Principles of Abstract Interpretation

MIT press

Ch. **34**, Fixpoint approximation by extrapolation and interpolation

Patrick Cousot

pcousot.github.io

PrAbsInt@gmail.com github.com/PrAbsInt/

These slides are available at
http://github.com/PrAbsInt/slides/slides-34--fixpoint-approximation-by-extrapolation-and-interpolation-PrAbsInt.pdf

Chapter 34

Ch. **34**, Fixpoint approximation by extrapolation and interpolation

Upward iteration convergence acceleration by overapproximating extrapolation with widening, formally

Iterations

Definition (34.1, iterations) The iterates of $f \in L \to L$ from $a \in L$ on a poset $\langle L, \sqsubseteq, \sqcup\rangle$ are $\langle f^n, n \in \mathbb{N}_\omega\rangle$ such that

1. $f^0 \triangleq a$
2. $f^{n+1} \triangleq f(f^n)$, $n \in \mathbb{N}$
3. $f^\omega \triangleq \bigsqcup_{n<\omega} f^n$

(where the least upper bound $\sqcup$ in $f^\omega \triangleq \bigsqcup\{f^n \mid n < \omega\}$ is assumed to exist in L *e.g.* for cpos when the iterates are increasing).

Convergence

Definition (Definition 34.2, convergence) The iterates $\langle f^n,\ n \in \mathbb{N}_\omega \rangle$ of $f \in L \rightarrow L$ from $a \in L$ *converge* to the limit $\ell \in L$ at $\epsilon \in \mathbb{N}_\omega$ if and only if $\forall n \geqslant \epsilon \mathrel{.} f^n = \ell$ (the iterates are then said to be *ultimately stationary* at ϵ).

© P. Cousot, NYU, CIMS, CS

Widening

- In case the iterates do not converge, we can enforce or speed up convergence using a widening in an abstract domain.

Definition (34.3) Let $\langle L, \sqsubseteq \rangle$ and $\langle \overline{L}, \overline{\sqsubseteq} \rangle$ be concrete and abstract posets with increasing concretization $\gamma \in \overline{L} \xrightarrow{\nearrow} L$.

A *limit widening* $\boldsymbol{\nabla} \in \wp(\overline{L}) \to \overline{L}$ is *sound* if and only if it is an abstract upper bound *i.e.* $\forall X \in \wp(\overline{L}) \mathrel{.} \forall \overline{x} \in X \mathrel{.} \overline{x} \mathrel{\overline{\sqsubseteq}} \boldsymbol{\nabla} X$.

A *successor widening* $\nabla \in \overline{L} \times \overline{L} \to \overline{L}$ is sound if and only if $\forall \overline{x}, \overline{y} \in \overline{L} \mathrel{.} \overline{x} \mathrel{\overline{\sqsubseteq}} \overline{x} \mathbin{\nabla} \overline{y} \wedge \overline{y} \mathrel{\overline{\sqsubseteq}} \overline{x} \mathbin{\nabla} \overline{y}$.

 © P. Cousot, NYU, CIMS, CS

Iteration with widening

Definition (34.4) The *upward iterates* of $\overline{f} \in \overline{L} \rightarrow \overline{L}$ from $a \in \overline{L}$ with widening ∇ on a poset $\langle \overline{L}, \sqsubseteq \rangle$ are $\langle \hat{f}^n, n \in \mathbb{N}_\omega \rangle$ such that

1. $\hat{f}^0 \triangleq a$,
2. $\hat{f}^{n+1} \triangleq \llbracket \overline{f}(\hat{f}^n) \sqsubseteq \hat{f}^n \mathrel{?} \hat{f}^n \mathrel{⁏} \hat{f}^n \nabla \overline{f}(\hat{f}^n) \rrbracket$ when $n \in \mathbb{N}$,
3. $\hat{f}^\omega \triangleq \displaystyle\mathop{\nabla}_{n<\omega} \hat{f}^n$.

- The successor widening $\hat{f}^{\,n} \nabla \overline{f}(\hat{f}^{\,n})$ depends on the previous iterate $\hat{f}^{\,n}$ to extrapolate the next iterate $\overline{f}(\hat{f}^{\,n})$.

- More generally, it might be made more precise by depending of all previous iterates as in $\langle \hat{f}^{\,\delta}, \delta \leqslant n \rangle \nabla \overline{f}(\hat{f}^{\,n})$.

