

# Pátá přednáška

NAIL062 Výroková a predikátová logika

---

Jakub Bulín (KTIML MFF UK)

Zimní semestr 2024

## Program

- věta o kompaktnosti
- hilbertovský kalkulus
- rezoluční metoda
- korektnost a úplnost rezoluce
- LI-rezoluce a Horn-SAT

## Materiály

**Zápisky z přednášky**, Sekce 4.7-4.8 z Kapitoly 4, Kapitola 5

## 4.7 Věta o kompaktnosti

---

**Věta (O kompaktnosti):** Teorie má model, právě když každá její konečná část má model.

**Důkaz:**  $\Rightarrow$  **Snadné:** Model  $T$  je zjevně modelem každé její části.

$\Leftarrow$  **Nepřímo:** buď  $T$  sporná, najdeme spornou konečnou  $T' \subseteq T$ .

Z **úplnosti** víme, že  $T \vdash \perp$ , tedy existuje i **konečný** tablo důkaz  $\tau$  výroku  $\perp$  z  $T$ . Konstrukce  $\tau$  má konečně mnoho kroků, použili jsme tedy jen konečně mnoho axiomů z  $T$ . Definujme:

$$T' = \{\alpha \in T \mid T\alpha \text{ je položka v tablu } \tau\}$$

Tedy  $\tau$  je tablo jen z teorie  $T'$ , máme tablo důkaz  $T' \vdash \perp$ , dle **korektnosti** je  $T'$  sporná. □

vlastnost nekonečného objektu  $\mathcal{O}$



vlastnost všech konečných podobjektů  $\mathcal{O}'$

- vlastnost popíšeme pomocí (nekonečné) teorie  $T$
- ke každé konečné  $T' \subseteq T$  sestojíme konečný podobjekt  $\mathcal{O}'$
- $\mathcal{O}'$  splňuje danou vlastnost
- to nám dává model  $T'$
- dle Věty o kompaktnosti má i  $T$  model
- což ukazuje, že i nekonečný objekt  $\mathcal{O}$  splňuje vlastnost

Věta o kompaktnosti má mnoho aplikací (několik z nich uvidíme později), následující příklad chápejte jako 'šablonu'.

## Aplikace kompaktnosti: příklad

**Důsledek:** Spočetně nekonečný graf je bipartitní, právě když je každý jeho konečný podgraf bipartitní.

**Důkaz:**  $\Rightarrow$  Každý podgraf bipartitního grafu je bipartitní.

$\Leftarrow$   $G$  je bipartitní, právě když je obarvitelný 2 barvami. Mějme jazyk  $\mathbb{P} = \{p_v \mid v \in V(G)\}$  (kde  $p_v$  je barva  $v$ ) a uvažme teorii

$$T = \{p_u \leftrightarrow \neg p_v \mid \{u, v\} \in E(G)\}$$

Zřejmě  $G$  je bipartitní, právě když  $T$  má model. Dle Věty o kompaktnosti stačí ukázat, že každá konečná  $T' \subseteq T$  má model.

Bud'  $G'$  podgraf  $G$  indukovaný na vrcholech, o kterých  $T'$  mluví:

$$V(G') = \{v \in V(G) \mid p_v \in \text{Var}(T')\}$$

Protože je  $T'$  konečná, je  $G'$  také konečný, tedy je dle předpokladu 2-obarvitelný. Libovolné 2-obarvení  $V(G')$  ale určuje model  $T'$ .  $\square$

## 4.8 Hilbertovský kalkulus

---

# Hilbertovský deduktivní systém

- jiný, původní dokazovací systém
- používá jen logické spojky  $\neg$ ,  $\rightarrow$
- **schémata logických axiomů** ( $\varphi, \psi, \chi$  jsou libovolné výroky)
  - (i)  $\varphi \rightarrow (\psi \rightarrow \varphi)$
  - (ii)  $(\varphi \rightarrow (\psi \rightarrow \chi)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \chi))$
  - (iii)  $(\neg\varphi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \varphi)$

- **odvozovací pravidlo**: tzv. **modus ponens**

$$\frac{\varphi, \varphi \rightarrow \psi}{\psi}$$

- **hilbertovský důkaz** výroku  $\varphi$  z teorie  $T$  je **konečná** posloupnost výroků  $\varphi_0, \dots, \varphi_n = \varphi$ , ve které pro každé  $i \leq n$ :
  - $\varphi_i$  je **logický axiom**, nebo
  - $\varphi_i$  je **axiom teorie** ( $\varphi_i \in T$ ), nebo
  - $\varphi_i$  lze odvodit z předchozích pomocí **odvozovacího pravidla**
- existuje-li hilbertovský důkaz, píšeme:  $T \vdash_H \varphi$



