Logika i teoria typów

Wykład 11

21 grudnia 2022

Tydzień temu: semantyka algebraiczna

Interpretujemy formuły w $\mathcal{H}$-*strukturach* postaci

$$\mathcal{A} = \langle A, f^A, g^A, \ldots, r^A, s^A, \ldots \rangle:$$

gdzie:

– $\mathcal{H}$ to zupełna algebra Heytinga;

– $r^A : A^{n_r} \to \mathcal{H}$;

– $s^A : A^{n_s} \to \mathcal{H}$.

Twierdzenie o pełności

Twierdzenie:

1) Jeśli $\Gamma \vdash \varphi$, to $\Gamma \models \varphi$.
2) Jeśli $\Gamma \models \varphi$, to $\Gamma \vdash \varphi$.

Zbudowaliśmy algebrę formuł $\mathcal{L}_\Gamma$, w której

$$\Gamma \vdash \varphi \quad \Leftrightarrow \quad [\![\varphi]\!]_{id} = 1$$

Ale algebra $\mathcal{L}_\Gamma$ nie musi być zupełna.

Uzupełnianie algebr Heytinga

Twierdzenie: *Niech $\mathcal{H}$ – algebra Heytinga. Istnieje taka zupełna algebra Heytinga $\mathcal{G}$, że:*

- *Algebra $\mathcal{H}$ jest podalgebrą $\mathcal{G}$;*
- *Jeśli dla $B \subseteq \mathcal{H}$ istnieje $\sup_\mathcal{H} B$, to $\sup_\mathcal{G} B = \sup_\mathcal{H} B$;*
- *Jeśli dla $B \subseteq \mathcal{H}$ istnieje $\inf_\mathcal{H} B$, to $\inf_\mathcal{G} B = \inf_\mathcal{H} B$.*

Jaki z tego pożytek?

Jeśli ζ jest wartościowaniem w $\mathcal{H}$-strukturze, to $[\![\alpha]\!]^\mathcal{H}_\zeta = [\![\alpha]\!]^\mathcal{G}_\zeta$, dla każdej formuły α. Zatem jeśli $\Gamma \models \alpha$ oraz $\mathcal{H} := \mathcal{L}_\Gamma$, to:

– po pierwsze $\mathcal{G}, id \models \Gamma$, bo $\mathcal{L}_\Gamma, id \models \Gamma$;

– po drugie, wtedy $\mathcal{G}, id \models \alpha$, więc $\mathcal{L}_\Gamma, id \models \alpha$, czyli $\Gamma \vdash \alpha$.

Uzupełnianie algebr Heytinga

Twierdzenie: *Niech $\mathcal{H}$ – algebra Heytinga. Istnieje taka zupełna algebra Heytinga $\mathcal{G}$, że:*

- *Algebra $\mathcal{H}$ jest podalgebrą $\mathcal{G}$;*
- *Jeśli dla $B \subseteq \mathcal{H}$ istnieje $\sup_\mathcal{H} B$, to $\sup_\mathcal{G} B = \sup_\mathcal{H} B$;*
- *Jeśli dla $B \subseteq \mathcal{H}$ istnieje $\inf_\mathcal{H} B$, to $\inf_\mathcal{G} B = \inf_\mathcal{H} B$.*

Dowód: *Ideał zupełny* w $\mathcal{H}$ to taki zbiór $I \subseteq \mathcal{H}$, że

- Jeśli $a \sqsubseteq b \in I$, to $a \in I$;
- Jeśli $A \subseteq I$ ma kres górny w $\mathcal{H}$, to $\sup_\mathcal{H} I \in I$.

Jako $\mathcal{G}$ bierzemy zbiór wszystkich ideałów zupełnych w $\mathcal{H}$.
Włożenie $i : \mathcal{H} \to \mathcal{G}$ określamy $i(a) = a\!\downarrow = \{b \mid b \sqsubseteq a\}$.

Kontrprzykłady topologiczne

$\mathcal{H} = \mathcal{O}(\mathbb{R}), \quad A = \mathbb{N} - \{0\}$

Przykład 1: $\neg\neg\forall x(r(x) \vee \neg r(x))$

Relacja: $r^A(n) = \mathbb{R} - \{w_n\}$, gdzie $\mathbb{Q} = \{w_i \mid i \in \mathbb{N} - \{0\}\}$.

