IMP: Eingaben

$$S \in \mathrm{Stm} ::= \ldots \mid \texttt{newvar}\ x\ \texttt{:=}\ a\ \texttt{in}\ S \mid \texttt{abort} \mid \texttt{out}\ a \mid \texttt{in}\ x$$

Erweiterter, rekursiver semantischer Bereich

$$\Omega \cong (\hat{\Sigma} + (\mathbb{Z} \times \Omega) + (\mathbb{Z} \to \Omega))_\perp$$

Isomorphismus $\Omega \underset{\psi}{\overset{\varphi}{\rightleftarrows}} (\hat{\Sigma} + (\mathbb{Z} \times \Omega) + (\mathbb{Z} \to \Omega))_\perp$

Injektionen

$$\iota_{\mathrm{norm}} : \Sigma \to \hat{\Sigma} \qquad \iota_{\mathrm{norm}}\sigma = \sigma$$

$$\iota_{\mathrm{abnorm}} : \Sigma \to \hat{\Sigma} \qquad \iota_{\mathrm{abnorm}}\sigma = (\texttt{abort}, \sigma)$$

$$\psi \circ \lfloor - \rfloor \circ \iota_1 \circ \iota_{\mathrm{norm}} = \iota_{\mathrm{term}} : \Sigma \to \Omega$$

$$\psi \circ \lfloor - \rfloor \circ \iota_1 \circ \iota_{\mathrm{abnorm}} = \iota_{\mathrm{abort}} : \Sigma \to \Omega$$

$$\psi \circ \lfloor - \rfloor \circ \iota_2 = \iota_{\mathrm{out}} : (\mathbb{Z} \times \Omega) \to \Omega$$

$$\psi \circ \lfloor - \rfloor \circ \iota_3 = \iota_{\mathrm{in}} : (\mathbb{Z} \to \Omega) \to \Omega$$

IMP: Eingaben

Funktionserweiterung $f : \Sigma \to \Omega$ zu $f_* : \Omega \to \Omega$

$$
\begin{aligned}
f_* \bot_\Omega &= \bot_\Omega \\
f_*(\iota_{\text{term}}\, \sigma) &= f\, \sigma \\
f_*(\iota_{\text{abort}}\, \sigma) &= \iota_{\text{abort}} \sigma \\
f_*(\iota_{\text{out}}(n, \omega)) &= \iota_{\text{out}}(n, f_*\, \omega) \\
f_*(\iota_{\text{in}}\, g) &= \iota_{\text{in}}(\lambda v\, .\, f_*(g\, v))
\end{aligned}
$$

Funktionserweiterung $f : \Sigma \to \Sigma$ zu $f_\dagger : \Omega \to \Omega$

$$
\begin{aligned}
f_\dagger \bot_\Omega &= \bot_\Omega \\
f_\dagger(\iota_{\text{term}}\, \sigma) &= \iota_{\text{term}}(f\, \sigma) \\
f_\dagger(\iota_{\text{abort}}\, \sigma) &= \iota_{\text{abort}}(f\, \sigma) \\
f_\dagger(\iota_{\text{out}}(n, \omega)) &= \iota_{\text{out}}(n, f_\dagger\, \omega) \\
f_\dagger(\iota_{\text{in}}\, g) &= \iota_{\text{in}}(\lambda v\, .\, f_\dagger(g\, v))
\end{aligned}
$$

IMP: Eingaben

$$S \in \mathrm{Stm} ::= \ldots \mid \texttt{newvar}\ x\ \texttt{:=}\ a\ \texttt{in}\ S \mid \texttt{abort} \mid \texttt{out}\ a \mid \texttt{in}\ x$$

