Abstract Interpretation, continued.

$$\text{ceval} : 2^{\text{cstates}} \times E \to 2^{\mathbb{Z}}$$

$\text{Vars} \to \mathbb{Z}$

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

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

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

$$\text{ceval}(s, E_1 \text{ op } E_2) = \{ v_1 \text{ op } v_2 \mid v_1 \in \text{ceval}(s, E_1) \wedge v_2 \in \text{ceval}(s, E_2) \}$$

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

set of states reachable after line l_i

E.g. $x := E$

monotone

2^{cstates}

$$\text{Signs} = \{+, -, 0, \top, \bot\}$$

$$\text{AState} = \text{Vars} \to \text{Signs}$$

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

Vars → Signs

$$\text{aeval}(a, x) = a(x)$$

$$\text{aeval}(a, E_1 \hat{+} E_2) =$$

$$\text{let } x_1 = \text{aeval}(a, E_1)$$
$$x_2 = \text{aeval}(a, E_2)$$

$+^{\#}$

$\tilde{+}$

$+^{*}$

x_2 \ x_1	$+$	$-$	0	$\top$	$\bot$
$+$	$+$	$\top$	$+$	$\top$	$\bot$
$-$	$\top$	$-$	$-$	$\top$	$\bot$
0	⋮				
$\top$	⋮				
$\bot$	⋮				

$$a_1 \hat{+} a_2 = \alpha(\gamma(a_1) + \gamma(a_2))$$

$$[\![\hat{l}_i]\!] = a[x \mapsto aeval(a, E)] \text{ where } a = [\![l_{i-1}]\!]$$

