Rezolvencia

11. prednáška
Logika pre informatikov a Úvod do matematickej logiky

Ján Kľuka, Ján Mazák, Jozef Šiška

Letný semester 2024/2025

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

Obsah 11. prednášky

- Rezolvencia
  - Rezolvencia vo výrokovej logike
  - Prevod do klauzálnej teórie a skolemizácia
  - Rezolvencia v logike prvého rádu

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 $O(2^n \cdot f)$ pre n atómov a formulu dĺžky f.

Logika prvého rádu **nie je rozhodnuteľná**
(ak by bola, vedeli by sme riešiť problém zastavenia — viac nabudúce).

Vďaka tomu, že je úplná, však ku každému pravdivému tvrdeniu (vyplývaniu formuly z teórie) existuje dôkaz. Možno preto postupne enumerovať všetky dôkazy, až kým nenájdeme vyhovujúci. Problém vyplývania v prvorádovej logike je teda **čiastočne rozhodnuteľný**.

Dokazovací systém má podstatný vplyv na to, ako dlho v praxi potrvá nájdenie dôkazu (a či nám vystačí dostupná pamäť).

Ako fungujú automatické dokazovače v logike prvého rádu

Prvé automatické dokazovače využívali prvorádovú verziu DPLL.

Niektoré automatické dokazovače využívajú modifikované tablá.

Väčšina automatických dokazovačov (napr. Prover9 a Vampire)
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:

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

Rezolvencia

Predchádzajúce pravidlo sa dá zovšeobecniť na ľub. dvojicu 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 ľub. literály $K_1, \dots, K_m, L_1, \dots, L_n$.

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. (Rezolventa je pravdivá v každom ohodnotení, v ktorom sú pravdivé pôvodné klauzuly.)

Špeciálne prípady rezolvencie

Viacero pravidiel sa dá chápať ako špeciálne prípady rezolvencie:

$$\frac{(\neg A \lor B) \quad (\neg B \lor C)}{(\neg A \lor C)} \qquad \frac{(A \to B) \quad (B \to C)}{(A \to C)} \qquad \text{(HS)}$$

$$\frac{(\neg A \lor B) \quad A}{B} \qquad \frac{(A \to B) \quad A}{B} \qquad \text{(MP)}$$

$$\frac{(\neg A \lor B) \quad \neg B}{\neg A} \qquad \frac{(A \to B) \quad \neg B}{\neg A} \qquad \text{(MT)}$$

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:

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

  vtedy premisy nie sú súčasne splniteľné

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

Častá chyba pri rezolvencii

Niektoré dvojice klauzúl možno rezolvovať na viacerých literáloch:

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

ale **je chyba urobiť to naraz**:

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

Toto **nie je** inštancia rezolvencie ani korektný úsudok.

Prečo?

Častá chyba pri rezolvencii

Niektoré dvojice klauzúl možno rezolvovať na viacerých literáloch:

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

ale je chyba urobiť to naraz:

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

Toto nie je inštancia rezolvencie ani korektný úsudok.

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.

Rezolvenčné odvodenie a problém

Opakovaním rezolvencie môžeme odvodzovať ďalšie dôsledky:

Príklad 14.3

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

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

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

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

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

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

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

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

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

$\vdots$

Problematické prípady

Odvodeniami v príklade dostaneme iba existujúce alebo nové **dvojprvkové** klauzuly ($(A \lor A)$, $(B \lor C)$, $(B \lor B)$, $\dots$) ale žiadnu jednotkovú, lebo rezolventa má $m + n - 2$ literálov.

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

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

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

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 $C_1, C_2, \dots, C_n, \dots$, 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)

Množine klauzúl budeme hovoriť aj *klauzálna teória*.

Tvrdenie 14.6

Ak pre klauzálnu teóriu S existuje zamietnutie, je nesplniteľná.

(Ak by nejaké ohodnotenie bolo modelom S, bolo by vďaka korektnosti pravidla rezolvencie modelom každej odvodenej klauzuly, vrátane nesplniteľnej prázdnej.)

Vyskúšajte si 14.1

Dokážte nesplniteľnosť
$S = \{(A \lor B \lor \neg C), (\neg A \lor \neg C), (A \lor \neg B), (\neg A \lor C), (A \lor B \lor C)\}$.

Rezolvencia a SAT

Možno pomocou rezolvencie znížiť počet atómov?

