

Výroková a predikátová logika - I

Petr Gregor

KTIML MFF UK

ZS 2013/2014

Nová koncepce přednášky

- **více logického “programování”, méně teorie modelů**
 - + rezoluce v predikátové logice, unifikace, “pozadí” Prologu
 - eliminace kvantifikátorů, Lindenbaumovy algebry, ...
- **tablo metoda namísto Hilbertovského kalkulu**
 - + algoritmicky intuitivnější, mnohdy elegantnější důkazy
 - nedostupnost literatury (zejména v čj), omezení na spočetné jazyky
- **nejprve samostatně výroková logika**
 - + ideální “hřiště” pro pochopení základních konceptů
 - zpočátku volnější tempo výkladu
- **nerozhodnutelnost a neúplnost méně formálně**
 - + důraz na principy
 - nebezpečí nepřesnosti

Plán přednášky 1/2

- Úvod

1. Předběžnosti, trocha historie, “paradoxy”, logika jako jazyk matematiky, rozdíl a vztah syntaxe a sémantiky.

- Výroková logika

2. Základní syntax a sémantika, normální tvary, složitost 2-SAT a Horn-SAT, analýza teorií s konečně prvovýroky, univerzálnost logických spojek.
3. Tablo metoda pro VL, korektnost, úplnost, kompaktnost.
4. Axiomatický přístup. Rezoluce, reprezentace programů v Prologu, lineární rezoluce pro Hornovy formule.

- Predikátová logika

5. Základní syntax a sémantika, instance a varianty. Struktury a podstruktury, otevřené teorie. Booleovy algebry.
6. Tablo metoda pro PL, korektnost, úplnost, kompaktnost. Rovnost v PL.
7. Věta o konstantách, prenexní tvar, skolemizace, Herbrandova věta.
8. Unifikace, rezoluce v PL, lifting lemma, úplnost rezoluce.

Plán přednášky 2/2

- **Teorie, modely, definovatelnost**

9. Isomorfismus struktur, kategoričnost, kompletnost, extenze. Konečná a otevřená axiomatizovatelnost.
10. Elementární vnoření, prvomodely. Löwenheim-Skolemovy věty. Definovatelné množiny.
11. Základní matematické teorie a jejich vlastnosti. Aritmetické teorie.

- **Nerozhodnutelnost, neúplnost**

12. Rozhodnutelné teorie, nerozhodnutelnost PL. Aritmetizace formulí, princip self-reference, věta o pevném bodě, nedefinovatelnost pravdy v aritmetice.
13. Aritmetizace důkazů, predikát dokazatelnosti, reprezentovatelnost. Gödelovy věty o neúplnosti, důsledky.

- **Dodatek**

14. TBA. (teorie množin / temporální / modální logika.)

Doporučená literatura

● Knihy

- ▶ A. Nerode, R.A. Shore, *Logic for Applications*, Springer, 2nd edition, 1997.
- ▶ V. Švejdar, *Logika, neúplnost, složitost a nutnost*, Academia, Praha, 2002.
- ▶ W. Hodges, *Shorter Model Theory*, Cambridge University Press, 1997.
- ▶ P. Pudlák, *Logical Foundations of Mathematics and Computational Complexity - A Gentle Introduction*, Springer, 2013.

● Elektronické zdroje

- ▶ J. Mlček, *Výroková a predikátová logika*, skripta k přednášce, 2012. [[www](#)]
- ▶ P. Štěpánek, *Meze formální metody*, skripta k přednášce, 2000. [[pdf](#)]
- ▶ slidy k přednášce

Trocha historie

- **Aristotelés** (384-322 př.n.l.) - **sylogismy**, např.
z *'žádný Q není R'* a *'každý P je Q'* odvod *'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)
- **Déscartes: Rozprava o metodě** (1637) - **algebraizace** geometrie
- **Leibnitz** - 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)
$$\text{Pro } a = \{x \mid \neg(x \in x)\} \text{ je } a \in a ?$$
- **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

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

- “Existuje nejmenší prvek.”

1. řádu

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

- Axiom indukce.

