

Výroková a predikátová logika - II

Petr Gregor

KTIML MFF UK

ZS 2020/21

Sémantika

- Uvažujeme pouze **dvouhodnotovou** logiku.
- Prvovýroky reprezentují atomická tvrzení, jejich význam je určen přiřazením **pravdivostní hodnoty** 0 (*nepravda*) nebo 1 (*pravda*).
- Sémantika logických spojek je dána jejich **pravdivostními tabulkami**.

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

Ty **jednoznačně** určují hodnotu každého výroku z hodnot prvovýroků.

- K výrokům tedy můžeme také přiřadit “*pravdivostní tabulky*”. Říkáme, že **reprezentují** Booleovské funkce (až na určení pořadí proměnných).
- **Booleovská funkce** je n -ární operace na $2 = \{0, 1\}$, tj. $f: \{0, 1\}^n \rightarrow \{0, 1\}$.

Hodnota výroku

- **Ohodnocení** prvovýroků je funkce $\nu: \mathbb{P} \rightarrow \{0, 1\}$, tj. $\nu \in {}^{\mathbb{P}}2$.
- **Hodnota** $\bar{\nu}(\varphi)$ výroku φ při ohodnocení ν je dána induktivně

$$\bar{\nu}(p) = \nu(p) \text{ jestliže } p \in \mathbb{P} \qquad \bar{\nu}(\neg\varphi) = \neg_1(\bar{\nu}(\varphi))$$

$$\bar{\nu}(\varphi \wedge \psi) = \wedge_1(\bar{\nu}(\varphi), \bar{\nu}(\psi))$$

$$\bar{\nu}(\varphi \vee \psi) = \vee_1(\bar{\nu}(\varphi), \bar{\nu}(\psi))$$

$$\bar{\nu}(\varphi \rightarrow \psi) = \rightarrow_1(\bar{\nu}(\varphi), \bar{\nu}(\psi))$$

$$\bar{\nu}(\varphi \leftrightarrow \psi) = \leftrightarrow_1(\bar{\nu}(\varphi), \bar{\nu}(\psi))$$

kde $\neg_1, \wedge_1, \vee_1, \rightarrow_1, \leftrightarrow_1$ jsou Booleovské funkce dané tabulkami.

Tvrzení *Hodnota výroku φ závisí pouze na ohodnocení $\text{var}(\varphi)$.*

Důkaz Snadno indukcí dle struktury formule. \square

- \rightarrow Množina všech výroků z prvovýroků \mathbb{P} .

Poznámka Jelikož funkce $\bar{\nu}: \text{VF}_{\mathbb{P}} \rightarrow \{0, 1\}$ je jednoznačnou **extenzí** funkce ν , můžeme psát ν místo $\bar{\nu}$ aniž by došlo k nedorozumění.

Sémantické pojmy

Výrok φ nad $\mathbb{P}2$ je

- **splněn** (*platí*) **při ohodnocení** $v \in \mathbb{P}2$, pokud $\bar{v}(\varphi) = 1$.
Pak v je **splňující ohodnocení** výroku φ , značíme $v \models \varphi$.
- **pravdivý** ((logicky) **platí, tautologie**), pokud $\bar{v}(\varphi) = 1$ pro každé $v \in \mathbb{P}2$, tj. φ je splněn při každém ohodnocení, značíme $\models \varphi$.
- **lživý** (**sporný**), pokud $\bar{v}(\varphi) = 0$ pro každé $v \in \mathbb{P}2$, tj. $\neg\varphi$ je pravdivý.
- **nezávislý**, pokud $\bar{v}_1(\varphi) = 0$ a $\bar{v}_2(\varphi) = 1$ pro nějaká $v_1, v_2 \in \mathbb{P}2$, tj. φ není ani pravdivý ani lživý.
- **splnitelný**, pokud $\bar{v}(\varphi) = 1$ pro nějaké $v \in \mathbb{P}2$, tj. φ není lživý.

Výroky φ a ψ jsou (logicky) **ekvivalentní**, psáno $\varphi \sim \psi$, pokud $\bar{v}(\varphi) = \bar{v}(\psi)$ pro každé $v \in \mathbb{P}2$, tj. výrok $\varphi \leftrightarrow \psi$ je pravdivý.

Modely

Předchozí definice ekvivalentně přeformulujeme v terminologii modelů.