## Příklad hilbertovského důkazu

Ukažme, že pro teorii  $T = \{\neg\varphi\}$  a pro libovolný výrok  $\psi$  platí:

$$T \vdash_H \varphi \rightarrow \psi$$

Hilbertovským důkazem je následující posloupnost výroků:

1.  $\neg\varphi$  *axiom teorie*
2.  $\neg\varphi \rightarrow (\neg\psi \rightarrow \neg\varphi)$  *logický axiom (i)*
3.  $\neg\psi \rightarrow \neg\varphi$  *modus ponens na 1. a 2.*
4.  $(\neg\psi \rightarrow \neg\varphi) \rightarrow (\varphi \rightarrow \psi)$  *logický axiom (iii)*
5.  $\varphi \rightarrow \psi$  *modus ponens na 3. a 4.*

**Věta (o korektnosti hilbertovského kalkulu):**  $T \vdash_H \varphi \Rightarrow T \models \varphi$

**Důkaz:** Indukcí dle délky důkazu ukážeme, že každý výrok  $\varphi_i$  z důkazu (tedy i  $\varphi_n = \varphi$ ) platí v  $T$ .

- Je-li  $\varphi_i$  logický axiom,  $T \models \varphi_i$  platí protože logické axiomy jsou tautologie.
- Je-li  $\varphi_i \in T$ , jistě platí  $T \models \varphi_i$ .
- Získáme-li  $\varphi_i$  pomocí modus ponens z  $\varphi_j$  a  $\varphi_k = \varphi_j \rightarrow \varphi_i$  (pro nějaká  $j, k < i$ ), víme z indukčního předpokladu, že platí  $T \models \varphi_j$  a  $T \models \varphi_j \rightarrow \varphi_i$ . Potom ale platí i  $T \models \varphi_i$ . (Modus ponens je **korektní** odvozovací pravidlo)  $\square$

**Věta (o úplnosti hilbertovského kalkulu):**  $T \models \varphi \Rightarrow T \vdash_H \varphi$

Důkaz vynecháme.

## KAPITOLA 5: REZOLUČNÍ METODA

---

# Rezoluční metoda

- jiný důkazový systém než tablo metoda
- mnohem efektivnější implementace
- logické programování, automatické dokazování, SAT solvery (důkaz jako **certifikát** nesplnitelnosti)
- pracuje s CNF (každý výrok/teorii lze převést do CNF)
- jediné inferenční pravidlo: **rezoluční pravidlo**

$$\frac{\{p\} \cup C_1, \{\neg p\} \cup C_2}{C_1 \cup C_2}$$

- platí obecnější **pravidlo řezu**:

$$\frac{\varphi \vee \psi, \neg \varphi \vee \chi}{\psi \vee \chi}$$

## 5.1 Množinová reprezentace

---

# Množinová reprezentace

- **literál**  $\ell$  je  $p$  nebo  $\neg p$  (pro  $p \in \mathbb{P}$ ),  $\bar{\ell}$  je **opačný literál** k  $\ell$
- **klauzule**  $C$  je konečná množina literálů
- **prázdná klauzule**  $\square$  je nespílitelná
- **CNF formule**  $S$  je množina klauzulí (může být i **nekonečná!**)
- **prázdná formule**  $\emptyset$  je vždy splněna

Modely reprezentujeme jako množiny literálů:

- **(částečné) ohodnocení** je libovolná **konzistentní** množina literálů (tj. nesmí obsahovat dvojici opačných literálů)
- **úplné ohodnocení** obsahuje  $p$  nebo  $\neg p$  pro každý prvovýrok
- ohodnocení  $\mathcal{V}$  **splňuje** formuli  $S$ , píšeme  $\mathcal{V} \models S$ , pokud  $\mathcal{V}$  obsahuje nějaký literál z každé klauzule v  $S$ :

$$\mathcal{V} \cap C \neq \emptyset \text{ pro každou } C \in S$$

# Množinová reprezentace: příklad

$$\varphi = (\neg p_1 \vee p_2) \wedge (\neg p_1 \vee \neg p_2 \vee p_3) \wedge (\neg p_3 \vee \neg p_4) \wedge (\neg p_4 \vee \neg p_5) \wedge p_4$$

- v množinové reprezentaci:

$$S = \{\{\neg p_1, p_2\}, \{\neg p_1, \neg p_2, p_3\}, \{\neg p_3, \neg p_4\}, \{\neg p_4, \neg p_5\}, \{p_4\}\}$$

