Logika intuicjonistyczna

Wykład 1

16 lutego 2012

Motywujący przykład

CURIOSA

339. A Simple Proof That a Power of an Irrational Number to an Irrational Exponent May Be Rational. $\sqrt{2}^{\sqrt{2}}$ is either rational or irrational. If it is rational, our statement is proved. If it is irrational, $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$ proves our statement.

DOV JARDEN

JERUSALEM

340. A Minor Curiosity.

$11 \times 372 = 4092$ and $11 \times 273 = 3003$
$12 \times 341 = 4092$ and $21 \times 143 = 3003$
$31 \times 132 = 4092$ and $13 \times 231 = 3003$.

ROYAL V. HEATH

(*Scripta Mathematica*, 19:229, 1953)

Alternatywne rozwiązania:

- Udowodnić, że $(\sqrt{2})^{\sqrt{2}}$ jest liczbą niewymierną;
- Sprawdzić, że $(\sqrt{2})^{2\log_2 3} = 3$.

Jeszcze jeden przykład

Zadanie: *Udowodnić, że co najmniej jedna z liczb* $e + \pi$ *i* $e\pi$ *nie jest algebraiczna.*

Rozwiązanie: W przeciwnym razie współczynniki wielomianu $x^2 - x(e + \pi) + e\pi = (x - e)(x - \pi)$ są algebraiczne, więc algebraiczne są też pierwiastki.

Wielki wynalazek

Koncepcja wartości logicznej:

- Każde poprawnie zbudowane zdanie orzekające jest *prawdziwe* albo *fałszywe*.
- Wartość logiczna zdania złożonego zależy tylko od wartości logicznych jego składowych.
- W szczególności implikacja jest *materialna*:
  znaczenie zdania „jeśli A to B" ma się nijak do
  – związku przyczynowo-skutkowego,
  – następstwa w czasie,
  – zakresu znaczeniowego, itp.

Małe odkrycia

- Koncepcja wartości logicznej to *wynalazek*.
  Jest to pewien *model* naszego wnioskowania.
- Każdy model opisuje tylko część rzeczywistości.
  Dygresja:
  - *Joe poszedł i kupił osła*;
  - *Kupił osła, chyba że zapomniał*;
  - *Teraz jeśli ma osła, to go bije.*
- Mogą być inne modele i inne wynalazki.

Logika intuicjonistyczna

- Dwuwartościowa logika to nadmierne uproszczenie:
  Czy w rozwinięciu dziesiętnym liczby π występuje gdzieś siedem siódemek pod rząd?
- Istnienie obiektów matematycznych nie jest absolutne,
  ich źródłem jest *creative subject*.
- Dowód istnienia obiektu wymaga więc jego konstrukcji.
- To samo dotyczy prawdy matematycznej:
  "There are no non-experienced truths" (Brouwer)
- Nie da się obronić prawa wyłączonego środka.

Tako rzecze Houyhnhnm:

. . . because reason taught us to affirm or deny

only where we are certain;

and beyond our knowledge we cannot do either.

(Jonathan Swift, *Gulliver's Travels*)

Prekursorzy:

- Immanuel Kant (1724–1804);
- Leopold Kronecker (1823–1891);
- Jules Molk (1857-1914);
- Jules Henri Poincaré (1854–1912);
- Emil Borel (1871–1956);
- Henri Léon Lebesgue (1875–1941).

Autorzy:

- Luitzen Egbertus Jan Brouwer (1881–1966);
- Валерий Иванович Гливенко (1896–1940);
- Arend Heyting (1898–1980);
- Андрей Николаевич Колмогоров (1903–1987).

O czym będzie ten wykład

- Logika intuicjonistyczna jako system formalny:
  - Rachunek zdań;
  - Rachunek predykatów;
  - Rachunek zdań drugiego rzędu.
- Teoria dowodu i semantyka. Problemy decyzyjne.
- Sens obliczeniowy: izomorfizm Curry'ego-Howarda.
- Dygresje i wycieczki:
  - Logika liniowa i logiki podstrukturalne;
  - Rachunek lambda;
  - Interpretacja obliczeniowa logiki klasycznej.

O czym to nie będzie:

- O filozofii;
- O matematyce konstruktywnej.

Przedmiot i metoda:

- Przedmiot: logika intuicjonistyczna, jej metody wnioskowania i semantyka.
- Metoda: zdroworozsądkowa ("klasyczna") metalogika.

Boole, Tarski: The logical value paradigm

- Formula = a declarative assertion about some "reality".
- Correctness criterion = truth (logical value).
- Semantics has priority over proof.
- Proof = just a tool; its shape is not essential, we only ask if one exists.
- Logic = determining if a sentence is true.
- The role of a logical connective = define the truth of a compound sentence in terms of the values of its components.
- Tautologia = schemat stwierdzenia, który zawsze ma wartość prawdy.

Brouwer: The construction paradigm

- Reality? What is it?
- Reasoning is primary, semantics is just a tool.
- Correctness criterion = construction.
- The role of a logical connective = express a construction of a compound sentence in terms of constructions of its components.
- Tautologia = schemat stwierdzenia, który zawsze ma konstrukcję.

BHK Interpretation

Nieformalna definicja konstrukcji

- *A construction of $\alpha \wedge \beta$ is a pair of constructions, one for α and one for β.*
- *A construction of $\alpha \vee \beta$ consists of a construction of either α or β (and an indication which one).*

Brouwer-Heyting-Kołmogorow

- *A construction of $\alpha \to \beta$ is a method that turns any construction of α into a construction of β.*
- *There is no construction of $\bot$.*

Negation: $\neg\varphi = \varphi \to \bot$.

- *A construction of $\neg\varphi$ is a method that turns any hypothetical construction of φ into a nonsense ($\bot$: "the thing which is not").*

Możliwe rozumienie BHK

Konstrukcja formuły α to *zapis obliczenia* wartości 1 przy ustalonym wartościowaniu zdaniowym ρ.
(Formuła może mieć wiele konstrukcji.)

- $[\![\bot]\!]_\rho = 0$, $[\![\top]\!]_\rho = 1$, $[\![p]\!]_\rho = \rho(p)$;
- $[\![\alpha \vee \beta]\!]_\rho = 1$, gdy $[\![\alpha]\!]_\rho = 1$ lub $[\![\beta]\!]_\rho = 1$;
- $[\![\alpha \wedge \beta]\!]_\rho = 1$, gdy $[\![\alpha]\!]_\rho = [\![\beta]\!]_\rho = 1$;
- $[\![\alpha \to \beta]\!]_\rho = 1$, gdy $[\![\alpha]\!]_\rho = 0$ lub $[\![\beta]\!]_\rho = 1$;
- $[\![\neg\alpha]\!]_\rho = 1 - [\![\alpha]\!]_\rho$;

Składnia rachunku zdań

- *Zmienne zdaniowe* ($p, q, r, \ldots$) są formułami.
- Stała $\bot$ jest formułą.
- Jeśli α i β są formułami to

  $$(\alpha \to \beta), \quad (\alpha \vee \beta), \quad (\alpha \wedge \beta)$$

  też są formułami.

Skróty i konwencje

- Napis $\neg\alpha$ jest skrótem napisu $\alpha \to \bot$.
- Napis $\top$ jest skrótem napisu $\bot \to \bot$.
- Napis $\alpha \leftrightarrow \beta$ jest skrótem napisu $(\alpha \to \beta) \wedge (\beta \to \alpha)$.
- Zewnętrzne nawiasy opuszczamy.
- Implikacja wiąże w prawo:
  $\alpha \to \beta \to \gamma$ oznacza $\alpha \to (\beta \to \gamma)$.
- Priorytety:
  1. Negacja,
  2. Koniunkcja i alternatywa,
  3. Implikacja i równoważność.

Przykłady łatwe

- $p \to p$;
- $p \to q \to p$;
- $p \to (p \to q) \to q$;
- $p \to \neg\neg p$, czyli $p \to (p \to \bot) \to \bot$;
- $(p \to q) \to (q \to r) \to p \to r$;
- $(p \to q) \to (\neg q \to \neg p)$;
- $(p \to q \to r) \to (p \to q) \to p \to r$;
- $(p \vee q \to r) \to (p \to r) \wedge (q \to r)$;
- $\neg(p \vee q) \to \neg p \wedge \neg q$.

Mniej oczywiste

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

Całkiem wątpliwe

- $\neg\neg p \to p$;
- $\neg p \vee p$;
- $(\neg q \to \neg p) \to (p \to q)$;
- $\neg(p \wedge q) \to (\neg p \vee \neg q)$;
- $(p \to q) \to (\neg p \to q) \to q$;
- $p \vee (p \to q)$;
- $((p \to q) \to p) \to p$ (prawo Peirce'a).

Logika intuicjonistyczna

Wykład 2

23 lutego 2012

W poprzednim odcinku:

- *A construction of $\alpha \to \beta$ is a method that turns any construction of α into a construction of β.*
- *There is no construction of $\bot$.*

Negation: $\neg\varphi = \varphi \to \bot$.

- *A construction of $\neg\varphi$ is a method that turns any hypothetical construction of φ into a nonsense ($\bot$: "the thing which is not").*

W poprzednim odcinku:

- *A construction of $\alpha \wedge \beta$ is a pair of constructions, one for α and one for β.*
- *A construction of $\alpha \vee \beta$ consists of a construction of either α or β (and an indication which one).*

Implementacja BHK: naturalna dedukcja

Dowodzimy *osądów* postaci $\Gamma \vdash A$, gdzie Γ jest zbiorem formuł, a A jest formułą. Sens: A wynika z założeń Γ.

- Reguły *wprowadzania* spójników logicznych: jak można udowodnić formułę danej postaci?
- Reguły *eliminacji* spójników: jak można wykorzystać formułę tej postaci do udowodnienia innej?

Reguły wnioskowania dla rachunku zdań (1)

$$\frac{}{\Gamma \cup \{A\} \vdash A}\,(\mathrm{Ax})$$

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\,(\mathrm{W}\wedge) \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\,(\mathrm{E}\wedge) \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\,(\mathrm{E}\wedge)$$

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash A \to B}{\Gamma \vdash B}\,(\mathrm{E}\to) \qquad \frac{\Gamma \cup \{A\} \vdash B}{\Gamma \vdash A \to B}\,(\mathrm{W}\to)$$

Reguły wnioskowania dla rachunku zdań (2)

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\,(\mathrm{W}\vee) \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\,(\mathrm{W}\vee)$$

$$\frac{\Gamma \vdash A \vee B \qquad \Gamma \cup \{A\} \vdash C \qquad \Gamma \cup \{B\} \vdash C}{\Gamma \vdash C}\,(\mathrm{E}\vee)$$

$$\frac{\Gamma \cup \{A\} \vdash \bot}{\Gamma \vdash \neg A}\,(\mathrm{W}\neg) \qquad \frac{\Gamma \vdash \neg A \qquad \Gamma \vdash A}{\Gamma \vdash \bot}\,(\mathrm{E}\neg)$$

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A}\,(\mathrm{E}\bot)$$

Classical (unnatural) deduction

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

Dowód formalny

Dowód formalny osądu $\Gamma \vdash \varphi$ w naturalnej dedukcji, to drzewo skończone, w którym każdemu wierzchołkowi przypisano pewien osąd. Przy tym:

- Korzeniowi drzewa przypisano osąd $\Gamma \vdash \varphi$.
- Osąd przypisany dowolnemu wierzchołkowi powstaje z osądów przypisanych jego dzieciom poprzez zastosowanie jednej z reguł wnioskowania.
- Liściom przypisano osądy postaci $\Delta, \alpha \vdash \alpha$.

Przykład

$$\dfrac{p \vdash p}{\vdash p \to p}\,(\to \mathrm{I})$$

Przykład

$$\dfrac{\dfrac{p, q \vdash p}{p \vdash q \to p}\,(\to \mathrm{I})}{\vdash p \to q \to p}\,(\to \mathrm{I})$$

Przykład

Niech $\Gamma = \{p \to q \to r, p \to q, p\}$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Gamma \vdash p \to q \to r \quad \Gamma \vdash p}{\Gamma \vdash q \to r}\,(\to \mathrm{E}) \qquad \dfrac{\Gamma \vdash p \to q \quad \Gamma \vdash p}{\Gamma \vdash q}\,(\to \mathrm{E})}{\Gamma \vdash q}\,(\to \mathrm{E})}{p \to q \to r, p \to q \vdash p \to r}\,(\to \mathrm{I})}{p \to q \to r \vdash (p \to q) \to p \to r}\,(\to \mathrm{I})}{\vdash (p \to q \to r) \to (p \to q) \to p \to r}\,(\to \mathrm{I})$$

Przykład

$$\dfrac{\dfrac{\dfrac{(p{\to}p){\to}q,\ p \vdash p}{(p{\to}p){\to}q \vdash p{\to}p}\,(\mathrm{W}{\to}) \qquad (p{\to}p){\to}q \vdash (p{\to}p){\to}q}{(p{\to}p){\to}q \vdash q}\,(\mathrm{E}{\to})}{\vdash ((p{\to}p){\to}q) \to q}\,(\mathrm{W}{\to})$$

Dowód formalny to drzewo, którego liście (u góry!) są aksjomatami, a korzeń (u dołu!), to udowodniony osąd.

Przykład

$$\dfrac{\dfrac{\neg p,\ p \wedge q \vdash \neg p \qquad \dfrac{\neg p,\ p \wedge q \vdash p \wedge q}{\neg p,\ p \wedge q \vdash p}\,(\mathrm{E}\wedge)}{\neg p, p \wedge q \vdash \bot}\,(\mathrm{E}\neg)}{\neg p \vdash \neg(p \wedge q)}\,(\mathrm{W}\neg)$$

Proste własności

- **Osłabianie:**
  Jeśli $\Gamma \vdash \varphi$ *oraz* $\Gamma \subseteq \Delta$, *to* $\Delta \vdash \varphi$.
- **Podstawianie:**
  Jeśli $\Gamma \vdash \varphi$, *to* $\Gamma[p := \psi] \vdash \varphi[p := \psi]$.

Dowód: Indukcja ze względu na dowód.

In the meantime. . .

. . . Alonzo Church invented λ-calculus.

The untyped λ-calculus

Terms:

- Variables x, y, z,. . .
- Applications (MN);
- Abstractions $(\lambda x\, M)$.

Beta-reduction;

$$(\lambda x\, M)N \quad \Rightarrow \quad M[x := N]$$

Simply typed lambda-calculus

$$\Gamma, x : \sigma \vdash x : \sigma$$

$$\frac{\Gamma, x : \sigma \vdash M : \tau}{\Gamma \vdash (\lambda x : \sigma . M) : \sigma \to \tau}$$

$$\frac{\Gamma \vdash M : \sigma \to \tau \qquad \Gamma \vdash N : \sigma}{\Gamma \vdash (MN) : \tau}$$

Back to natural deduction ($\to$ only)

$$\Gamma, \sigma \vdash \sigma$$

$$\frac{\Gamma, \sigma \vdash \tau}{\Gamma \vdash \sigma \to \tau}$$

$$\frac{\Gamma \vdash \sigma \to \tau \qquad \Gamma \vdash \sigma}{\Gamma \vdash \tau}$$

Proof notation for natural deduction

$$\Gamma, x : \sigma \vdash x : \sigma$$

$$\frac{\Gamma, x : \sigma \vdash M : \tau}{\Gamma \vdash M \not\downarrow x : \sigma : \sigma \to \tau}$$

$$\frac{\Gamma \vdash M : \sigma \to \tau \qquad \Gamma \vdash N : \sigma}{\Gamma \vdash M \mathbin{@} N : \tau}$$

Proof notation for natural deduction

$$\Gamma, x : \sigma \vdash x : \sigma$$

$$\frac{\Gamma, x : \sigma \vdash M : \tau}{\Gamma \vdash \not\downarrow x : \sigma . M : \sigma \to \tau}$$

$$\frac{\Gamma \vdash M : \sigma \to \tau \qquad \Gamma \vdash N : \sigma}{\Gamma \vdash M \mathbin{@} N : \tau}$$

Proof notation for natural deduction

$$\Gamma, x:\sigma \vdash x : \sigma$$

$$\frac{\Gamma, x:\sigma \vdash M : \tau}{\Gamma \vdash \lambda x:\sigma.\, M : \sigma \to \tau}$$

$$\frac{\Gamma \vdash M : \sigma \to \tau \qquad \Gamma \vdash N : \sigma}{\Gamma \vdash M\,N : \tau}$$

Rozszerzony rachunek λ (1)

$$\Gamma, x{:}\tau \vdash M : \tau \qquad \frac{\Gamma \vdash M{:}\bot}{\Gamma \vdash \varepsilon_\tau(M) : \tau}$$

$$\frac{\Gamma, x{:}\alpha \vdash M : \beta}{\Gamma \vdash \lambda x{:}\alpha\, M : \alpha \to \beta} \qquad \frac{\Gamma \vdash M : \alpha \to \beta \quad \Gamma \vdash N : \alpha}{\Gamma \vdash MN : \beta}$$

Rozszerzony rachunek λ (2)

$$\frac{\Gamma \vdash M : \alpha \quad \Gamma \vdash N : \beta}{\Gamma \vdash \langle M, N\rangle : \alpha \wedge \beta} \qquad \frac{\Gamma \vdash M : \alpha_1 \wedge \alpha_2}{\Gamma \vdash M\{i\} : \alpha_i}$$

$$\frac{\Gamma \vdash M : \alpha_i}{\Gamma \vdash \mathsf{in}_i(M) : \alpha_1 \vee \alpha_2}$$

$$\frac{\Gamma \vdash M : \alpha \vee \beta \quad \Gamma, u{:}\alpha \vdash R : \tau \quad \Gamma, v{:}\beta \vdash Q : \tau}{\Gamma \vdash \mathsf{case}\ M\ \mathsf{of}\ [u]R\ \mathsf{or}\ [v]Q : \tau}$$

Curry-Howard Isomorphism

A propositional formula α is an intuitionistic theorem iff in the extended lambda-calculus there exists a closed term of type α (type α is nonempty).

"Propositions-as-Types"

- Formula = type = specification.
- Proof = program = implementation.
- Proof normalization = computation.

Przykłady

$\vdash \lambda x^{p}\, x : p \to p$;

$\vdash \lambda x^{p} y^{q}.\, x : p \to q \to p$;

$\vdash \lambda x^{p\to q\to r} y^{p\to q} z^{p}.\, xz(yz) : (p\to q\to r)\to(p\to q)\to p\to q$;

$\vdash \lambda x^{(p\to p)\to q}\, p(\lambda y^{p}\, y) : ((p\to p)\to q) \to q$;

$x : \neg p \vdash \lambda y^{p\wedge q}\, x(y\{1\}) : \neg(p \wedge q)$.

Przykłady

$\vdash \lambda x^{\alpha}\, \mathsf{in}_1(x) : \alpha \to \alpha \vee \beta$;

$\vdash \lambda x^{\beta}\, \mathsf{in}_2(x) : \beta \to \alpha \vee \beta$;

$y{:}\alpha\to\gamma, z{:}\beta\to\gamma \vdash \lambda x^{\alpha\vee\beta}.\, \mathsf{case}\ x\ \mathsf{of}\ [u]yu\ \mathsf{or}\ [v]zv : (\alpha\vee\beta) \to \gamma$;

$\vdash \lambda x^{\alpha\wedge\beta}\, x\{1\} : \alpha \wedge \beta \to \alpha$;

$\vdash \lambda x^{\alpha\wedge\beta}\, x\{2\} : \alpha \wedge \beta \to \beta$;

$y : \gamma \to \alpha, z : \gamma \to \beta \vdash \lambda x^{\gamma}\, \langle yx, yz\rangle : \gamma \to \alpha \wedge \beta$.

Logika intuicjonistyczna

Wykład 3

1 marca 2012

W poprzednim odcinku: naturalna dedukcja

$$\frac{}{\Gamma \cup \{A\} \vdash A}\,(\mathrm{Ax})$$

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\,(\mathrm{W}\wedge) \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\,(\mathrm{E}\wedge) \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\,(\mathrm{E}\wedge)$$

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash A \to B}{\Gamma \vdash B}\,(\mathrm{E}\to) \qquad \frac{\Gamma \cup \{A\} \vdash B}{\Gamma \vdash A \to B}\,(\mathrm{W}\to)$$

W poprzednim odcinku: naturalna dedukcja

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\,(\mathrm{W}\vee) \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\,(\mathrm{W}\vee)$$

$$\frac{\Gamma \vdash A \vee B \qquad \Gamma \cup \{A\} \vdash C \qquad \Gamma \cup \{B\} \vdash C}{\Gamma \vdash C}\,(\mathrm{E}\vee)$$

$$\frac{\Gamma \cup \{A\} \vdash \bot}{\Gamma \vdash \neg A}\,(\mathrm{W}\neg) \qquad \frac{\Gamma \vdash \neg A \qquad \Gamma \vdash A}{\Gamma \vdash \bot}\,(\mathrm{E}\neg)$$

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A}\,(\mathrm{E}\bot)$$

Semantyka algebraiczna

Relacja $\leq_\Gamma$ w zbiorze $\mathcal{F}$ wszystkich formuł:

$$\varphi \leq_\Gamma \psi \qquad \Leftrightarrow \qquad \Gamma \vdash \varphi \to \psi.$$

jest quasi-porządkiem (jest zwrotna i przechodnia).[1]

Równoważność indukowana przez $\leq$

$$\varphi \sim_\Gamma \psi \qquad \Leftrightarrow \qquad \Gamma \vdash \varphi \leftrightarrow \psi.$$

Zbiór $\mathcal{L}_\Gamma = \mathcal{F}/_\sim$ jest częściowo uporządkowany przez

$$[\varphi] \leq [\psi] \qquad \Leftrightarrow \qquad \Gamma \vdash \varphi \to \psi.$$

[1] Opuszczamy indeksy gdzie się da.

Własności porządku $\mathcal{L} = \langle \mathcal{F}/_{\sim}, \leq \rangle$

- Elementem najmniejszym („zerem") jest
$$0 = [\bot] = \{\varphi \mid \Gamma \vdash \neg\varphi\}.$$
- Elementem największym („jedynką") jest
$$1 = [\top] = \{\varphi \mid \Gamma \vdash \varphi\}.$$
- Kresem dolnym zbioru $\{[\varphi], [\psi]\}$ jest $[\varphi \wedge \psi]$, a kresem górnym jest $[\varphi \vee \psi]$.

Krata: zbiór częściowo uporządkowany, w którym każdy podzbiór dwuelementowy ma kres górny i dolny.

Kraty

Krata: zbiór częściowo uporządkowany, w którym każdy podzbiór dwuelementowy ma kres górny i dolny.

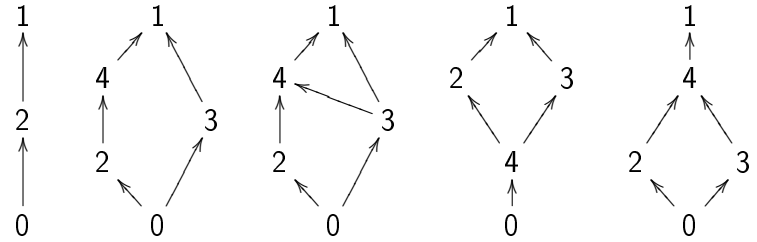
Oznaczenia: $a \sqcup b = \sup\{a, b\}$, $a \sqcap b = \inf\{a, b\}$.

Element najmniejszy kraty (jeśli istnieje) nazywamy *zerem*, a największy *jedynką*

Fakt: *Następujące warunki są równoważne w kracie:*

- $a \leq b$;
- $a \sqcap b = a$;
- $a \sqcup b = b$.

Przykłady krat



(a) (b) (c) (d) (e)

W kracie (b) zachodzi:

$(2 \sqcup 3) \sqcap 4 = 1 \sqcap 4 = 4$ oraz $(2 \sqcap 4) \sqcup (3 \sqcap 4) = 2 \sqcup 0 = 2$

Krata dystrybutywna

Krata jest *dystrybutywna*, gdy dla dowolnych a, b, c:

$$(a \sqcup b) \sqcap c = (a \sqcap c) \sqcup (b \sqcap c)$$
$$(a \sqcap b) \sqcup c = (a \sqcup c) \sqcap (b \sqcup c)$$

Fakt: *Krata $\mathcal{L}$ jest dystrybutywna, bo*

$$\vdash (\varphi \vee \psi) \wedge \vartheta \leftrightarrow (\varphi \wedge \vartheta) \vee (\psi \wedge \vartheta)$$
$$\vdash (\varphi \wedge \psi) \vee \vartheta \leftrightarrow (\varphi \vee \vartheta) \wedge (\psi \vee \vartheta)$$

Dystrybutywność (część)

$x : (\varphi \vee \psi) \wedge \vartheta \vdash$
$\quad$ case $x\{1\}$ of $[u^{\varphi}]\mathsf{in}_1(\langle u, x\{2\}\rangle)$
$\quad\quad$ or $[v^{\psi}]\mathsf{in}_2(\langle v, x\{2\}\rangle) : (\varphi \wedge \vartheta) \vee (\psi \wedge \vartheta)$

$x : (\varphi \wedge \vartheta) \vee (\psi \wedge \vartheta) \vdash$
$\quad$ case x of $[z^{\varphi\wedge\vartheta}]\langle \mathsf{in}_1(z\{1\}), z\{2\}\rangle$
$\quad\quad$ or $[y^{\psi\wedge\vartheta}]\langle \mathsf{in}_1(y\{1\}), y\{2\}\rangle : (\varphi \vee \psi) \wedge \vartheta$

Algebra Boole'a

Krata dystrybutywna z zerem i jedynką jest *algebrą Boole'a*, gdy dla dowolnego a istnieje *dopełnienie*, tj. takie b, że

$$a \sqcup b = 1 \qquad \text{oraz} \qquad a \sqcap b = 0.$$

W kracie $\mathcal{L}$ mamy problem: wprawdzie $[\varphi \wedge \neg\varphi] = 0$, ale nie umiemy udowodnić $[\varphi \wedge \neg\varphi] = 1$. To nie będzie dopełnienie, a $\mathcal{L}$ nie będzie algebrą Boole'a.

Pseudodopełnienie

Fakt:
Klasa $[\neg\varphi]$ *jest największym elementem* $\mathcal{L}$*, który daje zero w przecięciu z* $[\varphi]$ *— czyli pseudodopełnieniem klasy* $[\varphi]$.

Dowód: Bo jeśli $[\alpha] \sqcap [\varphi] = 0$, to $\Gamma \vdash \alpha \wedge \varphi \to \bot$, skąd $\Gamma, \alpha \vdash \varphi \to \bot$. A to wszystko dlatego, że formuły

$$\alpha \wedge \beta \to \gamma \quad \text{i} \quad \alpha \to \beta \to \gamma$$

są równoważne. To się nazywa „currying".

Uogólnienie

Currying: $\quad \vdash (\alpha \wedge \beta \to \gamma) \quad \leftrightarrow \quad (\alpha \to \beta \to \gamma).$

W algebrze $\mathcal{L}$ mamy więc:

$$[\alpha] \sqcap [\beta] \leq [\gamma] \quad \Leftrightarrow \quad [\alpha] \leq [\beta \to \gamma]$$

Morał:
Klasa $[\beta \to \gamma]$ *to największy element* $c \in \mathcal{L}$ *o własności* $c \sqcap [\varphi] \leq [\psi]$.