Semantische Funktion $\mathcal{S}[\![-]\!] : \mathrm{Stm} \to [\Sigma \to \Omega]$

$$\mathcal{S}[\![\texttt{skip}]\!] = \iota_{\mathrm{term}}$$
$$\mathcal{S}[\![x\ \texttt{:=}\ a]\!] = \lambda\sigma\,.\,\iota_{\mathrm{term}}\sigma[x \mapsto \mathcal{A}[\![a]\!]\,\sigma]$$
$$\mathcal{S}[\![S_1\ \texttt{;}\ S_2]\!] = \mathcal{S}[\![S_2]\!]_* \circ \mathcal{S}[\![S_1]\!]$$
$$\mathcal{S}[\![\texttt{if}\ b\ \texttt{then}\ S_1\ \texttt{else}\ S_2]\!] = \mathrm{ite}(\mathcal{B}[\![b]\!], \mathcal{S}[\![S_1]\!], \mathcal{S}[\![S_2]\!])$$
$$\mathcal{S}[\![\texttt{while}\ b\ \texttt{do}\ S]\!] = \mathbf{Y}_{[\Sigma\to\Omega]}(\lambda f\,.\,\mathrm{ite}(\mathcal{B}[\![b]\!], f_* \circ \mathcal{S}[\![S]\!], \iota_{\mathrm{term}}))$$
$$\mathcal{S}[\![\texttt{newvar}\ x\ \texttt{:=}\ a\ \texttt{in}\ S]\!] =$$
$$\lambda\sigma\,.\,(\lambda\sigma' \in \Sigma\,.\,\sigma'[x \mapsto \sigma(x)])_\dagger(\mathcal{S}[\![S]\!](\sigma[x \mapsto \mathcal{A}[\![a]\!]\,\sigma]))$$
$$\mathcal{S}[\![\texttt{out}\ a]\!] = \lambda\sigma\,.\,\iota_{\mathrm{out}}(\mathcal{A}[\![a]\!]\,\sigma, \iota_{\mathrm{term}}\sigma)$$
$$\mathcal{S}[\![\texttt{in}\ x]\!] = \lambda\sigma\,.\,\iota_{\mathrm{in}}(\lambda v\,.\,\iota_{\mathrm{term}}(\sigma[x \mapsto v]))$$

IMP: Fortsetzungssemantik

$$S \in \mathrm{Stm} ::= \ldots \mid \texttt{newvar}\ x\ \texttt{:=}\ a\ \texttt{in}\ S$$

Semantische Funktion $\mathcal{C}[\![-]\!] : \mathrm{Stm} \to [\Sigma \to \mathrm{P}] \to [\Sigma \to \mathrm{P}]$

$$\mathcal{C}[\![\texttt{skip}]\!]\,\kappa = \kappa$$
$$\mathcal{C}[\![x\ \texttt{:=}\ a]\!]\,\kappa = \lambda\sigma\,.\,\kappa\,\sigma[x \mapsto \mathcal{A}[\![a]\!]\,\sigma]$$
$$\mathcal{C}[\![S_1\ \texttt{;}\ S_2]\!]\,\kappa = \mathcal{C}[\![S_1]\!]\,(\mathcal{C}[\![S_2]\!]\,\kappa)$$
$$\mathcal{C}[\![\texttt{if}\ b\ \texttt{then}\ S_1\ \texttt{else}\ S_2]\!]\,\kappa = \mathrm{ite}(\mathcal{B}[\![b]\!], \mathcal{C}[\![S_1]\!]\,\kappa, \mathcal{C}[\![S_2]\!]\,\kappa)$$
$$\mathcal{C}[\![\texttt{while}\ b\ \texttt{do}\ S]\!]\,\kappa = \mathbf{Y}_{[\Sigma\to\mathrm{P}]}(\lambda\kappa'\,.\,\mathrm{ite}(\mathcal{B}[\![b]\!], \mathcal{C}[\![S]\!]\,\kappa', \kappa))$$
$$\mathcal{C}[\![\texttt{newvar}\ x\ \texttt{:=}\ a\ \texttt{in}\ S]\!]\,\kappa = \lambda\sigma\,.\,\mathcal{C}[\![S]\!](\lambda\sigma' \in \Sigma\,.\,\kappa\,\sigma'[x \mapsto \sigma(x)])(\sigma[x \mapsto \mathcal{A}[\![a]\!]\,\sigma])$$

parametrisch in Bereich P

Für $\mathrm{P} = \Sigma_\perp$ $\qquad \mathcal{C}[\![S]\!]\,\kappa\,\sigma = \kappa_{\perp\!\!\perp}(\mathcal{S}[\![S]\!]\,\sigma)$