Przykład 2: $\forall x(p \vee r(x)) \to p \vee \forall x.r(x)$

Relacje: $r^A(n) = (-\frac{1}{n}, \frac{1}{n}), \quad p^A = \mathbb{R} - \{0\}$.

Liczby rzeczywiste

Twierdzenie: Jeśli formuła zdaniwa jest prawdziwa w algebrze $\mathcal{O}(\mathbb{R})$, to jest intuicjonistyczną tautologią.

Czy to prawda dla logiki pierwszego rzędu?

Zasada Markowa

Przykład 3: $\forall x(\varphi \vee \neg\varphi) \wedge \neg\neg\exists x\varphi \to \exists x\varphi$

Kontrprzykład: $\mathcal{H} = \mathcal{O}(\mathbb{Q}), \quad A = \mathbb{N} - \{0\}, \quad \varphi = r(x)$

$$r^A(n) = (-\infty, -z_n) \cup (z_n, \infty),$$

gdzie $0 < z_n \notin \mathbb{Q}$ oraz $\lim_{n\to\infty} z_n = 0$.

Fakt: *Zasada Markowa jest prawdziwa w $\mathcal{O}(\mathbb{R})$-strukturach.*

Zasada Markowa: $\forall x(\varphi \vee \neg\varphi) \wedge \neg\neg\exists x\varphi \to \exists x\varphi$

Fakt: *Zasada Markowa jest prawdziwa w $\mathcal{O}(\mathbb{R})$-strukturach.*

Dowód: Dla rodziny zbiorów otwartych $\{F_a \mid a \in A\}$ należy udowodnić, że $\mathrm{Int}(\bigcap_a (F_a \cup {\sim}F_a)) \cap {\sim\sim}\bigcup_a F_a \subseteq \bigcup_a F_a$.

No to niech $d \in \mathrm{LS}$. Wtedy $d \in S \subseteq \mathrm{LS}$ dla pewnego odcinka S. Ponieważ S jest spójny, więc dla każdego elementu $a \in A$ albo zachodzi $S \subseteq F_a$ albo $S \subseteq {\sim}F_a$. Jeśli to drugie zawsze zachodzi, to $d \in \bigcap_a {\sim}F_a = {\sim}\bigcup_a F_a$. Ale to niemożliwe, bo $S \subseteq {\sim\sim}\bigcup_a F_a$, więc odcinek S musi być rozłączny ze zbiorem ${\sim}\bigcup_a F_a$. Zatem $S \subseteq F_a$ dla jakiegoś a.

Zadanie domowe:

Czy każda formuła pierwszego rzędu, prawdziwa we wszystkich $\mathcal{O}(\mathbb{Q})$-strukturach, jest tautologią?

Kripke semantics for first-order logic

Model: $\mathcal{C} = \langle C, \leq, \{\mathcal{A}_c \mid c \in C\}\rangle$

Dla $c \leq d \in C$ struktura $\mathcal{A}_c$ zawiera się w $\mathcal{A}_d$, tj.

– nośnik $|\mathcal{A}_c|$ jest podzbiorem $|\mathcal{A}_d|$;

– relacje w $\mathcal{A}_c$ są podzbiorami relacji w $\mathcal{A}_d$;

– funkcje w $\mathcal{A}_c$ są obcięciami funkcji w $\mathcal{A}_d$.

Semantyka Kripkego

$c, \varrho \Vdash rt_1 \ldots t_n \quad \equiv \quad \mathcal{A}_c, \varrho \models rt_1 \ldots t_n$ (klasycznie);

$c, \varrho \nVdash \bot$;

$c, \varrho \Vdash \varphi \vee \psi \quad \equiv \quad c, \varrho \Vdash \varphi$ lub $c, \varrho \Vdash \psi$;

$c, \varrho \Vdash \varphi \wedge \psi \quad \equiv \quad c, \varrho \Vdash \varphi$ oraz $c, \varrho \Vdash \psi$;

$c, \varrho \Vdash \varphi \to \psi \quad \equiv \quad$ jeśli $c \leq c'$ i $c', \varrho \Vdash \varphi$, to $c', \varrho \Vdash \psi$;

$c, \varrho \Vdash \exists a\varphi \quad \equiv \quad c, \varrho[a \mapsto \mathrm{d}] \Vdash \varphi$, dla pewnego $\mathrm{d} \in \mathcal{A}_c$;

$c, \varrho \Vdash \forall a\varphi \quad \equiv \quad$ jeśli $c \leq c'$ i $\mathrm{d} \in \mathcal{A}_{c'}$, to $c', \varrho[a \mapsto \mathrm{d}] \Vdash \varphi$.

