Lean & ITP

Michał Dobranowski

5 listopada 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

Typowym przykładem ilustrującym różnicę między logiką klasyczną a intuicjonistyczną (konstruktywną) jest twierdzenie:

> Istnieją takie liczby niewymierne a i b, że a^b jest liczbą wymierną.

oraz jego dowód:

> Jeśli $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$, to $a = b = \sqrt{2}$, w przeciwnym razie niech $a = \sqrt{2}^{\sqrt{2}}$ oraz $b = \sqrt{2}$, wtedy $a^b = 2 \in \mathbb{Q}$.

Dowód ten jest oczywiście słuszny na gruncie logiki klasycznej, ale nie jest konstruktywny, ponieważ dalej nie znamy odpowiednich liczb a i b. W logice konstruktywnej zdanie jest prawdziwe, jeśli można podać jest *konstrukcję* (tzn. intuicyjny dowód), zgodnie z interpretacją Brouwera-Heytinga-Kolmogorowa:

- konstrukcja dla $A \land B$ to konstrukcja dla A oraz konstrukcja dla B,
- konstrukcja dla $A \lor B$ to konstrukcja dla A lub konstrukcja dla B wraz z zaznaczeniem, która z nich to jest,
- konstrukcja dla $A \to B$ to przekształcenie każdej konstrukcji dla A w konstrukcję dla B,
- nie istnieje konstrukcja dla fałszu.

Formalnie, logika intuicjonistyczna to pewien system logiczny. Nie różni się od logiki klasycznej składnią, ale regułami wnioskowania. Fałsz oznaczamy przez $\bot$, a *osąd* zapisany w postaci $\Gamma \vdash A$ oznacza, że formuła A wynika ze zbioru formuł (założeń) Γ. Zamiast $\Gamma \cup \{B\}$ będziemy często pisać Γ, B.

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

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

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

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

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

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

Oznaczamy również prawdę przez $\top := \neg\bot = \bot \to \bot$.

> **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 $A \to ((A \to \bot) \to \bot)$.

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

□

> **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 $(A \to B) \to ((B \to \bot) \to (A \to \bot))$.

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

□

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:

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

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

Problem 1.3. Pokazać, że prawo wyłączonego środka nie jest 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 + $(\neg A \lor \neg\neg A)$[a] — logika Jankova (de Morgana), w której zachodzą wszystkie cztery prawa de Morgana,
> - IRZ + $((A \to B) \lor (B \to A))$ — 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 $\land, \lor, \to$). 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. Warto jednak wiedzieć, że formuła logiczna jest tautologią IRZ wtedy i tylko wtedy, gdy jest prawdziwa w każdej algebrze Heytinga.

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

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

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

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

Semantyka kraty dystrybutywnej Krata to zbiór częściowo uporządkowany, w którym istnieją kresy dolne i górne dowolnych par elementów. Będziemy je przedstawiać za pomocą *diagramów Hassego*[1]. Definiujemy działania

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

[1] Czym dokładnie jest diagram Hassego można dowiedzieć się na Wikipedii.

Krata dystrybutywna to krata, w której zachodzą prawa rozdzielności:

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

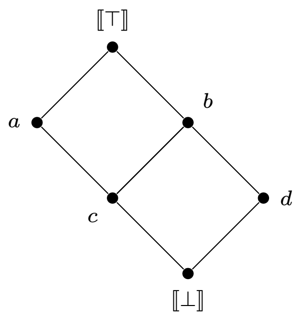
Można udowodnić, że każda niepusta i skończona krata jest ograniczona, czyli posiada elementy najmniejszy i największy. Krata, która jest niepusta, skończona i dystrybutywna posłuży nam do zdefiniowania semantyki:

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

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. Jeśli weźmiemy $[\![A]\!] = c$, to $[\![\neg A]\!] = d$, więc $[\![A \vee \neg A]\!] = c \vee d = b \neq [\![\top]\!]$.

Problem 1.4. Pokazać, że silne prawo podwójnej negacji nie jest dowodliwe w IRZ na podstawie dwóch powyższych semantyk.

Problem 1.5. Stwierdzić, które z czterech praw de Morgana są dowodliwe w IRZ.

