereas the sign is $[0,+\infty]$. This is why the interval widening was refined in [16] into $[a,b] \nabla [c,d] \triangleq [\!(0 \leqslant c < a \,?\, 0 \,[\!]\, c < a \,?\, -\infty : a)\!], [\!(d > b \geqslant 0 \,?\, 0 \,[\!]\, d > b \,?\, +\infty : b)\!]$. This can be further improved by using static thresholds in addition to zero [28] or even dynamic thresholds chosen during the static analysis [52]. In all cases, these widenings are not increasing in their first parameter $[0,1] \sqsubseteq [0,2]$ but $[0,1] \nabla [2,2] = [0,+\infty] \not\sqsubseteq [0,2] = [0,2] \nabla [2,2]$. □

Counter-example 6 (Top widening). The top widening $X \nabla_\top Y \triangleq \top$ is terminating, increasing in its first parameter, but does not satisfy (∇.b). A solution $\overline{F}(\overline{X}^k) \sqsubseteq \overline{X}^k$ is degraded to $\overline{X}^{k+1} = \overline{X}^k \nabla \overline{F}(\overline{X}^k) = \top$. This imprecision can be avoided by choosing $X \nabla Y \triangleq [\!(Y \sqsubseteq X \,?\, X : \top)\!]$, which is more accurate but not increasing. If $X_1 \sqsubset Y \sqsubset X_2 \sqsubset T$ then $X_1 \nabla Y = \top \not\sqsubseteq X_2 \nabla Y = X_2$. □

Theorem 7 (Non-monotonicity of terminating [dual] widening). *Let $\langle \overline{\mathcal{D}}, \sqsubseteq \rangle$ be a poset and $\nabla \in \overline{\mathcal{D}} \times \overline{\mathcal{D}} \mapsto \overline{\mathcal{D}}$ be a widening satisfying* (∇.a), (∇.b)*, and* (∇.c)*. Then ∇ cannot be increasing in its first parameter. The dual holds for the dual-widening $\widetilde{\nabla}$ satisfying the order-dual* ($\widetilde{\nabla}$.a), ($\widetilde{\nabla}$.b)*, and* ($\widetilde{\nabla}$.c) *of conditions* (∇.a), (∇.b) *and possibly* (∇.c).

Proof. By reflexivity, $\overline{Y} \sqsubseteq \overline{Y}$ so (∇.b) implies $\overline{Y} \nabla \overline{Y} = \overline{Y}$. By reductio ad absurdum, if ∇ is increasing in its first parameter then $\overline{X} \sqsubseteq \overline{Y}$ implies $\overline{X} \nabla \overline{Y} \sqsubseteq \overline{Y} \nabla \overline{Y} = \overline{Y} \sqsubseteq \overline{X} \nabla \overline{Y}$ by (∇.a) which implies that $\overline{X} \nabla \overline{Y} = \overline{Y}$ by antisymmetry. By (∇.c), $\forall k \geqslant n$, $\overline{X}^{n+k} = \overline{X}^k \nabla \overline{Y}^k = \overline{X}^k = \overline{X}^n$. By hypothesis $\overline{X}^k \sqsubseteq \overline{Y}^k$ so $\overline{X}^k \nabla \overline{Y}^k = \overline{Y}^k$ which implies $\forall k \geqslant n : \overline{Y}^k = \overline{X}^n$, in contradiction with the fact that $\langle \overline{Y}^k,\ k \in \mathbb{N} \rangle$ is an arbitrary sequence of elements of $\overline{\mathcal{D}}$, hence in general not ultimately stationary. □

When $D \sqsubseteq \overline{F}(D)$ and $\overline{F}$ is continuous, hence increasing and such that $\lim_{k \to +\infty} \overline{F}^k(D) = \mathbf{lfp}^{\sqsubseteq}_D \overline{F}$, the intuition for **Th. 7** is that applications of $\overline{F}$ and ∇ from below this fixpoint would remain below the fixpoint, making any over-approximation impossible. The jump over the least fixpoint must be extensive but cannot be increasing (dually decreasing hence monotone in general).

Many non-Noetherian static analyzes of infinite-state systems proceed by successive analyzes in different abstract domains $\langle \overline{\mathcal{D}}_i, \sqsubseteq_i \rangle$, $i = 1, \ldots, n$, *e.g.* by refinement. A comparison of the successive iterative analyzes performed in these domains is possible by concretizing to the most precise one (or their reduced product). Then **Th. 7** shows that there is no guarantee of precision improvement. This problem is soundly taken into account by [54, Sect. 7] and [59, Sect. 5.1], but is otherwise too often completely ignored.

When transformers $\overline{F}[\![\mathtt{C}]\!]$ are defined by structural induction on the syntax of the command `C` as in Astrée [28], this command `C` may involve loops, which abstract semantics is defined by fixpoint iterations with terminating widenings, hence may be non-increasing. In the worst case, $\mathbf{lfp}^{\sqsubseteq} \overline{F}[\![\mathtt{C}]\!]$ may simply not exist.

Example 8 (Non-increasing transformer). Consider the program `while (TRUE) {if (x == 0) {x = 1} else {x = 2}}`. To ensure termination of the static analysis, the forward transformer for this program is $\overline{F}_{\mathtt{while}}(I) = \mathbf{lfp}^{\sqsubseteq} \boldsymbol{\lambda} X \cdot X \nabla (I \sqcup \overline{F}_{\mathtt{if}}(X))$ where ∇ is the basic widening of *Ex. 5* and $\overline{F}_{\mathtt{if}}(X) = [\!(0 \in X \,?\, [1,1] : \emptyset)\!] \sqcup [\!(\exists x \in X : x \neq 0 \,?\, [2,2] : \emptyset)\!]$ is the transformer for the conditional.

The iterates for $\overline{F}_{\mathtt{while}}([0,0])$ are $\overline{X}^0 = \emptyset$, $\overline{X}^1 = \overline{X}^0 \nabla \overline{F}_{\mathtt{if}}(\overline{X}^0) = [0,0]$, and $\overline{X}^2 = \overline{X}^1 \nabla \overline{F}_{\mathtt{if}}(\overline{X}^1) = [0,0] \nabla ([0,0] \sqcup ([1,1] \sqcup \emptyset)) = [0,+\infty]$ such that $\overline{F}_{\mathtt{if}}(\overline{X}^2) \sqsubseteq \overline{X}^2$. The iterates for

[8] The conditional expression is $[\!(\mathrm{tt} \,?\, a : b)\!] \triangleq a$ and $[\!(\mathrm{ff} \,?\, a : b)\!] \triangleq b$.

$\overline{F}_{\texttt{while}}([0,2])$ are $\overline{Y}^0 = \emptyset$, $\overline{Y}^1 = \overline{Y}^0 \mathbin{\overline{\nabla}} \overline{F}_{\texttt{if}}(\overline{Y}^0) = [0,2]$, and $\overline{Y}^2 = \overline{Y}^1 \mathbin{\overline{\nabla}} \overline{F}_{\texttt{if}}(\overline{Y}^1) = [0,2] \mathbin{\overline{\nabla}} ([0, 0] \sqcup ([1,1] \sqcup [2,2])) = [0,2]$ such that $\overline{F}_{\texttt{if}}(\overline{Y}^2) \sqsubseteq \overline{Y}^2$.

So the transformer $\overline{F}_{\texttt{while}}$ is *not* increasing since $[0,0] \sqsubseteq [0,2]$ but $\overline{F}_{\texttt{while}}([0,0]) \not\sqsubseteq \overline{F}_{\texttt{while}}([0, 2])$. It follows that the transformer of any program containing this `while` command will be a composition of transformers involving $\overline{F}_{\texttt{while}}$ and so will not, in general, be increasing. □

5. Hypotheses on widening, dual-widening, and correspondence

Widening and dual-widening are extrapolators in that their result is outside the range of their parameters.

5.1 Widening

Soundness conditions on widenings are usually expressed in the abstract domain (such as ($\overline{\nabla}$.a)) but can be weakened into conditions expressed in the concrete domain, as follows:

Hypotheses 9 (Sound widening for concretization γ).

(a) • for $\overline{\nabla} \in \overline{\mathcal{D}} \times \overline{\mathcal{D}} \mapsto \overline{\mathcal{D}}$, $\quad \forall \overline{P}, \overline{Q} \in \overline{\mathcal{D}} : \gamma(\overline{P}) \subseteq \gamma(\overline{P} \mathbin{\overline{\nabla}} \overline{Q}) \wedge \gamma(\overline{Q}) \sqsubseteq \gamma(\overline{P} \mathbin{\overline{\nabla}} \overline{Q})$

(a′) $\quad \forall \overline{P}, \overline{Q} \in \overline{\mathcal{D}} : \overline{P} \sqsubseteq (\overline{P} \mathbin{\overline{\nabla}} \overline{Q}) \wedge \overline{Q} \sqsubseteq (\overline{P} \mathbin{\overline{\nabla}} \overline{Q})$

(b) • for $\overline{\nabla} \in \wp(\overline{\mathcal{D}}) \mapsto \overline{\mathcal{D}}$, $\quad \forall \mathfrak{X} \in \wp(\overline{\mathcal{D}}) : \forall \overline{P} \in \mathfrak{X} : \gamma(\overline{P}) \subseteq \gamma(\overline{\nabla}\mathfrak{X})$ □

Widenings have to be defined for each specific abstract domains like intervals [19], polyhedra [30,2], *etc.* or combinations of abstract domains like reduced product, powerset domains [3], cofibred domains [68], *etc.* It follows that the Galois calculus to define abstract interpretations [27] can be extended to widening and more generally to all interpolators and extrapolators.

5.2 Dual-widening

The dual-widening $\overline{\widetilde{\nabla}}$ satisfies the order dual of **Hyp. 9** hence the dual of the following theorem **Th. 10** reformulating [11, Ch. 4, Th. 4.1.1.0.3 & Th. 4.1.1.0.9]. This is useful to under-approximate greatest fixpoints *e.g.* [7].

6. Over-approximating increasing abstract iterates by extrapolation with widening

We reformulate the abstract static analysis by iteration with widening of **Sect. 4.** for non-increasing transformers. Soundness proofs can no longer be done in the abstract. They can be done instead with respect to an increasing concrete semantics (**Th. 10**).

6.1 Increasing iteration with widening

We have the following reformulation of [11, Ch. 4, Th. 4.1.1.0.2 & Th. 4.1.1.0.6].

Theorem 10 (Over-approximation of increasing abstract iterates by widening). *Let $\langle X^\delta, \delta \in \mathbb{O}\rangle$ be the least upper bound iterates of the increasing transformer $F \in \mathcal{D} \mapsto \mathcal{D}$ on a concrete poset $\langle \mathcal{D}, \subseteq\rangle$ from $D \in \mathcal{D}$ such that $D \subseteq F(D)$. By* **Lem. 4** (b)*, $\langle X^\delta, \delta \in \mathbb{O}\rangle$ is therefore increasing and ultimately stationary at $X^\epsilon = \mathit{lfp}^{\subseteq}_D F$.*

Let $\overline{\mathcal{D}}$ be the abstract domain, $\gamma \in \overline{\mathcal{D}} \mapsto \mathcal{D}$ be the concretization, $\overline{F} \in \overline{\mathcal{D}} \mapsto \overline{\mathcal{D}}$ be the abstract transformer, $\overline{\nabla} \in \overline{\mathcal{D}} \times \overline{\mathcal{D}} \mapsto \overline{\mathcal{D}}$ be a widening satisfying **Hyp. 9** (a) *and $\overline{\nabla} \in \wp(\overline{\mathcal{D}}) \mapsto \overline{\mathcal{D}}$ be a widening satisfying* **Hyp. 9** (b) *for all $\mathfrak{X} = \{\overline{X}^\delta \mid \delta < \lambda \wedge \lambda \in \mathbb{O}$ is a limit ordinal$\}$ where the abstract iterates are the transfinite sequence $\langle \overline{X}^\delta \in \overline{\mathcal{D}}, \delta \in \mathbb{O}\rangle$ defined such that $\overline{X}^{\delta+1} \triangleq \overline{X}^\delta \mathbin{\overline{\nabla}} \overline{F}(\overline{X}^\delta)$ and $\overline{X}^\lambda \triangleq \overline{\nabla}_{\beta<\lambda} \overline{X}^\beta$ for limit ordinals λ. Then*

(a) *The concretization $\langle \gamma(\overline{X}^\delta), \delta \in \mathbb{O}\rangle$ of the abstract iterates $\langle \overline{X}^\delta, \delta \in \mathbb{O}\rangle$ is increasing and ultimately stationary with limit $\gamma(\overline{X}^\epsilon)$.*

Moreover, if $D \subseteq \gamma(\overline{X}^0)$ and the semi-commutation condition $\forall \delta \in \mathbb{O} : F \circ \gamma(\overline{X}^\delta) \subseteq \gamma \circ \overline{F}(\overline{X}^\delta)$ holds, then

(b) $\forall \delta \in \mathbb{O} : X^\delta \subseteq \gamma(\overline{X}^\delta)$ (*so, in particular* $X^\epsilon \subseteq \gamma(\overline{X}^\varepsilon)$).

Moreover if the abstract domain $\langle \overline{\mathcal{D}}, \sqsubseteq \rangle$ *is a pre-order* ($\sqsubseteq$ *is reflexive and transitive, but not necessarily antisymmetric) and the concretization* $\gamma \in \overline{\mathcal{D}} \mapsto \mathcal{D}$ *is increasing* ($\overline{X} \sqsubseteq \overline{Y} \implies \gamma(\overline{X}) \subseteq \gamma(\overline{Y})$), *then*

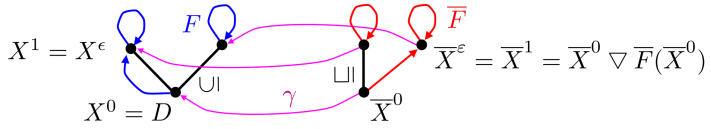
(c) $\forall \delta \in \mathbb{O} : F(\gamma(\overline{X}^\delta)) \subseteq \gamma(\overline{X}^\delta) \implies \mathit{lfp}_D^\subseteq F \subseteq \gamma(\overline{X}^\delta)$.

(d) *Moreover, if* ∇ *is terminating i.e. the iterates are ultimately stationary at some rank* $n \in \mathbb{N}$ *then* $\overline{F}(\overline{X}^n) \nabla \overline{X}^n = \overline{X}^n$ *so* $\gamma(\overline{F}(\overline{X}^n)) \subseteq \gamma(\overline{X}^n)$, $F(\gamma(\overline{X}^n)) \subseteq \gamma(\overline{X}^n)$, *and* $\mathit{lfp}_D^\subseteq F \subseteq \gamma(\overline{X}^n)$.

(e) *Moreover, if the terminating widening satisfies* ∇ *satisfies* **Hyp. 9** (a′) *then* $\exists n \in \mathbb{N} : \overline{F}(\overline{X}^n) \sqsubseteq \overline{X}^n$ *so* $\mathit{lfp}_D^\subseteq F \subseteq \gamma(\overline{X}^n)$. □

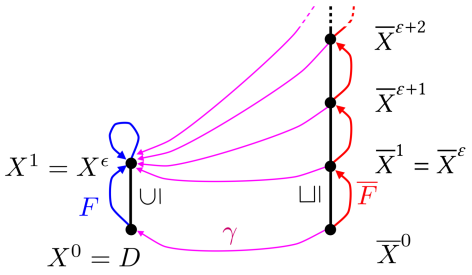
Condition **Th. 10**.(c) is a sufficient condition for stopping the abstract iteration, always applicable by **Th. 10**.(d) for terminating widenings, and in case **Hyp. 9** (a′) checkable with the abstract pre-order $\sqsubseteq$ by **Th. 10**.(e). Note that in **Th. 10**.(d), the abstract domain is a pre-order, maybe not antisymmetric, so that the widening must avoid the problem of iterating within an equivalence class under equivalence $(X \equiv Y) \triangleq (X \sqsubseteq Y \wedge X \sqsupseteq Y)$. Interesting examples are given in [42].

Remark 11. Notice that in **Th. 10**, F is assumed to be increasing but $\overline{F}$ is not assumed to be either $\sqsubseteq$-extensive or increasing because, in case $\overline{F}$ is defined by structural induction, it might depend upon widenings that are not increasing, see *Ex. 8* and **Th. 7**. Nevertheless, the limit of the abstract iterates over-approximate that of the concrete iterates. This may not be the case with the hypotheses of **Lem. 4**.(a). In the following counter-example, F is extensive but not increasing. Both concrete and abstract iterates have limits but $X^\epsilon \not\subseteq \gamma(\overline{X}^\varepsilon)$.



