michelepasqua.github.io/
michele.pasqua@univr.it

UNIVERSITÀ di VERONA
Dipartimento di INFORMATICA

Principles and Applications of Abstract Interpretation

Abstract Interpretation Primer

Michele Pasqua, PhD

Verona, IT

October 2024

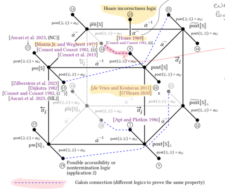
PhD Course @ UniVR 2024/2025

A gentle introduction...

Assertional Postcondition Transformer

- $\text{post}[S] = \lambda P. \{\sigma' \mid \exists \sigma \in P. \langle \sigma, \sigma' \rangle \in S\}$
- Preserves joins $\text{Post}[S] \bigcup_i P_i = \bigcup_i \text{Post}[S] P_i$
- Isomorphism
  $T = \text{post}[R]$
  $\Leftrightarrow R = \{\langle \sigma, \sigma' \rangle \mid \sigma' \in T(\{\sigma\})\}$
  $\triangleq \text{post}^{-1}(T)$
- $\langle \wp(\Sigma \times \Sigma_\perp), \subseteq \rangle \underset{\text{post}}{\overset{\text{post}^{-1}}{\leftrightarrows}} \langle \wp(\Sigma) \overset{\cup}{\rightarrow} \wp(\Sigma_\perp), \dot{\subseteq} \rangle$

The subhierarchy of assertional logics



$\alpha^{\neg}$ can be added everywhere (32 logics)

equivalent logics (a proof by one logic can be transformed into a proof by the other logic)

iteration

symbolic rules ↓ — Aczel semantics of the rules

$$\sigma \vdash W \overset{i}{\Rightarrow} \sigma \qquad \text{i.e.} \quad \frac{\emptyset}{\langle \sigma, \sigma \rangle} \quad \sigma \in \Sigma \text{ axioms}$$

$$\frac{\mathcal{B}[\![B]\!]\sigma, \quad \sigma \vdash S \overset{e}{\Rightarrow} \sigma', \quad \sigma' \vdash W \overset{i}{\Rightarrow} \sigma''}{\sigma \vdash W \overset{i}{\Rightarrow} \sigma''} \qquad \text{i.e.} \quad \frac{\{\langle \sigma', \sigma'' \rangle\}}{\langle \sigma, \sigma'' \rangle} \quad \mathcal{B}[\![B]\!]\sigma \; \langle \sigma, \sigma' \rangle \in [\![S]\!]^e$$

structural induction ↑

Consequence operator

$$F^e(X) = \{\langle \sigma, \sigma \rangle \mid \sigma \in \Sigma\} \cup \{\langle \sigma, \sigma'' \rangle \mid \mathcal{B}[\![B]\!]\sigma \wedge \langle \sigma, \sigma' \rangle \in [\![S]\!]^e \wedge \langle \sigma', \sigma'' \rangle \in X\}$$

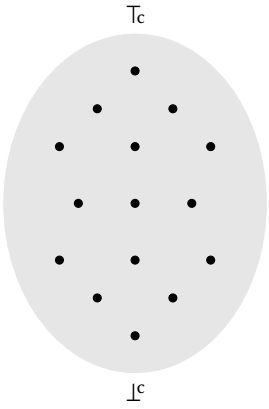
$$= \text{id} \cup ([\![B]\!] \,⨟\, [\![S]\!]^e \,⨟\, (X \setminus \Sigma \times \{\perp\})),$$

this is the termination case

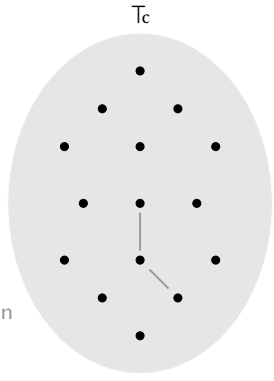
defines $\text{lfp}^{\subseteq} F^e = ([\![B]\!] \,⨟\, [\![S]\!]^e)^*$

The Abstraction Process

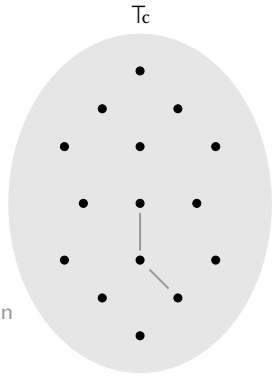
Concrete domain $\langle C, \sqsubseteq^c \rangle$

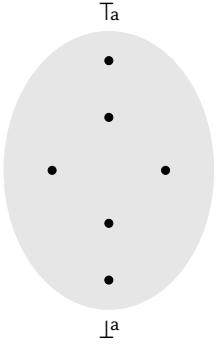


Concrete domain $\langle C, \sqsubseteq^c \rangle$



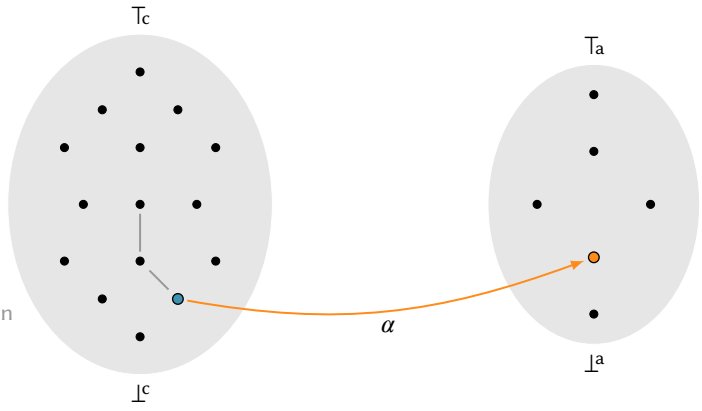
Concrete domain $\langle C, \sqsubseteq^c \rangle$ $\langle A, \sqsubseteq^a \rangle$ Abstract domain





$\sqsubseteq^c$ models relative precision

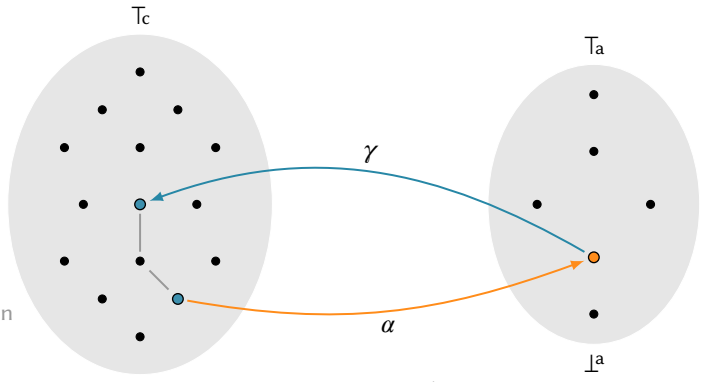
Concrete domain $\langle C, \sqsubseteq^c \rangle$ $\langle A, \sqsubseteq^a \rangle$ Abstract domain



$\sqsubseteq^c$ models relative precision

What is abstraction? (formally)

Concrete domain $\langle C, \sqsubseteq^c \rangle$ $\langle A, \sqsubseteq^a \rangle$ Abstract domain

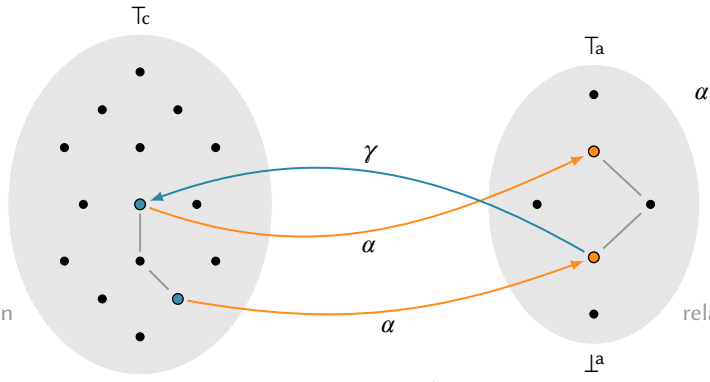


$\sqsubseteq^c$ models relative precision

$\gamma \circ \alpha$ extensive

What is abstraction? (formally)

Concrete domain $\langle C, \sqsubseteq^c \rangle$ $\langle A, \sqsubseteq^a \rangle$ Abstract domain



α monotonic

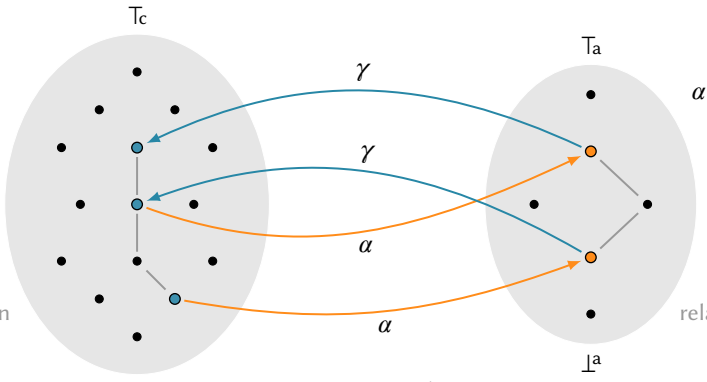
$\sqsubseteq^c$ models relative precision

$\sqsubseteq^a$ models relative precision

$\gamma \circ \alpha$ extensive

What is abstraction? (formally)

Concrete domain $\langle C, \sqsubseteq^c \rangle$ $\langle A, \sqsubseteq^a \rangle$ Abstract domain



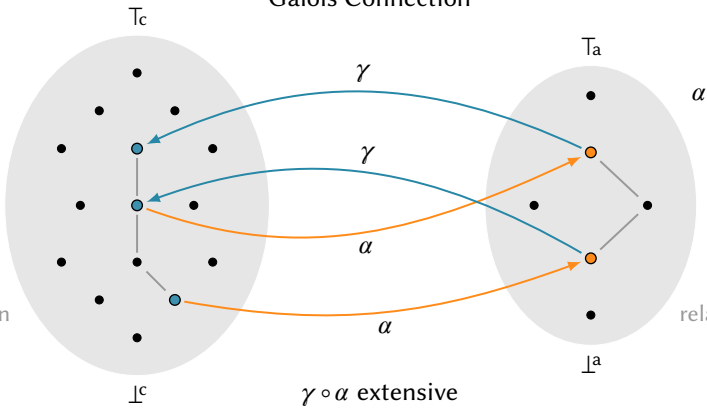
What is abstraction? (formally)

Concrete domain

$\langle C, \sqsubseteq^c \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle A, \sqsubseteq^a \rangle$

Abstract domain

Galois Connection



γ monotonic

α monotonic

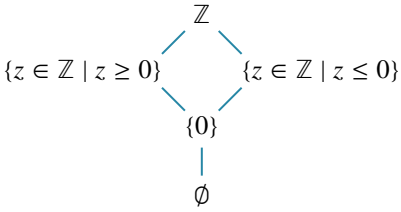
$\sqsubseteq^c$ models relative precision

$\sqsubseteq^a$ models relative precision

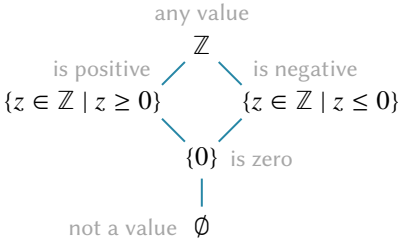
$\gamma \circ \alpha$ extensive

Isolate the subsets of integers $\mathbb{Z}$ we are interested in

Isolate the subsets of integers $\mathbb{Z}$ we are interested in

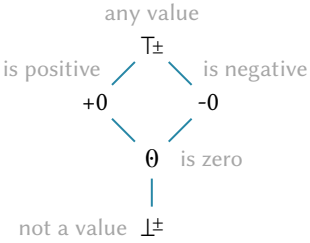


Isolate the subsets of integers $\mathbb{Z}$ we are interested in



Isolate the subsets of integers $\mathbb{Z}$ we are interested in

Encode subsets into a machine-representable domain $\mathbb{Z}^{\pm}$

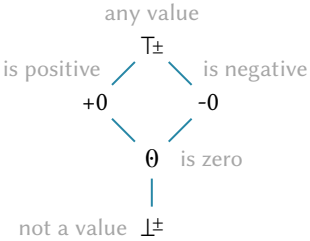


Isolate the subsets of integers $\mathbb{Z}$ we are interested in

Encode subsets into a machine-representable domain $\mathbb{Z}^{\pm}$

Define an abstraction (encoding) function $\alpha : \wp(\mathbb{Z}) \to \mathbb{Z}^{\pm}$

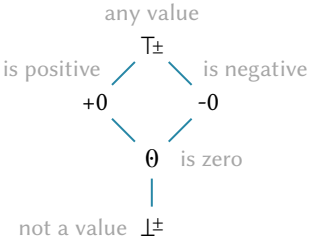
$$\alpha(X) \triangleq \begin{cases} \bot^{\pm} & \text{if } X = \emptyset \\ 0 & \text{if } X = \{0\} \\ +0 & \text{if } X \subseteq \{z \in \mathbb{Z} \mid z \geq 0\} \wedge X \neq \emptyset \\ -0 & \text{if } X \subseteq \{z \in \mathbb{Z} \mid z \leq 0\} \wedge X \neq \emptyset \\ \top^{\pm} & \text{otherwise} \end{cases}$$