© P. Cousot, NYU, CIMS, CS

Terminating widening

Definition (34.5, terminating widening) A successor widening $\nabla \in \overline{L} \times \overline{L} \rightarrow \overline{L}$ on a poset $\langle \overline{L}, \overline{\sqsubseteq} \rangle$ is *terminating* if and only if for any increasing sequence $\langle x^n, n \in \mathbb{N} \rangle$ of elements of $\overline{L}$ and any arbitrary sequence $\langle y^n, n \in \mathbb{N} \rangle$ and such that $\forall n \in \mathbb{N} \,.\, x^{n+1} = x^n \nabla y^n$, the sequence $\langle x^n, n \in \mathbb{N} \rangle$ is converging *i.e.* $\exists \epsilon \in \mathbb{N} \,.\, x^{\epsilon+1} = x^{\epsilon}$.

- In this definition $\langle x^n, n \in \mathbb{N} \rangle$ stands for the increasing iterates $\langle \hat{f}^{\,n}, n \in \mathbb{N} \rangle$ of $\overline{f}$
- $\langle y^n, n \in \mathbb{N} \rangle$ stands for their image $\langle \overline{f}(\hat{f}^{\,n}), n \in \mathbb{N} \rangle$ by $\overline{f}$, which is not assumed to be increasing, so that $\langle y^n, n \in \mathbb{N} \rangle$ can be an arbitrary overapproximation of $\langle x^n, n \in \mathbb{N} \rangle$.
- Of course the hypotheses of the definition can be restricted to the case of an increasing chain.

© P. Cousot, NYU, CIMS, CS

Upward iteration with (terminating) widening

Theorem (34.6) Let $f \in L \xrightarrow{uc} L$ be an upper continuous function on a cpo $\langle L, \sqsubseteq, \bot\rangle$ with infimum $\bot$. Let $\langle f^n, n \in \mathbb{N}_\omega\rangle$ be the iterates of f from $\bot$.

Let $\langle \overline{L}, \overline{\sqsubseteq}\rangle$ be an abstract domain with increasing concretization $\gamma \in \overline{L} \xrightarrow{\nearrow} L$.

Let $\overline{f} \in \overline{L} \to \overline{L}$ be such that $f \circ \gamma \mathrel{\dot{\sqsubseteq}} \gamma \circ \overline{f}$ (semi-commutation).

Let ∇ be a widening on $\overline{L}$.

Then

- The iterates $\langle \hat{f}^n, n \in \mathbb{N}_\omega\rangle$ of $\overline{f}$ from any $a \in \overline{L}$ with widening ∇ are increasing.
- There exists $\Delta \in \mathbb{N}_\omega$ such that $\mathsf{lfp}^{\sqsubseteq} f \sqsubseteq \gamma(\hat{f}^{\Delta})$.
- if ∇ is terminating then $\Delta \in \mathbb{N}$ and $\overline{f}(\hat{f}^{\Delta}) \mathrel{\overline{\sqsubseteq}} \hat{f}^{\Delta}$. □

Iteration with widening

- Note that $\langle \overline{L}, \overline{\sqsubseteq} \rangle$ is not assumed to have lubs (even for increasing chains) and
- $\overline{f}$ is not assumed to be increasing.

Proof of Theorem 34.6 Let $\langle f^n, n \in \mathbb{N}_\omega\rangle$ be the iterates of f from $\bot$ in Definition 34.1 and $\langle \hat{f}^n, n \in \mathbb{N}_\omega\rangle$ be the iterates of $\overline{f}$ from $\overline{a} \in \overline{L}$ with widening ∇ in Definition 34.4.

(1) The abstract iterates overapproximate the concrete iterates.

