Matematická logika

Rostislav Horčík

horcik@math.feld.cvut.cz
horcik@cs.cas.cz
www.cs.cas.cz/~horcik

Rezoluce v predikátové logice

- Minule jsme viděli, že k ukázání nesplnitelnosti množiny klausulí S v predikátové logice stačí použít výrokovou rezoluční metodu na ground instancích klausulí z S.
- Nicméně resoluční pravidlo funguje i na obecných klausulích.
- V důsledku toho je možné přeskočit krok s generováním ground instancí a odvozovat rezolventy rovnou.
- Nicméně občas budeme muset klausule trochu upravit před použitím rezolučního pravidla.

Příklad I

- Mějme klausule $C_1 = P(x) \vee \neg Q(x, y)$ a $C_2 = Q(x, y) \vee R(y)$.
- Vidíme, že C_1 obsahuje negativní literál $\neg Q(x, y)$ a C_2 pozitivní $Q(x, y)$.
- V tomto případě můžeme najít rezolventu C_1 a C_2 analogicky jako ve výrokové logice, tj. $C = P(x) \vee R(y)$.
- Navíc $\{C_1, C_2\} \models C$. Tzn. že každý model množiny $\{C_1, C_2\}$ je i model C.
- Z toho také plyne, že $\{C_1, C_2\}$ je ekvisplnitelná s $\{C_1, C_2, C\}$.

Příklad II

- Mějme klausule $C_1 = P(x) \vee \neg Q(x)$ a $C_2 = Q(a) \vee R(b)$.
- C_1 obsahuje negativní literál $\neg Q(x)$ a C_2 pozitivní $Q(a)$.
- Predikát Q není použit na stejné termy, tudíž nemůžeme postupovat jako v minulém příkladě.
- Nicméně substituce termu a za proměnnou x v C_1 nám dá klausuli $P(a) \vee \neg Q(a)$.
- Nyní již můžeme postupovat obdobně najít rezolventu $C = P(a) \vee R(b)$.
- Stejně jako předtím $\{C_1, C_2\}$ je ekvisplnitelná s $\{C_1, C_2, C\}$.

Příklad III

- Nechť $C_1 = \neg P(x, y) \vee Q(x, y, a)$, $C_2 = \neg Q(g(v), z, z) \vee R(v, z)$.
- C_1 obsahuje pozitivní literál $Q(x, y, a)$ a C_2 negativní $\neg Q(g(v), z, z)$.
- Podobně jako předtím je třeba najít substituci, která oba literály sjednotí. Možností je obecně víc. Nás bude zajímat tzv. neobecnější substituce (zachovávající pokud možno, co nejvíce proměnných).
- Uvažujme následující substituci z/a, y/a, $x/g(v)$, která oba literály sjednotí.
- Pak výsledná rezolventa je $C = \neg P(g(v), a) \vee R(v, a)$.
- Uvedená substituce je “nejobecnější”. Příklad jiné, která však již není “nejobecnější” je např. z/a, y/a, v/a, $x/g(a)$.

Substituce

Definice

Nechť $x_1, \ldots, x_n$ jsou navzájem různé proměnné a $t_1, \ldots, t_n$ termy takové, že $x_i \neq t_i$. Substituce je množina $\{x_1/t_1, \ldots, x_n/t_n\}$.

Definice

Nechť φ je formule a $\sigma = \{x_1/t_1, \ldots, x_n/t_n\}$ substituce. Pak symbolem $\varphi\sigma$ značíme formuli, která vznikne z φ současným nahrazením proměnných x_i ve formuli φ termy t_i. Podobně pro term t definujeme $t\sigma$.

