Tipi

λ-račun s preprostimi tipi (simply-typed λ-calculus / STLC)

$$M, N ::= x \mid \lambda x.M \mid MN \mid \underline{n} \mid M+N \mid M*N \mid M<N \mid \mathsf{true} \mid \mathsf{false} \mid \mathsf{if}\ M\ \mathsf{then}\ N_1\ \mathsf{else}\ N_2 \mid \mathsf{rec}\ f\ x.\,M$$

izrazi

$$\dfrac{\dfrac{\dfrac{x:int \vdash x:int \qquad x:int \vdash \underline{2}:int}{x:int \vdash x<\underline{2}:bool}}{\emptyset \vdash (\lambda x.\, x<\underline{2}): int \to bool} \qquad \dfrac{}{\emptyset \vdash \underline{3}:int}}{\emptyset \vdash (\lambda x.\, x<\underline{2})\ \underline{3} : bool}$$

$$A, B ::= int \mid bool \mid A \to B$$

tipi

$$\boxed{\Gamma \vdash M : A}$$

kontekst - seznam, ki vsakemu izmed spr. $x_1, \dots, x_n$ priredi natanko en tip.

$x_1:A_1, x_2:A_2, \dots, x_n:A_n$

$$\dfrac{x:A \in \Gamma}{\Gamma \vdash x : A} \qquad \dfrac{\Gamma, x:A \vdash M : B}{\Gamma \vdash \lambda x.M : A \to B} \qquad \dfrac{\Gamma \vdash M : A \to B \qquad \Gamma \vdash N : A}{\Gamma \vdash M N : B}$$

$$\dfrac{}{\Gamma \vdash \underline{n} : int} \qquad \dfrac{\Gamma \vdash M : int \qquad \Gamma \vdash N : int}{\Gamma \vdash M + N : int} \qquad \dfrac{\Gamma \vdash M : int \qquad \Gamma \vdash N : int}{\Gamma \vdash M * N : int} \qquad \dfrac{\Gamma \vdash M : int \qquad \Gamma \vdash N : int}{\Gamma \vdash M < N : bool}$$

$$\dfrac{}{\Gamma \vdash \mathsf{true} : bool} \qquad \dfrac{}{\Gamma \vdash \mathsf{false} : bool} \qquad \dfrac{\Gamma \vdash M : bool \qquad \Gamma \vdash N_1 : A \qquad \Gamma \vdash N_2 : A}{\Gamma \vdash \mathsf{if}\ M\ \mathsf{then}\ N_1\ \mathsf{else}\ N_2 : A}$$

$$\dfrac{\Gamma, f : A \to B, x : A \vdash M : B}{\Gamma \vdash \mathsf{rec}\ f\ x.\,M : A \to B}$$

$$V ::= \lambda x.M \mid \underline{n} \mid \mathsf{true} \mid \mathsf{false} \mid \mathsf{rec}\ f\ x.\,M$$

$$\boxed{M \leadsto M'}$$

$$\dfrac{M \leadsto M'}{M N \leadsto M' N} \qquad \dfrac{N \leadsto N'}{(\lambda x.M) N \leadsto (\lambda x.M) N'} \qquad \dfrac{}{(\lambda x.M)\, V \leadsto M[V/x]}$$

$$\dfrac{M \leadsto M'}{M + N \leadsto M' + N} \qquad \dfrac{N \leadsto N'}{\underline{m} + N \leadsto \underline{m} + N'} \qquad \dfrac{}{\underline{m} + \underline{n} \leadsto \underline{m+n}}$$