Pseudodopełnienie względne

Pseudodopełnienie elementu a *względem* b,
to największy element c o własności $c \sqcap a \leq b$.

Jeśli taki element istnieje, to jest tylko jeden.
Oznaczamy go przez $a \Rightarrow b$. Dla każdego x zachodzi wtedy

$$x \sqcap a \leq b \quad \Leftrightarrow \quad x \leq a \Rightarrow b.$$

Pseudodopełnienie (względem zera) oznaczamy przez $\sim A$

Algebra Heytinga

Krata dystrybutywna z zerem i jedynką jest *algebrą Heytinga*, (albo *algebrą pseudoboole'owską*) wtedy i tylko wtedy, gdy dla dowolnych a i b istnieje pseudodopełnienie względne $a \Rightarrow b$.

Morał: *Krata $\mathcal{L}$ jest algebrą Heytinga.*

Nazywamy ją też *algebrą formuł* albo *algebrą Lindenbauma* dla intuicjonistycznego rachunku zdań.

(Algebra Lindenbauma dla klasycznego rachunku zdań jest algebrą Boole'a.)

Dwie pożyteczne wiadomości

1. *Jeśli $a \Rightarrow b$ istnieje dla dowolnych a i b, to krata jest dystrybutywna.*
2. *Każda skończona krata dystrybutywna jest algebrą Heytinga.*

Jeszcze lepsza wiadomość

Rodzina podzbiorów otwartych przestrzeni topologicznej tworzy algebrę Heytinga (ze względu na inkluzję i zwykłe działania).

Pseudodopełnienie względne: $A \Rightarrow B = \mathrm{Int}(-A \cup B)$;

Pseudodopełnienie: $\sim A = \mathrm{Int}(-A)$

Poprawność definicji

Fakt: Jeśli zbiory X, A i B są otwarte, to

$$X \cap A \subseteq B \qquad \Leftrightarrow \qquad X \subseteq \mathrm{Int}(-A \cup B).$$

Dowód: Zadanie dla pierwszego roku: dla *dowolnych* X, A, B:

$$X \cap A \subseteq B \qquad \Leftrightarrow \qquad X \subseteq -A \cup B$$

Ponadto, jeśli $X \subseteq Y$ i X otwarty, to $X \subseteq \mathrm{Int}(Y)$.

Przykład przestrzeni topologicznej

Niech $\langle A, \leq \rangle$ - częściowy porządek.

Zbiór $B \subseteq A$ jest otwarty, gdy z $a \geq b \in B$ wynika $a \in B$.

Na przykład $a{\uparrow} = \{b \mid a \leq b\}$.

To jest przestrzeń topologiczna:
Zbiory $\varnothing$, A, suma i iloczyn otwartych są otwarte.

Wnętrze: $\mathrm{Int}(A) = \{a \mid a{\uparrow} \subseteq A\}$.

Pseudodopełnienie:

$$A \Rightarrow B = \mathrm{Int}(-A \cup B) = \{a \mid a{\uparrow} \subseteq -A \cup B\} = \{a \mid A \cap a{\uparrow} \subseteq B\}$$

$$A \Rightarrow B = \{a \mid \forall x (a \leq x \in A \to x \in B)\}$$

Semantyka algebraiczna

$\mathcal{H} = \langle H, \sqcup, \sqcap, \Rightarrow, -, 0, 1 \rangle$ – algebra Heytinga;

$v : Z \to H$ – wartościowanie zmiennych ze zbioru Z;

$[\![\varphi]\!]_v^{\mathcal{H}}$ (lub $[\![\varphi]\!]_v$) – znaczenie formuły φ przy wartościowaniu v.

$$\begin{array}{lcl}
[\![p]\!]_v & = & v(p), \quad \text{dla } p \in Z; \\
[\![\bot]\!]_v & = & 0; \\
[\![\varphi \vee \psi]\!]_v & = & [\![\varphi]\!]_v \sqcup [\![\psi]\!]_v\,; \\
[\![\varphi \wedge \psi]\!]_v & = & [\![\varphi]\!]_v \sqcap [\![\psi]\!]_v\,; \\
[\![\varphi \to \psi]\!]_v & = & [\![\varphi]\!]_v \Rightarrow [\![\psi]\!]_v\,.
\end{array}$$

Piszemy:

- $\mathcal{H}, v \models \varphi$, gdy $[\![\varphi]\!]_v^{\mathcal{H}} = 1$;
- $\mathcal{H} \models \varphi$, gdy $\mathcal{H}, v \models \varphi$, dla wszystkich v;
- $\mathcal{H}, v \models \Gamma$, gdy $\mathcal{H}, v \models \varphi$, dla wszystkich $\varphi \in \Gamma$;
- $\mathcal{H} \models \Gamma$, gdy $\mathcal{H}, v \models \Gamma$, dla wszystkich v;
- $\Gamma \models \varphi$, gdy $\mathcal{H}, v \models \Gamma$ zawsze pociąga $\mathcal{H}, v \models \varphi$;
- $\models \varphi$, gdy $\mathcal{H}, v \models \varphi$, dla wszystkich $\mathcal{H}, v$.
  I to się wtedy nazywa *tautologia*.

Twierdzenie o pełności

1. Poprawność: *Jeśli* $\Gamma \vdash \varphi$, *to* $\Gamma \models \varphi$.
2. Pełność: *I na odwrót.*

Dowód (1): Jeśli $\Gamma = \{\vartheta_1, \ldots, \vartheta_n\}$ to przez $[\![\Gamma]\!]_v$ oznaczamy element $[\![\vartheta_1]\!]_v \sqcap \cdots \sqcap [\![\vartheta_n]\!]_v$. (Uwaga: $[\![\varnothing]\!]_v = 1$.)

Przez indukcję ze względu na rozmiary dowodu pokazujemy że jeśli $\Gamma \vdash \varphi$, to $[\![\Gamma]\!]_v \leq [\![\varphi]\!]_v$, dla dowolnych $\mathcal{H}, v$. W kroku indukcyjnym mamy różne przypadki, wg ostatniej uzytej reguły.

Przyp. 1: Aksjomat $\Gamma \vdash \varphi$, gdzie $\varphi \in \Gamma$ – oczywiste.

Przyp. 2: Dowód $\Gamma \vdash \varphi$ otrzymano przez (E$\rightarrow$) z dowodów $\Gamma \vdash \psi$ i $\Gamma \vdash \psi \rightarrow \varphi$. Wtedy $[\![\Gamma]\!]_v \leq [\![\psi]\!]_v$ i $[\![\Gamma]\!]_v \leq [\![\psi \rightarrow \varphi]\!]_v$, zatem $[\![\Gamma]\!]_v \leq [\![\psi]\!]_v \sqcap [\![\psi \rightarrow \varphi]\!]_v \leq [\![\varphi]\!]_v$.

Twierdzenie o pełności

1. Poprawność: *Jeśli* $\Gamma \vdash \varphi$, *to* $\Gamma \models \varphi$.
2. Pełność: *I na odwrót.*

Dowód (1): Pozostałe przypadki też łatwe (tablica?)

Dowód (2): W algebrze $\mathcal{L}_\Gamma$ weźmy takie wartościowanie v, że $v(p) = [p]_\sim$ dla $p \in Z$.

Wtedy zawsze $[\![\varphi]\!]_v = [\varphi]_\sim$ (trywialna indukcja).

Jeśli $\gamma \in \Gamma$, to $[\![\gamma]\!]_v = [\gamma]_\sim = 1$. A więc $\mathcal{L}_\Gamma, v \models \Gamma$.

Skoro $\Gamma \models \varphi$, to $\mathcal{L}_\Gamma, v \models \varphi$, czyli $[\varphi]_\sim = [\![\varphi]\!]_v = 1 = \{\alpha \mid \Gamma \vdash \alpha\}$.

A zatem $\Gamma \vdash \varphi$.

Wniosek *Następujące formuły nie są intuicjonistycznie prawdziwe:*

1. $\neg p \vee p$;
2. $\neg\neg p \rightarrow p$.

Dowód: Zbiory otwarte na prostej rzeczywistej tworzą algebrę Heytinga $\mathcal{O}(\mathbb{R})$ z działaniami $\cup$, $\cap$, $0 = \varnothing$, $1 = \mathbb{R}$, oraz:

$$\sim A = \mathrm{Int}(-A), \qquad A \Rightarrow B = \mathrm{Int}(-A \cup B).$$

W tej algebrze, przy wartościowaniu $v(p) = \mathbb{R} - \{0\}$ mamy:

- $[\![\neg p]\!]_v = \sim(\mathbb{R} - \{0\}) = \mathrm{Int}(\{0\}) = \varnothing$;
- $[\![\neg p \vee p]\!]_v = \varnothing \cup (\mathbb{R} - \{0\}) = \mathbb{R} - \{0\} \neq 1$;
- $[\![\neg\neg p]\!]_v = \sim\varnothing = \mathrm{Int}(\mathbb{R}) = \mathbb{R}$;
- $[\![\neg\neg p \rightarrow p]\!] = \mathrm{Int}(-\mathbb{R} \cup (\mathbb{R} - \{0\})) =$
  $\mathrm{Int}(\varnothing \cup (\mathbb{R} - \{0\})) = \mathrm{Int}(\mathbb{R} - \{0\}) = \mathbb{R} - \{0\} \neq 1$.

Czytanie z listu Charlesa Sandersa Peirce'a do Williama Jamesa

I have long felt that it is a serious defect in existing logic that it takes no heed of the limit between two realms. I do not say that the Principle of Excluded Middle is downright false; but I do say that in every field of thought whatsoever there is an intermediate ground between positive assertion and positive negation which is just as Real as they.
(NEM 3:851, Feb. 26, 1909)

Dalsze wnioski

Następujące formuły nie są intuicjonistycznie prawdziwe:

1. $(\neg\neg p \to p) \to \neg p \vee p$;
2. $(\neg q \to \neg p) \to (p \to q)$;
3. $(p \to q) \to (\neg p \to q) \to q$;
4. $\neg(p \wedge q) \to (\neg p \vee \neg q)$;
5. $((p \to q) \to p) \to p$ (prawo Peirce'a).

Dowód: Ćwiczenia.

Własność skończonego („małego") modelu

Twierdzenie:

Jeśli $\mathcal{H} \models \varphi$ dla wszystkich skończonych algebr $\mathcal{H}$, to $\models \varphi$.

(Inaczej: *Jeśli $\not\models \varphi$, to istnieje skończony kontrprzykład.*)

Dowód: Dla danych $\mathcal{H}, v, \varphi$, gdzie $|\varphi| = n$, konstruujemy $\mathcal{H}', v'$ tak, że $\mathcal{H}'$ ma co najwyżej 2^{2^n} elementów, oraz

$\mathcal{H}, v \models \varphi$ wtedy i tylko wtedy, gdy $\mathcal{H}', v' \models \varphi$

A więc jeśli $\not\models \varphi$, to istnieje „mały" kontrprzykład.

Podformuły

Definicja:

- Każda formuła jest swoją podformułą.
- Podformuły α są też podformułami $\alpha \vee \beta$, $\alpha \wedge \beta$, $\alpha \to \beta$.
- Podformuły β są też podformułami $\alpha \vee \beta$, $\alpha \wedge \beta$, $\alpha \to \beta$.

Fakt: *Formuła o długości n ma co najwyżej n podformuł.*

Własność skończonego modelu – dowód

Ustalmy φ, $\mathcal{H}$, v. Niech $\varphi_1, \ldots, \varphi_m$ będą wszystkimi podformułami φ, i niech $\mathcal{G}$ – podkrata generowana w $\mathcal{H}$ przez elementy $[\![\varphi_i]\!]_v^{\mathcal{H}} = a_i$. Ona ma co najwyżej 2^{2^m} elementów, bo jest dystrybutywna.

Z tego samego powodu, krata $\mathcal{G}$ jest algebrą Heytinga.

Pułapka: Operacja $\Rightarrow_{\mathcal{G}}$ nie musi być taka sama jak $\Rightarrow_{\mathcal{H}}$.

Pseudodopełnienie w podkracie

Jeśli $\mathcal{G}$ jest podkratą $\mathcal{H}$, to dla dowolnych $a, b \in G$:

$$a \Rightarrow_{\mathcal{G}} b \quad \leq \quad a \Rightarrow_{\mathcal{H}} b.$$

Ale jeśli $a \Rightarrow_{\mathcal{H}} b \in \mathcal{G}$, to zachodzi równość.

Własność skończonego modelu – dowód

Dla dowolnej podformuły ψ formuły φ zachodzi $[\![\psi]\!]_v^{\mathcal{G}} = [\![\psi]\!]_v^{\mathcal{H}}$.

Indukcja ze względu na budowę ψ. Przypadek $\psi = \alpha \to \beta$:
$[\![\psi]\!]_v^{\mathcal{G}} = [\![\alpha]\!]_v^{\mathcal{G}} \Rightarrow_{\mathcal{G}} [\![\beta]\!]\mathcal{G}_v = [\![\alpha]\!]_v^{\mathcal{H}} \Rightarrow_{\mathcal{H}} [\![\beta]\!]\mathcal{H}_v = [\![\psi]\!]_v^{\mathcal{H}}$,
ponieważ wiadomo, że wartość $[\![\psi]\!]_v^{\mathcal{H}}$ jest w $\mathcal{G}$.
Pozostałe przypadki są łatwe.

Morał: Jeśli $[\![\varphi]\!]_v^{\mathcal{H}} = a_i \neq 1$, to $[\![\varphi]\!]_v^{\mathcal{G}} = a_i \neq 1$.

Rozstrzygalność

Wniosek: Intuicjonistyczny rachunek zdań jest rozstrzygalny.

Dowód: Dla danej formuły φ albo istnieje dowód albo istnieje skończony kontrprzykład. Szukamy obu na raz.

Złożoność (tego algorytmu): zniechęcająca.

Logika intuicjonistyczna

Wykład 4

8 marca 2012

W poprzednim odcinku:

Własność skończonego modelu:

Jeśli $\mathcal{H} \models \varphi$ dla wszystkich skończonych algebr $\mathcal{H}$, to $\models \varphi$.

Nie wystarczy jeden skończony model

Fakt: *Formuła* $\bigvee\{p_i \to p_j \mid i, j \in \{1, \ldots, n\} \wedge i \neq j\}$

- *nie jest tautologią;*
- *jest prawdziwa w każdej algebrze Heytinga, która ma mniej niż n elementów.*

Morał:

Logika intuicjonistyczna nie jest logiką „wielowartościową”: nie wystarczy skończony zbiór wartości.

Filtry

Niech $h : \mathcal{H} \to \mathcal{G}$ będzie homomorfizmem algebr Heytinga. Jakie własności ma zbiór $F = h^{-1}(\{1\})$?

1. F jest niepusty.
2. Jeśli $a, b \in F$, to $a \sqcap b \in F$.
3. Jeśli $a \in F$ i $a \leq b$, to $b \in F$.

Zbiór o własnościach (1–3) nazywamy *filtrem*.

- Zawsze $1 \in F$;
- Jeśli $a, a \Rightarrow b \in F$, to $b \in F$.

(Dualne pojęcie to *ideał* – przeciwobraz zera.)

Dwa lematy

Lemat: $a \sqcap b = a \sqcap (a \Rightarrow b) \sqcap (b \Rightarrow a)$.

Dowód: ($\leq$) $a \sqcap b \leq a$, $a \sqcap b \leq a \Rightarrow b$, $a \sqcap b \leq b \Rightarrow a$.

($\geq$) PS $\leq a$, PS $\leq a \sqcap (a \Rightarrow b) \leq b$.

Lemat: *Następujące warunki są równoważne:*

1. *Istnieje takie $f \in F$, że $a \sqcap f = b \sqcap f$;*
2. $(a \Rightarrow b) \sqcap (b \Rightarrow a) \in F$.

Dowód: Jeśli (1), to $a \sqcap f = b \sqcap f \leq b$, więc $f \leq a \Rightarrow b$.

Jeśli (2), to $a \sqcap f = b \sqcap f$ dla $f = (a \Rightarrow b) \sqcap (b \Rightarrow a)$.

Kongruencja

Definicja: $a \sim_F b \quad \Leftrightarrow \quad (a \Rightarrow b) \sqcap (b \Rightarrow a) \in F$.

Fakt:

- Relacja $\sim_F$ jest kongruencją ze względu na $\sqcap$, $\sqcup$, $\Rightarrow$.
- $a \sim_F 1 \quad \Leftrightarrow \quad a \in F$

Wniosek: Algebra ilorazowa $\mathcal{H}/_F = \mathcal{H}/_{\sim_F}$ jest algebrą Heytinga, przy czym $[1]_F = F$.

Przykład filtru

Fakt: W algebrze Heytinga:

- $\sim\sim\sim a = \sim a$.
- $\sim (\sim a \sqcup a) = 0$.

Definicja: Element a jest *gęsty*, gdy $\sim a = 0$ (równoważnie $\sim\sim a = 1$).

Fakt: Elementy gęste tworzą filtr. Iloraz jest algebrą Boole'a.

Dowód: Element $\sim a \sqcup a$ jest gęsty, zatem w algebrze ilorazowej $\sim[a] \sqcup [a] = 1$ (prawdziwe dopełnienie).

Twierdzenie Gliwenki

Twierdzenie: *Formuła α jest klasyczną tautologią wtedy i tylko wtedy, gdy $\neg\neg\alpha$ jest tautologią intuicjonistyczną.*

Dowód: ($\Rightarrow$) Wtedy α prawdziwa w każdej algebrze Boole'a, w tym w algebrze $\mathcal{H}/_F$, gdzie F to filtr elementów gęstych. Znaczenie formuły α w $\mathcal{H}$ musi więc zawsze być gęste. A więc znaczenie $\neg\neg\alpha$ jest jedynką.

($\Leftarrow$) Wtedy $\neg\neg\alpha$ jest tautologią klasyczną i α też.

Filtr: $F \neq \emptyset, \quad a, b \in F \to a \sqcap b \in F, \quad a \in F, a \leq b \to b \in F.$

Filtr *generowany* przez $A \subseteq \mathcal{H}$:

$b \in F(A)$, wtedy i tylko wtedy, gdy
$b \geq a_1 \sqcap \cdots \sqcap a_n$, dla pewnych $a_1, \ldots, a_n \in A$.

Fakt: Jeśli żaden skończony iloczyn elementów A nie jest zerem (A jest *scentrowany*), to filtr $F(A)$ jest właściwy.

Filtr: $F \neq \emptyset, \quad a, b \in F \to a \sqcap b \in F, \quad a \in F, a \leq b \to b \in F.$

Szczególne rodzaje filtrów:

- Filtr *właściwy*: $F \neq \mathcal{H}$ (inaczej: $0 \notin F$),
- Filtr *główny*: $F = a\uparrow = \{b \mid a \leq b\}$.
- Filtr *pierwszy*: filtr właściwy o własności

  Jeśli $a \sqcup b \in F$, to $a \in F$ lub $b \in F$.
- Filtr *maksymalny*: maksymalny wśród właściwych.
- *Ultrafiltr*: Zawsze albo $a \in F$ albo $\sim a \in F$.

Filtr: $F \neq \emptyset, \quad a, b \in F \to a \sqcap b \in F, \quad a \in F, a \leq b \to b \in F.$

Fakt: *Każdy filtr maksymalny jest pierwszy*

Dowód: Niech F maksymalny i $a \sqcup b \in F$, ale $a \notin F$ i $b \notin F$.

Wtedy filtr F_a generowany przez $F \cup \{a\}$, i F_b – generowany przez $F \cup \{b\}$, są niewłaściwe: $0 \in F_a \cap F_b$.

To znaczy, że istnieją takie $f_1, f_2 \in F$, że $f_1 \sqcap a = 0 = f_2 \sqcap b$.

Zatem $0 = 0 \sqcup 0 = (f_1 \sqcap a) \sqcup (f_2 \sqcap b) \geq$
$(f_1 \sqcap f_2 \sqcap a) \sqcup (f_1 \sqcap f_2 \sqcap b) = f_1 \sqcap f_2 \sqcap (a \sqcup b) \in F$.

Filtr: $F \neq \emptyset, \quad a, b \in F \to a \sqcap b \in F, \quad a \in F, a \leq b \to b \in F.$

Lemat: *Suma łańcucha filtrów jest filtrem.*

Lemat: *Każdy filtr właściwy rozszerza się do filtru pierwszego.*

Dowód: Niech F – filtr właściwy i niech

$$\mathcal{F} = \{G \mid G \text{ jest filtrem, oraz } F \subseteq G \neq \mathcal{H}\}$$

Rodzina $\mathcal{F}$ uporządkowana przez inkluzję spełnia założenia lematu Kuratowskiego-Zorna. Zatem ma element maksymalny. On jest filtrem maksymalnym, więc jest pierwszy.

Trochę mocniejsza wersja tego lematu

Lemat: *Niech F – filtr właściwy i niech $a \notin F$. Istnieje taki filtr pierwszy G, że $F \subseteq G$ oraz $a \notin G$.*

Dowód: Podobny do poprzedniego.

Wniosek:
Jeśli a należy do każdego filtru pierwszego to $a = 1$.

Dowód: W przeciwnym razie filtr $\{1\}$ można tak rozszerzyć do filtru pierwszego F, że $a \notin F$.

Wymuszanie

Ustalamy $\mathcal{H}$ i v.
Niech $\mathcal{C}$ – rodzina wszystkich filtrów pierwszych w $\mathcal{H}$.

Piszemy $F \Vdash \varphi$ (F *wymusza* φ), gdy $[\![\varphi]\!]_v \in F$.
Dla $F \in \mathcal{C}$:

- $F \Vdash \varphi \vee \psi \quad \equiv \quad F \Vdash \varphi$ lub $F \Vdash \psi$;
- $F \Vdash \varphi \wedge \psi \quad \equiv \quad F \Vdash \varphi$ i $F \Vdash \psi$;
- $F \nVdash \bot$;
- $F \Vdash \varphi \to \psi \quad \equiv$ jeśli $F \subseteq F' \Vdash \varphi$, to $F' \Vdash \psi$;
- $F \Vdash \neg\varphi \quad \equiv$ jeśli $F \subseteq F'$, to $F' \nVdash \varphi$.

$F \vdash \varphi \to \psi \quad \equiv$ jeśli $F \subseteq F' \Vdash \varphi$, to $F' \Vdash \psi$

$[\![\varphi \to \psi]\!]_v \in F \quad \equiv$ jeśli $F \subseteq F' \ni [\![\varphi]\!]_v$, to $[\![\psi]\!]_v \in F'$.

Dowód: ($\Rightarrow$) Niech $[\![\varphi \to \psi]\!]_v \in F \subseteq F'$ oraz $[\![\varphi]\!]_v \in F'$.
Wtedy $[\![\varphi \to \psi]\!]_v \sqcap [\![\varphi]\!]_v \leq [\![\psi_v]\!]$, więc $[\![\psi_v]\!] \in F'$.

($\Leftarrow$) Niech G' – filtr generowany przez $F \cup \{[\![\varphi]\!]_v\}$.

Jeśli $[\![\psi_v]\!] \in G'$, to $[\![\psi_v]\!] \geq [\![\varphi]\!]_v \sqcap f$, gdzie $f \in F$.
Wtedy $f \leq [\![\varphi \to \psi]\!]_v$, więc $[\![\varphi \to \psi]\!]_v \in F$.

Zatem $[\![\psi_v]\!] \notin G'$. Niech G pierwszy, $G' \subseteq G$, $[\![\psi_v]\!] \notin G$.
Sprzeczność, bo $F \subseteq G \ni [\![\varphi]\!]_v$.

Abstrakcja: model Kripkego

Definicja: *Model Kripkego:* struktura $\mathcal{C} = \langle C, \leq, \Vdash \rangle$, gdzie:

- C jest zbiorem *stanów*;
- $\leq$ jest częściowym porządkiem;
- $\Vdash \subseteq C \times \{p, q, r, \dots\}$;
- jeśli $c \Vdash p$ i $c \leq c'$, to $c' \Vdash p$.

Fakt: Filtry pierwsze w algebrze Heytinga (przy ustalonym v) tworzą model Kripkego, gdzie $\leq$ to $\subseteq$ oraz

$$F \Vdash p \quad \equiv \quad v(p) \in F.$$

Wymuszanie

Definicja: Rozszerzamy $\Vdash$ na dowolne formuły:

- $c \Vdash \varphi \vee \psi \quad \equiv \quad c \Vdash \varphi$ lub $c \Vdash \psi$;
- $c \Vdash \varphi \wedge \psi \quad \equiv \quad c \Vdash \varphi$ i $c \Vdash \psi$;
- $c \Vdash \varphi \to \psi \quad \equiv \quad$ jeśli $c \leq c' \Vdash \varphi$, to $c' \Vdash \psi$;
- $c \nVdash \bot$;
- $c \Vdash \neg\varphi \quad \equiv \quad$ jeśli $c \leq c'$, to $c' \nVdash \varphi$.

Fakt: W modelu wyznaczonym przez v:

$$F \Vdash \varphi \quad \equiv \quad [\![\varphi]\!]_v \in F.$$

Wymuszanie

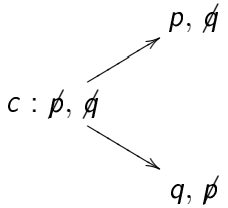
Definicja: Rozszerzamy $\Vdash$ na dowolne formuły:

- $c \Vdash \varphi \vee \psi \quad \equiv \quad c \Vdash \varphi$ lub $c \Vdash \psi$;
- $c \Vdash \varphi \wedge \psi \quad \equiv \quad c \Vdash \varphi$ i $c \Vdash \psi$;
- $c \Vdash \varphi \to \psi \quad \equiv \quad$ jeśli $c \leq c' \Vdash \varphi$, to $c' \Vdash \psi$;
- $c \nVdash \bot$;
- $c \Vdash \neg\varphi \quad \equiv \quad$ jeśli $c \leq c'$, to $c' \nVdash \varphi$.

Monotoniczność:

Jeśli $c \Vdash \varphi$ oraz $c \leq c'$, to $c' \Vdash \varphi$.

Przykład



$c \Vdash \neg\neg(p \vee q)$ $\qquad$ $c \Vdash (p \to q) \to q$, $\qquad$ $c \nVdash p \vee \neg p$.

Spełnianie w sensie Kripkego

- $\mathcal{C} \Vdash \varphi$, $\quad$ gdy $\quad c \Vdash \varphi$, dla wszystkich $c \in C$.
- $\mathcal{C} \Vdash \Gamma$, $\quad$ gdy $\quad \mathcal{C} \Vdash \varphi$, dla wszystkich $\varphi \in \Gamma$.
- $\Gamma \Vdash \varphi$, $\quad$ gdy $\quad \mathcal{C} \Vdash \Gamma$ zawsze pociąga $\mathcal{C} \Vdash \varphi$
- $\Vdash \varphi$, $\quad$ gdy $\quad \mathcal{C} \Vdash \varphi$, dla wszystkich $\mathcal{C}$.

Jeśli $\Gamma \Vdash \varphi$, *to* $\Gamma \models \varphi$.

Dowód: Niech $\mathcal{H}, v \models \Gamma$.

Jeśli $\gamma \in \Gamma$, to $[\![\gamma]\!]_v = 1 \in F$, dla każdego filtru F.

Zatem $\mathcal{C} \Vdash \Gamma$, gdzie $\mathcal{C}$ to model Kripkego z filtrów pierwszych.

Z założenia wynika $\mathcal{C} \Vdash \varphi$.

