Logika i teoria typów

Wykład 12

11 stycznia 2022

W poprzednim odcinku: 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

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

Twierdzenie Kreisela

Jeśli $\mathsf{PA} \vdash \forall a(\mathsf{int}(a) \to \exists b\, (\mathsf{int}(b) \wedge W(a, b)))$,

gdzie W jest pierwotnie rekurencyjne.

to istnieje dowód konstruktywny (w arytmetyce Heytinga).

Program extraction

Suppose we can prove in HA/PA:
$\forall a(\mathsf{int}(a) \to \exists b\, (\mathsf{int}(b) \wedge W(a, b)))$.

This theorem erases to a type $\mathsf{int} \to \mathsf{int} \times \tau$
The proof erases to a term $F : \mathsf{int} \to \mathsf{int} \times \tau$.

The term $\lambda a.\pi_1(Fa) : \mathsf{int} \to \mathsf{int}$ defines a function f such that:

$$\forall n \in \mathbb{N}.\, W(n, f(n))).$$

Własności systemu T

- System **T** ma własność silnej normalizacji (dowód „metodą Taita").
- Definiowalne są wszystkie funkcje dowodliwie rekurencyjne w PA.
- Własność SN dla systemu **T** jest niezależna od PA.

Metoda Taita

Definition: *Stable (computable,reducible...)* terms:

- $[\![\mathsf{int}]\!] := \mathsf{SN}$;
- $[\![\tau \to \sigma]\!] := \{M \mid \forall N(N \in [\![\tau]\!] \Rightarrow MN \in [\![\sigma]\!])\}$;

Główny lemat:

- Termy stabilne mają własność SN.
- Każdy term jest stabilny.

To jest trudne

Metoda Taita (zwana też metodą obliczalności) nie formalizuje się w PA, bo posługuje się dowolnymi zbiorami termów. Tego się nie da zakodować liczbami.

Strong normalization for system T cannot be derived in PA.

Idea dowodu: Silna normalizacja implikuje całkowitość funkcji uniwersalnej $f(n, m) = f_n(m)$, gdzie f_n to wszystkie funkcje definiowalne w T. Ale funkcja f nie jest definiowalna, bo jeśli $f(n, n) + 1 = f_k(n)$, to $f(k, k) + 1 = f(k, k)$.

Logika drugiego rzędu,

czyli Polimorfizm

Klasyczna logika drugiego rzędu

Składnia: Zmienne relacyjne i kwantyfikatory $\forall R, \exists R$.

Semantyka w stylu Tarskiego: Interpretujemy zmienne relacyjne jako relacje. Na przykład formuła

$$Nat(a) = \forall R(\forall b(R(b) \to R(sb)) \to R(0) \to R(a))$$

definiuje standardowe liczby naturalne.

Wniosek: *Aksjomaty Peana plus* $\forall a Nat(a)$ *definiują standardowy model arytmetyki z dokładnością do izomorfizmu.*

Wniosek: *Zbiór tautologii drugiego rzędu nie jest rekurencyjnie przeliczalny (bo* $\mathrm{Th}(\mathbb{N})$ *nie jest).*

Wniosek: *Nie ma pełnego systemu wnioskowania.*

Siła wyrazu języka drugiego rzędu

Przykład: Dodawanie liczb naturalnych ($m + n = k$):

$$\forall R(\forall a(Ra0a) \to \forall abc\,(Rabc \to Ra(sb)(sc)) \to Rmnk).$$

Dodawanie jest najmniejszym punktem stałym operatora:

$$R \mapsto \{\langle a, 0, a\rangle \mid a \in \mathbb{N}\} \cup \{\langle a, sb, sc\rangle \mid \langle a, b, c\rangle \in R\}.$$

Uogólnienie: Najmniejszy punkt stały operatora Φ:

$$\mathrm{LFP}_\Phi(a) := \forall R((\Phi(R) \subseteq R) \to Ra)$$
$$\mathrm{LFP}_\Phi(a) := \forall R(\forall b(\Phi(R)b \to Rb) \to Ra)$$

Logika drugiego rzędu w stylu Henkina

Semantyka (nieformalna): Interpretujemy zmienne relacyjne jako *definiowalne* predykaty.
To ma sens klasycznie i intuicjonistycznie.

