Vypracované otázky k skúške z NAIL062

Výroková a predikátová logika

Pojmy

1. Model vo výrokovej logike, pravidvostné funkcie výroku

Model jazyka $\mathbb{P}$ je libovolné pravdivostní ohodnocení $v : \mathbb{P} \to \{0,1\}$. Množinu (všech) modelů jazyka $\mathbb{P}$ označíme $\mathbf{M}_{\mathbb{P}}$:

$$\mathrm{M}_{\mathbb{P}} = \{v \mid v : \mathbb{P} \to \{0,1\}\} = \{0,1\}^{\mathbb{P}}$$

Pravdivostní funkce výroku φ v konečném jazyce $\mathbb{P}$ je funkce $f_{\varphi,\mathbb{P}} : \{0,1\}^{|\mathbb{P}|} \to \{0,1\}$ definovaná induktivně:

- je-li φ i-tý prvovýrok z $\mathbb{P}$, potom $f_{\varphi,\mathbb{P}}(x_0,\ldots,x_{n-1}) = x_i$,
- je-li $\varphi = (\neg\varphi')$, potom

$$f_{\varphi,\mathbb{P}}(x_0,\ldots,x_{n-1}) = f_{\neg}\left(f_{\varphi',\mathbb{P}}(x_0,\ldots,x_{n-1})\right)$$

- je-li $(\varphi'\Box\varphi'')$ kde $\Box \in \{\wedge,\vee,\to,\leftrightarrow\}$, potom

$$f_{\varphi,\mathbb{P}}(x_0,\ldots,x_{n-1}) = f_{\Box}\left(f_{\varphi',\mathbb{P}}(x_0,\ldots,x_{n-1}), f_{\varphi'',\mathbb{P}}(x_0,\ldots,x_{n-1})\right).$$

2. Sémantické pojmy (pravdivosť, lživosť, nezávislosť, splniteľnosť) v logike vzhľadom k teórii

Říkáme, že výrok φ(v jazyce $\mathbb{P}$) je

- pravdivý, tautologie, platí (v logice/logicky), a píšeme $\models \varphi$, pokud platí v každém modelu (jazyka $\mathbb{P}$), $\mathrm{M}_{\mathbb{P}}(\varphi) = \mathrm{M}_{\mathbb{P}}$
- lživý, sporný, pokud nemá žádný model, $\mathrm{M}_{\mathbb{P}}(\varphi) = \emptyset$
- nezávislý, pokud platí v nějakém modelu, a neplatí v nějakém jiném modelu, tj. není pravdivý ani lživý, $\emptyset \subsetneq \mathrm{M}_{\mathbb{P}}(\varphi) \subsetneq \mathrm{M}_{\mathbb{P}}$
- splnitelný, pokud má nějaký model, tj. není lživý, $\mathrm{M}_{\mathbb{P}}(\varphi) \neq \emptyset$.

Dále říkáme, že výroky φ, ψ (ve stejném jazyce $\mathbb{P}$) jsou (logicky) ekvivalentní, píšeme $\varphi \sim \psi$ pokud mají stejné modely.

Mějme teorii T v jazyce $\mathbb{P}$. Říkáme, že výrok φ v jazyce $\mathbb{P}$ je

- pravdivý vT, důsledek T, platí vT, a píšeme $T \models \varphi$, pokud φ platí v každém modelu teorie T, neboli $\mathrm{M}_{\mathbb{P}}(T) \subseteq \mathrm{M}_{\mathbb{P}}(\varphi)$,
- lživý vT, sporný vT, pokud neplatí v žádném modelu T, neboli $\mathrm{M}_{\mathbb{P}}(\varphi) \cap \mathrm{M}_{\mathbb{P}}(T) = \mathrm{M}_{\mathbb{P}}(T,\varphi) = \emptyset$
- nezávislý vT, pokud platí v nějakém modelu T, a neplatí v nějakém jiném modelu T, tj. není pravdivý v T ani lživý v $T, \emptyset \subsetneq \mathrm{M}_{\mathbb{P}}(T,\varphi) \subsetneq \mathrm{M}_{\mathbb{P}}(T)$,
- splnitelný vT, konzistentní s T, pokud platí v nějakém modelu T, tj. není lživý v T, $\mathrm{M}_{\mathbb{P}}(T,\varphi) \neq \emptyset$.

3. Ekvivalencia výrokov, resp. výrokových teórií, T-ekvivalencia

Výroky φ, ψ (ve stejném jazyce $\mathbb{P}$) jsou (logicky) ekvivalentní, píšeme $\varphi \sim \psi$ pokud mají stejné modely, tj.

A říkáme, že výroky φ, ψ (ve stejném jazyce $\mathbb{P}$) jsou ekvivalentní v T, T-ekvivalentní, píšeme $\varphi \sim_T \psi$ pokud platí v týchž modelech T, tj. $\varphi \sim_T \psi$ právě když $\mathrm{M}_{\mathbb{P}}(T, \varphi) = \mathrm{M}_{\mathbb{P}}(T, \psi)$.

4. Sémantické pojmy o teorii (sporná, bezsporná, kompletná, splniteľná)

Je-li T teorie v jazyce L a φ L-formule, potom říkáme, že φ je:

- pravdivá (platí) v T, značíme $T \models \varphi$, pokud $\mathcal{A} \models \varphi$ pro všechna $\mathcal{A} \in \mathrm{M}(T)$ (neboli: $\mathrm{M}(T) \subseteq \mathrm{M}(\varphi)$)
- lživá v T, pokud $T \models \neg\varphi$, t. pokud je lživá v každém modelu T (neboli: $\mathrm{M}(T) \cap \mathrm{M}(\varphi) = \emptyset$),
- nezávislá v T, pokud není pravdivá v T ani lživá v T.
- Máme-li prázdnou teorii $T = \emptyset$ (tj.$\mathrm{M}(T) = \mathrm{M}_L$), potom teorii T vynecháváme, píšeme $\models \varphi$, a říkáme, že φ je pravdivá (v logice), (logicky) platí, je tautologie; podobně pro ostatní pojmy.
- Teorie je sporná, jestliže v ní platí spor $\bot$, který v predikátové logice můžeme definovat jako $R(x_1, \ldots, x_n) \wedge \neg R(x_1, \ldots, x_n)$, kde R je libovolný (třeba první) relační symbol z jazyka nebo rovnost (nemá-li jazyk relační symbol, musí být s rovností). Teorie je sporná, právě když v ní platí každá formule, nebo, ekvivalentně, právě když nemá žádný model. Jinak říkáme, že je teorie bezesporná (neplatí-li v ní spor, ekvivalentně má-li alespoň jeden model).

Sentencím pravdivým v T říkáme důsledky T; množina všech důsledků T v jazyce L je:

$$\mathrm{Csq}_L(T) = \{\varphi \mid \varphi \text{ je sentence a } T \models \varphi\}$$

Teorie je kompletní, je-li bezesporná a každá sentence je v ní bud' pravdivá, nebo lživá.

5. Extenzia teórie (jednoduchá, konzervatívna), zodpovedajúce sémantické kritéria

Výroková

Mějme teorii T v jazyce $\mathbb{P}$.

- Extenze teorie T je libovolná teorie T' v jazyce $\mathbb{P}' \supseteq \mathbb{P}$ splňující $\mathrm{Csq}_{\mathbb{P}}(T) \subseteq \mathrm{Csq}_{\mathbb{P}'}(T')$,
- je to jednoduchá extenze, pokud $\mathbb{P}' = \mathbb{P}$,
- je to konzervativní extenze, pokud $\mathrm{Csq}_{\mathbb{P}}(T) = \mathrm{Csq}_{\mathbb{P}}(T') = \mathrm{Csq}_{\mathbb{P}'}(T') \cap \mathrm{VF}_{\mathbb{P}}$.

Je-li T teorie v jazyce $\mathbb{P}$ a T' teorie v jazyce $\mathbb{P}'$ obsahujícím jazyk P. Potom platí:

- T' je jednoduchou extenzí T, právě když $\mathbb{P}' = \mathbb{P}$ a $\mathrm{M}_{\mathbb{P}}(T') \subseteq \mathrm{M}_{\mathbb{P}}(T)$,
- T' je extenzí T, právě když $\mathrm{M}_{\mathbb{P}'}(T') \subseteq \mathrm{M}_{\mathbb{P}'}(T)$. Uvažujeme tedy modely teorie T nad rozšířeným jazykem $\mathbb{P}'$.21 Jinými slovy, restrikce [22] libovolného modelu $v \in \mathrm{M}_{\mathbb{P}'}(T')$ na původní jazyk $\mathbb{P}$ musí být modelem T, mohli bychom psát $v\rceil_{\mathbb{P}} \in \mathrm{M}_{\mathbb{P}}(T)$ nebo:

$$\{v\rceil_{\mathbb{P}} \mid v \in \mathrm{M}_{\mathbb{P}'}(T')\} \subseteq \mathrm{M}_{\mathbb{P}}(T)$$

- T' je konzervativní extenzí T, pokud je extenzí a navíc platí, že každý model T (v jazyce $\mathbb{P}$) lze nějak expandovat (rozšířit) [23] na model T' (v jazyce $\mathbb{P}'$), neboli každý model T (v jazyce $\mathbb{P}$) získáme restrikcí nějakého modelu T' na jazyk $\mathbb{P}$. Mohli bychom psát:

$$\{v\|_{\mathbb{P}} \mid v \in \mathrm{M}_{\mathbb{P}'}(T')\} = \mathrm{M}_{\mathbb{P}}(T)$$

- T' je extenzí T a zároveň T je extenzí T', právě když $\mathbb{P}' = \mathbb{P}$ a $\mathrm{M}_{\mathbb{P}}(T') = \mathrm{M}_{\mathbb{P}}(T)$, neboli $T' \sim T$.
- Kompletní jednoduché extenze T jednoznačně až na ekvivalenci odpovídají modelům T. Sentencím pravdivým v T říkáme důsledky T; množina všech důsledků T v jazyce L je:

$$\mathrm{Csq}_L(T) = \{\varphi \mid \varphi \text{ je sentence a } T \models \varphi\}$$

Predikátová

Mějme teorii T v jazyce L.

- Extenze teorie T je libovolná teorie T'v jazyce $L' \supseteq L$ splňující $\mathrm{Csq}_L(T) \subseteq \mathrm{Csq}_{L'}(T')$,
- je to jednoduchá extenze, pokud $L' = L$,
- je to konzervativní extenze, pokud $\mathrm{Csq}_L(T) = \mathrm{Csq}_L(T') = \mathrm{Csq}_{L'}(T') \cap \mathrm{Fm}_L$, kde[2] Fm_L značí množinu všech formulí v jazyce L.
- Teorie T' (v jazyce L) je ekvivalentní teorii T, pokud je T' extenzí T a T extenzí T'.

Mějme teorie T, T' v jazyce L. Potom:

- T' je extenze T, právě když $\mathrm{M}_L(T') \subseteq \mathrm{M}_L(T)$.
- T' je ekvivalentní s T, právě když $\mathrm{M}_L(T') = \mathrm{M}_L(T)$.

6. Tablo z teórie, tablo dôkaz

Výroková

Konečné tablo z teorie T je uspořádaný, položkami označkovaný strom zkonstruovaný aplikací konečně mnoha následujících pravidel:

- jednoprvkový strom označkovaný libovolnou položkou je tablo z teorie T,
- pro libovolnou položkou P na libovolné větvi V, můžeme na konec větve V připojit atomické tablo pro položku P,
- na konec libovolné větve můžeme připojit položku T α pro libovolný axiom teorie $\alpha \in T$.

Tablo z teorie T je bud' konečné, nebo i nekonečné: v tom případě vzniklo ve spočetně mnoha krocích. Můžeme ho formálně vyjádřit jako sjednocení $\tau = \bigcup_{i \geq 0} \tau_i$, kde τ_i jsou konečná tabla z T, τ_0 je jednoprvkové tablo, a τ_{i+1} vzniklo z τ_i v jednom kroku. Tablo pro položku P je tablo, které má položku P v kořeni.

Tablo důkaz výroku φ z teorie T je sporné tablo z teorie T s položkou Fφ v kořeni. Pokud existuje, je φ (tablo) dokazatelný z T, píšeme $T \vdash \varphi$. (Definujme také tablo zamítnutí jako sporné tablo s Tφ v kořeni. Pokud existuje, je φ (tablo) zamítnutelný z T, tj. platí $T \vdash \neg\varphi$.)

- Tablo je sporné, pokud je každá jeho větev sporná.
- Větev je sporná, pokud obsahuje položky T ψ a F ψ pro nějaký výrok ψ, jinak je bezesporná.
- Tablo je dokončené, pokud je každá jeho větev dokončená.
- Větev je dokončená, pokud
  - je sporná, nebo
  - je každá její položka na této větvi redukovaná a zároveň obsahuje položku T α pro každý axiom $\alpha \in T$
- Položka P je redukovaná na větvi V procházející touto položkou, pokud
  - je tvaru Tp resp. Fp pro nějakou výrokovou proměnnou $p \in \mathbb{P}$, nebo
  - při konstrukci tabla již došlo k jejímu rozvoji na V, tj. vyskytuje se na V jako kořen atomického tabla.

Predikátová

Konečné tablo z teorie T je uspořádaný, položkami označkovaný strom zkonstruovaný aplikací konečně mnoha následujících pravidel:

- jednoprvkový strom označkovaný libovolnou položkou je tablo z teorie T,
- pro libovolnou položkou P na libovolné větvi V, můžeme na konec větve V připojit atomické tablo pro položku P, přičemž je-li P typu 'svědek', můžeme použít jen pomocný konstantní symbol $c_i \in C$, který se na větvi V dosud nevyskytuje (pro položky typu 'všichni' můžeme použít libovolný konstantní L_C-term t_i),
- na konec libovolné větve můžeme připojit položku T α pro libovolný axiom teorie $\alpha \in T$.

Tablo z teorie T je bud' konečné, nebo i nekonečné: v tom případě vzniklo ve spočetně mnoha krocích. Můžeme ho formálně vyjádřit jako sjednocení $\tau = \bigcup_{i \geq 0} \tau_i$, kde τ_i jsou konečná tabla z T, τ_0 je jednoprvkové tablo, a τ_{i+1} vzniklo z τ_i v jednom kroku. Tablo pro položku P je tablo, které má položku P v kořeni.

Tablo důkaz sentence φ z teorie T je sporné tablo z teorie T s položkou $F\varphi$ v kořeni. Pokud existuje, je φ (tablo) dokazatelná z T, píseme $T \vdash \varphi$. (Definujme také tablo zamítnutí jako sporné tablo s T φ v kořeni. Pokud existuje, je φ (tablo) zamítnutelná z T, tj. platí $T \vdash \neg\varphi$.)

- Tablo je sporné, pokud je každá jeho větev sporná.
- Větev je sporná, pokud obsahuje položky T ψ a F ψ pro nějakou sentenci ψ, jinak je bezesporná.
- Tablo je dokončené, pokud je každá jeho větev dokončená.
- Větev je dokončená, pokud
  - je sporná, nebo
  - je každá položka na této větvi redukovaná a zároveň větev obsahuje položku T α pro každý axiom $\alpha \in T$.
- Položka P je redukovaná na větvi V procházející touto položkou, pokud
  - není typu 'všichni' a při konstrukci tabla již došlo k jejímu rozvoji na V, tj. vyskytuje se na V jako kořen atomického tabla. [4]
  - je typu 'všichni' a všechny její výskyty na V jsou na větvi V redukované.
- Výskyt položky P typu 'všichni' na větvi V je i-tý, pokud má na V právě $i-1$ předků označených touto položkou, a i-tý výskyt je redukovaný na V, pokud
  - položka P má $(i+1)$-ní výskyt na V, a zároveň
  - na V se vyskytuje položka $\mathrm{T}\varphi\,(x/t_i)$ (je-li $P = \mathrm{T}(\forall x)\varphi(x)$) resp. F $\varphi\,(x/t_i)$ (je-li $P = \mathrm{F}(\exists x)\varphi(x)$), kde t_i je i-tý konstantní L_C-term.

