Výroková a predikátová logika - XI

Petr Gregor

KTIML MFF UK

ZS 2013/2014

Obecné rezoluční pravidlo

Nechť klauzule C_1, C_2 neobsahují stejnou proměnnou a jsou ve tvaru

$$C_1 = C_1' \sqcup \{A_1, \ldots, A_n\}, \quad C_2 = C_2' \sqcup \{\neg B_1, \ldots, \neg B_m\},$$

kde $S = \{A_1, \ldots, A_n, B_1, \ldots, B_m\}$ lze unifikovat a $n, m \geq 1$. Pak klauzule

$$C = C_1'\sigma \cup C_2'\sigma,$$

kde σ je nejobecnější unifikace pro S, je *rezolventa* klauzulí C_1 a C_2.

Např. v klauzulích $\{P(x), Q(x,z)\}$ *a* $\{\neg P(y), \neg Q(f(y), y)\}$ *lze unifikovat* $S = \{Q(x,z), Q(f(y), y)\}$ pomocí nejobecnější unifikace $\sigma = \{x/f(y), z/y\}$ a získat z nich rezolventu $\{P(f(y)), \neg P(y)\}$.

Poznámka *Podmínce o různých proměnných lze vyhovět přejmenováním proměnných v rámci klauzule. Je to nutné, např. z* $\{\{P(x)\}, \{\neg P(f(x))\}\}$ *lze po přejmenování získat* $\square$, *ale* $\{P(x), P(f(x))\}$ *nelze unifikovat.*

Rezoluční důkaz

Pojmy zavedeme jako ve VL, jen navíc dovolíme přejmenování proměnných.

- *Rezoluční důkaz (odvození)* klauzule C z formule S je konečná posloupnost $C_0, \ldots, C_n = C$ taková, že pro každé $i \leq n$ je $C_i = C_i'\sigma$, kde $C_i' \in S$ a σ je přejmenování proměnných, nebo je C_i rezolventou nějakých dvou předchozích klauzulí (i stejných).
- Klauzule C je (rezolucí) *dokazatelná* z S, psáno $S \vdash_R C$, pokud má rezoluční důkaz z S.
- *Zamítnutí* formule S je rezoluční důkaz $\square$ z S.
- S je (rezolucí) *zamítnutelná*, pokud $S \vdash_R \square$.

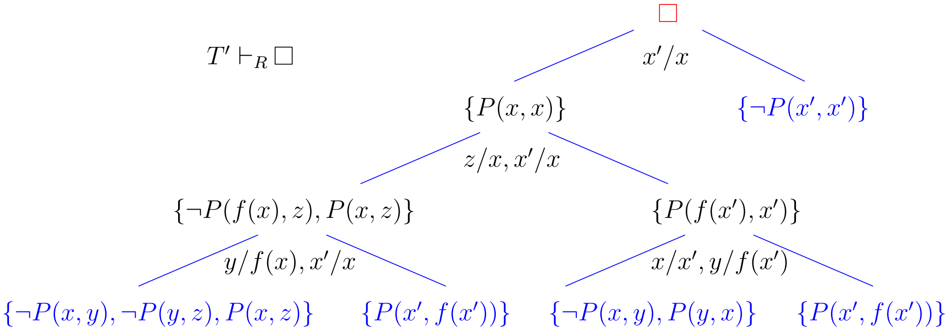
Poznámka *Eliminace více literálů najednou je někdy nezbytná, např.* $S = \{\{P(x), P(y)\}, \{\neg P(x), \neg P(y)\}\}$ *je rezolucí zamítnutelná, ale nemá zamítnutí, při kterém by se v každém kroku eliminoval pouze jeden literál.*

Příklad rezoluce

Mějme teorii $T = \{\neg P(x,x),\ P(x,y) \rightarrow P(y,x),\ P(x,y) \wedge P(y,z) \rightarrow P(x,z)\}$.

