# VÝROKOVÁ LOGIKA

• Syntaxe výrokové logiky

syntaxe = soubor formálních pravidel pro vytváření korektních vět ze slov nebo formálních výrazů ze symbolů

→ v logice pracujeme s formálními nápisy

Def: Jazyk je určený množinou výrokových proměnných (prvovýroků), kterou značíme $\mathbb{P}$. Je spočetná a má dané uspořádání.

$$\mathbb{P} = \{p_1, p_2, p_3\}$$

Jazyk dále obsahuje logické spojky $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$ a závorky ( , ).

Def: Pro jazyk $\mathbb{P}$ definujeme množinu $VF_{\mathbb{P}}$ jako nejmenší množinu splňující

1, $\forall p \in \mathbb{P} : p \in VF_{\mathbb{P}}$

2, $\forall \varphi \in VF_{\mathbb{P}} : (\neg\varphi) \in VF_{\mathbb{P}}$

3, $\forall \varphi, \psi \in VF_{\mathbb{P}} : (\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \rightarrow \psi), (\varphi \leftrightarrow \psi) \in VF_{\mathbb{P}}$.

induktivní definice

Výrok (výroková formule) v jazyce $\mathbb{P}$ je prvek množiny $VF_{\mathbb{P}}$.

Značení: Místo binárních logických spojek občas používáme zástupný symbol $\square$.

Def: Podvýrok je podřetězec výroku, který je sám o sobě výrokem.

👁 Výroky jsou konečné řetězce napsané pomocí symbolů z jejich jazyka.

Def: $Var(\varphi) := \{p \in \mathbb{P} \mid p \text{ je podřetězec } \varphi\}$ ... množina všech prvovýroků ve $\varphi$.

Def: Definujeme zkratky za dva speciální výroky

• pravda $\top := (p \vee (\neg p))$

• spor $\bot := (p \wedge (\neg p))$

$p \in \mathbb{P}$ je pevně zvolený

Značení: Můžeme vynechávat některé závorky. Priorita operátorů

1. $\neg$  2. $\wedge, \vee$  3. $\rightarrow, \leftrightarrow$

$((p \vee (\neg q)) \leftrightarrow (r \rightarrow (p \wedge q))) \rightsquigarrow p \vee \neg q \leftrightarrow (r \rightarrow p \wedge q)$

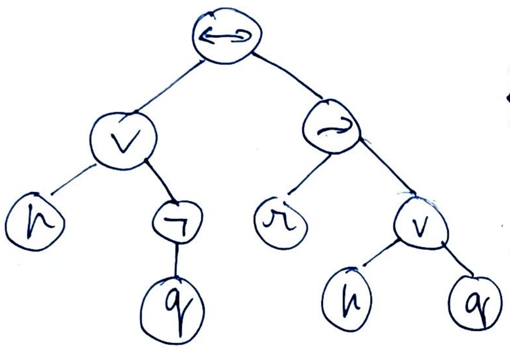
→ protože $\wedge$ a $\vee$ jsou asociativní:

$(p \wedge (q \wedge (r \wedge s))) \rightsquigarrow p \wedge q \wedge r \wedge s$

**Def:** Strom výroku $\varphi$, značíme $Tree(\varphi)$, je zakořeněný strom, kde záleží na pořadí potomků, definovaný induktivně takto:

1, pokud $\varphi = p \in \mathbb{P}$: $Tree(\varphi)$ obsahuje jediný vrchol, s labelem $p$
2, pokud $\varphi = (\neg\varphi')$: kořen s labelem $\neg$, jediný syn je kořen $Tree(\varphi')$
3, pokud $\varphi = (\varphi' \square \varphi'')$: kořen s labelem $\square$, dva synové $\begin{cases} \text{levý: kořen } Tree(\varphi') \\ \text{pravý: kořen } Tree(\varphi'') \end{cases}$

**Příklad:** $(p \vee \neg q) \leftrightarrow (r \rightarrow p \vee q)$




👁 $Tree(\varphi)$ je jednoznačně určený

**Def:** Teorie v jazyce $\mathbb{P}$ je libovolná množina výroků v $\mathbb{P}$, tedy $T \subseteq VF_{\mathbb{P}}$.
Prvkům teorie říkáme axiomy.