Reguły wnioskowania:

$$(\forall^2\mathrm{I})\ \frac{\Gamma \vdash \varphi}{\Gamma \vdash \forall R\,\varphi}\ (R \notin \mathrm{FV}(\Gamma)) \qquad (\forall^2\mathrm{E})\ \frac{\Gamma \vdash \forall R\,\varphi}{\Gamma \vdash \varphi[R := \lambda\vec{a}.\psi]}$$

$$(\exists^2\mathrm{I})\ \frac{\Gamma \vdash \varphi[R := \lambda\vec{a}.\psi]}{\Gamma \vdash \exists R\,\varphi} \qquad (\exists^2\mathrm{E})\ \frac{\Gamma \vdash \exists R\,\varphi \quad \Gamma, \varphi \vdash \psi}{\Gamma \vdash \psi}$$
$$(R \notin \mathrm{FV}(\Gamma, \psi))$$

Brouwer-Heyting-Kołmogorow

- *A construction of* $\forall R\,\varphi(R)$ *is a method (function) transforming every predicate* R *into a proof of* φ(R).
- *A construction of* $\exists R\,\varphi(R)$ *consists of a predicate* **R** *and a construction of* φ(R).

Zdaniowa logika drugiego rzędu

Zdaniowa logika drugiego rzędu

Zdaniowa logika drugiego rzędu

Składnia:

- Zmienne zdaniowe $p, q, r, \ldots$ są formułami;
- Stała $\bot$ jest formułą;
- Jeśli α i β są formułami, to $\alpha \to \beta$, $\alpha \vee \beta$ i $\alpha \wedge \beta$ są formułami;
- Jeśli α jest formułą i p jest zmienną zdaniową, to $\forall p\,\alpha$ i $\exists p\,\alpha$ są formułami.

Brouwer-Heyting-Kołmogorow

- *A construction of* $\forall p\varphi(p)$ *is a method (function) transforming any proposition* **P** *into a proof of* φ(**P**).
- *A construction of* $\exists p\varphi(p)$ *consists of a proposition* **P** *and a construction of* φ(**P**).

Przykłady

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

$$\forall p(q \vee (q \to p)) \leftrightarrow \neg q \vee q$$

$$\exists p.\,((p \to q) \to p) \to r$$

$$\forall p(q \vee p) \to q \vee \forall p\,p$$

Naturalna dedukcja (implikacyjno-uniwersalna)

$$(\mathrm{Ax})\ \Gamma, \varphi \vdash \varphi$$

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

$$(\forall \mathrm{I})\ \frac{\Gamma \vdash \varphi}{\Gamma \vdash \forall p\, \varphi}\ (p \notin FVT(\Gamma)) \qquad (\forall \mathrm{E})\ \frac{\Gamma \vdash \forall p\, \varphi}{\Gamma \vdash \varphi[p := \vartheta]}$$

Dwa slogany

- *Full comprehension:* Propositional variables range over all formulas:

  $$\exists p\, (\varphi \leftrightarrow p)$$

  $$\forall p\, \varphi(p) \to \varphi(\psi)$$

  The meaning of p in $\forall p\, \varphi$ can be $\forall p\, \varphi$ itself.

- *Impredicativity:* The meaning of $\forall p\, \varphi$ is defined by a reference to a domain to which $\forall p\, \varphi$ itself belongs.

Semantyka Kripkego

Model $\mathcal{C} = \langle C, \leq, \{D_c \mid c \in C\}\rangle$.

Zbiory $D_c \subseteq \mathrm{P}(C)$ spełniają warunki:
– jeśli $c \leq d$, to $D_c \subseteq D_d$;
– jeśli $d \in X \in D_c$ oraz $d \leq d'$, to $d' \in X$.