Je $T \models (\exists x)\neg P(x,f(x))$? Tedy, je následující formule T' nesplnitelná?

$T' = \{\{\neg P(x,x)\}, \{\neg P(x,y), P(y,x)\}, \{\neg P(x,y), \neg P(y,z), P(x,z)\}, \{P(x,f(x))\}\}$



Korektnost rezoluce

Nejprve ukážeme, že obecné rezoluční pravidlo je korektní.

Tvrzení Nechť C je rezolventa klauzulí C_1, C_2. Pro každou L-strukturu $\mathcal{A}$,

$$\mathcal{A} \models C_1 \text{ a } \mathcal{A} \models C_2 \quad \Rightarrow \quad \mathcal{A} \models C.$$

Důkaz Nechť $C_1 = C_1' \sqcup \{A_1, \ldots, A_n\}$, $C_2 = C_2' \sqcup \{\neg B_1, \ldots, \neg B_m\}$, σ je nejobecnější unifikace pro $S = \{A_1, \ldots, A_n, B_1, \ldots, B_m\}$ a $C = C_1'\sigma \cup C_2'\sigma$.

- Jelikož C_1, C_2 jsou otevřené, platí i $\mathcal{A} \models C_1\sigma$ a $\mathcal{A} \models C_2\sigma$.
- Máme $C_1\sigma = C_1'\sigma \cup \{S\sigma\}$ a $C_2\sigma = C_2'\sigma \cup \{\neg(S\sigma)\}$.
- Ukážeme, že $\mathcal{A} \models C[e]$ pro každé e. Je-li $\mathcal{A} \models S\sigma[e]$, pak $\mathcal{A} \models C_2'\sigma[e]$ a tedy $\mathcal{A} \models C[e]$. Jinak $\mathcal{A} \not\models S\sigma[e]$, pak $\mathcal{A} \models C_1'\sigma[e]$ a tedy $\mathcal{A} \models C[e]$. □

Věta (korektnost) *Je-li formule S rezolucí zamítnutelná, je S nesplnitelná.*

Důkaz Nechť $S \vdash_R \square$. Kdyby $\mathcal{A} \models S$ pro nějakou strukturu $\mathcal{A}$, z korektnosti rezolučního pravidla by platilo i $\mathcal{A} \models \square$, což není možné. ■

Lifting lemma

Rezoluční důkaz na úrovni VL lze "zdvihnout" na úroveň PL.

Lemma *Nechť $C_1^* = C_1\tau_1$, $C_2^* = C_2\tau_2$ jsou základní instance klauzulí C_1, C_2 neobsahující stejnou proměnnou a C^* je rezolventa C_1^* a C_2^*. Pak existuje rezolventa C klauzulí C_1 a C_2 taková, že $C^* = C\tau_1\tau_2$ je základní instance C.*

Důkaz Předpokládejme, že C^* je rezolventa C_1^*, C_2^* přes literál $P(t_1, \ldots, t_k)$.

- Pak lze psát $C_1 = C_1' \sqcup \{A_1, \ldots, A_n\}$ a $C_2 = C_2' \sqcup \{\neg B_1, \ldots, \neg B_m\}$, kde $\{A_1, \ldots, A_n\}\tau_1 = \{P(t_1, \ldots, t_k)\}$ a $\{\neg B_1, \ldots, \neg B_m\}\tau_2 = \{\neg P(t_1, \ldots, t_k)\}$.
- Tedy $(\tau_1\tau_2)$ unifikuje $S = \{A_1, \ldots, A_n, B_1, \ldots, B_m\}$ a je-li σ mgu pro S z unifikačního algoritmu, pak $C = C_1'\sigma \cup C_2'\sigma$ je rezolventa C_1 a C_2.
- Navíc $(\tau_1\tau_2) = \sigma(\tau_1\tau_2)$ z vlastnosti $(*)$ pro σ a tedy

