Desátá přednáška

NAIL062 Výroková a predikátová logika

Jakub Bulín (KTIML MFF UK)

Zimní semestr 2023

Desátá přednáška

Program

- grounding, Herbrandova věta
- unifikace, unifikační algoritmus
- rezoluční pravidlo, rezoluční důkaz

Materiály

Zápisky z přednášky, Sekce 8.3-8.5 z Kapitoly 8

8.3 Grounding

Grounding

- základní (ground) instance otevřené φ ve volných proměnných $x_1, \ldots, x_n$ je $\varphi(x_1/t_1, \ldots, x_n/t_n)$, kde vš. t_i jsou konstantní

  Herbrandova věta říká, že je-li otevřená teorie nesplnitelná, lze to doložit "na konkrétních prvcích": existuje konečně mnoho základních instancí axiomů, jejichž konjunkce je nesplnitelná

- např. pro $T = \{P(x, y) \vee R(x, y), \neg P(c, y), \neg R(x, f(x))\}$ substituujeme konstantní termy $\{x/c, y/f(c)\}$:

  $$(P(c, f(c)) \vee R(c, f(c))) \ \wedge\ \neg P(c, f(c)) \ \wedge\ \neg R(c, f(c))$$

- základní atomické sentence chápeme jako prvovýroky:

  $$(p_1 \vee p_2) \wedge \neg p_1 \wedge \neg p_2$$

- to už snadno zamítneme výrokovou rezolucí
- p_1 znamená "platí $P(c, f(c))$", p_2 znamená "platí $R(c, f(c))$"

Přímá redukce do výrokové logiky

Herbrandova věta + korektnost a úplnost výrokové rezoluce dává následující, neefektivní postup (S' je moc velká, i nekonečná):

1. $S \rightsquigarrow S'$ = množina všech základních instancí klauzulí z S
2. atomické sentence v S' chápeme jako prvovýroky
3. S nesplnitelná $\Leftrightarrow$ S' zamítnutelná 'na úrovni výrokové logiky'

Např. pro $S = \{\{P(x,y), R(x,y)\}, \{\neg P(c,y)\}, \{\neg R(x, f(x))\}\}$

$$
\begin{aligned}
S' = \{&\{P(c,c), R(c,c)\}, \{P(c,f(c)), R(c,f(c))\}, \{P(f(c),c), R(f(c),c)\}, \ldots, \\
&\{\neg P(c,c)\}, \{\neg P(c,f(c))\}, \{\neg P(c,f(f(c)))\}, \{\neg P(c,f(f(f(c))))\}, \ldots, \\
&\{\neg R(c,f(c))\}, \{\neg R(f(c),f(f(c)))\}, \{\neg R(f(f(c)),f(f(f(c))))\}, \ldots\}
\end{aligned}
$$

S' je nesplnitelná obsahuje konečnou nesplnitelnou podmnožinu:

$$\{\{P(c,f(c)), R(c,f(c))\}, \{\neg P(c,f(c))\}, \{\neg R(c,f(c))\}\} \vdash_R \square$$

Efektivnější je hledat vhodné základní instance unifikací [za chvíli]

Herbrandův model

Mějme jazyk $L = \langle \mathcal{R}, \mathcal{F} \rangle$ s alespoň jedním konstantním symbolem. L-struktura $\mathcal{A} = \langle A, \mathcal{R}^{\mathcal{A}}, \mathcal{F}^{\mathcal{A}} \rangle$ je Herbrandův model, jestliže:

- A je množina všech konst. L-termů (Herbrandovo univerzum)
- pro každý n-ární $f \in \mathcal{F}$ a (konstantní) "t_1", …, "t_n" $\in A$:
$$f^{\mathcal{A}}(\text{“}t_1\text{”}, \ldots, \text{“}t_n\text{”}) = \text{“}f(t_1, \ldots, t_n)\text{”}$$
- speciálně, pro konstantní symbol $c \in \mathcal{F}$ je $c^{\mathcal{A}} = \text{“}c\text{”}$
- na relační symboly neklademe podmínky

Např. $L = \langle P, f, c \rangle$ (P unární rel., f binární funkční, c konstantní)
Herbrandův model je každá struktura $\mathcal{A} = \langle A, P^{\mathcal{A}}, f^{\mathcal{A}}, c^{\mathcal{A}} \rangle$, kde

- $A = \{\text{“}c\text{”}, \text{“}f(c,c)\text{”}, \text{“}f(c,f(c,c))\text{”}, \text{“}f(f(c,c),c)\text{”} \ldots\}$
- $c^{\mathcal{A}} = \text{“}c\text{”}$
- $f^{\mathcal{A}}(\text{“}c\text{”}, \text{“}c\text{”}) = \text{“}f(c,c)\text{”}$, $f^{\mathcal{A}}(\text{“}c\text{”}, \text{“}f(c,c)\text{”}) = \text{“}f(c,f(c,c))\text{”}$, $f^{\mathcal{A}}(\text{“}f(c,c)\text{”}, \text{“}c\text{”}) = \text{“}f(f(c,c),c)\text{”}$, atd.
- $P^{\mathcal{A}} \subseteq A$ může být libovolná

Věta (Herbrandova): Je-li T otevřená, v jazyce bez rovnosti a s alespoň jedním konstantním symbolem, potom:

- buď má T Herbrandův model, nebo
- existuje konečně mnoho základních instancí axiomů T, jejichž konjunkce je nesplnitelná.

