Denotacijske semantika

Ideja Vsakemu programu priredimo **osnovni** pomen, izražen z znanimi matematičnimi pojmi.
⇒ lažji dokazi
⇒ vodilo pri razvoju programskih jezikov

Vprašanje Ali program 1+1 vedno lahko nadomestimo z 2 ?

Očitno ja, ampak ...
... sta različna izraza (ampak to nas ne moti)
... drugi je vrednost, prvi pa ni (ampak 1+1 ⇝ 2)
... $\lambda x.1+1 \Downarrow \lambda x.1+1 \neq \lambda x.2 \Downarrow \lambda x.2$
(ampak tc razlike navzven ne vidimo
- če obe funkciji uporabimo, vedno dobimo isti rezultat)

Kontekstna ekvivalenca

Def kontekst $\mathcal{C} ::= [] \mid n \mid \mathcal{C}_1 + \mathcal{C}_2 \mid \mathcal{C}_1 - \mathcal{C}_2 \mid \mathcal{C}_1 * \mathcal{C}_2 \mid \ldots$
$\mid \lambda x.\mathcal{C} \mid \mathcal{C}_1\,\mathcal{C}_2 \mid \ldots$

Primer $\lambda x.$ if $[]$ then $1+5$ else 10

$(\lambda x.\ x + []\,)\,(\,[] * 2)$

Def $\mathcal{C}[e]$ je izraz, ki ga dobimo, če vse $[]$ nadomestimo z e.

$[][e] = e$ $\qquad$ $(\lambda x.\mathcal{C})[e] = \lambda x.\mathcal{C}[e]$

$n[e] = n$ $\qquad$ $(\mathcal{C}_1\,\mathcal{C}_2)[e] = \mathcal{C}_1[e]\ \mathcal{C}_2[e]$

$(\mathcal{C}_1 + \mathcal{C}_2)[e] = \mathcal{C}_1[e] + \mathcal{C}_2[e]$

Primer $(\lambda x.$ if $[]$ then $1+5$ else $10)\,[3>2]$
$= \lambda x.$ if $3>2$ then $1+5$ else 10

$(\lambda x.$ if $[]$ then $1+5$ else $10)\,[2>x]$
$= \lambda x.$ if $2>x$ then $1+5$ else 10.

Def Izraza e_1 in e_2 sta navzven ekvivalentna (observationally / contextually equivalent), pišemo $e_1 \cong e_2$, če za poljuben kontekst $\mathcal{C}$ velja
$\mathcal{C}[e_1] \rightsquigarrow^* \text{true} \iff \mathcal{C}[e_2] \rightsquigarrow^* \text{true}$.

Lema $e_1 \cong e_2 \iff (\forall \mathcal{C}.\ \mathcal{C}[e_1] \rightsquigarrow^* \text{false} \iff \mathcal{C}[e_2] \rightsquigarrow^* \text{false})$.

$\Rightarrow$) vzemimo $\mathcal{C}$, in privzemimo, da velja $\mathcal{C}[e_1] \rightsquigarrow^* \text{false}$
Tedaj $\mathcal{C}' \overset{\text{def}}{=}$ if $\mathcal{C}$ then false else true.
$\mathcal{C}'[e_1] \rightsquigarrow^* \text{true} \Rightarrow \mathcal{C}'[e_2] \rightsquigarrow^* \text{true} \Rightarrow \mathcal{C}[e_2] \rightsquigarrow^* \text{false}$.

$\Leftarrow$) podobno.

Lema $1+1 \cong 2$

Dokaz Direktno težko, ker moramo kvantificirati čez vse kontekste.

Naivna denotacijska semantika

Vsakemu tipu A priredimo množico $[\![A]\!]$

$[\![int]\!] = \mathbb{Z}$

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

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

$[\![\text{sintaksa}]\!] =$ matematični pomen

Vsakemu izrazu $\Gamma \vdash e : A$ bomo priredili funkcijo

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

kjer je $[\![x_1 : A_1, \ldots, x_n : A_n]\!] = [\![A_1]\!] \times [\![A_2]\!] \times \cdots \times [\![A_n]\!]$

$[\![\cdot]\!] = \mathbb{1} = \{()\} = \{*\}$

$[\![\Gamma \vdash n : int]\!](\eta) = n$

$[\![\Gamma \vdash e_1 + e_2 : int]\!](\eta) = [\![e_1]\!](\eta) + [\![e_2]\!](\eta)$

$[\![\Gamma \vdash e_1 - e_2 : int]\!](\eta) = [\![e_1]\!](\eta) - [\![e_2]\!](\eta)$

$[\![\Gamma \vdash e_1 * e_2 : int]\!](\eta) = [\![e_1]\!](\eta) \cdot [\![e_2]\!](\eta)$

$$[\![\Gamma \vdash \text{if } e \text{ then } e_1 \text{ else } e_2]\!](\eta) = \begin{cases} [\![e_1]\!](\eta) & \text{če je } [\![e]\!](\eta) = tt \\ [\![e_2]\!](\eta) & \text{če je } [\![e]\!](\eta) = ff \end{cases}$$

