Kontekstna ekvivalenca je tisto, kar želimo, vendar je delo z njo precej neobvladljivo, saj moramo kvantificirati čez vse kontekste, ki nimajo preveč lepih lastnosti. Namesto tega se vrnemo nazaj na začetek. Pojme iz našega jezika bomo prevedli na dobro znane matematične pojme, kot so množice in funkcije, saj lahko na njih uporabimo običajno enakost.

Interpretacije tipov in izrazov

Ko delamo s tipi, si v ozadju vedno predstavljamo množico vrednosti, ki jih zasedajo. To bomo formalizirali in za vsak tip A definirali njegovo *interpretacijo* $[\![A]\!]$, ki je množica, rekurzivno definirana kot:

$$\begin{aligned}[\![\mathbf{bool}]\!] &= \mathbb{B} = \{tt, ff\} \\ [\![\mathbf{int}]\!] &= \mathbb{Z} \\ [\![A \to B]\!] &= [\![B]\!]^{[\![A]\!]}\end{aligned}$$

Pri interpretaciji izrazov se bomo omejili na tiste, ki imajo dobro definiran tip. Predstavljamo si lahko, da bomo vsak izraz M tipa A interpretirali z elementom $[\![M]\!] \in [\![A]\!]$. Stvar se malo zaplete, ker se v M lahko pojavijo proste spremenljivke iz nekega konteksta Γ, kar pomeni, da moramo tudi za vsako izmed njih določiti ustrezno vrednost. Zato definiramo interpretacijo kontekstov s kartezičnim produktom

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

Tedaj lahko interpretacijo izraza $\Gamma \vdash M : A$ podamo s preslikavo $[\![M]\!] : [\![\Gamma]\!] \to [\![A]\!]$. Pri tem moramo biti pozorni, da preslikava ni odvisna samo od izraza, temveč od celotne določitve tipa, zato bi v resnici morali pisati

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

čeprav bomo povečini uporabljali krajši zapis. Interpretacijo podamo rekurzivno kot:

$$\begin{aligned}[\![\Gamma \vdash x_i : A_i]\!](a_1, \ldots, a_n) &= a_i \\ [\![\Gamma \vdash \mathbf{true} : \mathbf{bool}]\!](\gamma) &= tt \\ [\![\Gamma \vdash \mathbf{false} : \mathbf{bool}]\!](\gamma) &= ff \\ [\![\Gamma \vdash \mathbf{if}\ M\ \mathbf{then}\ M_1\ \mathbf{else}\ M_2 : A]\!](\gamma) &= \begin{cases} [\![M_1]\!](\gamma) & [\![M]\!](\gamma) = tt \\ [\![M_2]\!](\gamma) & [\![M]\!](\gamma) = ff \end{cases} \\ [\![\Gamma \vdash \underline{n} : \mathbf{int}]\!](\gamma) &= n \\ [\![\Gamma \vdash M_1 + M_2 : \mathbf{int}]\!](\gamma) &= [\![M_1]\!](\gamma) + [\![M_2]\!](\gamma) \\ [\![\Gamma \vdash M_1 * M_2 : \mathbf{int}]\!](\gamma) &= [\![M_1]\!](\gamma) \cdot [\![M_2]\!](\gamma) \\ [\![\Gamma \vdash M_1 < M_2 : \mathbf{bool}]\!](\gamma) &= \begin{cases} tt & [\![M_1]\!](\gamma) < [\![M_2]\!](\gamma) \\ ff & \text{sicer} \end{cases} \\ [\![\Gamma \vdash \lambda x.\, M : A \to B]\!](\gamma) &= a \mapsto [\![\Gamma, x : A \vdash M : B]\!](\gamma, a) \\ [\![\Gamma \vdash M_1\, M_2 : B]\!](\gamma) &= \big([\![M_1]\!](\gamma)\big)\big([\![M_2]\!](\gamma)\big)\end{aligned}$$

Na primer, interpretacija izraza $x : \mathbf{int} \vdash \lambda y.\, \underline{2} * x > y + 5$ je funkcija $\mathbb{Z} \to \mathbb{B}^{\mathbb{Z}}$, podana z

$$\begin{aligned}[\![x : \mathbf{int} \vdash \lambda y.\, \underline{2} * x > y + 5]\!](m) &= n \mapsto [\![x : \mathbf{int}, y : \mathbf{int} \vdash \underline{2} * x > y + 5]\!](m, n) \\ &= n \mapsto \begin{cases} tt & [\![\underline{2} * x]\!](m, n) > [\![y + 5]\!](m, n) \\ ff & \text{sicer} \end{cases} \\ &= n \mapsto \begin{cases} tt & 2 \cdot m > n + 5 \\ ff & \text{sicer} \end{cases}\end{aligned}$$

