

Rezolvencia

11. prednáška

Logika pre informatikov a Úvod do matematickej logiky

Ján Klúka, Ján Mazák, Jozef Šiška

Letný semester 2023/2024

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

Rezolvencia

Rezolvencia vo výrokovej logike

Prevod do klauzálnej teórie a skolemizácia

Rezolvencia v logike prvého rádu

Rezolvencia

Automatické dokazovanie v logike prvého rádu

Vyplyvanie 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**
(ak by bola, vedeli by sme riešiť problém zastavenia — viac nabadúce).

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

Dokazovací systém má podstatný vplyv na to, ako dlho v praxi potrvá
nájdanie 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?

$$\frac{(A \rightarrow B) \quad (B \rightarrow C)}{(A \rightarrow C)}$$

Nahradíme implikácie disjunkciami:

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

Rezolvencia

Predchádzajúce pravidlo sa dá zovšeobecniť na ľub. dvojicu klauzúl:

Definícia 14.1

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

$$\frac{(K_1 \vee \dots \vee A \vee \dots \vee K_m) \quad (L_1 \vee \dots \vee \neg A \vee \dots \vee L_n)}{(K_1 \vee \dots \vee K_m \vee L_1 \vee \dots \vee L_n)}$$

pre ľubovoľný atóm A a ľub. literály $K_1, \dots, K_m, L_1, \dots, L_n$.

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

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:

$$\frac{(\neg A \vee B) \quad (\neg B \vee C)}{(\neg A \vee C)} \quad \text{(HS)}$$

$$\frac{(\neg A \vee B) \quad A}{B} \quad \text{(MP)}$$

$$\frac{(\neg A \vee B) \quad \neg B}{\neg A} \quad \text{(MT)}$$

Pozorovania o rezolvencii

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

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

- Rezolvenca môže odvodiť **prázdnu klauzulu**:

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

vtedy premisy **nie sú súčasne splniteľné**

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

Častá chyba pri rezolvencii

Niektoré dvojice klauzúl možno rezolvovať na viacerých literáloch:

$$\frac{(\neg p \vee q) \quad (p \vee \neg q)}{(q \vee \neg q)} \quad \checkmark$$

$$\frac{(\neg p \vee q) \quad (p \vee \neg q)}{(\neg p \vee p)} \quad \checkmark$$

ale **je chyba urobiť to naraz:**

~~$$\frac{(\neg p \vee q) \quad (p \vee \neg q)}{\square} \quad \times$$~~

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

Prečo?

Častá chyba pri rezolvencii

Niektoré dvojice klauzúl možno rezolvovať na viacerých literáloch:

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

ale **je chyba urobiť to naraz**:

~~$$\frac{(\neg p \vee q) \quad (p \vee \neg q)}{\square} \quad \times$$~~

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

Prečo?

Lebo $\{(\neg p \vee q), (p \vee \neg q)\}$ 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 \square je nesplniteľná.

Rezolvenčné odvodenie a problém

Opakovaním rezolvenzie 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)
- ⋮

Problematické prípady

Odvedeniami v príklade dostaneme iba existujúce alebo nové

dvojprvkové klauzuly $((A \vee A), (B \vee C), (B \vee B), \dots)$

ale žiadnu jednotkovú, lebo rezolventa má $m + n - 2$ literálov.

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

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

Klauzula $(A \vee A)$ je evidentne ekvivalentná s A ;

A sa ale z množiny S iba rezolvenciou odvodiť nedá.

Potrebuje ešte **pravidlo idempotencie**:

$$\frac{(K_1 \vee \dots \vee L \vee \dots \vee L \vee \dots \vee K_n)}{(K_1 \vee L \vee \dots \vee K_n)}$$

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 rezolvenca (6) a (2)
- (8) $\neg C$ rezolvenca (6) a (4)
- (9) \square rezolvenca (7) a (8)

Množine klauzúl budeme hovoriť aj *klauzálna teória*.

Tvrdenie 14.6

Ak pre klauzálnu teóriu S existuje zamietnutie, je nespĺniteľná.

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

Vyskúšajte si 14.1

Dokážte nespĺniteľnosť

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

Rezolvencia a SAT

Možno pomocou rezolvenencie znížiť počet atómov?

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

Preskúmame 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 nespĺniteľná.
- 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!

