Výroková a predikátová logika - II

Petr Gregor

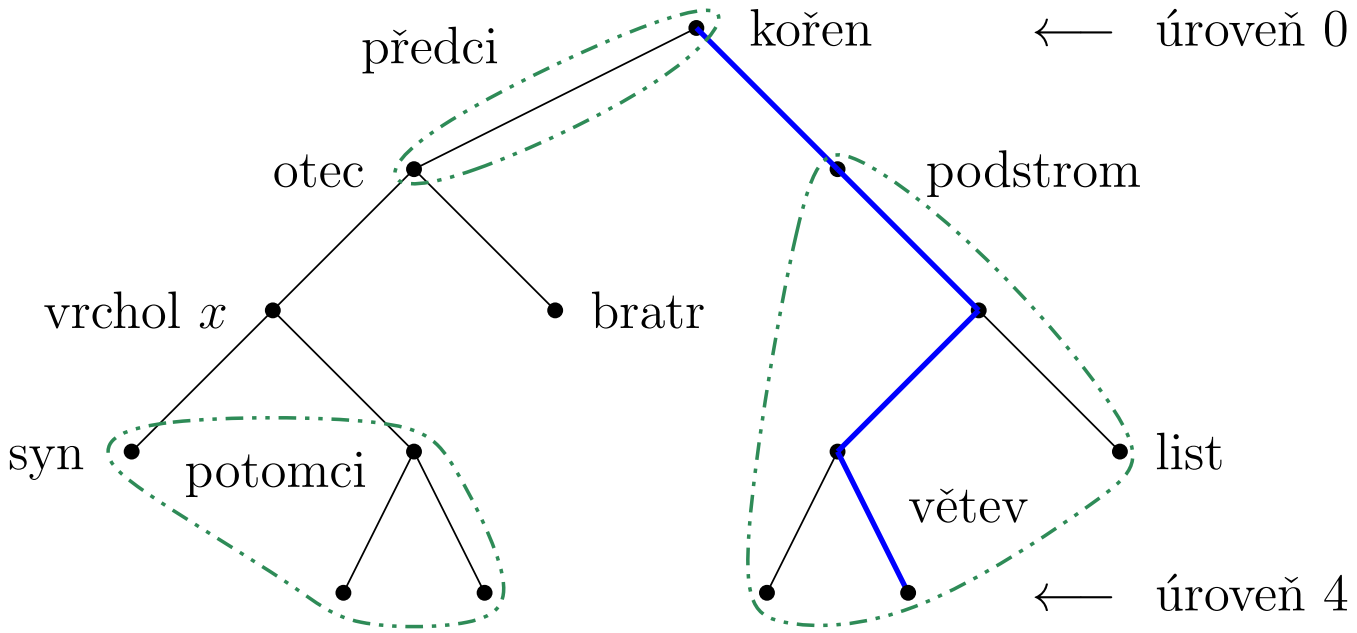
KTIML MFF UK

ZS 2017/2018

n-ární relace a funkce

- Relace *arity* (*četnosti*) $n \in \mathbb{N}$ na X je libovolná množina $R \subseteq X^n$, tedy pro $n = 0$ je $R = \emptyset = 0$ nebo $R = \{\emptyset\} = 1$, pro $n = 1$ je $R \subseteq X$,
- (Částečná) funkce *arity* (*četnosti*) $n \in \mathbb{N}$ z X do Y je libovolná funkce $f \subseteq X^n \times Y$. Řekneme, že f je *totální* na X^n, pokud $\mathrm{dom}(f) = X^n$, značíme $f \colon X^n \to Y$. Je-li navíc $Y = X$, je to *operace* na X.
- Funkce $f \colon X^n \to Y$ je *konstantní*, pokud $\mathrm{rng}(f) = \{y\}$ pro nějaké $y \in Y$, pro $n = 0$ je $f = \{(\emptyset, y)\}$ a f ztotožňujeme s *konstantou* y.
- Aritu relace či funkce značíme $\mathrm{ar}(R)$ či $\mathrm{ar}(f)$ a mluvíme o *nulárních*, *unárních*, *binárních*, obecně *n-árních* relacích a funkcích (operacích).

Stromy



- *Strom* je množina T s částečným uspořádáním $<_T$, ve kterém existuje (jedinečný) nejmenší prvek, zvaný *kořen*, a množina předků libovolného prvku je dobře uspořádaná,
- *větev* stromu T je maximální lineárně uspořádaná podmnožina T,
- adoptujeme standardní terminologii o stromech z teorie grafů, pak např.

větev v konečném stromu je cesta z kořene do listu.

Königovo lemma

Budeme pracovat *(pro jednoduchost)* obvykle s konečně větvícími se stromy, ve kterých má každý vrchol kromě kořene bezprostředního předka (*otce*).