$$\begin{aligned} C\tau_1\tau_2 &= (C_1'\sigma \cup C_2'\sigma)\tau_1\tau_2 = C_1'\sigma\tau_1\tau_2 \cup C_2'\sigma\tau_1\tau_2 = C_1'\tau_1 \cup C_2'\tau_2 \\ &= (C_1 \setminus \{A_1, \ldots, A_n\})\tau_1 \cup (C_2 \setminus \{\neg B_1, \ldots, \neg B_m\})\tau_2 \\ &= (C_1^* \setminus \{P(t_1, \ldots, t_k)\}) \cup (C_2^* \setminus \{\neg P(t_1, \ldots, t_k)\}) = C^*. \quad \square \end{aligned}$$

Úplnost

Důsledek *Nechť S' je množina všech základních instancí klauzulí formule S. Je-li $S' \vdash_R C'$ (na úrovni VL), kde C' je základní klauzule, pak existuje klauzule C a základní substituce σ taková, že $C' = C\sigma$ a $S \vdash_R C$ (na úrovni PL).*

Důkaz Indukcí dle délky rezolučního odvození pomocí lifting lemmatu. $\square$

Věta (úplnost) *Je-li formule S nesplnitelná, je $S \vdash_R \square$.*

Důkaz Je-li S nesplnitelná, dle (důsledku) Herbrandovy věty je nesplnitelná i množina S' všech základních instancí klauzulí z S.

- Dle úplnosti rezoluční metody ve VL je $S' \vdash_R \square$ (na úrovni VL).
- Dle předchozího důsledku existuje klauzule C a substituce σ taková, že $\square = C\sigma$ a $S \vdash_R C$ (na úrovni PL).
- Jediná klauzule, jejíž instance je $\square$, je klauzule $C = \square$. $\blacksquare$

Lineární rezoluce

Stejně jako ve VL, rezoluční metodu lze značně omezit (bez ztráty úplnosti).

- *Lineární důkaz* klauzule C z formule S je konečná posloupnost dvojic $(C_0, B_0), \dots, (C_n, B_n)$ t.ž. C_0 je varianta klauzule v S a pro každé $i \leq n$
  - $i)$ B_i je varianta klauzule v S nebo $B_i = C_j$ pro nějaké $j < i$, a
  - $ii)$ C_{i+1} je rezolventa C_i a B_i, kde $C_{n+1} = C$.
- C je *lineárně dokazatelná* z S, psáno $S \vdash_L C$, má-li lineární důkaz z S.
- *Lineární zamítnutí* S je lineární důkaz $\square$ z S.
- S je *lineárně zamítnutelná*, pokud $S \vdash_L \square$.

Věta *S je lineárně zamítnutelná, právě když S je nesplnitelná.*

Důkaz $(\Rightarrow)$ Každý lineární důkaz lze transformovat na rezoluční důkaz.
$(\Leftarrow)$ Plyne z úplnosti lineární rezoluce ve VL (nedokazováno), neboť lifting lemma zachovává linearitu odvození. $\square$

LI-rezoluce

Stejně jako ve VL, pro Hornovy formule můžeme lineární rezoluci dál omezit.

- *LI-rezoluce* (*"linear input"*) z formule S je lineární rezoluce z S, ve které je každá boční klauzule B_i variantou klauzule ze (vstupní) formule S.
- Je-li klauzule C dokazatelná LI-rezolucí z S, píšeme $S \vdash_{LI} C$.
- *Hornova klauzule* je klauzule obsahující nejvýše jeden pozitivní literál.
- *Hornova formule* je množina (i nekonečná) Hornových klauzulí.
- *Fakt* je (Hornova) klauzule $\{P\}$, kde P je pozitivní literál.
- *Pravidlo* je (Hornova) klauzule s právě jedním pozitivním a aspoň jedním negativním literálem. Pravidla a fakta jsou *programové klauzule*.
- *Cíl* je neprázdná (Hornova) klauzule bez pozitivního literálu.