IMP: Fortsetzungssemantik

$$S \in \mathrm{Stm} ::= \ldots \mid \texttt{newvar}\ x\ \texttt{:=}\ a\ \texttt{in}\ S \mid \texttt{abort} \mid \texttt{out}\ a \mid \texttt{in}\ x$$

$$\mathcal{C}[\![-]\!] : \mathrm{Stm} \to [\Sigma \to \Omega] \to [\Sigma \to \Omega] \to [\Sigma \to \Omega]$$

$$\mathcal{C}[\![\texttt{skip}]\!]\,\kappa_\mathrm{t}\,\kappa_\mathrm{f} = \kappa_\mathrm{t}$$

$$\mathcal{C}[\![x\ \texttt{:=}\ a]\!]\,\kappa_\mathrm{t}\,\kappa_\mathrm{f} = \lambda\sigma\,.\,\kappa_\mathrm{t}\,\sigma[x \mapsto \mathcal{A}[\![a]\!]\,\sigma]$$

$$\mathcal{C}[\![S_1\ \texttt{;}\ S_2]\!]\,\kappa_\mathrm{t}\,\kappa_\mathrm{f} = \mathcal{C}[\![S_1]\!]\,(\mathcal{C}[\![S_2]\!]\,\kappa_\mathrm{t}\,\kappa_\mathrm{f})\,\kappa_\mathrm{f}$$

$$\mathcal{C}[\![\texttt{if}\ b\ \texttt{then}\ S_1\ \texttt{else}\ S_2]\!]\,\kappa_\mathrm{t}\,\kappa_\mathrm{f} = \mathrm{ite}(\mathcal{B}[\![b]\!], \mathcal{C}[\![S_1]\!]\,\kappa_\mathrm{t}\,\kappa_\mathrm{f}, \mathcal{C}[\![S_2]\!]\,\kappa_\mathrm{t}\,\kappa_\mathrm{f})$$

$$\mathcal{C}[\![\texttt{while}\ b\ \texttt{do}\ S]\!]\,\kappa_\mathrm{t}\,\kappa_\mathrm{f} = \mathbf{Y}_{[\Sigma\to\Omega]}(\lambda\kappa'\,.\,\mathrm{ite}(\mathcal{B}[\![b]\!], \mathcal{C}[\![S]\!]\,\kappa'\,\kappa_\mathrm{f}, \kappa_\mathrm{t}))$$

$$\mathcal{C}[\![\texttt{newvar}\ x\ \texttt{:=}\ a\ \texttt{in}\ S]\!]\,\kappa_\mathrm{t}\,\kappa_\mathrm{f} =$$

$$\lambda\sigma\,.\,\mathcal{C}[\![S]\!](\lambda\sigma'\,.\,\kappa_\mathrm{t}\,\sigma'[x \mapsto \sigma(x)])$$

$$(\lambda\sigma'\,.\,\kappa_\mathrm{f}\,\sigma'[x \mapsto \sigma(x)])(\sigma[x \mapsto \mathcal{A}[\![a]\!]\,\sigma])$$

$$\mathcal{C}[\![\texttt{abort}]\!]\,\kappa_\mathrm{t}\,\kappa_\mathrm{f} = \kappa_\mathrm{f}$$

$$\mathcal{C}[\![\texttt{out}\ a]\!]\,\kappa_\mathrm{t}\,\kappa_\mathrm{f} = \lambda\sigma\,.\,\iota_\mathrm{out}(\mathcal{A}[\![a]\!]\,\sigma, \kappa_\mathrm{t}\,\sigma)$$

$$\mathcal{C}[\![\texttt{in}\ x]\!]\,\kappa_\mathrm{t}\,\kappa_\mathrm{f} = \lambda\sigma\,.\,\iota_\mathrm{in}(\lambda v \in \mathbb{Z}\,.\,\kappa_\mathrm{t}\,\sigma[x \mapsto v])$$

