Druhá přednáška

NAIL062 Výroková a predikátová logika

Jakub Bulín (KTIML MFF UK)

Zimní semestr 2023

Druhá přednáška

Program

- sémantika výrokové logiky (pokračování)
- normální formy
- vlastnosti a důsledky teorií
- extenze teorií

Materiály

Zápisky z přednášky, Sekce 2.2.5- z Kapitoly 2

Další sémantické pojmy

- výrok φ (nad $\mathbb{P}$) je pravdivý, tautologie, platí (v logice), $\models \varphi$, pokud platí v každém modelu, $\mathrm{M}_{\mathbb{P}}(\varphi) = \mathrm{M}_{\mathbb{P}}$
- lživý, sporný, pokud nemá žádný model, $\mathrm{M}_{\mathbb{P}}(\varphi) = \emptyset$
  (Být lživý není totéž, co nebýt pravdivý!)
- nezávislý, pokud platí v nějakém modelu a neplatí v nějakém jiném modelu, tj. není pravdivý ani lživý, $\emptyset \subsetneq \mathrm{M}_{\mathbb{P}}(\varphi) \subsetneq \mathrm{M}_{\mathbb{P}}$
- splnitelný, pokud má nějaký model, tj. není lživý, $\mathrm{M}_{\mathbb{P}}(\varphi) \neq \emptyset$

výroky φ, ψ (ve stejném jazyce) jsou (logicky) ekvivalentní, $\varphi \sim \psi$, pokud mají stejné modely, tj. $\varphi \sim \psi \;\Leftrightarrow\; \mathrm{M}_{\mathbb{P}}(\varphi) = \mathrm{M}_{\mathbb{P}}(\psi)$

- pravdivé jsou např.: $\top$, $p \vee q \leftrightarrow q \vee p$
- lživé: $\bot$, $(p \vee q) \wedge (p \vee \neg q) \wedge \neg p$
- nezávislé a také splnitelné: p, $p \wedge q$
- ekvivalentní: $p \sim p \vee p$, $p \to q \sim \neg p \vee q$, $\neg p \to (p \to q) \sim \top$

Sémantické pojmy vzhledem k teorii

relativně k dané teorii T (omezíme se na její modely):

- pravdivý/platí v T, důsledek T, $T \models \varphi$ je-li $\mathrm{M}_{\mathbb{P}}(T) \subseteq \mathrm{M}_{\mathbb{P}}(\varphi)$
- lživý/sporný v T pokud $\mathrm{M}_{\mathbb{P}}(\varphi) \cap \mathrm{M}_{\mathbb{P}}(T) = \mathrm{M}_{\mathbb{P}}(T, \varphi) = \emptyset$.
- nezávislý v T pokud $\emptyset \subsetneq \mathrm{M}_{\mathbb{P}}(T, \varphi) \subsetneq \mathrm{M}_{\mathbb{P}}(T)$,
- splnitelný v T, konzistentní s T pokud $\mathrm{M}_{\mathbb{P}}(T, \varphi) \neq \emptyset$ (platí v alespoň jednom modelu T)
- φ a ψ jsou ekvivalentní v T, T-ekvivalentní, $\varphi \sim_T \psi$ platí-li v týchž modelech T, tj. $\varphi \sim_T \psi \;\Leftrightarrow\; \mathrm{M}_{\mathbb{P}}(T, \varphi) = \mathrm{M}_{\mathbb{P}}(T, \psi)$

např. pro $T = \{p \vee q, \neg r\}$:

- výroky $q \vee p$, $\neg p \vee \neg q \vee \neg r$ jsou pravdivé v T
- výrok $(\neg p \wedge \neg q) \vee r$ je v T lživý
- výroky $p \leftrightarrow q$, $p \wedge q$ jsou v T nezávislé, a také splnitelné
- platí $p \sim_T p \vee r$ (ale $p \not\sim p \vee r$)

Univerzálnost logických spojek

množina logických spojek je univerzální, pokud:

- každá booleovská funkce je pravdivostní funkcí nějakého výroku vybudovaného z těchto spojek
- ekvivalentně: každá množina modelů nad konečným jazykem je množinou modelů nějakého výroku

Tvrzení: $\{\neg, \wedge, \vee\}$ a $\{\neg, \rightarrow\}$ jsou univerzální.

[Důkaz na příštím slidu.]

