Výroková a predikátová logika - XI

Petr Gregor

KTIML MFF UK

ZS 2015/2016

Lineární rezoluce

Stejně jako ve VL, rezoluční metodu lze značně omezit (bez ztráty úplnosti).

- *Lineární důkaz* klauzule C z formule S je konečná posloupnost dvojic $(C_0, B_0), \ldots, (C_n, B_n)$ t.ž. C_0 je varianta klauzule v S a pro každé $i \leq n$
  - $i)$ B_i je varianta klauzule v S nebo $B_i = C_j$ pro nějaké $j < i$, a
  - $ii)$ C_{i+1} je rezolventa C_i a B_i, kde $C_{n+1} = C$.
- C je *lineárně dokazatelná* z S, psáno $S \vdash_L C$, má-li lineární důkaz z S.
- *Lineární zamítnutí* S je lineární důkaz $\square$ z S.
- S je *lineárně zamítnutelná*, pokud $S \vdash_L \square$.

Věta *S je lineárně zamítnutelná, právě když S je nesplnitelná.*

Důkaz $(\Rightarrow)$ Každý lineární důkaz lze transformovat na rezoluční důkaz.
$(\Leftarrow)$ Plyne z úplnosti lineární rezoluce ve VL (nedokazováno), neboť lifting lemma zachovává linearitu odvození. $\square$

LI-rezoluce

Stejně jako ve VL, pro Hornovy formule můžeme lineární rezoluci dál omezit.

- *LI-rezoluce ("linear input")* z formule S je lineární rezoluce z S, ve které je každá boční klauzule B_i variantou klauzule ze (vstupní) formule S.
- Je-li klauzule C dokazatelná LI-rezolucí z S, píšeme $S \vdash_{LI} C$.
- *Hornova formule* je množina (i nekonečná) Hornových klauzulí.
- *Hornova klauzule* je klauzule obsahující nejvýše jeden pozitivní literál.
- *Fakt* je (Hornova) klauzule $\{p\}$, kde p je pozitivní literál.
- *Pravidlo* je (Hornova) klauzule s právě jedním pozitivním a aspoň jedním negativním literálem. Pravidla a fakta jsou *programové klauzule*.
- *Cíl* je neprázdná (Hornova) klauzule bez pozitivního literálu.

Věta *Je-li Hornova T splnitelná a $T \cup \{G\}$ nesplnitelná pro cíl G, lze $\square$ odvodit LI-rezolucí z $T \cup \{G\}$ začínající G.*

Důkaz Plyne z Herbrandovy věty, stejné věty ve VL a lifting lemmatu. $\square$

Program v Prologu

Program (v Prologu) je Hornova formule obsahující pouze programové klauzule, tj. fakta nebo pravidla.

$syn(X,Y) :- otec(Y,X), muz(X).$	$\{syn(X,Y), \neg otec(Y,X), \neg muz(X)\}$
$syn(X,Y) :- matka(Y,X), muz(X).$	$\{syn(X,Y), \neg matka(Y,X), \neg muz(X)\}$
$muz(jan).$	$\{muz(jan)\}$
$otec(jiri,jan).$	$\{otec(jiri,jan)\}$
$matka(julie,jan).$	$\{matka(julie,jan)\}$
$?- syn(jan,X)$ $\quad P \models (\exists X) syn(jan,X)\ ?$	$\{\neg syn(jan,X)\}$

Zajímá nás, zda daný existenční dotaz vyplývá z daného programu.

Důsledek *Pro program P a cíl $G = \{\neg A_1, \ldots, \neg A_n\}$ v proměnných $X_1, \ldots, X_m$*

(1) $P \models (\exists X_1) \ldots (\exists X_m)(A_1 \wedge \ldots \wedge A_n)$, *právě když*

