

# Izomorfizm Curry’ego-Howarda

Rafał Szacherski

2018

Październik

## 1 Rachunek $\lambda$ z typami prostymi

### 1.1 Typy proste

**Definicja 1.** (Typy proste)

Niech  $U$  będzie przeliczalnie nieskończonym zbiorem zmiennych przedmiotowych  $p, q, \dots$  (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  $\tau$  i  $\sigma$  są typami prostymi, to  $(\tau \rightarrow \sigma)$  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  $\mathbf{T}_{\rightarrow}$ .

Późniejsze litery alfabetu greckiego, tj.  $\sigma, \tau, \rho, \dots$  będą służyły nam za zmienne metasyntaktyczne do oznaczania typów prostych. Dla lepszej czytelności będziemy pomijali najbardziej zewnętrzne nawiasy. Konstruktor typu  $\rightarrow$  jest prawostronnie łączny, co oznacza, że typy  $\tau \rightarrow \sigma \rightarrow \theta$  oraz  $\tau \rightarrow (\sigma \rightarrow \theta)$  będziemy uznawali za tożsame.

Typy proste ujęte Definicją 1 mają strukturę drzewa binarnego. Wysokość takiego drzewa będziemy nazywali *stopniem* typu. Precyzyjnie ujmuje to pojęcie poniższa definicja.

**Definicja 2.** (Stopień typu)

Stopniem typu nazywamy funkcję

$$\begin{aligned}\delta(p) &= 0, \\ \delta(\tau \rightarrow \sigma) &= 1 + \max(\delta(\tau), \delta(\sigma)).\end{aligned}$$

## 1.2 Pseudotermy

Niech  $V$  będzie przeliczalnie nieskończonym zbiorem zmiennych przedmiotowych  $x, y, \dots$  (indeksowanych być może liczbami naturalnymi). Elementy takiego zbioru będziemy nazywali  $\lambda$ -zmiennymi.

**Definicja 3.** (Pseudo-pretermy)

*Pseudo-pretermami* będziemy nazywali najmniejszy (w sensie mnogościowym) zbiór  $\Lambda_T^-$  taki, że:

- i) Jeśli  $x \in V$ , to  $x \in \Lambda_T^-$ .
- ii) Jeśli  $M \in \Lambda_T^-$  i  $N \in \Lambda_T^-$ , to  $(MN) \in \Lambda_T^-$ .
- iii) Dla dowolnych  $x \in V$ ,  $\sigma \in \mathbf{T}_\rightarrow$ ,  $M \in \Lambda_T^-$  mamy, że  $(\lambda x^\sigma. M) \in \Lambda_T^-$ .

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

Za zmienne metasyntaktyczne obieramy duże litery alfabetu łacińskiego  $M, N, \dots$ . Podobnie jak w podrozdziale 1.1 stosujemy konwencję o opuszczaniu najbardziej zewnętrznych nawiasów. Aplikacja termów jest łączna lewostronnie, co oznacza, że będziemy utożsamiali wyrażenia  $MNP$  oraz  $(MN)P$ .

**Definicja 4.** (Zmienne wolne)

Dla pseudo-pretermu  $M$  określamy zbiór *termów wolnych*  $FV$  w następujący sposób:

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

Jesli  $FV(M) = \emptyset$ , to mówimy, że  $M$  jest *zamknięty*.

**Definicja 5.** (Podstawienie)

*Podstawieniem*  $[x/N]$  pseudo-pretermu  $N$  za  $\lambda$ -zmienną  $x$  w  $M$  nazwamy zdefiniowane następująco przekształcenie:

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

Zachodzą następujące fakty:

