

Pátá přednáška

NAIL062 Výroková a predikátová logika

Jakub Bulín (KTIML MFF UK)

Zimní semestr 2023

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 τ výroku \perp z T . Konstrukce τ 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 τ 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 $T' \subseteq T$ sestrojíme 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

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

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** (φ, ψ, χ 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 φ z teorie T je **konečná** posloupnost výroků $\varphi_0, \dots, \varphi_n = \varphi$, ve které pro každé $i \leq n$:
 - φ_i je **logický axiom**, nebo
 - φ_i je **axiom teorie** ($\varphi_i \in T$), nebo
 - φ_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 ψ 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 φ_i z důkazu (tedy i $\varphi_n = \varphi$) platí v T .

- Je-li φ_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 φ_i pomocí modus ponens z φ_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** ℓ je p nebo $\neg p$ (pro $p \in \mathbb{P}$), $\bar{\ell}$ je **opačný literál** k ℓ
- **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 ℓ takový, že $\ell \in C_1$ a $\bar{\ell} \in C_2$.
Potom **rezolventa** klauzulí C_1 a C_2 **přes literál ℓ** je klauzule:

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

tedy z první klauzule odstraníme ℓ 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 :

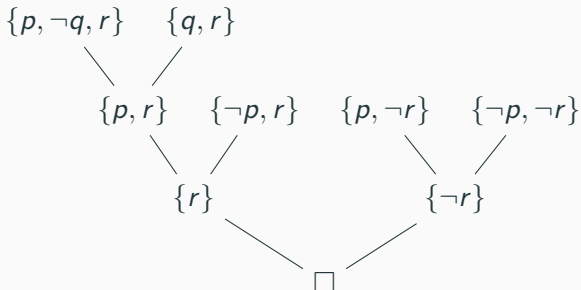
- $C_i \in S$, nebo
 - C_i je rezolventou nějakých C_j, C_k kde $j, k < i$
-
- existuje-li rez. důkaz, je C **rezolucí dokazatelná** z S , $S \vdash_R C$
 - **rezoluční zamítnutí** formule S je rezoluční důkaz \square z S
 - v tom případě je S **rezolucí zamítnutelná**

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 ℓ literál, potom **dosazení** ℓ do S je formule

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

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

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

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

Vezměme libovolnou klauzuli v S^ℓ . Ta je tvaru $C \setminus \{\bar{\ell}\}$ pro klauzuli $C \in S$ (neobsahující literál ℓ). 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 $\mathcal{V} \models C \setminus \{\bar{\ell}\}$.

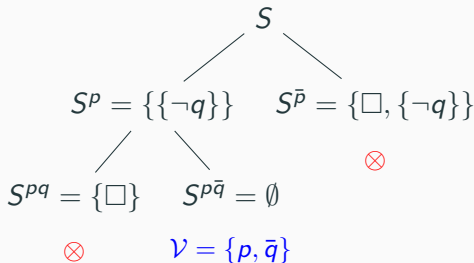
\Leftarrow BÚNO mějme ohodnocení $\mathcal{V} \models S^\ell$. Protože se $\bar{\ell}$ (ani ℓ) nevyskytuje v S^ℓ , platí také $\mathcal{V} \setminus \{\bar{\ell}\} \models S^\ell$. Ohodnocení $\mathcal{V}' = (\mathcal{V} \setminus \{\bar{\ell}\}) \cup \{\ell\}$ potom splňuje všechny $C \in S$, tedy $\mathcal{V}'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

- 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.