1.2. Rachunek lambda

Rachunek lambda to język złożony z termów, z których każdy to:

- zmienna (zazwyczaj oznaczana małą literą, np. x),
- λ-abstrakcja postaci $\lambda x.\, M$, gdzie x jest zmienną, a M jest termem,
- aplikacja postaci MN, gdzie M i N są termami.

Formalnie termy można więc zdefiniować następująco:

$$
M \mathrel{::=} x \mid (\lambda x.\, M) \mid (MM),
$$

gdzie x reprezentuje dowolną zmienną.

Aby uprościć zapis, będziemy pisać MNP zamiast $(MN)P$ – to znaczy stwierdzamy, że aplikacja jest łączna lewostronnie. Ponadto, wiele λ-abstrakcji zapisujemy jako $\lambda x_1 \dots x_n.\, M$, co jest równoważne termowi $\lambda x_1.\, (\lambda x_2.\, (\dots (\lambda x_n.\, M) \dots))$. Kropka w tym zapisie jest bardzo istotna, np.

$$\begin{aligned} \lambda xyz.\, M &= \lambda x.\, (\lambda y.\, (\lambda z.\, M)), \\ \lambda xy.\, zM &= \lambda x.\, (\lambda y.\, (zM)). \end{aligned}$$

W termie $\lambda x.\, M$ zmienna x jest *zmienną związaną* w M. Zmienne występujące w M, które nie są związane przez żadną λ-abstrakcję, nazywamy *zmiennymi wolnymi*. Na przykład w termie $\lambda x.\, (xy)$ zmienna x jest zmienną związaną, a y jest zmienną wolną. W termie $xz(\lambda xy.\, (xyz))$ zmienna x raz występuje jako zmienna wolna, a raz jako związana. Takich sytuacji będziemy unikać ze względów czysto estetycznych.

Zbiór zmiennych wolnych termu M oznaczamy jako $\mathrm{FV}(M)$. Term nazywamy *termem zamkniętym* lub *kombinatorem*, jeśli $\mathrm{FV}(M) = \emptyset$.

Uwaga 1.6

Formalnie definiujemy $\mathrm{FV}(M)$ rekurencyjnie:

$$\begin{aligned} \mathrm{FV}(x) &= \{x\}, \\ \mathrm{FV}(\lambda x.\, M) &= \mathrm{FV}(M) \setminus \{x\}, \\ \mathrm{FV}(MN) &= \mathrm{FV}(M) \cup FV(N). \end{aligned}$$

1.2.1. Alfa-konwersja

α-konwersja to przekształcenie termu, które polega na zmianie nazwy zmiennej (unikając kolizji oznaczeń zmiennych). Wprowadzamy relację równoważności $\equiv_\alpha$ w zbiorze termów Λ w ten sposób, że dane dwa termy M i N są równoważne, jeśli można otrzymać jeden z drugiego poprzez (wielokrotne) α-konwersje. Na przykład:

$$a(\lambda b.\, bc) \equiv_\alpha a(\lambda d.\, dc),$$

natomiast

$$\lambda a.\, ab \not\equiv_\alpha \lambda b.\, bb,$$

ponieważ zamiana zmiennej a na b prowadzi do kolizji oznaczeń zmiennych.

Od tej pory utożsamiamy ze sobą termy różniące się jedynie nazwami zmiennych, czyli jeśli $M \equiv_\alpha N$, to M i N są tym samym termem.

Uwaga 1.7

Bardziej formalnie, od tej pory będziemy operować na klasach abstrakcji relacji $\equiv_\alpha$ (elementach zbioru $\Lambda/{\equiv_\alpha}$), podobnie jak przy działaniach modulo operujemy na klasach abstrakcji relacji przystawania modulo p (elementach zbioru $\mathbb{Z}/{\equiv_p}$).

Będziemy stosować dosyć uniwersalny zapis $M[x := N]$ na term, który powstał z termu M poprzez zastąpienie wszystkich *wolnych* wystąpień zmiennej x termem N. Zakładamy przy tym, że żadna zmienna wolna w N nie zacznie być związana w $M[x := N]$ (ponownie unikamy kolizji oznaczeń).

