Druhá přednáška

NAIL062 Výroková a predikátová logika

Jakub Bulín (KTIML MFF UK)

Zimní semestr 2023

Druhá přednáška

Program

- sémantika výrokové logiky
- normální formy
- vlastnosti a důsledky teorií

Materiály

Zápisky z přednášky, Sekce 2.2-2.4 z Kapitoly 2

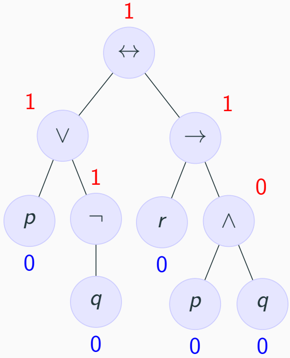
2.2 Sémantika výrokové logiky

Pravdivostní hodnota: příklad

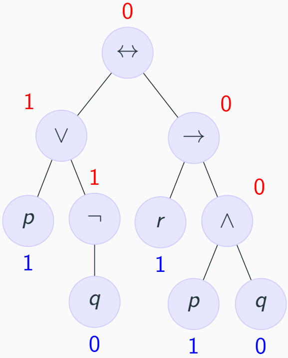
pravdivostní ohodnocení výrokových proměnných jednoznačně určuje pravdivostní hodnotu výroku (vyhodnoť od listů ke kořeni)

$$\varphi = ((p \vee (\neg q)) \leftrightarrow (r \rightarrow (p \wedge q)))$$

(a) φ platí při ohodnocení
$p = 0,\ q = 0,\ r = 0$



(b) φ neplatí při ohodnocení
$p = 1,\ q = 0,\ r = 1$



Sémantika logických spojek

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$
0	0	1	0	0	1	1
0	1	1	0	1	1	0
1	0	0	0	1	0	0
1	1	0	1	1	1	1

$$\begin{array}{cc} 0 & 1 \\ \hline 1 & 0 \end{array} \qquad f_{\neg}(x) = 1 - x$$

$$\begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array} \qquad f_{\wedge}(x, y) = \min(x, y)$$

$$\begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 1 & 1 \\ 1 & 1 & 0 \end{array} \qquad f_{\vee}(x, y) = \max(x, y)$$

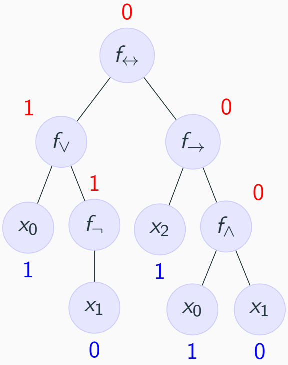
$$\begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 1 & 1 \\ 1 & 0 & 1 \end{array} \qquad f_{\rightarrow}(x, y)$$

$$\begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 1 & 0 \\ 1 & 0 & 1 \end{array} \qquad f_{\leftrightarrow}(x, y)$$

sémantika logických spojek je daná booleovskými funkcemi, každý výrok určuje *složenou* booleovskou funkci, tzv. pravdivostní funkci

např. $\varphi = ((p \vee (\neg q)) \leftrightarrow (r \rightarrow (p \wedge q)))$ v jazyce $\mathbb{P}' = \{p, q, r, s\}$

$$f_{\varphi,\mathbb{P}'}(x_0, x_1, x_2, x_3) = f_{\leftrightarrow}(f_{\vee}(x_0, f_{\neg}(x_1)), f_{\rightarrow}(x_2, f_{\wedge}(x_0, x_1)))$$



pravdivostní hodnota φ při ohodnocení $p = 1,\ q = 0,\ r = 1,\ s = 1$:

$$\begin{aligned} f_{\varphi,\mathbb{P}'}(1,0,1,1) &= f_{\leftrightarrow}(f_{\vee}(1, f_{\neg}(0)), f_{\rightarrow}(1, f_{\wedge}(1,0))) \\ &= f_{\leftrightarrow}(f_{\vee}(1,1), f_{\rightarrow}(1,0)) \\ &= f_{\leftrightarrow}(1,0) \\ &= 0 \end{aligned}$$