7. Kanonický model

Je-li V bezesporná větev dokončeného tabla, potom kanonický model pro V je model definovaný předpisem (pro $p \in \mathbb{P}$) :

$$v(p) = \begin{cases} 1 \text{ pokud se na } V \text{ vyskytuje položka } \mathrm{T}p, \\ 0 \text{ jinak.} \end{cases}$$

Mějme teorii T v jazyce $L = \langle \mathcal{F}, \mathcal{R} \rangle$ a nechť V je bezesporná větev nějakého dokončeného tabla z teorie T. Potom kanonický model pro V je L_C-struktura $\mathcal{A} = \left\langle A, \mathcal{F}^{\mathcal{A}} \cup C^{\mathcal{A}}, \mathcal{R}^{\mathcal{A}} \right\rangle$ definovaná následovně: Je-li jazyk L bez rovnosti, potom:

- Doména A je množina všech konstantních L_C-termů.
- Pro každý n-ární relační symbol $R \in \mathcal{R}$ a "s $s_1, \ldots$, "s $_n$ " z A : ("s_1", $\ldots$, " s_n") $\in R^{\mathcal{A}}$ právě když na větvi V je položka $\mathrm{T}R\,(s_1, \ldots, s_n)$
- Pro každý n-ární funkční symbol $f \in \mathcal{F}$ a "s $s_1, , \ldots$, "s n_n z A :

$$f^{\mathcal{A}}(\text{"}s_1\text{"},\ldots,\text{"}s_n\text{"}) = \text{"}f(s_1,\ldots,s_n)\text{"}$$

Speciálně, pro konstantní symbol c máme $c^{\mathcal{A}} =$ "c". Funkci $f^{\mathcal{A}}$ tedy interpretujeme jako 'vytvoření' nového termu ze symbolu f a vstupních termů Necht je L jazyk s rovností. Připomeňme, že naše tablo je nyní z teorie T^*, tj. z rozšíření T o axiomy rovnosti pro L. Nejprve vytvoříme kanonický model $\mathcal{B}$ pro V jakoby byl L bez rovnosti (jeho doména B je tedy množina všech konstantních L_C-termů). Dále definujeme relaci $=^B$ stejně jako pro ostatní relační symboly:

"s_1 "$=^B$ "s_2 " právě když na větvi V je položka T$s_1 = s_2$

Kanonický model pro V potom definujeme jako faktorstrukturu $\mathcal{A} = \mathcal{B}/=^B$. Jak plyne z diskuze v Sekci 7.3 , relace $=^B$ je opravdu kongruence struktury $\mathcal{B}$, definice je tedy korektní, a relace $=^{\mathcal{A}}$ je identita na A. Platí následující jednoduché pozorování:

Pozorování 7.4.4. Pro každou formuli φ máme $\mathcal{B} \models \varphi$ (kde symbol $=$ je interpretován jako binární relace $=^B$), právě když $\mathcal{A} = \mathcal{B}/=^B \models \varphi$(*kde* $=$ je interpretován jako identita).

8. Kongruencia štruktúry, faktorštruktúra, axiomy rovnosti.

Mějme ekvivalenci $\sim$ na množině A, funkci $f : A^n \to A$, a relaci $R \subseteq A^n$. Říkáme, že $\sim$ je:

- kongruencí pro funkci f, pokud pro všechna $x_i, y_i \in A$ taková, že $x_i \sim y_i (1 \leq i \leq n)$ platí $f(x_1,\ldots,x_n) \sim f(y_1,\ldots,y_n)$
- kongruencí pro relaci R, pokud pro všechna $x_i, y_i \in A$ taková, že $x_i \sim y_i (1 \leq i \leq n)$ platí $R(x_1,\ldots,x_n)$ právě když $R(y_1,\ldots,y_n)$.

Kongruence struktury $\mathcal{A}$ je ekvivalence $\sim$ na množině A, která je kongruencí pro všechny funkce a relace $\mathcal{A}$.

Mějme strukturu $\mathcal{A}$ a její kongruenci . Faktorstruktura (podílová struktura) $\mathcal{A}$ podle $\sim$ je struktura $\mathcal{A}/\sim$ v témž jazyce, jejíž univerzum $A/\sim$ je množina všech rozkladových tříd A podle $\sim$, a jejíž funkce a relace jsou definované pomocí reprezentantů, tj :

- $f^{\mathcal{A}/\sim}([x_1]_\sim,\ldots,[x_n]_\sim) = \left[f^{\mathcal{A}}(x_1,\ldots,x_n)\right]_\sim$, pro každý (n-ární) funkční symbol f, a
- $R^{\mathcal{A}/\sim}([x_1]_\sim,\ldots,[x_n]_\sim)$ právě když $R^{\mathcal{A}}(x_1,\ldots,x_n)$, pro každý (n-ární) relační symbol R.

Axiomy rovnosti pro jazyk L s rovností jsou následující: (i) $x = x$ (ii) $x_1 = y_1 \wedge \cdots \wedge x_n = y_n \to f(x_1,\ldots,x_n) = f(y_1,\ldots,y_n)$ pro každý n-ární funkční symbol f jazyka L (iii) $x_1 = y_1 \wedge \cdots \wedge x_n = y_n \to (R(x_1,\ldots,x_n) \to R(y_1,\ldots,y_n))$ pro každý n-ární relační symbol R jazyka L včetně rovnosti.

9. CNF a DNF, Hornov tvar, Množinová reprezentácia CNF, splňujúce ohodnotenie.

- Literál ℓ je bud' prvovýrok p nebo negace prvovýroku $\neg p$. Pro prvovýrok p označme $p^0 = \neg p$ a $p^1 = p$. Je-li ℓ literál, potom $\bar{\ell}$ označuje opačný literál k ℓ. Je-li $\ell = p$ (pozitivní literál), potom $\bar{\ell} = \neg p$, je-li $\ell = \neg p$ (negativní literál), potom $\bar{\ell} = p$
- Klauzule (clause) je disjunkce literálů $C = \ell_1 \vee \ell_2 \vee \cdots \vee \ell_n$. Jednotková klauzule (unit clause) je samotný literál ($n = 1$) a prázdnou klauzulí ($n = 0$) myslíme $\bot$.
- Výrok je v konjunktivní normální formě (v CNF) pokud je konjunkcí klauzulí. Prázdný výrok v CNF je $\top$.
- Elementární konjunkce je konjunkce literálů $E = \ell_1 \wedge \ell_2 \wedge \cdots \wedge \ell_n$. Jednotková elementární konjunkce je samotný literál ($n = 1$). Prázdná elementární konjunkce ($n = 0$) je $\top$.
- Výrok je v disjunktivní normální formě (v DNF) pokud je disjunkcí elementárních konjunkcí. Prázdný výrok v DNF je $\bot$. Nyní si ukážeme další fragment SATu řešitelný v polynomiálním čase, tzv. Horn-SAT neboli problém splnitelnosti hornovských výroků.
- Výrok je v hornovský (v Hornově tvaru), pokud je konjunkcí hornovských klauzulí, tj. klauzulí obsahujících nejvýše jeden *pozitivni* literál. Význam Hornovských klauzulí vyplývá z ekvivalentního vyjádření ve formě implikace:

$$\neg p_1 \vee \neg p_2 \vee \cdots \vee \neg p_n \vee q \sim (p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow q$$

Hornovské formule tedy dobře modelují systémy, kde splnění určitých podmínek zaručuje splnění jiné podmínky. Upozorněme, že jednotková klauzule ℓ je také hornovská. V kontextu logického programování se jí říká fakt, pokud je literál pozitivní, a cíl pokud je negativní. Hornovské formule s alespoň jedním pozitivním a alespoň jedním negativním literálem jsou pravidla.

V množinové reprezentaci odpovídají modely množinám literálů, které obsahují pro každou výrokovou proměnnou p právě jeden z literálo $p, \neg p$:

- (Částečné) ohodnocení $\mathcal{V}$ je libovolná množina literálů, která je konzistentní, tj. neobsahuje dvojici opačných literálů.
- Ohodnocení je úplné, pokud obsahuje pozitivní nebo negativní literál pro každou výrokovou proměnnou.
- Ohodnocení $\mathcal{V}$ splňuje formuli S, píšeme $\mathcal{V} \models S$, pokud $\mathcal{V}$ obsahuje nějaký literál z každé klauzule v S, tj.:

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

10. Rezolúčne pravidlo, unifikácia, najvšeobecnejšia unifikácia

Mějme konečnou množinu výrazů $S = \{E_1, \ldots, E_n\}$. Substituce σ je unifikace pro S, pokud $E_1\sigma = E_2\sigma = \cdots = E_n\sigma$, neboli $S\sigma$ obsahuje jediný výraz. Pokud existuje, potom říkáme také, že S je unifikovatelná.

Unifikace pro S je nejobecnější, pokud pro každou unifikaci τ pro S existuje substituce λ taková, že $\tau = \sigma\lambda$. Všimněte si, že nejobecnějších unifikací pro S může být více, ale liší se jen přejmenováním proměnných.

Mějme klauzule C_1 a C_2 s disjunktními množinami proměnných a necht' jsou tvaru

$$C_1 = C_1' \sqcup \{A_1, \ldots, A_n\}, \quad C_2 = C_2' \sqcup \{\neg B_1, \ldots, \neg B_m\}$$

kde $n, m \geq 1$ a množinu výrazů $S = \{A_1, \ldots, A_n, B_1, \ldots, B_m\}$ lze unifikovat. Buď σ nejobecnější unifikace S. Rezolventa klauzulí C_1 a C_2 je následující klauzule:

$$C = C_1'\sigma \cup C_2'\sigma$$

11. Rezolúčny dôkaz a zamietnutie, rezolučný strom

Rezoluční důkaz (odvození) klauzule C z formule S je konečná posloupnost klauzulí $C_0, C_1, \ldots, C_n = C$ taková, že pro každé i buď' $C_i \in S$ nebo C_i je rezolventou nějakých C_j, C_k kde $j < i$ a $k < i$.

Pokud rezoluční důkaz existuje, říkáme, že C je rezolucí dokazatelná z S, a píšeme $S \vdash_R C$. (Rezoluční) zamítnutí formule S je rezoluční důkaz $\square$ z S, v tom případě je S (rezolucí) zamítnutelná.

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

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

12. Lineárna rezolúcia, lineárny dôkaz, LI-rezolúcia, LI-dôkaz

Výroková

Lineární důkaz (rezolucí) klauzule C z formule S je konečná posloupnost

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

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.

LI-rezoluce V obecném lineárním důkazu může být každá následující boční klauzule buď axiom z S nebo jedna z předchozích centrálních klauzulí. Pokud zakážeme druhou možnost, budeme-li tedy požadovat, aby všechny boční klauzule byly z S, dostaneme tzv. LI (linear-input) rezoluci:

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

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

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.

Predikátová

Lineární důkaz (rezolucí) klauzule C z formule S je konečná posloupnost

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

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 je varianta klauzule z S, pro $i \leq n$ je C_{i+1} rezolventou C_i a B_i,
- B_0 je varianta klauzule z S, pro $i \leq n$ je 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 lineární důkaz, ve kterém je každá boční klauzule B_i variantou klauzule z S. Pokud existuje LI-důkaz, říkáme, že je C LI-dokazatelná z S, a píšeme $S \vdash_{LI} C$. Pokud $S \vdash_{LI} \square$, je S LI-zamítnutelná.

13. Signatúra a jazyk predikátovej logiky, štruktúra daného jazyka

Signatura je dvojice $\langle \mathcal{R}, \mathcal{F} \rangle$, kde $\mathcal{R}, \mathcal{F}$ jsou disjunktní množiny symbolů (relační a funkční, ty zahrnují konstantní) spolu s danými aritami (tj. danými funkcí ar: $\mathcal{R} \cup \mathcal{F} \to \mathbb{N}$) a neobsahující symbol '=' (ten je rezervovaný pro rovnost).

Do jazyka patří následující:

- spočetně mnoho proměnných $x_0, x_1, x_2, \ldots$ (ale píšeme také $x, y, z, \ldots$; množinu všech proměnných označíme Var),
- relační, funkční a konstantní symboly ze signatury, a symbol $=$ jde-li o jazyk s rovností,
- univerzální a existenční kvantifikátory $(\forall x), (\exists x)$ pro každou proměnnou $x \in \mathrm{Var}$,
- symboly pro logické spojky $\neg, \wedge, \vee, \to, \leftrightarrow$ a závorky $(,)$.

Struktura v signatuře $\langle \mathcal{R}, \mathcal{F} \rangle$ je trojice $\mathcal{A} = \langle A, \mathcal{R}^{\mathcal{A}}, \mathcal{F}^{\mathcal{A}} \rangle$, kde

- A je neprázdná množina, říkáme jí doména (také univerzum),
- $\mathcal{R}^{\mathcal{A}} = \{ R^{\mathcal{A}} \mid R \in \mathcal{R} \}$ kde $R^{\mathcal{A}} \subseteq A^{\mathrm{ar}(R)}$ je interpretace relačního symbolu R,
- $\mathcal{F}^{\mathcal{A}} = \{ f^{\mathcal{A}} \mid f \in \mathcal{F} \}$ kde $f^{\mathcal{A}} : A^{\mathrm{ar}(R)} \to A$ je interpretace funkčního symbolu f (speciálně pro konstantní symbol $c \in \mathcal{F}$ máme $c^{\mathcal{A}} \in A$).

14. Atomická formule, formule, sentence, otvorené formule

Termy jazyka L jsou konečné nápisy definované induktivně:

- každá proměnná a každý konstantní symbol z L je term,
- je-li f funkční symbol z L arity n a jsou-li $t_1, \ldots, t_n$ termy, potom nápis $f(t_1, t_2, \ldots, t_n)$ je také term.

Množinu všech termů jazyka L označíme Term_L.

Atomická formule jazyka L je nápis $R(t_1, \ldots, t_m)$, kde R je n-ární relační symbol z L (včetně $=$ jde-li o jazyk s rovností) a $t_i \in \mathrm{Term}_L$.

Formule jazyka L jsou konečné nápisy definované induktivně:

- každá atomická formule jazyka L je formule,
- je-li φ formule, potom $(\neg\varphi)$ je také formule,
- jsou-li φ, ψ formule, potom $(\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \to \psi)$, a $(\varphi \leftrightarrow \psi)$ jsou také formule,
- je-li φ formule a x proměnná, potom $((\forall x)\varphi)$ a $((\exists x)\varphi)$ jsou také formule.

Formule je otevřená, neobsahuje-li žádný kvantifikátor, a uzavřená (neboli sentence), pokud nemá žádnou volnou proměnnou.

15. Instance formule, substitovateľnosť, variant formule

Term t je substituovatelný za proměnnou x ve formuli φ, pokud po simultánním nahrazení všech volných výskyti x ve φ za t nevznikne ve φ žádný vázaný výskyt proměnné z t. V tom případě říkáme vzniklé formuli instance φ vzniklá substitucí t za x, a označujeme ji $\varphi(x/t)$.

Má-li formule φ podformuli tvaru $(Qx)\psi$ a je-li y proměnná, taková, že

- y je substituovatelná za x do ψ a
- y nemá volný výskyt v ψ, potom nahrazením podformule $(Qx)\psi$ formulí $(Qy)\psi(x/y)$ vznikne varianta formule φ v podformuli $(Qx)\psi$.

16. Pravdivostná hodnota formuly v štruktúre pri ohodnotení, platnosť formule v štruktúre

Hodnota termu t ve struktuře $\mathcal{A}$ pri ohodnocení e, kterou značíme $t^{\mathcal{A}}[e]$, je dána induktivně:

- $x^{\mathcal{A}}[e] = e(x)$ pro proměnnou $x \in \mathrm{Var}$,
- $c^{\mathcal{A}}[e] = c^{\mathcal{A}}$ pro konstantní symbol $c \in \mathcal{F}$, a
- je-li $t = f\,(t_1, \ldots, t_n)$ složený term, kde $f \in \mathcal{F}$, potom:

$$t^{\mathcal{A}}[e] = f^{\mathcal{A}}\left(t_1^{\mathcal{A}}[e], \ldots, t_n^{\mathcal{A}}[e]\right)$$

Mějme formuli φ v jazyce L, strukturu $\mathcal{A} \in \mathrm{M}(L)$, a ohodnocení proměnných $e : \mathrm{Var} \to A$. Pravdivostni hodnota φ v $\mathcal{A}$ při ohodnocení e, $\mathrm{PH}^{\mathcal{A}}(\varphi)[e]$, je definována induktivně podle struktury formule: Pro atomickou formuli $\varphi = R\,(t_1, \ldots, t_n)$ máme

$$\mathrm{PH}^{\mathcal{A}}(\varphi)[e] = \begin{cases} 1 & \text{pokud } \left(t_1^{\mathcal{A}}[e], \ldots, t_n^{\mathcal{A}}[e]\right) \in R^{\mathcal{A}}, \\ 0 & \text{jinak.} \end{cases}$$

Speciálně, je-li φ tvaru $t_1 = t_2$, potom $\mathrm{PH}^{\mathcal{A}}(\varphi)[e] = 1$ právě kdyz $\left(t_1^{\mathcal{A}}[e], t_2^{\mathcal{A}}[e]\right) \in =^{\mathcal{A}}$, kde $=^{-\mathcal{A}}$ je identita na A, tj. právě když $t_1^{\mathcal{A}}[e] = t_2^{\mathcal{A}}[e]$ (obě strany rovnosti jsou stejný prvek $a \in A$). Pravdivostní hodnota negace je definována takto:

$$\mathrm{PH}^{\mathcal{A}}(\neg\varphi)[e] = f_{\neg}\left(\mathrm{PH}^{\mathcal{A}}(\varphi)[e]\right) = 1 - \mathrm{PH}^{\mathcal{A}}(\varphi)[e]$$

Obdobně pro binární logické spojky, jsou-li φ, ψ a $\square \in \{\wedge, \vee, \to, \leftrightarrow\}$, potom:

$$\mathrm{PH}^{\mathcal{A}}(\varphi \square \psi)[e] = f_{\square}\left(\mathrm{PH}^{\mathcal{A}}(\varphi)[e], \mathrm{PH}^{\mathcal{A}}(\psi)[e]\right)$$

Zbývá definovat pravdivostní hodnotu pro kvantifikátory, tj. formule tvaru $(Qx)\varphi$. Budeme potřebovat následující značení: Změníme-li v ohodnocení $e : \mathrm{Var} \to A$ hodnotu pro proměnnou x na a, výsledné ohodnocení zapíšeme jako $e(x/a)$. Platí tedy $e(x/a)(x) = a$. Pravdivostní hodnotu pro $(Qx)\varphi$ definujeme takto:

$$\mathrm{PH}^{\mathcal{A}}((\forall x)\varphi)[e] = \min_{a \in A}\left(\mathrm{PH}^{\mathcal{A}}(\varphi)[e(x/a)]\right)$$
$$\mathrm{PH}^{\mathcal{A}}((\exists x)\varphi)[e] = \max_{a \in A}\left(\mathrm{PH}^{\mathcal{A}}(\varphi)[e(x/a)]\right)$$

Mějme formuli φ a strukturu $\mathcal{A}$ (ve stejném jazyce).

