Lean & ITP

Michał Dobranowski

10 października 2025

Spis treści

1. Wstęp teoretyczny

Aby zrozumieć, dlaczego systemowi wspomagającego dowodzenie (ang. *proof assistant*) możemy ufać bardziej niż tuszowi na papierze, należy zrozumieć narzędzia oferowane przez logikę, rachunek lambda oraz teorię typów, na których zbudowany jest każdy znany autorowi tego typu system. Chociaż ten kurs nigdy nie miał być teoretyczny, zdaniem autora formalizmy dotyczące (typowanego) rachunku lambda są niezwykle ciekawe, więc w odpowiednich miejscach Czytelnik jest zachęcany do pogłębienia wiedzy, w tym też przeprowadzenia lub przeczytania dowodów przytaczanych twierdzeń.

1.1. Logika intuicjonistyczna

Logika intuicjonistyczna (konstruktywna) to system logiczny będący alternatywą dla logiki klasycznej. Nie różni się od niej składnią, ale regułami wnioskowania. Fałsz oznaczamy przez $\bot$, prawdę przez $\top$, a pisząc $\Gamma \vdash A$ mamy na myśli, że formuła A jest dowodliwa z założeń Γ.

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

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ (\wedge\,\mathrm{I}) \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\ (\wedge\,\mathrm{E1}) \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\ (\wedge\,\mathrm{E2})$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ (\vee\,\mathrm{I1}) \qquad \frac{\Gamma \vdash A}{\Gamma \vdash B \vee A}\ (\vee\,\mathrm{I2}) \qquad \frac{\Gamma \vdash A \vee B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}\ (\vee\,\mathrm{E})$$

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

Rysunek 1: Reguły wnioskowania w intuicjonistycznym rachunku zdań (IRZ).

Oprócz tego, definiujemy negację jako $\neg A := A \to \bot$. Dzięki tej definicji oraz regule $(\to\,\mathrm{E})$ możemy wywieść

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

Przykład 1.1

Pokaż, że w IRZ zachodzi *słabe prawo podwójnej negacji*, czyli $A \to \neg\neg A$.

Rozwiązanie. Z definicji negacji mamy $\neg\neg A = (A \to \bot) \to \bot$, więc musimy pokazać $A \to ((A \to \bot) \to \bot)$.

$$\dfrac{\dfrac{\dfrac{A, A \to \bot \vdash A \to \bot \qquad A, A \to \bot \vdash A}{A, A \to \bot \vdash \bot}\ (\to\,\mathrm{E})}{A \vdash (A \to \bot) \to \bot}\ (\to\,\mathrm{I})}{\vdash A \to ((A \to \bot) \to \bot)}\ (\to\,\mathrm{I})$$

□

Przykład 1.2

Pokaż, że w IRZ zachodzi *prawo kontrapozycji*, czyli $(A \to B) \to (\neg B \to \neg A)$.

Rozwiązanie. Z definicji negacji mamy $\neg B = B \to \bot$ oraz $\neg A = A \to \bot$, więc musimy pokazać $(A \to B) \to ((B \to \bot) \to (A \to \bot))$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A \to B, B \to \bot, A \vdash B \to \bot \qquad \dfrac{A \to B, B \to \bot, A \vdash A \to B \qquad A \to B, B \to \bot, A \vdash A}{A \to B, B \to \bot, A \vdash B}\,(\to \mathrm{E})}{A \to B, B \to \bot, A \vdash \bot}\,(\to \mathrm{E})}{A \to B, B \to \bot \vdash A \to \bot}\,(\to \mathrm{I})}{A \to B \vdash (B \to \bot) \to (A \to \bot)}\,(\to \mathrm{I})}{\vdash (A \to B) \to ((B \to \bot) \to (A \to \bot))}\,(\to \mathrm{I})$$

□

1.1.1. Związek z logiką klasyczną

Dokładając do reguł wnioskowania IRZ *silne prawo podwójnej negacji* ($\neg\neg A \to A$) lub *prawo wyłączonego środka* ($A \vee \neg A$), otrzymujemy logikę klasyczną. W przypadku prawa podwójnej negacji jest to oczywiste. W przypadku prawa wyłączonego środka (EM) można to pokazać następująco:

$$\dfrac{\dfrac{}{(A \to \bot) \to \bot \vdash A \vee (A \to \bot)}\,(\mathrm{EM}) \qquad (A \to \bot) \to \bot, A \vdash A \qquad \dfrac{\Gamma \vdash (A \to \bot) \to \bot \qquad \Gamma \vdash A \to \bot}{\dfrac{\Gamma \vdash \bot}{\Gamma \vdash A}\,(\bot \mathrm{E})}\,(\to \mathrm{E})}{\dfrac{(A \to \bot) \to \bot \vdash A}{\vdash (A \to \bot) \to \bot \to A}\,(\to \mathrm{I})}\,(\vee \mathrm{E})$$

gdzie $\Gamma = \{(A \to \bot) \to \bot, A \to \bot\}$.

Problem 1.3. Pokazać, że prawo wyłączonego środka nie jest dowodliwe w IRZ.

