

Matematická logika

Obecná rezoluční metoda v predikátové logice
(přednáška 8.,9.)

Marie Duží

marie.duzi@vsb.cz



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

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:
 - $P_1, \dots, P_n \models Q$
 - tj. formule Q je pravdivá ve **všech modelech** množiny předpokladů $P_1, \dots, P_n$. Tedy $\models (P_1 \wedge \dots \wedge P_n) \supset Q$
- Co vyplývá z daných předpokladů?
 - $P_1, \dots, P_n \models ?$

Typické úlohy

- Jejich řešení rozbořem (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:

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

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.:

$$\begin{array}{l} P(x) \vee \neg Q(f(x),y) \\ \neg P(g(y)) \vee \neg Q(x,z) \end{array}$$

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

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

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. $\neg P(a, v) \vee \neg Q(v, w)$

- 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. $\neg Q(f(a), w)$ 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: $\forall x_1 \dots \forall x_n [C_1 \wedge \dots \wedge C_m]$, uzavřená formule, kde C_i jsou klausule, tj. disjunkce literálů, např.:

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

Skolemizace (odstranění existenčních kvantifikátorů):

$$\exists x \forall y_1 \dots \forall y_n A(x, y_1, \dots, y_n) \rightarrow \forall y_1 \dots \forall y_n A(\mathbf{c}, y_1, \dots, y_n)$$

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

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

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

Skolemizace zachovává splnitelnost

$$\begin{array}{ccc} \forall y_1 \dots \forall y_n \exists x A(x, y_1, \dots, y_n) & \rightarrow & \forall y_1 \dots \forall y_n A(\mathbf{f(y_1, \dots, y_n)}, y_1, \dots, y_n) \\ B & & B^s \end{array}$$

- **Důkaz:** Nechť interpretace I je model formule B^s na pravé straně. Pak pro libovolnou n -tici $i_1, i_2, \dots, i_n$ prvků universa platí, že $(n+1)$ -tice prvků universa $\langle i_1, i_2, \dots, i_n, f^U(i_1, i_2, \dots, i_n) \rangle \in A^U$ (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 $B = \forall y_1 \forall y_2 \dots \forall y_n \exists x A(x, y_1, y_2, \dots, y_n)$.
- Tedy každý model formule B^s je i modelem formule B , ale nikoliv naopak, tj. $B^s \models B$. Množina modelů M^{B^s} formule B^s je podmnožinou množiny M^B modelů formule B : $M^{B^s} \subseteq M^B$.
- Navíc, má-li B model I , pak má také B^s model I' (*ne nutně stejný*).
- Naopak, nemá-li B žádný model, tedy je nespílitelná ($M^B = \Phi$), je také B^s nespílitelná ($M^{B^s} = \Phi$).
- 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)

- Eliminace existenčních kvantifikátorů
(Skolemizace podformulí $Qx B(x)$, $Qx A(x)$ z kroku 6)
- Přesun všeobecných kvantifikátorů doleva
- 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 **nesplnitelná**, je **nesplnitelná** 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: $A \rightarrow$

- **AS** 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: $A \rightarrow$

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 $\neg A$ 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 $\neg A$.
- Důkaz platnosti úsudku $P_1, \dots, P_n \vdash Z$
 1. Závěr znegujeme
 2. Formule předpokladů a negovaného závěru převedeme do klausulární formy
 3. Postupným uplatňováním rezolučního pravidla se snažíme dokázat nesplnitelnost množiny $\{P_1, \dots, P_n, \neg Z\}$

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 našli *svědka nesplnitelnosti*.