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

Ak uvedený postup vedie k zamietnutiu, ohodnotenie neexistuje.

Ohodnotenie nájdené po eliminácii atómu popísaným spôsobom však nemusí vyhovovať pôvodným klauzulám!

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

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 rezolvenia jednej dvojice klauzúl použijeme rezolvenciu **súčasne pre všetky možné dvojice** obsahujúce komplementárne literály s atómom A .

Rezolvencia a SAT

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

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

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 $v_2 \models_p X_i \vee Y_j$ 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 nepokážime splnenie klauzúl v T , lebo neobsahujú A .

Naopak, ak ohodnotenie v_1 je modelom $S_1 \cup T$, tak $v_1 \models_p S_2 \cup T$: Ak $v_1(A) = t$, tak $v_1 \models_p Y_j$ pre všetky j , preto $v_1 \models_p S_2$. 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.

Využitím uvedeného postupu vieme dokázať úplnosť rezolvencie.

Tvrdenie 14.7 (Úplnosť rezolvencie)

Ak je klauzálna teória S nespľniteľná, existuje jej zamietnutie.

Dôkaz.

Uvažujme nespľniteľnú klauzálnu teóriu a rozdelíme 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 nespľniteľná vtt $T \cup S_2$ je nespľniteľná. Zároveň $T \cup S_2$ má o jeden atóm menej.

Opakovaním postupu nájdeme nespľniteľnú množinu klauzúl, ktorá má už len nezmiešané literály. Preto v nej musí byť aj \square .

(Kde v dôkaze využívame idempotenciu?) \square

Pomocou rezolvenzie vieme rozhodovať splniteľnosť.

Veta 14.8 (Korektnosť a úplnosť rezolvenzie)

Nech S je klauzálna teória.

S je výrokovologicky nesplniteľná vtt existuje zamietnutie S .

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

Rezolvencia

Prevod do klauzálnej teórie
a skolemizácia

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?

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 $\forall x_1 \cdots \forall x_k (L_1 \vee \cdots \vee L_n)$
kde L_1, \dots, L_n sú literály
a x_1, \dots, x_k sú **všetky** voľné premenné formuly $L_1 \vee \cdots \vee L_n$.
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 $\text{free}(A) = \text{free}(B)$.
Ak $A \Leftrightarrow B$, tak $X \Leftrightarrow X[A \mid B]$.

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

Príklad 14.12

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

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

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:

$$\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B \qquad \neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$$

- pravidla dvojitej negácie:

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

- zovšeobecnení de Morganových zákonov pre kvantifikátory:

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

Tvrdenie 14.14

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

Príklad 14.15

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

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

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 tabľách,
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 ekvisplniteľnosť)

Množiny formúl S a T

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

Skolemizácia — skolemovská konštantá

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

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

Konštantá c **pomenúva objekt**, ktorý existuje podľa $\exists y A$.

Príklad 14.17

$$\exists x (\text{dobré}(x) \wedge \text{dieťa}(x))$$

$$\rightsquigarrow \text{dobré}(\text{nejaké_dobré_dieťa}) \wedge \text{dieťa}(\text{nejaké_dobré_dieťa})$$

Skolemizácia — skolemovská funkcia

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

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

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

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

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

Príklad 14.18

$$\begin{aligned} & \forall x (\neg \text{dobré}(x) \vee \neg \text{dieťa}(x) \vee \exists y (\text{dostane}(x, y) \wedge \text{darček}(y))) \\ \rightsquigarrow & \forall x (\neg \text{dobré}(x) \vee \neg \text{dieťa}(x) \vee \\ & (\text{dostane}(x, \text{darček_pre}(x)) \wedge \text{darček}(\text{darček_pre}(x)))) \end{aligned}$$

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 **ekvisplnitelné**.