Problem 1.4. Stwierdzić, które z czterech praw de Morgana są dowodliwe w IRZ.

> **Uwaga** (ciekawostka)
>
> Istnieją tautologie KRZ, które nie są dowodliwe w IRZ, ale po dodaniu do IRZ jako aksjomaty nie prowadzą do logiki klasycznej, tworząc logiki „pomiędzy" intuicjonistyczną i klasyczną. Przykłady:
>
> - IRZ + $(\neg A \vee \neg\neg A)$[a] — logika Jankova (de Morgana), w której zachodzą wszystkie cztery prawa de Morgana,
> - IRZ + $((A \to B) \vee (B \to A))$ — logika Gödla-Dummeta, w której wartościowania formuł można interpretować jako liczby z przedziału $[0, 1]$.
>
> [a] słabe prawo wyłączonego środka

Skoro zbiór reguł wnioskowania IRZ jest podzbiorem zbioru reguł wnioskowania KRZ, to każda formuła dowodliwa IRZ jest również dowodliwa w KRZ.

1.1.2. Semantyka

Trochę zaniedbując formalizmy, skupimy się przez chwilę na wartościowaniach formuł logicznych. Możemy określić *semantykę* dla logiki klasycznej, przypisując formułom prawdziwym wartość 1, a formułom fałszywym wartość 0 (definiując przy okazji funkcje $\wedge, \vee, \to$). Dla logiki intuicjonistycznej jest to trudniejsze, ale i ciekawsze. Pokażemy dwa z (nieskończenie) wielu możliwych sposobów. Oba z nich są *algebrami Heytinga*, których nie będziemy tutaj definiować.

Semantyka topologiczna Możemy zdefiniować semantykę za pomocą topologii na $\mathbb{R}$:

$$\begin{aligned}
[\![\bot]\!] &= \emptyset, \\
[\![\top]\!] &= \mathbb{R}, \\
[\![A \wedge B]\!] &= [\![A]\!] \cap [\![B]\!], \\
[\![A \vee B]\!] &= [\![A]\!] \cup [\![B]\!], \\
[\![A \to B]\!] &= \operatorname{int}\left([\![A]\!]^{\mathsf{C}} \cup [\![B]\!]\right), \\
A &:= \text{dowolny otwarty podzbiór } \mathbb{R}
\end{aligned}$$

Wtedy

$$[\![\neg A]\!] = [\![A \to \bot]\!] = \operatorname{int}\left([\![A]\!]^{\mathsf{C}} \cup \emptyset\right) = \operatorname{int}\left([\![A]\!]^{\mathsf{C}}\right)$$

Można przy pomocy takiej semantyki pokazać, że prawo wyłączonego środka nie jest dowodliwe w IRZ. Pod A możemy podstawić np. zbiór $(0, \infty)$, wtedy

$$[\![A \vee \neg A]\!] = [\![A]\!] \cup [\![\neg A]\!] = [\![A]\!] \cup \operatorname{int}\left([\![A]\!]^{\mathsf{C}}\right) = (0, \infty) \cup (-\infty, 0) \neq \mathbb{R}$$

Semantyka kraty dystrybutywnej Krata to zbiór częściowo uporządkowany, w którym istnieją kresy dolne i górne dowolnych par elementów. Definiujemy działania

$$\begin{aligned}
a \wedge b &:= \inf\{a, b\}, \\
a \vee b &:= \sup\{a, b\}.
\end{aligned}$$

Krata dystrybutywna to krata, w której zachodzą prawa rozdzielności:

$$\begin{aligned}
a \wedge (b \vee c) &= (a \wedge b) \vee (a \wedge c), \\
a \vee (b \wedge c) &= (a \vee b) \wedge (a \vee c).
\end{aligned}$$

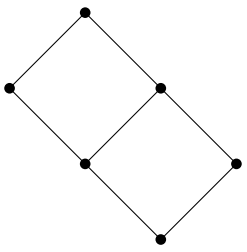
Można udowodnić, że każda niepusta i skończona krata jest ograniczona, czyli posiada elementy najmniejszy i największy. Krata, która jest niepusta, skończona i dystrybutywna posłuży nam do zdefiniowania semantyki:

$$\begin{aligned}
[\![\bot]\!] &= \text{element najmniejszy}, \\
[\![\top]\!] &= \text{element największy}, \\
[\![A \wedge B]\!] &= [\![A]\!] \wedge [\![B]\!], \\
[\![A \vee B]\!] &= [\![A]\!] \vee [\![B]\!], \\
[\![A \to B]\!] &= \sup\{c : c \wedge [\![A]\!] \leqslant [\![B]\!]\}, \\
A &:= \text{dowolny element kraty}
\end{aligned}$$

Wtedy

$$[\![\neg A]\!] = [\![A \to \bot]\!] = \sup\{c : c \wedge [\![A]\!] \leqslant [\![\bot]\!]\} = \sup\{c : c \wedge [\![A]\!] = [\![\bot]\!]\}$$

Biorąc przykładową kratę



możemy udowodnić, że prawo wyłączonego środka nie jest dowodliwe w IRZ. Dowód zostawiamy jako ćwiczenie dla Czytelnika.