Logika i teoria typów

Wykład 5

16 listopada 2021

Tydzień temu

Twierdzenie:

Intuicjonistyczny rachunek zdań jest PSPACE-zupełny.

Dowód: Redukcja problemu stopu dla automatów monotonicznych. Konfiguracja: $\Gamma \vdash q$.

- Cel atomowy q to stan maszyny;
- Otoczenie Γ to zawartość pamięci, w tym program.
- Założenie $p \to q$ umożliwia zmianę stanu z q na p.
- Założenie $(b \to p) \to q$ umożliwia zmianę stanu z q na p, z jednoczesnym zapisaniem b w pamięci.
- Założenie $a \to p \to q$ umożliwia zmianę stanu z q na p, pod warunkiem, że w pamięci jest zapisane a.
- Założenie $r \to p \to q$ umożliwia rozgałęzienie uniwersalne na stan p i stan r.

Rzędy

Rząd zero = atomy;
Rząd $n+1$ = formuły $\alpha_1 \to \cdots \alpha_k \to p$,
gdzie α_i są rzędu co najwyżej n.

Np. ta formuła jest rzędu 3:

$((p \to q) \to r) \to ((r \to p \to s) \to r) \to p$

Automaty monotoniczne są reprezentowane formułami rzędu 3.

Twierdzenie:

Intuicjonistyczny rachunek zdań jest PSPACE-zupełny.

To mało powiedziane.

W istocie PSPACE-zupełny jest fragment implikacyjny i to ograniczony do formuł rzędu 3.

Twierdzenie

Intuicjonistyczny rachunek zdań redukuje się w pamięci logarytmicznej do fragmentu implikacyjnego rzędu 3.

Dowód:

Dowolna formuła $\to$ automat $\to$ formuła implikacyjna rzędu 3.

Przykład:

Formuła $(((e \to d) \to c) \to b) \to a$ jest rzędu 4

i nie jest *równoważna* żadnej formule rzędu 3.

O wyższości Wajsberga i Ben-Yellesa nad Davisem i Putnamem

Klasyczny rachunek zdań:

– reprezentuje problemy obliczeniowe o złozoności NP;

– jako koniunkcje statycznych więzów (SAT);

– dla których trzeba szukać rozwiązań ad hoc.

Intuicjonistyczny rachunek zdań:

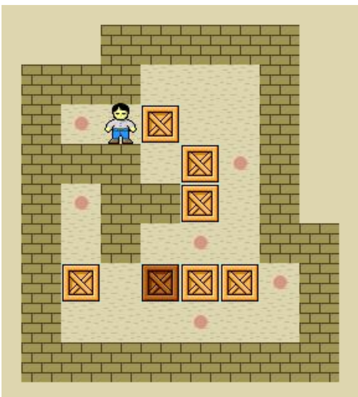
– reprezentuje problemy obliczeniowe o złożoności PSPACE;

– jako dynamiczne zadania dowodowe,

– których rozwiązania bezpośrednio realizują obliczenie.

Przykład

Do tego zadania SAT-solvery się nie nadają.



Silna normalizacja

Twierdzenie: *Jeśli istnieje dowód osądu $\Gamma \vdash \varphi$, to istnieje dowód normalny.*

Lepsze twierdzenie: *Każdy dowód osądu $\Gamma \vdash \varphi$ można przekształcić w dowód normalny.*

Przypadek implikacyjny

Term w postaci β-normalnej: term, którego nie można redukować.

To jest to samo co implikacyjny dowód normalny.

Normalizacja:
Jeśli $\Gamma \vdash M : \tau$, to $M \twoheadrightarrow_\beta N$, gdzie N jest normalny.

Silna normalizacja:
Jeśli $\Gamma \vdash M : \tau$, to każdy ciąg redukcji termu M jest skończony.

Silna normalizacja

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

Wstęp do dowodu

Konwencja:

- termy (w tym zmienne) mają ustalone typy;
- nie piszemy tych typów.

Lemat 0: *(1) Podterm termu silnie normalizowalnego jest silnie normalizowalny.*

(2) Jeśli $A[x := B] \in SN$, to $A \in SN$.

(3) Jeśli $A \in SN$ i $A \to B$, to $B \in SN$.

Wstęp do dowodu

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 $(\lambda x\, P)QN_1 \ldots N_k \in \mathcal{S}$.

Lemat 1: Jeśli $M \in \mathcal{S}$, to $M \in \mathrm{SN}_{\beta\eta}$.

Dowód: Indukcja ze względu na definicję $M \in \mathcal{S}$.

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 2: Jeśli $M \in \mathrm{SN}_\beta$, to $M \in \mathcal{S}$.

Dowód: Indukcja ze względu na dwa parametry:

– pierwszy to maksymalna długość redukcji termu M,
– drugi to długość termu M.

Główny lemat

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

Dowód twierdzenia: Z lematów 1 i 2 wynika, że $\mathrm{SN}_\beta = \mathrm{SN}_{\beta\eta} = \mathcal{S}$. Wystarczy więc udowodnić, że każdy (poprawny) term M jest w $\mathcal{S}$.

– Jeśli M jest zmienną, to oczywiste.

– Jeśli M jest abstrakcją, to teza wynika z założenia indukcyjnego.

– Jeśli M jest aplikacją PQ to stosujemy lemat 3 do podstawienia $(xQ)[x := P]$.

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.

Opuszczamy łatwe przypadki.

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:
$M[x := P] = PQ[x{:=}P]N_1[x{:=}P] \ldots N_k[x{:=}P] \in \mathrm{SN}$.

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 $\mathcal{S} = \mathrm{SN}$.

