

Rezoluce

Rezoluce v predikátové logice 1.řádu

- rezoluční princip: z $F \vee A, G \vee \neg A$ odvodit $F \vee G$
- dokazovací metoda používaná
 - v Prologu
 - ve většině systémů pro automatické dokazování
- procedura pro **vyvrácení**
 - hledáme důkaz pro negaci formule
 - snažíme se dokázat, že negace formule je nesplnitelná
 \Rightarrow formule je vždy pravdivá

Formule

- **literál** l
 - **pozitivní literál** = atomická formule $p(t_1, \dots, t_n)$
 - **negativní literál** = negace atomické formule $\neg p(t_1, \dots, t_n)$
 - t_1, \dots, t_n jsou termy
- **klauzule** C = konečná množina literálů reprezentující jejich disjunkci
 - příklad: $p(X) \vee q(a, f) \vee \neg p(Y)$ notace: $\{p(X), q(a, f), \neg p(Y)\}$
 - **klauzule je pravdivá** \Leftrightarrow je pravdivý alespoň jeden z jejích literálů
 - **prázdná klauzule** se značí \square a je vždy nepravdivá (neexistuje v ní pravdivý literál)
- **formule** F = množina klauzulí reprezentující jejich konjunkci
 - formule je v tzv. konjunktivní normální formě (konjunkce disjunkcí)
 - příklad: $(p \vee q) \wedge (\neg p) \wedge (p \vee \neg q \vee r)$ notace: $\{\{p, q\}, \{\neg p\}, \{p, \neg q, r\}\}$
 - **formule je pravdivá** \Leftrightarrow všechny klauzule jsou pravdivé
 - prázdná formule je vždy pravdivá (neexistuje klauzule, která by byla nepravdivá)
- **množinová notace**: literál je prvek klauzule, klauzule je prvek formule, ...

Splnitelnost

- **[Opakování:]** Interpretace \mathcal{I} jazyka \mathcal{L} je dána univerzem \mathcal{D} a zobrazením, které přiřadí konstantě c prvek \mathcal{D} , funkčnímu symbolu f/n n -ární operaci v \mathcal{D} a predikátovému symbolu p/n n -ární relaci.
 - příklad: $F = \{\{f(a, b) = f(b, a)\}, \{f(f(a, a), b) = a\}\}$
interpretace \mathcal{I}_1 : $\mathcal{D} = \mathbb{Z}, a := 1, b := -1, f := "+"$
- Formule je **splnitelná**, existuje-li interpretace, pro kterou je pravdivá
 - formule je konjunkce klauzulí, tj. všechny klauzule musí být v dané interpretaci pravdivé
 - příklad (pokrač.): F je splnitelná (je pravdivá v \mathcal{I}_1)
- Formule je **nesplnitelná**, neexistuje-li interpretace, pro kterou je pravdivá
 - tj. formule je ve všech interpretacích nepravdivá
 - tj. neexistuje interpretace, ve které by byly všechny klauzule pravdivé
 - příklad: $G = \{\{p(b)\}, \{p(a)\}, \{\neg p(a)\}\}$ je nesplnitelná
($\{p(a)\}$ a $\{\neg p(a)\}$ nemohou být zároveň pravdivé)

Rezoluční princip ve výrokové logice

- **Rezoluční princip** = pravidlo, které umožňuje odvodit z klauzulí $C_1 \cup \{l\}$ a $\{\neg l\} \cup C_2$ klauzuli $C_1 \cup C_2$

$$\frac{C_1 \cup \{l\} \quad \{\neg l\} \cup C_2}{C_1 \cup C_2}$$

- $C_1 \cup C_2$ se nazývá **rezolventou** původních klauzulí

- příklad:

$$\frac{\{p, r\} \quad \{\neg r, s\}}{\{p, s\}} \quad \frac{(p \vee r) \wedge (\neg r \vee s)}{p \vee s}$$

obě klauzule $(p \vee r)$ a $(\neg r \vee s)$ musí být pravdivé protože r nestačí k pravdivosti obou klauzulí, musí být pravdivé p (pokud je pravdivé $\neg r$) nebo s (pokud je pravdivé r), tedy platí klauzule $p \vee s$

Rezoluční důkaz

- **rezoluční důkaz klauzule C z formule F** je konečná posloupnost $C_1, \dots, C_n = C$ klauzulí taková, že C_i je buď klauzule z F nebo rezolventa C_j, C_k pro $k, j < i$.

