Operacijska semantika jezika IMP

↑ pomen podamo prek pravil izvajanja

Imamo množice Exp, BExp, Cmd vseh možnih izrazov.
Kako jim bi podali pomen?

- prek transformacij med izrazi
  - if true then c_1 else $c_2 \rightsquigarrow c_1$
  - op. sem. malih korakov
  - $\rightsquigarrow$ je relacija na Cmd
  - $\rightsquigarrow \subseteq Cmd \times Cmd$
- prek transformacij v končne vrednosti
  - če $e_1 \Downarrow m_1$ in $e_2 \Downarrow m_2$, potem $e_1 + e_2 \Downarrow m_1 + m_2$
  - op. sem. velikih korakov
  - $\Downarrow$ je relacija med Exp in $\mathbb{Z}$
  - $\Downarrow \subseteq Exp \times \mathbb{Z}$
- prek funkcij
  - $[\![e_1 + e_2]\!] = [\![e_1]\!] + [\![e_2]\!]$
  - den. semantika
  - $[\![\cdot]\!] : Exp \to \mathbb{Z}$

Definirajmo relacijo $s, e \Downarrow m$ med dolji, aritmetičnimi izrazi in celimi števili kot najmanjšo relacijo, zaprto za pravila:

$\Downarrow \subseteq S \times Exp \times \mathbb{Z}$

$$\frac{}{s, m \Downarrow m} \qquad \frac{s, e_1 \Downarrow m_1 \quad s, e_2 \Downarrow m_2}{s, e_1 + e_2 \Downarrow m_1 + m_2}$$

$$\frac{s, e_1 \Downarrow m_1 \quad s, e_2 \Downarrow m_2}{s, e_1 - e_2 \Downarrow m_1 - m_2} \qquad \frac{s, e_1 \Downarrow m_1 \quad s, e_2 \Downarrow m_2}{s, e_1 * e_2 \Downarrow m_1 \cdot m_2}$$

$$\frac{}{s, l \Downarrow s(l)} \; (s(l) \neq \perp)$$

↑ ob pogoju

$$\frac{h_1 \; h_2 \; \cdots \; h_m}{c}$$

Če veljajo hipoteze $h_1, h_2, \ldots, h_m$, potem velja zaključek c.

$\mathbb{L}$ .. množica možnih lokacij

$S = \mathbb{Z}^{\mathbb{L}}_{\perp}$

$A_\perp$ ... dvig A

$A_\perp = A + \{\perp\}$ (dno)

$S, b \Downarrow p$ V okolju S se logični izraz b evaluira v resničnostno vrednost $p \in \{tt, ff\}$

$$\frac{}{S, \text{true} \Downarrow tt} \qquad \frac{}{S, \text{false} \Downarrow ff} \qquad \frac{S, e_1 \Downarrow m_1 \quad S, e_2 \Downarrow m_1}{S, e_1 = e_2 \Downarrow m_1 = m_2}$$

$= : \mathbb{Z} \times \mathbb{Z} \to \{tt, ff\}$

$$\frac{S, e_1 \Downarrow m_1 \quad S, e_2 \Downarrow m_1}{S, e_1 < e_2 \Downarrow m_1 < m_2} \qquad \frac{S, e_1 \Downarrow m_1 \quad S, e_2 \Downarrow m_1}{S, e_1 > e_2 \Downarrow m_1 > m_2}$$

$S, c \Downarrow S'$ ukaz c stanje S spremeni v S'

$$\frac{}{S, \text{skip} \Downarrow S} \qquad \frac{S, c_1 \Downarrow S' \quad S', c_2 \Downarrow S''}{S, c_1; c_2 \Downarrow S''} \qquad \frac{S, e \Downarrow m}{S, l := e \Downarrow S[l := m]}$$

$$\mathcal{R} = \{ \ldots \underbrace{\{(S, \text{false}, ff), (S, \text{skip}, S)\}}_{H}, (S, \text{if true then skip else} \ldots, S) \}$$

$$\frac{S, b \Downarrow tt \qquad S, c_1 \Downarrow S'}{S, \text{if } b \text{ then } c_1 \text{ else } c_2 \Downarrow S'}$$

$$S[l := m] := l' \mapsto \begin{cases} m & l = l' \\ S(l') & \text{sicer} \end{cases}$$

$$\emptyset := l \mapsto \bot$$

$$\frac{S, b \Downarrow ff \qquad S, c_2 \Downarrow S'}{S, \text{if } b \text{ then } c_1 \text{ else } c_2 \Downarrow S'}$$

$$\frac{S, b \Downarrow tt \quad S, c \Downarrow S' \quad S', \text{while } b \text{ do } c \Downarrow S''}{S, \text{while } b \text{ do } c \Downarrow S''} \qquad \frac{S, b \Downarrow ff}{S, \text{while } b \text{ do } c \Downarrow S}$$