IMP: Ausnahmen

$$e \in \mathrm{Exc}$$

$$S \in \mathrm{Stm} ::= \ldots \mid \texttt{begin}\ S_1\ \texttt{handle}\ e\texttt{:}\ S_2 \mid \texttt{raise}\ e$$

$$\mathcal{C}[\![-]\!] : \mathrm{Stm} \to (\mathrm{Exc} \to [\Sigma \to \mathrm{P}]) \to [\Sigma \to \mathrm{P}] \to [\Sigma \to \mathrm{P}]$$

$$\mathcal{C}[\![\texttt{skip}]\!]\,\eta\,\kappa = \lambda\sigma\,.\,\kappa\sigma$$
$$\mathcal{C}[\![x\ \texttt{:=}\ a]\!]\,\eta\,\kappa = \lambda\sigma\,.\,\kappa(\sigma[x \mapsto \mathcal{A}[\![a]\!]\,\sigma])$$
$$\mathcal{C}[\![S_1\ \texttt{;}\ S_2]\!]\,\eta\,\kappa = \lambda\sigma\,.\,\mathcal{C}[\![S_1]\!]\,\eta(\lambda\sigma'\,.\,\mathcal{C}[\![S_2]\!]\,\eta\,\kappa\,\sigma')\sigma$$
$$\mathcal{C}[\![\texttt{if}\ b\ \texttt{then}\ S_1\ \texttt{else}\ S_2]\!]\,\eta\,\kappa = \mathrm{ite}(\mathcal{B}[\![b]\!], \mathcal{C}[\![S_1]\!]\,\eta\,\kappa, \mathcal{C}[\![S_2]\!]\,\eta\,\kappa)$$
$$\mathcal{C}[\![\texttt{while}\ b\ \texttt{do}\ S]\!]\,\eta\,\kappa = \mathbf{Y}_{[\Sigma\to\mathrm{P}]}(\lambda\kappa'\,.\,\mathrm{ite}(\mathcal{B}[\![b]\!], \mathcal{C}[\![S]\!]\,\eta\,\kappa', \kappa))$$
$$\mathcal{C}[\![\texttt{begin}\ S_1\ \texttt{handle}\ e\texttt{:}\ S_2]\!]\,\eta\,\kappa = \mathcal{C}[\![S_1]\!](\eta[e \mapsto \mathcal{C}[\![S_2]\!]\,\eta\,\kappa])\,\kappa$$
$$\mathcal{C}[\![\texttt{raise}\ e]\!]\,\eta\,\kappa = \eta e$$

ASSN: Syntaktische Kategorien

$$
\begin{aligned}
n &\in \mathrm{Num} \\
x &\in \mathrm{Var} \\
X &\in \mathrm{Log}
\end{aligned}
$$

$$
\begin{aligned}
t \in \mathrm{Term} ::= {} & n \mid x \mid X \\
& \mid t_1 + t_2 \mid t_1 - t_2 \mid t_1 \cdot t_2 \\
A \in \mathrm{Frm} ::= {} & tt \mid ff \\
& \mid t_1 = t_2 \mid t_1 \leq t_2 \\
& \mid \neg A \mid A_1 \wedge A_2 \mid A_1 \vee A_2 \mid A_1 \Rightarrow A_2 \\
& \mid \forall X \,.\, A \mid \exists X \,.\, A
\end{aligned}
$$

ASSN: Freie logische Variablen

$$\mathrm{flog} : \mathrm{Term} \cup \mathrm{Frm} \to \wp\mathrm{Log}$$

$$\mathrm{flog}(n) = \mathrm{flog}(x) = \emptyset$$
$$\mathrm{flog}(X) = \{X\}$$
$$\mathrm{flog}(t_1 + t_2) = \mathrm{flog}(t_1 - t_2) = \mathrm{flog}(t_1 \cdot t_2) = \mathrm{flog}(t_1) \cup \mathrm{flog}(t_2)$$

$$\mathrm{flog}(tt) = \mathrm{flog}(ff) = \emptyset$$
$$\mathrm{flog}(t_1 = t_2) = \mathrm{flog}(t_1 \leq t_2) = \mathrm{flog}(t_1) \cup \mathrm{flog}(t_2)$$
$$\mathrm{flog}(\neg A) = \mathrm{flog}(A)$$
$$\mathrm{flog}(A_1 \wedge A_2) = \mathrm{flog}(A_1 \vee A_2) = \mathrm{flog}(A_1 \Rightarrow A_2) = \mathrm{flog}(A_1) \cup \mathrm{flog}(A_2)$$
$$\mathrm{flog}(\forall X \,.\, A) = \mathrm{flog}(\exists X \,.\, A) = \mathrm{flog}(A) \setminus \{X\}$$

