Denotacijska semantika

$\lambda x.\, \underline{1} + \underline{1} + x$ $\qquad$ $\lambda x.\, \underline{2} + x$

$\lambda f.\, f(\underline{1} + \underline{1})$ $\qquad$ $\lambda f.\, f\,\underline{2}$

Def Izraza M in N sta kontekstno ekvivalentna $M \simeq N$, če za poljuben kontekst $\mathcal{C}$, podan z

$$\mathcal{C} ::= [\,] \mid x \mid \underline{n} \mid \mathrm{true} \mid \mathrm{false} \mid \mathcal{C}_1 + \mathcal{C}_2 \mid \dots \mid \mathrm{if}\ \mathcal{C}\ \mathrm{then}\ \mathcal{C}_1\ \mathrm{else}\ \mathcal{C}_2 \mid \lambda x.\, \mathcal{C} \mid \mathcal{C}_1\, \mathcal{C}_2$$

velja $\mathcal{C}[M] \rightsquigarrow^* \mathrm{true}$ natanko tedaj, kadar velja $\mathcal{C}[N] \rightsquigarrow^* \mathrm{true}$, kjer je $\mathcal{C}[M]$ izraz, ki ga dobimo, če vse pojavitve $[\,]$ v $\mathcal{C}$ zamenjamo z M.

Primer $M = \underline{1} + \underline{1}$ $\quad N = \underline{2}$ $\quad \mathcal{C} = \lambda f.\, f\,[\,]$

$\mathcal{C}[M] = \lambda f.\, f\,(\underline{1} + \underline{1})$ $\qquad$ $\mathcal{C}[N] = \lambda f.\, f\,\underline{2}$

Trditev Če velja $M \simeq N$, potem za poljuben kontekst $\mathcal{C}$ velja $\mathcal{C}[M] \rightsquigarrow^* \mathrm{false} \iff \mathcal{C}[N] \rightsquigarrow^* \mathrm{false}$.

Dokaz

$(\Rightarrow)$ $\mathcal{C}' = \mathrm{if}\ \mathcal{C}\ \mathrm{then\ false\ else\ true}$

$\mathcal{C}'[M] = \mathrm{if}\ \mathcal{C}[M]\ \mathrm{then\ false\ else\ true}$

$\qquad \rightsquigarrow^* \mathrm{if\ false\ then\ false\ else\ true} \rightsquigarrow \mathrm{true}$

$\mathcal{C}'[N] \rightsquigarrow^* \mathrm{true}$

$\Vert$

if $\mathcal{C}[N]$ then false else true

in edina možnost je, da je $\mathcal{C}[N] \rightsquigarrow^*$ false.

($\Leftarrow$) simetrično.

<u>Trditev</u> Če $M \simeq N$, tedaj za poljuben $\mathcal{C}$ velja

$$\mathcal{C}[M] \rightsquigarrow^* \underline{m} \iff \mathcal{C}[N] \rightsquigarrow^* \underline{m}$$

<u>Izrek</u> $\underline{1} + \underline{1} \simeq \underline{2}$

Dokaz je težaven, ker moramo kvantificirati čez vse kontekste.

Namesto tega si bomo pomagali z denotacijsko semantiko.

Vsakemu tipu A priredimo njegovo interpretacijo $[\![A]\!]$, ki je množica, definirana kot

$$[\![\text{int}]\!] = \mathbb{Z} \qquad\qquad x:\text{int} \vdash x + \underline{5} : \text{int}$$

$$[\![\text{bool}]\!] = \mathbb{B} = \{tt, ff\}$$

$$[\![A \to B]\!] = [\![B]\!]^{[\![A]\!]}$$

Pri izrazih bomo interpretirali le tiste z veljavnimi tipi, torej $\Gamma \vdash M : A$. Te bomo interpretirali s funkcijami

$$[\![\Gamma \vdash M : A]\!] : [\![\Gamma]\!] \to [\![A]\!]$$

kjer je

$$[\![x_1 : A_1, \dots, x_n : A_n]\!] = [\![A_1]\!] \times \dots \times [\![A_n]\!]$$

izrazi $M, N ::= x \mid \lambda x.M \mid MN$
$\mid \underline{m} \mid M+N \mid M*N \mid -M$
$\mid M=N \mid M<N \mid M>N$
$\mid \mathrm{true} \mid \mathrm{false} \mid \mathrm{if}\ M\ \mathrm{then}\ N_1\ \mathrm{else}\ N_2$
$\mid \mathrm{rec}\ f x.M$