- Je-li e ohodnocení a $\mathrm{PH}^{\mathcal{A}}(\varphi)[e] = 1$, potom říkáme, že φ platí v $\mathcal{A}$ při ohodnocení e, a píšeme $\mathcal{A} \models \varphi[e]$. (V opačném případě říkáme, že φ neplatí $v\mathcal{A}$ při ohodnocení e, a píšeme $\mathcal{A} \not\models \varphi[e]$.)
- Pokud φ platí v $\mathcal{A}$ při každém ohodnocení $e : \mathrm{Var} \to A$, potom říkáme, že φ je pravdivá (platí) $v\mathcal{A}$, a píšeme $\mathcal{A} \models \varphi$.
- Pokud $\mathcal{A} \models \neg\varphi$, tj. φ neplatí v $\mathcal{A}$ při žádném ohodnocení (pro každé e máme $\mathcal{A}\forall = \varphi[e]$), potom je φ lživá $v\mathcal{A}$.[20]

Shrňme několik jednoduchých vlastností, nejprve týkajících se platnosti při ohodnocení. Bud' $\mathcal{A}$ struktura, φ, ψ formule, a e ohodnocení.

- $\mathcal{A} = \neg\varphi[e]$ právě když $\mathcal{A} \not\models \varphi[e]$,
- $\mathcal{A} \models (\varphi \wedge \psi)[e]$ právě když $\mathcal{A} \models \varphi[e]$ a $\mathcal{A} \models \psi[e]$,
- $\mathcal{A} \models (\varphi \vee \psi)[e]$ právě když $\mathcal{A} \models \varphi[e]$ nebo $\mathcal{A} \models \psi[e]$,
- $\mathcal{A} \models (\varphi \to \psi)[e]$ právě když platí: jestliže $\mathcal{A} \models \varphi[e]$ potom $\mathcal{A} \models \psi[e]$,
- $\mathcal{A} \models (\varphi \leftrightarrow \psi)[e]$ právě když platí: $\mathcal{A} \models \varphi[e]$ právě když $\mathcal{A} \models \psi[e]$,
- $\mathcal{A} \models (\forall x)\varphi[e]$ právě když $\mathcal{A} \models \varphi[e(x/a)]$ pro všechna $a \in A$,
- $\mathcal{A} \models (\exists x)\varphi[e]$ právě když $\mathcal{A} \models \varphi[e(x/a)]$ pro nějaké $a \in A$.
- Je-li term t substituovatelný za proměnnou x do formule φ, potom

$$\mathcal{A} \models \varphi(x/t)[e] \text{ právě když } \mathcal{A} \models \varphi[e(x/a)] \text{ pro } a = t^{\mathcal{A}}[e].$$

- Je-li ψ varianta φ, potom $\mathcal{A} \models \varphi[e]$ právě když $\mathcal{A} \models \psi[e]$.

17. Kompletná teória v predikátovej logike, elementárna ekvivalencia

Teorie je kompletní, je-li bezesporná a každá sentence je v ní buď pravdivá, nebo lživá.

Struktury $\mathcal{A}, \mathcal{B}$ (v témž jazyce) jsou elementárně ekvivalentní, pokud v nich platí tytéž sentence. Značíme $\mathcal{A} \equiv \mathcal{B}$.

Teorie je kompletní, právě když má právě jeden model až na elementární ekvivalenci.

18. Podštruktúra, generovaná podštruktúra, expanzia a redukt štruktúry

Mějme strukturu $\mathcal{A} = \langle A, \mathcal{R}^{\mathcal{A}}, \mathcal{F}^{\mathcal{A}} \rangle$ v signatuře $\langle \mathcal{R}, \mathcal{F} \rangle$. Struktura $\mathcal{B} = \langle B, \mathcal{R}^{\mathcal{B}}, \mathcal{F}^{\mathcal{B}} \rangle$ je (indukovaná) podstruktura $\mathcal{A}$, značíme $\mathcal{B} \subseteq \mathcal{A}$, jestliže

- $\emptyset \neq B \subseteq A$
- $R^{\mathcal{B}} = R^{\mathcal{A}} \cap B^{\mathrm{ar(R)}}$ pro každý relační symbol $R \in \mathcal{R}$,
- $f^{\mathcal{B}} = f^{\mathcal{A}} \cap \left(B^{\mathrm{ar(f)}} \times B\right)$ pro každý funkční symbol $f \in \mathcal{F}$ (tj. funkce $f^{\mathcal{B}}$ je restrikce $f^{\mathcal{A}}$ na množinu B, a její výstupy jsou všechny také z B),
- speciálně, pro každý konstantní symbol $c \in \mathcal{F}$ máme $c^{\mathcal{B}} = c^{\mathcal{A}} \in B$.

Mějme strukturu $\mathcal{A} = \langle A, \mathcal{R}^{\mathcal{A}}, \mathcal{F}^{\mathcal{A}} \rangle$ a neprázdnou podmnožinu $X \subseteq A$. Označme jako B nejmenší podmnožinu A, která obsahuje množinu X a je uzavřená na všechny funkce struktury $\mathcal{A}$ (tj. také obsahuje všechny konstanty). Potom o podstruktuře $\mathcal{A}\lceil B$ říkáme, že je generovaná množinou X, a značíme ji $\mathcal{A}\langle X \rangle$.

Mějme jazyky $L \subseteq L'$, L-strukturu $\mathcal{A}$, a L'-strukturu $\mathcal{A}'$ na stejné doméně $A = A'$. Jestliže je interpretace každého symbolu [relačního, funkčního, konstantního] stejná [relace, funkce, konstanta] v $\mathcal{A}$ i v $\mathcal{A}'$ potom říkáme, že struktura $\mathcal{A}'$ je expanzí struktury $\mathcal{A}$ do jazyka L' (také říkáme, že je L'-expanzí) a že struktura $\mathcal{A}$ je reduktem struktury $\mathcal{A}'$ na jazyk L (také říkáme, že je L-reduktem).

19. Definovateľnosť v štruktúre

Mějme formuli $\varphi(x_1, \ldots, x_n)$ a strukturu $\mathcal{A}$ v témž jazyce. Množina definovaná formulí $\varphi(x_1, \ldots, x_n)$ ve struktuře $\mathcal{A}$, značíme $\varphi^{\mathcal{A}}(x_1, \ldots, x_n)$, je:

$$\varphi^{\mathcal{A}}(x_1, \ldots, x_n) = \{(a_1, \ldots, a_n) \in A^n \mid \mathcal{A} \models \varphi[e(x_1/a_1, \ldots, x_n/a_n)]\}$$

Zkráceně totéž zapíšeme také jako

$$\varphi^{\mathcal{A}}(\bar{x}) = \{\bar{a} \in A^n \mid \mathcal{A} \models \varphi[e(\bar{x}/\bar{a})]\}.$$

Mějme formuli $\varphi(\bar{x}, \bar{y})$, kde $|\bar{x}| = n$ a $|\bar{y}| = k$, strukturu $\mathcal{A}$ v témž jazyce, a k-tici prvků $\bar{b} \in A^k$. Množina definovaná formulí $\varphi(\bar{x}, \bar{y})$ s parametry $\bar{b}$ ve struktuře $\mathcal{A}$, značíme $\varphi^{\mathcal{A},\bar{b}}(\bar{x}, \bar{y})$, je:

$$\varphi^{\mathcal{A},\bar{b}}(\bar{x}, \bar{y}) = \left\{\bar{a} \in A^n \mid \mathcal{A} \models \varphi[e(\bar{x}/\bar{a}, \bar{y}/\bar{b})]\right\}$$

20. Extenze o definice

Máme-li L-teorii T a L'-teorii T', potom řekneme, že T' je extenzi T o definice, pokud vznikla z T postupnou extenzí o definice relačních a funkčních (příp. konstantních) symbolů.

Mějme teorii T a formuli $\psi(x_1, \ldots, x_n)$ v jazyce L. Označme jako L' rozšíření jazyka L o nový n-ární relační symbol R. Extenze teorie T o definici R formuli ψ je L'-teorie:

$$T' = T \cup \{R(x_1, \ldots, x_n) \leftrightarrow \psi(x_1, \ldots, x_n)\}$$

Mějme teorii T a formuli $\psi(x_1, \ldots, x_n, y)$ v jazyce L. Označme jako L' rozšírínení jazyka L o nový n-ární funkční symbol f. Nechť v teorii T platí:

- axiom existence $(\exists y)\psi(x_1, \ldots, x_n, y)$,
- axiom jednoznačnosti $\psi(x_1, \ldots, x_n, y) \wedge \psi(x_1, \ldots, x_n, z) \rightarrow y = z$. Potom extenze teorie T o definici f formuli ψ je L'-teorie:

$$T' = T \cup \{f(x_1, \ldots, x_n) = y \leftrightarrow \psi(x_1, \ldots, x_n, y)\}$$

Konstantní symbol je speciálním případem funkčního symbolu arity 0 . Platí tedy stejná tvrzení. Axiomy existence a jednoznačnosti jsou: $(\exists y)\psi(y)$ a $\psi(y) \wedge \psi(z) \rightarrow y = z$. A extenze o definici konstantního symbolu c formulí $\psi(y)$ je teorie $T' = T \cup \{c = y \leftrightarrow \psi(y)\}$.

21. Prenexná normálna forma, Skolemov variant

Formule φ je v prenexní normální formě (PNF), je-li tvaru

$$(Q_1 x_1) \ldots (Q_n x_n)\, \varphi'$$

kde Q_i je kvantifikátor ($\forall$ nebo $\exists$) a formule φ' je otevřená. Formuli φ' potom říkáme otevřené jádro φ a $(Q_1 x_1) \ldots (Q_n x_n)$ je kvantifikátorový prefix.

Mějme L-sentenci φ v PNF, a necht všechny její vázané proměnné jsou různé. Necht' existenční kvantifikátory z prefixu φ jsou $(\exists y_1), \ldots, (\exists y_n)$ (v tomto pořadí), a nechť pro každé i jsou $(\forall x_1), \ldots, (\forall x_{n_i})$ právě všechny univerzální kvantifikátory předcházející kvantifikátor $(\exists y_i)$ v prefixu φ.

Označme L' rozšíření L o nové n_i-ární funkční symboly $f_1, \ldots, f_n$, kde symbol f_i je arity n_i, pro každé i. Skolemova varianta sentence φ je L'-sentence φ_S vzniklá z φ tak, že pro každé $i = 1, \ldots, n$:

- odstraníme z prefixu kvantifikátor $(\exists y_i)$, a
- substituujeme za proměnnou y_i term $f_i(x_1, \ldots, x_{n_i})$.

Tomuto procesu říkáme také skolemizace.

22. Izomorfizmus štruktúr, izomorfné spektrum, ω-kategorická teória

Mějme struktury $\mathcal{A}, \mathcal{B}$ jazyka $L = \langle \mathcal{R}, \mathcal{F} \rangle$. Izomorfismus $\mathcal{A}$ a $\mathcal{B}$ (nebo ' $\mathcal{A}$ na ') je bijekce $h : A \to B$ splňující následující vlastnosti:

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

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

(Speciálně, je-li $c \in \mathcal{F}$ konstantní symbol, platí $h\left(c^{\mathcal{A}}\right) = c^{\mathcal{B}}$.)

- Pro každý (n-ární) relační symbol $R \in \mathcal{R}$ a pro všechna $a_i \in A$ platí:

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

Pokud existuje, říkáme, že $\mathcal{A}$ a $\mathcal{B}$ jsou izomorfní (nebo ' $\mathcal{A}$ je izomorfní s $\mathcal{B}$ via h ') a píšeme $\mathcal{A} \simeq \mathcal{B}$ (nebo $\mathcal{A} \simeq_h \mathcal{B}$). Automorfismus $\mathcal{A}$ je izomorfismus $\mathcal{A}$ na $\mathcal{A}$

Izomorfní spektrum teorie T je počet $I(\kappa, T)$ modelů T kardinality κ až na izomorfismus, pro každou kardinalitu κ (včetně transfinitních). Teorie T je κ-kategorická, pokud $I(\kappa, T) = 1$.

Nadále nás bude zajímat jen případ $\kappa = \omega$, totiž teorie s jediným spočetně nekonečným modelem (až na izomorfismus).

23. Axiomatizovateľnosť, konečná axiomatizovateľnosť, otvorená axiomatizovateľnosť

Mějme třídu struktur $K \subseteq \mathrm{M}_L$ v nějakém jazyce L. Říkáme, že K je

- axiomatizovatelná, pokud existuje L-teorie T taková, že $\mathrm{M}_L(T) = K$,
- konečně axiomatizovatelná, pokud je axiomatizovatelná konečnou teorií, a
- otevřeně axiomatizovatelná, pokud je axiomatizovatelná otevřenou teorií.

O L-teorii T' říkáme, že je konečně resp. otevřeně axiomatizovatelná, pokud to platí o třídě modelů $K = \mathrm{M}_L\left(T'\right)$.

24. Rekurzívna axiomatizácia, rekurzívna axiomatizovateľnosť, rekurzívne spočetná kompletácia

Teorie T je rekurzivně axiomatizovaná, pokud existuje algoritmus, který pro každou vstupní formuli φ doběhne a odpoví, zda $\varphi \in T$.

Třída L-struktur $K \subseteq \mathrm{M}_L$ je rekurzivně axiomatizovatelná, pokud existuje rekurzivně axiomatizovaná L-teorie T taková, že $K = M_L(T)$. Teorie T' je rekurzivně axiomatizovatelná, pokud je rekurzivně axiomatizovatelná třída jejích modelů, neboli pokud je T' ekvivalentní nějaké rekurzivně axiomatizované teorii.

Řekneme, že teorie T má rekurzivně spočetnou kompletaci, pokud (nějaká) množina až na ekvivalenci všech jednoduchých kompletních extenzí teorie T je rekurzivně spočetná, tj. existuje algoritmus, který pro danou vstupní dvojici přirozených čísel (i, j) vypíše na výstup i-tý axiom j-té extenze (v nějakém pevně daném uspořádání), nebo odpoví, že takový axiom už neexistuje.

25. Rozhodnuteľná a čiastočne rozhodnuteľná teória

O teorii T říkáme, že je

- rozhodnutelná, pokud existuje algoritmus, který pro každou vstupní formuli φ doběhne a odpoví, zda $T \models \varphi$,
- částečně rozhodnutelná, pokud existuje algoritmus, který pro každou vstupní formuli:
- pokud $T \models \varphi$, doběhne a odpoví "ano",
- pokud $T \not\models \varphi$, buď nedoběhne, nebo doběhne a odpoví "ne".

Nechť T je rekurzivně axiomatizovaná. Potom:

1. T je částečně rozhodnutelná,
2. je-li T navíc kompletní, potom je rozhodnutelná.

Ľahké otázky

1. Množinu modelov nad konečným jazykom je možné axiomatizovať výrokom v CNF, výrokom v DNF

Mějme konečný jazyk $\mathbb{P}$ a libovolnou množinu modelů $M \subseteq \mathrm{M}_{\mathbb{P}}$. Potom existuje výrok $\varphi_{\mathrm{DNF}} v$ DNF a výrok φ_{CNF} v CNF takový, že $M = \mathrm{M}_{\mathbb{P}}(\varphi_{\mathrm{DNF}}) = \mathrm{M}_{\mathbb{P}}(\varphi_{\mathrm{CNF}})$. Konkrétně:

$$\varphi_{\mathrm{DNF}} = \bigvee_{v \in M} \bigwedge_{p \in \mathbb{P}} p^{v(p)}$$
$$\varphi_{\mathrm{CNF}} = \bigwedge_{v \in \bar{M}} \bigvee_{p \in \mathbb{P}} \overline{p^{v(p)}} = \bigwedge_{v \notin M} \bigvee_{p \in \mathbb{P}} p^{1-v(p)}$$

Každá elementární konjunkce popisuje jeden model. Výrok φ_{CNF} je duální k výroku φ'_{DNF} sestrojenému pro doplněk $M' = \bar{M}$. Nebo můžeme dokázat přímo: modely klauzule $C_v = \bigvee_{p \in \mathbb{P}} p^{1-v(p)}$ jsou všechny modely kromě v, $\mathrm{M}_C = \mathrm{M}_P \backslash \{v\}$, tedy každá klauzule v konjunkci zakazuje jeden nemodel.

