Principles of Abstract Interpretation
MIT press

Ch. **18**, Fixpoint abstraction

Patrick Cousot

pcousot.github.io

PrAbsInt@gmail.com   github.com/PrAbsInt/

These slides are available at
http://github.com/PrAbsInt/slides/slides/slides-18--fixpoint-abstraction-PrAbsInt.pdf

Design of a verification/analysis method for a programming language by abstract interpretation

- Define the syntax and operational semantics of the language
- Define program properties and the collecting semantics
- Define an abstraction of properties (preferably by a Galois connection)
- Calculate a sound (and possibly complete) abstract semantics by abstraction of the collecting semantics ← this chapter
- Define an abstract inductive proof method/analysis algorithm

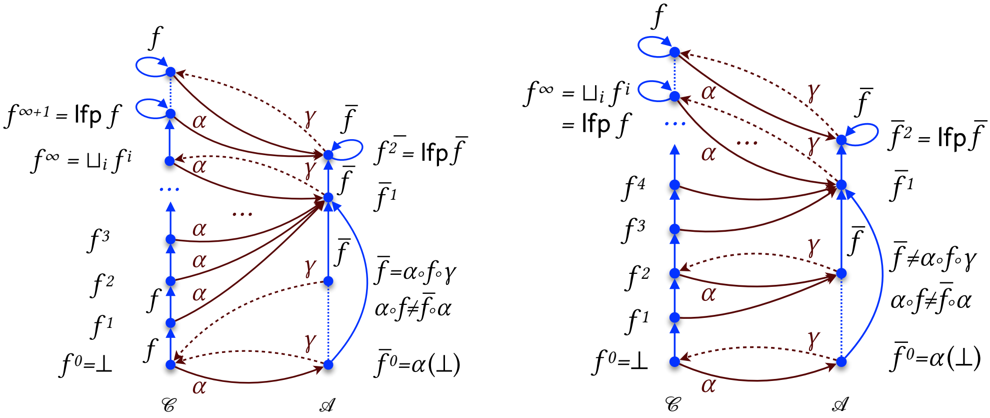
Chapter 18

Ch. **18**, Fixpoint abstraction

Fixpoint abstraction

- C is a concrete domain
- $f \in C \xrightarrow{\nearrow} C$ is an increasing concrete transformer
- $\langle C, \sqsubseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathcal{A}, \preccurlyeq\rangle$ is an abstraction into $\mathcal{A}$
- Problem: abstract $\mathsf{lfp}^{\sqsubseteq} f$
  - first abstract the concrete transformer f into an abstract transformer $\overline{f} \in \mathcal{A} \xrightarrow{\nearrow} \mathcal{A}$
  - then abstract $\alpha(\mathsf{lfp}^{\sqsubseteq} f)$ into $\mathsf{lfp}^{\preccurlyeq} \overline{f}$.
  - This abstraction may be
    - *exact* *i.e.* $\alpha(\mathsf{lfp}^{\sqsubseteq} f) = \mathsf{lfp}^{\preccurlyeq} \overline{f}$
    - or *sound* but imprecise, in which case we get an overapproximation $\alpha(\mathsf{lfp}^{\sqsubseteq} f) \preccurlyeq \mathsf{lfp}^{\preccurlyeq} \overline{f}$.

Example of fixpoint abstraction



(a) exact fixpoint abstraction

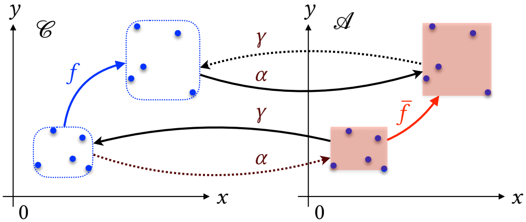
(b) imprecise fixpoint abstraction

Figure 18.1

Transformer abstraction

Transformer abstraction

- To abstract a fixpoint $\alpha(\mathsf{lfp}^{\sqsubseteq} f)$, we first abstract its transformer f.



Theorem (18.3, transformer abstraction) If $\langle C, \sqsubseteq\rangle \xleftrightarrow[\alpha]{\gamma} \langle \mathcal{A}, \preccurlyeq\rangle$ then $\langle C \xrightarrow{\nearrow} C, \dot{\sqsubseteq}\rangle \xleftrightarrow[\vec{\alpha}]{\vec{\gamma}} \langle \mathcal{A} \xrightarrow{\nearrow} \mathcal{A}, \dot{\preccurlyeq}\rangle$ where $\dot{\sqsubseteq}$ and $\dot{\preccurlyeq}$ are pointwise (*i.e.* $f \mathrel{\dot{\sqsubseteq}} g$ if and only if $\forall x \in C \mathrel{.} f(x) \sqsubseteq g(x)$), $\vec{\alpha}(f) = \alpha \circ f \circ \gamma$, and $\vec{\gamma}(\overline{f}) = \gamma \circ \overline{f} \circ \alpha$.