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

Unifikace literálů

Substitute: $x / a, z / f(a)$

Po provedení této substitute dostaneme klausule:

1'. $P(a, f(a))$

2. $Q(y, h(y))$

3'. $\neg P(a, f(a)) \vee \neg Q(f(a), v)$

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

4. $\neg Q(f(a), v)$

Abychom nyní mohli rezolvovat klausule 2. a 4., zvolíme opět substituci:

Substitute: $y / f(a), v / h(f(a))$. Dostaneme:

2'. $Q(f(a), h(f(a)))$

4'. $\neg Q(f(a), h(f(a)))$

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

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

Herbrandova procedura

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

Příklad:

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

- $H^A = \{a, f(a), h(a), f(f(a)), f(h(a)), h(f(a)), h(h(a)), \dots\}$.
Substitute **1**: $\{x/a, y/a, z/a, v/a\}$
- $P(a, f(a)) \wedge Q(a, h(a)) \wedge [\neg P(a, a) \vee \neg Q(a, a)]$
Substitute **2**: $\{x/a, y/a, z/a, v/f(a)\}$
- $P(a, f(a)) \wedge Q(a, h(a)) \wedge [\neg P(a, a) \vee \neg Q(a, f(a))] \dots$, atd., až
Substitute **n**: $\{x/a, y/f(a), z/f(a), v/h(f(a))\}$
- $P(a, f(a)) \wedge Q(f(a), h(f(a))) \wedge [\neg P(a, f(a)) \vee \neg Q(f(a), h(f(a)))]$
Nespíitelná

Herbrandova procedura

Herbrandova procedura *parciálně rozhoduje*, zda je předložená formule nespílnitelná (tj. pokud nespílnitelná 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 nespílnitelnosti, může být příliš velký.

Robinsonův algoritmus

(1965)

- Necht A je formule obsahující individuové proměnné x_i , $i=1,2,\dots,n$, a to buď přímo (jako bezprostřední argumenty) nebo zprostředkovaně (jako argumenty funkcí). Označme $\sigma = \{x_1/t_1, x_2/t_2, \dots, x_n/t_n\}$ **simultánní substituci** termů t_i za (*všechny výskyty*) proměnné x_i pro $i=1,2,\dots,n$. Potom zápisem $A\sigma$ označíme formuli, která vznikne z formule A *provedením substituce* σ .
- **Unifikace** (unifikační substituce, unifikátor) formulí A, B je substituce σ taková, že $A\sigma = B\sigma$.
- **Nejobecnější unifikace** formulí A, B je unifikace σ taková, že pro každou jinou unifikaci ρ formulí A, B platí $\rho = \sigma\tau$, kde $\tau \neq \varepsilon$, tj. každá unifikace vznikne z nejobecnější unifikace provedením další dodatečné substituce.

Robinsonův algoritmus

(1965)

Nalezení nejobecnější unifikace

Předpokládejme:

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

1. Pro $i = 1, 2, \dots, n$ prováděj:

- Je-li $t_i = s_i$, pak polož $\sigma_i = \varepsilon$ (prázdná substituce).
- 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).
- Jestliže ano, pak polož $\sigma_i = \{x/r\}$.
- Jestliže ne, pak ukonči práci s tím, že formule A , B nejsou unifikovatelné.

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

Robinsonův algoritmus - Příklad

$$A = P(\textcolor{blue}{x}, f(x), u), B = P(\textcolor{blue}{y}, z, g(x,y))$$

- $\sigma_1 = \{x/y\},$

$$A\sigma_1 = P(y, \textcolor{blue}{f(y)}, u), B\sigma_1 = P(y, z, g(\textcolor{blue}{y}, y))$$

- $\sigma_2 = \{z/f(y)\},$

$$A\sigma_1\sigma_2 = P(y, f(y), \textcolor{blue}{u}), B\sigma_1\sigma_2 = P(y, f(y), g(y, \textcolor{blue}{y}))$$

- $\sigma_3 = \{u/g(y,y)\},$

$$A\sigma_1\sigma_2\sigma_3 = P(y, f(y), g(y,y)),$$

$$B\sigma_1\sigma_2\sigma_3 = P(y, f(y), g(y,y)).$$

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

Zobecněné rezoluční pravidlo

$$A \vee L_1, B \vee \neg L_2 \vdash A\sigma \vee B\sigma,$$

kde σ je nejobecnější unifikátor L_1, L_2 : $L_1\sigma = L_2\sigma$

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

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

1. Formuli znegujeme (negace implikace!):

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

2. Odstraníme existenční kvantifikátory a přejmenujeme:

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

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



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

Dokazování platnosti úsudku

Kdo zná Pavla a Marii, ten Marii lituje. $\forall x ([Z(x, P) \wedge Z(x, M)] \supset L(x, M))$
Někteří nelitují Marii, ačkoli ji znají. $\exists x [\neg L(x, M) \wedge Z(x, M)]$