$$\frac{\dfrac{\dfrac{\dfrac{}{S_0, b \Downarrow tt} \quad \dfrac{}{S_0, c \Downarrow S_1}}{S_0, \text{while } b \text{ do } c \Downarrow S_n} \quad \dfrac{\dfrac{}{S_1, b \Downarrow tt} \quad \dfrac{}{S_1, c \Downarrow S_2}}{S_1, \text{while } b \text{ do } c \Downarrow S_n}}{\Downarrow S_n} \quad \dfrac{\dfrac{\vdots}{S_n, b \Downarrow ff}}{\Downarrow S_n}}{S_2, \text{while } b \text{ do } c \Downarrow S_n}$$

Drevo izpeljave za $\emptyset, l := 6; m := 7 * 6 \Downarrow [l := 6, m := 42]$

↳ v korenu je zaključek
↳ vozlišča so pravila relacij
↳ listi so aksiomi

$$\dfrac{\dfrac{}{\emptyset, 6 \Downarrow 6}}{\emptyset, l := 6 \Downarrow [l := 6]} \qquad \dfrac{\dfrac{\dfrac{}{[l := 6], 7 \Downarrow 7} \quad \dfrac{}{[l := 6], l \Downarrow 6}}{[l := 6], 7 * l \Downarrow 42}}{[l := 6], m := 7 * l \Downarrow [l := 6, m := 42]}$$

$$\dfrac{\emptyset, l := 6 \Downarrow [l := 6] \qquad [l := 6], m := 7 * l \Downarrow [l := 6, m := 42]}{\emptyset, l := 6; m := 7 * l \Downarrow [l := 6, m := 42]}$$

$$l' \mapsto \begin{cases} 6 & l' = l \\ 42 & l' = m \\ \bot & \text{sicer} \end{cases}$$

Ali znamo pokazati $\forall e.\ \exists n.\ \emptyset, e \Downarrow n$?

$$\dfrac{???}{\emptyset, l \Downarrow 42}$$

To ni res, želimo se omejiti samo na smiselne programe.

$L \vdash e$ ... izraz e je dobro definiran glede na množico lokacij $L \subseteq \mathbb{L}$

$$\dfrac{}{L \vdash n} \qquad \dfrac{(l \in L)}{L \vdash l} \qquad \dfrac{L \vdash e_1 \quad L \vdash e_2}{L \vdash e_1 + e_2} \qquad \dfrac{L \vdash e_1 \quad L \vdash e_2}{L \vdash e_1 - e_2}$$

$$\dfrac{L \vdash e_1 \quad L \vdash e_2}{L \vdash e_1 * e_2}$$

$L \vdash b$ ... logični izraz b —//—

$$\dfrac{}{L \vdash \text{true}} \qquad \dfrac{}{L \vdash \text{false}} \qquad \dfrac{L \vdash e_1 \quad L \vdash e_2}{L \vdash e_1 = e_2} \qquad \dfrac{L \vdash e_1 \quad L \vdash e_2}{L \vdash e_1 < e_2} \qquad \dfrac{L \vdash e_1 \quad L \vdash e_2}{L \vdash e_1 > e_2}$$

$dom(s) = \{ \ell \mid s(\ell) \neq \perp \}$

Trditev 1 Če velja $dom(s) \vdash e$, potem $\exists m \in \mathbb{Z}.\ s, e \Downarrow m$.

Dokaz Indukcija na velikost drevesa izpeljave za $dom(s) \vdash e$.
Analizirajmo primer, kako smo prišli do $dom(s) \vdash e$.

- $\dfrac{}{dom(s) \vdash n}$ potem je $e = n$, torej velja $s, e \Downarrow n$
- $\dfrac{\ell \in dom(s)}{dom(s) \vdash \ell}$ potem je $e = \ell$, za katerega velja $\ell \in dom(s)$, zato je $s(\ell) \neq \perp$, zato velja $s, \ell \Downarrow s(\ell)$.
- $\dfrac{dom(s) \vdash e_1 \quad dom(s) \vdash e_2}{dom(s) \vdash e_1 + e_2}$ Potem je $e = e_1 + e_2$ in velja $dom(s) \vdash e_1$ ter $dom(s) \vdash e_2$. Ker imata $dom(s) \vdash e_1$ in $dom(s) \vdash e_2$ manjši drevesi izpeljave, po indukcijski predpostavki dobimo $\exists m_1 \in \mathbb{Z}.\ s, e_1 \Downarrow m_1$. Podobno $\exists m_2 \in \mathbb{Z}.\ s, e_2 \Downarrow m_2$. Torej $s, e_1 + e_2 \Downarrow m_1 + m_2$
- $-$ in $*$ analogno.