Isolate the subsets of integers $\mathbb{Z}$ we are interested in

Encode subsets into a machine-representable domain $\mathbb{Z}^{\pm}$

Define a concretization (decoding) function $\gamma : \mathbb{Z}^{\pm} \to \wp(\mathbb{Z})$

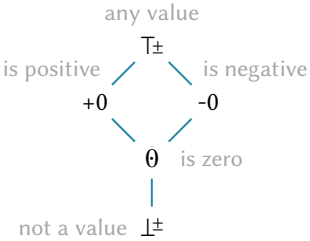


$$\gamma(z^{\pm}) \triangleq \begin{cases} \emptyset & \text{if } z^{\pm} = \bot^{\pm} \\ \{0\} & \text{if } z^{\pm} = 0 \\ \{z \in \mathbb{Z} \mid z \geq 0\} & \text{if } z^{\pm} = +0 \\ \{z \in \mathbb{Z} \mid z \leq 0\} & \text{if } z^{\pm} = -0 \\ \mathbb{Z} & \text{if } z^{\pm} = \top^{\pm} \end{cases}$$

Isolate the subsets of integers $\mathbb{Z}$ we are interested in

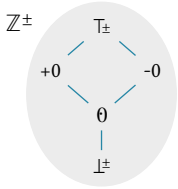
Encode subsets into a machine-representable domain $\mathbb{Z}^{\pm}$

Define a concretization (decoding) function $\gamma : \mathbb{Z}^{\pm} \to \wp(\mathbb{Z})$



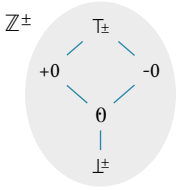
$$\gamma(z^{\pm}) \triangleq \begin{cases} \emptyset & \text{if } z^{\pm} = \bot^{\pm} \\ \{0\} & \text{if } z^{\pm} = 0 \\ \{z \in \mathbb{Z} \mid z \geq 0\} & \text{if } z^{\pm} = +0 \\ \{z \in \mathbb{Z} \mid z \leq 0\} & \text{if } z^{\pm} = -0 \\ \mathbb{Z} & \text{if } z^{\pm} = \top^{\pm} \end{cases}$$

Extensivity: $\{1,4,7\} \subseteq \gamma\alpha(\{1,4,7\})$
$\subseteq \gamma(+0)$
$\subseteq \{z \in \mathbb{Z} \mid z \geq 0\}$

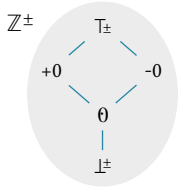

$\mathbb{Z}^{\pm}$
$\mathbb{T}_{\pm}$
+0
-0
θ
$\perp^{\pm}$

$\times^{\sharp}$	$\bot^{\pm}$	θ	+0	-0	$\top^{\pm}$
$\bot^{\pm}$	$\bot^{\pm}$	$\bot^{\pm}$	$\bot^{\pm}$	$\bot^{\pm}$	$\bot^{\pm}$
θ	$\bot^{\pm}$	θ	θ	θ	θ
+0	$\bot^{\pm}$	θ	+0	-0	$\top^{\pm}$
-0	$\bot^{\pm}$	θ	-0	+0	$\top^{\pm}$
$\top^{\pm}$	$\bot^{\pm}$	θ	$\top^{\pm}$	$\top^{\pm}$	$\top^{\pm}$

1×2

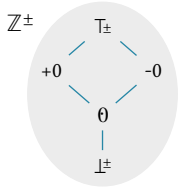


$\times^\sharp$	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$
θ	$\bot^\pm$	θ	θ	θ	θ
$+0$	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
-0	$\bot^\pm$	θ	-0	$+0$	$\top^\pm$
$\top^\pm$	$\bot^\pm$	θ	$\top^\pm$	$\top^\pm$	$\top^\pm$



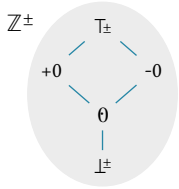
1×2 $\quad\quad$ $\alpha(1) \times^\sharp \alpha(2)$

$\times^\sharp$	$\bot^\pm$	θ	+0	-0	$\top^\pm$
$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$
θ	$\bot^\pm$	θ	θ	θ	θ
+0	$\bot^\pm$	θ	+0	-0	$\top^\pm$
-0	$\bot^\pm$	θ	-0	+0	$\top^\pm$
$\top^\pm$	$\bot^\pm$	θ	$\top^\pm$	$\top^\pm$	$\top^\pm$



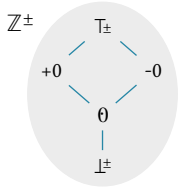
$1 \times 2 \qquad \alpha(1) \times^\sharp \alpha(2) = +0 \times^\sharp +0$

$\times^\sharp$	$\bot^\pm$	θ	+0	-0	$\top^\pm$
$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$
θ	$\bot^\pm$	θ	θ	θ	θ
+0	$\bot^\pm$	θ	+0	-0	$\top^\pm$
-0	$\bot^\pm$	θ	-0	+0	$\top^\pm$
$\top^\pm$	$\bot^\pm$	θ	$\top^\pm$	$\top^\pm$	$\top^\pm$



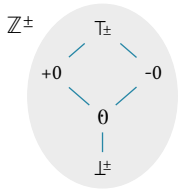
$1 \times 2 \quad +0 = \alpha(1) \times^\sharp \alpha(2) = +0 \times^\sharp +0$

$\times^\sharp$	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$
θ	$\bot^\pm$	θ	θ	θ	θ
$+0$	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
-0	$\bot^\pm$	θ	-0	$+0$	$\top^\pm$
$\top^\pm$	$\bot^\pm$	θ	$\top^\pm$	$\top^\pm$	$\top^\pm$



$$\alpha(1 \times 2) = +0 = \alpha(1) \times^\sharp \alpha(2) = +0 \times^\sharp +0$$

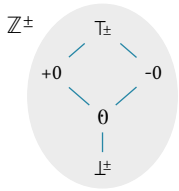
$\times^\sharp$	$\bot^\pm$	θ	+0	-0	$\top^\pm$
$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$
θ	$\bot^\pm$	θ	θ	θ	θ
+0	$\bot^\pm$	θ	+0	-0	$\top^\pm$
-0	$\bot^\pm$	θ	-0	+0	$\top^\pm$
$\top^\pm$	$\bot^\pm$	θ	$\top^\pm$	$\top^\pm$	$\top^\pm$



$$\alpha(1 \times 2) = +0 = \alpha(1) \times^\sharp \alpha(2) = +0 \times^\sharp +0$$

$$\alpha(-1 \times 0) = \theta = \alpha(-1) \times^\sharp \alpha(0) = -0 \times^\sharp \theta$$

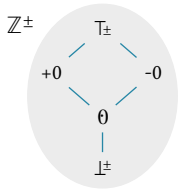
$\times^\sharp$	$\bot^\pm$	θ	+0	-0	$\top^\pm$
$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$
θ	$\bot^\pm$	θ	θ	θ	θ
+0	$\bot^\pm$	θ	+0	-0	$\top^\pm$
-0	$\bot^\pm$	θ	-0	+0	$\top^\pm$
$\top^\pm$	$\bot^\pm$	θ	$\top^\pm$	$\top^\pm$	$\top^\pm$



$$\alpha(1 \times 2) = +0 = \alpha(1) \times^\sharp \alpha(2) = +0 \times^\sharp +0$$
$$\alpha(-1 \times 0) = \theta = \alpha(-1) \times^\sharp \alpha(0) = -0 \times^\sharp \theta$$
$$\alpha(-1 \times 2) = -0 = \alpha(-1) \times^\sharp \alpha(2) = -0 \times^\sharp +0$$

$\times^\sharp$	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$
θ	$\bot^\pm$	θ	θ	θ	θ
$+0$	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
-0	$\bot^\pm$	θ	-0	$+0$	$\top^\pm$
$\top^\pm$	$\bot^\pm$	θ	$\top^\pm$	$\top^\pm$	$\top^\pm$

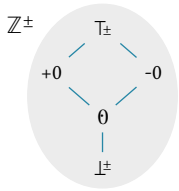
$+^\sharp$	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$
θ	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
$+0$	$\bot^\pm$	$+0$	$+0$	$\top^\pm$	$\top^\pm$
-0	$\bot^\pm$	-0	$\top^\pm$	-0	$\top^\pm$
$\top^\pm$	$\bot^\pm$	θ	$\top^\pm$	$\top^\pm$	$\top^\pm$



$$\alpha(1 \times 2) = +0 = \alpha(1) \times^\sharp \alpha(2) = +0 \times^\sharp +0$$
$$\alpha(-1 \times 0) = \theta = \alpha(-1) \times^\sharp \alpha(0) = -0 \times^\sharp \theta$$
$$\alpha(-1 \times 2) = -0 = \alpha(-1) \times^\sharp \alpha(2) = -0 \times^\sharp +0$$

$\times^\sharp$	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$
θ	$\bot^\pm$	θ	θ	θ	θ
$+0$	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
-0	$\bot^\pm$	θ	-0	$+0$	$\top^\pm$
$\top^\pm$	$\bot^\pm$	θ	$\top^\pm$	$\top^\pm$	$\top^\pm$

$+^\sharp$	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$
θ	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
$+0$	$\bot^\pm$	$+0$	$+0$	$\top^\pm$	$\top^\pm$
-0	$\bot^\pm$	-0	$\top^\pm$	-0	$\top^\pm$
$\top^\pm$	$\bot^\pm$	θ	$\top^\pm$	$\top^\pm$	$\top^\pm$



$\alpha(1 \times 2) = +0 = \alpha(1) \times^\sharp \alpha(2) = +0 \times^\sharp +0$

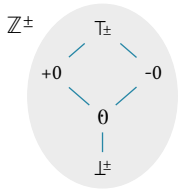
$\alpha(-1 \times 0) = \theta = \alpha(-1) \times^\sharp \alpha(0) = -0 \times^\sharp \theta$

$\alpha(-1 \times 2) = -0 = \alpha(-1) \times^\sharp \alpha(2) = -0 \times^\sharp +0$

$\alpha(1 + 2) = +0 = \alpha(1) +^\sharp \alpha(2) = +0 +^\sharp +0$

$\times^\sharp$	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$
θ	$\bot^\pm$	θ	θ	θ	θ
$+0$	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
-0	$\bot^\pm$	θ	-0	$+0$	$\top^\pm$
$\top^\pm$	$\bot^\pm$	θ	$\top^\pm$	$\top^\pm$	$\top^\pm$

$+^\sharp$	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$
θ	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
$+0$	$\bot^\pm$	$+0$	$+0$	$\top^\pm$	$\top^\pm$
-0	$\bot^\pm$	-0	$\top^\pm$	-0	$\top^\pm$
$\top^\pm$	$\bot^\pm$	θ	$\top^\pm$	$\top^\pm$	$\top^\pm$

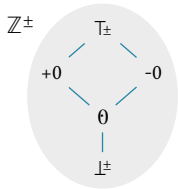


$$\alpha(1 \times 2) = +0 = \alpha(1) \times^\sharp \alpha(2) = +0 \times^\sharp +0$$
$$\alpha(-1 \times 0) = \theta = \alpha(-1) \times^\sharp \alpha(0) = -0 \times^\sharp \theta$$
$$\alpha(-1 \times 2) = -0 = \alpha(-1) \times^\sharp \alpha(2) = -0 \times^\sharp +0$$

$$\alpha(1 + 2) = +0 = \alpha(1) +^\sharp \alpha(2) = +0 +^\sharp +0$$
$$\alpha(-1 + 0) = -0 = \alpha(-1) +^\sharp \alpha(0) = -0 +^\sharp \theta$$

$\times^\sharp$	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$
θ	$\bot^\pm$	θ	θ	θ	θ
$+0$	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
-0	$\bot^\pm$	θ	-0	$+0$	$\top^\pm$
$\top^\pm$	$\bot^\pm$	θ	$\top^\pm$	$\top^\pm$	$\top^\pm$

$+^\sharp$	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$
θ	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
$+0$	$\bot^\pm$	$+0$	$+0$	$\top^\pm$	$\top^\pm$
-0	$\bot^\pm$	-0	$\top^\pm$	-0	$\top^\pm$
$\top^\pm$	$\bot^\pm$	θ	$\top^\pm$	$\top^\pm$	$\top^\pm$

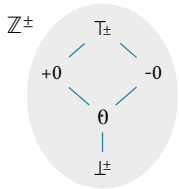


$$\alpha(1 \times 2) = +0 = \alpha(1) \times^\sharp \alpha(2) = +0 \times^\sharp +0$$
$$\alpha(-1 \times 0) = \theta = \alpha(-1) \times^\sharp \alpha(0) = -0 \times^\sharp \theta$$
$$\alpha(-1 \times 2) = -0 = \alpha(-1) \times^\sharp \alpha(2) = -0 \times^\sharp +0$$

$$\alpha(1 + 2) = +0 = \alpha(1) +^\sharp \alpha(2) = +0 +^\sharp +0$$
$$\alpha(-1 + 0) = -0 = \alpha(-1) +^\sharp \alpha(0) = -0 +^\sharp \theta$$
$$-1 + 2$$

