Prof. Martin Hofmann
Dr. Ulrich Schöpp

Ludwig-Maximilians-Universität München
Institut für Informatik
SS 2014

Übungen zur Vorlesung
Formale Spezifikation und Verifikation

Blatt 10

Aufgabe 10-1 Geben Sie jeweils konkrete τ und ϖ an, so dass die folgenden Urteile im Typsystem mit Referenzen herleitbar sind.

a) $\mathtt{r}\colon \mathtt{ref}_{\Pi}\ \mathtt{int} \vdash \mathtt{fn}_{\pi}\ \mathtt{x} \Rightarrow (\mathtt{r}{:=}\mathtt{x}) : \tau\ \&\ \varpi$

Lösung: $\tau = \mathtt{int} \xrightarrow{\Pi:=} \mathtt{int}$, $\varpi = \emptyset$

b) $\emptyset \vdash \mathtt{let\ x} = \mathtt{ref}_A\ 0\ \mathtt{in\ fn}_{\pi}\ \mathtt{f} \Rightarrow (\mathtt{f}\ (\mathtt{x}{:=}!\mathtt{x}+1)) : \tau\ \&\ \varpi$

Lösung: $\tau = (\mathtt{int} \xrightarrow{\Pi} \alpha) \xrightarrow{\Pi\cup\{!A,A:=\}} \alpha$, $\varpi = \{\mathtt{ref}A\}$

c) $\emptyset \vdash \mathtt{fn}_{\pi}\ \mathtt{x} \Rightarrow \mathtt{if}\ !\mathtt{x} < 10\ \mathtt{then}\ (\mathtt{x}{:=}!\mathtt{x}+1)\ \mathtt{else}\ 10 : \tau\ \&\ \varpi$

Lösung: $\tau = \mathtt{ref}_{\Pi}\mathtt{int} \xrightarrow{!\Pi,\Pi:=} \mathtt{int}$, $\varpi = \emptyset$

d) $y\colon \mathtt{ref}_{\{A,B\}}\mathtt{int} \vdash \mathtt{fun}_{\pi}\ \mathtt{f\ x} \Rightarrow \mathtt{if\ x} > 0\ \mathtt{then}\ (\mathtt{y}{:=}!\mathtt{y} * 2);\ \mathtt{f}\ (\mathtt{x}-1)\ \mathtt{else}\ !\mathtt{y} : \tau\ \&\ \varpi$

Lösung: $\tau = \mathtt{int} \xrightarrow{\{!A,!B,A:=,B:=\}} \mathtt{int}$, $\varpi = \emptyset$

Aufgabe 10-2 Geben Sie σ und ϖ an, so dass das folgenden Urteil im Typsystem mit Exceptions herleitbar ist:

$$\emptyset \vdash \mathtt{fn\ f}\ \Rightarrow \mathtt{fn\ g}\ \Rightarrow \mathtt{fn\ x}\ \Rightarrow \mathtt{g}\ (\mathtt{f\ x})\colon \sigma\ \&\ \varphi$$

Das Typschema τ soll nur Effektausdrücke enthalten, die von der Grammatik $\varphi ::= \varphi_1 \cup \varphi_2 \mid \varepsilon$ erzeugt werden, d.h. keinen Ausdruck der Form $\{s\}$ für eine konkrete Exception s.

Lösung: $\tau = \forall \alpha, \beta, \gamma, \varepsilon_1, \varepsilon_2. (\alpha \xrightarrow{\varepsilon_1} \beta) \xrightarrow{\emptyset} \Big((\beta \xrightarrow{\varepsilon_2} \gamma) \xrightarrow{\emptyset} (\alpha \xrightarrow{\varepsilon_1 \cup \varepsilon_2} \gamma) \Big)$, $\varphi = \emptyset$

Aufgabe 10-3 Für das Typsystem mit Exceptions sind auf Folie 229 die Regeln der operationellen Semantik für Applikations-Terme angegeben. Geben Sie Regeln für die operationelle Semantik für `fun`, `let` und `op` an.

Lösung:

$$\frac{}{\texttt{fn}\ x \Rightarrow e_1 \longrightarrow \texttt{fn}\ x \Rightarrow e_1}$$

$$\frac{}{\texttt{fun}\ f\ x \Rightarrow e_1 \longrightarrow \texttt{fn}\ x \Rightarrow e_1[f \mapsto \texttt{fun}\ f\ x \Rightarrow e_1]}$$

$$\frac{e_1 \longrightarrow v_1 \qquad e_2[x \mapsto v_1] \longrightarrow v_2}{\texttt{let}\ x = e_1\ \texttt{in}\ e_2 \longrightarrow v_2}$$

$$\frac{e_1 \longrightarrow \texttt{raise}\ s}{\texttt{let}\ x = e_1\ \texttt{in}\ e_2 \longrightarrow \texttt{raise}\ s}$$

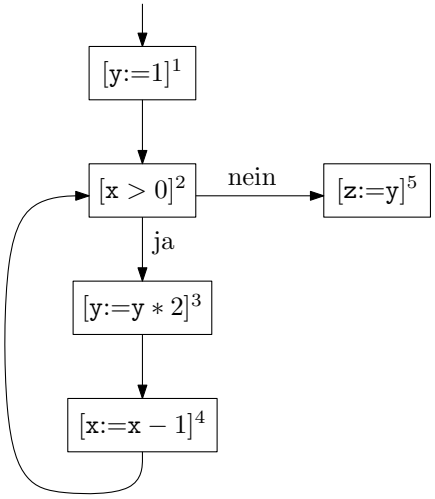
$$\frac{e_1 \longrightarrow v_1 \qquad e_2[x \mapsto v_1] \longrightarrow \texttt{raise}\ s}{\texttt{let}\ x = e_1\ \texttt{in}\ e_2 \longrightarrow \texttt{raise}\ s}$$

$$\frac{e_1 \longrightarrow v_1 \qquad e_2 \longrightarrow v_2 \qquad v = v_1\ \mathbf{op}\ v_2}{e_1\ \texttt{op}\ e_2 \longrightarrow v}$$

$$\frac{e_1 \longrightarrow \texttt{raise}\ s}{e_1\ \texttt{op}\ e_2 \longrightarrow \texttt{raise}s}$$

$$\frac{e_1 \longrightarrow v_1 \qquad e_2 \longrightarrow \texttt{raise}\ s}{e_1\ \texttt{op}\ e_2 \longrightarrow \texttt{raise}\ s}$$