Proof Let $f \in C \xrightarrow{\nearrow} C$ and $\overline{f} \in \mathcal{A} \xrightarrow{\nearrow} \mathcal{A}$.

$$
\begin{array}{ll}
& \vec{\alpha}(f) \mathrel{\dot{\preccurlyeq}} \overline{f} \\
\Leftrightarrow & \forall \overline{x} \in \mathcal{A} \mathrel{.} \vec{\alpha}(f)\overline{x} \preccurlyeq \overline{f}(\overline{x}) \hfill \text{(pointwise def. } \dot{\preccurlyeq}\text{)} \\
\Leftrightarrow & \forall \overline{x} \in \mathcal{A} \mathrel{.} \alpha \circ f \circ \gamma(\overline{x}) \preccurlyeq \overline{f}(\overline{x}) \hfill \text{(def. } \vec{\alpha}\text{)} \\
\Leftrightarrow & \forall \overline{x} \in \mathcal{A} \mathrel{.} f \circ \gamma(\overline{x}) \sqsubseteq \gamma \circ \overline{f}(\overline{x}) \hfill (\langle C, \sqsubseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathcal{A}, \preccurlyeq\rangle) \\
\Rightarrow & \forall x \in C \mathrel{.} f \circ \gamma \circ \alpha(x) \sqsubseteq \gamma \circ \overline{f} \circ \alpha(x) \hfill \text{(for } \overline{x} = \alpha(x)\text{)} \\
& \forall x \in C \mathrel{.} x \sqsubseteq \gamma \circ \alpha(x) \hfill \text{(Exercise 11.34.(3))} \\
\Leftrightarrow & \forall x \in C \mathrel{.} f(x) \sqsubseteq \gamma \circ \overline{f} \circ \alpha(x) \hfill (f \text{ is increasing and } \sqsubseteq \text{ is transitive}) \\
\Leftrightarrow & \forall x \in C \mathrel{.} f(x) \sqsubseteq \vec{\gamma}(\overline{f})(x) \hfill \text{(def. } \vec{\gamma}\text{)} \\
\Leftrightarrow & f \mathrel{\dot{\sqsubseteq}} \vec{\gamma}(\overline{f}) \hfill \text{(pointwise def. } \dot{\sqsubseteq}\text{)}
\end{array}
$$