Stąd $[\![\varphi]\!]_v \in F$, dla każdego filtru pierwszego, więc $[\![\varphi]\!]_v = 1$.

Jeśli $\Gamma \models \varphi$, *to* $\Gamma \Vdash \varphi$.

Dowód: Niech $\mathcal{C} \Vdash \Gamma$.

Rodzina zamkniętych w górę podzbiorów $\mathcal{C}$ tworzy algebrę Heytinga $\mathcal{H}$ z działaniami $\cup$, $\cap$, oraz

$$A \Rightarrow B = \{a \mid \forall x(a \leq x \in A \rightarrow x \in B)\}.$$

Jeśli przyjmiemy $v(p) = \{c \in \mathcal{C} \mid c \Vdash p\}$, to dla każdego α:

$$[\![\alpha]\!]_v = \{c \in \mathcal{C} \mid c \Vdash \alpha\}. \qquad (?)$$

Zatem $[\![\gamma]\!]_v = \mathcal{C} = 1$, dla $\gamma \in \Gamma$, czyli $\mathcal{H}, v \models \Gamma$.

Stąd $\mathcal{H}, v \models \varphi$, czyli $\mathcal{C} \Vdash \varphi$.

$A \Rightarrow B = \{c \mid \forall c'(c \leq c' \in A \rightarrow c' \in B)\}$.

$$[\![\varphi]\!]_v = \{c \in \mathcal{C} \mid c \Vdash \varphi\} \qquad (?)$$

Dowód: Indukcja ze względu na φ. Oczywiste dla $\vee$, $\wedge$, $\bot$.

Niech $\varphi = \alpha \rightarrow \beta$. Z założenia indukcyjnego:

$[\![\varphi]\!]_v = [\![\alpha]\!]_v \Rightarrow [\![\beta]\!]_v = \{c \mid \forall c'(c \leq c' \Vdash \alpha \rightarrow c' \Vdash \beta)\}$,

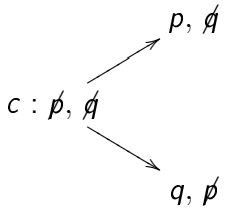
czyli $[\![\varphi]\!]_v = \{c \mid c \Vdash \alpha \rightarrow \beta\}$.

Morał:

Następujące warunki są równoważne:

- $\Gamma \vdash \varphi$;
- $\Gamma \models \varphi$;
- $\Gamma \Vdash \varphi$.

Przykład: $\not\Vdash p \vee \neg p$



Prawo alternatywy (disjunction property)

Twierdzenie: Jeśli $\vdash \alpha \vee \beta$, to $\vdash \alpha$ lub $\vdash \beta$.

Dowód: Przypuśćmy, że $\not\vdash \alpha$ i $\not\vdash \beta$.
Wtedy $\mathcal{C}_1, c_1 \not\Vdash \alpha$ i $\mathcal{C}_2, c_2 \not\Vdash \beta$.

Nowy model: $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2 \cup \{c_0\}$, gdzie c_0 nowy i najmniejszy. Relacja $\Vdash$ jest sumą relacji z $\mathcal{C}_1$ i $\mathcal{C}_2$. W stanie c_0 nie są wymuszane żadne zmienne zdaniowe.

Jeśli $\vdash \alpha \vee \beta$, to także $c_0 \Vdash \alpha \vee \beta$, skąd $c_0 \Vdash \alpha$ lub $c_0 \Vdash \beta$.
Ale wtedy także $c_1 \Vdash \alpha$ lub $c_2 \Vdash \beta$.

Logika intuicjonistyczna

Wykład 5

15 marca 2012

W poprzednim odcinku:

Definicja:

- $c \Vdash \varphi \vee \psi \quad \equiv \quad c \Vdash \varphi$ lub $c \Vdash \psi$;
- $c \Vdash \varphi \wedge \psi \quad \equiv \quad c \Vdash \varphi$ i $c \Vdash \psi$;
- $c \Vdash \varphi \to \psi \quad \equiv \quad$ jeśli $c \leq c' \Vdash \varphi$, to $c' \Vdash \psi$;
- $c \nVdash \bot$;
- $c \Vdash \neg\varphi \quad \equiv \quad$ jeśli $c \leq c'$, to $c' \nVdash \varphi$.

Monotoniczność: Jeśli $c \Vdash \varphi$ oraz $c \leq c'$, to $c' \Vdash \varphi$.

W poprzednim odcinku:

Model Kripkego: struktura $\mathcal{C} = \langle C, \leq, \Vdash \rangle$, gdzie:

- C jest zbiorem *stanów*;
- $\leq$ jest częściowym porządkiem;
- $\Vdash \subseteq C \times \{p, q, r, \dots\}$;
- jeśli $c \Vdash p$ i $c \leq c'$, to $c' \Vdash p$.

Pełność:

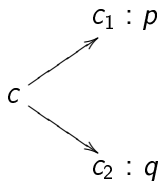
Następujące warunki są równoważne:

- $\Gamma \vdash \varphi$;
- $\Gamma \models \varphi$;
- $\Gamma \Vdash \varphi$.

„Separacja"

Twierdzenie: *Żadnego ze spójników* $\vee$, $\wedge$, $\rightarrow$, $\bot$, *nie można zdefiniować z pozostałych.*

1. Alternatywa:

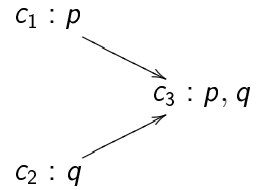


Jeśli φ – formuła bez $\vee$, to $\{c \mid c \Vdash \varphi\} \neq \{c_1, c_2\}$.
Inaczej: żadna formuła bez $\vee$ nie definiuje zbioru $\{c_1, c_2\}$.

„Separacja"

Twierdzenie: *Żadnego ze spójników* $\vee$, $\wedge$, $\rightarrow$, $\bot$, *nie można zdefiniować z pozostałych.*

2. Koniunkcja:

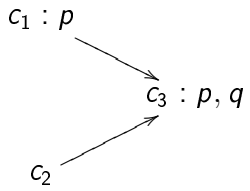


Żadna formuła bez $\wedge$ nie definiuje zbioru $\{c_3\}$.

„Separacja"

Twierdzenie: *Żadnego ze spójników* $\vee$, $\wedge$, $\rightarrow$, $\bot$, *nie można zdefiniować z pozostałych.*

3. Implikacja:



Żadna formuła bez $\rightarrow$ nie definiuje zbioru $\{c_2, c_3\}$.

„Separacja"

Twierdzenie: *Żadnego ze spójników* $\vee$, $\wedge$, $\rightarrow$, $\bot$, *nie można zdefiniować z pozostałych.*

4. Fałsz: Jeśli wszystkie zmienne formuły bez $\bot$ są wymuszone, to ta formuła też. (Formuła pozytywna nie może definiować w każdym modelu zbioru pustego.)

Fragment implikacyjny

Rozważamy formuły zbudowane ze zmiennych zdaniowych za pomocą samej implikacji i reguły naturalnej dedukcji:

$$\Gamma \cup \{A\} \vdash A \quad \text{(Ax)}$$

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash A \to B}{\Gamma \vdash B}\,(\mathrm{E}\to) \qquad \frac{\Gamma \cup \{A\} \vdash B}{\Gamma \vdash A \to B}\,(\mathrm{W}\to)$$

Twierdzenie: *System jw. jest pełny ze względu na semantykę Kripkego:* $\Gamma \vdash \varphi$ *zachodzi wtedy i tylko wtedy, gdy* $\Gamma \Vdash \varphi$.

Dowód: Część ($\Rightarrow$) wynika z poprawności całego systemu naturalnej dedukcji.

Jeśli $\Gamma \Vdash \varphi$, to $\Gamma \vdash \varphi$

Przypuśćmy, że $\Gamma \nvdash \varphi$. Budujemy model $\mathcal{C} = \langle C, \subseteq, \Vdash \rangle$, gdzie

$$C = \{\Delta \mid \forall \psi(\Delta \vdash \psi \to \psi \in \Delta)\}$$
$$\Delta \Vdash p \quad \leftrightarrow \quad p \in \Delta.$$

Dowodzimy, że dla dowolnego ψ zachodzi

$$\Delta \Vdash \psi \quad \leftrightarrow \quad \psi \in \Delta.$$

Indukcja. Nieoczywisty przypadek $\psi = \psi_1 \to \psi_2$

($\Leftarrow$) Niech $\psi_1 \to \psi_2 \in \Delta$ i niech $\Delta \subseteq \Delta' \Vdash \psi_1$. Wtedy $\psi_1 \in \Delta'$ oraz $\psi_1 \to \psi_2 \in \Delta'$, więc $\psi_2 \in \Delta'$ przez (E $\to$).

Jeśli $\Gamma \Vdash \varphi$, to $\Gamma \vdash \varphi$

Przypuśćmy, że $\Gamma \nvdash \varphi$. Budujemy model $\mathcal{C} = \langle C, \subseteq, \Vdash \rangle$, gdzie

$$C = \{\Delta \mid \forall \psi(\Delta \vdash \psi \to \psi \in \Delta)\}$$
$$\Delta \Vdash p \quad \leftrightarrow \quad p \in \Delta.$$

Dowodzimy, że dla dowolnego ψ zachodzi

$$\Delta \Vdash \psi \quad \leftrightarrow \quad \psi \in \Delta.$$

Indukcja. Nieoczywisty przypadek $\psi = \psi_1 \to \psi_2$

($\Rightarrow$) Niech $\Delta \Vdash \psi_1 \to \psi_2$ i niech $\Delta' = \{\vartheta \mid \Delta, \psi_1 \vdash \vartheta\}$. Wtedy $\Delta \subseteq \Delta' \Vdash \psi_1$, więc $\Delta' \Vdash \psi_2$, czyli $\psi_2 \in \Delta'$. Ale wtedy $\Delta \vdash \psi_1 \to \psi_2$ przez (W $\to$).

Morał: konserwatywność

Twierdzenie:

Jeśli formuła implikacyjna jest tautologią intuicjonistyczną, to można ją udowodnić z pomocą reguł (W $\to$) *i* (E $\to$).

Wniosek: *Typ prosty jest niepusty wtedy i tylko wtedy, gdy jest tautologią intuicjonistyczną.*

Własność skończonego modelu

Twierdzenie:
Jeśli $\mathcal{H} \models \varphi$ dla wszystkich skończonych algebr Heytinga, to $\models \varphi$.

Twierdzenie:
Jeśli $\mathcal{C} \Vdash \varphi$ dla każdego skończonego modelu Kripkego, to $\Vdash \varphi$.

Dowód: Był na ćwiczeniach.

Uwaga: Nie wystarczy jeden skończony model.

Wystarczy jeden model: np. topologia odcinka

Uniwersalna algebra Heytinga: $\mathcal{H} = \mathcal{O}(\mathbb{R})$.

(Równie dobre są np. $\mathcal{O}(\mathbb{Q})$, $\mathcal{O}(\mathbb{R}^2)$, $\mathcal{O}(0,1)$, itd.)

Twierdzenie: *Jeśli formuła jest prawdziwa w algebrze otwartych podzbiorów odcinka $(0,1)$, to jest tautologią.*

Jeśli $\mathcal{O}(0,1) \models \varphi$, to $\models \varphi$.

Dowód (wg Minca): Niech $\mathcal{C}$ – skończony model Kripkego. Określimy przekształcenie $\pi : (0,1) \xrightarrow{\text{na}} \mathcal{C}$ o własnościach:

1. Jeśli $A \subseteq (0,1)$ otwarty, to $\pi(A)$ zamknięty w górę.
2. Jeśli $Z \subseteq \mathcal{C}$ zamknięty w górę, to $\pi^{-1}(Z)$ otwarty.

Definiujemy wartościowanie $v(p) = \{x \in (0,1) \mid \pi(x) \Vdash p\}$ i dowodzimy, że $[\![\alpha]\!]_v = \{x \in (0,1) \mid \pi(x) \Vdash \alpha\}$.

Uwaga: te zbiory są otwarte, bo (2).

Dowód, ciąg dalszy

Niech $A_\alpha = \{x \in (0,1) \mid \pi(x) \Vdash \alpha\}$.

Definiujemy $v(p) = A_p$ i dowodzimy, że $[\![\alpha]\!]_v = A_\alpha$.

Przypadek $\alpha = \beta \to \delta$ (reszta łatwa): Wtedy

$$[\![\alpha]\!]_v = [\![\beta]\!]_v \Rightarrow [\![\delta]\!]_v = A_\beta \Rightarrow A_\delta.$$

($\subseteq$) Niech $x \in [\![\alpha]\!]_v$ i niech $\pi(x) \leq c \Vdash \beta$. Zbiór $\pi([\![\alpha]\!]_v)$ jest zamknięty w górę, więc istnieje takie $y \in [\![\alpha]\!]_v$, że $\pi(y) = c$. Zatem $y \in A_\beta \cap [\![\alpha]\!]_v = A_\beta \cap (A_\beta \Rightarrow A_\delta) \subseteq A_\delta$, tj. $c \Vdash \delta$.

Dowód, ciąg dalszy

Niech $A_\alpha = \{x \in (0,1) \mid \pi(x) \Vdash \alpha\}$.

Definiujemy $v(p) = A_p$ i dowodzimy, że $[\![\alpha]\!]_v = A_\alpha$.

Przypadek $\alpha = \beta \to \delta$ (reszta łatwa): Wtedy

$$[\![\alpha]\!]_v = [\![\beta]\!]_v \Rightarrow [\![\delta]\!]_v = A_\beta \Rightarrow A_\delta.$$

($\supseteq$) Niech $x \in A_\alpha$, tj. $\pi(x) \Vdash \beta \to \delta$. Ponieważ zbiór $\{c \mid c \Vdash \alpha\}$ jest zamknięty w górę, więc A_α jest otwarty, skąd $K(x,\varepsilon) \subseteq A_\alpha$, dla pewnego ε.

Niech $y \in K(x,\varepsilon)$. Wtedy $\pi(y) \Vdash \alpha$. Jeśli $\pi(y) \Vdash \beta$, to także $\pi(y) \Vdash \delta$ i $y \in A_\delta = [\![\delta]\!]_v$. Jeśli $\pi(y) \nVdash \beta$, to $y \in -[\![\beta]\!]_v$. To znaczy, że $K(x,\varepsilon) \subseteq -[\![\beta]\!]_v \cup [\![\delta]\!]_v$. Ale $K(x,\varepsilon)$ jest otwarty, więc $x \in K(x,\varepsilon) \subseteq \mathrm{Int}(-[\![\beta]\!]_v \cup [\![\delta]\!]_v) = [\![\alpha]\!]_v$.

Dowód, początek

Trzeba jeszcze zdefiniować $\pi : (0,1) \xrightarrow{\text{na}} \mathcal{C}$ o własnościach:

1. Jeśli $A \subseteq (0,1)$ otwarty, to $\pi(A)$ zamknięty w górę.
2. Jeśli $Z \subseteq \mathcal{C}$ zamknięty w górę, to $\pi^{-1}(Z)$ otwarty.

Dowód, końcówka

Wiemy, że $[\![\alpha]\!]_v = \{x \in (0,1) \mid \pi(x) \Vdash \alpha\}$.

Jeśli więc $c \nVdash \varphi$, to $x \notin [\![\varphi]\!]_v$, dla $\pi(x) = c$.

A funkcja π jest „na", więc takie x istnieje.

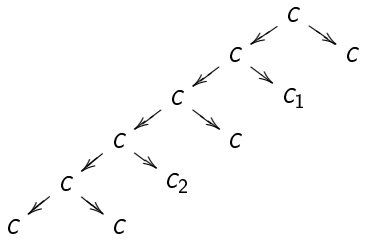
Etykietowanie drzewa binarnego

Najpierw $\ell(\varepsilon) = c_0$, gdzie c_0 – najmniejszy element modelu.

Potem (jeśli c ma m następników):

$$\begin{array}{lcll} \ell(w0^{2i}1) & = & c, & \text{for } i = 0,\ldots,m; \\ \ell(w0^{2i-1}1) & = & c_i, & \text{for } i = 1,\ldots,m; \\ \ell(w0^{i}) & = & c, & \text{for } i = 1,\ldots,2m+1. \end{array}$$

Obrazek dla $m = 2$:



Definicja $\pi : (0,1) \xrightarrow{\text{na}} \mathcal{C}$

Liczby $x \in (0,1)$ to ciągi z nieskończoną liczbą zer.

Przypadek skończony: $x = 0.b_1b_2 \ldots b_n1(00\ldots)$

Przypadek nieskończony: $x = 0.b_1b_2b_3\ldots$

Przypadek zabroniony: $x = 0.b_1b_2b_3111\ldots$

Definicja $\pi : (0,1) \xrightarrow{\text{na}} \mathcal{C}$

Przypadek skończony:

Jeśli $x = 0.b_1b_2 \ldots b_n1(00\ldots)$, to $\pi(x) = \ell(b_1b_2\ldots b_n)$ (bez jedynki!).

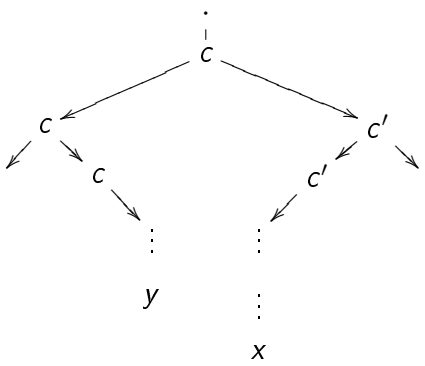
Przypadek nieskończony:

Jeśli $x = 0.b_1b_2b_3\ldots$, to ciąg $\ell(b_1) \le \ell(b_2) \le \ell(b_3)\ldots$ musi się ustalić na pewnym $c \in \mathcal{C}$.
Przyjmujemy $\pi(x) = c$.

Własności funkcji $\pi : (0,1) \xrightarrow{\text{na}} \mathcal{C}$

- Jeśli $\pi(x) = c \le c_1$, to dla każdego ε istnieje takie y, że
$$|x - y| < \varepsilon \quad \text{i} \quad \pi(y) = c_1$$

Przypadek najmniej łatwy wygląda tak:



Tego y należy szukać „nisko, po lewej stronie x".

Własności funkcji $\pi : (0,1) \xrightarrow{\text{na}} \mathcal{C}$

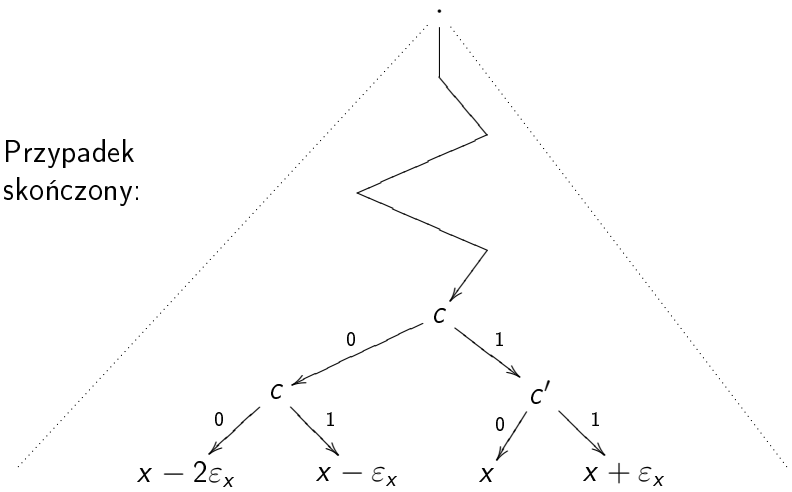
- Jeśli $\pi(x) \le c$, to dla każdego ε istnieje takie y, że
$$|x - y| < \varepsilon \quad \text{i} \quad \pi(y) = c$$

1) Jeśli $A \subseteq (0,1)$ otwarty, to $\pi(A)$ zamknięty w górę.

Dowód: Niech $x \in A$, $c_0 = \pi(x) \in \pi(A)$ i niech $c_0 \le c$.
Ponieważ A otwarty, więc $K(x,\varepsilon) \subseteq A$.
I mamy takie $y \in K(x,\varepsilon)$, że $\pi(y) = c$.
No to $c \in \pi(A)$.

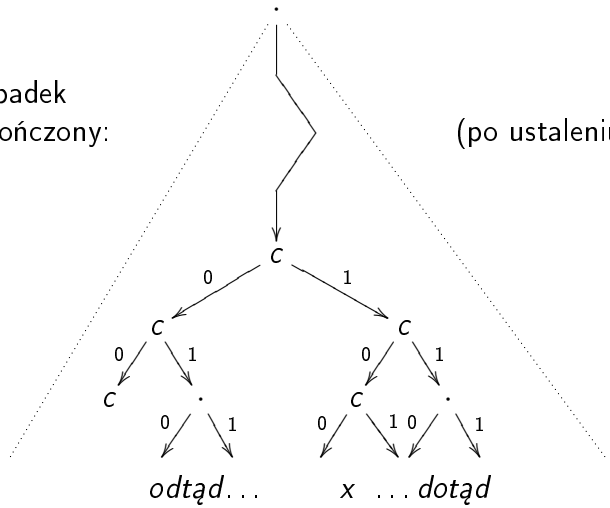
- Dla każdego $x \in (0,1)$ istnieje takie ε_x, że $\forall y \in (0,1).\, |x-y| < \varepsilon_x \to \pi(x) \leq \pi(y)$

Przypadek skończony:



- Dla każdego $x \in (0,1)$ istnieje takie ε_x, że $\forall y \in (0,1).\, |x-y| < \varepsilon_x \to \pi(x) \leq \pi(y)$

Przypadek nieskończony:



(po ustaleniu etykiety)

Udowodniliśmy...

- Dla każdego $x \in (0,1)$ istnieje takie ε_x, że $\forall y \in (0,1).\, |x-y| < \varepsilon_x \to \pi(x) \leq \pi(y)$

2. Jeśli $Z \subseteq \mathcal{C}$ zamknięty w górę, to $\pi^{-1}(Z)$ otwarty.

Dowód: Niech $x \in \pi^{-1}(Z)$, czyli $\pi(x) \in Z$.
Jest takie ε_x, że $K(x, \varepsilon_x) \subseteq \pi^{-1}(Z\uparrow)$.
Ale Z jest zamknięty w górę, więc $K(x, \varepsilon_x) \subseteq \pi^{-1}(Z)$.

Twierdzenie: *Jeśli formuła jest prawdziwa w algebrze otwartych podzbiorów odcinka* $(0,1)$*, to jest tautologią.*

Uwaga: ten sam dowód działa dla $\mathcal{O}(\mathbb{Q})$.

Powtórzenie z rachunku lambda

$$\Gamma, x{:}\tau \vdash M : \tau$$

$$\frac{\Gamma, x{:}\alpha \vdash M : \beta}{\Gamma \vdash \lambda x{:}\alpha\, M : \alpha \to \beta} \qquad \frac{\Gamma \vdash M : \alpha \to \beta \quad \Gamma \vdash N : \alpha}{\Gamma \vdash MN : \beta}$$

Powtórzenie z rachunku lambda: redukcje

Beta-redukcja:

$(\lambda x^{\tau}\, M^{\sigma})N^{\tau} \implies M[x := N] : \sigma.$

Eta-redukcja:

$\lambda x^{\tau}.\, M^{\tau\to\sigma} x \implies M : \tau \to \sigma$, gdy x nie jest wolne w M.

Notacja: $\to_{\beta}$, $\twoheadrightarrow_{\beta}$, $\to_{\eta}$, $\twoheadrightarrow_{\eta}$, $\to_{\beta\eta}$, $\twoheadrightarrow_{\beta\eta}$, $=_{\eta}$, $=_{\beta}$, $=_{\beta\eta}$

Logika intuicjonistyczna

Wykład 6

22 marca 2012

W poprzednim odcinku:

Beta-redukcja:

$(\lambda x^\tau\, M^\sigma)N^\tau \implies M[x := N] : \sigma.$

(*Najpierw wprowadzamy implikację* $\tau \to \sigma$,
potem ją eliminujemy do σ.)

Eta-redukcja:

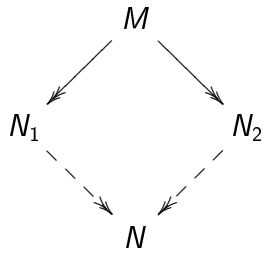
$\lambda x^\tau.\, M^{\tau\to\sigma} x \implies M : \tau \to \sigma$, gdy x nie jest wolne w M.

(*Najpierw eliminujemy implikację,*
potem ją wprowadzamy z powrotem.)

Postać normalna: term bez redeksów.

Twierdzenie Churcha-Rossera (CR)

Jeśli $M \twoheadrightarrow N_1$ *i* $M \twoheadrightarrow N_2$, *to jest* N, *że* $N_1 \twoheadrightarrow N$ *i* $N_2 \twoheadrightarrow N$.



Wniosek: *Jeśli term ma postać normalną, to tylko jedną.*

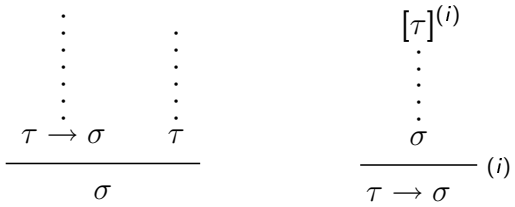
Poprawność redukcji

Subject Reduction Theorem:
Jeśli $\Gamma \vdash M : \sigma$ *oraz* $M \twoheadrightarrow_{\beta\eta} N$, *to* $\Gamma \vdash N : \sigma$.

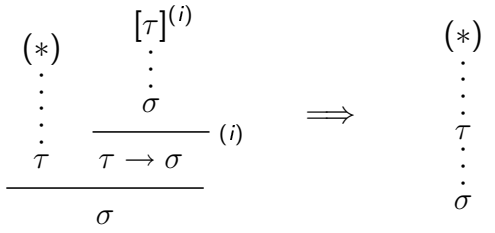
Dowód: Łatwy (ale w stylu Churcha).

Wniosek: *Normalizacja zachowuje typ.*

Tradycyjna notacja dla naturalnej dedukcji

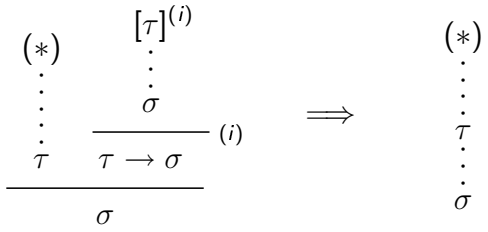


Normalizacja dowodu: implikacja



$$(\lambda x^{\tau}\, M^{\sigma})N^{\tau} \implies M[x := N] : \sigma.$$

Normalizacja dowodu: implikacja



Uwaga: Założenie $[\tau]^i$ może wystąpić w dowodzie wiele razy. Wtedy część $(*)$ występuje wielokrotnie po prawej i rozmiary dowodu rosną a nie maleją.

Pożytek z normalizacji: niesprzeczność

Definicja: Dowód *normalny* to dowód bez redeksów.

Twierdzenie: *Jeśli* $\vdash \varphi$, *to formuła* φ *ma dowód normalny.*

Wniosek (Niesprzeczność):
Nie każda formuła ma dowód (np. zmienna zdaniowa nie ma).

Silna normalizacja

Definicja: Term (dowód) M ma własność *silnej normalizacji* (jest *silnie normalizowalny*), gdy każdy ciąg redukcji tego termu prowadzi do postaci normalnej.

Przykład 1: Każdy term ma tę własność ze względu na η-redukcje. (Bo η-redukcja skraca termy.)