- $f^{\,0} = \bot \sqsubseteq \gamma(\overline{a}) = \gamma(\hat{f}^0)$ by def. of the concrete and abstract iterates and $\bot$ is the infimum of L;
- For a positive natural $n+1$, assume, by induction hypothesis, that $f^{\,n} \sqsubseteq \gamma(\hat{f}^n)$.
  - If $\overline{f}(\hat{f}^n) \mathrel{\overline{\sqsubseteq}} \hat{f}^n$ then, $f^{\,n+1} = f(f^{\,n}) \sqsubseteq f(\gamma(\hat{f}^n)) \sqsubseteq \gamma(\overline{f}(\hat{f}^n)) \sqsubseteq \gamma(\hat{f}^n) = \gamma(\hat{f}^{\,n+1})$ by def. of the iterates, f is upper continuous hence increasing, induction hypothesis, $\overline{f}$ and f semi-commute, $\overline{f}(\hat{f}^n) \mathrel{\overline{\sqsubseteq}} \hat{f}^n$, and γ is increasing.
  - Otherwise, $\overline{f}(\hat{f}^n) \mathrel{\overline{\not\sqsubseteq}} \hat{f}^n$, in which case $f^{\,n+1} = f(f^{\,n}) \sqsubseteq f(\gamma(\hat{f}^n)) \sqsubseteq \gamma(\overline{f}(\hat{f}^n)) \sqsubseteq \gamma(\hat{f}^n \mathbin{\nabla} \overline{f}(\hat{f}^n)) = \gamma(\hat{f}^{\,n+1})$ by def. of the iterates, f is upper continuous hence increasing, induction hypothesis, $\overline{f}$ and f semi-commute, soundness of the successor widening, and γ is increasing.

- For the limit ω, assume by induction hypothesis, that $\forall n < \omega \,.\, f^{\,n} \sqsubseteq \gamma(\hat{f}^n)$. By soundness of the limit widening and Definition 34.3, $f^{\,n} \sqsubseteq \gamma(\hat{f}^n) \sqsubseteq \gamma(\mathop{\nabla}\limits_{n<\omega} \hat{f}^n)$. By def. of the iterates and of the least upper bound $\bigsqcup\{f^{\,n} \mid n < \omega\}$ which is assumed to exist in L, $f^{\,\omega} = \bigsqcup_{n<\omega} f^{\,n} \sqsubseteq \gamma(\mathop{\nabla}\limits_{n<\omega} \hat{f}^n) = \gamma(\hat{f}^\omega)$.

By induction, we conclude that $\forall n \in \mathbb{N}_\omega \,.\, f^{\,n} \sqsubseteq \gamma(\hat{f}^n)$.

(2) The abstract iterates are increasing.

The abstract iterates $\langle \hat{f}^n, n \in \mathbb{N}_\omega \rangle$ form an increasing chain.

- For positive naturals, either $\overline{f}(\hat{f}^n) \mathrel{\overline{\sqsubseteq}} \hat{f}^n$ and the following iterates are stationary or else $\hat{f}^{n+1} = \hat{f}^n \mathbin{\nabla} \overline{f}(\hat{f}^n)$ so $\hat{f}^n \mathrel{\overline{\sqsubseteq}} \hat{f}^{n+1}$ by soundness of the widening in Definition 34.3.
- For the limit, $\hat{f}^\omega \triangleq \mathop{\nabla}\limits_{n<\omega} \hat{f}^n \mathrel{\overline{\sqsupseteq}} \hat{f}^n$ for all $n < \omega$.

© P. Cousot, NYU, CIMS, CS

(3) Fixpoint overapproximation.

- By Scott iterative fixpoint Theorem 15.26, $\langle f^n, n \in \mathbb{N}_\omega\rangle$ is an increasing chain which has a limit $f^\omega = \bigsqcup_{n\in\mathbb{N}_\omega} f^n = \mathsf{lfp}^{\sqsubseteq} f$.

- By (1), $f^\omega \sqsubseteq \gamma(\hat{f}^\omega)$

- Proving $\exists\Delta \in \mathbb{N}_\omega \;.\; \mathsf{lfp}^{\sqsubseteq} f \sqsubseteq \gamma(\hat{f}^\Delta)$ for $\Delta = \omega$.

© P. Cousot, NYU, CIMS, CS

(4) Terminating widenings enforce convergence.