Další zajímavé logické spojky:

- Shefferova spojka (NAND, $\uparrow$) $\quad p \uparrow q \sim \neg(p \wedge q)$,
- Pierceova spojka (NOR, $\downarrow$) $\quad p \downarrow q \sim \neg(p \vee q)$,
- Exclusive-OR (XOR, $\oplus$) $\quad p \oplus q \sim (p \vee q) \wedge \neg(p \wedge q)$

např. $\{\uparrow\}$ je univerzální, $\{\wedge, \vee\}$ není

Důkaz, že $\{\neg, \wedge, \vee\}$ a $\{\neg, \rightarrow\}$ jsou univerzální

Mějme $f\colon \{0,1\}^n \rightarrow \{0,1\}$, resp. $M = f^{-1}[1] \subseteq \{0,1\}^n$

Pro jediný model: $\varphi_v =$ 'musím být model v'

- příklad: $v = (1,0,1,0) \rightsquigarrow \varphi_v = p_1 \wedge \neg p_2 \wedge p_3 \wedge \neg p_4$
- obecně: $v = (v_1, \dots, v_n)$, použijeme značení $p^1 = p$, $p^0 = \neg p$

$$\varphi_v = p_1^{v_1} \wedge p_2^{v_2} \wedge \dots \wedge p_n^{v_n} = \bigwedge_{i=1}^{n} p_i^{v(p_i)} = \bigwedge_{p \in \mathbb{P}} p^{v(p)}$$

Pro více modelů: 'musím být alespoň jeden z modelů z M'

$$\varphi_M = \bigvee_{v \in M} \varphi_v = \bigvee_{v \in M} \bigwedge_{p \in \mathbb{P}} p^{v(p)}$$

Zřejmě $\mathrm{M}(\varphi_M) = M$ neboli $f_{\varphi_M,\mathbb{P}} = f$, a φ_M používá jen $\{\neg, \wedge, \vee\}$. Protože $p \wedge q \sim \neg(p \rightarrow \neg q)$ a $p \vee q \sim \neg p \rightarrow q$, mohli bychom φ_M ekvivalentně vyjádřit i pomocí $\{\neg, \rightarrow\}$. $\square$

2.3 Normální formy

CNF a DNF

- literál je prvovýrok nebo jeho negace, $\overline{\ell}$ je opačný literál k ℓ (pro *pozitivní* $\ell = p$ je $\overline{\ell} = \neg p$, pro *negativní* $\ell = \neg p$ je $\overline{\ell} = p$)
- klauzule je disjunkce literálů $C = \ell_1 \vee \ell_2 \vee \cdots \vee \ell_n$ (*jednotková klauzule* je samotný literál, *prázdná klauzule* je $\bot$)
- výrok je v konjunktivní normální formě (CNF) je-li konjunkcí klauzulí (prázdný CNF výrok je $\top$)
- elementární konjunkce je konjunkce literálů $E = \ell_1 \wedge \cdots \wedge \ell_n$ (*jednotková* el. konjunkce je samotný literál, *prázdná* je $\top$)
- výrok je v disjunktivní normální formě (DNF) je-li disjunkcí elementárních konjunkcí (prázdný DNF výrok je $\bot$)

například:

- $(p \vee q) \wedge (p \vee \neg q) \wedge \neg p$ je v CNF
- $\neg p \vee (p \wedge q)$ je v DNF
- φ_v je v CNF i DNF, φ_M je v DNF

O dualitě

zaměníme-li $0 \leftrightsquigarrow 1$, negace zůstává stejná, z $\land$ se stává $\lor$ a naopak

- φ nad $\{\neg, \land, \lor\}$, zaměníme-li $\land, \lor$ a znegujeme-li prvovýroky: duální $\psi \sim \neg\varphi$, modely φ jsou nemodely ψ, $f_\psi(\neg x) = \neg f_\varphi(x)$
- CNF a DNF jsou duální pojmy
- *pravdivost* je duální k *nesplnitelnosti*

Pozorování: Výrok v CNF je pravdivý, právě když každá klauzule má dvojici opačných literálů.

Duálně: Výrok v DNF je nesplnitelný, pokud každá elementární konjunkce má dvojici opačných literálů.