Przykład 2: Niech $\mathbf{K} = \lambda xy.\, x$ oraz $\mathbf{\Omega} = (\lambda x.\, xx)(\lambda x.\, xx)$. Term $\mathbf{K}x\mathbf{\Omega}$ ma postać β-normalną, ale nie jest silnie normalizowalny.

Notacja: $M \in \mathrm{SN}_\beta$, $M \in \mathrm{SN}_{\beta\eta}$.

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: *Podterm termu silnie normalizowalnego jest silnie normalizowalny.*

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) Wszystkie redukcje w termie $xN_1 \ldots N_k$ muszą być „wewnętrzne". Teza wynika od razu z założenia indukcyjnego.

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

Dowód: Przypadek (2) Jeśli $N \in \mathcal{S}$, to $\lambda x\, N \in \mathcal{S}$.

Jeśli wszystkie redukcje w $\lambda x\, N$ są wewnątrz N, to teza wynika z założenia indukcyjnego. Jedyna inna możliwość jest taka:

$$\lambda x\, N \twoheadrightarrow_{\beta\eta} \lambda x\, Px \to_{\eta} P \twoheadrightarrow_{\beta\eta} \cdots$$

gdzie $N \twoheadrightarrow_{\beta\eta} Px$. Ale wtedy $Px \in \mathrm{SN}_{\beta\eta}$ z założenia indukcyjnego, więc także $P \in \mathrm{SN}_{\beta\eta}$.

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 jego długość.

Przypadek 1: $M = (\lambda x\, P)QN_1 \ldots N_k$.
Wtedy $Q \in \mathcal{S}$ z założenia indukcyjnego
(drugi parametr mniejszy, pierwszy nie większy).

Także $P[x := Q]N_1 \ldots N_k \in \mathcal{S}$ (pierwszy parametr mniejszy).
Zatem oba te termy są w $\mathcal{S}$, skąd $M \in \mathcal{S}$.

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

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

Z założenia indukcyjnego $P, Q, N_1, \ldots, N_k \in \mathrm{SN}_{\beta\eta}$. Zatem redukcje wewnętrzne termu $M = (\lambda x\, P)QN_1 \ldots N_k$ muszą się skończyć. Jedyna inna możliwość jest taka:

$$M \twoheadrightarrow_{\beta\eta} (\lambda x\, P')Q'N_1' \ldots N_k' \to_{\beta} P'[x := Q']N_1' \ldots N_k' \twoheadrightarrow_{\beta\eta} \cdots$$

Ale $\mathrm{SN}_{\beta\eta} \ni P[x := Q]N_1 \ldots N_k \twoheadrightarrow_{\beta\eta} P'[x := Q']N_1' \ldots N_k'$, więc też $P'[x := Q']N_1' \ldots N_k' \in \mathrm{SN}_{\beta\eta}$.

Oczywiście: *Jeśli $M \in \mathrm{SN}_{\beta\eta}$, to $M \in \mathrm{SN}_{\beta}$.*

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 jego długość.

Przypadek 2: Term M nie jest postaci $(\lambda x\, P)QN_1 \ldots N_k$.
Wtedy teza wynika od razu z założenia indukcyjnego ze względu na drugi parametr.

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 jego długość.

Przypadek 1: $M = \lambda z\, N$.
Wtedy $M[x := P] = \lambda z\, N[x := P] \in \mathcal{S}$, z założenia indukcyjnego dla N (pierwszy parametr bez zmian, drugi nie większy, 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 jego długość.

Przypadek 2: $M = yN_1 \ldots N_k$.
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 jego długość.

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

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 jego długość.

Przypadek 4: $M = xQN_1 \ldots N_k$. Wtedy $M[x := P] = PQ[x{:=}P]N_1[x{:=}P] \ldots N_k[x{:=}P]$. Skoro $M \in \mathcal{S}$, to $M \in \mathrm{SN}$, więc także $Q, N_1 \ldots N_k \in \mathrm{SN}$, czyli $Q, N_1 \ldots N_k \in \mathcal{S}$. Z założenia indukcyjnego łatwo wynika $Q[x := P], N_1[x := P], \ldots, N_k[x := P] \in \mathcal{S}$.

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

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

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

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

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

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

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

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

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

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

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

Wniosek z normalizacji

Wniosek: *Jeśli $\Gamma \vdash \sigma$, to istnieje taki term M w postaci normalnej, że $\Gamma \vdash M : \sigma$.*

Dowód: Bo normalizacja zachowuje typ.

Morał: Wystarczy szukać dowodu normalnego.

Długa postać normalna

Definicja:

- If x is a variable of type $\tau_1 \to \cdots \to \tau_n \to p$, and $M_1^{\tau_1}, \ldots, M_n^{\tau_n}$ are in long normal form, then $(xM_1 \ldots M_n)^p$ is in long normal form.
- If M^σ is in long normal form then so is $(\lambda x{:}\tau.\, M)^{\tau\to\sigma}$.

Lemat:
Jeśli $\Gamma \vdash \sigma$, to $\Gamma \vdash M : \sigma$, gdzie M to długa postać normalna.

Dowód: Postać normalną można „wydłużyć”,
na przykład zamiast $x^{\sigma\to\tau}$ bierzemy $\lambda y{:}\sigma.xy$.

Przykład: prawo Peirce'a

Fakt: *Prawo Peirce'a* $\pi = ((p \to q) \to p) \to p$
nie jest twierdzeniem intuicjonistycznym.

Dowód: Jeśli $\vdash M : \pi$ i M jest w długiej postaci normalnej, to $M = \lambda x\, N$, gdzie $x : (p \to q) \to p \vdash N : p$.

Wtedy $N = xP$, gdzie $x : (p \to q) \to p \vdash P : p \to q$.

Dalej $P = \lambda y\, Q$, przy czym $x : (p \to q) \to p, y : p \vdash Q : q$, a to niemożliwe.

The inhabitation problem

Inhabitation problem:

Given Γ, τ, is there M such that $\Gamma \vdash M : \tau$?

Theorem (R. Statman):

Inhabitation in simple types is PSPACE*-complete.*

Basic lemmas:

- An inhabited type has a long normal inhabitant.
- If $\Gamma(x) = \rho$ and $\Gamma(y : \rho) \vdash M : \tau$ then $\Gamma \vdash M[y := x] : \tau$.

Searching for long normal forms

The Wajsberg/Ben-Yelles algorithm:

To answer $\Gamma \vdash ? : \alpha$, apply one of the following tactics:

- For $\alpha = \beta \to \gamma$, ask $\Gamma \cup \{x : \beta\} \vdash ? : \gamma$ (fresh x).

  (Solution $M = \lambda x{:}\beta.\, N^\gamma$.)

- For $\alpha = p$, choose $x : \beta_1 \to \cdots \to \beta_k \to p$ from Γ, then ask $\Gamma \vdash ? : \beta_i$, for all i. Success if $k = 0$.

  (Solution $M = xN_1^{\beta_1} \ldots N_k^{\beta_k}$.)

Alternation

- A solution of $\Gamma \vdash ? : p$ is of the form $M = xN_1^{\beta_1} \dots N_k^{\beta_k}$, for some $x : \beta_1 \to \dots \to \beta_k \to p$ in Γ.
- Nondeterminism: because there can be more than one x.
- Alternation (recursion): because $\Gamma \vdash N_i : \beta_i$ must be solved in parallel.

Termination

- The question $\Gamma \vdash ? : \beta \to \gamma$ leads to $\Gamma \cup \{x{:}\beta\} \vdash ? : \gamma$. The environment Γ is extended by $x : \beta$.
- Every such β is a subformula in the initial problem (there is only a linear number of types).
- New variables can be replaced by old ones, i.e., Γ must in fact stabilize (in polynomial time).

Complexity: Alternating Ptime, i.e., Pspace

Logika intuicjonistyczna

Wykład 7

29 marca 2012

Klasyczny rachunek zdań drugiego rzędu (QBF)

Składnia:

- Zmienne zdaniowe $p, q, r, \ldots$ są formułami;
- Jeśli α i β są formułami,
  to $\neg\alpha$, $\alpha \vee \beta$ 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.

QBF: semantyka

Wartość $[\![\varphi]\!]_\rho$ formuły φ przy danym wartościowaniu ρ definiuje się podobnie jak w klasycznym rachunku zdań, przyjmując dodatkowo, że

$$[\![\forall p\, \alpha]\!]_\rho = \min\{[\![\alpha]\!]_{\rho[p\mapsto 1]}, [\![\alpha]\!]_{\rho[p\mapsto 0]}\}$$
$$[\![\exists p\, \alpha]\!]_\rho = \max\{[\![\alpha]\!]_{\rho[p\mapsto 1]}, [\![\alpha]\!]_{\rho[p\mapsto 0]}\}$$

Tautologią (zdaniową drugiego rzędu) nazywamy formułę prawdziwą przy każdym wartościowaniu.

Na przykład $\exists p(\neg q \vee p)$ jest tautologią.

Powtórzenie z teorii złożoności

Problem QBF:

Czy dana zdaniowa formuła drugiego rzędu jest tautologią?

Twierdzenie: *Problem* QBF *jest* PSPACE*-zupełny.*

PSPACE-trudność problemu inhabitacji

Redukujemy problem QBF do problemu inhabitacji.

Niech Φ będzie formułą w języku QBF.
Bez straty ogólności możemy założyć, że

- Formuła Φ jest zdaniem (nie ma zmiennych wolnych);
- Negacja występuje w Φ tylko w kontekstach $\neg p$;
- Wszystkie zmienne związane w Φ są różne i nie są wolne.

Zmienne typowe potrzebne:

- s_p i $s_{\neg p}$ dla każdej zmiennej p w formule Φ;
- s_φ i $s_{\neg\varphi}$, dla każdej podformuły φ formuły Φ.

Kodowanie (w LOGSPACE)

Zbiór formuł Γ_Φ:

- $(s_p \to s_\psi) \to (s_{\neg p} \to s_\psi) \to s_\varphi$, dla $\varphi = \forall p\psi$;
- $(s_p \to s_\psi) \to s_\varphi$ i $(s_{\neg p} \to s_\psi) \to s_\varphi$, dla $\varphi = \exists p\psi$;
- $s_\psi \to s_\vartheta \to s_\varphi$, dla $\varphi = \psi \wedge \vartheta$;
- $s_\psi \to s_\varphi$ i $s_\vartheta \to s_\varphi$, dla $\varphi = \psi \vee \vartheta$.

Dla częściowego wartościowania v, zbiór Γ_v to Γ_Φ plus:

- s_p, gdy $v(p) = 1$;
- $s_{\neg p}$, gdy $v(p) = 0$,

Główny lemat:

Jeśli v jest określone na zmiennych wolnych formuły φ (i nie jest określone na związanych), to:

$\Gamma_v \vdash s_\varphi$ *wtedy i tylko wtedy, gdy* $[\![\varphi]\!]_v = 1$.

Morał: Formuła Φ jest prawdziwa wtw, gdy $\Gamma_\Phi \vdash s_\Phi$.

(Uwaga: $\Gamma_\Phi \vdash s_\Phi$ to to samo co $\gamma_1 \to \cdots \to \gamma_n \to s_\Phi$ dla odpowiednich γ_i.)

Lemat: $\Gamma_v \vdash s_\varphi \quad \Leftrightarrow \quad [\![\varphi]\!]_v = 1.$

Dowód: jest przez indukcję ze względu na φ.

Przypadek $\varphi = p$: Jeśli $\Gamma_v \vdash s_p$, to istnieje term M w długiej postaci normalnej, który jest typu s_p w Γ_v. Na to jest tylko jeden sposób: typ s_p musi być w Γ_v (żaden inny nie pasuje). Zatem $v(p) = 1$. W przeciwną stronę teza oczywista.

Przypadek $\varphi = \neg p$: analogiczny.

Lemat: $\Gamma_v \vdash s_\varphi \quad \Leftrightarrow \quad [\![\varphi]\!]_v = 1.$

Dowód: Indukcja ze względu na φ.

Przypadek $\varphi = \psi \wedge \vartheta$: Wtedy w Γ_v jest $x : s_\psi \to s_\vartheta \to s_\varphi$.
Jeśli $\Gamma_v \vdash s_\varphi$, to istnieje term M tego typu w długiej postaci normalnej. Jedyna możliwość $M = xM_1^{s_\psi} M_2^{s_\vartheta}$. Zatem $\Gamma_v \vdash s_\psi$ i $\Gamma_v \vdash s_\vartheta$ i stosujemy indukcję.
Na odwrót, jeśli $[\![\varphi]\!]_v = 1$, to $[\![\psi]\!]_v = [\![\varphi]\!]_v = 1$ i z zał. ind. mamy $\Gamma_v \vdash P : s_\psi$ oraz $\Gamma_v \vdash Q : s_\vartheta$. No to $\Gamma_v \vdash xPQ : s_\varphi$.

Lemat: $\Gamma_v \vdash s_\varphi \quad \Leftrightarrow \quad [\![\varphi]\!]_v = 1.$

Dowód: Indukcja ze względu na φ.

Przypadek $\varphi = \forall p \psi$, $(x : (s_p \to s_\psi) \to (s_{\neg p} \to s_\psi) \to s_\varphi) \in \Gamma_v$.
Jeśli $\Gamma_v \vdash s_\varphi$, to $\Gamma_v \vdash s_{\neg p} \to s_\psi$ oraz $\Gamma_v \vdash s_p \to s_\psi$, czyli $\Gamma_v, s_{\neg p} \vdash s_\psi$ oraz $\Gamma_v, s_p \vdash s_\psi$. Ponieważ $v(p)$ jest nieokreślone, więc mamy w istocie $\Gamma_{v_0} \vdash s_\psi$ oraz $\Gamma_{v_1} \vdash s_\psi$, dla wartościwań $v_0 = v[p \mapsto 0]$ i $v_1 = v[p \mapsto 1]$. Zatem $[\![\psi]\!]_{v_0} = [\![\psi]\!]_{v_1} = 1$, skąd $[\![\varphi]\!]_v = [\![\forall p \psi]\!]_v = 1$.
Na odwrót, jeśli $[\![\varphi]\!]_v = 1$, to $[\![\psi]\!]_{v_0} = [\![\psi]\!]_{v_1} = 1$, dla v_0, v_1 jak wyżej, skąd $\Gamma_{v_0} \vdash s_\psi$ oraz $\Gamma_{v_1} \vdash s_\psi$. To znaczy znowu, że $\Gamma_v, z : s_{\neg p} \vdash P : s_\psi$ oraz $\Gamma_v, y : s_p \vdash Q : s_\psi$, skąd wreszcie $\Gamma_v \vdash x(\lambda y\, Q)(\lambda z\, P) : s_\varphi$.

Lemat: $\Gamma_v \vdash s_\varphi \quad \Leftrightarrow \quad [\![\varphi]\!]_v = 1.$

Dowód: Indukcja ze względu na φ.

Przypadek $\varphi = \exists p\, \psi$. Wtedy w Γ_v są dwie deklaracje
$x : (s_p \to s_\psi) \to s_\varphi$ oraz $y : (s_{\neg p} \to s_\psi) \to s_\varphi$

Jeśli $\Gamma_v \vdash s_\varphi$, to $\Gamma_v \vdash s_{\neg p} \to s_\psi$, lub $\Gamma_v \vdash s_p \to s_\psi$, czyli albo $\Gamma_v, s_{\neg p} \vdash s_\psi$ albo $\Gamma_v, s_p \vdash s_\psi$. To znowu oznacza, że $\Gamma_{v_0} \vdash s_\psi$ lub $\Gamma_{v_1} \vdash s_\psi$, dla odpowiednich v_0, v_1 (bo $v(p)$ nieokreślone). Stosujemy indukcję jak poprzednio.

Na odwrót też podobnie.

Ben-Yelles algorithm

To answer $\Gamma \vdash ? : \alpha$, apply one of the following tactics:

- For $\alpha = \beta \to \gamma$, ask $\Gamma \cup \{x : \beta\} \vdash ? : \gamma$ (fresh x). (Solution $M = \lambda x{:}\beta.\, N^{\gamma}$.)
- For $\alpha = p$, choose $x : \beta_1 \to \cdots \to \beta_k \to p$ from Γ, then ask $\Gamma \vdash ? : \beta_i$, for all i. Success if $k = 0$. (Solution $M = xN_1^{\beta_1} \ldots N_k^{\beta_k}$.)

Ten alternujący proces można objaśniać jako grę między graczem $\exists$ (który dowodzi twierdzenia) i graczem $\forall$ (który wyszukuje trudne przypadki). Rozwiązanie istnieje wtedy i tylko wtedy, gdy gracz $\exists$ ma strategię.

Przykład (nieformalny): $(p \to \neg q) \to (\neg p \to \neg q) \to \neg q$

(*Assumptions:* $x : p \to \neg q$, $y : \neg p \to \neg q$, $z : q$. *Goal:* $\bot$)

Opponent ($\forall$): *Can you prove* $\bot$ *?*

Player ($\exists$): *I will use assumption* y *!*

Opponent ($\forall$): *Can you prove the 1st assumption* $\neg p$ *? That is, can you prove* $\bot$ *using an asumption* $v : p$ *?*

Player ($\exists$): *Yes, I will use assumption* x *!*

Opponent ($\forall$): *Can you prove the 2nd assumption* q *?*

Player ($\exists$): *Sure, take* z *!*

Proof = strategy = inhabitant: $\lambda xyz.\, y(\lambda v.\, xvz)z$

Another game: $\neg\neg(p \vee \neg p)$

$\forall$: $(p \vee \neg p) \to \bot \vdash \bot$?

$\exists$: $(p \vee \neg p) \to \bot \vdash p \vee \neg p$!

$\forall$: ?

$\exists$: $(p \vee \neg p) \to \bot \vdash \neg p$!

$\forall$: $(p \vee \neg p) \to \bot, p \vdash \bot$?

$\exists$: $(p \vee \neg p) \to \bot, p \vdash p \vee \neg p$!

$\forall$: ?!

$\exists$: $(p \vee \neg p) \to \bot, p \vdash p$!

Wnioskowanie w stylu Hilberta

Dowód w stylu Hilberta to ciąg formuł, w którym występują:

- Aksjomaty;
- Formuły otrzymane z wcześniejszych za pomocą reguł;
- Wolne założenia.

Piszemy $\Gamma \vdash \alpha$, gdy istnieje dowód kończący się formułą α, z wolnymi założeniami ze zbioru Γ.

Wnioskowanie w stylu Hilberta

Reguła *modus ponens*: $\dfrac{A \to B \quad A}{B}$

Aksjomaty implikacyjne: wszystkie formuły postaci:

K: $\alpha \to (\beta \to \alpha)$

S: $(\alpha \to \beta \to \gamma) \to (\alpha \to \beta) \to \alpha \to \gamma$

Dla logiki klasycznej dodatkowo:

P: $((\alpha \to \beta) \to \alpha) \to \alpha$.

Przykład: dowód formuły $\varphi \to \varphi$

1. $(\varphi \to (\psi \to \varphi) \to \varphi) \to (\varphi \to \psi \to \varphi) \to \varphi \to \varphi$
   (aksjomat **S**);
2. $\varphi \to (\psi \to \varphi) \to \varphi$
   (aksjomat **K**);
3. $(\varphi \to \psi \to \varphi) \to \varphi \to \varphi$
   (odrywanie 2 od 1);
4. $\varphi \to \psi \to \varphi$
   (aksjomat **K**);
5. $\varphi \to \varphi$
   (odrywanie 4 od 3).

Twierdzenie o dedukcji

Twierdzenie o dedukcji: Jeśli $\Gamma, \alpha \vdash \beta$, to $\Gamma \vdash \alpha \to \beta$.

Dowód: Indukcja ze względu na dowód $\Gamma, \alpha \vdash \beta$.

Przypadek 1: Jeśli założenie α nie jest użyte w dowodzie, to faktycznie $\Gamma \vdash \beta$. Aksjomat **K** w postaci $\beta \to \alpha \to \beta$ daje $\alpha \to \beta$ przez odrywanie.

Przypadek 2: Jeśli cały dowód polega na przywołaniu założenia α, to z poprzedniego przykładu mamy $\vdash \alpha \to \alpha$. Tym bardziej $\Gamma \vdash \alpha \to \alpha$.

Twierdzenie o dedukcji

Twierdzenie o dedukcji: Jeśli $\Gamma, \alpha \vdash \beta$, to $\Gamma \vdash \alpha \to \beta$.

Dowód: Indukcja ze względu na dowód $\Gamma, \alpha \vdash \beta$.

Przypadek 3: Jeśli $\Gamma, \alpha \vdash \beta$ uzyskano przez odrywanie, to dla pewnego γ są krótsze dowody:

$$\Gamma, \alpha \vdash \gamma \quad \text{oraz} \quad \Gamma, \alpha \vdash \gamma \to \beta.$$

Z założenia indukcyjnego

$$\Gamma \vdash \alpha \to \gamma \quad \text{oraz} \quad \Gamma \vdash \alpha \to \gamma \to \beta.$$

Stosujemy dwa razy odrywanie od aksjomatu

$$\mathbf{S} : (\alpha \to \gamma \to \beta) \to (\alpha \to \gamma) \to \alpha \to \beta.$$

Rachunek kombinatorów (z typami prostymi)

Składnia:

- Stałe $\mathsf{K}_{\alpha\beta}$ typu $\alpha \to (\beta \to \alpha)$;
- Stałe $\mathsf{S}_{\alpha\beta\gamma}$ typu $(\alpha \to \beta \to \gamma) \to (\alpha \to \beta) \to \alpha \to \gamma$;
- Zmienne (odpowiadające wolnym założeniom);
- Aplikacja (odp. modus ponens).

Alternatywna konwencja: dwie polimorficzne stałe K i S.

Redukcja w rachunku kombinatorów

- $\mathsf{K}AB \to_w A$ dla dowolnych A, B;
- $\mathsf{S}ABC \to_w AC(BC)$ dla dowolnych A, B, C;
- Jeśli $A \to_w B$, to $AC \to_w BC$ oraz $CA \to_w CB$.

Własności: Church-Rosser, poprawność redukcji, silna normalizacja (dla termów z typami).

Przykład

- $\mathsf{I} = \mathsf{SKK}$

  $\mathsf{I}F \to_w \mathsf{K}F(\mathsf{K}F) \to_w F$

Przypomnijmy ten dowód:

1. $\mathsf{S} : (\varphi \to (\psi \to \varphi) \to \varphi) \to (\varphi \to \psi \to \varphi) \to \varphi \to \varphi$;
2. $\mathsf{K} : \varphi \to (\psi \to \varphi) \to \varphi$;
3. $\mathsf{SK} : (\varphi \to \psi \to \varphi) \to \varphi \to \varphi$;
4. $\mathsf{K} : \varphi \to \psi \to \varphi$;
5. $\mathsf{SKK} : \varphi \to \varphi$.

Przykłady

- $\mathsf{W} = \mathsf{SS}(\mathsf{KI}) : (\alpha \to \alpha \to \beta) \to \alpha \to \beta$

  $\mathsf{W}FG \to_w \mathsf{S}F(\mathsf{KI}F)G \to_w \mathsf{S}F\mathsf{I}G \to_w FG(\mathsf{I}G) \twoheadrightarrow_w FGG$

- $\mathsf{B} = \mathsf{S}(\mathsf{KS})\mathsf{K} : (\alpha \to \beta) \to (\gamma \to \alpha) \to \gamma \to \beta$

  $\mathsf{B}FGH \to_w \mathsf{KS}F(\mathsf{K}F)GH \to_w \mathsf{S}(\mathsf{K}F)GH \to_w$
  $\to_w \mathsf{K}FH(GH) \to_w F(GH)$

- $\mathsf{C} = \mathsf{S}(\mathsf{BBS})(\mathsf{KK}) : (\alpha \to \beta \to \gamma) \to \beta \to \alpha \to \gamma$

  $\mathsf{C}FGH \twoheadrightarrow_w FHG$

- $\mathsf{B}' = \mathsf{CB} : (\alpha \to \beta) \to (\beta \to \gamma) \to \alpha \to \gamma$

  $\mathsf{B}'FGH \twoheadrightarrow_w G(FH)$

Remark: Each of those can be added as a new constant.

Przykłady

- $\mathbf{0} = \mathbf{KI}$ $\quad \mathbf{0}FG \twoheadrightarrow_w G$
- $\mathbf{1} = \mathbf{SB}(\mathbf{KI})$ $\quad \mathbf{1}FG \twoheadrightarrow_w FG$
- $\mathbf{2} = \mathbf{SB}(\mathbf{SB}(\mathbf{KI}))$ $\quad \mathbf{2}FG \twoheadrightarrow_w F(FG)$

From lambda to CL: combinatory abstraction

- $\lambda^* x.F = \mathbf{K}F$, when $x \notin \mathrm{FV}(F)$;
- $\lambda^* x.x = \mathbf{I}$;
- $\lambda^* x.FG = \mathbf{S}(\lambda^* x.F)(\lambda^* x.G)$, otherwise.

Fact: $(\lambda^* x.F)G \twoheadrightarrow_w F[x := G]$.

Fact: $(\lambda^* x.F)G \twoheadrightarrow_w F[x := G]$

Przypadek 1: Jeśli $x \notin \mathrm{FV}(F)$, to
$(\lambda^* x.F)G = \mathbf{K}FG \rightarrow_w F = F[x := G]$.

Przypadek 2: Jeśli $F = x$, to
$(\lambda^* x.F)G = \mathbf{I}G \twoheadrightarrow_w G = x[x := G]$.

Przypadek 3: Jeśli $F = F'F''$, to

$$(\lambda^* x.F)G = \mathbf{S}(\lambda^* x.F')(\lambda^* x.F'')G \rightarrow_w$$
$$\rightarrow_w (\lambda^* x.F')G((\lambda^* x.F'')G) \twoheadrightarrow_w F'[x := G]F''[x := G].$$

Kombinatoryczna abstrakcja z typami

Kombinatoryczna abstrakcja:
Jeśli $\Gamma, x : \alpha \vdash M : \beta$, to $\Gamma \vdash \lambda^* x.\, M : \alpha \rightarrow \beta$.

Co nam to przypomina?

Twierdzenie o dedukcji: Jeśli $\Gamma, \alpha \vdash \beta$, to $\Gamma \vdash \alpha \rightarrow \beta$.

Porównanie

Jeśli $\Gamma, \alpha \vdash \beta$, to $\Gamma \vdash \alpha \to \beta$.

Jeśli $\Gamma, x : \alpha \vdash M : \beta$, to $\Gamma \vdash \lambda^* x.\, M : \alpha \to \beta$.

Przypadek 1: Jeśli założenie α nie jest użyte w dowodzie, to $\Gamma \vdash \beta$. Odrywamy α od $\mathsf{K} : \beta \to \alpha \to \beta$, co daje $\alpha \to \beta$.

$\lambda^* x.\, F = \mathsf{K}F$, gdy $x \notin \mathrm{FV}(F)$;

Logika intuicjonistyczna

Wykład 8

5 kwietnia 2012

Przykłady implikacyjnych logik zdaniowych

- Logika intuicjonistyczna:
  - **K** : $\alpha \to (\beta \to \alpha)$;
  - **S** : $(\alpha \to \beta \to \gamma) \to (\alpha \to \beta) \to \alpha \to \gamma$.