1.2.2. Beta-redukcja

β-redukcja to taka relacja $\to_\beta$ w zbiorze termów Λ, że $M \to_\beta N$, gdy *β-redeks* postaci $(\lambda x.\, P)Q$ w termie M zostaje zastąpiony przez $P[x := Q]$ w termie N. Bardziej formalnie, jest to najmniejsza relacja w zbiorze Λ spełniająca następujące warunki:

1. $(\lambda x.\, P)Q \to_\beta P[x := Q]$,
2. jeśli $M \to_\beta M'$, to
   - $MN \to_\beta M'N$,
   - $NM \to_\beta NM'$,
   - $\lambda x.\, M \to_\beta \lambda x.\, M'$.

Jeśli w termie występuje więcej niż jeden β-redeks, to β-redukcja nie jest deterministyczna – możemy wybrać dowolny z nich i wykonać redukcję. Przez $\twoheadrightarrow_\beta$ oznaczamy domknięcie przechodnio-zwrotne relacji $\to_\beta$ (czyli najmniejsza relacja przechodnia i zwrotna, która zawiera relację $\to_\beta$), a przez $=_\beta$ jej domknięcie równoważnościowe.

Przykład 1.8

Pokazane poniżej są różne ścieżki redukcyjne dla podanego termu.

$$
\begin{tikzcd}
 & (\lambda x.\, xx)\, z \arrow[drr, "\beta"] & & \\
(\lambda x.\, xx)\, ((\lambda y.\, y)\, z) \arrow[ur, "\beta"] \arrow[dr, "\beta"'] & & & zz \\
 & ((\lambda y.\, y)\, z)\, ((\lambda y.\, y)\, z) \arrow[r, "\beta"'] & ((\lambda y.\, y)\, z)\, z \arrow[ur, "\beta"'] &
\end{tikzcd}
$$

Twierdzenie 1.9 (Churcha-Rossera)

Jeśli $M \twoheadrightarrow_\beta P$ oraz $M \twoheadrightarrow_\beta Q$, to istnieje takie M', że $P \twoheadrightarrow_\beta M'$ i $Q \twoheadrightarrow_\beta M'$.

Jest to jedno z ważniejszych twierdzeń rachunku lambda, mówiące o tym, że relacja $\twoheadrightarrow_\beta$ ma *własność rombu* (ang. *diamond property*), której notabene nie ma relacja $\to_\beta$ (czego dowodzi przykład 1.8). Jeśli dopełnienie przechodnio-zwrotne relacji ma własność rombu, to mówimy, że relacja ta jest *konfluentna*. Powyższe twierdzenie mówi więc, że relacja $\to_\beta$ jest konfluentna.

$$
\begin{tikzcd}
 & M \arrow[dl, two heads, "\beta"'] \arrow[dr, two heads, "\beta"] & \\
P \arrow[dr, two heads, "\beta"'] & & Q \arrow[dl, two heads, "\beta"] \\
 & \cdot &
\end{tikzcd}
$$

Rysunek 2: Własność rombu relacji $\twoheadrightarrow_\beta$.

Prostym wnioskiem z tego twierdzenia jest fakt, że każdy term ma co najwyżej jedną postać normalną, to znaczy pozbawioną β-redeksów. Dlaczego *co najwyżej*, a nie *dokładnie*? Na przykład term

$$\mathbf{\Omega} := (\lambda x.\, xx)\,(\lambda x.\, xx)$$

posiada tylko jeden β-redeks, a jego redukcja prowadzi do termu $\mathbf{\Omega}$ (co Czytelnik raczy sprawdzić), czyli $\mathbf{\Omega} \to_\beta \mathbf{\Omega}$. Term $\mathbf{\Omega}$ nie ma więc postaci normalnej.

1.2.3. Kombinator punktu stałego

Kombinator $\mathbf{Y} := \lambda f.\, (\lambda x.\, f(xx))(\lambda x.\, f(xx))$ nazywamy *kombinatorem punktu stałego*. Ma on tę ciekawą własność, że dla każdego termu $F \in \Lambda$, zachodzi

$$F(\mathbf{Y}(F)) =_\beta \mathbf{Y}(F),$$

ponieważ

$$F(\mathbf{Y}(F)) \to_\beta F((\lambda x.\, F(xx))(\lambda x.\, F(xx)))$$

oraz

$$\begin{aligned} \mathbf{Y}(F) &\to_\beta (\lambda x.\, F(xx))(\lambda x.\, F(xx)) \\ &\to_\beta F((\lambda x.\, F(xx))(\lambda x.\, F(xx)))\,. \end{aligned}$$

Problem 1.10. Znajdź term P taki, że $Px =_\beta P$.