Někdo zná Marii, ale ne Pavla. $\exists x [Z(x, M) \wedge \neg Z(x, P)]$

- $\forall x [\neg Z(x, P) \vee \neg Z(x, M) \vee L(x, M)]$ Odstranění implikace (1. předpoklad).
- $\neg L(a, M) \wedge Z(a, M)$ Skolemizace (2. předpoklad).
- $\forall y [\neg Z(y, M) \vee Z(y, P)]$ Negovaný závěr (přejmenování x).

Klausule:

1. $\neg Z(x, P) \vee \neg Z(x, M) \vee L(x, M)$
2. $\neg L(a, M)$ **(2. předpoklad jsou**
3. $Z(a, M)$ **dvě klausule - konjunkce!)**
4. $\neg Z(y, M) \vee Z(y, P)$
5. $\neg Z(a, P) \vee \neg Z(a, M)$ rezoluce 1., 2., substituce x/a
6. $\neg Z(a, P)$ rezoluce 3., 5.
7. $\neg Z(a, M)$ rezoluce 4., 6., substituce y/a
8. $\blacksquare$ rezoluce 3., 7.

- Obdrželi jsme prázdnou klausuli, tj. negovaný závěr je ve sporu s předpoklady, tedy původní závěr z předpokladů vyplývá.
- **Úsudek je platný**

Porovnání důkazu předchozího úsudku se sémantickým důkazem

- Znázorníme, jaké budou obory pravdivosti predikátů Z a L , tj. relace Z^U a L^U , aby byly pravdivé premisy:

- $Z^U = \{ \dots, \langle i_1, m \rangle, \langle i_1, k \rangle, \langle i_2, m \rangle, \langle i_2, k \rangle, \dots, \langle \alpha, m \rangle, \dots \}$

1. premisa

2. premisa

- $L^U = \{ \dots, \langle i_1, m \rangle, \dots, \langle i_2, m \rangle, \dots, \langle \alpha, m \rangle, \dots \}$

atd., sporem.

Dokazování platnosti úsudku

sporem:

- Využíváme toho, že pro **uzavřené** formule platí ekvivalence:

$$P_1, \dots, P_n \models Z \text{ iff } \models (P_1 \wedge \dots \wedge P_n) \supset Z$$

- A dále: $\models (P_1 \wedge \dots \wedge P_n) \supset Z$ iff **negovaná** formule je **kontradikce**: $(P_1 \wedge \dots \wedge P_n \wedge \neg Z)$

- Tedy negovaný závěr Z je ve sporu s konjunkcí předpokladů. Což je přesně v souladu s definicí platnosti úsudku:

- $P_1, \dots, P_n \models Z$ iff Z je pravdivá **ve všech modelech** množiny předpokladů $P_1, \dots, P_n$ iff

- $\neg Z$ není pravdivá v **žádném modelu** množiny předpokladů.

Dokazování logické pravdivosti

- Dokažte, že věta „Jistý filosof odporuje všem filosofům, tedy odporuje sám sobě“ je analyticky nutně pravdivá.
- Větu analyzujeme jako: (“zamýšlená” interpretace je nad množinou individuí, $P \rightarrow$ podmnožina filosofů, $Q \rightarrow$ relace, ve které budou ty dvojice, kde první odporuje druhému)
- $\exists x \{ [P(x) \wedge \forall y (P(y) \supset Q(x,y))] \supset Q(x,x) \}$ dokážeme, že je logicky pravdivá:
- Formuli znegujeme a převedeme na klausulární tvar:
- $\forall x \forall y \{ P(x) \wedge [\neg P(y) \vee Q(x,y)] \wedge \neg Q(x,x) \}$.
- K jednotlivým klausulím:
 1. $P(x)$
 2. $\neg P(y) \vee Q(x,y)$
 3. $\neg Q(x,x)$

je nejobecnějším unifikátorem substituce $\{y/x\}$:

 4. $\blacksquare Q(x,x)$ rezoluce 1. a 2.
 5. rezoluce 3. a 4.