Věta *Je-li Hornova formule T splnitelná a $T \cup \{G\}$ je nesplnitelná pro cíl G, lze $\square$ odvodit LI-rezolucí z $T \cup \{G\}$ začínající G.*

Důkaz Plyne z Herbrandovy věty, stejné věty ve VL a lifting lemmatu. $\square$

Program v Prologu

Program (v Prologu) je Hornova formule obsahující pouze programové klauzule, tj. fakta nebo pravidla.

$syn(X,Y) :\!-\ otec(Y,X), muz(X).$	$\{syn(X,Y), \neg otec(Y,X), \neg muz(X)\}$
$syn(X,Y) :\!-\ matka(Y,X), muz(X).$	$\{syn(X,Y), \neg matka(Y,X), \neg muz(X)\}$
$muz(jan).$	$\{muz(jan)\}$
$otec(jiri, jan).$	$\{otec(jiri, jan)\}$
$matka(julie, jan).$	$\{matka(julie, jan)\}$

$?\!-\ syn(jan, X)$ $\quad$ $P \models (\exists X) syn(jan, X)$? $\quad$ $\{\neg syn(jan, X)\}$

Zajímá nás, zda daný existenční dotaz vyplývá z daného programu.

Důsledek *Pro program P a cíl $G = \{\neg A_1, \ldots, \neg A_n\}$ v proměnných $X_1, \ldots, X_m$*

(1) $P \models (\exists X_1) \ldots (\exists X_m)(A_1 \wedge \ldots \wedge A_n)$, *právě když*

(2) $\square$ *lze odvodit LI-rezolucí z $P \cup \{G\}$ začínající (variantou) cíle G.*

LI-rezoluce nad programem

Je-li odpoveď na dotaz kladná, chceme navíc znát výstupní substituci.

Výstupní substituce σ LI-rezoluce $\square$ z $P \cup \{G\}$ začínající $G = \{\neg A_1, \ldots, \neg A_n\}$ je složení mgu v jednotlivých krocích (jen na proměnné v G). Platí,

$$P \models (A_1 \wedge \ldots \wedge A_n)\sigma.$$

$$\begin{array}{ll}
\{\neg syn(jan, X)\} & \{syn(X', Y'), \neg otec(Y', X'), \neg muz(X')\} \\
\quad X'/jan \mid Y'/X & \\
\{\neg otec(X, jan), \neg muz(jan)\} & \{muz(jan)\} \\
\quad \mid & \\
\{\neg otec(X, jan)\} & \{otec(jiri, jan)\} \\
\quad X/jiri \mid & \\
\quad \square & \\
a) &
\end{array}$$

$$\begin{array}{ll}
\{\neg syn(jan, X)\} & \{syn(X', Y'), \neg matka(Y', X'), \neg muz(X')\} \\
\quad X'/jan \mid Y'/X & \\
\{\neg matka(X, jan), \neg muz(jan)\} & \{muz(jan)\} \\
\quad \mid & \\
\{\neg matka(X, jan)\} & \{matka(julie, jan)\} \\
\quad X/julie \mid & \\
\quad \square & \\
b) &
\end{array}$$

Výstupní substituce $a)$ $X = jiri$, $b)$ $X = julie$.

Teorie struktury

Mnohdy nás zajímá, co platí v jedné konkrétní struktuře.

Teorie struktury $\mathcal{A}$ je množina $\mathrm{Th}(\mathcal{A})$ sentencí (stejného jazyka) platných v $\mathcal{A}$.

