Logika i teoria typów

Wykład 8

30 listopada 2022

Tydzień temu: silna normalizacja

Twierdzenie: *Rachunek lambda z typami prostymi ma własność silnej normalizacji: każdy poprawnie typowany term jest silnie $\beta\eta$-normalizowalny.*

Definicja: Określamy klasę termów $\mathcal{S}$ przez indukcję:

1. Jeśli $N_1, \ldots, N_k \in \mathcal{S}$, to $xN_1 \ldots N_k \in \mathcal{S}$;
2. Jeśli $N \in \mathcal{S}$, to $\lambda x\, N \in \mathcal{S}$;
3. Jeśli $Q \in \mathcal{S}$ oraz $P[x := Q]N_1 \ldots N_k \in \mathcal{S}$, to $(\lambda x\, P)QN_1 \ldots N_k \in \mathcal{S}$.

Lematy 1 i 2: $\mathcal{S} = \mathrm{SN}_{\beta\eta} = \mathrm{SN}_{\beta}$

Lemat 3

Już wiemy, że wystarczy udowodnić

Lemat 3: *Jeśli $M, P \in \mathcal{S}$, to $M[x := P] \in \mathcal{S}$.*

1. $N_1, \ldots, N_k \in \mathcal{S} \quad \Rightarrow \quad xN_1 \ldots N_k \in \mathcal{S}$;
2. $N \in \mathcal{S} \quad \Rightarrow \quad \lambda x\, N \in \mathcal{S}$;
3. $Q \in \mathcal{S},\quad P[x := Q]N_1 \ldots N_k \in \mathcal{S} \quad \Rightarrow \quad (\lambda x\, P)QN_1 \ldots N_k \in \mathcal{S}$.

Lemat 3: *Jeśli $M^\sigma, P^\tau \in \mathcal{S}$, to $M[x := P] \in \mathcal{S}$.*

Dowód: Indukcja ze względu na trzy parametry:

– pierwszy to długość typu τ termu P;
– drugi to maksymalna długość redukcji termu M,
– trzeci to długość termu M.

Przypadek 1: $M = \lambda z\, N$, gdzie $N \in \mathcal{S}$.
Wtedy $M[x := P] = \lambda z\, N[x := P] \in \mathcal{S}$, z założenia indukcyjnego dla N (pierwszy i drugi parametr bez zmian, trzeci mniejszy).

1. $N_1, \ldots, N_k \in \mathcal{S} \quad \Rightarrow \quad xN_1 \ldots N_k \in \mathcal{S}$;
2. $N \in \mathcal{S} \quad \Rightarrow \quad \lambda x\, N \in \mathcal{S}$;
3. $Q \in \mathcal{S},\quad P[x := Q]N_1 \ldots N_k \in \mathcal{S} \quad \Rightarrow \quad (\lambda x\, P)QN_1 \ldots N_k \in \mathcal{S}$.

Lemat 3: *Jeśli $M^\sigma, P^\tau \in \mathcal{S}$, to $M[x := P] \in \mathcal{S}$.*

Dowód: Indukcja ze względu na trzy parametry:

– pierwszy to długość typu τ termu P;
– drugi to maksymalna długość redukcji termu M,
– trzeci to długość termu M.

Przypadek 2: $M = yN_1 \ldots N_k$, gdzie $N_1, \ldots, N_k \in \mathcal{S}$.
Wtedy $M[x := P] = yN_1[x := P] \ldots N_k[x := P] \in \mathcal{S}$, z założenia indukcyjnego dla $N_1, \ldots, N_k$.

1. $N_1, \ldots, N_k \in \mathcal{S} \quad \Rightarrow \quad xN_1 \ldots N_k \in \mathcal{S}$;
2. $N \in \mathcal{S} \quad \Rightarrow \quad \lambda x\, N \in \mathcal{S}$;
3. $Q \in \mathcal{S},\quad P[x := Q]N_1 \ldots N_k \in \mathcal{S} \quad \Rightarrow \quad (\lambda x\, P)QN_1 \ldots N_k \in \mathcal{S}$.

Lemat 3: *Jeśli $M^\sigma, P^\tau \in \mathcal{S}$, to $M[x := P] \in \mathcal{S}$.*

Dowód: Indukcja ze względu na trzy parametry:

– pierwszy to długość typu τ termu P;
– drugi to maksymalna długość redukcji termu M,
– trzeci to długość termu M.

Przypadek 3: $M = x$.
Wtedy $M[x := P] = P \in \mathcal{S}$ z założenia.

1. $N_1, \ldots, N_k \in \mathcal{S} \quad \Rightarrow \quad xN_1 \ldots N_k \in \mathcal{S}$;
2. $N \in \mathcal{S} \quad \Rightarrow \quad \lambda x\, N \in \mathcal{S}$;
3. $Q \in \mathcal{S},\quad P[x := Q]N_1 \ldots N_k \in \mathcal{S} \quad \Rightarrow \quad (\lambda x\, P)QN_1 \ldots N_k \in \mathcal{S}$.