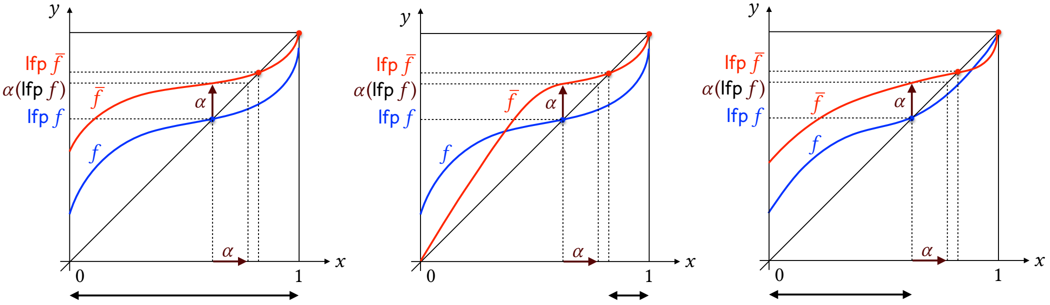
Conversely,

$$
\begin{array}{ll}
& f \mathrel{\dot{\sqsubseteq}} \vec{\gamma}(\overline{f}) \\
\Leftrightarrow & \forall x \in \mathcal{C} \,.\, f(x) \sqsubseteq \gamma \circ \overline{f} \circ \alpha(x) \hfill \wr \text{pointwise def. } \dot{\sqsubseteq} \text{ and def. } \vec{\gamma} \wr \\
\Leftrightarrow & \forall x \in \mathcal{C} \,.\, \alpha \circ f(x) \preccurlyeq \overline{f} \circ \alpha(x) \hfill \wr \langle \mathcal{C},\, \sqsubseteq \rangle \xleftarrow[\alpha]{\gamma} \hspace{-1em}\xrightarrow{} \langle \mathcal{A},\, \preccurlyeq \rangle \wr \\
\Rightarrow & \forall \overline{x} \in \mathcal{A} \,.\, \alpha \circ f \circ \gamma(\overline{x}) \preccurlyeq \overline{f} \circ \alpha \circ \gamma(\overline{x}) \hfill \wr \text{for } x = \gamma(\overline{x}) \wr \\
& \forall \overline{x} \in \mathcal{A} \,.\, \alpha \circ \gamma(\overline{x}) \preccurlyeq \overline{x} \hfill \wr \text{Exercise 11.34.(4)} \wr \\
\Rightarrow & \forall \overline{x} \in \mathcal{A} \,.\, \alpha \circ f \circ \gamma(\overline{x}) \preccurlyeq \overline{f}(\overline{x}) \hfill \wr \overline{f} \text{ is increasing and } \preccurlyeq \text{ is transitive} \wr \\
\Rightarrow & \forall \overline{x} \in \mathcal{A} \,.\, \vec{\alpha}(f)(\overline{x}) \preccurlyeq \overline{f}(\overline{x}) \hfill \wr \text{def. } \vec{\alpha}(f) \wr \\
\Rightarrow & \vec{\alpha}(f) \mathrel{\dot{\preccurlyeq}} \overline{f} \qquad \wr \text{pointwise def. } \dot{\preccurlyeq} \wr \hfill \square
\end{array}
$$

Fixpoint over-approximation

Fixpoint over-approximation

- In general abstracting the fixpoint transformer by a larger one yields a fixpoint over-approximation.



$f \mathrel{\dot{\sqsubseteq}} \overline{f}$ $\quad$ $\forall x \,.\, \overline{f}(x) \sqsubseteq x \Rightarrow f(x) \sqsubseteq x$ $\quad$ $\forall x \sqsubseteq \mathsf{lfp}^{\sqsubseteq} f \,.\, f(x) \sqsubseteq \overline{f}(x)$

Fixpoint over-approximation (cont'd)

Theorem (18.7, pointwise fixpoint over-approximation) Assume that $\langle C, \sqsubseteq, \bot, \top, \sqcup, \sqcap\rangle$ is a complete lattice, $f, g \in C \xrightarrow{\nearrow} C$ are increasing, and $f \,\dot{\sqsubseteq}\, g$ then $\mathsf{lfp}^{\sqsubseteq} f \sqsubseteq \mathsf{lfp}^{\sqsubseteq} g$.

Proof
- By $f \,\dot{\sqsubseteq}\, g$, for all $x \in C$, $g(x) \sqsubseteq x$ implies $f(x) \sqsubseteq x$ so $\{x \in C \mid g(x) \sqsubseteq x\} \subseteq \{x \in C \mid f(x) \sqsubseteq x\}$
- so, by Tarski's fixpoint Theorem 15.6 and def. of glbs, $\mathsf{lfp}^{\sqsubseteq} f = \bigsqcap\{x \in C \mid f(x) \sqsubseteq x\} \sqsubseteq \bigsqcap\{x \in C \mid g(x) \sqsubseteq x\} = \mathsf{lfp}^{\sqsubseteq} g$. $\square$

- Also valid for cpos (see Theorem 18.9).

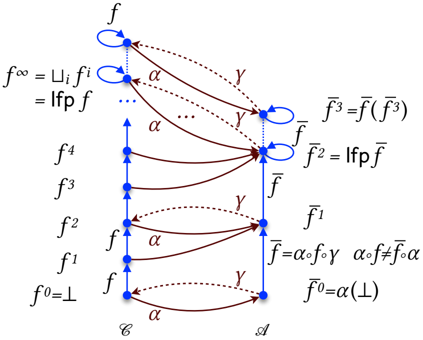
Sound fixpoint abstraction

- An abstract fixpoint $\mathsf{lfp}^{\preccurlyeq}\,\overline{f}$ is a sound fixpoint abstraction of a concrete fixpoint $\mathsf{lfp}^{\sqsubseteq}\,f$ whenever $\alpha(\mathsf{lfp}^{\sqsubseteq}\,f) \preccurlyeq \mathsf{lfp}^{\preccurlyeq}\,\overline{f}$.