  (PSPACE-zupełna)
- Logika klasyczna: schematy **K**, **S**, oraz:
  - **P** : $((\alpha \to \beta) \to \alpha) \to \alpha$

  (co-NP-zupełna)

Przykłady implikacyjnych logik zdaniowych

- Logika relewantna: schematy **S**, **I**, oraz:
  - **B** : $(\alpha \to \beta) \to (\gamma \to \alpha) \to \gamma \to \beta$;
  - **C** : $(\alpha \to \beta \to \gamma) \to \beta \to \alpha \to \gamma$.
- „Ticket entailment": schematy **B**, **B'**, **I**, **W**:
  - **B′** : $(\alpha \to \beta) \to (\beta \to \gamma) \to \alpha \to \gamma$;
  - **W** : $(\alpha \to \alpha \to \beta) \to \alpha \to \beta$.

  (Pomiędzy Exptime i Ackermannem)
- Logiki **BCK** i **BCI**: schematy **B**,**C**,**K** (**B**,**C**,**I**) – są w NP.

Jak trudny jest rachunek zdań

Problem wnioskowania w rachunku zdań:
Czy dana formuła (implikacyjnego) rachunku zdań jest konsekwencją danych schematów aksjomatów?

Twierdzenie (Linial, Post, 1949):
Problem wnioskowania w rachunku zdań jest nierozstrzygalny.

Automat dwulicznikowy: $\mathcal{A} = \langle Q, q_0, q_f, \delta \rangle$

- Q – skończony zbiór stanów;
- q_0 – stan początkowy;
- q_f – stan końcowy;
- δ – funkcja przejścia, $\mathrm{Dom}(f) = Q - \{q_f\}$;
- $\delta(q)$ jest jednej z postaci ($i = 1, 2$):
  - „$c_i := c_i + 1$; goto p";
  - „$c_i := c_i - 1$; goto p";
  - „if $c_i = 0$ then goto p else goto r".

Automat dwulicznikowy

Konfiguracja automatu: trójka $\mathcal{C} = \langle q, n_1, n_2 \rangle$.

Zmiana konfiguracji: $\mathcal{C} \to \mathcal{C}'$, gdzie $\mathcal{C}'$ zależy od $\delta(q)$:

- Jeśli $\delta(q) =$ „$c_1 := c_1 + 1$; goto p",
  to $\mathcal{C}' = \langle p, n_1 + 1, n_2 \rangle$;
- Jeśli $\delta(q) =$ „$c_1 := c_1 - 1$; goto p", oraz $n_1 > 0$,
  to $\mathcal{C}' = \langle p, n_1 - 1, n_2 \rangle$ (wpp. nieokreślone);
- Jeśli $\delta(q) =$ „if $c_1 = 0$ then goto p else goto r", to
  - $\mathcal{C}' = \langle p, n_1, n_2 \rangle$, w przypadku $n_1 = 0$;
  - $\mathcal{C}' = \langle r, n_1, n_2 \rangle$,w przypadku $n_1 \neq 0$.
- Dla instrukcji dotyczących c_2 – analogicznie.

Automat dwulicznikowy

Automat *akceptuje* konfigurację $\mathcal{C}$, jeżeli istnieje ciąg przejść

$$\mathcal{C} \to \mathcal{C}_1 \to \mathcal{C}_2 \to \cdots \to \mathcal{C}_n$$

do konfiguracji ze stanem końcowym.

Problem stopu:
Dany automat $\mathcal{A}$ i konfiguracja $\mathcal{C}$, czy $\mathcal{A}$ akceptuje $\mathcal{C}$?

Twierdzenie 1: *Problem stopu jest nierozstrzygalny.*

Twierdzenie 2: *Istnieje taki automat $\mathcal{A}$, że problem stopu jest nierozstrzygalny przy ustalonym $\mathcal{A}$.*

Definicje pomocnicze

$$\tau_n(\alpha) = \alpha^{n-1} \to \alpha = \underbrace{\alpha \to \cdots \to \alpha}_{n-1} \to \alpha.$$

$$\sigma(\alpha) = (\alpha \to \alpha) \to \alpha$$

Fakt: *Typy $\tau_n(\alpha)$ dla $n \neq m$ są „nieunifikowalne":*
dla każdych α, β i każdego podstawienia S zachodzi

$$S(\tau_n(\alpha)) \neq S(\tau_m(\beta)).$$

Fakt: *Typ $\sigma(\alpha)$* jest nieunifikowalny ze wszystkimi typami postaci $\tau_n(\beta)$: $S(\sigma(\alpha)) \neq S(\tau_n(\beta))$, dla wszystkich S, α, β.

Konwencja: Stany automatu to liczby od 4 do F,
przy czym $q_0 = 4$ i $q_f = F$.

Kodowanie konfiguracji

Kodem liczby n jest dowolna formuła postaci:

$$\tau_2(\alpha_1) \to \cdots \to \tau_2(\alpha_n) \to \tau_3(\beta),$$

czyli postaci

$$(\alpha_1 \to \alpha_1) \to \cdots \to (\alpha_n \to \alpha_n) \to (\beta \to \beta \to \beta).$$

Kodem stanu q jest dowolna formuła postaci $\tau_q(\alpha)$.

Kodem $\mathcal{C} = \langle q, n_1, n_2 \rangle$ jest dowolna formuła postaci

$$kod(q) \to kod(n_1) \to kod(n_2) \to \sigma(\xi).$$

Rachunek zdań określony przez automat

Dla każdej instrukcji $\delta(q)$ przyjmujemy jeden lub dwa schematy aksjomatów:

- Dla $\delta(q) =$ „$c_1 := c_1 + 1$; goto p”:

$[\tau_p(\alpha) \to (\tau_2(\varepsilon) \to \beta) \to \gamma \to \sigma(\xi)] \to [\tau_q(\alpha) \to \beta \to \gamma \to \sigma(\xi)]$;

- Dla $\delta(q) =$ „$c_1 := c_1 - 1$; goto p”:

$[\tau_p(\alpha) \to \beta \to \gamma \to \sigma(\xi)] \to [\tau_q(\alpha) \to (\tau_2(\varepsilon) \to \beta) \to \gamma \to \sigma(\xi)]$;

- Dla $\delta(q) =$ „if $c_1 = 0$ then goto p else goto r”:

$[\tau_p(\alpha) \to \tau_3(\beta) \to \gamma \to \sigma(\xi)] \to [\tau_q(\alpha) \to \tau_3(\beta) \to \gamma \to \sigma(\xi)]$,

$[\tau_r(\alpha) \to (\tau_2(\varepsilon) \to \beta) \to \gamma \to \sigma(\xi)] \to [\tau_q(\alpha) \to (\tau_2(\varepsilon) \to \beta) \to \gamma \to \sigma(\xi)]$.

- Dla instrukcji dotyczących c_2 – analogicznie.
- Na koniec jeszcze schemat $\tau_F(\alpha) \to \beta \to \gamma \to \sigma(\xi)$.

Główny lemat

Dla dowolnej konfiguracji $\mathcal{C} = \langle q, n_1, n_2 \rangle$ *i dowolnej formuły* φ, *która jest kodem* $\mathcal{C}$, *następujące warunki są równoważne:*

- *Automat* $\mathcal{A}$ *akceptuje konfigurację* $\mathcal{C}$;
- *Formuła* φ *ma dowód w rachunku zdań automatu* $\mathcal{A}$.

Dowód: Indukcja:

($\Downarrow$) ze względu na długość obliczenia;

($\Uparrow$) ze względu na długość dowodu.

Dowód – przykładowy krok indukcji

Jeśli $\mathcal{A}$ *akceptuje konfigurację* $\mathcal{C} = \langle q, n_1, n_2 \rangle$, *oraz* ψ_1 *i* ψ_2 *są kodami* n_1 *i* n_2, *to* $\tau_q(\alpha) \to \psi_1 \to \psi_2 \to \sigma(\xi)$ *ma dowód*

Niech $\mathcal{C} \to \mathcal{C}' = \langle p, n_1, n_2 + 1 \rangle$ wkutek wykonania instrukcji $\delta(q) =$ „$c_2 := c_2 + 1$; goto p”. Wtedy mamy taki aksjomat:

$[\tau_p(\alpha) \to \psi_1 \to (\tau_2(\varepsilon) \to \psi_2) \to \sigma(\xi)] \to [\tau_q(\alpha) \to \psi_1 \to \psi_2 \to \sigma(\xi)]$.

Formuła $\tau_p(\alpha) \to \psi_1 \to (\tau_2(\varepsilon) \to \psi_2) \to \sigma(\xi)$ jest kodem $\mathcal{C}'$, więc ma dowód z założenia indukcyjnego.

Zatem $\tau_q(\alpha) \to \psi_1 \to \psi_2 \to \sigma(\xi)$ otrzymamy przez odrywanie.

Dowód – przykładowy krok indukcji

Jeśli ψ_1 i ψ_2 są kodami n_1 i n_2, oraz $\tau_q(\alpha) \to \psi_1 \to \psi_2 \to \sigma(\xi)$ ma dowód, to $\mathcal{A}$ akceptuje konfigurację $\mathcal{C} = \langle q, n_1, n_2 \rangle$.

Jeśli $q \neq F$, to dowód formuły $\tau_q(\alpha) \to \psi_1 \to \psi_2 \to \sigma(\xi)$ polega na zastosowaniu modus ponens do aksjomatu, np.

$[\tau_p(\alpha) \to \tau_3(\beta) \to \gamma \to \sigma(\xi)] \to [\tau_q(\alpha) \to \tau_3(\beta) \to \gamma \to \sigma(\xi)]$,

Wtedy „oczywiście" $\psi_1 = \tau_3(\beta)$ i $\psi_2 = \gamma$, czyli test na zero jest poprawny. Zatem $\mathcal{C} \to \mathcal{C}' = \langle p, n_1, n_2 \rangle$. Formuła $[\tau_p(\alpha) \to \tau_3(\beta) \to \gamma \to \sigma(\xi)]$ ma dowód (krótszy) i jest kodem $\mathcal{C}'$. Z założenia indukcyjnego automat akceptuje $\mathcal{C}'$ a więc i $\mathcal{C}$.

Uwaga: Z powodu nieunifikowalności nie da się uzyskać kodu konfiguracji przez kilkakrotne odrywanie od aksjomatu (4 przypadki do sprawdzenia ręcznie).

Rozszerzony rachunek λ

$$\frac{\Gamma \vdash M : \alpha \quad \Gamma \vdash N : \beta}{\Gamma \vdash \langle M, N \rangle : \alpha \wedge \beta} \qquad \frac{\Gamma \vdash M : \alpha_1 \wedge \alpha_2}{\Gamma \vdash M\{i\} : \alpha_i}$$

Koniunkcja to produkt.

Rozszerzony rachunek λ

$$\frac{\Gamma \vdash M : \alpha_i}{\Gamma \vdash \mathsf{in}_i(M) : \alpha_1 \vee \alpha_2}$$

$$\frac{\Gamma \vdash M : \alpha \vee \beta \quad \Gamma, u{:}\alpha \vdash R : \tau \quad \Gamma, v{:}\beta \vdash Q : \tau}{\Gamma \vdash \mathsf{case}\ M\ \mathsf{of}\ [u]R\ \mathsf{or}\ [v]Q : \tau}$$

Alternatywa to koprodukt.

Rozszerzony rachunek λ

$$\frac{\Gamma \vdash M{:}\bot}{\Gamma \vdash \varepsilon_\tau(M) : \tau}$$

Absurd to typ pusty.

Ładna eliminacja

Konkluzja eliminacji jest podformułą głównej przesłanki:

$$\frac{\Gamma \vdash M : \alpha \to \beta \quad \Gamma \vdash N : \alpha}{\Gamma \vdash MN : \beta} \qquad \frac{\Gamma \vdash M : \alpha_1 \wedge \alpha_2}{\Gamma \vdash M\{i\} : \alpha_i}$$

Brzydka eliminacja

Konkluzja eliminacji nie jest podformułą głównej przesłanki:

$$\frac{\Gamma \vdash M : \alpha \vee \beta \quad \Gamma, u{:}\alpha \vdash R : \tau \quad \Gamma, v{:}\beta \vdash Q : \tau}{\Gamma \vdash \text{case } M \text{ of } [u]R \text{ or } [v]Q : \tau}$$

$$\frac{\Gamma \vdash M{:}\bot}{\Gamma \vdash \varepsilon_\tau(M) : \tau}$$

Beta-redukcja

Beta-redeks to eliminacja spójnika zastosowana bezpośrednio po jego wprowadzeniu. *Beta-redukcja* to „upraszcza”:

($\to$) $(\lambda x^\tau M^\sigma)N^\tau \implies M[x := N] : \sigma.$

($\wedge$) $\langle M^\tau, N^\sigma\rangle\{1\} \implies M : \tau, \qquad \langle M^\tau, N^\sigma\rangle\{2\} \implies N : \sigma.$

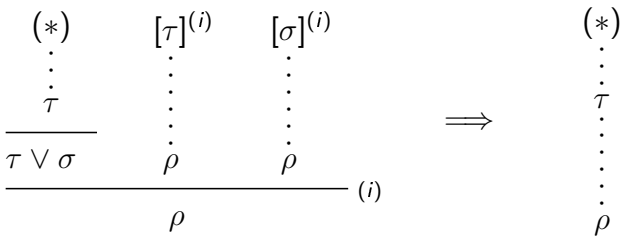
($\vee$) $\textbf{case } \textbf{in}_1\,(P)^{\tau\vee\sigma} \textbf{ of } [x^\tau]M^\rho, [y^\sigma]N^\rho \implies M[x := P] : \rho$
$\textbf{case } \textbf{in}_2 Q^{\tau\vee\sigma} \textbf{ of } [x^\tau]M^\rho, [y^\sigma]N^\rho \implies N[y := Q] : \rho.$

Normalizacja dowodu: koniunkcja

$$\dfrac{\dfrac{\begin{matrix}(*)\\ \vdots\\ \tau\end{matrix} \quad \begin{matrix}(**)\\ \vdots\\ \sigma\end{matrix}}{\tau \wedge \sigma}}{\tau} \implies \begin{matrix}(*)\\ \vdots\\ \tau\end{matrix}$$

$$\langle M^\tau, N^\sigma\rangle\{1\} \implies M : \tau$$

Normalizacja dowodu: alternatywa



case inl $(P)^{\tau\vee\sigma}$ **of** $[x^\tau]M^\rho, [y^\sigma]N^\rho \implies M[x := P] : \rho$

Pożytek z normalizacji: niesprzeczność

Fakt: *W logice z* $\to$, $\bot$ *i* $\wedge$ *nie istnieje dowód fałszu.*

Dowód: Wtedy istniałby dowód normalny, czyli taki term M w postaci normalnej, że:

$$\varnothing \vdash M : \bot.$$

Jak on może wyglądać?

- Nie może być wprowadzeniem, bo nie ma reguły $(W\bot)$.
- Nie może być postaci $xE_1 \ldots E_m$, bo nie ma zmiennych.
- Zostaje postać $\varepsilon_\bot(M')$, a wtedy $\varnothing \vdash M' : \bot$ jest krótszym dowodem sprzeczności.

Logika intuicjonistyczna

Wykład 9

12 kwietnia 2012

Rozszerzony rachunek λ (1)

$$\Gamma, x{:}\tau \vdash M : \tau \qquad \frac{\Gamma \vdash M{:}\bot}{\Gamma \vdash \varepsilon_\tau(M) : \tau}$$

$$\frac{\Gamma, x{:}\alpha \vdash M : \beta}{\Gamma \vdash \lambda x{:}\alpha\, M : \alpha \to \beta} \qquad \frac{\Gamma \vdash M : \alpha \to \beta \quad \Gamma \vdash N : \alpha}{\Gamma \vdash MN : \beta}$$

Rozszerzony rachunek λ (2)

$$\frac{\Gamma \vdash M : \alpha \quad \Gamma \vdash N : \beta}{\Gamma \vdash \langle M, N\rangle : \alpha \wedge \beta} \qquad \frac{\Gamma \vdash M : \alpha_1 \wedge \alpha_2}{\Gamma \vdash M\{i\} : \alpha_i}$$

$$\frac{\Gamma \vdash M : \alpha_i}{\Gamma \vdash \mathsf{in}_i(M) : \alpha_1 \vee \alpha_2}$$

$$\frac{\Gamma \vdash M : \alpha \vee \beta \quad \Gamma, u{:}\alpha \vdash R : \tau \quad \Gamma, v{:}\beta \vdash Q : \tau}{\Gamma \vdash \mathsf{case}\ M\ \mathsf{of}\ [u]R\ \mathsf{or}\ [v]Q : \tau}$$

Beta-redukcja

Beta-redeks to eliminacja spójnika zastosowana bezpośrednio po jego wprowadzeniu. *Beta-redukcja* to „upraszcza”:

$(\to)$ $(\lambda x^\tau\, M^\sigma)N^\tau \implies M[x := N] : \sigma.$

$(\wedge)$ $\langle M^\tau, N^\sigma\rangle\{1\} \implies M : \tau, \qquad \langle M^\tau, N^\sigma\rangle\{2\} \implies N : \sigma.$

$(\vee)$ $\mathbf{case}\ \mathbf{in}_1\, P^{\tau\vee\sigma}\ \mathbf{of}\ [x^\tau]M^\rho, [y^\sigma]N^\rho \implies M[x := P] : \rho$
$\mathbf{case}\ \mathbf{in}_2\, Q^{\tau\vee\sigma}\ \mathbf{of}\ [x^\tau]M^\rho, [y^\sigma]N^\rho \implies N[y := Q] : \rho.$

Silna normalizacja

Twierdzenie: *Rozszerzony rachunek lambda ma własność silnej normalizacji.*

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 (1)

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

Translacja dla termów (2)

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

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

Translacja dla termów (3)

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

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

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

Twierdzenie: *Rozszerzony rachunek lambda ma własność silnej normalizacji.*

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

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

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

Przypadek 1: $M = (\lambda x\, P)Q \to P[x := Q]$ tłumaczy się tak:

$|M| = (\lambda x\, |P|)|Q| \to_\beta |P|[x := |Q|] = |P[x := Q]|$.

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

Przypadek 2: $M = \langle P, Q\rangle\{1\} \to P$ tłumaczy się tak:

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

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

Przypadek 3:

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

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

Dlaczego to za mało

Dowód fałszu może wyglądać np. tak:

$$\varnothing \vdash \textbf{case}\ N^{\tau\vee\sigma}\ \textbf{of}\ [x^\tau]P^\perp, [y^\sigma]Q^\perp : \perp,$$

Term N sam może być np. postaci **case**...

Jak nad tym zapanować?

Wprowadzić dodatkowe redukcje porządkujące (*permutacje*).

Alternatywna składnia

Zamiast **case** M **of** $[x]P, [y]Q$ piszemy $M[x.P, y.Q]$.

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

Wada: mniej intuicyjne.

Zaleta: wszystkie eliminacje pisane jednolicie na końcu:

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

Permutacje

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

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

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

Permutacje:

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

Permutacje dla $\perp$

- $\varepsilon_\psi(\varepsilon_\perp(M)) \ \Rightarrow\ \varepsilon_\psi(M)$;
- $\varepsilon_{\varphi\to\psi}(M)N \ \Rightarrow\ \varepsilon_\psi(M)$;
- $\varepsilon_{\varphi_1\wedge\varphi_2}(M)\{i\} \ \Rightarrow\ \varepsilon_{\varphi_i}(M)$;
- **case** $\varepsilon_{\sigma\vee\tau}(M)$ **of** $[u]R^\rho$ **or** $[v]S^\rho \ \Rightarrow\ \varepsilon_\rho(M)$.

Permutacje dla **case**

- $\varepsilon_\varphi(\texttt{case}\ M\ \texttt{of}\ [x]P\ \texttt{or}\ [y]Q) \Rightarrow$
  $\texttt{case}\ M\ \texttt{of}\ [x]\varepsilon_\varphi(P)\ \texttt{or}\ [y]\varepsilon_\varphi(Q);$
- $(\texttt{case}\ M\ \texttt{of}\ [x]P\ \texttt{or}\ [y]Q)N \Rightarrow$
  $\texttt{case}\ M\ \texttt{of}\ [x]PN\ \texttt{or}\ [y]QN;$
- $(\texttt{case}\ M\ \texttt{of}\ [x]P\ \texttt{or}\ [y]Q)\{i\} \Rightarrow$
  $\texttt{case}\ M\ \texttt{of}\ [x]P\{i\}\ \texttt{or}\ [y]Q\{i\};$
- $\texttt{case}\ (\texttt{case}\ M\ \texttt{of}\ [x]P\ \texttt{or}\ [y]Q)\ \texttt{of}\ [u]R\ \texttt{or}\ [v]S \Rightarrow$
  $\texttt{case}\ M\ \texttt{of}\ [x](\texttt{case}\ P\ \texttt{of}\ [u]R\ \texttt{or}\ [v]S)$
  $\texttt{or}\ [y](\texttt{case}\ Q\ \texttt{of}\ [u]R\ \texttt{or}\ [v]S)$

Zła wiadomość

Translacja używana poprzednio 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".

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

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

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

Ogólniej, dla : $N : \text{int}$,

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

Kontynuacje dla funkcji

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	$p \to \mathbf{0}$	$(p \to \mathbf{0}) \to \mathbf{0}$
$\bot$	$\mathbf{0}$	$\mathbf{0} \to \mathbf{0}$	$(\mathbf{0} \to \mathbf{0}) \to \mathbf{0}$
$\tau \to \sigma$	$\underline{\tau} \to \underline{\sigma}$	$(\underline{\tau} \to \underline{\sigma}) \to \mathbf{0}$	$((\underline{\tau} \to \underline{\sigma}) \to \mathbf{0}) \to \mathbf{0}$

Kontynuacje dla koniunkcji i alternatywy

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

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

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

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

Sens $E@K$: eliminator E włączony do kontynuacji K.

Dołączanie eliminatora do kontynuacji

$$\begin{aligned} N@K &= \lambda m^{\underline{\tau} \to \underline{\sigma}}.\, m\underline{N}K : (\tau \to \sigma)^\bullet \to \mathbf{0} \\ \{1\}@K &= \lambda m^{(\underline{\tau} \to \underline{\sigma} \to \mathbf{0}) \to \mathbf{0}}.\, m(\lambda x^{\underline{\tau}} y^{\underline{\sigma}}.\, xK) : (\tau \wedge \sigma)^\bullet \to \mathbf{0} \\ [x^\tau.S, y^\sigma.T]@K &= \lambda m^{(\tau \vee \sigma)^\bullet}.\, m(\lambda x^{\underline{\tau}}.\, S \triangleright K)(\lambda y^{\underline{\sigma}}.\, T \triangleright K) \\ [\varepsilon_\sigma]@K &= (\lambda k m^{\mathbf{0}}.\, m)K \end{aligned}$$

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

Własności translacji

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

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

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

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

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

Zła wiadomość

Translacja nie zachowuje permutacji postaci

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

Rozwiązanie: Odkładanie epsilona.

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

Morał: Jeśli istnieje redukcja

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

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

Silna normalizacja

Wystarczy udowodnić, że nie istnieje nieskończona $\beta\delta$-redukcja ani nieskończona $\bot$-redukcja.

Lemat: *Nie istnieje nieskończona redukcja z samych permutacji (czyli $\bot\delta$-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:

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

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: *Rozszerzony rachunek lambda z permutacjami ma własność silnej normalizacji.*

Wniosek: *Jeśli formuła ma dowód, to ma dowód normalny.*

Postaci normalne

Konstruktory: $\lambda x : \alpha.\, N$, $\langle N_1, N_2\rangle$, $\mathrm{in}_i(N)$;

Ładne eliminatory: x, PN, $P\{i\}$;

Brzydkie eliminatory: $\varepsilon_\varphi(P)$, case P of $[x]N_1$ or $[y]N_2$.

[N – postać normalna, P – dobry („proper") eliminator.]

Uwaga: Ładne eliminatory „zaczynają się" od zmiennych.

Niesprzeczność

Wniosek: *Intuicjonistyczny rachunek zdań jest niesprzeczny.*

Dowód: W pustym otoczeniu:

- Nie ma ładnych eliminatorów $xE_1 \dots E_m$, bo nie ma zmiennych.
- Zatem nie ma też brzydkich eliminatorów postaci $\varepsilon_\perp(P)$, ani case P $\dots$, bo do tego potrzebny ładny.

Zatem jeśli $\varnothing \vdash M : \perp$, gdzie M jest normalny, to M musi być konstruktorem.

Ale nie ma konstruktorów typu $\perp$, bo nie ma reguły $(W\perp)$.

Postaci normalne (fragment implikacyjny)

Konstruktory: $\lambda x : \alpha.\, N$

Dobre eliminatory: $xN_1 \dots N_k$

Poszukiwanie dowodu:

To prove p, use an assumption with target p.
Otherwise proof is a constructor.

Poszukiwanie dowodu (przypadek ogólny)

Types of proper eliminators: direct remainders (suffixes), e.g.

$$xM^\gamma : \alpha \vee \beta \quad \text{where} \quad x : \gamma \to \alpha \vee \beta.$$

Types of improper eliminators may be reached indirectly:

case x of $[u]u\{2\}$ or $[v]$ case yv of $[u]uv$ or $[w]zw : p$

where $x : (q \wedge p) \vee r$, $y : r \to (r \to p) \vee q$, and $z : q \to p$.

But atomic types must be (direct or indirect) *targets*.

Suffixes $S(\tau)$ of a type τ

- $\tau \in S(\tau)$;
- If $\alpha \to \beta \in S(\tau)$ then $\beta \in S(\tau)$;
- If $\alpha \wedge \beta \in S(\tau)$ then $\alpha, \beta \in S(\tau)$;

Lemma:

If $\Gamma, x : \tau \vdash P : \sigma$, and P is a proper eliminator beginning with x then $\sigma \in S(\tau)$.

Targets $T(\tau)$ of a type τ

- $T(\bot) = \{\bot\}$ and $T(p) = \{p\}$, for a type variable;
- $T(\alpha \to \beta) = T(\beta)$;
- $T(\alpha \diamond \beta) = T(\alpha) \cup T(\beta)$, for $\diamond \in \{\wedge, \vee\}$;

Lemma:

If $\Gamma \vdash a$*, where* a *is an atom (a variable or* $\bot$*) then* $a \in T(\Gamma)$*, or* $\bot \in T(\Gamma)$ *and* $\Gamma \vdash \bot$*.*

Example application:

Disjunction property: *If* $\Gamma \vdash \alpha \vee \beta$*, and* $\vee$ *does not occur in* Γ*, then* $\Gamma \vdash \alpha$ *or* $\Gamma \vdash \beta$*.*

Proof: Show that if $\Gamma \vdash M : \alpha \vee \beta$ and M is normal, then either $\Gamma \vdash \bot$ or M is a constructor **in**.

Types of proper eliminators contain no $\vee$, so M is either an introduction (OK) or an „improper" eliminator.

If $M = \varepsilon(M')$ then $\Gamma \vdash M' : \bot$ (OK).

If $M =$ case $M' \ldots$ then M' is a proper eliminator of a disjunction type – excluded as above.

Logika intuicjonistyczna

Wykład 10

19 kwietnia 2012

W poprzednim odcinku: postaci normalne

Konstruktory: $\lambda x : \alpha.\, N$, $\langle N_1, N_2 \rangle$, $\mathsf{in}_i(N)$;

Ładne eliminatory: x, PN, $P\{i\}$;

Brzydkie eliminatory: $\varepsilon_\varphi(P)$, case P of $[x]N_1$ or $[y]N_2$.

