

Izomorfizm Curry’ego-Howarda

Rafał Szacherski

2018
Październik

1 Implikatywna logika minimalna

1.1 Język

Definicja 1.

- Zbiorem Φ_{\rightarrow} formuł implikatywnej logiki minimalnej $NJ(\rightarrow)$ nazywamy język generowany przez gramatykę

$$\begin{aligned}\Phi_{\rightarrow} &:= V \mid (\Phi_{\rightarrow} \rightarrow \Phi_{\rightarrow}) \mid \perp \\ V &:= p \mid V'\end{aligned}$$

- Wyrażenia powstałe z produkcji V nazywamy *zmiennymi zdaniowymi*. Zmienne zdaniowe oraz \perp są formułami *atomowymi*. Pozostałe wyrażenia nazywamy formułami *złożonymi*.
- Konwencje:

1. W języku podmiotowym wprowadzamy następujące oznaczenia

$$\begin{aligned}\neg\varphi &:= \text{‘}\varphi \rightarrow \perp\text{’} \\ \top &:= \text{‘}\perp \rightarrow \perp\text{’}\end{aligned}$$

2. Zamiast p', p'', p''', \dots używamy kolejno liter p, q, r, \dots
 3. Za zmienne podmiotowe dla oznaczeń formuł zdaniowych obieramy późniejsze litery alfabetu greckiego, tj. $\varphi, \psi, \theta \dots$
 4. \rightarrow jest łączna w prawo.
 5. \neg ma najwyższy priorytet, \rightarrow – najniższy.
 6. Pomijamy najbardziej zewnętrzne nawiasy.
- Każdą parę $(\Gamma, \varphi) \in \mathcal{P}(\Phi_{\rightarrow}) \times \Phi_{\rightarrow}$, gdzie Γ jest zbiorem skończonym nazywamy *sądem* (*asercją*) i oznaczamy $\Gamma \vdash \varphi$.

Piszemy:

- $\varphi_1, \varphi_2 \vdash \psi$ zamiast $\{\varphi_1, \varphi_2\} \vdash \psi$,
- Γ, φ zamiast $\{\Gamma \cup \varphi\}$,
- Γ, Δ zamiast $\{\Gamma \cup \Delta\}$,

$- \vdash \varphi$ zamiast $\emptyset \vdash \varphi$.

- Na zbiorze sądów $\mathcal{P}(\Phi_{\rightarrow}) \times \Phi_{\rightarrow}$ wprowadzamy relacje określające reguły wyprowadzania

$$\frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \rightarrow \psi} (\rightarrow I), \quad \frac{\Gamma \vdash \varphi \rightarrow \psi \quad \Gamma \vdash \varphi}{\Gamma \vdash \psi} (\rightarrow E).$$

oraz wybieramy spośród sądów jeden aksjomat postaci $\Gamma, \varphi \vdash \varphi$ (Ax).

- *Dowodem* sądu $\Gamma \vdash \varphi$ nazywamy skończone drzewo sądów spełniające poniższe warunki:
 1. W korzeniu drzewa znajduje się dowodzony sąd $\Gamma \vdash \varphi$.
 2. Liście są *aksjomatami*, tj. sądami postaci $\Gamma, \varphi \vdash \varphi$.
 3. Każdego rodzica można otrzymać z jego dzieci przez zastosowanie którejś z reguł wyprowadzania nowych sądów.

Jeśli istnieje dowód sądu $\Gamma \vdash \varphi$ to mówimy, że formuła φ jest *wyprowadzalna* ze zbioru *przesłanek* Γ i piszemy $\Gamma \vdash_N \varphi$. Formułę φ nazywamy wówczas *tezą* systemu NJ(\rightarrow).

Lemat 1. NJ(\rightarrow) jest zamknięty ze względu na

- (a) *osłabianie*: jeśli $\Gamma \vdash \varphi$, to tym bardziej $\Gamma, \psi \vdash \varphi$.
- (b) *podstawianie*: jeśli $\Gamma \vdash \varphi$, to $\Gamma[p/\psi] \vdash \varphi[p/\psi]$.

1.2 Semantyka

Twierdzenie 1. (O pełności) System dedukcyjny NJ(\rightarrow) jest pełny względem modeli Kripkego.

2 Typy proste w stylu Churcha

System λ_{\rightarrow} w stylu Churcha to zbiór typów T, zbiór pseudotermów Λ_T , rodzina otoczeń typowych, relacja β -kontrakcji \rightarrow_{β} i relacja przypisania typu \vdash .

2.1 Język

Definicja 2.

- *Typami prostymi* T nazywamy zbiór Φ_{\rightarrow} wszystkich formuł języka logiki NJ(\rightarrow). Zamiast mówić o zmiennych zdaniowych, będziemy używali określenia *zmiennie typowe*.

Za zmienne podmiotowe dla oznaczeń formuł zdaniowych obieramy późniejsze litery alfabetu greckiego, tj. $\sigma, \tau, \rho \dots$

- *Pseudo-pretermami* nazywamy język Λ_T generowany przez gramatykę

$$\Lambda_T^- := V \mid (\lambda V^T. \Lambda_T^-) \mid (\Lambda_T^- \Lambda_T^-)$$

gdzie V to przeliczalny zbiór λ -zmiennych x, y, \dots

W języku podmiotowym będziemy używali późniejszych liter alfabetu łacińskiego pisanych kursywą (M, N, O, \dots) oznaczając pseudotermy.

