Výroková a predikátová logika - dodatek

Petr Gregor

KTIML MFF UK

ZS 2019/2020

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 $\neg(x \in y)$, $\neg(x = y)$.
- $\{x_0, \ldots, x_{n-1}\}$ označuje množinu obsahující právě $x_0, \ldots, x_{n-1}$, $\{x\}$ se nazývá *singleton*, $\{x, y\}$ *neuspořádaná dvojice*.
- $\emptyset$, $\cup$, $\cap$, $\setminus$, $\triangle$ značí *prázdnou množinu*, *sjednocení*, *průnik*, *rozdíl*, *symetrický rozdíl* množin, např.
$$x \triangle y = (x \setminus y) \cup (y \setminus x) = \{z \mid (z \in x \land z \notin y) \lor (z \notin x \land z \in y)\}$$
- 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 $\bigcup x = \{z \mid \exists y(z \in y \land y \in x)\}$.
- *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 $(x_0, \ldots, x_{n-1}) = ((x_0, \ldots, x_{n-2}), x_{n-1})$ 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 $\mathrm{dom}(R) = \{x \mid \exists y\ (x, y) \in R\}$,
  obor hodnot R je $\mathrm{rng}(R) = \{y \mid \exists x\ (x, y) \in R\}$,
  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 $R \restriction z = \{(x, y) \in R \mid x \in z\}$,
- *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 $\mathrm{Id}_z = \{(x, x) \mid x \in z\}$.

Ekvivalence

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

$$R(x,x) \qquad \text{(reflexivita)}$$
$$R(x,y) \rightarrow R(y,x) \qquad \text{(symetrie)}$$
$$R(x,y) \wedge R(y,z) \rightarrow R(x,z) \qquad \text{(tranzitivita)}$$

- $R[x]$ se nazývá *třída ekvivalence* (*faktor*) prvku x dle R, značíme i $[x]_R$.
- $X/R = \{R[x] \mid x \in X\}$ je *faktorizace* 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 $x, y, z \in X$

$$x \leq x \qquad \text{(reflexivita)}$$
$$x \leq y \;\wedge\; y \leq x \;\rightarrow\; x = y \qquad \text{(antisymetrie)}$$
$$x \leq y \;\wedge\; y \leq z \;\rightarrow\; x \leq z \qquad \text{(tranzitivita)}$$

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

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

- *dobré uspořádání*, pokud navíc každá neprázdná 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 $x, y \in X$

$$x < y \;\rightarrow\; \exists z\,(x < z \wedge z < y) \qquad \text{(hustota)}$$

Funkce

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

- Pak říkáme, že y je *hodnotou* funkce f v x, píšeme $f(x) = y$,
- $f: X \to Y$ značí, že f je funkce s $\mathrm{dom}(f) = X$ a $\mathrm{rng}(f) \subseteq Y$,
- funkce f je *na* (*surjektivní*) Y, pokud $\mathrm{rng}(f) = Y$,
- funkce f je *prostá* (*injektivní*), pokud pro všechna $x, y \in \mathrm{dom}(f)$
$$x \neq y \quad \to \quad f(x) \neq f(y)$$
- $f: X \to Y$ je *bijekce* X a Y, je-li prostá a na Y,
- je-li $f: X \to Y$ 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 $f: X \to Y$ a $g: Y \to Z$, pak pro jejich složení platí $(f \circ g): X \to Z$ 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 $n = \{0, \ldots, n-1\}$, tedy
$$0 = \emptyset, \quad 1 = \{0\} = \{\emptyset\}, \quad 2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}, \quad \ldots$$
- 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
$$(a, b) \sim (c, d) \text{ právě když } a + d = b + c$$
- množina *racionálních* čísel je $\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}))/\approx$, kde $\approx$ je dána
$$(a, b) \approx (c, d) \text{ právě když } a.d = b.c$$
- 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 $f\colon x \to y$, $(x \preccurlyeq y)$
- x má *stejnou velikost* jako y, existuje-li bijekce $f\colon x \to y$, $(x \approx y)$
- x má *menší velikost* než y, pokud $x \preccurlyeq y$ 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 $f\colon x \to \mathcal{P}(x)$, tedy $x \preccurlyeq \mathcal{P}(x)$.
Pro spor předpokládejme, že existuje prostá $g\colon \mathcal{P}(x) \to x$. Definujme

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

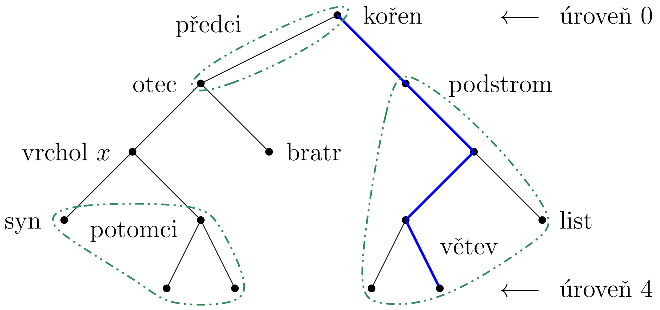
Dle definice, $g(y) \in y$ právě když $g(y) \notin y$, spor. $\square$

- pro každé x existuje *kardinální číslo* κ s $x \approx \kappa$, značíme $|x| = \kappa$,
- x je *konečná*, pokud $|x| = n$ pro nějaké $n \in \mathbb{N}$, jinak je *nekonečná*,
- x je *spočetná*, pokud je konečná nebo $|x| = |\mathbb{N}| = \omega$; jinak 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 $\mathrm{dom}(f) = X^n$, 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. $\square$

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