Příklad

Nechť $\varphi = \neg P(x, y) \vee Q(x, y, a)$ a $\sigma = \{z/a, y/a, x/g(v)\}$. Pak

$$\varphi\sigma = \neg P(g(v), a) \vee Q(g(v), a, a)\,.$$

Složená substituce

Definice

Mějme substituce $\theta = \{x_1/t_1, \ldots, x_n/t_n\}$ a $\sigma = \{y_1/s_1, \ldots, y_k/s_k\}$. Označme $X = \{x_1, \ldots, x_n\}$ a $Y = \{y_1, \ldots, y_k\}$. Složená sustituce $\theta\sigma$ je definována

$$\theta\sigma = \{x_i/t_i\sigma \mid x_i \in X, x_i \neq t_i\sigma\} \cup \{y_j/s_j \mid y_j \in Y, y_j \notin X\}\,.$$

Tvrzení

Nechť E je formule nebo term a θ, σ substituce. Pak $E(\theta\sigma) = (E\theta)\sigma$.

Příklad

- Mějme substituce $\theta = \{x/f(y), y/f(a), z/u\}$ a $\sigma = \{y/g(a), u/z, v/f(f(a))\}$.
- Pak $X = \{x, y, z\}$ a $Y = \{y, u, v\}$.
- Dále $f(y)\sigma = f(g(a))$, $f(a)\sigma = f(a)$, $u\sigma = z$.
- Tedy $\theta\sigma = \{x/f(g(a)), y/f(a), u/z, v/f(f(a))\}$.

- Mějme dále atomickou formuli $E = P(u, v, x, y, z)$.
- Pak

$$\begin{aligned} E(\theta\sigma) &= P(z, f(f(a)), f(g(a)), f(a), z)\,, \\ E\theta &= P(u, v, f(y), f(a), u)\,, \\ (E\theta)\sigma &= P(z, f(f(a)), f(g(a)), f(a), z)\,. \end{aligned}$$

Unifikace

Definice

Sustituce σ je pro atomické formule $\varphi_1, \ldots, \varphi_n$ unifikace, pokud $\varphi_1\sigma = \cdots = \varphi_n\sigma$. Podobně se definuje pro termy.

Definice

Unifikaci σ nazýváme nejobecnější unifikace (mgu), pokud pro každou unifikaci θ existuje substituce μ taková, že $\theta = \sigma\mu$.

- Unifikovat lze samozřejmě jen některé atomické formule.
- Nutná podmínka unifikace atomických formulí $\varphi_1, \ldots, \varphi_n$ je zřejmě to, že všechny obsahují stejný predikátový symbol.
- Pokud atomické formule $\varphi_1, \ldots, \varphi_n$ splňují tuto podmínku, pak existence unifikace již záleží jen na argumentech onoho stejného predikátového symbolu.

Termové rovnice

Příklad

Uvažujme atomické formule $\varphi = P(f(x), g(y))$ a $\psi = P(f(f(a)), g(x))$. Pak existence unifikace φ a ψ lze vyjádřit pomocí následujících termových rovnic:

$$f(x) = f(f(a)), \qquad g(y) = g(x).$$

Definice

Řekneme, že množina termových rovnic je ve vyřešeném tvaru, pokud

- každá rovnice má tvar $x_i = t_i$, kde x_i je proměnná a t_i term;
- každá proměnná vyskytující se na levé straně některé z rovnic se nevyskytuje nikde jinde.

Množina termových rovnic ve vyřešeném tvaru definuje substituci $\{x_1/t_1, \ldots, x_n/t_n\}$.

Unifikační algoritmus

Vstup: množina termových rovnic
Výstup: množina termových rovnic ve vyřešeném tvaru nebo “unifikace neexistuje”

1. Otoč rovnici $t = x$ na $x = t$, kde t není proměnná.
2. Vymaž rovnici $x = x$.
3. Pro rovnici $t = t'$, kde t, t' nejsou proměnné, tj. $t = f(s_1, \dots, s_n)$ a $t' = g(s'_1, \dots, s'_k)$; pokud $f \neq g$ vrať “unifikace neexistuje”, jinak nahraď rovnici $t = t'$ rovnicemi $s_1 = s'_1, \dots, s_n = s'_n$.
4. Pro rovnici $x = t$; pokud t obsahuje x vrať “unifikace neexistuje”, jinak nahraď všechny výskyty proměnné x termem t.