• **Sémantika výrokové logiky**

sémantika popisuje význam syntakticky korektních nápisů = výroků
↳ pro nás jen 2 možnosti: pravda a nepravda
⇓
pravdivostní hodnota

→ pravdivostní tabulka logických spojek

| $p$ | $q$ | $\neg p$ | $p \wedge q$ | $p \vee q$ | $p \rightarrow q$ | $p \leftrightarrow q$ |
|---|---|---|---|---|---|---|
| 1 | 1 | 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 1 | 0 | 0 |
| 0 | 1 | 1 | 0 | 1 | 1 | 0 |
| 0 | 0 | 1 | 0 | 0 | 1 | 1 |

👁 když ohodnotíme prvovýroky, tak pravdivostní hodnota složených výroků je jednoznačná

**Def:** Pro logické spojky definujeme odpovídající booleovské funkce:

- pro $\neg$ unární $f_\neg : \{0,1\} \rightarrow \{0,1\}$, $f_\neg : x \mapsto 1-x$.
- pro $\wedge, \vee, \rightarrow, \leftrightarrow$ binární $f_\wedge, f_\vee, f_\rightarrow, f_\leftrightarrow : \{0,1\}^2 \rightarrow \{0,1\}$, podle tabulky.

👁 Pokud do takové funkce dosadíme ohodnocení proměnných $p, q$, tak dostaneme pravdivostní hodnotu odpovídajícího složeného výroku.

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

číslujeme od 0
$0 \in \mathbb{N}$

1, je-li $\varphi$ $i$-tý prvovýrok z $\mathbb{P}$: $f_{\varphi,\mathbb{P}}(x_0, x_1, \dots x_{n-1}) := x_i$

2, je-li $\varphi = (\neg\varphi')$: $f_{\varphi,\mathbb{P}}(\underset{\sim}{x}) := f_\neg(f_{\varphi',\mathbb{P}}(\underset{\sim}{x}))$

3, je-li $\varphi = (\varphi' \square \varphi'')$: $f_{\varphi,\mathbb{P}}(\underset{\sim}{x}) := f_\square(f_{\varphi',\mathbb{P}}(\underset{\sim}{x}), f_{\varphi'',\mathbb{P}}(\underset{\sim}{x}))$

Příklad: $\varphi = (p \vee \neg q) \leftrightarrow (r \to (p \wedge q))$ v jazyce $\mathbb{P} = \{p, q, r, s\}$

$$f_{\varphi,\mathbb{P}}(x_0, x_1, x_2, x_3) = f_\leftrightarrow\Big(\underbrace{f_\vee(x_0, f_\neg(x_1))}_{p \vee \neg q}, \underbrace{f_\to(x_2, f_\wedge(x_0, x_1))}_{r \to p \wedge q}\Big)$$

→ pravdivostní hodnotu $\varphi$ při ohodnocení $p=1, q=0, r=1, s=1$ získáme dosazením těchto hodnot do pravdivostní funkce $\varphi$.

$$f_{\varphi,\mathbb{P}}(1,0,1,1) = f_\leftrightarrow(f_\vee(1, f_\neg(0)), f_\to(1, f_\wedge(1,0)))$$
$$= f_\leftrightarrow(f_\vee(1,1), f_\to(1,0)) = f_\leftrightarrow(1,0) = 0.$$

Pravdivostní funkce $f_{\varphi,\mathbb{P}}$ závisí pouze na proměnných, které odpovídají prvovýrokům z $\mathrm{Var}(\varphi)$.

Důsledek: Pokud je $\varphi$ v nekonečném jazyce, tak se můžeme omezit na $\mathrm{Var}(\varphi)$, který je konečný, a uvažovat pravdivostní funkci nad ním.

- Modely

→ ohodnocený prvovýrok modeluje nějakou reálnou situaci, kterou chceme studovat

Def: Model jazyka $\mathbb{P}$ je libovolné pravdivostní ohodnocení $v: \mathbb{P} \to \{0,1\}$.
Množinu všech modelů značíme $M_\mathbb{P}$.

$$M_\mathbb{P} := \{v \mid v: \mathbb{P} \to \{0,1\}\} = \{0,1\}^\mathbb{P} = 2^\mathbb{P} \ * \qquad \Rightarrow |M_\mathbb{P}| = 2^{|\mathbb{P}|}$$

* značení $X^A$, kde $X, A$ jsou množiny znamená množinu všech funkcí z $A$ do $X$
↳ $2^X$ ~ potenční množina $X$ ... funkce $X \to \{0,1\} =: 2$.