(podobno za * in <)

$$\dfrac{M \leadsto M'}{\mathsf{if}\ M\ \mathsf{then}\ N_1\ \mathsf{else}\ N_2 \leadsto \mathsf{if}\ M'\ \mathsf{then}\ N_1\ \mathsf{else}\ N_2}$$

$$\dfrac{}{\mathsf{if}\ \mathsf{true}\ \mathsf{then}\ N_1\ \mathsf{else}\ N_2 \leadsto N_1} \qquad \dfrac{}{\mathsf{if}\ \mathsf{false}\ \mathsf{then}\ N_1\ \mathsf{else}\ N_2 \leadsto N_2}$$

$$\dfrac{N \leadsto N'}{(\mathsf{rec}\ f\ x.\,M)\, N \leadsto (\mathsf{rec}\ f\ x.\,M)\, N'} \qquad \dfrac{}{(\mathsf{rec}\ f\ x.\,M)\, V \leadsto M[V/x, (\mathsf{rec}\ f\ x.\,M)/f]}$$

ali

$$\dfrac{N \leadsto N'}{V N \leadsto V N'}$$

Izrek o varnosti

Trditev (napredek): Če velja $\emptyset \vdash M : A$, tedaj:
- obstaja M', da velja $M \leadsto M'$
- je M vrednost.

Trditev (ohranitev): Če velja $\emptyset \vdash M : A$ in $M \leadsto M'$, tedaj velja $\emptyset \vdash M' : A$.

$1+2+\dots+n = \frac{n(n+1)}{2}$

$P(0) \qquad P(n) \Rightarrow P(n^+)$

$$\dfrac{}{0 \in \mathbb{N}} \quad \dfrac{}{0^+ \in \mathbb{N}} \quad \dfrac{}{0^{++} \in \mathbb{N}} \quad \dfrac{}{0^{+++} \in \mathbb{N}}$$

Dokaz (napredek):

Z indukcijo na $\emptyset \vdash M : A$.

$$\dfrac{x : A \in \Gamma}{\Gamma \vdash x : A} \qquad \dfrac{\Gamma, x : A \vdash M : B}{\Gamma \vdash \lambda x . M : A \to B} \qquad \dfrac{\Gamma \vdash M : A \to B \quad \Gamma \vdash N : A}{\Gamma \vdash M\,N : B}$$

$$\dfrac{}{\Gamma \vdash \underline{n} : \mathrm{int}} \qquad \dfrac{\Gamma \vdash M : \mathrm{int} \quad \Gamma \vdash N : \mathrm{int}}{\Gamma \vdash M + N : \mathrm{int}} \qquad \dfrac{\Gamma \vdash M : \mathrm{int} \quad \Gamma \vdash N : \mathrm{int}}{\Gamma \vdash M * N : \mathrm{int}} \qquad \dfrac{\Gamma \vdash M : \mathrm{int} \quad \Gamma \vdash N : \mathrm{int}}{\Gamma \vdash M < N : \mathrm{bool}}$$

$$\dfrac{}{\Gamma \vdash \mathrm{true} : \mathrm{bool}} \qquad \dfrac{}{\Gamma \vdash \mathrm{false} : \mathrm{bool}} \qquad \dfrac{\Gamma \vdash M : \mathrm{bool} \quad \Gamma \vdash N_1 : A \quad \Gamma \vdash N_2 : A}{\Gamma \vdash \mathrm{if}\ M\ \mathrm{then}\ N_1\ \mathrm{else}\ N_2 : A}$$

$$\dfrac{\dfrac{\dfrac{}{\emptyset \vdash 3 : \mathrm{int}} \quad \dfrac{}{\emptyset \vdash 2 : \mathrm{int}}}{\emptyset \vdash 3 > 2 : \mathrm{bool}} \quad \dfrac{\dfrac{}{\emptyset \vdash 1 : \mathrm{int}} \quad \dfrac{}{\emptyset \vdash 1 : \mathrm{int}}}{\emptyset \vdash 1+1 : \mathrm{int}} \quad \dfrac{}{\emptyset \vdash 0 : \mathrm{int}}}{\emptyset \vdash \mathrm{if}\ 3 > 2\ \mathrm{then}\ 1+1\ \mathrm{else}\ 0 : \mathrm{int}}$$

- $\dfrac{x : A \in \emptyset}{\emptyset \vdash x : A}$ Možnost je izključena.
- $\dfrac{x : A \vdash M : B}{\emptyset \vdash \lambda x . M : A \to B}$. Lambda je vrednost
- $\dfrac{\emptyset \vdash M : A \to B \quad \emptyset \vdash N : A}{\emptyset \vdash M\,N : B}$