□

Remark 12. If in **Th. 10** (d) the widening ∇ satisfies **Hyp. 9** (b) but not **Hyp. 9** (a′) then there may exist no $\delta \in \mathbb{O}$ such that $\overline{F}(\overline{X}^\delta) \sqsubseteq \overline{X}^\delta$. Here is a counter-example where ∇ is the lub.



□

6.2 Parameterized widening

The abstract iterates with widening in **Th. 10** can be generalized to widenings including additional parameters such the iteration rank δ, a list of thresholds T, possibly depending on the rank $T(\delta)$, the abstract transformer $\overline{F}$, all previous iterates $\langle \overline{X}^\beta,\ \beta \leqslant \delta \rangle$ and their transformation $\langle \overline{F}(\overline{X}^\beta),\ \beta \leqslant \delta \rangle$, *etc*, so that $\overline{X}^{\delta+1} \triangleq \nabla(\delta, T(\delta), \overline{F}, \langle \overline{X}^\beta,\ \beta \leqslant \delta \rangle, \langle \overline{F}(\overline{X}^\beta),\ \beta \leqslant \delta \rangle)$. The idea applies to all other extrapolators and interpolators.

Example 13 (Parameterized [dual-]widenings). Delayed widening [28] is an example of parameterized widening $\nabla(\delta)$ where a join or a standard widening is performed depending on the iteration rank parameter δ (often counted as the number of iterations in a loop).

n-bounded abstract model checking [4] for universal properties implicitly uses an iteration $\overline{X}^{k+1} \triangleq \overline{X}^k \nabla_{(k)} \overline{F}(\overline{X}^k)$ with an parameterized widening $\overline{X} \nabla_{(k)} \overline{Y} \triangleq \langle\!| k \leqslant n \ ? \ \overline{Y} \ : \ \overline{\top} |\!\rangle$ where $\overline{\top}$ is the abstract supremum: $\forall X \in \mathcal{D} : P \subseteq \gamma(\overline{\top})$. For existential properties, n-bounded abstract

model checking implicitly uses a dual-widening $\overline{X}\ \overline{\nabla}_{(k)}\ \overline{Y} \triangleq \langle\!|\, k \leqslant n \ ?\ \overline{Y} \,:\, \overline{\bot} \,|\!\rangle$. Unreachability after n steps is a correct under-approximation of the executions that do go on. It follows in both cases that everything is known exactly before n steps and completely unknown beyond n steps. This is an abstract interpretation of the concrete trace semantics, even when $\overline{\mathscr{D}} = \mathscr{D}$ and $\overline{F} = F$, since in both cases concrete traces are abstracted by the identity for the first n steps and by $\top$ (resp. $\bot$) for the remaining steps.

ESC/Java™ [39] implicitly uses a dual-widening which unrolls loops twice (and outs assume false, *i.e.* $\overline{\bot}$). This under-approximates the loop semantics which is unsound for checking invariance properties.

An extreme example avoiding any iteration is the so called *abstract acceleration* for specific abstract domains and programs where $\nabla(\sqsubseteq, \overline{D}, \overline{F}) = \overline{X}^{\mathcal{E}}$ so that the abstract solution can be computed exactly from the program text abstraction $\overline{F}$ [50], may be including a few iterations for iterative constraint solving methods.

Between these extreme examples, parameterized widenings can smoothly be made less and less precise over successive iterations (*e.g.* by widening to less and less given or program-dependent thresholds [28]). □

7. Hypotheses on narrowing, dual-narrowing, and correspondence

Narrowing and dual-narrowing are interpolators in that their result is within the range of their parameters.

7.1 Narrowing

A narrowing $\overline{\Delta} \in \overline{\mathscr{D}} \times \overline{\mathscr{D}} \mapsto \overline{\mathscr{D}}$ is an interpolation of its parameters, $\forall \overline{P}, \overline{Q} \in \overline{\mathscr{D}} : \overline{Q} \sqsubseteq \overline{P} \implies \overline{Q} \sqsubseteq \overline{P}\ \overline{\Delta}\ \overline{Q} \sqsubseteq \overline{P}$. We can also define $\overline{\Delta} \in \wp(\overline{\mathscr{D}}) \mapsto \overline{\mathscr{D}}$ such that $\forall \mathfrak{X} \in \wp(\overline{\mathscr{D}}) : \forall \overline{P} \in \overline{\mathscr{D}} : (\forall \overline{Q} \in \mathfrak{X} : \overline{P} \sqsubseteq \overline{Q}) \implies \overline{P} \sqsubseteq \overline{\Delta}\mathfrak{X}$. Otherwise stated, the narrowing $\overline{\Delta}\mathfrak{X}$ over-approximate any lower bound of X (hence its greatest lower bound if it exists).

These conditions expressed in the abstract domain can be weakened into conditions expressed in the concrete domain, as follows:

Hypotheses 14 (Sound narrowing for concretization γ).

- for $\overline{\Delta} \in \overline{\mathscr{D}} \times \overline{\mathscr{D}} \mapsto \overline{\mathscr{D}}$,

(a) $\quad \forall \overline{P}, \overline{Q} \in \overline{\mathscr{D}} : (\gamma(\overline{Q}) \subseteq \gamma(\overline{P})) \implies (\gamma(\overline{Q}) \subseteq \gamma(\overline{P}\ \overline{\Delta}\ \overline{Q}) \subseteq \gamma(\overline{P}))$

(a′) $\quad \forall \overline{P}, \overline{Q} \in \overline{\mathscr{D}} : (\gamma(\overline{Q}) \subseteq \gamma(\overline{P})) \implies (\overline{Q} \sqsubseteq (\overline{P}\ \overline{\Delta}\ \overline{Q}) \sqsubseteq \overline{P})$

(a″) $\quad \forall \overline{P}, \overline{Q} \in \overline{\mathscr{D}} : (\overline{Q} \sqsubseteq \overline{P}) \implies (\overline{Q} \sqsubseteq (\overline{P}\ \overline{\Delta}\ \overline{Q}) \sqsubseteq \overline{P})$

- for $\overline{\Delta} \in \wp(\overline{\mathscr{D}}) \mapsto \overline{\mathscr{D}}$,

(b) $\quad \forall P \in \mathscr{D} : \forall \mathfrak{X} \in \wp(\overline{\mathscr{D}}) : (\forall \overline{Q} \in \mathfrak{X} : P \subseteq \gamma(\overline{Q})) \implies (P \subseteq \gamma(\overline{\Delta}\mathfrak{X}) \subseteq \gamma(\overline{Q}))$ □

Example 15 (Interval narrowing). The narrowing of [13,20] for integer intervals $\mathbb{I}$ was $\emptyset\ \Delta\ X \triangleq X\ \Delta\ \emptyset = \emptyset$ for the infimum $\overline{\bot} = \emptyset$. Otherwise, $[a,b]\ \Delta\ [c,d] \triangleq [\langle\!|\, a = -\infty \ ?\ c \,:\, \min(a,c) \,|\!\rangle, \langle\!|\, b = +\infty \ ?\ d \,:\, \max(b,d) \,|\!\rangle]$ improves infinite bounds only. □

7.2 Dual-narrowing

The dual-narrowing $\widetilde{\Delta}$ satisfies the order dual of **Hyp. 14** hence the dual of **Th. 22** reformulating [11, Ch. 4, Th. 4.1.1.0.12].

Example 16 (Interval dual-narrowing). If $[a,b] \subseteq [c,d]$ then $c \leqslant a \leqslant b \leqslant d$ so we can define $[a,b]\ \widetilde{\Delta}\ [c,d] \triangleq [\langle\!|\, c = -\infty \ ?\ a \,:\, \lfloor (a+c)/2 \rfloor \,|\!\rangle, \langle\!|\, d = \infty \ ?\ b \,:\, \lceil (b+d)/2 \rceil \,|\!\rangle]$ where $\lfloor x \rfloor$ is the largest integer not greater than real x and $\lceil x \rceil$ is the smallest integer not less than real x since $c \leqslant \lfloor (a+c)/2 \rfloor \leqslant a \leqslant b \leqslant \lceil (b+d)/2 \rceil \leqslant d$ and therefore $[a,b] \subseteq ([a,b]\ \widetilde{\Delta}\ [c,d]) \subseteq [c,d]$. □

Example 17 (Bounded interval dual-narrowing). If $[a,b] \subseteq [c,d] \subseteq [\ell,h]$ (*e.g.* $\ell =$ `min_int`, $h =$ `max_int` for machine integers) then $[a,b]\ \widetilde{\Delta}\ [c,d] \triangleq [\lfloor (a+c)/2 \rfloor, \lceil (b+d)/2 \rceil] \subseteq [\ell,h]$. □

Example 18 (Craig interpolation). Craig's interpolation theorem [31] implies that for all first-order formulæ $\varphi, \psi \in \mathsf{FOL}$ such that $\neg(\varphi \wedge \psi)$ there exist a first-order formula ρ, called an interpolant, such that $\psi \implies \rho, \neg(\rho \wedge \psi)$, and $\mathsf{Vars}[\![\rho]\!] \subseteq (\mathsf{Vars}[\![\varphi]\!] \cap \mathsf{Vars}[\![\psi]\!])$. Letting $\psi' \triangleq \neg\psi$ this means that if $\varphi \implies \psi'$ then there exists an interpolant ρ such that $\varphi \implies \rho \implies \psi'$. So a dual-narrowing can be defined as $\varphi \mathbin{\widetilde{\Delta}} \psi' \triangleq \rho$ on the abstract domain $\langle \mathsf{FOL}, \implies \rangle$ of first-order formulæ pre-ordered by implication $\implies$, the concretization of a formula being its interpretation in a given domain of discourse. The interpolant is in general not unique, may contain exponentially more logical connectives than φ, and successive interpolations may not terminate. So arbitrary choices have to be done, for example, to compute quantifier-free interpolants with a minimal number of components and symbols [48].

[35, Sect. 5.2, page 145] recognized that Craig interpolation is a narrowing (in fact a dual-narrowing, see **Lem. 19** just below) without the syntactic constraints of Craig interpolation because the lattice is not necessarily constructed from formulae. In Boolean lattices, this coincide with McMillan's use of Craig interpolation [56], which is called separation, mapping a pair satisfying $A \sqcap B \sqsubseteq \bot$ to I such that $A \sqsubseteq I \wedge I \sqcap B \sqsubseteq \bot$ [44, p. 447].

Interpolants in the style of [57] require that abstract domains are or can be complemented [10]. When the interpolation cannot be directly applied to the representation of abstract properties A, B in the abstract domain $\overline{\mathscr{D}}$, it can be applied to their concretization into a pair of formulæ $\langle \gamma(A), \gamma(B) \rangle$ in $\langle \mathsf{FOL}, \implies \rangle$ and the interpolant $\gamma(A) \mathbin{\widetilde{\nabla}} \gamma(B)$ constructed from a refutation proof *e.g.* by an SMT solver [49] can be abstracted back to the abstract domain $\alpha(\gamma(A) \mathbin{\widetilde{\nabla}} \gamma(B))$, a technique is used *e.g.* to generate abstract transformers [67], which can also be used during the static analysis. □

7.3 Correspondence between narrowing and dual-narrowing

The **Hyp. 14** are not self dual. Nevertheless, the narrowing and dual-narrowing are essentially the same notion up to the inversion of their parameters: $X \mathbin{\Delta} Y = X \mathbin{\widetilde{\Delta}}^{-1} Y \triangleq Y \mathbin{\widetilde{\Delta}} X$ and $X \mathbin{\Delta} Y = X \mathbin{\Delta}^{-1} Y \triangleq Y \mathbin{\Delta} X$[9].

Lemma 19 (dual-narrowing as inverse narrowing and dually). *If Δ is a narrowing satisfying* **Hyp. 14** (a) *then Δ^{-1} is a dual-narrowing satisfying the order-dual of* **Hyp. 14** (a). *Reciprocally, the inverse $\widetilde{\Delta}^{-1}$ of a dual-narrowing $\widetilde{\Delta}$ is a narrowing.* □

The interpretation of **Lem. 19** in the context of **Table 1** is that if a narrowing is used for decreasing iterates in **Th. 22** then its inverse can be used for increasing iterates in the dual of **Th. 22**.

Example 20 (Interval narrowing). The inverse of the dual-narrowing of *Ex. 16* is the narrowing $[c, d] \mathbin{\Delta} [a, b] \triangleq [\![\, c = -\infty \mathbin{?} a \mathbin{:} \lfloor (a+c)/2 \rfloor, \, d = \infty \mathbin{?} b \mathbin{:} \lceil (b+d)/2 \rceil \,]\!]$ which is more precise than the narrowing of [13,20] in *Ex. 15*. Convergence in **Th. 22** is guaranteed but much slower. □

Example 21 (Polyhedral narrowing). By *Ex. 18*, Craig interpolation is a dual-narrowing, hence by **Lem. 19** and parameter inversion, a narrowing. For example, Craig interpolation for linear arithmetic over the rationals [8] should yield a narrowing $P \mathbin{\Delta} Q$ for polyhedral static analysis [30] when there is a difference in the variables appearing in both systems of constraints P and Q[10]. □

8. Over-approximating decreasing abstract iterates by interpolation with narrowing

A static analysis by increasing iteration with widening can be improved by any iterate of a decreasing iteration with narrowing. The narrowing cannot make downwards extrapolations which

[9] We use $^{-1}$ to denote the exchange of parameters as in the inverse of relations $r^{-1}(x, y) = r(y, x)$, not as the inverse image of a function $f^{-1}(x, y) = \{z \mid f(z) = \langle x, y \rangle\}$.

[10] Thanks to reviewer 7 for pointing out that the semantic notions of amalgamation might be more adequate than the purely syntactic notion of Craig interpolation in this context. This (together with the related Robinson joint consistency property) remains to be explored [60].

might jump over the least fixpoint. So the narrowing can only do interpolations which prevent jumping below any fixpoint (hence the least one which cannot be simply distinguished from the other fixpoints). We have the following reformulation of [11, Ch. 4, Th. 4.1.1.0.16].

Theorem 22 (Over-approximation of decreasing iterates with narrowing). *By the dual of* **Def. 3**, *let* $\langle Y^\delta,\ \delta \in \mathbb{O}\rangle$ *be the greatest lower bound iterates of the increasing transformer* $F \in \mathcal{D} \mapsto \mathcal{D}$ *on a concrete poset* $\langle \mathcal{D},\ \subseteq\rangle$ *from* $D \in \mathcal{D}$ *such that* $F(D) \subseteq D$. *By the dual of* **Lem. 4** (b), $\langle Y^\delta,\ \delta \in \mathbb{O}\rangle$ *is therefore decreasing and ultimately stationary at* $Y^\epsilon = \boldsymbol{gfp}^{\subseteq}_D F$.

Let the abstract domain $\langle \overline{\mathcal{D}},\ \sqsubseteq\rangle$ *be a pre-order, the concretization* $\gamma \in \overline{\mathcal{D}} \mapsto \mathcal{D}$ *be increasing, the abstract transformer be* $\overline{F} \in \overline{\mathcal{D}} \mapsto \overline{\mathcal{D}}$, $\Delta \in \overline{\mathcal{D}} \times \overline{\mathcal{D}} \mapsto \overline{\mathcal{D}}$ *be a narrowing satisfying* **Hyp. 14** (a) *and* $\Delta \in \wp(\overline{\mathcal{D}}) \mapsto \overline{\mathcal{D}}$ *satisfies* **Hyp. 14** (b) *for* $\mathcal{X} = \{\overline{Y}^\delta \mid \delta < \lambda \wedge \lambda \in \mathbb{O}$ *is a limit ordinal*$\}$, *where the abstract iterates are the transfinite sequence* $\langle \overline{Y}^\delta \in \overline{\mathcal{D}},\ \delta \in \mathbb{O}\rangle$ *such that* $D \subseteq \gamma(\overline{Y}^0)$, $\overline{Y}^{\delta+1} \triangleq \overline{Y}^\delta \,\overline{\Delta}\, \overline{F}(\overline{Y}^\delta)$, $\overline{Y}^\lambda \triangleq \overline{\bigtriangleup}_{\beta<\lambda} \overline{Y}^\beta$ *for limit ordinals* λ, *and do satisfy the semi-commutation condition* $\forall \delta \in \mathbb{O} : F \circ \gamma(\overline{Y}^\delta) \subseteq \gamma \circ \overline{F}(\overline{Y}^\delta)$.