Model jazyka nad \mathbb{P} je ohodnocení z \mathbb{P}^2 . Třída všech modelů jazyka nad \mathbb{P} se značí $M(\mathbb{P})$, tedy $M(\mathbb{P}) = \mathbb{P}^2$. Výrok φ nad \mathbb{P} (je)

- **platí v modelu** $v \in M(\mathbb{P})$, pokud $\bar{v}(\varphi) = 1$. Pak v je **model výroku** φ , značíme $v \models \varphi$ a $M^{\mathbb{P}}(\varphi) = \{v \in M(\mathbb{P}) \mid v \models \varphi\}$ je **třída modelů** φ .
- **pravdivý** ((logicky) **platí, tautologie**), pokud platí v každém modelu (jazyka), značíme $\models \varphi$.
- **lživý** (**sporný**), pokud nemá model.
- **nezávislý**, pokud platí v nějakém modelu a neplatí v jiném.
- **splnitelný**, pokud má model.

Výroky φ a ψ jsou (logicky) **ekvivalentní**, psáno $\varphi \sim \psi$, pokud mají stejné modely.

Univerzálnost spojek

Jazyk výrokové logiky obsahuje *základní* spojky \neg , \wedge , \vee , \rightarrow , \leftrightarrow .

Můžeme zavést obecně n -ární spojku pro libovolnou Booleovu funkci. Např.

$p \downarrow q$ “ani p ani q ” (NOR, Peirceova spojka)

$p \uparrow q$ “ne (p a q)” (NAND, Shefferova spojka)

} Obě jsou univerzální
Apolb bylo prave
2 Navedci

Množina spojek je *univerzální*, pokud lze každou Booleovskou funkci reprezentovat nějakým z nich (dobře) vytvořeným výrokem.

Tvrzení $\{\neg, \wedge, \vee\}$ je univerzální.

Důkaz Funkci $f: \{0, 1\}^n \rightarrow \{0, 1\}$ reprezentuje výrok $\bigvee_{v \in f^{-1}[1]} \bigwedge_{i=1}^n p_i^{v_i}$, kde $p_i^{v_i}$ značí prvovýrok p_i pokud $v_i = 1$, jinak výrok $\neg p_i$. Pro $f^{-1}[1] = \emptyset$ zvolíme výrok \perp . \square

Tvrzení $\{\neg, \rightarrow\}$ je univerzální.

Důkaz $(p \wedge q) \sim \neg(p \rightarrow \neg q)$, $(p \vee q) \sim (\neg p \rightarrow q)$. \square

CNF a DNF

- **Literál** je prvovýrok nebo jeho negace. Je-li p prvovýrok, označme p^0 literál $\neg p$ a p^1 literál p . Je-li l literál, označme \bar{l} literál **opačný** k l .
- **Klauzule** je disjunkce literálů, **prázdnou klauzulí** rozumíme \perp .
- Výrok je v **konjunktivně normálním tvaru** (**CNF**), je-li konjunkcí klauzulí. **Prázdným výrokem v CNF** rozumíme \top .
- **Elementární konjunkce** je konjunkce literálů, **prázdnou konjunkcí** je \top .
- Výrok je v **disjunktivně normálním tvaru** (**DNF**), je-li disjunkcí elementárních konjunktí. **Prázdným výrokem v DNF** rozumíme \perp .

Poznámka Klauzule nebo elementární konjunkce je zároveň v CNF i DNF.

Pozorování Výrok v CNF je pravdivý, právě když každá jeho klauzule obsahuje dvojici opačných literálů. Výrok v DNF je splnitelný, právě když aspoň jedna jeho elementární konjunkce neobsahuje dvojici opačných literálů.

