Rezolvencia

12. prednáška · Matematika (4): Logika pre informatikov

Ján Kľuka, Jozef Šiška

Letný semester 2019/2020

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky
Katedra aplikovanej informatiky

Obsah 12. prednášky

Rezolvencia

Automatické dokazovanie v logike prvého rádu

Vyplývanie vo výrokovej logike je rozhodnuteľné.

SAT solver vždy skončí a rozhodne splniteľnosť, v najhoršom prípade v čase $O(2^n)$ pre n atómov.

Logika prvého rádu nie je rozhodnuteľná.

- Prvorádovými formulami sa dá opísať fungovanie Turingovho stroja.
- Dá sa nájsť formula, ktorá opisuje, že TS zastaví na každom vstupe.

Existujú však prvorádové automatické dokazovače (Prover9, Vampire).

Nemusia zastaviť, ale ak existuje dôkaz vyplývania, teoreticky ho nájdu.

Ako fungujú automatické dokazovače v logike prvého rádu

Prvé automatické dokazovače využívali prvorádovú verziu DPLL.

Niektoré automatické dokazovače využívajú modifikované tablá.

Väčšina automatických dokazovačov je ale založená na **rezolvencii**:

- špeciálne pravidlo na klauzulách,
- kombinuje výrokové a kvantifikátorové odvodzovanie.

Rezolvenčný dôkaz je lineárny, nevetví sa.

Rezolvencia

Rezolvencia vo výrokovej logike

Tranzitivita implikácie

Vráťme sa k neoznačeným formulám.

Je nasledujúce pravidlo korektné?

$$\frac{(A \to B) \qquad (B \to C)}{(A \to C)}$$

Nahraďme implikácie disjunkciami:

$$\frac{(\neg A \lor B) \qquad (\neg B \lor C)}{(\neg A \lor C)}$$

Predchádzajúce pravidlo sa dá zovšeobecniť na ľubovoľné dvojice klauzúl:

Definícia 14.1

Rezolvenčný princíp (***rezolvencia***, angl. *resolution principle*) je pravidlo

$$\frac{(K_1 \lor \cdots \lor A \lor \cdots \lor K_m) \qquad (L_1 \lor \cdots \lor \neg A \lor \cdots \lor L_n)}{(K_1 \lor \cdots \lor K_m \lor L_1 \lor \cdots \lor L_n)}$$

pre ľubovoľný atóm A
a ľubovoľné literály $K_1, \ldots, K_m, L_1, \ldots, L_n$.

Klauzulu $(K_1 \lor \cdots \lor K_m \lor L_1 \lor \cdots \lor L_n)$ nazývame ***rezolventou*** klauzúl $(K_1 \lor \cdots \lor A \lor \cdots \lor K_m)$ a $(L_1 \lor \cdots \lor \neg A \lor \cdots \lor L_n)$.

Tvrdenie 14.2

Rezolvencia je korektné pravidlo.

Špeciálne prípady rezolvencie

Viacero pravidiel sa dá chápať ako špeciálne prípady rezolvencie:

$$\frac{(\neg A \vee B) \quad (\neg B \vee C)}{(\neg A \vee C)} \qquad \frac{(A \to B) \quad (B \to C)}{(A \to C)} \qquad \text{(tranzitivita } \to\text{)}$$

$$\frac{(\neg A \vee B) \quad A}{B} \qquad \frac{(A \to B) \quad A}{B} \qquad \text{(modus ponens)}$$

$$\frac{(\neg A \vee B) \quad \neg B}{\neg A} \qquad \frac{(A \to B) \quad \neg B}{\neg A} \qquad \text{(modus tolens)}$$

Pozorovania o rezolvencii

- Rezolvencia s **jednotkovou** klauzulou skráti druhú klauzulu:

$$\frac{\neg B \quad (A \lor B \lor \neg C)}{(A \lor \neg C)}$$

- Rezolvencia môže odvodiť **prázdnu klauzulu**:

$$\frac{\neg A \quad A}{\Box},$$

  vtedy premisy **nie sú súčasne splniteľné**

- Nie každý logický dôsledok sa dá odvodiť rezolvenciou:
  $\{A, B\} \vDash (A \lor B)$

Častá chyba pri rezolvencii

Niektoré dvojice klauzúl možno rezolvovať na viacerých literáloch, ale je **chyba urobiť to naraz**:

$$\frac{(\neg p \lor q) \quad (p \lor \neg q)}{(q \lor \neg q)} \qquad \frac{(\neg p \lor q) \quad (p \lor \neg q)}{(\neg p \lor p)}$$

$$\cancel{\frac{(\neg p \lor q) \quad (p \lor \neg q)}{\Box}}$$

Prečo?

Lebo $\{(\neg p \lor q), (p \lor \neg q)\}$ je ekvivalentná $p \leftrightarrow q$ a je splniteľná ($v_1 = \{p \mapsto t, q \mapsto t\}, v_2 = \{p \mapsto f, q \mapsto f\}$), ale $\Box$ je nesplniteľná.