$\times^\sharp$	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$
θ	$\bot^\pm$	θ	θ	θ	θ
$+0$	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
-0	$\bot^\pm$	θ	-0	$+0$	$\top^\pm$
$\top^\pm$	$\bot^\pm$	θ	$\top^\pm$	$\top^\pm$	$\top^\pm$

$+^\sharp$	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$
θ	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
$+0$	$\bot^\pm$	$+0$	$+0$	$\top^\pm$	$\top^\pm$
-0	$\bot^\pm$	-0	$\top^\pm$	-0	$\top^\pm$
$\top^\pm$	$\bot^\pm$	θ	$\top^\pm$	$\top^\pm$	$\top^\pm$

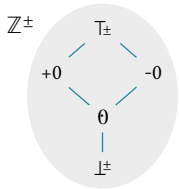


$$\alpha(1 \times 2) = +0 = \alpha(1) \times^\sharp \alpha(2) = +0 \times^\sharp +0$$
$$\alpha(-1 \times 0) = \theta = \alpha(-1) \times^\sharp \alpha(0) = -0 \times^\sharp \theta$$
$$\alpha(-1 \times 2) = -0 = \alpha(-1) \times^\sharp \alpha(2) = -0 \times^\sharp +0$$

$$\alpha(1 + 2) = +0 = \alpha(1) +^\sharp \alpha(2) = +0 +^\sharp +0$$
$$\alpha(-1 + 0) = -0 = \alpha(-1) +^\sharp \alpha(0) = -0 +^\sharp \theta$$
$$-1 + 2 \qquad \alpha(-1) +^\sharp \alpha(2)$$

$\times^\sharp$	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$
θ	$\bot^\pm$	θ	θ	θ	θ
$+0$	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
-0	$\bot^\pm$	θ	-0	$+0$	$\top^\pm$
$\top^\pm$	$\bot^\pm$	θ	$\top^\pm$	$\top^\pm$	$\top^\pm$

$+^\sharp$	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$
θ	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
$+0$	$\bot^\pm$	$+0$	$+0$	$\top^\pm$	$\top^\pm$
-0	$\bot^\pm$	-0	$\top^\pm$	-0	$\top^\pm$
$\top^\pm$	$\bot^\pm$	θ	$\top^\pm$	$\top^\pm$	$\top^\pm$



$\alpha(1 \times 2) = +0 = \alpha(1) \times^\sharp \alpha(2) = +0 \times^\sharp +0$

$\alpha(-1 \times 0) = \theta = \alpha(-1) \times^\sharp \alpha(0) = -0 \times^\sharp \theta$

$\alpha(-1 \times 2) = -0 = \alpha(-1) \times^\sharp \alpha(2) = -0 \times^\sharp +0$

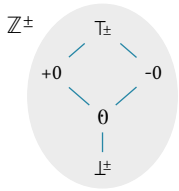
$\alpha(1 + 2) = +0 = \alpha(1) +^\sharp \alpha(2) = +0 +^\sharp +0$

$\alpha(-1 + 0) = -0 = \alpha(-1) +^\sharp \alpha(0) = -0 +^\sharp \theta$

$-1 + 2 \qquad \alpha(-1) +^\sharp \alpha(2) = -0 +^\sharp +0$

$\times^\sharp$	$\bot^\pm$	θ	+0	-0	$\top^\pm$
$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$
θ	$\bot^\pm$	θ	θ	θ	θ
+0	$\bot^\pm$	θ	+0	-0	$\top^\pm$
-0	$\bot^\pm$	θ	-0	+0	$\top^\pm$
$\top^\pm$	$\bot^\pm$	θ	$\top^\pm$	$\top^\pm$	$\top^\pm$

$+^\sharp$	$\bot^\pm$	θ	+0	-0	$\top^\pm$
$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$
θ	$\bot^\pm$	θ	+0	-0	$\top^\pm$
+0	$\bot^\pm$	+0	+0	$\top^\pm$	$\top^\pm$
-0	$\bot^\pm$	-0	$\top^\pm$	-0	$\top^\pm$
$\top^\pm$	$\bot^\pm$	θ	$\top^\pm$	$\top^\pm$	$\top^\pm$



$\alpha(1 \times 2) = +0 = \alpha(1) \times^\sharp \alpha(2) = +0 \times^\sharp +0$

$\alpha(-1 \times 0) = \theta = \alpha(-1) \times^\sharp \alpha(0) = -0 \times^\sharp \theta$

$\alpha(-1 \times 2) = -0 = \alpha(-1) \times^\sharp \alpha(2) = -0 \times^\sharp +0$

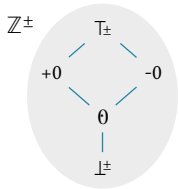
$\alpha(1 + 2) = +0 = \alpha(1) +^\sharp \alpha(2) = +0 +^\sharp +0$

$\alpha(-1 + 0) = -0 = \alpha(-1) +^\sharp \alpha(0) = -0 +^\sharp \theta$

$-1 + 2 \quad \top^\pm = \alpha(-1) +^\sharp \alpha(2) = -0 +^\sharp +0$

$\times^\sharp$	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$
θ	$\bot^\pm$	θ	θ	θ	θ
$+0$	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
-0	$\bot^\pm$	θ	-0	$+0$	$\top^\pm$
$\top^\pm$	$\bot^\pm$	θ	$\top^\pm$	$\top^\pm$	$\top^\pm$

$+^\sharp$	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$
θ	$\bot^\pm$	θ	$+0$	-0	$\top^\pm$
$+0$	$\bot^\pm$	$+0$	$+0$	$\top^\pm$	$\top^\pm$
-0	$\bot^\pm$	-0	$\top^\pm$	-0	$\top^\pm$
$\top^\pm$	$\bot^\pm$	θ	$\top^\pm$	$\top^\pm$	$\top^\pm$

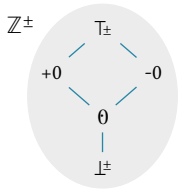


$$\alpha(1 \times 2) = +0 = \alpha(1) \times^\sharp \alpha(2) = +0 \times^\sharp +0$$
$$\alpha(-1 \times 0) = \theta = \alpha(-1) \times^\sharp \alpha(0) = -0 \times^\sharp \theta$$
$$\alpha(-1 \times 2) = -0 = \alpha(-1) \times^\sharp \alpha(2) = -0 \times^\sharp +0$$

$$\alpha(1 + 2) = +0 = \alpha(1) +^\sharp \alpha(2) = +0 +^\sharp +0$$
$$\alpha(-1 + 0) = -0 = \alpha(-1) +^\sharp \alpha(0) = -0 +^\sharp \theta$$
$$\alpha(-1 + 2) \neq \top^\pm = \alpha(-1) +^\sharp \alpha(2) = -0 +^\sharp +0$$

$\times^\sharp$	$\bot^\pm$	0	$+0$	-0	$\top^\pm$
$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$
0	$\bot^\pm$	0	0	0	0
$+0$	$\bot^\pm$	0	$+0$	-0	$\top^\pm$
-0	$\bot^\pm$	0	-0	$+0$	$\top^\pm$
$\top^\pm$	$\bot^\pm$	0	$\top^\pm$	$\top^\pm$	$\top^\pm$

$+^\sharp$	$\bot^\pm$	0	$+0$	-0	$\top^\pm$
$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$	$\bot^\pm$
0	$\bot^\pm$	0	$+0$	-0	$\top^\pm$
$+0$	$\bot^\pm$	$+0$	$+0$	$\top^\pm$	$\top^\pm$
-0	$\bot^\pm$	-0	$\top^\pm$	-0	$\top^\pm$
$\top^\pm$	$\bot^\pm$	0	$\top^\pm$	$\top^\pm$	$\top^\pm$



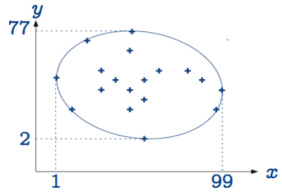
$$\alpha(1 \times 2) = +0 = \alpha(1) \times^\sharp \alpha(2) = +0 \times^\sharp +0$$
$$\alpha(-1 \times 0) = 0 = \alpha(-1) \times^\sharp \alpha(0) = -0 \times^\sharp 0$$
$$\alpha(-1 \times 2) = -0 = \alpha(-1) \times^\sharp \alpha(2) = -0 \times^\sharp +0$$

$$\alpha(1 + 2) = +0 = \alpha(1) +^\sharp \alpha(2) = +0 +^\sharp +0$$
$$\alpha(-1 + 0) = -0 = \alpha(-1) +^\sharp \alpha(0) = -0 +^\sharp 0$$
$$\alpha(-1 + 2) \neq \top^\pm = \alpha(-1) +^\sharp \alpha(2) = -0 +^\sharp +0$$

Abstract operations may lose precision during computation!

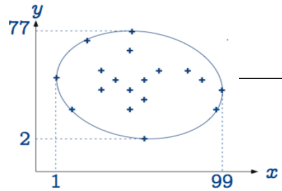
Abstraction: graphical example

Encode a set of points in $\mathbb{R}^2$ into an (integer) interval



Abstraction: graphical example

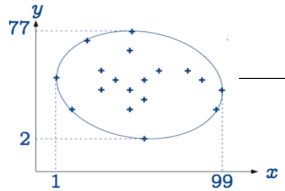
Encode a set of points in $\mathbb{R}^2$ into an (integer) interval



$\xrightarrow{\alpha}$ $\{ x \mapsto [1, 99],\ y \mapsto [2, 77] \}$

Abstraction: graphical example

Encode a set of points in $\mathbb{R}^2$ into an (integer) interval



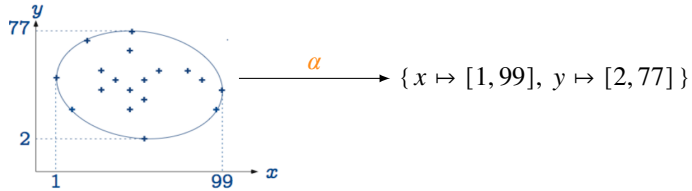
$\xrightarrow{\alpha}$ $\{ x \mapsto [1, 99],\ y \mapsto [2, 77] \}$

Decode an (integer) interval into a set of points in $\mathbb{R}^2$

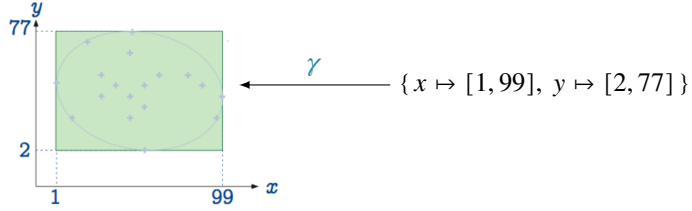
$\{ x \mapsto [1, 99],\ y \mapsto [2, 77] \}$

Abstraction: graphical example

Encode a set of points in $\mathbb{R}^2$ into an (integer) interval

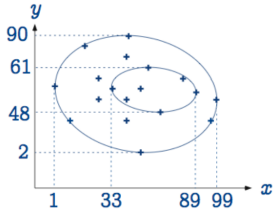


Decode an (integer) interval into a set of points in $\mathbb{R}^2$



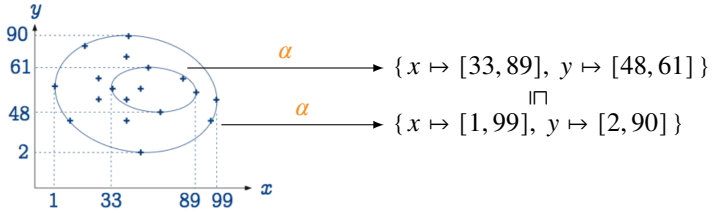
Abstraction: graphical example (Cont'd)

The abstraction α is monotone: $S_1 \subseteq S_2 \Rightarrow \alpha(S_1) \sqsubseteq \alpha(S_2)$



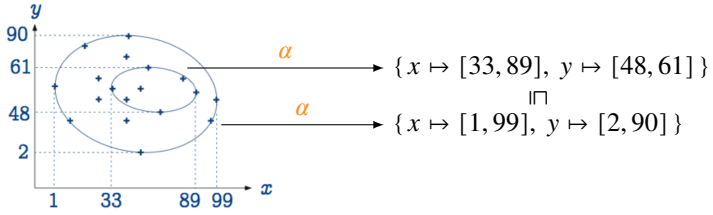
Abstraction: graphical example (Cont'd)

The abstraction α is monotone: $S_1 \subseteq S_2 \Rightarrow \alpha(S_1) \sqsubseteq \alpha(S_2)$



Abstraction: graphical example (Cont'd)

The abstraction α is monotone: $S_1 \subseteq S_2 \Rightarrow \alpha(S_1) \sqsubseteq \alpha(S_2)$

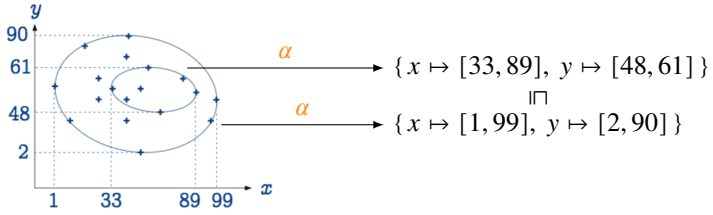


The concretization γ is monotone: $I_1 \sqsubseteq I_2 \Rightarrow \gamma(I_1) \subseteq \gamma(I_2)$

