Izomorfizm Curry'ego-Howarda

Rafał Szczerski

2018
Październik

1 Rachunek λ z typami prostymi

1.1 Typy proste

Definicja 1. (Typy proste)
Niech U będzie przeliczalnie nieskończonym zbiorem zmiennych przedmiotowych p, q, ... (być może indeksowanych liczbami naturalnymi), które będziemy nazywali *zmiennymi typowymi. Typami prostymi* będziemy nazywali najmniejszy w sensie mnogościowym zbiór wyrażeń taki, że:

i) Jeśli p jest zmienną typową, to p jest typem prostym.

ii) Jeśli τ i σ są typami prostymi, to $(\tau \to \sigma)$ jest typem prostym.

Typy proste zbudowane tylko wedle reguły i) nazywamy niekiedy typami *atomowymi*, zaś wyrażenia zbudowe wedle reguły ii) – typami *funkcyjnymi*. Zbiór typów prostych określony w myśl powyższej definicji będziemy oznaczali przez $\mathbf{T}_{\to}$.

Ustalmy w ramach konwencji, że późniejsze litery alfabetu greckiego, tj. $\sigma, \tau, \rho, \ldots$ będą służyły nam za zmienne metasyntaktyczne do oznaczania typów prostych. Dla lepszej czytelności będziemy pomijali najbardziej zewnętrzne nawiasy. Symbol „$\to$" (*konstruktor typu*) jest prawostronnie łączny, co oznacza, że typy $\tau \to \sigma \to \theta$ oraz $\tau \to (\sigma \to \theta)$ będziemy uznawali za tożsame.

1.2 Pseudotermy

Niech V będzie przeliczalnie nieskończonym zbiorem zmiennych przedmiotowych x, y, ... (również być może indeksowanych liczbami naturalnymi). Elementy takiego zbioru będziemy nazywali λ-*zmiennymi.*

Definicja 2. (Pseudo-pretermy)
Pseudo-pretermami będziemy nazywali najmniejszy (w sensie mnogościowym) zbiór $\mathbf{\Lambda}_{\mathrm{T}}^{-}$ taki, że:

i) Jeśli $x \in \mathrm{V}$, to $x \in \mathbf{\Lambda}_{\mathrm{T}}^{-}$.

ii) Jeśli $M \in \mathbf{\Lambda}_{\mathrm{T}}^{-}$ i $N \in \mathbf{\Lambda}_{\mathrm{T}}^{-}$, to $(MN) \in \mathbf{\Lambda}_{\mathrm{T}}^{-}$.

iii) Dla dowolnych $x \in \mathrm{V}$, $\sigma \in \mathbf{T}_{\to}$, $M \in \mathbf{\Lambda}_{\mathrm{T}}^{-}$ mamy, że $(\lambda x^{\sigma}. M) \in \mathbf{\Lambda}_{\mathrm{T}}^{-}$.

Wyrażenia postaci ii) nazywamy *aplikacjami* M do N, zaś wyrażenia postaci iii) – λ-abstrakcjami, gdzie o wszystkich podtermach termu M mówi się, że są w *zasięgu* λ-abstraktora, zaś o λ-zmiennej x mówi się, że jest *związana.*

Za zmienne metasyntaktyczne obieramy duże litery alfabetu łacińskiego M, N, ... Podobnie jak poprzednio, stosujemy konwencję o opuszczaniu najbardziej zewnętrznych nawiasów. Aplikacja termów jest łączna lewostronnie, co oznacza, że będziemy utożsamiać wyrażenia MNP i $(MN)P$.

Definicja 3. (Zmienne wolne)
Dla pseudo-pretermu M określamy zbiór *termów wolnych* FV w nastepujący sposób:

$$\begin{aligned} \mathrm{FV}(x) &= \{x\} \\ \mathrm{FV}(\lambda x^\sigma.\, P) &= \mathrm{FV}(P) \setminus \{x\} \\ \mathrm{FV}(PQ) &= \mathrm{FV}(P) \cup \mathrm{FV}(Q) \end{aligned}$$

Jesli $\mathrm{FV}(M) = \varnothing$, to mówimy, że M jest *zamknięty*.