Theorem (18.10, fixpoint over-approximation in a complete lattice) Assume that $\langle C, \sqsubseteq, \bot, \top, \sqcup, \sqcap\rangle$ and $\langle \mathcal{A}, \preccurlyeq, 0, 1, \curlyvee, \curlywedge\rangle$ are complete lattices, $\langle C, \sqsubseteq\rangle \xleftrightarrow[\alpha]{\gamma} \langle \mathcal{A}, \preccurlyeq\rangle$, and $f \in C \xrightarrow{\nearrow} C$ is increasing.
Then $\mathsf{lfp}^{\sqsubseteq}\,f \sqsubseteq \gamma(\mathsf{lfp}^{\preccurlyeq}\,\alpha \circ f \circ \gamma)$.

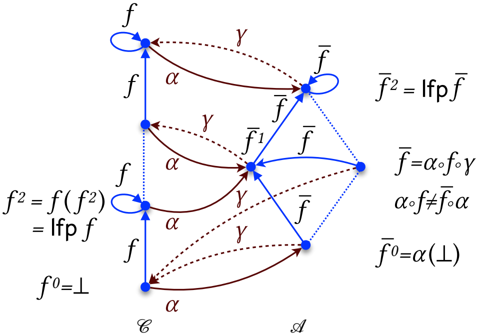
Example

The following two examples show that the inequality $\sqsubseteq$ can be strict or not.



$\mathrm{lfp}^{\sqsubseteq} f = \gamma(\mathrm{lfp}^{\preccurlyeq} \alpha \circ f \circ \gamma)$

(a) exact fixpoint abstraction



$\mathrm{lfp}^{\sqsubseteq} f \sqsubsetneq \gamma(\mathrm{lfp}^{\preccurlyeq} \alpha \circ f \circ \gamma)$

(b) imprecise fixpoint abstraction

Proof

$$
\begin{array}{ll}
& \mathsf{lfp}^{\sqsubseteq} f \\
= & \bigsqcap\{x \in C \mid f(x) \sqsubseteq x\} \hfill \text{(Tarski's fixpoint Theorem 15.6)} \\
\sqsubseteq & \bigsqcap\{\gamma(\overline{x}) \mid f(\gamma(\overline{x})) \sqsubseteq \gamma(\overline{x})\} \\
& \hfill \text{(since } \{\gamma(\overline{x}) \mid f(\gamma(\overline{x})) \sqsubseteq \gamma(\overline{x})\} \subseteq \{x \in C \mid f(x) \sqsubseteq x\} \text{ and def. glb } \bigsqcap\text{)} \\
= & \gamma(\curlywedge\{\overline{x} \mid f(\gamma(\overline{x})) \sqsubseteq \gamma(\overline{x})\}) \hfill \text{(}\gamma \text{ preserves existing glbs, by dual of Lemma 11.37)} \\
= & \gamma(\curlywedge\{\overline{x} \mid \alpha \circ f \circ \gamma(\overline{x}) \preccurlyeq \overline{x}\}) \hfill (\langle C, \sqsubseteq\rangle \xleftrightarrow[\alpha]{\gamma} \langle \mathcal{A}, \preccurlyeq\rangle) \\
= & \gamma(\mathsf{lfp}^{\preccurlyeq} \alpha \circ f \circ \gamma) \\
& \text{(since the composition of increasing functions is increasing and Tarski's fixpoint Theorem 15.6)} \qquad \square
\end{array}
$$

Sound fixpoint abstraction (cont'd)

Corollary (18.12, fixpoint approximation by transformer over-approximation) Assume that $\langle \mathcal{C}, \sqsubseteq, \bot, \top, \sqcup, \sqcap \rangle$ and $\langle \mathcal{A}, \preccurlyeq, 0, 1, \curlyvee, \curlywedge \rangle$ are complete lattices, $\langle \mathcal{C}, \sqsubseteq \rangle \xleftarrow[\alpha]{\gamma} \langle \mathcal{A}, \preccurlyeq \rangle$, $f \in \mathcal{C} \xrightarrow{\nearrow} \mathcal{C}$ and $\overline{f} \in \mathcal{A} \xrightarrow{\nearrow} \mathcal{A}$ are increasing, and $\alpha \circ f \circ \gamma \mathrel{\dot{\preccurlyeq}} \overline{f}$. Then $\mathsf{lfp}^{\sqsubseteq} f \sqsubseteq \gamma(\mathsf{lfp}^{\preccurlyeq} \overline{f})$.