- By (2), the abstract iterates $\langle \hat{f}^{\,n}, n \in \mathbb{N} \rangle$ form an increasing chain.
- Assume, by reductio ad absurdum that $\forall n \in \mathbb{N} \,.\, \overline{f}(\hat{f}^{\,n}) \mathrel{\overline{\not\sqsubseteq}} \hat{f}^{\,n}$.
- Let $x^n = \hat{f}^{\,n}$ and $y^n = \overline{f}(\hat{f}^{\,n})$ in Definition 34.5 so that $\langle x^n, n \in \mathbb{N} \rangle$ is increasing and $\forall n \in \mathbb{N} \,.\, x^{n+1} = x^n \mathbin{\nabla} y^n$.
- By Definition 34.5, $\exists \epsilon \in \mathbb{N} \,.\, x^{\epsilon+1} = x^{\epsilon}$ *i.e.* $\hat{f}^{\,\epsilon+1} = \hat{f}^{\,\epsilon}$.
- By Definition 34.4.2 of the iterates either $\overline{f}(\hat{f}^{\,\epsilon}) \mathrel{\overline{\sqsubseteq}} \hat{f}^{\,\epsilon}$ or else $\hat{f}^{\,\epsilon+1} = \hat{f}^{\,\epsilon} \mathbin{\nabla} \overline{f}(\hat{f}^{\,\epsilon})$.
- By Definition 34.3, $\overline{f}(\hat{f}^{\,\epsilon}) \mathrel{\overline{\sqsubseteq}} \hat{f}^{\,\epsilon} \mathbin{\nabla} \overline{f}(\hat{f}^{\,\epsilon}) = \hat{f}^{\,\epsilon+1} = \hat{f}^{\,\epsilon}$ proving that, in both cases, $\overline{f}(\hat{f}^{\,\epsilon}) \mathrel{\overline{\sqsubseteq}} \hat{f}^{\,\epsilon}$.

(5) The limit of the converging abstract iterates overapproximates all concrete iterates.

The proof is by induction.

- $f^0 = \bot \sqsubseteq \gamma(\hat{f}^{\,\epsilon})$ by def. iterates and infimum;
- If $f^n \sqsubseteq \gamma(\hat{f}^{\,\epsilon})$ by induction hypothesis, then $f^{n+1} = f(f^n) \sqsubseteq f(\gamma(\hat{f}^{\,\epsilon})) \sqsubseteq \gamma(\overline{f}(\hat{f}^{\,\epsilon})) = \gamma(\hat{f}^{\,\epsilon})$;
- For the limit ω, for all $n < \omega$, $f^n \sqsubseteq \gamma(\hat{f}^{\,\epsilon})$ then $f^\omega = \bigsqcup_{n\in\mathbb{N}_\omega} f^n = \mathsf{lfp}^{\sqsubseteq} f \sqsubseteq \gamma(\hat{f}^{\,\epsilon})$ by existence hypothesis and def. of the lub $\bigsqcup$ in L. It follows that we can choose $\Delta = \epsilon$. $\square$

Note that the proof of Theorem 34.6 remains valid when weakening the hypothesis $\forall \overline{x}, \overline{y} \in \overline{L} \,.\, \overline{y} \mathrel{\overline{\sqsubseteq}} \overline{x} \mathbin{\nabla} \overline{y}$ to $\forall \overline{x}, \overline{y} \in \overline{L} \,.\, \gamma(\overline{y}) \subseteq \gamma(\overline{x} \mathbin{\nabla} \overline{y})$.

Increasing widenings can-
not enforce termination

Widenings are not increasing in their first parameter

- The widening for intervals is not increasing in its first parameter.

- For example $[0,0] \mathbin{\nabla^i} [0,1] = [0,\infty]$, $[0,0] \sqsubseteq^i [0,1]$, $[0,1] \mathbin{\nabla^i} [0,1] = [0,1]$, and $[0,\infty] \not\sqsubseteq^i [0,1]$.

- This is a general property of terminating widenings.

Widenings cannot be increasing in their first parameter

Theorem (34.8, Terminating widenings are not increasing) Assume the hypotheses of Theorem 34.6 in an abstract domain $\langle \overline{L}, \overline{\sqsubseteq} \rangle$ where $\overline{f}$ has infinite non-converging increasing iterations $\langle \hat{f}^n, n \in \mathbb{N}_\omega \rangle$[1].

Define $x \mathbin{\nabla'} y \triangleq \llbracket y \mathrel{\overline{\sqsubseteq}} x \mathrel{?} x \mathrel{\S} x \mathbin{\nabla} y \rrbracket$ so that Definition 34.4.2 is $\hat{f}^{n+1} \triangleq \hat{f}^n \mathbin{\nabla'} \overline{f}(\hat{f}^n)$.

