Šestá přednáška

NAIL062 Výroková a predikátová logika

Jakub Bulín (KTIML MFF UK)

Zimní semestr 2023

Šestá přednáška

Program

- úvod do predikátové logiky
- syntaxe a sémantika predikátové logiky
- vlastnosti teorií

Materiály

Zápisky z přednášky, Sekce 6.1-6.5 z Kapitoly 6

ČÁST II – PREDIKÁTOVÁ LOGIKA

Kapitola 6: Syntaxe a sémantika predikátové logiky

6.1 Úvod

Predikátová logika neformálně

Výroková logika: popis světa pomocí výroků složených z prvovýroků (výrokových proměnných) – bitů informace

Predikátová logika [prvního řádu]:

- základní stavební kámen jsou proměnné reprezentující individua – nedělitelné objekty z nějaké množiny (např. přirozená čísla, vrcholy grafu, stavy mikroprocesoru)
- tato individua mají určité vlastnosti a vzájemné vztahy (relace), kterým říkáme predikáty
  - $\mathrm{Leaf}(x)$ nebo $\mathrm{Edge}(x, y)$ mluvíme-li o grafu
  - $x \leq y$ v přirozených číslech
- a mohou vstupovat do funkcí
  - $\mathrm{lowest\_common\_ancestor}(x, y)$ v zakořeněném stromu
  - $\mathrm{succ}(x)$ nebo $x + y$ v přirozených číslech
- a mohou být konstantami se speciálním významem, např. root v zakořeněném stromu, 0 v tělese.

Syntaxe neformálně

- atomické formule: predikát (včetně rovnosti $=$) o proměnných nebo o termech ('výrazy' složené z funkcí popř. konstant)
- formule jsou složené z atomických formulí pomocí logických spojek, a dvou kvantifikátorů:

$\forall x$ "pro všechna individua (reprezentovaná proměnnou x)"
$\exists x$ "existuje individuum (reprezentované proměnnou x)"

Např. *"Každý, kdo má dítě, je rodič."* lze formalizovat takto:

$$(\forall x)((\exists y)\mathrm{child\_of}(y, x) \rightarrow \mathrm{is\_parent}(x))$$

- $\mathrm{child\_of}(y, x)$ je binární predikát vyjadřující, že individuum reprezentované proměnnou y je dítětem individua reprezentovaného proměnnou x
- $\mathrm{is\_parent}(x)$ je unární predikát vyjadřující, že individuum reprezentované x je rodič

Sémantika neformálně

$$(\forall x)((\exists y)\mathrm{child\_of}(y, x) \to \mathrm{is\_parent}(x))$$

Platnost? Záleží na modelu světa/systému, který nás zajímá:

Model je...

- (neprázdná) množina individuí, spolu
- s binární relací interpretující binární relační symbol $\mathrm{child\_of}$, a
- s unární relací (tj. podmnožinou) interpretující unární relační symbol $\mathrm{is\_parent}$

Obecně mohou být relace jakékoliv, snadno sestrojíme model, ve kterém formule neplatí, např.

$$\mathcal{A} = \langle \{0, 1\}, \{(0, 0), (0, 1), (1, 0), (1, 1)\}, \emptyset \rangle$$

Příklad s funkcemi a konstantami

"Je-li $x_1 \leq y_1$ a $x_2 \leq y_2$, potom platí $(y_1 \cdot y_2) - (x_1 \cdot x_2) \geq 0$."

$$\varphi = (x_1 \leq y_1) \wedge (x_2 \leq y_2) \rightarrow ((y_1 \cdot y_2) + (-(x_1 \cdot x_2)) \geq 0)$$

- dva binární relační symboly $(\leq, \geq)$, binární funkční symbol $+$, unární funkční symbol $-$, a konstantní symbol 0
- model, ve kterém φ platí: $\mathbb{N}$ s binárními relacemi $\leq^{\mathbb{N}}, \geq^{\mathbb{N}}$, bin. funkcemi $+^{\mathbb{N}}, \cdot^{\mathbb{N}}$, unární funkcí $-^{\mathbb{N}}$, a konstantou $0^{\mathbb{N}} = 0$
- vezmeme-li ale podobně množinu $\mathbb{Z}$, φ už platit nebude

Poznámky:

- mohli bychom chápat '$-$' jako binární, obvykle ale bývá unární
- pro konstantní symbol 0 používáme (jak je zvykem) stejný symbol, jako pro přirozené číslo 0. Ale pozor, v našem modelu může být symbol 0 interpretován jako jiné číslo, nebo náš model vůbec nemusí sestávat z čísel!

