

Devátá přednáška

NAIL062 Výroková a predikátová logika

Jakub Bulín (KTIML MFF UK)

Zimní semestr 2023

Program

- Löwenheim-Skolemova věta
- věta o kompaktnosti
- hilbertovský kalkulus.
- úvod do rezoluce v predikátové logice
- skolemizace

Materiály

Zápisky z přednášky, Sekce 7.5-7.6 z Kapitoly 7, Sekce 8.1-8.2 z Kapitoly 8

7.5 Důsledky korektnosti a úplnosti

$$\vdash = \models$$

Syntaktickou analogií **důsledků** jsou **teorémy**:

$$\text{Thm}_L(T) = \{\varphi \mid \varphi \text{ je } L\text{-sentence a } T \vdash \varphi\}$$

Z korektnosti a úplnosti okamžitě dostáváme:

- $T \vdash \varphi$ právě když $T \models \varphi$
- $\text{Thm}_L(T) = \text{Csq}_L(T)$

Všude můžeme nahradit '**platnost**' pojmem '**dokazatelnost**'. Např:

- T je **sporná**, je-li v ní dokazatelný spor (tj. $T \vdash \perp$)
- T je **kompletní**, je-li pro každou sentenci buď $T \vdash \varphi$ nebo $T \vdash \neg\varphi$, ale ne obojí (jinak by byla sporná)

Věta (O dedukci): $T, \varphi \vdash \psi$ právě když $T \vdash \varphi \rightarrow \psi$.

Důkaz: Stačí dokázat: $T, \varphi \models \psi \Leftrightarrow T \models \varphi \rightarrow \psi$. To je snadné. \square

Löwenheim-Skolemova věta & Věta o kompaktnosti

Věta (Löwenheim-Skolemova): Je-li L spočetný bez rovnosti, potom každá bezesporná L -teorie má spočetně nekonečný model.

(Později ukážeme i verzi s rovností, kan. model může být konečný.)

Důkaz: ∇T není dokazatelný spor. Dokončené tablo z T s $F \perp$ v kořeni tedy musí obsahovat bezespornou větev. Hledaný model je L -redukt kanonického modelu pro tuto větev. \square

Věta o kompaktnosti, vč. důkazu, je stejná jako ve výrokové logice:

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

Důkaz: Model teorie je modelem každé části. Naopak, pokud T nemá model, je sporná, tedy $T \vdash \perp$. Vezměme nějaký **konečný** tablo důkaz \perp z T . K jeho konstrukci stačí konečně mnoho axiomů T , ty tvoří konečnou podteorii $T' \subseteq T$, která nemá model. \square

Nestandardní model přirozených čísel

- $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$ je **standardní model** přirozených čísel
- **teorie struktury** $\text{Th}(\underline{\mathbb{N}})$: všechny sentence **pravdivé** v $\underline{\mathbb{N}}$
- **n -tý numerál**: term $\underline{n} = S(S(\cdots (S(0) \cdots)))$, kde S je n -krát

Přidáme nový konstantní symbol c a vyjádříme, že je ostře větší než každý n -tý numerál:

$$T = \text{Th}(\underline{\mathbb{N}}) \cup \{\underline{n} < c \mid n \in \mathbb{N}\}$$

- každá konečná část T má model
- dle věty o kompaktnosti: i T má model
- říkáme mu **nestandardní model** (označme \mathcal{A})
- platí v něm tytéž sentence, které platí ve standardním modelu
- ale zároveň obsahuje prvek $c^{\mathcal{A}}$, který je větší než každé $n \in \mathbb{N}$ (tzn. větší než hodnota termu \underline{n} v nestandardním modelu \mathcal{A})