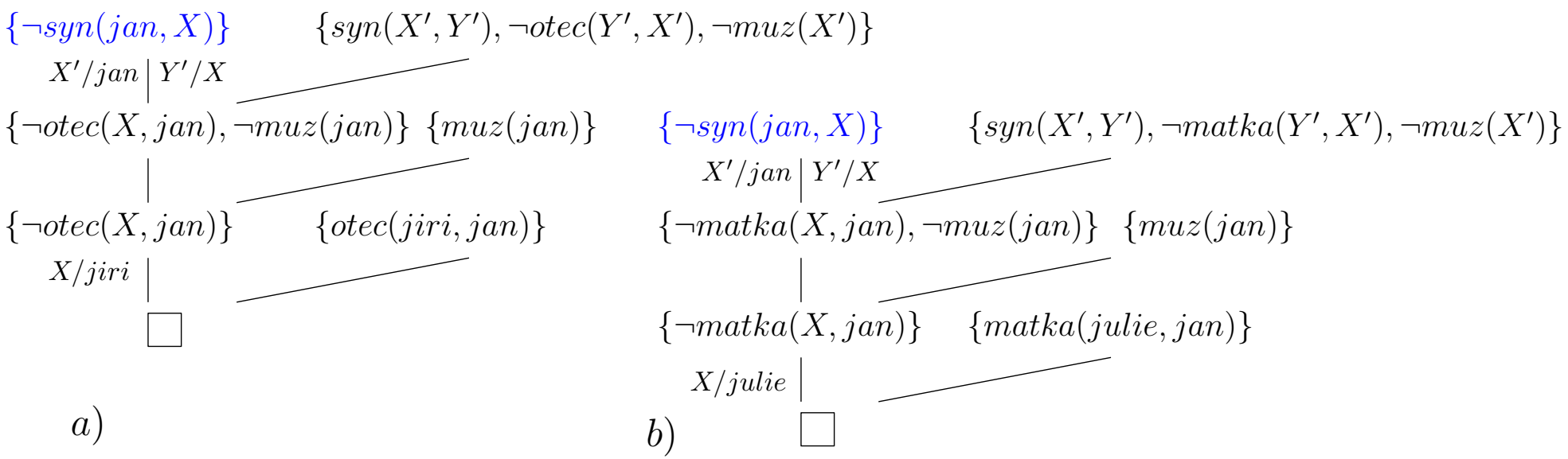
(2) $\square$ *lze odvodit LI-rezolucí z $P \cup \{G\}$ začínající (variantou) cíle G.*

LI-rezoluce nad programem

Je-li odpoveď na dotaz kladná, chceme navíc znát výstupní substituci.

Výstupní substituce σ LI-rezoluce $\square$ z $P \cup \{G\}$ začínající $G = \{\neg A_1, \ldots, \neg A_n\}$ je složení mgu v jednotlivých krocích (jen na proměnné v G). Platí,

$$P \models (A_1 \wedge \ldots \wedge A_n)\sigma.$$



Výstupní substituce $a)\ X = jiri,\ \ b)\ X = julie$.

Axiomatický přístup

- základní logické spojky a kvantifikátory: $\neg$, $\rightarrow$, $(\forall x)$ (ostatní odvozené)
- dokazují se libovolné formule (nejen sentence)
- *logické axiomy* (schémata logických axiomů)

$$
\begin{array}{lll}
(i) & \varphi \rightarrow (\psi \rightarrow \varphi) & \\
(ii) & (\varphi \rightarrow (\psi \rightarrow \chi)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \chi)) & \\
(iii) & (\neg\varphi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \varphi) & \\
(iv) & (\forall x)\varphi \rightarrow \varphi(x/t) & \text{je-li } t \text{ substituovatelný za } x \text{ do } \varphi \\
(v) & (\forall x)(\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow (\forall x)\psi) & \text{není-li } x \text{ volná proměnná ve } \varphi
\end{array}
$$

kde φ, ψ, χ jsou libovolné formule (daného jazyka), t je libovolný term a x je libovolná proměnná.

- je-li jazyk s rovností, mezi logické axiomy patří navíc axiomy rovnosti
- *odvozovací (deduktivní) pravidla*

$$\frac{\varphi,\ \varphi \rightarrow \psi}{\psi}$$ (modus ponens), $$\frac{\varphi}{(\forall x)\varphi}$$ (generalizace)

Pojem důkazu

Důkaz (*Hilbertova stylu*) formule φ z teorie T je konečná posloupnost $\varphi_0, \ldots, \varphi_n = \varphi$ formulí taková, že pro každé $i \leq n$

- φ_i je logický axiom nebo $\varphi_i \in T$ (axiom teorie), nebo
- φ_i lze odvodit z předchozích formulí pomocí odvozovacích pravidel.

