Statische Analyse durch abstrakte Interpretation WS 2007/08

Hinweise zum Tutorium

Termin: 14.11.2007

Teil 1: Spezifikation konkrete Semantik

Wir betrachten weiterhin das Programm

```
p0: while isEven(x) {
        p1: x = x div 2;
    }
p2: x = 4 * x;
p3: exit
```

Die Menge der Programmlabels:

$$P =_{def} \{p_0, p_1, p_2, p_3\}$$

Die Menge der möglichen Werte für x:

$$x \in \mathbb{Z}$$

Der Zustandsraum:

$$S_c =_{def} P \times \mathbb{Z}$$

Die Transitionsrelation $\longrightarrow_c$:

$$\frac{isEven(x)}{(p_0, x) \longrightarrow_c (p_1, x)}, \frac{\neg isEven(x)}{(p_0, x) \longrightarrow_c (p_2, x)}, \frac{}{(p_1, x) \longrightarrow_c (p_0, x \textbf{ div } 2)}, \frac{}{(p_2, x) \longrightarrow_c (p_3, 4 * x)}$$

Mögliche Menge der Startzustände:

$$S_{0_c} =_{def} \{(p_0, x) \mid x \in \mathbb{Z}\}$$

Das Transitionssystem:

$$TS_c =_{def} (S_c, S_{0_c}, \longrightarrow_c)$$

Teil 2: Potenzmengenverband

Der Potenzmengenverband von S_c:

$$S_{\mathbf{P}} =_{def} (\mathbf{P}(S_c), \subseteq)$$

Die Transitionsrelation $\longrightarrow_{\mathbf{P}}$:

$$\frac{x_p^q \in \mathbb{Z}}{\begin{array}{c}\{p_0\} \times \{x_0^1, \ldots, x_0^{n_0}\} \cup \\ \{p_1\} \times \{x_1^1, \ldots, x_1^{n_1}\} \cup \\ \{p_2\} \times \{x_2^1, \ldots, x_2^{n_2}\} \cup \\ \{p_3\} \times \{x_3^1, \ldots, x_3^{n_3}\} \\ \longrightarrow_{\mathbf{P}} \\ \{p_1\} \times \{x_0^i \mid i \in 1 \ldots n_0 \wedge isEven(x_0^i)\} \cup \\ \{p_2\} \times \{x_0^i \mid i \in 1 \ldots n_0 \wedge \neg isEven(x_0^i)\} \cup \\ \{p_0\} \times \{x_1^i \ \mathbf{div}\ 2 \mid i \in 1 \ldots n_1\} \cup \\ \{p_3\} \times \{4 * x_2^i \mid i \in 1 \ldots n_2\} \cup \\ \{p_3\} \times \{x_3^i \mid i \in 1 \ldots n_3\}\end{array}}$$

Mögliche Menge der Startzustände:

$$S_{0_{\mathbf{P}}} =_{def} \{S_{0_c}\}$$

Das Potenzmengentransitionssystem:

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

Teil 3: Abstraktes Transitionssystem

Mögliche Werte für x:

$$x \in \{even, odd\}$$

Zustandsraum:

$$S_a =_{def} (\mathbf{P}(P \times \{even, odd\}), \subseteq)$$

Zustandsübergangsrelation $\longrightarrow_a$:

$$\frac{E_0, E_1, E_2, E_3 \subseteq \{even, odd\}}{\begin{array}{c}\{p_0\} \times E_0 \cup \\ \{p_1\} \times E_1 \cup \\ \{p_2\} \times E_2 \cup \\ \{p_3\} \times E_3 \\ \longrightarrow_a \\ \{p_1\} \times \{even \mid even \in E_0\} \cup \\ \{p_2\} \times \{odd \mid odd \in E_0\} \cup \\ \{p_0\} \times \{even, odd \mid E_1 \neq \emptyset\} \cup \\ \{p_3\} \times \{even \mid E_2 \neq \emptyset\} \cup \\ \{p_3\} \times \{e \mid e \in E_3\}\end{array}}$$