$$[\![x_1:A_1, \dots, x_n:A_n \vdash x_i : A_i]\!](a_1, \dots, a_n) = a_i$$

$$[\![\Gamma \vdash \lambda x.M : A \to B]\!](\vec{a}) = y \in [\![A]\!] \longmapsto [\![\Gamma, x:A \vdash M : B]\!](\vec{a}, \overset{[\![A]\!]}{y})$$

$$[\![\Gamma \vdash MN : B]\!](\vec{a}) = \overset{[\![B]\!]^{[\![A]\!]}}{[\![\Gamma \vdash M : A \to B]\!](\vec{a})}\Big([\![\Gamma \vdash N : A]\!](\vec{a})\Big)$$

$$[\![\Gamma \vdash \underline{m} : \mathrm{int}]\!](\vec{a}) = m$$

$$[\![\Gamma \vdash \quad + N : \mathrm{int}]\!](\vec{a}) = [\![\Gamma \vdash M : \mathrm{int}]\!](\vec{a}) + [\![\Gamma \vdash N : \mathrm{int}]\!](\vec{a})$$

$$[\![\Gamma \vdash M * N : \mathrm{int}]\!](\vec{a}) = [\![M]\!](\vec{a}) \cdot [\![N]\!](\vec{a})$$

$$\vdots$$

$$[\![\Gamma \vdash \mathrm{true} : \mathrm{bool}]\!](\vec{a}) = \mathrm{tt}$$

$$\vdots$$

$$[\![\Gamma \vdash \mathrm{if}\ M\ \mathrm{then}\ N_1\ \mathrm{else}\ N_2 : A]\!](\vec{a}) = \begin{cases} [\![N_1]\!](\vec{a}) ; & [\![M]\!](\vec{a}) = \mathrm{tt} \\ [\![N_2]\!](\vec{a}) ; & [\![M]\!](\vec{a}) = \mathrm{ff} \end{cases}$$

Primer

$$[\![x : \mathrm{int} \vdash \lambda y.\, y*6 > x : \mathrm{int} \to \mathrm{bool}]\!] : \mathbb{Z} \to \mathbb{B}^{\mathbb{Z}}$$

$$[\![\ \cdots\ ]\!](m) = n \in \mathbb{Z} \longmapsto [\![x:\mathrm{int}, y:\mathrm{int} \vdash y*6 > x : \mathrm{bool}]\!](m, n)$$

$$= n \in \mathbb{Z} \longmapsto \begin{cases} \mathrm{tt} & [\![y*6]\!](m,n) > [\![x]\!](m,n) \\ \mathrm{ff} & \text{sicer} \end{cases}$$

$$= n \in \mathbb{Z} \longmapsto \begin{cases} \mathrm{tt} & 6 \cdot n > m \\ \mathrm{ff} & \text{sicer} \end{cases}$$

Lema $[\![\vdash \underline{1} + \underline{1} : \mathrm{int}]\!] = [\![\vdash \underline{2} : \mathrm{int}]\!]$

Trditev (skladnost / soundness)

Če $\Gamma \vdash M : A$ in $M \rightsquigarrow M'$, tedaj je

$$[\![\Gamma \vdash M : A]\!] = [\![\Gamma \vdash M' : A]\!]$$

obstaja po ohranitvi

Dokaz

Z indukcijo na $M \rightsquigarrow M'$

- $\dfrac{M \rightsquigarrow M'}{MN \rightsquigarrow M'N}$

Po I.P. je $[\![M]\!] = [\![M']\!]$. Zato je

$$[\![MN]\!](\vec{a}) = [\![M]\!](\vec{a})\left([\![N]\!](\vec{a})\right) = [\![M']\!](\vec{a})\left([\![N]\!](\vec{a})\right)$$
$$= [\![M'N]\!](\vec{a}).$$

- $\dfrac{N \rightsquigarrow N'}{VN \rightsquigarrow VN'}$ podobno

- $\dfrac{}{(\lambda x . M)\, V \rightsquigarrow M[V/x]}$

$$[\![(\lambda x . M)\, V]\!](\vec{a}) = \left(y \mapsto [\![M]\!](\vec{a}, y)\right)\left([\![V]\!](\vec{a})\right)$$
$$= [\![M]\!]\left(\vec{a}, [\![V]\!](\vec{a})\right)$$
$$= [\![M[V/x]]\!](\vec{a})$$ po lemi o substituciji.

