Kaj gre v λ-računu lahko narobe?

- izrazi, ki nimajo pričakovanega tipa

  $false + 3$

  logična vrednost namesto celega števila

- spremenljivke, ki nimajo definirane vrednosti

  $x + 3$

- ???

Vsem tem težavam se bomo izognili s tipi.

$$\text{tip } A, B ::= int \mid bool \mid A \to B$$

$\lambda x. x+3$

$\lambda x. x>3$

$e ::= n \mid e_1 + e_2 \mid e_1 - e_2 \mid e_1 * e_2 \mid true \mid false \mid e_1 = e_2 \mid e_1 < e_2 \mid e_1 > e_2 \mid \text{if } e \text{ then } e_1 \text{ else } e_2 \mid \lambda x. e \mid x \mid e_1 e_2$

Definirajmo relacijo

$\Gamma \vdash e : A$ ... v kontekstu Γ ima e tip A

Kontekst $x_1 : A_1, \dots, x_n : A_n$ je seznam, v katerem je spremenljivki x_i prirejen enoličen tip A_i

$$\frac{}{\Gamma \vdash n : int} \qquad \frac{\Gamma \vdash e_1 : int \quad \Gamma \vdash e_2 : int}{\Gamma \vdash e_1 + e_2 : int}$$

podobno za $-$, $*$

$$\frac{}{\Gamma \vdash true : bool} \qquad \frac{}{\Gamma \vdash false : bool} \qquad \frac{\Gamma \vdash e_1 : int \quad \Gamma \vdash e_2 : int}{\Gamma \vdash e_1 = e_2 : bool}$$

podobno za $<$, $>$

$$\frac{\Gamma \vdash e : bool \quad \Gamma \vdash e_1 : A \quad \Gamma \vdash e_2 : A}{\Gamma \vdash \text{if } e \text{ then } e_1 \text{ else } e_2 : A} \qquad \frac{\Gamma, x : A \vdash e : B}{\Gamma \vdash \lambda x. e : A \to B} \qquad \frac{(x : A \in \Gamma)}{\Gamma \vdash x : A} \qquad \frac{\Gamma \vdash e_1 : A \to B \quad \Gamma \vdash e_2 : A}{\Gamma \vdash e_1 e_2 : B}$$

$$\dfrac{\dfrac{\dfrac{}{f : int \to bool \vdash f : int \to bool} \quad \dfrac{}{f : int \to bool \vdash 3 : int}}{f : int \to bool \vdash f\,3 : bool}}{\emptyset \vdash \lambda f. f\,3 : (int \to bool) \to bool} \qquad \dfrac{\dfrac{\dfrac{}{x : int \vdash x : int} \quad \dfrac{}{x : int \vdash 0 : int}}{x : int \vdash x > 0 : bool}}{\emptyset \vdash \lambda x. x > 0 : int \to bool}$$

$$\emptyset \vdash (\lambda f. f\,3)(\lambda x. x > 0) : bool$$

Nekateri izrazi imajo več možnih tipov in ustreznih dreves izpeljave

$$\dfrac{\dfrac{}{x : bool \vdash x : bool}}{\emptyset \vdash \lambda x . x : bool \to bool}$$

$$\dfrac{\vdots}{\emptyset \vdash \lambda x . x : (int \to bool) \to (int \to bool)}$$

Izrek o varnosti

safety

Napredek Če velja $\emptyset \vdash e : A$, potem velja

progress

- e je vrednost ali
- obstaja e', da velja $e \leadsto e'$

Ohranitev Če velja $\Gamma \vdash e : A$ in $e \leadsto e'$, potem velja $\Gamma \vdash e' : A$.

preservation

Dokaz napredka

Z indukcije na $\emptyset \vdash e : A$. Možni primeri:

- $\dfrac{}{\emptyset \vdash m : int}$ je vrednost ✓
- $\dfrac{\emptyset \vdash e_1 : int \quad \emptyset \vdash e_2 : int}{\emptyset \vdash e_1 + e_2 : int}$

  Po ind. predp. je e_1 vrednost ali pa obstaja e_1', da velja $e_1 \leadsto e_1'$.