Převod tabulkou

Tvrzení Necht' $K \subseteq \mathbb{P}2$ pro \mathbb{P} konečné. Označme $\bar{K} = \mathbb{P}2 \setminus K$. Pak

$$M^{\mathbb{P}} \left(\bigvee_{v \in K} \bigwedge_{p \in \mathbb{P}} p^{v(p)} \right) = K = M^{\mathbb{P}} \left(\bigwedge_{v \in \bar{K}} \bigvee_{p \in \mathbb{P}} \overline{p^{v(p)}} \right)$$

DNF *CNF*

Důkaz První rovnost plyne z $\bar{w}(\bigwedge_{p \in \mathbb{P}} p^{v(p)}) = 1$ právě když $w = v$, kde $w \in \mathbb{P}2$. Druhá obdobně z $\bar{w}(\bigvee_{p \in \mathbb{P}} \overline{p^{v(p)}}) = 1$ právě když $w \neq v$. \square

Např. $K = \{(1, 0, 0), (1, 1, 0), (0, 1, 0), (1, 1, 1)\}$ namodelujeme

$$\begin{aligned} & (p \wedge \neg q \wedge \neg r) \vee (p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge \neg r) \vee (p \wedge q \wedge r) \sim \\ & (p \vee q \vee r) \wedge (p \vee q \vee \neg r) \wedge (p \vee \neg q \vee \neg r) \wedge (\neg p \vee q \vee \neg r) \quad \text{CNF} \end{aligned}$$

$\bar{K} = (0, 0, 0), \dots$

Důsledek Každý výrok je ekvivalentní nějakému výroku v CNF/DNF.

Důkaz Hodnota výroku φ závisí pouze na ohodnocení jeho proměnných, kterých je konečně. Lze tedy použít tvrzení pro $K = M^{\mathbb{P}}(\varphi)$ a $\mathbb{P} = \text{var}(\varphi)$. \square

Převod úpravami

Tvrzení *Nechť φ' je výrok vzniklý z výroku φ nahrazením některých výskytů podvýroku ψ za výrok ψ' . Jestliže $\psi \sim \psi'$, pak $\varphi \sim \varphi'$.*

Důkaz Snadno indukcí dle struktury formule. \square

$$(1) (\varphi \rightarrow \psi) \sim (\neg\varphi \vee \psi), \quad (\varphi \leftrightarrow \psi) \sim ((\neg\varphi \vee \psi) \wedge (\neg\psi \vee \varphi))$$

$$(2) \neg\neg\varphi \sim \varphi, \quad \neg(\varphi \wedge \psi) \sim (\neg\varphi \vee \neg\psi), \quad \neg(\varphi \vee \psi) \sim (\neg\varphi \wedge \neg\psi)$$

$$(3) (\varphi \vee (\psi \wedge \chi)) \sim ((\psi \wedge \chi) \vee \varphi) \sim ((\varphi \vee \psi) \wedge (\varphi \vee \chi))$$

$$(3)' (\varphi \wedge (\psi \vee \chi)) \sim ((\psi \vee \chi) \wedge \varphi) \sim ((\varphi \wedge \psi) \vee (\varphi \wedge \chi))$$

Tvrzení *Každý výrok lze pomocí (1), (2), (3)/(3)' převést na CNF / DNF.*

Důkaz Snadno indukcí dle struktury formule. \square

Tvrzení *Nechť výrok φ obsahuje pouze spojky \neg, \wedge, \vee . Pak pro výrok φ^* vzniklý z φ záměnou \wedge a \vee a znegováním všech literálů platí $\neg\varphi \sim \varphi^*$.*

Důkaz Snadno indukcí dle struktury formule. \square

Problém splnitelnosti a řešiče

- Problém **SAT**: Je daná výroková formule splnitelná?
- **Příklad** *Lze šachovnici bez dvou protilehlých rohů perfektně pokrýt kostkami domina?*

Snadno vytvoříme výrokovou formuli, která je **splnitelná**, právě když to lze. Pak ji můžeme zkusit ověřit pomocí nějakého SAT řešiče.

- Nejlepší řešiče pro SAT: www.satcompetition.org.
- Řešič v ukázce: [Glucose](#), formát pro CNF soubory: [DIMACS](#).
- Obecnější otázka: *Lze celou matematiku převést do logických formulí?*
AI, strojové dokazování, [Peano: Formulario](#) (1895-1908), [Mizar system](#)
- *Proč to lidé (většinou) nedělají?*
Jak vyřešíme uvedený příklad *elegantněji*? V čem náš postup spočívá?

2-SAT

- Výrok je v ***k*-CNF**, je-li v CNF a každá jeho klauzule má **nejvýše** k literálů.
- ***k*-SAT** je následující problém (pro pevné $k > 0$)

INSTANCE: Výrok φ v k -CNF.

OTÁZKA: Je φ splnitelný?

Zatímco už pro $k = 3$ jde o **NP-úplný** problém, ukážeme, že 2-SAT lze řešit v **lineárním** čase (vzhledem k délce φ).

