# Metateorija programskih jezikov

## (dinamična) Operacijska semantika jezika IMP

množica lokacij
stanja $s$ bo delna preslikava $\mathcal{L} \to \mathbb{Z}$

stanje — celo število
$s, e \Downarrow n$
arit. izr.

$$\frac{}{s, n \Downarrow n}$$

$$\frac{s, e_1 \Downarrow n_1 \quad s, e_2 \Downarrow n_2}{s, e_1 + e_2 \Downarrow n_1 + n_2}$$

$$\frac{s, e_1 \Downarrow n_1 \quad s, e_2 \Downarrow n_2}{s, e_1 * e_2 \Downarrow n_1 \cdot n_2}$$

$$\frac{s, e \Downarrow n}{s, -e \Downarrow -n}$$

$$\frac{s(l) = n}{s, \#l \Downarrow n}$$

stanje — logična vrednost $\top, \bot$ $tt$ $ff$ 1 0
$s, b \Downarrow r$
Bool. izraz

D.N.

$$s, c \rightsquigarrow s', c'$$

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

$$\frac{s, c_1 \rightsquigarrow s', c_1'}{s, (c_1; c_2) \rightsquigarrow s', (c_1'; c_2)}$$

$$\frac{}{s, (\text{skip}; c_2) \rightsquigarrow s, c_2}$$

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

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

$$\frac{s, b \Downarrow tt}{s, \text{while } b \text{ do } c \rightsquigarrow s, (c; \text{while } b \text{ do } c)}$$

$$\frac{s, b \Downarrow ff}{s, \text{while } b \text{ do } c \rightsquigarrow s, \text{skip}}$$

**Trditev**

Če velja $s, c \rightsquigarrow s', c'$ in $s, c \rightsquigarrow s'', c''$, tedaj je $s' = s''$ in $c' = c''$.

**Dokaz**

Rutinska indukcija

# Statična semantika

$L \vdash e$ (množica lokacij)

$L \vdash b$

$L \vdash c, L'$

$$\frac{}{L \vdash n} \qquad \frac{\ell \in L}{L \vdash \#\ell} \qquad \frac{L \vdash e_1 \quad L \vdash e_2}{L \vdash e_1 + e_2} \qquad \frac{L \vdash e_1 \quad L \vdash e_2}{L \vdash e_1 * e_2} \qquad \frac{L \vdash e}{L \vdash -e}$$

za $L \vdash b$ podobno

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

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

$\emptyset \vdash \ell := 1; m := \#\ell$

$$\frac{\emptyset \vdash \ell := 1, \{\ell\} \qquad \{\ell\} \vdash m := \#\ell, \{\ell, m\}}{\emptyset \vdash \ell := 1; m := \#\ell, \{\ell, m\}}$$

# Izrek o varnosti

## Trditev (napredek) (progres)

Če velja $L \vdash c$, potem bodisi

1. $c = \text{skip}$
2. za vsak $s$, ki je definiran na $L$ obstajata $s', c'$, da velja $s, c \rightsquigarrow s', c'$

## Trditev (ohranitev) (preservation)

Če velja $L \vdash c$ in $s, c \rightsquigarrow s', c'$, tedaj velja $L \vdash c'$.

## Posledica (varnost)

Če velja $L \vdash c$, potem za vsak $s$, definiran na $L$ obstaja bodisi

$$s, c = s_0, c_0 \rightsquigarrow s_1, c_1 \rightsquigarrow s_2, c_2 \rightsquigarrow \dots \rightsquigarrow s_n, \text{skip}$$

bodisi

$$s, c = s_0, c_0 \rightsquigarrow s_1, c_1 \rightsquigarrow s_2, c_2 \rightsquigarrow \dots$$

## Dokaz (napredek)

Z indukcijo na $L \vdash c$. Če je bilo zadnje uporabljeno pravilo:

- $\dfrac{}{L \vdash \text{skip}}$, je $c = \text{skip}$ 1. ✓
- $\dfrac{L \vdash e}{L \vdash l := e}$, po Lemi D.N. velja $s, e \Downarrow n$ za nek $n$, zato $\dfrac{}{s, l := e \rightsquigarrow s[l \mapsto n], \text{skip}}$ 2. ✓
- $\dfrac{L \vdash c_1 \quad L \vdash c_2}{L \vdash c_1; c_2}$ po I.P. za $L \vdash c_1$ velja:
  1. $c_1 = \text{skip}$, zato $s, (\text{skip}; c_2) \rightsquigarrow s, c_2$ 2. ✓
  2. $s, c_1 \rightsquigarrow s', c_1'$, zato $\dfrac{s, c_1 \rightsquigarrow s', c_1'}{s, (c_1; c_2) \rightsquigarrow s', (c_1'; c_2)}$ 2. ✓
- $\dfrac{L \vdash b \quad \dots}{L \vdash \text{if } b \text{ then } c_1 \text{ else } c_2}$ Po Lemi DN2 velja $s, b \Downarrow tt$ ali $s, b \Downarrow ff$, zato lahko v obeh primerih naredimo korak 2. ✓
- $\dfrac{L \vdash b \quad \dots}{L \vdash \text{while } b \text{ do } c}$ Podobno. 2. ✓

$\dfrac{}{L \vdash \text{skip}} \qquad \dfrac{L \vdash e}{L \vdash l := e} \qquad \dfrac{L \vdash c_1 \quad L \vdash c_2}{L \vdash c_1; c_2}$

$\dfrac{L \vdash b \quad L \vdash c_1 \quad L \vdash c_2}{L \vdash \text{if } b \text{ then } c_1 \text{ else } c_2} \qquad \dfrac{L \vdash b \quad L \vdash c}{L \vdash \text{while } b \text{ do } c}$

**Lema D.N.**
Če $L \vdash e$ in $s$ definiran na $L$, obstaja $n$, da velja $s, e \Downarrow n$.