Příklad: Jazyk $\mathbb{P} = \{p, q, r\}$, ohodnocení $p, r$ pravda, $q$ nepravda:

$v = \{(p,1), (q,0), (r,1)\}$, protože $\mathbb{P}$ je uspořádaný, tak můžeme psát jen $v = (1,0,1)$. Ztotožňujeme tak $\{0,1\}^\mathbb{P}$ s $\{0,1\}^{|\mathbb{P}|}$.

$M_\mathbb{P} = \{(0,0,0), (0,0,1), (0,1,0), (1,0,0), (1,1,0), (1,0,1), (0,1,1), (1,1,1)\}$.

• Platnost

→ neformálně: výrok je platný ≡ jeho pravdivostní hodnota je 1.

Def: Nechť $\varphi$ je výrok v jazyce $\mathbb{P}$ a $v$ je model $\mathbb{P}$. → $\varphi \in VF_{\mathbb{P}}$, $v \in M_{\mathbb{P}}$

• $v \models \varphi$ ≡ $f_{\varphi,\mathbb{P}}(v) = 1$ ... $\varphi$ platí v modelu $v$, $v$ je modelem $\varphi$

Množinu všech modelů výroku $\varphi$ značíme $M_{\mathbb{P}}(\varphi)$.

$$M_{\mathbb{P}}(\varphi) = \{v \in M_{\mathbb{P}} \mid v \models \varphi\} = f_{\varphi,\mathbb{P}}^{-1}[1]$$

$$M_{\mathbb{P}} \setminus M_{\mathbb{P}}(\varphi) = \{v \in M_{\mathbb{P}} \mid v \not\models \varphi\} = f_{\varphi,\mathbb{P}}^{-1}[0]$$

Def: Nechť $T$ je teorie v jazyce $\mathbb{P}$ a $v$ je model $\mathbb{P}$. → $T \subseteq VF_{\mathbb{P}}$, $v \in M_{\mathbb{P}}$

• $v \models T$ ≡ $\forall \varphi \in T: v \models \varphi$ ... $T$ platí v modelu $v$, $v$ je modelem $T$

Množinu všech modelů teorie $T$ značíme $M_{\mathbb{P}}(T)$.

↳ teorie platí v modelu ≡ v něm platí všechny její axiomy.

Značení: Když do teorie přidáme nový axiom, tak místo $M_{\mathbb{P}}(T \cup \{\varphi\})$ píšeme $M_{\mathbb{P}}(T, \varphi)$.

$$M_{\mathbb{P}}(T, \varphi) = M_{\mathbb{P}}(T) \cap M_{\mathbb{P}}(\varphi)$$

$$M_{\mathbb{P}}(T) = \bigcap_{\varphi \in T} M_{\mathbb{P}}(\varphi)$$

$$M_{\mathbb{P}}(\varphi_1) \supseteq M_{\mathbb{P}}(\varphi_1, \varphi_2) \supseteq M_{\mathbb{P}}(\varphi_1, \varphi_2, \varphi_3) \supseteq \dots \supseteq M_{\mathbb{P}}(\varphi_1, \varphi_2, \varphi_3, \dots \varphi_n).$$

Příklad: $T = \{p \vee q \vee r, q \to r, \neg r\}$ v jazyce $\mathbb{P} = \{p, q, r\}$.

$M(\neg r) = \{(0,0,0), (0,1,0), (1,0,0), (1,1,0)\}$

$M(\neg r, q \to r) = \{(0,0,0), (1,0,0)\}$

$M(T) = M(\neg r, q \to r, p \vee q \vee r) = \{(1,0,0)\}$.