Pozorování *Pro každou strukturu $\mathcal{A}$ a teorii T jazyka L,*

(i) $\mathrm{Th}(\mathcal{A})$ *je kompletní teorie,*

(ii) *je-li $\mathcal{A} \models T$, je $\mathrm{Th}(\mathcal{A})$ jednoduchá (kompletní) extenze teorie T,*

(iii) *je-li $\mathcal{A} \models T$ a T je kompletní, je $\mathrm{Th}(\mathcal{A})$ ekvivalentní s T,*
tj. $\theta^L(T) = \mathrm{Th}(\mathcal{A})$.

Např. pro $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$ je $\mathrm{Th}(\underline{\mathbb{N}})$ je aritmetika přirozených čísel.

Poznámka *Později uvidíme, že ačkoliv je $\mathrm{Th}(\underline{\mathbb{N}})$ kompletní teorie, je (algoritmicky) nerozhodnutelná.*

Elementární ekvivalence

- Struktury $\mathcal{A}$ a $\mathcal{B}$ jazyka L jsou *elementárně ekvivalentní*, psáno $\mathcal{A} \equiv \mathcal{B}$, pokud v nich platí stejné formule (jazyka L), tj. $\mathrm{Th}(\mathcal{A}) = \mathrm{Th}(\mathcal{B})$.

  Např. $\langle \mathbb{R}, \leq \rangle \equiv \langle \mathbb{Q}, \leq \rangle$, ale $\langle \mathbb{Q}, \leq \rangle \not\equiv \langle \mathbb{Z}, \leq \rangle$, neboť v $\langle \mathbb{Z}, \leq \rangle$ má každý prvek bezprostředního následníka, zatímco v $\langle \mathbb{Q}, \leq \rangle$ ne.

- T je kompletní, právě když má až na el. ekvivalenci právě jeden model.

  Např. teorie DeLO hustých lineárních uspořádání bez konců je kompletní.

Zajímá nás, jak vypadají modely dané teorie (až na elementární ekvivalenci).

Pozorování *Pro modely $\mathcal{A}, \mathcal{B}$ teorie T platí $\mathcal{A} \equiv \mathcal{B}$, právě když $\mathrm{Th}(\mathcal{A})$, $\mathrm{Th}(\mathcal{B})$ jsou ekvivalentní (jednoduché kompletní extenze teorie T).*

Poznámka *Lze-li efektivně (rekurzivně) popsat pro efektivně danou teorii T, jak vypadají všechny její kompletní extenze, je T (algoritmicky) rozhodnutelná.*

Jednoduché kompletní extenze - příklad

Teorie $DeLO^*$ hustého lineárního uspořádání jazyka $L = \langle \leq \rangle$ s rovností je

$$
\begin{array}{ll}
x \leq x & \text{(reflexivita)} \\
x \leq y \ \wedge \ y \leq x \ \rightarrow \ x = y & \text{(antisymetrie)} \\
x \leq y \ \wedge \ y \leq z \ \rightarrow \ x \leq z & \text{(tranzitivita)} \\
x \leq y \ \vee \ y \leq x & \text{(dichotomie)} \\
x < y \ \rightarrow \ (\exists z)\,(x < z \ \wedge \ z < y) & \text{(hustota)} \\
(\exists x)(\exists y)(x \neq y) & \text{(netrivialita)}
\end{array}
$$

kde '$x < y$' je zkratka za '$x \leq y \ \wedge \ x \neq y$'.

Označme φ, ψ sentence $(\exists x)(\forall y)(x \leq y)$, resp. $(\exists x)(\forall y)(y \leq x)$. Uvidíme, že

$$
\begin{array}{llll}
DeLO & = DeLO^* \cup \{\neg\varphi, \neg\psi\}, & DeLO^{\pm} & = DeLO^* \cup \{\varphi, \psi\}, \\
DeLO^{+} & = DeLO^* \cup \{\neg\varphi, \psi\}, & DeLO^{-} & = DeLO^* \cup \{\varphi, \neg\psi\}
\end{array}
$$

jsou všechny (neekvivalentní) jednoduché kompletní extenze teorie $DeLO^*$.