$P(\emptyset \vdash \underline{n} : \mathrm{int})$

$P(\emptyset \vdash M : \mathrm{int}) \wedge P(\emptyset \vdash N : \mathrm{int}) \Rightarrow P(\emptyset \vdash M > N : \mathrm{bool})$

$P(\emptyset \vdash M : \mathrm{int}) \wedge P(\emptyset \vdash N : \mathrm{int}) \Rightarrow P(\emptyset \vdash M + N : \mathrm{int})$

$P(\emptyset \vdash M : \mathrm{bool}) \wedge P(\emptyset \vdash N_1 : A) \wedge P(\emptyset \vdash N_2 : A) \Rightarrow P(\emptyset \vdash \mathrm{if}\ M\ \mathrm{then}\ N_1\ \mathrm{else}\ N_2 : A)$

Za $\emptyset \vdash M : A \to B$ in $\emptyset \vdash N : A$ velja indukcijska predpostavka. Tedaj velja:

- obstaja M', da velja $M \leadsto M'$. Zato velja $\dfrac{M \leadsto M'}{M\,N \leadsto M'\,N}$
- M je vrednost. Ker velja $\emptyset \vdash M : A \to B$, je edina možnost, da je $M = \lambda x . M'$. Po indukcijski predpostavki za $\emptyset \vdash N : A$ velja:
  - * obstaja N', da velja $N \leadsto N'$. Tedaj velja $\dfrac{N \leadsto N'}{(\lambda x . M')\,N \leadsto (\lambda x . M')\,N'}$
  - * N je vrednost. Tedaj velja $\dfrac{}{(\lambda x . M')\,N \leadsto M'[N/x]}$

- ostali primeri podobno.

Dokaz (ohranitev)

Z indukcijo na $M \leadsto M'$.

$$\dfrac{M \leadsto M'}{M\,N \leadsto M'\,N} \qquad \dfrac{N \leadsto N'}{(\lambda x . M)\,N \leadsto (\lambda x . M)\,N'} \qquad \dfrac{}{(\lambda x . M)\,V \leadsto M[V/x]}$$

$$\dfrac{M \leadsto M'}{M + N \leadsto M' + N} \qquad \dfrac{N \leadsto N'}{\underline{m} + N \leadsto \underline{m} + N'} \qquad \dfrac{}{\underline{m} + \underline{n} \leadsto \underline{m + n}}$$ (podobno za $*$ in $<$)

$$\dfrac{M \leadsto M'}{\mathrm{if}\ M\ \mathrm{then}\ N_1\ \mathrm{else}\ N_2 \leadsto \mathrm{if}\ M'\ \mathrm{then}\ N_1\ \mathrm{else}\ N_2}$$

$$\dfrac{}{\mathrm{if}\ \mathrm{true}\ \mathrm{then}\ N_1\ \mathrm{else}\ N_2 \leadsto N_1} \qquad \dfrac{}{\mathrm{if}\ \mathrm{false}\ \mathrm{then}\ N_1\ \mathrm{else}\ N_2 \leadsto N_2}$$

- $\dfrac{M \leadsto M'}{M\,N \leadsto M'\,N}$

Ker velja $\emptyset \vdash M\,N : A$, mora veljati $\emptyset \vdash M : B \to A$ in $\emptyset \vdash N : B$. Po I.P. velja $\emptyset \vdash M' : B \to A$ torej je

$$\dfrac{\emptyset \vdash M' : B \to A \quad \emptyset \vdash N : B}{\emptyset \vdash M'\,N : A}$$

$$\dfrac{\dfrac{}{x : \mathrm{int} \vdash 1 : \mathrm{int}} \quad \dfrac{}{x : \mathrm{int} \vdash x : \mathrm{int}}}{x : \mathrm{int} \vdash 1 + x : \mathrm{int}} \quad \dfrac{}{x : \mathrm{int} \vdash 0 : \mathrm{int}}$$

$$x : \mathrm{int} \vdash 1 + x > 0 : \mathrm{bool}$$

$$\frac{\emptyset \vdash 1 : int \qquad \emptyset \vdash 3 : int}{\emptyset \vdash 1+3 : int} \qquad \frac{}{\emptyset \vdash 0 : int}$$
$$\overline{\emptyset \vdash 1+3>0 : bool}$$

- $$\frac{N \rightsquigarrow N'}{(\lambda x. M)\, N \rightsquigarrow (\lambda x. M)\, N'}$$ Podobno kot v prejšnjem koraku.