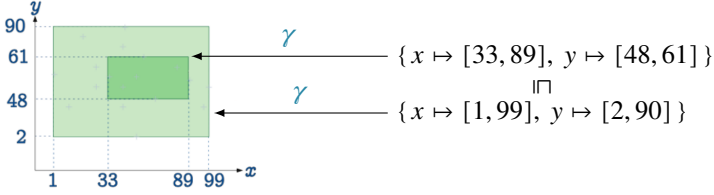
$$\{ x \mapsto [33, 89],\ y \mapsto [48, 61] \}$$
$$\sqsubseteq$$
$$\{ x \mapsto [1, 99],\ y \mapsto [2, 90] \}$$

Abstraction: graphical example (Cont'd)

The abstraction α is monotone: $S_1 \subseteq S_2 \Rightarrow \alpha(S_1) \sqsubseteq \alpha(S_2)$

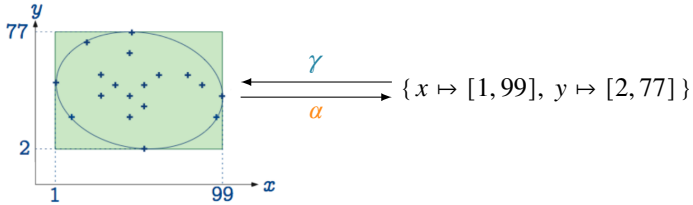


The concretization γ is monotone: $I_1 \sqsubseteq I_2 \Rightarrow \gamma(I_1) \subseteq \gamma(I_2)$

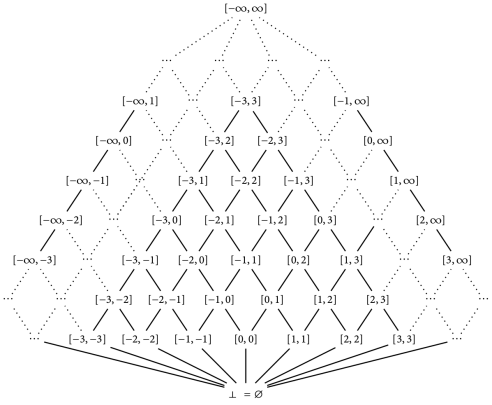


Abstraction: graphical example (Cont'd)

The composition $\gamma \circ \alpha$ is extensive: $S \subseteq \gamma\,\alpha(S)$

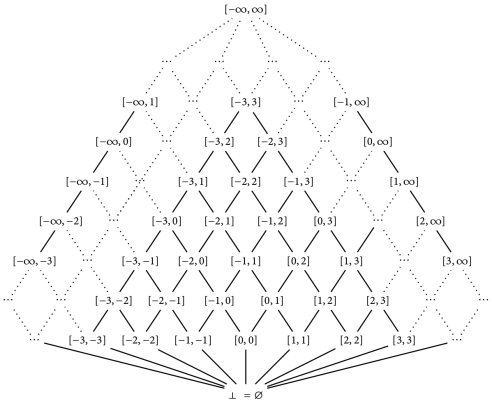


Bounded integer intervals $\langle (\mathbb{Z} \cup \{-\infty\}) \times (\mathbb{Z} \cup \{\infty\}), \sqsubseteq, \sqcup, \sqcap, \bot, \top \rangle$



Bounded integer intervals $\langle (\mathbb{Z} \cup \{-\infty\}) \times (\mathbb{Z} \cup \{\infty\}), \sqsubseteq, \sqcup, \sqcap, \bot, \top \rangle$

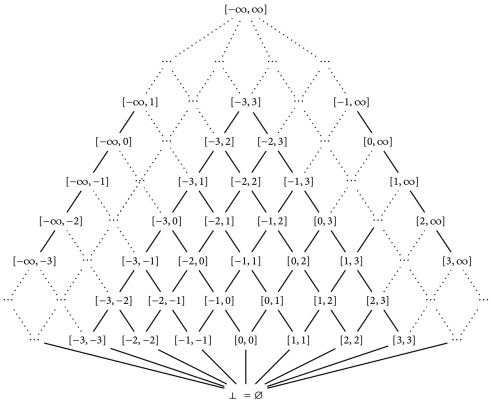
- $[a,b] \sqsubseteq [a',b'] \triangleq a \geq a' \wedge b \leq b'$
- $[a,b] \sqcap [a',b'] \triangleq \left(\max\{a,a'\} \leq \min\{b,b'\} \ ? \ [\max\{a,a'\}, \min\{b,b'\}] \ : \bot \right)$
- $[a,b] \sqcup [a',b'] \triangleq [\min\{a,a'\}, \max\{b,b'\}]$
- $\bot \triangleq [\infty, -\infty]$ and $\top \triangleq [-\infty, \infty]$



Bounded integer intervals $\langle (\mathbb{Z} \cup \{-\infty\}) \times (\mathbb{Z} \cup \{\infty\}), \sqsubseteq, \sqcup, \sqcap, \bot, \top \rangle$

- $[a,b] \sqsubseteq [a',b'] \triangleq a \geq a' \wedge b \leq b'$
- $[a,b] \sqcap [a',b'] \triangleq \left(\max\{a,a'\} \leq \min\{b,b'\} \; ? \; [\max\{a,a'\}, \min\{b,b'\}] \; : \; \bot \right)$
- $[a,b] \sqcup [a',b'] \triangleq [\min\{a,a'\}, \max\{b,b'\}]$
- $\bot \triangleq [\infty, -\infty]$ and $\top \triangleq [-\infty, \infty]$

Abstraction $\alpha \triangleq \lambda X \,.\, \left(X = \emptyset \; ? \; \bot \; : \; [\min X, \max X] \right)$

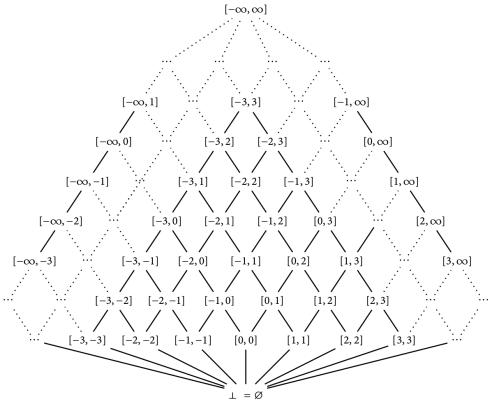


Bounded integer intervals $\langle (\mathbb{Z} \cup \{-\infty\}) \times (\mathbb{Z} \cup \{\infty\}), \sqsubseteq, \sqcup, \sqcap, \bot, \top \rangle$

- $[a,b] \sqsubseteq [a',b'] \triangleq a \geq a' \wedge b \leq b'$
- $[a,b] \sqcap [a',b'] \triangleq \left(\max\{a,a'\} \leq \min\{b,b'\} \; ? \; [\max\{a,a'\}, \min\{b,b'\}] \; : \; \bot \right)$
- $[a,b] \sqcup [a',b'] \triangleq [\min\{a,a'\}, \max\{b,b'\}]$
- $\bot \triangleq [\infty, -\infty]$ and $\top \triangleq [-\infty, \infty]$

Abstraction $\alpha \triangleq \lambda X \,.\, \left(X = \emptyset \; ? \; \bot \; : \; [\min X, \max X] \right)$

Concretization $\gamma \triangleq \lambda [a,b] \,.\, \{z \in \mathbb{Z} \mid a \leq z \leq b\}$



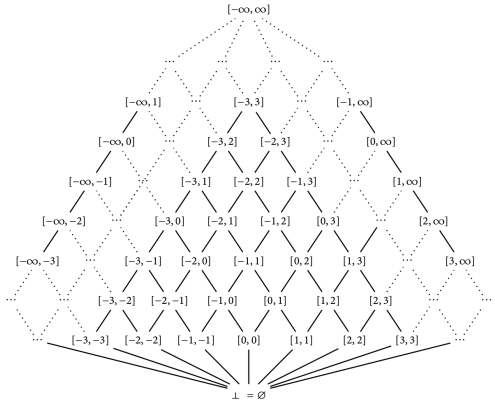
Bounded integer intervals $\langle (\mathbb{Z} \cup \{-\infty\}) \times (\mathbb{Z} \cup \{\infty\}), \sqsubseteq, \sqcup, \sqcap, \bot, \top \rangle$

- $[a,b] \sqsubseteq [a',b'] \triangleq a \geq a' \wedge b \leq b'$
- $[a,b] \sqcap [a',b'] \triangleq \left(\max\{a,a'\} \leq \min\{b,b'\} \; ? \; [\max\{a,a'\}, \min\{b,b'\}] \; : \; \bot \right)$
- $[a,b] \sqcup [a',b'] \triangleq [\min\{a,a'\}, \max\{b,b'\}]$
- $\bot \triangleq [\infty, -\infty]$ and $\top \triangleq [-\infty, \infty]$

Abstraction $\alpha \triangleq \lambda X \,.\, \left(X = \emptyset \; ? \; \bot \; : \; [\min X, \max X] \right)$

Concretization $\gamma \triangleq \lambda [a,b] \,.\, \{z \in \mathbb{Z} \mid a \leq z \leq b\}$

Galois Connection



The bounded integer intervals abstraction (Cont'd)

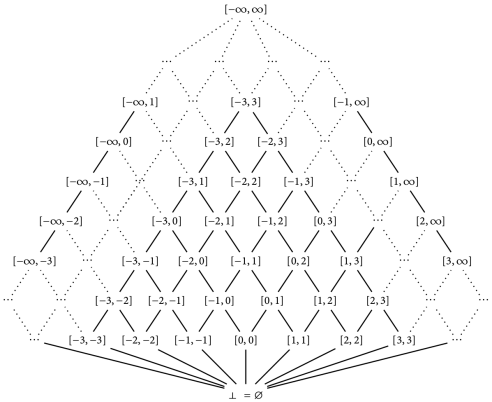
α is not surjective

$\forall a \in A\ \exists c \in C\ .\ \alpha(c) = a$

Abstraction $\alpha \triangleq \lambda X\ .\ (\!|\ X = \emptyset\ ?\ \bot\ :\ [\min X, \max X]\ |\!)$

Concretization $\gamma \triangleq \lambda [a, b]\ .\ \{z \in \mathbb{Z} \mid a \leq z \leq b\}$

Galois Connection



The bounded integer intervals abstraction (Cont'd)

α is not surjective

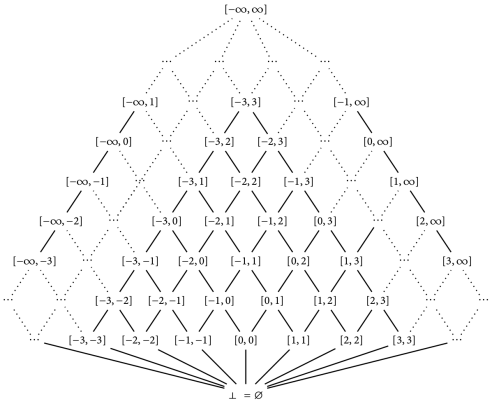
$\forall a \in A\ \exists c \in C\ .\ \alpha(c) = a$

$[3,1] \in (\mathbb{Z} \cup \{-\infty\}) \times (\mathbb{Z} \cup \{\infty\})$ but $[3,1] \notin \text{image}(\alpha)$

Abstraction $\alpha \triangleq \lambda X\ .\ (\!|\ X = \emptyset\ ?\ \bot\ :\ [\min X, \max X]\ |\!)$

Concretization $\gamma \triangleq \lambda [a,b]\ .\ \{z \in \mathbb{Z} \mid a \le z \le b\}$

Galois Connection



The bounded integer intervals abstraction (Cont'd)

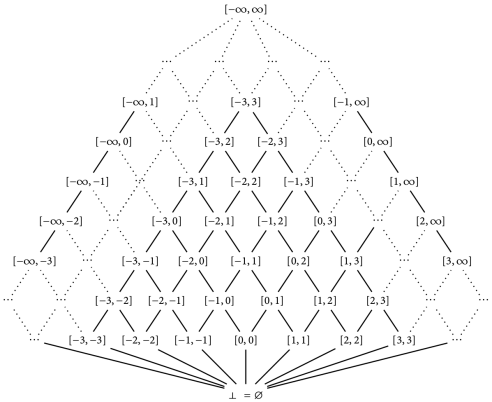
γ is not injective

$$\forall a, a' \in A \,.\, \gamma(a) = \gamma(a') \Rightarrow a = a'$$

Abstraction $\alpha \triangleq \lambda X \,.\, (\!| X = \emptyset \,?\, \bot :? [\min X, \max X] |\!)$

Concretization $\gamma \triangleq \lambda [a, b] \,.\, \{z \in \mathbb{Z} \mid a \leq z \leq b\}$

Galois Connection



The bounded integer intervals abstraction (Cont'd)

γ is not injective

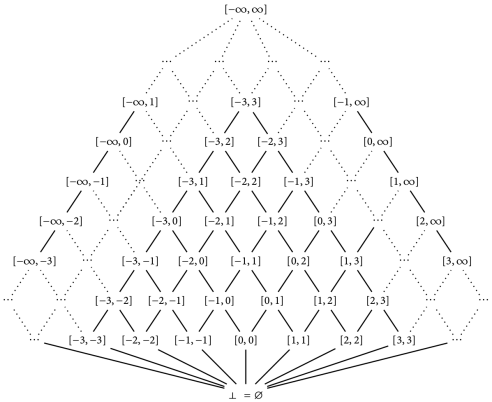
$\forall a, a' \in A \,.\, \gamma(a) = \gamma(a') \Rightarrow a = a'$