Pravidlá zachovávajú splniteľnosť, ale ich chybné použitia nie

Rezolvenčné odvodenie a problém

Opakovaním rezolvencie môžeme odvodzovať ďalšie dôsledky:

Príklad 14.3

Z množiny $S = \{(A \vee B), (\neg A \vee C), (\neg B \vee A), (\neg A \vee \neg C)\}$ odvodíme:

(1) $(A \vee B)$ predpoklad z S

(2) $(\neg A \vee C)$ predpoklad z S

(3) $(\neg B \vee A)$ predpoklad z S

(4) $(\neg A \vee \neg C)$ predpoklad z S

(5) $(A \vee A)$ rezolventa (3) a (1)

(6) $(B \vee C)$ rezolventa (1) a (2)

(7) $(B \vee \neg C)$ rezolventa (1) a (4)

(8) $(B \vee B)$ rezolventa (6) a (7)

$\vdots$

Problematické prípady

Odvodeniami v príklade dostaneme iba existujúce alebo nové **dvojprvkové** klauzuly ($(A \lor A)$, $(B \lor C)$, $(B \lor B)$, $\ldots$) ale žiadnu jednotkovú.

Klauzula $(A \lor A)$ je evidentne ekvivalentná s A;
A sa ale z množiny S iba rezolvenciou odvodiť nedá.

$S = \{(A \lor B), (\neg A \lor C), (\neg B \lor A), (\neg A \lor \neg C)\}$ je ale nesplniteľná, mali by sme nejak odvodiť prázdnu klauzulu.

To sa nedá bez odvodenia nejakej jednotkovej klauzuly (napr. A).

Potrebujeme ešte ***pravidlo idempotencie***:

$$\frac{(K_1 \lor \cdots \lor L \lor \cdots \lor L \lor \cdots \lor K_n)}{(K_1 \lor L \lor \cdots \lor K_n)}$$

Definícia 14.4

Výrokovologické rezolvenčné odvodenie z množiny klauzúl S je každá (aj nekonečná) postupnosť klauzúl $C_1, C_2, \ldots, C_n, \ldots$, ktorej každý člen C_i je:

- prvkom S alebo
- rezolventou dvoch predchádzajúcich klauzúl C_j a C_k pre $j < i$ a $k < i$, alebo
- záverom pravidla idempotencie pre nejakú predchádzajúcu klauzulu C_j, $j < i$.

Zamietnutím (angl. *refutation*) množiny klauzúl S je **konečné** rezolvenčné odvodenie, ktorého posledným prvkom je prázdna klauzula $\square$.

Príklad 14.5

Nech $S = \{(A \vee B), (\neg A \vee C), (\neg B \vee A), (\neg A \vee \neg C)\}$.

Kombináciou rezolvencie a idempotencie nájdeme zamietnutie S:

(1) $(A \vee B)$ predpoklad z S

(2) $(\neg A \vee C)$ predpoklad z S

(3) $(\neg B \vee A)$ predpoklad z S

(4) $(\neg A \vee \neg C)$ predpoklad z S

(5) $(A \vee A)$ rezolventa (3) a (1)

(6) A idempotencia (5)

(7) C rezolvencia (6) a (2)

(8) $\neg C$ rezolvencia (6) a (4)

(9) $\square$ rezolvencia (7) a (8)

Korektnosť a úplnosť rezolvencie

Definícia 14.6

Množinu klauzúl budeme nazývať aj ***klauzálna teória***.

Veta 14.7 (Korektnosť rezolvencie)

Nech S je množina klauzúl.

Ak existuje zamietnutie S, tak S je výrokovologické nesplniteľná.

Veta 14.8 (Úplnosť rezolvencie)

Nech S je množina klauzúl.

Ak S je výrokovologické nesplniteľná, tak existuje zamietnutie S.

Rezolvencia

Prevod do klauzálnej teórie a skolemizácia

Rezolvencia vs. prvorádové teórie

Výrokovologická rezolvencia pracuje s klauzálnymi teóriami.

Výrokovologickú teóriu ľahko upravíme na klauzálnu — ekvivalentnými úpravami do CNF.

Ale čo s formulami v logike prvého rádu,
kde sú spojky zložito skombinované s kvantifikátormi?

Definícia 14.9

Nech $\mathcal{L}$ je jazyk logiky prvého rádu.

Literál je atomická formula $P(t_1, \dots, t_m)$ jazyka $\mathcal{L}$ alebo jej negácia $\neg P(t_1, \dots, t_m)$.

Klauzula je všeobecný uzáver disjunkcie literálov, teda uzavretá formula jazyka $\mathcal{L}$ v tvare $\forall x_1 \cdots \forall x_k (L_1 \lor \cdots \lor L_n)$ kde $L_1, \dots, L_n$ sú literály a $x_1, \dots, x_k$ sú *všetky* voľné premenné formuly $L_1 \lor \cdots \lor L_n$. Klauzula môže byť aj ***jednotková*** ($\forall \vec{x}\, L_1$) alebo ***prázdna*** ($\Box$).

Klauzálna teória je množina klauzúl $\{C_1, \dots, C_n\}$. Môže byť tvorená aj jedinou klauzulou alebo byť prázdna.

Prvorádová ekvivalencia

Definícia 14.10 (Prvorádová ekvivalencia)

Množiny formúl S a T sú *(prvorádovo) ekvivalentné* ($S \Leftrightarrow T$) vtt pre každú štruktúru $\mathcal{M}$ a každé ohodnotenie e platí $\mathcal{M} \models S[e]$ vtt $\mathcal{M} \models T[e]$.