ASSN: Substitutionen

Substitution $\zeta : \mathrm{Log} \to \mathrm{Term}$

Für $A \in \mathrm{Frm}$ sei $X_{\zeta,A}\ \varepsilon\ \mathrm{Log} \setminus \bigcup\{\mathrm{flog}(\zeta(X')) \mid X' \in \mathrm{flog}(A) \setminus \{X\}\}$.

$$n\zeta = n, \qquad x\zeta = x, \qquad X\zeta = \zeta X$$

$$(t_1\ bop\ t_2)\zeta = (t_1\zeta)\ bop\ (t_2\zeta), \quad \text{für } bop \in \{+, -, \cdot\}$$

$$(t_1\ bop\ t_2)\zeta = (t_1\zeta)\ bop\ (t_2\zeta), \quad \text{für } bop \in \{=, \leq\}$$

$$(\neg A)\zeta = \neg(A\zeta)$$

$$(A_1\ bop\ A_2)\zeta = (A_1\zeta)\ bop\ (A_2\zeta), \quad \text{für } bop \in \{\wedge, \vee, \Rightarrow\}$$

$$(QX\,.\,A)\zeta = QX_{A,\zeta}\,.\,A(\zeta[X \mapsto X_{A,\zeta}]), \quad \text{für } Q \in \{\forall, \exists\}$$

Analog für Substitutionen $\zeta : \mathrm{Var} \to \mathrm{Term}$

ASSN: Kompositionale Semantik von Termen

Semantischer Bereich

- Interpretationen $\quad Val = \mathrm{Log} \to \mathbb{Z}$

Semantische Funktion $\quad \mathcal{T}[\![-]\!] : \mathrm{Term} \to (Val \to \Sigma \to \mathbb{Z})$

$$\mathcal{T}[\![n]\!]\, I\, \sigma = \mathcal{N}[\![n]\!]$$
$$\mathcal{T}[\![x]\!]\, I\, \sigma = \sigma(x)$$
$$\mathcal{T}[\![X]\!]\, I\, \sigma = I(x)$$

$$\mathcal{T}[\![t_1 + t_2]\!]\, I\, \sigma = \mathcal{T}[\![t_1]\!]\, I\, \sigma + \mathcal{T}[\![t_2]\!]\, I\, \sigma$$
$$\mathcal{T}[\![t_1 - t_2]\!]\, I\, \sigma = \mathcal{T}[\![t_1]\!]\, I\, \sigma - \mathcal{T}[\![t_2]\!]\, I\, \sigma$$
$$\mathcal{T}[\![t_1 \cdot t_2]\!]\, I\, \sigma = \mathcal{T}[\![t_1]\!]\, I\, \sigma \cdot \mathcal{T}[\![t_2]\!]\, I\, \sigma$$

Einbettung von AExp in Term $(+ \mapsto +,\ - \mapsto -,\ \star \mapsto \cdot)$

ASSN: Gültigkeit von Formeln

Semantische Relation $\models \subseteq (\mathit{Val} \times \Sigma) \times \mathrm{Frm}$

$I, \sigma \models tt$

$I, \sigma \models t_1 = t_2$, falls $\mathcal{T}[\![t_1]\!]\, I\, \sigma = \mathcal{T}[\![t_2]\!]\, I\, \sigma$

$I, \sigma \models t_1 \leq t_2$, falls $\mathcal{T}[\![t_1]\!]\, I\, \sigma \leq \mathcal{T}[\![t_2]\!]\, I\, \sigma$

$I, \sigma \models \neg A$, falls $I, \sigma \not\models A$

$I, \sigma \models A_1 \wedge A_2$, falls $I, \sigma \models A_1$ und $I, \sigma \models A_2$

$I, \sigma \models A_1 \vee A_2$, falls $I, \sigma \models A_1$ oder $I, \sigma \models A_2$

$I, \sigma \models A_1 \Rightarrow A_2$, falls $I, \sigma \not\models A_1$ oder $I, \sigma \models A_2$

$I, \sigma \models \forall X\,.\,A$, falls $I[X \mapsto v], \sigma \models A$ für alle $v \in \mathbb{Z}$

$I, \sigma \models \exists X\,.\,A$, falls $I[X \mapsto v], \sigma \models A$ für ein $v \in \mathbb{Z}$

- Erweiterung zu $\models_{\perp\!\!\!\perp} \subseteq (\mathit{Val} \times \Sigma_\perp) \times \mathrm{Frm}$ mit $I, \perp \models_{\perp\!\!\!\perp} A$
- $I \models A \iff \forall \sigma \in \Sigma\,.\, I, \sigma \models A$
- $\models A \iff \forall I \in \mathit{Val},\ \sigma \in \Sigma\,.\, I, \sigma \models A$

Einbettung von BExp in Frm ($\texttt{true} \mapsto tt$, $\texttt{false} \mapsto ff$, $= \mapsto =$, &c.)