Dokazování logické pravdivosti

- Dokažte, že věta „*Existuje někdo takový, že je-li génius, pak jsou všichni géniové*“ je analyticky nutně pravdivá.
- Formule: $\exists x [G(x) \supset \forall x G(x)]$ (pozor na závorkování!)
- Dokážeme, že negovaná formule je kontradikce:
 - $\forall x [G(x) \wedge \exists x \neg G(x)]$, tedy po přejmenování proměnných
 - $\forall x [G(x) \wedge \exists y \neg G(y)]$, **krok 6**: $[\forall x G(x) \wedge \exists y \neg G(y)]$ a po Skolemizaci:
 - $\forall x [G(x) \wedge \neg G(a)]$.

1. $G(x)$
2. $\neg G(a)$
3. ■ rezoluce 1. a 2., substituce x / a

Obdrželi jsme prázdnou klauzuli, negovaná formule je kontradikce, tedy původní formule je logicky pravdivá.

1. Všichni členové vedení jsou majiteli obligací nebo akcionáři.
 2. Žádný člen vedení není zároveň majitel obligací i akcionář.
 3. Všichni majitelé obligací jsou členy vedení.
-

4. Žádný majitel obligací není akcionář.

- $\forall x [V(x) \supset (O(x) \vee A(x))]$
- $\forall x [V(x) \supset \neg(O(x) \wedge A(x))]$
- $\forall x [O(x) \supset V(x)]$
- -----
- $\forall x [O(x) \supset \neg A(x)]$

- Klausule:
1. $\neg V(x) \vee O(x) \vee A(x)$ 1. předpoklad
 2. $\neg V(y) \vee \neg O(y) \vee \neg A(y)$ 2. předpoklad
 3. $\neg O(z) \vee V(z)$ 3. předpoklad
 4. $O(k)$ negovaný závěr
 5. $A(k)$ (po Skolemizaci)
 6. $\neg O(y) \vee \neg A(y)$ rezoluce 2., 3., substituce z/y
 7. $\neg A(k)$ rezoluce 4., 6., substituce y/k
 8. rezoluce 5., 7.

Pozn.: Všimněme si, že jsme první klausuli při důkazu nepoužili. Tedy závěr vyplývá již z druhého a třetího předpokladu (první je pro odvození důsledku nadbytečný).

Každý, kdo má rád Jiřího, bude spolupracovat s Milanem.
Milan nekamarádí s nikým, kdo kamarádí s Láďou.
Petr bude spolupracovat pouze s kamarády Karla.

Jestliže Karel kamarádí s Láďou, pak Petr nemá rád Jiřího.

- $\forall x [R(x, J) \supset S(x, M)]$
- $\forall x [K(x, L) \supset \neg K(M, x)]$
- $\forall x [S(P, x) \supset K(x, Kr)]$
- -----
- $K(Kr, L) \supset \neg R(P, J)$

Klausule:

1. $\neg R(x, J) \vee S(x, M)$

2. $\neg K(y, L) \vee \neg K(M, y)$

3. $\neg S(P, z) \vee K(z, Kr)$

4. $K(Kr, L)$

5. $R(P, J)$

6. $\neg K(M, Kr)$

7. $\neg S(P, M)$

8. $\neg R(P, J)$

9. ■

1. předpoklad

2. předpoklad

3. předpoklad

negovaný závěr

negovaný závěr

rezoluce 4., 2., substituce y/Kr

rezoluce 3., 6., substituce z/M

rezoluce 1., 7., substituce x/P

rezoluce 5., 8.

Co vyplývá z daných

Varianta předchozího příkladu. Premisy neobsahují žádné existenciální tvrzení.
předpokladů?

P1: Každý, kdo má rád Jiřího, bude spolupracovat s Milanem.

P2: Milan nekamarádí s nikým, kdo kamarádí s Láďou.

P3: Petr bude spolupracovat pouze s kamarády Karla.

P4: Karel kamarádí s Láďou.

Závěr: ???