• Sémantické pojmy

Def: Výrok $\varphi$ v jazyce $\mathbb{P}$ je

$\varphi$ platí v logice

1) pravdivý, tautologie ≡ $M_{\mathbb{P}}(\varphi) = M_{\mathbb{P}}$ ... píšeme $\models \varphi$
2) lživý, sporný ≡ $M_{\mathbb{P}}(\varphi) = \emptyset$
3) nezávislý ≡ není pravdivý ani lživý
4) splnitelný ≡ není lživý

Def: Výroky $\varphi, \psi$ v jazyce $\mathbb{P}$ jsou ekvivalentní $\varphi \sim \psi$ ≡ $M_{\mathbb{P}}(\varphi) = M_{\mathbb{P}}(\psi)$.

Příklad:

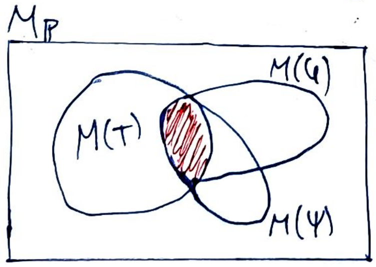
- $\top$, $p \vee q \leftrightarrow q \vee p$ jsou pravdivé
- $\perp$, $(p \vee q) \wedge (p \vee \neg q) \wedge \neg p$ jsou lživé
- $p$, $q \wedge p$ jsou nezávislé a splnitelné
- $p \sim p \vee p$, $p \to q \sim \neg p \vee q$, $p \to p \sim \neg p \vee p \sim \top$
- $\neg p \to (p \to q) \sim \neg p \to (\neg p \vee q) \sim p \vee \neg p \vee q \sim \top$

- Sémantické pojmy vzhledem k teorii

Def: Nechť $T$ je teorie v jazyce $\mathbb{P}$. Výrok $\varphi$ v jazyce $\mathbb{P}$ je

1) pravdivý v $T$, důsledek $T \equiv M_{\mathbb{P}}(T) \subseteq M_{\mathbb{P}}(\varphi)$ ... píšeme $T \models \varphi$
   ↳ $\varphi$ platí v každém modelu $T$: $\forall v \in M_{\mathbb{P}}(T)$: $v \models \varphi$
2) lživý v $T$, sporný v $T \equiv M_{\mathbb{P}}(T) \cap M_{\mathbb{P}}(\varphi) = \emptyset$
   ↳ $\varphi$ neplatí v žádném modelu $T$: $\forall v \in M_{\mathbb{P}}(T)$: $v \not\models \varphi$
3) nezávislý v $T$ $\equiv$ není pravdivý v $T$ ani sporný v $T$
4) splnitelný v $T$, konzistentní s $T$ $\equiv$ není lživý v $T$ $\Rightarrow M(T, \varphi) \neq \emptyset$

Def: Výroky $\varphi, \psi$ jsou ekvivalentní v teorii $T$ $\varphi \sim_T \psi \equiv M_{\mathbb{P}}(T, \varphi) = M_{\mathbb{P}}(T, \psi)$.
↳ platí ve stejných modelech $T$: $\forall v \in M_{\mathbb{P}}(T)$: $v \models \varphi \Leftrightarrow v \models \psi$




Příklad: $T = \{p \vee q, \neg r\}$, $\mathbb{P} = \{p, q, r\}$

- $q \vee p$, $\neg p \vee \neg q \vee \neg r$ jsou pravdivé v $T$
- $(\neg p \wedge \neg q) \vee r$ je lživý v $T$ $(\neg p \wedge \neg q) \sim \neg(p \vee q)$
- $p \leftrightarrow q$, $p \wedge q$ jsou v $T$ nezávislé a splnitelné
- $p \sim_T p \vee r$ ... ale $p \not\sim p \vee r$

• Vlastnosti teorií

Def: Teorie $T, T'$ v jazyce $\mathbb{P}$ jsou ekvivalentní $T \sim T' \equiv M_{\mathbb{P}}(T) = M_{\mathbb{P}}(T')$.
↳ vyjadřují tytéž vlastnosti, ale jsou jinak axiomatizované

Příklad: $\{p \to q,\ p \leftrightarrow r\} \sim \{(\neg p \vee q) \wedge (\neg p \vee r) \wedge (\neg r \vee p)\}$

