Metateorija programskih jezikov

pravila, ki opisujejo jezik

lastnosti, ki jim zadošča teorija

teorija

metateorija

Teorija IMPa

Operacijska semantika

$S, e \Downarrow m$ (izraz, vrednost)

evalvacija
op. sem. velikih korakov
naravna semantika

$$\frac{}{S, n \Downarrow n} \qquad \frac{l \mapsto m \in S}{S, !l \Downarrow m} \qquad \frac{S, e_1 \Downarrow m_1 \quad S, e_2 \Downarrow m_2}{S, e_1 + e_2 \Downarrow m_1 + m_2}$$

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

$S, b \Downarrow t$ podobno

$S, c \rightsquigarrow S', c'$ op. sem. malih korakov

(Za skip ne bo pravila, ker ji takrat konec programa)

$$\frac{S, e \Downarrow m}{S, l := e \rightsquigarrow S[l \mapsto m], \text{skip}}$$

$$\frac{S, c_1 \rightsquigarrow S', c_1'}{S, c_1; c_2 \rightsquigarrow S', c_1'; c_2} \qquad \frac{}{S, \text{skip}; c_2 \rightsquigarrow S, c_2}$$

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

$$\frac{S, b \Downarrow tt}{S, \text{while } b \text{ do } c \rightsquigarrow S, c; \text{while } b \text{ do } c} \qquad \frac{S, b \Downarrow ff}{S, \text{while } b \text{ do } c \rightsquigarrow S, \text{skip}}$$

Trditev Če velja $S, c \rightsquigarrow s', c'$ in $S, c \rightsquigarrow s'', c''$, potem je $s' = s''$ in $c' = c''$.

Dokaz z indukcija.

Statična semantika

$L \vdash e$ e dostopa le do lokacij iz množice L

$L \vdash b$ b dostopa le do lokacij iz množice L

$L \vdash c, L'$ c dostopa do lokacij iz množice L in po njegovem izvajanju so definirane vse lokacije iz L'

$$\frac{}{L \vdash \underline{n}} \qquad \frac{\ell \in L}{L \vdash !\ell} \qquad \frac{L \vdash e_1 \quad L \vdash e_2}{L \vdash e_1 + e_2}$$

ostalo podobno

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

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

Izrek o varnosti

safety theorem

Trditev (napredek / progress)

Naj bo $s : L \to \mathbb{Z}$

- Če velja $L \vdash e$, obstaja $n \in \mathbb{Z}$, da velja $S, e \Downarrow n$
- Če velja $L \vdash b$, obstaja $r \in \{tt, ff\}$, da velja $S, b \Downarrow r$
- Če velja $L \vdash c, L'$: 1) obstaja c', s', da velja $S, c \rightsquigarrow s', c'$.
  2) $c = \text{skip}$.

Dokaz

- Z indukcije na $L \vdash c$. Obravnavamo vsa pravila, ki podajajo relacijo.
  - $\dfrac{n \in \mathbb{Z}}{L \vdash \underline{n}}$. Tedaj velja $s, \underline{n} \Downarrow n$. ✓
  - $\dfrac{l \in L}{L \vdash !l}$ Ker je $l \in L$, obstaja $n \in \mathbb{Z}$, da je $l \mapsto n \in s$, saj je po predpostavki s definiran na vsem L.
    Torej velja $s, !l \Downarrow n$ ✓
  - $\dfrac{L \vdash e_1 \quad L \vdash e_2}{L \vdash e_1 + e_2}$ Po ind. pred. $\exists n_1, n_2 \in \mathbb{Z}$, da je $s, e_1 \Downarrow n_1$ in $s, e_2 \Downarrow n_2$.
    Tedaj velja $s, e_1 + e_2 \Downarrow n_1 + n_2$ ✓
  - ostali primeri podobno. ✓
- Logične izraze obravnamo podobno kot aritmetične. ✓
- Z indukcije na $L \vdash c, L'$
  - $\dfrac{}{L \vdash \text{skip}, L}$ Velja točka 2) ✓
  - $\dfrac{L \vdash e}{L \vdash l := e, L \cup \{l\}}$ Od prej vemo, da $\exists n \in \mathbb{Z}$, da velja $s, e \Downarrow n$.
    Torej velja $s, l := e \rightsquigarrow s[l \mapsto n], \text{skip}$ ✓
  - $\dfrac{L \vdash c_1, L' \quad L' \vdash c_2, L''}{L \vdash c_1; c_2, L''}$ Po ind. predp. iz $L \vdash c_1, L'$ sledi:
    1) $s, c_1 \rightsquigarrow s', c_1'$. Tedaj $s, (c_1; c_2) \rightsquigarrow s', (c_1'; c_2)$ ✓
    2) $c_1 = \text{skip}$. Tedaj $s, \text{skip}; c_2 \rightsquigarrow s, c_2$ ✓
  - $\dfrac{L \vdash b \quad L \vdash c_1, L' \quad L \vdash c_2, L''}{L \vdash \text{if } b \text{ then } c_1 \text{ else } c_2, L' \cap L''}$ Vemo, da $\exists r \in \{tt, ff\}$, da velja $s, b \Downarrow r$.
    1) Če je $s, b \Downarrow tt$, potem $s, \text{if} \ldots \rightsquigarrow s, c_1$ ✓
    2) Če je $s, b \Downarrow ff$, potem $s, \text{if} \ldots \rightsquigarrow s, c_2$ ✓
  - $\dfrac{L \vdash b \quad L \vdash c, L'}{L \vdash \text{while } b \text{ do } c, L}$ Vemo, da $\exists r$, da velja $s, b \Downarrow r$.
    Kot prej v obeh primerih vidimo, da velja $s, \text{while} \ldots \rightsquigarrow s, \ldots$ ✓

Trditev (ohranitev / preservation)

Če velja $L \vdash c, L'$ in $s, c \rightsquigarrow s', c'$ za nek $s : L \to \mathbb{Z}$,
tedaj $L'' \vdash c', L'$ za nek L'' in $s' : L'' \to \mathbb{Z}$.