If the abstract transformer $\overline{F} \in \overline{\mathcal{D}} \mapsto \overline{\mathcal{D}}$ *is reductive on the abstract iterates* $\langle \overline{Y}^\delta,\ \delta \in \mathbb{O}\rangle$ (*i.e.* $\forall \delta \in \mathbb{O} : \gamma(\overline{F}(\overline{Y}^\delta)) \subseteq \gamma(\overline{Y}^\delta)$[11]) *then their concretization* $\langle \gamma(\overline{Y}^\delta),\ \delta \in \mathbb{O}\rangle$ *is decreasing and ultimately stationary with limit* $\gamma(\overline{Y}^\epsilon)$ *such that* $\forall \delta \in \mathbb{O} : \boldsymbol{gfp}^{\subseteq}_D F = Y^\epsilon \subseteq \gamma(\overline{Y}^\epsilon) \subseteq \gamma(\overline{Y}^\delta)$. □

Lemma 23 (Traditional soundness requirement for narrowing). *The more traditional hypotheses that* $(P \sqsubseteq Q) \implies (P \sqsubseteq P \,\overline{\Delta}\, Q \sqsubseteq Q)$, $\forall i \in \Delta : (P \sqsubseteq Q_i) \implies (P \sqsubseteq \overline{\bigtriangleup}_{j\in\Delta} Q_j \sqsubseteq Q_i)$, *the initial iterate is* $\overline{F}(\overline{Y}^0) \sqsubseteq \overline{Y}^0$, *and* $\overline{F}$ *is increasing imply that* $\overline{F}$ *is reductive on the iterates.* □

9. Over-approximating bounded increasing abstract iterates by interpolation with dual-narrowing

When the upper bound $\gamma(\overline{Y}^n)$ of the concrete least fixpoint can no longer be improved in the decreasing abstract iterates with narrowing interpolation of **Sect. 8.**, *i.e.* $\overline{F}(\overline{Y}^n) \sqsubseteq \overline{Y}^{n+1} = \overline{Y}^n \,\overline{\Delta}\, \overline{F}(\overline{Y}^n) = \overline{Y}^n$, the upper bound $\overline{Y}^n$ can still be further improved by computing increasing abstract iterates with dual-narrowing interpolation bounded by the *bound specification* $\overline{S} \triangleq \overline{Y}^n$.

9.1 Bounded increasing iteration with dual-narrowing

Let us now consider increasing iterates bounded by a given specification.

Theorem 24 (Over-approximation of bounded increasing iterates with dual-narrowing). *Let* $\langle Z^\delta,\ \delta \in \mathbb{O}\rangle$ *be the least upper bound iterates of the increasing transformer* $F \in \mathcal{D} \mapsto \mathcal{D}$ *on a concrete poset* $\langle \mathcal{D},\ \subseteq\rangle$ *from* $D \in \mathcal{D}$ *such that* $D \subseteq F(D)$. *By* **Lem. 4** (b), $\langle Z^\delta,\ \delta \in \mathbb{O}\rangle$ *is therefore increasing and ultimately stationary at* $Z^\epsilon = \boldsymbol{lfp}^{\subseteq}_D F$.

Let $\overline{\mathcal{D}}$ *be the abstract domain,* $\gamma \in \overline{\mathcal{D}} \mapsto \mathcal{D}$ *be the concretization,* $\overline{S} \in \overline{\mathcal{D}}$ *be the bound specification,* $\overline{F} \in \overline{\mathcal{D}} \mapsto \overline{\mathcal{D}}$ *be the abstract transformer,* $\overline{\Delta} \in \overline{\mathcal{D}} \times \overline{\mathcal{D}} \mapsto \overline{\mathcal{D}}$ *be the dual-narrowing satisfying the order dual of* **Hyp. 14** (a), *and* $\overline{\Delta} \in \wp(\overline{\mathcal{D}}) \mapsto \overline{\mathcal{D}}$ *be the dual-narrowing satisfying the order dual of* **Hyp. 14** (b) *for* $\mathcal{X} \triangleq \{\overline{Z}^\lambda \mid \delta < \lambda \wedge \lambda \in \mathbb{O}$ *is a limit ordinal*$\}$ *where the abstract iterates are the transfinite sequence* $\langle \overline{Z}^\delta \in \overline{\mathcal{D}},\ \delta \in \mathbb{O}\rangle$ *such that* $D \subseteq \gamma(\overline{Z}^0) \subseteq \gamma(\overline{S})$, $\overline{Z}^{\delta+1} \triangleq (\!|\, \gamma(\overline{F}(\overline{Z}^\delta)) \subseteq \gamma(\overline{S}) \;?\; \overline{F}(\overline{Z}^\delta) \,\overline{\Delta}\, \overline{S} \;:\; \overline{S} \,|\!)$, $\overline{Z}^\lambda \triangleq \overline{\Delta}_{\beta<\lambda} \overline{Z}^\beta$ *for limit ordinals* λ, *which are assumed to satisfy the semi-commutation condition* $\forall \delta \in \mathbb{O} : F \circ \gamma(\overline{Z}^\delta) \subseteq \gamma \circ \overline{F}(\overline{Z}^\delta)$. *Then*

(a) *The concretization* $\langle \gamma(\overline{Z}^\delta),\ \delta \in \mathbb{O}\rangle$ *of the abstract iterates* $\langle \overline{Z}^\delta,\ \delta \in \mathbb{O}\rangle$ *is such that* $\forall \delta \in \mathbb{O} : (Z^\delta \subseteq \gamma(\overline{S})) \implies (Z^\delta \subseteq \gamma(\overline{Z}^\delta) \subseteq \gamma(\overline{S}))$;

[11] Since γ is increasing this is implied by $\forall \delta \in \mathbb{O} : \overline{F}(\overline{Y}^\delta) \sqsubseteq \overline{Y}^\delta$.

(b) *Moreover, if* $\langle\overline{\mathcal{D}},\sqsubseteq\rangle$ *is a pre-order and the concretization* $\gamma\in\overline{\mathcal{D}}\mapsto\mathcal{D}$ *is increasing, then* $\forall\delta\in\mathbb{O}$, *if* $\gamma(\overline{F}(\overline{Z}^\delta))\subseteq\gamma(\overline{Z}^\delta)$ *then* $\mathit{lfp}^{\subseteq}_{D}\,F=Z^\delta\subseteq\gamma(\overline{Z}^\delta)\subseteq\gamma(\overline{S})$. □

Note 25. In case (b), the definition $\overline{Z}^{\delta+1}\triangleq\langle\!|\,\gamma(\overline{F}(\overline{Z}^\delta))\subseteq\gamma(\overline{S})\;?\;\overline{F}(\overline{Z}^\delta)\;\overline{\Delta}\;\overline{S}\;:\;\overline{S}\,|\!\rangle$ of the next iterate can be over-approximated by $\overline{Z}^{\delta+1}\triangleq\langle\!|\,\overline{F}(\overline{Z}^\delta)\sqsubseteq\overline{S}\;?\;\overline{F}(\overline{Z}^\delta)\;\overline{\Delta}\;\overline{S}\;:\;\overline{S}\,|\!\rangle$.

Note 26. In case (b), if $\overline{F}$ is extensive or $\overline{Z}^0\sqsubseteq\overline{F}(\overline{Z}^0)$ and $\overline{F}$ is increasing then the abstract iterates $\langle\overline{Z}^\delta,\,\delta\in\mathbb{O}\rangle$ in **Th. 24** form an increasing chain, but this is not necessarily the case in general. □

Note 27. In the definition of the abstract iterates $\langle\overline{Z}^\delta,\,\delta\in\mathbb{O}\rangle$ in **Th. 24**, the dual-narrowing $\overline{\Delta}$ in $\overline{Z}^{\delta+1}\triangleq\langle\!|\,\gamma(\overline{F}(\overline{Z}^\delta))\subseteq\gamma(\overline{S})\;?\;\overline{F}(\overline{Z}^\delta)\;\overline{\Delta}\;\overline{S}\;:\;\overline{S}\,|\!\rangle$ does not use the information provided by $\overline{Z}^\delta$. It would be more informative to use a ternary dual-narrowing with $\overline{Z}^{\delta+1}\triangleq\langle\!|\,\gamma(\overline{F}(\overline{Z}^\delta))\subseteq\gamma(\overline{S})\;?\;\overline{\Delta}(\overline{Z}^\delta,\overline{F}(\overline{Z}^\delta),\overline{S})\;:\;\overline{S}\,|\!\rangle$ such that $\overline{P}\sqsubseteq\overline{Q}\sqsubseteq\overline{S}$ implies $\overline{Q}\sqsubseteq\overline{\Delta}(\overline{P},\overline{Q},\overline{S})\sqsubseteq\overline{S}$. □

Example 28. A variant of *Ex. 17* where $[a,b]\subseteq[c,d]\subseteq[\ell,h]=\overline{S}$ would be $\overline{\Delta}([a,b],[c,d],\overline{S})\triangleq[\langle\!|\,\lfloor(3c-2a+\ell)\,2\rfloor>\ell\;?\;\lfloor(3c-2a+\ell)\,2\rfloor\;:\;\ell\,|\!\rangle,\langle\!|\,\lceil(3d-2b+h)/2\rceil<h\;?\;\lceil(3d-2b+h)/2\rceil\;:\;h\,|\!\rangle]$ which doubles the growth of $[a,b]$ to $[c,d]$. Another example is the widening "up-to" of [46] for polyhedra. □

9.2 Bounded widening versus dual-narrowing

A widening $\nabla_{\overline{S}}$ is bounded by $\overline{S}\in\overline{\mathcal{D}}$ if and only if it satisfies **Hyp. 9** (a′) and $\forall\overline{P},\overline{Q}:\overline{P}\,\nabla_{\overline{S}}\,\overline{Q}\sqsubseteq\overline{S}$. An example is the interval widening on machine integers bounded by [min_int,max_int] which can be generalized to any interval bound $[\ell,h]$.

Then, continuing *Note 27*, $\overline{\Delta}(\overline{P},\overline{Q},\overline{S})\triangleq\overline{P}\,\nabla_{\overline{S}}\,\overline{Q}$ is a dual-narrowing since if $\overline{P}\sqsubseteq\overline{Q}\sqsubseteq\overline{S}$ then by **Hyp. 9** (a′), $\overline{Q}\sqsubseteq\overline{P}\,\nabla_{\overline{S}}\,\overline{Q}$ and $\overline{P}\,\nabla_{\overline{S}}\,\overline{Q}\sqsubseteq\overline{S}$ since the widening is bounded so that $\overline{Q}\sqsubseteq\overline{\Delta}(\overline{P},\overline{Q},\overline{S})\sqsubseteq\overline{S}$.

Reciprocally, if $\overline{\Delta}$ is a dual-narrowing then $\overline{P}\,\nabla_{\overline{S}}\,\overline{Q}\triangleq\overline{\Delta}(\overline{P},\overline{Q},\overline{S})$ may not satisfy **Hyp. 9** (a′) in case $\overline{P}\not\sqsubseteq\overline{P}\,\nabla_{\overline{S}}\,\overline{Q}$. However, in case $\overline{F}$ is increasing or extensive in **Th. 10**, the widening is used only when $\overline{P}\sqsubseteq\overline{Q}$ in which case **Hyp. 9** (a′) holds.

In conclusion, although widenings and dual-narrowing are different concepts, they are equivalent in the specific contexts considered in this **Sect. 9.2**.

Example 29. Observe that $\overline{\Delta}([a,b],[c,d],\overline{S})$ in *Ex. 28* is a bounded widening. □

10. Terminating extrapolators and interpolators

Extrapolators/interpolators $\mathbin{\overline{\boxtimes}}\in\{\nabla,\widetilde{\nabla},\Delta,\widetilde{\Delta}\}$ over/under-approximate the limit of increasing/decreasing chains by abstract induction. *Terminating* operators also enforce termination.

Enforcing termination by extrapolators/interpolators For terminating extrapolators/interpolator, the abstract iterates $\overline{X}^0,\ldots,\overline{X}^{i+1}\triangleq\overline{X}^i\mathbin{\overline{\boxtimes}}\overline{F}(\overline{X}^i),\ldots$ must be ultimately stationary at some rank $n\in\mathbb{N}$. Let us say that the widening ∇ and dual-narrowing $\widetilde{\Delta}$ are *increasing* (since they operate on increasing chains $\langle\gamma(\overline{X}^i),\,i\in\mathbb{N}\rangle$) and, dually that the dual-widening $\widetilde{\nabla}$ and narrowing Δ are *decreasing* (since they operate on decreasing chains $\langle\gamma(\overline{X}^i),\,i\in\mathbb{N}\rangle$). Since we don't want to make hypotheses on the abstract transformer $\overline{F}$, we can consider abstract iterates of the form $\overline{X}^0,\ldots,\overline{X}^{i+1}\triangleq\overline{X}^i\mathbin{\overline{\boxtimes}}\overline{Y}^i,\ldots$ where $\langle\gamma(\overline{X}^i),\,i\in\mathbb{N}\rangle$ is a chain and $\langle\overline{Y}^i,\,i\in\mathbb{N}\rangle$ is arbitrary.

Definition 30 (Terminating extrapolator/interpolator). *An increasing (resp. decreasing) extrapolator/interpolator* $\mathbin{\overline{\boxtimes}}\in\{\nabla,\widetilde{\nabla},\Delta,\widetilde{\Delta}\}$ *such that* $\mathbin{\overline{\boxtimes}}\in\overline{\mathcal{D}}\times\overline{\mathcal{D}}\mapsto\overline{\mathcal{D}}$ *is* terminating *whenever for any chain* $\langle\overline{X}^i\in\overline{\mathcal{D}},\,i\in\mathbb{N}\rangle$ *increasing (resp. decreasing) in the concrete and arbitrary sequence* $\langle\overline{Y}^i\in\overline{\mathcal{D}},\,i\in\mathbb{N}\rangle$, *the sequence* $\overline{X}^0,\ldots,\overline{X}^{i+1}\triangleq\overline{X}^i\mathbin{\overline{\boxtimes}}\overline{Y}^i,\ldots$ *is ultimately stationary at some rank* $n\in\mathbb{N}$. □

The interval widenings of *Ex. 5* and narrowing of *Ex. 15* are all terminating.

Definition 31 (Terminating bounded interpolation operator). *An increasing (resp. decreasing) interpolator* $\mathbin{\overline{\boxtimes}}\in\{\Delta,\widetilde{\Delta}\}$ *such that* $\mathbin{\overline{\boxtimes}}\in\overline{\mathcal{D}}\times\overline{\mathcal{D}}\times\overline{\mathcal{D}}\mapsto\overline{\mathcal{D}}$ *is* terminating *whenever for any chain*

$\langle \overline{Y}^i \in \overline{\mathcal{D}},\ i \in \mathbb{N}\rangle$ *increasing (resp. decreasing) in the concrete and bound* $\overline{S} \in \overline{\mathcal{D}}$*, the sequence* $\overline{X}^0 = \overline{Y}^0, \ldots, \overline{X}^{i+1} = \overline{\boxtimes}(\overline{X}^i, \overline{Y}^i, \overline{S})$[12]*, ... is ultimately stationary at some rank* $n \in \mathbb{N}$*.* □

Example 32. The dual-narrowing of *Ex. 16* bounded by $[-\infty, h]$ or $[\ell, +\infty]$ is not terminating. The bounded interval dual-narrowing of *Ex. 17* is terminating but convergence may be slow. □

11. Fixpoint over-approximation strategy

Given a concrete fixpoint $\mathbf{lfp}^{\subseteq}_{\bot} F$ of a concrete increasing operator $F \in \mathcal{D} \mapsto \mathcal{D}$ on a partially ordered concrete domain $\langle \mathcal{D}, \subseteq, \bot, \cup\rangle$ such that $\mathbf{lfp}^{\subseteq}_{\bot} F = \bigcup_{\delta \in \mathbb{O}} F^\delta(\bot)$ does exist, the static analysis problem is to effectively compute an over approximation of this fixpoint. The abstraction method consists in designing a pre-ordered abstract domain $\langle \overline{\mathcal{D}}, \sqsubseteq, \overline{\bot}, \sqcup\rangle$, an abstract transformer $\overline{F} \in \overline{\mathcal{D}} \mapsto \overline{\mathcal{D}}$, and an increasing concretization function $\gamma \in \overline{\mathcal{D}} \mapsto \mathcal{D}$ satisfying the semi-commutation condition $F \circ \gamma \mathrel{\dot\subseteq} \gamma \circ \overline{F}$, pointwise. We obtain the fixpoint over-approximation by the following successive over-approximations, the first two ones (A) and (B) being classical, as illustrated in **Fig. 3**.