Tvrdenie 14.11 (Ekvivalentná úprava)

Nech X, A, B sú formuly a nech $\mathrm{free}(A) = \mathrm{free}(B)$.

Ak $A \Leftrightarrow B$, tak $X \Leftrightarrow X[\, A \mid B \,]$.

Nahradenie implikácií

Rovnako ako vo výrokovej logike môžeme každú formulu $(A \to B)$ ekvivalentne nahradiť formulou $(\neg A \lor B)$.

Príklad 14.12

$$\begin{aligned} &\forall x(\mathtt{dobr\acute{e}}(x) \land \mathtt{die\check{t}a}(x) \to \exists y(\mathtt{dostane}(x,y) \land \mathtt{dar\check{c}ek}(y))) \\ \Leftrightarrow\ &\forall x(\neg(\mathtt{dobr\acute{e}}(x) \land \mathtt{die\check{t}a}(x)) \lor \exists y(\mathtt{dostane}(x,y) \land \mathtt{dar\check{c}ek}(y))) \end{aligned}$$

$$\begin{aligned} &\forall x(\neg\mathtt{dobr\acute{e}}(x) \to \neg\exists y\,\mathtt{dostane}(x,y)) \\ \Leftrightarrow\ &\forall x(\neg\neg\mathtt{dobr\acute{e}}(x) \lor \neg\exists y\,\mathtt{dostane}(x,y)) \end{aligned}$$

Konverzia do negačného normálneho tvaru (NNF)

Definícia 14.13

Formula X je v ***negačnom normálnom tvare*** (NNF) vtt
neobsahuje implikáciu
a pre každú jej podformulu $\neg A$ platí, že A je atomická formula.

Formulu bez implikácií do NNF upravíme pomocou

- de Morganovych zákonov pre spojky:

$$\neg(A \land B) \Leftrightarrow \neg A \lor \neg B \qquad \neg(A \lor B) \Leftrightarrow \neg A \land \neg B$$

- pravidla dvojitej negácie:

$$\neg\neg A \Leftrightarrow A$$

- zovšeobecnení de Morganovych zákonov pre kvantifikátory:

$$\neg \exists x\, A \Leftrightarrow \forall x \neg A \qquad \neg \forall x\, A \Leftrightarrow \exists x \neg A$$

Konverzia do NNF

Tvrdenie 14.14

Pre každú formulu X *existuje formula* Y *v NNF taká, že* $X \Leftrightarrow Y$.

Príklad 14.15

$$\begin{aligned} & \forall x(\neg(\mathtt{dobré}(x) \land \mathtt{dieťa}(x)) \lor \exists y(\mathtt{dostane}(x,y) \land \mathtt{darček}(y))) \\ \Leftrightarrow\ & \forall x((\neg\mathtt{dobré}(x) \lor \neg\mathtt{dieťa}(x)) \lor \exists y(\mathtt{dostane}(x,y) \land \mathtt{darček}(y))) \end{aligned}$$

$$\begin{aligned} & \forall x(\neg\neg\mathtt{dobré}(x) \lor \neg\exists y\, \mathtt{dostane}(x,y)) \\ \Leftrightarrow\ & \forall x(\mathtt{dobré}(x) \lor \forall y\, \neg\mathtt{dostane}(x,y)) \end{aligned}$$

Skolemizácia

Skolemizácia (podľa nórskeho logika Thoralfa Skolema) je úprava formuly X v NNF, ktorou nahradíme existenčné kvantifikátory **novými** konštantami alebo funkčnými symbolmi.

Podobá sa pravidlu δ v tablách,
ale aplikuje sa naraz na všetky kvantifikátory.

Výsledná formula je v novom, **rozšírenom jazyku**.

Nie je ekvivalentná s pôvodnou, ale je **ekvisplniteľná**.

Definícia 14.16 (Prvorádová ekvi*splniteľnosť*)

Množiny formúl S a T
sú *(prvorádovo) rovnako splniteľné* (*ekvisplniteľné*, equisatisfiable) vtt
S má model vtt T má model.

Skolemizácia — skolemovská konštanta

Ľahký prípad (v podstate pravidlo δ):

Vo formule X sa vyskytuje $\exists y\, A$ mimo všetkých oblastí platnosti všeobecných kvantifikátorov.

1. Pridáme do jazyka novú, *skolemovskú konštantu* c (nebola doteraz v jazyku v žiadnej úlohe).
2. Každý výskyt podformuly $\exists y\, A$ v X mimo všetkých oblastí platnosti všeobecných kvantifikátorov nahradíme formulou

$$A\{y \mapsto c\}$$

Pomenujeme objekt, ktorý existuje podľa $\exists y\, A$.