Príklad 14.20

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

$\rightsquigarrow \dots?$

Definícia 14.21

Formula X je v *prenexnom normálnom tvare* (PNF) vtt má tvar $Q_1x_1 Q_2x_2 \cdots Q_nx_n A$, 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 ,

$$(\forall x A \wedge B) \Leftrightarrow \forall x (A \wedge B) \quad (B \wedge \forall x A) \Leftrightarrow \forall x (B \wedge A)$$

$$(\forall x A \vee B) \Leftrightarrow \forall x (A \vee B) \quad (B \vee \forall x A) \Leftrightarrow \forall x (B \vee A)$$

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

$$(\forall x A \wedge B) \Leftrightarrow (\forall y A\{x \mapsto y\} \wedge B) \quad (B \wedge \forall x A) \Leftrightarrow (B \wedge \forall y A\{x \mapsto y\})$$

$$(\forall x A \vee B) \Leftrightarrow (\forall y A\{x \mapsto y\} \vee B) \quad (B \vee \forall x A) \Leftrightarrow (B \vee \forall y A\{x \mapsto y\})$$

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

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

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

$$\begin{aligned} & (\forall x A(x) \vee \forall x B(x)) \not\Leftrightarrow \forall x (A(x) \vee B(x)) \quad \text{✗} \\ & (\forall x A(x) \vee \forall x B(x)) \Leftrightarrow \forall x (A(x) \vee \forall x B(x)) \Leftrightarrow \\ & \forall x (A(x) \vee \forall y B(y)) \Leftrightarrow \forall x \forall y (A(x) \vee B(y)) \quad \text{✓} \end{aligned}$$

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:

$$(A \vee (X \wedge Y)) \Leftrightarrow ((A \vee X) \wedge (A \vee Y))$$

$$((X \wedge Y) \vee A) \Leftrightarrow ((X \vee A) \wedge (Y \vee A))$$

Príklad 14.24

$$\begin{aligned} & \forall x(\neg \text{dobré}(x) \vee \neg \text{dieťa}(x) \vee \\ & \quad (\text{dostane}(x, \text{darček_pre}(x)) \wedge \text{darček}(\text{darček_pre}(x)))) \\ \Leftrightarrow & \forall x((\neg \text{dobré}(x) \vee \neg \text{dieťa}(x) \vee \text{dostane}(x, \text{darček_pre}(x))) \wedge \\ & \quad (\neg \text{dobré}(x) \vee \neg \text{dieťa}(x) \vee \text{darček}(\text{darček_pre}(x)))) \end{aligned}$$

Konverzia do klauzálnej teórie

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

$$\forall x(A \wedge B) \Leftrightarrow (\forall x A \wedge \forall x B)$$

a konjunkcia klauzúl je ekvivalentná s ich množinou:

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

Príklad 14.25

$$\begin{aligned} & \{ \forall x ((\neg \text{dobré}(x) \vee \neg \text{dieťa}(x) \vee \text{dostane}(x, \text{darček_pre}(x))) \wedge \\ & \quad (\neg \text{dobré}(x) \vee \neg \text{dieťa}(x) \vee \text{darček}(\text{darček_pre}(x)))) \} \\ \Leftrightarrow & \{ (\forall x (\neg \text{dobré}(x) \vee \neg \text{dieťa}(x) \vee \text{dostane}(x, \text{darček_pre}(x))) \wedge \\ & \quad \forall x (\neg \text{dobré}(x) \vee \neg \text{dieťa}(x) \vee \text{darček}(\text{darček_pre}(x)))) \} \\ \Leftrightarrow & \{ \forall x (\neg \text{dobré}(x) \vee \neg \text{dieťa}(x) \vee \text{dostane}(x, \text{darček_pre}(x))), \\ & \quad \forall x (\neg \text{dobré}(x) \vee \neg \text{dieťa}(x) \vee \text{darček}(\text{darček_pre}(x))) \} \end{aligned}$$

Veta 14.26

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

Príklad 14.27

$$\left\{ \begin{array}{l} \forall x (\text{dobré}(x) \wedge \text{dieťa}(x) \rightarrow \exists y (\text{dostane}(x, y) \wedge \text{darček}(y))), \\ \exists x (\text{dobré}(x) \wedge \text{dieťa}(x)), \\ \forall x (\neg \text{dobré}(x) \rightarrow \neg \exists y \text{ dostane}(x, y)) \end{array} \right\} \rightsquigarrow$$
$$\left\{ \begin{array}{l} \forall x_1 (\neg \text{dobré}(x_1) \vee \neg \text{dieťa}(x_1) \vee \text{dostane}(x_1, \text{darček_pre}(x_1))), \\ \forall x_2 (\neg \text{dobré}(x_2) \vee \neg \text{dieťa}(x_2) \vee \text{darček}(\text{darček_pre}(x_2))), \\ \text{dobré}(\text{nejaké_dobré_dieťa}), \text{dieťa}(\text{nejaké_dobré_dieťa}), \\ \forall x_3 \forall y (\text{dobré}(x_3) \vee \neg \text{dostane}(x_3, y)) \end{array} \right\}$$

Konverzia do prvorádovej CNF

Dôkaz/algorithmus

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): distribuuujeme disjunkcie do konjunkcií.

