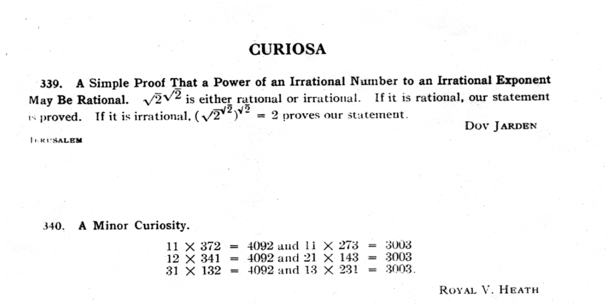
Logika i teoria typów

Wykład 2

12 października 2022

Logika intuicjonistyczna

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 pojechał na targ i kupił osła;*
  - *Kupił osła, chyba że przepił pieniądze;*
  - *Teraz jeśli ma osła, to go bije.*
- Mogą być inne modele i inne wynalazki.

Brouwer: paradygmat konstrukcji

- 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 *podmiot kreatywny*.
- Dowód istnienia obiektu wymaga więc jego *konstrukcji*.
- To samo dotyczy prawdy matematycznej:
  "There are no non-experienced truths" (Brouwer)
- Wnioskowanie jest pierwotne, semantyka jest wtórna, *albo raczej: właściwą semantyką jest konstrukcja.*

Tako rzecze Brouwer:

The belief in the universal validity of the principle of the excluded third in mathematics is considered by the intuitionists as a phenomenon of the history of civilization of the same kind as the former belief in the rationality of pi, or in the rotation of the firmament about the earth.

(*L.E.J. Brouwer, 1951*)

Brouwer-Heyting-Kołmogorow

- Sens spójnika logicznego: sposób w jaki konstrukcja zdania złożonego zależy od konstrukcji składowych.
- *Konstrukcja dla* $\varphi \wedge \psi$ *polega na podaniu konstrukcji dla* φ *i konstrukcji dla* ψ*;*
- *Konstrukcja dla* $\varphi \vee \psi$ *polega na wskazaniu jednego ze składników* φ, ψ *i podaniu konstrukcji dla tego składnika.*

Brouwer-Heyting-Kołmogorow

- *Konstrukcja dla implikacji* $\varphi \to \psi$ *to metoda (funkcja) przekształcająca każdą konstrukcję przesłanki* φ *w konstrukcję dla konkluzji* ψ*.*
- *Nie ma konstrukcji dla fałszu* $\perp$*.* *(„the thing which is not”).*

Negacja: $\neg\varphi = \varphi \to \perp$.

- *Konstrukcja dla* $\neg\varphi$ *to metoda obracająca każdą ewentualną konstrukcję* φ *w absurd*

Składnia rachunku zdań

- *Zmienne zdaniowe* $(p, q, r, \ldots)$ są formułami.
- Stała $\perp$ 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 $\alpha \to \perp$.
- Napis $\top$ jest skrótem napisu $\perp \to \perp$.
- 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

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

Trochę mniej oczywiste

- $(p \to q \to r) \to (p \to q) \to p \to r$;
- $p \to q \to p$;
- $\perp \to p$;
- $(p \vee q) \to \neg p \to q$, w szczególności:
- $(p \vee \neg p) \to \neg\neg p \to p$;

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).

Zasada wyłączonego środka nie ma konstrukcji

. . . 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*)

Przykłady nieoczywiste, ale poprawne:

- $\neg\neg(p \vee \neg p)$;
- $(p \to \neg q) \to (\neg p \to \neg q) \to \neg q$;
- Wiele innych podobnych.

Przykład: Konstrukcja dla $\neg\neg(p \vee \neg p)$:

Należy otrzymać absurd $\perp$ z założenia $\neg(p \vee \neg p)$.
W tym celu skonstruujemy $p \vee \neg p$, wskazując na $\neg p$.
Zakładamy więc p i znowu:
Należy otrzymać absurd $\perp$ z założenia $\neg(p \vee \neg p)$.
W tym celu skonstruujemy $p \vee \neg p$, wskazując na . . . p!