- ohodnocení  $\mathcal{V} = \{\neg p_1, \neg p_3, p_4, \neg p_5\}$  splňuje  $S$ ,  $\mathcal{V} \models S$
- není úplné, můžeme rozšířit libovolným literálem pro  $p_2$ , platí
  - $\mathcal{V} \cup \{p_2\} \models S$
  - $\mathcal{V} \cup \{\neg p_2\} \models S$
- tato dvě úplná ohodnocení odpovídají modelům
  - $(0, 1, 0, 1, 0)$
  - $(0, 0, 0, 1, 0)$

## 5.2 Rezoluční důkaz

---



# Rezoluční pravidlo

Mějme klauzule  $C_1$  a  $C_2$  a literál  $\ell$  takový, že  $\ell \in C_1$  a  $\bar{\ell} \in C_2$ .  
Potom **rezolventa** klauzulí  $C_1$  a  $C_2$  **přes literál  $\ell$**  je klauzule:

$$C = (C_1 \setminus \{\ell\}) \cup (C_2 \setminus \{\bar{\ell}\})$$

tedy z první klauzule odstraníme  $\ell$  a z druhé  $\bar{\ell}$  (musely tam být!) a zbylé literály sjednotíme, mohli bychom také psát:

$$C'_1 \cup C'_2 \text{ je rezolventou klauzulí } C'_1 \dot{\cup} \{\ell\} \text{ a } C'_2 \dot{\cup} \{\bar{\ell}\}$$

- z klauzulí  $C_1 = \{\neg q, r\}$  a  $C_2 = \{\neg p, \neg q, \neg r\}$  odvodíme klauzuli  $\{\neg p, \neg q\}$  přes literál  $r$
- z  $\{p, q\}$  a  $\{\neg p, \neg q\}$  odvodíme  $\{p, \neg p\}$  přes literál  $q$ , nebo  $\{q, \neg q\}$  přes literál  $p$  (obojí jsou ale tautologie)
- nelze z nich ale odvodit  $\square$  “*rezolucí přes  $p$  a  $q$  najednou*”!  
( $S = \{\{p, q\}, \{\neg p, \neg q\}\}$  je splnitelná, např.  $(1, 0)$  je model)

# Rezoluční důkaz

Rezoluční pravidlo je **korektní**, tj. pro libovolné ohodnocení  $\mathcal{V}$  platí:

Pokud  $\mathcal{V} \models C_1$  a  $\mathcal{V} \models C_2$ , potom  $\mathcal{V} \models C$ .

V rezolučním důkazu můžeme vždy napsat buď axiom, nebo rezolventu již napsaných klauzulí; tím zaručíme korektnost důkazů:

**Rezoluční důkaz (odvození)** klauzule  $C$  z formule  $S$  je konečná posloupnost klauzulí  $C_0, C_1, \dots, C_n = C$  taková, že pro každé  $i$ :

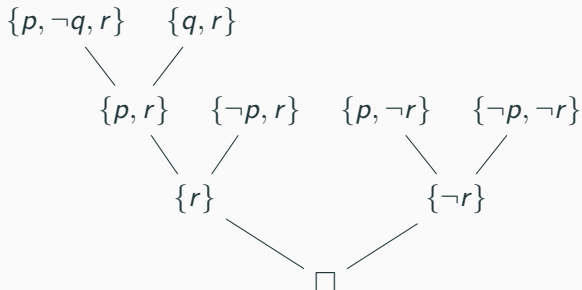
- $C_i \in S$ , nebo
  - $C_i$  je rezolventou nějakých  $C_j, C_k$  kde  $j, k < i$
- 
- existuje-li rez. důkaz, je  $C$  **rezolucí dokazatelná** z  $S$ ,  $S \vdash_R C$
  - **rezoluční zamítnutí** formule  $S$  je rezoluční důkaz  $\square$  z  $S$
  - v tom případě je  $S$  **rezolucí zamítnutelná**

## Příklad

Formule  $S = \{\{p, \neg q, r\}, \{p, \neg r\}, \{\neg p, r\}, \{\neg p, \neg r\}, \{q, r\}\}$  je rezolucí zamítnutelná, jedno z možných zamítnutí je:

$$\{p, \neg q, r\}, \{q, r\}, \{p, r\}, \{\neg p, r\}, \{r\}, \{p, \neg r\}, \{\neg p, \neg r\}, \{\neg r\}, \square$$

Rezoluční důkaz má přirozeně stromovou strukturu, tzv. **rezoluční strom**: na listech jsou axiomy, vnitřní vrcholy jsou rezoluční kroky.



