

# Rezolvencia

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

---

Ján Klúka, Ján Mazák

Letný semester 2021/2022

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

### 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 výrokovvej 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 (aj 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 výrokovvej 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 ľubovoľné dvojice 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 ľubovoľné 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.*



## Špeciálne prípady rezolvenzie

Viacero pravidiel sa dá chápať ako špeciálne prípady rezolvenzie:

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

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

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

## 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:

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

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?

## 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 rezolvenzie 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 nespĺniteľná.

# 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

Odvodzeniami 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 nejak odvodiť prázdnu klauzulu.

To sa nedá bez odvodenia 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 rezolvenzie 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)  $C$  rezolvenzia (6) a (2)
- (8)  $\neg C$  rezolvenzia (6) a (4)
- (9)  $\square$  rezolvenzia (7) a (8)



# Korektnosť a úplnosť rezolvenzie

Množinu klauzúl nazývame aj *klauzálna teória*.

## Veta 14.6 (Korektnosť a úplnosť rezolvenzie)

*Nech  $S$  je množina klauzálna teória.*

*$S$  je výrokovologicky nespĺniteľná vtt existuje zamietnutie  $S$ .*

Už vieme, že ku každej formule (a teórii) existuje ekvivalentná klauzálna teória (formula v CNF). Výrokovologická splniteľnosť a vyplývanie sa teda dajú rozhodnúť pomocou rezolvenzie.

## 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

---

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 14.7

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 14.8 (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 14.9 (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 14.10

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

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

# Konverzia do negačného normálneho tvaru (NNF)

## Definícia 14.11

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:

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

- pravidla dvojitej negácie:

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

- zovšeobecnení de Morganovych zákonov pre kvantifikátory:

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

## Tvrdenie 14.12

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

## Príklad 14.13

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

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



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

Podobá sa pravidlu  $\delta$  v tabľách,  
ale aplikuje sa naraz na všetky existenčné kvantifikátory.

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

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

## Definícia 14.14 (Prvorádová ekvisplniteľnosť)

Množiny formúl  $S$  a  $T$

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

# Skolemizácia — skolemovská konštanta

Ľahký prípad (v podstate pravidlo  $\delta$ ):

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

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

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

## Príklad 14.15

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

$$\rightsquigarrow \text{dobré}(\text{nejaké\_dobré\_dieťa}) \wedge \text{dieťa}(\text{nejaké\_dobré\_dieťa})$$

# 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 14.16

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

## Tvrdenie 14.17

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 14.18

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

$\rightsquigarrow \dots?$

## Definícia 14.19

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 (*matrica* 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 14.20

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

## Príklad 14.21

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

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

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

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 14.22

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

# 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 14.23

$$\{\forall x((\neg \text{dobré}(x) \vee \neg \text{dieťa}(x) \vee \text{dostane}(x, \text{darček\_pre}(x))) \wedge (\neg \text{dobré}(x) \vee \neg \text{dieťa}(x) \vee \text{darček}(\text{darček\_pre}(x))))\}$$

$$\Leftrightarrow \{(\forall x(\neg \text{dobré}(x) \vee \neg \text{dieťa}(x) \vee \text{dostane}(x, \text{darček\_pre}(x))) \wedge \forall x(\neg \text{dobré}(x) \vee \neg \text{dieťa}(x) \vee \text{darček}(\text{darček\_pre}(x))))\}$$

$$\Leftrightarrow \{\forall x(\neg \text{dobré}(x) \vee \neg \text{dieťa}(x) \vee \text{dostane}(x, \text{darček\_pre}(x))), \forall x(\neg \text{dobré}(x) \vee \neg \text{dieťa}(x) \vee \text{darček}(\text{darček\_pre}(x)))\}$$



## Veta 14.24

*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 14.25

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

# Konverzia do prvorádovej CNF

## Dôkaz/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.

$T_D$ : **Konjunktívny normálny tvar** (CNF): distribuujeme 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 14.26

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  $L_1 \vee \cdots \vee L_m$ .

# Úsudky s klauzulami

## Príklad 14.27

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

$$\forall y \, r(nk(y), y)$$

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:

$$r(nk(D), D)$$

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

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

Preto (výrokovou rezolvenciou):

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

# 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, potrebovali sme substitúciu:

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

Po substitúcii  $\sigma$  majú komplementárne literály rovnaké argumenty predikátu:

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

## Definícia 14.28

Nech  $A, B$  sú postupnosti symbolov,  $\sigma$  je substitúcia.