Then ∇' is a widening and ∇ cannot enforce convergence if ∇' is $\overline{\sqsubseteq}$-increasing in its first parameter.

[1] Either $\overline{f}$ is increasing and the iterates start from the infimum or it involves a widening and so is extensive by Def. 34.3

Proof ∇' is a widening since
(a) $x \mathrel{\overline{\sqsubseteq}} x \nabla' y$ since either $y \mathrel{\overline{\sqsubseteq}} x = x \nabla' y$ or $x \mathrel{\overline{\sqsubseteq}} x \nabla y = x \nabla' y$ by Definition 34.3.
(b) $y \mathrel{\overline{\sqsubseteq}} x \nabla' y$ since either $y \mathrel{\overline{\sqsubseteq}} x = x \nabla' y$ or $y \mathrel{\overline{\sqsubseteq}} x \nabla y = x \nabla' y$ by Definition 34.3.
Moreover,
(c) $y \mathrel{\overline{\sqsubseteq}} x \Rightarrow x \nabla' y = x$ by def. ∇'. In particular $y \mathrel{\overline{\sqsubseteq}} y$ so $y \nabla' y = y$.

Assume that ∇' is increasing in its first parameter. Then $x \mathrel{\overline{\sqsubseteq}} y$ implies that $y \mathrel{\overline{\sqsubseteq}} x \nabla' y \mathrel{\overline{\sqsubseteq}} y \nabla' y = y$ by (b) and (c) so $x \nabla' y = y$ by antisymmetry.

The contradiction is that Definition 34.4.2 is $\hat{f}^{n+1} \triangleq \hat{f}^{n} \nabla' \overline{f}(\hat{f}^{n}) = \overline{f}(\hat{f}^{n})$ and so if $\overline{f}$ has infinite non-converging iterations *i.e.* such that $\forall \ell \in \mathbb{N} \,.\, \overline{f}(\hat{f}^{\ell}) \mathrel{\overline{\not\sqsubseteq}} \hat{f}^{\ell}$, the widening ∇' yields the same iterates hence ∇ does not enforce convergence. $\square$

Non-increasing abstract iteration transformers

- When considering nested loops, the transformer $\mathscr{F}^{\,\natural}[\![\texttt{while}\,^{\ell}\,\texttt{(B) S}_b]\!]$ in (21.11) of the outer loop does depend on the approximation of the fixpoint semantics of the inner loop
- Because the widening is not increasing, the inner transformer may be non-increasing when using the convergence acceleration 34.6,
- Therefore in Theorem 34.6, the abstract transformer $\overline{f}$ cannot be assumed to be increasing.
- Soundness relies only on the increasingness of the concrete transformer f, which is always the case since, intuitively, more possible interactions with the execution environments yield more possible program executions.

Comparing the precision of static analyzes using widenings

- More precise abstractions may yield less precise analyzes.
- For example, consider the program

$$
\begin{aligned}
\mathtt{P}_5 \quad = \quad & \ell_1 \ \mathtt{x = 1 ;} \\
& \mathtt{while}\ \ell_2\ (\mathtt{tt}) \\
& \quad \ell_3 \ \mathtt{x = 0 ;} \\
& \ell_4
\end{aligned}
$$

- The sign analysis yields $\mathtt{x} \geqslant 0$
- The interval analysis yields $\mathtt{x} \in [-\infty, 1]$.
- This is because of the widening $[1, 1] \mathbin{\nabla^i} [0, 1] = [-\infty, 1]$.
- So the interval abstraction α_i in Section **33.2** is more precise than the sign abstraction in Section **3.12**, but the interval analysis is not always more precise than the sign analysis.

Comparing the precision of static analyzes using widenings

- To ensure that the interval analysis is more precise than the sign analysis we must ensure that the interval widening is more precise than the sign join

- *i.e.* $\forall x, y \in \mathbb{P}^i \,.\, x \mathbin{\nabla^i} y \sqsubseteq^i \alpha_i\Big(\gamma_\pm\Big(\alpha_\pm(\gamma_i(x)) \sqcup_\pm \alpha_\pm(\gamma_i(y))\Big)\Big)$ where $\sqcup_\pm$ is the join of signs defined in Section **3.12**.