$\gamma([3,1]) = \emptyset = \gamma([3,2])$ but $[3,1] \neq [3,2]$

Abstraction $\alpha \triangleq \lambda X \,.\, (\!| X = \emptyset \;?\; \bot \;:\; [\min X, \max X] |\!)$

Concretization $\gamma \triangleq \lambda [a,b] \,.\, \{z \in \mathbb{Z} \mid a \leq z \leq b\}$

Galois Connection



The bounded integer intervals abstraction (Cont'd)

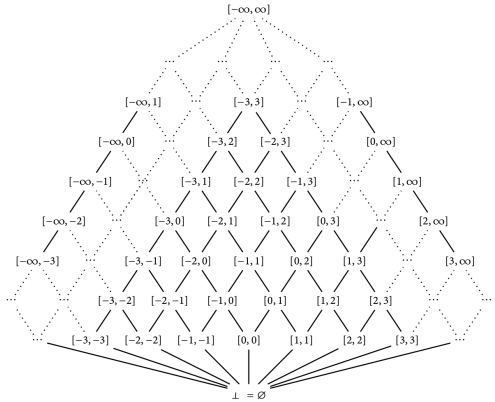
Bounded integer intervals $\langle \{[a,b] \in (\mathbb{Z} \cup \{-\infty\}) \times (\mathbb{Z} \cup \{\infty\}) \mid a \leq b\}, \sqsubseteq, \sqcup, \sqcap, \bot, \top \rangle$

- $[a,b] \sqsubseteq [a',b'] \triangleq a \geq a' \wedge b \leq b'$
- $[a,b] \sqcap [a',b'] \triangleq \left(\max\{a,a'\} \leq \min\{b,b'\} \; ? \; [\max\{a,a'\}, \min\{b,b'\}] \; : \; \bot \right)$
- $[a,b] \sqcup [a',b'] \triangleq [\min\{a,a'\}, \max\{b,b'\}]$
- $\bot \triangleq [\infty, -\infty]$ and $\top \triangleq [-\infty, \infty]$

Abstraction $\alpha \triangleq \lambda X \,.\, \left(X = \emptyset \; ? \; \bot \; : \; [\min X, \max X] \right)$

Concretization $\gamma \triangleq \lambda [a,b] \,.\, \{z \in \mathbb{Z} \mid a \leq z \leq b\}$

Galois Insertion



A Galois Connection can always be made into a Galois Injection

- Given $\langle C, \leqslant_C \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle A, \leqslant_A \rangle$ we can reduce A forcing the surjectivity of α

A Galois Connection can always be made into a Galois Injection

- Given $\langle C, \leqslant_C \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle A, \leqslant_A \rangle$ we can reduce A forcing the surjectivity of α
- We merge the elements in A with the same image under γ by quotienting A:

$$a \equiv a' \triangleq \gamma(a) = \gamma(a')$$

A Galois Connection can always be made into a Galois Injection

- Given $\langle C, \leqslant_C \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle A, \leqslant_A \rangle$ we can reduce A forcing the surjectivity of α
- We merge the elements in A with the same image under γ by quotienting A:

$$a \equiv a' \triangleq \gamma(a) = \gamma(a')$$

The set of equivalence classes $A/_{\equiv} \triangleq \{[a]_{\equiv} \mid a \in A\}$ forms a Galois Injection with C

$$\alpha_{\equiv} \triangleq \lambda c \,.\, [\alpha(c)]_{\equiv} \qquad\qquad \gamma_{\equiv} \triangleq \lambda [a]_{\equiv} \,.\, \gamma(a)$$

A Galois Connection can always be made into a Galois Injection

- Given $\langle C, \leqslant_C \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle A, \leqslant_A \rangle$ we can reduce A forcing the surjectivity of α
- We merge the elements in A with the same image under γ by quotienting A:

$$a \equiv a' \triangleq \gamma(a) = \gamma(a')$$

The set of equivalence classes $A/_{\equiv} \triangleq \{[a]_{\equiv} \mid a \in A\}$ forms a Galois Injection with C

$$\alpha_{\equiv} \triangleq \lambda c \,.\, [\alpha(c)]_{\equiv} \qquad\qquad \gamma_{\equiv} \triangleq \lambda [a]_{\equiv} \,.\, \gamma(a)$$

We have $\langle C, \leqslant_C \rangle \underset{\alpha_{\equiv}}{\overset{\gamma_{\equiv}}{\leftrightarrows}} \langle A/_{\equiv}, \leqslant_{\equiv} \rangle$ where $[a]_{\equiv} \leqslant_{\equiv} [a']_{\equiv} \triangleq a \leqslant_A a'$

Given a concrete $\langle C, \sqsubseteq^c \rangle$ with top element $\top_c$

Given a concrete $\langle C, \sqsubseteq^c \rangle$ with top element $\top_c$

A trivial abstraction for C is:

$$\langle C, \sqsubseteq^c \rangle \underset{\lambda c \,.\, \top_c}{\overset{id}{\leftrightarrows}} \langle \{\top_c\}, = \rangle$$

Given a concrete $\langle C, \sqsubseteq^c \rangle$ with top element $\top_c$

A trivial abstraction for C is:

$$\langle C, \sqsubseteq^c \rangle \underset{\lambda c \,.\, \top_c}{\overset{id}{\leftrightarrows}} \langle \{\top_c\}, = \rangle$$

- This abstraction says nothing about C

Given a concrete $\langle C, \sqsubseteq^c \rangle$ with top element $\top_c$

A trivial abstraction for C is:

$$\langle C, \sqsubseteq^c \rangle \underset{\lambda c \,.\, \top_c}{\overset{id}{\leftrightarrows}} \langle \{\top_c\}, = \rangle$$

- This abstraction says nothing about C

Another trivial abstraction for C is:

$$\langle C, \sqsubseteq^c \rangle \underset{id}{\overset{id}{\leftrightarrows}} \langle C, \sqsubseteq^c \rangle$$

Given a concrete $\langle C, \sqsubseteq^c \rangle$ with top element $\top_c$

A trivial abstraction for C is:

- This abstraction says nothing about C

$$\langle C, \sqsubseteq^c \rangle \underset{\lambda c\,.\,\top_c}{\overset{id}{\leftrightarrows}} \langle \{\top_c\}, = \rangle$$

Another trivial abstraction for C is:

- This abstraction says everything about C

$$\langle C, \sqsubseteq^c \rangle \underset{id}{\overset{id}{\leftrightarrows}} \langle C, \sqsubseteq^c \rangle$$

Given two abstractions $\langle \mathrm{C}, \sqsubseteq^c \rangle \underset{\gamma_a}{\overset{\alpha_a}{\leftrightarrows}} \langle \mathrm{A}, \sqsubseteq^a \rangle$ and $\langle \mathrm{C}, \sqsubseteq^c \rangle \underset{\gamma_b}{\overset{\alpha_b}{\leftrightarrows}} \langle \mathrm{B}, \sqsubseteq^b \rangle$ of C

Given two abstractions $\langle \mathrm{C}, \sqsubseteq^c \rangle \underset{\gamma_a}{\overset{\alpha_a}{\leftrightarrows}} \langle \mathrm{A}, \sqsubseteq^a \rangle$ and $\langle \mathrm{C}, \sqsubseteq^c \rangle \underset{\gamma_b}{\overset{\alpha_b}{\leftrightarrows}} \langle \mathrm{B}, \sqsubseteq^b \rangle$ of C

We say that A is more precise than B when

$$\forall b \in B \, \exists a \in A \, . \, \gamma_b(b) = \gamma_a(a)$$

In other words, A is more precise than B when $\{\gamma_b(b) \mid b \in B\} \subseteq \{\gamma_a(a) \mid a \in A\}$

Given two abstractions $\langle C, \sqsubseteq^c \rangle \underset{\gamma_a}{\overset{\alpha_a}{\leftrightarrows}} \langle A, \sqsubseteq^a \rangle$ and $\langle C, \sqsubseteq^c \rangle \underset{\gamma_b}{\overset{\alpha_b}{\leftrightarrows}} \langle B, \sqsubseteq^b \rangle$ of C

We say that A is more precise than B when

$$\forall b \in B \, \exists a \in A \, . \, \gamma_b(b) = \gamma_a(a)$$

In other words, A is more precise than B when $\{\gamma_b(b) \mid b \in B\} \subseteq \{\gamma_a(a) \mid a \in A\}$

Prove that $\langle \{\top_c\}, = \rangle$ is the less precise abstraction of C

Abstract Computation

$$\langle C, \sqsubseteq^c \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle A, \sqsubseteq^a \rangle$$

What we ideally want compute: a concrete function $f : C \to C$ on $\langle C, \sqsubseteq^c \rangle$

$$\langle C, \sqsubseteq^c \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle A, \sqsubseteq^a \rangle$$

What we ideally want compute: a concrete function $f : C \to C$ on $\langle C, \sqsubseteq^c \rangle$

$$\langle C, \sqsubseteq^c \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle A, \sqsubseteq^a \rangle$$

What we actually can compute: an abstract function $f^\sharp : A \to A$ on $\langle A, \sqsubseteq^a \rangle$

What we ideally want compute: a concrete function $f : C \to C$ on $\langle C, \sqsubseteq^c \rangle$

$$\langle C, \sqsubseteq^c \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle A, \sqsubseteq^a \rangle$$

What we actually can compute: an abstract function $f^\sharp : A \to A$ on $\langle A, \sqsubseteq^a \rangle$

Idea: mimic concrete computation (f) on on abstract elements (on A)

What we ideally want compute: a concrete function $f : C \to C$ on $\langle C, \sqsubseteq^c \rangle$

$$\langle C, \sqsubseteq^c \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle A, \sqsubseteq^a \rangle$$

What we actually can compute: an abstract function $f^\sharp : A \to A$ on $\langle A, \sqsubseteq^a \rangle$

Idea: mimic concrete computation (f) on on abstract elements (on A)

Note: we usually aim at computing the fixpoints of f (and $f^\sharp$)

The abstract computation must be sound (i.e., correct):

The abstract computation must be sound (i.e., correct):

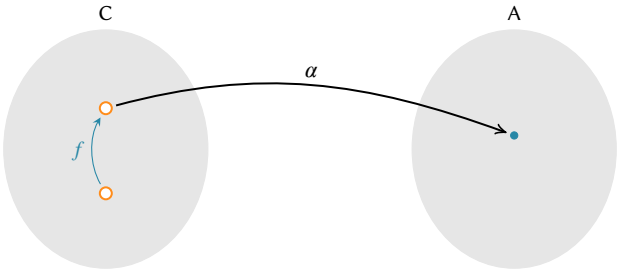
$$\forall c \in \mathbf{C} \,.\, \alpha \circ f(c) \sqsubseteq^{a} f^{\sharp} \circ \alpha(c)$$

The abstract computation must be sound (i.e., correct):

$$\forall c \in \mathsf{C} \,.\, \alpha \circ f(c) \sqsubseteq^{a} f^{\sharp} \circ \alpha(c)$$

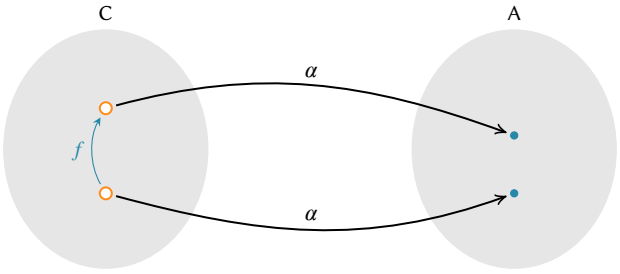
The abstract computation must be sound (i.e., correct):

$$\forall c \in \mathbf{C} \,.\, \alpha \circ f(c) \sqsubseteq^{a} f^{\sharp} \circ \alpha(c)$$



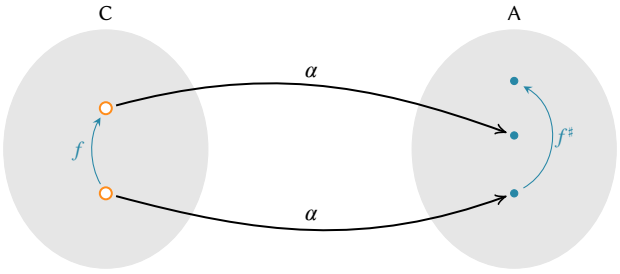
The abstract computation must be sound (i.e., correct):

$$\forall c \in \mathbf{C} \,.\, \alpha \circ f(c) \sqsubseteq^{a} f^{\sharp} \circ \alpha(c)$$



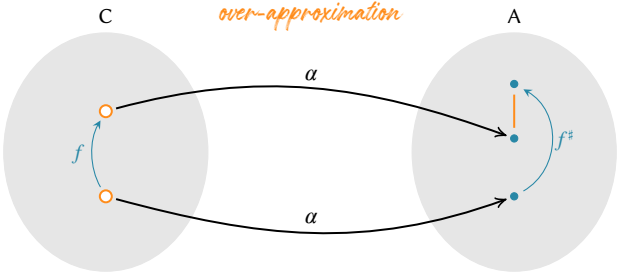
The abstract computation must be sound (i.e., correct):

$$\forall c \in \mathbf{C} \,.\, \alpha \circ f(c) \sqsubseteq^{a} f^{\sharp} \circ \alpha(c)$$