# Rezoluční strom

**Rezoluční strom** klauzule  $C$  z formule  $S$  je konečný binární strom s vrcholy označenými klauzulemi, kde

- v kořeni je  $C$ ,
- v listech jsou klauzule z  $S$ ,
- v každém vnitřním vrcholu je rezolventa klauzulí ze synů tohoto vrcholu.

**Pozorování:**  $C$  má rezoluční strom z  $S$ , právě když  $S \vdash_R C$ .  
(Důkaz snadno indukcí dle hloubky stromu a délky důkazu.)

- rezolučnímu důkazu odpovídá **jednoznačný** rezoluční strom
- z rezolučního stromu můžeme získat více důkazů (jsou dané libovolnou procházkou po vrcholech, která navštíví vnitřní vrchol až poté, co navštívila oba jeho syny)

# Rezoluční uzávěr

jaké všechny klauzule se můžeme rezolucí 'naučit' z dané formule?  
(není praktické je všechny najít, jde o užitečný teoretický pohled)

**Rezoluční uzávěr**  $\mathcal{R}(S)$  formule  $S$  je definován induktivně jako nejmenší množina klauzulí splňující:

- $C \in \mathcal{R}(S)$  pro všechna  $C \in S$ ,
- jsou-li  $C_1, C_2 \in \mathcal{R}(S)$  a  $C$  jejich rezolventa, potom i  $C \in \mathcal{R}(S)$

Pro  $S = \{\{p, \neg q, r\}, \{p, \neg r\}, \{\neg p, r\}, \{\neg p, \neg r\}, \{q, r\}\}$  máme:

$$\begin{aligned}\mathcal{R}(S) = \{ & \{p, \neg q, r\}, \{p, \neg r\}, \{\neg p, r\}, \{p, s\}, \{q, r\}, \\ & \{p, \neg q\}, \{\neg q, r\}, \{r, \neg r\}, \{p, \neg p\}, \{r, s\}, \\ & \{p, r\}, \{p, q\}, \{r\}, \{p\}\}\end{aligned}$$

## 5.3 Korektnost a úplnost rezoluční metody

---

# Korektnost rezoluce

Korektnost dokážeme snadno indukcí podle délky důkazu (nebo alternativně indukcí dle hloubky rezolučního stromu).

**Věta (O korektnosti rezoluce):** Je-li CNF formule  $S$  rezolucí zamítnutelná, potom je  $S$  nesplnitelná.

**Důkaz:** Nechť  $S \vdash_R \square$ , a vezměme nějaký rezoluční důkaz  $C_0, C_1, \dots, C_n = \square$ . **Sporem:** nechť existuje ohodnocení  $\mathcal{V} \models S$ . Indukcí podle  $i$  dokážeme, že  $\mathcal{V} \models C_i$ . Potom i  $\mathcal{V} \models \square$ , což je spor.

Pro  $i = 0$  to platí, neboť  $C_0 \in S$ . Pro  $i > 0$  máme dva případy:

- $C_i \in S$ : v tom případě  $\mathcal{V} \models C_i$  plyne z předpokladu, že  $\mathcal{V} \models S$ ,
- $C_i$  je rezolventou  $C_j, C_k$ , kde  $j, k < i$ : z indukčního předpokladu víme  $\mathcal{V} \models C_j$  a  $\mathcal{V} \models C_k$ ,  $\mathcal{V} \models C_i$  plyne z korektnosti rezolučního pravidla □

Je-li  $S$  CNF formule a  $\ell$  literál, potom **dosazení**  $\ell$  do  $S$  je formule

$$S^\ell = \{C \setminus \{\bar{\ell}\} \mid \ell \notin C \in S\}$$

- $S^\ell$  je výsledkem **jednotkové propagace** aplikované na  $S \cup \{\{\ell\}\}$ .
- $S^\ell$  neobsahuje v žádné klauzuli literál  $\ell$  ani  $\bar{\ell}$  (vůbec tedy neobsahuje prvovýrok z  $\ell$ )
- Pokud  $S$  neobsahovala literál  $\ell$  ani  $\bar{\ell}$ , potom  $S^\ell = S$ .
- Pokud  $S$  obsahovala jednotkovou klauzuli  $\{\bar{\ell}\}$ , potom  $\square \in S^\ell$ , tedy  $S^\ell$  je sporná.



**Lemma:**  $S$  je splnitelná, právě když je splnitelná  $S^\ell$  nebo  $S^{\bar{\ell}}$ .

**Důkaz:**  $\Rightarrow$  Ohodnocení  $\mathcal{V} \models S$  nemůže obsahovat  $\ell$  i  $\bar{\ell}$ ; BÚNO  $\bar{\ell} \notin \mathcal{V}$ . Ukážeme, že potom  $\mathcal{V} \models S^\ell$ .