- (The interval lattice operations will all be precise than the sign lattice operations by virtue of the Galois connections $\alpha_\pm$ and α_i, but all operations $1^{¤}$, $\ominus^{¤}$, $\ominus^{\underline{¤}_1}$, $\otimes^{\underline{¤}_1}$, $\overline{\otimes}^{\underline{¤}_1}$ must also be more or equality precise).

Terminating widenings can be refined for ever

- The widening can be improved to satisfy this requirement by introducing thresholds $\langle -\infty,\ -1,\ 0,\ 1,\ \infty\rangle$.
- The thresholds T can be any strictly increasing sequence of elements of $\mathbb{Z}$ bounded by $-\infty$ and ∞.
- The widening with thresholds T is then

$$\begin{aligned}\perp^i \nabla^i_T x &\triangleq x \nabla^i_T \perp^i \triangleq x \\ [\ell_1, h_1] \nabla^i_T [\ell_2, h_2] &\triangleq [\llparenthesis\, \ell_2 < \ell_1 \mathrel{?} \max\{t \in T \mid t \leqslant \ell_2\} \mathrel{:} \ell_1 \,\rrparenthesis, \\ &\qquad \llparenthesis\, h_2 > h_1 \mathrel{?} \min\{t \in T \mid t \geqslant h_2\} \mathrel{:} h_1 \,\rrparenthesis]\end{aligned} \tag{34.11}$$

- The previous widening (33.5) was for $\langle -\infty,\ \infty\rangle$.
- By adding more thresholds (and, more generally, more patterns of abstract properties to widen to), the precision of the analysis can be strictly improved in that it will be strictly more precise for at least one program.
- T can be augmented during the analysis (using *e.g*. heuristics to determine "interesting" constants *e.g*. found in declarations).

Delayed widening

- In Theorem 34.6 the iteration with terminating widening applies the same widening at each iteration step.
- More generally, the widening ∇_n^i may depend on the iteration step n.
- For example the widening may become coarser over time n.
- An example is delayed widening of Astrée which is the join $\sqcup$ for the k iterates after entering the loop, or after a new path has been explored in a loop. The further iterates use ∇ to enforce termination.

© P. Cousot, NYU, CIMS, CS

Downward iteration convergence acceleration by overapproximating interpolation with narrowing, formally

Narrowing

Definition (34.14) Let $\langle \overline{L}, \overline{\sqsubseteq} \rangle$ be a poset.
A successor narrowing $\Delta \in \overline{L} \times \overline{L} \to \overline{L}$ is *sound* if and only if $\forall \overline{x}, \overline{y} \in \overline{L} \,.\, (\overline{y} \mathrel{\overline{\sqsubseteq}} \overline{x}) \Rightarrow (\overline{y} \mathrel{\overline{\sqsubseteq}} \overline{x} \,\Delta\, \overline{y} \mathrel{\overline{\sqsubseteq}} \overline{x})$.

Iteration with narrowing

Definition (34.15) The iterates of $\overline{f} \in \overline{L} \to \overline{L}$ from $a \in \overline{L}$ with narrowing Δ on a poset $\langle \overline{L}, \overline{\sqsubseteq} \rangle$ are $\langle \check{f}^{\,n}, n \in \mathbb{N} \rangle$ such that

1. $\check{f}^{\,0} \triangleq a$,
2. $\check{f}^{\,n+1} \triangleq [\![\overline{f}(\check{f}^{\,n}) \mathrel{\overline{\sqsubset}} \check{f}^{\,n} \mathrel{?} \check{f}^{\,n} \mathbin{\Delta} \overline{f}(\check{f}^{\,n}) \mathrel{\text{⨾}} \check{f}^{\,n}]\!]$.

Iteration with narrowing

Theorem (34.16) Let $f \in L \xrightarrow{uc} L$ be an upper continuous function on a cpo $\langle L, \sqsubseteq, \bot\rangle$ with infimum $\bot$.

Let $\langle f^n, n \in \mathbb{N}_\omega\rangle$ be the iterates of f from $\bot$.

Let $\langle \overline{L}, \overline{\sqsubseteq}\rangle$ be an abstract domain with increasing concretization $\gamma \in \overline{L} \xrightarrow{\nearrow} L$.