Povezava med denotacijsko in operacijsko semantiko

Ker imamo za isti jezik dve različni semantiki, se lahko vprašamo, ali se ujemata. In res, če en izraz naredi korak v drugega, se njuni interpretaciji ujemata. Po izreku o varnosti vemo, da bo tudi drugi izraz imel interpretacijo, če jo ima prvi.

Trditev (skladnost). Če za izraz $\vdash M : A$ velja $M \rightsquigarrow M'$, potem je $[\![M]\!] = [\![M']\!]$.

V dokazu bomo uporabili lemo o substituciji, ki jo dokažemo z rutinsko indukcijo.

Lema. Za izraza $\Gamma, x : A \vdash M : B$ in $\Gamma \vdash N : A$ velja

$$[\![\Gamma \vdash M[N/x] : B]\!](\gamma) = [\![M]\!](\gamma, [\![N]\!](\gamma))$$

Dokaz. Dokaz poteka z indukcijo na $M \rightsquigarrow M'$. Za primer si oglejmo pravilo

$$\frac{M_1 \rightsquigarrow M_1'}{}$$

$$\frac{}{M_1\, M_2 \rightsquigarrow M_1'\, M_2}$$

Če velja $\vdash M_1\, M_2 : A$, potem je $[\![M_1\, M_2]\!] = [\![M_1]\!]([\![M_2]\!])$, pri čemer smo zaradi praznega konteksta izpustili pisanje trivialnih argumentov. Po indukcijski predpostavki je $[\![M_1]\!] = [\![M_1']\!]$, zato je tudi $[\![M_1\, M_2]\!] = [\![M_1'\, M_2]\!]$.

Pri pravilu

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

pa na levi strani dobimo

$$[\![(\lambda x.\, M)\, V]\!](\gamma) = [\![M]\!](\gamma, [\![V]\!](\gamma))$$

kar je po lemi o substituciji enako $[\![M[V/x]]\!]$. ■

V obratno smer trditev ne velja. Na primer, $[\![\lambda x.\, x + x]\!] = [\![\lambda x.\, \underline{2} * x]\!]$, čeprav gre za različna izraza, ki sta vrednosti, zato noben ne more narediti enega ali več korakov v drugega. A kot smo omenili že na začetku, ne zanima nas enakost, temveč samo ekvivalentnost rezultatov. Dovolj je, če obrat pokažemo že v enem konkretnem primeru.

Trditev (zadostnost). Če za $\vdash M : \mathbf{bool}$ velja $[\![M]\!] = \mathit{tt}$, potem velja $M \rightsquigarrow^* \mathbf{true}$.

Dokaz je zahteven, zato ga bomo izpustili. Lažji pa je dokaz splošnejše posledice.

Izrek. Če za $\Gamma \vdash M : A$ in $\Gamma \vdash N : A$ velja $[\![M]\!] = [\![N]\!]$, potem velja tudi $M \simeq N$.

Dokaz. Vzemimo poljuben kontekst $\mathcal{C}$, za katerega velja $\mathcal{C}[M] \rightsquigarrow^* \mathbf{true}$. Brez škode za splošnost (čeprav tega nismo dokazali) se lahko omejimo na kontekste, za katere je $\vdash \mathcal{C}[M] : \mathbf{bool}$, torej je $[\![\mathcal{C}[M]]\!]$ definirana in po skladnosti z operacijsko semantiko enaka $[\![\mathbf{true}]\!] = \mathit{tt}$. Ker je interpretacija podana strukturno, je vrednost $[\![\mathcal{C}[M]]\!]$ na tistih mestih, kjer se v $\mathcal{C}$ pojavljajo luknje $[\,]$, odvisna le od $[\![M]\!]$. Ker je $[\![M]\!] = [\![N]\!]$, je torej tudi $[\![\mathcal{C}[N]]\!] = [\![\mathcal{C}[M]]\!] = \mathit{tt}$. Po zadostnosti torej obstaja zaporedje korakov $\mathcal{C}[N] \rightsquigarrow^* \mathbf{true}$, kar smo želeli pokazati. Obrat pokažemo simetrično. ■

By Matija Pretnar