Pravdivostní funkce formálně

Pravdivostní funkce výroku φ v *konečném* jazyce $\mathbb{P}$ je funkce $f_{\varphi,\mathbb{P}} \colon \{0,1\}^{|\mathbb{P}|} \to \{0,1\}$ definovaná induktivně:

- je-li φ i-tý prvovýrok z $\mathbb{P}$: $f_{\varphi,\mathbb{P}}(x_0,\dots,x_{n-1}) = x_i$
- je-li $\varphi = (\neg\varphi')$: $f_{\varphi,\mathbb{P}}(x_0,\dots,x_{n-1}) = f_\neg(f_{\varphi',\mathbb{P}}(x_0,\dots,x_{n-1}))$
- je-li $(\varphi' \,\square\, \varphi'')$ kde $\square \in \{\wedge,\vee,\rightarrow,\leftrightarrow\}$: $f_{\varphi,\mathbb{P}}(x_0,\dots,x_{n-1}) = f_\square(f_{\varphi',\mathbb{P}}(x_0,\dots,x_{n-1}), f_{\varphi'',\mathbb{P}}(x_0,\dots,x_{n-1}))$

Poznámka: Pravdivostní funkce $f_{\varphi,\mathbb{P}}$ závisí pouze na proměnných odpovídajících prvovýrokům z $\mathrm{Var}(\varphi) \subseteq \mathbb{P}$.

Je-li výrok v *nekonečném* jazyce $\mathbb{P}$, můžeme se omezit na jazyk $\mathrm{Var}(\varphi)$ (který je konečný) a uvažovat pravdivostní funkci nad ním.

Modely

Pravdivostní ohodnocení reprezentuje 'reálný svět' (systém) v námi zvoleném 'formálním světě', proto mu také říkáme model

Model jazyka $\mathbb{P}$: libovolné pravdivostní ohodnocení $v\colon \mathbb{P} \to \{0,1\}$
Množina všech modelů: $\mathrm{M}_{\mathbb{P}} = \{v \mid v\colon \mathbb{P} \to \{0,1\}\} = \{0,1\}^{\mathbb{P}}$

$\mathbb{P} = \{p, q, r\}$, ohodnocení p je pravda, q nepravda, a r pravda:
formálně $v = \{(p,1),(q,0),(r,1)\}$ ale píšeme[1] jen $v = (1,0,1)$

$$\mathrm{M}_{\mathbb{P}} = \{(0,0,0),(0,0,1),(0,1,0),(0,1,1),(1,0,0),(1,0,1),(1,1,0),(1,1,1)\}$$

[1] Formálně ztotožňujeme $\{0,1\}^{\mathbb{P}}$ s $\{0,1\}^{|\mathbb{P}|}$, množina $\mathbb{P}$ je uspořádaná.

Platnost

výrok platí v modelu, pokud je jeho pravdivostní hodnota rovna 1

Výrok φ v jazyce $\mathbb{P}$, model $v \in \mathrm{M}_{\mathbb{P}}$. Pokud $f_{\varphi,\mathbb{P}}(v) = 1$, potom říkáme, že φ **platí** v modelu v, v je **modelem** φ, a píšeme $v \models \varphi$.

Množina všech modelů resp. *nemodelů* φ:

$$\mathrm{M}_{\mathbb{P}}(\varphi) = \{v \in \mathrm{M}_{\mathbb{P}} \mid v \models \varphi\} = f^{-1}_{\varphi,\mathbb{P}}[1]$$

$$\overline{\mathrm{M}_{\mathbb{P}}(\varphi)} = M_{\mathbb{P}} \setminus M_{\mathbb{P}}(\varphi) = \{v \in \mathrm{M}_{\mathbb{P}} \mid v \not\models \varphi\} = f^{-1}_{\varphi,\mathbb{P}}[0]$$

Je-li jazyk zřejmý z kontextu, můžeme vynechat, ale jinak ne!

$$\mathrm{M}_{\{p,q\}}(p \to q) = \{(0,0),(0,1),(1,1)\}$$

$$\mathrm{M}_{\{p,q,r\}}(p \to q) = \{(0,0,0),(0,0,1),(0,1,0),(0,1,1),(1,1,0),(1,1,1)\}$$

Platnost teorie, model teorie

Teorie T platí v modelu v, pokud každý axiom $\varphi \in T$ platí ve v.