7.6 Hilbertovský kalkulus v predikátové logice

Hilbertovský kalkulus v predikátové logice

- používá jen \neg a \rightarrow , dokazuje lib. formule (nejen sentence)
 - **schémata log. axiomů** (φ, ψ, χ formule, t term, x proměnná)
 - (i) $\varphi \rightarrow (\psi \rightarrow \varphi)$
 - (ii) $(\varphi \rightarrow (\psi \rightarrow \chi)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \chi))$
 - (iii) $(\neg\varphi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \varphi)$
 - (iv) $(\forall x)\varphi \rightarrow \varphi(x/t)$ je-li t substituovatelný za x do φ
 - (iiv) $(\forall x)(\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow (\forall x)\psi)$ není-li x volná ve φ
- a navíc **axiomy rovnosti**, je-li jazyk s rovností

- **odvozovací pravidla:**

$$\frac{\varphi, \varphi \rightarrow \psi}{\psi} \text{ (modus ponens)}$$

$$\frac{\varphi}{(\forall x)\varphi} \text{ (generalizace)}$$

- **hilbertovský důkaz** formule φ z T je **konečná** posloupnost $\varphi_0, \dots, \varphi_n = \varphi$, kde φ_i je **logický axiom** (vč. axiomů rovnosti), **axiom teorie**, nebo lze odvodit z předchozích pomocí pravidel
- existuje-li, píšeme $T \vdash_H \varphi$

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

Důkaz: Indukcí dle délky důkazu: každá φ_i (vč. $\varphi_n = \varphi$) platí v T

- logické axiomy (vč. axiomů rovnosti) jsou tautologie, platí v T
- axiomy z T jistě v T také platí
- modus ponens i generalizace jsou **korektní** inferenční pravidla:
 - je-li $T \models \varphi$ a $T \models \varphi \rightarrow \psi$, potom $T \models \psi$
 - je-li $T \models \varphi$, potom $T \models (\forall x)\varphi$ □

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

Důkaz vynecháme.

KAPITOLA 8: REZOLUCE V PREDIKÁTOVÉ LOGICE

8.1 Úvod

Rezoluce v predikátové logice

$T \models \varphi? \rightsquigarrow T \cup \{\neg\varphi\} \rightsquigarrow$ CNF formule $S \rightsquigarrow$ rezoluční zamítnutí

- **literál** je **atomická formule** $R(t_1, \dots, t_n)$ nebo její negace
- **klauzule** je konečná množina literálů, **formule** množina klauzulí
- otevřenou formuli snadno převedeme do CNF, i univerzální kvantifikátor na začátku: $(\forall x)(P(x) \vee \neg Q(x)) \rightsquigarrow \{P(x), \neg Q(x)\}$
- co s existenčními kvantifikátory? nové symboly pro ‘svědky’
 $(\exists x)(P(x) \vee \neg Q(x)) \rightsquigarrow \{P(c), \neg Q(c)\}$ “**skolemizace**”
- není ekvivalentní, ale zachovává **[ne]splnitelnost**, to nám stačí
- rezoluční krok? literály nemusí být stejné, stačí **unifikovatelné**
z klauzulí $\{P(x), \neg Q(x)\}$ a $\{Q(f(c))\}$ odvodíme $\{P(f(c))\}$
- **unifikace** je substituce $\{x/f(c)\}$

1. $T = \{(\forall x)P(x), (\forall x)(P(x) \rightarrow Q(x))\}, \varphi = (\exists x)Q(x)$

$$\neg\varphi = \neg(\exists x)Q(x) \sim (\forall x)\neg Q(x) \sim \neg Q(x)$$

$T \cup \{\neg\varphi\}$ je **ekvivalentní** $S = \{\{P(x)\}, \{\neg P(x), Q(x)\}, \{\neg Q(x)\}\}$
rezoluční zamítnutí: představte si p místo $P(x)$, q místo $Q(x)$