Lemat 3: *Jeśli $M^\sigma, P^\tau \in \mathcal{S}$, to $M[x := P] \in \mathcal{S}$.*

Dowód: Indukcja ze względu na trzy parametry:

– pierwszy to długość typu τ termu P;
– drugi to maksymalna długość redukcji termu M,
– trzeci to długość termu M.

Przypadek 4: $M = xQN_1 \ldots N_k$, gdzie $Q, N_1 \ldots N_k \in \mathcal{S}$.
Wtedy $M[x := P] = PQ[x{:=}P]N_1[x{:=}P] \ldots N_k[x{:=}P]$.
Z założenia indukcyjnego łatwo wynika
$Q[x := P], N_1[x := P], \ldots, N_k[x := P] \in \mathcal{S}$.

Wystarczy pokazać, że $M[x := P] \in \mathrm{SN}_\beta$.

Wiemy: $Q[x := P], N_1[x := P], \ldots, N_k[x := P] \in \mathcal{S}$.
Chcemy:
$M[x := P] = PQ[x{:=}P]N_1[x{:=}P] \ldots N_k[x{:=}P] \in \mathrm{SN}_\beta$.

Redukcje wewnętrzne muszą się zakończyć. Niech:

$M[x{:=}P] \twoheadrightarrow (\lambda y\, R)Q'N'_1 \ldots N'_k \to R[y{:=}Q']N'_1 \ldots N'_k \twoheadrightarrow \cdots$

gdzie $P \twoheadrightarrow \lambda y\, R : \tau$. No to $\tau = \tau_1 \to \tau_2$ oraz $Q' : \tau_1$.
Ale typ τ_1 jest krótszy niż τ, więc $R[y{:=}Q'] \in \mathcal{S}$.

Skoro $N_1, \ldots, N_k \in \mathrm{SN}$, to $zN'_1 \ldots N'_k \in \mathrm{SN} = \mathcal{S}$. Chytry trick:

$$R[y := Q']N'_1 \ldots N'_k = (zN'_1 \ldots N'_k)[z := R[y := Q']],$$

gdzie $z : \tau_2$, i znowu krótszy typ, więc całość jest w $\mathcal{S} = \mathrm{SN}$.

3. $Q \in \mathcal{S}$, $P[x := Q]N_1 \dots N_k \in \mathcal{S} \;\Rightarrow\; (\lambda x\, P)QN_1 \dots N_k \in \mathcal{S}$.

Lemat 3: *Jeśli $M^\sigma, P^\tau \in \mathcal{S}$, to $M[x := P] \in \mathcal{S}$.*

Dowód: Indukcja ze względu na trzy parametry:
1. długość typu τ; 2. długość redukcji M; 3. długość M.

Przypadek 5: $M = (\lambda z R)QN_1 \dots N_k$, gdzie $Q \in \mathcal{S}$ oraz $R[z := Q]N_1 \dots N_k \in \mathcal{S}$. Mamy wtedy

$$M[x{:=}P] = (\lambda z R[x{:=}P])Q[x{:=}P]N_1[x{:=}P] \dots N_k[x{:=}P]$$

i wystarczy pokazać, że $Q[x := P] \in \mathcal{S}$ (z zał. ind.), oraz, że

$$R[x{:=}P][z{:=}Q[x{:=}P]]N_1[x{:=}P] \dots N_k[x{:=}P] \in \mathcal{S}.$$

Inaczej, ma być $(R[z := Q]N_1 \dots N_k)[x := P] \in \mathcal{S}$.

Ale $M \twoheadrightarrow^+ R[z := Q]N_1 \dots N_k$, więc drugi parametr zmalał.

Przypadek ogólny

Twierdzenie: *Rozszerzony rachunek lambda ma własność silnej normalizacji ze względu na β-redukcje.*

Dowód: Redukujemy rozszerzony rachunek lambda do zwykłego (z jedną stałą typową).
Najpierw tłumaczymy typy:

$$\begin{aligned}
|\alpha| &= 0, \quad \text{gdy } \alpha = \bot, p, q, \dots \\
|\sigma \to \tau| &= |\sigma| \to |\tau| \\
|\sigma \wedge \tau| &= (|\sigma| \to |\tau| \to 0) \to 0 \\
|\sigma \vee \tau| &= (|\sigma| \to 0) \to (|\tau| \to 0) \to 0
\end{aligned}$$

Uwaga: zawsze $|\sigma| = \sigma_1 \to \dots \to \sigma_n \to 0$.