  - Če je e_1 vrednost, je lahko oblike m_1, ~~true~~, ~~false~~ ali ~~λx~~ ...

    odpadeje zaradi $\emptyset \vdash e_1 : int$

    Po IP je tudi e_2 vrednost ali pa obstaja e_2', da je $e_2 \leadsto e_2'$

    * Če je e_2 vrednost, je oblike m_2; zato $e_1 + e_2 = \underline{m_1} + \underline{m_2} \leadsto \underline{m_1 + m_2}$
    * Če obstaja e_2', da je $e_2 \leadsto e_2'$, velja $e_1 + e_2 = m_1 + e_2 \leadsto m_1 + e_2'$
  - Če obstaja e_1', da je $e_1 \leadsto e_1'$, velja $e_1 + e_2 \leadsto e_1' + e_2$

- $-, *, true, false, <, >, =$ podobno kot zgoraj.
- $\dfrac{\emptyset \vdash e : bool \quad \ldots}{\emptyset \vdash \text{if } e \text{ then } e_1 \text{ else } e_2 : A}$

  Po IP. za $\emptyset \vdash e : bool$ dobimo:

  - e vrednost
    * $e = true$ $\quad$ if true then e_1 else $e_2 \leadsto e_1$
    * $e = false$ $\quad$ if false then e_1 else $e_2 \leadsto e_2$

- $e \rightsquigarrow e'$

  if e then e_1 else $e_2 \rightsquigarrow$ if e' then e_1 else e_2

- $\overline{\emptyset \vdash \lambda x . e : A \to B}$ je vrednost

- $\emptyset \vdash x : A$ se ne more zgoditi

- $\dfrac{\emptyset \vdash e_1 : A \to B \qquad \emptyset \vdash e_2 : A}{\emptyset \vdash e_1 e_2 : B}$ **DOMAČA NALOGA**

Za dokaz ohranitve potrebujemo

<u>Lema o substituciji</u>

Če velja $\Gamma \vdash e : A$ in $\Gamma, x : A \vdash e' : B$, potem $\Gamma \vdash e'[e/x] : B$

<u>Dokaz</u>

Indukcija na $\Gamma, x : A \vdash e' : B$.

- $\Gamma, x : A \vdash e_1 + e_2 : \mathrm{int}$. Potem je $\Gamma, x : A \vdash e_1 : \mathrm{int}$ in $\Gamma, x : A \vdash e_2 : \mathrm{int}$.
  Po I.P. dobimo $\Gamma \vdash e_1[e/x] : \mathrm{int}$ in $\Gamma \vdash e_2[e/x] : \mathrm{int}$, zato je
  $\Gamma \vdash e_1[e/x] + e_2[e/x] : \mathrm{int}$, ampak $e_1[e/x] + e_2[e/x] = (e_1 + e_2)[e/x]$.
- $\Gamma, x : A \vdash \overset{e'}{x} : \overset{B}{A}$, potem $\Gamma \vdash e : A$.
- $\Gamma, x : A \vdash y : B$ za $y \neq x$. Potem je $y : B \in \Gamma$, zato $\Gamma \vdash y : B$.
- ...

$$\frac{e_1 \rightsquigarrow e_1'}{e_1 + e_2 \rightsquigarrow e_1' + e_2} \qquad \frac{e_2 \rightsquigarrow e_2'}{m_1 + e_2 \rightsquigarrow m_1 + e_2'} \qquad \frac{}{\underline{m_1} + \underline{m_2} \rightsquigarrow \underline{m_1 + m_2}}$$

+ iz sintakse   + na $\mathbb{Z}$

podobno
za $-, *, =, <, >$

$$\frac{e \rightsquigarrow e'}{\text{if } e \text{ then } e_1 \text{ else } e_2 \rightsquigarrow \text{if } e' \text{ then } e_1 \text{ else } e_2}$$

$$\frac{}{\text{if true then } e_1 \text{ else } e_2 \rightsquigarrow e_1} \qquad \frac{}{\text{if false then } e_1 \text{ else } e_2 \rightsquigarrow e_2}$$

$$\frac{e_1 \rightsquigarrow e_1'}{e_1 e_2 \rightsquigarrow e_1' e_2} \qquad \frac{e_2 \rightsquigarrow e_2'}{(\lambda x. e) e_2 \rightsquigarrow (\lambda x. e) e_2'} \qquad \frac{}{(\lambda x. e) v \rightsquigarrow e[v/x]}$$