Věta

Unifikační algoritmus skončí po konečně mnoha krocích a pokud vrátí množinu termových rovnic ve vyřešeném tvaru, pak tato definuje hledanou nejobecnější unifikaci.

Příklad

Uvažujme termové rovnice

$$\begin{aligned} g(y) &= x\,, \\ f(x, h(x), y) &= f(g(z), w, z)\,. \end{aligned}$$

Příklad

Uvažujme termové rovnice

$$\begin{aligned} g(y) &= x\,, \\ f(x, h(x), y) &= f(g(z), w, z)\,. \end{aligned}$$

Pravidlo 1:

$$\begin{aligned} x &= g(y)\,, \\ f(x, h(x), y) &= f(g(z), w, z)\,. \end{aligned}$$

Příklad

Uvažujme termové rovnice

$$\begin{aligned} g(y) &= x\,, \\ f(x, h(x), y) &= f(g(z), w, z)\,. \end{aligned}$$

Pravidlo 3:

$$\begin{aligned} x &= g(y)\,, \\ x &= g(z)\,, \\ h(x) &= w\,, \\ y &= z\,. \end{aligned}$$

Příklad

Uvažujme termové rovnice

$$\begin{aligned} g(y) &= x\,, \\ f(x, h(x), y) &= f(g(z), w, z)\,. \end{aligned}$$

Pravidlo 4 na 2. rovnici:

$$\begin{aligned} g(z) &= g(y)\,, \\ x &= g(z)\,, \\ h(g(z)) &= w\,, \\ y &= z\,. \end{aligned}$$

Příklad

Uvažujme termové rovnice

$$\begin{aligned} g(y) &= x\,, \\ f(x, h(x), y) &= f(g(z), w, z)\,. \end{aligned}$$

Pravidlo 3 na 1. rovnici:

$$\begin{aligned} z &= y\,, \\ x &= g(z)\,, \\ h(g(z)) &= w\,, \\ y &= z\,. \end{aligned}$$

Příklad

Uvažujme termové rovnice

$$\begin{aligned} g(y) &= x\,, \\ f(x, h(x), y) &= f(g(z), w, z)\,. \end{aligned}$$

Pravidlo 4 na 4. rovnici:

$$\begin{aligned} z &= z\,, \\ x &= g(z)\,, \\ h(g(z)) &= w\,, \\ y &= z\,. \end{aligned}$$

Příklad

Uvažujme termové rovnice

$$\begin{aligned} g(y) &= x\,, \\ f(x, h(x), y) &= f(g(z), w, z)\,. \end{aligned}$$

Pravidlo 2 na 1. rovnici:

$$\begin{aligned} x &= g(z)\,, \\ h(g(z)) &= w\,, \\ y &= z\,. \end{aligned}$$

Příklad

Uvažujme termové rovnice

$$\begin{aligned} g(y) &= x\,, \\ f(x, h(x), y) &= f(g(z), w, z)\,. \end{aligned}$$

Pravidlo 1 na 2. rovnici:

$$\begin{aligned} x &= g(z)\,, \\ w &= h(g(z))\,, \\ y &= z\,. \end{aligned}$$

Příklad

Uvažujme termové rovnice

$$
\begin{aligned}
g(y) &= x\,, \\
f(x, h(x), y) &= f(g(z), w, z)\,.
\end{aligned}
$$

Pravidlo 1 na 2. rovnici:

$$
\begin{aligned}
x &= g(z)\,, \\
w &= h(g(z))\,, \\
y &= z\,.
\end{aligned}
$$

Výsledná unifikace $\{x/g(z), w/h(g(z)), y/z\}$.