Definicja 4. (Podstawienie)
Podstawieniem $[x/N]$ pseudo-pretermu N za λ-zmienną x w M nazwamy zdefiniowane następująco przekształcenie:

$$\begin{aligned} x[x/N] &= N, & & \\ y[x/N] &= y, & & \text{o ile } x \neq y, \\ (PQ)[x/N] &= P[x/N]\, Q[x/N], & & \\ (\lambda y^\sigma.\, P)[x/N] &= \lambda y^\sigma.\, P[x/N], & & \text{gdzie } x \neq y \text{ i } y \notin \mathrm{FV}(N). \end{aligned}$$

Zachodzą następujące fakty:

Fakt 1. *(a) Jeśli $x \notin \mathrm{FV}(M)$, to $M[x/N]$ jest poprawnym podstawieniem i $M[x/N] = M$.*

(b) Jeśli $M[x/N]$ jest poprawnym podstawieniem, to $y \in \mathrm{FV}(M[x/N]$ wtw, gdy albo $y \in \mathrm{FV}(M)$ i $x \neq y$, albo $y \in \mathrm{FV}(N)$ i $x \in \mathrm{FV}(M)$.

(c) Podstawienie $M[x/x]$ jest poprawne i $M[x/x] = M$.

(d) Jeśli $M[x/y]$ jest poprawnym podstawieniem, to $M[x/y]$ ma tę samą długość, co M.

Fakt 2. *Powiedzmy, że $M[x/N]$ jest poprawnym podstawieniem i $N[y/L]$ i $M[x/N][y/L]$ są poprawnymi podstawieniami, gdzie $x \neq y$. Jeśli $x \notin \mathrm{FV}(L)$ lub $y \notin \mathrm{FV}(M)$, to $M[y/L]$ i $M[y/L]\,[x/N[y/L]]$ jest poprawnym podstawieniem oraz*

$$M[x/N][y/L] = M[y/L][x/N[y/L]].$$

Fakt 3. *Jesli $M[x/y]$ jest poprawnym postawieniem i $y \notin \mathrm{FV}(M)$, to $M[x/y][y/x]$ jest poprawnym podstawieniem oraz $M[x/y][y/x] = M$.*

Definicja 5. (α-konwersja)
α-konwersją nazywamy najmniejszą (w sensie mnogościowym) zwrotną i przechodnią relację binarną $=_\alpha$ określoną na zbiorze pseudotermów Λ_{T}^{-} spełniającą poniższe warunki:

(a) Jeśli $y \notin \mathrm{FV}(M)$ i $M[x/y]$ jest poprawnym podstawieniem, to $\lambda x.\, M =_\alpha \lambda y.\, M[x/y]$.

(b) Jeśli $M =_\alpha N$, to dla każdej λ-zmiennej x mamy $\lambda x.\, M =_\alpha \lambda x.\, N$.

(c) Jeśli $M =_\alpha N$, to $MZ =_\alpha NZ$.

(d) Jeśli $M =_\alpha N$, to $ZM =_\alpha ZN$.

Bez dowodu podajemy następujące twierdzenia:

Fakt 4. *Relacja* $=_\alpha$ *jest symetryczna.*

Fakt 5. $=_\alpha$ *jest relacją równoważności.*

Fakt 6. *Jeśli* $M =_\alpha N$, *to* $\mathrm{FV}(M) = \mathrm{FV}(N)$.

Dysponując powyższymi rozstrzygnięciami otrzymujemy wygodne utożsamienie pseudo-pretermów, które różnią się między sobą tylko zmiennymi związanymi.

Definicja 6. (Pseudotermy)
Pseudotermami nazywamy zbiór ilorazowy $\mathbf{\Lambda}_\mathrm{T}$ relacji α-konwersji

$$\mathbf{\Lambda}_\mathrm{T} = \{[M]_\alpha \mid M \in \mathbf{\Lambda}_\mathrm{T}^-\}$$