Def: Teorie $T$ v jazyce $\mathbb{P}$ je

1) sporná $\equiv$ v ní platí spor ... $T \models \bot$ → $M_{\mathbb{P}}(T) \subseteq M_{\mathbb{P}}(\bot) = \emptyset$
⟺ nemá žádný model $M_{\mathbb{P}}(T) = \emptyset$ ↗ $\emptyset \subseteq M_{\mathbb{P}}(\varphi)$
⟺ v ní platí všechny výroky $\forall \varphi \in VF_{\mathbb{P}}: T \models \varphi$

2) bezesporná (splnitelná) $\equiv$ není sporná
⟺ má alespoň 1 model

nemá nezávislé výroky

3) kompletní $\equiv$ není sporná & každý výrok je ní pravdivý nebo lživý
⟺ má právě 1 model
↳ důkaz příkladem: 2 různé modely $(1,0,1,1)$, $(0,0,1,1)$
↳ $p_1 \wedge \neg p_2 \wedge p_3 \wedge p_4$ ✓ ✗
⇒ tenhle výrok by byl nezávislý v $T$ ↯

Příklad

- $T_1 = \{p,\ p \to q,\ \neg q\}$ je sporná
- $T_2 = \{p \vee q,\ r\}$ je bezesporná, ale není kompletní → $p \wedge q$ $\begin{cases} (1,1,1) \text{ platí} \\ (1,0,1) \text{ neplatí} \end{cases}$
- $T_2 \cup \{\neg p\}$ je kompletní → jediný model $(0,1,1)$

• Důsledky a extenze teorií

Def: Množinu všech důsledků teorie $T$ (výroků pravdivých v $T$) značíme jako

$$Csq_{\mathbb{P}}(T) := \{\varphi \in VF_{\mathbb{P}} \mid T \models \varphi\} = \{\varphi \in VF_{\mathbb{P}} \mid M_{\mathbb{P}}(T) \subseteq M_{\mathbb{P}}(\varphi)\}$$

$T \subseteq Csq_{\mathbb{P}}(T)$ ... axiomy $T$ platí v $T$

- pokud $\varphi \in Csq_{\mathbb{P}}(T)$, tak $M_{\mathbb{P}}(T, \varphi) = M(T) \cap M(\varphi) = M(T)$ ... $\because M(T) \subseteq M(\varphi)$
⇒ $M(Csq(T)) = M(T)$ ⇒ $Csq(Csq(T)) = Csq(T)$ → důsledky důsledků jsou důsledky
- pokud $T \subseteq T'$, tak $M(T) \supseteq M(T')$ ... víc podmínek ⇒ míň modelů
⇒ $Csq(T) \subseteq Csq(T')$ $\because$ pokud $\varphi \in Csq(T)$, tak $M(\varphi) \supseteq M(T) \supseteq M(T')$

**Def:** Nechť T je teorie v jazyce $\mathbb{P}$. Teorie T' v jazyce $\mathbb{P}' \supseteq \mathbb{P}$ je

1) extenze teorie T $\equiv Csq_{\mathbb{P}}(T) \subseteq Csq_{\mathbb{P}'}(T')$

↳ všechno, co platí v T, platí i v T'

→ navíc, pokud to je extenze, tak to je

2) jednoduchá extenze $\equiv \mathbb{P}' = \mathbb{P}$ ... nezvětšuje jazyk

3) konzervativní extenze $\equiv Csq_{\mathbb{P}}(T) = Csq_{\mathbb{P}'}(T') \cap VF_{\mathbb{P}}$

↳ neměníme platnost tvrzení vyjádřených v původním jazyce

⇒ ∀ nový důsledek musí obsahovat nějakou novou proměnnou

👁 Jednoduchá & konzervativní extenze je ekvivalentní původní teorii.

