Jedenáctá přednáška

NAIL062 Výroková a predikátová logika

Jakub Bulín (KTIML MFF UK)

Zimní semestr 2023

Jedenáctá přednáška

Program

- korektnost rezoluce
- lifting lemma a úplnost rezoluce
- LI-rezoluce a Prolog
- elementární ekvivalence

Materiály

Zápisky z přednášky, Sekce 8.6-8.7 z Kapitoly 8, Sekce 9.1 z Kapitoly 9

8.6 Korektnost a úplnost

Korektnost rezolučního kroku

Tvrzení: Mějme klauzule C_1, C_2 a jejich rezolventu C. Platí-li v nějaké struktuře $\mathcal{A}$ klauzule C_1 a C_2, potom v ní platí i C.

Důkaz: Buď $C_1 = C_1' \sqcup \{A_1, \ldots, A_n\}$, $C_2 = C_2' \sqcup \{\neg B_1, \ldots, \neg B_m\}$, a $C = C_1'\sigma \cup C_2'\sigma$, kde $S\sigma = \{A_1\sigma\}$ (a σ je nejobecnější). Klauzule jsou otevřené formule, proto platí i jejich instance:

$$\mathcal{A} \models C_1\sigma \ \text{ a } \ \mathcal{A} \models C_2\sigma$$

Po aplikaci unifikace máme:

$$C_1\sigma = C_1'\sigma \cup \{A_1\sigma\}$$
$$C_2\sigma = C_2'\sigma \cup \{\neg A_1\sigma\}$$

Chceme ukázat, že $\mathcal{A} \models C[e]$ pro lib. ohodnocení e.

- Je-li $\mathcal{A} \models A_1\sigma[e]$, potom $\mathcal{A} \not\models \neg A_1\sigma[e]$ a musí $\mathcal{A} \models C_2'\sigma[e]$. Tedy i $\mathcal{A} \models C[e]$.
- Je-li $\mathcal{A} \not\models A_1\sigma[e]$, musí být $\mathcal{A} \models C_1'\sigma[e]$ a opět $\mathcal{A} \models C[e]$. $\square$

Korektnost rezoluce

Věta (O korektnosti rezoluce): Pokud je CNF formule S rezolucí zamítnutelná, potom je nesplnitelná.

Důkaz: Víme, že $S \vdash_R \square$, vezměme tedy nějaký rezoluční důkaz $\square$ z S. Kdyby existoval model $\mathcal{A} \models S$, díky korektnosti rezolučního pravidla bychom dokázali (indukcí podle délky důkazu) i $\mathcal{A} \models \square$, což ale není možné. $\square$

Lifting lemma

úplnost rezoluce dokážeme převedením na případ výrokové logiky: rezoluční důkaz 'na úrovni VL' je možné 'zvednout' na úroveň PL

Lifting lemma: Buďte C_1 a C_2 klauzule s disj. množ. proměnných, C_1^* a C_2^* jejich základní instance, C^* rezolventa C_1^* a C_2^*. Potom C_1 a C_2 mají rezolventu C takovou, že C^* je základní instance C.

(důkaz na příštím slidu)

Důsledek: Buď S CNF formule a označme S^* množinu všech jejích základních instancí. Pokud $S^* \vdash_R C^*$ pro nějakou základní klauzuli C^* ('na úrovni VL'), potom existuje klauzule C a základní substituce σ taková, že $C^* = C\sigma$ a $S \vdash_R C$ ('na úrovni PL').

Důkaz: Snadno z Lifting lemmatu indukcí dle délky důkazu. $\square$

Důkaz Lifting lemmatu

Nechť $C_1^* = C_1\tau_1$ a $C_2^* = C_2\tau_2$, τ_1 a τ_2 zákl. substituce nesdílející žádnou proměnnou. Najdeme rezolventu C, že $C^* = C\tau_1\tau_2$.