[N – postać normalna, P – dobry („proper") eliminator.]

Uwaga: Ładne eliminatory „zaczynają się" od zmiennych.

Wniosek: prawo alternatywy

Twierdzenie:

Jeśli $\Gamma \vdash \alpha \vee \beta$, *oraz* $\vee$ *nie występuje w* Γ, *to* $\Gamma \vdash \alpha$ *lub* $\Gamma \vdash \beta$

Separation theorem (Mordchaj Wajsberg, 1938)

Disjunction: *There is no* α *without* $\vee$ *such that* $p \vee q \leftrightarrow \alpha$.

Proof:

If $\alpha \vdash p \vee q$ then $\alpha \vdash p$ or $\alpha \vdash q$. But $p \vee q \nvdash p$ and $p \vee q \nvdash q$.

Separation theorem

Implication: *There is no* α *without* $\to$ *such that* $p \to q \vdash \alpha$.

Proof: Induction.

If $\alpha = \beta \wedge \gamma$ then $p \to q \vdash \beta$.

If $\alpha = \beta \vee \gamma$ then either $p \to q \vdash \beta$ or $p \to q \vdash \gamma$.

Targets $T(\tau)$ of a type τ

- $T(\bot) = \{\bot\}$ and $T(p) = \{p\}$, for a type variable;
- $T(\alpha \to \beta) = T(\beta)$;
- $T(\alpha \diamond \beta) = T(\alpha) \cup T(\beta)$, for $\diamond \in \{\wedge, \vee\}$;

Lemma:

If $\Gamma \vdash a$, *where* a *is an atom* (*a variable or* $\bot$)
then $a \in T(\Gamma)$, *or* $\bot \in T(\Gamma)$ *and* $\Gamma \vdash \bot$.

Separation theorem

Conjunction: *If* $\alpha \vdash p \wedge q$ *and* $\wedge$ *is not in* α *then* $\alpha \vdash \bot$.

Proof: If $\alpha = \beta \vee \gamma$ then $\beta \vdash \bot$ and $\gamma \vdash \bot$ by induction.

Assume that $\alpha = \beta \to \gamma$.

Then also $\beta \to \bot \vdash p$,
whence $\beta \to \bot \vdash \bot$, as p is not a target.

On the other hand, also $\gamma \vdash p \wedge q$, so $\gamma \vdash \bot$, by induction.

Thus we have $\beta \to \gamma \vdash \beta \to \bot$,
and therefore $\beta \to \gamma \vdash \bot$.

Ben-Yelles algorithm

To answer $\Gamma \vdash ? : \alpha$, apply one of the following tactics:

- For $\alpha = \beta \to \gamma$, ask $\Gamma \cup \{x : \beta\} \vdash ? : \gamma$ (fresh x).
  (Solution $M = \lambda x{:}\beta.\, N^{\gamma}$.)
- For $\alpha = p$, choose $x : \beta_1 \to \cdots \to \beta_k \to p$ from Γ,
  then ask $\Gamma \vdash ? : \beta_i$, for all i. Success if $k = 0$.
  (Solution $M = xN_1^{\beta_1} \ldots N_k^{\beta_k}$.)

Wajsberg's algorithm (dla $\vee$, $\rightarrow$, $\bot$)

To answer if $\Gamma \vdash \alpha$, apply one of the following tactics:

- For $\alpha = \beta \rightarrow \gamma$, ask if $\Gamma, \beta \vdash \gamma$?
- For $\alpha = \mathbf{a}$ (atom), pick $\beta_1 \rightarrow \cdots \rightarrow \beta_k \rightarrow \mathbf{b}$ from Γ, where $k \geq 0$ and $\mathbf{b} \in \{\mathbf{a}, \bot\}$, then ask if $\Gamma \vdash \beta_i$, for all i.
- Pick $\beta_1 \rightarrow \cdots \rightarrow \beta_k \rightarrow \beta \vee \gamma$ from Γ, and ask if $\Gamma \vdash \beta_i$, for all i. Also ask if $\Gamma, \beta \vdash \alpha$ and $\Gamma, \gamma \vdash \alpha$.
- For $\alpha = \alpha_1 \vee \alpha_2$, pick $i \in \{1, 2\}$ and ask if $\Gamma \vdash \alpha_i$.

Wajsberg's algorithm (dla $\vee$, $\rightarrow$, $\bot$, $\wedge$)

$Path(p) = \{(p)\}$, $Path(\bot) = \{(\bot)\}$,
$Path(\alpha \vee \beta) = \{(\alpha \vee \beta)\}$,
$Path(\alpha \rightarrow \beta) = \{\alpha \cdot P \mid P \in Path(\beta)\}$,
$Path(\alpha \wedge \beta) = Path(\alpha) \cup Path(\beta)$

Taktyki dla koniunkcji:

- *For $\alpha = \mathbf{a}$ (atom), pick $\varphi \in \Gamma$ with $(\beta_1, \beta_2, \ldots, \beta_k, \mathbf{b}) \in Path(\varphi)$, and $\mathbf{b} \in \{\mathbf{a}, \bot\}$. Then ask if $\Gamma \vdash \beta_i$, for all β_i.*
- *Pick $\varphi \in \Gamma$ with $(\beta_1, \beta_2, \ldots, \beta_k, \beta \vee \gamma) \in Path(\varphi)$. Ask if $\Gamma \vdash \beta_i$, for all i, and $\Gamma, \beta \vdash \alpha$ and $\Gamma, \gamma \vdash \alpha$.*
- *For $\alpha = \alpha_1 \wedge \alpha_2$, ask if $\Gamma \vdash \alpha_1$ and $\Gamma \vdash \alpha_2$.*

A little game: $\neg\neg(p \vee \neg p)$

$\forall$: $(p \vee \neg p) \rightarrow \bot \vdash \bot$?
$\exists$: $(p \vee \neg p) \rightarrow \bot \vdash p \vee \neg p$!
$\forall$: ?
$\exists$: $(p \vee \neg p) \rightarrow \bot \vdash \neg p$!
$\forall$: $(p \vee \neg p) \rightarrow \bot, p \vdash \bot$?
$\exists$: $(p \vee \neg p) \rightarrow \bot, p \vdash p \vee \neg p$!
$\forall$: ?!
$\exists$: $(p \vee \neg p) \rightarrow \bot, p \vdash p$!

A little cheating: $p \vee \neg p$

$\forall$: $(p \vee \neg p) \rightarrow \bot \vdash \bot$?
$\exists$: $(p \vee \neg p) \rightarrow \bot \vdash p \vee \neg p$!
$\forall$: ?
$\exists$: $(p \vee \neg p) \rightarrow \bot \vdash \neg p$!
$\forall$: $(p \vee \neg p) \rightarrow \bot, p \vdash \bot$?
$\exists$: $(p \vee \neg p) \rightarrow \bot, p \vdash p \vee \neg p$!
$\forall$: ?!
$\exists$: $(p \vee \neg p) \rightarrow \bot, p \vdash p$!

$\exists$: $p \vee \neg p$!
$\forall$: ??
$\exists$: $\neg p$!
$\forall$: $p \vdash \bot$??
$\exists$: $p \vdash p \vee \neg p$!!

Logika klasyczna

$$\frac{\Gamma, a{:}\neg\alpha \vdash M : \bot}{\Gamma \vdash \mu a{:}\neg\alpha.\, M : \alpha} \qquad \frac{\Gamma, a{:}\neg\alpha \vdash M : \alpha}{\Gamma, a{:}\neg\alpha \vdash [a]M : \bot}$$

Jeśli $a \notin \mathrm{FV}(M)$, to zamiast $\mu a{:}\neg\alpha.\, M$ piszemy $\varepsilon_\alpha(M)$.

Sens obliczeniowy

Co można zrobić z dowodem postaci $\mu a^{\neg\alpha} \ldots [a]M^\alpha \ldots$?

Wyjąć dowód $M : \alpha$ ze środka, i wyrzucić resztę!

Co wyjąć z tego dowodu:

$$\lambda x^{(p\to q)\to p} \mu a^{\neg p}.\, [a](x(\lambda z^p\, \varepsilon_q([a]z)))\,?$$

Przeszkody: niebieskie $[a]$, czerwone z.

Idziemy w zaparte

Kiedy jest naprawdę ważne, co jest wewnątrz $[a]M$?

Przy ewaluacji wyrażenia $[a]M$ w jakimś kontekście.

Niedospecyfikowane fragmenty termu M mogą wtedy

– okazać się nieistotne;

– zostać dookreślone.

Sens obliczeniowy

$$\mu a^{\neg\alpha}(\ldots [a]M^\alpha \ldots) \quad \Longrightarrow \quad M^\alpha\ ?$$

$$\mu a^{\neg\alpha} N \quad \Longrightarrow \quad N[[a] := \lambda m.\, \mathtt{abort}(m)]\ ?$$

Timothy Griffin (1990):

$$E[\mu a^{\neg\alpha} N] \quad \Longrightarrow \quad N[[a] := \lambda m.\, \mathtt{abort}(E[m])]$$

Sens obliczeniowy: działanie imperatywne

$$\mu a.\, M \quad \equiv \quad \texttt{catch}\ a\ \texttt{in}\ M$$

$$[a]M \quad \equiv \quad \texttt{throw}\ M\ \texttt{to}\ [a]$$

Internalizacja Griffina

$$E[\mu a^{\neg\alpha} N] \qquad \Longrightarrow \qquad N[[a] := \lambda m.\, \texttt{abort}(E[m])]$$

Rachunek $\lambda\mu$ (Michel Parigot, 1992[2]):

– Otoczenie E może być „wchłaniane" częściowo.

[2] Nie mylić z rachunkiem μ.

Rachunek $\lambda\mu$: fragment implikacyjny

(β) $(\lambda x^{\alpha} M)N \;\Rightarrow\; M[x := N].$

(η_μ) $\mu a^{\neg\alpha}.\,[a]M^{\alpha} \;\Rightarrow\; M,$ gdy $a \notin \mathrm{FV}(M).$

(ζ) $(\mu a^{\neg(\alpha\to\beta)}.\, M)N \;\Rightarrow\; \mu b^{\neg\beta}.\, M[a := \lambda\!\!\lambda X.\,[b](XN)]$

Zeta inaczej:

(ζ) $(\mu a^{\neg(\alpha\to\beta)}.\, M)N \;\Rightarrow\; \mu b^{\neg\beta}.\, M[\,[a]\Box := [b](\Box N)\,]$

Może być jeszcze:

(β^{μ}) $[b](\mu a^{\neg\alpha}.\, M) \;\Rightarrow\; M[a := b]$

Semantyka kontynuacyjna

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	$p \to \mathbf{0}$	$(p \to \mathbf{0}) \to \mathbf{0}$
$\bot$	$\mathbf{0}$	$\mathbf{0} \to \mathbf{0}$	$(\mathbf{0} \to \mathbf{0}) \to \mathbf{0}$
$\tau \to \sigma$	$\underline{\tau} \to \underline{\sigma}$	$(\underline{\tau} \to \underline{\sigma}) \to \mathbf{0}$	$((\underline{\tau} \to \underline{\sigma}) \to \mathbf{0}) \to \mathbf{0}$

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

$$
\begin{aligned}
x^\tau \triangleright K &= x^{\underline{\tau}}(K) \\
(\lambda x^\sigma.\, M^\tau) \triangleright K &= K(\lambda x^{\underline{\sigma}}.\, \underline{M^\tau}) \\
MN \triangleright K &= M \triangleright (\lambda m.\, m\underline{N}K) \\
[a]M^\sigma \triangleright K &= M \triangleright k_a \\
(\mu a^{\neg\sigma} M) \triangleright K &= (M \triangleright \lambda m\, m)[k_a := K]
\end{aligned}
$$

Dla $a : \neg\sigma$, nowa zmienna $k_a : \sigma^\bullet \to \mathbf{0}$.

Wniosek: silna normalizacja (dla β, η_μ, ζ).

CPS na poziomie typów

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

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

Przyjmując $\mathbf{0} = \bot$, dostajemy:

$$\underline{\tau \to \sigma} = \neg\neg(\underline{\tau} \to \underline{\sigma}).$$

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:

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

Translacja Kołmogorowa

Twierdzenie:

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

Dowód:

($\Rightarrow$) Jeśli $\Gamma \vdash_\mu M : \alpha$, to $\underline{\Gamma} \vdash_\lambda \underline{M} : \underline{\alpha}$.

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

To działa nie tylko dla rachunku zdań.

Morał: Logika klasyczna *m*-redukuje się do logiki intuicjonistycznej (jest „łatwiejsza").

Klasyczny rachunek sekwentów

Sekwenty: $\overbrace{\varphi_1, \ldots, \varphi_n}^{\text{koniunkcja}} \vdash \overbrace{\psi_1, \ldots, \psi_m}^{\text{alternatywa}}$ $(n, m \geq 0)$

$\underbrace{\varphi_1, \ldots, \varphi_n}_{\text{założenia}} \quad \underbrace{\psi_1, \ldots, \psi_m}_{\text{wnioski}}$

Aksjomaty: $\varphi \vdash \varphi$

Reguły:

- strukturalne,
- logiczne,
- reguła cięcia.

Porównanie

Naturalna dedukcja: Eliminacja i wprowadzanie

$$\frac{\Gamma \vdash \alpha \diamond \beta \quad \ldots}{\ldots}\ (\text{Elim } \diamond) \qquad \frac{\ldots \alpha \ldots \beta \ldots}{\Gamma \vdash \alpha \diamond \beta}\ (\text{Intro } \diamond)$$

Rachunek sekwentów: Wprowadzanie z prawej i z lewej

$$\frac{\Gamma \vdash \ldots \quad \ldots}{\Gamma, \alpha \diamond \beta \vdash \ldots}\ (\text{L } \diamond) \qquad \frac{\ldots \alpha \ldots \beta \ldots}{\ldots \vdash \alpha \diamond \beta, \Delta}\ (\text{R } \diamond)$$

Reguły strukturalne

Wymiana: $\dfrac{\Gamma, \varphi, \psi, \Delta \vdash \Sigma}{\Gamma, \psi, \varphi, \Delta \vdash \Sigma}(\text{LW}) \qquad \dfrac{\Gamma \vdash \Delta, \varphi, \psi, \Sigma}{\Gamma \vdash \Delta, \psi, \varphi, \Sigma}(\text{PW})$

Osłabianie: $\dfrac{\Gamma \vdash \Sigma}{\Gamma, \varphi \vdash \Sigma}(\text{LO}) \qquad \dfrac{\Gamma \vdash \Sigma}{\Gamma \vdash \varphi, \Sigma}(\text{PO})$

Skracanie: $\dfrac{\Gamma, \varphi, \varphi \vdash \Sigma}{\Gamma, \varphi \vdash \Sigma}(\text{LS}) \qquad \dfrac{\Gamma \vdash \varphi, \varphi, \Sigma}{\Gamma \vdash \varphi, \Sigma}(\text{PS})$

Można uważać, że sekwent to para zbiorów.

Reguły logiczne

$$\frac{\Gamma, \varphi_i \vdash \Sigma}{\Gamma, \varphi_1 \wedge \varphi_2 \vdash \Sigma}\ (\text{LK}) \qquad \frac{\Gamma \vdash \varphi, \Sigma \quad \Gamma \vdash \psi, \Sigma}{\Gamma \vdash \varphi \wedge \psi, \Sigma}\ (\text{PK})$$

$$\frac{\Gamma, \varphi \vdash \Sigma \quad \Gamma, \psi \vdash \Sigma}{\Gamma, \varphi \vee \psi \vdash \Sigma}\ (\text{LA}) \qquad \frac{\Gamma \vdash \varphi_i, \Sigma}{\Gamma \vdash \varphi_1 \vee \varphi_2, \Sigma}\ (\text{PA})$$

$$\frac{\Gamma \vdash \varphi, \Sigma \quad \Gamma, \psi \vdash \Sigma}{\Gamma, \varphi \to \psi \vdash \Sigma}\ (\text{LI}) \qquad \frac{\Gamma, \varphi \vdash \psi, \Sigma}{\Gamma \vdash \varphi \to \psi, \Sigma}\ (\text{PI})$$

$$\frac{\Gamma \vdash \varphi, \Sigma}{\Gamma, \neg\varphi \vdash \Sigma}\ (\text{LN}) \qquad \frac{\Gamma, \varphi \vdash \Sigma}{\Gamma \vdash \neg\varphi, \Sigma}\ (\text{PN})$$

$\Gamma, \bot \vdash$ (LF) $\qquad \Gamma \vdash \top, \Sigma$ (PP)

Przykład: $\vdash ((p \to q) \to p) \to p$

$$\dfrac{\dfrac{\dfrac{\dfrac{p \vdash p}{p \vdash q, p}\,(\mathrm{PO})}{\vdash p \to q, p}\,(\mathrm{PI}) \qquad p \vdash p}{(p \to q) \to p \vdash p}\,(\mathrm{LI})}{\vdash ((p \to q) \to p) \to p}\,(\mathrm{PI})$$

Przykład: $\vdash p \vee \neg p$

$$\dfrac{\dfrac{\dfrac{\dfrac{p \vdash p}{\vdash \neg p, p}\,(\mathrm{PN})}{\vdash p \vee \neg p, p}\,(\mathrm{PA})}{\vdash p, p \vee \neg p}\,(\mathrm{PW})}{\vdash p \vee \neg p, p \vee \neg p}\,(\mathrm{PA})}{\vdash p \vee \neg p}\,(\mathrm{PS})$$

Logika intuicjonistyczna

Wykład 11

26 kwietnia 2012

Klasyczny rachunek sekwentów

Sekwenty: $\overbrace{\varphi_1, \ldots, \varphi_n}^{\text{koniunkcja}} \vdash \overbrace{\psi_1, \ldots, \psi_m}^{\text{alternatywa}}$ $(n, m \geq 0)$

$\underbrace{\qquad\qquad}_{\text{założenia}} \qquad\qquad \underbrace{\qquad\qquad}_{\text{wnioski}}$

Aksjomaty: $\varphi \vdash \varphi$

Reguły:

- strukturalne,
- logiczne,
- reguła cięcia.

Reguły strukturalne

Wymiana: $\dfrac{\Gamma, \varphi, \psi, \Delta \vdash \Sigma}{\Gamma, \psi, \varphi, \Delta \vdash \Sigma}$(LW) $\qquad$ $\dfrac{\Gamma \vdash \Delta, \varphi, \psi, \Sigma}{\Gamma \vdash \Delta, \psi, \varphi, \Sigma}$(PW)

Osłabianie: $\dfrac{\Gamma \vdash \Sigma}{\Gamma, \varphi \vdash \Sigma}$(LO) $\qquad$ $\dfrac{\Gamma \vdash \Sigma}{\Gamma \vdash \varphi, \Sigma}$(PO)

Skracanie: $\dfrac{\Gamma, \varphi, \varphi \vdash \Sigma}{\Gamma, \varphi \vdash \Sigma}$(LS) $\qquad$ $\dfrac{\Gamma \vdash \varphi, \varphi, \Sigma}{\Gamma \vdash \varphi, \Sigma}$(PS)

Można uważać, że sekwent to para zbiorów.

Reguły logiczne (addytywne)

$\dfrac{\Gamma, \varphi_i \vdash \Sigma}{\Gamma, \varphi_1 \wedge \varphi_2 \vdash \Sigma}$ (LK) $\qquad$ $\dfrac{\Gamma \vdash \varphi, \Sigma \quad \Gamma \vdash \psi, \Sigma}{\Gamma \vdash \varphi \wedge \psi, \Sigma}$ (PK)

$\dfrac{\Gamma, \varphi \vdash \Sigma \quad \Gamma, \psi \vdash \Sigma}{\Gamma, \varphi \vee \psi \vdash \Sigma}$ (LA) $\qquad$ $\dfrac{\Gamma \vdash \varphi_i, \Sigma}{\Gamma \vdash \varphi_1 \vee \varphi_2, \Sigma}$ (PA)

$\dfrac{\Gamma \vdash \varphi, \Sigma \quad \Gamma, \psi \vdash \Sigma}{\Gamma, \varphi \to \psi \vdash \Sigma}$ (LI) $\qquad$ $\dfrac{\Gamma, \varphi \vdash \psi, \Sigma}{\Gamma \vdash \varphi \to \psi, \Sigma}$ (PI)

$\dfrac{\Gamma \vdash \varphi, \Sigma}{\Gamma, \neg\varphi \vdash \Sigma}$ (LN) $\qquad$ $\dfrac{\Gamma, \varphi \vdash \Sigma}{\Gamma \vdash \neg\varphi, \Sigma}$ (PN)

$\Gamma, \bot \vdash$ (LF) $\qquad$ $\Gamma \vdash \top, \Sigma$ (PP)

Reguła cięcia

$$\frac{\Gamma \vdash \varphi, \Sigma \quad \Gamma, \varphi \vdash \Sigma}{\Gamma \vdash \Sigma}\ (\text{cut})$$

Pełność: *Sekwent* $\varphi_1, \ldots, \varphi_n \vdash \psi_1, \ldots, \psi_m$ *ma dowód wtw, gdy* $\varphi_1 \wedge \cdots \wedge \varphi_n \to \psi_1 \vee \cdots \vee \psi_m$ *jest tautologią.*

Dowód używa reguły cięcia, np. tak:

$$\frac{\Gamma \vdash \varphi \to \psi \qquad \dfrac{\Gamma \vdash \varphi \quad \Gamma, \psi \vdash \psi}{\Gamma, \varphi \to \psi \vdash \psi}}{\Gamma \vdash \psi}\ (\text{MP})$$

Gentzen's Hauptsatz

Twierdzenie (o eliminacji cięcia):

Jeśli sekwent $\Gamma \vdash \Delta$ *ma dowód, to ma dowód bez cięcia.*

Zasada podformuł:

Formuły wystepujące w przesłankach każdej reguły są podformułami formuł występujących w konkluzji.

Dowód bez cięcia sekwentu $\vdash \varphi$ używa tylko podformuł φ.

Dowód budujemy od końca, „rozbierając" formuły na części.

Przykład eliminacji cięcia: Dowód

$$\dfrac{\begin{array}{ccc}(1) & & (2)\quad (3)\\ \vdots & & \vdots\quad\ \vdots\\ \dfrac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \to \psi}(\mathrm{R}\to) & & \dfrac{\Gamma \vdash \varphi \qquad \Gamma, \psi \vdash \vartheta}{\Gamma,\ \varphi \to \psi \vdash \vartheta}(\mathrm{L}\to)\end{array}}{\Gamma \vdash \vartheta}(\mathrm{Cut})$$

przekształcamy w dowód:

$$\dfrac{\begin{array}{ccc}(2) & (1) & \\ \vdots & \vdots & \\ \dfrac{\Gamma \vdash \varphi \qquad \Gamma, \varphi \vdash \psi}{\Gamma \vdash \psi}(\mathrm{Cut}) & & (3)\\ & & \vdots\\ & & \Gamma, \psi \vdash \vartheta\end{array}}{\Gamma \vdash \vartheta}(\mathrm{Cut})$$

Intuicjonistyczny rachunek sekwentów

Sekwenty mają co najwyżej jedną formułę po prawej stronie.

Wymiana: $\dfrac{\Gamma, \varphi, \psi, \Delta \vdash \sigma}{\Gamma, \psi, \varphi, \Delta \vdash \sigma}\ (\text{LW})$

Osłabianie: $\dfrac{\Gamma \vdash \sigma}{\Gamma, \varphi \vdash \sigma}\ (\text{LO})$ $\qquad$ $\dfrac{\Gamma \vdash}{\Gamma \vdash \sigma}\ (\text{PO})$

Skracanie: $\dfrac{\Gamma, \varphi, \varphi \vdash \sigma}{\Gamma, \varphi \vdash \sigma}\ (\text{LS})$

Intuicjonistyczny rachunek sekwentów

$$\frac{\Gamma, \varphi_i \vdash \sigma}{\Gamma, \varphi_1 \wedge \varphi_2 \vdash \sigma}\ (\mathrm{LK}) \qquad \frac{\Gamma \vdash \varphi \quad \Gamma \vdash \psi}{\Gamma \vdash \varphi \wedge \psi}\ (\mathrm{PK})$$

$$\frac{\Gamma, \varphi \vdash \sigma \quad \Gamma, \psi \vdash \sigma}{\Gamma, \varphi \vee \psi \vdash \sigma}\ (\mathrm{LA}) \qquad \frac{\Gamma \vdash \varphi_i}{\Gamma \vdash \varphi_1 \vee \varphi_2}\ (\mathrm{PA})$$

$$\frac{\Gamma \vdash \varphi \quad \Gamma, \psi \vdash \sigma}{\Gamma, \varphi \to \psi \vdash \sigma}\ (\mathrm{LI}) \qquad \frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \to \psi}\ (\mathrm{PI})$$

$$\frac{\Gamma \vdash \varphi}{\Gamma, \neg\varphi \vdash \bot}\ (\mathrm{LN}) \qquad \frac{\Gamma, \varphi \vdash \bot}{\Gamma \vdash \neg\varphi}\ (\mathrm{PN})$$

$$\Gamma, \bot \vdash \sigma\ (\mathrm{LF}) \qquad \Gamma \vdash \top\ (\mathrm{PP})$$

Przypisanie termów (1)

$$\frac{\Gamma \vdash M : \varphi \quad \Gamma \vdash N : \psi}{\Gamma \vdash \langle M, N\rangle : \varphi \wedge \psi}\ (\mathrm{PK})$$

$$\frac{\Gamma \vdash M : \varphi_i}{\Gamma \vdash \mathsf{in}_i(M) : \varphi_1 \vee \varphi_2}\ (\mathrm{PA})$$

$$\frac{\Gamma, x : \varphi \vdash M : \psi}{\Gamma \vdash \lambda x^{\varphi}.M : \varphi \to \psi}\ (\mathrm{PI})$$

Przypisanie termów (2)

$$\frac{\Gamma, x : \varphi_i \vdash M : \sigma}{\Gamma, y : \varphi_1 \wedge \varphi_2 \vdash M[x := y\{i\}] : \sigma}\ (\mathrm{LK})$$

$$\frac{\Gamma, x : \varphi \vdash M : \sigma \quad \Gamma, y : \psi \vdash N : \sigma}{\Gamma, z : \varphi \vee \psi \vdash \mathtt{case}\ z\ \mathtt{of}\ [x]M\ \mathtt{or}\ [y]N : \sigma}\ (\mathrm{LA})$$

$$\frac{\Gamma \vdash M : \varphi \quad \Gamma, x : \psi \vdash N : \sigma}{\Gamma, y : \varphi \to \psi \vdash N[x := yM] : \sigma}\ (\mathrm{LI})$$

$$\Gamma, x : \bot \vdash \varepsilon_\sigma(x)\ (\mathrm{LF})$$

Postaci normalne

Fakt: *Termy dowodowe dla rachunku sekwentów bez cięcia, to dokładnie postaci normalne ze względu na beta-redukcje i permutacje.*

Wniosek: *Jeśli* $\vdash \alpha \vee \beta$, *to* $\vdash \alpha$ *lub* $\vdash \beta$.

Dowód: Jeśli $\varnothing \vdash M : \alpha \vee \beta$, to $M = \mathsf{in} \ldots$.
Inaczej: żadna reguła nie pasuje oprócz $(R\vee)$.

No dobrze, ale dlaczego to nie działa dla logiki klasycznej?

Bo jest jeszcze skracanie z prawej.

