$\sigma^{\perp} = \{x \mapsto \perp, y \mapsto \perp, z \mapsto \perp\}$

Worklist algorithm

initialize $\sigma_i^{in} = \sigma_i^{out} = \sigma^{\perp}$

worklist = $\{1 \dots |P|\}$

while let Some(i) = dequeue worklist:

$\quad \sigma_i^{in} = \bigsqcup_{j \in pred(i)} \sigma_j^{out}$

$\quad \sigma_i^{out} = f(P_i, \sigma_i^{in})$

$\quad$ if σ_i^{out} changed:

$\quad\quad$ enqueue succ(i) onto worklist

Termination argument

- terminates when worklist is empty
- true if $\exists k$ iterations s.t. $\forall i$, σ_i^{out} does not change
- $\sqcup$ is inflationary

  $\forall_{j \in pred(i)}, \sigma_i^{in} \sqsupseteq \sigma_j^{out}$
- f is monotonic

  $\sigma_i^{in} \sqsubseteq \sigma_i^{in'} \Rightarrow f(P_i, \sigma_i^{in}) \sqsubseteq f(P_i, \sigma_i^{in'})$

Inflationary

$f: \mathbb{R} \to \mathbb{R}$ is inflationary

if $\forall x,\ f(x) \geq x$

$f(x) = x + 1$

$f(x) = \text{abs}(x)$

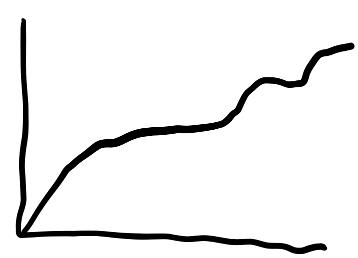
$-2 \leq -1 \not\Rightarrow |-2| \leq |-1|$

Monotonic

$f: \mathbb{R} \to \mathbb{R}$ is monotonic if

f is order-preserving

$x \leq y \Rightarrow f(x) \leq f(y)$



$f(x) = x + 1$

$f(x) = x^3 \qquad F(x) = x/$

Constant analysis

$1 \not\sqsubseteq 2$

$2 \not\sqsubseteq 1$

$1 \sqsubseteq 1$

$2 \sqsubseteq 2$

$\sigma_1 \leq \sigma_2 \Rightarrow f(\sigma_1) \sqsubseteq f(\sigma_2)$

$\sigma_2 = \{x \mapsto 1, y \mapsto \top, z = \top\}$

$\sigma_1 = \{x \mapsto 1 \;\; y \mapsto \bot, z = \bot\}$

$f(\sigma_2) = \{x \mapsto \bot, \ldots\}$

$f(\sigma_1) = \{x \mapsto \top, \ldots\}$

$f(\sigma_1) \not\sqsubseteq f(\sigma_2)$

$f(x = y \oplus z, \sigma)$

if $\sigma[y] = c_1$

$\sigma[z] = c_2$

$\Rightarrow \sigma[x \mapsto c_1 \oplus c_2]$

$f(x = y \oplus z, \sigma)$

if $\sigma[y] = \top \lor \sigma[z] = \top$

then $\sigma[x \mapsto \bot]$

else $\sigma[x \mapsto \top]$

$\{y \mapsto \top, z \mapsto \top, x \mapsto 1\}$

$\downarrow$

$x = y + z$

$\downarrow$

$\{y \mapsto \top, z \mapsto \top, x \mapsto \bot\}$

$x = 0$

$\downarrow \; x \mapsto 0$

$x = x + 1$

$\downarrow$

jump 2

$x \mapsto 1$

Bytecode semantics

Configurations $C = \{\text{prog } P;\ \text{pc } i;\ \text{locals } \{\text{Var} \mapsto \text{Const}\}\}$

$C_1 \hookrightarrow C_2$

$$\frac{C.\text{prog}[C.\text{pc}] = \text{“}x = rv\text{”} \quad C.\text{locals} \vdash rv \Downarrow c}{C \hookrightarrow \{C \text{ with locals} = C.\text{locals}[x \mapsto c] \;\; \text{pc} = C.\text{pc} + 1\}}$$

$E \vdash c \Downarrow c \qquad E \vdash x \Downarrow E[x]$

"$C_1 \hookrightarrow C_2 \hookrightarrow C_3 \ldots \hookrightarrow C_n$" is a **trace** T

Soundness

An abstraction function α : Configuration $\rightarrow$ AbsDomain

$\uparrow$ C $\qquad \uparrow$ σ

Zero analysis: $\alpha(C) = \{x \mapsto \text{if } x = 0 \text{ then } Z \text{ else } NZ\}$

for all $x \in C.\text{locals}$

$$\alpha(\{ \ldots \text{locals} = \{x \mapsto 0, y \mapsto 1\}\}) = \{x \mapsto Z, y \mapsto NZ\}$$

$C_5 = \{ pc = 2, \text{locals} = \{x \mapsto 1\}\}$

$\sigma_2^{out} = \{x \mapsto \top\}$ ✓ $\{x \mapsto 1\}$ ✓

$\{x \mapsto 2\}$ ✗ $\{x \mapsto \bot\}$ ✗

Constant: $\alpha(C) = \{x \mapsto x\}$

An analysis is sound wrt α if:

$$\forall T, \forall C_i \in T, \alpha(C_i) \sqsubseteq \sigma^{out}_{C_i.pc}$$

$\{\} \sqsubseteq \{x \mapsto \bot\}$

Soundness of liveness

C_1 agree with C_2 at $\sigma \triangleq \forall x \in \sigma.\ C_1.\text{locals}[x] = C_2.\text{locals}[x]$

$\forall C_1, C_2.\ C_1$ agrees with C_2 at $\sigma^{in}_{C_1.pc} \Rightarrow$

$C_1 \hookrightarrow C_1' \quad C_2 \hookrightarrow C_2'$

C_1' agrees with C_2' at $\sigma^{out}_{C_1'.pc}$