Translacja dla termów (1)

$$\begin{aligned}
|x^\sigma| &= x^{|\sigma|} \\
|\lambda x^\tau . M^\sigma| &= \lambda x^{|\tau|}.\, |M|^{|\sigma|} \\
|M^{\sigma \to \tau} N^\sigma| &= |M|^{|\sigma| \to |\tau|} |N|^{|\sigma|} \\
|\langle M, N \rangle^{\sigma \wedge \tau}| &= \lambda z^{|\sigma| \to |\tau| \to 0}.\, z|M|^{|\sigma|}|N|^{|\tau|} \\
|\mathrm{in}_1(A^\sigma)^{\sigma \vee \tau}| &= \lambda x^{|\sigma| \to 0}.\lambda y^{|\tau| \to 0}.\, x|A|^{|\sigma|} \\
|\mathrm{in}_2(B^\tau)^{\sigma \vee \tau}| &= \lambda x^{|\sigma| \to 0}.\lambda y^{|\tau| \to 0}.\, y|B|^{|\tau|}
\end{aligned}$$

Translacja dla termów (2)

$(|\sigma| = \sigma_1 \to \dots \to \sigma_n \to 0, \quad |\tau| = \tau_1 \to \dots \to \tau_m \to 0.)$

$$|\sigma \wedge \tau| = (|\sigma| \to |\tau| \to 0) \to 0$$

$$\begin{aligned}
|P^{\sigma \wedge \tau}\{1\}| &= \lambda x_1^{\sigma_1} \dots \lambda x_n^{\sigma_n}.\, |P|^{|\sigma \wedge \tau|}(\lambda x^{|\sigma|} \lambda y^{|\tau|}.\, (xx_1 \dots x_n)^0) \\
|P^{\sigma \wedge \tau}\{2\}| &= \lambda x_1^{\tau_1} \dots \lambda x_m^{\tau_m}.\, |P|^{|\sigma \wedge \tau|}(\lambda x^{|\sigma|} \lambda y^{|\tau|}\, (yx_1 \dots x_m)^0) \\
|M^\bot[\sigma]| &= \lambda x_1^{\sigma_1} \dots \lambda x_n^{\sigma_n}.|M|^0
\end{aligned}$$

Jak to działa?

$M = \langle P, Q \rangle\{1\} \to P$ tłumaczy się tak:

$$\begin{aligned}
|M| = {} & \lambda x_1^{\sigma_1} \dots \lambda x_n^{\sigma_n}.\, (\lambda z.\, z|P||Q|)(\lambda xy.\, xx_1 \dots x_n) \\
& \to_\beta \lambda x_1^{\sigma_1} \dots \lambda x_n^{\sigma_n}.\, (\lambda xy.\, xx_1 \dots x_n)|P||Q| \\
& \twoheadrightarrow_\beta \lambda x_1^{\sigma_1} \dots \lambda x_n^{\sigma_n}.\, |P|x_1 \dots x_n \\
& \twoheadrightarrow_\eta |P|
\end{aligned}$$

Translacja dla termów (3)

$$|M^{\sigma \vee \tau}[x^\sigma.\, P^\rho;\; y^\tau.\, Q^\rho]| =$$

$$\lambda x_1^{\rho_1} \dots \lambda x_k^{\rho_k}.|M|(\lambda x^{|\sigma|}.|P|^{|\rho|}x_1 \dots x_k)(\lambda y^{|\tau|}.|Q|^{|\rho|}x_1 \dots x_k),$$

gdzie $|M| : (|\sigma| \to 0) \to (|\tau| \to 0) \to 0$,

oraz $|\rho| = \rho_1 \to \dots \to \rho_k \to 0$.

Jak to działa?

$M = (\mathrm{in}_1\, P^\tau)[u^\tau.\, Q^\rho;\; v^\sigma.\, R^\rho] \;\to\; Q[u := P]$
tłumaczy się tak:

$$\begin{aligned}
|M| &= \lambda \vec{x}.\, |\mathrm{in}_1\, P|(\lambda u.\, |Q|\, \vec{x})(\lambda v.\, |R|\, \vec{x}) \\
&= \lambda \vec{x}.\, (\lambda xy.\, x|P|)(\lambda u.\, |Q|\, \vec{x})(\lambda v.\, |R|\, \vec{x}) \\
&\twoheadrightarrow \lambda \vec{x}.\, (\lambda u.\, |Q|\, \vec{x})|P| \\
&\twoheadrightarrow \lambda \vec{x}.\, |Q|[u := |P|]\vec{x} \\
&= \lambda \vec{x}.\, |Q[u := P]|\vec{x} \\
&\twoheadrightarrow_\eta |Q[u := P]|
\end{aligned}$$

Własności translacji

Lemat:
- $|M[x := N]| = |M|[x := |N|]$.
- Jeśli $M : \sigma$, to $|M| : |\sigma|$.
- Jeśli $M \to_\beta M'$, to $|M| \twoheadrightarrow^+_{\beta\eta} |M'|$.

Twierdzenie: *Rozszerzony rachunek lambda ma własność silnej normalizacji ze względu na β-redukcje.*

Dowód: Przypuśćmy, że $M_0^\tau \to M_1^\tau \to M_2^\tau \to \cdots$

Wtedy także $|M_0| \twoheadrightarrow^+_{\beta\eta} |M_1| \twoheadrightarrow^+_{\beta\eta} |M_2| \twoheadrightarrow^+_{\beta\eta} \cdots$

Silna normalizacja

Twierdzenie: *Rozszerzony rachunek lambda ma własność silnej normalizacji ze względu na β-redukcje.*

I co z tego?