Twierdzenie o poprawności

Lemat 1: Jeśli $c, \varrho \Vdash \varphi$ i $c \leq c'$, to $c', \varrho \Vdash \varphi$.

Lemat 2: $c, \varrho \Vdash \varphi[a := t] \quad \Leftrightarrow \quad c, \varrho[a \mapsto [\![t]\!]_\varrho] \Vdash \varphi$.

Twierdzenie: *Jeśli $\Gamma \vdash \varphi$ oraz $c, \varrho \Vdash \Gamma$, to $c, \varrho \Vdash \varphi$.*

(W skrócie: jeśli $\Gamma \vdash \varphi$, to $\Gamma \Vdash \varphi$.)

Dowód: Indukcja.

Przykład: $\nVdash \neg\neg\forall a\,(ra \vee \neg ra)$

Model $\mathcal{C} = \langle \mathbb{N}, \leq, \{\mathcal{A}_n \mid n \in \mathbb{N}\}\rangle$, porządek jak zwykle.
Struktury $\mathcal{A}_n = \langle \mathbb{N}, r^n\rangle$, gdzie $r^n = \{m \mid m < n\}$.

W tym modelu żaden stan nie wymusza $\forall a\,(ra \vee \neg ra)$.
Zatem każdy stan wymusza $\neg\forall a\,(ra \vee \neg ra)$.

Uwaga: (1) Nie działa twierdzenie Gliwienki.
(2) Spełnialność intuicjonistyczna nie implikuje klasycznej.

Fakt: *Jeśli model $\mathcal{C}$ ma skończony zbiór stanów, to $\mathcal{C} \Vdash \neg\neg\forall a\,(ra \vee \neg ra)$.*

Przykład: $\nVdash \forall x(p \vee r(x)) \to p \vee \forall x.r(x)$

Model $\mathcal{C} = \langle \{1,2\}, \leq, \{\mathcal{A}_1, \mathcal{A}_2\}\rangle$, gdzie $1 < 2$, oraz

$$\begin{array}{ll} \mathcal{A}_1 = \langle \{1\}, r^1, p^1\rangle, & \mathcal{A}_2 = \langle \{1,2\}, r^2, p^2\rangle \\ r^1 = \{1\}, p^1 = \varnothing, & r^2 = \{1\}, p^2 = \{1,2\} \end{array}$$

W tym modelu $1 \Vdash \forall x(p \vee r(x))$, ale $1 \nVdash p \vee \forall x.r(x)$.

Fakt (Schemat Grzegorczyka)

1. *Jeśli w modelu $\mathcal{C}$ wszystkie $|A_c|$ są takie same, to*

   $$\mathcal{C} \Vdash \forall a(\psi \vee \varphi(a)) \to \psi \vee \forall a\,\varphi(a).$$

2. *Schemat jw. aksjomatyzuje „logikę stałych dziedzin"*

Twierdzenie o pełności: $\Gamma \vdash \varphi \Leftrightarrow \Gamma \Vdash \varphi$

1. Metoda stałych Henkina: stany modelu to zbiory formuł spełniające prawo alternatywy i prawo egzystencjalne. W kolejnych stanach struktury z termów nad rosnącymi zbiorami stałych.
2. Gry pierwszego rzędu: jedno z dwojga ma strategię. Zatem albo jest dowód (normalny) albo kontrmodel.

Example: $(\forall x\,(P(x) \vee (P(x) \to Q)) \to Q) \to Q$

$\exists$: `intro` !

$\forall$: $X : \forall x\,(P(x) \vee (P(x) \to Q)) \to Q \;\vdash\; Q$?

$\exists$: `apply` X !

