Logika i teoria typów

Wykład 9

14 grudnia 2020

Zdaniowa logika drugiego rzędu

Motywujący przykład

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

Dowód formuły $Nat(0)$ można zapisać tak: $\lambda R \lambda X \lambda Y.\, Y$, gdzie $X : \forall b(R(b) \to R(sb))$, $Y : R(0)$

Dowodem $Nat(1)$, czyli $Nat(s0)$, jest $\lambda R \lambda X \lambda Y.\, X0(Y)$ (po wytarciu zostaje $\lambda R \lambda X \lambda Y.\, X(Y)$).

Dowód formuły $Nat(s^n 0)$ to $\lambda R \lambda X \lambda Y.\, X^n(Y)$, i tak dalej.

Wycieranie zależności

Formuła

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

pozbawiona treści indywiduowej wygląda tak:

$$\omega = \forall r((r \to r) \to r \to r)$$

To jest polimorficzny typ liczebników Churcha $\mathbf{n} = \lambda f x.\, f^n x$. Liczebnik $\mathbf{n}$ jest wytarciem dowodu formuły $Nat(s^n(0))$.

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 $\mathbf{P}$ into a proof of $\varphi(\mathbf{P})$.*
- *A construction of $\exists p \varphi(p)$ consists of a proposition $\mathbf{P}$ and a construction of $\varphi(\mathbf{P})$.*

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 $D_c \subseteq \mathbf{P}(C)$ 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:

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

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:*

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

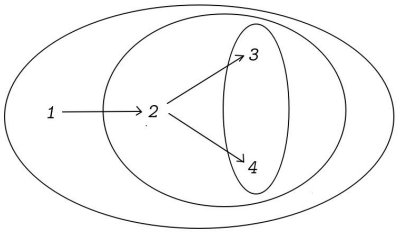
Pełność Kripkego

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:

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

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

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

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! □

Natural numbers

Numerals:

$$\mathbf{n} = \Lambda p \lambda f^{p \to p} \lambda x^{p}.\, f(f(\cdots f(x)))$$

are of type

$$\omega = \forall p((p \to p) \to (p \to p)).$$

Examples of representable functions:

- **A**$dd = \lambda mn.\Lambda p.\lambda fx.mpf(npfx)$;
- **M**$ult = \lambda mn.\Lambda p.\lambda fx.mp(npf)x$;
- **E**$xp = \lambda mn.\Lambda p.\lambda fx.m(p \to p)(np)fx$.

Słowa i listy

Słowa nad alfabetem dwuliterowym:

$$\forall p((p \to p) \to (p \to p) \to p \to p)$$

Słowo baba to term $\Lambda p \lambda a^{p \to p} \lambda b^{p \to p} \lambda x^{p}.\, b(a(b(a\,x)))$

Listy liczb naturalnych:

$$\forall p((\omega \to p \to p) \to p \to p)$$

$\mathrm{nil} = \Lambda p \lambda c^{\omega \to p \to p} \lambda x^{p}.\, x \qquad n :: \ell = \Lambda p \lambda c^{\omega \to p \to p} \lambda x^{p}.\, cn(\ell pcx)$

Data types

Empty type: $\bot = \forall p\, p$

Ex falso quodlibet:

If $\Gamma \vdash M : \bot$ *then* $\Gamma \vdash M\tau : \tau$.

Cartesian product

$$\sigma \wedge \tau = \forall p((\sigma \to \tau \to p) \to p)$$

Pairs and projections:

- Term $\langle M^{\sigma}, N^{\tau} \rangle = \Lambda p \lambda y^{\sigma \to \tau \to p}.yMN$ has type $\sigma \wedge \tau$.
- Term $\pi_1(M^{\sigma \wedge \tau}) = M\sigma(\lambda x^{\sigma} \lambda y^{\tau}.x)$ has type σ.
- Term $\pi_2(M^{\sigma \wedge \tau}) = M\tau(\lambda x^{\sigma} \lambda y^{\tau}.y)$ has type τ.