- příklad: rezoluční důkaz $\{p\}$ z formule $F = \{\{p, r\}, \{q, \neg r\}, \{\neg q\}\}$

$C_1 = \{p, r\}$ klauzule z F

$C_2 = \{q, \neg r\}$ klauzule z F

$C_3 = \{p, q\}$ rezolventa C_1 a C_2

$C_4 = \{\neg q\}$ klauzule z F

$C_5 = \{p\} = C$ rezolventa C_3 a C_4

Rezoluční vyvrácení

- důkaz pravdivosti formule F spočívá v **demonstraci nesplnitelnosti $\neg F$**
 - $\neg F$ nesplnitelná $\Rightarrow \neg F$ je nepravdivá ve všech interpretacích $\Rightarrow F$ je vždy pravdivá
- začneme-li z klauzulí reprezentujících $\neg F$, musíme postupným uplatňováním rezolučního principu **dospět k prázdné klauzuli \square**

- Příklad:

$F \dots \neg a \vee a$

$G = \neg F \dots a \wedge \neg a$

$G = \neg F \dots \{\{a\}, \{\neg a\}\}$

$C_1 = \{a\}, C_2 = \{\neg a\}$

rezolventa C_1 a C_2 je \square , tj. F je vždy pravdivá

- rezoluční důkaz \square z formule G se nazývá **rezoluční vyvrácení formule G**

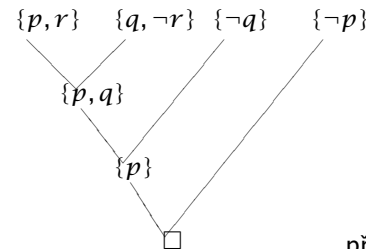
- a tedy G je nepravdivá ve všech interpretacích, tj. G je nesplnitelná

Strom rezolučního důkazu

- **strom rezolučního důkazu** klauzule C z formule G je binární strom:

- kořen je označen klauzulí C ,
- listy jsou označeny klauzulemi z G a
- každý uzel, který není listem,
 - má bezprostředními potomky označené klauzulemi C_1 a C_2
 - je označen rezolventou klauzulí C_1 a C_2

- příklad: $G = \{\{p, r\}, \{q, \neg r\}, \{\neg q\}, \{\neg p\}\}$ $C = \square$



strom rezolučního vyvrácení
(rezoluční důkaz \square z G)

příklad: $\{\{p, r\}, \{q, \neg r\}, \{\neg q\}, \{\neg p, t\}, \{\neg s\}, \{s, \neg t\}\}$

Substituce

- **co s proměnnými? vhodná substituce a unifikace**
 - $f(X, a, g(Y)) < 1, f(h(c), a, Z) < 1, \quad X = h(c), Z = g(Y) \implies f(h(c), a, g(Y)) < 1$
- **substituce** je libovolná funkce θ zobrazující výrazy do výrazů tak, že platí
 - $\theta(E) = E$ pro libovolnou konstantu E
 - $\theta(f(E_1, \dots, E_n)) = f(\theta(E_1), \dots, \theta(E_n))$ pro libovolný funkční symbol f
 - $\theta(p(E_1, \dots, E_n)) = p(\theta(E_1), \dots, \theta(E_n))$ pro libovolný predik. symbol p
- **substituce** je tedy homomorfismus výrazů, který **zachová vše kromě proměnných** – ty lze nahradit čímkoliv
- substituce zapisujeme zpravidla ve tvaru seznamu $[X_1/\xi_1, \dots, X_n/\xi_n]$ kde X_i jsou proměnné a ξ_i substituované termy
 - příklad: $p(X)[X/f(a)] \equiv p(f(a))$
- **přejmenování proměnných**: speciální náhrada proměnných proměnnými
 - příklad: $p(X)[X/Y] \equiv p(Y)$

Rezoluční princip v PL1

- základ:
 - rezoluční princip ve výrokové logice $\frac{C_1 \cup \{I\} \quad \{\neg I\} \cup C_2}{C_1 \cup C_2}$
 - substituce, unifikátor, nejobecnější unifikátor
- **rezoluční princip v PL1** je pravidlo, které
 - připraví příležitost pro uplatnění vlastního rezolučního pravidla nalezením vhodného unifikátoru
 - provede rezoluci a získá rezolventu
$$\frac{C_1 \cup \{A\} \quad \{\neg B\} \cup C_2}{C_1 \rho \sigma \cup C_2 \sigma}$$
 - kde ρ je přejmenováním proměnných takové, že klauzule $(C_1 \cup A)\rho$ a $\{B\} \cup C_2$ nemají společné proměnné
 - σ je nejobecnější unifikátor klauzulí $A\rho$ a B