Już wiemy, że beta-redukcja to za mało: term w postaci beta-normalnej może np. wyglądać tak:

$$(\mathsf{case}\ N^{\tau\vee\sigma}\ \mathsf{of}\ [x^\tau]P^{\alpha\to\beta}, [y^\sigma]Q^{\alpha\to\beta})M^\alpha$$

Permutacje

Potrzebujemy SN dla systemu z permutacjami.

$$M^{\sigma\vee\tau}[x^\sigma.P^\rho, y^\tau.Q^\rho]E \ \Rightarrow\ M^{\sigma\vee\tau}[x^\sigma.P^\rho E, y^\tau.Q^\rho E]$$

$$(M^\perp[\sigma]E)^\mu \ \Rightarrow\ M^\perp[\mu]$$

Zła wiadomość

Translacja używana dla beta-redukcji nie działa dla permutacji.

(To nie jest wcale takie proste.)

Przykład: $M \to M'$, ale $|M| \twoheadrightarrow^+_{\beta\eta} |M|'$.

$|\sigma| = \vec{\sigma} \to 0 \qquad |\perp| = 0$

$|\alpha\vee\beta| = (|\alpha| \to 0) \to (|\beta| \to 0) \to 0$

$M = N^{\alpha\vee\beta}[x^\alpha.\, P^\perp;\ y^\beta.\, Q^\perp]\,[\sigma]$

$|M| = \lambda\vec{z} : \vec{\sigma}.\, |N|(\lambda x.\, |P|)(\lambda y.\, |Q|)$

$M' = N^{\alpha\vee\beta}[x^\alpha.\, P^\perp[\sigma];\ y^\beta.\, Q^\perp[\sigma]]$

$|M'| = \lambda\vec{z} : \vec{\sigma}.\, |N|\,(\lambda x.\, |P^\perp[\sigma]|\,\vec{z})\,(\lambda y.\, |Q^\perp[\sigma]|\,\vec{z})$

$\quad = \lambda\vec{z} : \vec{\sigma}.\, |N|(\lambda x\, (\lambda\vec{z}.\, |P|)\,\vec{z})(\lambda y\, (\lambda\vec{z}.|Q|)\,\vec{z})$

Permutacje

Potrzebujemy SN dla systemu z permutacjami.

$$M^{\sigma\vee\tau}[x^\sigma.P^\rho, y^\tau.Q^\rho]E \ \Rightarrow\ M^{\sigma\vee\tau}[x^\sigma.P^\rho E, y^\tau.Q^\rho E]$$

$$(M^\perp[\sigma]E)^\mu \ \Rightarrow\ M^\perp[\mu]$$

Użyjemy metody CPS ("continuation passing style")

Semantyka kontynuacyjna

Znaczenie wyrażenia = jego wpływ na „cały program".

0 – typ „całego programu" (typ efektu).

$k : \mathsf{int} \to 0$ – „kontynuacja typu int"

Znaczenie wyrażenia $N : \mathsf{int}$, to funkcja $\underline{N} : (\mathsf{int} \to 0) \to 0$.

Na przykład $\underline{5} = \lambda k^{\mathsf{int}\to 0}.\, k(5)$.

Ogólniej, dla : $N : \mathsf{int}$,

$\underline{N} = \lambda k^{\mathsf{int}\to 0}.\, N \rhd k$, gdzie $N \rhd k$ to „N przekazane do k".

Kontynuacje dla funkcji (CBN)

typ termu	sposób użycia	typ kontynuacji	semantyka
τ	$\tau^\bullet$	$\tau^\bullet \to 0$	$\underline{\tau} = (\tau^\bullet \to 0) \to 0$
p	p	$p \to 0$	$(p \to 0) \to 0$
$\perp$	0	$0 \to 0$	$(0 \to 0) \to 0$
$\tau \to \sigma$	$\underline{\tau} \to \underline{\sigma}$	$(\underline{\tau} \to \underline{\sigma}) \to 0$	$((\underline{\tau} \to \underline{\sigma}) \to 0) \to 0$

Kontynuacje dla koniunkcji i alternatywy

Naturalny „sposób użycia":

$(\tau\wedge\sigma)^\bullet = (\underline{\tau}\wedge\underline{\sigma})$

$(\tau\vee\sigma)^\bullet = (\underline{\tau}\vee\underline{\sigma})$

Funkcyjny „sposób użycia":

$(\tau\wedge\sigma)^\bullet = (\underline{\tau} \to \underline{\sigma} \to 0) \to 0$

$(\tau\vee\sigma)^\bullet = (\underline{\tau} \to 0) \to (\underline{\sigma} \to 0) \to 0$

Translacja dla typów: $\underline{\tau} = (\tau^\bullet \to 0) \to 0$

$$
\begin{aligned}
p^\bullet &= p \\
\bot^\bullet &= 0 \\
(\tau \to \sigma)^\bullet &= (\underline{\tau} \to \underline{\sigma}) \\
(\tau \wedge \sigma)^\bullet &= (\underline{\tau} \to \underline{\sigma} \to 0) \to 0 \\
(\tau \vee \sigma)^\bullet &= (\underline{\tau} \to 0) \to (\underline{\sigma} \to 0) \to 0
\end{aligned}
$$

Translacja dla termów: czego chcemy?

