

# Výroková a predikátová logika - II

Petr Gregor

KTIML MFF UK

ZS 2015/2016

# Jazyk

Výroková logika je “*logikou spojek*”. Vycházíme z (neprázdnej) množiny  $\mathbb{P}$  *výrokových proměnných* (*prvovýroků*). Např.

$$\mathbb{P} = \{p, p_1, p_2, \dots, q, q_1, q_2, \dots\}$$

Obvykle budeme předpokládat, že  $\mathbb{P}$  je spočetná.

*Jazyk* výrokové logiky (nad  $\mathbb{P}$ ) obsahuje *symbols*

- výrokové proměnné z  $\mathbb{P}$
- logické spojky  $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$
- závorky  $(, )$

Jazyk je tedy určen množinou  $\mathbb{P}$ . Říkáme, že logické spojky a závorky jsou *logické symbols*, zatímco výrokové proměnné jsou *mimologické symbols*.

Budeme používat i *konstantní* symbols  $\top$  (pravda),  $\perp$  (spor), jež zavedeme jako *zkratky* za  $p \vee \neg p$ , resp.  $p \wedge \neg p$ , kde  $p$  je pevný prvovýrok z  $\mathbb{P}$ .

# Formule

**Výrokové formule** (**výroky**) (nad  $\mathbb{P}$ ) jsou dány indukčním předpisem

- (i) každá výroková proměnná z  $\mathbb{P}$  je výrokovou formulí,
- (ii) jsou-li  $\varphi, \psi$  výrokové formule, pak rovněž

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

jsou výrokové formule,

- (iii) každá výroková formule vznikne **konečným** užitím pravidel (i), (ii).

- Výrokové formule jsou tedy (dobře vytvořené) **konečné posloupnosti** symbolů jazyka (**řetězce**).
- Výrokovou formuli, která je součástí jiné výrokové formule  $\varphi$  nazveme **podformulí** (**podvýrokem**)  $\varphi$ .
- Množinu všech výrokových formulí nad  $\mathbb{P}$  značíme  **$VF_{\mathbb{P}}$** .
- Množinu všech výrokových proměnných s výskytem ve  $\varphi$  značíme  **$\text{var}(\varphi)$** .

# Konvence zápisu

Zavedení (obvyklých) *priorit* logických spojek umožňuje v **zkráceném zápisu** vypouštět závorky okolo podvýroku vzniklého spojkou s **vyšší** prioritou.

(1)  $\rightarrow, \leftrightarrow$

(2)  $\wedge, \vee$

(3)  $\neg$

Rovněž vnější závorky můžeme vynechat. Např.

$$(((\neg p) \wedge q) \rightarrow (\neg(p \vee (\neg q)))) \quad \text{lze zkrátit na} \quad \neg p \wedge q \rightarrow \neg(p \vee \neg q)$$

**Poznámka** Nerespektováním priorit může vzniknout **nejednoznačný** zápis nebo dokonce jednoznačný zápis **neekvivalentní** formule.

Další možnosti zjednodušení zápisu vyplývají ze sémantických vlastností spojek (**asociativita**  $\vee, \wedge$ ).

# Vytvořující strom

**Vytvořující strom** je konečný **uspořádaný strom**, jehož vrcholy jsou označeny výroky dle následujících pravidel

- listy (a jen listy) jsou označeny prvovýroky,
- je-li vrchol označen  $(\neg\varphi)$ , má jediného syna označeného  $\varphi$ ,
- je-li vrchol označen  $(\varphi \wedge \psi)$ ,  $(\varphi \vee \psi)$ ,  $(\varphi \rightarrow \psi)$  nebo  $(\varphi \leftrightarrow \psi)$ , má dva syny, přičemž **levý** syn je označen  $\varphi$  a **pravý** je označen  $\psi$ .