- *Otoczeniem typowym* nazywamy skończoną funkcję częściową $\Gamma : V \rightarrow T$ przeprowadzającą zbiór λ -zmiennych w zbiór typów prostych. Nadużywając notacji piszemy

$$\begin{aligned} - \Gamma &= \{x_1 : \tau_1, \dots, x_n : \tau_n\} \\ - \text{dom}(\Gamma) &= \{x \in V \mid \exists \tau. (x : \tau) \in \Gamma\} \\ - \text{rg}(\Gamma) &= \{\tau \in \Phi_{\rightarrow} \mid \exists x. (x : \tau) \in \Gamma\} \end{aligned}$$

- Dla pseudotermu M następująco określamy zbiór *termów wolnych* FV :

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

- *Podstawieniem* $[x/N]$ pseudotermu N za λ -zmienną x w M nazwamy zdefiniowane następująco przekształcenie:

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

Jesli $\text{FV}(M) = \emptyset$, to pseudoterm M nazywamy *zamkniętym*.

Fakt 1.

- Jeśli $x \notin \text{FV}(M)$, to $M[x/N]$ jest poprawnym podstawieniem i $M[x/N] = M$.
- 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 $x \in \text{FV}(M)$.
- Podstawienie $M[x/x]$ jest poprawne i $M[x/x] = M$.
- 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 $M[x/y][y/x] = M$.

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

- Jeśli $y \notin \text{FV}(M)$ i $M[x/y]$ jest poprawnym podstawieniem, to $\lambda x. M =_\alpha \lambda y. M[x/y]$.
- Jeśli $M =_\alpha N$, to dla każdej λ -zmiennnej x mamy $\lambda x. M =_\alpha \lambda x. N$.
- Jeśli $M =_\alpha N$, to $MZ =_\alpha NZ$.

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

Fakt 4. Relacja $=_{\alpha}$ jest symetryczna.

Fakt 5. $=_{\alpha}$ jest relacją równoważności.

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

- *Pseudotermami* nazywamy zbiór ilorazowy Λ_T relacji α -konwersji

$$\Lambda_T = \{[M]_{\alpha} \mid M \in \Lambda_T^{\sim}\}$$

- *Sądem (asercją)* nazywamy każdą trójkę $(\Gamma, M, \sigma) \in \mathcal{P}(V \times T) \times \Lambda_T \times T$, gdzie Γ jest otoczeniem typowym i oznaczamy $\Gamma \vdash M^{\sigma}$.

Piszemy:

- $\varphi_1, \varphi_2 \vdash \psi$ zamiast $\{\varphi_1, \varphi_2\} \vdash \psi$,
- Γ, x^{φ} zamiast $\Gamma \cup \{x^{\varphi}\}$, o ile $x^{\varphi} \notin \Gamma$.
- Γ, Δ zamiast $\{\Gamma \cup \Delta\}$, o ile $\Gamma \cap \Delta = \emptyset$.
- $\vdash \varphi$ zamiast $\emptyset \vdash \varphi$.

- Na zbiorze sądów wprowadzamy relacje określające reguły wyprowadzania termów

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

oraz wybieramy spośród sądów jeden aksjomat postaci $\Gamma, x^{\tau} \vdash x^{\tau}$ (Var).

Dowód sądu określamy analogicznie jak w logice NJ(\rightarrow).

Mówimy, że M jest *termem* typu τ w otoczeniu Γ , jeśli istnieje dowód sądu $\Gamma \vdash M^{\tau}$ w powyższym systemie dedukcyjnym.

2.2 Redukcja

Definicja 3. • Relację R na zbiorze pseudotermów Λ_T nazywamy *zgodną*, jeśli dla $M, N, Z \in \Lambda_T$ spełnia następujące warunki

- (a) Jeśli MRN , to $(\lambda x^{\sigma}. M)R(\lambda x^{\sigma}. N)$ dla każdej λ -zmiennnej x dla której istnieje $\sigma \in T$.
- (b) Jeśli MRN , to $(MZ)R(NZ)$.
- (c) Jeśli MRN , to $(ZM)R(ZN)$.

- *Kongruencją* nazywamy zgodną relację równoważności na Λ_T .
- *Redukcją* nazywamy zgodną, zwrotną i przechodnią relację na Λ_T .
- β -redukcją nazywamy najmniejszą w sensie mnogościowym *zgodną* relację „ \rightarrow_{β} ” określoną zbiorze pseudotermów Λ_T za pomocą podstawienia

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

\rightarrow_{β}^{+} jest przechodnim domknięciem relacji \rightarrow_{β} w zbiorze pseudotermów Λ_T .

\rightarrow_{β}^{*} jest domknięciem przechodnio-zwrotnym w Λ_T relacji \rightarrow_{β} , a zatem jest *redukcją*.

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

Fakt 7. *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 $x \notin \text{FV}(M)$.

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

2.3 Normalizacja