E.g. $x := E$

AState instead of 2^{CState}

monotone

---

abstraction function

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

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

$$\hookrightarrow Vars \longrightarrow Sign$$

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

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

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

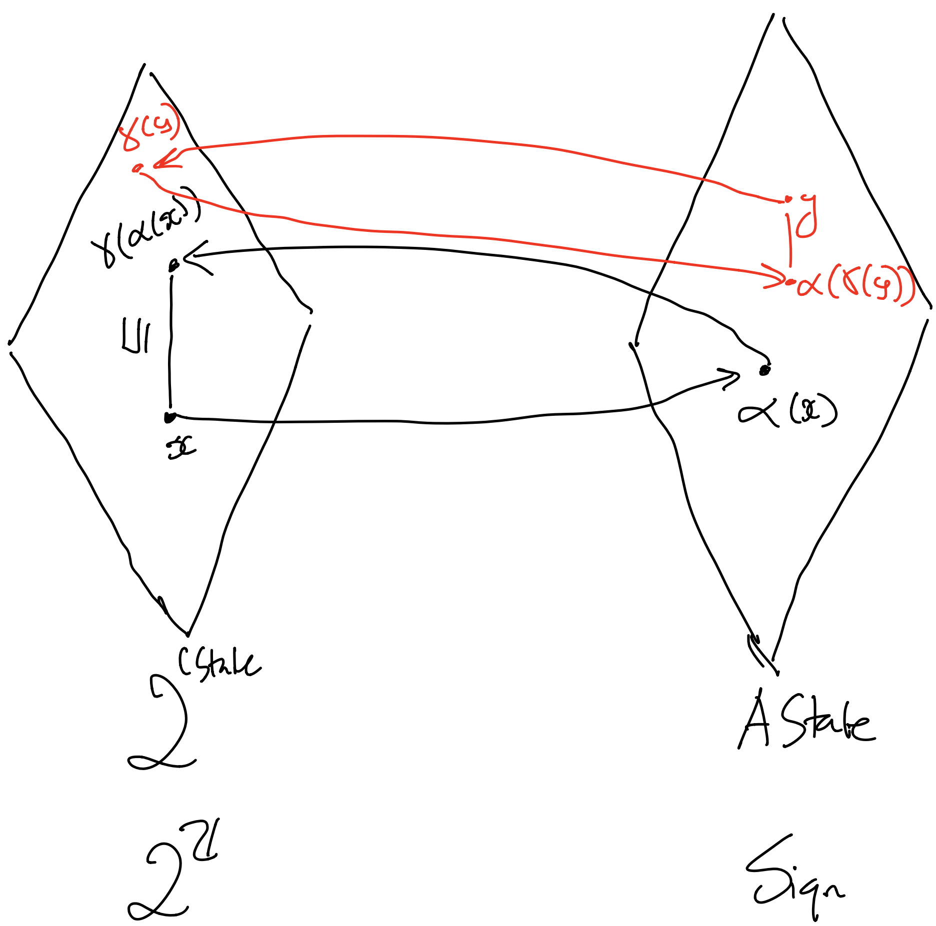
$$\alpha_a(\emptyset) = \bot$$

concretization function

$$\gamma_a : Sign \to 2^{\mathbb{Z}}$$

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

Galois connections



Soundness

R concrete states

E expression

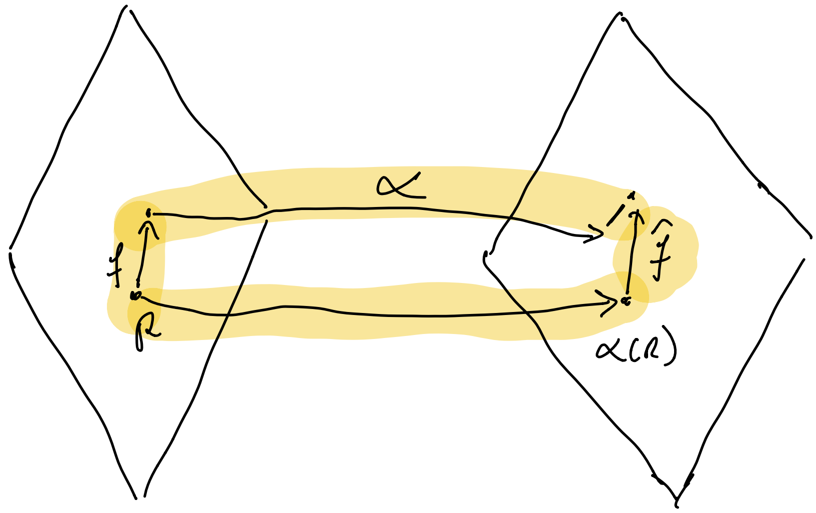
$$\boxed{\alpha_a(\underbrace{\text{ceval}(R, E)}_{2^{\mathbb{Z}}}) \sqsubseteq \underbrace{\text{aeval}(\alpha_b(R), E)}_{\text{Sign}}}$$

$$f : 2^{\text{CState}} \longrightarrow 2^{\text{CStates}}$$

$$\hat{f} : \text{AState} \longrightarrow \text{AState}$$

abstract transformer

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



$2^{cstates}$

---

we have α, γ, f

I want $\hat{f}$

for all a, $\hat{f}(a) = \alpha(f(\gamma(a)))$

$\hat{f}$ is a sound approximation of f

because of Galois connection

If L_1, L_2 are lattices. $\alpha : L_1 \to L_2$ and $\gamma : L_2 \to L_1$ form a Galois connection.

$f : L_1 \to L_1$, $\hat{f}$ is a safe approximation (sound)

$\hat{f} : L_2 \to L_2$

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

Soundness theorem

Optimality

for $a_1 \hat{+} a_2 = \top$

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

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

$$\hat{f}(a) = \alpha(f(\gamma(a)))$$

the most precise transformer

$$ceval(s, x - x) = 0$$

$$aeval(a, \underset{+}{x} - \underset{+}{x}) = \top$$

our analysis is <u>non-relational</u>

$x := \text{input}$ $\quad [x \mapsto \top, \ldots]$

$y := x$ $\quad [x \mapsto \top, y \mapsto \top]$

$z := x - y$ $\quad [x \mapsto \top, y \mapsto \top, z \mapsto \top]$

interval domain (non-relational)

$$x \mapsto +, -, 0, \top, \bot$$

$$x \mapsto [-10, 11]$$

Zonotope domain (relational domain)