Statische Analyse durch abstrakte Interpretation

Jan Peleska
Helge Löding

hloeding@informatik.uni-bremen.de

Universität Bremen — Technologiezentrum Informatik TZI

Tutorium
28. November 2007

Überblick

Programm

Semantik

Abstraktion

Berechnung

Programm

sample1.c

```
float x, y;
if(x < y){

  x = sqrt(y - x);

}

else{

  x = 0;

}

return x;
```

Konkrete Semantik

Locations: $Loc = Lang(G)$
Variablen: X
Valuationen:

$$
\begin{aligned}
D_x &= \mathit{float} \\
D_y &= \mathit{float} \\
D &= \textstyle\bigcup_{v \in X} D_v = \mathit{float} \\
\Sigma &= X \not\to D
\end{aligned}
$$

Konkrete Semantik

Erweiterte Valuationsfunktionen:

$$
\begin{aligned}
&\sigma^* \in exp \not\rightarrow D\\
&\sigma^*(v) =_{def} \sigma(v)\\
&\sigma^*(exp_1 - exp_2) =_{def} \sigma^*(exp_1) - \sigma^*(exp_2)\\
&\sigma^*(sqrt(exp)) =_{def} sqrt(\sigma^*(exp))
\end{aligned}
$$

$$
\begin{aligned}
&\sigma^+ \in bexp \not\rightarrow \mathbb{B}\\
&\sigma^+(v_1 < v_2) =_{def} \sigma(v_1) < \sigma(v_2)
\end{aligned}
$$

Konkrete Semantik

Zustandsraum: $S = Loc \times \Sigma$

Startzustände: $S_0 = \{(c, \sigma) \in S \mid c = P \wedge dom\,\sigma = \{x, y\}\}$

Transitionsrelation $\longrightarrow$:

$$\frac{}{(v = exp; P, \sigma) \longrightarrow (P, \sigma[v \mapsto \sigma^*(exp)])}$$

$$\frac{\sigma^+(bexp) = true}{(if(bexp)\{P_1\}else\{P_2\}; P_3, \sigma) \longrightarrow (P_1; P_3, \sigma)}$$

$$\frac{\sigma^+(bexp) = false}{(if(bexp)\{P_1\}else\{P_2\}; P_3, \sigma) \longrightarrow (P_2; P_3, \sigma)}$$

Transitionssystem: $TS = (S, S_0, \longrightarrow)$

Potenzmengentransitionssystem

Zustandsraum: $S_{\mathbf{P}} = \mathbf{P}(S)$
Startzustandsmenge: $S_{0_{\mathbf{P}}} = \{S_0\}$
Transitionsrelation $\longrightarrow_{\mathbf{P}}$:

$$\frac{\forall i \in I, s_i, s_i' \in S : s_i \longrightarrow s_i'}{\{s_i | i \in I\} \longrightarrow_{\mathbf{P}} \{s_i' \mid i \in I\}}$$

Transitionssystem: $TS_{\mathbf{P}} = (S_{\mathbf{P}}, S_{0_{\mathbf{P}}}, \longrightarrow_{\mathbf{P}})$

Abstraktionssemantik

Verwendung von $\mathbb{IR}$ als Wertigkeiten von Variablen ($L(D)$).
Valuationen:

$$L(D_x) = \mathbb{IR}$$
$$L(D_y) = \mathbb{IR}$$
$$L(D) = \bigcup_{v \in X} L(D_v) = \mathbb{IR}$$
$$\Sigma_L = X \not\rightarrow L(D)$$

Kleinste obere Schranke:

$$\bigsqcup \in \mathbf{P}(L(D)) \rightarrow L(D)$$
$$\bigsqcup\{[\underline{a_1}, \overline{a_1}], \ldots, [\underline{a_n}, \overline{a_n}]\} =_{def} [min(\{\underline{a_1}, \ldots, \underline{a_n}\}), max(\{\overline{a_1}, \ldots, \overline{a_n}\}]$$

Abstraktionssemantik

GC zwischen $\mathbf{P}(D)$ und $L(D)$:

$$\begin{aligned}
&\rhd \in \mathbf{P}(D) \to L(D)\\
&V \in \mathbf{P}(\mathit{float})\\
&V^{\rhd} =_{def} [\mathit{min}(v), \mathit{max}(v)]
\end{aligned}$$

$$\begin{aligned}
&\lhd \in L(D) \to \mathbf{P}(D)\\
&w = [\underline{w}, \overline{w}] \in \mathbb{IR}\\
&w^{\lhd} =_{def} \{f \in \mathit{float} \mid \underline{w} \leq f \leq \overline{w}\}
\end{aligned}$$