- $$\frac{}{(\lambda x. M)\, V \rightsquigarrow M[V/x]}.$$
  Ker velja $\emptyset \vdash (\lambda x. M)\, V : A$, velja $\emptyset \vdash \lambda x. M : B \to A$ in $\emptyset \vdash V : B$, zato je $x : B \vdash M : A$. Uporabimo lemo o substituciji, ($\Gamma, x:A \vdash M:B \wedge \Gamma \vdash N:A \Rightarrow \Gamma \vdash M[N/x]:B$) da dobimo $\emptyset \vdash M[V/x] : A$ ✓
- Ostali primeri podobno. ✓

<u>Lema</u> (substitucija)
Če velja $\Gamma, x:A, \Gamma' \vdash M:B$ in $\Gamma, \Gamma' \vdash N:A$, tedaj velja $\Gamma, \Gamma' \vdash M[N/x] : B$.

<u>Dokaz</u>
Z indukcijo na $\Gamma, x:A, \Gamma' \vdash M:B$.

$$\frac{x{:}A \in \Gamma}{\Gamma \vdash x : A} \qquad \frac{\Gamma, x{:}A \vdash M : B}{\Gamma \vdash \lambda x. M : A \to B} \qquad \frac{\Gamma \vdash M : A \to B \qquad \Gamma \vdash N : A}{\Gamma \vdash M\, N : B}$$

$$\frac{}{\Gamma \vdash \underline{n} : int} \qquad \frac{\Gamma \vdash M : int \qquad \Gamma \vdash N : int}{\Gamma \vdash M + N : int} \qquad \frac{\Gamma \vdash M : int \qquad \Gamma \vdash N : int}{\Gamma \vdash M * N : int} \qquad \frac{\Gamma \vdash M : int \qquad \Gamma \vdash N : int}{\Gamma \vdash M < N : bool}$$

$$\frac{}{\Gamma \vdash true : bool} \qquad \frac{}{\Gamma \vdash false : bool} \qquad \frac{\Gamma \vdash M : bool \qquad \Gamma \vdash N_1 : A \qquad \Gamma \vdash N_2 : A}{\Gamma \vdash \text{if } M \text{ then } N_1 \text{ else } N_2 : A}$$

- Recimo, da je izraz M spremenljivka v kontekstu $\Gamma, x:A, \Gamma'$. Obravnavamo dva primera
  - $M = y \neq x$. Tedaj je $y : B \in \Gamma, \Gamma'$.
    Ker je $M[N/x] = y[N/x] = y$, velja
    $\Gamma, \Gamma' \vdash M[N/x] : B$. ✓
  - $M = x$. Tedaj je $M[N/x] = x[N/x] = N$.
    Zato je $\Gamma, \Gamma' \vdash M[N/x] : B$, saj je po predpostavki
    $\Gamma, \Gamma' \vdash N : A$, hkrati pa mora veljati $A = B$. ✓ ✓

- $$\frac{\Gamma, x:A, \Gamma', y:A' \vdash M' : B'}{\Gamma, x:A, \Gamma' \vdash \lambda y. M' : \underbrace{A' \to B'}_{B}}$$
  D.N.
  Po lemi o zamenjavi velja $\Gamma, y:A', x:A \vdash M' : B'$.
  Po ind. predp. velja $\Gamma, \Gamma', y:A' \vdash M'[N/x] : B'$
  Tedaj velja $\Gamma, \Gamma' \vdash \lambda y. (M'[N/x]) : A' \to B'$
  torej je $\Gamma, \Gamma' \vdash (\lambda y. M')[N/x] : \underbrace{A' \to B'}_{B}$. ✓

-