Vezměme libovolnou klauzuli v  $S^\ell$ . Ta je tvaru  $C \setminus \{\bar{\ell}\}$  pro klauzuli  $C \in S$  (neobsahující literál  $\ell$ ). Víme, že  $\mathcal{V} \models C$ , protože ale  $\mathcal{V}$  neobsahuje  $\bar{\ell}$ , muselo ohodnocení  $\mathcal{V}$  splnit nějaký jiný literál v  $C$ , takže platí i  $\mathcal{V} \models C \setminus \{\bar{\ell}\}$ .

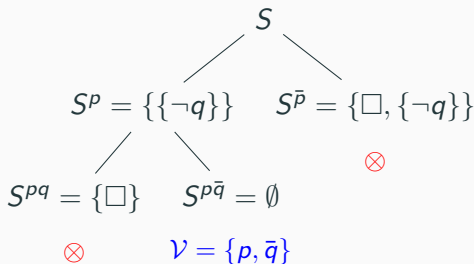
$\Leftarrow$  BÚNO mějme ohodnocení  $\mathcal{V} \models S^\ell$ . Protože se  $\bar{\ell}$  (ani  $\ell$ ) nevyskytuje v  $S^\ell$ , platí také  $\mathcal{V} \setminus \{\bar{\ell}\} \models S^\ell$ . Ohodnocení  $\mathcal{V}' = (\mathcal{V} \setminus \{\bar{\ell}\}) \cup \{\ell\}$  potom splňuje všechny  $C \in S$ , tedy  $\mathcal{V}' \models S$ :

- pokud  $\ell \in C$ , potom  $\ell \in C \cap \mathcal{V}'$  a  $C \cap \mathcal{V}' \neq \emptyset$
- jinak  $C \cap \mathcal{V}' = C \cap (\mathcal{V} \setminus \{\bar{\ell}\}) = (C \setminus \{\bar{\ell}\}) \cap (\mathcal{V} \setminus \{\bar{\ell}\}) \neq \emptyset$   
neboť  $\mathcal{V} \setminus \{\bar{\ell}\} \models C \setminus \{\bar{\ell}\} \in S^\ell$

# Strom dosazení

Zda je *konečná* formule  $S$  splnitelná můžeme zjišťovat rekurzivně, dosazením obou literálů pro některý prvovýrok  $p$ , a rozvětvením na  $S^p, S^{\bar{p}}$  (jako v DPLL). Výslednému stromu říkáme **strom dosazení**.

Např. pro  $S = \{\{p\}, \{\neg q\}, \{\neg p, \neg q\}\}$  :



- jakmile větev obsahuje  $\square$ , je nesplnitelná a nepokračujeme v ní
- listy jsou buď nesplnitelné, nebo prázdné teorie: v tom případě z posloupnosti dosazení získáme splňující ohodnocení.

# Strom dosazení a nesplnitelnost

**Důsledek:** CNF formule  $S$  (ve spočetném jazyce, může být i nekonečná) je nesplnitelná, právě když každá větev stromu dosazení obsahuje  $\square$ .

**Důkaz:** Pro konečnou  $S$  snadno dokážeme indukcí dle  $|\text{Var}(S)|$ :

- Je-li  $|\text{Var}(S)| = 0$ , máme  $S = \emptyset$  nebo  $S = \{\square\}$ , v obou případech je strom dosazení jednoprvkový a tvrzení platí.
- V indukčním kroku vybereme libovolný literál  $\ell \in \text{Var}(S)$  a aplikujeme Lemma.

Je-li  $S$  nekonečná a splnitelná, má splňující ohodnocení, to se 'shoduje' s odpovídající (nekonečnou) větví ve stromu dosazení.

Je-li nekonečná a nesplnitelná, dle Věty o kompaktnosti existuje konečná  $S' \subseteq S$ , která je také nesplnitelná. Po dosazení pro všechny proměnné z  $\text{Var}(S')$  bude v každé větvi  $\square$ , to nastane po konečně mnoha krocích.  $\square$  20

# Úplnost rezoluce

**Věta (O úplnosti rezoluce):** Je-li CNF formule  $S$  nesplnitelná, je rezolucí zamítnutelná (tj.  $S \vdash_R \square$ ).

**Důkaz:** Je-li  $S$  nekonečná, má z kompaktnosti konečnou nesplnitelnou část, její rezoluční zamítnutí je také zamítnutí  $S$ .

Je-li  $S$  konečná, ukážeme indukcí dle počtu proměnných: Je-li  $|\text{Var}(S)| = 0$ , jediná možná nesplnitelná formule bez proměnných je  $S = \{\square\}$ , a máme jednokrokový důkaz  $S \vdash_R \square$ .

