Úvod do TI - logika

Obecná rezoluční metoda v predikátové logice

(přednáška 8.)

Marie Duží

marie.duzi@vsb.cz

Typické úlohy

- Dokázat logickou pravdivost formule PL1:
  - $\models F$
  - tj. formule F je pravdivá ve ***všech interpretacích,*** tj. každá interpretace je jejím modelem.

- Dokázat platnost úsudku v PL1:
  - $P_1, \ldots, P_n \models Q$
  - tj. formule Q je pravdivá ve ***všech modelech*** množiny předpokladů $P_1, \ldots, P_n$. Tedy $\models (P_1 \wedge \ldots \wedge P_n) \supset Q$

Typické úlohy

- Jejich řešení rozborem (nekonečné) množiny modelů je obtížné, sémantické důkazy jsou pracné a nedají se snadno automatizovat.
- Proto hledáme jiné metody.
- Jednou z nich je metoda sémantických tabel, kterou jsme se již naučili, tj. převod na disjunktivní normální formu (nevýhoda – často příliš mnoho distributivních úprav).
- Nyní se naučíme velice efektivní metodu používanou také pro automatické dokazování a logické programování – zobecnění rezoluční metody výrokové logiky.
- Rezoluční metoda využívá **konjunktivní normální formu** formule.

Rezoluční metoda

- Je aplikovatelná na formuli ve spec. **konjunktivní normální formě (Skolemova *klauzulární forma*).**

- Je zobecněním rezoluční metody ve výrokové logice: důkaz sporem.

- Je základem pro automatizované deduktivní metody a logické programování.

- Je základem pro programovací jazyk **PROLOG.**

Rezoluční metoda

Dva problémy:

1. Převod do Skolemovy klauzulární formy:

$$\forall x_1 \ldots \forall x_n\ [C_1 \wedge \ldots \wedge C_m]$$

   C_i jsou klausule, tj. disjunkce literálů, např. $P(x) \vee \neg Q(f(x,y))$

2. Uplatňování pravidla rezoluce na různé literály – **unifikace literálů.** Např.:

$$P(x) \vee \neg Q(f(x),y)$$
$$\neg P(g(y)) \vee \neg Q(x,z)$$

   Literály $P(x)$, $\neg P(g(y))$ bychom mohli „škrtnout“, kdyby byly stejné .

Převod do klausulární formy (Skolem str. 78)

1. Utvoření existenčního uzávěru
   (zachovává *splnitelnost*)
2. Eliminace nadbytečných kvantifikátorů
3. Eliminace spojek $\supset$, $\equiv$
4. Přesun negace dovnitř
5. Přejmenování proměnných
6. Přesun kvantifikátorů doprava
7. Eliminace existenčních kvantifikátorů
   (Skolemizace – zachovává splnitelnost)
8. Přesun všeobecných kvantifikátorů doleva
9. Použití distributivních zákonů

Rezoluční metoda – příklad

|= $[\forall x\, \exists y\, P(x,y) \wedge \forall y\, \exists z\, Q(y,z)] \supset \forall x\, \exists y\, \exists z\, [P(x,y) \wedge Q(y,z)]$

1. **Formuli znegujeme** a přejmenujeme proměnné:

$[\forall x\, \exists y'\, P(x,y') \wedge \forall y\, \exists z\, Q(y,z)] \wedge \exists u\, \forall v\, \forall w\, [\neg P(u,v) \vee \neg Q(v,w)]$

2. Odstraníme existenční kvantifikátory. **POZOR !**

$[\forall x\, P(x, f(x)) \wedge \forall y\, Q(y, g(y))] \wedge \forall v\, \forall w\, [\neg P(a,v) \vee \neg Q(v,w)]$

3. Přesuneme kvantifikátory doleva:

$\forall x\, \forall y\, \forall v\, \forall w\, [P(x, f(x)) \wedge Q(y, g(y)) \wedge [\neg P(a,v) \vee \neg Q(v,w)]]$

4. Formule je evidentně nesplnitelná, jak to dokážeme?

5. Vypíšeme klausule pod sebe a budeme provádět **unifikaci literálů, tj. substituci termů za proměnné** *tak, abychom mohli uplatnit rezoluční pravidlo*:

Rezoluční metoda – příklad

1. P(*x*, *f*(*x*))
2. Q(*y*, *g*(*y*))
3. ¬P(*a*,*v*) ∨ ¬Q(*v*,*w*)

- Nyní se budeme pokoušet o rezoluci. Abychom mohli uplatnit rezoluci na klausule 1. a 3., musíme substituovat term *a* za **všechny výskyty** proměnné *x*.