👁 Často je jednodušší pracovat s modely, než s důsledky

- T' je jednoduchá extenze T $\iff \mathbb{P}' = \mathbb{P}$ & $M_{\mathbb{P}}(T') \subseteq M_{\mathbb{P}}(T)$

  ↳ když $\varphi \in Csq_{\mathbb{P}}(T)$, tak $M_{\mathbb{P}}(\varphi) \supseteq M_{\mathbb{P}}(T) \supseteq M_{\mathbb{P}}(T') \Rightarrow \varphi \in Csq_{\mathbb{P}}(T')$

- T' je extenze T $\iff M_{\mathbb{P}'}(T') \subseteq M_{\mathbb{P}'}(T)$ $\qquad (1,1,1,\underset{\times}{0}) \to (1,1,1)$

  $\iff \forall v \in M_{\mathbb{P}'}(T')$: restrikce $v$ na $\mathbb{P}$ je modelem T

- T' je konzervativní extenze T $\iff$ je extenze & ∀ model T lze rozšířit na model T'

  $\iff \forall v \in M_{\mathbb{P}'}(T')$: restrikce $v$ na $\mathbb{P}$ je modelem T

  & $\forall w \in M_{\mathbb{P}}(T)\ \exists v \in M_{\mathbb{P}'}(T')$: restrikce $v$ na $\mathbb{P} = w$

  $\iff \{$restrikce $v$ na $\mathbb{P} \mid v \in M_{\mathbb{P}'}(T')\} = M_{\mathbb{P}}(T)$

**Neformálně:**

- extenze nepřidává nové modely (když se omezíme na původní jazyk)
- jednoduchá extenze navíc nezvětšuje jazyk
- konzervativní extenze navíc neodebírá modely

**Příklad:** $T = \{p \to q\}$, $\mathbb{P} = \{p, q\} \Rightarrow M_{\mathbb{P}}(T) = \{(0,0), (0,1), (1,1)\}$

- $T_1 = \{p \wedge q\}$ nad $\mathbb{P} \Rightarrow M_{\mathbb{P}}(T_1) = \{(1,1)\} \Rightarrow T_1$ je jedn. extenze T
- $T' = \{p \leftrightarrow (q \wedge r)\}$ nad $\mathbb{P}' = \mathbb{P} \cup \{r\}$

  $\Rightarrow M_{\mathbb{P}'}(T') = \{(1,1,1), (0,1,0), (0,0,1), (0,0,0)\}$

  → restrikce na $\mathbb{P}$: $\{(1,1), (0,1), (0,0)\} = M_{\mathbb{P}}(T)$

  ⇒ T' je konzervativní extenze T

• Univerzálnost logických spojek

Def: Množina logických spojek je univerzální $\equiv$ $|\mathbb{P}| = n$ pro $n$-ární $f$

$\forall$ booleovská funkce $f$ je pravdivostní funkce $f_{\varphi,\mathbb{P}}$ nějakého výroku $\varphi$.

Ekvivalentně: Pro $\forall$ konečný $\mathbb{P}$ a $\forall M \subseteq M_{\mathbb{P}}$ $\exists \varphi \in VF_{\mathbb{P}}$: $M_{\mathbb{P}}(\varphi) = M$.

Tvrzení: $\{\neg, \wedge, \vee\}$ jsou univerzální.

Dk: Mějme $f: \{0,1\}^n \to \{0,1\}$, respektive $M := f^{-1}[1]$

$\to$ chceme najít $\varphi$ t.ž. $M(\varphi) = M$

1, pokud $|M| = 1$ ... jediný model $v \in M$.

$\hookrightarrow$ vyrobíme $\varphi_v$ = „musím mít model $v$"

$\to$ příklad: $v = (1,0,1,0) \rightsquigarrow \varphi_v = p_1 \wedge \neg p_2 \wedge p_3 \wedge \neg p_4$

2, pokud $|M| > 1$

$\to \varphi_M := \bigvee_{v \in M} \varphi_v$ ... $M = \{(1,0,1), (0,0,1)\} \to (p_1 \wedge \neg p_2 \wedge p_3) \vee (\neg p_1 \wedge \neg p_2 \wedge p_3)$

$\to$ zřejmě $M(\varphi_M) = M$ ■

Důsledek: NOR a NAND jsou univerzální.

Dk: lze z nich vyrobit $\neg, \vee, \wedge$

• Výrokové normální formy – CNF, DNF

Def: Literál $l$ je buď prvovýrok nebo jeho negace. Opačný literál $\neg l$ značíme $\bar{l}$.

Def: Klauzule je disjunkce literálů $C = l_1 \vee l_2 \vee \dots \vee l_n$

Jednotková klauzule je samotný literál, prázdná klauzule je $\perp$.

Def: Výrok je v CNF $\equiv$ je to konjunkce klauzulí. Prázdný CNF výrok je $\top$.