$\forall$: $X : \forall x\,(P(x) \vee (P(x) {\to} Q)) \to Q \;\vdash\; \forall x\,(P(x) \vee (P(x) {\to} Q))$?

$\exists$: `intro` !

$\forall$: $X : \forall x\,(P(x) \vee (P(x) \to Q)) \to Q \;\vdash\; P(x_0) \vee (P(x_0) \to Q)$?

$\exists$: `right; intro` !

$\forall$: $X : \forall x\,(P(x) \vee (P(x) {\to} Q)) {\to} Q,\; Y_0 : P(x_0) \;\vdash\; Q$?

$(\ldots)$

$\forall$: $X : \forall x\,(P(x) \vee (P(x) {\to} Q)) {\to} Q,\; Y_0 : P(x_0),\; Y_1 : P(x_1) \;\vdash\; Q$?

Nierozstrzygalność

czyli: programs into 1st order proofs

Generating a chain

Assumptions:

$\ldots, H0 : Z(x_0), \quad H1 : \forall x(\forall y(S(x,y) \to state) \to state)$.

To prove $state$ one applies $H1$ to x_0:

New goal: $\quad \forall y(S(x_0, y) \to state)$

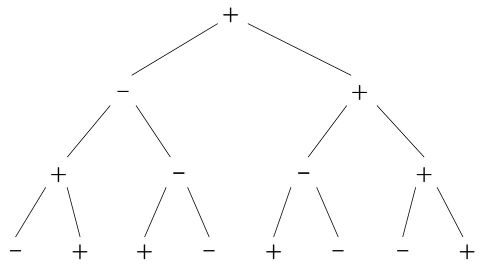
That is: $\quad S(x_0, x_1) \to state$, with fresh x_1.

Now we have new assumption $S(x_0, x_1)$.

We can add more: $S(x_0, x_1), S(x_1, x_2), S(x_2, x_3), \ldots$

Positive and Negative

Założenia są negatywne, tezy są pozytywne.



Monotoniczność: Jeśli p występuje w φ tylko pozytywnie, to

$$p \to p' \vdash \varphi(p) \to \varphi(p').$$

First-order proof search as computation

Negative quantification expands knowledge:

$\ldots, \forall x\,(((\varphi(x) \to state_2) \to state_1) \vdash state_1$

yields new task: $\quad \ldots, \varphi(t) \vdash state_2$

Positive quantification adds new variables:

$\ldots, \forall x\,(\varphi(x) \to state_2) \to state_1 \vdash state_1$

yields new task: $\quad \ldots, \varphi(y) \vdash state_2$,

where y is fresh.

Układanie kafelków (Domino problem)

Dany jest skończony zbiór T rodzajów kafelków

i relacje $H, V \subseteq T \times T$ zgodności poziomej i pionowej.

Pokrycie zbioru $A \subseteq \mathbb{Z} \times \mathbb{Z}$ to taka funkcja $P : A \to T$, że:

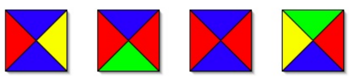
$\langle P(x,y), P(x+1,y)\rangle \in H$, gdy $\langle x,y\rangle \in A$ i $\langle x+1,y\rangle \in A$;

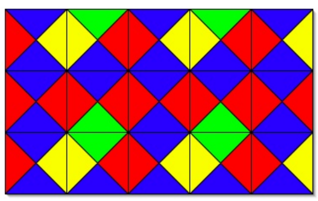
$\langle P(x,y), P(x,y+1)\rangle \in V$, gdy $\langle x,y\rangle \in A$ i $\langle x,y+1\rangle \in A$.

Pokrycie może spełniać *warunek początkowy* $P(0,0) = t_0$.

Domino: relacje H, V to relacje zgodności kolorów na brzegach.

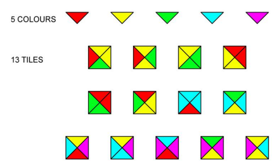
Przykład domina

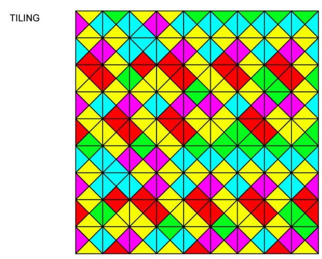




http://www.cs4fn.org/algorithms/tiles.php

Trudny przykład





https://grahamshawcross.com/2012/10/12/wang-tiles-and-aperiodic-tiling/

Nierozstrzygalność

Dla danej maszyny M definiujemy zbiór klocków T_M.