4. ¬Q(*f*(*a*),*w*) rezoluce 1., 3., substituce *x / a*, ***v / f(a)***
5. ■ rezoluce 2., 4., substituce *y / f(a)*, ***w / g(f(a))***

QED – negovaná formule je kontradikce, původní je tedy logicky pravdivá

Pozn.: Je nutno substituovat za ***všechny výskyty*** proměnné!

Skolemova klauzulární forma

Literál: atomická formule nebo negace atomické formule, např.:

$$P(x, g(y)), \neg Q(z)$$

Klausule: disjunkce literálů, např.:

$$P(x, g(y)) \vee \neg Q(z)$$

Skolemova klauzulární forma: $\forall x_1 \ldots \forall x_n\ [C_1 \wedge \ldots \wedge C_m]$, *uzavřená formule*, kde C_i jsou klausule, tj. disjunkce literálů, např.:

$$P(x) \vee \neg Q(f(x,y))$$

Skolemizace (odstranění existenčních kvantifikátorů):

$$\exists \boldsymbol{x}\ \forall y_1 \ldots \forall y_n\ A(x, y_1, \ldots, y_n) \rightarrow \forall y_1 \ldots \forall y_n\ A(\boldsymbol{c}, y_1, \ldots, y_n)$$

kde ***c*** je **nová, dosud v jazyce nepoužitá konstanta.**

$$\forall y_1 \ldots \forall y_n\ \exists \boldsymbol{x}\ A(x, y_1, \ldots, y_n) \rightarrow \forall y_1 \ldots \forall y_n\ A(\boldsymbol{f(y_1, \ldots, y_n)}, y_1, \ldots, y_n)$$

kde ***f*** je **nový**, dosud v jazyce **nepoužitý funkční symbol.**

Skolemizace zachovává splnitelnost

$\forall y_1 \ldots \forall y_n \, \mathbf{\exists x} \, A(x, y_1, \ldots, y_n) \quad \rightarrow \quad \forall y_1 \ldots \forall y_n \, A(\mathbf{f(y_1, \ldots, y_n)}, y_1, \ldots, y_n)$

B B^S

- **Důkaz**: Nechť interpreatce I je model formule B^S na pravé straně. Pak pro libovolnou *n*-tici $i_1, i_2, \ldots, i_n$ prvků universa platí, že (*n*+1)-tice prvků universa $\langle i_1, i_2, \ldots, i_n, f^U(i_1, i_2, \ldots, i_n) \rangle \in A^U$ (leží v oboru pravdivosti A), kde f^U je funkce přiřazená interpretací I symbolu f a A^U je relace – obor pravdivosti formule A v interpretaci I. Pak je ovšem interpretace I rovněž modelem formule $B = \forall y_1 \forall y_2 \ldots \forall y_n \, \exists x \, A(x, y_1, y_2, \ldots, y_n)$.
- Tedy každý model formule B^S je i modelem formule B, ale nikoliv naopak, tj. $\mathbf{B^S \models B}$. Množina modelů M^{BS} formule B^S je podmnožinou množiny M^B modelů formule B: $\mathbf{M^{BS} \subseteq M^B}$.
- Navíc, má-li B model I, pak má také B^S model I' (*ne nutně stejný*).
- Naopak, nemá-li B *žádný model,* tedy je nesplnitelná ($M^B = \Phi$), je také B^S nesplnitelná ($M^{BS} = \Phi$).
- Což pro důkaz sporem postačuje.

Thoralf Albert Skolem

Born: 23 May 1887 in Sandsvaer, Buskerud, Norway

Died: 23 March 1963 in Oslo, Norway

Skolem was remarkably productive publishing around 180 papers on topics such as Diophantine equations, mathematical logic, group theory, lattice theory and set theory.