Buď C^* rezolventa C_1^* a C_2^* přes literál $P(t_1, \dots, t_k)$. Víme, že:

$C_1 = C_1' \sqcup \{A_1, \dots, A_n\}$, kde $\{A_1, \dots, A_n\}\tau_1 = \{P(t_1, \dots, t_k)\}$

$C_2 = C_2' \sqcup \{\neg B_1, \dots, \neg B_m\}, \{\neg B_1, \dots, \neg B_m\}\tau_2 = \{\neg P(t_1, \dots, t_k)\}$

Tedy $(\tau_1\tau_2)$ unifikuje $S = \{A_1, \dots, A_n, B_1, \dots, B_m\}$. Buď σ nejob. unifikace pro S z Unifikačního algoritmu. Zvolme $C = C_1'\sigma \cup C_2'\sigma$.

$$C\tau_1\tau_2 = (C_1'\sigma \cup C_2'\sigma)\tau_1\tau_2 = C_1'\sigma\tau_1\tau_2 \cup C_2'\sigma\tau_1\tau_2 = C_1'\tau_1\tau_2 \cup C_2'\tau_1\tau_2$$

$$= C_1'\tau_1 \cup C_2'\tau_2 = (C_1 \setminus \{A_1, \dots, A_n\})\tau_1 \cup (C_2 \setminus \{\neg B_1, \dots, \neg B_m\})\tau_2$$

$$= (C_1^* \setminus \{P(t_1, \dots, t_k)\}) \cup (C_2^* \setminus \{\neg P(t_1, \dots, t_k)\}) = C^*$$

Zde $=$ plyne z vlastnosti 'navíc' Unif. algoritmu $(\tau_1\tau_2) = \sigma(\tau_1\tau_2)$, a $=$ z toho, že jde o základní substituce nesdílející proměnnou. $\square$

Úplnost rezoluce

Věta (O úplnosti rezoluce): Je-li CNF formule S nesplnitelná, potom je zamítnutelná rezolucí.

Důkaz: Množina S^* všech základních instancí klauzulí z S je také nesplnitelná (důsledek Herbrandovy věty). Úplnost výrokové rezoluce dává $S^* \vdash_R \square$ ('na úrovni VL').

Z důsledku Lifting lemmatu dostáváme klauzuli C a základní substituci σ takové, že $C\sigma = \square$ a $S \vdash_R C$ ('na úrovni PL').

Ale protože prázdná klauzule $\square$ je instancí C, musí být $C = \square$. Tím jsme našli rezoluční zamítnutí $S \vdash_R \square$. $\square$

8.7 LI-rezoluce

Lineární důkaz a LI-důkaz

- Lineární důkaz klauzule C z formule S je konečná posloupnost

$$\begin{bmatrix} C_0 \\ B_0 \end{bmatrix}, \begin{bmatrix} C_1 \\ B_1 \end{bmatrix}, \ldots, \begin{bmatrix} C_n \\ B_n \end{bmatrix}, C_{n+1}$$

  kde: B_0 a C_0 jsou varianty klauzulí z S, $C_{n+1} = C$,
  - C_{i+1} je rezolventa C_i a B_i
  - B_i varianta klauzule z S nebo $B_i = C_j$ pro nějaké $j < i$.
- Lineární zamítnutí S je lineární důkaz $\square$ z S
- LI-důkaz je lin. důkaz, kde vš. B_i jsou varianty klauzulí z S
- C LI-dokazatelná z S, $S \vdash_{LI} C$, pokud existuje LI-důkaz
- S je LI-zamítnutelná, pokud $S \vdash_{LI} \square$
- korektnost (lineární i LI-rezoluce) je zřejmá

Úplnost LI-rezoluce pro Hornovy formule

Věta (O úplnosti lineární rezoluce): C má lineární důkaz z S, právě když má rezoluční důkaz z S (tj. $S \vdash_R C$).

Důkaz: převodem na VL (Lifting lemma zachovává linearitu) $\square$

Věta (O úplnosti LI-rezoluce pro Hornovy formule): Je-li Hornova formule T splnitelná, a $T \cup \{G\}$ je nesplnitelná pro cíl G, potom $T \cup \{G\} \vdash_{LI} \square$, a to LI-zamítnutím, které začíná cílem G.

Důkaz: úplnost ve VL + Herbrandova věta + Lifting lemma $\square$

- Hornova formule: množina Hornových klauzulí
- Hornova klauzule: nejvýše jeden pozitivní literál
- Pravidlo: klauzule s 1 pozitivním a alespoň 1 negativním literálem
- Fakt: pozitivní jednotková klauzule
- Cíl: neprázdná klauzule bez pozitivního literálu
- Programové klauzule: pravidla a fakta
- Program: Hornova formule obsahující jen programové klauzule

Rezoluce v Prologu

TODO

ČÁST III – POKROČILÉ PARTIE

Kapitola 9: Teorie modelů

Teorie modelů

- vztah mezi vlastnostmi teorií a tříd jejich modelů
- bližší matematice než informatice a aplikacím
- jen několik vybraných dostupných výsledků