Množiny logických spojek $\{\neg, \wedge, \vee\} a \{\neg, \rightarrow\}$ jsou univerzální. **Důkaz**. Mějme funkci $f : \{0,1\}^n \rightarrow \{0,1\}$, resp. množinu modelů $M = f^{-1}[1] \subseteq \{0,1\}^n$. Náš jazyk bude $\mathbb{P} = \{p_1, \ldots, p_n\}$. Pokud by množina M obsahovala jediný model, např. $v = (1,0,1,0)$ mohli bychom ji reprezentovat výrokem $\varphi_v = p_1 \wedge \neg p_2 \wedge p_3 \wedge \neg p_4$, který říká 'musím být model v '. Pro obecný model v bychom výrok φ_v zapsali takto:

$$\varphi_v = p_1^{v_1} \wedge p_2^{v_2} \wedge \cdots \wedge p_n^{v_n} = \bigwedge_{i=1}^{n} p_i^{v(p_i)} = \bigwedge_{p \in \mathbb{P}} p^{v(p)}$$

kde zavádíme následující užitečné značení: $p^{v(p)}$ je výrok p pokud $v(p) = 1$, a výrok $\neg p$ pokud $v(p) = 0$
Obsahuje-li množina M více modelů, řekneme 'musím být alespoň jeden z modelů z M':

$$\varphi_M = \bigvee_{v \in M} \varphi_v = \bigvee_{v \in M} \bigwedge_{p \in \mathbb{P}} p^{v(p)}$$

Zřejmě platí $M_{\mathbb{P}}(\varphi_M) = M$ neboli $f_{\varphi_M, \mathbb{P}} = f$. (Pokud $M = \emptyset$, potom z definice $\bigvee_{v \in M} \varphi_v = L$).

2. Algebra výrokov bezspornej teórie nad konečným jazykom je izomorfná potenčnej algebre

uvažujeme množinu ekvivalenčních tříd na množině všech výroků $\mathrm{VF}_{\mathbb{P}}$, kterou označíme $\mathrm{VF}_{\mathbb{P}} / \sim$. Prvky této množiny jsou množiny ekvivalentních výroků, např. $[p \rightarrow q]_\sim = \{p \rightarrow q, \neg p \vee q, \neg(p \wedge \neg q), \neg p \vee q \vee q, \ldots\}$. A máme zobrazení $h : \mathrm{VF}_{\mathrm{P}} / \sim \rightarrow \mathcal{P}(\mathrm{M}_{\mathrm{P}})$ (kde $\mathcal{P}(X)$ je množina všech podmnožin X) definované předpisem:

$$h([\varphi]_\sim) = \mathrm{M}(\varphi)$$

tj. třídě ekvivalentních výroků přiřadíme množinu modelů libovolného z nich. Je snadné ověřit, že toto zobrazení je korektně definované (nezáleží na tom, jaký výrok z třídy ekvivalence jsme si vybrali) a prosté, a že je-li jazyk $\mathbb{P}$ konečný, je h dokonce bijekce. (Ověřte!) Na množině $\mathrm{VF}_{\bar{F}} / \sim$ můžeme zavést operace $\neg, \wedge, \vee$ pomocí předpisu

$$\neg[\varphi]_\sim = [\neg\varphi]_\sim$$
$$[\varphi]_\sim \wedge [\psi]_\sim = [\varphi \wedge \psi]_\sim$$
$$[\varphi]_\sim \vee [\psi]_\sim = [\varphi \vee \psi]_\sim$$

tedy vybereme reprezentanta resp. reprezentanty, a provedeme operaci s nimi, např. 'konjunkce' tříd $[p \rightarrow q]_\sim$ a $[q \vee \neg r]_\sim$ je:

$$[p \rightarrow q]_\sim \wedge [q \vee \neg r]_\sim = [(p \rightarrow q) \wedge (q \vee \neg r)]_\sim$$

Přidáme-li také konstanty $\bot = [\bot]_\sim$ a $\top = [\top]_\sim$, dostáváme (matematickou) strukturu [26]

$$\mathbf{AV}_{\mathbb{P}} = \langle \mathrm{VF}_{\mathrm{P}} / \sim; \neg, \wedge, \vee, \bot, \top \rangle$$

které říkáme algebra výroků jazyka $\mathbb{P}$.
Zobrazení $h : \mathrm{VF}_{\mathrm{P}} / \sim \rightarrow \mathcal{P}(\mathrm{M}_{\mathbb{P}})$ je tedy zobrazení z algebry výroků $\mathbf{AV}_{\mathbb{P}}$ na potenční algebru

$$\mathcal{P}\left(\mathrm{M}_{\mathbb{P}}\right)=\left\langle \mathcal{P}\left(\mathrm{M}_{\mathbb{P}}\right);-,\cap,\cup,\emptyset,\mathrm{M}_{\mathbb{P}}\right\rangle$$

a je-li jazyk konečný, je to bijekce. Toto zobrazení 'zachovává' operace a konstanty, tj. platí $h(\bot)=\emptyset, h(\top)=\mathrm{M}_{\mathbb{P}}$, a

$$\begin{aligned} h\left(\neg[\varphi]_{\sim}\right)&=\overline{h\left([\varphi]_{\sim}\right)}=\overline{\mathrm{M}(\varphi)}=\mathrm{M_P}\backslash\mathrm{M}(\varphi)\\ h\left([\varphi]_{\sim}\wedge[\psi]_{\sim}\right)&=h\left([\varphi]_{\sim}\right)\cap h\left([\psi]_{\sim}\right)=\mathrm{M}(\varphi)\cap\mathrm{M}(\psi)\\ h\left([\varphi]_{\sim}\vee[\psi]_{\sim}\right)&=h\left([\varphi]_{\sim}\right)\cup h\left([\psi]_{\sim}\right)=\mathrm{M}(\varphi)\cup\mathrm{M}(\psi)\end{aligned}$$

Takovému zobrazení říkáme homomorfismus Booleových algeber, a je-li to bijekce, jde o izomorfismus. **Poznámka** 2.5.2. Tyto vztahy můžeme také využít při hledání modelů: například pro výrok $\varphi\to(\neg\psi\wedge\chi)$ platí (s využitím toho, že $\mathrm{M}\left(\varphi\to\varphi'\right)=M\left(\neg\varphi\vee\varphi'\right)$) :

$$\mathrm{M}(\varphi\to(\neg\psi\wedge\chi))=\overline{\mathrm{M}(\varphi)}\cup(\overline{\mathrm{M}(\psi)}\cap\mathrm{M}(\chi))$$

Všechny předchozí úvahy můžeme také relativizovat vzhledem k dané teorii T v jazyce $\mathbb{P}$, a to tak, že ekvivalenci $\sim$ nahradíme T-ekvivalencí $\sim_T$ a množinu modelů jazyka $\mathrm{M}_{\mathbb{P}}$ nahradíme množinou modelů teorie $\mathrm{M}_{\mathbb{P}}(T)$. Dostáváme:

$$\begin{aligned} h(\bot)&=\emptyset,\\ h(\top)&=\mathrm{M}(T)\\ h\left(\neg[\varphi]_{\sim_T}\right)&=\mathrm{M}(T)\backslash\mathrm{M}(T,\varphi)\\ h\left([\varphi]_{\sim_T}\wedge[\psi]_{\sim_T}\right)&=\mathrm{M}(T,\varphi)\cap\mathrm{M}(T,\psi)\\ h\left([\varphi]_{\sim_T}\vee[\psi]_{\sim_T}\right)&=\mathrm{M}(T,\varphi)\cup\mathrm{M}(T,\psi)\end{aligned}$$

Výslednou algebru výroků vzhledem k teorii T označíme $\mathbf{AV}_{\mathbb{P}}(T)$. Algebra výroků jazyka je tedy totéž co algebra výroků vzhledem k prázdné teorii. Z technických důvodů potřebujeme, aby $\mathrm{M}(T)$ byla neprázdná, tj. T musí být bezesporná. Shrňme naše úvahy:

Důsledek 2.5.3. Je-li T bezesporná teorie nad konečným jazykem $\mathbb{P}$, potom je algebra výroků $\mathbf{AV}_{\mathbb{P}}(T)$ izomorfní potenční algebre $\mathcal{P}\left(\mathrm{M}_{\mathbb{P}}(\mathbf{T})\right)$ prostřednictvím zobrazení $h\left([\varphi]_{\sim_T}\right)=M(T,\varphi)$

3. 2-SAT, Algoritmus implikačného grafu, jeho korektnosť

Výrok φ je v k-CNF, pokud je v CNF a každá klauzule má nejvýše k literálů. Problému k-SAT se ptá, zda je daný k-CNF formule splnitelná. Pro $k\geq 3$ je k-SAT nadále NP-úplný, každou CNF formuli lze zakódovat do 3-CNF formule.

Implikační graf 2-CNF výroku φ je založený na myšlence, že 2-klauzuli $\ell_1\vee\ell_2$ (kde ℓ_1,ℓ_2 jsou literály) lze chápat jako dvojici implikací: $\overline{\ell_1}\to\ell_2$ a $\overline{\ell_2}\to\ell_1$.[4] Například, z klauzule $\neg p_1\vee p_2$ vzniknou implikace $p_1\to p_2$ a také , $\neg p_2\to\neg p_1$. Tedy pokud p_1 platí v nějakém modelu, musí platit i p_2, a pokud p_2 neplatí, nesmí platit ani p_1. Jednotkovou klauzuli ℓ můžeme také vyjádřit pomocí implikace jako $\bar{\ell}\to\ell$, např. z p_1 dostáváme $\neg p_1\to p_1$.

Implikační graf $\mathcal{G}_\varphi$ je tedy orientovaný graf, jehož vrcholy jsou všechny literály (proměnné z $\mathrm{Var}(\varphi)$ a jejich negace) a hrany jsou dané implikacemi popsanými výše:

- $V\left(\mathcal{G}_\varphi\right)=\{p,\neg p\mid p\in\mathrm{Var}(\varphi)\}$
- $E\left(\mathcal{G}_\varphi\right)=\left\{\left(\overline{\ell_1},\ell_2\right),\left(\overline{\ell_2},\ell_1\right)\mid \ell_1\vee\ell_2 \text{ je klauzule } \varphi\right\}\cup\{(\bar{\ell},\ell)\mid \ell \text{ je jednotková klauzule } \varphi\}$

V našem příkladě máme množinu vrcholů

$$V\left(\mathcal{G}_\varphi\right)=\{p_1,p_2,p_3,p_4,p_5,\neg p_1,\neg p_2,\neg p_3,\neg p_4,\neg p_5\}$$

a hrany jsou:

$$\begin{aligned} E\left(\mathcal{G}_\varphi\right)=\{&(p_1,p_2),(\neg p_2,\neg p_1),(p_2,\neg p_3),(p_3,\neg p_2),(\neg p_1,p_3),(\neg p_3,p_1),(\neg p_3,\neg p_4),\\ &(p_4,p_3),(p_1,p_5),(\neg p_5,\neg p_1),(\neg p_2,p_5),(\neg p_5,p_2),(\neg p_1,p_1),(p_4,\neg p_4)\}\end{aligned}$$

3.2.1 Silně souvislé komponenty Nyní musíme najít komponenty silné souvislosti [5] tohoto grafu. V našem příkladě dostáváme následující komponenty: $C_1=\{p_4\},C_2=\{\neg p_5\},C_3=\{\neg p_1,\neg p_2,p_3\},\overline{C_3}=\{p_1,p_2,\neg p_3\}$, $\overline{C_2}=\{p_5\},\overline{C_1}=\{\neg p_4\}$

Všechny literály v jedné komponentě musí být ohodnoceny stejně. Pokud bychom tedy našli dvojici opačných literálů v jedné komponentě, znamená to, že výrok je nesplnitelný. V opačném případě vždy můžeme najít splňující ohodnocení.

Při hledání splňujícího ohodnocení (pokud nám nestačí informace, že výrok je splnitelný) potom postupujeme tak, že vezmeme nejlevější dosud neohodnocenou komponentu, ohodnotíme ji 0 , opačnou komponentu ohodnotíme 1, a postup opakujeme dokud zbývá nějaká [5] Silná souvislost znamená, že existuje orientovaná cesta zu do v i z v do u, neboli každé dva vrcholy v jedné komponentě leží v orientovaném cyklu. A naopak, každý orientovaný cyklus leží uvnitř nějaké komponenty. neohodnocená komponenta. Například, topologické uspořádání na Obrázku 3.3 odpovídá modelu $v = (1, 1, 0, 0, 1)$ Na závěr shrneme naše úvahy do následujícího tvrzení: **Tvrzení** 3.2.2. Výrok φ je splnitelný, právě když žádná silně souvislá komponenta $v\mathcal{G}_\varphi$ neobsahuje dvojici opačných literálů $\ell, \bar{\ell}$.

Důkaz. Každý model, neboli splňující ohodnocení, musí ohodnotit všechny literály ze stejné komponenty stejnou hodnotou. (V opačném případě by nutně existovala implikace $\ell_1 \to \ell_2$, kde ℓ_1v modelu platí ale ℓ_2 neplatí.) V jedné komponentě tedy nemohou být opačné literály. Naopak předpokládejme, že žádná komponenta neobsahuje dvojici opačných literálo, a ukažme, že potom existuje model. Označme $\mathcal{G}^*_\varphi$ graf vzniklý z $\mathcal{G}_\varphi$ kontrakcí silně souvislých komponent. Tento graf je acyklický, zvolme nějaké topologické uspořádání. Model zkonstruujeme tak, že zvolíme první dosud neohodnocenou komponentu v našem topologickém uspořádání, všechny literály v ní obsažené ohodnotíme 0 , a opačné literály ohodnotíme 1. Takto pokračujeme dokud nejsou všechny komponenty ohodnoceny.

Proč v takto získaném modelu platí výrok φ ? Kdyby ne, neplatila by některá z klauzulí. Jednotková klauzule ℓ musí platit, nebot v grafu $\mathcal{G}_\varphi$ máme hranu $\bar{\ell} \to \ell$. Stejná hrana je i v grafu komponent, tedy $\bar{\ell}$ předchází v topologickém uspořádání komponentu obsahující ℓ. Při konstrukci modelu jsme museli ohodnotit $\bar{\ell}$ dříve než ℓ, tedy $\bar{\ell} = 0$ a $\ell = 1$. Podobně, 2-klauzule $\ell_1 \vee \ell_2$ také musí platit: máme hrany $\overline{\ell_1} \to \ell_2$ a $\overline{\ell_2} \to \ell_1$. Pokud jsme ℓ_1 ohodnotili dříve než ℓ_2, museli jsme kvůli hraně $\overline{\ell_1} \to \ell_2$ ohodnotit $\overline{\ell_1} = 0$, tedy ℓ_1 platí. Podobně pokud jsme ohodnotili nejdříve ℓ_2, musí být $\overline{\ell_2} = 0$ a $\ell_2 = 1$.

4. Horn-SAT, Algoritmus jednotkovej propagácie, jeho korektnosť

Horn-SAT neboli problém splnitelnosti hornovských výroků. Výrok je v hornovský (v Hornově tvaru), pokud je konjunkcí hornovských klauzulí, tj. klauzulí obsahujících nejvýše jeden *pozitivní literál. Význam Hornovských klauzulí vyplývá z ekvivalentního vyjádření ve formě implikace:

$$\neg p_1 \vee \neg p_2 \vee \cdots \vee \neg p_n \vee q \sim (p_1 \wedge p_2 \wedge \cdots \wedge p_n) \to q$$

Polynomiální algoritmus pro řešení problému Horn-SAT je založený na jednoduché myšlence jednotkové propagace: Pokud náš výrok obsahuje jednotkovou klauzuli, víme, jak musí být ohodnocenena výroková proměnná obsažená v této klauzuli.

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

Náš výrok φ obsahuje jednotkovou klauzuli p_4. Víme tedy, že v každém jeho modelu $v \in \mathrm{M}(\varphi)$ musí platit $v\,(p_4) = 1$. To ale znamená, že v libovolném modelu výroku φ:

- každá klauzule obsahující pozitivní literál p_4 je splněna, můžeme ji tedy z výroku odstranit,
- negativní literál $\neg p_4$ nemůže být splněn, můžeme ho tedy odstranit ze všech klauzulí, které ho obsahují.