Převod do normální formy: sémanticky (příklad)

mějme výrok $\varphi = p \leftrightarrow (q \vee \neg r)$

jeho modely jsou $M = \{(0,0,1),(1,0,0),(1,1,0),(1,1,1)\}$

najdeme DNF a CNF výroky se stejnými modely, tj. ekvivalentní φ

DNF sestrojíme tak, že pro každý model přidáme elementární konjunkci vynucující právě tento model:

$\varphi_{\mathrm{DNF}} = (\neg p \wedge \neg q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \vee (p \wedge q \wedge \neg r) \vee (p \wedge q \wedge r)$

při konstrukci CNF potřebujeme nemodely φ:

$$\overline{M} = \{(0,0,0),(0,1,0),(0,1,1),(1,0,1)\}$$

každá klauzule zakáže jeden nemodel:

$\varphi_{\mathrm{CNF}} = (p \vee q \vee r) \wedge (p \vee \neg q \vee r) \wedge (p \vee \neg q \vee \neg r) \wedge (\neg p \vee q \vee \neg r)$

Převod do normální formy: sémanticky

Tvrzení: Buď $\mathbb{P}$ konečný, $M \subseteq \mathrm{M}_\mathbb{P}$ libovolná. Potom existují DNF a CNF výroky $\varphi_{\mathrm{DNF}}, \varphi_{\mathrm{CNF}}$, že $M = \mathrm{M}_\mathbb{P}(\varphi_{\mathrm{DNF}}) = \mathrm{M}_\mathbb{P}(\varphi_{\mathrm{CNF}})$.

$$\varphi_{\mathrm{DNF}} = \bigvee_{v \in M} \bigwedge_{p \in \mathbb{P}} p^{v(p)}$$

$$\varphi_{\mathrm{CNF}} = \bigwedge_{v \in \overline{M}} \bigvee_{p \in \mathbb{P}} \overline{p^{v(p)}} = \bigwedge_{v \notin M} \bigvee_{p \in \mathbb{P}} p^{1-v(p)}$$

Důkaz: $\varphi_{\mathrm{DNF}} = \varphi_M$ říká 'jsem jeden z modelů z M'

φ_{CNF} říká 'nejsem žádný z nemodelů z M', je duální k $\varphi'_{\mathrm{DNF}} = \varphi_{\overline{M}}$ pro doplněk M, nebo přímo: modely klauzule $C_v = \bigvee_{p \in \mathbb{P}} p^{1-v(p)}$ jsou $\mathrm{M}_C = \mathrm{M}_\mathbb{P} \setminus \{v\}$, tedy každá klauzule zakáže jeden nemodel $\square$

Důsledek: Každý výrok (v libovolném, i nekonečném jazyce $\mathbb{P}$) je ekvivalentní nějakému výroku v CNF a nějakému výroku v DNF.

Důkaz: použijeme konečný jazyk $\mathbb{P}' = \mathrm{Var}(\varphi)$, $M = \mathrm{M}_{\mathbb{P}'}(\varphi)$ $\square$

Převod do normální formy: syntakticky

Hledat všechny modely je neefektivní, lze i syntakticky pomocí ekvivalentních úprav.

Pozorování: Nahradíme-li podvýrok ψ výroku φ ekvivalentním ψ', výsledný výrok φ' je také ekvivalentní φ.

Postup úprav:

1. přepiš ekvivalenci a implikaci pomocí $\neg, \wedge, \vee$
2. přesuň negace dolů (k listům) ve stromu výroku pomocí de Morganových pravidel, odstraň dvojité negace
3. přesuň dolů disjunkce (pro CNF) resp. konjunkce (pro DNF) pomocí distributivity $\wedge$ a $\vee$
4. případně zjednoduš (odstranění duplicit, tautologií apod.)

Důkaz, že funguje: indukcí dle struktury výroku

Převod do normální formy: syntakticky (příklad)

mějme opět výrok $\varphi = p \leftrightarrow (q \vee \neg r)$

- přepsat ekvivalence a implikace

$$\begin{aligned} p \leftrightarrow (q \vee \neg r) &\sim (p \rightarrow (q \vee \neg r)) \wedge ((q \vee \neg r) \rightarrow p) \\ &\sim (\neg p \vee q \vee \neg r) \wedge (\neg(q \vee \neg r) \vee p) \end{aligned}$$

- negace dolů

$$(\neg p \vee q \vee \neg r) \wedge ((\neg q \wedge r) \vee p)$$

- do CNF (+ seřadíme prvovýroky v klauzulích)

$$(\neg p \vee q \vee \neg r) \wedge (p \vee \neg q) \wedge (p \vee r)$$

- do DNF (+ zjednodušení)

$$(\neg p \wedge \neg q \wedge r) \vee (p \wedge q \wedge r) \vee (p \wedge \neg r)$$