Klausule:

- | | |
|-------------------------------------|------------------------------------|
| 1. $\neg R(x, J) \vee S(x, M)$ | 1. předpoklad |
| 2. $\neg K(y, L) \vee \neg K(M, y)$ | 2. předpoklad |
| 3. $\neg S(P, z) \vee K(z, Kr)$ | 3. předpoklad |
| 4. $K(Kr, L)$ | 4. předpoklad |
| 5. $\neg K(M, Kr)$ | důsledek, rezoluce 2,4, y/Kr |
| 6. $\neg R(P, J) \vee K(M, Kr)$ | důsledek, rezoluce 1,3, $x/P, z/M$ |
| 7. $\neg R(P, J)$ | důsledek, rezoluce 5,6 |
| 8. $\neg S(P, M)$ | důsledek, rezoluce 3,5, z/M |

Důkaz správnosti úsudku - sporem

Každý muž má rád fotbal a pivo.

Xaver má rád pouze ty, kdo mají rádi fotbal a pivo.

Někdo má rád fotbal a nemá rád pivo.

Kdo není muž, je žena. (*nezamlčujeme předpoklady*)

Některé ženy nemá Xaver rád.

$\forall x [M(x) \supset (R(x,f) \wedge R(x,p))]$ 1. předpoklad

$\forall x [R(Xa,x) \supset (R(x,f) \wedge R(x,p))]$ 2. předpoklad

$\exists x [R(x,f) \wedge \neg R(x,p)]$ 3. předpoklad

$\forall x [\neg M(x) \supset Z(x)]$ 4. předpoklad

$\neg \exists x [Z(x) \wedge \neg R(Xa,x)]$ negovaný závěr

Důkaz správnosti úsudku - sporem

Klausule:

1. $\neg M(x) \vee R(x,f)$
2. $\neg M(x) \vee R(x,p)$
3. $\neg R(Xa,y) \vee R(y,f)$
4. $\neg R(Xa,y) \vee R(y,p)$
5. $R(k,f)$
6. $\neg R(k,p)$
7. $M(z) \vee Z(z)$
8. $\neg Z(u) \vee R(Xa,u)$

-
9. $\neg R(Xa,k)$
 10. $\neg Z(k)$
 11. $M(k)$
 12. $R(k,p)$
 13. 

1. předpoklad
1. předpoklad
2. předpoklad
2. předpoklad
3. předpoklad
- po Skolemizaci: x/k
4. předpoklad
- negovaný závěr

- rezoluce 4., 6. **(y/k)**
- rezoluce 8., 9. **(u/k)**
- rezoluce 7., 10. **(z/k)**
- rezoluce 2., 11. **(x/k)**
- rezoluce 6., 12.

Opět jsme zjistili, že negovaný závěr je ve sporu s předpoklady,
proto je úsudek **platný**.

Víte, které předpoklady nebyly nutné pro odvození závěru?

Úsudky rezolucí

~~Je-li číslo sudé, pak jeho druhá mocnina je sudá.~~

$\models$ Je-li číslo sudé, pak jeho čtvrtá mocnina je sudá.

~~$\forall y [P(y) \supset P(f(y))]$~~

$\models \forall x [P(x) \supset P(f(f(x)))]$ *znegujeme závěr:*

$\exists x [P(x) \wedge \neg P(f(f(x)))]$ *Skolemizujeme:*

$[P(a) \wedge \neg P(f(f(a)))]$ *sepíšeme klauzule:*

1. $\neg P(y) \vee P(f(y))$ předpoklad
2. $P(a)$ negovaný závěr
3. $\neg P(f(f(a)))$ negovaný závěr
4. $P(f(a))$ rezoluce 1.,2., substituce y/a
5. $P(f(f(a)))$ rezoluce 1.,4., substituce $y/f(a)$
6. $\blacksquare$ rezoluce 3.,5., spor

Úsudek je platný

Matematická indukce

$$P(a), \forall y [P(y) \supset P(f(y))] \vdash \forall x P(x)$$

Vyplývá odvozená formule z premis? Jinými slovy, je důkazové pravidlo matematické indukce korektní, zachovává pravdivost?

