

Jedenáctá přednáška

NAIL062 Výroková a predikátová logika

Jakub Bulín (KTIML MFF UK)

Zimní semestr 2024

Program

- LI-rezoluce a Prolog
- elementární ekvivalence
- izomorfismus a konečné modely
- definovatelnost a automorfismy
- ω -kategoricita a úplnost

Materiály

Zápisky z přednášky, Sekce 8.7 z Kapitoly 8, Sekce 9.1-9.3 z Kapitoly 9

8.7 LI-rezoluće

Lineární důkaz a LI-důkaz

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

$$\begin{bmatrix} C_0 \\ B_0 \end{bmatrix}, \begin{bmatrix} C_1 \\ B_1 \end{bmatrix}, \dots, \begin{bmatrix} C_n \\ B_n \end{bmatrix}, C_{n+1}$$

kde: B_0 a C_0 jsou varianty klauzulí z S , $C_{n+1} = C$,

- C_{i+1} je rezolventa C_i a B_i
- B_i **varianta** klauzule z S nebo $B_i = C_j$ pro nějaké $j < i$.
- **Lineární zamítnutí** S je lineární důkaz \square z S
- **LI-důkaz** je lin. důkaz, kde vš. B_i jsou varianty klauzulí z S
- C **LI-dokazatelná** z S , $S \vdash_{LI} C$, pokud existuje LI-důkaz
- S je **LI-zamítnutelná**, pokud $S \vdash_{LI} \square$
- korektnost (lineární i LI-rezoluce) je zřejmá

Úplnost LI-rezoluce pro Hornovy formule

Věta (O úplnosti lineární rezoluce): C má lineární důkaz z S , právě když má rezoluční důkaz z S (tj. $S \vdash_R C$).

Důkaz: převodem na VL (Lifting lemma zachovává linearitu) \square

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: úplnost ve VL + Herbrandova věta + Lifting lemma \square

- **Hornova formule:** množina Hornových klauzulí
- **Hornova klauzule:** nejvýše jeden pozitivní literál
- **Pravidlo:** klauzule s 1 pozitivním a alespoň 1 negativním literálem
- **Fakt:** pozitivní jednotková klauzule
- **Cíl:** neprázdná klauzule bez pozitivního literálu
- **Programové klauzule:** pravidla a fakta
- **Program:** Hornova formule obsahující jen programové klauzule

Program v Prologu

```
son(X,Y):-father(Y,X),man(X).    {son(X, Y), ¬father(Y, X), ¬man(X)}  
son(X,Y):-mother(Y,X),man(X).   {son(X, Y), ¬mother(Y, X), ¬man(X)}  
man(charlie).                    {man(charlie)}  
father(bob,charlie).             {father(bob, charlie)}  
mother(alice,charlie).           {mother(alice, charlie)}  
  
?-son(charlie,X).                {¬son(charlie, X)}
```

Platí v programu daný **existenční dotaz**, $P \models (\exists X)son(charlie, X)$?

Důsledek: Pro program P a cíl $G = \{\neg A_1, \dots, \neg A_k\}$ v proměnných X_1, \dots, X_n jsou následující ekvivalentní:

- $P \models (\exists X_1) \dots (\exists X_n)(A_1 \wedge \dots \wedge A_k)$
- $P \cup \{G\}$ má LI-zamítnutí začínající G

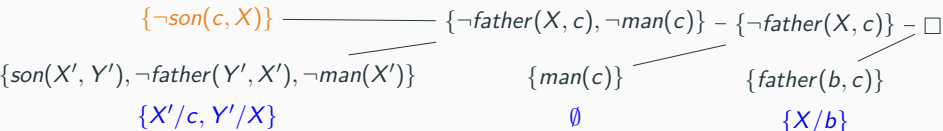
Důkaz: Plyne z Důkazu sporem a Úplnosti LI-rezoluce pro Hornovy formule (Program je vždy splnitelný). □

Je-li odpověď na dotaz kladná, chceme znát i **výstupní substituci** σ , tj. složení unifikací z rez. kroků, zúžené na proměnné v G . Platí:

$$P \models (A_1 \wedge \dots \wedge A_k)\sigma$$

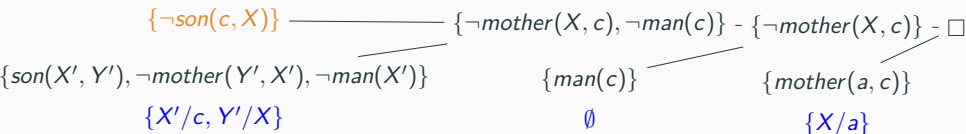
Příklady

?-son(charlie,X).