1.3 Typowalność

Definicja 7. (Kontekst)
Kontekstem (ang. *enviroment*) nazywamy skończoną funkcję częściową $\Gamma : \mathrm{V} \to \mathbf{T}_\to$, czyli zbiór par postaci $\Gamma = \{x_1^{\tau_1}, \ldots, x_n^{\tau_n}\}$, gdzie $(x_i^{\tau_i}) = (x_i, \tau_i)$ oraz $x_i \neq x_j$ dla $i \neq j$. Zbiór

$$\mathrm{dom}(\Gamma) = \{x \in \mathrm{V} \mid \exists\tau(x^\tau \in \Gamma)\}$$

nazywamy *dziedziną* kontekstu Γ, zaś

$$\mathrm{rg}(\Gamma) = \{\tau \in \mathbf{T}_\to \mid \exists x(x^\tau \in \Gamma)\}$$

– *zakresem* kontekstu Γ. Piszemy:

- $x_1^{\tau_1}, x_2^{\tau_2}$ zamiast $\{x_1^{\tau_1}, x_2^{\tau_2}\}$, o ile $x_1^{\tau_1}$ i $x_2^{\tau_2}$ są różne,
- Γ, x^φ zamiast $\Gamma \cup \{x^\varphi\}$, o ile $x^\varphi \notin \Gamma$,
- Γ, Δ zamiast $\Gamma \cup \Delta$, o ile $\Gamma \cap \Delta = \varnothing$.

Wprowadzimy teraz system w stylu dedukcji naturalnej. *Sekwentami* będziemy nazywali wyrażenia postaci $\Gamma \vdash M^\sigma$, gdzie $M \in \mathbf{\Lambda}_\mathrm{T}$, $\sigma \in \mathbf{T}_\to$, zaś Γ jest pewnym otoczeniem typowym.

Wprowadzamy następujące reguły dowodzenia:

$$\frac{}{\Gamma, x^\tau \vdash x^\tau}\ (\mathrm{Var}), \qquad \frac{\Gamma, x^\varphi \vdash M^\psi}{\Gamma \vdash (\lambda x^\varphi.\, M)^{\varphi\to\psi}}\ (\mathrm{Abs}), \qquad \frac{\Gamma \vdash M^{\varphi\to\psi} \qquad \Gamma \vdash N^\varphi}{\Gamma \vdash (MN)^\psi}\ (\mathrm{App}).$$

Definicja 8. (Typowalność)
Mówimy, że pseudoterm M jest typu σ w kontekście Γ (jest *typowalny*), jeśli istnieje skończone drzewo sekwentów spełniające poniższe warunki:

1. W korzeniu drzewa znajduje się sekwent $\Gamma \vdash M^\sigma$.
2. Liście są *aksjomatami*, tj. sekwentami postaci $\Gamma, x^\sigma \vdash x^\sigma$.
3. Każdego rodzica można otrzymać z jego dzieci przez zastosowanie którejś z reguł wyprowadzania nowych sekwentów.

Wszystkie typowalne pseudotermy w pewnym kontekście Γ nazywamy λ-*termami* (z typami prostymi).

Uwaga. λ-term w kontekście Γ_1 może nie być typowalny w innym kontekście Γ_2.

Fakt 7. *Jesli* $\Gamma \vdash M^\sigma$ *oraz* $\Gamma \vdash M^\tau$, *to* $\sigma = \tau$.

1.4 Redukcja

Definicja 9. (Zgodność)
Relację R na zbiorze termów $\mathbf{\Lambda}_{\mathrm{T}}$ nazywamy *zgodną*, jeśli dla M, N, $Z \in \mathbf{\Lambda}_{\mathrm{T}}$ spełnia następujące warunki:

i) Jeśli $M \mathrm{R} N$, to $(\lambda x^{\sigma}. M) \,\mathrm{R}\, (\lambda x^{\sigma}. N)$ dla dowolnych $x \in \mathrm{V}$ i $\sigma \in \mathbf{T}_{\rightarrow}$.

ii) Jeśli $M \mathrm{R} N$, to $(MZ) \,\mathrm{R}\, (NZ)$.

iii) Jeśli $M \mathrm{R} N$, to $(ZM) \,\mathrm{R}\, (ZN)$.

Kongruencją nazywamy zgodną relację równowazności na $\mathbf{\Lambda}_{\mathrm{T}}$.
Redukcją nazywamy zgodną, zwrotną i przechodnią relację na $\mathbf{\Lambda}_{\mathrm{T}}$.