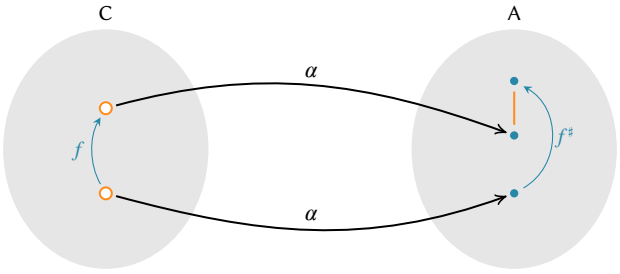
The abstract computation must be sound (i.e., correct):

$$\forall c \in \mathbf{C} \,.\, \alpha \circ f(c) \sqsubseteq^{a} f^{\sharp} \circ \alpha(c)$$



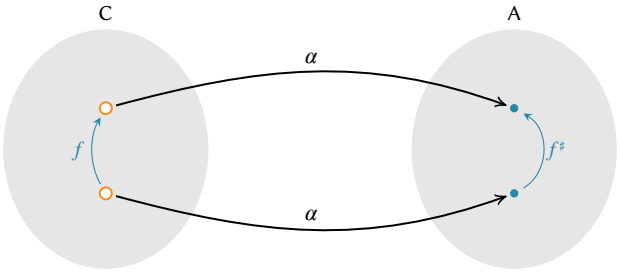
The abstract computation may be complete (i.e., precise):

$$\forall c \in \mathsf{C} \,.\, \alpha \circ f(c) = f^\sharp \circ (c)$$



The abstract computation may be complete (i.e., precise):

$$\forall c \in \mathsf{C} \,.\, \alpha \circ f(c) = f^\sharp \circ (c)$$



Given a concrete function $f : \mathsf{C} \to \mathsf{C}$ on $\langle \mathsf{C}, \sqsubseteq^{c} \rangle$, then

Given a concrete function $f : \mathsf{C} \to \mathsf{C}$ on $\langle \mathsf{C}, \sqsubseteq^{c} \rangle$, then

$$f^{bca} \triangleq \alpha \circ f \circ \gamma : \mathsf{A} \to \mathsf{A}$$

is the best correct approximation of f (in A)

Given a concrete function $f : \mathrm{C} \to \mathrm{C}$ on $\langle \mathrm{C}, \sqsubseteq^{c} \rangle$, then

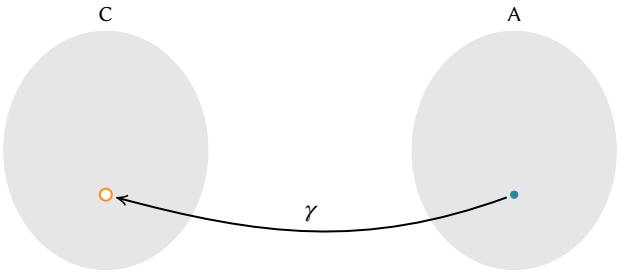
$$f^{bca} \triangleq \alpha \circ f \circ \gamma : \mathrm{A} \to \mathrm{A}$$

is the best correct approximation of f (in A)

Given a concrete function $f : \mathsf{C} \to \mathsf{C}$ on $\langle \mathsf{C}, \sqsubseteq^{c} \rangle$, then

$$f^{bca} \triangleq \alpha \circ f \circ \gamma : \mathsf{A} \to \mathsf{A}$$

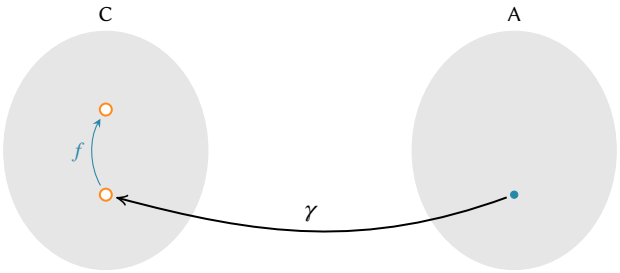
is the best correct approximation of f (in A)



Given a concrete function $f : \mathsf{C} \to \mathsf{C}$ on $\langle \mathsf{C}, \sqsubseteq^{c} \rangle$, then

$$f^{bca} \triangleq \alpha \circ f \circ \gamma : \mathsf{A} \to \mathsf{A}$$

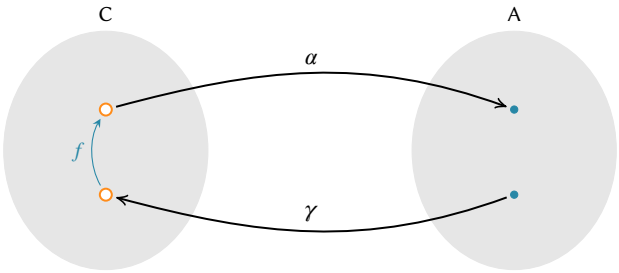
is the best correct approximation of f (in A)



Given a concrete function $f : \mathsf{C} \to \mathsf{C}$ on $\langle \mathsf{C}, \sqsubseteq^{c} \rangle$, then

$$f^{bca} \triangleq \alpha \circ f \circ \gamma : \mathsf{A} \to \mathsf{A}$$

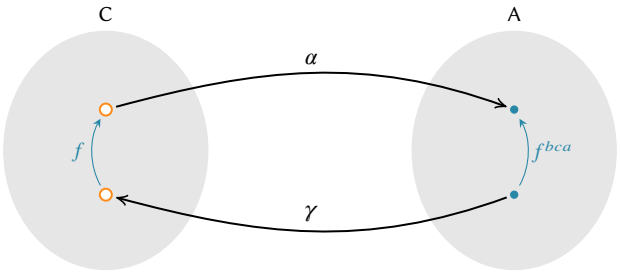
is the best correct approximation of f (in A)



Given a concrete function $f : \mathsf{C} \to \mathsf{C}$ on $\langle \mathsf{C}, \sqsubseteq^{c} \rangle$, then

$$f^{bca} \triangleq \alpha \circ f \circ \gamma : \mathsf{A} \to \mathsf{A}$$

is the best correct approximation of f (in A)



We have that f^{bca} is correct by construction, and it is the best possible approximation of f

Best correct approximation (Cont'd)

We have that f^{bca} is correct by construction, and it is the best possible approximation of f

- Any correct approximation $f^\sharp$ of f (in A) cannot be more precise than f^{bca}

$$f^{bca} \dot{\sqsubseteq}^a f^\sharp \qquad \text{for any sound } f^\sharp$$

Best correct approximation (Cont'd)

We have that f^{bca} is correct by construction, and it is the best possible approximation of f

- Any correct approximation $f^\sharp$ of f (in A) cannot be more precise than f^{bca}

$$f^{bca} \dot{\sqsubseteq}^a f^\sharp \quad \text{for any sound } f^\sharp$$

- There exists $f^\sharp$ complete for f (in A) if and only if f^{bca} is complete for f

We are interested in the fixpoints of $f : C \to C$ (usually the least one)

We are interested in the fixpoints of $f : C \to C$ (usually the least one)

- $\mathrm{lfp} f$ is not computable, in general

We are interested in the fixpoints of $f : C \to C$ (usually the least one)

- $\mathrm{lfp} f$ is not computable, in general
- Define an abstraction $\langle C, \sqsubseteq^c \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle A, \sqsubseteq^a \rangle$

We are interested in the fixpoints of $f : C \to C$ (usually the least one)

- $\mathrm{lfp} f$ is not computable, in general
- Define an abstraction $\langle C, \sqsubseteq^c \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle A, \sqsubseteq^a \rangle$
- Define an abstract version $f^\sharp : A \to A$ of f

We are interested in the fixpoints of $f : C \to C$ (usually the least one)

- $\mathrm{lfp} f$ is not computable, in general
- Define an abstraction $\langle C, \sqsubseteq^c \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle A, \sqsubseteq^a \rangle$
- Define an abstract version $f^\sharp : A \to A$ of f
- Compute $\mathrm{lfp} f^\sharp$

We are interested in the fixpoints of $f : C \to C$ (usually the least one)

- $\mathrm{lfp} f$ is not computable, in general
- Define an abstraction $\langle C, \sqsubseteq^c \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle A, \sqsubseteq^a \rangle$
- Define an abstract version $f^\sharp : A \to A$ of f
- Compute $\mathrm{lfp} f^\sharp$

The (fixpoint) abstraction must be sound: $\alpha(\mathrm{lfp} f) \sqsubseteq^a \mathrm{lfp} f^\sharp$ $\qquad \mathrm{lfp} f \sqsubseteq^c \gamma(\mathrm{lfp} f^\sharp)$

We are interested in the fixpoints of $f : C \to C$ (usually the least one)

- $\mathrm{lfp} f$ is not computable, in general
- Define an abstraction $\langle C, \sqsubseteq^c \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle A, \sqsubseteq^a \rangle$
- Define an abstract version $f^\sharp : A \to A$ of f
- Compute $\mathrm{lfp} f^\sharp$

The (fixpoint) abstraction must be sound: $\alpha(\mathrm{lfp} f) \sqsubseteq^a \mathrm{lfp} f^\sharp$ $\qquad \mathrm{lfp} f \sqsubseteq^c \gamma(\mathrm{lfp} f^\sharp)$

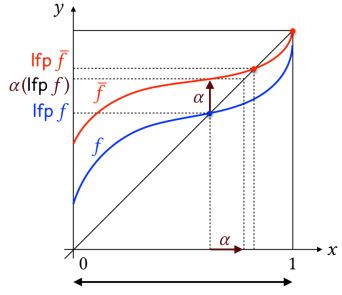
Sometimes the abstraction is exact (or complete): $\alpha(\mathrm{lfp} f) = \mathrm{lfp} f^\sharp$

THEOREM :: Point-wise Fixpoint Over-approximation

Given two monotonic functions $f, \overline{f} : \mathscr{S} \to \mathscr{S}$ on a complete lattice $\langle \mathscr{S}, \sqsubseteq, \sqcup, \sqcap, \bot, \top \rangle$, if $f \dot{\sqsubseteq} \overline{f}$ then $\mathrm{lfp}\, f \sqsubseteq \mathrm{lfp}\, \overline{f}$.

THEOREM :: Point-wise Fixpoint Over-approximation

Given two monotonic functions $f, \overline{f} : \mathscr{S} \to \mathscr{S}$ on a complete lattice $\langle \mathscr{S}, \sqsubseteq, \sqcup, \sqcap, \bot, \top \rangle$, if $f \mathrel{\dot{\sqsubseteq}} \overline{f}$ then $\mathrm{lfp}\, f \sqsubseteq \mathrm{lfp}\, \overline{f}$.

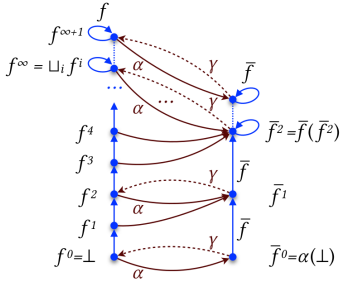


THEOREM :: Bca Fixpoint Over-approximation

Consider a monotonic function $f : \mathscr{S} \to \mathscr{S}$ on a complete lattice $\langle \mathscr{S}, \sqsubseteq \rangle$ and a Galois Connection $\langle \mathscr{S}, \sqsubseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathscr{L}, \preccurlyeq \rangle$, with $\langle \mathscr{L}, \preccurlyeq \rangle$ complete lattice. Then $\mathrm{lfp}^{\sqsubseteq} f \sqsubseteq \gamma(\mathrm{lfp}^{\preccurlyeq}\ \alpha \circ f \circ \gamma)$.

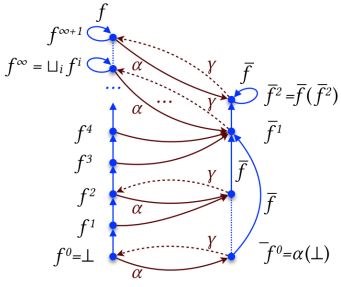
THEOREM :: Bca Fixpoint Over-approximation

Consider a monotonic function $f : \mathscr{S} \to \mathscr{S}$ on a complete lattice $\langle \mathscr{S}, \sqsubseteq \rangle$ and a Galois Connection $\langle \mathscr{S}, \sqsubseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathscr{L}, \preccurlyeq \rangle$, with $\langle \mathscr{L}, \preccurlyeq \rangle$ complete lattice. Then $\mathrm{lfp}^{\sqsubseteq} f \sqsubseteq \gamma(\mathrm{lfp}^{\preccurlyeq}\ \alpha \circ f \circ \gamma)$.