- Fakt 1.** (a) *Jeśli  $x \notin \text{FV}(M)$ , to  $M[x/N]$  jest poprawnym podstawieniem i  $M[x/N] = M$ .*
- (b) *Jeśli  $M[x/N]$  jest poprawnym podstawieniem, to  $y \in \text{FV}(M[x/N])$  wtw, gdy albo  $y \in \text{FV}(M)$  i  $x \neq y$ , albo  $y \in \text{FV}(N)$  i  $x \in \text{FV}(M)$ .*
- (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  $x \notin \text{FV}(L)$  lub  $y \notin \text{FV}(M)$ , 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.** *Jeśli  $M[x/y]$  jest poprawnym podstawieniem i  $y \notin \text{FV}(M)$ , to  $M[x/y][y/x]$  jest poprawnym podstawieniem oraz  $M[x/y][y/x] = M$ .*

**Definicja 6.** ( $\alpha$ -konwersja)

$\alpha$ -konwersją nazywamy najmniejszą (w sensie mnogościowym) zwrotną i przechodnią relację binarną  $=_\alpha$  określoną na zbiorze pseudotermów  $\Lambda_T^-$  spełniającą poniższe warunki:

- (a) *Jeśli  $y \notin \text{FV}(M)$  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  $\lambda$ -zmiennnej  $x$  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  $\text{FV}(M) = \text{FV}(N)$ .*

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

**Definicja 7.** (Pseudotermy)

Klasy abstrakcji relacji  $\alpha$ -konwersji nazywamy *pseudotermami*. Zbiór wszystkich pseudotermów oznaczamy następująco:

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

Nadużywając notacji będziemy odnosili się do pseudotermów tylko przez ich reprezentantów.

### 1.3 Typowalność

**Definicja 8.** (Kontekst)

*Kontekstem* nazywamy skończoną funkcję częściową  $\Gamma : V \longrightarrow \mathbf{T}_\rightarrow$ , czyli zbiór par postaci  $\Gamma = \{x_1^{\tau_1}, \dots, x_n^{\tau_n}\}$ , gdzie  $(x_i^{\tau_i}) = (x_i, \tau_i)$  oraz  $x_i \neq x_j$  dla  $i \neq j$ . Zbiór

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

nazywamy *dziedziną* kontekstu  $\Gamma$ , zaś

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

– *zakresem* kontekstu  $\Gamma$ . 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,
- $\Gamma, x^\varphi$  zamiast  $\Gamma \cup \{x^\varphi\}$ , o ile  $x^\varphi \notin \Gamma$ ,
- $\Gamma, \Delta$  zamiast  $\Gamma \cup \Delta$ , o ile  $\Gamma \cap \Delta = \emptyset$ .

Określimy teraz system przypisywania typów do pseudotermów w stylu dedukcji naturalnej. *Sekwentami* będziemy nazywali wyrażenia postaci  $\Gamma \vdash M^\sigma$ , gdzie  $M \in \mathbf{\Lambda}_T$ ,  $\sigma \in \mathbf{T}_\rightarrow$ , zaś  $\Gamma$  jest pewnym kontekstem.

Wprowadzamy następujące reguły dowodzenia:

$$\frac{}{\Gamma, x^\tau \vdash x^\tau} \text{ (Var)}, \quad \frac{\Gamma, x^\varphi \vdash M^\psi}{\Gamma \vdash (\lambda x^\varphi. M)^\varphi \rightarrow^\psi} \text{ (Abs)}, \quad \frac{\Gamma \vdash M^{\varphi \rightarrow \psi} \quad \Gamma \vdash N^\varphi}{\Gamma \vdash (MN)^\psi} \text{ (App)}.$$

**Definicja 9.** (Typowalność)

Mówimy, że pseudoterm  $M$  jest typu  $\sigma$  w kontekście  $\Gamma$  (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.

**Definicja 10.** ( $\lambda$ -termy)

Wszystkie typowalne pseudotermy w pewnym kontekście  $\Gamma$  nazywamy  $\lambda$ -termami (z typami prostymi w kontekście  $\Gamma$ ).

*Uwaga.*  $\lambda$ -term w kontekście  $\Gamma_1$  może nie być typowalny w innym kontekście  $\Gamma_2$ .