Príklad 14.17

$\exists x\,(\mathtt{dobré}(x) \land \mathtt{dieťa}(x))$

$\rightsquigarrow \mathtt{dobré}(\mathtt{nejaké\_dobré\_dieťa}) \land \mathtt{dieťa}(\mathtt{nejaké\_dobré\_dieťa})$

Skolemizácia — skolemovská funkcia

Vo formule X sa vyskytuje $\exists y\, A$ v oblasti platnosti všeobecných kvantifikátorov premenných $x_1, \ldots, x_n$:

$$X = \cdots \forall x_1(\cdots \forall x_2(\cdots \forall x_n(\cdots \exists y\, A \cdots) \cdots) \cdots) \cdots$$

1. Pridáme do jazyka nový funkčný symbol, *skolemovskú funkciu* f.
2. Každý výskyt $\exists y\, A$ v X v oblasti platnosti kvantifikátorov $\forall x_1$, $\ldots$, $\forall x_n$ nahradíme formulou

$$A\{y \mapsto f(x_1, x_2, \ldots, x_n)\}$$

Pomenujeme priradenie objektu y objektom $x_1, \ldots, x_n$.

Príklad 14.18

$$\forall x(\,\neg\mathtt{dobré}(x) \lor \neg\mathtt{dieťa}(x) \lor \exists y(\mathtt{dostane}(x, y) \land \mathtt{darček}(y))\,)$$

$$\rightsquigarrow \forall x(\,\neg\mathtt{dobré}(x) \lor \neg\mathtt{dieťa}(x) \lor$$
$$(\mathtt{dostane}(x, \mathtt{darček\_pre}(x)) \land \mathtt{darček}(\mathtt{darček\_pre}(x)))\,)$$

Skolemizácia

Tvrdenie 14.19

Pre každú uzavretú formulu X v jazyku $\mathcal{L}$ existuje formula Y vo vhodnom rozšírení $\mathcal{L}'$ jazyka $\mathcal{L}$ taká, že Y neobsahuje existenčné kvantifikátory a X a Y sú ekvisplniteľné.

Príklad 14.20

$$\begin{aligned}\exists z\Big(R(z,z) \land \forall x\big(\neg R(x,z) &\lor \exists u(R(x,u) \land R(u,z))\\ &\lor \forall y\, \exists v(\neg R(y,v) \land R(x,v))\\ &\lor \exists v\, \forall w(R(x,v) \land R(v,w))\big)\Big)\end{aligned}$$

$\rightsquigarrow \ldots ?$

Konverzia do PNF

Definícia 14.21

Formula X je v ***prenexnom normálnom tvare*** (PNF) vtt
má tvar $Q_1 x_1\, Q_2 x_2 \cdots Q_n x_n\, A$, kde $Q_i \in \{\forall, \exists\}$, x_i je premenná
a A je formula bez kvantifikátorov (***matica*** formuly X).

Skolemizovanú formulu v NNF upravíme do PNF
opakovanou aplikáciou nasledujúcich transformácií:

- ak x **nemá voľný výskyt** v B,

$$(\forall x\, A \land B) \Leftrightarrow \forall x\, (A \land B) \qquad (B \land \forall x\, A) \Leftrightarrow \forall x\, (B \land A)$$
$$(\forall x\, A \lor B) \Leftrightarrow \forall x\, (A \lor B) \qquad (B \lor \forall x\, A) \Leftrightarrow \forall x\, (B \lor A)$$

- ak sa x má voľný výskyt v B a y je **nová** premenná,

$$(\forall x\, A \land B) \Leftrightarrow (\forall y\, A\{x \mapsto y\} \land B) \quad (B \land \forall x\, A) \Leftrightarrow (B \land \forall y\, A\{x \mapsto y\})$$
$$(\forall x\, A \lor B) \Leftrightarrow (\forall y\, A\{x \mapsto y\} \lor B) \quad (B \lor \forall x\, A) \Leftrightarrow (B \lor \forall y\, A\{x \mapsto y\})$$

Konverzia do PNF

Tvrdenie 14.22

Pre každú formulu X v NNF bez existenčných kvantifikátorov existuje ekvivalentná formula Y v PNF a NNF.

Príklad 14.23

$$\forall x(\,\mathtt{dobr\acute{e}}(x) \lor \forall y\,\neg\mathtt{dostane}(x, y)\,)$$
$$\Leftrightarrow \forall x\,\forall y\,(\,\mathtt{dobr\acute{e}}(x) \lor \neg\mathtt{dostane}(x, y)\,)$$

Pozor! Pre ekvivalentnosť prenexovania je nutné, aby boli premenné viazané rôznymi kvantifikátormi rôzne:

$$(\forall x\, A(x) \lor \forall x\, B(x)) \not\Leftrightarrow \forall x\,(A(x) \lor B(x))$$

$$(\forall x\, A(x) \lor \forall x\, B(x)) \Leftrightarrow \forall x(\,A(x) \lor \forall x\, B(x)\,)$$
$$\Leftrightarrow \forall x\,\forall y\,(\,A(x) \lor B(y)\,)$$

Prenexujte **po jednom** alebo premenujte premenné (ešte pred skolemizáciou)

Konverzia do CNF

Maticu (najväčšiu podformulu bez kvantifikátorov) formuly v PNF upravíme do CNF pomocou distributívnosti a komutatívnosti disjunkcie:

$$(A \lor (X \land Y)) \Leftrightarrow ((A \lor X) \land (A \lor Y))$$
$$((X \land Y) \lor A) \Leftrightarrow ((X \lor A) \land (Y \lor A))$$