Implementacja BHK: naturalna dedukcja

- Reguły *wprowadzania*[1] spójników logicznych: jak można udowodnić formułę danej postaci?
- Reguły *eliminacji* spójników: jak można wykorzystać formułę tej postaci do udowodnienia innej?

[1] introduction

Tradycyjna notacja dla naturalnej dedukcji: implikacja

$$\dfrac{\begin{array}{c}\vdots\\ \tau \to \sigma\end{array} \qquad \begin{array}{c}\vdots\\ \tau\end{array}}{\sigma} \qquad\qquad \dfrac{\begin{array}{c}\cancel{\tau}\\ \vdots\\ \sigma\end{array}}{\tau \to \sigma}$$

Tradycyjna notacja dla naturalnej dedukcji: implikacja

$$\dfrac{\begin{array}{c}\vdots\\ \tau \to \sigma\end{array} \qquad \begin{array}{c}\vdots\\ \tau\end{array}}{\sigma} \qquad\qquad \dfrac{\begin{array}{c}[\tau]\\ \vdots\\ \sigma\end{array}}{\tau \to \sigma}$$

Tradycyjna notacja dla naturalnej dedukcji: implikacja

$$\dfrac{\begin{array}{c}\vdots\\ \tau \to \sigma\end{array} \qquad \begin{array}{c}\vdots\\ \tau\end{array}}{\sigma} \qquad\qquad \dfrac{\begin{array}{c}[\tau]_i\\ \vdots\\ \sigma\end{array}}{\tau \to \sigma}\, i$$

Normalizacja dowodu: implikacja

$$\dfrac{\begin{array}{c}(*)\\ \vdots\\ \tau\end{array} \qquad \dfrac{\begin{array}{c}[\tau]^{(i)}\\ \vdots\\ \sigma\end{array}}{\tau \to \sigma}\,(i)}{\sigma} \qquad \Longrightarrow \qquad \begin{array}{c}(*)\\ \vdots\\ \tau\\ \vdots\\ \sigma\end{array}$$

Normalizacja dowodu: implikacja

$$\dfrac{\begin{array}{c}(*)\\ \vdots\\ \tau\end{array} \qquad \dfrac{\begin{array}{c}[\tau]^{(i)}\\ \vdots\\ \sigma\end{array}}{\tau \to \sigma}\,(i)}{\sigma} \qquad \Longrightarrow \qquad \begin{array}{c}(*)\\ \vdots\\ \tau\\ \vdots\\ \sigma\end{array}$$

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

Tradycyjna notacja dla naturalnej dedukcji: koniunkcja

$$\frac{\begin{array}{c}\vdots\\ \tau\end{array} \qquad \begin{array}{c}\vdots\\ \sigma\end{array}}{\tau \wedge \sigma} \qquad\qquad \frac{\begin{array}{c}\vdots\\ \tau \wedge \sigma\end{array}}{\tau}$$

Normalizacja dowodu: koniunkcja

$$\dfrac{\dfrac{\begin{array}{c}(*)\\ \vdots\\ \tau\end{array} \qquad \begin{array}{c}(**)\\ \vdots\\ \sigma\end{array}}{\tau \wedge \sigma}}{\tau} \quad \Longrightarrow \quad \begin{array}{c}(*)\\ \vdots\\ \tau\end{array}$$

Tradycyjna notacja dla naturalnej dedukcji: alternatywa

$$\frac{\begin{array}{c}\vdots\\ \tau\end{array}}{\tau \vee \sigma} \qquad\qquad \frac{\begin{array}{c}\vdots\\ \tau \vee \sigma\end{array} \quad \begin{array}{c}[\tau]\\ \vdots\\ \rho\end{array} \quad \begin{array}{c}[\sigma]\\ \vdots\\ \rho\end{array}}{\rho}$$