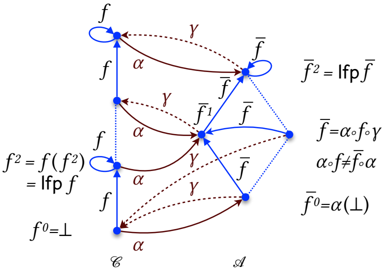
Proof By Theorem 18.10 and Theorem 18.7. □

Corollary (18.14, fixpoint approximation by semi-commuting transformer) Under the hypotheses of Corollary 18.12 assume instead that $\alpha \circ f \mathrel{\dot{\preccurlyeq}} \overline{f} \circ \alpha$ (*semi-commutation*). Then $\mathsf{lfp}^{\sqsubseteq} f \sqsubseteq \gamma(\mathsf{lfp}^{\preccurlyeq} \overline{f})$.

Proof If $\alpha \circ f \mathrel{\dot{\preccurlyeq}} \overline{f} \circ \alpha$ then, in particular, $\alpha \circ f \circ \gamma \mathrel{\dot{\preccurlyeq}} \overline{f} \circ \alpha \circ \gamma \mathrel{\dot{\preccurlyeq}} \overline{f}$ since $\alpha \circ \gamma$ is reductive by Exercise 11.34.(4) and $\overline{f}$ increasing by hypothesis. We conclude by Corollary 18.12. □

Theorem (18.16, fixpoint over-approximation in a cpo) Assume that $\langle C, \sqsubseteq, \bot, \sqcup\rangle$ is a cpo and $\langle \mathcal{A}, \preccurlyeq, 0, \curlywedge\rangle$ are cpos, $\langle C, \sqsubseteq\rangle \xleftarrow[\alpha]{\gamma} \langle \mathcal{A}, \preccurlyeq\rangle$, and $f \in C \xrightarrow{uc} C$ is upper continuous.
Then $\mathsf{lfp}^{\sqsubseteq} f \sqsubseteq \gamma(\mathsf{lfp}^{\preccurlyeq} \alpha \circ f \circ \gamma)$.

The inequality can be strict:



Exact fixpoint abstraction

Exact versus sound fixpoint abstraction

- A sound fixpoint abstraction $\alpha(\mathsf{lfp}^{\sqsubseteq} f) \preccurlyeq \mathsf{lfp}^{\preccurlyeq} \overline{f}$ is
  - *exact* when $\alpha(\mathsf{lfp}^{\sqsubseteq} f) = \mathsf{lfp}^{\preccurlyeq} \overline{f}$.
  - It is *sound but approximate (or imprecise)* when $\alpha(\mathsf{lfp}^{\sqsubseteq} f) \prec \mathsf{lfp}^{\preccurlyeq} \overline{f}$.

Exact fixpoint abstraction

Theorem (18.21, exact fixpoint abstraction in a complete lattice) Assume that $\langle C, \sqsubseteq, \bot, \top, \sqcup, \sqcap\rangle$ and $\langle \mathcal{A}, \preccurlyeq, 0, 1, \curlyvee, \curlywedge\rangle$ are complete lattices, $f \in C \xrightarrow{\nearrow} C$ is increasing, $\langle C, \sqsubseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathcal{A}, \preccurlyeq\rangle$, $\overline{f} \in \mathcal{A} \xrightarrow{\nearrow} \mathcal{A}$ is increasing, and $\alpha \circ f = \overline{f} \circ \alpha$ (*commutation property*). Then $\alpha(\mathsf{lfp}^{\sqsubseteq} f) = \mathsf{lfp}^{\preccurlyeq} \overline{f}$.

Proof of Theorem 18.21 $\mathsf{lfp}^{\sqsubseteq} f$ and $\mathsf{lfp}^{\preccurlyeq} \overline{f}$ do exist by Tarski's fixpoint Theorem 15.6.

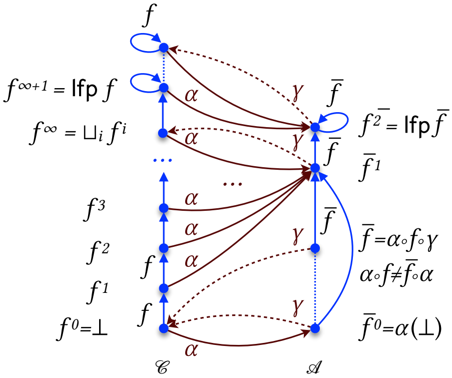
$$\begin{aligned} \alpha(\mathsf{lfp}^{\sqsubseteq} f) &= \alpha \circ f(\mathsf{lfp}^{\sqsubseteq} f) && \text{(fixpoint property)} \\ &= \overline{f} \circ \alpha(\mathsf{lfp}^{\sqsubseteq} f) && \text{(commutation property)} \end{aligned}$$

so $\alpha(\mathsf{lfp}^{\sqsubseteq} f)$ is a fixpoint of $\overline{f}$ proving that $\mathsf{lfp}^{\preccurlyeq} \overline{f} \preccurlyeq \alpha(\mathsf{lfp}^{\sqsubseteq} f)$ for the least fixpoint.