Príklad 14.24

$$\forall x(\, \neg\mathtt{dobr\acute{e}}(x) \lor \neg\mathtt{die\check{t}a}(x) \lor (\mathtt{dostane}(x, \mathtt{dar\check{c}ek\_pre}(x)) \land \mathtt{dar\check{c}ek}(\mathtt{dar\check{c}ek\_pre}(x)))\,)$$
$$\Leftrightarrow \forall x(\,(\neg\mathtt{dobr\acute{e}}(x) \lor \neg\mathtt{die\check{t}a}(x) \lor \mathtt{dostane}(x, \mathtt{dar\check{c}ek\_pre}(x))) \land (\neg\mathtt{dobr\acute{e}}(x) \lor \neg\mathtt{die\check{t}a}(x) \lor \mathtt{dar\check{c}ek}(\mathtt{dar\check{c}ek\_pre}(x)))\,)$$

Konverzia do klauzálnej teórie

Formula, ktorej matica je v CNF, je ekvivalentná s konjunkciou klauzúl:

$$\forall x(A \land B) \Leftrightarrow (\forall x\, A \land \forall x\, B)$$

a konjunkcia klauzúl je ekvivalentná s ich množinou:

$$\{(\forall x\, A \land \forall x\, B)\} \Leftrightarrow \{\forall x\, A, \forall x\, B\}$$

Príklad 14.25

$$\begin{aligned}
&\{\forall x(\,(\neg\mathtt{dobré}(x) \lor \neg\mathtt{dieťa}(x) \lor \mathtt{dostane}(x, \mathtt{darček_pre}(x))) \land \\
&\qquad (\neg\mathtt{dobré}(x) \lor \neg\mathtt{dieťa}(x) \lor \mathtt{darček}(\mathtt{darček_pre}(x)))\,)\} \\
\Leftrightarrow\ &\{(\,\forall x(\neg\mathtt{dobré}(x) \lor \neg\mathtt{dieťa}(x) \lor \mathtt{dostane}(x, \mathtt{darček_pre}(x))) \land \\
&\quad \forall x(\neg\mathtt{dobré}(x) \lor \neg\mathtt{dieťa}(x) \lor \mathtt{darček}(\mathtt{darček_pre}(x)))\,)\} \\
\Leftrightarrow\ &\{\forall x(\neg\mathtt{dobré}(x) \lor \neg\mathtt{dieťa}(x) \lor \mathtt{dostane}(x, \mathtt{darček_pre}(x))), \\
&\quad \forall x(\neg\mathtt{dobré}(x) \lor \neg\mathtt{dieťa}(x) \lor \mathtt{darček}(\mathtt{darček_pre}(x)))\}
\end{aligned}$$

Konverzia do klauzálnej teórie

Veta 14.26

Ku každej teórii T v jazyku logiky prvého rádu $\mathcal{L}$ existuje ekvisplniteľná klauzálna teória v nejakom rozšírení $\mathcal{L}'$ jazyka $\mathcal{L}$ o Skolemove konštanty a funkcie.

Príklad 14.27

$$\left\{\begin{array}{l}\forall x\,(\mathtt{dobré}(x) \land \mathtt{dieťa}(x) \rightarrow \exists y(\mathtt{dostane}(x,y) \land \mathtt{darček}(y))),\\ \exists x\,(\mathtt{dobré}(x) \land \mathtt{dieťa}(x)),\\ \forall x\,(\neg\mathtt{dobré}(x) \rightarrow \neg\exists y\,\mathtt{dostane}(x,y))\end{array}\right\} \rightsquigarrow$$

$$\left\{\begin{array}{l}\forall x_1(\neg\mathtt{dobré}(x_1) \lor \neg\mathtt{dieťa}(x_1) \lor \mathtt{dostane}(x_1, \mathtt{darček\_pre}(x_1))),\\ \forall x_2(\neg\mathtt{dobré}(x_2) \lor \neg\mathtt{dieťa}(x_2) \lor \mathtt{darček}(\mathtt{darček\_pre}(x_2))),\\ \mathtt{dobré}(\mathtt{nejaké\_dobré\_dieťa}), \mathtt{dieťa}(\mathtt{nejaké\_dobré\_dieťa}),\\ \forall x_3\,\forall y\,(\mathtt{dobré}(x_3) \lor \neg\mathtt{dostane}(x_3, y))\end{array}\right\}$$

Konverzia do prvorádovej CNF

Dôkaz/algoritmus

T_{I}: Implikácie nahradíme disjunkciami.

T_{N}: *Negačný normálny tvar* (NNF): Presunieme negácie k atómom.

T_{V}: Premenujeme premenné tak,
aby každý kvantifikátor viazal inú premennú ako ostatné kvantifikátory.

T_{S}: *Skolemizácia*: Existenčné kvantifikátory nahradíme substitúciou nimi viazaných premenných za Skolemove konštanty/aplikácie Skolemovych funkcií na všeobecne príslušné kvantifikované premenné.

T_{P}: *Prenexný normálny tvar* (PNF):
presunieme všeobecné kvantifikátory na začiatok formuly.

T_{D}: *Konjunktívny normálny tvar* (CNF): distribuujeme disjunkcie do konjunkcií.

T_{K}: Odstránime konjunkcie rozdelením konjunktov do samostatne kvantifikovaných klauzúl.