Vynecháme implementační detaily (výpočetní model, reprezentace v paměti) a využijeme následující znalosti, viz [ADS I].

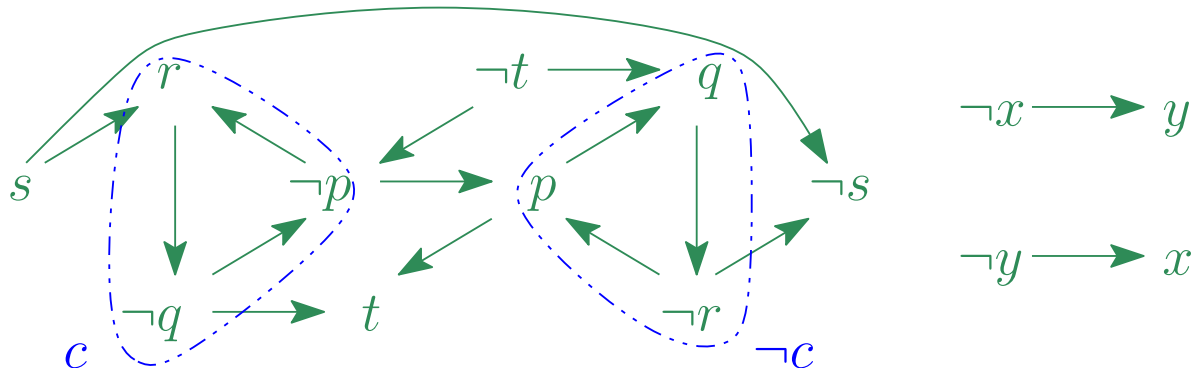
Tvrzení *Rozklad orientovaného grafu (V, E) na silně souvislé komponenty lze nalézt v čase $\mathcal{O}(|V| + |E|)$.*

- Orientovaný graf G je **silně souvislý**, pokud pro každé dva vrcholy u a v existují v G orientované cesty jak z u do v , tak i z v do u .
- Silně souvislá **komponenta** grafu G je **maximální** silně souvislý podgraf G .

Implikační graf

Implikační graf výroku φ v 2-CNF je orientovaný graf G_φ , v němž

- vrcholy jsou proměnné výroku φ nebo jejich negace,
- klauzuli $l_1 \vee l_2$ výroku φ reprezentujeme dvojicí hran $\bar{l}_1 \rightarrow l_2, \bar{l}_2 \rightarrow l_1$,
- klauzuli l_1 výroku φ reprezentujeme hranou $\bar{l}_1 \rightarrow l_1$.



$$p \wedge (\neg p \vee q) \wedge (\neg q \vee \neg r) \wedge (p \vee r) \wedge (r \vee \neg s) \wedge (\neg p \vee t) \wedge (q \vee t) \wedge \neg s \wedge (x \vee y)$$

Tvrzení φ je splnitelný, právě když žádná silně souvislá komponenta v G_φ neobsahuje dvojici opačných literálů.

Důkaz Každé splňující ohodnocení ohodnotí všechny literály ze stejné komponenty stejně. Implikace zleva doprava tedy platí.

Nalezení ohodnocení

Naopak, označme G_φ^* graf vzniklý z G_φ **kontrakcí** silně souvislých komponent.

Pozorování G_φ^* je *acyklický*, má tedy *topologické uspořádání* $<$.

- Orientovaný graf je *acyklický*, neobsahuje-li orientovaný *cyklus*.
- Lineární uspořádání $<$ vrcholů orientovaného grafu je *topologické*, pokud $p < q$ pro každou hranu z p do q .

Nyní pro každou komponentu v rostoucím pořadí dle $<$, nejsou-li její literály dosud ohodnocené, nastav je na 0 a literály v opačné komponentě na 1.

Zbývá ukázat, že takto získané ohodnocení v splňuje φ . Kdyby ne, existovaly by v G_φ^* hrany $p \rightarrow q$ a $\bar{q} \rightarrow \bar{p}$ s $v(p) = 1$ a $v(q) = 0$. To je ve sporu s pořadím nastavení komponent na 0 resp. 1, neboť $p < q$ a $\bar{q} < \bar{p}$. \square

Důsledek 2-SAT je řešitelný v lineárním čase.