Beta-reduction works: $\pi_1(\langle M, N \rangle) \twoheadrightarrow M$, because
$(\Lambda p \lambda y^{\sigma \to \tau \to p}.yMN)\sigma(\lambda x^{\sigma} \lambda y^{\tau}.x) \twoheadrightarrow (\lambda x^{\sigma} \lambda y^{\tau}.x)MN \twoheadrightarrow M$.

Eta-reduction does not work:

$$\langle \pi_1(M), \pi_2(M) \rangle = \Lambda p \lambda y.y(\pi_1(M))(\pi_2(M)) \not\twoheadrightarrow M$$

Coproduct

$$\sigma \vee \tau = \forall p((\sigma \to p) \to (\tau \to p) \to p)$$

Embedings and cases:

- Term $\mathbf{inl}_{\sigma \vee \tau} M = \Lambda p \lambda u^{\sigma \to p} \lambda v^{\tau \to p}.uM$ has type $\sigma \vee \tau$.
- Term $\mathbf{inr}_{\sigma \vee \tau} M = \Lambda p \lambda u^{\sigma \to p} \lambda v^{\tau \to p}.vM$ has type $\sigma \vee \tau$.
- And **case** M **of** $[x]P^{\vartheta}, [y]Q^{\vartheta} = M\vartheta(\lambda x^{\sigma}P)(\lambda y^{\tau}Q) : \vartheta$.

Beta-reduction:

$\mathbf{case}\ \mathbf{in}_1(P)\ \mathbf{of}\ [x]M, [y]N = (\mathbf{in}_1(P))\vartheta(\lambda x^{\sigma}M)(\lambda y^{\tau}N) =$
$(\Lambda p \lambda uv.uP)\vartheta(\lambda x^{\sigma}M)(\lambda y^{\tau}N) \twoheadrightarrow (\lambda x^{\sigma}M)P \twoheadrightarrow M[x := P]$.

Abstract (encapsulated) type

Idea: Type $\exists p\, \sigma(p)$ is of shape $\sigma(\tau)$, where τ is unspecified (abstract) and not accesible to the user.

Example: An abstract pds object is of type

$$\exists p\,(p \times p \times (p \to p) \times (p \to \omega) \times (\omega \times p \to p))$$

Existential types

Type assignment:

$$(\text{pack})\ \frac{\Gamma \vdash M : \sigma[p := \tau]}{\Gamma \vdash [M, \tau]_{\exists p.\,\sigma} : \exists p.\,\sigma}$$

$$(\text{unpack})\ \frac{\Gamma \vdash M : \exists p.\,\sigma \quad \Gamma(x : \sigma) \vdash N : \rho}{\Gamma \vdash \textbf{unpack}\ M\ \textbf{as}\ [x, p]\ \textbf{in}\ N : \rho}\ (p \notin FV(\Gamma, \rho))$$

Beta reduction:

$\textbf{unpack}\ [M, \tau]_{\exists p.\,\sigma)}\ \textbf{as}\ [x, p]\ \ \textbf{in}\ N \longrightarrow_\beta N[p := \tau][x := M]$.

Implementing existential quantifier

Definitions:

- $\exists p\,\sigma \ = \ \forall q(\forall p(\sigma \to q) \to q)$.
- $[M^{\sigma[p:=\tau]}, \tau]_{\exists p.\,\sigma} \ = \ \Lambda q \lambda z^{\forall p(\sigma \to q)}.z\tau M$;
- $\textbf{unpack}\ M^{\exists p.\,\sigma}\ \textbf{as}\ [x, p]\ \textbf{in}\ N^\rho \ = \ M\rho(\Lambda p \lambda x^\sigma.N)$.

Correcteness:

$$\begin{aligned}
&\textbf{unpack}\ [M, \tau]\ \textbf{as}\ [x, p]\ \ \textbf{in}\ N^\rho \\
&\quad = (\Lambda q \lambda z^{\forall p(\sigma \to q)}.\, z\tau M)\rho(\Lambda p \lambda x^\sigma.N) \\
&\quad \to (\lambda z^{\forall p(\sigma \to \rho)}.\, z\tau M)(\Lambda p \lambda x^\sigma.N) \\
&\quad \to (\Lambda p \lambda x^\sigma.N)\tau M \\
&\quad \twoheadrightarrow N[p := \tau][x := M].
\end{aligned}$$