Rezolvencia

Rezolvencia v logike prvého rádu

Prvorádovou rezolvenciou budeme odvodzovať dôsledky klauzálnych teórií.

Dohoda 14.28

Všeobecné kvantifikátory v zápise klauzúl budeme zanedbávať.

Teda namiesto $\forall x_1 \cdots \forall x_n (L_1 \lor \cdots \lor L_m)$ píšeme iba $L_1 \lor \cdots \lor L_m$.

Úsudky s klauzulami

Príklad 14.29

- Každého má niekto rád: $\forall y\, \mathtt{má\_rád}(\mathtt{obdivovateľ}(y), y)$,
  teda aj Dadu má niekto rád: $\mathtt{má\_rád}(\mathtt{obdivovateľ}(\mathtt{Dada}), \mathtt{Dada})$
- Kto má rád Dadu, toho nemá rád Edo:

  $$\forall x(\neg\mathtt{má\_rád}(x, \mathtt{Dada}) \lor \neg\mathtt{má\_rád}(\mathtt{Edo}, x)),$$

  ak Dadan obdivovateľ má rád Dada, tak ho Edo má rád:

  $$\neg\mathtt{má\_rád}(\mathtt{obdivovateľ}(\mathtt{Dada}), \mathtt{Dada}) \lor \neg\mathtt{má\_rád}(\mathtt{Edo}, \mathtt{obdivovateľ}(\mathtt{Dada})).$$

- Preto (výrokovou rezolvenciou):

  $$\frac{\begin{array}{c}\mathtt{má\_rád}(\mathtt{obdivovateľ}(\mathtt{Dada}), \mathtt{Dada}) \\ \big(\neg\,\mathtt{má\_rád}(\mathtt{obdivovateľ}(\mathtt{Dada}), \mathtt{Dada}) \\ \quad \lor\neg\mathtt{má\_rád}(\mathtt{Edo}, \mathtt{obdivovateľ}(\mathtt{Dada}))\big)\end{array}}{\neg\mathtt{má\_rád}(\mathtt{Edo}, \mathtt{obdivovateľ}(\mathtt{Dada}))}$$

Úsudky s klauzulami

Celý úsudok z príkladu aj s dosadeniami:

$$\frac{\forall y\, \texttt{má\_rád}(\texttt{obdivovateľ}(y), y) \quad \forall x(\neg\texttt{má\_rád}(x, \texttt{Dada}) \lor \neg\texttt{má\_rád}(\texttt{Edo}, x))}{\neg\texttt{má\_rád}(\texttt{Edo}, \texttt{obdivovateľ}(\texttt{Dada}))}$$

Aby sme klauzuly mohli rezolvovať, potrebovali sme substitúciu:

$$\sigma = \{x \mapsto \texttt{obdivovateľ}(\texttt{Dada}), y \mapsto \texttt{Dada}\}$$

Po substitúcii σ majú komplementárne literály rovnaké argumenty predikátu:

$$\texttt{má\_rád}(\texttt{obdivovateľ}(y), y)\sigma = \texttt{má\_rád}(\texttt{obdivovateľ}(\texttt{Dada}), \texttt{Dada})$$
$$\neg\texttt{má\_rád}(x, \texttt{Dada})\sigma = \neg\texttt{má\_rád}(\texttt{obdivovateľ}(\texttt{Dada}), \texttt{Dada})$$

Unifikátory

Definícia 14.30

Nech A, B sú postupnosti symbolov, σ je substitúcia.

Substitúcia σ je *unifikátorom* A a B vtt $A\sigma = B\sigma$.

Príklad 14.31

- $A_1 = \mathtt{má\_rád}(\mathtt{filantrop}, y)$, $B_1 = \mathtt{má\_rád}(x, \mathtt{Dada})$,
  $\sigma_1 = \{x \mapsto \mathtt{filantrop}, y \mapsto \mathtt{Dada}\}$
- $A_2 = \mathtt{má\_rád}(\mathtt{obdivovateľ}(y), y)$, $B_2 = \mathtt{má\_rád}(x, \mathtt{Dada})$,

Unifikátory

Definícia 14.30

Nech A, B sú postupnosti symbolov, σ je substitúcia.

Substitúcia σ je *unifikátorom* A a B vtt $A\sigma = B\sigma$.

Príklad 14.31

- $A_1 = \texttt{má\_rád}(\texttt{filantrop}, y)$, $B_1 = \texttt{má\_rád}(x, \texttt{Dada})$,
  $\sigma_1 = \{x \mapsto \texttt{filantrop}, y \mapsto \texttt{Dada}\}$
- $A_2 = \texttt{má\_rád}(\texttt{obdivovateľ}(y), y)$, $B_2 = \texttt{má\_rád}(x, \texttt{Dada})$,
  $\sigma_2 = \{x \mapsto \texttt{obdivovateľ}(\texttt{Dada}), y \mapsto \texttt{Dada}\}$
- $A_3 = \texttt{má\_rád}(\texttt{obdivovateľ}(y), y)$, $B_3 = \texttt{má\_rád}(\texttt{Edo}, x)$,

Unifikátory

Definícia 14.30

Nech A, B sú postupnosti symbolov, σ je substitúcia.