- Inversely, $\alpha \circ f = \overline{f} \circ \alpha$ implies $\alpha \circ f \circ \gamma = \overline{f} \circ \alpha \circ \gamma \mathrel{\dot{\preccurlyeq}} \overline{f}$ since $\alpha \circ \gamma$ is reductive and $\overline{f}$ is increasing.
- By Corollary 18.12 and $\langle C, \sqsubseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathcal{A}, \preccurlyeq\rangle$, $\alpha(\mathsf{lfp}^{\sqsubseteq} f) \preccurlyeq \mathsf{lfp}^{\preccurlyeq} \overline{f}$.
- By antisymmetry, $\alpha(\mathsf{lfp}^{\sqsubseteq} f) = \mathsf{lfp}^{\preccurlyeq} \overline{f}$. □

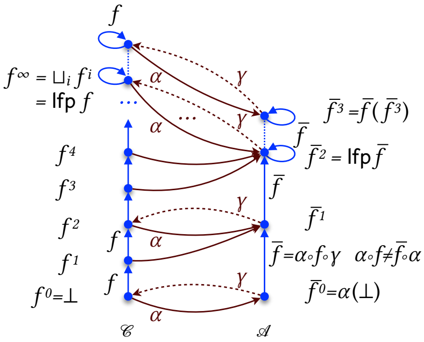
Example

The commutation condition is not necessary.

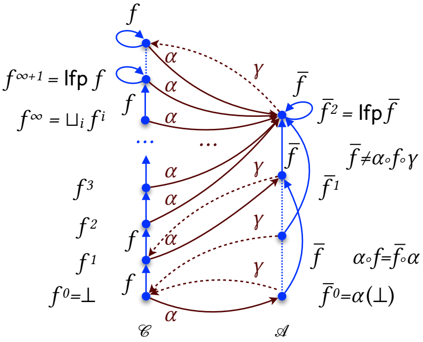


Example (cont'd)

The commutation condition is sufficient. It may hold whether $\overline{f} = \alpha \circ f \circ \gamma$ or not.



(a) $\overline{f} = \alpha \circ f \circ \gamma$

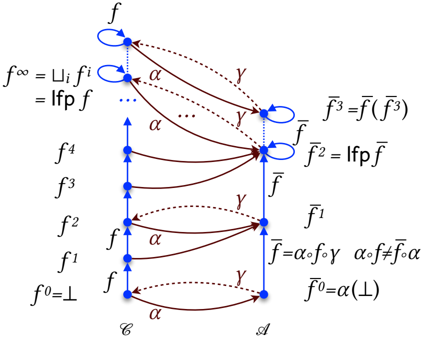


(b) $\overline{f} \sqsupsetneq \alpha \circ f \circ \gamma$

Exact fixpoint abstraction (cont'd)

Theorem (18.24, exact fixpoint abstraction in a cpo) Assume that $\langle C, \sqsubseteq, \perp, \sqcup\rangle$ is a cpo, $f \in C \xrightarrow{uc} C$ is upper continuous, $\langle C, \sqsubseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathcal{A}, \preccurlyeq\rangle$ is a Galois retraction, and $\overline{f} \in \mathcal{A} \to \mathcal{A}$ satisfies the commutation property $\alpha \circ f = \overline{f} \circ \alpha$. Then $\overline{f} = \alpha \circ f \circ \gamma$ is increasing and $\alpha(\mathsf{lfp}^{\sqsubseteq} f) = \mathsf{lfp}^{\preccurlyeq} \overline{f} = \bigvee_{n\in\mathbb{N}} \overline{f}^{\,n}(\alpha(\perp))$.

Example:



Exact iterates abstraction

- The hypotheses of Theorem 18.24 on the exact fixpoint abstraction in a cpo can be weakened as was the case for Tarski iterative fixpoint Theorem 15.21 for Scott's iterative fixpoint Theorem 15.26 by considering only the concrete iterates.