Formule φ je *dokazatelná* v T, má-li důkaz z T, značíme $T \vdash_H \varphi$.

Věta *Pro každou teorii T a formuli φ, $T \vdash_H \varphi \Rightarrow T \models \varphi$.*

Důkaz

- Je-li $\varphi \in T$ nebo logický axiom, je $T \models \varphi$ (logické axiomy jsou tautologie),
- jestliže $T \models \varphi$ a $T \models \varphi \to \psi$, pak $T \models \psi$, *tj. modus ponens je korektní*,
- jestliže $T \models \varphi$, pak $T \models (\forall x)\varphi$, *tj. pravidlo generalizace je korektní*,
- tedy každá formule vyskytující se v důkazu z T platí v T. □

Poznámka *Platí i úplnost, tj. $T \models \varphi \Rightarrow T \vdash_H \varphi$ pro každou teorii T a formuli φ.*

Teorie struktury

Mnohdy nás zajímá, co platí v jedné konkrétní struktuře.

Teorie struktury $\mathcal{A}$ je množina $\mathrm{Th}(\mathcal{A})$ sentencí (stejného jazyka) platných v $\mathcal{A}$.

Pozorování *Pro každou strukturu $\mathcal{A}$ a teorii T jazyka L,*

- (i) $\mathrm{Th}(\mathcal{A})$ *je kompletní teorie,*
- (ii) *je-li $\mathcal{A} \models T$, je $\mathrm{Th}(\mathcal{A})$ jednoduchá (kompletní) extenze teorie T,*
- (iii) *je-li $\mathcal{A} \models T$ a T je kompletní, je $\mathrm{Th}(\mathcal{A})$ ekvivalentní s T, tj. $\theta^L(T) = \mathrm{Th}(\mathcal{A})$.*

Např. pro $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$ je $\mathrm{Th}(\underline{\mathbb{N}})$ je aritmetika přirozených čísel.

Poznámka *Později uvidíme, že ačkoliv je $\mathrm{Th}(\underline{\mathbb{N}})$ kompletní teorie, je (algoritmicky) nerozhodnutelná.*

Elementární ekvivalence

- Struktury $\mathcal{A}$ a $\mathcal{B}$ jazyka L jsou *elementárně ekvivalentní*, psáno $\mathcal{A} \equiv \mathcal{B}$, pokud v nich platí stejné formule (jazyka L), tj. $\mathrm{Th}(\mathcal{A}) = \mathrm{Th}(\mathcal{B})$.

  Např. $\langle \mathbb{R}, \leq \rangle \equiv \langle \mathbb{Q}, \leq \rangle$, *ale* $\langle \mathbb{Q}, \leq \rangle \not\equiv \langle \mathbb{Z}, \leq \rangle$, *neboť v* $\langle \mathbb{Z}, \leq \rangle$ *má každý prvek bezprostředního následníka, zatímco v* $\langle \mathbb{Q}, \leq \rangle$ *ne.*

- T je kompletní, právě když má až na el. ekvivalenci právě jeden model.

  Např. teorie $DeLO$ *hustých lineárních uspořádání bez konců je kompletní.*

Zajímá nás, jak vypadají modely dané teorie (až na elementární ekvivalenci).

Pozorování *Pro modely* $\mathcal{A}, \mathcal{B}$ *teorie* T *platí* $\mathcal{A} \equiv \mathcal{B}$, *právě když* $\mathrm{Th}(\mathcal{A})$, $\mathrm{Th}(\mathcal{B})$ *jsou ekvivalentní (jednoduché kompletní extenze teorie* T*).*

Poznámka *Lze-li efektivně (rekurzivně) popsat pro efektivně danou teorii* T*, jak vypadají všechny její kompletní extenze, je* T *(algoritmicky) rozhodnutelná.*