2. řádu

$$\forall X ((X(0) \wedge \forall x (X(x) \rightarrow X(x+1))) \rightarrow \forall x X(x))$$

- “Libovolné sjednocení otevřených množin je otevřená množina.”

3. řádu

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

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 krét'ana*

Krét'an řekl: “Všichni krét'ané 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.

Množinové pojmy

Veškeré pojmy zavádíme v rámci **teorie množin** pouze pomocí predikátu náležení a rovnosti (a prostředků logiky).

- Množinová vlastnost $\varphi(x)$ definuje **třídu** $\{x \mid \varphi(x)\}$. Třída, která není množinou, se nazývá **vlastní**, např. $\{x \mid x = x\}$.
- $x \notin y$, $x \neq y$ jsou zkratkou za $\neg(x \in y)$, $\neg(x = y)$.
- $\{x_0, \dots, x_{n-1}\}$ označuje množinu obsahující právě x_0, \dots, x_{n-1} , $\{x\}$ se nazývá **singleton**, $\{x, y\}$ **neuspořádaná dvojice**.
- \emptyset , \cup , \cap , \setminus , Δ značí **prázdnou množinu**, **sjednocení**, **průnik**, **rozdíl**, **symetrický rozdíl** množin, např.

$$x \Delta y = (x \setminus y) \cup (y \setminus x) = \{z \mid (z \in x \wedge z \notin y) \vee (z \notin x \wedge z \in y)\}$$

- x, y jsou **disjunktní** pokud $x \cap y = \emptyset$. $x \subseteq y$ značí, že x je **podmnožinou** y .
- **Potenční množina** (**potence**) x je $\mathcal{P}(x) = \{y \mid y \subseteq x\}$.
- **Sjednocení** (**suma**) x je $\bigcup x = \{z \mid \exists y(z \in y \wedge y \in x)\}$.
- **Pokrytí** množiny x je množina $y \subseteq \mathcal{P}(x) \setminus \{\emptyset\}$ s $\bigcup y = x$. Jsou-li navíc každé dvě (různé) množiny v y disjunktní, je y **rozklad** x .

Relace

- *uspořádaná dvojice* je $(x, y) = \{x, \{x, y\}\}$, tedy $(x, x) = \{x, \{x\}\}$,
uspořádaná n -tice je $(x_0, \dots, x_{n-1}) = ((x_0, \dots, x_{n-2}), x_{n-1})$ pro $n > 2$,
- *kartézský součin* je $a \times b = \{(x, y) \mid x \in a, y \in b\}$,
kartézská mocnina je $x^0 = \{\emptyset\}$, $x^1 = x$, $x^n = x^{n-1} \times x$ pro $n > 1$,
- *disjunktní sjednocení* je $x \uplus y = (\{\emptyset\} \times x) \cup (\{\{\emptyset\}\} \times y)$,
- *relace* je jakákoliv množina R uspořádaných dvojic,
 namísto $(x, y) \in R$ píšeme obvykle $R(x, y)$ nebo $x R y$,
definiční obor (doména) R je $\text{dom}(R) = \{x \mid \exists y (x, y) \in R\}$,
obor hodnot R je $\text{rng}(R) = \{y \mid \exists x (x, y) \in R\}$,
extenze prvku x v R je $R[x] = \{y \mid (x, y) \in R\}$,
inverzní relace k R je $R^{-1} = \{(y, x) \mid (x, y) \in R\}$,
restrikce R na množinu z je $R \upharpoonright z = \{(x, y) \in R \mid x \in z\}$,
- *složení* relací R a S je relace $R \circ S = \{(x, z) \mid \exists y ((x, y) \in R \wedge (y, z) \in S)\}$,
- *identita* na množině z je relace $\text{Id}_z = \{(x, x) \mid x \in z\}$.