X=bob

výstupní substituce $\sigma = \{X/b\}$



X=alice

výstupní substituce $\sigma = \{X/a\}$

ČÁST III – POKROČILÉ PARTIE

KAPITOLA 9: TEORIE MODELŮ

- vztah mezi vlastnostmi teorií a tříd jejich modelů
 - bližší matematice než informatice a aplikacím
 - jen několik vybraných dostupných výsledků
- + co je třeba pro Gödelovy věty (Kapitola 10)
- + co se nevešlo jinam

9.1 Elementární ekvivalence

Teorie struktury \mathcal{A} (v jazyce L):

$$\text{Th}(\mathcal{A}) = \{\varphi \mid \varphi \text{ je } L\text{-sentence a } \mathcal{A} \models \varphi\}$$

Např. pro standardní model aritmetiky $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$ říkáme $\text{Th}(\underline{\mathbb{N}})$ aritmetika přirozených čísel, je nerozhodnutelná (neexistuje algoritmus, který pro každou φ doběhne a odpoví, zda $T \models \varphi$)

Pozorování: Nechť \mathcal{A} je L -struktura a T je L -teorie.

- $\text{Th}(\mathcal{A})$ je kompletní teorie
- $\mathcal{A} \in M_L(T) \Rightarrow \text{Th}(\mathcal{A})$ je (kompletní) jednoduchá extenze T
- $\mathcal{A} \in M_L(T)$, T kompletní $\Rightarrow \text{Th}(\mathcal{A}) = \text{Csq}_L(T) \sim T$

Elementární ekvivalence

L -struktury \mathcal{A} a \mathcal{B} jsou **elementárně ekvivalentní** ($\mathcal{A} \equiv \mathcal{B}$), pokud v nich platí tytéž L -sentence, neboli: $\mathcal{A} \equiv \mathcal{B} \Leftrightarrow \text{Th}(\mathcal{A}) = \text{Th}(\mathcal{B})$

Například pro $\langle \mathbb{R}, \leq \rangle$, $\langle \mathbb{Q}, \leq \rangle$, $\langle \mathbb{Z}, \leq \rangle$

- $\langle \mathbb{R}, \leq \rangle \equiv \langle \mathbb{Q}, \leq \rangle$: snadno pomocí **hustoty**
- $\langle \mathbb{Q}, \leq \rangle \not\equiv \langle \mathbb{Z}, \leq \rangle$: v $\langle \mathbb{Z}, \leq \rangle$ má každý prvek bezprostředního následníka, v $\langle \mathbb{Q}, \leq \rangle$ ne, tedy $\varphi \in \text{Th}(\langle \mathbb{Z}, \leq \rangle) \setminus \text{Th}(\langle \mathbb{Q}, \leq \rangle)$ pro následující sentenci:

$$\varphi = (\forall x)(\exists y)(x \leq y \wedge \neg x = y \wedge (\forall z)(x \leq z \rightarrow z = x \vee y \leq z))$$

Kompletní jednoduché extenze

Pro teorii T nás hlavně zajímá, jak vypadají modely.

- T je **kompletní**, právě když má jediný model až na elementární ekvivalenci (všechny modely jsou elementárně ekvivalentní)
- Modely T až na elementární ekvivalenci jednoznačně odpovídají **kompletním jednoduchým extenzím** T , ty jsou tvaru $\text{Th}(\mathcal{A})$ pro $\mathcal{A} \in \mathcal{M}(T)$, kde $\mathcal{A} \equiv \mathcal{B} \Leftrightarrow \text{Th}(\mathcal{A}) = \text{Th}(\mathcal{B})$

Místo hledání modelů stačí najít kompletní jednoduché extenze!

Motivace: ukážeme, že lze-li **efektivně popsat** všechny kompletní jednoduché extenze **efektivně dané** teorie, potom je **rozhodnutelná**.

