Logika intuicjonistyczna i izomorfizm Curry'ego Howarda

Julia Majkowska

21 Października 2018

Wstęp

- Logika oparta na konstukcji zmiennej
- Koncepcję przypisuje się matematykowi filozofowi Luitzen Egbertus Jan Brouwer (początek XX w)
- Formalna gałąź logiki od 1930r.

Semantyka

Interpretacja BHK zasad tworzenia formuł

1. Konstrukcja $\phi_1 \wedge \phi_2$ składa się z konstrukcji ϕ_1 i ϕ_2.
2. Konstrukcja $\phi_1 \vee \phi_2$ składa się z kostukcji $i \in \{1, 2\}$ i ϕ_i.
3. Konstrukcja $\phi_1 \rightarrow \phi_2$ to funkcja zamieniająca konstrukcje ϕ_1 na konstrukcje ϕ_2.
4. $\perp$ oznacza brak konstrukcji.
5. $\neg\phi$ to skrócony zapis $\phi \rightarrow \perp$

Example

1. $\perp \rightarrow \phi$
2. $p \rightarrow \neg\neg p$

Semantyka

Konwencje zapisu formuł

1. $\neg p$ to skrót dla $p \to \bot$
2. $p \leftrightarrow q$ to skrót dla $(p \to q) \wedge (q \to p)$
3. $\to$ wiąże do prawej i ma najniższy priorytet
4. $\neg$ ma najwyższy proprytet
5. $\wedge$ i $\vee$ wiążą do lewej i mają ten sam priorytet
6. Nie piszemy najbardziej zewnętrznych nawiasów

Example

$\neg p \wedge q \to r \Leftrightarrow (((\neg p) \wedge q) \to r)$

Dedukcja naturalna logiki intuicjonistycznej

Oznaczenia

1. PV - zbiór wszystkich zmiennych
2. $\Phi ::= \bot | PV | (\Phi \to \Phi) | (\Phi \vee \Phi) | (\Phi \wedge \Phi)$ - zbiór formuł
3. Kontekst to skończony podzbiór Φ.Będziemy używali Γ i Δ do oznaczania kontekstów
4. $\Gamma \vdash p$ intuicyjnie oznacza, że p wynika z założeń Γ.
5. Zamiast $\Gamma \cup \Delta$ będziemy pisać Γ, Δ, a zamiast $\{\} \vdash p$ będziemy pisać $\vdash p$.
6. Formalnym dowodem $\Gamma \vdash p$ jest drzewo, w którym $\Gamma \vdash p$ jest korzeniem, liśćmi są axiomy, a przejścia od ojca do syna odbywają się zgodnie z niżej podanymi zasadmi.
7. Jeśli $\vdash p$ to p jest tautologią logiki inuicjonistycznej

Dedukcja naturalna logiki intuicjonistycznej

$$\Gamma, \varphi \vdash \varphi \ (\mathrm{Ax})$$

$$\frac{\Gamma \vdash \varphi \quad \Gamma \vdash \psi}{\Gamma \vdash \varphi \wedge \psi} \ (\wedge\mathrm{I}) \qquad \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \varphi} (\wedge\mathrm{E}) \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \psi}$$

$$\frac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi} \ (\vee\mathrm{I}) \ \frac{\Gamma \vdash \psi}{\Gamma \vdash \varphi \vee \psi} \qquad \frac{\Gamma, \varphi \vdash \rho \quad \Gamma, \psi \vdash \rho \quad \Gamma \vdash \varphi \vee \psi}{\Gamma \vdash \rho} \ (\vee\mathrm{E})$$

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

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

Przykłady dowodów

(i)

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

(ii)

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

(iii)

$$\dfrac{\dfrac{\dfrac{\dfrac{(\to \mathrm{E})\dfrac{\Gamma \vdash \varphi \to (\psi \to \vartheta) \quad \Gamma \vdash \varphi}{\Gamma \vdash \psi \to \vartheta} \qquad \dfrac{\Gamma \vdash \varphi \to \psi \quad \Gamma \vdash \varphi}{\Gamma \vdash \psi}(\to \mathrm{E})}{\Gamma \vdash \vartheta}\,(\to \mathrm{E})}{\varphi \to (\psi \to \vartheta), \varphi \to \psi \vdash \varphi \to \vartheta}\,(\to \mathrm{I})}{\varphi \to (\psi \to \vartheta) \vdash (\varphi \to \psi) \to (\varphi \to \vartheta)}\,(\to \mathrm{I})}{\vdash (\varphi \to (\psi \to \vartheta)) \to (\varphi \to \psi) \to (\varphi \to \vartheta)}\,(\to \mathrm{I})$$