Ještě o syntaxi

$$\varphi = (x_1 \leq y_1) \wedge (x_2 \leq y_2) \to ((y_1 \cdot y_2) + (-(x_1 \cdot x_2)) \geq 0)$$

- φ nemá žádné kvantifikátory, tj. je otevřená
- x_1, x_2, y_1, y_2 jsou volné proměnné této formule (nejsou vázané žádným kvantifikátorem), píšeme $\varphi(x_1, x_2, y_1, y_2)$
- sémantiku φ chápeme stejně jako $(\forall x_1)(\forall x_2)(\forall y_1)(\forall y_2)\varphi$
- používáme konvence (infixový zápis, vynechání závorek), jinak:

$$\varphi = ((\leq (x_1, y_1) \wedge \leq (x_2, y_2)) \to \leq (+(\cdot(y_1, y_2), -(\cdot(x_1, x_2))), 0))$$

- cvičení: definujte strom formule, nakreslete ho pro φ

Termy vs. atomické formule

$$\varphi = (x_1 \leq y_1) \land (x_2 \leq y_2) \rightarrow ((y_1 \cdot y_2) + (-(x_1 \cdot x_2)) \geq 0)$$

- výraz $(y_1 \cdot y_2) + (-(x_1 \cdot x_2))$ je term
- výrazy $(x_1 \leq y_1)$, $(x_2 \leq y_2)$ a $((y_1 \cdot y_2) + (-(x_1 \cdot x_2)) \geq 0)$ jsou (všechny) atomické (pod)formule φ

V čem je rozdíl? Máme-li konkrétní model, a konkrétní ohodnocení proměnných individui (prvky) tohoto modelu:

- výsledkem termu (při daném ohodnocení proměnných) je konkrétní individuum z modelu, zatímco
- atomickým formulí lze přiřadit pravdivostní hodnotu (a tedy kombinovat je logickými spojkami)

6.2 Struktury

Signatura

- specifikuje jakého typu bude daná struktura, tj. jaké má relace, funkce (jakých arit) a konstanty, a symboly pro ně
- konstanty lze chápat jako funkce arity 0, tj. funkce bez vstupů

Signatura je dvojice $\langle \mathcal{R}, \mathcal{F} \rangle$, kde $\mathcal{R}, \mathcal{F}$ jsou disjunktní množiny symbolů (relační a funkční, ty zahrnují konstantní) spolu s danými aritami (tj. danými funkcí $\mathrm{ar} \colon \mathcal{R} \cup \mathcal{F} \to \mathbb{N}$) a neobsahující symbol '$=$' (ten je rezervovaný pro rovnost).

- často zapíšeme jen výčtem symbolů, jsou-li arity a zda jsou relační nebo funkční zřejmé
- kromě běžně používaných symbolů typicky používáme:
  - pro relační symboly $P, Q, R, \ldots$
  - pro funkční (nekonstantní) symboly $f, g, h, \ldots$
  - pro konstantní symboly $c, d, a, b, \ldots$

Příklady signatur

- $\langle E \rangle$ signatura grafů: E je binární relační symbol (struktury jsou uspořádané grafy)
- $\langle \leq \rangle$ signatura částečných uspořádání: stejná jako signatura grafů, jen jiný symbol (ne každá struktura v této signatuře je částečné uspořádání! k tomu musí splňovat příslušné axiomy)
- $\langle +, -, 0 \rangle$ signatura grup: $+$ je binární funkční, $-$ unární funkční, 0 konstantní symbol
- $\langle +, -, 0, \cdot, 1 \rangle$ signatura těles: $\cdot$ je binární funkční, 1 konstantní symbol
- $\langle +, -, 0, \cdot, 1, \leq \rangle$ signatura uspořádaných těles: $\leq$ je binární relační symbol
- $\langle -, \wedge, \vee, \bot, \top \rangle$ signatura Booleových algeber: $\wedge, \vee$ jsou binární funkční, $\bot, \top$ jsou konstantní symboly
- $\langle S, +, \cdot, 0, \leq \rangle$ signatura aritmetiky: S je unární funkční symbol

Struktury

Strukturu dané signatury získáme tak, že:

- zvolíme neprázdnou doménu, a na ní
- zvolíme realizace (také říkáme interpretace) všech relačních a funkčních symbolů (a konstant)
- to znamená konkrétní relace resp. funkce příslušných arit
- realizací konstantního symbolu je zvolený prvek z domény
- na tom, jaké konkrétní symboly jsou v signatuře nezáleží (např. $+$ neznamená, že realizace musí souviset se sčítáním)