- algoritmus, který pro vstup (i, j) vypíše j -tý axiom i -té kompletní jednoduché extenze (v nějakém očíslování)
- algoritmus, který postupně vygeneruje všechny axiomy teorie

Schopnost efektivně popsat kompletní jedn. extenze je vzácná, vyžaduje silné předpoklady, ale u mnoha důležitých teorií to lze.

Příklad: DeLO*

Teorie **hustého lin. uspořádání (DeLO*)** je extenze teorie uspořádání o **linearitu (dichotomii)**, **hustotu**, a někdy se přidává **netrivialita**:

- $x \leq y \vee y \leq x$
- $x \leq y \wedge \neg x = y \rightarrow (\exists z)(x \leq z \wedge z \leq y \wedge \neg z = x \wedge \neg z = y)$
- $(\exists x)(\exists y)(\neg x = y)$

Tvrzení: Buď $\varphi = (\exists x)(\forall y)(x \leq y)$ a $\psi = (\exists x)(\forall y)(y \leq x)$.
Následující jsou právě všechny kompletní jednoduché extenze DeLO* (až na ekvivalenci):

- | | |
|--|--|
| ▪ $\text{DeLO} = \text{DeLO}^* \cup \{\neg\varphi, \neg\psi\}$ | ▪ $\text{DeLO}^- = \text{DeLO}^* \cup \{\varphi, \neg\psi\}$ |
| ▪ $\text{DeLO}^+ = \text{DeLO}^* \cup \{\neg\varphi, \psi\}$ | ▪ $\text{DeLO}^\pm = \text{DeLO}^* \cup \{\varphi, \psi\}$ |

Stačí ukázat, že jsou kompletní. Potom už je zřejmé, že žádná další kompletní jednoduchá extenze DeLO* nemůže existovat.

Jak ukážeme, kompletnost plyne z faktu, že jsou **ω -kategorické**, tj. mají jediný spočetný model až na **izomorfismus**.

Důsledky Löwenheim-Skolemovy věty bez rovnosti

Připomeňme:

Věta (L.-S. bez rovnosti): Ve spočetném jazyce bez rovnosti má každá bezesporná teorie spočetně nekonečný model.

Jednoduchý důsledek:

Důsledek: Je-li L spočetný bez rovnosti, potom ke každé L -struktuře existuje elementárně ekvivalentní spočetně nekonečná struktura.

Důkaz: $\text{Th}(\mathcal{A})$ je bezesporná (má model \mathcal{A}), tedy dle L.-S. věty má spočetně nekonečný model $\mathcal{B} \models \text{Th}(\mathcal{A})$, to znamená $\mathcal{B} \equiv \mathcal{A}$. \square

Bez rovnosti tedy nelze vyjádřit např. 'model má právě 42 prvků'.

Důsledky Löwenheim-Skolemovy věty s rovností

V důkazu L.-S. věty máme kanonický model pro bezespornou větev tabla z T pro $F \perp$; pro jazyk s rovností stačí faktorizovat dle $=^A$:

Věta (L.-S. s rovností): Ve spočetném jazyce s rovností má každá bezesporná teorie spočetný model (konečný, nebo nekonečný).

I tato verze má snadný důsledek pro konkrétní struktury:

Důsledek: Je-li L spočetný s rovností, ke každé **nekonečné** L -struktuře existuje elem. ekvivalentní spočetně nekonečná struktura.

Důkaz: Mějme nekonečnou L -strukturu \mathcal{A} . Podobně jako v důkazu Důsledku bez rovnosti najdeme **spočetnou** $\mathcal{B} \equiv \mathcal{A}$.

Protože v \mathcal{A} platí pro každé $n \in \mathbb{N}$ sentence vyjadřující 'existuje alespoň n prvků' (což lze pomocí rovnosti snadno zapsat), platí i v \mathcal{B} , tedy \mathcal{B} musí být nekonečná. □

Spočetné algebraicky uzavřené těleso

- algebraicky uzavřené těleso: každý polynom nenulového stupně v něm má kořen
- \mathbb{Q} není, $x^2 - 2$ nemá v \mathbb{Q} kořen
- \mathbb{R} není, $x^2 + 1$ nemá v \mathbb{R} kořen
- \mathbb{C} je algebraicky uzavřené, ale je nespočetné

Algebraickou uzavřenost vyjádříme sentencemi ψ_n , pro $n > 0$:

$$(\forall x_{n-1}) \dots (\forall x_0)(\exists y)(y^n + x_{n-1} \cdot y^{n-1} + \dots + x_1 \cdot y + x_0) = 0$$

kde y^k je zkratka za term $y \cdot y \cdot \dots \cdot y$

Důsledek: Existuje spočetné algebraicky uzavřené těleso.

