Izomorfizm Curry'ego-Howarda

Rafał Szczerski

2018
Październik

1 Implikatywna logika minimalna

1.1 Język

Definicja 1.

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

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

- Wyrażenia powstałe z produkcji V nazywamy *zmiennymi zdaniowymi*. Zmienne zdaniowe oraz $\bot$ są formułami *atomowymi*. Pozostałe wyrażenia nazywamy formułami *złożonymi*.
- Konwencje:
  1. W języku podmiotowym wprowadzamy następujące oznaczenia

$$\begin{aligned}\neg\varphi &:= \ulcorner \varphi \rightarrow \bot \urcorner \\ \top &:= \ulcorner \bot \rightarrow \bot \urcorner\end{aligned}$$

  2. Zamiast p', p'', p''', ... używamy kolejno liter p, q, r, ...
  3. Za zmienne podmiotowe dla oznaczeń formuł zdaniowych obieramy późniejsze litery alfabetu greckiego, tj. φ, ψ, θ ...
  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 $\varnothing \vdash \varphi$.

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

$$\frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \to \psi}\ (\to\mathrm{I}), \qquad \frac{\Gamma \vdash \varphi \to \psi \qquad \Gamma \vdash \varphi}{\Gamma \vdash \psi}\ (\to\mathrm{E}).$$

  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($\to$).

Lemat 1. NJ($\to$) *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($\to$) *jest pełny względem modeli Kripkego.*

2 Typy proste w stylu Churcha

System $\lambda_\to$ w stylu Churcha to zbiór typów T, zbiór pseudotermów Λ_T, rodzina otoczeń typowych, relacja β-kontrakcji $\to_\beta$ i relacja przypisania typu $\vdash$.

2.1 Język

Definicja 2.

- *Typami prostymi* T nazywamy zbiór $\Phi_\to$ wszystkich formuł języka logiki NJ($\to$). Zamiast mówić o zmiennych zdaniowych, będziemy używali określenia *zmienne typowe*.

  Za zmienne podmiotowe dla oznaczeń formuł zdaniowych obieramy późniejsze litery alfabetu greckiego, tj. σ, τ, ρ ...

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

$$\Lambda_\mathrm{T}^- \coloneqq \mathrm{V} \mid \left(\lambda V^\mathrm{T}.\Lambda_\mathrm{T}^-\right) \mid (\Lambda_\mathrm{T}^-\Lambda_\mathrm{T}^-)$$

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

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

- *Otoczeniem typowym* nazywamy skończoną funkcję częściową $\Gamma : \mathrm{V} \to \mathrm{T}$ przeprowadzającą zbiór λ-zmiennych w zbiór typów prostych. Nadużywając notacji piszemy
  - $\Gamma = \{x_1 : \tau_1, \ldots, x_n : \tau_n\}$
  - $\mathrm{dom}(\Gamma) = \{x \in \mathrm{V} \mid \exists \tau. (x : \tau) \in \Gamma\}$
  - $\mathrm{rg}(\Gamma) = \{\tau \in \Phi_\to \mid \exists x. (x : \tau) \in \Gamma\}$
- Dla pseudotermu M następująco określamy zbiór *termów wolnych* FV:

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

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

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

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

  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 $M[x/y][y/x] = M$.*

- *α-konwersją* $=_\alpha$ nazywamy najmniejszą w sensie mnogościowym relację zwrotną i przechodnią 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 $ZM =_\alpha ZN$.

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

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

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

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

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

- *Sądem* (*asercją*) nazywamy każdą trójkę $(\Gamma,\ M,\ \sigma) \in \mathcal{P}(\mathrm{V} \times \mathrm{T}) \times \Lambda_\mathrm{T} \times \mathrm{T}$, 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 $\Gamma \cap \Delta = \varnothing$.
  - $\vdash \varphi$ zamiast $\varnothing \vdash \varphi$.

- Na zbiorze sądów wprowadzamy relacje określające reguły wyprowadzania termów

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

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

  Dowód sądu określamy analogicznie jak w logince $\mathrm{NJ}(\to)$.

  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 $M,\ N,\ Z \in \Lambda_\mathrm{T}$ spełnia następujące warunki

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

- *Kongruencją* nazywamy zgodną relację równowazności na Λ_T.

- *Redukcją* nazywamy zgodną, zwrotną i przechodnią relację na Λ_T.

- β-redukcją nazywamy najmniejsza w sensie mnogościowym *zgodną* relację „$\longrightarrow_\beta$” określoną zbiorze pseudotermów Λ_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 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 $x \notin \mathrm{FV}(M)$.

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

2.3 Normalizacja

- λ-term M ma własność *normalizacji* (co symbolicznie oznaczamy $M \in \mathrm{WN}_\beta$) wtw, gdy *istnieje* ciąg β-redukcji rozpoczynający się od M i kończący się termem w postaci normalnej N. 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 2. *Każdy λ-term w stylu Churcha ma postać normalną.*