Lemat: *Następujące warunki są równoważne:*

1) *Maszyna M ma nieskończone obliczenie dla pustego słowa wejściowego.*
2) *Istnieje takie pokrycie P zbioru $\mathbb{N} \times \mathbb{N}$ dominem T_M, że $P(0,0) = t_0$.*

Kodowanie domina: zbiór założeń Γ

1. $\forall x(X(x) \to Y(x) \to t_0(x) \to loop) \to start$;
2. $\forall x(X(x) \to \forall y(H(x,y) \to X(y) \to set(y)) \to loop)$;
3. $\forall x(Y(x) \to \forall y(V(x,y) \to Y(y) \to set(y)) \to loop)$;
4. $\forall xyz(H(x,y) \to V(x,z) \to$
   $\forall u(H(z,u) \to V(y,u) \to set(u)) \to loop)$;
5. $\forall x((t_0(x) \to loop) \to \cdots \to (t_n(x) \to loop) \to set(x))$;
6. $\forall xy(V(x,y) \to t(x) \to t'(y) \to loop)$,
   for all pairs $\langle t, t' \rangle \notin v$;
7. $\forall xy(H(x,y) \to t(x) \to t'(y) \to loop)$,
   for all pairs $\langle t, t' \rangle \notin h$.

Kodowanie domina: główny lemat

Osąd $\Gamma \vdash start$ ma dowód $\Leftrightarrow$ nie istnieje pokrycie.

Jak to działa?

Zbiór Δ *reprezentuje* pokrycie $P : A \to T$ skończonego zbioru $A \subseteq \mathbb{N} \times \mathbb{N}$, gdy składa się z założeń postaci

$X(x_{i0})$, dla $\langle i, 0 \rangle \in A$;

$Y(x_{0j})$, dla $\langle 0, j \rangle \in A$;

$t(x_{ij})$, dla $P(i,j) = t$;

$H(x_{ij}, x_{i+1\,j})$, dla $\langle i,j \rangle, \langle i+1, j \rangle \in A$;

$V(x_{ij}, x_{i\,j+1})$, dla $\langle i,j \rangle, \langle i, j+1 \rangle \in A$.

Jak to działa?

Aby wyprowadzić osąd $\Gamma \vdash start$ musimy użyć założenia

(1) $\forall x(X(x) \to Y(x) \to t_0(x) \to loop) \to start$;

To prowadzi do pozycji

$$\Gamma, X(x_{00}), Y(x_{00}), t_0(x_{00}) \vdash loop,$$

która reprezentuje sytuację początkową.

Jak to działa?

Chcemy udowodnić osąd postaci $\Gamma, \Delta \vdash loop$, gdzie Δ reprezentuje częściowe pokrycie. Możemy użyć założenia

(2) $\forall x(X(x) \to \forall y(H(x,y) \to X(y) \to set(y)) \to loop)$

dla jakiegoś x_{i0}, takiego że $X(x_{i0}) \in \Delta$. Otrzymamy nowe zadanie $\Gamma, \Delta, H(x_{i0}, y), X(y) \vdash set(y)$, gdzie y jest nową zmienną, którą warto przemianować na $x_{i+1\,0}$.

Teraz trzeba do zmiennej $x_{i+1\,0}$ zastosować założenie

(5) $\forall x((t_0(x) \to loop) \to \cdots \to (t_n(x) \to loop) \to set(x))$

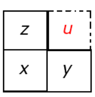
To tworzy n zadań postaci $\Gamma, \Delta' \vdash loop$, gdzie Δ' reprezentuje pokrycie z nowym klockiem w pozycji $\langle i+1, 0 \rangle$.

Jak to działa?

Chcemy udowodnić osąd postaci $\Gamma, \Delta \vdash loop$, gdzie Δ reprezentuje częściowe pokrycie. Możemy użyć założenia

(4) $\forall xyz(H(x,y) \to V(x,z) \to$
$\forall u(H(z,u) \to V(y,u) \to set(u)) \to loop)$

To odpowiada sytuacji przedstawionej na obrazku:



Natomiast założenie (3) dokłada klocek u góry na osi Y.