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

Preskúmajme nasledovný postup na hľadanie spĺňajúceho ohodnotenia:

- Ak v nejakej klauzule je A, v inej $\neg A$, spravíme na nich rezolvenciu. Ak odvodíme $\square$, vstupná formula je nesplniteľná.
- Ak už také dvojice nie sú, tak A alebo $\neg A$ je nezmiešaný literál, a preto vieme, ako A ohodnotiť.
  Takto sme sa úplne zbavili atómu A.
- Toto zopakujeme postupne s ďalšími atómami, až kým nenájdeme spĺňajúce ohodnotenie.

Je tento postup polynomiálnym algoritmom pre SAT?

Ak uvedený postup vedie k zamietnutiu, ohodnotenie neexistuje. Ohodnotenie nájdené po eliminácii atómu popísaným spôsobom však nemusí vyhovovať pôvodným klauzulám!

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

Rezolvencia a SAT

Ak uvedený postup vedie k zamietnutiu, ohodnotenie neexistuje. Ohodnotenie nájdené po eliminácii atómu popísaným spôsobom však nemusí vyhovovať pôvodným klauzulám!

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

Spodné klauzuly sú pravdivé pri ohodnotení $\{A \mapsto f, B \mapsto f, C \mapsto t\}$, kým vrchné nie.

Postup sa však dá upraviť, aby fungoval. Miesto rezolvencie jednej dvojice klauzúl použijeme rezolvenciu **súčasne pre všetky možné dvojice** obsahujúce komplementárne literály s atómom A.

Nahraďme klauzuly S_1 obsahujúce A klauzulami S_2
(X_i, Y_j sú disjunkcie literálov neobsahujúcich A):

$$S_1 = \left\{ \begin{array}{cc} A \lor X_1 & \neg A \lor Y_1 \\ A \lor X_2 & \neg A \lor Y_2 \\ \vdots & \vdots \\ A \lor X_n & \neg A \lor Y_m \end{array} \right\} \quad S_2 = \left\{ \begin{array}{ccc} X_1 \lor Y_1 & \dots & X_n \lor Y_1 \\ \vdots & & \vdots \\ X_1 \lor Y_m & \dots & X_n \lor Y_m \end{array} \right\}$$

Nech T je množina klauzúl, ktoré neobsahujú A.
Predpokladajme, že pre nejaké ohodnotenie v_2 platí $v_2 \models_p S_2 \cup T$.
Nájdeme v_1 také, že $v_1 \models_p S_1 \cup T$:

- Ak $v_2 \not\models_p X_i$ pre nejaké i, tak z $v_2 \models_p X_i \lor Y_j$ vyplýva $v_2 \models_p Y_j$ pre každé j. Vtedy stačí zvoliť $v_1 = v_2 \cup \{A \mapsto t\}$.
- Ak pre každé i platí $v_2 \models_p X_i$, zvolíme $v_1 = v_2 \cup \{A \mapsto f\}$.

Týmto nepokazíme splnenie klauzúl v T, lebo neobsahujú A.

Naopak, ak ohodnotenie v_1 je modelom $S_1 \cup T$, tak $v_1 \vDash_\mathrm{p} S_2 \cup T$: Ak $v_1(A) = t$, tak $v_1 \vDash_\mathrm{p} Y_j$ pre všetky j, preto $v_1 \vDash_\mathrm{p} S_2$.
Podobne pre $v_1(A) = f$.

Takto sme naozaj znížili počet atómov;
podobné postupy sa využívajú pri predspracovaní vstupu pre SAT.
(Čo sa stane s veľkosťou klauzúl?)

Počet pridaných klauzúl však môže narásť exponenciálne,
preto sme polynomiálny algoritmus pre SAT nezískali.

Úplnosť rezolvencie

Využitím uvedeného postupu vieme dokázať úplnosť rezolvencie.

Tvrdenie 14.7 (Úplnosť rezolvencie)

Ak je klauzálna teória S nesplniteľná, existuje jej zamietnutie.

Dôkaz.