Aufgabe 10-4 Gegeben sei folgender Kontrollflussgraph.



Vervollständigen Sie die folgenden Gleichungen, so dass eine Lösung für die Datenflussinklusionen für Hoare-Logik entsteht.

$$
\begin{aligned}
HL_{entry}(1) &= \\
HL_{exit}(1) &= \\
HL_{entry}(2) &= \{(\sigma_{init}, \sigma) \mid \sigma(\mathtt{y}) = 2^{\sigma_{init}(\mathtt{x})-\sigma(\mathtt{x})}, \sigma(\mathtt{x}) \geq 0\} = [\![(\mathtt{y} = 2^{\mathtt{x}_{init}-\mathtt{x}}) \wedge (\mathtt{x} \geq 0)]\!] \\
HL_{exit}(2) &= \\
HL_{entry}(3) &= \\
HL_{exit}(3) &= \\
HL_{entry}(4) &= \\
HL_{exit}(4) &= \\
HL_{entry}(5) &= \\
HL_{exit}(5) &= \{(\sigma_{init}, \sigma) \mid \sigma(\mathtt{z}) = 2^{\sigma_{init}(\mathtt{x})}\} = [\![(\mathtt{z} = 2^{\mathtt{x}_{init}})]\!]
\end{aligned}
$$

Lösung:

$$
\begin{aligned}
HL_{entry}(1) &= \{(\sigma_{init}, \sigma) \mid 1 = 2^{\sigma_{init}(\mathtt{x})-\sigma(\mathtt{x})}, \sigma(\mathtt{x}) \geq 0\} \\
HL_{exit}(1) &= \{(\sigma_{init}, \sigma) \mid \sigma(\mathtt{y}) = 2^{\sigma_{init}(\mathtt{x})-\sigma(\mathtt{x})}, \sigma(\mathtt{x}) \geq 0\} \\
HL_{entry}(2) &= \{(\sigma_{init}, \sigma) \mid \sigma(\mathtt{y}) = 2^{\sigma_{init}(\mathtt{x})-\sigma(\mathtt{x})}, \sigma(\mathtt{x}) \geq 0\} = [\![(\mathtt{y} = 2^{\mathtt{x}_{init}-\mathtt{x}}) \wedge (\mathtt{x} \geq 0)]\!] \\
HL_{exit}(2) &= \{(\sigma_{init}, \sigma) \mid \sigma(\mathtt{y}) = 2^{\sigma_{init}(\mathtt{x})-\sigma(\mathtt{x})}, \sigma(\mathtt{x}) \geq 0\} \\
HL_{entry}(3) &= \{(\sigma_{init}, \sigma) \mid 2\sigma(\mathtt{y}) = 2^{\sigma_{init}(\mathtt{x})-\sigma(\mathtt{x})+1}, \sigma(\mathtt{x}) > 0\} \\
&= \{(\sigma_{init}, \sigma) \mid \sigma(\mathtt{y}) = 2^{\sigma_{init}(\mathtt{x})-\sigma(\mathtt{x})}, \sigma(\mathtt{x}) > 0\} \\
HL_{exit}(3) &= \{(\sigma_{init}, \sigma) \mid \sigma(\mathtt{y}) = 2^{\sigma_{init}(\mathtt{x})-\sigma(\mathtt{x})+1}, \sigma(\mathtt{x}) > 0\} \\
HL_{entry}(4) &= \{(\sigma_{init}, \sigma) \mid \sigma(\mathtt{y}) = 2^{\sigma_{init}(\mathtt{x})-(\sigma(\mathtt{x})-1)}, \sigma(\mathtt{x}) - 1 \geq 0\} \\
&= \{(\sigma_{init}, \sigma) \mid \sigma(\mathtt{y}) = 2^{\sigma_{init}(\mathtt{x})-\sigma(\mathtt{x})+1}, \sigma(\mathtt{x}) > 0\} \\
HL_{exit}(4) &= \{(\sigma_{init}, \sigma) \mid \sigma(\mathtt{y}) = 2^{\sigma_{init}(\mathtt{x})-\sigma(\mathtt{x})}, \sigma(\mathtt{x}) \geq 0\} \\
HL_{entry}(5) &= \{(\sigma_{init}, \sigma) \mid \sigma(\mathtt{y}) = 2^{\sigma_{init}(\mathtt{x})}\} \\
HL_{exit}(5) &= \{(\sigma_{init}, \sigma) \mid \sigma(\mathtt{z}) = 2^{\sigma_{init}(\mathtt{x})}\} = [\![\mathtt{z} = 2^{\mathtt{x}_{init}}]\!]
\end{aligned}
$$

Folgern Sie, dass das Hoare-Tripel $\{\mathtt{x} \geq 0\}\ P\ \{\mathtt{z} = 2^{x_{init}}\}$ gültig ist, wobei P das durch den Kontrollflussgraphen gegebene Programm ist.