Jak to się kończy?

Aby zakończyć dowód musimy wykryć niezgodność klocków i użyć jednego z założeń

(6) $\forall xy(V(x,y) \to t(x) \to t'(y) \to loop)$;
(7) $\forall xy(H(x,y) \to t(x) \to t'(y) \to loop)$.

To się musi udać w każdej gałęzi dowodu, czyli dla każdego możliwego pokrycia.

Słaby punkt?

Używając założeń (2,3,4) można umieścić kilka klocków w tym samym miejscu. I to różnych.

Ale, po pierwsze nie trzeba tego robić, więc:

– jeśli nie ma pokrycia, to istnieje dowód bez takich efektów.

I po drugie: dokładanie nowych klocków nie ułatwia dowodu. I tak trzeba zakończyć wszystkie gałęzie dowodu, także te, w których nie ma „sprzeczności”. A więc:

– jeśli istnieje dowód, to tym bardziej nie ma pokrycia.

Erasing dependencies

Wycieranie zależności z typów

- $\kappa(Pt_1 \dots t_n) = P$ (zmienna zdaniowa);
- $\kappa(\varphi \to \psi) = \kappa(\varphi) \to \kappa(\psi)$;
- $\kappa(\varphi \vee \psi) = \kappa(\varphi) \vee \kappa(\psi)$;
- $\kappa(\varphi \wedge \psi) = \kappa(\varphi) \wedge \kappa(\psi)$;
- $\kappa(\bot) = \bot$;
- $\kappa(\exists a \varphi) = \kappa(\varphi)$;
- $\kappa(\forall a \varphi) = \kappa(\varphi)$.

Przykład

$\kappa(\forall x.\, (P \vee Q(x)) \to P \vee \forall x.\, Q(x)) = P \vee Q \to P \vee Q$

Wycieranie zależności z termów (1)

- $\kappa(x^\varphi) = x^{\kappa(\varphi)}$
- $\kappa(\lambda x{:}\varphi.M) = \lambda x{:}\kappa(\varphi).\kappa(M)$
- $\kappa(MN) = \kappa(M)\kappa(N)$
- $\kappa(\langle M, N\rangle) = \langle \kappa(M), \kappa(N)\rangle$
- $\kappa(\pi_i(M)) = \pi_i(\kappa(M))$
- $\kappa(\mathrm{in}_1\, M) = \mathrm{in}_1\, \kappa(M)$
- $\kappa(\mathrm{in}_2\, M) = \mathrm{in}_2\, \kappa(M)$
- $\kappa(M[x.\, P; y.\, Q]) = \kappa(M)[x.\, \kappa(P); y.\, \kappa(Q)])$

Wycieranie zależności z termów (2)

- $\kappa(\lambda a.M) = \kappa(M)$.
- $\kappa(Mt) = \kappa(M)$.
- $\kappa([t, M]) = \kappa(M)$.
- $\kappa(\mathrm{let}\ M = [a, y{:}\varphi]\ \mathrm{in}\ N) = (\lambda y{:}\kappa(\varphi).\kappa(N))\kappa(M)$.

Lemat: *Jeśli* $\Gamma \vdash M : \varphi$, *to* $\kappa(\Gamma) \vdash \kappa(M) : \kappa(\varphi)$.

Example use: strong normalization

Lemat: *Jeśli* $M \to_\beta M'$, *to* $\kappa(M) \twoheadrightarrow^+ \kappa(M')$, *z wyjątkiem redukcji „indywiduowych” (gdy redeks* $(\lambda a.N)t$ *zamieniamy na* $N[a := t]$*). W tym przypadku* $\kappa(M) = \kappa(M')$.

Na przykład:

$$\kappa(\mathrm{let}\ [t, M] = [a, y{:}\varphi]\ \mathrm{in}\ N) = (\lambda y.\, \kappa(N))\kappa(M) \to \kappa(N)[y := \kappa(M)] = \kappa(N[a := t][y := M])$$

Lemat: *Każdy ciąg redukcji indywiduowych jest skończony.*

Dowód: Maleje liczba lambd.