Unifikace

- Ztotožnění dvou literálů p, q pomocí vhodné substituce σ takové, že $p\sigma = q\sigma$ nazýváme **unifikací** a příslušnou substitucí **unifikátorem**.
- **Unifikátorem** množiny S literálů nazýváme substituce θ takovou, že množina

$$S\theta = \{t\theta \mid t \in S\}$$
 má jediný prvek.
 - příklad: $S = \{ \text{datum}(D1, M1, 2003), \text{datum}(1, M2, Y2) \}$
unifikátor $\theta = [D1/1, M1/2, M2/2, Y2/2003]$ $S\theta = \{ \text{datum}(1, 2, 2003) \}$
- Unifikátor σ množiny S nazýváme **nejobecnějším unifikátorem (mgu – most general unifier)**, jestliže pro libovolný unifikátor θ existuje substituce λ taková, že $\theta = \sigma\lambda$.
 - příklad (pokrač.): nejobecnější unifikátor $\sigma = [D1/1, Y2/2003, M1/M2], \quad \lambda = [M2/2]$

Příklad: rezoluce v PL1

- příklad: $C_1 = \{p(X, Y), q(Y)\} \quad C_2 = \{\neg q(a), s(X, W)\}$
- přejmenování proměnných: $\rho = [X/Z]$

$$C_1 = \{p(Z, Y), q(Y)\} \quad C_2 = \{\neg q(a), s(X, W)\}$$
- nejobecnější unifikátor: $\sigma = [Y/a]$

$$C_1 = \{p(Z, a), q(a)\} \quad C_2 = \{\neg q(a), s(X, W)\}$$
- rezoluční princip: $C = \{p(Z, a), s(X, W)\}$
- vyzkoušejte si:

$$C_1 = \{q(X), \neg r(Y), p(X, Y), p(f(Z), f(Z))\}$$

$$C_2 = \{n(Y), \neg r(W), \neg p(f(W), f(W))\}$$

Rezoluce v PL1

▪ Obecný rezoluční princip v PL1

$$\frac{C_1 \cup \{A_1, \dots, A_m\} \quad \{\neg B_1, \dots, \neg B_n\} \cup C_2}{C_1 \rho \sigma \cup C_2 \sigma}$$

- kde ρ je přejmenováním proměnných takové, že množiny klauzulí $\{A_1 \rho, \dots, A_m \rho, C_1 \rho\}$ a $\{B_1, \dots, B_n, C_2\}$ nemají společné proměnné
- σ je nejobecnější unifikátor množiny $\{A_1 \rho, \dots, A_m \rho, B_1, \dots, B_n\}$
- příklad: $A_1 = a(X)$ vs. $\{\neg B_1, \neg B_2\} = \{\neg a(b), \neg a(Z)\}$
v jednom kroku potřebuji vyrezolvovat zároveň B_1 i B_2

▪ Rezoluce v PL1

- **korektní:** jestliže existuje rezoluční vyvrácení F , pak F je nespíitelná
- **úplná:** jestliže F je nespíitelná, pak existuje rezoluční vyvrácení F

Zefektivnění rezoluce

▪ rezoluce je intuitivně efektivnější než axiomatické systémy

- axiomatické systémy: který z axiomů a pravidel použít?
- rezoluce: pouze jedno pravidlo
- stále ale příliš mnoho možností, jak hledat důkaz v prohledávacím prostoru
- problém SAT = $\{S \mid S \text{ je splnitelná}\}$ NP úplný, nicméně: menší prohledávací prostor vede k rychlejšímu nalezení řešení
- strategie pro zefektivnění prohledávání \Rightarrow varianty rezoluční metody
- vylepšení prohledávání
 - zastavit prohledávání cest, které nejsou slibné
 - specifikace pořadí, jak procházíme alternativními cestami

Varianty rezoluční metody

▪ **Věta:** Každé omezení rezoluce je korektní.

- stále víme, že to, co jsme dokázali, platí

▪ **T-rezoluce:** klauzule účastníci se rezoluce nejsou tautologie úplná

- tautologie nepomůže ukázat, že formule je nespíitelná

▪ **sémantická rezoluce:** úplná

zvolíme libovolnou interpretaci a pro rezoluci používáme jen takové klauzule, z nichž alespoň jedna je v této interpretaci nepravdivá

- pokud jsou obě klauzule pravdivé, těžko odvodíme nespíitelnost formule

▪ **vstupní (input) rezoluce:** neúplná alespoň jedna z klauzulí, použitá při rezoluci, je z výchozí **vstupní množiny** S

- $\{\{p, q\}, \{\neg p, q\}, \{p, \neg q\}, \{\neg p, \neg q\}\}$

existuje rezoluční vyvrácení

neexistuje rezoluční vyvrácení pomocí vstupní rezoluce