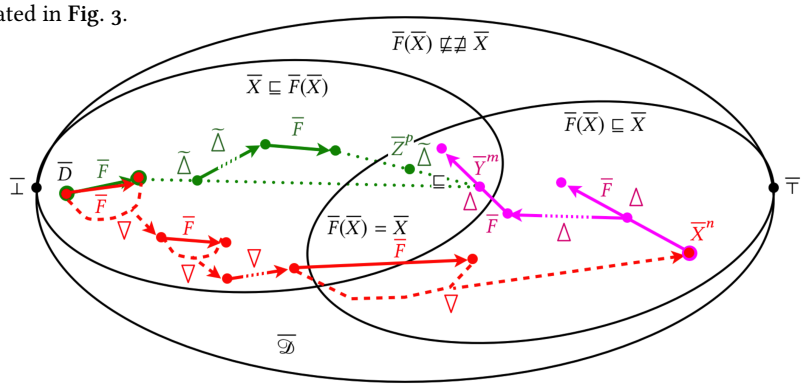


Fig. 3. Successive extrapolations and interpolations

Algorithm 33 (Fixpoint over-approximation by successive extrapolations and interpolations). Input $\overline{F} \in \overline{\mathcal{D}} \mapsto \overline{\mathcal{D}}$ and $\overline{D} \in \overline{\mathcal{D}}$ on a pre-order $\langle \overline{\mathcal{D}}, \sqsubseteq\rangle$. Define $\overline{X} \equiv \overline{Y} \triangleq \overline{X} \sqsubseteq \overline{Y} \wedge \overline{X} \sqsupseteq \overline{Y}$.

(A) Using a terminating widening $\nabla \in \overline{\mathcal{D}} \times \overline{\mathcal{D}} \mapsto \overline{\mathcal{D}}$, compute the iterates $\overline{X}^0 \triangleq \overline{D}, \ldots, \overline{X}^{k+1} \triangleq \overline{X}^k \nabla \overline{F}(\overline{X}^k)$ until convergence $\overline{X}^{n+1} \equiv \overline{X}^n$ at some rank n[13, 14]

(B) If $\overline{F}(\overline{X}^n) \not\equiv \overline{X}^n$ then compute the iterates $\overline{Y}^0 \triangleq \overline{X}^n, \ldots, \overline{Y}^{k+1} \triangleq \overline{Y}^k \Delta \overline{F}(\overline{Y}^k)$ with terminating narrowing $\Delta \in \overline{\mathcal{D}} \times \overline{\mathcal{D}} \mapsto \overline{\mathcal{D}}$, until convergence $\overline{Y}^{m+1} \equiv \overline{Y}^m$ at some rank m.
Otherwise $\overline{F}(\overline{X}^n) \equiv \overline{X}^n$ so skip this step (B) with $\overline{Y}^m \triangleq \overline{X}^n$.

(C) Using a terminating dual-narrowing $\widetilde{\Delta} \in \overline{\mathcal{D}} \times \overline{\mathcal{D}} \mapsto \overline{\mathcal{D}}$, compute the iterates $\overline{Z}^0 \triangleq \overline{D}, \ldots, \overline{Z}^{k+1} \triangleq \overline{F}(\overline{Z}^k) \mathbin{\widetilde{\nabla}} \overline{Y}^m$ until reaching $\overline{Z}^{p+1} \equiv \overline{Z}^p$ at some rank p.

Optionally, if $F(\gamma(\overline{Z}^p)) \subseteq \gamma(\overline{Z}^p)$ and $\overline{Z}^p \not\equiv \overline{Y}^m$, repeat the interpolation steps (B) and (C) from $\overline{X}'^n \triangleq \overline{Z}^p \mathbin{\Delta'} \overline{Y}^m$ (where Δ' is a terminating narrowing satisfying **Hyp. 14** (a)) until convergence to $\overline{Z}^p \mathbin{\Delta'} \overline{Y}^m \equiv \overline{Y}^m$[15]. If $F(\gamma(\overline{Z}^p)) \subseteq \gamma(\overline{Z}^p)$ then return $\overline{Z}^p$ else $\overline{Z}^p \triangleq \overline{Y}^m$ (no improvement). □

[12] $\overline{X}^{i+1} = \overline{Y}^i \mathbin{\overline{\boxtimes}} \overline{S}$ for binary interpolators $\overline{\boxtimes} \in \overline{\mathcal{D}} \times \overline{\mathcal{D}} \mapsto \overline{\mathcal{D}}$.

[13] As shown by **Fig. 3**, checking that $\overline{F}(\overline{F}(\overline{X}^n)) \sqsubseteq \overline{F}(\overline{X}^n)$ might sometimes avoid a last useless widening but **Alg. 33** (A) follows the classical iteration method [20].

[14] The traditional termination condition of reaching a post-fixpoint $\overline{F}(\overline{X}^n) \sqsubseteq \overline{X}^n$ is obtained by $\overline{X} \mathbin{\nabla'} \overline{Y} \triangleq (\!| \overline{Y} \sqsubseteq \overline{X} \mathbin{?} \overline{X} \mathbin{:} \overline{X} \nabla \overline{Y} |\!)$.

[15] In case of static checking (**Sect. 12.**) of a specification $\overline{S}$, one can stop as soon as $\overline{Z}^p \sqsubseteq \overline{S}$. Otherwise, one can also restart at (A) with the new specification $\overline{S} \triangleq \overline{Z}^p$, see **Th. 36**.

Theorem 34 (Soundness and termination of Alg. 33). *Let $\langle \mathscr{D}, \subseteq, \cup \rangle$ be a poset, $F \in \mathscr{D} \mapsto \mathscr{D}$ be increasing, $D \in \mathscr{D}$ be such that $D \subseteq F(D)$, and the concrete iterates $X^0 \triangleq D$, $X^{\delta+1} \triangleq F(X^\delta)$ for successor ordinals, and $X^\lambda \triangleq \bigcup_{\beta<\lambda} X^\beta$ for limit ordinals λ, be well defined in the poset $\langle \mathscr{D}, \subseteq, \cup \rangle$ (i.e. the lubs $\bigcup$ do exist).*

Let the abstract domain $\langle \overline{\mathscr{D}}, \overline{\sqsubseteq} \rangle$ be a pre-order, the concretization $\gamma \in \overline{\mathscr{D}} \mapsto \mathscr{D}$ be increasing, the abstract transformer be $\overline{F} \in \overline{\mathscr{D}} \mapsto \overline{\mathscr{D}}$ satisfying the pointwise semi-commutation condition $F \circ \gamma \dot{\subseteq} \gamma \circ \overline{F}$.

Let $\overline{D} \in \overline{\mathscr{D}}$ be such that $D \subseteq \gamma(\overline{D})$ and $\forall \overline{X} \in \overline{\mathscr{D}} : (\gamma(\overline{D}) \subseteq \gamma(\overline{X}) \wedge \gamma(\overline{F}(\overline{X})) \subseteq \gamma(\overline{X})) \implies (\gamma(\overline{D}) \subseteq \gamma(\overline{F}(\overline{X})))$, $\nabla \in \overline{\mathscr{D}} \times \overline{\mathscr{D}} \mapsto \overline{\mathscr{D}}$ be a terminating widening satisfying **Hyp. 9** (a), *$\Delta \in \overline{\mathscr{D}} \times \overline{\mathscr{D}} \mapsto \overline{\mathscr{D}}$ be a terminating narrowing satisfying* **Hyp. 14** (a) *such that $\forall \overline{X} \in \overline{\mathscr{D}} : (\gamma(\overline{F}(\overline{X})) \subseteq \gamma(\overline{X})) \implies (\gamma(\overline{F}(\overline{X} \mathbin{\Delta} \overline{F}(\overline{X}))) \subseteq \gamma(\overline{X} \mathbin{\Delta} \overline{F}(\overline{X})))$, and $\overline{\Delta} \in \overline{\mathscr{D}} \times \overline{\mathscr{D}} \mapsto \overline{\mathscr{D}}$ be a terminating dual-narrowing satisfying the order dual of* **Hyp. 14** (a).

Then static analysis **Alg. 33** *always terminates with a sound fixpoint over-approximation $\overline{Z}^p$ such that $\mathbf{lfp}^{\subseteq}_D F \subseteq \gamma(\overline{Z}^p) \subseteq \gamma(\overline{Y}^m) \subseteq \gamma(\overline{X}^n)$.*

Given an abstract specification $\overline{S} \in \overline{\mathscr{D}}$, if $\gamma(\overline{Z}^p) \subseteq \gamma(\overline{S})$ (which is implied by $\overline{Z}^p \overline{\sqsubseteq} \overline{S}$) then $\mathbf{lfp}^{\subseteq}_D F \subseteq \gamma(\overline{S})$ else it is unknown whether the specification holds. □

Note 35 (Skipping phases). As suggested by **Fig. 2**, phase (A) of **Alg. 33** can be skipped by starting directly with (B) from the supremum $\overline{X}^n = \overline{\top}$ of $\overline{\mathscr{D}}$ (or a given specification, see **Sect. 12.**). Phase (B) will then over-approximate $\mathbf{gfp}^{\overline{\sqsubseteq}}_{\overline{\top}} \overline{F}$ (which is imprecise in general). Phase (A) of **Alg. 33** is useful to provide an initial over-approximation of $\mathbf{gfp}^{\overline{\sqsubseteq}}_{\overline{X}^n} \overline{F}$, which, in general, is below $\mathbf{gfp}^{\overline{\sqsubseteq}}_{\overline{\top}} \overline{F}$. The narrowing iteration (B) of **Alg. 33** can also be skipped by choosing $Y \mathbin{\Delta} X \triangleq X$. Both phases (A) and (B) of **Alg. 33** can be skipped by starting (C) with an abstract specification $\overline{S} \in \overline{\mathscr{D}}$. □

12. Static verification, checking, and analysis

The static inductive proof $\exists \overline{I} \in \overline{\mathscr{D}} : \overline{F}(\overline{I}) \overline{\sqsubseteq} \overline{I} \wedge \overline{I} \overline{\sqsubseteq} \overline{S}$ can be done in various forms.

(a) In *static verification* by deductive verification methods, the induction hypothesis $\overline{I}$ is provided by the end-user so that the problem is to generate and check the verification condition $\overline{F}(\overline{I}) \overline{\sqsubseteq} \overline{I} \wedge \overline{I} \overline{\sqsubseteq} \overline{S}$.

(b) In *static checking*, the induction hypothesis $\overline{I}$ must be automatically inferred from the transformer $\overline{F}$ and the specification $\overline{S}$ (and also checked to satisfy the verification condition $\overline{F}(\overline{I}) \overline{\sqsubseteq} \overline{I} \wedge \overline{I} \overline{\sqsubseteq} \overline{S}$).

(c) In *static analysis*, the induction hypothesis $\overline{I}$ must be automatically inferred from the transformer $\overline{F}$ (independently of a particular specification $\overline{S}$) and checked to satisfy the verification $\overline{F}(\overline{I}) \overline{\sqsubseteq} \overline{I}$. Then later, when a specification $\overline{S}$ is given, it remains to check that $\overline{I} \overline{\sqsubseteq} \overline{S}$.

Of course static verification (a) such as Boogie [5], ESC/Java [39,40], Dafny [53], *etc* is a subproblem of static checking/analysis since it consists in proving an implication only.

There is no essential difference between static analysis (c) and static checking (b).

– Static analysis (c) is static checking (b) where the specification $\overline{S} = \overline{\top}$ is the always true *i.e.* $\forall \overline{I} : \overline{I} \overline{\sqsubseteq} \overline{\top}$.
– Static checking (b) is static analysis (c) in the abstract domain $\overline{\mathscr{D}}' \triangleq \{P \in \overline{\mathscr{D}} \mid P \overline{\sqsubseteq} \overline{S}\}$. The idea is therefore to assume that the specification $\overline{S}$ does hold and to calculate by **Alg. 33** a more precise inductive fixpoint over-approximation $\overline{Z}^p$ in $\overline{\mathscr{D}}'$. Upon termination it remains to check that the fixpoint over-approximation $\overline{Z}^p$ is inductive and stronger than the specification $\overline{S}$ in $\overline{\mathscr{D}}$.

The following **Th. 36** shows that static checking can be reduced to a static analysis by **Alg. 33** using a widening and transformers bounded by the specification (so that the specification is assumed to hold), to infer a conditionally sound invariant, and then checking that the invariant is inductive.

Theorem 36 (Static checking). *Assume the hypotheses of* **Th. 34**. *Let $\overline{S} \in \overline{\mathscr{D}}$ be a (non-inductive) abstract specification, define $\overline{\mathscr{D}}' \triangleq \{P \in \overline{\mathscr{D}} \mid \gamma(P) \subseteq \gamma(\overline{S})\}$, and let $\overline{D} \in \overline{\mathscr{D}}'$ such that $D \subseteq$*

$\gamma(\overline{D}) \subseteq \gamma(\overline{S})$ *and* $\gamma(\overline{F}(\overline{S})) \not\subseteq \gamma(\overline{S})$[16]. *Let* $\overline{Z}'^{p}$ *be the result of* **Alg. 33** *applied to the restriction* $\overline{F}'(\overline{X}) \triangleq \langle\!| \gamma(\overline{F}(\overline{X})) \subseteq \gamma(\overline{S}) \mathbin{?} \overline{F}(\overline{X}) \mathbin{:} \overline{S} |\!\rangle$ *of* $\overline{F}$ *to* $\overline{\mathscr{D}}'$*, with bounded widening* $\overline{X} \mathbin{\overline{\nabla}'} \overline{Y} \triangleq \langle\!| \overline{X} \mathbin{\overline{\nabla}} \overline{Y} \sqsubseteq \overline{S} \mathbin{?} \overline{X} \mathbin{\overline{\nabla}} \overline{Y} \mathbin{:} \overline{S} |\!\rangle$ *restricting widening* $\overline{\nabla}$ *satisfying* **Hyp. 9** (a) *to* $\overline{\mathscr{D}}'$*, and same narrowing satisfying* **Hyp. 14** (a) *and same dual-narrowing satisfying the dual of* **Hyp. 14** (a)*. If* $F(\gamma(\overline{Z}'^{p})) \subseteq \gamma(\overline{Z}'^{p})$ (*which is implied by* $\overline{F}(\overline{Z}'^{p}) \sqsubseteq \overline{Z}'^{p}$) *then* $\mathbf{lfp}^{\subseteq}_{D}\, F \subseteq \gamma(\overline{S})$. □

13. Discussion

The proposal of [45] is to iterate the widening (A) and narrowing (B) phases of **Alg. 33** to get a sequence of results $\overline{Y}_i^{m_i}$, $i = 1, \ldots, k$ and to return their intersection $\bigcap_{i=1}^{k} \overline{Y}_i^{m_i}$. After each widening/narrowing phase, the result $\overline{Y}_i^{m_i}$ is heuristically perturbated (after observing the origin of the imprecision of the widening) to get a $\sqsubseteq$-smaller value $\overline{D}$ used to restart with the next widening/narrowing phase. One such heuristic perturbation can be done by considering the dual-narrowing $\left(\bigcap_{j=1}^{i-1} \overline{Y}_j^{m_j}\right) \mathbin{\overline{\Delta}} \overline{Y}_i^{m_i}$ with the intersection of the previous iterates, which in general will not be one of the already explored iterates $\overline{Y}_j^{m_j}$, $j = 1, \ldots, i$. However, by **Th. 7**, the widening is not increasing, so that, in contrast to the dual-narrowing phase (C) of **Alg. 33**, there is no guarantee of improvement after a perturbation, whichever perturbation method is chosen.

If ∇ is a widening and $\widetilde{\Delta}$ is a dual-narrowing on an abstract pre-ordered domain $\langle \overline{\mathscr{D}}, \sqsubseteq \rangle$, and the widening overshoots the specification, then $P \mathbin{\nabla'} Q \triangleq Q \mathbin{\widetilde{\Delta}} (P \mathbin{\nabla} Q)$ is a more precise widening (although termination might be lost). This is the essence of [44] where the dual-narrowing is by interpolation.

Following [58], let us compare widening (extrapolation) versus interpolation (narrowing/dual-narrowing), more precisely, **Alg. 33** (A) and (B) on any abstract domain $\overline{\mathscr{D}}$ versus **Alg. 33** (C) alone on the abstract domain $\langle \mathsf{FOL}, \Longrightarrow \rangle$ of first-order predicates pre-ordered FOL by implication $\Longrightarrow$ with Craig interpolation as dual-narrowing.

– It is argued that **Alg. 33** (A) and (B) uses a weak/inexpressive abstract domain with efficient representations and small search space while **Alg. 33** (c) uses a strong/expressive abstract domain $\langle \mathsf{FOL}, \Longrightarrow \rangle$ with generic representations and large search space. In fact both approaches rely on an abstract domain, with loss of information, and this choice is independent of the chosen iteration method. For example [29] shows that combinations of theories in SMT solvers are reduced products of abstract domains (just lacking extrapolation and interpolation operators). Some theories in SMT solvers rely on specific internal representations for efficiency (like affine inequalities).