Příklady struktur 1/3

- Struktura v prázdné signatuře $\langle\ \rangle$ je libovolná neprázdná množina. (Nemusí být konečná, ani spočetná! Formálně to bude trojice $\langle A, \emptyset, \emptyset \rangle$, ale rozdíl zanedbáme.)
- Struktura v signatuře grafů je $\mathcal{G} = \langle V, E \rangle$, kde $V \neq \emptyset$ a $E \subseteq V^2$, říkáme jí orientovaný graf.
  - je-li E ireflexivní a symetrická, je to jednoduchý graf
  - je-li E reflexivní, tranzitivní, a antisymetrická, jde o částečné uspořádání
  - je-li E reflexivní, tranzitivní, a symetrická, je to ekvivalence
- Struktury v signatuře částečných uspořádání jsou tytéž, jako v signatuře grafů, signatury se liší jen symbolem. (Ne každá struktura v signatuře částečných uspořádání je č. uspořádání!)

Příklady struktur 2/3

Struktury v signatuře grup jsou například následující grupy:

- $\underline{\mathbb{Z}_n} = \langle \mathbb{Z}_n, +, -, 0 \rangle$, aditivní grupa celých čísel modulo n (operace jsou modulo n).

  Poznámka: $\underline{\mathbb{Z}_n}$ znamená strukturu, zatímco $\mathbb{Z}_n$ jen její doménu. Často se to ale nerozlišuje a $\mathbb{Z}_n$ se používá i pro strukturu. Podobně $+, -, 0$ jsou jak symboly, tak interpretace.
- $\mathcal{S}_n = \langle \mathrm{Sym}_n, \circ, {}^{-1}, \mathrm{id} \rangle$ je symetrická grupa (grupa všech permutací) na n prvcích.
- $\underline{\mathbb{Q}}^* = \langle \mathbb{Q} \setminus \{0\}, \cdot, {}^{-1}, 1 \rangle$ je multiplikativní grupa (nenulových) racionálních čísel. (Interpretací symbolu 0 je číslo 1!)

Všechny tyto struktury splňují axiomy teorie grup, snadno ale najdeme jiné, které axiomy nesplňují, nejsou tedy grupami.

Příklady struktur 3/3

- Struktury $\underline{\mathbb{Q}} = \langle \mathbb{Q}, +, -, 0, \cdot, 1, \leq \rangle$ a $\underline{\mathbb{Z}} = \langle \mathbb{Z}, +, -, 0, \cdot, 1, \leq \rangle$ (se standardními operacemi a uspořádáním) jsou v signatuře uspořádaných těles (ale jen první z nich je uspořádané těleso).
- $\underline{\mathcal{P}(X)} = \langle \mathcal{P}(X), \bar{\ }, \cap, \cup, \emptyset, X \rangle$, tzv. potenční algebra nad množinou X, je struktura v signatuře Booleových algeber. (Booleova algebra je to pokud $X \neq \emptyset$.)
- $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$, kde $S(x) = x + 1$, a ostatní symboly jsou interpretovány standardně, je standardní model aritmetiky.

Definice struktury

Struktura v signatuře $\langle \mathcal{R}, \mathcal{F} \rangle$ je trojice $\mathcal{A} = \langle A, \mathcal{R}^{\mathcal{A}}, \mathcal{F}^{\mathcal{A}} \rangle$, kde

- A je neprázdná množina, říkáme jí doména (také univerzum),
- $\mathcal{R}^{\mathcal{A}} = \{R^{\mathcal{A}} \mid R \in \mathcal{R}\}$ kde $R^{\mathcal{A}} \subseteq A^{\mathrm{ar}(R)}$ je interpretace relačního symbolu R,
- $\mathcal{F}^{\mathcal{A}} = \{f^{\mathcal{A}} \mid f \in \mathcal{F}\}$ kde $f^{\mathcal{A}} \colon A^{\mathrm{ar}(f)} \to A$ je interpretace funkčního symbolu f (speciálně pro konstantní symbol $c \in \mathcal{F}$ máme $c^{\mathcal{A}} \in A$).

Příklad: rozmyslete si, jak vypadají struktury v signatuře n konstant $\langle c_1, c_2, \ldots, c_n \rangle$? Popište všechny 5-prvkové v signatuře 3 konstant.

6.3 Syntaxe

6.4 Sémantika

6.5 Vlastnosti teorií