Tomu kroku se říká jednotková propagace. Výsledkem je následující zjednodušený výrok, který označíme φ^{p_4} (obecně φ^ℓ máme-li jednotkovou klauzuli ℓ):

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

Výsledný výrok už neobsahuje jednotkovou klauzuli. To ale znamená, že každá klauzule obsahuje alespoň dva literály, a nejvýše jeden z nich může být pozitivní! (Zde potřebujeme hornovskost výroku.) Protože každá klauzule obsahuje negativní literál, stačí ohodnotit všechny zbývající proměnné 0 , a výrok bude splněn: $v\,(p_1) = v\,(p_2) = v\,(p_3) = 0$. Dostáváme tedy model $v = (0, 0, 0, 1, 1)$.

Algoritmus (Horn-SAT). vstup: výrok φ v Hornově tvaru, výstup: model φ nebo informace, že φ není splnitelný

1. Pokud φ obsahuje dvojici opačných jednotkových klauzulí $\ell, \bar{\ell}$, není splnitelný.
2. Pokud φ neobsahuje žádnou jednotkovou klauzuli, je splnitelný, ohodnot všechny zbývající proměnné 0 .

3. Pokud φ obsahuje jednotkovou klauzuli ℓ, ohodnot literál ℓ hodnotou 1 , proved' jednotkovou propagaci, nahrad' φ výrokem φ^ℓ, a vrat' se na začátek.

4.

5. Algoritmus DPLL pre riešenie SAT

Algoritmus používá jednotkovou propagaci spolu s následujícím pozorováním: Řekneme, že literál ℓ má čistý výskyt vφ, pokud se vyskytuje ve φ, ale opačný literál $\bar{\ell}$ se ve φ nevyskytuje. Máme-li literál s čistým výskytem, můžeme jeho hodnotu nastavit na 1 , a splnit (a odstranit) tak všechny klauzule, které ho obsahují. Pokud výrok neumíme takto zjednodušit, rozvětvíme výpočet dosazením obou možných hodnot pro vybranou výrokovou proměnnou. Jinými slovy, v dalším kroku bychom provedli jednotkovou propagaci r, odstranili jednotkovou klauzuli r, a ze zbývající jednotkové klauzule $\neg r$ bychom odstranili literál $\neg r$, čímž by vznikla prázdná klauzule, která je nesplnitelná.

Algoritmus (DPLL). vstup: výrok φ v CNF, výstup: model φ nebo informace, že φ není splnitelný

1. Dokud φ obsahuje jednotkovou klauzuli ℓ, ohodnot' literál ℓ hodnotou 1 , proved' jednotkovou propagaci, a nahrad' φ výrokem φ^ℓ.

2. Dokud existuje literál ℓ, který má ve φ čistý výskyt, ohodnot ℓ hodnotou 1 , a odstran klauzule obsahující ℓ.

3. Pokud φ neobsahuje žádnou klauzuli, je splnitelný.

4. Pokud φ obsahuje prázdnou klauzuli, není splnitelný.

5. Jinak zvol dosud neohodnocenou výrokovou proměnnou p, a zavolej algoritmus rekurzivně na $\varphi \wedge p$ a na $\varphi \wedge \neg p$.

6. Veta o konštantách

Mějme formuli φ v jazyce L s volnými proměnnými $x_1, \ldots, x_n$. Označme L' rozšíření jazyka o nové konstantní symboly $c_1, \ldots, c_n$ a bud' T' stejná teorie jako T ale v jazyce L'. Potom platí:

$$T \models \varphi \text{ právě } kdyžT' \models \varphi\left(x_1/c_1, \ldots, x_n/c_n\right)$$

Důkaz. **Tvrzení** stačí dokázat pro jednu volnou proměnnou x a jednu konstantu c, indukcí se snadno rozšíríí na n konstant.

Předpokládejme nejprve, že φ platí v každém modelu teorie T. Chceme ukázat, že $\varphi(x/c)$ platí v každém modelu $\mathcal{A}'$ teorie T'. Vezměme tedy takový model $\mathcal{A}'$ a libovolné ohodnocení e : Var $\to A$ a ukažme, že $\mathcal{A}' \models \varphi(x/c)[e]$

Označme jako $\mathcal{A}$ redukt $\mathcal{A}'$ na jazyk L ('zapomeneme' konstantu $c^{\mathcal{A}'}\Big)$. Všimněte si, že $\mathcal{A}$ je model teorie T (axiomy T jsou tytéž jako T', neobsahují symbol c) tedy v něm platí φ. Protože dle předpokladu platí $\mathcal{A} \models \varphi\left[e'\right]$ pro libovolné ohodnocení e', platí i pro ohodnocení $e\left(x/c^{\mathcal{A}'}\right)$ ve kterém ohodnotíme proměnnou x interpretací konstantního symbolu c ve struktuře $\mathcal{A}'$, máme tedy $\mathcal{A} \models \varphi\left[e\left(x/\mathcal{A}^{\mathcal{A}'}\right)\right]$. To ale znamená, že $\mathcal{A}' \models \varphi(x/c)[e]$, což jsme chtěli dokázat. Naopak, předpokládejme, že $\varphi(x/c)$ platí v každém modelu teorie T' a ukažme, že φ platí v každém modelu $\mathcal{A}$ teorie T. Zvolme tedy takový model $\mathcal{A}$ a nějaké ohodnocení e : Var $\to A$ a ukažme, že $\mathcal{A} \models \varphi[e]$

Označme jako $\mathcal{A}'$ expanzi $\mathcal{A}$ do jazyka L', kde konstantní symbol c interpretujeme jako prvek $c^{\mathcal{A}'} = e(x)$. Protože dle předpokladu platí $\mathcal{A}' \models \varphi(x/c)\left[e'\right]$ pro všechna ohodnocení e', platí i $\mathcal{A}' \models \varphi(x/c)[e]$, což ale znamená, že $\mathcal{A}' \models \varphi[e]$. (Nebot' $e = e(x/c)$ a $\mathcal{A}' \models \varphi(x/c)[e(x/c)]$ platí právě když $\mathcal{A}' \models \varphi[e(x/c)]$.) Formule φ ale neobsahuje c (zde používáme, že c je nový), máme tedy i $\mathcal{A} \models \varphi[e]$.

7. Vlastnosti extenzie o definície

Je-li T' extenze teorie T o definice, potom platí:

- Každý model teorie T lze jednoznačně expandovat na model T'.
- T' je konzervativni extenze T.

- Pro každou L'-formuli φ' existuje L-formule φ taková, že $T' \models \varphi' \leftrightarrow \varphi$.

Pro kazdou L'-formuli φ' existuje L-formule φ taková, že $T' \models \varphi' \leftrightarrow \varphi$. **Důkaz**. Stačí dokázat pro formuli φ' s jediným výskytem symbolu f; je-li výskytů více, aplikujeme postup induktivně, v případě vnořených výskytů v jednom termu $f(\ldots f(\ldots)\ldots)$ postupujeme od vnitřních k vnějším.

Označme φ^* formuli vzniklou zφ' nahrazením termu $f(t_1, \ldots, t_n)$ novou proměnnou z. Formuli φ zkonstruujeme takto:

$$(\exists z)\left(\varphi^* \wedge \psi'\left(x_1/t_1, \ldots, x_n/t_n, y/z\right)\right)$$

kde ψ' je varianta ψ zaručující substituovatelnost všech termů. Mějme model $\mathcal{A}$ teorie T' a ohodnocení e. Označme $a = f^{\mathcal{A}}(t_1, \ldots, t_n)[e]$. Díky existenci a jednoznačnosti platí:

$$\mathcal{A} \models \psi'\left(x_1/t_1, \ldots, x_n/t_n, y/z\right)[e] \text{ právě když } e(z) = a$$

Máme tedy $\mathcal{A} \models \varphi[e]$, právě když $\mathcal{A} \models \varphi^*[e(z/a)]$, právě když $\mathcal{A} \models \varphi'[e]$. To platí pro libovolné ohodnocení e, tedy $\mathcal{A} = \varphi' \leftrightarrow \varphi$ pro každý model T', tedy $T' \models \varphi' \leftrightarrow \varphi$. Extenze o definice Máme-li L-teorii T a L'-teorii T', potom řekneme, že T' je extenzí T o definice, pokud vznikla z T postupnou extenzí o definice relačních a funkčních (příp. konstantních) symbolů. Vlastnosti, které jsme dokázali o extenzích o jeden symbol (at už relační nebo funkční), se snadno rozšíríi indukcí na více symbolů: **Důsledek** 6.7.11. T' je konzervativni extenze T.

8. Vzťah definovateľných množín a automorfizmov

Je-li $D \subseteq A^n$ definovatelná ve struktuře $\mathcal{A}$, potom pro každý automorfismus $h \in \mathrm{Aut}(\mathcal{A})$ platí $h[D] = D(kdeh[D]$ značí $\{(h(\bar{a}) \mid \bar{a} \in D\})$.

Je-li D definovatelná s parametry $\bar{b}$, platí totéž pro automorfismy identické na $\bar{b}$, tj. takové, $žeh(\bar{b}) = \bar{b}$(neboli $h(b_i) = b_i$ pro všechna i).

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

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

9. Tablo metóda v jazyku s rovnosťou

Axiomy rovnosti pro jazyk L s rovností jsou následující:

1. $x = x$
2. $x_1 = y_1 \wedge \cdots \wedge x_n = y_n \rightarrow f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)$ pro každý n-ární funkční symbol f jazyka L,
3. $x_1 = y_1 \wedge \cdots \wedge x_n = y_n \rightarrow (R(x_1, \ldots, x_n) \rightarrow R(y_1, \ldots, y_n))$ pro každý n-ární relační symbol R jazyka L včetně rovnosti. Z axiomů (i) a (iii) tedy plyne, že relace $= \mathcal{A}$ je ekvivalence na A, a axiomy (ii) a (iii) vyjadřují, že $= {}^{\mathcal{A}}$ je kongruencí $\mathcal{A}$. V tablo metodě v případě jazyka s rovností implicitně přidáme všechny axiomy rovnosti:

Definice 7.3.4 (Tablo důkaz s rovností). Je-li T teorie v jazyce L s rovností, potom označme jako T^* rozšíření teorie T o generální uzávěry axiomů rovnosti pro jazyk L. Tablo důkaz z teorie T je tablo důkaz z T^*, podobně pro tablo zamítnutí (a obecně jakékoliv tablo).

10. Veta o kompaktnosti a jej aplikácie

Teorie má model, právě když každá jeji konečná část má model.

Důkaz. Každý model teorie T je zjevně modelem každé její části. Druhou implikaci dokážeme nepřímým důkazem: Předpokládejme, že T nemá model, tj. je sporná, a najděme konečnou část $T' \subseteq T$, která je také sporná.

Protože je T sporná, platí $T \vdash \bot$ (zde potřebujeme Větu o úplnosti). Potom existuje konečný tablo důkaz τ výroku $\bot$ z T. Konstrukce tohoto důkazu má jen konečně mnoho kroků, použili jsme tedy jen konečně mnoho axiomů z T. Definujeme-li $T' = \{\alpha \in T \mid \mathrm{T}\ \alpha \text{ je položka v tablu } \tau\}$, potom τ je také tablo důkaz sporu z teorie T'. Teorie T' je tedy sporná konečná část T.

Aplikace kompaktnosti Následující jednoduchou aplikaci Věty o kompaktnosti můžete chápat jako šablonu, kterou následuje i mnoho dalších, složitějších aplikací této věty.

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

Důkaz. Každý podgraf bipartitního grafu je zjevně také bipartitní. Ukažme opačnou implikaci. Graf je bipartitní, právě když je obarvitelný 2 barvami. Označme barvy 0,1 .

Sestrojíme výrokovou teorii T v jazyce $\mathbb{P} = \{p_v \mid v \in V(G)\}$, kde hodnota výrokové proměnné p_v reprezentuje barvu vrcholu v.

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

Zřejmě platí, že G je bipartitní, právě když T má model. Podle Věty o kompaktnosti stačí ukázat, že každá konečná část T má model. Vezměme tedy konečnou $T' \subseteq T$. Bud' G' podgraf G indukovaný na množině vrcholů, o kterých se zmiňuje teorie T', tj.$V(G') = \{v \in V(G) \mid p_v \in \mathrm{Var}(T')\}$. Protože je T' konečná, je G' také konečný, a podle předpokladu je 2-obarvitelný. Libovolné 2-obarvení $V(G')$ ale určuje model teorie T'.

Slovo kompaktnost pochází z kompaktních (tj. omezených a uzavřených) mnozin v Euklidovských prostorech, ve kterých lze z každé posloupnosti vybrat konvergentní podposloupnost. Můžete si představit posloupnost zvětšujících se konečných částí 'konvergující' k nekonečnému celku.

V predikátovej

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

11. Veta o korektnosti rezolúcie vo výrokovej logike

Je-li formule S rezolucí zamítnutelná, potom je S nesplnitelná.

Důkaz. Necht' $S \vdash_R \square$ a vezměme nějaký rezoluční důkaz $C_0, C_1, \ldots, C_n = \square$. Předpokládejme pro spor, že S je splnitelná, tedy $\mathcal{V} \models S$ pro nějaké ohodnocení $\mathcal{V}$. Indukcí podle i dokážeme, že $\mathcal{V} \models C_i$. Pro $i = 0$ to platí, nebot $C_0 \in S$. 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.

12. Veta o korektnosti rezolúcie v predikátovej logike

Pokud je CNF formule S rezolucí zamítnutelná, potom je nesplnitelná.

Důkaz. Víme, že $S \vdash_R \square$, vezměme tedy nějaký rezoluční důkaz $\square$ z S. Kdyby existoval model $\mathcal{A} \models S$, díky korektnosti rezolučního pravidla bychom mohli dokázat indukcí podle délky důkazu, že i $\mathcal{A} \models \square$, což ale není možné.

13. Súvislosť stromu dosiahnutia a splniteľnosti CNF formule

Je-li S formule a ℓ literál, potom dosazením ℓ do S myslíme formuli:

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

Zde shrneme několik jednoduchých faktů o dosazení:

- S^ℓ je výsledkem jednotkové propagace aplikované na $S \cup \{\{\ell\}\}$.
- 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.

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

Důkaz. Mějme ohodnocení $\mathcal{V} \models S$, to nemůže obsahovat ℓ i $\bar{\ell}$ (musí být konzistentní); bez újmy na obecnosti předpokládejme, že $\bar{\ell} \notin \mathcal{V}$, a ukažme, že $\mathcal{V} \models S^\ell$. Vezměme libovolnou klauzuli v S^ℓ. Ta je tvaru $C\backslash\{\bar{\ell}\}$ 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 C, takže platí i $\mathcal{V} \equiv C\backslash\{\bar{\ell}\}$

Naopak, předpokládejme že existuje ohodnocení $\mathcal{V}$ splňující S^ℓ (opět bez újmy na obecnosti). Protože se $\bar{\ell}$ (ani ℓ) nevyskytuje vS^ℓ, platí také $\mathcal{V}\backslash\{\bar{\ell}\} \models S^\ell$. Ohodnocení $\mathcal{V}' = (\mathcal{V}\backslash\{\bar{\ell}\}) \cup \{\ell\}$ potom splňuje každou klauzuli $C \in S$: pokud $\ell \in C$, potom $\ell \in C \cap \mathcal{V}'$ a $C \cap \mathcal{V}' \neq \emptyset$, jinak $C \cap \mathcal{V}' = (C\backslash\{\bar{\ell}\}) \cap \mathcal{V}' \neq \emptyset$ nebot $\mathcal{V}\backslash\{\bar{\ell}\} \models C\backslash\{\bar{\ell}\} \in S^\ell$. Ověřili jsme, že $\mathcal{V}' \models S$, tedy S je splnitelná.

14. Unifikačný algoritmus (korektnosť)

Algoritmus (Unifikační algoritmus).

- vstup: konečná množina výrazů $S \neq \emptyset$,
- výstup: nejobecnější unifikace σ pro S nebo informace, že S není unifikovatelná (0) nastav $S_0 := S, \sigma_0 := \emptyset, k := 0$ (1) pokud $|S_k| = 1$, vrat' $\sigma = \sigma_0\sigma_1 \cdots \sigma_k$ (2) zjisti, zda v $D(S_k)$ existuje proměnná x a term t neobsahující x (3) pokud ano, nastav $\sigma_{k+1} := \{x/t\}, S_{k+1} := S_k\sigma_{k+1}, k := k + 1$, a jdi na (1) (4) pokud ne, odpověz, že S není unifikovatelná **Poznámka** 8.4.11. Hledání proměnné x a termu tv kroku (2) může být relativně výpočetně náročné.

Tvrzení 8.4.13. Unifikační algoritmus je korektní. Pro každý vstup S skončí v konečně mnoha krocích, a je-li S unifikovatelná, odpoví nejobecnější unifikaci σ, jinak odpoví, že S neni unifikovatelná. Je-li S unifikovatelná, potom pro sestrojenou nejobecnější unifikaci σ navíc platí, že je-li τ libovolná unifikace, potom $\tau = \sigma\tau$.