Linear logic: the data flow paradigm

- Correctness criterion = construction respecting resources.
- Intuitionistic construction is a *function*, linear construction is an *action*.
- An assumption has to be used (consumed) exactly once: cannot be re-used nor abandoned.
- But some resources are re-usable ($!\alpha$).

Rules for conjunction in sequent calculus

First choice:

$$\frac{\Sigma, \alpha \vdash \rho}{\Sigma, \alpha \wedge \beta \vdash \rho}\,(L\&) \qquad \frac{\Gamma \vdash \alpha \quad \Gamma \vdash \beta}{\Gamma \vdash \alpha \wedge \beta}\,(R\&)$$

Second choice:

$$\frac{\Sigma, \alpha, \beta \vdash \rho}{\Sigma, \alpha \wedge \beta \vdash \rho}\,(L\otimes) \qquad \frac{\Gamma \vdash \alpha \quad \Delta \vdash \beta}{\Gamma, \Delta \vdash \alpha \wedge \beta}\,(R\otimes)$$

Dwie koniunkcje

Wraz (with):

$$\frac{\Sigma, \alpha \vdash \rho}{\Sigma, \alpha \,\&\, \beta \vdash \rho}\,(L\&) \qquad \frac{\Gamma \vdash \alpha \quad \Gamma \vdash \beta}{\Gamma \vdash \alpha \,\&\, \beta}\,(R\&)$$

Tensor:

$$\frac{\Sigma, \alpha, \beta \vdash \rho}{\Sigma, \alpha \otimes \beta \vdash \rho}\,(L\otimes) \qquad \frac{\Gamma \vdash \alpha \quad \Delta \vdash \beta}{\Gamma, \Delta \vdash \alpha \otimes \beta}\,(R\otimes)$$

Tensor

An object of type $\alpha \otimes \beta$ is a pair of objects: one of type α, the other of type β. Creating each component of the pair requires separate resources. Consuming a pair requires using both components.

$$\frac{\Sigma, \alpha, \beta \vdash \rho, \Pi}{\Sigma, \alpha \otimes \beta \vdash \rho, \Pi}\,(L\otimes) \qquad \frac{\Gamma \vdash \alpha, \Pi \quad \Delta \vdash \beta, \Sigma}{\Gamma, \Delta \vdash \alpha \otimes \beta, \Pi, \Sigma}\,(R\otimes)$$

With

An object of type $\alpha \,\&\, \beta$ is a "virtual" pair of objects (one of type α, the other of type β), from which exactly one can be potentially created from the same resources. In other words, $\alpha \,\&\, \beta$ is a "right of choice" between α or β. This right belongs to the consumer.

$$\frac{\Sigma, \alpha \vdash \rho, \Pi}{\Sigma, \alpha \,\&\, \beta \vdash \rho, \Pi}\,(L\&) \qquad \frac{\Gamma \vdash \alpha, \Pi \quad \Gamma \vdash \beta, \Pi}{\Gamma \vdash \alpha \,\&\, \beta, \Pi}\,(R\&)$$

Lizak

Linear implication $\alpha \multimap \beta$ represents the type of process in which the assumption (resource) α is processed into the conclusion β, without re-using any part of it, and without leaving any unused garbage.

$$\frac{\Gamma \vdash \varphi, \Sigma \quad \Delta, \psi \vdash \Pi}{\Gamma, \Delta, \varphi \multimap \psi \vdash \Sigma, \Pi}\,(\mathrm{L}\multimap) \qquad \frac{\Gamma, \varphi \vdash \psi, \Sigma}{\Gamma \vdash \varphi \multimap \psi, \Sigma}\,(\mathrm{R}\multimap)$$

Negacja i dualność

Negation: Linear negation $\alpha^\perp$ is the dual type of α. Producing data of type α is the same as consuming data of type $\alpha^\perp$.

$$\frac{\Gamma \vdash \varphi, \Sigma}{\Gamma, \varphi^\perp \vdash \Sigma}\,(\mathrm{L}^\perp) \qquad \frac{\Gamma, \varphi \vdash \Sigma}{\Gamma \vdash \varphi^\perp, \Sigma}\,(\mathrm{R}^\perp)$$

Note: Implications $\alpha \multimap \beta$ and $\beta^\perp \multimap \alpha^\perp$ are equivalent. (Analogy with electric current.)

Plus: An object of type $\alpha \oplus \beta$ is a pair consisting of an object of type α or of type β, and a flag showing which case actually holds. The right of choice between α or β belongs to the producer. The consumer opens a box and uses the contents according to the instruction on the flag.

$$\frac{\Gamma, \varphi \vdash \Sigma \quad \Gamma, \psi \vdash \Sigma}{\Gamma, \varphi \oplus \psi \vdash \Sigma}\,(\mathrm{L}\oplus) \qquad \frac{\Gamma \vdash \varphi_i, \Sigma}{\Gamma \vdash \varphi_1 \oplus \varphi_2, \Sigma}\,(\mathrm{R}\oplus)$$

Duality: Plus ($\oplus$) is the other side of With ($\&$):

$$(\alpha \oplus \beta)^\perp \multimap\!\!\circ\; \alpha^\perp \,\&\, \beta^\perp$$

$$(\alpha \,\&\, \beta)^\perp \multimap\!\!\circ\; \alpha^\perp \oplus \beta^\perp$$

(Receiving a surprise is sending the right of choice.)

Of course: Type $!\alpha$ represents the ability to create *any required* amount of data of type α.
(Consumer of $!\alpha$ makes the decision.)

Maybe: An object of type $?\alpha$ is the ability to consume *a certain* amount of data of type α.
(Producer of $?\alpha$ makes the decision.)

Duality: $(!\alpha)^\perp \multimap\!\circ\, ?(\alpha^\perp)$ and $(?\alpha)^\perp \multimap\!\circ\, !(\alpha^\perp)$

Przykład obiadowy

$$10\ zł \multimap (pomidorowa \,\&\, krupnik) \otimes (kotlet \,\&\, ryba) \otimes (!ziemniaki \,\&\, !ryż) \otimes (kompot \oplus jabłko)$$

Tego nie udowodnimy:

- $\alpha, \alpha \nvdash \alpha$;
- $\alpha,\ \alpha \multimap \alpha \multimap \beta \nvdash \beta$;
- $\alpha, \alpha, \alpha \multimap \beta, \beta \multimap \beta \multimap \gamma \nvdash \gamma$;
- $\nvdash \alpha \multimap \beta \multimap \alpha$
- $\nvdash (\alpha \multimap \beta \multimap \gamma) \multimap (\alpha \multimap \beta) \multimap \alpha \multimap \gamma$.

Równoważność

$$\alpha \multimap\!\circ\, \beta \quad := \quad (\alpha \multimap \beta) \,\&\, (\beta \multimap \alpha)$$

Fakt: $\Gamma \vdash \alpha \multimap\!\circ\, \beta$ *wtw, gdy* $\Gamma \vdash \alpha \multimap \beta$ *oraz* $\Gamma \vdash \beta \multimap \alpha$.

What is dual to $\otimes$?

$$(\alpha \otimes \beta)^{\perp} \multimap \alpha^{\perp} \parr \beta^{\perp} \qquad (\alpha \parr \beta)^{\perp} \multimap \alpha^{\perp} \otimes \beta^{\perp}$$

$$\frac{\Gamma, \alpha \vdash \Sigma \quad \Delta, \beta \vdash \Pi}{\Gamma, \Delta, \alpha \parr \beta \vdash \Sigma, \Pi}\ (\mathrm{L}\parr) \qquad \frac{\Gamma \vdash \alpha, \beta, \Sigma}{\Gamma \vdash \alpha \parr \beta, \Sigma}\ (\mathrm{R}\parr)$$

Par: Type $\alpha \parr \beta$ represents *communication*: a "fair contract" between α and β. (Receiving a pair of type $\alpha \otimes \beta$ is the same as sending $\alpha^{\perp} \parr \beta^{\perp}$ ii.e., sending entanglement of $\alpha^{\perp}$ and $\beta^{\perp}$.)

$$(\alpha \multimap \beta) \multimap \alpha^{\perp} \parr \beta$$

Translacja Girarda

- $p^* = p$, $\top^* = 1$, $\bot^* = 0$;
- $(\alpha \wedge \beta)^* = \alpha^* \,\&\, \beta^*$;
- $(\alpha \vee \beta)^* = !\alpha^* \oplus !\beta^*$;
- $(\alpha \to \beta)^* = !\alpha^* \multimap \beta^*$.

Twierdzenie:

Następujące warunki są równoważne:

1) $\Gamma \vdash \varphi$ w logice intuicjonistycznej;
2) $!\Gamma^* \vdash \varphi^*$ w intuicjonistycznej logice liniowej;
3) $!\Gamma^* \vdash \varphi^*$ w klasycznej logice liniowej.

Logika intuicjonistyczna

Wykład 12

17 maja 2012

Logika pierwszego rzędu: składnia

Sygnatura: Ustalone symbole relacyjne, funkcyjne i stałe. Sygnatura może być nieskończona.

Termy: Zmienne $a, b, \ldots$, stałe, wyrażenia $ft_1 \ldots t_n$.

Formuły:

– atomowe: $rt_1 \ldots t_n$, $\bot$;

– $\varphi \to \psi$, $\varphi \vee \psi$, $\varphi \wedge \psi$;

– $\forall a\, \varphi$, $\exists a\, \varphi$.

Zmienne wolne: $\mathrm{FV}(\forall a\, \varphi) = \mathrm{FV}(\exists a\, \varphi) = \mathrm{FV}(\varphi) - \{a\}$.

Utożsamiamy formuły różniące się tylko zmiennymi związanymi.

Semantyka klasyczna

Struktura (model) dla sygnatury $f, g, \ldots, r, s, \ldots$:

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

Wartościowanie: funkcja $\zeta : \mathrm{Zmienne} \to A$.

Wartość termu: $[\![f\, t_1 \ldots t_n]\!]_\zeta = f^A([\![t_1]\!]_\zeta, \ldots, [\![t_n]\!]_\zeta)$

Wartość formuły:

$$[\![\forall a\, \alpha]\!]_\zeta = \min \{ [\![\alpha]\!]_{\zeta[a \mapsto \mathbf{a}]} \mid \mathbf{a} \in A \}$$

$$[\![\exists a\, \alpha]\!]_\zeta = \max \{ [\![\alpha]\!]_{\zeta[a \mapsto \mathbf{a}]} \mid \mathbf{a} \in A \}$$

Interpretacja BHK

- A construction of $\forall a\, \varphi(a)$ is a method that turns any possible value $\mathbf{d}$ of a into a construction of $\varphi(\mathbf{d})$;
- A construction of $\exists a\, \varphi$ is a pair consisting of a value $\mathbf{d}$ of a and a construction of $\varphi(\mathbf{d})$.

Przykłady niewątpliwe

- $\forall a(\varphi \to \psi) \to (\forall a\varphi \to \forall a\psi)$;
- $\forall a(\varphi \to \psi) \to (\exists a\varphi \to \exists a\psi)$;
- $\neg\exists a\varphi \leftrightarrow \forall a\neg\varphi$;
- $\forall a\varphi \to \exists a\varphi$;
- $\exists a(\psi \wedge \varphi(a)) \leftrightarrow \psi \wedge \exists a\varphi(a)$, gdy $a \notin \mathrm{FV}(\psi)$.

Przykłady wątpliwe

- $\neg\forall a\varphi \leftrightarrow \exists a\neg\varphi$;
- $\forall a(\psi \vee \varphi(a)) \to \psi \vee \forall a\,\varphi(a)$;
- $\neg\neg\forall a\,(\varphi(a) \vee \neg\varphi(a))$;
- $\exists b(\varphi(b) \to \forall a\varphi(a))$;
- $\exists a(\exists b\varphi(b) \to \varphi(a))$.

Naturalna dedukcja

$$(\forall\mathrm{I})\ \frac{\Gamma \vdash \varphi}{\Gamma \vdash \forall a\,\varphi}\ (a \notin \mathrm{FV}(\Gamma)) \qquad (\forall\mathrm{E})\ \frac{\Gamma \vdash \forall a\,\varphi}{\Gamma \vdash \varphi[a := t]}$$

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

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

(Te same reguły dla logiki klasycznej.)

Rachunek sekwentów

$$(\mathrm{L}\forall)\ \frac{\Gamma, \varphi[a := t] \vdash \sigma}{\Gamma, \forall a\varphi \vdash \sigma} \qquad (\mathrm{R}\forall)\ \frac{\Gamma \vdash \varphi}{\Gamma \vdash \forall a\varphi}\ (a \notin \mathrm{FV}(\Gamma))$$

$$(\mathrm{L}\exists)\ \frac{\Gamma, \varphi \vdash \sigma}{\Gamma, \exists a\varphi \vdash \sigma}\ (a \notin \mathrm{FV}(\Gamma, \sigma)) \qquad (\mathrm{R}\exists)\ \frac{\Gamma \vdash \varphi[a := t]}{\Gamma \vdash \exists a\varphi}$$

(Podobne reguły dla logiki klasycznej.)

Rachunek sekwentów

Twierdzenie o eliminacji cięcia pozostaje prawdziwe.

Wniosek 1: Jeśli $\vdash \exists a\,\varphi$, to istnieje takie t, że $\vdash \varphi[a := t]$.

Dowód: Ostatnia musiała być reguła (R$\exists$).

Wniosek 2: Rachunek pierwszego rzędu jest konserwatywny nad rachunkiem zdań.

Dowód: Z zasady podformuł: dowód bez cięcia dla formuły bez kwantyfikatorów nie zawiera kwantyfikatorów.

Aksjomaty w stylu Hilberta

(Q1) $\forall a\varphi \to \varphi[a := t]$;

(Q2) $\varphi[a := t] \to \exists a\varphi$;

(Q3) $\forall a(\varphi \to \psi) \to \varphi \to \forall a\psi$, gdy $a \notin \mathrm{FV}(\varphi)$;

(Q4) $\forall a(\varphi \to \psi) \to \exists a\varphi \to \psi$, gdy $a \notin \mathrm{FV}(\psi)$.

(Te same aksjomaty dla logiki klasycznej.)

Translacja Kołmogorowa

$$
\begin{aligned}
k(rt_1 \dots t_n) &= \neg\neg\, rt_1 \dots t_n \\
k(\bot) &= \bot \\
k(\tau \vee \sigma) &= \neg\neg(k(\tau) \vee k(\sigma)) \\
k(\tau \to \sigma) &= \neg\neg(k(\tau) \to k(\sigma)) \\
k(\tau \wedge \sigma) &= \neg\neg(k(\tau) \wedge k(\sigma)) \\
k(\forall a\,\tau) &= \neg\neg\forall a\, k(\tau) \\
k(\exists a\,\tau) &= \neg\neg\exists a\, k(\tau)
\end{aligned}
$$

Translacja Kołmogorowa

Twierdzenie:

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

Dowód: ($\Rightarrow$) Ćwiczenia.

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

Wniosek: Logika intuicjonistyczna pierwszego rzędu jest nierozstrzygalna. Klasyczny Entscheidungsproblem redukuje się do intuicjonistycznego.

Semantyka Kripkego

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

$c, \varrho \Vdash r t_1 \dots t_n \equiv \mathcal{A}_c, \varrho \models r t_1 \dots t_n$ (klasycznie);

$c, \varrho \nVdash \bot$;

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

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

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

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

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

Twierdzenie o pełności

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: $\Gamma \vdash \varphi \quad \Leftrightarrow \quad \Gamma \Vdash \varphi$

Dowód: ($\Rightarrow$) Indukcja. ($\Leftarrow$) Metoda stałych Henkina.

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 Gliwenki.
(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: $\not\Vdash \forall a(p \vee ra) \to (p \vee \forall a.ra)$

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

$$\mathcal{A}_1 = \langle \{1\}, r^1, p^1 \rangle, \qquad \mathcal{A}_2 = \langle \{1,2\}, r^2, p^2 \rangle$$
$$r^1 = \{1\}, p^1 = \bot, \qquad r^2 = \{1\}, p^2 = \top$$

(Relacje $\bot$ i $\top$ są zeroargumentowe.)

W tym modelu $1 \Vdash \forall a(p \vee ra)$, ale $1 \not\Vdash p \vee \forall a.ra$.

Fakt (Schemat Grzegorczyka)

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

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

Typy zależne (*Dependent types*)

M : **array**(n)	M jest tablicą rozmiaru n;
array : **Int** $\to *$	**array** jest *konstruktorem typu*
Samezera(n) : **array**(n)	tablica z samych zer;
Samezera : **Int** $\to$ **array**(?)	*tak się nie da...*
Samezera : Πn : **Int**. **array**(n)	

Typy zależne (*Dependent types*)

M : **array**(n)	M jest tablicą rozmiaru n;
array : **Int** $\to *$	**array** jest *konstruktorem typu*
Samezera(n) : **array**(n)	tablica z samych zer;
Samezera : **Int** $\to$ **array**(?)	*tak się nie da...*
Samezera : $\forall n$: **Int**. **array**(n)	

Typy zależne (*Dependent types*)

$P(\mathbf{a_1}, \ldots, \mathbf{a_n})$ — a type that *depends* on the choice of individual values $\mathbf{a_1}, \ldots, \mathbf{a_n}$.

$\forall a P(a)$ — a type of a function that turns an arbitrary value $\mathbf{a}$ into something of type $P(\mathbf{a})$.

Rachunek lambda

$$(\forall \mathrm{I})\ \frac{\Gamma \vdash M : \varphi}{\Gamma \vdash (\lambda a\, M) : \forall a\, \varphi}\ (a \notin FV(\Gamma))$$

$$(\forall \mathrm{E})\ \frac{\Gamma \vdash M : \forall a\, \varphi}{\Gamma \vdash (Mt) : \varphi[a := t]}$$

$$(\lambda a.M)t \Rightarrow_\beta M[a := t]$$

Logika intuicjonistyczna

Wykład 12a

24 maja 2012

Semantyka Kripkego

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

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

$c, \varrho \nVdash \bot$;

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

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

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

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

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

Twierdzenie o pełności

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: $\Gamma \vdash \varphi \quad \Leftrightarrow \quad \Gamma \Vdash \varphi$

Dowód: ($\Rightarrow$) Indukcja. ($\Leftarrow$) Metoda stałych Henkina.

Lemat Henkina

Definicja: Zbiór formuł Γ jest *pierwszy* (ze względu na sygnaturę $\mathcal{L}$), gdy:

- $\Gamma \vdash \varphi \vee \psi$ implikuje $\Gamma \vdash \varphi$ lub $\Gamma \vdash \psi$;
- $\Gamma \vdash \exists a\, \varphi(a)$ implikuje $\Gamma \vdash \varphi(\mathbf{s})$, dla pewnego $\mathbf{s} \in \mathcal{L}$.

Lemat: Niech $\Gamma \nvdash \varphi$ (gdzie Γ, φ w sygnaturze $\mathcal{L}$) i niech S będzie nieskończonym zbiorem nowych stałych. Istnieje zbiór Γ', pierwszy nad $\mathcal{L} \cup S$ i taki, że $\Gamma \subseteq \Gamma'$ oraz $\Gamma' \nvdash \varphi$.

Zał.: $\Gamma \nvdash \varphi$, S nieskończony zbiór nowych stałych.
Teza: $\Gamma \subseteq \Gamma' \nvdash \varphi$, zbiór Γ' pierwszy zwn $\mathcal{L} \cup S$.

Dowód: Numerujemy jako ξ_n wszystkie formuły nad $\mathcal{L} \cup S$. Definiujemy taki ciąg zbiorów $\Gamma = \Gamma_0 \subseteq \Gamma_1 \subseteq \Gamma_2 \ldots$, że:

(1) $\Gamma_n \nvdash \varphi$ (2) Γ_n używa tylko skończonego podzbioru S.

Mając Γ_n, weźmy najmniejsze takie m, że $\Gamma_n \vdash \xi_m$, ale:

A) $\xi_m = \exists a\, \psi(a)$ i $\Gamma_n \nvdash \psi(\mathbf{s})$, dla $\mathbf{s} \in S$, albo:
B) $\xi_m = \psi \vee \vartheta$ i $\Gamma_n \nvdash \psi$ i $\Gamma_n \nvdash \vartheta$.

Jeśli takiego m nie ma, to $\Gamma_{n+1} = \Gamma_n$.

Jeśli (B), oraz $\Gamma_n \cup \{\psi\} \nvdash \varphi$, to $\Gamma_{n+1} = \Gamma_n \cup \{\psi\}$.

Wpp. $\Gamma_n \cup \{\vartheta\} \nvdash \varphi$ i $\Gamma_{n+1} = \Gamma_n \cup \{\vartheta\}$.

Zał.: $\Gamma \nvdash \varphi$, S nieskończony zbiór nowych stałych.
Teza: $\Gamma \subseteq \Gamma' \nvdash \varphi$, zbiór Γ' pierwszy zwn $\mathcal{L} \cup S$.

Dowód: Numerujemy jako ξ_n wszystkie formuły nad $\mathcal{L} \cup S$. Definiujemy taki ciąg zbiorów $\Gamma = \Gamma_0 \subseteq \Gamma_1 \subseteq \Gamma_2 \ldots$, że:

(1) $\Gamma_n \nvdash \varphi$ (2) Γ_n używa tylko skończonego podzbioru S.

Mając Γ_n, weźmy najmniejsze takie m, że $\Gamma_n \vdash \xi_m$, ale:

A) $\xi_m = \exists a\, \psi(a)$ i $\Gamma_n \nvdash \psi(\mathbf{s})$, dla $\mathbf{s} \in S$, albo:
B) $\xi_m = \psi \vee \vartheta$ i $\Gamma_n \nvdash \psi$ i $\Gamma_n \nvdash \vartheta$.

Jeśli takiego m nie ma, to $\Gamma_{n+1} = \Gamma_n$.

Jeśli (A), to $\Gamma_{n+1} = \Gamma_n \cup \{\psi(\mathbf{s})\}$, gdzie $\mathbf{s}$ jest nowe.

Gdyby $\Gamma_n \cup \{\psi(\mathbf{s}) \vdash \varphi$, to $\Gamma_n \cup \{\exists a\, \psi(a)\} \vdash \varphi$, czyli $\Gamma_n \vdash \varphi$.

Zał.: $\Gamma \nvdash \varphi$, S nieskończony zbiór nowych stałych.
Teza: $\Gamma \subseteq \Gamma' \nvdash \varphi$, zbiór Γ' pierwszy zwn $\mathcal{L} \cup S$.

Dowód: Mamy ciąg $\Gamma = \Gamma_0 \subseteq \Gamma_1 \subseteq \Gamma_2 \ldots \nvdash \varphi$.

Wtedy $\Gamma' = \bigcup_n \Gamma_n \nvdash \varphi$. Czy zbiór Γ' jest pierwszy?

Przypuśćmy, że $\Gamma' \vdash \psi \vee \vartheta = \xi_m$, ale $\Gamma' \nvdash \psi$, $\Gamma' \nvdash \vartheta$.

Wtedy $\Gamma_n \vdash \xi_m$, dla pewnego n.

Formuła ξ_m jest najdalej m-ta w kolejce, zatem na pewno $\Gamma_{n+m} \vdash \psi$ lub $\Gamma_{n+m} \vdash \vartheta$.

Przypadek $\exists$ jest podobny.

Model ze stałych

Niech $\varnothing = S_0 \subseteq S_1 \subseteq S_2 \subseteq \ldots$, gdzie $S_{n+1} - S_n$ nieskończone.

Definiujemy model Kripkego $\mathcal{C}$:

– Stany, to pary (Δ, n), gdzie Δ pierwszy zwn $\mathcal{L} \cup S_n$.

– Porządek $(\Delta, n) \leq (\Pi, m)$, gdy $\Delta \subseteq \Pi$ oraz $n \leq m$.

– Struktura $\mathcal{A}_c$ dla $c = (\Delta, n)$ to model z termów dla $\mathcal{L} \cup S_n$, w którym $r^{\mathcal{A}} = \{(t_1, \ldots, t_n) \mid \Delta \vdash r t_1 \ldots t_n\}$.

– Wartościowanie $\varrho(a) = a$. Wtedy $[\![t]\!]_\varrho = t$.

Lemat: Dla formuł sygnatury $\mathcal{L} \cup S_n$:

$$(\Delta, n), \varrho \Vdash \psi \quad \Leftrightarrow \quad \Delta \vdash \psi.$$

Lemat: $(\Delta, n), \varrho \Vdash \psi \quad \Leftrightarrow \quad \Delta \vdash \psi.$

Dowód: Indukcja zwn ψ. Przykładowe przypadki:

($\psi = \forall a\, \alpha(a)$, część $\Rightarrow$) Jeśli $\Delta \nvdash \forall a\, \alpha(a)$, to $\Delta \nvdash \alpha(a)$, więc także $\Delta \nvdash \alpha(\mathsf{s})$, gdzie $\mathsf{s} \in S_{n+1} - S_n$.

Niech $\Delta \subseteq \Delta'$ pierwsze zwn $\mathcal{L} \cup S_{n+2}$ i $\Delta' \nvdash \alpha(\mathsf{s})$.
Z założenia indukcyjnego wynika $(\Delta', n+2), \varrho \nVdash \alpha(\mathsf{s})$, sprzeczność.

($\psi = \forall a\, \alpha(a)$, część $\Leftarrow$) Niech $\Delta \vdash \forall a\, \alpha(a)$ i niech $(\Delta, n) \leq (\Delta', m)$. Skoro $\Delta \subseteq \Delta'$, to nadal $\Delta' \vdash \forall a\, \alpha(a)$, skąd $\Delta' \vdash \alpha(t)$, dla dowolnego t. Z założenia indukcyjnego wynika $(\Delta', m), \varrho \Vdash \alpha(t)$, czyli $(\Delta', m), \varrho[a \mapsto t] \Vdash \alpha$.
I o to chodzi.

Dowód: Indukcja zwn ψ. Przykładowe przypadki:

($\psi = \alpha \to \beta$, część $\Rightarrow$) Wystarczy udowodnić, że $\Delta, \alpha \vdash \beta$. Jeśli nie, to $\Delta \cup \{\alpha\} \subseteq \Delta' \nvdash \beta$, gdzie Δ' jest pierwszy ze względu na $\mathcal{L} \cup S_{n+1}$. Z założenia indukcyjnego mamy $(\Delta', n+1) \Vdash \alpha$. Ponieważ $(\Delta, n) \leq (\Delta', n+1)$, więc także $(\Delta', n+1) \Vdash \beta$, skąd $\Delta' \vdash \beta$ z zał. ind. Sprzeczność.

($\psi = \exists a\, \alpha(a)$, część $\Leftarrow$) Wynika z pierwszości.

($\psi = \alpha \vee \beta$, część $\Leftarrow$) Wynika z pierwszości.

Dowód pełności

Przypuśćmy, że $\Gamma \nvdash \varphi$. Jest $\Gamma \subseteq \Delta$, pierwszy zwn $\mathcal{L} \cup S_1$, i taki, że $\Delta \nvdash \varphi$. Z lematu

$$(\Delta, n), \varrho \Vdash \psi \quad \Leftrightarrow \quad \Delta \vdash \psi$$

wynika, że $(\Delta, 1), \varrho \nVdash \varphi$. Ale $(\Delta, 1), \varrho \Vdash \Gamma$, bo $\Gamma \subseteq \Delta$.
Zatem $\Gamma \nVdash \varphi$.

