

Denotacijska semantika

Ideja Vsakemu programu prisredimo **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 jn, ampak ...

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

Kontekstna ekvivalenca

Def

$$\text{kontekst } \mathcal{C} ::= [] \mid n \mid \mathcal{C}_1 + \mathcal{C}_2 \mid \mathcal{C}_1 - \mathcal{C}_2 \mid \mathcal{C}_1 * \mathcal{C}_2 \mid \dots \\ \mid \lambda x. \mathcal{C} \mid \varphi_1 \mathcal{C}_2 \mid \dots$$

Primer

$$\lambda x. \text{if } [] \text{ then } 1+5 \text{ else } 10$$

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

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

$$[] [e] = e$$

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

$$n[e] = n$$

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

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

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

$$= \lambda x. \text{if } 3 > 2 \text{ then } 1+5 \text{ else } 10$$

$(\lambda x. \text{if } [] \text{ then } 1+5 \text{ else } 10) [2 > x]$

$$= \lambda x. \text{if } 2 > x \text{ then } 1+5 \text{ else } 10.$$

Def

Izrazi e_1 in e_2 sta navzven ekvivalentne

(observationally / contextually equivalent),

pisemo $e_1 \cong e_2$, če za poljuben kontekst \mathcal{C} velja

$$\mathcal{C}[e_1] \rightsquigarrow^* \text{true} \Leftrightarrow \mathcal{C}[e_2] \rightsquigarrow^* \text{true}.$$

Lema

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

\Rightarrow vzemimo \mathcal{C} , in prizemimo, da velja $\mathcal{C}[e_1] \rightsquigarrow^* \text{false}$

Tedaj $\mathcal{C}' \stackrel{\text{def}}{=} \text{if } \mathcal{C} \text{ then false else true.}$

$$\mathcal{C}'[e_1] \rightsquigarrow^* \text{true} \Rightarrow \mathcal{C}'[e_2] \rightsquigarrow^* \text{true} \Rightarrow \mathcal{C}[e_2] \rightsquigarrow^* \text{false}.$$

\Leftarrow podobno.

Lema

$$1+1 \cong 2$$

Dokaz Direktno težko, ker moramo kvantificirati čez vse kontekste.

Najnava denotacijske semantike

✓ Sistemski tipu A pripredimo množico $\llbracket A \rrbracket$

$$\begin{aligned}\llbracket \text{int} \rrbracket &= \mathbb{Z} \\ \llbracket \text{bool} \rrbracket &= B = \{\text{tt}, \text{ff}\} \\ \llbracket A \rightarrow B \rrbracket &= \llbracket B \rrbracket^{\llbracket A \rrbracket}\end{aligned}$$

$\boxed{\text{sintaksa}}$ = matematični
pomen

✓ Sistemski izrazu $\Gamma \vdash e : A$ bomo pripredili funkcijo

$$\llbracket \Gamma \vdash e : A \rrbracket : \llbracket \Gamma \rrbracket \rightarrow \llbracket A \rrbracket$$

$$\text{kjer je } \llbracket x_1 : A_1, \dots, x_n : A_n \rrbracket = \llbracket A_1 \rrbracket \times \llbracket A_2 \rrbracket \times \dots \times \llbracket A_n \rrbracket$$

$$\llbracket \Gamma \vdash m : \text{int} \rrbracket (\eta) = m$$

$$\llbracket \Gamma \vdash e_1 + e_2 : \text{int} \rrbracket (\eta) = \llbracket e_1 \rrbracket(\eta) + \llbracket e_2 \rrbracket(\eta)$$

$$\llbracket \Gamma \vdash e_1 - e_2 : \text{int} \rrbracket (\eta) = \llbracket e_1 \rrbracket(\eta) - \llbracket e_2 \rrbracket(\eta)$$

$$\llbracket \Gamma \vdash e_1 * e_2 : \text{int} \rrbracket (\eta) = \llbracket e_1 \rrbracket(\eta) \cdot \llbracket e_2 \rrbracket(\eta)$$

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

$$\llbracket x_1 : A_1, \dots, x_n : A_n \vdash x_i : A_i \rrbracket ((a_1, \dots, a_n)) = a_i$$

$$\llbracket \Gamma \vdash \lambda x. e : A \rightarrow B \rrbracket (\eta) = a \mapsto \llbracket \Gamma, x : A \vdash e : B \rrbracket (\eta, a)$$

(a_1, \dots, a_n) (η, a)

$$\llbracket \Gamma \vdash e_1 e_2 : B \rrbracket (\eta) = \underbrace{\left(\llbracket e_1 \rrbracket(\eta) \right)}_{\in \llbracket B \rrbracket^{[A]}} \underbrace{\left(\llbracket e_2 \rrbracket(\eta) \right)}_{\in \llbracket A \rrbracket}$$

Primer $\llbracket x : \text{int} \mid -x + x : \text{int} \rrbracket : \mathbb{Z} \rightarrow \mathbb{Z}$

$$\llbracket x : \text{int} \mid -x + x : \text{int} \rrbracket(m) = \llbracket x \rrbracket(n) + \llbracket x \rrbracket(m) = n + m = 2 \cdot m$$

$$\llbracket 1 + 1 : \text{int} \rrbracket(*) = \llbracket 1 \rrbracket(*) + \llbracket 1 \rrbracket(*) = 1 + 1 = 2$$

Trditev (začasnost) $\bar{c} e \rightsquigarrow e'$, potem $\llbracket e \rrbracket = \llbracket e' \rrbracket$.