Jinak vyberme  $p \in \text{Var}(S)$ . Podle Lemmatu jsou  $S^p$  i  $S^{\bar{p}}$  nesplnitelné. Mají o proměnnou méně, tedy dle ind. předpokladu existují rezoluční stromy  $T$  pro  $S^p \vdash_R \square$  a  $T'$  pro  $S^{\bar{p}} \vdash_R \square$ .

Ukážeme, jak z  $T$  vyrobit rezoluční strom  $\hat{T}$  pro  $S \vdash_R \neg p$ . Analogicky  $\hat{T}'$  pro  $S \vdash_R p$  a potom už snadno vyrobíme rezoluční strom pro  $S \vdash_R \square$ : ke kořeni  $\square$  připojíme kořeny stromů  $\hat{T}$  a  $\hat{T}'$  jako levého a pravého syna (tj. získáme  $\square$  rezolucí z  $\{\neg p\}$  a  $\{p\}$ ).

# Dokončení důkazu

Rezoluční strom  $T$  pro  $S^p \vdash_R \Box \rightsquigarrow \hat{T}$  pro  $S \vdash_R \neg p$ :

Vrcholy i uspořádání jsou stejné, jen do některých klauzulí ve vrcholech přidáme literál  $\neg p$ .

Na každém listu stromu  $T$  je nějaká klauzule  $C \in S^p$ , a

- buď  $C \in S$ ,
- nebo  $C \notin S$ , ale  $C \cup \{\neg p\} \in S$

V prvním případě necháme label stejný. Ve druhém případě přidáme do  $C$  a do všech klauzulí nad tímto listem literál  $\neg p$ .

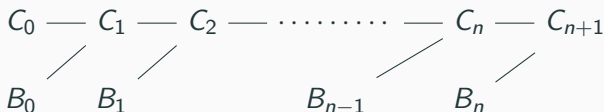
Listy jsou nyní klauzule z  $S$ , a každý vnitřní vrchol je nadále rezolventou svých synů. V kořeni jsme  $\Box$  změnili na  $\neg p$  (ledaže každý list  $T$  už byl klauzule z  $S$ , to ale už  $T$  dává  $S \vdash_R \Box$ ).  $\square$

## 5.4 LI-rezoluční a Horn-SAT

---

## Lineární důkaz: neformálně

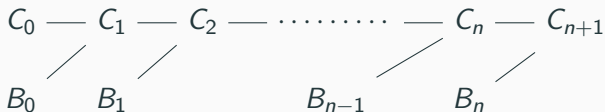
Rezoluční důkaz můžeme kromě rezolučního stromu zorganizovat i jinak, jako tzv. **lineární důkaz**:



- v každém kroku máme jednu **centrální** klauzuli
- tu resolvujeme s **boční** ('side') klauzulí
- boční klauzule je buď axiom z  $S$ , nebo některá z předchozích centrálních (jako bychom odvozené klauzule přidávali k axiomům)
- výsledná **rezolventa** je novou **centrální klauzulí**

(Tento pohled lépe odpovídá procedurálnímu výpočtu, jde jen o to, jak vybírat vhodné boční klauzule.)

## Lineární důkaz: formálně



**Lineární důkaz** klauzule  $C$  z formule  $S$  je konečná posloupnost

$$\left[ \begin{array}{c} C_0 \\ B_0 \end{array} \right], \left[ \begin{array}{c} C_1 \\ B_1 \end{array} \right], \dots, \left[ \begin{array}{c} C_n \\ B_n \end{array} \right], C_{n+1}$$

kde  $C_i$  říkáme **centrální** klauzule,  $C_0$  je **počáteční**,  $C_{n+1} = C$  je **koncová**,  $B_i$  jsou **boční** klauzule, a platí:

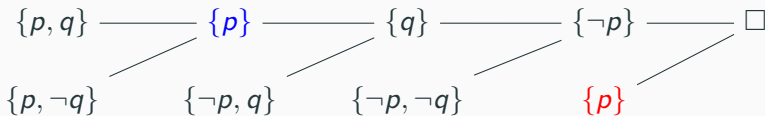
- $C_0 \in S$ , pro  $i \leq n$  je  $C_{i+1}$  rezolventou  $C_i$  a  $B_i$ ,
- $B_0 \in S$ , pro  $i \leq n$  je  $B_i \in S$  nebo  $B_i = C_j$  pro nějaké  $j < i$ .