Převod do klausulární formy (str. 78)

1. Utvoření existenčního uzávěru (zachovává *splnitelnost*)
2. Eliminace nadbytečných kvantifikátorů
3. Eliminace spojek $\supset$, $\equiv$ (dle zákonů VL)
4. Přesun negace dovnitř dle de Morganových zákonů
5. Přejmenování proměnných
6. Přesun kvantifikátorů doprava:

   $Qx\ (A\ @\ B(x)) \rightarrow A\ @\ Qx\ B(x)$,

   $Qx\ (A(x)\ @\ B) \rightarrow Qx\ A(x)\ @\ B$,

   kde @ je spojka konjunkce nebo disjunkce,
   Q kvantifikátor (všeobecný nebo existenční)
7. Eliminace existenčních kvantifikátorů (Skolemizace podformulí $Qx\ B(x)$, $Qx\ A(x)$ z kroku 6)
8. Přesun všeobecných kvantifikátorů doleva
9. Použití distributivních zákonů

Převod do klauzulární formy: $A \rightarrow A^S$

- Výsledná formule A^s není ekvivalentní původní formuli A (ani z ní nevyplývá), ale platí, že

  je-li A splnitelná, je splnitelná i A^s,
  a naopak, je-li A **ne**splnitelná, je **ne**splnitelná i A^s

  protože $A^s \models A$.

- Kroky převodu, které nejsou ekvivalentní, pouze zachovávají splnitelnost jsou:
  - Utvoření existenčního uzávěru
  - Skolemizace (odstranění existenčních kvantifikátorů)

- Proto používáme rezoluční metodu v PL1 pro důkaz **sporem**.

- Pouze tehdy, když formule neobsahují existenční kvantifikátory, můžeme ji použít pro přímý důkaz toho, co vyplývá z daných předpokladů.

Převod do klauzulární formy: A → A^S

- Provádíme vždy dle Skolemova algoritmu (9 kroků). Tedy **ne tak,** že bychom formuli převedli nejprve do konjunktivní normální formy, a pak skolemizovali, jak se někdy uvádí.
- Příklad: důležitost kroku 6 (kvantifikátory doprava).

Ukážeme **chybný postup**:

$\models\ \forall x\, A(x) \supset \forall x\, A(x)$, *formuli znegujeme*:

$\forall x\, A(x) \wedge \exists x\, \neg A(x)$, *přejmenujeme proměnné*:

$\forall x\, A(x) \wedge \exists y\, \neg A(y)$, *přesuneme kvantifikátory doleva*:

$\forall x\, [A(x) \wedge \exists y\, \neg A(y)]$,

$\forall x\, \exists y\, [A(x) \wedge \neg A(y)]$, *skolemizujeme*:

$\forall x\, [A(x) \wedge \neg A(f(x))]$.

Ovšem nesplnitelnost této formule nedokážeme, termy x a $f(x)$ nejsou unifikovatelné.

- Přitom rezoluční metoda je **úplná důkazová metoda.** Každá logicky pravdivá formule je dokazatelná: $\models$ **A** $\Rightarrow$ $\vdash$ **A**

Převod do klauzulární formy: A → A^S

Příklad:
$\forall x \{P(x) \supset \exists z \{\neg\forall y [Q(x,y) \supset P(f(x_1))] \wedge \forall y [Q(x,y) \supset P(x)]\}\}$

1.,2. Existenční uzávěr a eliminace $\exists z$:
$\exists x_1 \forall x \{P(x) \supset \{\neg\forall y [Q(x,y) \supset P(f(x_1))] \wedge \forall y [Q(x,y) \supset P(x)]\}\}$

3.,4. Přejmenování y, eliminace $\supset$:
$\exists x_1 \forall x \{\neg P(x) \vee \{\neg\forall y [\neg Q(x,y) \vee P(f(x_1))] \wedge \forall z [\neg Q(x,z) \vee P(x)]\}\}$

5.,6. Negace dovnitř a kvantifikátory doprava:
$\exists x_1 \forall x \{\neg P(x) \vee \{[\exists y\, Q(x,y) \wedge \neg P(f(x_1))] \wedge [\forall z\, \neg Q(x,z) \vee P(x)]\}\}$

7. Eliminace existenčních kvantifikátorů:
$\forall x \{\neg P(x) \vee \{[Q(x,g(x)) \wedge \neg P(f(a))] \wedge [\forall z\, \neg Q(x,z) \vee P(x)]\}\}$