2. $T = \{(\forall x)(\exists y)R(x, y), R(x, y) \rightarrow Q(x)\}, \varphi = (\exists x)Q(x)$

$$T \cup \{\neg\varphi\} \sim \{(\forall x)(\exists y)R(x, y), \neg R(x, y) \vee Q(x), \neg Q(x)\}$$

formuli $(\forall x)(\exists y)R(x, y)$ nahradíme $R(x, f(x))$, kde f je nový unární funkční symbol (reprezentuje **výběr svědka**):

$$S = \{\{R(x, f(x))\}, \{\neg R(x, y), Q(x)\}, \{\neg Q(x)\}\}$$

není ekvivalentní, ale **ekvisplnitelná** (zde obě nesplnitelné), vidíme po **substituci** $y/f(x)$, která **unifikuje** $R(x, f(x))$ a $R(x, y)$

$$S = \{\{R(x, f(x))\}, \{\neg R(x, y), Q(x)\}, \{\neg Q(x)\}\}$$

- na úrovni výrokové logiky (ground level):

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

není nesplnitelné! musíme využít, že $R(x, f(x))$ a $R(x, y)$ mají 'podobnou strukturu' (jsou **unifikovatelné**)

- klauzule $\{\neg R(x, y), Q(x)\}$ platí i po provedení libovolné substituce: $\{\neg R(x/t), Q(x/t)\}$ je důsledek S pro lib. term t
- představme si 'přidání' všech takto získaných klauzulí do S : potom už je na ground level nesplnitelné (ale nekonečné)
- **unifikační algoritmus** nám dá správnou substituci $y/f(x)$
- zahrneme už do **rezolučního pravidla**, tedy **rezolventou** klauzulí $\{P(c)\}$ a $\{\neg P(x), Q(x)\}$ bude klauzule $\{Q(c)\}$.

- zahrnuje aplikaci unifikace
- lze vybrat **více literálů najednou**, ale musí být unifikovatelné:

např. z $\{R(x, f(x)), R(g(y), z)\}, \{\neg R(g(c), u), P(u)\}$
odvodíme rezolventu $\{P(f(g(c)))\}$ za použití **unifikace**

$$\{x/g(c), y/c, z/f(g(c)), u/f(g(c))\}$$

- budeme vyžadovat disjunktní množiny proměnných v klauzulích; lze přejmenovat, proměnné mají **lokální význam**:

$$\models (\forall x)(\psi \wedge \chi) \leftrightarrow (\forall x)\psi \wedge (\forall x)\chi$$

8.2 Skolemizace

Ekvisplnitelná otevřená teorie

- teorie T v jazyce L a T' v (ne nutně stejném) jazyce L' jsou **ekvisplnitelné**, pokud platí: T má model $\Leftrightarrow T'$ má model
- zajímá nás jen [ne]splnitelnost (dokazujeme sporem)
- pro převod do CNF a rezoluci potřebujeme otevřené formule

Cíl: Ke každé teorii T sestrojíme **ekvisplnitelnou, otevřenou** T' .

1. převod do **prenexní normální formy** (vytkneme kvantifikátory)
2. nahradíme generálními uzávěry (**potřebujeme sentence!**)
3. nahradíme sentence **Skolemovými variantami** (odstranění \exists)
4. odstraníme zbývající \forall , máme otevřené formule

Prenexní normální forma

Formule φ je v **prenexní normální formě (PNF)**, je-li následujícího tvaru, kde $Q_i \in \{\forall, \exists\}$ a formule φ' je otevřená:

$$(Q_1x_1) \dots (Q_nx_n)\varphi'$$

- $(Q_1x_1) \dots (Q_nx_n)$ je **kvantifikátorový prefix**, φ' **otevřené jádro**
- **univerzální** formule: v PNF a všechny kvantifikátory jsou \forall

Tvrzení: Ke každé formuli φ existuje **ekvivalentní** formule v PNF.