Ekvivalence

- Relace R je **ekvivalence** na X , pokud pro všechna $x, y, z \in X$ platí

$$R(x, x) \quad (\text{reflexivita})$$

$$R(x, y) \rightarrow R(y, x) \quad (\text{symetrie})$$

$$R(x, y) \wedge R(y, z) \rightarrow R(x, z) \quad (\text{tranzitivita})$$

- $R[x]$ se nazývá **třída ekvivalence** (**faktor**) prvku x dle R , značíme $[x]_R$.
- $X/R = \{R[x] \mid x \in X\}$ je **faktoriace** množiny X dle R .
- Platí, že X/R je rozklad X , neboť třídy jsou disjunktní a pokrývají X .
- Naopak, je-li S rozklad X , určuje ekvivalenci (na X)

$$\{(x, y) \mid x \in z, y \in z \text{ pro nějaké } z \in S\}.$$

Uspořádání

Nechť \leq je relace na množině X . Řekneme, že \leq je

- **částečné uspořádání** (množiny X), pokud pro všechna $x, y, z \in X$

$$x \leq x \quad (\text{reflexivita})$$

$$x \leq y \wedge y \leq x \rightarrow x = y \quad (\text{antisymetrie})$$

$$x \leq y \wedge y \leq z \rightarrow x \leq z \quad (\text{tranzitivita})$$

- **lineární (totální) uspořádání**, pokud navíc pro všechna $x, y \in X$

$$x \leq y \vee y \leq x \quad (\text{dichotomie})$$

- **dobré uspořádání**, pokud navíc každá neprázdna podmnožina X obsahuje *nejmenší* prvek.

Označme ' $x < y$ ' za ' $x \leq y \wedge x \neq y$ '. Lineární uspořádání \leq na X je

- **husté uspořádání**, pokud X není singleton a pro všechna $x, y \in X$

$$x < y \rightarrow \exists z (x < z \wedge z < y) \quad (\text{hustota})$$

Funkce

Relace f je **funkce**, pokud pro každé $x \in \text{dom}(f)$ existuje jediné y s $(x, y) \in f$.

- Pak říkáme, že y je **hodnotou** funkce f v x , píšeme $f(x) = y$,
- $f: X \rightarrow Y$ značí, že f je funkce s $\text{dom}(f) = X$ a $\text{rng}(f) \subseteq Y$,
- funkce f je **na** (**surjektivní**) Y , pokud $\text{rng}(f) = Y$,
- funkce f je **prostá** (**injektivní**), pokud pro všechna $x, y \in \text{dom}(f)$

$$x \neq y \rightarrow f(x) \neq f(y)$$

- $f: X \rightarrow Y$ je **bijekce** X a Y , je-li prostá a na Y ,
- je-li $f: X \rightarrow Y$ prostá, pak $f^{-1} = \{(y, x) \mid (x, y) \in f\}$ je **inverzní funkce**,
- **obraz** množiny A přes f je $f[A] = \{y \mid (x, y) \in f \text{ pro nějaké } x \in A\}$,
- je-li $f: X \rightarrow Y$ a $g: Y \rightarrow Z$, pak pro jejich **složení** platí $(f \circ g): X \rightarrow Z$ a

$$(f \circ g)(x) = g(f(x))$$

- ${}^X Y$ značí množinu všech funkcí z X do Y .

Čísla

Uvedeme příklady explicitních konstrukcí.

- **Přirozená čísla** definujeme induktivně vztahem $n = \{0, \dots, n - 1\}$, tedy

$$0 = \emptyset, \quad 1 = \{0\} = \{\emptyset\}, \quad 2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}, \quad \dots$$

- množina **přirozených** čísel \mathbb{N} je definována jako nejmenší množina obsahující \emptyset uzavřená na $S(x) := x \cup \{x\}$ (**následník**).
- množina **celých** čísel je $\mathbb{Z} = (\mathbb{N} \times \mathbb{N}) / \sim$, kde \sim je ekvivalence definovaná

$$(a, b) \sim (c, d) \text{ právě když } a + c = b + d$$

- množina **racionálních** čísel je $\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})) / \approx$, kde \approx je dána

$$(a, b) \approx (c, d) \text{ právě když } a \cdot d = b \cdot c$$

- množina **reálných** čísel \mathbb{R} je množina **řezů** racionálních čísel, tj. netriviálních, dolů uzavřených podmnožin \mathbb{Q} bez **největšího** prvku. ($A \subset \mathbb{Q}$ je **dolů uzavřená**, pokud $y < x \in A$ implikuje $y \in A$.)