Dla dowolnego termu M chcielibyśmy zdefiniować $\underline{M}$, tak aby:

- *Jeśli* $\Gamma \vdash M : \tau$, *to* $\underline{\Gamma} \vdash \underline{M} : \underline{\tau}$, *gdzie* $\underline{\Gamma}(x) = \underline{\Gamma(x)}$.
- *Jeśli* $M \to M'$, *to najlepiej* $\underline{M} \to^+ \underline{M'}$ ...
- *A jak się nie da, to chociaż* $\underline{M} = \underline{M'}$.

I to się prawie da zrobić.

Translacja dla typów: $\underline{\tau} = (\tau^\bullet \to 0) \to 0$
Translacja dla termów: $\underline{M} = \lambda k^{\tau^\bullet \to 0}.\, M \rhd k$

$$
\begin{aligned}
x^\tau \rhd K &= x^{\underline{\tau}}(K) \\
(\lambda x^\sigma.\, M^\mu) \rhd K &= K(\lambda x^{\underline{\sigma}}.\, \underline{M}^{\underline{\mu}}) \\
\langle M^\sigma, N^\mu \rangle \rhd K &= K(\lambda z^{\underline{\mu} \to \underline{\sigma} \to 0}.\, z \underline{M}\, \underline{N}) \\
\mathrm{in}_1(M) \rhd K &= K(\lambda y^{\underline{\mu} \to 0} z^{\underline{\sigma} \to 0}.\, y \underline{M}) \\
(M^\rho E)^\tau \rhd K &= M \rhd (E@K)
\end{aligned}
$$

$E@K : \rho^\bullet \to 0$ to eliminator E włączony do kontynuacji K.

Dołączanie eliminatora do kontynuacji $K : \tau^\bullet \to 0$

Ma być tak:

$(M^\rho E)^\tau \rhd K = M \rhd (E@K)$

Przypadek aplikacji: $\rho = \sigma \to \tau$.

$(M^{\sigma \to \tau} N^\sigma)^\tau \rhd K = M \rhd (N@K)$

$N^\sigma @K = \lambda m^{\underline{\sigma} \to \underline{\tau}}.\, m\underline{N}K : (\sigma \to \tau)^\bullet \to 0$

Tutaj $K : \tau^\bullet \to 0$ jest kontynuacją dla $MN : \tau$.

$N@K : (\underline{\sigma} \to \underline{\tau}) \to 0$ jest kontynuacją dla $M : \sigma \to \tau$.

Dołączanie eliminatora do kontynuacji $K : \tau^\bullet \to 0$

$$
\begin{aligned}
N@K &= \lambda m^{\underline{\sigma} \to \underline{\tau}}.\, m\underline{N}K : (\tau \to \sigma)^\bullet \to 0 \\
\{2\}@K &= \lambda m^{(\underline{\tau} \to \underline{\sigma} \to 0) \to 0}.\, m(\lambda x^{\underline{\tau}} y^{\underline{\sigma}}.\, yK) : (\tau \wedge \sigma)^\bullet \to 0 \\
[x^\mu.S^\tau, y^\rho.T^\tau]@K &= \lambda m^{(\mu \vee \rho)^\bullet}.\, m(\lambda x^{\underline{\mu}}.\, S \rhd K)(\lambda y^{\underline{\rho}}.\, T \rhd K) \\
[\rho]@K &= (\lambda k m^0.\, m)K : 0 \to 0
\end{aligned}
$$

Przypomnienie:
$(\mu \vee \rho)^\bullet = (\underline{\mu} \to 0) \to (\underline{\rho} \to 0) \to 0$
$(\tau \wedge \sigma)^\bullet = (\underline{\tau} \to \underline{\sigma} \to 0) \to 0$

Własności translacji

- *Jeśli* $\Gamma \vdash M : \tau$, *to* $\underline{\Gamma} \vdash \underline{M} : \underline{\tau}$, *gdzie* $\underline{\Gamma}(x) = \underline{\Gamma(x)}$.
- $(M \rhd K)[x^{\underline{\sigma}} := \underline{N}] \twoheadrightarrow_\beta M[x^\sigma := N] \rhd K[x^{\underline{\sigma}} := \underline{N}]$.
- *Jeśli* $M \to_\beta M'$, *to* $\underline{M} \twoheadrightarrow_\beta^+ \underline{M'}$.
- *Niech* $\to_\pi$ *oznacza permutacje postaci*
  $N[x.S, y.T]E \to_\pi N[x.SE, y.TE]$.
  Jeśli $M \to_\pi M'$, *to* $\underline{M} = \underline{M'}$.

