Abstract interpretation

$$ceval : 2^{cstate} \times E \longrightarrow 2^{\mathbb{Z}}$$

$$cstate : Vars \to \mathbb{Z}$$

$ceval(s, x) = \{s(x)\}$

$ceval(s, \text{input}) = \mathbb{Z}$

$\vdots$

concrete/collecting semantics

$$ceval(R, E) = \bigcup_{s \in R} ceval(s, E)$$

$$[\![l_i]\!] = \{ s[x \mapsto ceval(s, E)] \mid s \in [\![l_{i-1}]\!] \}$$

$i-1: \ \ldots$

$i: \quad x = E$

Define aeval

$Signs : \{+, -, 0, \top, \bot\}$

$AState = Vars \longrightarrow Signs$

$aeval : AState \times E \longrightarrow Signs$

$$aeval(a, \text{input}) = \top$$

a: AState

$$aeval(a, x) = a(x)$$

$$aeval(a, E_1 + E_2) =$$

let $a_1 = aeval(a, E_1)$
$\quad a_2 = aeval(a, E_2)$
$\quad a_1 \hat{+} a_2$

$\hat{+} \quad +^{\#} \quad \tilde{+}$

	+	-	0	⊤	⊥
+	+	⊤	+	⊤	⊥
-					
0					
⊤					
⊥					

$$[\![\hat{l}_i]\!] = a[x \mapsto aeval(a, E)]$$

$x := E$ $\qquad$ $a = [\![l_{i-1}]\!]$

$[\![l_i]\!] \subseteq 2^{CState}$

$[\![\hat{l}_i]\!] \in AState$

abstraction function

$\alpha_a : 2^{\mathbb{Z}} \longrightarrow Signs$

$\alpha_b : 2^{CState} \longrightarrow AState$

Vars $\longrightarrow$ Signs

$\alpha_c : (2^{CState})^n \longrightarrow AState^n$

$\alpha_a(\{0,1,2\}) = \top$

$\alpha_a(\{1,2\}) = +$

$\alpha_a(\emptyset) = \bot$

concretization function

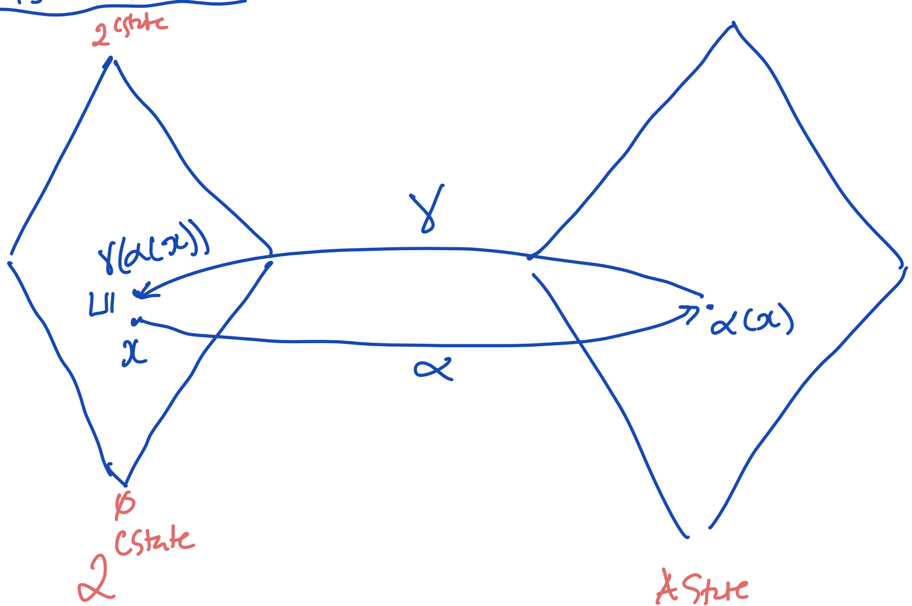
$\gamma_a : Signs \longrightarrow 2^{\mathbb{Z}}$

