Logika i teoria typów

Wykład 4

26 października 2022

Semantyka algebraiczna

Algebra formuł

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

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

jest quasi-porządkiem (jest zwrotna i przechodnia).

Równoważność indukowana przez $\leq$

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

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

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

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
  $1 = [\top] = \{\varphi \mid \Gamma \vdash \varphi\}$.
  Uwaga: $[\alpha \to \beta] = 1 \Leftrightarrow [\alpha] \leq [\beta]$.
- Kresem dolnym zbioru $\{[\varphi], [\psi]\}$ jest $[\varphi \wedge \psi]$,
  a kresem górnym jest $[\varphi \vee \psi]$.

Krata (lattice): zbiór częściowo uporządkowany (poset), w którym każdy podzbiór dwuelementowy ma kres górny (l.u.b.) i kres dolny (g.l.b.).

Kraty

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

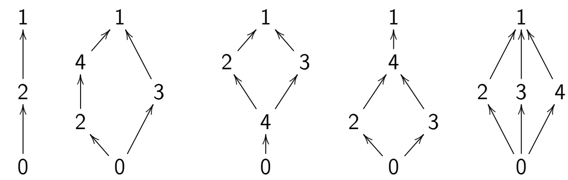
Oznaczenia: $a \sqcup b = \sup\{a, b\}$, $a \sqcap b = \inf\{a, b\}$.

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

Podobny problem z kratą (e).

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)

$x : (\varphi \vee \psi) \wedge \vartheta \vdash$

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

$x : (\varphi \wedge \vartheta) \vee (\psi \wedge \vartheta) \vdash$

$x[z^{\varphi\wedge\vartheta}.\langle \mathsf{in}_1(z\{1\}), z\{2\}\rangle,\ y^{\psi\wedge\vartheta}.\langle \mathsf{in}_2(y\{1\}), y\{2\}\rangle] :$
$(\varphi \vee \psi) \wedge \vartheta$

Algebra Boole'a

Krata dystrybutywna z zerem i jedynką jest *algebrą Boole'a*, gdy dla dowolnego a istnieje *dopełnienie* (complement), 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 niekoniecznie $[\varphi \vee \neg\varphi] = 1$. To nie będzie dopełnienie, więc $\mathcal{L}$ nie będzie algebrą Boole'a.

Pseudodopełnienie (pseudocomplement)

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 $[\alpha] \leq [\varphi \to \bot]$. A to dlatego, że formuły

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

są równoważne. To się nazywa „currying".

Co to jest implikacja?

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

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 $c \sqcap [\beta] \leq [\gamma]$.

Pseudodopełnienie względne (relative p.)

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

Def: *Przestrzeń topologiczna* to zbiór z wyróżnioną rodziną zbiorów *otwartych*. Zbiory otwarte są zamknięte ze względu na dowolne sumy i skończone iloczyny. Zbiór pusty i cała przestrzeń są otwarte.

Wnętrze $\mathrm{Int}(A)$ zbioru A to największy zbiór otwarty zawarty w 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 otwarty i $X \subseteq Y$, to $X \subseteq \mathrm{Int}(Y)$.

Semantyka algebraiczna

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

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

$[\![\varphi]\!]^{\mathcal{H}}_v$ (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 $[\![\varphi]\!]^{\mathcal{H}}_v = 1$;
- $\mathcal{H} \models \varphi$, 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 użytej reguły.

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

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

Twierdzenie o pełności

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

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

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. $\neg\neg p \to p$.

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:

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

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 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.*)

Szkic dowodu: Wystarczy podkrata algebry $\mathcal{H}$ generowana przez wartości podformuł formuły φ. Jest co najwyżej $n = |\varphi|$ podformuł, zatem najwyżej 2^{2^n} elementów.

Uwaga: to nie jest takie proste, bo co z implikacją?

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.

Nie wystarczy jeden skończony model

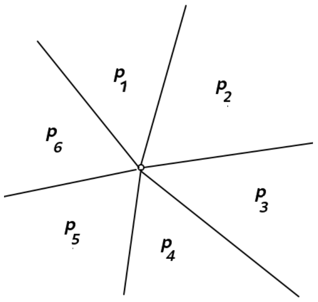
Fakt: *Formuła* $\bigvee\{p_i \to p_j \mid i,j \in \{1,\dots,n\} \wedge i \neq j\}$

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

Morał:

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

$$\not\models \bigvee\{p_i \to p_j \mid i,j \in \{1,\dots,n\} \wedge i \neq j\}$$



Na pocieszenie:

Wystarczy jeden model: np. topologia płaszczyzny.
Albo prostej.

Semantyka topologiczna

- Formuła jest twierdzeniem intuicjonistycznym wtedy i tylko wtedy, gdy jest prawdziwa w każdej algebrze pseudoboole'owskiej (Heytinga);
- Rodzina zbiorów otwartych przestrzeni topologicznej tworzy algebrę Heytinga.
- Nie każda algebra Heytinga jest (izomorficzna z) rodziną zbiorów otwartych przestrzeni topologicznej. (Algebra nie musi być zupełna.)

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 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 $c' \Vdash p$.

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

$$\begin{tikzcd}[row sep=small] & p, \not{q} \\ c : \not{p}, \not{q} \arrow[ur] \arrow[dr] & \\ & q, \not{p} \end{tikzcd}$$

$c \not\Vdash p \vee \neg p \qquad c \Vdash (p \to q) \to q, \qquad c \Vdash \neg\neg(p \vee q)$

Spełnianie w sensie Kripkego

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

Poprawność

Fakt: *Jeśli* $\Gamma \vdash \varphi$, *to* $\Gamma \Vdash \varphi$.

Dowód: Indukcja ze względu na dowód $\Gamma \vdash \varphi$.

Np. jeśli $\Gamma \Vdash \alpha \vee \beta$ oraz $\Gamma, \alpha \Vdash \gamma$ i $\Gamma, \beta \Vdash \gamma$,
to łatwo widzieć, że $\Gamma \Vdash \gamma$.

Pozostałe przypadki też łatwe (ćwiczenia?).

Inaczej: Model Kripkego to w istocie pewna topologia.