Jeśli $M \to_\beta M'$, to $\underline{M} \twoheadrightarrow_\beta^+ \underline{M'}$. Na przykład:

$$
\begin{aligned}
\underline{\langle P, Q \rangle \{1\}} &= \lambda k.\, \langle P, Q \rangle \{1\} \rhd k \\
&= \lambda k.\, \langle P, Q \rangle \rhd \{1\}@k \\
&= \lambda k.\, \langle P, Q \rangle \rhd (\lambda m.\, m(\lambda xy.xk)) \\
&= \lambda k.\, (\lambda m.\, m(\lambda xy.xk))(\lambda z.\, z\underline{P}\underline{Q}) \\
&\to_\beta \lambda k.\, (\lambda z.\, z\underline{P}\underline{Q})(\lambda xy.xk) \\
&\to_\beta \lambda k.\, (\lambda xy.xk)\underline{P}\underline{Q} \\
&\twoheadrightarrow_\beta^+ \lambda k.\, \underline{P}k = \lambda k.\, (\lambda k.\, P \rhd k)k \\
&\to_\beta \lambda k.\, P \rhd k = \underline{P}
\end{aligned}
$$

Jeśli $M \to_\pi M'$, to $\underline{M} = \underline{M'}$.

$$
\begin{aligned}
\underline{M[x.S, y.T]E} &= \lambda k.\, M[x.S, y.T]E \rhd k \\
&= \lambda k.\, M[x.S, y.T] \rhd E@k \\
&= \lambda k.\, M \rhd [x.S, y.T]@E@k \\
&= \lambda k.\, M \rhd (\lambda m.\, m(\lambda x.\, S \rhd E@k)(\lambda y.\, T \rhd E@k)) \\
&= \lambda k.\, M \rhd (\lambda m.\, m(\lambda x.\, SE \rhd k)(\lambda y.\, TE \rhd k)) \\
&= \lambda k.\, M \rhd [x.SE, y.TE]@k \\
&= \lambda k.\, M[x.SE, y.TE] \rhd k = \underline{M[x.SE, y.TE]}
\end{aligned}
$$

Zła wiadomość

Translacja nie zachowuje permutacji postaci

$$M[\sigma]E^{\rho} \to_{\perp} M[\rho].$$

Bo tak: $\underline{x^{\perp}[\sigma]E^{\rho}} = \lambda k.\, x^{\perp}[\sigma]E^{\rho} \triangleright k$,

$= \lambda k.\, x^{\perp} \triangleright [\sigma]@E^{\rho}@k = \lambda k.\, x^{\underline{0}}((\lambda lm.m)(E^{\rho}@k))$.

oraz $\underline{x^{\perp}[\rho]} = \lambda k.\, x^{\perp}[\rho] \triangleright k = \lambda k.\, x^{\underline{0}}((\lambda lm.m)k)$

Zagadka

Translacja nie zachowuje permutacji postaci

$$M[\sigma]E^{\rho} \to_{\perp} M[\rho].$$

Ale ten problem znika jeśli zamienić definicję

$[\sigma]@K = (\lambda k m^0.\, m)K : 0 \to 0$

na prostszą:

$[\sigma]@K = \lambda m^0.\, m$

To czemu tak nie robimy?

Zła wiadomość

Translacja nie zachowuje permutacji postaci

$$M[\sigma]E^{\rho} \to_{\perp} M[\rho].$$

Rozwiązanie: Odkładanie ex falso.

Jeśli $M \twoheadrightarrow_{\perp} N \to_{\beta\pi} P$, *to* $M \to_{\beta\pi} Q \twoheadrightarrow_{\beta\pi\perp} P$, *dla pewnego* Q.

Morał: Jeśli istnieje redukcja

$$M_1 \to M_2 \to M_3 \to \cdots$$

w której kroki $\to_{\beta\pi}$ występują nieskończenie wiele razy, to istnieje nieskończona $\beta\pi$-redukcja.

Silna normalizacja

Wystarczy udowodnić, że nie istnieje nieskończona $\beta\pi$-redukcja ani nieskończona $\perp$-redukcja.

Lemat: *Nie istnieje nieskończona redukcja z samych permutacji (czyli $\perp\pi$-redukcja).*

Dowód: Permutacje przesuwają eliminatory w głąb termu, z grubsza tak: $NE_1E_2 \to NE_1^{E_2}$. Można zdefiniować „miarę termu”, której wartość zmniejsza się po każdej permutacji. Np. jeśli $|NE| = |N|^2|E|$, to

$$|NE_1E_2| = (|N|^2|E_1|)^2|E_2| > |N|^2|E_1^{E_2}| = |NE_1^{E_2}|$$

Silna normalizacja

Przypuśćmy, że w rozszerzonym rachunku lambda:

$$M_1 \to_{\pi\beta} M_2 \to_{\pi\beta} M_3 \to_{\pi\beta} M_4 \to_{\pi\beta} \cdots$$

Wtedy w zwykłym rachunku lambda:

$$\underline{M_1} \rightsquigarrow \underline{M_2} \rightsquigarrow \underline{M_3} \rightsquigarrow \underline{M_4} \rightsquigarrow \cdots$$

gdzie każde $\rightsquigarrow$, to albo $\twoheadrightarrow_{\beta}^{+}$, albo $=$.
Równośc zachodzi w przypadku permutacji.