Uvažujme nesplniteľnú klauzálnu teóriu a rozdeľme jej klauzuly na dve množiny: v S_1 budú tie, čo obsahujú atóm A, v T ostatné. Každú klauzulu z S_2 vieme odvodiť z S_1 pomocou pravidla pre rezolvenciu. Ako sme ukázali, množina $T \cup S_1$ je nesplniteľná vtt $T \cup S_2$ je nesplniteľná. Zároveň $T \cup S_2$ má o jeden atóm menej.
Opakovaním postupu nájdeme nesplniteľnú množinu klauzúl, ktorá má už len nezmiešané literály. Preto v nej musí byť aj $\square$.

$\square$

(Kde v dôkaze využívame idempotenciu?)

Pomocou rezolvencie vieme rozhodovať splniteľnosť.

Veta 14.8 (Korektnosť a úplnosť rezolvencie)

Nech S je klauzálna teória.

S je výrokovologicky nesplniteľná vtt existuje zamietnutie S.

Pomocou rezolvencie možno rozhodovať aj výrokovologické vyplývanie formuly X z teórie T: vieme, že $T \vDash X$ vtt $T \cup \{\neg X\}$ je nesplniteľná. Aby sme mohli použiť rezolvenciu, ostáva previesť všetky formuly z T aj $\neg X$ do CNF (čo sa vždy dá).

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?

Prvorádové klauzuly a klauzálne teórie

Ujasnime si najprv, aký tvar chceme dosiahnuť.

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 $L_1, \ldots, L_n$ sú literály a $x_1, \ldots, x_k$ sú **všetky** voľné premenné formuly $L_1 \lor \cdots \lor L_n$. Klauzula môže byť aj *jednotková* ($\forall \vec{x}\, L_1$) alebo *prázdna* ($\square$).

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

Prvorádová ekvivalencia

Postupovať budeme podobne ako vo výrokovologickom prípade: Postupne odstránime z teórie implikácie, negácie zložených formúl, existenčné kvantifikátory, disjunkcie konjunkcií, vnorené všeobecné kvantifikátory.

Podľa možnosti budeme používať ekvivalentné úpravy v prvorádovom zmysle:

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 $(\neg A \vee B)$.

Príklad 14.12

$$\begin{aligned} &\forall x(\texttt{dobré}(x) \wedge \texttt{dieťa}(x) \to \exists y(\texttt{dostane}(x, y) \wedge \texttt{darček}(y))) \\ \Leftrightarrow\ &\forall x(\neg(\texttt{dobré}(x) \wedge \texttt{dieťa}(x)) \vee \exists y(\texttt{dostane}(x, y) \wedge \texttt{darček}(y))) \end{aligned}$$

$$\begin{aligned} &\forall x(\neg\texttt{dobré}(x) \to \neg\exists y\, \texttt{dostane}(x, y)) \\ \Leftrightarrow\ &\forall x(\neg\neg\texttt{dobré}(x) \vee \neg\exists y\, \texttt{dostane}(x, y)) \end{aligned}$$

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 Morganových 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 Morganových 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 existenčné 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 práve vtedy, keď 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 (symbol c doteraz nebol v jazyku v žiadnej úlohe).
2. Každý výskyt podformuly $\exists y\, A$ v X mimo všetkých oblastí platnosti všeobecných kvantifikátorov nahradíme formulou

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

Konštanta c pomenúva 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 $\forall x_1$, …, $\forall x_n$ nahradíme formulou

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

Funkcia f **pomenúva priradenie** objektu y objektom $x_1, \ldots, x_n$.

Príklad 14.18

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

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

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

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

$$
\begin{aligned}
\rightsquigarrow\ & R(c,c) \land \forall x\big(\neg R(x,c) \lor (R(x,f_1(x)) \land R(f_1(x),c))\\
&\qquad \lor \forall y\big(\neg R(y,f_2(x,y)) \land R(x,f_2(x,y))\big)\\
&\qquad \lor \forall w\big(R(x,f_3(x)) \land R(f_3(x),w)\big)\big)
\end{aligned}
$$

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 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

$$\forall x(\,\mathtt{dobré}(x) \lor \forall y\,\neg\mathtt{dostane}(x, y)\,)$$
$$\Leftrightarrow \forall x\,\forall y\,(\,\mathtt{dobré}(x) \lor \neg\mathtt{dostane}(x, y)\,)$$

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

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

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

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

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

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

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

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 skolemovské konštanty a funkcie.

Príklad 14.27

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

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

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 skolemovské konštanty/aplikácie skolemovských funkcií na príslušné všeobecne kvantifikované premenné.