Własności dedukcji

Lemat

Logika intuicjonistyczna jest zamknięta na osłabienie i podstawienie. To znaczy :

$\Gamma \vdash p \Rightarrow \Gamma, \psi \vdash p$

$\Gamma \vdash p \Rightarrow \Gamma[q := \psi] \vdash p[q := \psi]$

Dowód - indukcja

Logika klasyczna

Wartościowanie dla logiki klasycznej

Niech $v : \Phi \longrightarrow \{0, 1\}$
Zdefinujemy funkcję mapującą $[\cdot]_v : \Phi \longrightarrow \{0, 1\}$, spełniającą :

$$[p]_v = v(p)$$

$$[\bot]_v = 0$$

$$[\phi \vee \psi]_v = max\{[\phi]_v, [\psi]_v\}$$

$$[\phi \wedge \psi]_v = min\{[\phi]_v, [\psi]_v\}$$

$$[\phi \rightarrow \psi]_v = max\{1 - [\phi]_v, [\psi]_v\}$$

Ciało zbiorów

Definicja

Ciało zbiorów nad X to niepusta rodzina pozdbiorów X zamknięta na sumę, przecięcie i dopełnienie zbiorów

Example

1. P(X)
2. $\{\{\}\} \cup X$

Algebra zbiorów

Wartościowanie na zbiorach

Niech $\mathcal{R}$ ciało zbiorów nad zbiorem X.
Wartosciowaniem v w $\mathcal{R}$ nazywamy $v : PV \to \mathcal{R}$
Zdefinujemy funkcję mapującą $[\cdot]_v : \Phi \to X$, spełniającą :

$$[p]_v = v(p)$$

$$[\bot]_v = \{\}$$

$$[\phi \vee \psi]_v = [\phi]_v \cup [\psi]_v$$

$$[\phi \wedge \psi]_v = [\phi]_v \cap [\psi]_v$$

$$[\phi \to \psi]_v = X - [\phi]_v \cup [\psi]_v$$

Twierdzenie

Powyższe dwie semantyki są równoważne.
ϕ jest tautologią $\Leftrightarrow$ $v(\phi) = X$ dla każdego v w $\mathcal{R}$.

Dowód

$\Rightarrow$
Załóżmy nie wprost, że istnieje a takie, że $a \notin v(\phi)$. Więc tworzymy wartościowanie zmiennych w PV takie, że w(p) = 1 wtw. gdy $a \in v(p)$. Indukcyjnie można udowodnić że $w(\phi) \neq 1$.
$\Leftarrow$
Wartościowanie 0/1 kowe to interpretacja $v(\phi) \in \{\{\}, X\}$.

Algebra boolowska

Definicja

Algebrą boolowską nazywamy $\mathcal{B} =< B, \cup, \cap, -, 0, 1 >$, gdzie:

1. $\cup, \cap$ są łączne, przemienne i rozdzielne jedno względem drugiego.
2. $a \cup 0 = a$ i $a \cap 1 = a$
3. $-a \cup a = 1$ i $-a \cap a = 0$

Relacja $a \leqslant b \Leftrightarrow a \cup b = b$ jest częściowym porządkiem dla wszyskich algebr boolowskich. $\cup$ $\cap$ są odpowiednio infimum (glb) i supremum (lub) na tym porządku.

Algebra Lindenbauma

Definicja

Niech Φ - zbiór wszystkich formuł i $\Gamma \in \Phi$
Zdefiniujmy relację $\phi \sim \psi \Leftrightarrow (\Gamma, \phi \vdash \psi) \wedge (\Gamma, \psi \vdash \phi)$. Relacja jest relacją równoważności ponieważ następujące formuły są dowodliwe:

1. $\phi \rightarrow \phi$
2. $(\phi \rightarrow \psi) \rightarrow ((\psi \rightarrow \gamma) \rightarrow (\phi \rightarrow \gamma))$

Zbiór Lindenbauma

Niech $\mathcal{L}_\Gamma = \Phi / \sim = \{[\phi]_\sim : \phi \in \Phi\}$.
Zdefiniujmy częściowy porządek $[\phi]_\sim \leqslant [\psi]_\sim \Leftrightarrow \Gamma, \phi \vdash \psi$

Algebra Lindenbauma

Operatory

Możemy zdefiniować dodatkowe operatory nad $\mathcal{L}_\Gamma$

1. $[\alpha]_\sim \cup [\beta]_\sim = [\alpha \vee \beta]_\sim$
2. $[\alpha]_\sim \cap [\beta]_\sim = [\alpha \wedge \beta]_\sim$
3. $-[\alpha]_\sim = [\neg\alpha]_\sim$
4. $1 = [\bot \to \phi]_\sim$, $0 = [\bot]_\sim$