Rachunek lambda

$$(\forall \mathrm{I})\ \frac{\Gamma \vdash M : \varphi}{\Gamma \vdash (\lambda a\, M) : \forall a\, \varphi}\ (a \notin FV(\Gamma))$$

$$(\forall \mathrm{E})\ \frac{\Gamma \vdash M : \forall a\, \varphi}{\Gamma \vdash (Mt) : \varphi[a := t]}$$

$$(\lambda a.M)t \Rightarrow_\beta M[a := t]$$

Typy egzystencjalne?

$$(\exists \mathrm{I})\frac{\Gamma \vdash M : \varphi[a := t]}{\Gamma \vdash [M, t] : \exists a\, \varphi}$$

$$(\exists \mathrm{E})\frac{\Gamma \vdash M : \exists a\, \varphi \quad \Gamma, y : \varphi \vdash N : \psi}{\Gamma \vdash \textbf{let}\ [y{:}\varphi, a] = M\ \textbf{in}\ N : \psi}\ (a \notin FV(\Gamma \cup \{\psi\}))$$

Typy egzystencjalne = abstrakcyjne

$[M, t] : \exists a\, \varphi(a)$ – konkretna implementacja

$\textbf{let}\ [y{:}\varphi(a), a] = M^{\exists a\, \varphi(a)}\ \textbf{in}\ N^{\psi} : \psi$

– użycie danej implementacji M w kontekście N.

Redukcja: $\textbf{let}\ [y{:}\varphi, a] = [M, t]\ \textbf{in}\ N \Rightarrow_\beta N[a := t][y := M]$

$\textbf{Array} = \exists n.\, \textbf{array}(n)$

$\mathit{Suma} : \textbf{Array} \to \textbf{int}$

$\mathit{Append} : \textbf{Array} \to \textbf{Array} \to \textbf{Array}$

Curry-Howard

Theorem
A first-order formula α is intuitionistically valid if and only if there exists M such that $\vdash M : \alpha$.

Warning: A normal inhabitant $\lambda x{:}\forall a\alpha.[xb, b]$ of $\forall a\alpha \to \exists a\alpha$ has free variable b.

Wycieranie zależności z typów

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

Wycieranie zależności z termów (1)

- $\kappa(x^{\varphi}) = x^{\kappa(\varphi)}$
- $\kappa(\lambda x{:}\varphi.M) = \lambda x{:}\kappa(\varphi).\kappa(M)$
- $\kappa(MN) = \kappa(M)\kappa(N)$
- $\kappa(\langle M, N\rangle) = \langle \kappa(M), \kappa(N)\rangle$
- $\kappa(\pi_i(M)) = \pi_i(\kappa(M))$
- $\kappa(\mathbf{inl}\, M) = \mathbf{inl}\, \kappa(M)$
- $\kappa(\mathbf{inr}\, M) = \mathbf{inr}\, \kappa(M)$
- $\kappa(\mathbf{case}\, M\, \mathbf{of}\, [x]P, [y]Q) = \mathbf{case}\, \kappa(M)\, \mathbf{of}\, [x]\kappa(P), [y]\kappa(Q)$

Wycieranie zależności z termów (2)

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

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

Silna normalizacja

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

Na przykład:

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

Lemat: *Każdy ciąg redukcji indywiduowych jest skończony.*

Dowód: Maleje liczba lambd.

Silna normalizacja

Twiedzenie: *Termy dla logiki pierwszego rzędu mają własność silnej normalizacji.*

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.

Postaci normalne

Lemat: *Let M be a term in normal form without free proof variables. Then:*

0) *M is not of type $\bot$.*
1) *If $M : \varphi \vee \psi$ then $M = \mathbf{in}_i\, N$, for some i and N.*
2) *If $M : \exists a \varphi$ then $M = [N, t]$ for some N, t.*

Wnioski:

- *Logika pierwszego rzędu jest niesprzeczna ($\nvdash \bot$).*
- *Jeśli $\vdash \varphi \vee \psi$, to $\vdash \varphi$ lub $\vdash \psi$.*
- *Jeśli $\vdash \exists a\, \varphi$, to $\vdash \varphi[a := t]$.*

Semantyka algebraiczna

Definicje:

Algebra Heytinga jest *zupełna*, wtw, gdy każdy podzbiór ma kres górny i dolny.

Niech $\mathcal{H}$ – (zupełna) algebra Heytinga. Wtedy $\mathcal{H}$-strukturą nazywamy twór postaci $\mathcal{A} = \langle A, f^A, g^A, \ldots, r^A, s^A, \ldots \rangle$, gdzie $r^A : A^{n_r} \to \mathcal{H}$, $s^A : A^{n_s} \to \mathcal{H}, \ldots$

(Relacje rozumiemy jako funkcje o wartościach w $\mathcal{H}$.)

Semantyka algebraiczna

Znaczenie formuły φ w $\mathcal{H}$-strukturze: $[\![\varphi]\!]_\zeta \in \mathcal{H}$.

- $[\![r(t_1, \ldots, t_n)]\!]_\zeta = r^{\mathcal{A}}(\zeta(t_1), \ldots, \zeta(t_n))$;
- $[\![\alpha \to \beta]\!]_\zeta = \mathrm{Int}(\sim [\![\alpha]\!]_\zeta \cup [\![\beta]\!]_\zeta)$;
- $[\![\alpha \vee \beta]\!]_\zeta = [\![\alpha]\!]_\zeta \cup [\![\beta]\!]_\zeta$;
- $[\![\alpha \wedge \beta]\!]_\zeta = [\![\alpha]\!]_\zeta \cap [\![\beta]\!]_\zeta$;
- $[\![\bot]\!]_\zeta = \emptyset$;
- $[\![\exists a\, \varphi]\!]_\zeta = \sup_{\mathbf{a} \in A} [\![\varphi]\!]_{\zeta[a \mapsto \mathbf{a}]}$
- $[\![\forall a\, \varphi]\!]_\zeta = \inf_{\mathbf{a} \in A} [\![\varphi]\!]_{\zeta[a \mapsto \mathbf{a}]}$

Piszemy $\mathcal{A}, \zeta \models \varphi$, gdy $[\![\varphi]\!]_\zeta = 1_{\mathcal{H}}$.

Twierdzenie o pełności

Twierdzenie:

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

Dowód: (1) Indukcja.

(2) Budujemy algebrę formuł $\mathcal{L}_\Gamma$. W tej algebrze zachodzi:

$[\forall a\, \alpha(a)]_\sim = \inf_t [\alpha(t)]_\sim$ oraz $[\exists a\, \alpha(a)]_\sim = \sup_t [\alpha(t)]_\sim$

W algebrze termów $\mathcal{A}$ niech $r^{\mathcal{A}}(t_1, \ldots, t_n) = [r t_1 \ldots t_n]_\sim$.
Wtedy $\mathcal{A}$ jest $\mathcal{L}_\Gamma$-strukturą i $[\![\varphi]\!]_{id} = [\varphi]_\sim$ dla każdego φ.

Jeśli $\Gamma \models \varphi$, to $[\![\varphi]\!]_{id} = 1$ i dobrze... ??

Nie bardzo: 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 $\inf_{\mathcal{G}} B = \inf_{\mathcal{H}} B$.*

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

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

Przykład 1: $\neg\neg\forall a(ra \vee \neg ra)$

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

Przykład 2: $\forall a(p \vee ra) \to p \vee \forall a.ra$

Relacje: $r^{\mathcal{A}}(n) = (-\infty, -\frac{1}{n}) \cup (\frac{1}{n}, \infty)$, $p^{\mathcal{A}} = (-2, 2)$.

Zasada Markowa

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

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

$$r^{\mathcal{A}}(n) = (-\infty, w_n) \cup (w_n, \infty),$$

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

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

Zadanie domowe:

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

Logika intuicjonistyczna

Wykład 14

31 maja 2012

Logika drugiego rzędu w stylu Henkina

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

Reguły wnioskowania:

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

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

$$(*) \qquad R \notin \mathrm{FV}(\Gamma, \psi)$$

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

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

definiuje standardowe liczby naturalne.

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

Wniosek: *Nie ma pełnego systemu wnioskowania (bo nie ma zwartości).*

Brouwer-Heyting-Kołmogorow

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

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 $\mathbf{n} = \lambda fx.\, f^n x$.
Liczebnik $\mathbf{n}$ jest wytarciem dowodu formuły $Nat(s^n(0))$.

Dygresja: „Program extraction"

Przypuśćmy, że mamy dowód formuły postaci

$$\forall a(Nat(a) \to \exists b\,(Nat(b) \wedge W(a, b)).$$

Ta formuła wyciera się do typu postaci $\omega \to \omega \wedge \tau$.
Dowód wyciera się (w odpowiednim rachunku lambda) do termu $F : \omega \to \omega \wedge \tau$. Wtedy term

$$\lambda a.Fa\{1\} : \omega \to \omega$$

definiuje funkcję f o własności

$$\forall a(Nat(a) \to W(a, f(b))).$$

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* $\varphi(\mathbf{P})$.

Naturalna dedukcja

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

$$(\exists \mathrm{I})\ \frac{\Gamma \vdash \varphi[p := \vartheta]}{\Gamma \vdash \exists p\, \varphi} \qquad (\exists^2 \mathrm{E})\ \frac{\Gamma \vdash \exists p\, \varphi \quad \Gamma, \varphi \vdash \psi}{\Gamma \vdash \psi}\ (*)$$

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

Dwa slogany

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

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

  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.

Siła wyrazu: suma/alternatywa

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

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

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

Siła wyrazu: iloczyn/koniunkcja

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

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

Siła wyrazu: zbiór (typ) pusty czyli fałsz

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

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

Siła wyrazu: kwantyfikator szczegółowy

$$x \in \bigcup_p A_p \;\Leftrightarrow\; \forall Q(\forall P(A_p \subseteq Q) \to x \in Q)$$

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

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 $I\tau$ 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)

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

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

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

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:

$v(p) \in D_c$, 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: *Warunki* $\vdash \varphi$ *i* $\Vdash \varphi$ *są równoważne.*

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.*

Rachunek lambda z $\forall$ i $\exists$

$$\frac{\Gamma \vdash M : \alpha}{\Gamma \vdash \Lambda p M : \forall p \alpha}\ (*) \qquad \frac{\Gamma \vdash M : \forall p \alpha(p)}{\Gamma \vdash M\beta : \alpha(\beta)}$$

$$\frac{\Gamma \vdash M : \alpha(\beta)}{\Gamma \vdash [\beta, M] : \exists p \alpha(p)}$$

$$\frac{\Gamma \vdash M : \exists p \alpha(p) \quad \Gamma, x{:}\alpha(p) \vdash N : \gamma}{\Gamma \vdash \text{unpack } M \text{ as } x : \alpha(p) \text{ in } N : \gamma}\ (**)$$

(*) p not free in Γ (**) p not free in Γ nor γ

Reductions

Beta:

$$(\Lambda p M)\beta \ \Rightarrow\ M[p := \beta]$$

$$\text{unpack } [\beta, M]^{\exists p\, \alpha(p)} \text{ as } x{:}\alpha(p) \text{ in } N^\gamma \ \Rightarrow\ N[p := \beta][x := M].$$

Permutations:

$$\mathit{elim}(\text{unpack } M \text{ as } x{:}\alpha \text{ in } N) \Rightarrow$$
$$\Rightarrow \text{unpack } M \text{ as } x{:}\alpha \text{ in } \mathit{elim}(N)$$

Normal forms

Introductions: $\lambda x:\tau.\, N$, $\Lambda p\, N$, $\langle N_1, N_2\rangle$, $\mathrm{in}_i(N)$, $[\tau, N]$;

Proper eliminators: x, PN, $P\tau$, $P\{i\}$;

Improper eliminators: $\varepsilon_\varphi(P)$, case P of $[x]N_1$ or $[y]N_2$, unpack P as $x:\sigma$ in N,

[N — normal form, P — proper eliminator]

Suffixes

- $\tau \in S(\tau)$;
- If $\alpha \to \beta \in S(\tau)$ then $\beta \in S(\tau)$;
- If $\alpha \wedge \beta \in S(\tau)$ then $\alpha, \beta \in S(\tau)$;
- If $\forall p\, \alpha \in S(\tau)$ then $\alpha[p := \beta] \in S(\tau)$, for all types β.

Lemma: *If $\Gamma, x:\tau \vdash P:\sigma$, and P is a proper eliminator beginning with x, then $\sigma \in S(\tau)$.*

Targets

Below, the symbol $\mathbb{A}$ stands for the set of all atoms.

- $T(\bot) = \{\bot\}$ and $T(p) = \{p\}$, for a type variable;
- $T(\alpha \to \beta) = T(\beta)$;
- $T(\alpha \diamond \beta) = T(\alpha) \cup T(\beta)$, for $\diamond \in \{\wedge, \vee\}$;
- $T(\forall p\, \alpha) = \begin{cases} \mathbb{A}, & \text{if } p \in T(\alpha); \\ T(\alpha), & \text{otherwise;} \end{cases}$
- $T(\exists p\, \alpha) = \begin{cases} \mathbb{A}, & \text{jeśli } T(\alpha) = \mathbb{A}; \\ T(\alpha) - \{p\}, & \text{w przeciwnym przypadku.} \end{cases}$

Lemma: *If $\Gamma \vdash a$, where a is an atom (a variable or $\bot$) then $a \in T(\Gamma)$, or $\bot \in T(\Gamma)$ and $\Gamma \vdash \bot$.*

Warning

With bound targets anything can be a suffix:

$$x\tau M^\gamma : \tau, \quad \text{where } x : \forall p(\gamma \to p).$$

Dangerous case: $\forall p\, \varphi$ with $p \in T(\varphi)$.

Good news: either $T(\tau) = \mathbb{A}$ or $T(\tau) \subseteq \mathrm{FV}(\tau)$.

Splits

A suffix is *weak* when it is of the form $\alpha \vee \beta$ or $\exists p\, \alpha$.
An *indirect* target is a target of a weak suffix.

Lemma: *Assume that* $\Gamma \vdash \zeta$ *and* $\Gamma \nvdash \bot$. *Then there exists a "split"* $\Gamma \vdash \exists \vec{p}(\sigma_1 \vee \cdots \vee \sigma_n)$ *such that, for all* i,

- *targets of* σ_i *are either in* $\vec{p}$ *or are indirect targets of* Γ;
- $\Gamma, \sigma_i \nvdash \bot$;
- *there is a constructor or a proper eliminator* N_i *with* $\Gamma, \sigma_i \vdash N_i : \zeta$.

(A split can be trivial: $\exists p\, p$.)

Separation of second-order

Lemma: *If* $\vdash \alpha \to \forall p(p \vee \neg p)$, *and* $\forall$ *does not occur in* α, *then* $\vdash \alpha \leftrightarrow \bot$.

Proof: From $\alpha \vdash \forall p(p \vee \neg p)$ it follows that $\alpha \vdash p \vee \neg p$ for p not free in α, in particular for p fresh.

There is a split $\alpha \vdash \exists \vec{p}(\sigma_1 \vee \cdots \vee \sigma_n)$ with $\alpha, \sigma_i \vdash P_i : p \vee \neg p$, where all P_i are either introductions or proper eliminators.

Since p is not a target at the lhs, proper eliminators are excluded, so either $\alpha, \sigma_i \vdash p$ or $\alpha, \sigma_i \vdash \neg p$, for each i.

As p is not free at lhs, either $\alpha, \sigma_i \vdash \forall p\, p$ or $\alpha, \sigma_i \vdash \forall p\, \neg p$, in other words, $\alpha, \sigma_i \vdash \bot$, for all i. Therefore $\alpha \vdash \bot$.

Separation of second-order

Corollary: *The universal quantifier is not definable from the other connectives in the intuitionistic second-order propositional logic: there is no formula* α *without* $\forall$ *such that* $\vdash \alpha \leftrightarrow \forall p(p \vee \neg p)$.

Proof: Immediate from the Lemma, as $\forall p(p \vee \neg p) \nvdash \bot$.

Existence property

Lemma: *If* $\Gamma \vdash \exists p\, \beta(p)$ *and* Γ *contains no quantifiers, then* $\Gamma \vdash \beta(\sigma_1) \vee \cdots \vee \beta(\sigma_n)$, *for some* $\sigma_1, \ldots, \sigma_n$.

Proof: Induction wrt the length of a normal proof. The only interesting case is $\Gamma \vdash \mathtt{case}\ P^{\gamma \vee \delta}\ \mathtt{of}\ [x]Q\ \mathtt{or}\ [y]R : \exists p\, \beta(p)$ where we apply induction to Q and R obtaining $\Gamma, \gamma \vdash \beta(\sigma_1) \vee \cdots \vee \beta(\sigma_n)$ and $\Gamma, \delta \vdash \beta(\sigma_{n+1}) \vee \cdots \vee \beta(\sigma_m)$. Clearly, $\Gamma \vdash \beta(\sigma_1) \vee \cdots \vee \beta(\sigma_m)$.

Separation of second-order

Corollary: *The existential quantifier is not definable from the propositional connectives in the intuitionistic second-order propositional logic: there is no propositional formula α such that $\vdash \alpha \leftrightarrow \exists q((p \to (\neg q \vee q)) \to p)$.*

Proof: Write $\beta(p,q)$ for $(p \to (\neg q \vee q)) \to p$, and assume that $\vdash \alpha \leftrightarrow \exists q\, \beta(p,q)$. Then $\alpha \vdash \beta(p,\sigma_1) \vee \cdots \vee \beta(p,\sigma_n)$, whence $\beta(p,q) \vdash \beta(p,\sigma_1) \vee \cdots \vee \beta(p,\sigma_n)$, if q not in σ_i.

No suffix of $\beta(p,q)$ is disjunction, so the proof is introduction, and we have $\beta(p,q) \vdash \beta(p,\sigma)$, for some σ, that is,

$$(p \to (\neg q \vee q)) \to p,\ p \to (\neg\sigma \vee \sigma) \vdash p.$$

proof continued

(...) for some σ with $q \notin \mathrm{FV}(\sigma)$:

$$(p \to (\neg q \vee q)) \to p,\ p \to (\neg\sigma \vee \sigma) \vdash p.$$

An ex-falso proof requires a proper eliminator of type $\bot$.

A proof by case-elimination requires a shorter proof of p.

So the *shortest* proof is by proper elimination. Then

$$(p \to (\neg q \vee q)) \to p,\ p \to (\neg\sigma \vee \sigma),\ p \vdash \neg q \vee q,$$

and therefore also $\neg\sigma \vee \sigma,\ p \vdash \neg q \vee q$.

proof continued

$$(\ldots) \qquad \neg\sigma \vee \sigma,\ p \vdash \neg q \vee q.$$

Since $\neg\sigma \vee \sigma,\ p \nvdash \bot$, we have a split

$$\neg\sigma \vee \sigma,\ p \vdash \exists \vec{r}(\sigma_1 \vee \cdots \vee \sigma_n)$$

$$\neg\sigma \vee \sigma,\ p,\ \sigma_i \vdash \neg q \vee q.$$

As q is not a target, $\neg\sigma \vee \sigma,\ p,\ \sigma_i \vdash \neg q$, for each i.

But then $\neg\sigma \vee \sigma,\ p \vdash \neg q$ – contradiction.

Nierozstrzygalność

Theorem 1 (M.H. Löb):

There is an effective (Logspace) *reduction from the intuitionistic first-order logic to second- order propositional intuitionistic logic.*

Question: Does it hold with function symbols?

Wniosek: *Zdaniowa logika drugiego rzędu jest nierozstrzygalna* (*wystarczy* $\{\forall, \to\}$ *lub* $\{\exists, \to, \vee, \wedge, \neg\}$).

Uwaga: *Fragmenty* $\{\exists, \wedge, \neg\}$ *i* $\{\forall, \exists, \wedge, \neg\}$ *są rozstrzygalne (Tatsuta, Fujita i inni).*

Logika intuicjonistyczna

Niedobitki z 2012

31 maja 2012

Coding of first-order logic

Goal: Reduce first-order logic (no terms) to propositional second-order logic.

Idea: Translate every formula φ to a formula $\overline{\varphi}$, replacing each atom $\mathrm{P}(a,b)$ by a certain formula $\overline{\mathrm{p}}(a,b)$. Prove that $\Gamma \vdash \varphi$ in first-order logic iff $\overline{\Gamma} \vdash \overline{\varphi}$ in second-order logic.

Difficulty (in $\Leftarrow$): An universal assumption $x : \forall a \varphi(a)$ in $\overline{\Gamma}$ can be instantiated as $x\tau : \varphi(A)$ where A is an *ad hoc* type. That can be used to play dirty tricks.

Solution: Use bounded quantification $\overline{\forall a \psi} = \forall a(\mathcal{U}(a) \to \overline{\psi})$, where $\mathcal{U}(A)$ holds (almost) only for individual variables.

Coding of first-order logic

- $\overline{\mathrm{P}(a,b)} = \mathrm{p}(a,b)$ and $\overline{\bot} = \star$;
- $\overline{\vartheta \diamond \psi} = \overline{\vartheta} \diamond \overline{\psi}$, for $\diamond \in \{\to, \wedge, \vee\}$;
- $\overline{\forall a \psi} = \forall a(\mathcal{U}(a) \to \overline{\psi})$ and $\overline{\exists a \psi} = \exists a(\mathcal{U}(a) \wedge \overline{\psi})$.

Definitions:

- $A^\bullet = A \to \bullet$;
- $\mathrm{p}_{AB} = (A^\bullet \to \mathrm{p}_1) \to (B^\bullet \to \mathrm{p}_2) \to \mathrm{p}$;
- $\mathrm{p}(A,B) = \mathrm{p}_{AB} \vee \star$;
- $\mathcal{U}(A)$ is the conjunction of all types of the form
$$(A^\bullet \to \mathrm{p}_i) \to \circ \quad \text{and} \quad A^\bullet \to \triangledown.$$

Representing individual variables

Recall that $\mathcal{U}(A)$ is the conjunction of all types of the form $(A^\bullet \to \mathrm{p}_i) \to \circ$ and $A^\bullet \to \triangledown$

and $\quad \mathrm{p}(A,B) = ((A^\bullet \to \mathrm{p}_1) \to (B^\bullet \to \mathrm{p}_2) \to \mathrm{p}) \vee \star$

Def: A variable a *represents* type A in Γ iff the conditions

$$\Gamma, A^\bullet \vdash a^\bullet, \qquad \Gamma, A^\bullet \to \mathrm{p}_i \ \vdash a^\bullet \to \mathrm{p}_i,$$

hold for every relation symbol P and every $i \in \{1,2\}$.

(Note that this suffices e.g., for $\Gamma \vdash \mathrm{p}(A,B) \leftrightarrow \mathrm{p}(a,b)$.)

Uniqueness

Lemma: Assume that no individual variable nor $\bullet$, $\bot$, p_i, q_j are in $T(\Gamma)$. If $\Gamma, A^\bullet \vdash a^\bullet$, and $\Gamma, A^\bullet \to \mathrm{p}_i \ \vdash b^\bullet \to \mathrm{q}_j$, then $a = b$, $\mathrm{p} = \mathrm{q}$ and $i = j$.

Proof: From $\Gamma, A^\bullet \vdash a^\bullet$ we obtain $\Gamma, a^\bullet \to \mathrm{p}_i \vdash A^\bullet \to \mathrm{p}_i$. Therefore $\Gamma, a^\bullet \to \mathrm{p}_i \vdash b^\bullet \to \mathrm{q}_j$ and thus $\Gamma, x : a^\bullet \to \mathrm{p}_i, \ y : b^\bullet \vdash N : \mathrm{q}_j$, for some normal form N. Since $\mathrm{q}_j, \bot \notin T(\Gamma)$, we must have $\mathrm{q}_j = \mathrm{p}_i$. Similarly $\mathrm{p}_i \notin T(\Gamma, b^\bullet)$, so we have $\Gamma, a^\bullet \to \mathrm{p}_i, b^\bullet \vdash a^\bullet$, i.e., $\Gamma, a^\bullet \to \mathrm{p}_i, b \to \bullet, a \vdash \bullet$. We conclude that $\Gamma, a^\bullet \to \mathrm{p}_i, b \to \bullet, a \vdash b$. The only individual variable in $T(\Gamma, a^\bullet \to \mathrm{p}_i, b \to \bullet, a)$ is a, so it must be the case that $a = b$.

Reducing arbitrary types to variables

Fact: *Under some conditions on* Γ *(like that* $\circ$ *and* $\triangledown$ *only occur in some* $\mathcal{U}(a)$*'s) if* $\Gamma \vdash \mathcal{U}(A)$*, then there exists a unique individual variable* a *representing* A *in* Γ*.*

Proof: We have $\Gamma \vdash (A^\bullet \to \triangledown) \wedge \bigwedge\{(A^\bullet \to \mathrm{p}_i) \to \circ \mid \mathrm{all}\ \mathrm{p}, i\}$. Targets $\circ$ and $\triangledown$ must come from some $\mathcal{U}(a)$'s, perhaps different. In every component of a certain split we have $\Gamma, A^\bullet, \sigma_k \vdash a^\bullet$, for some a, and in some other split we have $\Gamma, A^\bullet \to \mathrm{p}_i, \tau_l \ \vdash b^\bullet \to \mathrm{q}_j$. But then $\mathrm{p}_i = \mathrm{q}_j$ and $a = b$, by the previous Lemma applied to Γ, σ_k, τ_l.

No surprise possible

Lemma: Assume that Δ satisfies some conditions (such as Δ only consists of formulas $\overline{\varphi}(A)$, $\mathcal{U}(a)$, p_{CD}, and all such C, D are represented by ind. variables).

If $\Delta \vdash \mathrm{p}_{AB}$, where A and B are represented in Δ by individual variables then there is $\mathrm{p}_{CD} \in \Delta$ such that A and C are represented in Δ by the same individual variable, and similarly for B and D.

Definitions:

For first-order Σ:

$\overline{\Sigma} = \{\overline{\varphi} \mid \varphi \in \Sigma\} \cup \{\mathcal{U}(a) \mid a \in FV(\Sigma)\}$.

For second-order Γ, consisting ony of $\overline{\varphi}(A)$, $\mathcal{U}(a)$, p_{CD}

$|\Gamma| = \{\varphi(\vec{a}) \mid \overline{\varphi}(\vec{A}) \in \Gamma, \text{ for some } \vec{A}, \text{ and } \vec{a} \text{ represent } \vec{A} \text{ in } \Gamma\}$

Note that $|\overline{\Sigma}| = \Sigma$.

Main result

Main Lemma: *Under some conditions on* Γ, *if* $\Gamma \vdash \overline{\varphi}(\vec{A})$ *with* $\Gamma \vdash \mathcal{U}(A)$ *for each* $A \in \vec{A}$, *then* $|\Gamma| \vdash \varphi(\vec{a})$, *in first-order logic, where* $\vec{a}$ *represent* $\vec{A}$ *in* Γ.

Proof: Essentially routine induction.

Therefore: *If* $\overline{\Sigma} \vdash \overline{\varphi}$ *then* $\Sigma \vdash \varphi$.

Conclusions

Theorem 1:

There is an effective (Logspace) *syntactic reduction from the intuitionistic first-order logic to second- order propositional intuitionistic logic.*

Question: Does it hold with function symbols?

Theorem 2:

The $\forall$*-free fragment* $\{\exists, \to, \vee, \wedge, \neg\}$ *of second-order intuitionistic propositional logic is undecidable.*

NB. Fragments $\{\exists, \wedge, \neg\}$ and $\{\forall, \exists, \wedge, \neg\}$ are decidable. (Tatsuta, Fujita and others)