Mögliche Menge der Startzustände:

$$S_{0_a} =_{def} \{\{p_0\} \times \{even, odd\}\}$$

Das abstrakte Transitionssystem:

$$TS_a =_{def} (S_a, S_{0_a}, \longrightarrow_a)$$

Teil 4: Galois Zusammenhang

Abstraktion:

$$\{(q_1, x_1), \ldots, (q_n, x_n)\}^{\triangleright} =_{def} \left\{ \begin{array}{l} (q_1, \textbf{if } \mathit{isEven}(x_1) \textbf{ then } \mathit{even} \textbf{ else } \mathit{odd}), \\ \ldots, \\ (q_n, \textbf{if } \mathit{isEven}(x_n) \textbf{ then } \mathit{even} \textbf{ else } \mathit{odd}) \end{array} \right\}$$

Konkretisierung:

$$\{(q_1, e_1), \ldots, (q_n, e_2)\}^{\triangleleft} =_{def} \begin{array}{l} \{(q_i, 2*m) | i \in 1, \ldots, n \wedge m \in \mathbb{Z} \wedge e_i = \mathit{even}\} \cup \\ \{(q_i, 2*m+1) | i \in 1, \ldots, n \wedge m \in \mathbb{Z} \wedge e_i = \mathit{odd}\} \end{array}$$

Galois Zusammenhang Eigenschaft:

$$\forall Z_{\mathbf{P}} \in S_{\mathbf{P}}, Z_a \in S_a : Z_{\mathbf{P}}^{\triangleright} \subseteq Z_a \Leftrightarrow Z_{\mathbf{P}} \subseteq Z_a^{\triangleleft}$$

- Informeller Beweis $\Rightarrow$:

  Betrachte jedes (q_i, x_i) separat. Ist x_i gerade, so entsteht unter $\triangleright$ ein (q_i, even). Daraus entsteht unter $\triangleleft$ eine Menge

  $$\{\ldots, (q_i, -2), (q_i, 0), (q_i, 2), \ldots\}$$

  Da x_i gerade war, ist (q_i, x_i) enthalten. Analog für jedes (q_i, x_i) mit ungeradem x_i. Also gilt:

  $$\forall Z_{\mathbf{P}} \in S_{\mathbf{P}} : Z_{\mathbf{P}} \subseteq Z_{\mathbf{P}}^{\triangleright\triangleleft}$$

  Da $\triangleleft$ offensichtlich monoton ist, folgt damit aus der Voraussetzung:

  $$\begin{array}{l} Z_{\mathbf{P}}^{\triangleright} \subseteq Z_a \Leftrightarrow \\ Z_{\mathbf{P}}^{\triangleright\triangleleft} \subseteq Z_a^{\triangleleft} \Leftrightarrow \\ Z_{\mathbf{P}} \subseteq Z_a^{\triangleleft} \end{array}$$

- Informeller Beweis $\Leftarrow$:

  Betrachte jedes (q_i, e_i) separat. Ist $e_i = \mathit{even}$, so entsteht daraus unter $\triangleleft$ eine Menge

  $$\{\ldots, (q_i, -2), (q_i, 0), (q_i, 2), \ldots\}$$

  Jedes Element dieser Menge erzeugt unter $\triangleright$ ein (q_i, even). Diese sind in (q_i, e_i) für $e_i = \mathit{even}$ enthalten. Analog für $e_i = \mathit{odd}$. Also gilt:

  $$\forall Z_a \in S_a : Z_a^{\triangleleft\triangleright} \subseteq Z_a$$

  Da $\triangleright$ offensichtlich monoton ist, folgt damit aus der Voraussetzung:

  $$\begin{array}{l} Z_{\mathbf{P}} \subseteq Z_a^{\triangleleft} \Leftrightarrow \\ Z_{\mathbf{P}}^{\triangleright} \subseteq Z_a^{\triangleleft\triangleright} \Leftrightarrow \\ Z_{\mathbf{P}}^{\triangleright} \subseteq Z_a \end{array}$$