Dowód

Operatory są dobrze zdefiniowane ponieważ następujące fomuły są dowodliwe

1. $(\alpha \to \alpha') \to ((\beta \to \beta') \to ((\alpha \vee \beta) \to (\alpha' \vee \beta')))$
2. $(\alpha \to \alpha') \to ((\beta \to \beta') \to ((\alpha \wedge \beta) \to (\alpha' \wedge \beta')))$
3. $(\alpha \to \alpha') \to (\neg\alpha' \to \neg\alpha)$

Algebra Lindenbauma

Twierdzenie

$\cup$ i $\cap$ są łączne, przemienne i rozdzielne oraz są operatorami lub i glb na porządku $\leqslant$.

Algebra Heytinga

Definicja

Algebrą Heytinga nazywamy system algebraiczny w postaci $\mathcal{H} =< H, \cup, \cap, \Rightarrow, -, 0, 1 >$ spełniający

1. $\cup, \cap$ są łączne, przemienne i rozdzielne jedno względem drugiego.
2. $a \cup 0 = a$ i $a \cap 1 = a$
3. $a \cup a = a$
4. $a \cap c \leqslant b$ jest równoważne $c \leqslant a \Rightarrow b$ (gdzie $a \leqslant b$ to $a \cup b = b$)
5. $-a = a \Rightarrow 0$

Algebra Heytinga

Definicja

Niech $\mathcal{H} =< H, \cup, \cap, \Rightarrow, -, 0, 1 >$ będzie algebrą Heytinga.
Wartosciowaniem v w $\mathcal{H}$ nazywamy $v : PV \rightarrow H$
Zdefinujmy funkcję mapującą $[\cdot]_v : \Phi \rightarrow H$, spełniającą :

$$[p]_v = v(p)$$

$$[\bot]_v = 0$$

$$[\phi \vee \psi]_v = [\phi]_v \cup [\psi]_v$$

$$[\phi \wedge \psi]_v = [\phi]_v \cap [\psi]_v$$

$$[\phi \rightarrow \psi]_v = [\phi]_v \Rightarrow [\psi]_v$$

Dowodliwość a algebra Heytinga

Twierdzenie

Następujące zdania sa równoważne

1. $\Gamma \vdash \phi$
2. $\Gamma \models \phi$ tzn. $\forall_{\mathcal{C},v}(\forall_{\gamma \in \Gamma} v(\gamma) = 1) \Rightarrow v(\phi) = 1$

Twierdzenie

1. Formuła ϕ o długości n jest dowodliwa jeśli jest prawdziwa we wszystkich algebrach Heytinga o liczności nie większej niż 2^{2^n}
2. Niech $\mathcal{H}$ będzie algebrą wszystkich podzbiorów gestej przestrzeni metrycznej. $\mathcal{H} \models \phi$ wtw. gdy ϕ jest prawdziwe.

Model Kripkego

Definicja

Jeśli $\mathcal{C} =< C, \leqslant, \Vdash, f >$ jest **modelem Kripkego** wtedy :

1. $f : PV \rightarrow C$ $f(p) = inf\{c \in C : c \Vdash p\}$ - wartościowanie ziennych
2. $c \Vdash \phi \vee \psi \Leftrightarrow c \Vdash \phi$ lub $c \Vdash \psi$
3. $c \Vdash \phi \wedge \psi \Leftrightarrow c \Vdash \phi$ i $c \Vdash \psi$
4. $c \Vdash \phi \rightarrow \psi \Leftrightarrow c' \Vdash \psi$ dla każdego c', takiego że $c \leqslant c' c' \Vdash \phi$
5. $c \Vdash \perp$ nie jest prawdą

Wnioski

1. $c \Vdash \neg\phi \Leftrightarrow c' \nVdash \phi$ dla każdego $c' \geqslant c$.
2. $c \leqslant c' \wedge c \Vdash \phi \Rightarrow c' \Vdash \phi$

Zupełność

Twierdzenie

Poniższe zdanie są równoważne

1. $\Gamma \vdash \phi$
2. $c \Vdash \Gamma \Rightarrow c \Vdash \phi$

Logika inuicjonistyczna z samą impllikacją

Twierdzenie

Rachunek zdań z samą implikacją jest zupełny w kontekscie modelu Kripkego. :

1. $\Gamma \vdash \phi$
2. $\mathcal{C} \Vdash \Gamma \Rightarrow \mathcal{C} \Vdash \phi$

są równoważne.