Podobně jako pro výrok: v je modelem T, $v \models T$, $v \in \mathrm{M}_{\mathbb{P}}(T)$.

Někdy píšeme $\mathrm{M}_{\mathbb{P}}(T, \varphi)$ místo $\mathrm{M}_{\mathbb{P}}(T \cup \{\varphi\})$, $\mathrm{M}_{\mathbb{P}}(\varphi_1, \varphi_2, \ldots, \varphi_n)$ místo $\mathrm{M}_{\mathbb{P}}(\{\varphi_1, \varphi_2, \ldots, \varphi_n\})$.

Všimněte si:

- $\mathrm{M}_{\mathbb{P}}(T, \varphi) = \mathrm{M}_{\mathbb{P}}(T) \cap \mathrm{M}_{\mathbb{P}}(\varphi)$
- $\mathrm{M}_{\mathbb{P}}(T) = \bigcap_{\varphi \in T} \mathrm{M}_{\mathbb{P}}(\varphi)$
- $\mathrm{M}_{\mathbb{P}}(\varphi_1) \supseteq \mathrm{M}_{\mathbb{P}}(\varphi_1, \varphi_2) \supseteq \cdots \supseteq \mathrm{M}_{\mathbb{P}}(\varphi_1, \varphi_2, \ldots, \varphi_n)$

Najděme modely $T = \{p \vee q \vee r, q \rightarrow r, \neg r\}$ (v jazyce $\mathbb{P} = \{p, q, r\}$):

$$\mathrm{M}_{\mathbb{P}}(r) = \{(0,0,0), (0,1,0), (1,0,0), (1,1,0)\}$$

$$\mathrm{M}_{\mathbb{P}}(r, q \rightarrow r) = \{(0,0,0), (1,0,0)\}$$

$$\mathrm{M}_{\mathbb{P}}(T) = \{(1,0,0)\}$$

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. $\varphi \sim \psi \iff \mathrm{M}_{\mathbb{P}}(\varphi) = \mathrm{M}_{\mathbb{P}}(\psi)$

- 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: $p \sim p \vee p$, $p \rightarrow q \sim \neg p \vee q$, $\neg p \rightarrow (p \rightarrow q) \sim \top$

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 $\neg p \vee \neg q \vee r$ 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 $f\colon \{0,1\}^n \to \{0,1\}$, 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 $p \wedge q \sim \neg(p \to \neg q)$ a $p \vee q \sim \neg p \to q$, mohli bychom φ_M ekvivalentně vyjádřit i pomocí $\{\neg, \to\}$. $\square$

2.3 Normální formy

CNF a DNF

- *Literál* ℓ je buď prvovýrok p nebo negace prvovýroku $\neg p$. Pro prvovýrok p označme $p^0 = \neg p$ a $p^1 = p$. Je-li ℓ literál, potom $\overline{\ell}$ označuje *opačný literál* k ℓ. Je-li $\ell = p$ (*pozitivní literál*), potom $\overline{\ell} = \neg p$, je-li $\ell = \neg p$ (*negativní literál*), potom $\overline{\ell} = p$
- *Klauzule (clause)* je disjunkce literálů $C = \ell_1 \vee \ell_2 \vee \cdots \vee \ell_n$. *Jednotková klauzule (unit clause)* je samotný literál ($n = 1$) a *prázdnou klauzulí* ($n = 0$) myslíme $\perp$.
- Výrok je *v konjunktivní normální formě (v CNF)* pokud je konjunkcí klauzulí. *Prázdný výrok v CNF* je $\top$.
- *Elementární konjunkce* je konjunkce literálů $E = \ell_1 \wedge \ell_2 \wedge \cdots \wedge \ell_n$. *Jednotková elementární konjunkce* je samotný literál ($n = 1$). *Prázdná elementární konjunkce* ($n = 0$) je $\top$.
- Výrok je *v disjunktivní normální formě (v DNF)* pokud je disjunkcí elementárních konjunkcí. *Prázdný výrok v DNF* je $\perp$.

2.4 Vlastnosti a důsledky teorií