8. Kvantifikátor doleva:
$\forall x \forall z \{\neg P(x) \vee \{[Q(x,g(x)) \wedge \neg P(f(a))] \wedge [\neg Q(x,z) \vee P(x)]\}\}$

9. Distributivní zákon:
$\forall x \forall z \{[\neg P(x) \vee Q(x,g(x))] \wedge [\neg P(x) \vee \neg P(f(a))] \wedge [\neg P(x) \vee \neg Q(x,z) \vee P(x)]\}$

10. zjednodušení:
$\forall x \{[\neg P(x) \vee Q(x,g(x))] \wedge [\neg P(x) \vee \neg P(f(a))]\}$

Postup důkazů rezoluční metodou

- Důkaz, že formule A je logicky pravdivá:
  1. Formuli znegujeme.
  2. Formuli ¬A převedeme do klausulární Skolemovy formy $(\neg A)^s$.
  3. Postupným uplatňováním rezolučního pravidla se snažíme dokázat nesplnitelnost formule $(\neg A)^s$ a tedy také formule ¬A.
- Důkaz platnosti úsudku $P_1,\ldots,P_n \mid\!-\ Z$
  1. Závěr znegujeme
  2. Formule předpokladů a negovaného závěru převedeme do klausulární formy
  3. Postupným uplatňováním rezolučního pravidla se snažíme dokázat nesplnitelnost množiny $\{P_1,\ldots,P_n , \neg Z\}$

Unifikace literálů

- Problémem je v obou případech bod 3.
- *Příklad*: $\forall x \forall y \forall z \forall v[P(x, f(x)) \wedge Q(y, h(y)) \wedge (\neg P(a, z) \vee \neg Q(z, v))]$
- Jak dokázat nesplnitelnost?

1. $P(x, f(x))$
2. $Q(y, h(y))$
3. $\neg P(a, z) \vee \neg Q(z, v)$

Chceme-li rezolvovat klauzule např. 1. a 3., brání nám to, že termy – argumenty nejsou stejné. Ale – všechny proměnné jsou kvantifikovány všeobecným kvantifikátorem. Můžeme použít zákon konkretizace („co platí pro všechny, platí i pro některé“), dosazovat za proměnné termy tak, abychom nalezli *svědka nesplnitelnosti*.

Provedeme proto substituci tak, abychom jednotlivé literály ***unifikovali***:

Unifikace literálů

Substituce: x / a, z / f(a)
Po provedení této substituce dostaneme klausule:
1´. P(a, f(a))
2. Q(y, h(y))
3´. ¬P(a, f(a)) ∨ ¬Q(f(a), v)

kde na 1‘ a 3‘ již lze uplatnit pravidlo rezoluce:

4. ¬Q(f(a), v)

Abychom nyní mohli rezolvovat klausule 2. a 4., zvolíme opět substituci:
Substituce: y / f(a), v / h(f(a)). Dostaneme:

2‘. Q(f(a), h(f(a)))
4’. ¬Q(f(a), h(f(a)))

a jejich rezolucí již obdržíme prázdnou klausuli. Tedy formule A je nesplnitelná.

Unifikace literálů

Jednotlivé substituce jsme však hledali intuitivně. Musíme najít nějaký *algoritmus*, jak provádět příslušné *unifikace.*

a) Herbrandova procedura
b) Robinsonův unifikační algoritmus

Ad a) Formule je nesplnitelná, když je nepravdivá v každé interpretaci *nad všemi možnými* universy. Nešlo by nalézt jedno universum takové, že je-li nad ním formule nesplnitelná, je pak již nesplnitelná nad každým? Ano – **Herbrandovo universum**.

Jacques Herbrand

Born: 12 Feb 1908 in Paris, France
Died: 27 July 1931 in La Bérarde, Isère, France

École Normale Supérieure at the age of 17 (!). His doctoral thesis was approved in April 1929. On a holiday in the Alps he died in a mountaineering accident at the age of 23.

John Alan Robinson

In his 1965 article " A Machine-Oriented Logic Based on the Resolution Principle " John Alan Robinson laid an important foundation for a whole branch of automated deduction systems. The original Prolog is essentially a refined automated theorem prover based on Robinson's resolution .