Substitúcia σ je *unifikátorom* A a B vtt $A\sigma = B\sigma$.

Príklad 14.31

- $A_1 = \mathtt{má\_rád}(\mathtt{filantrop}, y)$, $B_1 = \mathtt{má\_rád}(x, \mathtt{Dada})$,
  $\sigma_1 = \{x \mapsto \mathtt{filantrop}, y \mapsto \mathtt{Dada}\}$
- $A_2 = \mathtt{má\_rád}(\mathtt{obdivovateľ}(y), y)$, $B_2 = \mathtt{má\_rád}(x, \mathtt{Dada})$,
  $\sigma_2 = \{x \mapsto \mathtt{obdivovateľ}(\mathtt{Dada}), y \mapsto \mathtt{Dada}\}$
- $A_3 = \mathtt{má\_rád}(\mathtt{obdivovateľ}(y), y)$, $B_3 = \mathtt{má\_rád}(\mathtt{Edo}, x)$,
  $\sigma_3 =$??? **neexistuje!**
- $A_4 = \mathtt{má\_rád}(\mathtt{obdivovateľ}(y), y)$, $B_4 = \mathtt{má\_rád}(x, x)$,

Unifikátory

Definícia 14.30

Nech A, B sú postupnosti symbolov, σ je substitúcia.

Substitúcia σ je *unifikátorom* A a B vtt $A\sigma = B\sigma$.

Príklad 14.31

- $A_1 = \mathtt{má\_rád}(\mathtt{filantrop}, y)$, $B_1 = \mathtt{má\_rád}(x, \mathtt{Dada})$,
  $\sigma_1 = \{x \mapsto \mathtt{filantrop}, y \mapsto \mathtt{Dada}\}$
- $A_2 = \mathtt{má\_rád}(\mathtt{obdivovateľ}(y), y)$, $B_2 = \mathtt{má\_rád}(x, \mathtt{Dada})$,
  $\sigma_2 = \{x \mapsto \mathtt{obdivovateľ}(\mathtt{Dada}), y \mapsto \mathtt{Dada}\}$
- $A_3 = \mathtt{má\_rád}(\mathtt{obdivovateľ}(y), y)$, $B_3 = \mathtt{má\_rád}(\mathtt{Edo}, x)$,
  $\sigma_3 = ???$ **neexistuje!**
- $A_4 = \mathtt{má\_rád}(\mathtt{obdivovateľ}(y), y)$, $B_4 = \mathtt{má\_rád}(x, x)$,
  $\sigma_4 = ???$ **neexistuje!**

Skladanie substitúcií, premenovanie premenných

Definícia 14.32

Nech $\sigma = \{x_1 \mapsto t_1, \dots, x_n \mapsto t_n\}$ a $\theta = \{y_1 \mapsto s_1, \dots, y_m \mapsto s_m\}$ sú substitúcie.

Zložením (kompozíciou) substitúcií σ a θ je substitúcia
$\sigma\theta = \{x_1 \mapsto t_1\theta, \dots, x_n \mapsto t_n\theta, y_{i_1} \mapsto s_{i_1}, \dots, y_{i_k} \mapsto s_{i_k}\}$,
kde $\{y_{i_1}, \dots, y_{i_k}\} = \{y_1, \dots, y_m\} \setminus \{x_1, \dots, x_n\}$.

Príklad 14.33

$$\sigma = \{x \mapsto \mathtt{obdivovateľ}(y),\ z \mapsto y\}$$

$$\theta = \{y \mapsto \mathtt{filantrop}\}$$

$$\begin{aligned}\sigma\theta = \{&x \mapsto \mathtt{obdivovateľ}(\mathtt{filantrop}),\\ &z \mapsto \mathtt{filantrop},\ y \mapsto \mathtt{filantrop}\}\end{aligned}$$

Unifikátory

Definícia 14.34

Nech A, B sú postupnosti symbolov, σ a θ sú substitúcie.

σ je *všeobecnejšia* ako θ vtt existuje subst. γ taká, že $\theta = \sigma\gamma$.

σ je *najvšeobecnejším unifikátorom* A a B vtt

- σ je unifikátorom A a B a zároveň
- pre každý unifikátor θ A a B je σ všeobecnejšia ako θ.

Príklad 14.35

$A_5 = \mathtt{má\_rád}(\mathtt{obdivovateľ}(x), y)$, $B_5 = \mathtt{má\_rád}(u, v)$

- $\sigma_{51} = \{u \mapsto \mathtt{obdivovateľ}(\mathtt{Dada}), v \mapsto y, x \mapsto \mathtt{Dada}\}$
  $\theta_{51} = \{u \mapsto \mathtt{obdivovateľ}(\mathtt{Dada}), v \mapsto \mathtt{Biba}, x \mapsto \mathtt{Dada}, y \mapsto \mathtt{Biba}\}$
  $\gamma_{51} = \{y \mapsto \mathtt{Biba}\}$
- $\sigma_{52} = \{u \mapsto \mathtt{obdivovateľ}(x), v \mapsto y\}$
  $\theta_{52} = \{u \mapsto \mathtt{obdivovateľ}(\mathtt{Dada}), v \mapsto y, x \mapsto \mathtt{Dada}\}$
  $\gamma_{52} = \{x \mapsto \mathtt{Dada}\}$