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

$[\![\Gamma \vdash \lambda x.e : A \to B]\!](\eta)_{(a_1,\ldots,a_n)} = a \mapsto [\![\Gamma, x : A \vdash e : B]\!](\eta, a)_{(a_1,\ldots,a_n,a)}$

$[\![\Gamma \vdash e_1 e_2 : B]\!](\eta) = ([\![e_1]\!](\eta))([\![e_2]\!](\eta))$

$[\![e_1]\!](\eta) \in [\![B]\!]^{[\![A]\!]}$, $[\![e_2]\!](\eta) \in [\![A]\!]$

Primer $[\![x : int \vdash x + x : int]\!] : \mathbb{Z} \to \mathbb{Z}$

$[\![x : int \vdash x + x : int]\!](n) = [\![x]\!](n) + [\![x]\!](n) = n + n = 2 \cdot n$

$[\![1 + 1 : int]\!](*) = [\![1]\!](*) + [\![1]\!](*) = 1 + 1 = 2$

Trditev (zdravost / soundness) Če $e \rightsquigarrow e'$, potem $[\![e]\!] = [\![e']\!]$.

Dokaz z indukcijo.

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

$$[\![\text{if } e \text{ then } e_1 \text{ else } e_2]\!](\eta) \overset{\text{DEF}}{=} \begin{cases} [\![e_1]\!](\eta) & , \text{če } [\![e]\!](\eta) = \# \\ [\![e_2]\!](\eta) & , \text{če } [\![e]\!](\eta) = ff \end{cases}$$

$$\overset{\text{I.P.}}{=} \begin{cases} [\![e_1]\!](\eta) & , \text{če } [\![e']\!](\eta) = \# \\ [\![e_2]\!](\eta) & , \text{če } [\![e']\!](\eta) = ff \end{cases}$$

$$= [\![\text{if } e' \text{ then } e_1 \text{ else } e_2]\!](\eta)$$

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

$$[\![\text{if true then } e_1 \text{ else } e_2]\!](\eta) = \begin{cases} [\![e_1]\!](\eta) & , \text{če } [\![\text{true}]\!](\eta) = \# \\ \ldots \end{cases}$$

$$= [\![e_1]\!](\eta)$$

- $\dfrac{e_1 \rightsquigarrow e_1'}{e_1 e_2 \rightsquigarrow e_1' e_2}$ & $\dfrac{e_2 \rightsquigarrow e_2'}{v_1 e_2 \rightsquigarrow v_1 e_2'}$ ... podobno kot pri $\dfrac{e \rightsquigarrow e'}{\text{if } e \cdots \rightsquigarrow \text{if } e'}$.

- $$\frac{}{(\lambda x . e) v \rightsquigarrow e[v/x]}$$

$$[\![(\lambda x.e)\,n]\!](\eta) \overset{DEF}{=} [\![\lambda x.e]\!](\eta)([\![n]\!](\eta)) \overset{DEF}{=} [\![e]\!](\eta, [\![n]\!](\eta)) \overset{LEMA}{=} [\![e[n/x]]\!](\eta)$$ ∎

Lema Če $\Gamma, x:A \vdash e:B$ in $\Gamma \vdash e':A$, potem

$$[\![\Gamma \vdash e[e'/x]:B]\!](\eta) = [\![\Gamma, x:A \vdash e:B]\!](\eta, [\![\Gamma \vdash e':A]\!](\eta))$$

Primer $[\![x:int \vdash x+2:int]\!]([\![\vdash 3:int]\!]) = (n \mapsto n+2)3 = 5$

$[\![\vdash (x+2)[3/x]:int]\!] = [\![\vdash 3+2]\!] = [\![3]\!] + [\![2]\!] = 3+2 = 5$

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

Lema Za poljuben* $\mathcal{C}$ obstaja $[\![\mathcal{C}]\!]$, da za vsak* e velja $[\![\mathcal{C}[e]]\!](\eta) = [\![\mathcal{C}]\!](\eta)([\![e]\!](\eta))$.

* tako da so vse interpretacije definirane

Dokaz Indukcija na strukturo $\mathcal{C}$.

Izrek (zadostnost / adequacy)
Če $[\![\vdash e:bool]\!] = tt$, tedaj $e \rightsquigarrow^* true$.

Posledica Če je $[\![\Gamma \vdash e:A]\!] = [\![\Gamma \vdash e':A]\!]$, tedaj je $e \cong e'$.

Dokaz Vzemimo poljuben $\mathcal{C}$, da je $\mathcal{C}[e] \rightsquigarrow^* true$.
Po zdravosti velja $[\![\mathcal{C}[e]]\!] = tt$.
Po lemi je $[\![\mathcal{C}[e]]\!] = [\![\mathcal{C}]\!]([\![e]\!]) = [\![\mathcal{C}]\!]([\![e']\!]) = [\![\mathcal{C}[e']]\!]$
Torej je $[\![\mathcal{C}[e']]\!] = tt$. Po zadostnosti velja $\mathcal{C}[e'] \rightsquigarrow^* true$.
V drugi smer je simetrično. ∎