Klausule:

1. $P(a)$
2. $\neg P(y) \vee P(f(y))$
3. $P(f(a))$ důsledek 2.1., subst. y/a
4. $P(f(f(a)))$ důsledek 2.3., subst. $y/f(a)$
5. $P(f(f(f(a))))$ důsledek 2.4., subst. $y/f(f(a))$
6. *Atd.*

Ani sporem to nedokážeme, neboť negovaný závěr po Skolemizaci je: $\neg P(b)$ a termy $b, a, f(a), f(f(a)), \dots$ nejsou unifikovatelné. Nikdy nedokážeme, že $\forall x P(x)$ – aktuální nekonečno. Dokážeme to pouze potenciálně ...

Ověřování konzistence

- Jistý holič holí právě ty všechny, kdo se neholí sami.
- Holí tento holič sám sebe?

$$\exists x \forall y [\neg H(y,y) \equiv H(x,y)] \models ? H(x,x)$$

V přednášce 7 jsme viděli, že předpoklad je nesplnitelný, tedy takový holič neexistuje. Ověříme rezoluční metodou. K předpokladu přidáme negovaný závěr a upravíme do klauzulí.

1. $H(y,y) \vee H(a,y) \Rightarrow H(a,a)$ substituce y/a
2. $\neg H(y,y) \vee \neg H(a,y) \Rightarrow \neg H(a,a)$ substituce y/a
3. $\neg \blacksquare(x,x)$ negovaný závěr
4. rezoluce 1., 2., substituce y/a

K odvození sporu jsme **nepotřebovali klauzuli 3.** (negovaný závěr), tedy sporný, nesplnitelný, nekonzistentní je již předpoklad.

Takový holič neexistuje

Poznámka

Robinsonův algoritmus obecné rezoluce a unifikace pracuje tak, že unifikuje rovněž jednotlivé literály v klauzuli. Tak například klauzule:

$$1. P(x,y) \vee \neg Q(a,f(y)) \vee P(x,a) \vee \neg Q(y,x) \Rightarrow P(f(a),a) \vee \neg Q(a,f(a))$$

$$2. \neg P(f(z),z) \vee \neg P(v,a) \Rightarrow \neg P(f(a),a)$$

dají po unifikaci $x/f(a)$, y/a , z/a , $v/f(a)$ rezolventu $\neg Q(a,f(a))$, neboť první klauzule se unifikuje na $P(f(a),a) \vee \neg Q(a,f(a))$ a druhá na $\neg P(f(a),a)$.

Poznámka – pozor na ekvivalence

- a) Formule $A \equiv B$ není sporná, je splnitelná
- b) Formule $A \equiv \neg A$ je sporná

Klauzule ad a)

1. $\neg A \vee B$

2. $A \vee \neg B$

nyní v každém kroku můžeme generovat rezolventu pouze škrtnutím **jednoho** literálu, tedy **ne** prázdnou klauzuli:

3. $B \vee \neg B$ **tautologie** vyplývá z jakékoli formule

4. $A \vee \neg A$

Klauzule ad b)

1. $\neg A \vee \neg A \Rightarrow \neg A$

2. $A \vee A \Rightarrow A$

3. 1. a 2. rezolvuji na prázdnou klauzuli.

Ověřování konzistence

- Pan X přešel na kvalifikovanější práci (K).
- Pan X dobře rozumí mzdovým otázkám (M).
- Jestliže pan X přešel na kvalifikovanější práci, pak je správné, aby jeho žádost byla projednána (P).
- Jestliže je správné, aby jeho žádost byla v komisi projednána, pak by neměl být členem komise (C).
- Rozumí-li výtečně mzdovým otázkám, měl by být členem komise.

Co z toho vyplývá?

Ověříme nejprve konzistenci této množiny tvrzení.

$$K \wedge M \wedge (K \supset P) \wedge (P \supset \neg C) \wedge (M \supset C)$$

1. K
2. M
3. $\neg K \vee P$
4. $\neg P \vee \neg C$
5. $\neg M \vee C$
6. P rezoluce 1, 3
7. $\neg C$ rezoluce 4, 6
8. C rezoluce 2, 5
9. spor rezoluce 7, 8

Daná množina tvrzení je sporná, **nekonzistentní**, proto z ní **vyplývá cokoli**.