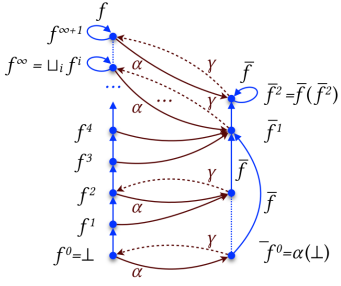
THEOREM :: Correct Fixpoint Over-approximation

Consider two monotonic functions $f : \mathscr{S} \to \mathscr{S}$ and $\overline{f} : \mathscr{L} \to \mathscr{L}$ on the complete lattices $\langle \mathscr{S}, \sqsubseteq \rangle$ and $\langle \mathscr{L}, \preccurlyeq \rangle$ such that $\langle \mathscr{S}, \sqsubseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathscr{L}, \preccurlyeq \rangle$ and $\alpha \circ f \circ \gamma \mathrel{\dot{\preccurlyeq}} \overline{f}$. Then $\mathrm{lfp}^{\sqsubseteq} f \sqsubseteq \gamma(\mathrm{lfp}^{\preccurlyeq} \overline{f})$.



THEOREM :: Correct Fixpoint Over-approximation

Consider two monotonic functions $f : \mathscr{S} \to \mathscr{S}$ and $\overline{f} : \mathscr{L} \to \mathscr{L}$ on the complete lattices $\langle \mathscr{S}, \sqsubseteq \rangle$ and $\langle \mathscr{L}, \preccurlyeq \rangle$ such that $\langle \mathscr{S}, \sqsubseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathscr{L}, \preccurlyeq \rangle$ and $\alpha \circ f \mathrel{\dot{\preccurlyeq}} \overline{f} \circ \alpha$. Then $\mathrm{lfp}^{\sqsubseteq} f \sqsubseteq \gamma(\mathrm{lfp}^{\preccurlyeq} \overline{f})$.

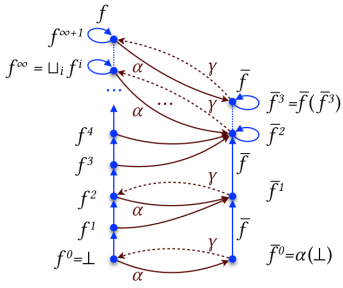


THEOREM :: Exact Fixpoint Over-approximation

Consider two monotonic functions $f : \mathscr{S} \to \mathscr{S}$ and $\overline{f} : \mathscr{L} \to \mathscr{L}$ on the complete lattices $\langle \mathscr{S}, \sqsubseteq \rangle$ and $\langle \mathscr{L}, \preccurlyeq \rangle$ such that $\langle \mathscr{S}, \sqsubseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathscr{L}, \preccurlyeq \rangle$ and $\alpha \circ f = \overline{f} \circ \alpha$. Then $\mathrm{lfp}^{\sqsubseteq} f = \gamma(\mathrm{lfp}^{\preccurlyeq} \overline{f})$.

THEOREM :: Exact Fixpoint Over-approximation

Consider two monotonic functions $f : \mathscr{S} \to \mathscr{S}$ and $\overline{f} : \mathscr{L} \to \mathscr{L}$ on the complete lattices $\langle \mathscr{S}, \sqsubseteq \rangle$ and $\langle \mathscr{L}, \preccurlyeq \rangle$ such that $\langle \mathscr{S}, \sqsubseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathscr{L}, \preccurlyeq \rangle$ and $\alpha \circ f = \overline{f} \circ \alpha$. Then $\mathrm{lfp}^{\sqsubseteq} f = \gamma(\mathrm{lfp}^{\preccurlyeq} \overline{f})$.



Fixpoint Acceleration

Computing fixpoints may involve an infinite number of iterations: non-termination

Computing fixpoints may involve an infinite number of iterations: non-termination

- The iteration terminates if the lattice is finite

Computing fixpoints may involve an infinite number of iterations: non-termination

- The iteration terminates if the lattice is finite
- The iteration terminates if the lattice is ACC (no infinite ascending chains)

Computing fixpoints may involve an infinite number of iterations: non-termination

- The iteration terminates if the lattice is finite
- The iteration terminates if the lattice is ACC (no infinite ascending chains)

Even if the iterations are finite in number, their computation can be practically intractable

Computing fixpoints may involve an infinite number of iterations: non-termination

- The iteration terminates if the lattice is finite
- The iteration terminates if the lattice is ACC (no infinite ascending chains)

Even if the iterations are finite in number, their computation can be practically intractable

Idea: exploit fixpoint extrapolation

Computing fixpoints may involve an infinite number of iterations: non-termination

- The iteration terminates if the lattice is finite
- The iteration terminates if the lattice is ACC (no infinite ascending chains)

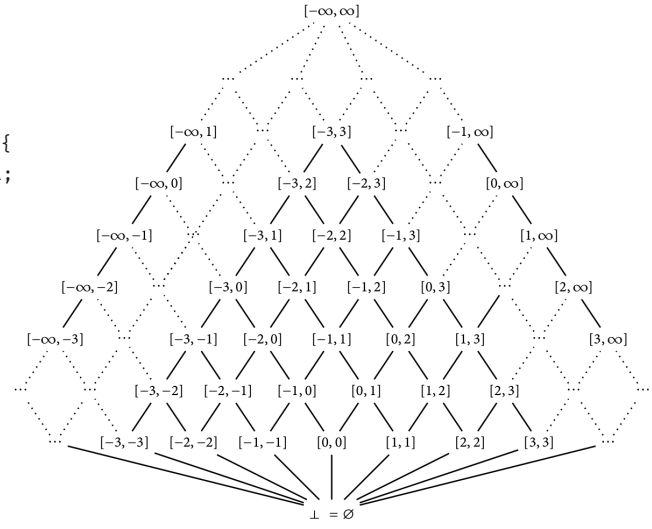
Even if the iterations are finite in number, their computation can be practically intractable

Idea: exploit fixpoint extrapolation

- To force iteration termination
- To speed-up iteration computation

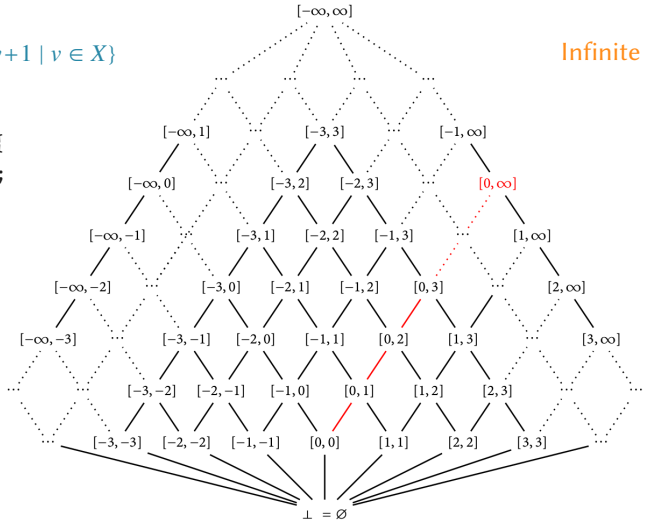
Infinite iterations: example


```
1 x = 0;
2 while (true) {
3   x = x + 1;
4 }
```



$f \triangleq \lambda X\,.\,\{0\} \cup \{v+1 \mid v \in X\}$

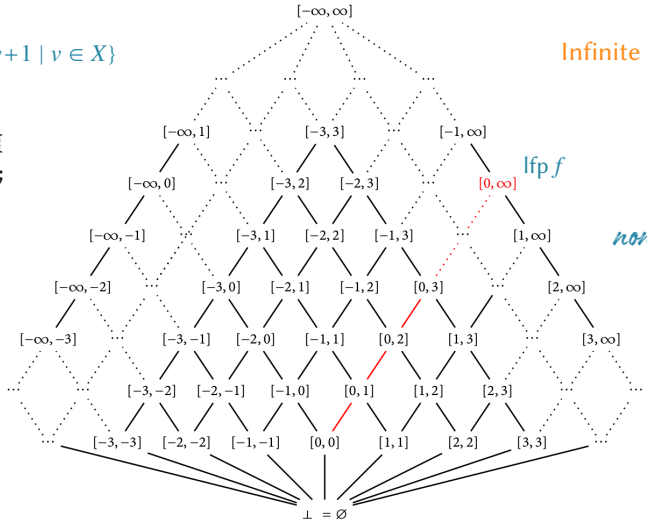
```
1 x = 0;
2 while (true) {
3     x = x + 1;
4 }
```



Infinite ascending chain

$f \triangleq \lambda X\,.\,\{0\} \cup \{v+1 \mid v \in X\}$

```
1 x = 0;
2 while (true) {
3   x = x + 1;
4 }
```



Infinite ascending chain

lfp f

non-termination

Idea: extrapolate from subsequent iterates f^n and f^{n+1} to an upper bound $f^n \nabla f^{n+1}$

Widening operator $\nabla : \mathcal{L} \times \mathcal{L} \to \mathcal{L}$

Idea: extrapolate from subsequent iterates f^n and f^{n+1} to an upper bound $f^n \nabla f^{n+1}$

Widening operator $\nabla : \mathscr{L} \times \mathscr{L} \to \mathscr{L}$

Idea: extrapolate from subsequent iterates f^n and f^{n+1} to an upper bound $f^n \nabla f^{n+1}$

- Accelerate or enforce the convergence of the iterates in finitely many steps

Widening operator $\nabla : \mathcal{L} \times \mathcal{L} \to \mathcal{L}$

Idea: extrapolate from subsequent iterates f^n and f^{n+1} to an upper bound $f^n \nabla f^{n+1}$

- Accelerate or enforce the convergence of the iterates in finitely many steps
- Unavoidable loss of precision

Widening operator $\nabla : \mathscr{L} \times \mathscr{L} \to \mathscr{L}$

Idea: extrapolate from subsequent iterates f^n and f^{n+1} to an upper bound $f^n \nabla f^{n+1}$

- Accelerate or enforce the convergence of the iterates in finitely many steps
- Unavoidable loss of precision

Rationale: a sound although imprecise answer is better than no answer at all

Given a poset $\langle \mathscr{L}, \sqsubseteq \rangle$, a widening operator $\nabla : \mathscr{L} \times \mathscr{L} \to \mathscr{L}$ must satisfy:

Given a poset $\langle \mathscr{L}, \sqsubseteq \rangle$, a widening operator $\nabla : \mathscr{L} \times \mathscr{L} \to \mathscr{L}$ must satisfy:

- For any $a, b \in \mathscr{L}$, it must be that $a \sqsubseteq a \nabla b$ and $b \sqsubseteq a \nabla b$

Given a poset $\langle \mathscr{L}, \sqsubseteq \rangle$, a widening operator $\nabla : \mathscr{L} \times \mathscr{L} \to \mathscr{L}$ must satisfy:

- For any $a, b \in \mathscr{L}$, it must be that $a \sqsubseteq a \nabla b$ and $b \sqsubseteq a \nabla b$

In other words, ∇ computes upper bounds

Given a poset $\langle \mathscr{L}, \sqsubseteq \rangle$, a widening operator $\nabla : \mathscr{L} \times \mathscr{L} \to \mathscr{L}$ must satisfy:

- For any $a, b \in \mathscr{L}$, it must be that $a \sqsubseteq a \nabla b$ and $b \sqsubseteq a \nabla b$
- For all infinite ascending chains $a_1 \sqsubseteq a_2 \sqsubseteq \ldots \sqsubseteq a_n \sqsubseteq \ldots$ in $\mathscr{L}$, the ascending chain $b_0 \triangleq a_0 \sqsubseteq b_1 = b_0 \nabla a_1 \sqsubseteq \ldots \sqsubseteq b_n \triangleq b_{n-1} \nabla a_n \sqsubseteq \ldots$ stabilizes in a finite number of steps

In other words, ∇ computes upper bounds

Given a poset $\langle \mathscr{L}, \sqsubseteq \rangle$, a widening operator $\nabla : \mathscr{L} \times \mathscr{L} \to \mathscr{L}$ must satisfy:

- For any $a, b \in \mathscr{L}$, it must be that $a \sqsubseteq a \nabla b$ and $b \sqsubseteq a \nabla b$
- For all infinite ascending chains $a_1 \sqsubseteq a_2 \sqsubseteq \ldots \sqsubseteq a_n \sqsubseteq \ldots$ in $\mathscr{L}$, the ascending chain $b_0 \triangleq a_0 \sqsubseteq b_1 = b_0 \nabla a_1 \sqsubseteq \ldots \sqsubseteq b_n \triangleq b_{n-1} \nabla a_n \sqsubseteq \ldots$ stabilizes in a finite number of steps

In other words, ∇ computes upper bounds and $\exists k \in \mathbb{N}$ such that $b_k = b_{k-1}$

Given a poset $\langle \mathscr{L}, \sqsubseteq \rangle$, a widening operator $\nabla : \mathscr{L} \times \mathscr{L} \to \mathscr{L}$ must satisfy:

- For any $a, b \in \mathscr{L}$, it must be that $a \sqsubseteq a \nabla b$ and $b \sqsubseteq a \nabla b$
- For all infinite ascending chains $a_1 \sqsubseteq a_2 \sqsubseteq \ldots \sqsubseteq a_n \sqsubseteq \ldots$ in $\mathscr{L}$, the ascending chain $b_0 \triangleq a_0 \sqsubseteq b_1 = b_0 \nabla a_1 \sqsubseteq \ldots \sqsubseteq b_n \triangleq b_{n-1} \nabla a_n \sqsubseteq \ldots$ stabilizes in a finite number of steps

In other words, ∇ computes upper bounds and $\exists k \in \mathbb{N}$ such that $b_k = b_{k-1}$

$$f^0 \quad \sqsubseteq \quad f^1 \quad \sqsubseteq \quad \cdots \quad \sqsubseteq \quad \cdots \quad \sqsubseteq \quad f^n \quad \sqsubseteq \quad \cdots$$