– The transformers F (and $\overline{F}$) can be weakest pre- or strongest post-conditions (and their abstraction). The fact that the equivalence formalized in the concrete by the Galois connection $\langle \mathscr{D}, \subseteq \rangle \underset{\widetilde{\mathsf{post}}[\tau]}{\overset{\widetilde{\mathsf{pre}}[\tau]}{\leftrightarrows}} \langle \mathscr{D}, \subseteq \rangle$ is preserved in the abstract depends on the abstract domain not on the convergence acceleration method (widening, narrowing, and duals).

– The decision to abstract to (relational) invariants or sets of computation histories is part of the choice of the abstract domain. For example trace-based abstraction [21,9] and trace partitioning [63] can lift any abstraction to reason by case analysis on computation histories.

– Incompleteness comes from the choice of the abstract domain and the extrapolation/interpolation operators. The abstraction is fundamentally incomplete by undecidability. Extrapolation itself is not necessarily non-terminating and incomplete. A counter-example is *abstract acceleration* where the abstract fixpoint can be computed exactly [50].

– Ockham's razor (*lex parsimoniae*) can be made part of the definition of the abstract transformer and the extrapolation/interpolation operators. As pointed out in [24], it is always possible to introduce simplification heuristics *e.g.* by using $\boldsymbol{\lambda}\, X \cdot X \mathbin{\nabla} \overline{F}(X)$ or it's n-unrolling version

[16] If $D \not\subseteq \gamma(\overline{S})$ the problem has no solution and if $\gamma(\overline{F}(\overline{S})) \subseteq \gamma(\overline{S})$ so $F(\gamma(\overline{S})) \subseteq \gamma(\overline{S})$ by semi-commutativity, it is solved, two cases without any interest.

$\boldsymbol{\lambda} X \cdot (\ldots((X \nabla \overline{F}(X)) \nabla \overline{F}^2(X)) \ldots \nabla \overline{F}^n(X))$ where the local widening ∇ performs heuristic simplifications or to approximate the transformer based on interpolation *e.g.* by using $\boldsymbol{\lambda} X \cdot \overline{F}(X) \mathbin{\widetilde{\Delta}} \overline{S}$ as proposed in [56]. Notice that the main contribution to get a simplified transformer $\overline{F} \in \overline{\mathcal{D}} \mapsto \overline{\mathcal{D}}$ is through the careful design of the abstract domain $\overline{\mathcal{D}}$ (and, up to the machine representation of abstract properties in $\overline{\mathcal{D}}$, one can always perform exactly the same static analysis in the concrete domain $\mathcal{D}$ using a widening on $\mathcal{D}$ [22]).

14. Conclusion

The unifying of apparently diverging points of view on extrapolation and interpolation in the abstract interpretation theory leaves opened the question of which part of the fixpoint over-approximation strategy of **Sect. 11.** should be used. Obviously. using only one phase is imprecise while iterating three successive phases in **Alg. 33** will be costly. In our opinion this depends on how close the specification $\overline{S}$ is from the inductive argument $\overline{I}$ to be calculated to do the proof $\overline{F}(\overline{I}) \sqsubseteq \overline{I} \sqsubseteq \overline{S}$ in the abstract. In [51, Sect. 2.5], James H. Morris and Ben Wegbreit observed that subgoal induction (which is a relational backward deductive positive induction method as shown in [15]) "can often be used to prove a loop's correctness directly from its input-output specification without the use of an invariant." or " with weaker-than-normal inductive assertions inside the loops.". Looking at their examples, one sees that the induction hypothesis $\overline{I}$ (is or is a very simple variant of) the specification $\overline{S}$ itself. This was also exploited by Dijsktra for calculational program design [32,33], and more recently in program checking by interpolation [56] and abductive inference [34]. Of course this favorable situation is more frequent for tiny programs than very large ones, in particular when the specification is very far from the inductive invariant.

Such a challenging example is the automatic inference of an interval in the following filter program, intervals being usually considered to be a very simple property.

```
typedef enum {FALSE = 0, TRUE = 1} BOOLEAN; BOOLEAN INIT; float P, X;
void filter () { static float E[2], S[2];
   if (INIT) {S[0] = X; P = X; E[0] = X;}
   else { P = (((((0.5*X)-(E[0]*0.7))+(E[1]*0.4))+(S[0]*1.5))-(S[1]*0.7));}
   E[1] = E[0]; E[0] = X; S[1] = S[0]; S[0] = P;
   /* S[0], S[1] in [l, h] */ }
void main () { X = 0.2*X+5; INIT = TRUE;  /* simulated filter input */
   while (1) { X = 0.9*X+35; filter (); INIT = FALSE; } }
```

The problem is to infer automatically maximal `l` and minimal `h` bounds such that `S[0], S[1]` $\in$ `[l, h]` is invariant in the program. Because `l` and `h` are unknown in the invariant `S[0], S[1]` $\in$ `[l, h]`, neither static verification nor static checking methods can be helpful. The full burden of finding the bounds, which is not easy, is entirely put by these methods on the end-users. But static analyzers, like Astrée [28,38], automatically infer that `[l, h]` $\subseteq$ `[-1418.3753, 1418.3753]`, with no user hint or interaction. This is challenging in purely syntactic domains such as $\langle \mathsf{FOL}, \Longrightarrow \rangle$.

Acknowledgements. Work supported by NSF Expeditions in Computing CMACS, award 0926166.

References

[1] Albarghouthi, A., Li, Y., Gurfinkel, A., Chechik, M.: Ufo: A framework for abstraction- and interpolation-based software verification. CAV. LNCS 7358, 672–678, Spr.inger (2012)

[2] Bagnara, R., Hill, P.M., Ricci, E., Zaffanella, E.: Precise widening operators for convex polyhedra. Sci. Comput. Program. 58(1-2), 28–56 (2005)

[3] Bagnara, R., Hill, P.M., Zaffanella, E.: Widening operators for powerset domains. STTT 9(3-4), 413–414 (2007)

[4] Biere, A., Cimatti, A., Clarke, E.M., Zhu, Y.: Symbolic model checking without BDDs. TACAS. LNCS 1579, 193–207. Springer (1999)

[5] Böhme, S., Leino, K.R.M., Wolff, B.: HOL-Boogie – an interactive prover for the Boogie program-verifier. TPHOLs. LNCS 5170, 150–166. Springer (2008)

[6] Burstall, R.M.: Program proving as hand simulation with a little induction. IFIP Congress. 308–312 (1974)

[7] Chakarov, A., Sankaranarayanan, S.: Expectation invariants for probabilistic program loops as fixed points. SAS, LNCS 8723, 85–100. Springer (2014)

[8] Cimatti, A., Griggio, A., Sebastiani, R.: Efficient generation of Craig interpolants in satisfiability modulo theories. ACM Trans. Comput. Log. 12(1), 7 (2010)

[9] Colby, C., Lee, P.: Trace-based program analysis. POPL. 195–207. ACM (1996)

[10] Cortesi, A., Filé, G., Giacobazzi, R., Palamidessi, C., Ranzato, F.: Complementation in abstract interpretation. ACM TOPLAS 19(1), 7–47 (1997)

[11] Cousot, P.: Méthodes itératives de construction et d'approximation de points fixes d'opérateurs monotones sur un treillis, analyse sémantique de programmes. Thèse d'État ès sciences mathématiques, Université Joseph Fourier, Grenoble, France (21 Mar. 1978)

[12] Cousot, P., Cousot, R.: Static verification of dynamic type properties of variables. Research Report R.R. 25, Laboratoire IMAG, Université Joseph Fourier, Grenoble, France (Nov. 1975)

[13] Cousot, P., Cousot, R.: Static determination of dynamic properties of programs. Proc. Secont Int. Symp. on Programming. 106–130. Dunod, Paris, (1976)

[14] Cousot, P., Cousot, R.: Constructive versions of Tarski's fixed point theorems. Pacific J. of Math. 82(1), 43–57 (1979)

[15] Cousot, P., Cousot, R.: Induction principles for proving invariance properties of programs. *In* Tools & Notions for Program Construction: an Advanced Course. 75–119. Cambridge University Press, (Aug 1982)

[16] Cousot, P.: Semantic foundations of program analysis. *In* Program Flow Analysis: Theory and Applications, chap. 10, pp. 303–342. Prentice-Hall, (1981)

[17] Cousot, P.: Methods and logics for proving programs. *In* Handbook of Theoretical Computer Science, Volume B: Formal Models and Sematics (B), pp. 841–994. Elsevier (North-Holland) (1990)

[18] Cousot, P.: Verification by abstract interpretation. *In* Verification: Theory and Practice. LNCS 2772, 243–268. Springer (2003)

[19] Cousot, P., Cousot, R.: Vérification statique de la cohérence dynamique des programmes. Rapport du contrat IRIA SESORI No 75-035, Laboratoire IMAG, Université Joseph Fourier, Grenoble, France (23 Sep 1975), 125 p.

[20] Cousot, P., Cousot, R.: Abstract interpretation: A unified lattice model for static analysis of programs by construction or approximation of fixpoints. POPL. 238–252. ACM (1977)

[21] Cousot, P., Cousot, R.: Systematic design of program analysis frameworks. POPL. 269–282. ACM (1979)

[22] Cousot, P., Cousot, R.: Comparing the Galois connection and widening/narrowing approaches to abstract interpretation. PLILP. LNCS 631, pp. 269–295. Springer (1992)

[23] Cousot, P., Cousot, R.: Galois connection based abstract interpretations for strictness analysis. *In* Formal Methods in Programming and Their Applications. LNCS 735, 98–127. Springer (1993)

[24] Cousot, P., Cousot, R.: Formal language, grammar and set-constraint-based program analysis by abstract interpretation. FPCA. 170–181. ACM (1995)

[25] Cousot, P., Cousot, R.: Grammar semantics, analysis and parsing by abstract interpretation. TCS 412(44), 6135–6192 (2011)

[26] Cousot, P., Cousot, R.: An abstract interpretation framework for termination. POPL. 245–258. ACM (2012)

[27] Cousot, P., Cousot, R.: A Galois connection calculus for abstract interpretation. POPL. pp. 3–4. ACM (2014)

[28] Cousot, P., Cousot, R., Feret, J., Mauborgne, L., Miné, A., Rival, X.: Why does Astrée scale up? Formal Methods in System Design 35(3), 229–264 (2009)

[29] Cousot, P., Cousot, R., Mauborgne, L.: Theories, solvers and static analysis by abstract interpretation. J. ACM 59(6), 31 (2012)

[30] Cousot, P., Halbwachs, N.: Automatic discovery of linear restraints among variables of a program. POPL. 84–96. ACM (1978)

[31] Craig, W.: Three uses of the Herbrand-Gentzen theorem in relating model theory and proof theory. Journal of Symbolic Logic 22(3), 269–285 (1957)

[32] Dijkstra, E.W.: Heuristics for a calculational proof. Inf. Process. Lett. 53(3), 141–143 (1995)

[33] Dijkstra, E.W., Scholten, C.S.: Predicate calculus and program semantics. Texts and monographs in computer science, Springer (1990)

[34] Dillig, I., Dillig, T., Li, B., McMillan, K.L.: Inductive invariant generation via abductive inference. OOPSLA. 443–456. ACM (2013)

[35] D'Silva, V., Haller, L., Kroening, D.: Abstract satisfaction. POPL. 139–150. ACM (2014)
[36] Esparza, J., Kiefer, S., Luttenberger, M.: Newtonian program analysis. J. ACM 57(6), 33 (2010)
[37] Feferman, S.: Harmonious logic: Craig's interpolation theorem and its descendants. Synthese 164(3), 341–357 (2008)
[38] Feret, J.: Static analysis of digital filters. ESOP. LNCS 2986, 33–48. Springer (2004)
[39] Flanagan, C., Leino, K.R.M., Lillibridge, M., Nelson, G., Saxe, J.B., Stata, R.: Extended static checking for Java. PLDI. 234–245. ACM (2002)
[40] Flanagan, C., Leino, K.R.M., Lillibridge, M., Nelson, G., Saxe, J.B., Stata, R.: PLDI 2002: Extended static checking for Java. SIGPLAN Notices 48(4S), 22–33 (2013)
[41] Floyd, R.: Assigning meaning to programs. Proc. Symposium in Applied Mathematics, vol. 19, 19–32. Amer. Math. Soc. (1967)
[42] Gange, G., Navas, J.A., Schachte, P., Søndergaard, H., Stuckey, P.J.: Abstract interpretation over non-lattice abstract domains. SAS, LNCS 7935, 6–24. Springer (2013)
[43] Graf, S., Saïdi, H.: Construction of abstract state graphs with PVS. CAV. LNCS 1254, pp. 72–83. Springer (1997)
[44] Gulavani, B.S., Chakraborty, S., Nori, A.V., Rajamani, S.K.: Automatically refining abstract interpretations. TACAS. LNCS 4963, 443–458. Springer (2008)
[45] Halbwachs, N., Henry, J.: When the decreasing sequence fails. SAS. LNCS 7460, 198–213. Springer (2012)
[46] Halbwachs, N., Proy, Y., Roumanoff, P.: Verification of real-time systems using linear relation analysis. FMSD 11(2), 157–185 (1997)
[47] Hoare, C.A.R.: An axiomatic basis for computer programming. C. ACM 12(10), 576–580 (1969)
[48] Hoder, K., Kovács, L., Voronkov, A.: Playing in the grey area of proofs. POPL. 259–272, ACM (2012)
[49] Huang, G.: Constructing Craig interpolation formulas. COCOON. LNCS 959, 181–190. Springer (1995)
[50] Jeannet, B., Schrammel, P., Sankaranarayanan, S.: Abstract acceleration of general linear loops. POPL. 529–540. ACM (2014)
[51] Morris Jr., J.H., Wegbreit, B.: Subgoal induction. C. ACM 20(4), 209–222 (1977)
[52] Lakhdar-Chaouch, L., Jeannet, B., Girault, A.: Widening with thresholds for programs with complex control graphs. ATVA. LNCS 6996, 492–502. Springer (2011)
[53] Leino, K.R.M., Wüstholz, V.: The Dafny integrated development environment. F-IDE. EPTCS, vol. 149, 3–15 (2014)
[54] Logozzo, F., Lahiri, S.K., Fähndrich, M., Blackshear, S.: Verification modulo versions: towards usable verification. PLDI, p. 32. ACM (2014)
[55] McMillan, K.L.: Interpolation and SAT-based model checking. CAV. LNCS 2725, 1–13. Springer (2003)
[56] McMillan, K.L.: Applications of Craig interpolants in model checking. TACAS. LNCS 3440, 1–12. Springer (2005)
[57] McMillan, K.L.: An interpolating theorem prover. TCS 345(1), 101–121 (2005)
[58] McMillan, K.L.: Widening and interpolation. SAS. LNCS 6887, p. 1. Springer (2011), slides `sas2011.cs.technion.ac.il/slides/mcmillan.pptx`
[59] Meshman, Y., Dan, A.M., Vechev, M.T., Yahav, E.: Synthesis of memory fences via refinement propagation. SAS, LNCS 8723, 237–252. Springer (2014)
[60] Metcalfe, G., Montagna, F., Tsinakis, C.: Amalgamation and interpolation in ordered algebras. J. of Algebra 402, 21–82 (2014)
[61] Mycroft, A.: The theory and practice of transforming call-by-need into call-by-value. *In* Symp. on Programming. LNCS 83, 269–281. Springer (1980)
[62] Naur, P.: Proofs of algorithms by general snapshots. BIT 6, 310–316 (1966)
[63] Rival, X., Mauborgne, L.: The trace partitioning abstract domain. TOPLAS 29(5) (2007)
[64] Scott, D.S.: Continuous lattices. Toposes, Algebraic Geometry and Logic. LNM 274. Springer (1972)
[65] Scott, D., Strachey, C.: Towards a mathematical semantics for computer languages. Technical Report PRG-6, Oxford University Computer Laboratory (Aug 1971)
[66] Tarski, A.: A lattice theoretical fixpoint theorem and its applications. Pacific J. of Math. 5, 285–310 (1955)
[67] Thakur, A.V., Elder, M., Reps, T.W.: Bilateral algorithms for symbolic abstraction. SAS. LNCS 7460, 111–128. Springer (2012)
[68] Venet, A.: Abstract cofibered domains: Application to the alias analysis of untyped programs. SAS. LNCS 1145, 366–382. Springer (1996)