T_K : Odstránime konjunkcie rozdelením konjunktov do samostatne kvantifikovaných klauzúl.

Skolemizácia vytvorí ekvivalentnú teóriu, ostatné úpravy sú ekvivalentné.

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 $\forall x_1 \cdots \forall x_n (L_1 \vee \cdots \vee L_m)$ píšeme iba $L_1 \vee \cdots \vee L_m$.

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

Úsudky s klauzulami

Príklad 14.29

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

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

Kto má rád Dadu, toho Edo nemá rád:

$$\forall x (\neg r(x, D) \vee \neg r(E, x)),$$

Teda aj Dadu má niekto rád:

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

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

$$\neg r(\text{nk}(D), D) \vee \neg r(E, \text{nk}(D)).$$

Preto (výrokovou rezolvenciou):

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

Úsudky s klauzulami

Celý úsudok z príkladu aj s dosadeniami:

$$\frac{\forall y \, r(\text{nk}(y), y) \quad \forall x (\neg r(x, D) \vee \neg r(E, x))}{\neg r(E, \text{nk}(D))}$$

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

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

Po substitúcii σ majú komplementárne literály rovnaké argumenty predikátu r :

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

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

Príklad 14.30

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

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

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

Príklad 14.31

Rovnaké premenné v klauzulách môžu zabrániť unifikácii literálov:

$$r(nk(x), x) \qquad \neg r(x, D) \vee \neg r(E, x)$$

Klauzuly sú však všeobecne kvantifikované **nezávisle** od seba.

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

$$r(nk(y), y) \qquad \neg r(x, D) \vee \neg r(E, x)$$

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.

Definícia 14.33

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

Rezolvenca (angl. resolution) je odvodzovacie pravidlo

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

Faktorizácia (angl. factoring) je odvodzovacie pravidlo

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

Faktorizácia je zovšeobecnenie idempotencie pri výrokovej rezolvencii.

Rezolvencia postupne

Rezolvenciu

$$\frac{\neg P(x) \vee \neg Q(y, x) \vee R(f(x, y), y) \quad \neg R(x, c)}{\neg P(x) \vee \neg Q(c, x)}$$

si môžeme predstaviť ako postupný proces:

$$\begin{array}{lcl} & \neg R(x, c) & \\ & \downarrow \{x \mapsto z\} & \text{premenovanie} \\ \neg P(x) \vee \neg Q(y, x) \vee R(f(x, y), y) & \neg R(z, c) & \\ & \downarrow \{y \mapsto c, z \mapsto f(x, c)\} & \text{unifikácia} \\ \neg P(x) \vee \neg Q(c, x) \vee R(f(x, c), c) & \neg R(f(x, c), c) & \\ \hline & \neg P(x) \vee \neg Q(c, x) & \text{výrokovolog.} \\ & & \text{rezolvencia} \end{array}$$

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. Rezolvenca je v tomto zmysle neúplná (napr. z A nevieme odvodiť $A \vee B$ či $A \vee \neg A$).

Vieme však rezolvenciou z ľubovoľnej nespĺniteľnej teórie odvodiť \square (prázdna klauzula, ktorá je zjavne nespĺniteľná). 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 nespĺniteľná.

Refutačná korektnosť a úplnosť rezolvenzie

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

Dôsledok 14.36 (Úplnosť rezolvenzie)

Nech T je teória, nech X je uzavretá formula.

Nech $T'_X = \{C_1, \dots, C_n\}$ je klauzálna teória ekvisplnitelná s $T \cup \{\neg X\}$.

Potom z T vyplýva X vtt existuje zamietnutie T'_X .

Príklad 14.37

Dokážme nesplniteľnosť:

$$\left\{ \begin{array}{l} \forall x \, r(\text{nk}(x), x), \\ \forall x \, \forall y \, r(x, \text{nk}(y)), \\ \forall x (\neg r(x, D) \vee \neg r(E, x)) \end{array} \right\}$$