**Vytvořující strom výroku**  $\varphi$  je vytvořující strom s kořenem označeným  $\varphi$ .

**Tvrzení** Každý výrok má jednoznačně určený vytvořující strom.

**Důkaz** Snadno indukcí dle počtu vnoření závorek (odpovídající hloubce vytvořujícího stromu).  $\square$

**Poznámka** Takovéto důkazy nazýváme důkazy indukcí **dle struktury formule**.

# 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  $2 = \{0, 1\}$ .

# Hodnota výroku

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

$$\begin{aligned}
 \bar{v}(p) &= v(p) \text{ jestliže } p \in \mathbb{P} & \bar{v}(\neg\varphi) &= -_1(\bar{v}(\varphi)) \\
 \bar{v}(\varphi \wedge \psi) &= \wedge_1(\bar{v}(\varphi), \bar{v}(\psi)) & \bar{v}(\varphi \vee \psi) &= \vee_1(\bar{v}(\varphi), \bar{v}(\psi)) \\
 \bar{v}(\varphi \rightarrow \psi) &= \rightarrow_1(\bar{v}(\varphi), \bar{v}(\psi)) & \bar{v}(\varphi \leftrightarrow \psi) &= \leftrightarrow_1(\bar{v}(\varphi), \bar{v}(\psi))
 \end{aligned}$$

kde  $-_1, \wedge_1, \vee_1, \rightarrow_1, \leftrightarrow_1$  jsou Booleovské funkce dané tabulkami.

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

**Důkaz** Snadno indukcí dle struktury formule.  $\square$

**Poznámka** Jelikož funkce  $\bar{v}: \text{VF}_{\mathbb{P}} \rightarrow 2$  je jednoznačnou **extenzí** funkce  $v$ , můžeme psát  $v$  místo  $\bar{v}$  aniž by došlo k nedorozumění.

# Sémantické pojmy

Výrok  $\varphi$  nad  $\mathbb{P}$  je

- **splněn** (*platí*) **při ohodnocení**  $v \in \mathbb{P}2$ , pokud  $\bar{v}(\varphi) = 1$ .  
Pak  $v$  je **splňující ohodnocení** výroku  $\varphi$ , značíme  $v \models \varphi$ .
- **pravdivý** ((logicky) **platí, tautologie**), pokud  $\bar{v}(\varphi) = 1$  pro **každé**  $v \in \mathbb{P}2$ , tj.  $\varphi$  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.  $\varphi$  není ani pravdivý ani lživý.
- **splnitelný**, pokud  $\bar{v}(\varphi) = 1$  pro nějaké  $v \in \mathbb{P}2$ , tj.  $\varphi$  není lživý.

Výroky  $\varphi$  a  $\psi$  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  $\varphi$  nad  $\mathbb{P}$  (je)

- **platí v modelu**  $v \in M(\mathbb{P})$ , pokud  $\bar{v}(\varphi) = 1$ . Pak  $v$  je **model výroku**  $\varphi$ , značíme  $v \models \varphi$  a  **$M^{\mathbb{P}}(\varphi) = \{v \in M(\mathbb{P}) \mid v \models \varphi\}$**  je **třída modelů**  $\varphi$ .
- **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  $\varphi$  a  $\psi$  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)

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

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

**Důkaz** Funkci  $f: {}^n 2 \rightarrow 2$  reprezentuje výrok  $\bigvee_{v \in f^{-1}[1]} \bigwedge_{i=0}^{n-1} p_i^{v(i)}$ , kde  $p_i^{v(i)}$  je prvovýrok  $p_i$  pokud  $v(i) = 1$ , jinak výrok  $\neg p_i$ . Pro  $f^{-1}[1] = \emptyset$  zvolíme  $\perp$ .  $\square$

**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 prvvýrok nebo jeho negace. Je-li  $p$  prvvýrok, 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 konjunkcí**. **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  $\overline{K} = {}^{\mathbb{P}}2 \setminus K$ . Pak

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

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

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

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

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

**Důkaz** Hodnota výroku  $\varphi$  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  $\varphi'$  je výrok vzniklý z výroku  $\varphi$  nahrazením některých výskytů podvýroku  $\psi$  za výrok  $\psi'$ . 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  $\varphi$  obsahuje pouze spojky  $\neg$ ,  $\wedge$ ,  $\vee$ . Pak pro výrok  $\varphi^*$  vzniklý z  $\varphi$  záměnou  $\wedge$  a  $\vee$  a znegováním všech literálů platí  $\neg\varphi \sim \varphi^*$ .*

**Důkaz** Snadno indukcí dle struktury formule.  $\square$

## 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  $\varphi$  v  $k$ -CNF.

OTÁZKA: Je  $\varphi$  splnitelný?