Def: Elementární konjunkce je konjunkce literálů $E = l_1 \wedge l_2 \wedge \dots \wedge l_n$. $\top$

Def: Výrok je v DNF $\equiv$ je disjunkcí el. konjunkcí. Prázdný DNF je $\perp$.

Výrok v CNF je pravdivý $\Leftrightarrow$ $\forall$ klauzule obsahuje dvojici opačných literálů.

Výrok v DNF je lživý $\Leftarrow$ $\forall$ el. konj. ——— " ———

Příklad: Převeď $\varphi = p \Leftrightarrow (q \vee \neg r)$ do CNF a DNF.

• modely $M = \{(0,0,1), (1,0,0), (1,1,0), (1,1,1)\}$

$\Rightarrow \varphi_{DNF} = (\neg p \wedge \neg q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \vee (p \wedge q \wedge \neg r) \vee (p \wedge q \wedge r)$

↳ tento výrok říká „jsem jeden z modelů M"

↳ je to ten výrok $\varphi_M$ z minulého důkazu

• nemodely $\overline{M} = \{(1,0,1), (0,0,0), (0,1,0), (0,1,1)\}$

$\Rightarrow \varphi_{CNF} = (\neg p \vee q \vee \neg r) \wedge (p \vee q \vee r) \wedge (p \vee \neg q \vee r) \wedge (p \vee \neg q \vee \neg r)$

↳ $\forall$ klauzule zakazuje 1 nemodel

↳ kdyby (1,0,1) byl model, tak není splněná $(\neg p \vee q \vee \neg r)$

Tvrzení: Nechť $\mathbb{P}$ je konečný jazyk a $M \subseteq M_{\mathbb{P}}$ libovolná množina modelů.

Potom existují výroky $\varphi_{DNF}$ v DNF a $\varphi_{CNF}$ v CNF takové, že

$M = M_{\mathbb{P}}(\varphi_{CNF}) = M_{\mathbb{P}}(\varphi_{DNF})$.

Dk: Zavedeme značení $p^1 := p$, $p^0 := \neg p$. Potom pro model $v \in M$ definujeme

$$\varphi_v := \bigwedge_{p \in \mathbb{P}} p^{v(p)} \quad \text{a} \quad C_v := \bigvee_{p \in \mathbb{P}} p^{1-v(p)}$$

Označme

$$\varphi_{DNF} := \bigvee_{v \in M} \varphi_v \qquad \varphi_{CNF} := \bigwedge_{v \notin M} C_v$$

$\rightarrow \varphi_v$ má pouze model $v$ $\Rightarrow$ $\varphi_{DNF}$ má všechny modely z M

$\rightarrow C_v$ má všechny modely kromě $v$ $\Rightarrow$ $\varphi_{CNF}$ má všechny modely, kromě těch, které nejsou v M

**Důsledek:** Každý výrok (i v nekonečném jazyce) je ekvivalentní nějakému výroku v CNF a nějakému výroku v DNF.

**Dk:** Pokud je $\mathbb{P}$ nekonečný, tak se omezíme na konečný $\mathbb{P}' := \mathrm{var}(\varphi)$ a $M := M_{\mathbb{P}'}(\varphi)$ a můžeme použít předchozí tvrzení. ∎

- **Převod do CNF/DNF pomocí ekviv. úprav**

  - $\varphi \to \psi \sim \neg\varphi \vee \psi$

    $\varphi \leftrightarrow \psi \sim (\neg\varphi \vee \psi) \wedge (\neg\psi \vee \varphi)$

  - $\neg(\varphi \wedge \psi) \sim \neg\varphi \vee \neg\psi$

    $\neg(\varphi \vee \psi) \sim \neg\varphi \wedge \neg\psi$

  DNF:

  $\varphi \wedge (\psi \vee \chi) \sim (\varphi \wedge \psi) \vee (\varphi \wedge \chi)$

  CNF:

  $\varphi \vee (\psi \wedge \chi) \sim (\varphi \vee \psi) \wedge (\varphi \vee \chi)$

- **Problém SAT** – satisfiability

  Vstup: výrok v CNF

  Výstup: je tento výrok splnitelný? Případně jaký má model?

