Výroková a predikátová logika - I

Petr Gregor

KTIML MFF UK

ZS 2019/2020

K čemu je logika?

Pro matematiky: *“matematika o matematice”*.

Pro informatiky:

- formální specifikace (viz spor EU vs. Microsoft),
- testování software i hardware (formální verifikace, model checking),
- deklarativní programování (např. Prolog),
- složitost (Booleovské funkce, obvody, rozhodovací stromy),
- vyčíslitelnost (nerozhodnutelnost, věty o neúplnosti),
- umělá inteligence (automatické odvozování, rezoluce),
- univerzální nástroje: SAT a SMT řešiče (SAT modulo theory),
- návrh databází (konečné relační struktury, Datalog), ...

Koncepce přednášky

- klasická logika
  - + výroková logika (nejprve samostatně)
  - + predikátová logika
  - + teorie modelů, nerozhodnutelnost, neúplnost
- logika pro informatiky
  - + tablo metoda namísto Hilbertovského kalkulu
  - + dokazování jako forma výpočtu (systematické hledání protipříkladu)
  - + rezoluce v predikátové logice, unifikace, “pozadí” Prologu
  - + důraz na algoritmické otázky
  - + omezení na spočetné jazyky

Doporučená literatura

- Knihy
  - A. Nerode, R. A. Shore, *Logic for Applications*, Springer, 2^{nd} edition, 1997.
  - P. Pudlák, *Logical Foundations of Mathematics and Computational Complexity - A Gentle Introduction*, Springer, 2013.
  - V. Švejdar, *Logika, neúplnost, složitost a nutnost*, Academia, Praha, 2002.
  - A. Sochor, *Klasická matematická logika*, UK v Praze - Karolinum, 2001.
  - W. Hodges, *Shorter Model Theory*, Cambridge University Press, 1997.
  - W. Rautenberg, *A concise introduction to mathematical logic*, Springer, 2009.
- Elektronické zdroje
  - J. Mlček, *Výroková a predikátová logika*, skripta k přednášce, 2012. [www]
  - P. Štěpánek, *Meze formální metody*, skripta k přednášce, 2000. [pdf]
  - M. Pilát, Propositional and Predicate Logic, lecture notes, 2017. [pdf]
  - slidy k přednášce

Trocha historie

- Aristotelés (384-322 př.n.l.) - sylogismy, např.

  z *'žádný Q není R'* a *'každý P je Q'* odvoď *'žádný P není R'*.

- Eukleidés: *Základy* (asi 330 př.n.l.) - axiomatický přístup ke geometrii

  "Pro každou přímku p a bod x, který neleží na p, existuje přímka skrze x neprotínající p." (5. postulát)

- Descartes: *Geometrie* (1637) - algebraizace geometrie
- Leibniz - sen o *"lingua characteristica"* a *"calculus ratiocinator"* (1679-90)
- De Morgan - zavedení logických spojek (1847)

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

- Boole - výrok jako binární funkce, algebraizace logiky (1847)
- Schröder - sémantika predikátové logiky, koncept modelu (1890-1905)

Trocha historie - teorie množin

- Cantor - *intuitivní* teorie množin (1878), např. princip zahrnutí

  "Pro každou vlastnost $\varphi(x)$ *existuje množina* $\{x \mid \varphi(x)\}$*."*

- Frege - logika s kvantifikátory a predikáty, pojem důkazu jako odvození, axiomatická teorie množin (1879, 1884)
- Russel - Fregeho teorie množin je sporná (1903)

  Pro $a = \{x \mid \neg(x \in x)\}$ *je* $a \in a$ *?*

- Russel, Whitehead - teorie typů (1910-13)
- Zermelo (1908), Fraenkel (1922) - *standardní* teorie množin ZFC, např.

  "Pro každou vlastnost $\varphi(x)$ *a množinu* y *existuje množina* $\{x \in y \mid \varphi(x)\}$*."*

- Bernays (1937), Gödel (1940) - teorie množin založená na třídách, např.

  "Pro každou množinovou vlastnost $\varphi(x)$ *existuje třída* $\{x \mid \varphi(x)\}$*."*

Trocha historie - algoritmizace

- Hilbert - kompletní axiomatizace Euklidovské geometrie (1899),
  formalismus - striktní odproštění se od významu, mechaničnost

  "... musí být možné místo o bodu, přímce a rovině mluvit o stolu, židli a půllitru." (Grundlagen der Geometrie)

- Brouwer - intuicionismus, důraz na konstruktivní důkazy

  "Matematické tvrzení je myšlenková konstrukce ověřitelná intuicí."