Důkaz: Dle Důsledku L.S. věty (s rovností) existuje spočetně nekonečná $\mathcal{A} \equiv \mathbb{C}$. Protože \mathbb{C} je těleso a splňuje ψ_n pro všechna $n > 0$, je i \mathcal{A} algebraicky uzavřené těleso. □

9.2 Izomorfismus struktur

Definice izomorfismu

Izomorfismus \mathcal{A} a \mathcal{B} ($\forall L = \langle \mathcal{R}, \mathcal{F} \rangle$) je bijekce $h: A \rightarrow B$ splňující:

- pro každý (n -ární) $f \in \mathcal{F}$ a pro všechna $a_i \in A$:

$$h(f^{\mathcal{A}}(a_1, \dots, a_n)) = f^{\mathcal{B}}(h(a_1), \dots, h(a_n))$$

- speciálně, je-li $c \in \mathcal{F}$ konstantní: $h(c^{\mathcal{A}}) = c^{\mathcal{B}}$
- pro každý (n -ární) $R \in \mathcal{R}$ a pro všechna $a_i \in A$:

$$R^{\mathcal{A}}(a_1, \dots, a_n) \text{ právě když } R^{\mathcal{B}}(h(a_1), \dots, h(a_n))$$

Existuje-li, jsou **izomorfní** ('via h '), $\mathcal{A} \simeq \mathcal{B}$ (nebo $\mathcal{A} \simeq_h \mathcal{B}$).

Automorfismus \mathcal{A} je izomorfismus \mathcal{A} a \mathcal{A} .

- tj. liší se jen 'pojmenováním prvků'
- relace 'být izomorfní' je ekvivalence
- např. potenční algebra $\mathcal{P}(X) = \langle \mathcal{P}(X), -, \cap, \cup, \emptyset, X \rangle$, $|X| = n$,
je izomorfní s $\underline{2}^n = \langle \{0, 1\}^n, -, \wedge_n, \vee_n, (0, \dots, 0), (1, \dots, 1) \rangle$
(operace po složkách) via $h(A) = \chi_A$ (charakt. vektor $A \subseteq X$)

Izomorfismus zachovává sémantiku & vztah \simeq a \equiv

Tvrzení: Bijekce $h: A \rightarrow B$ je izomorfismus \mathcal{A} a \mathcal{B} , právě když:

(i) pro každý term t a $e: \text{Var} \rightarrow A$: $h(t^{\mathcal{A}}[e]) = t^{\mathcal{B}}[e \circ h]$

(ii) pro každou φ a $e: \text{Var} \rightarrow A$: $\mathcal{A} \models \varphi[e] \Leftrightarrow \mathcal{B} \models \varphi[e \circ h]$

Důkaz: \Rightarrow snadno indukcí podle struktury termu resp. formule

\Leftarrow je-li h bijekce splňující (i)&(ii), dosazení $t = f(x_1, \dots, x_n)$ resp. $\varphi = R(x_1, \dots, x_n)$ dává vlastnosti z definice izomorfismu \square

Důsledek: $\mathcal{A} \simeq \mathcal{B} \Rightarrow \mathcal{A} \equiv \mathcal{B}$.

Důkaz: pro každou sentenci φ máme z (ii) $\mathcal{A} \models \varphi \Leftrightarrow \mathcal{B} \models \varphi$ \square

Naopak obecně ne, $\langle \mathbb{Q}, \leq \rangle \equiv \langle \mathbb{R}, \leq \rangle$, $\langle \mathbb{Q}, \leq \rangle \not\equiv \langle \mathbb{R}, \leq \rangle$ Platí ale:

Tvrzení: Jsou-li \mathcal{A}, \mathcal{B} konečné v jazyce s rovností, potom

$$\mathcal{A} \simeq \mathcal{B} \Leftrightarrow \mathcal{A} \equiv \mathcal{B}$$

Důsledek Pokud má kompletní teorie v jazyce s rovností konečný model, potom jsou všechny její modely izomorfní.