Ekvivalentní úpravy

- Implikace a ekvivalence:

$$\varphi \to \psi \sim \neg\varphi \vee \psi$$
$$\varphi \leftrightarrow \psi \sim (\neg\varphi \vee \psi) \wedge (\neg\psi \vee \varphi)$$

- Negace:

$$\neg(\varphi \wedge \psi) \sim \neg\varphi \vee \neg\psi$$
$$\neg(\varphi \vee \psi) \sim \neg\varphi \wedge \neg\psi$$
$$\neg\neg\varphi \sim \varphi$$

- Konjunkce (převod do DNF):

$$\varphi \wedge (\psi \vee \chi) \sim (\varphi \wedge \psi) \vee (\varphi \wedge \chi)$$
$$(\varphi \vee \psi) \wedge \chi \sim (\varphi \wedge \chi) \vee (\psi \wedge \chi)$$

- Disjunkce (převod do CNF):

$$\varphi \vee (\psi \wedge \chi) \sim (\varphi \vee \psi) \wedge (\varphi \vee \chi)$$
$$(\varphi \wedge \psi) \vee \chi \sim (\varphi \vee \chi) \wedge (\psi \vee \chi)$$

2.4 Vlastnosti a důsledky teorií

Vlastnosti teorií

- sporná: $T \models \bot$, ekvivalentně: nemá model, platí v ní vše
- bezesporná (splnitelná): není sporná, tj. má model
- kompletní: bezesporná + každý výrok je v ní pravdivý nebo lživý (nemá nezávislé výroky), ekvivalentně: právě jeden model
- ekvivalence teorií: $T \sim T'$ právě když $\mathrm{M}_{\mathbb{P}}(T) = \mathrm{M}_{\mathbb{P}}(T')$ (různé *axiomatizace* týchž vlastností)

- $T_1 = \{p, p \to q, \neg q\}$ je sporná
- $T_2 = \{p \vee q, r\}$ je bezesporná, ale není kompletní, např. $p \wedge q$ je v ní nezávislý: platí v modelu $(1, 1, 1)$, neplatí v $(1, 0, 1)$
- $T_2 \cup \{\neg p\}$ je kompletní, jediným modelem je $(0, 1, 1)$.
- ekvivalentní teorie: $\{p \to q, r\} \sim \{(\neg p \vee q) \wedge r\}$

Důsledky teorií

Buď T teorie v jazyce $\mathbb{P}$. Množina všech důsledků T v jazyce $\mathbb{P}'$:

$$\mathrm{Csq}_{\mathbb{P}'}(T) = \{\varphi \in \mathrm{VF}_{\mathbb{P}'} \mid T \models \varphi\}$$

pokud $\mathbb{P}' = \mathbb{P}$: $\mathrm{Csq}_{\mathbb{P}}(T) = \{\varphi \in \mathrm{VF}_{\mathbb{P}} \mid \mathrm{M}_{\mathbb{P}}(T) \subseteq \mathrm{M}_{\mathbb{P}}(\varphi)\}$

Tvrzení: Jsou-li T, T' teorie a $\varphi, \varphi_1, \ldots, \varphi_n$ výroky v jazyce $\mathbb{P}$:

(i) $T \subseteq \mathrm{Csq}_{\mathbb{P}}(T)$

(ii) $\mathrm{Csq}_{\mathbb{P}}(T) = \mathrm{Csq}_{\mathbb{P}}(\mathrm{Csq}_{\mathbb{P}}(T))$

(iii) pokud $T \subseteq T'$, potom $\mathrm{Csq}_{\mathbb{P}}(T) \subseteq \mathrm{Csq}_{\mathbb{P}}(T')$

(iv) $\varphi \in \mathrm{Csq}_{\mathbb{P}}(\{\varphi_1, \ldots, \varphi_n\})$ právě když $\models (\varphi_1 \wedge \cdots \wedge \varphi_n) \rightarrow \varphi$

Důkaz: snadný, použijte následující:

- $\mathrm{M}(\mathrm{Csq}(T)) = \mathrm{M}(T)$
- je-li $T \subseteq T'$ potom $\mathrm{M}(T) \supseteq \mathrm{M}(T')$
- $\models \psi \rightarrow \varphi$ právě když $\mathrm{M}(\psi) \subseteq \mathrm{M}(\varphi)$ $\square$