> **Corollary (18.31, exact iterates abstraction)** Assume $\langle C, \sqsubseteq\rangle$ and $\langle \mathcal{A}, \preccurlyeq\rangle$ are posets, $\perp$ is the infimum of $\langle C, \sqsubseteq\rangle$, $f \in C \to C$, the lub $\bigsqcup_{n\in\mathbb{N}} f^n(\perp)$ exists in $\langle C, \sqsubseteq\rangle$ such that $\mathsf{lfp}^{\sqsubseteq} f = \bigsqcup_{n\in\mathbb{N}} f^n(\perp)$, $\langle C, \sqsubseteq\rangle \xleftrightarrow[\alpha]{\gamma} \langle \mathcal{A}, \preccurlyeq\rangle$, $\overline{f} \in \mathcal{A} \to \mathcal{A}$, and $\forall n \in \mathbb{N} \,.\, \alpha(f^{n+1}(\perp)) = \overline{f}(\alpha(f^n(\perp)))$.
> Then the lub $\bigvee_{n\in\mathbb{N}} \overline{f}^n(\alpha(\perp))$ exists in $\langle \mathcal{A}, \preccurlyeq\rangle$ such that $\alpha(\mathsf{lfp}^{\sqsubseteq} f) = \bigvee_{n\in\mathbb{N}} \overline{f}^n(\alpha(\perp))$.

Proof of Corollary 18.31

- We have $\alpha(f^0(\bot)) = \alpha(\bot) = \overline{f}^0(\alpha(\bot))$.
- Assume that $\alpha(f^n(\bot)) = \overline{f}^n(\alpha(\bot))$ by induction hypothesis.
- Then $\alpha(f^{n+1}(\bot)) = \overline{f}(\alpha(f^n(\bot))) = \overline{f}(\overline{f}^n(\alpha(\bot))) = \overline{f}^{n+1}(\alpha(\bot))$, proving $\forall n \in \mathbb{N} \,.\, \alpha(f^n(\bot)) = \overline{f}^n(\alpha(\bot))$
- and so, α preserving existing lubs, $\alpha(\mathsf{lfp}^{\sqsubseteq} f) = \alpha(\bigsqcup_{n\in\mathbb{N}} f^n(\bot)) = \bigcurlyvee_{n\in\mathbb{N}} \alpha(f^n(\bot)) = \bigcurlyvee_{n\in\mathbb{N}} \overline{f}^n(\alpha(\bot))$. $\square$

Abstraction of deductive definitions

Exact and approximate deductive definition abstraction

Theorem (18.41, deductive definition abstraction) Let $R = \{\frac{P_i}{c_i} \mid i \in \Delta\}$ be the inference rules of the deductive definition of $D \in \wp(C)$.

Assume that $\langle \wp(C), \subseteq\rangle \xleftarrow[\alpha]{\gamma} \langle \wp(\mathcal{A}), \subseteq\rangle$.

Let $\overline{R} = \{\frac{\alpha(P)}{\bar{c}} \mid \frac{P}{c} \in R \wedge \bar{c} \in \alpha(\{c\})\}$ and $\overline{D} \in \wp(\mathcal{A})$ be defined by $\overline{R}$.

Then

- $\alpha(D) \subseteq \overline{D}$;
- if $\forall X \subseteq D \mathrel{.} \gamma \circ \alpha(X) \subseteq X$ then $\alpha(D) = \overline{D}$ (this hypothesis on X is necessary only for the iterates $X = F_R^n(\varnothing)$ of the consequence operator F_R of rules R).

Proof of Theorem 18.41

- By Theorem 16.11, $D = \mathrm{lfp}^{\subseteq} F_R$ and $\overline{D} = \mathrm{lfp}^{\subseteq} \overline{F}_{\overline{R}}$ where $F_R(X) \triangleq \{c \mid \exists \frac{P}{c} \in R \,.\, P \subseteq X\}$ and $\overline{F}_{\overline{R}}(Y) \triangleq \{\overline{c} \mid \exists \frac{\alpha(P)}{\overline{c}} \,.\, \frac{P}{c} \in R \wedge \overline{c} \in \alpha(\{c\}) \wedge \alpha(P) \subseteq Y\}$.
- We have