Ověření logické platnosti formule

$$\models ? \quad \forall x [P(x) \wedge \forall y \exists x (\neg Q(x,y) \supset \forall z R(a,x,y))] \\ \supset \\ \exists z [(P(b) \wedge Q(f(z), z)) \vee R(a, f(b), z)]$$

Antecedent převedeme do klauzulární formy:

- a) Metodou dle Skolemova algoritmu.
- b) Nejdříve do prenexní formy a pak Skolemizujeme.

Ověření logické platnosti vs.

krok 6

Antecedent - převod do klauzulární formy, **postup a)**
 $\forall x [P(x) \wedge \forall y \exists x (\neg Q(x,y) \supset \forall z R(a,x,y))]$

Kroky 2., 5. Přejmenujme proměnnou x a odstraníme $\forall z$:
 $\forall x [P(x) \wedge \forall y \exists u (\neg Q(u,y) \supset R(a,u,y))]$

Krok 3. Odstraníme implikaci:

$$\forall x [P(x) \wedge \forall y \exists u (Q(u,y) \vee R(a,u,y))]$$

Krok 6. Nyní přesuneme kvantifikátor $\forall x$ doprava:

$$\forall x P(x) \wedge \forall y \exists u (Q(u,y) \vee R(a,u,y))$$

Krok 7. Skolemizujeme (tj. za proměnnou u substitujeme $g(y)$,
neboť funkční

symbol f je již použit v závěru):

$$\forall x P(x) \wedge \forall y (Q(g(y), y) \vee R(a, g(y), y))$$

Krok 8. přesuneme kvantifikátory doleva:

$$\text{SK1: } \forall x \forall y [P(x) \wedge (Q(g(y), y) \vee R(a, g(y), y))].$$

Ověření logické platnosti vs. krok 6

Antecedent - převod do klauzulární formy, **postup b)** bez kroku 6

$$\forall x [P(x) \wedge \forall y \exists x (\neg Q(x,y) \supset \forall z R(a,x,y))]$$

Kroky 2, 5: Přejmenujme proměnnou x a odstraníme $\forall z$:

$$\forall x [P(x) \wedge \forall y \exists u (\neg Q(u,y) \supset R(a,u,y))]$$

Krok 3. Odstraníme implikaci:

$$\forall x [P(x) \wedge \forall y \exists u (Q(u,y) \vee R(a,u,y))]$$

Krok 7. Skolemizujeme (tj. za proměnnou u substitujeme $g(x,y)$,

neboť proměnná u je v rozsahu $\forall x$):

$$\forall x [P(x) \wedge \forall y (Q(\mathbf{g}(x,y), y) \vee R(a, \mathbf{g}(x,y), y))]$$

Krok 8. přesuneme kvantifikátory doleva:

$$\text{SK2: } \forall x \forall y [P(x) \wedge (Q(\mathbf{g}(x,y), y) \vee R(a, \mathbf{g}(x,y), y))].$$

Ověření logické platnosti vs. krok 6

Negovaný závěr (již je v klauzulární formě):

$$\forall z [(\neg P(b) \vee \neg Q(f(z), z)) \wedge \neg R(a, f(b), z)].$$

Pokusíme se dokázat spor s SK1 (klauzulární forma antecedentu).

Sepíšeme klauzule, postup a):

1. $P(x)$ předpoklad
2. $Q(g(y), y) \vee R(a, g(y), y)$ předpoklad
3. $\neg P(b) \vee \neg Q(f(z), z)$ negovaný závěr
4. $\neg R(a, f(b), z)$ negovaný závěr
5. $\neg Q(f(z), z)$ rezoluce 1., 3., substituce x / b
6. ???

Dále nemůžeme rezolvovat, neboť termy $g(y)$ a $f(z)$, či $g(y)$ a $f(b)$ nejsou unifikovatelné.

Formule není logicky pravdivá.