Jednoduché kompletní extenze - příklad

Teorie $DeLO^*$ hustého lineárního uspořádání jazyka $L = \langle \leq \rangle$ s rovností je

$$x \leq x \qquad \text{(reflexivita)}$$
$$x \leq y \ \wedge \ y \leq x \ \rightarrow \ x = y \qquad \text{(antisymetrie)}$$
$$x \leq y \ \wedge \ y \leq z \ \rightarrow \ x \leq z \qquad \text{(tranzitivita)}$$
$$x \leq y \ \vee \ y \leq x \qquad \text{(dichotomie)}$$
$$x < y \ \rightarrow \ (\exists z)\,(x < z \ \wedge \ z < y) \qquad \text{(hustota)}$$
$$(\exists x)(\exists y)(x \neq y) \qquad \text{(netrivialita)}$$

kde '$x < y$' je zkratka za '$x \leq y \ \wedge \ x \neq y$'.

Označme φ, ψ sentence $(\exists x)(\forall y)(x \leq y)$, resp. $(\exists x)(\forall y)(y \leq x)$. Uvidíme, že

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

jsou všechny (neekvivalentní) jednoduché kompletní extenze teorie $DeLO^*$.

Důsledek věty o spočetném modelu

Pomocí kanonického modelu (s rovností) jsme dříve dokázali následující větu.

Věta *Nechť T je bezesporná teorie spočetného jazyka L. Je-li L bez rovnosti, má T model, který je spočetně nekonečný. Je-li L s rovností, má T model, který je spočetný.*

Důsledek *Ke každé struktuře $\mathcal{A}$ spočetného jazyka bez rovnosti existuje spočetně nekonečná elementárně ekvivalentní struktura $\mathcal{B}$.*

Důkaz Teorie $\mathrm{Th}(\mathcal{A})$ je bezesporná, neboť má model $\mathcal{A}$. Dle předchozí věty má spočetně nek. model $\mathcal{B}$. Jelikož je teorie $\mathrm{Th}(\mathcal{A})$ kompletní, je $\mathcal{A} \equiv \mathcal{B}$. □

Důsledek *Ke každé nekonečné struktuře $\mathcal{A}$ spočetného jazyka s rovností existuje spočetně nekonečná elementárně ekvivalentní struktura $\mathcal{B}$.*

Důkaz Obdobně jako výše. Jelikož v $\mathcal{A}$ neplatí sentence *"existuje právě n prvků"* pro žádné $n \in \mathbb{N}$ a $\mathcal{A} \equiv \mathcal{B}$, není B konečná, tedy je nekonečná. □

Spočetné algebraicky uzavřené těleso

Řekneme, že těleso $\mathcal{A}$ je *algebraicky uzavřené*, pokud v něm každý polynom (nenulového stupně) má kořen, tj. pro každé $n \geq 1$ platí

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

kde y^k je zkratka za term $y \cdot y \cdot \dots \cdot y$ ($\cdot$ aplikováno $(k-1)$-krát).

Např. těleso $\underline{\mathbb{C}} = \langle \mathbb{C}, +, -, \cdot, 0, 1 \rangle$ je algebraicky uzavřené, zatímco tělesa $\mathbb{R}$ a $\underline{\mathbb{Q}}$ nejsou (neboť polynom $x^2 + 1$ v nich nemá kořen).

Důsledek *Existuje spočetné algebraicky uzavřené těleso.*

Důkaz Dle předchozího důsledku existuje spočetná struktura (nekonečná), která je elementárně ekvivalentní s tělesem $\underline{\mathbb{C}}$, tedy je to rovněž algebraicky uzavřené těleso. □

Izomorfismus struktur

Nechť $\mathcal{A}$, $\mathcal{B}$ jsou struktury jazyka $L = \langle \mathcal{F}, \mathcal{R} \rangle$.