Silna normalizacja

Twierdzenie: *Termy dla logiki pierwszego rzędu mają własność silnej normalizacji ze względu na beta-redukcje.*

Dowód: Jeśli $M_1 \to M_2 \to \cdots$ to $\kappa(M_1) \twoheadrightarrow \kappa(M_2) \twoheadrightarrow \cdots$

Nieskończenie wiele razy zachodzi „prawdziwa" redukcja.

Silna normalizacja dla permutacji też zachodzi.
Dowód podobny jak dla rachunku zdań.

Przykład: arytmetyka Peana (1889)

- $\mathsf{int}(0)$;
- $\forall x(\mathsf{int}(x) \to \mathsf{int}(\mathsf{s}x))$;
- $\forall xy(\mathsf{s}x = \mathsf{s}y \to x = y)$;
- $\neg\exists x.\, 0 = \mathsf{s}(x)$;
- Schemat indukcji:
  $\tau(0) \to \forall y(\mathsf{int}(y) \to \tau(y) \to \tau(\mathsf{s}y)) \to \forall x(\mathsf{int}(x) \to \tau(x))$.
- Schemat indukcji trochę inaczej napisany:
  $\forall x(\mathsf{int}(x) \to \tau(0) \to \forall y(\mathsf{int}(y) \to \tau(y) \to \tau(\mathsf{s}y)) \to \tau(x))$.

Jak działa aksjomat indukcji?

Dwa pierwsze aksjomaty to dwie dodatkowe stałe:

$$Z : \mathsf{int}(0) \qquad S : \forall x(\mathsf{int}(x) \to \mathsf{int}(\mathsf{s}x))$$

Aksjomat indukcji to stała R_τ typu

$\forall x(\mathsf{int}(x) \to \tau(0) \to \forall y(\mathsf{int}(y) \to \tau(y) \to \tau(\mathsf{s}y)) \to \tau(x))$.

Jeśli $L : \mathsf{int}(t)$, $P : \tau(0)$, $Q : \forall y(\mathsf{int}(y) \to \tau(y) \to \tau(\mathsf{s}y))$,
to aplikacja $R_\tau tLPQ$ ma typ $\tau(t)$.

Dla $t = 0$ to można uprościć do $P : \tau(0)$.
A dowód $R_\tau(\mathsf{s}u)(SuL)PQ$ zredukujemy do $QuL(R_\tau uLPQ)$.

Erasing dependencies from Peano Arithmetic

Weźmy aksjomat indukcji Peana z 1889 roku:

$$\tau(0) \to \forall y(\mathsf{int}(y) \to \tau(y) \to \tau(\mathsf{s}y)) \to \forall x(\mathsf{int}(x) \to \tau(x)).$$

Napiszmy go trochę inaczej:

$$\forall x(\mathsf{int}(x) \to \tau(0) \to \forall y(\mathsf{int}(y) \to \tau(y) \to \tau(\mathsf{s}y)) \to \tau(x)).$$

I wytrzyjmy zależności:

$$\mathsf{int} \to \tau \to (\mathsf{int} \to \tau \to \tau) \to \tau.$$

System T Gödla

Typy: Typy proste zbudowane z jednej stałej typowej **int**.
(Czasem dodaje się **bool**, produkty itp.)

Termy: Jak w rachunku lambda z typami prostymi plus stałe:

$$0 : \mathsf{int} \qquad \mathsf{s} : \mathsf{int} \to \mathsf{int}$$

$$\mathsf{R}_\tau : \mathsf{int} \to \tau \to (\mathsf{int} \to \tau \to \tau) \to \tau,$$

Redukcja: Zwykła beta-redukcja oraz:

$$\mathsf{R}_\tau\, 0\, P\, Q \Rightarrow P \qquad \mathsf{R}_\tau(\mathsf{s}\, n)\, P\, Q \Rightarrow Q\, n\, (\mathsf{R}_\tau n\, P\, Q)$$

Przykład: Funkcja poprzednika

$$pred = \lambda n^{\mathsf{int}}.\, \mathsf{R}_{\mathsf{int}}\, n\, 0\, (\lambda xy.\, x)$$