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

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

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

Skolemizácia vytvorí ekvisplniteľnú teóriu, ostatné úpravy sú ekvivalentné.

Rezolvencia

Rezolvencia v logike prvého rádu

Rezolvencia a skrátenie zápisu

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 $L_1 \lor \cdots \lor L_m$.

Pozor: konštanty a premenné treba naďalej striktne rozlišovať,
za konštanty nie je možné dosádzať iné termy!

Príklad 14.29

Každého má niekto rád — jeho najlepší kamarát/najlepšia kamarátka (NK):

$$\forall y\, \mathtt{r}(\mathtt{nk}(y), y)$$

Kto má rád Dadu, toho Edo nemá rád:

$$\forall x(\neg \mathtt{r}(x, \mathtt{D}) \lor \neg \mathtt{r}(\mathtt{E}, x)),$$

Teda aj Dadu má niekto rád:

$$\mathtt{r}(\mathtt{nk}(\mathtt{D}), \mathtt{D})$$

Ak Dadin NK má rád Dadu, tak ho Edo nemá rád:

$$\neg \mathtt{r}(\mathtt{nk}(\mathtt{D}), \mathtt{D}) \lor \neg \mathtt{r}(\mathtt{E}, \mathtt{nk}(\mathtt{D})).$$

Preto (výrokovou rezolvenciou):

$$\frac{\begin{array}{l} \mathtt{r}(\mathtt{nk}(\mathtt{D}), \mathtt{D}) \\ \big(\neg\, \mathtt{r}(\mathtt{nk}(\mathtt{D}), \mathtt{D}) \lor \neg \mathtt{r}(\mathtt{E}, \mathtt{nk}(\mathtt{D}))\big) \end{array}}{\neg \mathtt{r}(\mathtt{E}, \mathtt{nk}(\mathtt{D}))}$$

Úsudky s klauzulami

Celý úsudok z príkladu aj s dosadeniami:

$$\frac{\forall y\, \mathtt{r}(\mathtt{nk}(y), y) \qquad \forall x(\neg\mathtt{r}(x, \mathtt{D}) \lor \neg\mathtt{r}(\mathtt{E}, x))}{\neg\mathtt{r}(\mathtt{E}, \mathtt{nk}(\mathtt{D}))}$$

Aby sme klauzuly mohli rezolvovať, použili sme **unifikátor**:

$$\sigma = \{x \mapsto \mathtt{nk}(\mathtt{D}), y \mapsto \mathtt{D}\}$$

Po substitúcii σ majú komplementárne literály rovnaké argumenty predikátu $\mathtt{r}$:

$$\begin{aligned} \mathtt{r}(\mathtt{nk}(y), y)\sigma &= \mathtt{r}(\mathtt{nk}(\mathtt{D}), \mathtt{D}) \\ \neg\mathtt{r}(x, \mathtt{D})\sigma &= \neg\mathtt{r}(\mathtt{nk}(\mathtt{D}), \mathtt{D}) \end{aligned}$$

Ak chceme čo najvšeobecnejší úsudok,
hľadáme **najvšeobecnejší unifikátor**.

Uvedený úsudok predstavuje jeden krok rezolvencie.

Príklad 14.30

$$\frac{\begin{array}{c}\mathrm{r}(\mathrm{nk}(y), y)\sigma \\ (\neg\mathrm{r}(x, \mathrm{D}) \lor \neg\mathrm{r}(\mathrm{E}, x))\sigma\end{array}}{\neg\mathrm{r}(\mathrm{E}, x)\sigma}$$

$$\sigma = \{x \mapsto \mathrm{nk}(\mathrm{D}), y \mapsto \mathrm{D}\}$$

$$\frac{\begin{array}{c}\mathrm{r}(\mathrm{nk}(\mathrm{D}), \mathrm{D}) \\ \neg\,\mathrm{r}(\mathrm{nk}(\mathrm{D}), \mathrm{D}) \lor \neg\mathrm{r}(\mathrm{E}, \mathrm{nk}(\mathrm{D}))\end{array}}{\neg\mathrm{r}(\mathrm{E}, \mathrm{nk}(\mathrm{D}))}$$

Premenovanie premenných

Príklad 14.31

Rovnaké premenné v klauzulách môžu zabrániť unifikácii literálov:

$$\mathtt{r}(\mathtt{nk}(x), x) \qquad\qquad \neg\mathtt{r}(x, \mathtt{D}) \lor \neg\mathtt{r}(\mathtt{E}, x)$$