Důkaz $\equiv \Rightarrow \simeq$ pro konečné struktury s rovností

Díky = vyjádříme “existuje právě n prvků”, z toho plyne $|A| = |B|$.

Bud' \mathcal{A}' expanze \mathcal{A} o jména prvků, v jazyce $L' = L \cup \{c_a \mid a \in A\}$.

Ukážeme, že \mathcal{B} lze expandovat na L' -strukturu \mathcal{B} tak, že $\mathcal{A}' \equiv \mathcal{B}'$.

Potom je $h(a) = c_a^{\mathcal{B}'}$ izomorfismus \mathcal{A}' a \mathcal{B}' , i pro L -redukty $\mathcal{A} \simeq \mathcal{B}$.

Stačí ukázat, že pro $c_a^{\mathcal{A}'} = a \in A$ existuje $b \in B$ tak, že expanze o interpretaci konstantního symbolu c_a splňují $\langle \mathcal{A}, a \rangle \equiv \langle \mathcal{B}, b \rangle$.

Bud' Ω množina ‘vlastností prvku a ’, tj. formulí $\varphi(x)$ splňujících $\langle \mathcal{A}, a \rangle \models \varphi(x/c_a)$, neboli $\mathcal{A} \models \varphi[e(x/a)]$. Protože je A konečná, existuje konečně mnoho $\varphi_1(x), \dots, \varphi_m(x)$ tak, že pro každou $\varphi \in \Omega$ existuje i takové, že $\mathcal{A} \models \varphi \leftrightarrow \varphi_i$. Potom i $\mathcal{B} \models \varphi \leftrightarrow \varphi_i$.

Protože v \mathcal{A} platí sentence $(\exists x) \bigwedge_{i=1}^m \varphi_i$ (je splněna díky $a \in A$) a $\mathcal{B} \equiv \mathcal{A}$, máme i $\mathcal{B} \models (\exists x) \bigwedge_{i=1}^m \varphi_i$. Neboli existuje $b \in B$ takové, že $\mathcal{B} \models \bigwedge_{i=1}^m \varphi_i[e(x/b)]$. Tedy pro každou $\varphi \in \Omega$ platí $\mathcal{B} \models \varphi[e(x/b)]$, tj. $\langle \mathcal{B}, b \rangle \models \varphi(x/c_a)$, z toho $\langle \mathcal{A}, a \rangle \equiv \langle \mathcal{B}, b \rangle$. \square

Definovatelnost a automorfismy

definovatelné množiny jsou **invariantní** na automorfismy (např. automorfismus grafu musí zobrazit trojúhelník na trojúhelník):

Tvrzení: Je-li $D \subseteq A^n$ definovatelná v \mathcal{A} , potom pro každý automorfismus $h \in \text{Aut}(\mathcal{A})$ platí $h[D] = D$ (kde $h[D]$ značí $\{(h(\bar{a}) \mid \bar{a} \in D)\}$).
Je-li definovatelná s parametry \bar{b} , platí to pro automorfismy identické na \bar{b} (tj. $h(\bar{b}) = \bar{b}$ neboli $h(b_i) = b_i$ pro všechna i).

Důkaz: Ukážeme jen verzi s parametry. Nechť $D = \varphi^{A, \bar{b}}(\bar{x}, \bar{y})$.
Potom pro každé $\bar{a} \in A^n$ platí následující ekvivalence:

$$\begin{aligned}\bar{a} \in D &\Leftrightarrow \mathcal{A} \models \varphi[\bar{e}(\bar{x}/\bar{a}, \bar{y}/\bar{b})] \\ &\Leftrightarrow \mathcal{A} \models \varphi[(e \circ h)(\bar{x}/\bar{a}, \bar{y}/\bar{b})] \\ &\Leftrightarrow \mathcal{A} \models \varphi[\bar{e}(\bar{x}/h(\bar{a}), \bar{y}/h(\bar{b}))] \\ &\Leftrightarrow \mathcal{A} \models \varphi[\bar{e}(\bar{x}/h(\bar{a}), \bar{y}/\bar{b})] \\ &\Leftrightarrow h(\bar{a}) \in D.\end{aligned}$$

Příklad

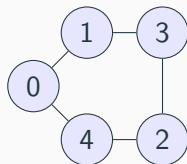
Množiny definovatelné s parametrem 0, $\text{Df}^1(\mathcal{G}, \{0\})$?