Translacja dla termów (1)

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

O co tu chodzi?

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

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

O co tu chodzi?

$M = \mathbf{case}\ \mathbf{in}_1\, P^\tau\ \mathbf{of}\ [u^\tau]Q^\rho, [v^\sigma]R^\rho \ \to\ Q[u := P]$
tłumaczy się tak:

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

Silna normalizacja

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:

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

Uwaga: zawsze $|\sigma| = \sigma_1 \to \cdots \to \sigma_n \to \mathbf{0}$.

Translacja dla termów (2)

$(|\sigma| = \sigma_1 \to \cdots \to \sigma_n \to \mathbf{0}, \quad |\tau| = \tau_1 \to \cdots \to \tau_m \to \mathbf{0}.)$

$$|\sigma \wedge \tau| = (|\sigma| \to |\tau| \to \mathbf{0}) \to \mathbf{0}$$

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

Translacja dla termów (3)

$$|\mathrm{case}\ M^{\sigma\vee\tau}\ \mathrm{of}\ [x^\sigma]P^\rho\ \mathrm{or}\ [y^\tau]Q^\rho| =$$

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

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

oraz $|\rho| = \rho_1 \to \cdots \to \rho_k \to \mathbf{0}$.

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 $\quad M_0^\tau \to M_1^\tau \to M_2^\tau \to \cdots$

Wtedy także $\quad |M_0| \twoheadrightarrow_{\beta\eta}^{+} |M_1| \twoheadrightarrow_{\beta\eta}^{+} |M_2| \twoheadrightarrow_{\beta\eta}^{+} \cdots$

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:

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

Potrzebne są dodatkowe redukcje porządkujące (*permutacje*).

Uproszczona składnia

Zamiast $\mathbf{case}\ M\ \mathbf{of}\ [x]P\ \mathrm{or}\ [y]Q$ piszemy $M[x.P, y.Q]$.

Zamiast $\varepsilon_\sigma(M)$ piszemy $M[\sigma]$.

Wada: mniej intuicyjne.

Zaleta: wszystkie eliminacje pisane jednolicie na końcu:

$$MN, \quad M\{i\}, \quad M[x.P, y.Q], \quad M[\sigma].$$

Permutacje

Kłopotliwa sytuacja:
Brzydka eliminacja, a potem znowu eliminacja, czyli

$$M^{\sigma\vee\tau}[x^\sigma.P^\rho, y^\tau.Q^\rho]E \qquad \text{i} \qquad M^\perp[\sigma]E$$

Eliminator E nie ma dostępu do termu „właściwego'' typu.

Nie ma własności podformuł,

np. $M^{\sigma\vee\tau}[x^\sigma.P^{\alpha\to\beta}, y^\tau.Q^{\alpha\to\beta}]N^\alpha : \beta$

Permutacje:

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

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

Zła wiadomość

Translacja używana dla beta-redukcji nie działa dla permutacji.

(To nie jest wcale takie proste.)

Użyjemy metody CPS („continuation passing style'')

Semantyka kontynuacyjna

Znaczenie wyrażenia = jego wpływ na „cały program''.

$\mathbf{0}$ – typ „całego programu'' (typ efektu).

$k : \mathrm{int} \to \mathbf{0}$ – „kontynuacja typu int''

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

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

Ogólniej, dla $: N : \mathrm{int}$,

$\underline{N} = \lambda k^{\mathrm{int}\to\mathbf{0}}.\, N \triangleright k$, gdzie $N \triangleright k$ to „N przekazane do k''.

Kontynuacje dla funkcji (CBN)

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

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'':

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

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

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

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

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 termów: $\underline{M} = \lambda k^{\tau^\bullet \to \mathbf{0}}.\, M \rhd k$

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

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

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

Ma być tak:

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

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

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

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

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

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

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

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

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

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:

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

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

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

Zła wiadomość

Translacja nie zachowuje permutacji postaci

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

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

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

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

Zagadka

Translacja nie zachowuje permutacji postaci

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

Ale ten problem znika jeśli zamienić definicję

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

na prostszą:

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

To czemu tak nie robimy?

Zła wiadomość

Translacja nie zachowuje permutacji postaci

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

Rozwiązanie: Odkładanie epsilona.

Jeśli $M \twoheadrightarrow_{\perp} N \to_{\beta\pi} P$*, to* $M \to_{\beta\pi} Q \twoheadrightarrow_{\perp} P$*, 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 $=$.
Równość 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?

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

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

Sens logiczny translacji CPS?

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

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

Oznaczenie: $\sim\alpha = \alpha \to \mathbf{0}$.
Podobieństwo do $\neg\alpha = \alpha \to \perp$ jest zamierzone.

Liczymy:

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

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

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

$$\sim\sim(\sim p \to \sim(\sim\sim p \to \sim\sim q) \to \mathbf{0}).$$

$\vdash \sim\sim(\sim p \to \sim(\sim\sim p \to \sim\sim q) \to \mathbf{0})$

Założenie $x : \sim(\sim p \to \sim(\sim\sim p \to \sim\sim q) \to \mathbf{0})$, teza $\mathbf{0}$.

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

założenia $y : \sim p$, $z : \sim(\sim\sim p \to \sim\sim q)$, teza $\mathbf{0}$.

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

założenia $u : \sim\sim p$, $v : \sim q$, teza $\mathbf{0}$.

Wystarczy uy.

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

Nienaturalna dedukcja

Reguły wnioskowania jak zwykle, i do tego:

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

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:

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

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

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

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 $k(\alpha)$.

Translacja Kołmogorowa

Twierdzenie:

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

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.

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.