Dokaz z indukcijo.

$$\frac{e \rightsquigarrow e'}{\quad}$$

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

$$\llbracket \text{if } e \text{ then } e_1 \text{ else } e_2 \rrbracket(\eta) \stackrel{\text{def}}{=} \begin{cases} \llbracket e_1 \rrbracket(\eta), & \bar{c} e \llbracket e \rrbracket(\eta) = \top \\ \llbracket e_2 \rrbracket(\eta), & \bar{c} e \llbracket e \rrbracket(\eta) = \text{ff} \end{cases}$$

$$\stackrel{\text{i.p.}}{=} \begin{cases} \llbracket e_1 \rrbracket(\eta), & \bar{c} e' \llbracket e' \rrbracket(\eta) = \top \\ \llbracket e_2 \rrbracket(\eta), & \bar{c} e' \llbracket e' \rrbracket(\eta) = \text{ff} \end{cases}$$

$$= \llbracket \text{if } e' \text{ then } e_1 \text{ else } e_2 \rrbracket(\eta)$$

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

$$\llbracket \text{if true then } e_1 \text{ else } e_2 \rrbracket(\eta) = \begin{cases} \llbracket e_1 \rrbracket(\eta), & \bar{c} e \llbracket \text{true} \rrbracket(\eta) = \top \\ \dots \\ = \llbracket e_1 \rrbracket(\eta) \end{cases}$$

$$\bullet \frac{e_1 \rightsquigarrow e'_1}{e_1 e_2 \rightsquigarrow e'_1 e'_2} \& \frac{e_2 \rightsquigarrow e'_2}{N_1 e_2 \rightsquigarrow N_1 e'_2}, \dots \text{podobno kot pri } \frac{e \rightsquigarrow e'}{4e \rightsquigarrow \text{if } e'}$$

$$\bullet \frac{}{(\lambda x \cdot e)_N \rightsquigarrow e[N/x]}$$

$$\begin{aligned}
 \llbracket (\lambda x.e) v \rrbracket(\eta) &\stackrel{\text{DEF}}{=} \llbracket \lambda x.e \rrbracket(\eta)(\llbracket v \rrbracket(\eta)) \\
 &\stackrel{\text{DEF}}{=} \llbracket e \rrbracket(\eta), \llbracket v \rrbracket(\eta)) \\
 &\stackrel{\text{LEMA}}{=} \llbracket e[v/x] \rrbracket(\eta)
 \end{aligned}$$

■

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

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

Primer $\llbracket x:\text{int} \vdash x+2:\text{int} \rrbracket(\llbracket \vdash 3:\text{int} \rrbracket) = (m \mapsto m+2)3 = 5$

$$\llbracket \vdash (x+2)[3/x]:\text{int} \rrbracket = \llbracket \vdash 3+2 \rrbracket = \llbracket 3 \rrbracket + \llbracket 2 \rrbracket = 3+2 = 5$$

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

Lema Za poljuben* ℓ obstaja $\llbracket \ell \rrbracket$, da za vsak* e velja $\llbracket \ell[e] \rrbracket(\eta) = \llbracket \ell \rrbracket(\eta)(\llbracket e \rrbracket(\eta))$.

* tako da so vse interpretacije definirane

Dokaz Indukcija na strukturo ℓ .

Izrek (zadostnost/adegnacy)

Če $\llbracket \vdash e:\text{bool} \rrbracket = \text{tt}$, tedaj $e \rightsquigarrow^* \text{true}$.

Posledica Če je $\llbracket \Gamma \vdash e:A \rrbracket = \llbracket \Gamma \vdash e':A \rrbracket$, tedaj je $e \cong e'$.

Dokaz Vzemimo poljuben ℓ , da je $\ell[e] \rightsquigarrow^* \text{true}$.

Po zdravosti velja $\llbracket \ell[e] \rrbracket = \text{tt}$.

Po tem je $\llbracket \ell[e] \rrbracket = \llbracket \ell \rrbracket(\llbracket e \rrbracket) = \llbracket \ell \rrbracket(\llbracket e' \rrbracket) = \llbracket \ell[e'] \rrbracket$

Torej je $\llbracket \ell[e'] \rrbracket = \text{tt}$. Po zadostnosti velja $\ell[e'] \rightsquigarrow^* \text{true}$.

V drugi smislu je samodružno. ■