Jediný netriviální automorfismus zachovávající 0:

$h(i) = (5 - i) \bmod 5$, orbity $\{0\}$, $\{1, 4\}$, a $\{2, 3\}$.

Tyto množiny jsou definovatelné:

- $\{0\}$ formulí $x = y$, tj. $(x = y)^{\mathcal{G}, \{0\}} = \{0\}$
- $\{1, 4\}$ lze definovat pomocí $E(x, y)$
- $\{2, 3\}$ formulí $\neg E(x, y) \wedge \neg x = y$



$\text{Df}^1(\mathcal{G}, \{0\})$ je podalgebra $\underline{\mathcal{P}(V(\mathcal{G}))}$, tedy uzavřená na doplněk, sjednocení, průnik, obsahuje \emptyset a $V(\mathcal{G})$. Podalgebra generovaná $\{\{0\}, \{1, 4\}, \{2, 3\}\}$ už ale obsahuje všechny podmnožiny zachovávající automorfismus h . Dostáváme:

$$\begin{aligned}\text{Df}^1(\mathcal{G}, \{0\}) = \{ & \emptyset, \{0\}, \{1, 4\}, \{2, 3\}, \{0, 1, 4\}, \{0, 2, 3\}, \\ & \{1, 4, 2, 3\}, \{0, 1, 2, 3, 4\} \}\end{aligned}$$

9.3 ω -kategorické teorie

Izomorfní spektrum T je počet modelů T kardinality κ až na \simeq .
 T je κ -kategorická pokud $I(\kappa, T) = 1$, ω -kategorická má-li jediný spočetně nekonečný model až na izomorfismus.

Tvrzení: Teorie DeLO je ω -kategorická.

Důkaz: Budte \mathcal{A}, \mathcal{B} spočetně nekonečné modely, $A = \{a_i \mid i \in \mathbb{N}\}$, $B = \{b_i \mid i \in \mathbb{N}\}$. Z hustoty najdeme indukci $h_0 \subseteq h_1 \subseteq h_2 \subseteq \dots$ prosté parciální fce z A do B zach. usp., $\{a_0, \dots, a_{n-1}\} \subseteq \text{dom } h_n$, $\{b_0, \dots, b_{n-1}\} \subseteq \text{rng } h_n$. Potom $\mathcal{A} \simeq \mathcal{B}$ via $h = \bigcup_{n \in \mathbb{N}} h_n$. \square

Důsledek: Izomorfní spektrum teorie DeLO*:

- $I(\kappa, \text{DeLO}^*) = 0$ pro $\kappa \in \mathbb{N}$
- $I(\omega, \text{DeLO}^*) = 4$

Spočetné modely až na izomorfismus jsou například:

$$\mathbb{Q} = \langle \mathbb{Q}, \leq \rangle \simeq \mathbb{Q} \upharpoonright (0, 1), \mathbb{Q} \upharpoonright (0, 1], \mathbb{Q} \upharpoonright [0, 1), \mathbb{Q} \upharpoonright [0, 1]$$

Důkaz: Husté uspořádání nemůže být konečné. Izomorfismus zobrazí minimum na minimum a maximum na maximum. \square

Věta: Buď T ω -kategorická ve spočetném jazyce L . Je-li

(i) L bez rovnosti, nebo

(ii) L s rovností a T nemá konečné modely,

potom je T complete.

Důkaz: (i) Důsledek L.-S. věty bez rovnosti říká, že každý model je elementárně ekvivalentní nějakému spočetně nekonečnému, ten je ale až na izomorfismus jediný.

(ii) Důsledek L.-S. věty s rovností podobně říká, že všechny nekonečné modely jsou elementárně ekvivalentní. Mohla by mít elementárně neekvivalentní konečné modely, to jsme ale zakázali. \square

Důsledek: DeLO , DeLO^+ , DeLO^- , a DeLO^\pm jsou complete, jsou to všechny (navzájem neekvivalentní) complete jedn. extenze DeLO^* .

Analogické kritérium platí i pro kardinality κ větší než ω .