Twierdzenie

Niech ϕ zdanie implikacyjne, a Γ zbiór formuł implikacyjnych. Jeśli $\Gamma \vdash \phi$ jest prawdą w rachunku intuicjonistycznym to jest też prawdą w rachunku z samymi implikacjami.

Dedukcja bez kontekstu

Założenia są umieszczane w liściu drzewa i uwalniane w momencie kiedy stosujemy w dowodzie wprowadzenie implikacji.

$$\dfrac{\dfrac{[\varphi] \qquad \dfrac{(\varphi \to \psi) \wedge (\varphi \to \rho)}{\varphi \to \psi}}{\psi} \qquad \dfrac{[\varphi] \qquad \dfrac{(\varphi \to \psi) \wedge (\varphi \to \rho)}{\varphi \to \rho}}{\rho}}{\dfrac{\psi \wedge \rho}{\varphi \to \psi \wedge \rho}}$$

Normalizacja dowodów

Niektóre dowody wprowadzają nowe spójniki, tylko po to, żeby je wyeliminować później

Example

$$\dfrac{\dfrac{[\varphi]^{(3)}}{\varphi \to \varphi^{(3)}} \qquad \dfrac{\dfrac{[\varphi \to \varphi]^{(1)}}{\psi \to \varphi \to \varphi^{(2)}}}{(\varphi \to \varphi) \to \psi \to \varphi \to \varphi^{(1)}}}{\psi \to \varphi \to \varphi}$$

$$\dfrac{\dfrac{[\varphi]^{(3)}}{\varphi \to \varphi^{(3)}}}{\psi \to \varphi \to \varphi^{(2)}}$$

Normalizacja dowodów

$$\dfrac{\dfrac{\dfrac{\Sigma}{\varphi} \qquad \dfrac{\Pi}{\psi}}{\varphi \wedge \psi}}{\varphi} \quad \to \quad \dfrac{\Sigma}{\varphi}$$

$$\dfrac{\dfrac{\Sigma}{\psi} \qquad \dfrac{\dfrac{\dfrac{[\psi]^{(i)}}{\Pi}}{\varphi}}{\psi \to \varphi^{(i)}}}{\varphi} \quad \to \quad \dfrac{\dfrac{\dfrac{\Sigma}{\psi}}{\Pi}}{\varphi}$$

$$\dfrac{\dfrac{\dfrac{\Theta}{\varphi}}{\varphi \vee \psi} \qquad \dfrac{\dfrac{[\varphi]^{(i)}}{\Sigma}}{\rho} \qquad \dfrac{\dfrac{[\psi]^{(j)}}{\Pi}}{\rho}}{\rho^{(i,j)}} \quad \to \quad \dfrac{\dfrac{\dfrac{\Theta}{\varphi}}{\Sigma}}{\rho}$$

Izomorfizm Currego Howarda

Twierdzenie

Będziemy rozpatrywać część implikacyjną logiki inuicjonistycznej.

1. Jeśli $\Gamma \vdash M : \phi$ to $|\Gamma| \vdash \phi$ gdzie $|\cdot|$ oznacza zbiór typów zbioru zmiennych.
2. Jeśli $\Gamma \vdash \phi$ to istnieje $M \in \Lambda_\pi$ takie, że $\Delta \vdash M : \phi$ gdzie $\Delta = \{(X_\phi : \phi) | \phi \in \Gamma\}$

Dowód - indukcja po konstrukcji formuły / dowodu.

Izomorfizm Currego Howarda a logika intuicjonistyczna

Aby rozszerzyć izomorfizm do pełnego rachunku zdań logiki intuicjonistycznej należy dołożyć następujące typy do prostego typowango rachunku lambda.

$$\begin{array}{lll} \Lambda_\Pi & ::= & \ldots \quad | < \Lambda_\Pi, \Lambda_\Pi > | \pi_1(\Lambda_\Pi) | \pi_2(\Lambda_\Pi) \\ & & \qquad | \mathrm{in}_1^{\psi \vee \varphi}(\Lambda_\Pi) | \mathrm{in}_2^{\psi \vee \varphi}(\Lambda_\Pi) | \mathrm{case}(\Lambda_\Pi; V.\Lambda_\Pi; V.\Lambda_\Pi) \end{array}$$