Extenze teorií: neformálně

Extenze teorie T je jakákoliv teorie, která splňuje vše, co platí v T

- dodatečné požadavky o systému: jednoduchá extenze
- přidání nových částí k systému (a v původním platí totéž, co předtím): konzervativní extenze

Úvodní příklad o barvení grafů:

- T_3 (úplná obarvení s hranovou podmínkou) je jednoduchou extenzí teorie T_1 (částečná obarvení bez ohledu na hrany)
- T_3' (přidání nového vrcholu) je konzervativní, ale ne jednoduchou extenzí T_3
- T_3' je extenze T_1, která není ani jednoduchá, ani konzervativní

Extenze teorií: formálně

Buď T v jazyce $\mathbb{P}$. Extenze teorie T je libovolná teorie T' v jazyce $\mathbb{P}' \supseteq \mathbb{P}$ splňující $\mathrm{Csq}_{\mathbb{P}}(T) \subseteq \mathrm{Csq}_{\mathbb{P}'}(T')$,

- jednoduchá: $\mathbb{P}' = \mathbb{P}$
- konzervativní: $\mathrm{Csq}_{\mathbb{P}}(T) = \mathrm{Csq}_{\mathbb{P}}(T') = \mathrm{Csq}_{\mathbb{P}'}(T') \cap \mathrm{VF}_{\mathbb{P}}$

"nové důsledky musí obsahovat nové prvovýroky"

Pozorování:

1. T' je jednoduchá extenze T, právě když $\mathbb{P}' = \mathbb{P}$ a $\mathrm{M}_{\mathbb{P}}(T') \subseteq \mathrm{M}_{\mathbb{P}}(T)$
2. T' je extenze T, právě když $\mathrm{M}_{\mathbb{P}'}(T') \subseteq \mathrm{M}_{\mathbb{P}'}(T)$. Tj. restrikce modelů T' na $\mathbb{P}$ musí být modely T: $\{v\restriction_{\mathbb{P}} \mid v \in \mathrm{M}_{\mathbb{P}'}(T')\} \subseteq \mathrm{M}_{\mathbb{P}}(T)$
3. T' je konzervativní extenze T, je-li to extenze a navíc každý model T lze expandovat na model T' (tj. *každý* model T získáme restrikcí *nějakého* modelu T' na jazyk $\mathbb{P}$): $\{v\restriction_{\mathbb{P}} \mid v \in \mathrm{M}_{\mathbb{P}'}(T')\} = \mathrm{M}_{\mathbb{P}}(T)$
4. T' je extenze T a zároveň T je extenze T', právě když $T \sim T'$
5. Kompletní jednoduché extenze T odpovídají modelům T (až na $\sim$)

Extenze teorií: příklad

- mějme $T = \{p \rightarrow q\}$ v jazyce $\mathbb{P} = \{p, q\}$, teorie $T_1 = \{p \wedge q\}$ v jazyce $\mathbb{P}$ je jednoduchá extenze T: $\mathrm{M}_{\mathbb{P}}(T_1) \subseteq \mathrm{M}_{\mathbb{P}}(T)$
- T_1 je kompletní, až na ekvivalenci všechny jednoduché kompletní extenze T jsou: T_1, $T_2 = \{\neg p, q\}$, a $T_3 = \{\neg p, \neg q\}$
- teorie $T' = \{p \leftrightarrow (q \wedge r)\}$ v $\mathbb{P}' = \{p, q, r\}$ je extenzí teorie T: $\mathbb{P} \subseteq \mathbb{P}'$ a $\mathrm{M}_{\mathbb{P}'}(T') \subseteq \mathrm{M}_{\mathbb{P}'}(T)$, restrikce modelů T' na $\mathbb{P}$ jsou $\{(0,0), (0,1), (1,1)\} \subseteq \mathrm{M}_{\mathbb{P}}(T)$
- protože dokonce $\{(0,0), (0,1), (1,1)\} = \mathrm{M}_{\mathbb{P}}(T)$, každý model T lze rozšířit na model T', T' je konzervativní extenze T
- každý výrok v jazyce $\mathbb{P}$ platí v T, právě když platí v T', ale výrok $p \rightarrow r$ je novým důsledkem: platí v T' ale ne v T
- teorie $T'' = \{\neg p \vee q, \neg q \vee r, \neg r \vee p\}$ v jazyce $\mathbb{P}'$ je extenze T, ale není konzervativní, neboť v ní platí $p \leftrightarrow q$, což neplatí v T (nebo proto, že model $(0,1)$ teorie T nelze rozšířit na model teorie T'')