$$
\begin{array}{ll}
\quad \alpha(F_R(X)) & \\
= \alpha(\bigcup\{\{c\} \mid \exists \dfrac{P}{c} \in R \,.\, P \subseteq X\}) & \wr\text{def. } F_R \text{ and } S = \bigcup\{\{x\} \mid x \in S\}\int \\
= \bigcup\{\alpha(\{c\}) \mid \exists \dfrac{P}{c} \in R \,.\, P \subseteq X\} & \wr\alpha \text{ preserves existing joins}\int \\
= \{\overline{c} \mid \exists \dfrac{P}{c} \in R \,.\, \overline{c} \in \alpha(\{c\}) \wedge P \subseteq X\} & \wr S = \bigcup\{\{x\} \mid x \in S\}\int \\
= \{\overline{c} \mid \exists \dfrac{\alpha(P)}{\overline{c}} \in \overline{R} \,.\, P \subseteq X\} & \wr\text{def. } \overline{R}\int \\
\subseteq \{\overline{c} \mid \exists \dfrac{\alpha(P)}{\overline{c}} \in \overline{R} \,.\, \alpha(P) \subseteq \alpha(X)\} & \wr\alpha \text{ increasing}\int \\
= \overline{F}_{\overline{R}}(\alpha(X)) & \wr\text{def. } \overline{F}_{\overline{R}}\int
\end{array}
$$

proving, by Corollary 18.14, that $\alpha(D) = \alpha(\mathrm{lfp}^{\subseteq} F_R) \subseteq \mathrm{lfp}^{\subseteq} \overline{F}_{\overline{R}} = \overline{D}$.

- Assume, by hypothesis, that $\forall X \subseteq D \;.\; \gamma \circ \alpha(X) \subseteq X$.
- It follows that $\alpha(P) \subseteq \alpha(X)$ implies $P \subseteq \gamma \circ \alpha(X) \subseteq X$
- Therefore, in the above proof, the hypothesis implies that we now have $\alpha(F_R(X)) = \overline{F}_{\overline{R}}(\alpha(X))$
- F_R preserves non-empty joins so by Tarski-Kantorovich fixpoint Theorem 15.21, $\mathsf{lfp}^{\subseteq} F_R = \bigcup_{n \in \mathbb{N}} F_R^n(\varnothing)$.
- We have $\forall n \in \mathbb{N} \;.\; F_R^n(\varnothing) \subseteq \mathsf{lfp}^{\subseteq} F_R = D$ by def. lub
- Since $X = F_R^n(\varnothing) \subseteq D$, we have $\gamma \circ \alpha(F_R^n(\varnothing)) \subseteq F_R^n(\varnothing)$ by hypothesis.
- Therefore $\alpha(F_R^{n+1}(\varnothing)) = \overline{F}_{\overline{R}}(\alpha(F_R^n(\varnothing)))$, as shown above for $X = F_R^n(\varnothing)$
- By Corollary 18.31, we conclude that $\alpha(D) = \alpha(\mathsf{lfp}^{\sqsubseteq} F_R) = \bigcup_{n \in \mathbb{N}} \overline{F}_{\overline{R}}^n(\alpha(\varnothing)) = \bigcup_{n \in \mathbb{N}} \overline{F}_{\overline{R}}^n(\varnothing) = \mathsf{lfp}^{\sqsubseteq} \overline{F}_{\overline{R}} = \overline{D}$ (since $\varnothing \subseteq \gamma(\varnothing)$ so $\alpha(\varnothing) \subseteq \varnothing$ and $\alpha(\varnothing) = \varnothing$ by antisymmetry). $\square$

Inductive and structural abstraction

- The abstraction of an inductive definition of $D \in S \to \wp(\mathbb{U})$ (where $\langle S, \preccurlyeq\rangle$ ($\triangleleft$ for structural definition) is well-founded) by Galois connection $\langle \wp(\mathbb{U}), \subseteq\rangle \xrightleftharpoons[\alpha]{\gamma} \langle \mathcal{A}, \sqsubseteq\rangle$ is $\overline{D} \in S \to \mathcal{A}$ such that $\forall s \in S \,.\, \overline{D}(s) \triangleq \alpha(D(s))$.
- Each $D(s)$ is defined as a function of the $\langle D(s'), s' \prec s\rangle$ using in general a fixpoint definition or a deductive definition and so the abstraction is obtained by induction using the fixpoint and deductive definition abstraction theorems introduced in this class.

Conclusion on the abstraction of semantics

- Fixpoints/deductive definitions are used to define the semantics of iteration.
- The fixpoint/deductive definition abstraction and approximation theorems provide methods for constructing exact or else sound abstractions of the semantics of iteration [P. Cousot and R. Cousot, 1979].

Bibliography I

Cousot, Patrick and Radhia Cousot (1979). "Systematic Design of Program Analysis Frameworks". In: *POPL*. ACM Press, pp. 269–282.

Home work

- Read Ch. **18** "Fixpoint abstraction" of

Principles of Abstract Interpretation
Patrick Cousot
MIT Press

The End, Thank you