Dokaz ohranitve

Indukcija na $e \rightsquigarrow e'$

- $\dfrac{e_1 \rightsquigarrow e_1'}{e_1 + e_2 \rightsquigarrow e_1' + e_2}$. Edina možnost za $\Gamma \vdash e : A$ je $\Gamma \vdash e_1 + e_2 : \text{int}$. Tedaj je $\Gamma \vdash e_1 : \text{int}$ in $\Gamma \vdash e_2 : \text{int}$. Ker je $e_1 \rightsquigarrow e_1'$, je po I.P. $\Gamma \vdash e_1' : \text{int}$ torej je $\Gamma \vdash e_1' + e_2 : \text{int}$.

- preostali dve pravili za $+$: Podobno
- preostala pravila za $-, *, <, >, =$, if then : podobno

- $\dfrac{e_1 \rightsquigarrow e_1'}{e_1 e_2 \rightsquigarrow e_1' e_2}$. Edina možnost za $\Gamma \vdash e : A$ je $\dfrac{\Gamma \vdash e_1 : B \to A \quad \Gamma \vdash e_2 : B}{\Gamma \vdash e_1 e_2 : A}$.

  Po indukciji velja $\Gamma \vdash e_1' : B \to A$. Torej $\dfrac{\Gamma \vdash e_1' : B \to A \quad \Gamma \vdash e_2 : B}{\Gamma \vdash e_1' e_2 : A}$

- $\dfrac{e_2 \rightsquigarrow e_2'}{(\lambda x. e_1) e_2 \rightsquigarrow (\lambda x. e_1) e_2'}$ podobno

- $\dfrac{}{(\lambda x. e) v \rightsquigarrow e[v/x]}$. Edina možnost za tip je $\dfrac{\dfrac{\Gamma, x : B \vdash e : A}{\Gamma \vdash \lambda x. e : B \to A} \quad \Gamma \vdash v : B}{\Gamma \vdash (\lambda x. e) v : A}$

  Po lemi o substituciji je $\Gamma \vdash e[v/x] : A$ ∎

Curry-Howardov izomorfizem

izjava $P ::= \top \mid \bot \mid P_1 \land P_2 \mid P_1 \lor P_2 \mid P_1 \Rightarrow P_2 \mid \exists x. P \mid \forall x. P \mid \psi(x, y, \dots)$

$\Psi \vdash P$ … P je resnična izjava ob predpostavkah $\Psi = P_1, \dots, P_n$

$$\frac{}{\Psi \vdash \top} \qquad \frac{\Psi \vdash \bot}{\Psi \vdash P} \qquad \frac{\Psi \vdash P_1 \quad \Psi \vdash P_2}{\Psi \vdash P_1 \land P_2} \qquad \frac{\Psi \vdash P_1 \land P_2}{\Psi \vdash P_1} \qquad \frac{\Psi \vdash P_1 \land P_2}{\Psi \vdash P_2}$$

$$\frac{\Psi \vdash P_1}{\Psi \vdash P_1 \lor P_2} \qquad \frac{\Psi \vdash P_2}{\Psi \vdash P_1 \lor P_2} \qquad \frac{\Psi \vdash P_1 \lor P_2 \quad \Psi, P_1 \vdash Q \quad \Psi, P_2 \vdash Q}{\Psi \vdash Q}$$

$$\frac{\Psi, P_1 \vdash P_2}{\Psi \vdash P_1 \Rightarrow P_2} \qquad \frac{\Psi \vdash P_1 \Rightarrow P_2 \quad \Psi \vdash P_1}{\Psi \vdash P_2} \qquad \frac{P \in \Psi}{\Psi \vdash P}$$

$\Longrightarrow$ implikacija … $\longrightarrow$ funkcijski tip

$\land$ konjunkcija … $\times$ produkt

$\lor$ disjunkcija … $+$ vsote

$$\frac{e : A}{\mathrm{inl}\ e : A + B} \qquad \frac{e : B}{\mathrm{inr}\ e : A + B}$$

$$\frac{e : A + B \quad x : A \vdash e_1 : C \quad x : B \vdash e_2 : C}{\mathrm{match}\ e\ \mathrm{with}\ \mathrm{inl}\ x \to e_1 \mid \mathrm{inr}\ x \to e_2 : C}$$

IZJAVE … TIPI

DOKAZI … IZRAZI