Klauzuly sú však všeobecne kvantifikované **nezávisle** od seba.
Premenovanie premenných v jednej z nich nezmení jej význam, ale umožní unifikáciu (viď predchádzajúci príklad).

$$\mathtt{r}(\mathtt{nk}(y), y) \qquad\qquad \neg\mathtt{r}(x, \mathtt{D}) \lor \neg\mathtt{r}(\mathtt{E}, x)$$

Definícia 14.32

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 14.33

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

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

Faktorizácia (angl. factoring) je odvodzovacie pravidlo

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

Faktorizácia je zovšeobecnenie idempotencie pri výrokovej rezolvencii.

Rezolvencia postupne

Rezolvenciu

$$\frac{\neg \mathrm{P}(x) \lor \neg \mathrm{Q}(y, x) \lor \mathrm{R}(\mathrm{f}(x, y), y) \qquad \neg \mathrm{R}(x, \mathrm{c})}{\neg \mathrm{P}(x) \lor \neg \mathrm{Q}(\mathrm{c}, x)}$$

si môžeme predstaviť ako postupný proces:

$$\begin{array}{ccl}
 & \neg \mathrm{R}(x, \mathrm{c}) & \\
 & \downarrow \{x \mapsto z\} & \text{premenovanie} \\
\neg \mathrm{P}(x) \lor \neg \mathrm{Q}(y, x) \lor \mathrm{R}(\mathrm{f}(x, y), y) & \neg \mathrm{R}(z, \mathrm{c}) & \\
\downarrow \qquad \{y \mapsto \mathrm{c}, z \mapsto \mathrm{f}(x, \mathrm{c})\} & \downarrow & \text{unifikácia} \\
\neg \mathrm{P}(x) \lor \neg \mathrm{Q}(\mathrm{c}, x) \lor \mathrm{R}(\mathrm{f}(x, \mathrm{c}), \mathrm{c}) & \neg \mathrm{R}(\mathrm{f}(x, \mathrm{c}), \mathrm{c}) & \\
\hline
\multicolumn{2}{c}{\neg \mathrm{P}(x) \lor \neg \mathrm{Q}(\mathrm{c}, x)} & \text{výrokovolog. rezolvencia}
\end{array}$$

Rezolvenčné odvodenie a zamietnutie

Definícia 14.34

Nech T je klauzálna teória.

Rezolvenčným odvodením z T je každá (aj nekonečná) postupnosť klauzúl $\mathcal{Z} = (C_1, C_2, \dots, C_n, \dots)$, 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 konečné rezolvenčné odvodenie $\mathcal{Z} = (C_1, C_2, \dots, C_n)$, kde $C_n = \square$.

Refutačná korektnosť a úplnosť rezolvencie

Pri klasickom poňatí dôkazu ako postupnosti formúl, ktoré sú odvodené z predošlých formúl pomocou fixnej sady pravidiel, pod *úplnosťou* rozumieme schopnosť odvodiť z teórie hociktorú formulu, ktorá je jej logickým dôsledkom. Rezolvencia je v tomto zmysle neúplná (napr. z A nevieme odvodiť $A \lor B$ či $A \lor \neg A$).

Vieme však rezolvenciou z ľubovoľnej nesplniteľnej teórie odvodiť nesplniteľnú prázdnu klauzulu $\square$. Tejto vlastnosti hovoríme *refutačná úplnosť*.

Veta 14.35 (Refutačná korektnosť a úplnosť rezolvencie)

Nech T je klauzálna teória.

Potom existuje zamietnutie T vtt T je nesplniteľná.

Refutačná korektnosť a úplnosť rezolvencie

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

Dôsledok 14.36 (Úplnosť rezolvencie)

Nech T je 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.

Príklad 14.37

Dokážme nesplniteľnosť:

$$\left\{\begin{array}{c} \forall x\, \mathtt{r}(\mathtt{nk}(x), x), \\ \forall x\, \forall y\, \mathtt{r}(x, \mathtt{nk}(y)), \\ \forall x(\neg \mathtt{r}(x, \mathtt{D}) \lor \neg \mathtt{r}(\mathtt{E}, x)) \end{array}\right\}$$