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

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

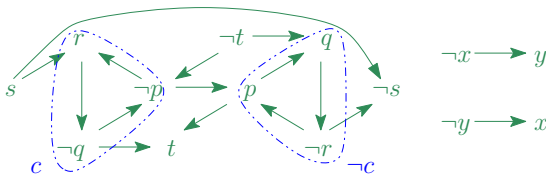
**Tvrzení** Rozklad orientovaného grafu  $(V, E)$  na silně souvislé komponenty lze nalézt v čase  $\mathcal{O}(|V| + |E|)$ .

- 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  $\varphi$  v 2-CNF je orientovaný graf  $G_\varphi$ , v němž

- vrcholy jsou proměnné výroku  $\varphi$  nebo jejich negace,
- klauzuli  $l_1 \vee l_2$  výroku  $\varphi$  reprezentujeme dvojicí hran  $\overline{l_1} \rightarrow l_2, \overline{l_2} \rightarrow l_1$ ,
- klauzuli  $l_1$  výroku  $\varphi$  reprezentujeme hranou  $\overline{l_1} \rightarrow l_1$ .



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

**Tvrzení**  $\varphi$  je splnitelný, právě když žádná silně souvislá komponenta v  $G_\varphi$  neobsahuje dvojici opačných literálů.

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

# Nalezení ohodnocení

Naopak, označme  $G_\varphi^*$  graf vzniklý z  $G_\varphi$  kontrakcí silně souvislých komponent.

**Pozorování**  $G_\varphi^*$  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  $\varphi$ . Kdyby ne, existovaly by v  $G_\varphi^*$  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.



# Horn-SAT

- *Jednotková klauzule* je klauzule obsahující jediný literál,
- *Hornova klauzule* je klauzule obsahující nejvýše jeden pozitivní literál,

$$\neg p_1 \vee \dots \vee \neg p_n \vee q \quad \sim \quad (p_1 \wedge \dots \wedge p_n) \rightarrow q$$

- *Hornův výrok* je konjunkcí Hornových klauzulí,
- *Horn-SAT* je problém splnitelnosti daného Hornova výroku.

## Algoritmus

- (1) obsahuje-li  $\varphi$  dvojici jednotkových klauzulí  $l$  a  $\bar{l}$ , není splnitelný,
- (2) obsahuje-li  $\varphi$  jednotkovou klauzuli  $l$ , nastav  $l$  na 1, odstraň všechny klauzule obsahující  $l$ , odstraň  $\bar{l}$  ze všech klauzulí a opakuj od začátku,
- (3) neobsahuje-li  $\varphi$  jednotkovou klauzuli, je splnitelný ohodnocením 0 všech zbývajících proměnných.

Krok (2) se nazývá *jednotková propagace*.

# Jednotková propagace

$$\begin{array}{ll}
 (\neg p \vee q) \wedge (\neg p \vee \neg q \vee r) \wedge (\neg r \vee \neg s) \wedge (\neg t \vee s) \wedge s & v(s) = 1 \\
 (\neg p \vee q) \wedge (\neg p \vee \neg q \vee r) \wedge \neg r & v(\neg r) = 1 \\
 (\neg p \vee q) \wedge (\neg p \vee \neg q) & v(p) = v(q) = v(t) = 0
 \end{array}$$

**Pozorování** Necht'  $\varphi^l$  je výrok získaný z  $\varphi$  *jednotkovou propagací*. Pak  $\varphi^l$  je splnitelný, právě když  $\varphi$  je splnitelný.

**Důsledek** Algoritmus je korektní (řeší Horn-SAT).

**Důkaz** Korektnost 1. kroku je zřejmá, v 2. kroku plyne z pozorování, v 3. kroku díky *Hornově tvaru*, neboť každá zbývajících klauzule obsahuje negativní literál.

**Poznámka** Přímočará implementace vyžaduje kvadratický čas, při vhodné reprezentaci v paměti lze dosáhnout lineárního času (vzhledem k délce  $\varphi$ ).