Jeśli w górnej redukcji jest nieskończenie wiele β-kroków, to w dolnej też. Niemożliwe, bo SN_{β}.

Zatem w górnej redukcji są prawie same permutacje.
Też niemożliwe, bo lemat.

Morał:

Twierdzenie (Philippe de Groote)

Rozszerzony rachunek lambda z permutacjami ma własność silnej normalizacji.

Wniosek: *Każdy dowód można zredukować do normalnego.*

Sens logiczny translacji CPS?

$$\underline{\tau} = (\tau^{\bullet} \to 0) \to 0$$

$$\begin{array}{rcl}
p^{\bullet} & = & p \\
\perp^{\bullet} & = & 0 \\
(\tau \to \sigma)^{\bullet} & = & (\underline{\tau} \to \underline{\sigma}) \\
(\tau \wedge \sigma)^{\bullet} & = & (\underline{\tau} \to \underline{\sigma} \to 0) \to 0 \\
(\tau \vee \sigma)^{\bullet} & = & (\underline{\tau} \to 0) \to (\underline{\sigma} \to 0) \to 0
\end{array}$$

Sens logiczny translacji CPS?

$$\underline{\tau} = (\tau^{\bullet} \to 0) \to 0$$

Twierdzenie: *Jeśli* $\Gamma \vdash M : \tau$, *to* $\underline{\Gamma} \vdash \underline{M} : \underline{\tau}$.

W szczególności, jeśli τ *jest twierdzeniem, to* $\underline{\tau}$ *też.*

A na odwrót? **Nie!**

Przykład: $\vdash \underline{p \vee (p \to q)}$, $\quad \nvdash p \vee (p \to q)$

Oznaczenie: $\sim\alpha = \alpha \to 0$.
Podobieństwo do $\neg\alpha = \alpha \to \bot$ jest zamierzone.

Liczymy:

$\underline{p \vee (p \to q)} = \sim\sim(\sim\underline{p} \to \sim(\underline{p \to q}) \to 0)$.

$\sim\underline{p} = \sim\sim\sim p, \qquad \underline{p \to q} = \sim\sim p \to \sim\sim q$.

Zatem $\underline{p \vee (p \to q)}$ jest równoważne formule:

$$\sim\sim(\sim p \to \sim(\sim\sim p \to \sim\sim q) \to 0).$$

$\vdash \sim\sim(\sim p \to \sim(\sim\sim p \to \sim\sim q) \to 0)$

Założenie $x : \sim(\sim p \to \sim(\sim\sim p \to \sim\sim q) \to 0)$, cel 0.

Cel: $\sim p \to \sim(\sim\sim p \to \sim\sim q) \to 0$, czyli:

założenia $y : \sim p$, $z : \sim(\sim\sim p \to \sim\sim q)$, cel 0.

Cel: $\sim\sim p \to \sim\sim q$, czyli:

założenia $u : \sim\sim p$, $v : \sim q$, cel 0.

Wystarczy uy.

Cały term: $\lambda x.\, x(\lambda yz.\, z(\lambda uv.\, uy))$.

Jeszcze jeden przykład

Translacją formuły $((p \to q) \to p) \to p$
jest intuicjonistyczne twierdzenie:

$\sim\sim(\sim\sim(\sim\sim(\sim\sim p \to \sim\sim q) \to \sim\sim p) \to \sim\sim p)$

Chyba odkryliśmy jakąś nową logikę?

Klasyczną.

Nienaturalna dedukcja

Reguły wnioskowania jak zwykle, i do tego:

$$\frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ (\text{Cheat})$$

Translacja Kołmogorowa

$$\begin{aligned} k(p) &= \neg\neg p \\ k(\bot) &= \bot \\ k(\tau \to \sigma) &= \neg\neg(k(\tau) \to k(\sigma)) \end{aligned}$$

Analogicznie:

$$k(\tau \diamond \sigma) = \neg\neg(k(\tau) \diamond k(\sigma))$$

Note: $\neg\neg k(\alpha)$ is equivalent to $k(\alpha)$.

Dygresja (ćwiczenie)

- $\neg(p \to q \to \bot) \leftrightarrow \neg\neg(p \wedge q)$;
- $(\neg p \to \neg q \to \bot) \leftrightarrow \neg\neg(p \vee q)$.

Wniosek: można równie dobrze zdefiniować $k(\tau) = \underline{\tau}$.

Translacja Kołmogorowa

Twierdzenie:

$$\Gamma \vdash_{klas} \alpha \quad \Leftrightarrow \quad k(\Gamma) \vdash_{int} k(\alpha).$$

Dowód:

($\Rightarrow$) Indukcja ze względu na dowód.

($\Leftarrow$) Formuły α i $k(\alpha)$ są klasycznie równoważne.

Morał: Logika klasyczna redukuje się w pamięci logarytmicznej do logiki intuicjonistycznej (jest „łatwiejsza").