Príklad 14.36

$$\frac{\mathtt{má\_rád}(\mathtt{obdivovateľ}(y), y)\sigma \qquad (\neg\mathtt{má\_rád}(x, \mathtt{Dada}) \lor \neg\mathtt{má\_rád}(\mathtt{Edo}, x))\sigma}{\neg\mathtt{má\_rád}(\mathtt{Edo}, x)\sigma}$$

$$\sigma = \{x \mapsto \mathtt{obdivovateľ}(\mathtt{Dada}), y \mapsto \mathtt{Dada}\}$$

$$\frac{\mathtt{má\_rád}(\mathtt{obdivovateľ}(\mathtt{Dada}), \mathtt{Dada}) \qquad \neg\mathtt{má\_rád}(\mathtt{obdivovateľ}(\mathtt{Dada}), \mathtt{Dada}) \lor \neg\mathtt{má\_rád}(\mathtt{Edo}, \mathtt{obdivovateľ}(\mathtt{Dada}))}{\neg\mathtt{má\_rád}(\mathtt{Edo}, \mathtt{obdivovateľ}(\mathtt{Dada}))}$$

Príklad 14.37

Rovnaké premenné v klauzulách môžu zabrániť unifikácii literálov:

$$\mathtt{má\_rád}(\mathtt{obdivovateľ}(x), x) \quad \neg\mathtt{má\_rád}(x, \mathtt{Dada}) \lor \neg\mathtt{má\_rád}(\mathtt{Edo}, x)$$

Klauzuly sú však všeobecne kvantifikované nezávisle od seba.

Premenovanie premenných v jednej z nich nezmení jej význam, ale umožní unifikáciu (viď predchádzajúci príklad).

$$\mathtt{má\_rád}(\mathtt{obdivovateľ}(y), y) \quad \neg\mathtt{má\_rád}(x, \mathtt{Dada}) \lor \neg\mathtt{má\_rád}(\mathtt{Edo}, x)$$

Definícia 14.38

Premenovaním premenných je každá substitúcia $\sigma = \{x_1 \mapsto y_1, \dots, x_n \mapsto y_n\}$, kde $y_1, \dots, y_n$ sú premenné.

Prvorádová rezolvencia — pravidlá

Definícia 14.39

Nech C a D sú prvorádové klauzuly, nech A a B sú atómy, nech L a K sú literály.

Rezolvencia (angl. resolution) je odvodzovacie pravidlo

$$\frac{A \lor C \qquad \neg B \lor D}{(C\theta \lor D)\sigma} \qquad \begin{array}{l}\sigma \text{ je unifikátor } A\theta \text{ a } B,\\ \theta \text{ je premenovanie premenných.}\end{array}$$

Faktorizácia (angl. factoring) je odvodzovacie pravidlo

$$\frac{L \lor K \lor C}{(L \lor C)\sigma} \qquad \sigma \text{ je unifikátor } L \text{ a } K.$$

Faktorizácia je zovšeobecnenie idempotencie pri výrokovej rezolvencii.

Rezolvenčné odvodenie a zamietnutie

Definícia 14.40

Nech T je klauzálna teória.

Rezolvenčným odvodením z T je každá konečná postupnosť klauzúl $\mathcal{Z} = (C_1, C_2, \dots, C_n)$, kde každá klauzula C_i, $1 \leq i \leq n$, je:

- prvkom T, alebo
- odvodená pravidlom rezolvencie z klauzúl C_j a C_k, ktoré sa v $\mathcal{Z}$ nachádzajú pred C_i (teda $j, k < i$), alebo
- odvodená pravidlom faktorizácie z klauzuly C_j, ktorá sa v $\mathcal{Z}$ nachádza pred C_i (teda $j < i$).

Zamietnutím T (angl. refutation) je každé rezolvenčné odvodenie $\mathcal{Z} = (C_1, C_2, \dots, C_n)$, kde $C_n = \square$.

Refutačná korektnosť a úplnosť rezolvencie

Veta 14.41 (Refutačná korektnosť a úplnosť rezolvencie)

Nech T je klauzálna teória.

Potom existuje zamietnutie $\{C_1, \ldots, C_n\}$ vtt T je nesplniteľná.

Príklad 14.42

Dokážme nesplniteľnosť:

$$\left\{\begin{array}{c} \forall x\, \texttt{má\_rád}(\texttt{obdivovateľ}(x), x), \\ \forall x\, \forall y\, \texttt{má\_rád}(x, \texttt{obdivovateľ}(y)), \\ \forall x(\neg \texttt{má\_rád}(x, \texttt{Dada}) \lor \neg \texttt{má\_rád}(\texttt{Edo}, x)) \end{array}\right\}$$

Pretože každú teóriu môžeme transformovať na ekvisplniteľnú klauzálnu teóriu, dostávame:

Dôsledok 14.43 (Úplnosť rezolvencie)

Nech T je konečná teória, nech X je uzavretá formula.
Nech $T'_X = \{C_1, \dots, C_n\}$ je klauzálna teória ekvisplniteľná s $T \cup \{\neg X\}$.
Potom z T vyplýva X vtt existuje zamietnutie T'_X.