Let $\overline{f} \in \overline{L} \to \overline{L}$ semi-commute with f *i.e.* $\forall \overline{x} \in \overline{L} \;.\; f(\gamma(\overline{x})) \sqsubseteq \gamma(\overline{f}(\overline{x}))$.

Let Δ be a narrowing on $\overline{L}$.

Then the iterates $\langle \check{f}^n, n \in \mathbb{N}\rangle$ of $\overline{f}$ from any $b \in \overline{L}$ such that $\overline{f}(b) \overline{\sqsubseteq} b$ with narrowing Δ are decreasing and $\forall n \in \mathbb{N} \;.\; \mathsf{lfp}^{\sqsubseteq} f \sqsubseteq \gamma(\check{f}^n)$.

Moreover if $\overline{f}$ is increasing and the downward iteration with narrowing $\langle \check{f}^n, n \in \mathbb{N}\rangle$ converges to the limit $\check{f}^\ell$, then $\check{f}^\ell$ is a fixpoint of $\overline{f}$.

© P. Cousot, NYU, CIMS, CS

Proof

(1) Lemma.

Let us first show that if $\overline{f}(x) \mathrel{\overline{\sqsubseteq}} x$ then $\forall n < \omega \,.\, f^{\,n} \sqsubseteq \gamma(x)$. The proof is by induction.

- We have $f^{\,0} = \bot \sqsubseteq \gamma(x)$ by def. of the iterates and the infimum;
- If $f^{\,n} \sqsubseteq \gamma(x)$ then $f^{\,n+1} = f(f^{\,n}) \sqsubseteq f(\gamma(x)) \sqsubseteq \gamma(\overline{f}(\overline{x})) \sqsubseteq \gamma(x)$ by def. of the iterates, induction hypothesis and γ increasing, $\overline{f}$ and f semi-commute, hypothesis $\overline{f}(x) \mathrel{\overline{\sqsubseteq}} x$ and γ increasing. By transitivity, $f^{\,n+1} \sqsubseteq \gamma(x)$;
- $\forall n < \omega \,.\, f^{\,n} \sqsubseteq \gamma(x)$ by recurrence
- For the limit $\omega \in \mathbb{N}_\omega$, $f^{\,\omega} = \bigsqcup_{n<\omega} f^{\,n} \sqsubseteq \gamma(x)$ by def. of the iterates, existence hypothesis of the lub $\bigsqcup$, smaller than or equal to any upper bound.

By induction, $\overline{f}(x) \mathrel{\overline{\sqsubseteq}} x$ implies $\forall n < \omega \,.\, f^{\,n} \sqsubseteq \gamma(x)$.

© P. Cousot, NYU, CIMS, CS

(2) Concrete iterates overapproximation.

- Let us show that $\forall n, m \in \mathbb{N} \,.\, f^{\,n} \sqsubseteq \gamma(\check{f}^{\,m})$ by recurrence on m.
- For the basis $m = 0$, we have $\overline{f}(b) \mathrel{\overline{\sqsubseteq}} b$ that implies $\forall n \in \mathbb{N} \,.\, f^{\,n} \sqsubseteq \gamma(b) = \gamma(\check{f}^{0})$ by the lemma and Definition 34.15.1 of the abstract iterates;
- Assume by induction hypothesis that $\forall n \in \mathbb{N} \,.\, f^{\,n} \sqsubseteq \gamma(\check{f}^{\,m})$
- By Definition 34.15.2, either $\overline{f}(\check{f}^{\,m}) \mathrel{\overline{\not\sqsubset}} \check{f}^{\,m}$, so, by Definition 34.15.2, $\check{f}^{\,m+1} = \check{f}^{\,m}$ hence $\forall n \in \mathbb{N} \,.\, f^{\,n} \sqsubseteq \gamma(\check{f}^{\,m+1})$ by induction hypothesis.
- Otherwise, $\overline{f}(\check{f}^{\,m}) \mathrel{\overline{\sqsubset}} \check{f}^{\,m}$, in which that $\check{f}^{\,m+1} = \check{f}^{\,m} \mathbin{\Delta} \overline{f}(\check{f}^{\,m})$ with $\overline{f}(\check{f}^{\,m}) \mathrel{\overline{\sqsubseteq}} \check{f}^{\,m+1} \mathrel{\overline{\sqsubseteq}} \check{f}^{\,m}$ by soundness 34.14 of the narrowing Δ.
- Since f and γ are increasing, and $\overline{f}$ and f semi-commute, we have $f(\gamma(\check{f}^{\,m+1})) \sqsubseteq f(\gamma(\check{f}^{\,m})) \sqsubseteq \gamma(\overline{f}(\check{f}^{\,m})) \sqsubseteq \gamma(\check{f}^{\,m+1})$.
- Therefore $\forall n \in \mathbb{N} \,.\, f^{\,n} \sqsubseteq f^{\,n+1} = f(f^{\,n}) \sqsubseteq f(\gamma(\check{f}^{\,m})) \sqsubseteq \gamma(\check{f}^{\,m+1})$.