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

## Príklad 14.29

- $A_1 = r(\text{filantrop}, y), B_1 = r(x, D),$   
 $\sigma_1 = \{x \mapsto \text{filantrop}, y \mapsto D\}$
- $A_2 = r(\text{nk}(y), y), B_2 = r(x, D),$

## Definícia 14.28

Nech  $A, B$  sú postupnosti symbolov,  $\sigma$  je substitúcia.

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

## Príklad 14.29

- $A_1 = r(\text{filantrop}, y), B_1 = r(x, D),$   
 $\sigma_1 = \{x \mapsto \text{filantrop}, y \mapsto D\}$
- $A_2 = r(\text{nk}(y), y), B_2 = r(x, D),$   
 $\sigma_2 = \{x \mapsto \text{nk}(D), y \mapsto D\}$
- $A_3 = r(\text{nk}(y), y), B_3 = r(E, x),$



## Definícia 14.28

Nech  $A, B$  sú postupnosti symbolov,  $\sigma$  je substitúcia.

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

## Príklad 14.29

- $A_1 = r(\text{filantrop}, y), B_1 = r(x, D),$   
 $\sigma_1 = \{x \mapsto \text{filantrop}, y \mapsto D\}$
- $A_2 = r(\text{nk}(y), y), B_2 = r(x, D),$   
 $\sigma_2 = \{x \mapsto \text{nk}(D), y \mapsto D\}$
- $A_3 = r(\text{nk}(y), y), B_3 = r(E, x),$   
 $\sigma_3 = ???$  **neexistuje!**
- $A_4 = r(\text{nk}(y), y), B_4 = r(x, x),$

## Definícia 14.28

Nech  $A, B$  sú postupnosti symbolov,  $\sigma$  je substitúcia.

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

## Príklad 14.29

- $A_1 = r(\text{filantrop}, y), B_1 = r(x, D),$   
 $\sigma_1 = \{x \mapsto \text{filantrop}, y \mapsto D\}$
- $A_2 = r(\text{nk}(y), y), B_2 = r(x, D),$   
 $\sigma_2 = \{x \mapsto \text{nk}(D), y \mapsto D\}$
- $A_3 = r(\text{nk}(y), y), B_3 = r(E, x),$   
 $\sigma_3 = ???$  **neexistuje!**
- $A_4 = r(\text{nk}(y), y), B_4 = r(x, x),$   
 $\sigma_4 = ???$  **neexistuje!**

## Definícia 14.30

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**  $\sigma$  a  $\theta$  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 14.31

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

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

$$\sigma\theta = \{x \mapsto \text{nk}(\text{filantrop}), \\ z \mapsto \text{filantrop}, y \mapsto \text{filantrop}\}$$

## Definícia 14.32

Nech  $A, B$  sú postupnosti symbolov,  $\sigma$  a  $\theta$  sú substitúcie.

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

$\sigma$  je **najvšeobecnejším unifikátorom**  $A$  a  $B$  vtt

- $\sigma$  je unifikátorom  $A$  a  $B$  a zároveň
- pre každý unifikátor  $\theta$   $A$  a  $B$  je  $\sigma$  všeobecnejšia ako  $\theta$ .

## Príklad 14.33

$A_5 = r(nk(x), y), B_5 = r(u, v)$

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

## Príklad 14.34

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

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

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

## Príklad 14.35

Rovnaké premenné v klauzulách môžu zabrániť unifikácii literálov:

$$r(nk(x), x)$$

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

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

$$r(nk(y), y)$$

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

## Definícia 14.36

**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 14.37

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:

	$\neg R(x, c)$
prenenovanie:	$\downarrow \{x \mapsto z\}$
	$\neg P(x) \vee \neg Q(y, x) \vee R(f(x, y), y) \quad \neg R(z, c)$
unifikácia:	$\downarrow \{y \mapsto c, z \mapsto f(x, c)\} \quad \downarrow$
	$\neg P(x) \vee \neg Q(c, x) \vee R(f(x, c), c) \quad \neg R(f(x, c), c)$
	$\hline \neg P(x) \vee \neg Q(c, x)$



## Definícia 14.38

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  $C_n = \square$ .

## Veta 14.39 (Refutačná korektnosť a úplnosť rezolvencie)

*Nech  $T$  je klauzálna teória.*

*Potom existuje zamietnutie  $T$  vtt  $T$  je nesplniteľná.*

## Príklad 14.40

Dokážme nesplniteľnosť:

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

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

### Dôsledok 14.41 (Úplnosť rezolvenčie)

*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  $T'_X$ .*