**Lineární zamítnutí**  $S$  je lineární důkaz  $\square$  z  $S$ .



## Příklad a ekvivalence s rezolučním důkazem

Lineární zamítnutí  $S = \{\{p, q\}, \{p, \neg q\}, \{\neg p, q\}, \{\neg p, \neg q\}\}$  :



Poslední boční klauzule  $\{p\}$  není z  $S$ , ale je rovna předchozí centrální klauzuli.

**Poznámka:**  $C$  má lineární důkaz z  $S$ , právě když  $S \vdash_B C$ .

⇒ Z lineárního důkazu snadno vyrobíme rezoluční strom. Indukcí dle délky důkazu: máme-li boční klauzuli  $B_i \notin S$ , potom  $B_i = C_j$  pro nějaké  $j < i$ : místo  $B_i$  připojíme rezoluční strom pro  $C_j$  z  $S$ .

⇒ Plyne z úplnosti lineární rezoluce, důkaz najdete v učebnici.

- **lineární důkaz**: boční klauzule je **axiom nebo dřívější centrální**
- co když požadujeme, aby boční klauzule byly **pouze axiomy**?  
⇒ **LI-rezolute (linear-input)**

**LI-důkaz** (rezolucí) klauzule  $C$  z formule  $S$  je lineární důkaz

$$\left[ \begin{array}{c} C_0 \\ B_0 \end{array} \right], \left[ \begin{array}{c} C_1 \\ B_1 \end{array} \right], \dots, \left[ \begin{array}{c} C_n \\ B_n \end{array} \right], C$$

ve kterém je každá boční klauzule  $B_i$  axiom z  $S$ . Pokud LI-důkaz existuje, říkáme, že je  $C$  **LI-dokazatelná** z  $S$ , a píšeme  $S \vdash_{LI} C$ . Pokud  $S \vdash_{LI} \square$ , je  $S$  **LI-zamítnutelná**.

- LI-důkaz odpovídá rezolučnímu stromu tvaru “*chlupaté cesty*”
- z toho plyne korektnost
- ztrácíme úplnost, ale hledání důkazů je snazší
- ukážeme **úplnost pro Hornovy formule**, je základem Prologu

# Hornovy formule

- **Hornova klauzule** má nejvýše jeden pozitivní literál
- **Hornova formule** je množina Hornových klauzulí (i nekonečná)
- **Fakt** je pozitivní jednotková klauzule, např.  $\{p\}$
- **Pravidlo** je klauzule s právě jedním pozitivním a alespoň jedním negativním literálem
- Pravidlům a faktům říkáme **programové klauzule**
- **Cíl** je neprázdná klauzule bez pozitivního literálu
- dokazujeme sporem: **cíl** je negací toho, co chceme dokázat (konjunkce faktů)

**Pozorování:** Je-li Hornova formule  $S$  nesplnitelná a  $\square \notin S$ , potom obsahuje fakt i cíl.

**Důkaz:** Neobsahuje-li fakt, ohodnotíme všechny proměnné 0; neobsahuje-li cíl, ohodnotíme 1. □

## Příklad konstrukce LI-zamítnutí

Ukážeme:  $T = \{\{p, \neg r, \neg s\}, \{\neg q, r\}, \{q, \neg s\}, \{s\}\} \models p \wedge q$

Sestrojíme LI-zamítnutí  $T \cup \{G\} \vdash_{LI} \square$  pro cíl  $G = \{\neg p, \neg q\}$ .

V  $T$  najdeme fakt, a provedeme jednotkovou propagaci v  $T \cup \{G\}$ .

Opakujeme, dokud není formule prázdná:

- $T = \{\{p, \neg r, \neg s\}, \{\neg q, r\}, \{q, \neg s\}, \{s\}\}, G = \{\neg p, \neg q\}$
- $T^s = \{\{p, \neg r\}, \{\neg q, r\}, \{q\}\}, G^s = \{\neg p, \neg q\}$
- $T^{sq} = \{\{p, \neg r\}, \{r\}\}, G^{sq} = \{\neg p\}$
- $T^{sqr} = \{\{p\}\}, G^{sqr} = \{\neg p\}$
- $T^{sqrp} = \emptyset, G^{sqrp} = \square$

To, že vždy najdeme fakt, plyne z Pozorování pro  $T \cup \{G\}$ .

Nyní zpětným postupem sestrojíme LI-zamítnutí, podobně jako v důkazu úplnosti rezoluce.