Given a poset $\langle \mathscr{L}, \sqsubseteq \rangle$, a widening operator $\nabla : \mathscr{L} \times \mathscr{L} \to \mathscr{L}$ must satisfy:

- For any $a, b \in \mathscr{L}$, it must be that $a \sqsubseteq a \nabla b$ and $b \sqsubseteq a \nabla b$
- For all infinite ascending chains $a_1 \sqsubseteq a_2 \sqsubseteq \ldots \sqsubseteq a_n \sqsubseteq \ldots$ in $\mathscr{L}$, the ascending chain $b_0 \triangleq a_0 \sqsubseteq b_1 = b_0 \nabla a_1 \sqsubseteq \ldots \sqsubseteq b_n \triangleq b_{n-1} \nabla a_n \sqsubseteq \ldots$ stabilizes in a finite number of steps

In other words, ∇ computes upper bounds and $\exists k \in \mathbb{N}$ such that $b_k = b_{k-1}$

$$f^0 \quad \sqsubseteq \quad f^1 \quad \sqsubseteq \quad \cdots \quad \sqsubseteq \quad \cdots \quad \sqsubseteq \quad f^n \quad \sqsubseteq \quad \cdots$$

$$w^0 \quad \sqsubseteq \quad w^1 \quad \sqsubseteq \quad \cdots \quad \sqsubseteq \quad w^{n-1} \quad \sqsubseteq \quad w^n \quad \sqsubseteq \quad \cdots$$

Given a poset $\langle \mathscr{L}, \sqsubseteq \rangle$, a widening operator $\nabla : \mathscr{L} \times \mathscr{L} \to \mathscr{L}$ must satisfy:

- For any $a, b \in \mathscr{L}$, it must be that $a \sqsubseteq a \nabla b$ and $b \sqsubseteq a \nabla b$
- For all infinite ascending chains $a_1 \sqsubseteq a_2 \sqsubseteq \ldots \sqsubseteq a_n \sqsubseteq \ldots$ in $\mathscr{L}$, the ascending chain $b_0 \triangleq a_0 \sqsubseteq b_1 = b_0 \nabla a_1 \sqsubseteq \ldots \sqsubseteq b_n \triangleq b_{n-1} \nabla a_n \sqsubseteq \ldots$ stabilizes in a finite number of steps

In other words, ∇ computes upper bounds and $\exists k \in \mathbb{N}$ such that $b_k = b_{k-1}$

$$f^0 \sqsubseteq f^1 \sqsubseteq \cdots \sqsubseteq \cdots \sqsubseteq f^n \sqsubseteq \cdots$$

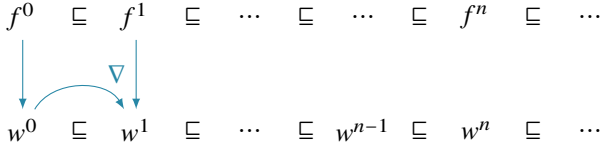
$$\downarrow$$

$$w^0 \sqsubseteq w^1 \sqsubseteq \cdots \sqsubseteq w^{n-1} \sqsubseteq w^n \sqsubseteq \cdots$$

Given a poset $\langle \mathscr{L}, \sqsubseteq \rangle$, a widening operator $\nabla : \mathscr{L} \times \mathscr{L} \to \mathscr{L}$ must satisfy:

- For any $a, b \in \mathscr{L}$, it must be that $a \sqsubseteq a \nabla b$ and $b \sqsubseteq a \nabla b$
- For all infinite ascending chains $a_1 \sqsubseteq a_2 \sqsubseteq \ldots \sqsubseteq a_n \sqsubseteq \ldots$ in $\mathscr{L}$, the ascending chain $b_0 \triangleq a_0 \sqsubseteq b_1 = b_0 \nabla a_1 \sqsubseteq \ldots \sqsubseteq b_n \triangleq b_{n-1} \nabla a_n \sqsubseteq \ldots$ stabilizes in a finite number of steps

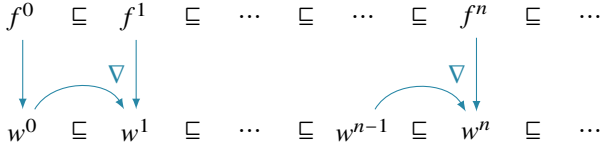
In other words, ∇ computes upper bounds and $\exists k \in \mathbb{N}$ such that $b_k = b_{k-1}$



Given a poset $\langle \mathscr{L}, \sqsubseteq \rangle$, a widening operator $\nabla : \mathscr{L} \times \mathscr{L} \to \mathscr{L}$ must satisfy:

- For any $a, b \in \mathscr{L}$, it must be that $a \sqsubseteq a \nabla b$ and $b \sqsubseteq a \nabla b$
- For all infinite ascending chains $a_1 \sqsubseteq a_2 \sqsubseteq \ldots \sqsubseteq a_n \sqsubseteq \ldots$ in $\mathscr{L}$, the ascending chain $b_0 \triangleq a_0 \sqsubseteq b_1 = b_0 \nabla a_1 \sqsubseteq \ldots \sqsubseteq b_n \triangleq b_{n-1} \nabla a_n \sqsubseteq \ldots$ stabilizes in a finite number of steps

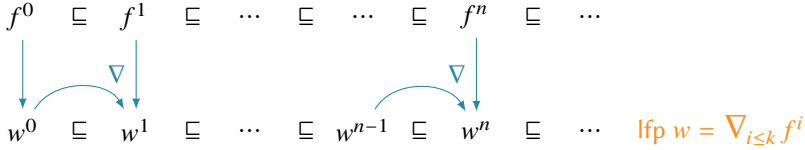
In other words, ∇ computes upper bounds and $\exists k \in \mathbb{N}$ such that $b_k = b_{k-1}$



Given a poset $\langle \mathscr{L}, \sqsubseteq \rangle$, a widening operator $\nabla : \mathscr{L} \times \mathscr{L} \to \mathscr{L}$ must satisfy:

- For any $a, b \in \mathscr{L}$, it must be that $a \sqsubseteq a \nabla b$ and $b \sqsubseteq a \nabla b$
- For all infinite ascending chains $a_1 \sqsubseteq a_2 \sqsubseteq \ldots \sqsubseteq a_n \sqsubseteq \ldots$ in $\mathscr{L}$, the ascending chain $b_0 \triangleq a_0 \sqsubseteq b_1 = b_0 \nabla a_1 \sqsubseteq \ldots \sqsubseteq b_n \triangleq b_{n-1} \nabla a_n \sqsubseteq \ldots$ stabilizes in a finite number of steps

In other words, ∇ computes upper bounds and $\exists k \in \mathbb{N}$ such that $b_k = b_{k-1}$

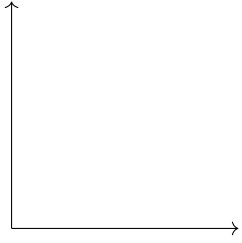


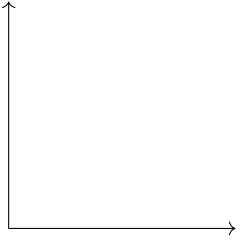
Extrapolate unstable bounds to infinity:

$$\bot \nabla [l, h] \triangleq [l, h] \nabla \bot \triangleq [l, h]$$
$$[l_1, h_1] \nabla [l_2, h_2] \triangleq [(\!| l_2 < l_1 \,?\, -\infty : l_1 |\!), (\!| h_2 > h_1 \,?\, \infty : h_1 |\!)]$$

Extrapolate unstable bounds to infinity:

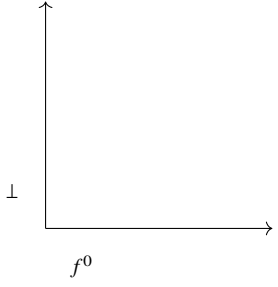
$$\bot \nabla [l,h] \triangleq [l,h] \nabla \bot \triangleq [l,h]$$
$$[l_1,h_1] \nabla [l_2,h_2] \triangleq [(\!| l_2 < l_1 \,?\, -\infty : l_1 |\!), (\!| h_2 > h_1 \,?\, \infty : h_1 |\!)]$$

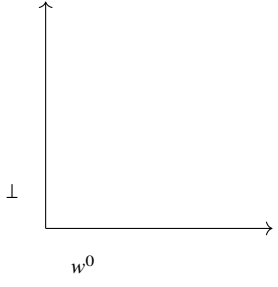




Extrapolate unstable bounds to infinity:

$$\bot \nabla [l,h] \triangleq [l,h] \nabla \bot \triangleq [l,h]$$
$$[l_1,h_1] \nabla [l_2,h_2] \triangleq [(\!| l_2 < l_1 \,?\, -\infty : l_1 |\!), (\!| h_2 > h_1 \,?\, \infty : h_1 |\!)]$$

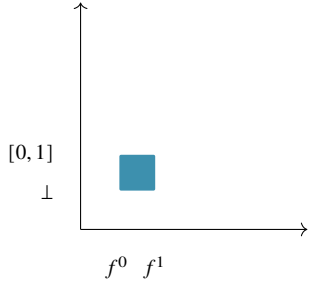


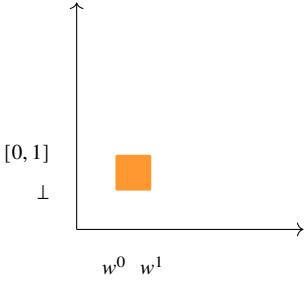


$w^0 = f^0 = \bot$

Extrapolate unstable bounds to infinity:

$$\bot \nabla [l,h] \triangleq [l,h] \nabla \bot \triangleq [l,h]$$
$$[l_1,h_1] \nabla [l_2,h_2] \triangleq [(\!| l_2 < l_1 \,?\, -\infty : l_1 |\!), (\!| h_2 > h_1 \,?\, \infty : h_1 |\!)]$$

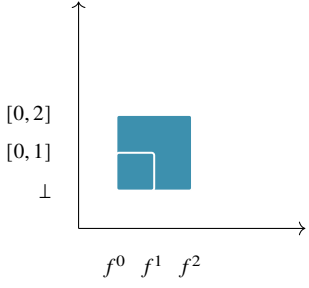


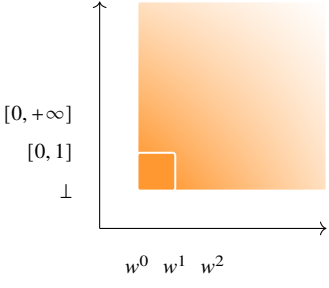


$$w^1 = w^0 \nabla f^1 =$$
$$= \bot \nabla [0,1] = [0,1]$$

Extrapolate unstable bounds to infinity:

$$\bot \nabla [l,h] \triangleq [l,h] \nabla \bot \triangleq [l,h]$$
$$[l_1,h_1] \nabla [l_2,h_2] \triangleq [(\!| l_2 < l_1 \,?\, -\infty : l_1 |\!), (\!| h_2 > h_1 \,?\, \infty : h_1 |\!)]$$

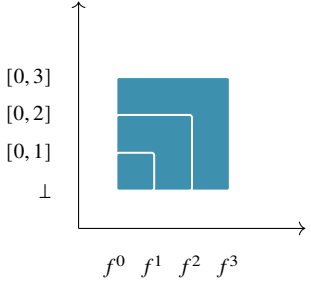


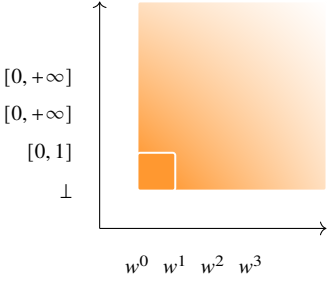


$$w^2 = w^1 \nabla f^2 =$$
$$= [0,1] \nabla [0,2] = [0, +\infty]$$

Extrapolate unstable bounds to infinity:

$$\bot \nabla [l,h] \triangleq [l,h] \nabla \bot \triangleq [l,h]$$
$$[l_1,h_1] \nabla [l_2,h_2] \triangleq [(\!| l_2 < l_1 \,?\, -\infty : l_1 |\!), (\!| h_2 > h_1 \,?\, \infty : h_1 |\!)]$$





$$w^3 = w^2 \nabla f^3 =$$
$$= [0,+\infty] \nabla [0,3] = [0,+\infty]$$

Widening computation is correct (sound)

Widening computation is correct (sound)

- Iterations sequences with widening are increasing and stationary after finitely many steps
- The limit of the iteration sequence with widening $\nabla_{i \leq k} f^i$ is a post-fixpoint of f

Widening computation is correct (sound)

- Iterations sequences with widening are increasing and stationary after finitely many steps
- The limit of the iteration sequence with widening $\nabla_{i \leq k} f^i$ is a post-fixpoint of f

Hence, $\nabla_{i \leq k} f^i$ is an over-approximation of the least fixpoint of f:

$$\mathrm{lfp}\, f \sqsubseteq \nabla_{i \leq k} f^i$$

computable in finite time

Thanks for the attention!

LaTeX is the way

Additional Slides

Further reading

CC-LOGCOM-1992 "Abstract Interpretation Frameworks", P. Cousot and R. Cousot, In: *Journal of logic and computation* (1992)