Uwaga: To działa nie tylko dla rachunku zdań.

Translacja Kołmogorowa

Twierdzenie: *Jeśli $\Gamma \vdash_{klas} \alpha$, to $k(\Gamma) \vdash_{int} k(\alpha)$.*

Dowód: Indukcja ze względu na dowód. Przykładowy przypadek: reguła wnioskowania przez zaprzeczenie.

$$\frac{\Gamma, \neg\alpha \vdash \bot}{\Gamma \vdash \alpha}$$

Z założenia indukcyjnego wynika $k(\Gamma), k(\neg\alpha) \vdash_{int} k(\bot)$.

Ale $k(\neg\alpha) = \neg\neg(k(\alpha) \to \bot) = \neg\neg\neg k(\alpha)$,

czyli w istocie $k(\Gamma), \neg k(\alpha) \vdash_{int} \bot$.

Albo lepiej: $k(\Gamma) \vdash_{int} \neg\neg k(\alpha)$.

Stąd $k(\Gamma) \vdash_{int} k(\alpha)$.

Translacja Kołmogorowa

Twierdzenie: *Jeśli* $\Gamma \vdash_{klas} \alpha$, *to* $k(\Gamma) \vdash_{int} k(\alpha)$.

Dowód: Indukcja ze względu na dowód.
Przykładowy przypadek: *modus ponens*.

$$\frac{\Gamma \vdash \alpha \to \beta \qquad \Gamma \vdash \alpha}{\Gamma \vdash \beta}$$

Z założenia indukcyjnego wynika

$k(\Gamma) \vdash_{int} \neg\neg(k(\alpha) \to k(\beta))$ i $k(\Gamma) \vdash_{int} k(\alpha)$.

Ponieważ $k(\beta)$ zaczyna się od $\neg$, więc wystarczy sprawdzić, że

$$\vdash \neg\neg(p \to \neg q) \to p \to \neg q.$$

Dygresja

Z punktu widzenia negatywnego celu, założenie postaci $\neg\neg\alpha$ jest równie dobre jak założenie α:

$\ldots, \neg\neg\alpha, \ldots \;\vdash\; \neg\beta?$

$\ldots, \neg\neg\alpha, \ldots, \beta \;\vdash\; \bot?$

$\ldots, \neg\neg\alpha, \ldots, \beta \;\vdash\; \neg\alpha?$

$\ldots, \neg\neg\alpha, \ldots, \beta, \alpha \;\vdash\; \bot?$

Translacja Kołmogorowa

Twierdzenie: *Jeśli* $\Gamma \vdash_{klas} \alpha$, *to* $k(\Gamma) \vdash_{int} k(\alpha)$.

Dowód: Indukcja ze względu na dowód.
Przykładowy przypadek: *ex falso*.

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash \beta}$$

Z założenia indukcyjnego wynika $k(\Gamma) \vdash_{int} \bot$.

Ponieważ $k(\beta)$ zaczyna się od $\neg$, więc wystarczy wiedzieć, że

$$\vdash \bot \to p \to \bot.$$

Ważne: Nie korzystamy z *ex falso*.

Translacja Kołmogorowa

Twierdzenie:

$$\Gamma \vdash_{klas} \alpha \qquad \Leftrightarrow \qquad k(\Gamma) \vdash_{min} k(\alpha),$$

gdzie $\vdash_{min}$ oznacza wnioskowanie w *logice minimalnej*,
tj. bez reguły *ex falso*. Zamiast $\bot$ może być cokolwiek.

O wyższości Kołmogorowa nad Gliwienką

Twierdzenie Gliwienki: *Formuła* φ *jest klasyczną tautologią wtedy i tylko wtedy, gdy* $\vdash_{int} \neg\neg\varphi$

- Tu potrzebne jest *ex falso*.
- To nieprawda np. dla logiki 1 rzędu.

Rachunek lambda?

Czy dla logiki klasycznej można zdefiniować rachunek lambda?

1. Notacja dla dowodów – to łatwe: trzeba tylko wymyślić składnię dla reguły (Cheat).
2. Ale czy to ma sens obliczeniowy?
3. A jak wyglądają klasyczne reguły gry?

Bajka Selingera

The evil king calls the poor shepherd and gives him these orders: *"You must bring me the philosopher's stone, or you have to find a way to turn the philosopher's stone into gold. If you don't, your head will be taken off tomorrow!"*
What can the poor shepherd do to save his life?

Bajka Selingera: ciąg dalszy

The next day the poor shepherd brings to the king's palace a huge machine. The machine has two openings.
One is marked *"Put the philosopher's stone here!"*
and the other *"The gold will fall out from here"*.

That will perfectly work as long as the king cannot put the philosopher's stone into the machine.

But what if, somehow, the king comes into the possession of the philosopher's stone?

Then the shepherd's brother, hidden inside the machine, will grab the stone, and hand it discretely to the shepherd. The shepherd now can say: *"Oops, Your Majesty, I've been mistaken. Here is the philosopher's stone!"*.