Definicja 10. (β-redukcja)
β-redukcją nazywamy najmniejsza w sensie mnogościowym *zgodną* relację binarną $\longrightarrow_{\beta}$ określoną zbiorze na pseudotermów $\mathbf{\Lambda}_{\mathrm{T}}$ za pomocą podstawienia

$$(\lambda x^{\sigma}. P)Q \longrightarrow_{\beta} P[x/Q].$$

β-redeksem nazywamy wyrażenia postaci $(\lambda x^{\sigma}. M)N$. Rezultatem β-redukcji jest term postaci $M[x/N]$, który nazywamy *β-reduktem.*

Mówimy, że λ-term M jest w *postaci normalnej*, jeśli żadna jego podformuła nie jest β-redeksem.
M ma postać normalną, jeśli $M =_{\beta} N$ dla pewnego N, który jest w postaci normalnej.
$\longrightarrow_{\beta}^{+}$ jest przechodnim domknięciem relacji $\longrightarrow_{\beta}$ w zbiorze pseudotermów Λ_{T}.
$\longrightarrow_{\beta}^{*}$ jest domknięciem przechodnio-zwrotnim w Λ_{T} relacji $\longrightarrow_{\beta}$, a zatem jest *redukcją.*
$=_{\beta}$ jest najmniejszą relację równowazności zawierającą relację $\longrightarrow_{\beta}$, a zatem *kongruencją.*

Fakt 8. *Jeśli* $\Gamma \vdash M^{\sigma}$ *i* $M \longrightarrow_{\beta}^{*} N$*, to* $\Gamma \vdash N^{\sigma}$*.*

η-redukcją nazywamy najmniejszą (w sensie mnogościowym) *zgodną* relację w Λ_{T} taką, że

$$\lambda x^{\sigma}. Mx \longrightarrow_{\eta} M,$$

o ile $x \notin \mathrm{FV}(M)$.

Fakt 9. *Jeśli* $\Gamma \vdash M^{\sigma}$ *i* $M \longrightarrow_{\eta}^{*} N$*, to* $\Gamma \vdash N^{\sigma}$*.*

1.5 Normalizacja

λ-term M ma własność *(słabej) normalizacji* (co symbolicznie oznaczamy $M \in \mathrm{WN}_{\beta}$) wtedy i tylko wtedy, gdy istnieje ciąg β-redukcji rozpoczynający się od M i kończący się termem w postaci normalnej N. Powiemy, że λ-term M ma własność *silnej normalizacji* (symbolicznie: $M \in \mathrm{SN}_{\beta}$), jeśli wszystkie ciągi β-redukcji rozpoczynające się M są skończone.

Strategią redukcji nazywamy odwzorowanie $F : \Lambda_{\mathrm{T}} \to \Lambda_{\mathrm{T}}$ takie, że $F(M) = M$, gdy M jest w postaci normalnej i $M \to_{\beta} F(M)$ w przeciwnym wypadku. Mówimy, że strategia F jest *normalizująca*, jeśli dla każdego $M \in \mathrm{WN}_{\beta}$ istnieje $i \in \mathbb{N}$ takie, że $F^{i}(M)$ jest w postaci normalnej.

Twierdzenie 1. *(*Własność WN_{β}*) Każdy λ-term w stylu Churcha ma postać normalną.*

Twierdzenie 2. *(*Własność SN_{β}*) Każdy λ-term w stylu Churcha własność silnej normalizacji.*

- WCR: $\forall a, b, c \in A\, (a \longrightarrow b \wedge a \longrightarrow c) \to \exists d \in A\, (b \longrightarrow^* d \wedge c \longrightarrow^* d)$
- CR: $\forall a, b, c \in A\, (a \longrightarrow^* b \wedge a \longrightarrow^* c) \to \exists d \in A\, (b \longrightarrow^* d \wedge c \longrightarrow^* d)$

Twierdzenie 3. (Lemat Newmana) *Niech $\to$ bedzie relacją binarną spełniającą SN. Jeśli $\to$ spełnia WCR, to spełnia CR.*

Twierdzenie 4. *(*Własność SN_β*) Każdy λ-term w stylu Churcha własność silnej normalizacji.*