Problem 1.11. Znajdź term P taki, że $Px =_\beta xP$.

1.2.4. Eta-redukcja

η-redukcja to taka relacja $\to_\eta$ w zbiorze termów Λ, że $M \to_\eta N$, gdy *η-redeks* postaci $\lambda x.\, Px$ w termie M zostaje zastąpiony przez P w termie N, zakładając $x \notin \mathrm{FV}(P)$. Bardziej formalnie, jest to najmniejsza relacja w zbiorze Λ spełniająca następujące warunki:

1. jeśli $x \notin \mathrm{FV}(P)$, to $\lambda x.\, Px \to_\eta P$,
2. jeśli $M \to_\eta M'$, to
   - $MN \to_\eta M'N$,
   - $NM \to_\eta NM'$,
   - $\lambda x.\, M \to_\eta \lambda x.\, M'$.

Tak jak poprzednio, domknięcie przechodnio-zwrotne relacji $\to_\eta$ oznaczamy przez $\twoheadrightarrow_\eta$. Ponadto, sumę relacji $\to_\beta$ i $\to_\eta$ oznaczamy przez $\to_{\beta\eta}$, a jej domknięcie przechodnio-zwrotne przez $\twoheadrightarrow_{\beta\eta}$.

Twierdzenie 1.12 (Churcha-Rossera dla η-redukcji i $\beta\eta$-redukcji)
Relacje $\to_\eta$ oraz $\to_{\beta\eta}$ są konfluentne.

1.2.5. Wyrażalność algorytmów w rachunku lambda

Liczby naturalne możemy reprezentować w rachunku lambda za pomocą tzw. *liczebników Churcha*:

$$\mathbf{n} = \lambda fx.\, f^n(x),$$

na przykład

$$\begin{aligned}\mathbf{0} &= \lambda fx.\, x,\\ \mathbf{1} &= \lambda fx.\, f(x),\\ \mathbf{2} &= \lambda fx.\, f(f(x)),\\ \mathbf{3} &= \lambda fx.\, f(f(f(x))).\end{aligned}$$

Wtedy operacja następnika jest reprezentowana przez term

$$\mathbf{succ} = \lambda nfx.\, f(nfx),$$

a dodawanie przez term

$$\mathbf{add} = \lambda mnfx.\, mf(nfx).$$

Instrukcje warunkowe można zaimplementować za pomocą termów

$$\mathbf{true} = \lambda xy.\, x,$$

$$\mathbf{false} = \lambda xy.\, y,$$

wtedy instrukcja warunkowa `if B then M else N` jest reprezentowana przez term

$$\mathbf{if} = \lambda BMN.\, BMN.$$

Istotnie,

$$\begin{aligned}\mathbf{if}\ \mathbf{true}\ M\ N &\to_\beta (\lambda xy.\, x)MN \to_\beta M,\\ \mathbf{if}\ \mathbf{false}\ M\ N &\to_\beta (\lambda xy.\, y)MN \to_\beta N.\end{aligned}$$

Porównanie liczby n do zera można zaimplementować za pomocą termu

$$\mathbf{iszero} = \lambda n.\, n(\lambda x.\, \mathbf{false})\ \mathbf{true}.$$

Problem 1.13. Zdefiniuj w rachunku lambda negację, koniunkcję, alternatywę oraz implikację.

Problem 1.14. Zdefiniuj w rachunku lambda funkcje mnożenia oraz potęgowania liczb naturalnych.

Problem 1.15. Zdefiniuj w rachunku lambda funkcję poprzednika liczby naturalnej. Poprzednik zera powinien zwracać zero.

Problem 1.16. Zdefiniuj w rachunku lambda funkcję obliczającą $n!$.

Twierdzenie 1.17 (Kleene'a)

Każda funkcja częściowo rekurencyjna jest reprezentowalna w rachunku lambda.

Twierdzenie odwrotne również jest prawdziwe. Funkcje częściowo rekurencyjne to dokładnie te funkcje, które są obliczalne przez maszyny Turinga. Z powyższego twierdzenia wynika więc, że rachunek lambda jest modelem obliczalności równoważnym maszynom Turinga.