Wartościowanie *dopuszczalne* dla φ w stanie c:

$v(p) \in D_c$, gdy $p \in \mathrm{FV}(\varphi)$

Wymuszanie

$c, v \Vdash p \quad \equiv \quad c \in v(p)$;

$c, v \nVdash \bot$;

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

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

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

$c, v \Vdash \exists p \varphi \quad \equiv \quad c, v[p \mapsto X] \Vdash \varphi$, dla pewnego $X \in D_c$;

$c, v \Vdash \forall p \varphi \quad \equiv$ jeśli $c \leq c'$ i $X \in D_{c'}$, to $c', v[p \mapsto X] \Vdash \varphi$.

Kompletny model

Znaczenie formuły φ w stanie c, przy wartościowaniu v:

$$[\![\varphi]\!]_c = \{c' \mid c \leq c' \text{ oraz } c', v \Vdash \varphi\}$$

Model jest *kompletny*, gdy zawsze $[\![\varphi]\!]_c \in D_c$

Fakt: *Model $\mathcal{C}$ jest kompletny wtw, gdy dla każdego φ:*

$\mathcal{C} \Vdash \exists p (p \leftrightarrow \varphi)$.

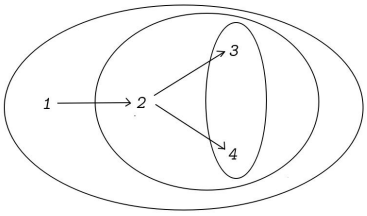
Pełność Kripkego

Piszemy $\Vdash \varphi$, gdy $\mathcal{C} \Vdash \varphi$, dla każdego kompletnego modelu $\mathcal{C}$.

Twierdzenie (Gabbay, Sobolew):

Warunki $\vdash \varphi$ i $\Vdash \varphi$ są równoważne.

$\nVdash \forall p\, (q \vee \neg p \vee \neg\neg p) \to q \vee \forall p\, (\neg p \vee \neg\neg p)$



D_1: zbiory jak na rysunku plus zbiór pusty. D_n: dowolne.
Wartościowanie $v(q) = \{2, 3, 4\}$. Wtedy:

$1, v \Vdash \forall p\, (q \vee \neg p \vee \neg\neg p)$,
$1, v \nVdash q$ oraz $1, v \nVdash \forall p\, (\neg p \vee \neg\neg p)$.

Semantyka Heytinga

W zupełnej algebrze Heytinga:

$$[\![\exists p\, \varphi]\!]_\zeta = \sup_{h \in \mathcal{H}} [\![\varphi]\!]_{\zeta[p \mapsto h]}$$

$$[\![\forall p\, \varphi]\!]_\zeta = \inf_{h \in \mathcal{H}} [\![\varphi]\!]_{\zeta[p \mapsto h]}$$

Fakt: *Jeśli $\vdash \varphi$, to $\models \varphi$*

Hipoteza: *I na odwrót.*

Nierozstrzygalność

Twierdzenie (Löb, 1976, Gabbay, 1974, Sobolew, 1977)
Intuicjonistyczna logika zdaniowa drugiego rzędu jest nierozstrzygalna.

Uwaga:

(0) Najprostszy znany dowód: Dudenhefner, Rehof, 2018 (zweryfikowany w Coqu)

(1) Wystarczy $\{\forall, \to\}$ lub $\{\exists, \to, \vee, \wedge, \neg\}$.

(2) Fragment $\{\forall, \exists, \wedge, \neg\}$ jest rozstrzygalny.

Comparison with classical logic

- Validity/provability in classical propositional logic is complete in the complexity class *co*-NP.
- Provability in intuitionistic propositional logic is Pspace-complete.
- Validity/provability in second-order classical propositional logic (known as the *QBF problem*) is Pspace-complete.
- Provability in second-order intuitionistic propositional logic is undecidable.