15. Neštandardný model prirodzených čísel

Nechť $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$ je standardní model přirozených čísel. Označme $Th(\underline{\mathbb{N}})$ množinu všech sentencí pravdivých ve struktuře $\underline{\mathbb{N}}$ (tzv. teorii struktury $\underline{\mathbb{N}}$). Pro $n \in \mathbb{N}$ definujme n-tý numerál jako term $\underline{n} = S(S(\cdots(S(0)\cdots))$, kde S je aplikováno n-krát.

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

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

Všimněte si, že každá konečná část teorie T má model. Z věty o kompaktnosti tedy plyne, že i teorie T má model. Říkáme mu nestandardní model (označme ho $\mathcal{A}$). Platí v něm tytéž sentence, které platí ve standardním modelu, ale zároveň obsahuje prvek $c^{\mathcal{A}}$, který je větší než každé $n \in \mathbb{N}$ (čímž zde myslíme hodnotu termu $\underline{n}$ v nestandardním modelu $\mathcal{A}$).

16. Kompletné jednoduché extenzie DeLO*

Teorie uspořádání je teorie v jazyce uspořádání $L = \langle \leq \rangle$ s rovností, jejíž axiomy jsou:

$$\begin{aligned} T = \{&x \leq x, \\ &x \leq y \wedge y \leq x \to x = y, \\ &x \leq y \wedge y \leq z \to x \leq z\} \end{aligned}$$

Těmto axiomům říkáme reflexivita, antisymetrie, tranzitivita. Modely T jsou L-struktury $\langle S, \leq^S \rangle$, ve kterých platí axiomy T, tzv. (částečně) uspořádané množiny. Např: $\mathcal{A} = \langle \mathbb{N}, \leq \rangle$, $\mathcal{B} = \langle \mathcal{P}(X), \subseteq \rangle$ pro $X = \{0, 1, 2\}$

- Formule $x \leq y \vee y \leq x$ (linearita) platí v $\mathcal{A}$, ale neplatí v $\mathcal{B}$, nebot neplatí např. při ohodnocení kde $e(x) = \{0\}, e(y) = \{1\}$ (píšeme $\mathcal{B} \not\models \varphi[e]$). Je tedy nezávislá v T.
- Sentence $(\exists x)(\forall y)(y \leq x)$ (označme ji ψ) je pravdivá v$\mathcal{B}$ a lživá v$\mathcal{A}$, píšeme $\mathcal{B} \models \psi$, $\mathcal{A} \models \neg\psi$. Je tedy také nezávislá v T.
- Formule $(x \leq y \wedge y \leq z \wedge z \leq x) \to (x = y \wedge y = z$) (označme ji χ) je pravdivá vT, píšeme $T \models \chi$. Totéž platí pro její generální uzávěr $(\forall x)(\forall y)(\forall z)\chi$.

Teorie hustého lineárniho uspořádání (DeLO*) je extenze teorie uspořádání o následující axiomy:

- axiom linearity (někdy se mu říká také dichotomie):

$$x \leq y \vee y \leq x$$

- axiom hustoty

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

Tvrzení 9.1.6. Mějme sentence $\varphi = (\exists x)(\forall y)(x \leq y)$ a $\psi = (\exists x)(\forall y)(y \leq x)$ vyjadřující existenci minimálního resp. maximálního prvku. Následující čtyři teorie jsou právě všechny kompletní jednoduché extenze teorie DeLO*:

- $\mathrm{DeLO} = \mathrm{DeLO}^* \cup \{\neg\varphi, \neg\psi\}$
- $\mathrm{DeLO}^+ = \mathrm{DeLO}^* \cup \{\neg\varphi, \psi\}$
- $\mathrm{DeLO}^- = \mathrm{DeLO}^* \cup \{\varphi, \neg\psi\}$
- $\mathrm{DeLO}^\pm = \mathrm{DeLO}^* \cup \{\varphi, \psi\}$ Stačí ukázat, že tyto čtyři teorie jsou kompletní. Potom už je zřejmé, že žádná další kompletní jednoduchá extenze DeLO* nemůže existovat. Kompletnost plyne z faktu, že jsou ω-kategorické, tj. mají jediný spočetný model až na izomorfismus.

17. Existencia spočetného algebraicky uzavreného telesa

Je-li L spočetný jazyk s rovností, potom ke každé nekonečné L-struktuře existuje elementárně ekvivalentní spočetně nekonečná struktura.

Důkaz. Mějme nekonečnou L-strukturu $\mathcal{A}$. Najdeme spočetně nekonečnou strukturu $\mathcal{B} \equiv \mathcal{A}$. Protože v$\mathcal{A}$ neplatí pro žádné $n \in \mathbb{N}$ sentence vyjadřující 'existuje nejvýše n prvků' (což lze pomocí rovnosti snadno zapsat), neplatí tato sentence ani v $\mathcal{B}, \mathcal{B}$ tedy nemůže být konečná struktura.

Těleso $\mathcal{A}$ je algebraicky uzavřené, pokud každý polynom nenulového stupně v něm má kořen. Těleso reálných čísel $\mathbb{R}$ není algebraicky uzavřené, neboť $x^2 + 1$ nemá v $\mathbb{R}$ kořen, stejně tak těleso $\mathbb{Q}($ v něm nemá kořen ani $x^2 - 2\big)$. Těleso komplexních čísel $\mathbb{C}$ algebraicky uzavřené je, je ale nespočetné.

Algebraickou uzavřenost lze vyjádřit pomocí následujících sentencí ψ_n, pro každé $n > 0$:

$$(\forall x_{n-1}) \ldots (\forall x_0)\,(\exists y)\left(y^n + x_{n-1} \cdot y^{n-1} + \cdots + x_1 \cdot y + x_0\right) = 0$$

kde y^k je zkratka za term $y \cdot y \cdot \cdots \cdot y$ (kde $\cdot$ je aplikováno $(k-1)$-krát). **Důsledek**: Existuje spočetné algebraicky uzavřené těleso. **Důkaz**. Existuje spočetně nekonečná struktura $\mathcal{A}$ elementárně ekvivalentní tělesu $\mathbb{C}$. Protože $\mathbb{C}$ je těleso a splňuje sentence ψ_n pro všechna $n > 0$, je i $\mathcal{A}$ algebraicky uzavřené těleso.

18. Telesá charakteristiky 0 nie sú konečne axiomatizovateľné

Mějme třídu struktur $K \subseteq \mathrm{M}_L$ a uvažme také její doplněk $\bar{K} = \mathrm{M}_L \backslash K$. Potom K je konečně axiomatizovatelná, právě když $Ki\bar{K}$ jsou axiomatizovatelné.

Stačí ukázat, že $\bar{K}$ (tělesa nenulové charakteristiky) není axiomatizovatelná, což dokážeme sporem. Necht' existuje teorie S taková, že $\mathrm{M}(S) = \bar{K}$. Potom teorie $S' = S \cup T'$ má model, nebot' každá její konečná část má model: stačí vzít těleso prvočíselné charakteristiky větší než jakékoliv p z axiomu T' tvaru $\neg p1 = 0$. Necht $\mathcal{A}$ je model S'. Potom je i $\mathcal{A} \in \mathrm{M}(S) = \bar{K}$. Zároveň je ale $\mathcal{A} \in \mathrm{M}\,(T') = K$, což je spor.

19. Kritérium otvorenej axiomatizovateľnosti

Pokud je teorie T otevřeně axiomatizovatelná, potom je každá podstruktura modelu T také modelem T. Nechť T' je otevřená axiomatizace T. Mějme model $\mathcal{A} \models T'$ a podstrukturu $\mathcal{B} \subseteq \mathcal{A}$. Pro každou formuli $\varphi \in T'$ platí $\mathcal{B} \models \varphi$ (nebot' φ je otevřená), tedy i $\mathcal{B} \models T'$.

Uved'me několik příkladů:

- Teorie DeLO není otevřeně axiomatizovatelná, například žádná konečná podstruktura modelu DeLO nemůže být hustá.
- Teorie těles není otevřeně axiomatizovatelná, podstruktura $\mathbb{Z} \subseteq \mathbb{Q}$ tělesa celých čísel není tělesem, v $\mathbb{Z}$ neexistuje inverzní prvek vůči násobení k číslu 2 .

- Pro dané $n \in \mathbb{N}$ jsou nejvýše n-prvkové grupy otevřeně axiomatizovatelné(podgrupy jsou jistě také nejvýše n-prvkové). Jako otevřenou axiomatizaci lze vzít následující extenzi (otevřené) teorie grup T :

$$T \cup \left\{ \bigvee_{1 \leq i < j \leq n+1} x_i = x_j \right\}$$

20. Rekurzívne axiomatizovaná teória je čiastočne rozhodnuteľná, kompletná je rozhodnuteľná

O teorii T říkáme, že je

- rozhodnutelná, pokud existuje algoritmus, který pro každou vstupní formuli φ doběhne a odpoví, zda $T \models \varphi$,
- částečně rozhodnutelná, pokud existuje algoritmus, který pro každou vstupní formuli:
- pokud $T \models \varphi$, doběhne a odpoví "ano",
- pokud $T \not\models \varphi$, bud' nedoběhne, nebo doběhne a odpoví "ne".

Teorie T je rekurzivně axiomatizovaná, pokud existuje algoritmus, který pro každou vstupní formuli φ doběhne a odpoví, zda $\varphi \in T$.

Nechť T je rekurzivně axiomatizovaná. Potom:

1. T je částečně rozhodnutelná,
2. je-li T navíc kompletní, potom je rozhodnutelná. **Důkaz**. Algoritmem ukazujícím částečnou rozhodnutelnost je konstrukce systematického tabla pro F φ.[4] Pokud φ v T platí, konstrukce skončí v konečně mnoha krocích a snadno ověříme, že je tablo sporné, jinak ale skončit nemusí.

Je-li T kompletní, víme, že $T \vdash \varphi$ právě když $T \nvdash \varphi$. Budeme tedy paralelně konstruovat tablo pro Fφ a tablo pro Tφ (důkaz a zamítnutí φ z T): jedna z konstrukcí po konečně mnoha krocích skončí.

21. Teória konečnej štruktúry v konečnom jazyku s rovnosťou je rozhodnuteľná

Mějme L-strukturu $\mathcal{A}$. Teorie struktury $\mathcal{A}$, značíme $Th(\mathcal{A})$ je množina všech L-sentencí platných v $\mathcal{A}$:

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

Je-li $\mathcal{A}$ konečná struktura v konečném jazyce s rovností, potom je teorie $\mathrm{Th}(\mathcal{A})$ rekurzivně axiomatizovatelná.

Důkaz. Očíslujme prvky domény jako $A = \{a_1, \ldots, a_n\}$. Teorii $\mathrm{Th}(\mathcal{A})$ lze axiomatizovat jedinou sentencí, která je tvaru "existuje právě n prvků $a_1, \ldots, a_n$ splňujících právě ty základní vztahy o funkčních hodnotách a relacích, které platí ve struktuře $\mathcal{A}$ ".

22. Godelové vety o neúplnosti a ich dôsledky (bez dôkazu)

(První věta o neúplnosti). Pro každou bezespornou rekurzivně axiomatizovanou extenzi T Robinsonovy aritmetiky existuje sentence, která je pravdivá v $\mathbb{N}$, ale není dokazatelná v T.

(Druhá věta o neúplnosti). Pro každou bezespornou rekurzivně axiomatizovanou extenzi T Peanovy aritmetiky platí, že C_T není dokazatelná v T.

Ťažké otázky

1. Veta o korektnosti tablo metódy vo výrokovej logike

Je-li výrok φ tablo dokazatelný z teorie T, potom je φ pravdivý v T, t j . $T \vdash \varphi \Rightarrow T \models \varphi$.

Důkaz. Dokážeme sporem. Předpokládejme, že φ v T neplatí, tj. existuje protipříklad: model $v \in \mathrm{M}(T)$, ve kterém φ neplatí. Protože je φ dokazatelná z T, existuje tablo důkaz φ z T, což je sporné tablo z T s položkou Fφ v kořeni. Model v se shoduje s položkou Fφ

1. Shoduje-li se model teorie T s položkou v kořeni tabla z teorie T, potom se shoduje s některou větví. **Důkaz**. Mějme tablo $\tau = \bigcup_{i\geq 0} \tau_i$ z teorie T a model $v \in \mathrm{M}(T)$ shodující se s kořenem τ, tedy s (jednoprvkovou) větví V_0 v (jednoprvkovém) τ_0. Indukcí podle i (podle kroků v při konstrukci tabla) najdeme posloupnost $V_0 \subseteq V_1 \subseteq \ldots$ takovou, že V_i je větev v tablu τ_i shodující se s modelem v, a V_{i+1} je prodloužením V_i. Požadovaná větev tabla τ je potom $V = \bigcup_{i\geq 0} V_i$.

   - Pokud τ_{i+1} vzniklo z τ_i bez prodloužení větve V_i, definujeme $V_{i+1} = V_i$.
   - Pokud τ_{i+1} vzniklo z τ_i připojením položky T α (pro nějaký axiom $\alpha \in T$) na konec větve V_i, definujeme V_{i+1} jako tuto prodlouženou větev. Protože v je model T, platí v něm axiom α, tedy shoduje se i s novou položkou T α.
   - Necht' τ_{i+1} vzniklo z τ_i připojením atomického tabla pro nějakou položku P na konec větve V_i. Protože se model v shoduje s položkou P (která leží na větvi V_i), shoduje se i s kořenem připojeného atomického tabla, a proto se shoduje i s některou z jeho větví. (Tuto vlastnost snadno ověříme pro všechna atomická tabla.) Definujeme V_{i+1} jako prodloužení V_i o tuto větev atomického tabla.

Všechny větve jsou ale sporné, včetně V. Takže V obsahuje položky T ψ a F ψ (pro nějaký výrok ψ), a model v se s těmito položkami shoduje. Máme tedy $v \models \psi$ a zároveň $v \not\models \psi$, což je spor.

2. Veta o korektnosti tablo metódy v predikátovej logike

Je-li sentence φ tablo dokazatelná z teorie T, potom je φ pravdivá $vT, tj. T \vdash \varphi \Rightarrow T \models \varphi$.

Důkaz. Předpokládejme pro spor, že $T \not\models \varphi$, tj. existuje $\mathcal{A} \in \mathrm{M}(T)$ takový, že $\mathcal{A} \not\models \varphi$. Protože $T \vdash \varphi$, existuje sporné tablo z T s F φ v kořeni. Model $\mathcal{A}$ se shoduje s Fφ, lze tedy expandovat do jazyka L_C tak, že se expanze shoduje s nějakou větví V.

1. **Důkaz**. Mějme tablo $\tau = \bigcup_{i>0} \tau_i$ z teorie T a model $\mathcal{A} \in \mathrm{M}_L(T)$ shodující se s kořenem τ, tedy s (jednoprvkovou) větví V_0v (jednoprvkovém) τ_0. Indukcí podle i najdeme posloupnost větví V_i a expanzí $\mathcal{A}_i$ modelu $\mathcal{A}$ o konstanty $c^{\mathcal{A}} \in C$ vyskytující se na V_i takových, že V_i je větev v tablu τ_i shodující se s modelem $\mathcal{A}_i, V_{i+1}$ je prodloužením V_i, a $\mathcal{A}_{i+1}$ je expanzí $\mathcal{A}_i$ (mohou si být i rovny). Požadovaná větev tabla τ je potom $V = \bigcup_{i\geq 0} V_i$. Expanzi modelu $\mathcal{A}$ do jazyka L_C získáme jako 'limitu' expanzí $\mathcal{A}_i$, tj. vyskytuje-li se symbol $c \in C$ na V, vyskytuje se na nějaké z větví V_i a interpretujeme ho stejně jako v$\mathcal{A}_i$ (ostatní pomocné symboly interpretujeme libovolně).