Appendix

Proof of Lem. 1

Assume the $\preceq$-increasing transfinite sequence $\langle X^\delta,\ \delta \in \mathbb{O}\rangle$ is not ultimately stationary. Then $\forall \delta \in \mathbb{O} : \exists \delta' \in \mathbb{O} : \delta' > \delta \wedge X^\delta \prec X^{\delta'}$. By skolemization, define $N \in \mathbb{O} \to \mathbb{O}$ such that $\delta' = N(\delta)$ so $\forall \delta \in \mathbb{O} : N(\delta) > \delta$. It follows that $\langle X^{N(\delta)},\ \delta \in \mathbb{O}\rangle$ is $\prec$-strictly increasing transfinite sequence of elements of $\mathcal{P}$. The subset $\mathcal{P}' \triangleq \{X^{N(\delta)} \mid \delta \in \mathbb{O}\}$ of $\mathcal{P}$ is a poset $\langle \mathcal{P}', \preceq\rangle$. Let $\mu(\mathcal{P}') \in \mathbb{O}$ be the smallest ordinal whose cardinality is strictly greater than the cardinality of the set $\mathcal{P}'$. Because $\langle X^{N(\delta)},\ \delta \in \mathbb{O}\rangle$ is strictly increasing no two elements can be equal so its cardinality is greater that or equal to $\mu(\mathcal{P}')$. But all elements of $\langle X^{N(\delta)},\ \delta \in \mathbb{O}\rangle$ belong to $\mathcal{P}'$ so its cardinality is less than or equal to that of $\mathcal{P}'$. This is a contradiction since the cardinality of $\mu(\mathcal{P}')$ is strictly greater than the cardinality of the set $\mathcal{P}'$. By *reductio ad absurdum*, $\exists \delta \in \mathbb{O} : \forall \delta' \geqslant \delta : X^\delta \not\prec X^{\delta'}$. By the increasing chain hypothesis $X^\delta \preceq X^{\delta'}$ so $X^\delta = X^{\delta'}$, proving that $\langle X^\delta,\ \delta \in \mathbb{O}\rangle$ is ultimately stationary. □

Proof of Lem. 4

(a) $X^0 \triangleq D$ so $\langle X^\delta,\ \delta \leqslant 0\rangle$ is a trivial $\subseteq$-increasing chain. For successor ordinals $\beta + 1$, $\langle X^\delta,\ \delta \leqslant \beta\rangle$ is a $\subseteq$-increasing chain by induction hypothesis. Then $X^{\delta+1} \triangleq F(X^\delta)$ so $X^\delta \subseteq X^{\delta+1}$ since F is extensive so $\langle X^\delta,\ \delta \leqslant \beta + 1\rangle$ is a $\subseteq$-increasing chain. For limit ordinals λ, the sequence $\langle X^\delta, \delta < \lambda\rangle$ is a $\subseteq$-increasing chain by induction hypothesis. The iterates are assumed to be upper bounded so X^λ is such that $\forall \delta < \lambda : X^\delta \subseteq X^\lambda$. Then $\langle X^\delta,\ \delta \leqslant \lambda\rangle$ is a $\subseteq$-increasing chain. By transfinite induction, $\langle X^\delta,\ \delta \in \mathbb{O}\rangle$ is a transfinite increasing chain which, by Lem. **1**, is ultimately stationary at rank ϵ. Then $X^\epsilon = X^{\epsilon+1} = f(X^\epsilon)$ is a fixpoint of F $\subseteq$-greater than or equal to $X^0 = D$.

(b) We have $X^0 \triangleq D \subseteq F(D) \triangleq X^1$. If by induction hypothesis $X^\delta \subseteq X^{\delta+1}$ then $X^{\delta+1} \triangleq F(X^\delta) \subseteq F(X^{\delta+1}) \triangleq X^{\delta+2}$ since F is increasing. If λ is a limit ordinal then $\forall \delta < \lambda : X^\delta \subseteq X^\lambda$ by **Def. 2** of the upper bounded iterates, proving that $\langle X^\delta,\ \delta \in \mathbb{O}\rangle$ is an increasing chain. The restriction of F to this increasing chain is extensive so by **Lem. 4** (a), it has a fixpoint $D = X^0 \subseteq X^\epsilon = F(X^\epsilon)$ where ϵ is the smallest ordinal with that property, proving that F has a fixpoint $\subseteq$-greater than of equal to D.

Assume that the iterates are least upper bounded. Let $Y \in \mathcal{D}$ be any fixpoint of F such that $X^0 = D \subseteq Y$. If $X^\delta \subseteq Y$ then $X^{\delta+1} \triangleq F(X^\delta) \subseteq F(Y) = Y$ since $F \in \mathcal{D} \mapsto \mathcal{D}$ is increasing. For a limit ordinal λ, the induction hypothesis $X^\beta \subseteq Y$ for all $\beta < \lambda$ implies $X^\lambda \triangleq \bigcup_{\beta<\lambda} X^\beta \subseteq Y$. By transfinite induction $\forall \delta \in \mathbb{O} : D \subseteq X^\delta \subseteq Y$ so in particular $D \subseteq X^\epsilon \subseteq Y$ proving that $X^\epsilon = \mathbf{lfp}^{\subseteq}_D F$.

(c) By def. iterates and hypothesis $X^0 \triangleq D \subseteq Y$. If, by induction hypothesis, $X^\delta \subseteq Y$ then $X^{\delta+1} \triangleq F(X^\delta) \subseteq F(Y) \subseteq Y$ since F is increasing. If λ is a limit ordinal and $X^\delta \subseteq Y$ for all $\delta < \lambda$ then $X^\lambda \triangleq \bigcup_{\delta<\lambda} X^\delta \subseteq Y$ by def. lub. By transfinite induction $\forall \delta \in \mathbb{O} : X^\delta \subseteq Y$ so in particular $\mathbf{lfp}^{\subseteq}_D F = X^\epsilon \subseteq Y$. □

Proof of Th. 10

(a) By **Hyp. 9** (a) on the widening and definition of the transfinite iterates, we have $\gamma(\overline{X}^\delta) \subseteq \gamma(\overline{X}^\delta \nabla \overline{F}(\overline{X}^\delta)) \triangleq \gamma(\overline{X}^{\delta+1})$ for successor ordinals $\delta + 1$ and by **Hyp. 9** (b), $\forall \beta < \lambda : \gamma(\beta) \subseteq \gamma(\bigvee_{\beta'<\lambda} \overline{X}^{\beta'}) \triangleq \gamma(\overline{X}^\lambda)$ for all limit ordinals λ so that $\langle \gamma(\overline{X}^\delta),\ \delta \in \mathbb{O}\rangle$ is increasing. By lemma 1, it is ultimately stationary with limit $\gamma(\overline{X}^\varepsilon)$ such that $\gamma(\overline{X}^\varepsilon) = \gamma(\overline{X}^{\varepsilon+1}) = \gamma(\overline{X}^\varepsilon \nabla \overline{F}(\overline{X}^\varepsilon))$.

(b) By hypothesis $X^0 = D \subseteq \gamma(\overline{X}^0)$. By induction hypothesis, assume that $X^\delta \subseteq \gamma(\overline{X}^\delta)$. It follows by definition of the concrete iterates, induction hypothesis and F increasing, semi-commutation hypothesis, **Hyp. 9** (a), definition of the abstract iterates, and transitivity that $X^{\delta+1} \triangleq F(X^\delta) \subseteq F(\gamma(\overline{X}^\delta)) \subseteq \gamma(\overline{F}(\overline{X}^\delta)) \subseteq \gamma(\overline{X}^\delta \nabla \overline{F}(\overline{X}^\delta)) \triangleq \gamma(\overline{X}^{\delta+1})$. Moreover, if λ is a limit ordinal

and $\forall \beta < \lambda : X^\beta \subseteq \gamma(\overline{X}^\beta)$ by induction hypothesis then by **Hyp. 9** (b), definition of the abstract iterates, and transitivity $X^\beta \subseteq \gamma(\mathop{\nabla}_{\beta<\lambda} \overline{X}^\beta) \triangleq \gamma(\overline{X}^\lambda)$ proving that $X^\lambda \triangleq \bigcup_{\beta<\lambda} X^\beta \subseteq \gamma(\overline{X}^\lambda)$ by def. lub $\bigcup$ assumed to exist and definition of the concrete iterates. By transitivity and transfinite induction, we conclude that $\forall \delta \in \mathbb{O} : X^\delta \subseteq \gamma(\overline{X}^\delta)$.

Let $\upsilon = \max(\epsilon, \varepsilon)$. We have $\upsilon \geqslant \epsilon$ and $\upsilon \geqslant \varepsilon$ so $\mathbf{lfp}^{\subseteq}_{X^0} F = X^\epsilon = X^\upsilon \subseteq \gamma(\overline{X}^\upsilon) = \gamma(\overline{X}^\varepsilon)$.

(c) By **Lem. 4** (c), if $F(\gamma(\overline{X}^\delta)) \subseteq \gamma(\overline{X}^\delta)$ then $\mathbf{lfp}^{\subseteq}_D F \subseteq \gamma(\overline{X}^\delta)$.

(d) If ∇ is terminating at rank $n \in \mathbb{N}$ then $\overline{X}^{n+1} = \overline{X}^n \nabla \overline{F}(\overline{X}^n) = \overline{X}^n$ so by semi-commutation and **Hyp. 9** (a), $F(\gamma(\overline{X}^n)) \subseteq \gamma(\overline{F}(\overline{X}^n)) \subseteq \gamma(\overline{X}^n \nabla \overline{F}(\overline{X}^n)) = \gamma(\overline{X}^n)$ proving, by (c), that $\mathbf{lfp}^{\subseteq}_D F \subseteq \gamma(\overline{X}^n)$.

(e) If ∇ satisfies **Hyp. 9** (a′) and is terminating at rank $n \in \mathbb{N}$ then $\overline{F}(\overline{X}^n) \sqsubseteq \overline{X}^n \nabla \overline{F}(\overline{X}^n) = \overline{X}^n$ so $\gamma(\overline{F}(\overline{X}^n)) \subseteq \gamma(\overline{X}^n)$ since γ is increasing. This implies $F(\gamma(\overline{X}^n)) \subseteq \gamma(\overline{X}^n)$ by the semi-commutation condition hence $\mathbf{lfp}^{\subseteq}_D F \subseteq \gamma(\overline{X}^n)$ by (c). □

Proof of Lem. 19

A narrowing satisfies **Hyp. 14** (a) $\forall P, Q \in \overline{\mathcal{D}} : (\gamma(Q) \subseteq \gamma(P)) \implies (\gamma(Q) \subseteq \gamma(P \mathbin{\underline{\Delta}} Q) \subseteq \gamma(P))$ while a dual-narrowing satisfies the order dual of **Hyp. 14** (a) which is $\forall P, Q \in \overline{\mathcal{D}} : (\gamma(Q) \supseteq \gamma(P)) \implies (\gamma(Q) \supseteq \gamma(P \mathbin{\overline{\Delta}} Q) \supseteq \gamma(P))$ or equivalently $\forall P, Q \in \overline{\mathcal{D}} : (\gamma(P) \subseteq \gamma(Q)) \implies (\gamma(P) \subseteq \gamma(P \mathbin{\overline{\Delta}} Q) \subseteq \gamma(Q))$, which by renaming P into Q and inversely is $\forall P, Q \in \overline{\mathcal{D}} : (\gamma(Q) \subseteq \gamma(P)) \implies (\gamma(Q) \subseteq \gamma(Q \mathbin{\overline{\Delta}} P) \subseteq \gamma(P))$, which is identical to **Hyp. 14** (a) by letting $P \mathbin{\underline{\Delta}} Q \triangleq Q \mathbin{\overline{\Delta}} P$. By duality, the inverse of a dual-narrowing is a narrowing. □

Proof of Th. 22

By hypothesis, $Y^0 = D \subseteq \gamma(\overline{Y}^0)$. Assume by induction hypothesis that $Y^\delta \subseteq \gamma(\overline{Y}^\delta)$. By def. of the concrete iterates, F is increasing, semi-commutativity, $\overline{F}$ reductive on the iterates, and γ increasing $Y^{\delta+1} \triangleq F(Y^\delta) \subseteq F(\gamma(\overline{Y}^\delta)) \subseteq \gamma(\overline{F}(\overline{Y}^\delta)) \subseteq \gamma(\overline{Y}^\delta))$. By def. of the abstract iterates and **Hyp. 14** (a) (or **Hyp. 14** (a′) which implies **Hyp. 14** (a) since γ is increasing), it follows that $Y^{\delta+1} \subseteq \gamma(\overline{F}(\overline{Y}^\delta)) \subseteq \gamma(\overline{Y}^\delta \mathbin{\underline{\Delta}} \overline{F}(\overline{Y}^\delta)) \triangleq \gamma(\overline{Y}^{\delta+1}) \subseteq \gamma(\overline{Y}^\delta)$. If λ is a limit ordinal and $\forall \delta < \lambda : Y^\delta \subseteq \gamma(\overline{Y}^\delta)$ then, by the dual of **Def. 3** of the greatest lower bound concrete iterates $Y^\lambda = \bigcap_{\delta<\lambda} Y^\delta$ and def. of glbs, $\forall \delta < \lambda : Y^\lambda \subseteq \gamma(\overline{Y}^\delta)$. By **Hyp. 14** (b) where $P = Y^\lambda$ and $Y = \{\overline{Y}^\beta \mid \beta < \lambda\}$, it follows that $\forall \delta < \lambda : Y^\lambda \subseteq \gamma(\mathop{\underline{\Delta}}_{\beta<\lambda} \overline{Y}^\beta) \triangleq \gamma(\overline{Y}^\lambda) \subseteq \gamma(\overline{Y}^\delta)$. By transfinite induction, we conclude that $\langle \gamma(\overline{Y}^\delta), \delta \in \mathbb{O} \rangle$ is decreasing and $\forall \delta \in \mathbb{O} : Y^\delta \subseteq \gamma(\overline{Y}^\delta)$.

So by the dual of **Lem. 4** (b), these concrete iterates $\langle \gamma(\overline{Y}^\delta), \delta \in \mathbb{O} \rangle$ are decreasing, ultimately stationary, and converge to Y^ϵ such that $\forall \delta \in \mathbb{O} : \mathbf{gfp}^{\subseteq}_D F = Y^\epsilon \subseteq \gamma(\overline{Y}^\epsilon) \subseteq \gamma(\overline{Y}^\delta)$. □

Proof of Lem. 23

We have $\overline{F}(\overline{Y}^0) \sqsubseteq \overline{Y}^0$ by hypothesis so $\overline{F}(\overline{Y}^0) \sqsubseteq \overline{Y}^1 \triangleq \overline{Y}^0 \mathbin{\underline{\Delta}} \overline{F}(\overline{Y}^0) \sqsubseteq \overline{Y}^0$ and so $\overline{F}(\overline{Y}^1) \sqsubseteq \overline{F}(\overline{Y}^0)$ which implies $\overline{F}(\overline{Y}^1) \sqsubseteq \overline{Y}^1 \sqsubseteq \overline{Y}^0$. If $\overline{F}(\overline{Y}^{\delta+1}) \sqsubseteq \overline{Y}^{\delta+1} \sqsubseteq \overline{Y}^\delta$ by induction hypothesis then $\overline{F}(\overline{Y}^{\delta+1}) \sqsubseteq \overline{Y}^{\delta+2} \triangleq \overline{Y}^{\delta+1} \mathbin{\underline{\Delta}} \overline{F}(\overline{Y}^{\delta+1}) \sqsubseteq \overline{Y}^{\delta+1}$ and so $\overline{F}(\overline{Y}^{\delta+2}) \sqsubseteq \overline{F}(\overline{Y}^{\delta+1})$ which implies $\overline{F}(\overline{Y}^{\delta+2}) \sqsubseteq \overline{Y}^{\delta+2} \sqsubseteq \overline{Y}^{\delta+1}$. If λ is a limit ordinal and $\forall \delta < \lambda : \overline{F}(\overline{Y}^\delta) \sqsubseteq \overline{Y}^\delta$ by induction hypothesis, then $\mathop{\underline{\Delta}}_{\beta<\lambda} \overline{Y}_\beta \sqsubseteq \overline{Y}_\delta$ implies $\overline{F}(\mathop{\underline{\Delta}}_{\beta<\lambda} \overline{Y}_\beta) \sqsubseteq \overline{F}(\overline{Y}_\delta) \sqsubseteq \overline{Y}_\delta$ and so $\overline{F}(\mathop{\underline{\Delta}}_{\beta<\lambda} \overline{Y}_\beta) \sqsubseteq \mathop{\underline{\Delta}}_{\beta<\lambda} \overline{Y}_\beta \sqsubseteq \overline{Y}_\delta$ that is $\overline{F}(\overline{Y}_\lambda) \sqsubseteq \overline{Y}_\lambda \sqsubseteq \overline{Y}_\delta$. By transfinite induction, $\overline{F}$ is reductive on the abstract iterates which are decreasing. □

Proof of Th. 24

(a) • We have $Z^0 \triangleq D \subseteq \gamma(\overline{Z}^0) \subseteq \gamma(\overline{S})$ which implies that $(Z^0 \subseteq \gamma(\overline{S})) \implies (Z^0 \subseteq \gamma(\overline{Z}^0) \subseteq \gamma(\overline{S}))$.