\+ co je třeba pro Gödelovy věty (Kapitola 10)

\+ co se nevešlo jinam

9.1 Elementární ekvivalence

Teorie struktury $\mathcal{A}$ (v jazyce L):

$$\mathrm{Th}(\mathcal{A}) = \{\varphi \mid \varphi \text{ je } L\text{-sentence a } \mathcal{A} \models \varphi\}$$

Např. pro standardní model aritmetiky $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$ říkáme $\mathrm{Th}(\underline{\mathbb{N}})$ aritmetika přirozených čísel, je nerozhodnutelná (neexistuje algoritmus, který pro každou φ doběhne a odpoví, zda $T \models \varphi$)

Pozorování: Nechť $\mathcal{A}$ je L-struktura a T je L-teorie.

- $\mathrm{Th}(\mathcal{A})$ je kompletní teorie
- $\mathcal{A} \in \mathrm{M}_L(T) \Rightarrow \mathrm{Th}(\mathcal{A})$ je (kompletní) jednoduchá extenze T
- $\mathcal{A} \in \mathrm{M}_L(T)$, T kompletní $\Rightarrow \mathrm{Th}(\mathcal{A}) = \mathrm{Csq}_L(T) \sim T$

Elementární ekvivalence

L-struktury $\mathcal{A}$ a $\mathcal{B}$ jsou elementárně ekvivalentní ($\mathcal{A} \equiv \mathcal{B}$), pokud v nich platí tytéž L-sentence, neboli: $\mathcal{A} \equiv \mathcal{B} \;\Leftrightarrow\; \mathrm{Th}(\mathcal{A}) = \mathrm{Th}(\mathcal{B})$

Například pro $\langle \mathbb{R}, \leq \rangle$, $\langle \mathbb{Q}, \leq \rangle$, $\langle \mathbb{Z}, \leq \rangle$

- $\langle \mathbb{R}, \leq \rangle \equiv \langle \mathbb{Q}, \leq \rangle$: snadno pomocí hustoty
- $\langle \mathbb{Q}, \leq \rangle \not\equiv \langle \mathbb{Z}, \leq \rangle$: v $\langle \mathbb{Z}, \leq \rangle$ má každý prvek bezprostředního následníka, v $\langle \mathbb{Q}, \leq \rangle$ ne, tedy $\varphi \in \mathrm{Th}(\langle \mathbb{Z}, \leq \rangle) \setminus \mathrm{Th}(\langle \mathbb{Q}, \leq \rangle)$ pro následující sentenci:

$$\varphi = (\forall x)(\exists y)(x \leq y \wedge \neg x = y \wedge (\forall z)(x \leq z \rightarrow z = x \vee y \leq z))$$

Kompletní jednoduché extenze

Pro teorii T nás hlavně zajímá, jak vypadají modely.

- T je kompletní, právě když má jediný model až na elementární ekvivalenci (všechny modely jsou elementárně ekvivalentní)
- Modely T až na elementární ekvivalenci jednoznačně odpovídají kompletním jednoduchým extenzím T, ty jsou tvaru $\mathrm{Th}(\mathcal{A})$ pro $\mathcal{A} \in \mathrm{M}(T)$, kde $\mathcal{A} \equiv \mathcal{B} \Leftrightarrow \mathrm{Th}(\mathcal{A}) = \mathrm{Th}(\mathcal{B})$

Místo hledání modelů stačí najít kompletní jednoduché extenze!

Motivace: ukážeme, že lze-li efektivně popsat všechny kompletní jednoduché extenze efektivně dané teorie, potom je rozhodnutelná.

- algoritmus, který pro vstup (i, j) vypíše j-tý axiom i-té kompletní jednoduché extenze (v nějakém očíslování)
- algoritmus, který postupně vygeneruje všechny axiomy teorie

Schopnost efektivně popsat kompletní jedn. extenze je vzácná, vyžaduje silné předpoklady, ale u mnoha důležitých teorií to lze.