Abstraktionssemantik

Lifting von $-$:

$$a, b \in \mathbb{IR}, a[-]b =_{def} \{x - y \mid x \in a^{\triangleleft} \wedge y \in b^{\triangleleft}\}^{\triangleright}$$

$$\Leftrightarrow [\underline{a}, \overline{a}][-][\underline{b}, \overline{b}] = [\underline{a} - \overline{b}, \overline{a} - \underline{b}]$$

Abstraktionssemantik

Lifting von *sqrt*:

$$a \in \mathbb{IR}, [sqrt](a) =_{def} \{sqrt(x) \mid x \in a^{\lhd}\}^{\rhd}$$

$$\Leftrightarrow [sqrt]([\underline{a}, \overline{a}]) = [sqrt(\underline{a}), sqrt(\overline{a})]$$

Abstraktionssemantik

Lifting von $<$:

$$a, b \in \mathbb{IR}, a[<]b =_{def} \{x < y \mid x \in a^{\triangleleft} \wedge y \in b^{\triangleleft}\}$$

$$\Leftrightarrow [\underline{a}, \overline{a}][<][\underline{b}, \overline{b}] = \begin{cases} \{true\} \text{ falls } \overline{a} < \underline{b} \\ \{false\} \text{ falls } \overline{b} < \underline{a} \\ \{true, false\} \text{ sonst} \end{cases}$$

Abstraktionssemantik

Erweiterte Valuationsfunktionen:

$$\begin{aligned}
&\lambda^* \in exp \not\to L(D)\\
&\lambda^*(v) =_{def} \lambda(v)\\
&\lambda^*(exp_1 - exp_2) =_{def} \lambda^*(exp_1)[-]\lambda^*(exp_2)\\
&\lambda^*(sqrt(exp)) =_{def} [sqrt](\lambda^*(exp))
\end{aligned}$$

$$\begin{aligned}
&\lambda^+ \in bexp \not\to \mathbb{B}\\
&\lambda^+(v_1 < v_2) =_{def} \lambda(v_1)[<]\lambda(v_2)
\end{aligned}$$

Abstraktionssemantik

Zusammenfassen von Zuständen aus $\mathbf{P}(Loc \times \Sigma_L)$ nach Locations:

$$\begin{aligned}
&\kappa \in \mathbf{P}(Loc \times \Sigma_L) \rightarrow \mathbf{P}(Loc \times \Sigma_L)\\
&\kappa(U) = \{(c, \lambda) \in Loc \times \Sigma_L \mid \forall x \in X :\\
&\qquad \lambda(x) = \bigsqcup\{w \in \mathbb{IR} \mid\\
&\qquad\qquad \exists(c', \lambda') \in U : c = c' \wedge \lambda'(x) = w\}\}
\end{aligned}$$

Abstraktionssemantik

GC zwischen L und $S_{\mathbf{P}}$:

$$\begin{aligned}
&\triangleright \in \mathbf{P}(Loc \times \Sigma) \rightarrow \mathbf{P}(Loc \times \Sigma_L)\\
&S \in \mathbf{P}(Loc \times \Sigma)\\
&S^{\triangleright} =_{def} \kappa(\{(c,\lambda) \in Loc \times \Sigma_L \mid \exists \sigma \in \Sigma : (c,\sigma) \in S \wedge dom\,\sigma = dom\,\lambda \wedge\\
&\qquad (\forall x \in dom\,\sigma : \{\sigma(x)\}^{\triangleright} = \lambda(x))\})
\end{aligned}$$

$$\begin{aligned}
&\triangleleft \in \mathbf{P}(Loc \times \Sigma_L) \rightarrow \mathbf{P}(Loc \times \Sigma)\\
&U \in \mathbf{P}(Loc \times \Sigma_L)\\
&U^{\triangleleft} =_{def} \{(c,\sigma) \in Loc \times \Sigma \mid \exists \lambda \in \Sigma_L : (c,\lambda) \in U \wedge dom\,\sigma = dom\,\lambda \wedge\\
&\qquad (\forall x \in dom\,\sigma : \{\sigma(x)\} \subseteq \lambda(x)^{\triangleleft})\}
\end{aligned}$$