Velikosti množin

- x má **stejnou nebo menší velikost** než y (x je **subvalentní** y),
pokud existuje prostá funkce $f: x \rightarrow y$, $(x \preceq y)$
- x má **stejnou velikost** jako y , existuje-li bijekce $f: x \rightarrow y$, $(x \approx y)$
- x má **menší velikost** než y , pokud $x \preceq y$ a není $x \approx y$, $(x \prec y)$

Věta (Cantor) $x \prec \mathcal{P}(x)$ pro každou množinu x .

Důkaz $f(y) = \{y\}$ pro $y \in x$ je prostá funkce $f: x \rightarrow \mathcal{P}(x)$, tedy $x \preceq \mathcal{P}(x)$.

Pro spor předpokládejme, že existuje prostá $g: \mathcal{P}(x) \rightarrow x$. Definujme

$$y = \{g(z) \mid z \subseteq x \wedge g(z) \notin z\}$$

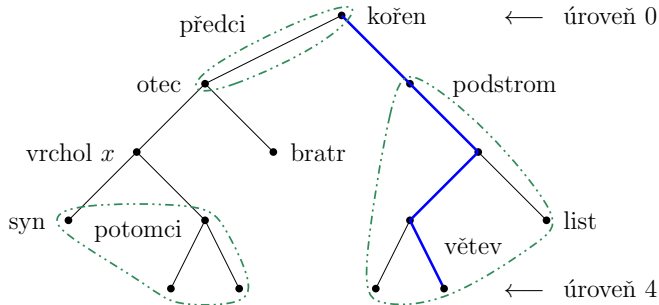
Dle definice, $g(y) \in y$ právě když $g(y) \notin y$, spor. \square

- pro každé x existuje **kardinální číslo** κ s $x \approx \kappa$, značíme $|x| = \kappa$,
- x je **konečná**, pokud $|x| = n$ pro nějaké $n \in \mathbb{N}$,
- x je **spočetná**, pokud $|x| = |\mathbb{N}| = \omega$; není-li ani konečná, je **nespočetná**,
- x má **mohutnost kontinua**, pokud $|x| = |\mathcal{P}(\mathbb{N})| = \mathfrak{c}$.

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 $\text{dom}(f) = X^n$, značíme $f: X^n \rightarrow Y$. Je-li navíc $Y = X$, je to **operace** na X .
- Funkce $f: A^n \rightarrow B$ je **konstantní**, pokud $\text{rng}(f) = \{y\}$ pro nějaké $y \in Y$, pro $n = 0$ je $f = \{(\emptyset, y)\}$ a f ztotožňujeme s **konstantou** y .
- Aritu relace či funkce značíme $\text{ar}(R)$ či $\text{ar}(f)$ 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 větvičími se stromy, ve kterých má každý vrchol kromě kořene **bezprostředního** předka (*otce*).

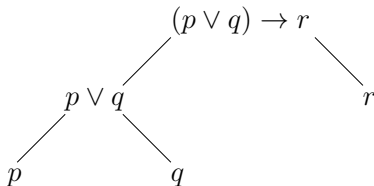
- ***n-tá úroveň*** stromu T pro $n \in \mathbb{N}$ je daná indukcí, obsahuje syny vrcholů z $(n - 1)$ -ní úrovně, 0-tá úroveň obsahuje právě kořen,
- ***hloubka*** stromu T je maximální číslo $n \in \mathbb{N}$ neprázdné úrovně; pokud má T nekonečnou větev, je ***hloubka nekonečná*** či ω .
- strom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

Lemma (König) *Každý nekonečný, konečně větvičí 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



Na závěr

- *Lze celou matematiku převést do logických formulí?*
programování, AI, strojové dokazování, [Peano: Formulario](#) (1895-1908)
- *Proč to lidé (většinou) nedělají?*
- *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 např. [rezolucí](#).

Jak to vyřešíme *elegantněji*? V čem náš postup spočívá?