- Bijekce $h\colon A \to B$ je *izomorfismus* struktur $\mathcal{A}$ a $\mathcal{B}$, pokud platí zároveň

  (i) $h(f^{\mathcal{A}}(a_1, \ldots, a_n)) = f^{\mathcal{B}}(h(a_1), \ldots, h(a_n))$
  pro každý n-ární funkční symbol $f \in \mathcal{F}$ a každé $a_1, \ldots, a_n \in A$,

  (ii) $R^{\mathcal{A}}(a_1, \ldots, a_n) \;\Leftrightarrow\; R^{\mathcal{B}}(h(a_1), \ldots, h(a_n))$
  pro každý n-ární relační symbol $R \in \mathcal{R}$ a každé $a_1, \ldots, a_n \in A$.

- $\mathcal{A}$ a $\mathcal{B}$ jsou *izomorfní* (via h), psáno $\mathcal{A} \simeq \mathcal{B}$ ($\mathcal{A} \simeq_h \mathcal{B}$), pokud existuje izomorfismus h struktur $\mathcal{A}$ a $\mathcal{B}$. Říkáme rovněž, že $\mathcal{A}$ je *izomorfní s* $\mathcal{B}$.
- *Automorfismus* struktury $\mathcal{A}$ je izomorfismus $\mathcal{A}$ s $\mathcal{A}$.

Např. potenční algebra $\underline{\mathcal{P}(X)} = \langle \mathcal{P}(X), -, \cap, \cup, \emptyset, X \rangle$ *s* $X = n$ *je izomorfní s Booleovou algebrou* $\underline{{}^n 2} = \langle {}^n 2, -_n, \wedge_n, \vee_n, 0_n, 1_n \rangle$ *via* $h : A \mapsto \chi_A$, *kde* χ_A *je charakteristická funkce množiny* $A \subseteq X$.

Izomorfismus a sémantika

Uvidíme, že izomorfismus zachovává sémantiku.

Tvrzení *Nechť $\mathcal{A}, \mathcal{B}$ jsou struktury jazyka $L = \langle \mathcal{F}, \mathcal{R} \rangle$. Bijekce $h\colon A \to B$ je izomorfismus $\mathcal{A}$ a $\mathcal{B}$, právě když platí zároveň*

(i) $h(t^{\mathcal{A}}[e]) = t^{\mathcal{B}}[he]$ *pro každý term t a $e\colon \mathrm{Var} \to A$,*

(ii) $\mathcal{A} \models \varphi[e] \;\Leftrightarrow\; \mathcal{B} \models \varphi[he]$ *pro každou formuli φ a $e\colon \mathrm{Var} \to A$.*

Důkaz ($\Rightarrow$) Indukcí dle struktury termu t, respektive formule φ.
($\Leftarrow$) Dosazením termu $f(x_1, \ldots, x_n)$ do (i) či atomické formule $R(x_1, \ldots, x_n)$ do (ii) pro ohodnocení $e(x_i) = a_i$ máme, že h vyhovuje def. izomorfismu. □

Důsledek *Pro každé struktury $\mathcal{A}, \mathcal{B}$ stejného jazyka,*

$$\mathcal{A} \simeq \mathcal{B} \;\Rightarrow\; \mathcal{A} \equiv \mathcal{B}.$$

Poznámka *Obrácená implikace obecně neplatí, např. $\langle \mathbb{Q}, \leq \rangle \equiv \langle \mathbb{R}, \leq \rangle$, ale $\langle \mathbb{Q}, \leq \rangle \not\simeq \langle \mathbb{R}, \leq \rangle$, neboť $|\mathbb{Q}| = \omega$ a $|\mathbb{R}| = 2^{\omega}$.*

Konečné modely s rovností

Tvrzení *Pro každé konečné struktury $\mathcal{A}, \mathcal{B}$ stejného jazyka s rovností,*

$$\mathcal{A} \equiv \mathcal{B} \quad \Rightarrow \quad \mathcal{A} \simeq \mathcal{B}.$$

Důkaz Je $|A| = |B|$, neboť lze vyjádřit *"existuje právě n prvků"*.