Příklad: DeLO*

Teorie hustého lin. uspořádání (DeLO*) je extenze teorie uspořádání o linearitu (dichotomii), hustotu, a někdy se přidává netrivialita:

- $x \leq y \vee y \leq x$
- $x \leq y \wedge \neg\, x = y \rightarrow (\exists z)(x \leq z \wedge z \leq y \wedge \neg\, z = x \wedge \neg\, z = y)$
- $(\exists x)(\exists y)(\neg\, x = y)$

Tvrzení: Buď $\varphi = (\exists x)(\forall y)(x \leq y)$ a $\psi = (\exists x)(\forall y)(y \leq x)$. Následující jsou právě všechny kompletní jednoduché extenze DeLO*:

- $\mathrm{DeLO} = \mathrm{DeLO}^* \cup \{\neg\varphi, \neg\psi\}$
- $\mathrm{DeLO}^+ = \mathrm{DeLO}^* \cup \{\neg\varphi, \psi\}$
- $\mathrm{DeLO}^- = \mathrm{DeLO}^* \cup \{\varphi, \neg\psi\}$
- $\mathrm{DeLO}^\pm = \mathrm{DeLO}^* \cup \{\varphi, \psi\}$

Stačí ukázat, že jsou kompletní. Potom už je zřejmé, že žádná další kompletní jednoduchá extenze DeLO* nemůže existovat.

Jak ukážeme, kompletnost plyne z faktu, že jsou ω-kategorické, tj. mají jediný spočetný model až na izomorfismus.

Důsledky Löwenheim-Skolemovy věty bez rovnosti

Připomeňme:

Věta (L.-S. bez rovnosti): Ve spočetném jazyce bez rovnosti má každá bezesporná teorie spočetně nekonečný model.

Jednoduchý důsledek:

Důsledek: Je-li L spočetný bez rovnosti, potom ke každé L-struktuře existuje elementárně ekvivalentní spočetně nekonečná struktura.

Důkaz: $\mathrm{Th}(\mathcal{A})$ je bezesporná (má model $\mathcal{A}$), tedy dle L.-S. věty má spočetně nekonečný model $\mathcal{B} \models \mathrm{Th}(\mathcal{A})$, to znamená $\mathcal{B} \equiv \mathcal{A}$. $\square$

Bez rovnosti tedy nelze vyjádřit např. 'model má právě 42 prvků'.

Důsledky Löwenheim-Skolemovy věty s rovností

V důkazu L.-S. věty máme kanonický model pro bezespornou větev tabla z T pro $\mathrm{F}\bot$; pro jazyk s rovností stačí faktorizovat dle $=^A$:

Věta (L.-S. s rovností): Ve spočetném jazyce s rovností má každá bezesporná teorie spočetný model (konečný, nebo nekonečný).

I tato verze má snadný důsledek pro konkrétní struktury:

Důsledek: Je-li L spočetný s rovností, ke každé nekonečné L-struktuře existuje elem. ekvivalentní spočetně nekonečná struktura.

Důkaz: Mějme nekonečnou L-strukturu $\mathcal{A}$. Stejně jako v důkazu Důsledku bez rovnosti najdeme spočetně nekonečnou $\mathcal{B} \equiv \mathcal{A}$.

Protože v $\mathcal{A}$ neplatí pro žádné $n \in \mathbb{N}$ sentence vyjadřující 'existuje nejvýše n prvků' (což lze pomocí rovnosti snadno zapsat), neplatí ani v $\mathcal{B}$, tedy $\mathcal{B}$ nemůže být konečná. $\square$

Spočetné algebraicky uzavřené těleso

- algebraicky uzavřené těleso: každý polynom nenulového stupně v něm má kořen
- $\mathbb{Q}$ není, $x^2 - 2$ nemá v $\mathbb{Q}$ kořen
- $\mathbb{R}$ není, $x^2 + 1$ nemá v $\mathbb{R}$ kořen
- $\mathbb{C}$ je algebraicky uzavřené, ale je nespočetné

Algebraickou uzavřenost vyjádříme sentencemi ψ_n, pro $n > 0$:

$$(\forall x_{n-1}) \dots (\forall x_0)(\exists y)(y^n + x_{n-1} \cdot y^{n-1} + \dots + x_1 \cdot y + x_0) = 0$$

kde y^k je zkratka za term $y \cdot y \cdot \ \cdots \ \cdot y$

Důsledek: Existuje spočetné algebraicky uzavřené těleso.

Důkaz: Dle Důsledku L.S. věty (s rovností) existuje spočetně nekonečná $\mathcal{A} \equiv \mathbb{C}$. Protože $\mathbb{C}$ je těleso a splňuje ψ_n pro všechna $n > 0$, je i $\mathcal{A}$ algebraicky uzavřené těleso. $\square$