   - Pokud τ_{i+1} vzniklo z τ_i bez prodloužení větve V_i, definujeme $V_{i+1} = V_i$ a $\mathcal{A}_{i+1} = \mathcal{A}_i$.
   - Pokud τ_{i+1} vzniklo z τ_i připojením položky T α (pro nějaký axiom $\alpha \in T$) na konec větve V_i, definujeme V_{i+1} jako tuto prodlouženou větev a $\mathcal{A}_{i+1} = \mathcal{A}_i$ (nepřidali jsme žádný nový pomocný konstantní symbol). Protože $\mathcal{A}_{i+1}$ je modelem T, platí v něm axiom α, tedy shoduje se i s novou položkou Tα.
   - Necht τ_{i+1} vzniklo z τ_i připojením atomického tabla pro nějakou položku P na konec větve V_i. Protože se model $\mathcal{A}_i$ shoduje s položkou P (která leží na větvi V_i), shoduje se i s kořenem připojeného atomického tabla.
   - Pokud jsme připojili atomické tablo pro logickou spojku, položíme $\mathcal{A}_{i+1} = \mathcal{A}_i$ (nepřidali jsme nový pomocný symbol). Protože $\mathcal{A}_{i+1}$ se shoduje s kořenem atomického tabla, shoduje se i s některou z jeho větví (stejně jako ve výrokové logice); definujeme V_{i+1} jako prodloužení V_i o tuto větev.
   - Je-li položka P typu 'svědek': Pokud je $P = \mathrm{T}(\exists x)\varphi(x)$, potom $\mathcal{A}_i \models (\exists x)\varphi(x)$, tedy existuje $a \in A$ takové, že $\mathcal{A}_i \models \varphi(x)[e(x/a)]$. Větev V_{i+1} definujeme jako prodloužení V_i o nově přidanou položku T$\varphi(x/c)$ a model $\mathcal{A}_{i+1}$ jako expanzi $\mathcal{A}_i$o konstantu $c^{\mathcal{A}} = a$. Případ $P = \mathrm{F}(\forall x)\varphi(x)$ je obdobný.
   - Je-li položka P typu 'všichni', větev V_{i+1} definujeme jako prodloužení V_i o atomické tablo. Nově přidaná položka je T$\varphi(x/t)$ nebo F$\varphi(x/t)$ pro nějaký L_C-term t. Předpokládejme, že jde o první z těchto dvou možností, pro druhou je důkaz analogický. Model $\mathcal{A}_{i+1}$ definujeme jako libovolnou expanzi $\mathcal{A}_i$ o nové konstanty vyskytující se v t. Protože $\mathcal{A}_i \models (\forall x)\varphi(x)$, platí i $\mathcal{A}_{i+1} \models (\forall x)\varphi(x)$ a tedy i $\mathcal{A}_{i+1} \models \varphi(x/t)$; model $\mathcal{A}_{i+1}$ se tedy shoduje s větví V_i.

Všechny větve jsou ale sporné.

3. Veta o úplnosti tablo metódy vo výrokovej logike

Je-li výrok φ pravdivý v teorii T, potom je tablo dokazatelný z T, $tj. T \models \varphi \Rightarrow T \vdash \varphi$.

Důkaz. Ukážeme, že libovolné dokončené (tedy např. i systematické) tablo z T s položkou Fφv kořeni je nutně sporné. **Důkaz** provedeme sporem: kdyby takové tablo nebylo sporné, existovala by v něm bezesporná (dokončená) větev V. Uvažme kanonický model v pro tuto větev. Protože je V dokončená, obsahuje T α pro všechny axiomy $\alpha \in T$. Model v se shoduje se všemi položkami na V, splňuje tedy všechny axiomy a máme $v \models T$.

1. **Důkaz**. Ukážeme, že kanonický model v se shoduje se všemi položkami P na větvi V, a to indukcí podle struktury výroku v položce. Nejprve základ indukce:

   - Je-li $P = \mathrm{T}p$ pro nějaký prvovýrok $p \in \mathbb{P}$, máme podle definice $v(p) = 1; v$ se s P shoduje.
   - Je-li $P = \mathrm{F}p$, potom se na větvi V nemůže vyskytovat položka Tp, jinak by V byla sporná. Podle definice máme $v(p) = 0$ a v se s P opět shoduje. Nyní indukční krok. Rozebereme dva případy, ostatní se dokáží obdobně.
   - Necht $P = \mathrm{T}\varphi \wedge \psi$. Protože je V dokončená větev, je na ní položka P redukovaná. To znamená, že se na V vyskytují i položky T φ a T ψ. Podle indukčního předpokladu se s nimi model v shoduje, tedy $v \models \varphi$ a $v \models \psi$. Takže platí i $v \models \varphi \wedge \psi$ a v se shoduje s.
   - Necht $P = \mathrm{F}\varphi \wedge \psi$. Protože je P na V redukovaná, vyskytuje se na V položka Fφ nebo položka Fψ. Platí tedy $v \not\models \varphi$ nebo $v \not\models \psi$, z čehož plyne $v \not\models \varphi \wedge \psi$ a v se shoduje s P.

Protože se ale v shoduje i s položkou Fφ v kořeni, máme $v \not\models \psi$, což znamenám, že $T \not\models \psi$, spor. Tablo tedy muselo být sporné, tj. být tablo důkazem φ z T.

4. Veta o úplnosti tablo metódy v predikátovej logike

Je-li sentence φ pravdivá v teorii T, potom je tablo dokazatelná $z\ T, tj. T \models \varphi \Rightarrow T \vdash \varphi$.

Důkaz provedeme sporem: kdyby takové tablo nebylo sporné, existovala by v něm bezesporná (dokončená) větev V. Uvažme kanonický model $\mathcal{A}$ pro tuto větev, a označme jako $\mathcal{A}'$ jeho redukt na jazyk L. Protože je V dokončená, obsahuje T α pro všechny axiomy $\alpha \in T$. Model $\mathcal{A}$ se shoduje se všemi položkami na V, splňuje tedy všechny axiomy a máme i $\mathcal{A}' \models T$.

1. **Důkaz**. Nejprve uvažme jazyky bez rovnosti. Ukážeme indukcí podle struktury sentencí v položkách, že kanonický model $\mathcal{A}$ se shoduje se všemi položkami P na větvi V. Základ indukce, tj. případ, kdy $\varphi = R(s_1, \ldots, s_n)$ je atomická sentence, je jednoduchý: Je-li na V položka T φ, potom $(s_1, \ldots, s_n) \in R^{\mathcal{A}}$ plyne přímo z definice kanonického modelu, máme tedy $\mathcal{A} \models \varphi$. Je-li na V položka Fφ, potom na V není položka Tφ(V je bezesporná), $(s_1, \ldots, s_n) \notin R^{\mathcal{A}}$, a $\mathcal{A} \not\models \varphi$ Nyní indukční krok. Rozebereme jen několik případů, ostatní se dokáží obdobně. Pro logické spojky je důkaz zcela stejný jako ve výrokové logice, například je-li $P = \mathrm{F}\varphi \wedge \psi$, potom protože je P na V redukovaná, vyskytuje se na V položka Fφ nebo položka F ψ. Platí tedy $\mathcal{A}\forall\varphi$ nebo $\mathcal{A}\forall\psi$, z čehož plyne $\mathcal{A}\forall\varphi \wedge \psi$ a $\mathcal{A}$ se shoduje s P.

   - Máme-li položku typu "všichni", například $P = \mathrm{T}(\forall x)\varphi(x)$ (případ $P = \mathrm{F}(\exists x)\varphi(x)$ je obdobný), potom jsou na V i položky $T\varphi(x/t)$ pro každý konstantní L_C-term, tj. pro každý prvek " t " $\in A$. Dle indukčního předpokladu je $\mathcal{A} \models \varphi(x/t)$ pro každé "t" $\in A$, tedy $\mathcal{A} \models (\forall x)\varphi(x)$
   - Máme-li položku typu "svědek", například $P = \mathrm{T}(\exists x)\varphi(x)$ (případ $P = \mathrm{F}(\forall x)\varphi(x)$ je obdobný), potom je na V i položka $T\varphi(x/c)$ pro nějaké " c " $\in A$. Dle indukčního předpokladu je $\mathcal{A} \models \varphi(x/c)$, tedy i $\mathcal{A} \models (\exists x)\varphi(x)$.

   Je-li jazyk s rovností, máme kanonický model $\mathcal{A} = \mathcal{B}/ = B$, důkaz výše platí pro $\mathcal{B}$

Protože se ale $\mathcal{A}$ shoduje i s položkou Fφ v kořeni, platí i $\mathcal{A}' \not\models \varphi$, což znamená, že $\mathcal{A}' \in \mathrm{M}_L(T) \backslash \mathrm{M}_L(\varphi)$, tedy $T \not\models \varphi$, a to je spor. Tablo tedy muselo být sporné, tj. být tablo důkazem φ z T.

5. Veta o konečnosti sporu, dôsledky o konečnosti a systematičnosti dôkazov

Je-li $\tau = \bigcup_{i \geq 0} \tau_i$ sporné tablo, potom existuje $n \in \mathbb{N}$ takové, že τ_n je sporné konečné tablo. **Důkaz**. Uvažme množinu S všech vrcholů stromu τ, které nad sebou (ve stromovém uspořádání) neobsahují spor, tj. dvojici položek Tψ, Fψ.

Kdyby množina S byla nekonečná, podle Königova lemmatu (Nekonečný, konečně větvíci strom má nekonečnou větev.) použitého na podstrom τ na množině S bychom měli nekonečnou, bezespornou větev v S. To by ale znamenalo, že máme i bezespornou větev v τ, což je ve sporu s tím, že τ je sporné. (Podrobněji: Větev na S by byla podvětví nějaké větve V v τ, která je sporná, tj. obsahuje nějakou (konkrétní) spornou dvojici položek, která ale existuje už v nějakém konečném prefixu V.)

Množina S je tedy konečná. To znamená, že existuje $d \in \mathbb{N}$ takové, že celá S leží v hloubce nejvýše d. Každý vrchol na úrovni $d+1$ má tedy nad sebou spor. Zvolme n tak, že τ_n už obsahuje všechny vrcholy τ z prvních $d+1$ úrovní: každá větev τ_n je tedy sporná.

Důsledek Pokud při konstrukci tabla nikdy neprodlužujeme sporné větve, napr. pro systematické tablo, potom sporné tablo je konečné. **Důsledek** Pokud $T \vdash \varphi$, potom existuje i konečný tablo důkaz φ z T

Důsledek Systematičnost důkazů). Pokud $T \vdash \varphi$, potom systematické tablo je (konečným) tablo důkazem φ z T. K důkazu budeme potřebovat dvě fakta: pokud je φ dokazatelná z T, potom v T platí (Věta o korektnosti), tj. nemůže existovat protipříklad. A dále pokud by systematické tablo mělo bezespornou větev, znamenalo by to, že existuje protipříklad (to je klíčem k Větě o úplnosti).

Důkaz Z důkazu o uplnosti také dostáváme 'systematičnost důkazů', tj. že důkaz můžeme vždy hledat konstrukcí systematického tabla: Pokud $T \models \varphi$, tak je i systematické tablo pro položku Fφ nutně sporné, a je tedy tablo důkazem φzT.

6. Veta o úplnosti rezolúcie vo výrokovej logike

Je-li S nesplnitelná, je rezolucí zamítnutelná (tj. $S \vdash_R \square$). **Důkaz**. Je-li S nekonečná, má konečnou nesplnitelnou část S'. Rezoluční zamítnutí S' je také rezolučním zamítnutím S.

1. Teorie má model, právě když každá její konečná část má model. **Důkaz**. Každý model teorie T je zjevně modelem každé její části. Druhou implikaci dokážeme nepřímým důkazem: Předpokládejme, že T nemá model, tj. je sporná, a najděme konečnou část $T' \subseteq T$, která je také sporná. Protože je T sporná, platí $T \vdash \bot$. Pokud $T \vdash \varphi$, potom existuje i konečný tablo důkaz φ z T. Konstrukce tohoto důkazu má jen konečně mnoho kroků, použili jsme tedy jen konečně mnoho axiomů z T. Definujeme-li $T' = \{\alpha \in T \mid \mathrm{T}\ \alpha$ je položka v tablu $\tau\}$, potom τ je také tablo důkaz sporu z teorie T'. Teorie T' je tedy sporná konečná část T. **Důkaz** provedeme indukcí podle počtu proměnných v S. Je-li $|\operatorname{Var}(S)| = 0$, jediná možná nesplnitelná formule bez proměnných je $S = \{\square\}$ a máme jednokrokový důkaz $S \vdash_R \square$. Jinak vyberme $p \in \operatorname{Var}(S)$. S je splnitelná, právě když je splnitelná S^ℓ nebo $S^{\bar\ell}$. Mějme ohodnocení $\mathcal{V} \models S$, to nemůže obsahovat ℓ i $\bar\ell$ (musí být konzistentní); bez újmy na obecnosti předpokládejme, že $\bar\ell \notin \mathcal{V}$, a ukažme, že $\mathcal{V} \models S^\ell$. Vezměme libovolnou klauzuli v S^ℓ. Ta je tvaru $C\backslash\{\bar\ell\}$ 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 C, takže platí i $\mathcal{V} \models C\backslash\{\bar\ell\}$ Předpokládejme tedy, že S je konečná. Naopak, předpokládejme že existuje ohodnocení $\mathcal{V}$ splňující S^ℓ (opět bez újmy na obecnosti). Protože se $\bar\ell$ (ani ℓ) nevyskytuje vS^ℓ, platí také $\mathcal{V}\backslash\{\bar\ell\} \models S^\ell$. Ohodnocení $\mathcal{V}' = (\mathcal{V}\backslash\{\bar\ell\}) \cup \{\ell\}$ potom splňuje každou klauzuli $C \in S$: pokud $\ell \in C$, potom $\ell \in C \cap \mathcal{V}'$ a $C \cap \mathcal{V}' \neq \emptyset$, jinak $C \cap \mathcal{V}' = (C\backslash\{\bar\ell\}) \cap \mathcal{V}' \neq \emptyset$ nebot $\mathcal{V}\backslash\{\bar\ell\} \models C\backslash\{\bar\ell\} \in S^\ell$. Ověřili jsme, že $\mathcal{V}' \models S$, tedy S je splnitelná.

Tedy S^p i $S^{\bar p}$ nesplnitelné. Mají o jednu proměnnou méně, tedy podle indukčního předpokladu existují rezoluční stromy T pro $S^p \vdash_R \square$ a T' pro $S^{\bar p} \vdash_R \square$.

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

Zbývá ukázat konstrukci stromu $\widehat{T}$: množina vrcholů i uspořádání jsou stejné, změníme jen některé klauzule ve vrcholech, a to přidáním literálu $\neg p$. Na každém listu stromu T je nějaká klauzule $C \in S^p$, a bud' je $C \in S$, nebo není, 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 $\neg p$. V listech jsou nyní jen klauzule z S, v kořeni jsme $\square$ změnili na $\neg p$. A každý vnitřní vrchol je nadále rezolventou svých synů.

7. Veta o úplnosti LI-rezolúcie pre výrokové Hornove formule

Je-li Hornova formule T splnitelná, a $T \cup \{G\}$ je nesplnitelná pro cíl G, potom $T \cup \{G\} \vdash_{LI} \square$, a to LI-zamítnutím, které začíná cílem G.

Důkaz (konstrukci LI-zamítnutí) provedeme indukcí podle počtu proměnných v T.

Víme, že je-li Hornova formule S nesplnitelná a $\square \notin S$, potom obsahuje fakt i cíl. **Důkaz**. Neobsahuje-li fakt, můžeme ohodnotit všechny proměnné 0 ; neobsahuje-li cíl, ohodnotíme 1. Potom T obsahuje fakt $\{p\}$ pro

nějakou výrokovou proměnnou p. Protože $T \cup \{G\}$ je nesplnitelná, je nesplnitelná také $(T \cup \{G\})^p = T^p \cup \{G^p\}$, kde $G^p = G \backslash \{\neg p\}$

Pokud $G^p = \square$, potom $G = \{\neg p\}, \square$ je rezolventa G a $\{p\} \in T$, a máme jednokrokové LI-zamítnutí T (to je báze indukce).

Jinak je formule T^p splnitelná (stejným ohodnocením jako T, nebot to musí obsahovat p kvůli faktu $\{p\}$, tedy neobsahuje $\neg p$) a má méně proměnných než T. Tedy podle indukčního předpokladu existuje LI-odvození $\square z T^p \cup \{G^p\}$ začínající $G^p = G \backslash \{\neg p\}$.

Hledané LI-zamítnutí $T \cup \{G\}$ začínající G zkonstruujeme (podobně jako v důkazu Věty o úplnosti rezoluce) přidáním literálu $\neg p$ do všech listů, které už nejsou v $T \cup \{G\}$ (tedy 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 $\square$.

8. Veta o úplnosti rezolúcie v predikátovej logike (Lifting lemma)

Je-li CNF formule S nesplnitelná, potom je zamítnutelná rezolucí.

(Základní instance). Mějme otevřenou formuli φ ve volných proměnných $x_1, \ldots, x_n$. Řekneme, že instance $\varphi\left(x_1/t_1, \ldots, x_n/t_n\right)$ je základní (ground) instance, jsou-li všechny termy $t_1, \ldots, t_n$ konstantní (ground).

(Lifting lemma). Mějme klauzule C_1 a C_2 s disjunktní množinou proměnných. Jsou-li C_1^* a C_2^* základní instance klauzulí C_1 a C_2 a je-li C^* je rezolventou C_1^* a C_2^*, potom existuje rezolventa C klauzulí C_1 a C_2 taková, že C^* je základní instancí C. Z lifting lemma pak: Mějme CNF formuli S a označme jako S^* množinu všech jejích základních instancí. Pokud $S^* \vdash_R C^*$ ('na úrovni výrokové logiky') pro nějakou základni klauzuli C^*, potom existuje klauzule C a základní substituce σ taková, že $C^* = C\sigma$ a $S \vdash_R C$ ('na úrovni predikátové logiky').