Důkaz: nahrazujeme podformule ekvivalentními s cílem posunout kvantifikátory blíž kořeni $\text{Tree}(\varphi)$, dle pravidel z násl. Lemmatu. \square

Důsledek: Existuje i ekvivalentní PNF **sentence** (generální uzávěr).

Pravidla vytýkání kvantifikátorů

Lemma: Označme \overline{Q} opačný kvantifikátor ke Q . Jsou-li φ a ψ formule, kde x není volná v ψ , potom:

$$\begin{aligned}\neg(Qx)\varphi &\sim (\overline{Q}x)\neg\varphi \\ (Qx)\varphi \wedge \psi &\sim (Qx)(\varphi \wedge \psi) \\ (Qx)\varphi \vee \psi &\sim (Qx)(\varphi \vee \psi) \\ (Qx)\varphi \rightarrow \psi &\sim (\overline{Q}x)(\varphi \rightarrow \psi) \\ \psi \rightarrow (Qx)\varphi &\sim (Qx)(\psi \rightarrow \varphi)\end{aligned}$$

Důkaz: snadno ověříme sémanticky, nebo tablo metodou (potom ale nejsou-li sentence, musíme nahradit generálními uzávěry) \square

Pozorování: Nahradíme-li ve φ podformuli ψ ekvivalentní ψ' , je i výsledná formule φ' ekvivalentní φ . (Připomeňme: $\varphi \sim \varphi'$ právě když mají stejné modely, tj. $\models \varphi \leftrightarrow \varphi'$)

Převod do PNF: příklad

$$(\forall z)P(x, z) \wedge P(y, z) \rightarrow \neg(\exists x)P(x, y)$$

$$\sim (\forall u)P(x, u) \wedge P(y, z) \rightarrow (\forall x)\neg P(x, y)$$

$$\sim (\forall u)(P(x, u) \wedge P(y, z)) \rightarrow (\forall v)\neg P(v, y)$$

$$\sim (\exists u)(P(x, u) \wedge P(y, z) \rightarrow (\forall v)\neg P(v, y))$$

$$\sim (\exists u)(\forall v)(P(x, u) \wedge P(y, z) \rightarrow \neg P(v, y))$$

- v prvním kroku přejmenujeme z na u , **nesmí být volná** v $P(y, z)$
- podobně ve druhém kroku x na v
- která pravidla používáme? sledujte postup na stromu formule
- chceme-li sentenci:

$$(\forall x)(\forall y)(\forall z)(\exists u)(\forall v)(P(x, u) \wedge P(y, z) \rightarrow \neg P(v, y))$$

1. proč se při vytýkání z **antecedentu** mění kvantifikátor?

$$\begin{aligned}(Qx)\varphi \rightarrow \psi &\sim \neg(Qx)\varphi \vee \psi \\ &\sim (\overline{Q}x)(\neg\varphi) \vee \psi \\ &\sim (\overline{Q}x)(\neg\varphi \vee \psi) \sim (\overline{Q}x)(\varphi \rightarrow \psi)\end{aligned}$$

2. proč nesmí být x volná v ψ ? neplatilo by, např:

$$(\exists x)P(x) \wedge Q(x) \not\sim (\exists x)(P(x) \wedge Q(x))$$

musíme přejmenovat vázanou proměnnou x na novou:

$$(\exists x)P(x) \wedge Q(x) \sim (\exists y)P(y) \wedge Q(x) \sim (\exists y)(P(y) \wedge Q(x))$$

3. PNF není jednoznačná, lze vytýkat v různém pořadí; lepší je nejprve vytknout ty, **ze kterých se nakonec stanou existenční**:

$$(\exists y)(\forall x)\varphi(x, y) \text{ je lepší než } (\forall x)(\exists y)\varphi(x, y)$$

(protože “ y nezávisí na x ”)

Skolemova varianta

Je-li PNF sentence **univerzální**, tvaru $(\forall x_1) \dots (\forall x_n) \psi(x_1, \dots, x_n)$, nahradíme otevřeným jádrem ψ . Jinak musíme provést **skolemizaci**:

Buď φ **L-sentence** v PNF, všechny vázané proměnné různé. Nechť

- existenční kvantifikátory jsou $(\exists y_1), \dots, (\exists y_n)$ (v tom pořadí)
- pro každé i jsou $(\forall x_1), \dots, (\forall x_{n_i})$ právě všechny univerzální kvantifikátory předcházející $(\exists y_i)$ v prefixu φ

Buď L' rozšíření L o **nové** funkční symboly f_1, \dots, f_n , kde f_i je n_i -ární.

Skolemova varianta φ je L' -sentence φ_S vzniklá **odstraněním** $(\exists y_i)$ a substitucí termu $f_i(x_1, \dots, x_{n_i})$ za y_i , postupně pro $i = 1, \dots, n$.

$$\varphi = (\exists y_1)(\forall x_1)(\forall x_2)(\exists y_2)(\forall x_3) R(y_1, x_1, x_2, y_2, x_3)$$

$$\varphi_S = (\forall x_1)(\forall x_2)(\forall x_3) R(f_1, x_1, x_2, f_2(x_1, x_2), x_3)$$

- **musí být sentence!** pro $(\exists y)E(x, y)$ ne ~~$E(x, c)$~~ ale $E(x, f(x))$
- **nové symboly!** (jedinou rolí je reprezentovat 'svědky' ve φ)

Je to konzervativní extenze

Lemma: Bud' φ L -sentence $(\forall x_1) \dots (\forall x_n)(\exists y)\psi$, f nový funkční symbol, a φ' sentence $(\forall x_1) \dots (\forall x_n)\psi(y/f(x_1, \dots, x_n))$. Potom:

- (i) L -redukt každého modelu φ' je modelem φ , a
- (ii) každý model φ lze expandovat na model φ' .

Důkaz: (i) Bud' \mathcal{A}' model φ' , \mathcal{A} jeho L -redukt, $e : \text{Var} \rightarrow \mathcal{A}$.

$\mathcal{A} \models \varphi[e]$ platí neboť $\mathcal{A} \models \psi[e(y/a)]$ pro $a = (f(x_1, \dots, x_n))^{\mathcal{A}'}[e]$.

(ii) Protože $\mathcal{A} \models \varphi$, existuje funkce $f^A : A^n \rightarrow A$, že pro každé ohodnocení e platí $\mathcal{A} \models \psi[e(y/a)]$ pro $a = f^A(e(x_1), \dots, e(x_n))$.

To znamená, že expanze o funkci f^A splňuje φ' . □

- říká, že $\{\varphi'\}$ je konzervativní extenze $\{\varphi\}$, opakovaná aplikace dává **Skolemovu větu** (výsledek skolemizace je otevřená konzervativní extenze, speciálně je ekvivalentní)
- expanze v (ii) není jednoznačná (na rozdíl od extenze o definici nového funkčního symbolu)

Skolemova věta (shrnutí postupu)

Věta: Každá teorie má otevřenou konzervativní extenzi.

Důkaz Mějme L -teorii T . Axiomy nahradíme generálními uzávěry a převedeme do PNF, máme ekvivalentní L -teorii T' . V ní každý axiom nahradíme jeho Skolemovou variantou.

Tím získáme teorii T'' v rozšířeném jazyce L' . Lemma říká:

- L -redukt každého modelu T'' je model T'
- každý model T' lze expandovat do L' na model T''

Neboli T'' je konzervativní extenzí T' , tedy i T . Je axiomatizovaná univerzálními sentencemi, odstraníme kvantifikátorové prefixy (vezmeme jádra) a máme ekvivalentní otevřenou teorii T''' . \square

Důsledek: Ke každé teorii můžeme pomocí skolemizace najít ekvivalentní otevřenou teorii. (A tu už snadno převedeme do CNF.)