- Nechť $\mathcal{A}'$ je expanze $\mathcal{A}$ do jazyka $L' = L \cup \{c_a\}_{a \in A}$ o jména prvků z A.
- Ukážeme, že $\mathcal{B}$ lze expandovat na $\mathcal{B}'$ do jazyka L' tak, že $\mathcal{A}' \equiv \mathcal{B}'$. Pak zřejmě $h\colon a \mapsto c_a^{B'}$ je izomorfismus $\mathcal{A}'$ s $\mathcal{B}'$ a tedy i izomorfismus $\mathcal{A}$ s $\mathcal{B}$.
- Stačí ukázat, že pro každé $c_a^{A'} = a \in A$ existuje $b \in B$ t.ž. $\langle \mathcal{A}, a \rangle \equiv \langle \mathcal{B}, b \rangle$.
- Označme Ω množinu formulí $\varphi(x)$ t.ž. $\langle \mathcal{A}, a \rangle \models \varphi(x/c_a)$, tj. $\mathcal{A} \models \varphi[e(x/a)]$.
- Jelikož je A konečné, existuje konečně formulí $\varphi_0(x), \ldots, \varphi_m(x)$ tak, že pro každé $\varphi \in \Omega$ je $\mathcal{A} \models \varphi \leftrightarrow \varphi_i$ pro nějaké i.
- Jelikož $\mathcal{B} \equiv \mathcal{A} \models (\exists x) \bigwedge_{i \le m} \varphi_i$, existuje $b \in B$ t.ž. $\mathcal{B} \models \bigwedge_{i \le m} \varphi_i[e(x/b)]$.
- Tedy pro každou $\varphi \in \Omega$ je $\mathcal{B} \models \varphi[e(x/b)]$, tj. $\langle \mathcal{B}, b \rangle \models \varphi(x/c_a)$. □

Důsledek *Má-li kompletní teorie jazyka s rovností konečný model, jsou všechny její modely izomorfní.*

Kategoričnost

- *Izomorfní spektrum* teorie T je počet $I(\kappa, T)$ navzájem neizomorfních modelů teorie T pro každou kardinalitu κ.
- Teorie T je *κ-kategorická*, pokud má až na izomorfismus právě jeden model kardinality κ, tj. $I(\kappa, T) = 1$.

Tvrzení *Teorie $DeLO$ (tj. "bez konců") je ω-kategorická.*

Důkaz Nechť $\mathcal{A}, \mathcal{B} \models DeLO$ s $A = \{a_i\}_{i\in\mathbb{N}}$, $B = \{b_i\}_{i\in\mathbb{N}}$. Indukcí dle n lze nalézt prosté parciální funkce $h_n \subseteq h_{n+1} \subset A \times B$ zachovávající uspořádání tak, že $\{a_i\}_{i<n} \subseteq \mathrm{dom}(h_n)$ a $\{b_i\}_{i<n} \subseteq \mathrm{rng}(h_n)$. Pak $\mathcal{A} \simeq \mathcal{B}$ via $h = \cup h_n$. □

Obdobně dostaneme, že např. $\mathcal{A} = \langle \mathbb{Q}, \leq \rangle$, $\mathcal{A} \restriction (0, 1]$, $\mathcal{A} \restriction [0, 1)$, $\mathcal{A} \restriction [0, 1]$ jsou až na izomorfismus všechny spočetné modely teorie $DeLO^*$. Pak

$$I(\kappa, DeLO^*) = \begin{cases} 0 & \text{pro } \kappa \in \mathbb{N}, \\ 4 & \text{pro } \kappa = \omega. \end{cases}$$

ω-kategorické kritérium kompletnosti

Věta *Nechť jazyk L je spočetný.*

(i) *Je-li teorie T jazyka L bez rovnosti ω-kategorická, je kompletní.*

(ii) *Je-li teorie T jazyka L s rovností ω-kategorická a bez konečného modelu, je kompletní.*

Důkaz Každý model teorie T je elementárně ekvivalentní s nějakým spočetně nekonečným modelem T, ale ten je až na izomorfismus jediný. Tedy všechny modely T jsou elementárně ekvivalentní, tj. T je kompletní. □

Např. teorie $DeLO$, $DeLO^+$, $DeLO^-$, $DeLO^\pm$ jsou kompletní a jsou to všechny (navzájem neekvivalentní) jednoduché kompletní extenze teorie $DeLO^*$.

Poznámka *Obdobné kritérium platí i pro vyšší kardinality než ω.*