Ověření logické platnosti vs. krok 6

Ani spor SK2 (postup b) s naším negovaným závěrem nedokážeme:

1. $P(x)$
2. $Q(\mathbf{g}(x,y), y) \vee R(a, \mathbf{g}(x,y), y)$
3. $\neg P(b) \vee \neg Q(f(z), z)$
4. $\neg R(a, f(b), z)$
- . $\neg Q(f(z), z)$ *rezoluce 1., 3., substituce x / b*

Další kroky však již nelze provést, protože termy $g(x,y)$ a $f(z)$, případně $g(x,y)$ a $f(b)$ nejsou unifikovatelné.

Závěr: Formule není logicky pravdivá.

Příklad, hádanka

- Tom, Peter and John are members of a sport club. Every member of the club is a skier or a climber. No climber likes raining. All skiers like snow. Peter does not like what Tom likes, and does like what Tom does not like. Tom likes snow and raining.
- *Question:* Is there in the club a sportsman who is a climber but not a skier?
- *Solution: Knowledge base (+ query 11):*

1. $SC(t)$
2. $SC(p)$
3. $SC(j)$
4. $\forall x [SC(x) \supset (SKI(x) \vee CLIMB(x))]$
5. $\forall x [CLIMB(x) \supset \neg LIKE(x,r)]$
6. $\forall x [SKI(x) \supset LIKE(x,s)]$
7. $\forall x [LIKE(t,x) \supset \neg LIKE(p,x)]$
8. $\forall x [\neg LIKE(t,x) \supset LIKE(p,x)]$
9. $LIKE(t,s)$
10. $LIKE(t,r)$
11. **? $\exists x [SC(x) \wedge CLIMB(x) \wedge \neg SKI(x)]$**

Příklad, hádanka

Knowledge base (in Clausal form + negated query 11):

1. $SC(t)$ *sport-club(tom).*
2. $SC(p)$ *sport-club(peter).*
3. $SC(j)$ *sport-club(john).*
4. $\neg SC(y) \vee SKI(y) \vee CLIMB(y)$ *each club member is a skier or a climber*
- . $\neg CLIMB(z) \vee \neg LIKE(z,r)$ *each climber does not like raining*
- . $\neg SKI(v) \vee LIKE(v,s)$ *each skier does not like snowing*
- . $\neg LIKE(t,x1) \vee \neg LIKE(p,x1)$ *Tom and Peter have opposite tastes*
8. $LIKE(t,x2) \vee LIKE(p,x2)$ *tastes*
9. $LIKE(t,s)$ *like(tom, snow).*
10. $LIKE(t,r)$ *like(tom, raining).*
- . $\neg SC(x) \vee \neg CLIMB(x) \vee SKI(x)$ *Query*

Proof by resolution that 1-11 is inconsistent. In other words, we are looking for an instantiation of the variable x , that leads to a contradiction.

12. $\neg LIKE(p,s)$ *res.: 9, 7 by substituting s for $x1$*
- . $\neg SKI(p)$ *res.: 12, 6 by substituting p for v*
- . $\neg SC(p) \vee CLIMB(p)$ *res.: 13, 4 by substituting p for y*
15. $CLIMB(p)$ *res.: 14, 2*
16. *Resolution 11 + 2 + 13 + 15 by substituting p for x .*
(Obviously, **the solution is $p = \text{Peter}$**)

Ověření platnosti úsudku: hádanka

Situace: Sešli se přátelé, mezi nimi kněz A, který prohlásil: „První člověk, kterého jsem zpovídal, je vrah“. Po chvíli vešel pan B, uviděl kněze a řekl: „Já jsem byl první člověk, kterého kněz A zpovídal“.

Otázka: Porušil kněz zpovědní tajemství?

Řešení: $\forall x [(x = f(A)) \supset V(x)]$

$B = f(A)$

???

(*Zamýšlená interpretace:* f bude funkce, která každému knězi přiřazuje toho jediného člověka, kterého zpovídal jako prvního).

Klausule: 1. $\neg(x = f(A)) \vee V(x)$ 1. premisa
 2. $B = f(A)$ 2. premisa
 3. $V(B)$ **důsledek:** rezoluce
 (B je vrah) 1., 2., substituce x/B

Odpověď: Kněz zřejmě porušil zpovědní tajemství