Důkaz. Označme jako S^* množinu všech základních instancí klauzulí z S. Protože je S nesplnitelná, je díky Herbrandově větě nesplnitelná i S^*. Z věty o úplnosti výrokové rezoluce víme, že $S^* \vdash_R \square$ ('na úrovni výrokové logiky'). Z Lifting lemmatu postáváme klauzuli C a základní substituci σ takové, že $C\sigma = \square$ a $S \vdash_R C$ ('na úrovni predikátové logiky'). Ale protože prázdná klauzule $\square$ je instancí C, musí být $C = \square$. Tím jsme našli rezoluční zamítnutí $S \vdash_R \square$.

9. Skolemova veta

Každá teorie má otevřenou konzervativní extenzi.

(Skolemova varianta). Mějme L-sentenci φ v PNF, a necht všechny její vázané proměnné jsou různé. Necht existenční kvantifikátory z prefixu φ jsou $\left(\exists y_1\right), \ldots, \left(\exists y_n\right)$ (v tomto pořadí), a necht pro každé i jsou $\left(\forall x_1\right), \ldots, \left(\forall x_{n_i}\right)$ právě všechny univerzální kvantifikátory předcházející kvantifikátor $\left(\exists y_i\right)$ v prefixu φ.

Lemma: Mějme L-sentenci $\varphi = \left(\forall x_1\right) \ldots \left(\forall x_n\right) \left(\exists y\right) \psi$ a necht' φ' je sentence

$$\left(\forall x_1\right) \ldots \left(\forall x_n\right) \psi \left(y / f\left(x_1, \ldots, x_n\right)\right)$$

kde f je nový funkční symbol. Potom: (i) L-redukt každého modelu φ' je modelem φ, a (ii) každý model φ lze expandovat na model φ'. **Důkaz**. Nejprve dokažme část (i): Mějme model $\mathcal{A}' \models \varphi'$ a necht $\mathcal{A}$ je jeho redukt na jazyk L. Pro každé ohodnocení proměnných e platí $\mathcal{A} \models \psi[e(y/a)]$ pro $a = \left(f\left(x_1, \ldots, x_n\right)\right)^{\mathcal{A}'}[e]$, tedy $\mathcal{A} \models \varphi$

Nyní část (ii): Protože $\mathcal{A} \models \varphi$, existuje funkce $f^A : A^n \to A$ taková, že pro každé ohodnocení proměnných e platí $\mathcal{A} \models \psi[e(y/a)]$, kde $a = f^A\left(e\left(x_1\right), \ldots, e\left(x_n\right)\right)$. To znamená, že expanze struktury $\mathcal{A}$ vzniklá přidáním funkce f^A je modelem φ'.

Důkaz. Mějme L-teorii T. Každý axiom nahradíme jeho generálním uzávěrem (není-li to už sentence) a převedeme do PNF, tím získáme ekvivalentní teorii T'. Nyní nahradíme každý axiom teorie T' jeho Skolemovou variantou. Tím získáme teorii T'' v rozšířném jazyce L'. Z Lemmatu pak plyne, že L-redukt každého modelu T'' je modelem T', tedy T'' je extenzí T', a že každý model T' lze expandovat do jazyka L' na model T'', tedy jde o konzervativní extenzi. Teorie T'' je axiomatizovaná univerzálními sentencemi, odstraníme-li kvantifikátorové prefixy (tj. vezmeme-li jádra axiomů), získáme otevřenou teorii T''', která ekvivalentní s T'' a tedy je také konzervativní extenzí T.

10. Herbrandova veta

Mějme otevřenou teorii T v jazyce L bez rovnosti a s alespoň jedním konstantním symbolem. Potom bud' má T Herbrandův model, nebo existuje konečně mnoho základních instancí axiomů T, jejichž konjunkce je nesplnitelná.

(Herbrandův model). Mějme jazyk $L = \langle \mathcal{R}, \mathcal{F} \rangle$ s alespoň jedním konstantním symbolem. L-struktura $\mathcal{A} = \left\langle A, \mathcal{R}^{\mathcal{A}}, \mathcal{F}^{\mathcal{A}} \right\rangle$ je Herbrandův model, jestliže:

- A je množina všech konstantních L-termů (tzv. Herbrandovo univerzum), a
- pro každý n-ární funkční symbol $f \in \mathcal{F}$ a konstantní termy " t_1",..., " t_n" $\in A$ platí:

$$f^{\mathcal{A}}(\text{"}t_1\text{"},\ldots,\text{"}t_n\text{"}) = \text{"}f(t_1,\ldots,t_n)\text{"}$$

- Speciálně, pro každý konstantní symbol $c \in \mathcal{F}$ je $c^{\mathcal{A}} =$ "c".

Důkaz. Označme jako T_{ground} množinu všech základních instancí axomů teorie T. Zkonstruujeme systematické tablo z teorie T_{ground} s položkou F $\perp$ v kořeni, ale z jazyka L, bez rozšíření o pomocné konstantní symboly na jazyk $L_C \cdot$ Pokud tablo obsahuje bezespornou větev, potom je kanonický model pro tuto větev (opět bez přidání pomocných konstantních symbolů) Herbrandovým modelem T. V opačném případě máme tablo důkaz sporu, tedy teorie T_{ground} , a tím pádem i T, je nesplnitelná. Protože je tablo důkaz konečný, použili jsme v něm jen konečně mnoho základních instancí axiomů $\alpha_{\text{ground}} \in T_{\text{ground.}}$ Jejich konjunkce je tedy nesplnitelná.

11. Lowenheim-Skolemova veta vrátane variatnu s rovnosťou, jej dôsledky

Je-li L spočetný jazyk bez rovnosti, potom každá bezesporná L-teorie má spočetně nekonečný model.

Důkaz. Vezměme nějaké dokončené (např. systematické) tablo z teorie T s položkou F $\perp$ v kořeni. Protože T je bezesporná, není v ní dokazatelný spor, tedy tablo musí obsahovat bezespornou větev. Hledaný spočetně nekonečný model je L-redukt kanonického modelu pro tuto větev.

Tato věta má následující jednoduchý důsledek: **Důsledek** 1. Je-li L spočetný jazyk bez rovnosti, potom ke každé L-struktuře existuje elementárně ekvivalentní spočetně nekonečná struktura.

Důkaz. Mějme L-strukturu $\mathcal{A}$. Teorie Th($\mathcal{A}$) je bezesporná (má model $\mathcal{A}$), tedy dle LöwenheimSkolemovy má spočetně nekonečný model $\mathcal{B} \models Th(\mathcal{A})$. To ale znamená, že $\mathcal{B} \equiv \mathcal{A}$.

V jazyce bez rovnosti tedy nemůžeme vyjádřit například 'model má právě 42 prvků'. V důkazu Löwenheim-Skolemovy věty jsme sestrojený model získali jako kanonický model pro bezespornou větev tabla z T pro položku F $\perp$. Stejným způsobem se dokáže následující verze pro jazyky s rovností, stačí faktorizovat dle relace $=^{A}$:

Věta (Löwenheim-Skolemova s rovností). Je-li L spočetný jazyk s rovností, potom každá bezesporná L-teorie má spočetný model (tj. konečný, nebo spočetně nekonečný). I tato verze má snadný důsledek pro konkrétní struktury: **Důsledek** 2. Je-li L spočetný jazyk s rovností, potom ke každé nekonečné L-struktuře existuje elementárně ekvivalentní spočetně nekonečná struktura.

Důkaz. Mějme nekonečnou L-strukturu $\mathcal{A}$. Stejně jako v důkazu Důsledku 1. najdeme spočetně nekonečnou strukturu $\mathcal{B} \equiv \mathcal{A}$. Protože v $\mathcal{A}$ neplatí pro žádné $n \in \mathbb{N}$ sentence vyjadřující 'existuje nejvýše n prvků' (což lze pomocí rovnosti snadno zapsat), neplatí tato sentence ani v $\mathcal{B}, \mathcal{B}$ tedy nemůže být konečná struktura.

12. Vzťah izomorfizmu a elementárnej ekvivalencie

Mějme struktury $\mathcal{A}, \mathcal{B}$ jazyka $L = \langle \mathcal{R}, \mathcal{F} \rangle$. Izomorfismus $\mathcal{A}$ a $\mathcal{B}$ (nebo ' $\mathcal{A}$ na $\mathcal{B}'$) je bijekce $h : A \to B$ splňující následující vlastnosti:

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

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

(Speciálně, je-li $c \in \mathcal{F}$ konstantní symbol, platí $h\left(c^{\mathcal{A}}\right) = c^{\mathcal{B}}$.)

- Pro každý (n-ární) relační symbol $R \in \mathcal{R}$ a pro všechna $a_i \in A$ platí:

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

Pokud existuje, říkáme, že $\mathcal{A}$ a $\mathcal{B}$ jsou izomorfní (nebo ' $\mathcal{A}$ je izomorfni s $\mathcal{B}$ via h ') a píšeme $\mathcal{A} \simeq \mathcal{B}$ (nebo $\mathcal{A} \simeq_h \mathcal{B}$). Automorfismus $\mathcal{A}$ je izomorfismus $\mathcal{A}$ na $\mathcal{A}$

Struktury $\mathcal{A}, \mathcal{B}$ (v témž jazyce) jsou elementárně ekvivalentní, pokud v nich platí tytéž sentence. Značíme $\mathcal{A} \equiv \mathcal{B}$.

Mějme struktury $\mathcal{A}, \mathcal{B}$ jazyka $L = \langle \mathcal{R}, \mathcal{F} \rangle$. Bijekce $h : A \to B$ je izomorfismus $\mathcal{A}$ a $\mathcal{B}$, právě když platí následující: (i) pro každý L-term t a ohodnocení proměnných e : Var $\to A$:

$$h\left(t^{\mathcal{A}}[e]\right) = t^{\mathcal{B}}[e \circ h]$$

(ii) pro každou L-formuli φ a ohodnocení proměnných e : Var $\to A$:

$$\mathcal{A} \models \varphi[e] \quad \textit{pravěkdyž} \quad \mathcal{B} \models \varphi[e \circ h]$$

Důkaz. Je-li h izomorfismus, vlastnosti snadno dokážeme indukcí podle struktury termu resp. formule. Naopak, je-li h bijekce splňující (i) a (ii), dosazením $t = f(x_1, \ldots, x_n)$ resp. $\varphi = R(x_1, \ldots, x_n)$ dostáváme vlastnosti z definice izomorfismu.

Jako okamžitý důsledek dostáváme fakt, že izomorfní struktury jsou elementárně ekvivalentní: **Důsledek**Pokud $\mathcal{A} \simeq \mathcal{B}$, potom $\mathcal{A} \equiv \mathcal{B}$

13. ω-kategorické kritérium kompletnosti

Mějme ω-kategorickou teorii T ve spočetnem jazyce L. Je-li

- L bez rovnosti, nebo
- L s rovností a T nemá konečné modely, potom je T kompletní. **Důkaz**. Pro jazyk bez rovnosti víme z důsledku Löwenheim-Skolemovy věty, že každý model je elementárně ekvivalentní nějakému spočetně nekonečnému modelu. Ten je ale až na izomorfizmus jediný, takže všechny modely jsou elementárně ekvivalentní, což je sémantická definice kompletnosti.

Máme-li jazyk s rovností, použijeme podobně důsledek LS věty pro rovnost a dostaneme, že všechny nekonečné modely jsou elementárně ekvivalentní.

14. Neaxiomatizovateľnosť konečných modelov

Pokud má teorie libovolně velké konečné modely, potom má i nekonečný model. V tom případě není třída všech jejích konečných modelů axiomatizovatelná.

Důkaz. Je-li jazyk bez rovnosti, stačí vzít kanonický model pro některou bezespornou větev v tablu z T pro položku F $\perp$ (T je bezesporná, nebot má model(y), tedy tablo není sporné). Mějme jazyk s rovností a označme jako T' následující extenzi teorie T' do jazyka rozšířeného o spočetně mnoho nových konstantních symbolů c_i :

$$T' = T \cup \{\neg c_i = c_j \mid i \neq j \in \mathbb{N}\}$$

Každá konečná část teorie T' má model: necht k je největší takové, že symbol c_k se vyskytuje v T'. Potom stačí vzít libovolný alespoň $(k+1)$-prvkový model T a interpretovat konstanty $c_0, \ldots, c_k$ jako navzájem různé prvky tohoto modelu.

Dle věty o kompaktnosti má potom i T' model. Ten je nutně nekonečný. Jeho redukt na původní jazyk (zapomenutí konstant $c_i^{\mathcal{A}}$) je nekonečným modelem T.

15. Veta o konečnej axiomatizovateľnosti

Mějme třídu struktur $K \subseteq \mathrm{M}_L$ a uvažme také jeji doplněk $\bar{K} = \mathrm{M}_L \backslash K$. Potom K je konečně axiomatizovatelná, právě když $Ki\bar{K}$ jsou axiomatizovatelné.

Důkaz. Je-li K konečně axiomatizovatelná, potom je axiomatizovatelná i konečně mnoha sentencemi $\varphi_1, \ldots, \varphi_n$ (nahradíme formule jejich generálními uzávěry). Jako axiomatizaci $\bar{K}$ stačí vzít sentenci $\psi = \neg(\varphi_1 \wedge \varphi_2 \wedge \cdots \wedge \varphi_n)$. Zřejmě platí $\mathrm{M}(\psi) = \bar{K}$.

Naopak, necht T a S jsou teorie takové, že $\mathrm{M}(T) = K$ a $\mathrm{M}(S) = \bar{K}$. Uvažme teorii $T \cup S$. Tato teorie je sporná, nebot:

$$\mathrm{M}(T \cup S) = \mathrm{M}(T) \cap \mathrm{M}(S) = K \cap \bar{K} = \emptyset$$

Podle věty o kompaktnosti existují konečné podteorie $T' \subseteq T$ a $S' \subseteq S$ takové, že:

$$\emptyset = \mathrm{M}(T' \cup S') = \mathrm{M}(T') \cap \mathrm{M}(S')$$

Nyní si všimněme, že platí

$$\mathrm{M}(T) \subseteq \mathrm{M}(T') \subseteq \overline{\mathrm{M}(S')} \subseteq \overline{\mathrm{M}(S)} = \mathrm{M}(T)$$

tím jsme dokázali, že $M(T) = M(T')$, tj. teorie T' je hledanou konečnou axiomatizací K.

16. Rekurzívne axiomatizovaná teória s rekurzívne spočetnou kompletáciou je rozhodnuteľná

Pokud je teorie T rekurzivně axiomatizovaná a má rekurzivně spočetnou kompletaci, potom je T rozhodnutelná.

Důkaz. Pro danou sentenci φ bud' $T \vdash \varphi$, nebo existuje protipříklad $\mathcal{A} \not\models \varphi$, tedy kompletní jednoduchá extenze T_i teorie T taková, že $T_i \nvdash \varphi$. Z kompletnosti ale plyne, že $T_i \vdash \neg\varphi$. Náš algoritmus bude paralelně konstruovat tablo důkaz φ z T a (postupně) tablo důkazy $\neg\varphi$ ze všech kompletních jednoduchých extenzí $T_1, T_2, \ldots$ teorie T.[8] Víme, že alespoň jedno z paralelně konstruovaných tabel je sporné, a můžeme předpokládat, že konečné (neprodlužujeme-li sporné větve tabla), tedy algoritmus ho po konečně mnoha krocích zkonstruuje.

17. Nerozhodnuteľnosť predikátovej logiky

Neexistuje algoritmus, který by pro danou vstupní formuli φ rozhodl, zda je logicky platná.

Hilbertův desátý problém: "Nalezněte algoritmus, který po konečně mnoha krocích určí, zda daná Diofantická rovnice s libovolným počtem proměnných a celočíselnými koeficienty má celočíselné řešení." (Neexistuje)

Důkaz. Uvažme formuli φ tvaru

$$(\exists x_1) \ldots (\exists x_n)\, p\,(x_1, \ldots, x_n) = q\,(x_1, \ldots, x_n)$$

kde p a q jsou polynomy s přirozenými koeficienty. Platí:

$$\underline{\mathbb{N}} \models \varphi \text{ právě když } Q \vdash \varphi$$

Označme jako ψ_Q konjunkci (generálních uzávěrů) všech axiomů Q. Zřejmě $Q \vdash \varphi$, právě když $\psi_Q \vdash \varphi$, což platí právě když $\vdash \psi_Q \to \varphi$. Dle Věty o úplnosti je to ale ekvivalentní $\models \psi_Q \to \varphi$. Dostáváme tedy následující ekvivalenci:

$$\underline{\mathbb{N}} \models \varphi \text{ právě když } \vdash \psi_Q \to \varphi$$

To znamená, že pokud existoval algoritmus rozhodující logickou platnost, mohli bychom rozhodovat i existenci přirozeného řešení rovnice $p\,(x_1, \ldots, x_n) = q\,(x_1, \ldots, x_n)$, neboli Hilbertův desátý problém by byl rozhodnutelný. Což by byl spor.