Normalizacja dowodu: alternatywa

$$\dfrac{\dfrac{\begin{array}{c}(*)\\ \vdots\\ \tau\end{array}}{\tau \vee \sigma} \quad \begin{array}{c}[\tau]^{(i)}\\ \vdots\\ \rho\end{array} \quad \begin{array}{c}[\sigma]^{(i)}\\ \vdots\\ \rho\end{array}}{\rho}\,(i) \quad \Longrightarrow \quad \begin{array}{c}(*)\\ \vdots\\ \tau\\ \vdots\\ \rho\end{array}$$

Dowód w stylu Jaśkowskiego

Załóżmy $(p \to q) \to p$
 Załóżmy $\neg p$.
  Załóżmy p.
  Ponieważ p oraz $\neg p$, więc $\bot$.
  Ponieważ $\bot$, więc q.
 Zatem $p \to q$
 Ponieważ $p \to q$ oraz $(p \to q) \to p$, więc p.
 Ponieważ p i $\neg p$, więc $\bot$.
Zatem $\neg\neg p$.

Zatem $((p \to q) \to p) \to \neg\neg p$.

Notacja w stylu Gentzena

Dowodzimy *osądów*[2] postaci $\Gamma \vdash A$, gdzie Γ jest zbiorem formuł, a A jest formułą. Sens: A wynika z założeń Γ.

Przykład:

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

[2] judgments

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 $\Delta, \alpha \vdash \alpha$.

Reguły wnioskowania dla rachunku zdań (1)

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

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

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

Reguły wnioskowania dla rachunku zdań (2)

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

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

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

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

Reguły wnioskowania dla rachunku zdań...

... są w pliku duch.mimuw.edu.pl/~urzy/Litt/reguly_nd.pdf
i oczywiście na Moodlu.

Classical (unnatural) deduction

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

Inna reguła eliminacji koniunkcji

$$\frac{\Gamma \vdash A \wedge B \qquad \Gamma, A, B \vdash C}{\Gamma \vdash C}$$

Przykład

$$\frac{p \vdash p}{\vdash p \to p}(\to \mathrm{I})$$

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

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

Przykład

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

Notacja dla dowodów

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

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

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

Notacja dla dowodów

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

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

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

Notacja dla dowodów

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

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

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

Właśnie wymyśliliśmy rachunek lambda z typami prostymi.

Normalizacja dowodu to beta-redukcja

$$\dfrac{\begin{array}{c}(*)\\ \vdots\\ \tau\end{array} \qquad \dfrac{\begin{array}{c}[\tau]^{(i)}\\ \vdots\\ \sigma\end{array}}{\tau\to\sigma}\,(i)}{\sigma} \qquad\Longrightarrow\qquad \begin{array}{c}(*)\\ \vdots\\ \tau\\ \vdots\\ \sigma\end{array}$$

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

Natural Deduction: proste własności

- **Osłabianie (weakening):**

  Jeśli $\Gamma \vdash \varphi$ *oraz* $\Gamma \subseteq \Delta$, *to* $\Delta \vdash \varphi$.

- **Podstawianie (substitution):**

  Jeśli $\Gamma \vdash \varphi$, *to* $\Gamma[p := \psi] \vdash \varphi[p := \psi]$.

Dowód: Indukcja ze względu na dowód.

Rozszerzony rachunek λ: fałsz i koniunkcja

$$\frac{\Gamma \vdash M : \bot}{\Gamma \vdash M[\sigma] : \sigma}$$

Write also $\varepsilon_\sigma(M)$ for $M[\sigma]$.

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

Koniunkcja to iloczyn kartezjański. Fałsz to typ pusty.

Alternatywa to suma prosta

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

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

Write also case M of $[u]R$ or $[v]Q$ for $M[u.R, v.Q]$
inl, inr for in_1, in_2.

Uwaga:
Notacja $\mathsf{in}_i(M)$ jest niejednoznaczna. Powinno być np. $\mathsf{in}_i^{\alpha_1 \vee \alpha_2}(M)$.