Herbrandova procedura

Herbrandovo universum: všechny možné termy vytvořené z konstant a funkčních symbolů ve formuli, nebo libovolné konstanty, př.:

- Pro formuli $\boldsymbol{A = \forall x\, [P(a) \vee Q(b) \supset P(f(x))]}$ je $H_A = \{a, b, f(a), f(b), f(f(a)), f(f(b)), \ldots\}$
- Pro formuli $\boldsymbol{B = \forall x\, \forall y\, P(\ (f(x), y, g(x,y)\ )}$ je $H_B = \{a, f(a), g(a,a), f(f(a)), g(a,f(a)), g(f(a),a), \ldots\}$
- Základní instance klausule: všechny proměnné nahradíme prvky Herbrandova universa.

Herbrandova procedura

Herbrandova věta: Formule A v klausulární formě je nesplnitelná, právě když existuje konečná konjunkce základních instancí jejích klausulí, která je nesplnitelná.

Příklad:

1. $P(x, f(x))$
2. $Q(y, h(y))$
3. $\neg P(a, z) \vee \neg Q(z, v)$

- $H_A = \{a, f(a), h(a), f(f(a)), f(h(a)), h(f(a)), h(h(a)), \ldots\}$.
  Substituce **1**: $\{x/a, y/a, z/a, v/a\}$
- $P(a, f(a)) \wedge Q(a, h(a)) \wedge [\neg P(a, a) \vee \neg Q(a, a)]$
  Substituce **2**: $\{x/a, y/a, z/a, v/f(a)\}$
- $P(a, f(a)) \wedge Q(a, h(a)) \wedge [\neg P(a, a) \vee \neg Q(a, f(a))]$ …, atd., až
  Substituce ***n***: $\{x/a, y/f(a), z/f(a), v/h(f(a))\}$
- $P(a, f(a)) \wedge Q(\ f(a), h(f(a))\ ) \wedge [\neg P(a, f(a)) \vee \neg Q(\ f(a), h(f(a))\ )]$
  Nesplnitelná

Herbrandova procedura

Herbrandova procedura *parciálně rozhoduje*, zda je předložená formule nesplnitelná (tj. pokud nesplnitelná je, vydá po konečném počtu kroků odpověď Ano, jinak nemusí odpovědět).

Problém: *Prostorová a časová složitost* algoritmu – počet základních instancí, které musíme vygenerovat, než narazíme na svědka nesplnitelnosti, může být příliš velký.

Robinsonův algoritmus (1965)

- Nechť A je formule obsahující individuové proměnné x_i, i=1,2,...,n, a to buď přímo (jako bezprostřední argumenty) nebo zprostředkovaně (jako argumenty funkcí). Označme $\sigma = \{x_1/t_1, x_2/t_2,...,x_n/t_n\}$ ***simultánní substituci*** termů t_i za *(všechny výskyty)* proměnné x_i pro i=1,2,...,n. Potom zápisem **Aσ** označíme formuli, která vznikne z formule A *provedením substituce* $\boldsymbol{\sigma}$.

- ***Unifikace*** (unifikační substituce, unifikátor) formulí A, B je substituce $\boldsymbol{\sigma}$ taková, že A$\boldsymbol{\sigma}$ = B$\boldsymbol{\sigma}$.

- ***Nejobecnější unifikace*** formulí A, B je unifikace $\boldsymbol{\sigma}$ taková, že pro každou jinou unifikaci $\boldsymbol{\rho}$ formulí A, B platí $\boldsymbol{\rho} = \boldsymbol{\sigma\tau}$, kde $\boldsymbol{\tau} \neq \boldsymbol{\varepsilon}$, tj. každá unifikace vznikne z nejobecnější unifikace provedením další dodatečné substituce.

Robinsonův algoritmus (1965)

Nalezení nejobecnější unifikace

Předpokládejme:

$A = P(t_1, t_2, \ldots, t_n)$, $B = P(s_1, s_2, \ldots, s_n)$, kde vždy (pro jednoduchost) alespoň jeden z termů t_i, s_i je proměnná.