• Assume by induction hypothesis that $(Z^\delta \subseteq \gamma(\overline{S})) \implies (Z^\delta \subseteq \gamma(\overline{Z}^\delta) \subseteq \gamma(\overline{S}))$. If $Z^{\delta+1} \subseteq \gamma(\overline{S})$ then $Z^\delta \subseteq \gamma(\overline{S})$ since $\langle Z^\delta,\ \delta \in \mathbb{O}\rangle$ is increasing and so $Z^\delta \subseteq \gamma(\overline{Z}^\delta) \subseteq \gamma(\overline{S})$ by induction hypothesis. By definition of the concrete iterates, F increasing, and semi-commutation $Z^{\delta+1} \triangleq F(Z^\delta) \subseteq F(\gamma(\overline{Z}^\delta)) \subseteq \gamma(\overline{F}(\overline{Z}^\delta))$.
– If $\gamma(\overline{F}(\overline{Z}^\delta)) \subseteq \gamma(\overline{S})$ then $\overline{Z}^{\delta+1} \triangleq \overline{F}(\overline{Z}^\delta)\ \widetilde{\Delta}\ \overline{S}$ so $\gamma(\overline{F}(\overline{Z}^\delta)) \subseteq \gamma(\overline{S})$ implies, by the order dual of hypothesis **Hyp. 14** (a), that $\gamma(\overline{F}(\overline{Z}^\delta)) \subseteq \gamma(\overline{Z}^{\delta+1}) \subseteq \gamma(\overline{S})$. By transitivity $Z^{\delta+1} \subseteq \gamma(\overline{Z}^{\delta+1}) \subseteq \gamma(\overline{S})$.
– Otherwise $\gamma(\overline{F}(\overline{Z}^\delta)) \not\subseteq \gamma(\overline{S})$ and then $\overline{Z}^{\delta+1} \triangleq \overline{S}$ so that $Z^{\delta+1} \subseteq \gamma(\overline{S})$ implies $Z^{\delta+1} \subseteq \gamma(\overline{Z}^{\delta+1}) \subseteq \gamma(\overline{S})$ by reflexivity.
– In both cases, $(Z^{\delta+1} \subseteq \gamma(\overline{S})) \implies (Z^{\delta+1} \subseteq \gamma(\overline{Z}^{\delta+1}) \subseteq \gamma(\overline{S}))$.

• Assume that λ is a limit ordinal and by induction hypothesis $\forall \delta < \lambda : (Z^\delta \subseteq \gamma(\overline{S})) \implies (Z^\delta \subseteq \gamma(\overline{Z}^\delta) \subseteq \gamma(\overline{S}))$. If $Z^\lambda \subseteq \gamma(\overline{S})$ then $\forall \delta < \lambda : Z^\delta \subseteq \gamma(\overline{S})$ since $\langle Z^\delta,\ \delta \in \mathbb{O}\rangle$ is increasing and so, by induction hypothesis, $\forall \delta < \lambda : Z^\delta \subseteq \gamma(\overline{Z}^\delta) \subseteq \gamma(\overline{S})$. By the order dual of hypothesis **Hyp. 14** (b) (where $P = \gamma(\overline{S})$, $Q = \overline{Z}^\delta$, and $\mathfrak{X} = \{\overline{Z}^\beta \mid \beta < \lambda\}$) and def. of the abstract iterates, we have $\forall \delta < \lambda : \gamma(\overline{Z}^\delta) \subseteq \gamma(\underset{\beta<\lambda}{\Delta} \overline{Z}^\beta) = \gamma(\overline{Z}^\lambda) \subseteq \gamma(\overline{S})$. By transitivity $\forall \delta < \lambda : Z^\delta \subseteq \gamma(\underset{\beta<\lambda}{\Delta} \overline{Z}^\beta) = \gamma(\overline{Z}^\lambda) \subseteq \gamma(\overline{S})$ so that, by def. of the concrete iterates and the lub (assumed to exist in the concrete $\mathfrak{D}$), $Z^\lambda \triangleq \bigcup_{\beta<\lambda} Z^\delta \subseteq \gamma(\overline{Z}^\lambda) \subseteq \gamma(\overline{S})$.

• By transfinite induction, we conclude that $\forall \delta \in \mathbb{O} : (Z^\delta \subseteq \gamma(\overline{S})) \implies (Z^\delta \subseteq \gamma(\overline{Z}^\delta) \subseteq \gamma(\overline{S}))$.

(b) If $\delta \in \mathbb{O}$ and $\gamma(\overline{F}(\overline{Z}^\delta)) \subseteq \gamma(\overline{Z}^\delta)$ then $F(\gamma(\overline{Z}^\delta)) \subseteq \gamma(\overline{F}(\overline{Z}^\delta)) \subseteq \gamma(\overline{Z}^\delta)$ by semi-commutativity so that by **Lem. 4** (c), we have $\mathbf{lfp}^{\subseteq}_D F = Z^\delta \subseteq \gamma(\overline{Z}^\delta) \subseteq \gamma(\overline{S})$. □

Proof of Th. 34

By transfinite induction, $\langle X^\delta,\ \delta \in \mathbb{O}\rangle$ is an increasing chain since $D = X^0 \subseteq F(X^0)$ for the basis, F is increasing for successor ordinals, and def. and existence of lubs for limit ordinals. By **Lem. 4** (b), $\langle X^\delta,\ \delta \in \mathbb{O}\rangle$ is ultimately stationary at $X^\epsilon = \mathbf{lfp}^{\subseteq}_D F$.

(A) Let $\langle \overline{X}^k,\ k \in \mathbb{N}\rangle$ be the iterates from $\overline{X}^0 \triangleq \overline{D}$ defined in **Alg. 33** (A). By def. of the iterates and **Hyp. 9** (a), their concretization is an increasing chain since $\gamma(\overline{X}^k) \subseteq \gamma(\overline{X}^k \nabla \overline{F}(\overline{X}^k)) \triangleq \gamma(\overline{X}^{k+1})$. By **Def. 30**, they converge in finitely many steps to $\overline{X}^n$ at some finite rank $n \in \mathbb{N}$ and so can be extended to a transfinite sequence $\langle \gamma(\overline{X}^\delta),\ \delta \in \mathbb{O}\rangle$ with $\overline{X}^\delta = \overline{X}^n$ for all $\delta \geqslant n$. This increasing sequence is the one considered in **Th. 10** for the trivial widening $\nabla\mathfrak{X}$ taking the lub of the $\mathfrak{X} = \{\gamma(\overline{X}^\delta) \mid \delta < \lambda \wedge \lambda \text{ is a limit ordinal}\}$ which therefore satisfies **Hyp. 9** (b) for these sets since $\gamma(\nabla\mathfrak{X}) = \gamma(\text{lub } \mathfrak{X}) = \gamma(\overline{X}^n)$. By hypothesis $D \subseteq \gamma(\overline{D}) = \gamma(\overline{X}^0)$, **Hyp. 9** (a), semi-commutation hypothesis, γ increasing on the pre-ordered abstract domain, and **Th. 10**, we conclude that $\gamma(\overline{F}(\overline{X}^n)) \subseteq \gamma(\overline{X}^n)$, $F(\gamma(\overline{X}^n)) \subseteq \gamma(\overline{X}^n)$, and $\mathbf{lfp}^{\subseteq}_D F = X^\epsilon \subseteq \gamma(\overline{X}^n)$. We have $\gamma(\overline{D}) \subseteq \gamma(\overline{X}^n)$ and $F(\gamma(\overline{X}^n)) \subseteq \gamma(\overline{X}^n)$ so, by hypothesis on $\overline{D}$, $\gamma(\overline{D}) \subseteq \gamma(\overline{F}(\overline{X}^n)) \subseteq \gamma(\overline{X}^n)$.

(B) We apply **Th. 22** with iterates $\langle X'^\delta,\ \delta \in \mathbb{O}\rangle$ starting from $X'^0 = X^\epsilon$ so that $\forall \delta \in \mathbb{O} : X'^\delta = X^\epsilon = \mathbf{gfp}^{\subseteq}_{X^\epsilon} F = \mathbf{lfp}^{\subseteq}_D F$ since $\mathbf{lfp}^{\subseteq}_D F$ is obviously the greatest fixpoint less than or equal to itself.

We have $\gamma(\overline{D}) \subseteq \gamma(\overline{F}(\overline{Y}^0)) \subseteq \gamma(\overline{Y}^0)$ since $\overline{Y}^0 = \overline{X}^n$. Assume, by recurrence hypothesis, that $\gamma(\overline{D}) \subseteq \gamma(\overline{F}(\overline{Y}^k)) \subseteq \gamma(\overline{Y}^k)$. Then by def. of the iterates $\langle \overline{Y}^k,\ k \in \mathbb{N}\rangle$ of (B) and **Hyp. 14** (a) on $\overline{\Delta}$, we have $\gamma(\overline{D}) \subseteq \gamma(\overline{F}(\overline{Y}^k)) \subseteq \gamma(\overline{F}(\overline{Y}^k) \,\overline{\Delta}\, \overline{Y}^k) \triangleq \gamma(\overline{Y}^{k+1}) \subseteq \gamma(\overline{Y}^k)$. By hypothesis on $\overline{F}$ and $\overline{\Delta}$, we have $\gamma(\overline{F}(\overline{Y^k} \,\overline{\Delta}\, \overline{F}(\overline{Y^k}))) \subseteq \gamma(\overline{Y^k} \,\overline{\Delta}\, \overline{F}(\overline{Y^k}))$. It follows that $\overline{F}(\overline{Y}^{k+1}) \sqsubseteq \overline{Y}^{k+1}$. By recurrence, $\langle \gamma(\overline{Y}^k), k \in \mathbb{N}\rangle$ is a decreasing chain such that $\forall k \in \mathbb{N} : \gamma(\overline{D}) \subseteq \gamma(\overline{F}(\overline{Y}^k)) \subseteq \gamma(\overline{Y}^k)$ and therefore $\overline{F}$ is reductive on the chain $\langle \overline{Y}^k,\ k \in \mathbb{N}\rangle$ as defined in **Th. 22**.

By **Def. 30** of a terminating narrowing, the iterates $\langle \overline{Y}^k,\ k \in \mathbb{N}\rangle$ are stationary at rank $m \in \mathbb{N}$ such that $\gamma(\overline{D}) \subseteq \gamma(\overline{Y}^m) \subseteq \gamma(\overline{X}^n)$. It can be extended to $\langle \overline{Y}^\delta,\ \delta \in \mathbb{O}\rangle$ by $\forall \delta \geqslant m : \overline{Y}^\delta \triangleq \overline{Y}^m$.

It is therefore of the form considered in **Th. 22**, by taking $D = \gamma(Y^0) = \gamma(\overline{X}^n)$, $\Delta \in \wp(\overline{\mathfrak{D}}) \mapsto \overline{\Delta}$ to be the glb on that decreasing chain which satisfies **Hyp. 14** (b). $\overline{F}$ is obviously reductive on that extended transfinite chain $\langle \overline{Y}^\delta,\ \delta \in \mathbb{O}\rangle$. By **Th. 22**, we conclude that $X^\epsilon = \mathbf{gfp}^{\subseteq}_{X^\epsilon} F = \mathbf{lfp}^{\subseteq}_D F \subseteq \gamma(\overline{Y}^m) \subseteq \gamma(\overline{X}^n)$. Moreover $\gamma(\overline{D}) \subseteq \gamma(\overline{F}(\overline{Y}^m)) \subseteq \gamma(\overline{Y}^m) \subseteq \gamma(\overline{X}^n)$.

(C) By hypothesis that the dual-narrowing is terminating, the iterates $\langle \overline{Z}^k,\ k \in \mathbb{N}\rangle$ of (C) are stationary at rank $p \in \mathbb{N}$. By extending to the sequence $\langle \overline{Z}^\delta,\ \delta \in \mathbb{O}\rangle$ by $\forall \delta \geqslant p : \overline{Z}^\delta \triangleq \overline{Z}^p$ we have transfinite iterates of the form considered in **Th. 24** where $\overline{S} \triangleq \overline{Y}^m$ such that $\gamma(\overline{D}) \subseteq \gamma(\overline{F}(\overline{S})) \subseteq \gamma(\overline{S}) \subseteq \gamma(\overline{X}^n)$ and $\widetilde{\Delta}$ is defined as the lub of the iterates so satisfies the order dual of **Hyp. 14** (b) for $\mathfrak{X} \triangleq \{\overline{X}^\delta \mid \delta < \lambda \wedge \lambda \in \mathbb{O} \text{ is a limit ordinal}\}$ with $\widetilde{\Delta}\,\mathfrak{X} = \overline{Z}^p$.

In case $F(\gamma(\overline{Z}^p)) \subseteq \gamma(\overline{Z}^p)$[17] and $\overline{Z}^p \not\equiv \overline{Y}^m$, (C) has improved the solution (B). By **Th. 24** (b), it follows that $\mathbf{lfp}^{\subseteq}_D F \subseteq \gamma(\overline{Z}^p) \subseteq \gamma(\overline{Y}^m) \subseteq \gamma(\overline{X}^n)$.

Otherwise, (C) has not improved the solution (B), so we choose $\overline{Z}^p \triangleq \overline{Y}^m$ in which case $\mathbf{lfp}^{\subseteq}_D F \subseteq \gamma(\overline{Z}^p) = \gamma(\overline{Y}^m) \subseteq \gamma(\overline{X}^n)$.

We have proved that the individual phases (A), (B), and (C) do individually terminate with $\mathbf{lfp}^{\subseteq}_D F \subseteq \gamma(\overline{Z}^p) \subseteq \gamma(\overline{Y}^m) \subseteq \gamma(\overline{X}^n)$. When iterating from (B) with initial value $\overline{X'}^n = \overline{Z}^p \,\overline{\Delta}'\, \overline{Y}^m$ such that, by **Hyp. 14** (a) for $\overline{\Delta}'$, we have $\gamma(\overline{Z}^p) \subseteq \gamma(\overline{X'}^n) \subseteq \gamma(\overline{Y}^m)$, we end up with new $\gamma(\overline{Z'}^p) \subseteq \gamma(\overline{Y'}^m) \subseteq \gamma(\overline{X'}^n) \subseteq \gamma(\overline{Y}^m) \subseteq \gamma(\overline{X}^n)$. These iterations terminate since $\overline{\Delta}'$ is terminating.

Note that it is always possible to ensure definite improvement over $\overline{Z}^p$ by defining $X \overline{\Delta}' Y = Y$ and bounding the number of iterations.

Given an abstract specification $\overline{S} \in \overline{\mathfrak{D}}$, if $\overline{Z}^p \sqsubseteq \overline{S}$, we have $\gamma(\overline{Z}^p) \subseteq \gamma(\overline{S})$ which implies $\mathbf{lfp}^{\subseteq}_D F \subseteq \gamma(\overline{S})$ by transitivity. □

Proof of Th. 36

Let $\mathfrak{D}' \triangleq \{P \in \mathfrak{D} \mid P \subseteq \gamma(\overline{S})\}$. Since $\mathfrak{D}' \subseteq \mathfrak{D}$ and $\langle \mathfrak{D}, \subseteq\rangle$ is a poset, $\langle \mathfrak{D}', \subseteq\rangle$ is also a poset, with the same lub (since the lub in $\mathfrak{D}$ of elements of $\mathfrak{D}'$ bounded by $\gamma(\overline{S})$ is itself bounded by $\gamma(\overline{S})$ hence in $\mathfrak{D}'$).

Let us define $F' \in \mathfrak{D}' \mapsto \mathfrak{D}'$ by $F'(X) \triangleq \langle\!| F(X) \subseteq \gamma(\overline{S}) \;?\; F(X) \;:\; \gamma(\overline{S}) |\!\rangle$. It is increasing since $X \subseteq Y$ implies $F(X) \subseteq F(Y)$ by hypothesis. If $F(Y) \subseteq \gamma(\overline{S})$ then $F(X) \subseteq \gamma(\overline{S})$ and therefore $F'(X) = F(X) \subseteq F(Y) = F'(Y)$. Otherwise $F(Y) \not\subseteq \gamma(\overline{S})$ in which case $F'(X) \subseteq \gamma(\overline{S}) = F'(Y)$.