(3) Concrete fixpoint overapproximation.

- By $\forall n, m \in \mathbb{N} \,.\, f^{\,n} \sqsubseteq \gamma(\check{f}^{\,m})$ and Scott iterative fixpoint Theorem 15.26,

$$\mathsf{lfp}^{\sqsubseteq} f \quad = \quad \bigsqcup_{n \in \mathbb{N}} f^{\,n} \quad \sqsubseteq \quad \gamma(\check{f}^{\,m})$$

  for all $m \in \mathbb{N}$.

© P. Cousot, NYU, CIMS, CS

(4) Decreasing abstract iterates.

By Definition 34.15.2,

- either $\overline{f}(\check{f}^{\,n}) \not\sqsubset \check{f}^{\,n}$ and $\check{f}^{\,n+1} \triangleq \check{f}^{\,n}$
- or $\overline{f}(\check{f}^{\,n}) \sqsubset \check{f}^{\,n}$ and $\check{f}^{\,n+1} \triangleq \check{f}^{\,n} \mathbin{\Delta} \overline{f}(\check{f}^{\,n}) \sqsubseteq \check{f}^{\,n}$ by Definition 34.14.

(5) Fixpoint limit for increasing transformer $\overline{f}$.

- By hypothesis $\overline{f}(b) \sqsubseteq b$ so $\overline{f}(\check{f}^0) \sqsubseteq \check{f}^0$.
- Assume by induction hypothesis that $\overline{f}(\check{f}^n) \sqsubseteq \check{f}^n$.
  - If $\overline{f}(\check{f}^n) \not\sqsubset \check{f}^n$ then $\check{f}^{n+1} = \check{f}^n$ and so $\overline{f}(\check{f}^{n+1}) \sqsubseteq \check{f}^{n+1}$ by induction hypothesis.
  - Otherwise, $\overline{f}(\check{f}^n) \sqsubset \check{f}^n$ so $\check{f}^{n+1} = \check{f}^n \,\Delta\, \overline{f}(\check{f}^n)$ by Definition 34.15 and therefore $\overline{f}(\check{f}^n) \sqsubseteq \check{f}^{n+1} \sqsubseteq \check{f}^n$ by Definition 34.14. Since $\overline{f}$ is assumed to be increasing, $\overline{f}(\check{f}^{n+1}) \sqsubseteq \overline{f}(\check{f}^n)$ and so by transitivity, we conclude that $\overline{f}(\check{f}^{n+1}) \sqsubseteq \check{f}^{n+1}$.
- By recurrence, $\forall n \in \mathbb{N} \,.\, \overline{f}(\check{f}^n) \sqsubseteq \check{f}^n$.
- Assuming the iterates do converge to $\check{f}^\ell$. We have $\overline{f}(\check{f}^\ell) \not\sqsubset \check{f}^\ell$ by Definition 34.15 as well as $\overline{f}(\check{f}^\ell) \sqsubseteq \check{f}^\ell$, as shown above, so that $\overline{f}(\check{f}^\ell) = \check{f}^\ell$. $\square$

© P. Cousot, NYU, CIMS, CS

Remark 34.17: trivial narrowing

- The trivial narrowing $x \mathbin{\Delta} y = y$ satisfies Definition 34.14.
- Then Theorem 34.16 shows that it is sound to stop the iterates at any rank n to artificially enforce convergence.
- (Since this is not in general the limit of the iterates, the solution $\check{f}^{\,n}$ may not be a fixpoint of $\overline{f}$, even if $\overline{f}$ is increasing).

© P. Cousot, NYU, CIMS, CS