1. Pro i = 1, 2, ..., *n* prováděj:

a) Je-li $t_i = s_i$, pak polož $\sigma_i = \varepsilon$ (prázdná substituce).

b) Není-li $t_i = s_i$, pak zjisti, zda jeden z termů t_i, s_i představuje nějakou individuovou proměnnou x a druhý nějaký term r, který proměnnou *x neobsahuje* (tedy hledáme **první rozdíl**, zleva doprava).

c) Jestliže ano, pak polož $\sigma_i = \{x/r\}$.

d) Jestliže ne, pak ukonči práci s tím, že formule A, B nejsou unifikovatelné.

2. Po řádném dokončení cyklu urči $\sigma = \sigma_1\sigma_2\ldots\sigma_n$ (složená substituce). Substituce σ je nejobecnější unifikací formulí A, B.

Robinsonův algoritmus - Příklad

A = $P(x, f(x), u)$, B = $P(y, z, g(x,y))$

- $\sigma_1 = \{x/y\}$,
  $A\sigma_1 = P(y, f(y), u)$, $B\sigma_1 = P(y, z, g(y,y))$

- $\sigma_2 = \{z/f(y)\}$,
  $A\sigma_1\sigma_2 = P(y, f(y), u)$, $B\sigma_1\sigma_2 = P(y, f(y), g(y,y))$

- $\sigma_3 = \{u/g(y,y)\}$,
  $A\sigma_1\sigma_2\sigma_3 = P(y, f(y), g(y,y))$,
  $B\sigma_1\sigma_2\sigma_3 = P(y, f(y), g(y,y))$.

- Složená substituce $\sigma=\sigma_1\sigma_2\sigma_3$ je nejobecnější unifikací formulí A, B: $\{x / y, z / f(y), u / g(y,y)\}$

Zobecněné rezoluční pravidlo

$$\mathbf{A} \vee \mathbf{L_1}, \mathbf{B} \vee \neg \mathbf{L_2} \mid\!-\ \mathbf{A\sigma} \vee \mathbf{B\sigma},$$

kde $\boldsymbol{\sigma}$ je nejobecnější unifikátor L_1, L_2: $L_1\boldsymbol{\sigma} = L_2\boldsymbol{\sigma}$

Příklad: Dokažte logickou pravdivost formule:

$$\forall x \forall y \left[\{P(x,y) \supset Q(x, f(g(x)))\} \wedge \{R(x) \vee \exists x \neg Q(x, f(g(x)))\} \wedge \exists x \neg R(x) \right] \supset \exists x \neg P(x, g(x))$$

(dále příklady od str. 85)

Příklad

$\forall x \forall y\, [\{P(x,y) \supset Q(x, f(g(x)))\} \wedge$
$\quad \{R(x) \vee \exists x\, \neg Q(x, f(g(x)))\} \wedge \exists x\, \neg R(x)] \supset \exists x\, \neg P(x, g(x))$

1. Formuli znegujeme (negace implikace!):

$\forall x \forall y\, [\{P(x,y) \supset Q(x, f(g(x)))\} \wedge$
$\quad \{R(x) \vee \exists x\, \neg Q(x, f(g(x)))\} \wedge \exists x\, \neg R(x)] \wedge \forall x\, P(x, g(x))$

2. Odstraníme existenční kvantifikátory a přejmenujeme:

$\forall x \forall y\, [\{P(x,y) \supset Q(x, f(g(x)))\} \wedge$
$\quad \{R(x) \vee \neg Q(a, f(g(a)))\} \wedge \neg R(b)] \wedge \forall z\, P(z, g(z))$

3. Sepíšeme klauzule (po odstranění implikace):

Příklad

$\forall x \forall y\ [\{P(x,y) \supset Q(x, f(g(x)))\} \wedge$
$\{R(x) \vee \neg Q(a, f(g(a)))\} \wedge \neg R(b)] \wedge \forall z\ P(z, g(z))$

1. $\neg P(x,y) \vee Q(x, f(g(x)))$
2. $R(x) \vee \neg Q(a, f(g(a)))$
3. $\neg R(b)$
4. $P(z, g(z))$
5. $Q(x, f(g(x)))$ *rezoluce* 1., 4.; substituce *z / x, y / g(x)*
6. $\neg Q(a, f(g(a)))$ *rezoluce* 2., 3.; substituce *x / b*
7. *rezoluce 5., 6.; substituce* x / a

$\blacksquare$

Pozn.: Rodičovské klauzule pro vytváření rezolvent volíme tak, aby zůstalo co nejvíce proměnných volných.