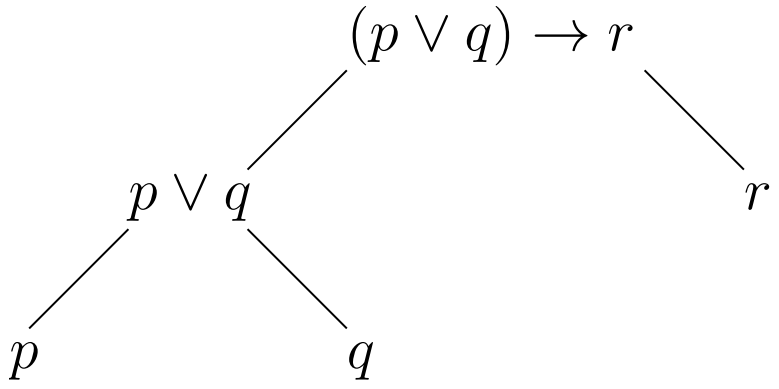
- *n-tá úroveň* stromu T pro $n \in \mathbb{N}$ je daná indukcí, obsahuje syny vrcholů z $(n-1)$-ní úrovně, 0-tá úroveň obsahuje právě kořen,
- *hloubka* stromu T je maximální číslo $n \in \mathbb{N}$ neprázdné úrovně; pokud má T nekonečnou větev, je *hloubka nekonečná* či ω.
- strom T je *n-ární* pro $n \in \mathbb{N}$, pokud každý vrchol má nejvýše n synů. Je *konečně větvící se*, má-li každý vrchol konečně mnoho synů.

Lemma (König) *Každý nekonečný, konečně větvící se strom T obsahuje nekonečnou větev.*

Důkaz Hledání nekonečné větve začneme v kořeni. Jelikož má jen konečně mnoho synů, existuje syn s nekonečně mnoha potomky. *Vybereme* ho a stejně pokračujeme v jeho podstromě. Takto získáme nekonečnou větev. □

Uspořádané stromy

- *Uspořádaný strom* je strom T, s kterým je dáno lineární uspořádání synů každého vrcholu, toto uspořádání se nazývá *pravolevé* a značí $<_L$. Oproti tomu, uspořádání $<_T$ se nazývá *stromové*.
- *značený strom* je strom T s libovolnou funkcí (*značící funkce*), která každému vrcholu T přiřazuje nějaký objekt (*značku*).
- značené uspořádané stromy např. zachycují strukturu formulí



Jazyk

Výroková logika je *"logikou spojek"*. Vycházíme z (neprázdné) 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 symboly

- 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 symboly*, zatímco výrokové proměnné jsou *mimologické symboly*.

Budeme používat i konstantní symboly $\top$ (pravda), $\bot$ (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 induktivním předpisem

(i) každá výroková proměnná z $\mathbb{P}$ je výrokovou formulí,

(ii) jsou-li φ, ψ 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 φ nazveme *podformulí* (*podvýrokem*) φ.
- Množinu všech výrokových formulí nad $\mathbb{P}$ značíme $\mathrm{VF}_{\mathbb{P}}$.
- Množinu všech výrokových proměnných s výskytem ve φ značíme $\mathrm{var}(\varphi)$.

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 φ,
- 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 φ a pravý je označen ψ.

Vytvořující strom výroku φ je vytvořující strom s kořenem označeným φ.

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 $v\colon \mathbb{P} \to \{0,1\}$, tj. $v \in {}^{\mathbb{P}}2$.
- *Hodnota* $\overline{v}(\varphi)$ výroku φ při ohodnocení v je dána induktivně

$$\overline{v}(p) = v(p) \text{ jestliže } p \in \mathbb{P} \qquad \overline{v}(\neg\varphi) = -_1(\overline{v}(\varphi))$$
$$\overline{v}(\varphi \wedge \psi) = \wedge_1(\overline{v}(\varphi), \overline{v}(\psi)) \qquad \overline{v}(\varphi \vee \psi) = \vee_1(\overline{v}(\varphi), \overline{v}(\psi))$$
$$\overline{v}(\varphi \to \psi) = \to_1(\overline{v}(\varphi), \overline{v}(\psi)) \qquad \overline{v}(\varphi \leftrightarrow \psi) = \leftrightarrow_1(\overline{v}(\varphi), \overline{v}(\psi))$$

kde $-_1$, $\wedge_1$, $\vee_1$, $\to_1$, $\leftrightarrow_1$ jsou Booleovské funkce dané tabulkami.

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

Důkaz Snadno indukcí dle struktury formule. $\square$

Poznámka Jelikož funkce $\overline{v}\colon \mathrm{VF}_{\mathbb{P}} \to 2$ je jednoznačnou extenzí funkce v, můžeme psát v místo $\overline{v}$ aniž by došlo k nedorozumění.

Sémantické pojmy

Výrok φ nad $\mathbb{P}$ je

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

Výroky φ a ψ jsou (logicky) *ekvivalentní*, psáno $\varphi \sim \psi$, pokud $\overline{v}(\varphi) = \overline{v}(\psi)$ 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 $\overline{v}(\varphi) = 1$. 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)

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

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

Důkaz Funkci $f\colon {}^n2 \rightarrow 2$ 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 $\bot$. $\square$

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 $\bot$.
- 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 $\bot$.

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 *Nechť $K \subseteq {}^{\mathbb{P}}2$ pro $\mathbb{P}$ konečné. Označme $\overline{K} = {}^{\mathbb{P}}2 \setminus K$. Pak*

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

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

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. □

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

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

(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. □

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. □