- ostalo doma

Lema Če imamo $\Gamma, x : A \vdash M : B$ in $\Gamma \vdash N : A$, tedaj

$$[\![\Gamma, x : A \vdash M : B]\!]\left(\vec{a}, [\![\Gamma \vdash N : A]\!](\vec{a})\right)$$
$$= [\![\Gamma \vdash M[N/x] : B]\!](\vec{a})$$

Dokaz

Z indukcije na $\Gamma, x{:}A \vdash M : B$

- $[\![\Gamma, x : A \vdash \mathrm{true} : \mathrm{bool}]\!](\vec{a}, \dots) = tt$

  $[\![\Gamma \vdash \mathrm{true}[N/x] : \mathrm{bool}]\!](\vec{a}) = [\![\Gamma \vdash \mathrm{true} : \mathrm{bool}]\!](\vec{a}) = tt$

- $[\![\Gamma, x : A \vdash M_1 + M_2 : \mathrm{int}]\!](\vec{a}, [\![N]\!](\vec{a}))$

  $\overset{\text{po def.}}{=} [\![\Gamma, x{:}A \vdash M_1]\!](\vec{a}, [\![N]\!](\vec{a})) + [\![\Gamma, x{:}A \vdash M_2]\!](\vec{a}, [\![N]\!](\vec{a}))$

  $\overset{\text{po I.P.}}{=} [\![\Gamma \vdash M_1[N/x] : \mathrm{int}]\!](\vec{a}) + [\![\Gamma \vdash M_2[N/x] : \mathrm{int}]\!](\vec{a})$

  $= [\![M_1[N/x] + M_2[N/x]]\!](\vec{a}) = [\![(M_1 + M_2)[N/x]]\!](\vec{a})$.

- $[\![\Gamma, x{:}A \vdash x{:}A]\!](\vec{a}, [\![N]\!](\vec{a})) = [\![N]\!](\vec{a})$

  $= [\![x[N/x]]\!](\vec{a})$

- ostalo rutinska indukcija.

$\blacksquare$

Opazimo, da je interpretacija izrazov definirana strukturno, torej če v izrazu M podizraz N zamenjamo z N', da velja $[\![N]\!] = [\![N']\!]$, tedaj bo tudi $[\![M]\!] = [\![M']\!]$.

Konkretno, če je $[\![N]\!] = [\![N']\!]$, je $[\![\mathcal{C}[N]]\!] = [\![\mathcal{C}[N']]\!]$ (ob pogoju, da sta obe strani dobro definirani).

To se da doseči z preverjanjem tipov za kontekste $\mathcal{C}$ oblike $\Gamma \vdash \mathcal{C}[\Delta \vdash A] : B$, ampak bomo izpustili.

$\underbrace{\lambda f.\, f\,[\,]}_{\mathcal{C}} + m$

Trditev (zadostnost / adequacy)

Če velja $[\![\vdash M : \mathrm{bool}]\!] = tt$, tedaj $M \rightsquigarrow^* \mathrm{true}$.

Dokaz

Ker nimamo rekurzije, obstaja vrednost V, da velja $M \rightsquigarrow^* V$ (dokaz je zoprn - glej stare izpite).

Po varnosti velja $\vdash V : \mathrm{bool}$, torej je $[\![V]\!] \in \{tt, ff\}$.

Od prej vemo, da $[\![M]\!] = [\![V]\!]$, zato je $[\![V]\!] = tt$, torej $V = \mathrm{true}$.

Posledica

Če je $[\![M]\!] = [\![N]\!]$, potem velja $M \simeq N$.

Dokaz

Naj bo $\mathcal{C}[M] \rightsquigarrow^* \mathrm{true}$. Torej je $[\![\mathcal{C}[M]]\!] = tt$.

Ker je interpretacija strukturna je $[\![\mathcal{C}[N]]\!] = [\![\mathcal{C}[M]]\!] = tt$.

Po zadostnosti velja $\mathcal{C}[N] \rightsquigarrow^* \mathrm{true}$.

Obrat pokažemo simetrično. $\blacksquare$

Kaj pa $[\![\mathrm{rec}\ f x. M]\!]$?

$$[\![(\mathrm{rec}\ f x. f x + \underline{1})\ \underline{0}]\!] = [\![(\mathrm{rec}\ f x. f x + \underline{1})\ \underline{0} + \underline{1}]\!]$$

$$= [\![(\mathrm{rec}\ f x. f x + \underline{1})\ \underline{0}]\!] + 1$$

$$\Phi(f) = \lambda n.\ \mathrm{if}\ n = 0\ \mathrm{then}\ 1\ \mathrm{else}\ n * f(n-1)$$