Teil 5: Zulässigkeit der Abstraktion

Unter anderem zu zeigen:

$$\forall(Z_{\mathbf{P}}, Z'_{\mathbf{P}}) \in \longrightarrow_{\mathbf{P}} : \exists Z_a \in S_a : Z_{\mathbf{P}}^{\triangleright} \longrightarrow_a Z_a \wedge Z'^{\triangleright}_{\mathbf{P}} \subseteq Z_a$$

$Z_{\mathbf{P}}$:

$$Z_{\mathbf{P}} = \bigcup_{i=0}^{3} \{p_i\} \times \{x_i^1, \ldots, x_i^{n_i}\}$$

$Z_{\mathbf{P}}^{\triangleright}$:

$$\begin{aligned} Z_{\mathbf{P}}^{\triangleright} = & \textstyle\bigcup_{i=0}^{3} \{p_i\} \times \{even \mid \exists j \in 1, \ldots, n_i : isEven(x_i^j)\} \cup \\ & \textstyle\bigcup_{i=0}^{3} \{p_i\} \times \{odd \mid \exists j \in 1, \ldots, n_i : \neg isEven(x_i^j)\} \end{aligned}$$

Z_a:

$$\begin{aligned} Z_a = & \{(p_1, even) \mid \exists j \in 1, \ldots, n_0 : isEven(x_0^j)\} \cup \\ & \{(p_2, odd) \mid \exists j \in 1, \ldots, n_0 : \neg isEven(x_0^j)\} \cup \\ & \{(p_0, even), (p_0, odd) \mid n_1 > 0\} \cup \\ & \{(p_3, even) \mid n_2 > 0\} \cup \\ & \{(p_3, even) \mid \exists j \in 1, \ldots, n_3 : isEven(x_3^j)\} \cup \\ & \{(p_3, odd) \mid \exists j \in 1, \ldots, n_3 : \neg isEven(x_3^j)\} \end{aligned}$$

$Z_a^{\triangleleft}$:

$$\begin{aligned} Z_a^{\triangleleft} = & \{(p_1, 2*m) \mid m \in \mathbb{Z} \wedge \exists j \in 1, \ldots, n_0 : isEven(x_0^j)\} \cup \\ & \{(p_2, 2*m+1) \mid m \in \mathbb{Z} \wedge \exists j \in 1, \ldots, n_0 : \neg isEven(x_0^j)\} \cup \\ & \{(p_0, m) \mid m \in \mathbb{Z} \wedge n_1 > 0\} \cup \\ & \{(p_3, 2*m \mid m \in \mathbb{Z} \wedge n_2 > 0\} \cup \\ & \{(p_3, 2*m \mid m \in \mathbb{Z} \wedge \exists j \in 1, \ldots, n_3 : isEven(x_3^j)\} \cup \\ & \{(p_3, 2*m+1 \mid m \in \mathbb{Z} \wedge \exists j \in 1, \ldots, n_3 : \neg isEven(x_3^j)\} \end{aligned}$$

$Z'_{\mathbf{P}}$:

$$\begin{aligned} Z'_{\mathbf{P}} = & \{p_1\} \times \{x_0^i \mid i \in 1, \ldots, n_0 \wedge isEven(x_0^i)\} \cup \\ & \{p_2\} \times \{x_0^i \mid i \in 1, \ldots, n_0 \wedge \neg isEven(x_0^i)\} \cup \\ & \{p_0\} \times \{x_1^i \ \mathbf{div}\ 2 \mid i \in 1, \ldots, n_1\} \cup \\ & \{p_3\} \times \{4 * x_2^i \mid i \in 1, \ldots, n_2\} \cup \\ & \{p_3\} \times \{x_3^i \mid i \in 1, \ldots, n_3\} \end{aligned}$$

Es gilt:

$$Z_{\mathbf{P}}^{\triangleright} \longrightarrow_a Z_a \wedge Z'_{\mathbf{P}} \subseteq Z_a^{\triangleleft}$$

Somit nach Galois Zusammenhang:

$$Z_{\mathbf{P}}^{\triangleright} \longrightarrow_a Z_a \wedge Z'^{\triangleright}_{\mathbf{P}} \subseteq Z_a$$