ASSN: Substitutionslemmata

Lemma Seien $I \in \mathit{Val}$, $\sigma \in \Sigma$, $t, t' \in \mathrm{Term}$, $A \in \mathrm{Frm}$ und $X \in \mathrm{Log}$.

1. $\mathcal{T}[\![t[X \mapsto t']]\!]\, I\, \sigma = \mathcal{T}[\![t]\!]\, I[X \mapsto \mathcal{T}[\![t']\!]\, I\, \sigma]\, \sigma$;
2. $I, \sigma \models A[X \mapsto t] \iff I[X \mapsto \mathcal{T}[\![t]\!]\, I\, \sigma], \sigma \models A$.

Lemma Seien $I \in \mathit{Val}$, $\sigma \in \Sigma$, $t, t' \in \mathrm{Term}$, $A \in \mathrm{Frm}$ und $x \in \mathrm{Var}$.

1. $\mathcal{T}[\![t[x \mapsto t']]\!]\, I\, \sigma = \mathcal{T}[\![t]\!]\, I\, \sigma[x \mapsto \mathcal{T}[\![t']\!]\, I\, \sigma]$;
2. $I, \sigma \models A[x \mapsto t] \iff I, \sigma[x \mapsto \mathcal{T}[\![t]\!]\, I\, \sigma] \models A$.

IMP/ASSN: Hoare-Tripel für partielle Korrektheit

Partielle Korrektheitsaussage $\{A\}\, S\, \{A'\}$ mit $A, A' \in \mathrm{Frm}$, $S \in \mathrm{Stm}$

Gültigkeitsrelation $I \in \mathit{Val}$, $\sigma \in \Sigma$, $A, A' \in \mathrm{Frm}$

$$I, \sigma \models \{A\}\, S\, \{A'\} \iff (I, \sigma \models A \Rightarrow I, \mathcal{S}[\![S]\!]\, \sigma \models_{\perp\!\!\!\perp} A')$$

- $I \models \{A\}\, S\, \{A'\} \iff \forall \sigma \in \Sigma\,.\, I, \sigma \models \{A\}\, S\, \{A'\}$
- $\models \{A\}\, S\, \{A'\} \iff \forall I \in \mathit{Val},\ \sigma \in \Sigma\,.\, I, \sigma \models \{A\}\, S\, \{A'\}$

Ableitbarkeitsrelation

- $\vdash$ gemäß Hoare-Kalkül für partielle Korrektheit

IMP/ASSN: Hoare-Kalkül für partielle Korrektheit

(skip$_{hp}$) $\{A\}\ \texttt{skip}\ \{A\}$

(assign$_{hp}$) $\{A[x \mapsto a]\}\ x := a\ \{A\}$

(seq$_{hp}$) $$\frac{\{A\}\ S_1\ \{A'\} \qquad \{A'\}\ S_2\ \{A''\}}{\{A\}\ S_1\ ;\ S_2\ \{A''\}}$$

(if$_{hp}$) $$\frac{\{A \wedge b\}\ S_1\ \{A'\} \qquad \{A \wedge \neg b\}\ S_2\ \{A'\}}{\{A\}\ \texttt{if}\ b\ \texttt{then}\ S_1\ \texttt{else}\ S_2\ \{A'\}}$$

(while$_{hp}$) $$\frac{\{A \wedge b\}\ S\ \{A\}}{\{A\}\ \texttt{while}\ b\ \texttt{do}\ S\ \{A \wedge \neg b\}}$$

(cons$_{hp}$) $$\frac{\{A_1'\}\ S\ \{A_2'\}}{\{A_1\}\ S\ \{A_2\}},$$ falls $\models A_1 \Rightarrow A_1'$, $\models A_2' \Rightarrow A_2$