Mówiąc o  $\lambda$ -termach i nie podając żadnego związanego z nimi kontekstu  $\Gamma$  będziemy implicite zakładali, że istnieje pewien kontekst w którym są one typowalne. Zakładamy również, że ustalone są typy dla wszystkich  $\lambda$ -zmiennych. Typ dowolnego  $\lambda$ -termu będziemy w ramach konwencji notowali używając górnego indeksu. Dla przykładu,  $\lambda$ -term  $(M^{\sigma \rightarrow \tau} N^\sigma)^\tau$  jest w pewnym kontekście  $\Gamma$  typu  $\tau$ .

Przez *stopień*  $\lambda$ -termu  $M^\sigma$  będziemy mieli na myśli stopień typu  $\sigma$ . Nadużywając notacji będziemy pisali

$$\delta(M^\sigma) = \delta(\sigma),$$

gdzie  $\delta$  występująca po prawej stronie powyższej równości to funkcja określona w myśl Definicji 2.

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

## 1.4 Redukcja

**Definicja 11.** (Zgodność)

Relację  $R$  na zbiorze termów  $\mathbf{\Lambda}_T$  nazywamy *zgodną*, jeśli dla  $M, N, Z \in \mathbf{\Lambda}_T$  spełnia ona następujące warunki:

- i) Jeśli  $MRN$ , to  $(\lambda x^\sigma. M)R(\lambda x^\sigma. N)$  dla dowolnych  $x \in V$  i  $\sigma \in \mathbf{T}_\rightarrow$ .
- ii) Jeśli  $MRN$ , to  $(MZ)R(NZ)$ .
- iii) Jeśli  $MRN$ , to  $(ZM)R(ZN)$ .

*Kongruencją* nazywamy zgodną relację równoważności na  $\mathbf{\Lambda}_T$ .

*Redukcją* nazywamy zgodną, zwrotną i przechodnią relację na  $\mathbf{\Lambda}_T$ .

**Definicja 12.** ( $\beta$ -redukcja)

$\beta$ -redukcją nazywamy najmniejsza w sensie mnogościowym *zgodną* relację binarną  $\rightarrow_\beta$  określoną na zbiorze pseudotermów  $\mathbf{\Lambda}_T$  za pomocą podstawienia

$$(\lambda x^\sigma. P)Q \rightarrow_\beta P[x/Q].$$

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

Mówimy, że  $\lambda$ -term  $M$  jest w *postaci normalnej*, jeśli żadna jego podformuła nie jest  $\beta$ -redexem.

$M$  ma *postać normalną*, jeśli  $M =_{\beta} N$  dla pewnego  $N$ , który jest w postaci normalnej.

$\rightarrow_{\beta}^+$  jest przechodnim domknięciem relacji  $\rightarrow_{\beta}$  w zbiorze pseudotermów  $\Lambda_T$ .

$\rightarrow_{\beta}^*$  jest domknięciem przechodnio-zwrotnym w  $\Lambda_T$  relacji  $\rightarrow_{\beta}$ , a zatem jest *redukcją*.

$=_{\beta}$  jest najmniejszą relacją równoważności zawierającą relację  $\rightarrow_{\beta}$ , a zatem *kongruencją*.

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

$\eta$ -redukcją nazywamy najmniejszą (w sensie mnogościowym) *zgodną* relację w  $\Lambda_T$  taką, że

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

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

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

## 1.5 Normalizacja

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

**Definicja 13.** (Strategia redukcji)

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

**Twierdzenie 1.** (Własność  $\text{WN}_{\beta}$ ) *Każdy  $\lambda$ -term w stylu Churcha ma postać normalną.*

**Dowód.**

**Twierdzenie 2.** (Własność  $\text{SN}_{\beta}$ ) *Każdy  $\lambda$ -term w stylu Churcha własność silnej normalizacji.*

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

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

**Dowód.**

**Twierdzenie 4.** (Własność  $SN_\beta$ ) *Każdy  $\lambda$ -term w stylu Churcha własność silnej normalizacji.*

**Dowód.**