Izomorfizm Currego Howarda a logika intuicjonistyczna

Należy dołożyć także dodatkowe zasady typowanie i redukcji

$$\frac{\Gamma \vdash M : \psi \quad \Gamma \vdash N : \varphi}{\Gamma \vdash < M, N >: \psi \wedge \varphi} \qquad \frac{\Gamma \vdash M : \psi \wedge \varphi}{\Gamma \vdash \pi_1(M) : \psi} \qquad \frac{\Gamma \vdash M : \psi \wedge \varphi}{\Gamma \vdash \pi_2(M) : \varphi}$$

$$\frac{\Gamma \vdash M : \psi}{\Gamma \vdash \mathrm{in}_1^{\psi \vee \varphi}(M) : \psi \vee \varphi} \qquad \frac{\Gamma \vdash M : \varphi}{\Gamma \vdash \mathrm{in}_2^{\psi \vee \varphi}(M) : \psi \vee \varphi}$$

$$\frac{\Gamma \vdash L : \psi \vee \varphi \quad \Gamma, x : \psi \vdash M : \rho \quad \Gamma, y : \varphi \vdash N : \rho}{\Gamma \vdash \mathrm{case}(L; x.M; y.N) : \rho}$$

$$\begin{array}{lcl} \pi_1(< M_1, M_2 >) & \to & M_1 \\ \pi_2(< M_1, M_2 >) & \to & M_2 \end{array}$$

$$\begin{array}{lcl} \mathrm{case}(\mathrm{in}_1^{\varphi}(N); x.K; y.L) & \to & K\{x := N\} \\ \mathrm{case}(\mathrm{in}_2^{\varphi}(N); x.K; y.L) & \to & L\{y := N\} \end{array}$$

Przedstawienie dowodu jako λ termu

Można zauważyć podobieństwa pomiędzy cechami dowodu a cechami λ -termu.

$\lambda\rightarrow$	IPC($\rightarrow$)
term variable	assumption
term	construction (proof)
type variable	propositional variable
type	formula
type constructor	connective
inhabitation	provability
typable term	construction for a proposition
redex	construction representing proof tree with redundancy
reduction	normalization
value	normal construction

Przedstawienie dowodu jako λ termu - redukcja

$$\dfrac{\dfrac{\dfrac{y:\psi \vdash y:\psi}{\vdash \lambda y{:}\psi \,.\, y : \psi \to \psi} \qquad \dfrac{x:\varphi \vdash x:\varphi}{\vdash \lambda x{:}\varphi \,.\, x : \varphi \to \varphi}}{\vdash < \lambda x{:}\varphi \,.\, x, \lambda y{:}\psi \,.\, y >: (\varphi \to \varphi) \wedge (\psi \to \psi)}}{\vdash \pi_1(< \lambda x{:}\varphi \,.\, x, \lambda y{:}\psi \,.\, y >) : \varphi \to \varphi}$$

Własność silnej redukcji

Twierdzenie

Każda redukcja termu typowanego rachunku lambda ma skończoną długość.

Ćwiczenia

1. Udowodnij w systemie dedukcji naturalnej używając termów logiki inuicjonistycznej. Staraj się aby powstały dowód był znormalizowany.
   1. $\bot \to p$
   2. $p \to \neg\neg p$
   3. $\neg\neg\neg p \to \neg p$
   4. $(p \to q) \to (\neg q \to \neg p)$
   5. $(\neg p \vee \neg q) \to \neg(q \wedge p)$
   6. $((p \wedge q) \to r) \to (p \to (q \to r))$
2. Znajdź lambda termy odpowiadające tym dowodom.

Ćwiczenia

1. Udowodnij, że $a \leqslant b \Leftrightarrow a \cup b = b$ zdefiniowana na algebrze boolowskiej jest porządkiem częściowym oraz:
    1. $a \cap b \leqslant a$
    2. $a \leqslant b$ wtw $a \cap b = a$
    3. $\cap, \cup$ to odpowiednio infimum i supremum względem porządku $\leqslant$
    4. 0 i 1 to odpowiednio najmiejszy i największy element w tym porządku.
2. Udowodnij izomorfizm Currego Howarda dla cześci implikacyjnej logiki intuicjonistycznej i typowanego rachunku lambda.
3. Udowodnij (korzystając z odpowiedniego modelu Kripkego), że $p \vee \neg p$ nie jest tautologią logiki intuicjonistycznej. (Podpowiedź : istnieje model o $|C| = 2$, dla którego ta formuła nie jest prawdziwa)

Sources I

Morten Heine B. Sørensen, Paweł Urzyczyn
Lectures on the Curry-Howard Isomorphism.

Paweł Urzyczyn
Materiały do wykładu Rachunek Lambda.

Stuart.A Kurz
https://www.classes.cs.uchicago.edu/archive/2003/spring/15300-1/intuitionism.pdf