Abstraktionssemantik

Zustandsraum:

$$L =_{def} \mathbf{P}(Loc \times \Sigma_L)$$

Startzustandsmenge:

$$L_0 = {S_{0_\mathbf{P}}}^{\triangleright}$$

Transitionsrelation $\longrightarrow_L$ (Sei $p, p' \in S_\mathbf{P}$ und $a \in S_L$):

$$\frac{p^{\triangleright\triangleleft} \longrightarrow_\mathbf{P} p'}{p^{\triangleright} \longrightarrow_L p'^{\triangleright}}$$

$$\frac{a^{\triangleleft} \longrightarrow_\mathbf{P} p'}{a \longrightarrow_L p'^{\triangleright}}$$

Transitionssystem:

$$TS_L = (L, L_0, \longrightarrow_L)$$

Berechnung

Betrachte konkreten Zustand:

$$S = \{(P, \sigma) \mid \underline{x} \leq \sigma(x) \leq \overline{x} \wedge \underline{y} \leq \sigma(y) \leq \overline{y}\}$$

Daraus wird unter $\triangleright$:

$$S^{\triangleright} = \{(P, \lambda) \mid \lambda(x) = [\underline{x}, \overline{x}] \wedge \lambda(y) = [\underline{y}, \overline{y}]\}$$

Und wieder unter $\triangleleft$:

$$S^{\triangleright\triangleleft} = S$$

Berechnung

$$S = \{(P, \sigma) \mid \underline{x} \leq \sigma(x) \leq \overline{x} \wedge \underline{y} \leq \sigma(y) \leq \overline{y}\}$$

Betrachte Folgezustand S' mit $S \longrightarrow_P S'$:

$$\begin{aligned} S' = \{ & x = \mathit{sqrt}(y - x); \mathit{return}\, x, \sigma) \mid \\ & \underline{x} \leq \sigma(x) \leq \overline{x} \wedge \underline{y} \leq \sigma(y) \leq \overline{y} \wedge \sigma^+(x < y) = \mathit{true}\} \cup \\ & \{x = 0; \mathit{return}\, x, \sigma) \mid \\ & \underline{x} \leq \sigma(x) \leq \overline{x} \wedge \underline{y} \leq \sigma(y) \leq \overline{y} \wedge \sigma^+(x < y) = \mathit{false}\} \end{aligned}$$

Dieses unter $\triangleright$:

$$\begin{aligned} S'^{\triangleright} = \{ & x = \mathit{sqrt}(y - x); \mathit{return}\, x, \lambda) \mid \\ & \lambda(x) = [\underline{x}, \overline{x}] \wedge \lambda(y) = [\underline{y}, \overline{y}] \wedge \lambda^+(x < y) = \{\mathit{true}\}\} \cup \\ & \{x = 0; \mathit{return}\, x, \sigma) \mid \\ & \lambda(x) = [\underline{x}, \overline{x}] \wedge \lambda(y) = [\underline{y}, \overline{y}] \wedge \lambda^+(x < y) = \{\mathit{false}\}\} \end{aligned}$$

Berechnung

Aus Regel

$$\frac{p^{\triangleright\triangleleft} \longrightarrow_{\mathbf{P}} p'}{p^{\triangleright} \longrightarrow_{L} p'^{\triangleright}}$$

geht hervor, dass $S^{\triangleright} \longrightarrow_L S'^{\triangleright}$, also:

$$\frac{\lambda^{+}(x < y) = \{true\}}{\begin{array}{l}(P, \langle x \mapsto [\underline{x}, \overline{x}], y \mapsto [\underline{y}, \overline{y}]\rangle) \longrightarrow_L \\ (x = sqrt(y - x); return\, x, \langle x \mapsto [\underline{x}, \overline{x}], y \mapsto [\underline{y}, \overline{y}]\rangle)\end{array}}$$

Berechnung

Ein Fehler tritt im nächsten Schritt auf, wenn $y - x < 0$, oder abstrakt:

$$
\begin{aligned}
& [\underline{y}, \overline{y}][-][\underline{x}, \overline{x}][<][0,0] = \{\mathit{true}\} \\
\Leftrightarrow\ & [\underline{y} - \overline{x}, \overline{y} - \underline{x}][<][0,0] = \{\mathit{true}\} \\
\Leftrightarrow\ & \overline{y} - \underline{x} < 0
\end{aligned}
$$

Berechnung

Aus der Voraussetzung wissen wir jedoch:

$$\begin{aligned}
&\lambda^+(x < y) = \{\mathit{true}\} \\
&\Leftrightarrow \overline{x} < \underline{y} \\
&\Rightarrow \underline{x} < \overline{y} \\
&\Leftrightarrow 0 < \overline{y} - \underline{x}
\end{aligned}$$