Siła wyrazu: suma/alternatywa

$$x \in A \cup B \quad \Leftrightarrow \quad \forall P(A \subseteq P \to B \subseteq P \to x \in P),$$

$$A(x) \vee B(x) \;\Leftrightarrow\; \forall P(\forall y(A(y) \to P(y)) \to \forall y(B(y) \to P(y)) \to P(x)).$$

$$A \vee B = \forall p((A \to p) \to (B \to p) \to p).$$

Siła wyrazu: iloczyn/koniunkcja

$$x \in A \cap B \quad \Leftrightarrow \quad \forall P(\forall z(z \in A \to z \in B \to z \in P) \to x \in P).$$

$$A \wedge B = \forall p((A \to B \to p) \to p).$$

Siła wyrazu: zbiór (typ) pusty czyli fałsz

$$x \in \varnothing \quad \Leftrightarrow \quad \forall P(x \in P).$$

$$\bot = \forall p\, p$$

Siła wyrazu: kwantyfikator szczegółowy

$$x \in \bigcup_P S_P \quad \Leftrightarrow \quad \forall Q(\forall P(S_P \subseteq Q) \to x \in Q)$$

$$\exists p\, \sigma = \forall q(\forall p(\sigma \to q) \to q).$$

Poprawność

Dla tak określonych spójników spełnione są zwykłe reguły wnioskowania, w tym:

$$(\exists \mathrm{I})\ \frac{\Gamma \vdash \varphi[p := \vartheta]}{\Gamma \vdash \exists p\, \varphi} \qquad (\exists \mathrm{E})\ \frac{\Gamma \vdash \exists p\, \varphi \quad \Gamma, \varphi \vdash \psi}{\Gamma \vdash \psi}$$

$$(p \notin \mathrm{FV}(\Gamma, \psi))$$

Polimorficzny rachunek lambda

Morał:

Można się ograniczyć do języka z implikacją i kwantyfikatorem ogólnym.

W ten sposób otrzymujemy system **F** Girarda.

Polymorphic types

- Basic idea: $\forall p.\, p \to p$ is a type of a generic identity.
- Church style (explicit polymorphism):
  - Generic identity I admits a type argument.
  - The application $\mathsf{I}\tau$ is of type $\tau \to \tau$.
- Curry style (implicit polymorphism):
  - Generic identity I has all types $\tau \to \tau$ at once.

Girard's System **F** (Church style)

$$\Gamma(x : \varphi) \vdash x : \varphi$$

$$\frac{\Gamma(x:\varphi) \vdash M : \psi}{\Gamma \vdash \lambda x{:}\varphi\, M : \varphi \to \psi} \qquad \frac{\Gamma \vdash M : \varphi \to \psi \quad \Gamma \vdash N : \varphi}{\Gamma \vdash MN : \psi}$$

$$\frac{\Gamma \vdash M : \varphi}{\Gamma \vdash \Lambda p\, M : \forall p\, \varphi}\ (p \notin \mathrm{FVT}(\Gamma)) \qquad \frac{\Gamma \vdash M : \forall p\, \varphi}{\Gamma \vdash M\vartheta : \varphi[p := \vartheta]}$$

Girard's System **F** (Church style)

$$\Gamma(x : \varphi) \vdash x : \varphi$$

$$\frac{\Gamma(x:\varphi) \vdash M : \psi}{\Gamma \vdash \lambda x{:}\varphi\, M : \varphi \to \psi} \qquad \frac{\Gamma \vdash M : \varphi \to \psi \quad \Gamma \vdash N : \varphi}{\Gamma \vdash MN : \psi}$$

$$\frac{\Gamma \vdash M : \varphi}{\Gamma \vdash \Lambda p\, M : \forall p\, \varphi}\ (p \notin \mathrm{FVT}(\Gamma)) \qquad \frac{\Gamma \vdash M : \forall p\, \varphi}{\Gamma \vdash M\vartheta : \varphi[p := \vartheta]}$$

A few examples

- Term $\Lambda q \lambda x^{\forall p(p \to p)}.x(q \to q)(xq)$
  has type $\forall q(\forall p(p \to p) \to q \to q)$;
- Term $2 = \Lambda p.\lambda f^{p \to p} \lambda x^{p}.f(fx)$
  has type $\forall p((p \to p) \to (p \to p))$;
- Term $\lambda f^{\forall p(p \to q \to p)} \Lambda p \lambda x^{p}.f(q \to p)(f\, p\, x)$
  has type $\forall p(p \to q \to p) \to \forall p(p \to q \to q \to p)$.