Důkaz: $T_{\text{ground}} =$ množina všech základních instancí axiomů T

Zkonstruujeme "systematické tablo" τ z T_{ground} s $\mathrm{F}\bot$ v kořeni, ale z jazyka L, bez rozšíření o pomocné konstantní symboly na L_C. (Nepotřebujeme je, protože v T_{ground} nejsou kvantifikátory.)

Pokud má τ bezespornou větev, je "kanonický model" (opět bez pomocných symbolů) Herbrandovým modelem T.

Jinak je τ důkaz sporu, T_{ground} (a tedy i T) je nesplnitelná. Tablo τ je konečné, používá jen konečně mnoho $\alpha_{\text{ground}} \in T_{\text{ground}}$, jejich konjunkce už je nesplnitelná. $\square$

Poznámky

- konstatní symbol potřebujeme, aby existovaly vůbec nějaké konstantní termy (ale není-li v L žádný, můžeme ho přidat)
- Herbrandův model je podobný kanonickému, ale nepřidáváme pomocné symboly, a neříkáme nic o relacích
- je-li jazyk s rovností, najdeme Herbrandův model pro T^* (přidané axiomy rovnosti) a faktorizujeme podle $=^A$

Důsledky Herbrandovy věty

Důsledek: Je-li T otevřená v jazyce s konstantním symbolem, potom T má model, právě když má model teorie T_{ground}.

Důkaz: $\Rightarrow$ V modelu T platí i všechny základní instance axiomů. Je tedy i modelem T_{ground}.

$\Leftarrow$ Pokud T nemá model, podle Herbrandovy věty je nějaká konečná podmnožina teorie T_{ground} nesplnitelná. $\square$

Důsledek: Mějme otevřenou $\varphi(x_1, \ldots, x_n)$ v L s konst. symbolem. Potom existuje $m \in \mathbb{N}$ a konstantní L-termy t_{ij} ($i \in [m], j \in [n]$), že sentence $(\exists x_1) \ldots (\exists x_n)\varphi(x_1, \ldots, x_n)$ je pravdivá, právě když je následující formule (výroková) tautologie:

$$\varphi(x_1/t_{11}, \ldots, x_n/t_{1n}) \vee \cdots \vee \varphi(x_1/t_{m1}, \ldots, x_n/t_{mn})$$

Důkaz: Je pravdivá, právě když $(\forall x_1) \ldots (\forall x_n)\neg\varphi$ neboli $\neg\varphi$ je nesplnitelná. Stačí aplikovat Herbrandovu větu na $T = \{\neg\varphi\}$. $\square$

8.4 Unifikace

Příklady substitucí

Místo všech základních použijeme ‘vhodné’ substituce (unifikace):

1. $\{P(x), Q(x, a)\}$ a $\{\neg P(y), \neg Q(b, y)\}$
   - substitucí $\{x/b, y/a\}$ získáme $\{P(b), Q(b, a)\}$ a $\{\neg P(a), \neg Q(b, a)\}$, z nich rezolucí $\{P(b), \neg P(a)\}$
   - nebo $\{x/y\}$ a rezolucí přes $P(y)$ máme $\{Q(y, a), \neg Q(b, y)\}$
   - šlo by např. $\{x/a\}$, získat $\{Q(a, a), \neg Q(b, a)\}$, ale to je horší
2. $\{P(x), Q(x, z)\}$ a $\{\neg P(y), \neg Q(f(y), y)\}$
   - lze použít $\{x/f(a), y/a, z/a\}$, získat $\{P(f(a)), Q(f(a), a)\}$ a $\{\neg P(a), \neg Q(f(a), a)\}$, rezolucí $\{P(f(a)), \neg P(a)\}$
   - lepší je $\{x/f(z), y/z\}$, dává $\{P(f(z)), Q(f(z), z)\}$ a $\{\neg P(z), \neg Q(f(z), z)\}$, rezolventu $\{P(f(z)), \neg P(z)\}$
   - proč lepší? obecnější, rezolventa ‘říká více’: $\{P(f(a)), \neg P(a)\}$ je důsledkem $\{P(f(z)), \neg P(z)\}$, ale nejsou ekvivalentní
   - $\{x/f(a), y/a, z/a\}$ získáme složením $\{x/f(z), y/z\}$ a $\{z/a\}$

Substituce formálně

- substituce je konečná množina $\sigma = \{x_1/t_1, \ldots, x_n/t_n\}$, kde x_i jsou navzájem různé proměnné, t_i jsou termy, t_i není x_i
  - základní: všechny termy t_i jsou konstantní
  - přejmenování proměnných: vš. t_i navzájem různé proměnné
- výraz je term nebo literál (atomická formule nebo její negace)
- instance výrazu E při substituci $\sigma = \{x_1/t_1, \ldots, x_n/t_n\}$, $E\sigma$: simultánně nahradíme všechny výskyty x_i za termy t_i
- pro množinu výrazů S je $S\sigma = \{E\sigma \mid E \in S\}$

- simultánně, aby výskyt x_i v termu t_j nevedl ke zřetězení
- např. $S = \{P(x), R(y,z)\}$, $\sigma = \{x/f(y,z), y/x, z/c\}$

$$S\sigma = \{P(f(y,z)), R(x,c)\}$$

Skládání substitucí

Vlastnosti skládání

Unifikace

Unifikační algoritmus

Ukázkový běh

Důkaz korektnosti

8.5 Rezoluční metoda