Obecné rezoluční pravidlo

Rezoluční pravidlo

Nechť $C_1 = \varphi \vee \alpha_1 \vee \cdots \vee \alpha_n$ a $C_2 = \psi \vee \neg\beta_1 \vee \cdots \vee \neg\beta_k$ jsou klausule neobsahující stejné proměnné, $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_k$ literály, které je možné unifikovat. Pak rezolventou klausulí C_1 a C_2 nazýváme klausuli

$$C = \varphi\sigma \vee \psi\sigma\,,$$

kde σ je neobecnější unifikace pro $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_k$.

Poznámka

Rezoluční pravidlo vyžaduje, aby dané klausule neměli společné proměnné (uvažme např. $\{P(a,x), \neg P(x,b)\}$). Takže před použitím většina implementací rezolučního pravidla přejmenuje proměnné u jedné z klausulí. Přejmenování nemění nic na splnitenosti nebo nesplnitelnosti množiny klausulí.

Rezoluční algortimus pro predikátovou logiku

Vstup: množina klausulí S
Výstup: "splnitelná" nebo "nesplnitelná" (algoritmus nemusí skončit!)

- Pokud S obsahuje prázdnou klausuli, vrať "nesplnitelná".
- Pokud neexistují klausule $C_1, C_2 \in S$, které mají rezolventu, vrať "splnitelná".

- $S_0 = S$.
- Předpokládejme, že S_i bylo již zkonstruováno.
- Pokud $F \in S_i$, pak vrať "nesplnitelná".
- Pokud existují klausule $C_1, C_2 \in S_i$, ke kterých je možné najít rezolventu $C \notin S_i$, pak $S_{i+1} = S_i \cup \{C\}$.
- Pokud neexistují, pak vrať "splnitelná".

Korektnost a úplnost

Věta

Množina klausulí S je nesplnitelná právě tehdy když existuje $n \in \mathbb{N}$ takové, že prázdná klausule F patří do množiny S_n z rezolučního algoritmu.

Poznámka

- Pokud je množina klausulí S nesplnitelná, pak rezoluční algoritmus skončí.
- Nicméně u některých splnitelných množin klausulí rezoluční algoritmus nemusí nikdy skončit.

Příklad

Uvažujme množinu klausulí 1–7:

1. $\neg P(x) \vee Q(x) \vee R(x, f(x))$
2. $\neg P(x) \vee Q(x) \vee S(f(x))$
3. $T(a)$
4. $P(a)$
5. $\neg R(a, y) \vee T(y)$
6. $\neg T(x) \vee \neg Q(x)$
7. $\neg T(x) \vee \neg S(x)$
8. $\neg Q(a)$; $(3{,}6,\{x/a\})$
9. $Q(a) \vee S(f(a))$; $(2{,}4,\{x/a\})$
10. $S(f(a))$; $(8{,}9)$
11. $Q(a) \vee R(a, f(a))$; $(1{,}4,\{x/a\})$
12. $R(a, f(a))$; $(8{,}11)$
13. $T(f(a))$; $(5{,}12,\{y/f(a)\})$
14. $\neg S(f(a))$; $(7{,}13,\{x/f(a)\})$
15. F; $(10{,}14)$

Příklad

Uvažujme množinu klausulí 1–4:

1. $\neg P(x,y) \vee P(y,x)$
2. $\neg P(x,y) \vee \neg P(y,z) \vee P(x,z)$
3. $P(x,f(x))$
4. $\neg P(x,x)$
5. $P(x',f(x'))$; (přejmenování 3)
6. $P(f(x),x)$; (1,5,$\{y/f(x), x'/x\}$)
7. $\neg P(f(x),z) \vee P(x,z)$; (2,5,$\{y/f(x), x'/x\}$)
8. $P(f(x'),x')$; (přejmenování 6)
9. $P(x,x)$; (7,8,$\{z/x, x'/x\}$)
10. $\neg P(x',x')$; (přejmenování 4)
11. F; (9,10,$\{x'/x\}$)

Všechny kroky, které přejmenovávají proměnné, je možné v tomto příkladě vynechat.