Reduction rules

Beta:

- $(\lambda x{:}\tau.M)N \Longrightarrow_\beta M[x := N]$;
- $(\Lambda\alpha.M)\tau \Longrightarrow_\beta M[\alpha := \tau]$,

Eta:

- $\lambda x{:}\tau.Mx \Longrightarrow_\eta M \quad (x \notin \mathrm{FV}(M))$;
- $\Lambda p.Mp \Longrightarrow_\eta M \quad (p \notin \mathrm{FVT}(M))$.

Subject reduction:

If $\Gamma \vdash M : \tau$ and $M \twoheadrightarrow_{\beta\eta} N$ then $\Gamma \vdash N : \tau$

System F w stylu Churcha

$$\Gamma(x : \varphi) \vdash x : \varphi$$

$$\frac{\Gamma(x:\varphi) \vdash M : \psi}{\Gamma \vdash \lambda x{:}\varphi\, M : \varphi \to \psi} \qquad \frac{\Gamma \vdash M : \varphi \to \psi \quad \Gamma \vdash N : \varphi}{\Gamma \vdash MN : \psi}$$

$$\frac{\Gamma \vdash M : \varphi}{\Gamma \vdash \Lambda p\, M : \forall p\, \varphi}\ (p \notin \mathrm{FVT}(\Gamma)) \qquad \frac{\Gamma \vdash M : \forall p\, \varphi}{\Gamma \vdash M\tau : \varphi[p := \tau]}$$

System F w stylu Curry'ego

$$\Gamma(x : \varphi) \vdash x : \varphi$$

$$\frac{\Gamma(x:\varphi) \vdash M : \psi}{\Gamma \vdash \lambda x \quad M : \varphi \to \psi} \qquad \frac{\Gamma \vdash M : \varphi \to \psi \quad \Gamma \vdash N : \varphi}{\Gamma \vdash MN : \psi}$$

$$\frac{\Gamma \vdash M : \varphi}{\Gamma \vdash \quad M : \forall p\, \varphi}\ (p \notin \mathrm{FVT}(\Gamma)) \qquad \frac{\Gamma \vdash M : \forall p\, \varphi}{\Gamma \vdash M \quad : \varphi[p := \tau]}$$

Wycieranie typów

$$\begin{aligned} |x| &= x \\ |MN| &= |M||N| \\ |\lambda x{:}\sigma.\, M| &= \lambda x.\, |M| \\ |\Lambda p.\, M| &= |M| \\ |M\tau| &= |M| \end{aligned}$$

Poprawność redukcji (Curry)

Twierdzenie:

Jeśli $\Gamma \vdash M : \tau$, *oraz* $M \to_\beta M'$ *to* $\Gamma \vdash M' : \tau$.

Dowód: Pomijamy. (Nie jest oczywisty.)

Uwaga: Powyższe nie zachodzi dla η-redukcji.

Subject reduction fails for η

Example:

$$x : p \to \forall q\,(q \to q) \quad \vdash \lambda y.\, xy : p \to q \to q.$$

$$x : p \to \forall q\,(q \to q) \quad \not\vdash \quad x : p \to q \to q.$$

Nierozstrzygalność

Twierdzenie 1: (wniosek z tw. Löba) Problem inhabitacji:

Dany typ τ, czy istnieje term zamknięty M typu τ?

jest nierozstrzygalny dla systemu **F**.

Twierdzenie 2: (J.B. Wells, 1993) Problem typowalności:

Dany term M, czy istnieją takie Γ i τ, że $\Gamma \vdash M : \tau$?

i problem sprawdzenia typu:

Dane są Γ, M i τ. Czy $\Gamma \vdash M : \tau$?

są dla systemu **F** (Curry) nierozstrzygalne.

Najprostszy dowód: A. Dudenhefner, 2020
(zweryfikowany w Coqu)

Silna normalizacja

Twierdzenie (Jean-Yves Girard, 1972)

System **F** *ma własność silnej normalizacji.*

Dowód: Metoda „Candidats de reductibilité". Wymaga kwantyfikowania zmiennych, które oznaczają rodziny zbiorów. To jest arytmetyka 3. rzędu! □