Trditev 2 Če velja $dom(s) \vdash b$, potem $\exists p \in \{tt, ff\}.\ s, b \Downarrow p$.

$L \vdash c : L'$ ... ukaz c je dobro definiran glede na L in po njegovem izvajanju so definirane lokacije L'.

$$\frac{}{L \vdash skip : L} \qquad \frac{L \vdash c_1 : L' \quad L' \vdash c_2 : L''}{L \vdash c_1; c_2 : L''} \qquad \frac{L \vdash e}{L \vdash \ell := e : L \cup \{\ell\}}$$

$$\frac{L \vdash b \quad L \vdash c_1 : L_1 \quad L \vdash c_2 : L_2}{L \vdash \text{if } b \text{ then } c_1 \text{ else } c_2 : L_1 \cap L_2} \qquad \frac{L \vdash b \quad L \vdash c : L'}{L \vdash \text{while } b \text{ do } c : L'}$$

Konstrukcija in lastnosti najmanjše podmnožice, zaprte za pravila

X osnovna množica

Soda števila:

$\frac{}{0 \text{ sodo}}$ $\qquad$ $\frac{n \text{ sodo}}{n+2 \text{ sodo}}$

R množica pravil $\subseteq \mathcal{P}_f(X) \times X$

Pravilo $\frac{h_1 \dots h_n}{c}$ predstavimo s parom $(\{h_1, \dots, h_n\}, c)$.

Natančneje, pravila $\frac{\cdots}{\cdots}$ bodo vzorci za vse možne elemente v R.

$R = \{(\emptyset, 0), (\{0\}, 2), (\{2\}, 4), (\{1\}, 3), (\{3\}, 5), (\{4\}, 6), \dots\}$

$A \subseteq X$ je zaprta za $R \iff \forall (H, c) \in R.\ H \subseteq A \Rightarrow c \in A.$

$F_R : \mathcal{P}(X) \to \mathcal{P}(X)$

$F_R(A) = \{c \in X \mid \exists (H, c) \in R.\ H \subseteq A\}$

A je zaprta za $R \iff F_R(A) \subseteq A.$

$\frac{h_1 \in A \dots h_n \in A}{c \in F_R(A)}$

$\emptyset = I_0$

$F_R(\emptyset) = \{0\} = I_1$

$F_R(\{0\}) = \{0, 2\} = I_2$

$F_R(\{1\}) = \{0, 3\}$

$F_R(\{0, 2\}) = \{0, 2, 4\} = I_3$

$\frac{}{0}$ $\qquad$ $\frac{0}{2}$ $\qquad$ $\frac{\frac{0}{2}}{4}$

F_R je monotona $\quad A \subseteq A' \Rightarrow F_R(A) \subseteq F_R(A')$

$I_0 := \emptyset$

$I_{n+1} := F_R(I_n)$

Pokažimo, da je $I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$

$I_0 = \emptyset \subseteq F_R(\emptyset) = I_1$ ✓

$I_{n-1} \subseteq I_n \Rightarrow I_n = F_R(I_{n-1}) \subseteq F_R(I_n) = I_{n+1}$

$I_R := \bigcup_{n=0}^{\infty} I_n$

I_R je zaprta za R

$c \in F_R(I_R)$. Po def. $\exists \{h_1, \dots, h_k\} . (\{h_1, \dots, h_k\}, c) \in R \wedge \forall i . h_i \in I_R$.

Zato za vsak i obstaja n_i, da je $h_i \in I_{n_i}$.

Če je $n = \max(\{n_1, n_2, \dots, n_k\})$, potem $\forall i . h_i \in I_n$.

Tedaj je $c \in I_{n+1} \subseteq I_R$. ∎

I_R je najmanjša $\subseteq X$, zaprta za R

Naj bo A zaprta za R.

$I_0 = \emptyset \subseteq A$

$I_{n-1} \subseteq A \Rightarrow I_n = F_R(I_{n-1}) \subseteq F_R(A) \subseteq A$.

Ker so torej vsi $I_n \subseteq A$, je tudi $I_R = \bigcup_{n=0}^{\infty} I_n \subseteq A$.

Indukcija za I_R

Naj bo ϕ predikat na X.

Če je $P = \{x \in X \mid \phi(x)\}$ zaprta za R, tedaj je $I_R \subseteq P$,

zato $\forall x \in I_R . \phi(x)$.

$$\frac{h_1 \dots h_n}{c} \cdot \Rightarrow \left(h_1 \in P \wedge \dots \wedge h_n \in P \Rightarrow c \in P\right)$$

$$\Rightarrow \left(\phi(h_1) \wedge \dots \wedge \phi(h_n) \Rightarrow \phi(c)\right)$$