$\gamma_a(+) = \{1,2,3,\dots\}$

$\gamma_a(\top) = \mathbb{Z}$

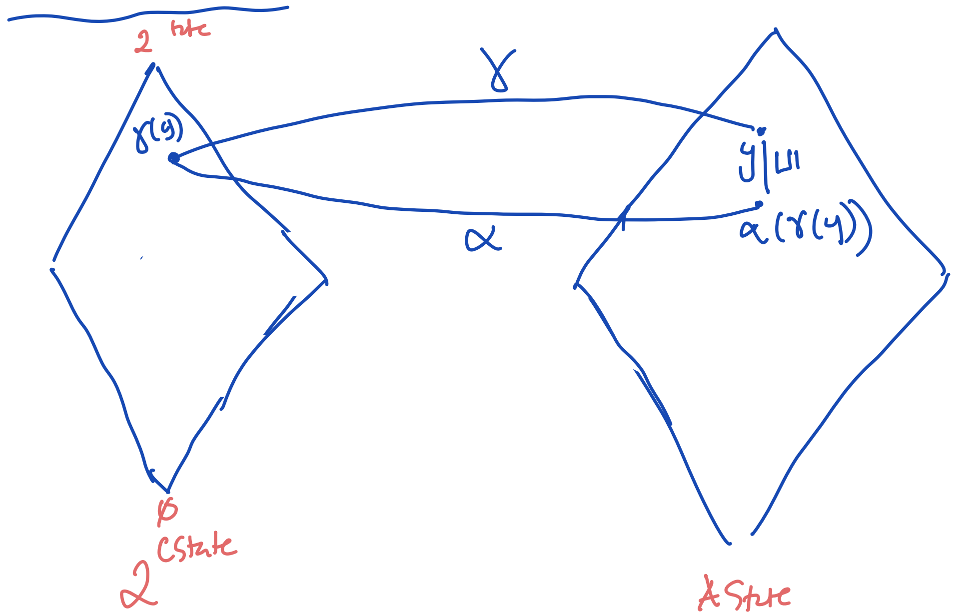
$\vdots$

Galois connections



① $x \sqsubseteq \gamma(\alpha(x))$

②



Soundness

R concrete states

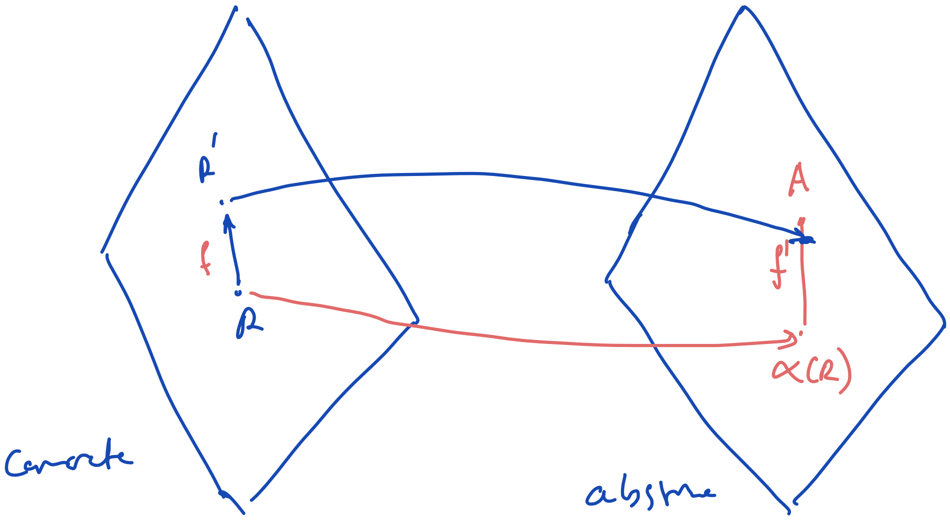
E expression

$$\alpha_b(\underbrace{ceval(R, E)}_{\in 2^{\mathbb{Z}}}) \sqsubseteq \underbrace{aeval(\alpha_b(R), E)}_{\in \text{Signs}}$$

$f : 2^{CState} \longrightarrow 2^{CState}$ concrete transformer

$\hat{f} : AState \longrightarrow AState$ abstract transformer

$$\alpha_b(f(R)) \sqsubseteq \hat{f}(\alpha_a(R))$$



α, γ, f

$+ \;\hat{+}\; 0 = +$

$+ \;\hat{+}\; 0 = \top$

$\hat{f}(a) = \alpha(f(\gamma(a)))$ — the most precise transformer

is a sound approximation of f because of Galois connection

If L_1 and L_2 are lattices

$$L_1 \underset{\gamma}{\overset{\alpha}{\rightleftarrows}} L_2$$

$f : L_1 \longrightarrow L_1$

$\hat{f} : L_2 \longrightarrow L_2$ is a sound approximation of f

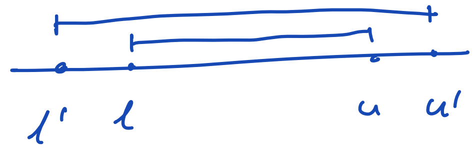
$$\alpha(fix(f)) \sqsubseteq fix(\hat{f})$$

<u>interval domain</u>

E.g. $[5, 10]$ — 5: lower, 10: upper

$(-\infty, \infty)$

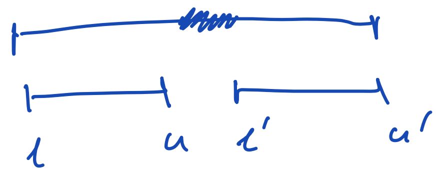
$(\infty, -\infty)$



$\sqsubseteq$

$[l, u] \sqsubseteq [l', u']$

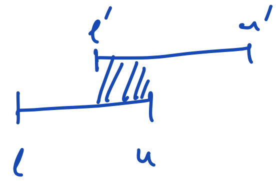
iff $l' \leq l$ and $u' \geq u$



LUB $\sqcup$ of two intervals

$[l, u] \sqcup [l', u']$

$= [\min(l, l'), \max(u, u')]$



GLB $\sqcap$ of two intervals

$[l, u] \sqcap [l', u']$

$= [\max(l, l'), \min(u, u')]$

empty

$[\infty, -\infty]$

$\hat{+}$

$[l, u] \mathbin{\hat{+}} [l', u'] =$

$[l + l', u + u']$

$2 * [10, 15]$

$[20, 30]$

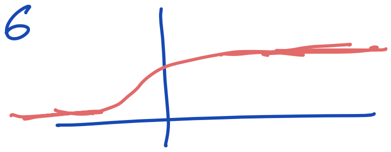
$c * [l, u] =$

$[\min(c * l, c * u), \max(c * l, c * u)]$

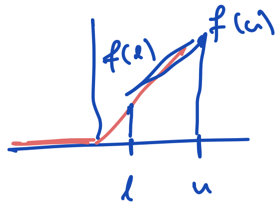
$-2 * [10, 15]$

$[-20, -30]$

$f : \mathbb{R} \to \mathbb{R}$ monotonic increasing e.g. σ



$\hat{f}$: Interval $\to$ Interval



$\hat{f}([l, u]) = [f(l), f(u)]$