- Post - úplnost výrokové logiky (1921)
- Gödel - úplnost predikátové logiky (1930), věty o neúplnosti (1931)
- Kleene, Post, Church, Turing - formalizace pojmu algoritmus,
  existence algoritmicky nerozhodnutelných problémů (1936)
- Robinson - rezoluční metoda (1965)
- Kowalski; Colmerauer, Roussel - Prolog (1972)

Jazyk matematiky

Logika formalizuje pojem důkazu a pravdivosti matematických tvrzení.
Lze ji postupně rozčlenit dle prostředků jazyka.

- logické spojky — *výroková logika*
  Umožňují vytvářet složená tvrzení ze základních.
- proměnné pro individua, funkční a relační symboly, kvantifikátory — *1. řádu*
  Tvrzení o individuích, jejich vlastnostech a vztazích. Teorii množin, která je *"světem"* (téměř) celé matematiky, lze popsat jazykem 1. řádu.

V jazyce vyšších řádů máme navíc

- proměnné pro množiny individuí (i relace a funkce) — *logika 2. řádu*
- proměnné pro množiny množin individuí, *atd.* — *logika 3. řádu*
- ...

Příklady tvrzení v jazycích různých řádů

- *"Nebude-li pršet, nezmoknem. A když bude pršet, zmokneme, na sluníčku zase uschneme."* *výrok*

$$(\neg p \to \neg z) \wedge (p \to (z \wedge u))$$

- *"Existuje nejmenší prvek."* *1. řádu*

$$\exists x \, \forall y \, (x \leq y)$$

- Axiom indukce. *2. řádu*

$$\forall X \, ((X(0) \wedge \forall x (X(x) \to X(x+1))) \to \forall x \, X(x))$$

- *"Libovolné sjednocení otevřených množin je otevřená množina."* *3. řádu*

$$\forall \mathcal{X} \forall Y ((\forall X (\mathcal{X}(X) \to \mathcal{O}(X)) \wedge \forall x (Y(x) \leftrightarrow \exists X (\mathcal{X}(X) \wedge X(x)))) \to \mathcal{O}(Y))$$

Syntax a sémantika

Budeme studovat vztahy mezi syntaxí a sémantikou:

- *syntax*: symboly, pravidla vytváření termů a formulí, odvozovací pravidla, dokazovací systém, důkaz, dokazatelnost,
- *sémantika*: přiřazení významu, struktury, modely, splnitelnost, pravdivost.

V logice zavedeme pojem důkazu jako přesný syntaktický koncept.

Formální dokazovací systém je

- *korektní*, pokud každé dokazatelné tvrzení je pravdivé,
- *úplný*, pokud každé pravdivé tvrzení je dokazatelné.

Uvidíme, že predikátová logika (1. řádu) má dokazovací systémy, které jsou korektní a zároveň úplné. Pro logiky vyšších řádů to neplatí.

Paradoxy

"Paradoxy" jsou inspirací k přesnému zadefinování základů logiky.

- *paradox kréťana*

  Kréťan řekl: "Všichni kréťané jsou lháři."

- *paradox holiče*

  V městě žije holič, jenž holí všechny, kteří se neholí sami.

  Holí sám sebe?

- *paradox lháře*

  Tato věta je lživá.

- *Berryho paradox*

  Výraz "nejmenší přirozené číslo, které nelze definovat méně než jedenácti slovy" ho definuje pomocí deseti slov.

Jazyk

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

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

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

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

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.

$(((\neg p) \wedge q) \rightarrow (\neg(p \vee (\neg q))))$ lze zkrátit na $\neg p \wedge q \rightarrow \neg(p \vee \neg q)$

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 $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \to \psi)$ 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). □

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	$\neg p$	$p \wedge q$	$p \vee q$	$p \to q$	$p \leftrightarrow q$
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. $f : \{0, 1\}^n \to \{0, 1\}$.

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. □

Poznámka Jelikož funkce $\overline{v}\colon \mathrm{VF}_{\mathbb{P}} \to \{0,1\}$ 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.