$D \in \mathfrak{D}'$ since $D \subseteq \gamma(\overline{S})$ by hypothesis. If $F(D) \subseteq \gamma(\overline{S})$ then $D \subseteq F(D) = F'(D)$ Otherwise $F(D) \not\subseteq \gamma(\overline{S})$ in which case $D \subseteq \gamma(\overline{S}) = F'(D)$. It follows that $D \subseteq F'(D)$.

As shown by the proof of **Th. 34**, the concrete iterates $\langle X^\delta,\ \delta \in \mathbb{O}\rangle$ for F are an increasing chain, well-defined in $\mathfrak{D}$. Let $\langle X'^\delta,\ \delta \in \mathbb{O}\rangle$ be the iterates for F'. Either $\forall \delta \in \mathbb{O} : X^\delta \subseteq \gamma(\overline{S})$ and $\langle X^\delta,\ \delta \in \mathbb{O}\rangle = \langle X'^\delta,\ \delta \in \mathbb{O}\rangle$. Or $\exists \delta \in \mathbb{O} : X^\delta \not\subseteq \gamma(\overline{S})$ and then $\langle X^\beta,\ \beta < \delta\rangle = \langle X'^\beta,\ \beta < \delta\rangle$ and

[17] which is implied by $\overline{F}(\overline{Z}^p) \sqsubseteq \overline{Z}^p$ since γ is increasing and by semi-commutation.

$\forall \beta \geqslant \delta : X'^{\beta} = \gamma(\overline{S})$. In both cases, $\langle X'^{\delta}, \delta \in \mathbb{O} \rangle$ is a well-defined increasing chain since lubs do exist.

Define the abstract domain $\overline{\mathcal{D}}' \triangleq \{\overline{P} \in \overline{\mathcal{D}} \mid \gamma(\overline{P}) \subseteq \gamma(\overline{S})\}$. It is a pre-order $\langle \overline{\mathcal{D}}', \sqsubseteq \rangle$ since $\langle \overline{\mathcal{D}}, \sqsubseteq \rangle$ is a pre-order and $\overline{\mathcal{D}}' \subseteq \overline{\mathcal{D}}$.

The concretization $\gamma \in \overline{\mathcal{D}}' \mapsto \mathcal{D}$ is the restriction of $\gamma \in \overline{\mathcal{D}} \mapsto \mathcal{D}$ to $\overline{\mathcal{D}}'$ hence is increasing.

Define the abstract transformer $\overline{F}'(\overline{X}) \triangleq (\!| \gamma(\overline{F}(\overline{X})) \subseteq \gamma(\overline{S}) \ ? \ \overline{F}(\overline{X}) \ : \ \overline{S} |\!)$ so that $\overline{F}' \in \overline{\mathcal{D}}' \mapsto \overline{\mathcal{D}}'$. By hypothesis, $F \circ \gamma \dot{\subseteq} \gamma \circ \overline{F}$ on $\overline{\mathcal{D}}$. We must show that $F' \circ \gamma \dot{\subseteq} \gamma \circ \overline{F}'$ on $\overline{\mathcal{D}}'$. Let $\overline{X} \in \overline{\mathcal{D}}'$ so that $\gamma(\overline{X}) \subseteq \gamma(\overline{S})$.

- If $\gamma(\overline{F}(\overline{X})) \subseteq \gamma(\overline{S})$ then $\overline{F}'(\overline{X}) = \overline{F}(\overline{X})$ by def. $\overline{F}'$. By semi-commutativity, $F(\gamma(\overline{X})) \subseteq \gamma(\overline{F}(\overline{X})) \subseteq \gamma(\overline{S})$ so that by def. of F', $F'(\gamma(\overline{X})) = F(\gamma(\overline{X}))$. It follows that $F'(\gamma(\overline{X})) = F \circ \gamma(\overline{X}) \subseteq \gamma \circ \overline{F}(\overline{X}) = \gamma \circ \overline{F}'(\overline{X})$.
- Otherwise $\gamma(\overline{F}(\overline{X})) \not\subseteq \gamma(\overline{S})$ and then $\overline{F}'(\overline{X}) = \overline{S}$.
  - If $F(\gamma(\overline{X})) \subseteq \gamma(\overline{S})$ then $F'(\gamma(\overline{X})) = F(\gamma(\overline{X})) \subseteq \gamma(\overline{S}) = \gamma(\overline{F}'(\overline{X}))$.
  - Otherwise $F(\gamma(\overline{X})) \not\subseteq \gamma(\overline{S})$ and then $F' \circ \gamma(\overline{X}) = \gamma(\overline{S}) = \gamma(\overline{F}'(\overline{X}))$.

We conclude that the abstract transformer $\overline{F}' \in \overline{\mathcal{D}}' \mapsto \overline{\mathcal{D}}'$ satisfies the pointwise semi-commutation condition $F' \circ \gamma \dot{\subseteq} \gamma \circ \overline{F}'$.

We have $\overline{D} \in \overline{\mathcal{D}}'$ so $\overline{D} \in \overline{\mathcal{D}}$ which, by hypothesis of **Th. 34**, satisfies $D \subseteq \gamma(\overline{D})$ and $\forall \overline{X} \in \overline{\mathcal{D}} : (\gamma(\overline{D}) \subseteq \gamma(\overline{X}) \wedge \gamma(\overline{F}(\overline{X})) \subseteq \gamma(\overline{X})) \implies (\gamma(\overline{D}) \subseteq \gamma(\overline{F}(\overline{X})))$. Let $\overline{X}' \in \overline{\mathcal{D}}'$ such that $\gamma(\overline{D}) \subseteq \gamma(\overline{X}') \wedge \gamma(\overline{F}'(\overline{X}')) \subseteq \gamma(\overline{X}')$.

- If $\gamma(\overline{F}(\overline{X}')) \subseteq \gamma(\overline{S})$ then $\overline{F}'(\overline{X}') = \overline{F}(\overline{X}')$ so $\gamma(\overline{D}) \subseteq \gamma(\overline{X}') \wedge \gamma(\overline{F}'(\overline{X}')) \subseteq \gamma(\overline{X}')$ implies $\gamma(\overline{D}) \subseteq \gamma(\overline{X}') \wedge \gamma(\overline{F}(\overline{X}')) \subseteq \gamma(\overline{X}')$ hence, by hypothesis, $\gamma(\overline{D}) \subseteq \gamma(\overline{F}(\overline{X}'))$ which implies $D \subseteq \gamma(\overline{D}) \subseteq \gamma(\overline{F}'(\overline{X}'))$.
- Otherwise $\gamma(\overline{F}(\overline{X}')) \not\subseteq \gamma(\overline{S})$ and then $\overline{F}'(\overline{X}') = \overline{S}$ so that $D \subseteq \gamma(\overline{D}) \subseteq \gamma(\overline{S})$ implies $D \subseteq \gamma(\overline{D}) \subseteq \gamma(\overline{F}'(\overline{X}'))$.

In both cases, we conclude that $\forall \overline{X}' \in \overline{\mathcal{D}}' : (\gamma(\overline{D}) \subseteq \gamma(\overline{X}') \wedge \gamma(\overline{F}'(\overline{X}')) \subseteq \gamma(\overline{X}')) \implies (\gamma(\overline{D}) \subseteq \gamma(\overline{F}'(\overline{X}')))$.

Let $\nabla \in \overline{\mathcal{D}} \times \overline{\mathcal{D}} \mapsto \overline{\mathcal{D}}$ be a terminating widening satisfying **Hyp. 9** (a). The bounded widening ∇' also satisfies **Hyp. 9** (a) for all $\overline{P}, \overline{Q} \in \overline{\mathcal{D}}'$ since either $\overline{P} \nabla \overline{Q} \in \overline{\mathcal{D}}'$ and then $\gamma(\overline{P}) \subseteq \gamma(\overline{P} \nabla \overline{Q}) = \gamma(\overline{P} \nabla' \overline{Q}) \wedge \gamma(\overline{Q}) \subseteq \gamma(\overline{P} \nabla \overline{Q}) = \gamma(\overline{P} \nabla' \overline{Q})$ else $\overline{P} \nabla' \overline{Q} = \overline{S}$ which implies $\gamma(\overline{P}) \subseteq \gamma(\overline{S}) = \gamma(\overline{P} \nabla' \overline{Q}) \wedge \gamma(\overline{Q}) \subseteq \gamma(\overline{S}) = \gamma(\overline{P} \nabla' \overline{Q})$ since $\overline{P}, \overline{Q} \in \overline{\mathcal{D}}'$. ∇' is terminating since otherwise a counter-example in $\overline{\mathcal{D}}'$ for ∇' would also be a counter-example in $\overline{\mathcal{D}}$ for ∇ since $\overline{\mathcal{D}}' \subseteq \overline{\mathcal{D}}$ and ∇ and ∇' coincide on $\overline{\mathcal{D}}'$. So $\nabla' \in \overline{\mathcal{D}}' \times \overline{\mathcal{D}}' \mapsto \overline{\mathcal{D}}'$ restricted to $\overline{\mathcal{D}}'$ is a terminating widening satisfying **Hyp. 9** (a).

Let $\Delta \in \overline{\mathcal{D}} \times \overline{\mathcal{D}} \mapsto \overline{\mathcal{D}}$ be a terminating narrowing satisfying **Hyp. 14** (a) and $\forall \overline{X} \in \overline{\mathcal{D}} : (\gamma(\overline{F}(\overline{X})) \subseteq \gamma(\overline{X})) \implies (\gamma(\overline{F}(\overline{X} \Delta \overline{F}(\overline{X}))) \subseteq \gamma(\overline{X} \Delta \overline{F}(\overline{X})))$. Let us prove that the same narrowing $\Delta \in \overline{\mathcal{D}}' \times \overline{\mathcal{D}}' \mapsto \overline{\mathcal{D}}'$ satisfies **Hyp. 14** (a). If $P, Q \in \overline{\mathcal{D}}'$ then $P, Q \in \overline{\mathcal{D}}$ and $\gamma(P) \subseteq \gamma(\overline{S})$ so that $\gamma(Q) \subseteq \gamma(P)$ implies $\gamma(Q) \subseteq \gamma(P \Delta Q) \subseteq \gamma(P) \subseteq \gamma(\overline{S})$ so $P \Delta Q \in \overline{\mathcal{D}}'$ and satisfies **Hyp. 14** (a).

We must also show that $\forall \overline{X}' \in \overline{\mathcal{D}}' : (\gamma(\overline{F}'(\overline{X}')) \subseteq \gamma(\overline{X}')) \implies (\gamma(\overline{F}'(\overline{X}' \Delta \overline{F}'(\overline{X}'))) \subseteq \gamma(\overline{X}' \Delta \overline{F}'(\overline{X}')))$.

Assume that $\overline{X}' \in \overline{\mathcal{D}}'$ (so $\gamma(\overline{X}') \subseteq \gamma(\overline{S})$) and $\gamma(\overline{F}'(\overline{X}')) \subseteq \gamma(\overline{X}')$ so that $\gamma(\overline{F}'(\overline{X}')) \subseteq \gamma(\overline{X}') \subseteq \gamma(\overline{S})$ by hypothesis.

- If $\gamma(\overline{F}(\overline{X}')) \subseteq \gamma(\overline{X}')$ then $\overline{F}'(\overline{X}') = \overline{F}(\overline{X}')$ so the hypothesis $\gamma(\overline{F}'(\overline{X}')) \subseteq \gamma(\overline{X}')$ implies $\gamma(\overline{F}(\overline{X}')) \subseteq \gamma(\overline{X}')$ in which case we have $\gamma(\overline{F}(\overline{X}' \Delta \overline{F}(\overline{X}'))) \subseteq \gamma(\overline{X}' \Delta \overline{F}(\overline{X}'))$ which implies $\gamma(\overline{F}(\overline{X}' \Delta \overline{F}'(\overline{X}'))) \subseteq \gamma(\overline{X}' \Delta \overline{F}'(\overline{X}'))$. By **Hyp. 14** (a), $\gamma(\overline{X}' \Delta \overline{F}'(\overline{X}')) \subseteq \gamma(\overline{F}'(\overline{X}'))$ and by hypothesis $\gamma(\overline{F}'(\overline{X}')) \subseteq \gamma(\overline{S})$ so $\gamma(\overline{F}(\overline{X}' \Delta \overline{F}(\overline{X}'))) \subseteq \gamma(\overline{S})$ by transitivity, proving that

$\overline{F}'(\overline{X}' \mathbin{\Delta} \overline{F}'(\overline{X}')) = \overline{F}(\overline{X}' \mathbin{\Delta} \overline{F}'(\overline{X}'))$ so that we conclude that $\gamma(\overline{F}'(\overline{X}' \mathbin{\Delta} \overline{F}'(\overline{X}'))) \subseteq \gamma(\overline{X}' \mathbin{\Delta} \overline{F}'(\overline{X}'))$ as required.

– Otherwise $\gamma(\overline{F}'(\overline{X}')) \not\subseteq \gamma(\overline{X}')$ and therefore $\overline{F}(\overline{X}') = \overline{S}$. By hypothesis $\gamma(\overline{F}'(\overline{X}')) \subseteq \gamma(\overline{X}') \subseteq \gamma(\overline{S})$ and antisymmetry, it follows that $\gamma(\overline{X}') = \gamma(\overline{S})$. This implies that $\gamma(\overline{X}' \mathbin{\Delta} \overline{F}'(\overline{X}')) = \gamma(\overline{S} \mathbin{\Delta} \overline{S}) = \gamma(\overline{S})$ by **Hyp. 14** (a). By hypothesis $\gamma(\overline{F}(\overline{S})) \not\subseteq \gamma(\overline{S})$ so $\overline{F}'(\overline{S}) = \overline{S}$. We conclude that $\gamma\overline{F}'(\overline{X}' \mathbin{\widetilde{\Delta}} \overline{F}'(\overline{X}'))) = \gamma\overline{F}'(\overline{S})) = \gamma\overline{S}) = \gamma\overline{X}' \mathbin{\widetilde{\Delta}} \overline{F}'(\overline{X}'))$.

In both cases we conclude that $\forall \overline{X}' \in \overline{\mathcal{D}}' : (\gamma(\overline{F}'(\overline{X}')) \subseteq \gamma(\overline{X}')) \implies (\gamma(\overline{F}'(\overline{X}' \mathbin{\widetilde{\Delta}} \overline{F}'(\overline{X}'))) \subseteq \gamma(\overline{X}' \mathbin{\widetilde{\Delta}} \overline{F}'(\overline{X}')))$.

If $\widetilde{\Delta} \in \overline{\mathcal{D}} \times \overline{\mathcal{D}} \mapsto \overline{\mathcal{D}}$ is a terminating dual-narrowing satisfying the order dual of **Hyp. 14** (a) then the same dual-narrowing $\widetilde{\Delta} \in \overline{\mathcal{D}}' \times \overline{\mathcal{D}}' \mapsto \overline{\mathcal{D}}'$ is a terminating dual-narrowing satisfying the order dual of **Hyp. 14** (a).

We have shown that all hypotheses of **Th. 34** do hold for $\mathcal{D}'$, F', $\overline{\mathcal{D}}'$, $\overline{F}'$, ∇', Δ, and $\widetilde{\Delta}$. Let $\overline{Z}'^{p}$ be the result of applying **Alg. 33** to $\overline{F}'$ and $\overline{D}$ on $\langle \overline{\mathcal{D}}', \sqsubseteq \rangle$. By **Th. 34**, $\mathbf{lfp}_D^{\subseteq} F' \subseteq \gamma(\overline{Z}'^{p})$ in $\mathcal{D}'$. So $\gamma(\overline{Z}'^{p}) \subseteq \gamma(\overline{S})$.

Then $\overline{F}(\overline{Z}'^{p}) \sqsubseteq \overline{Z}'^{p}$ implies $\gamma \circ \overline{F}(\overline{Z}'^{p}) \subseteq \gamma(\overline{Z}'^{p})$ since γ is increasing so $F(\gamma(\overline{Z}'^{p})) \subseteq \gamma(\overline{Z}'^{p})$ by semi-commutation and transitivity. It follows that $\mathbf{lfp}_D^{\subseteq} F \subseteq \gamma(\overline{Z}'^{p})$ by **Lem. 4** (c).

We conclude that $\mathbf{lfp}_D^{\subseteq} F \subseteq \gamma(\overline{Z}'^{p}) \subseteq \gamma(\overline{S})$. □