# Konstrukce zamítnutí zpětným postupem

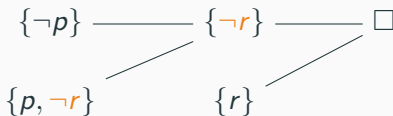
- $T^{sqrp}, G^{sqrp} \vdash_{LI} \Box$ :

$\Box$

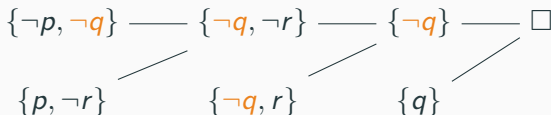
- $T^{sqr}, G^{sqr} \vdash_{LI} \Box$ :



- $T^{sq}, G^{sq} \vdash_{LI} \Box$ :



- $T^s, G^s \vdash_{LI} \square$ :



- $T, G \vdash_{LI} \square$



# Úplnost pro Hornovy formule

**Věta (O úplnosti LI-rezoluce pro Hornovy formule):** Je-li Hornova formule  $T$  splnitelná, a  $T \cup \{G\}$  je nespjitelná pro cíl  $G$ , potom  $T \cup \{G\} \vdash_{LI} \square$ , a to LI-zamítnutím, které začíná cílem  $G$ .

**Důkaz:** Opět lze díky Větě o kompaktnosti předpokládat, že  $T$  je konečná. LI-zamítnutí sestojíme indukcí podle počtu proměnných.

Z Pozorování víme, že  $T$  obsahuje fakt  $\{p\}$ . Protože  $T \cup \{G\}$  je nespjitelná, je dle Lemmatu o dosazení **nespjitelná i**  $(T \cup \{G\})^p = T^p \cup \{G^p\}$ , kde  $G^p = G \setminus \{\neg p\}$ .

Všimněte si, že  **$T^p$  je splnitelná**. (Stejným ohodnocením jako  $T$ , neboť to musí obsahovat  $p$  kvůli faktu  $\{p\}$ , tedy neobsahuje  $\neg p$ .)

Zároveň má  $T^p$  méně proměnných než  $T$ . **Je-li  $G^p$  cíl**, využijeme indukčního předpokladu (následující slide). Co když ale  $G^p$  není cíl?

Není-li  $G^P$  cíl, nutně  $G^P = \square$  a  $G = \{\neg p\}$ . Potom je  $\square$  rezolventou  $G$  a faktu  $\{p\} \in T$ , a máme jednokrokové LI-zamítnutí  $T \cup \{G\}$ . (To dává i bázi indukce.)

Je-li  $G^P$  cíl, dle indukčního předpokladu existuje LI-odvození  $\square$  z  $T^P \cup \{G^P\}$  začínající  $G^P = G \setminus \{\neg p\}$ .

Hledané LI-zamítnutí  $T \cup \{G\}$  začínající  $G$  zkonstruujeme (podobně jako v důkazu Věty o úplnosti rezoluce):

- Přidáme literál  $\neg p$  do všech listů, které už nejsou v  $T \cup \{G\}$  (vznikly odebráním  $\neg p$ ), a do všech vrcholů nad nimi.
- Tím získáme  $T \cup \{G\} \vdash_{LI} \neg p$ .
- Na závěr přidáme boční klauzuli  $\{p\}$  a odvodíme  $\square$ .  $\square$



# Program v Prologu

síla Prologu vychází z **unifikace** a rezoluce v predikátové logice, nyní si ale ukážeme příklad **výrokového** programu:

- **program** v Prologu je Hornova formule obsahující pouze **programové klauzule**, tj. **fakta** nebo **pravidla**
- **dotaz** je konjunkce faktů, negace dotazu je **cíl**

Např. program  $\{\{p, \neg r, \neg s\}, \{\neg q, r\}, \{q, \neg s\}, \{s\}\}$ , dotaz  $p \wedge q$

- klauzule  $\{p, \neg r, \neg s\}$  je ekvivalentní  $r \wedge s \rightarrow p$ , píšeme  $p:-r,s$ .
- výsledný program a dotaz:

$p:-r,s.$

$r:-q.$

$q:-s.$

$s.$

$?-p,q.$

**Důsledek:** Mějme program  $P$  a dotaz  $Q = p_1 \wedge \dots \wedge p_n$ , a označme  $G = \{\neg p_1, \dots, \neg p_n\}$  (tj.  $G \sim \neg Q$ ). Následující podmínky jsou ekvivalentní:

- (i)  $P \models Q$ ,
- (ii)  $P \cup \{G\}$  je nespílitelná,
- (iii)  $P \cup \{G\} \vdash_{LI} \square$ , a existuje LI-zamítnutí začínající cílem  $G$ .

**Důkaz:**

- (i) $\Leftrightarrow$ (ii) Věta o důkazu sporem
- (ii) $\Leftrightarrow$ (iii) Věta o úplnosti LI-rezoluce pro Hornovy formule  
(Program je vždy splnitelný) □