  → NP-úplný problém v obecném případě

**Def:** Výrok $\varphi$ je v $k$-CNF ≡ je v CNF & ∀ klauzule má nejvýše $k$ literálů.

→ pro $k \geq 3$ je $k$-SAT pořád NP-úplný

→ ale 2-SAT lze lineárně

• 2-SAT, Algoritmus implikačního grafu

Algoritmus:

Vstup: výrok $\varphi$ v 2-CNF

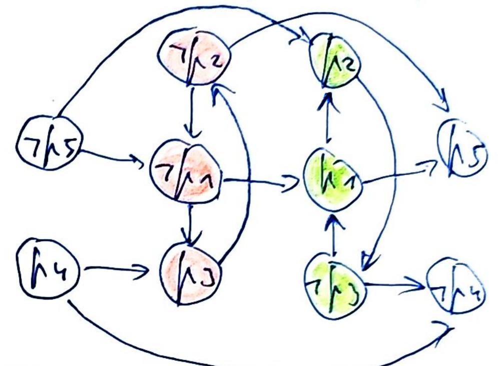
$$\varphi = (\neg p_1 \vee p_2) \wedge (\neg p_2 \vee \neg p_3) \wedge (p_1 \vee p_3) \wedge (p_3 \vee \neg p_4) \wedge (\neg p_1 \vee p_5) \wedge (p_2 \vee p_5) \wedge \overset{*}{p_1} \wedge \overset{\boxtimes}{\neg p_4}$$

1. Všechny klauzule převedeme na implikace: $p \vee q \rightsquigarrow \neg p \to q \wedge \neg q \to p$

$p_1 \to p_2$ $\quad p_2 \to \neg p_3$ $\quad \neg p_1 \to p_3$ $\quad \neg p_3 \to \neg p_4$ $\quad p_1 \to p_5$ $\quad \neg p_2 \to p_5$ $\quad \neg p_1 \to p_1$ *

$\neg p_2 \to \neg p_1$ $\quad p_3 \to \neg p_2$ $\quad \neg p_3 \to p_1$ $\quad p_4 \to p_3$ $\quad \neg p_5 \to \neg p_1$ $\quad \neg p_5 \to p_2$ $\quad p_4 \to \neg p_4$ ⊠

2. Vyrobíme implikační graf $G_\varphi$

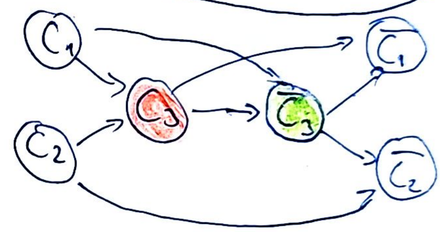



$G_\varphi$

$V = \{p, \neg p \mid p \in Var(\varphi)\}$

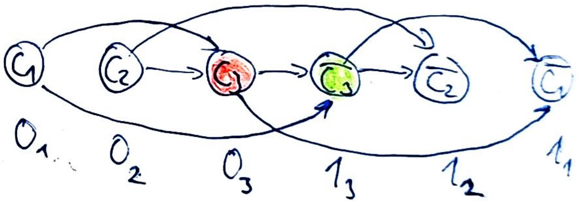
$$E = \{(\bar{l}_1, l_2), (\bar{l}_2, l_1) \mid l_1 \vee l_2 \text{ klauzule } \varphi\} \cup \{(\bar{l}, l) \mid l \text{ je jednot. klauzule } \varphi\}$$

3. Najdeme komponenty silné souvislosti, kontrahujeme je a získáme graf $G_\varphi^*$




4. Je to DAG (jinak bychom komponenty našli špatně)

$\Rightarrow$ má topologické uspořádání




5. Ohodnocujeme literály v komp.

↳ vždy 0 a opačné literály 1

literály ve stejné komponentě musí být ohodnoceny stejně

$\to$ jinak $0 \to 1$ $\Rightarrow 1 = 0$ ↯

$\Rightarrow$ pokud jsou ve stejné komponentě opačné literály $l, \bar{l}$, tak $\nexists$ model

Tvrzení: $\varphi$ má model $\Leftrightarrow$ $\nexists$ silná k. v $G_\varphi$ s dvojicí opačných literálů.

Dk: Stačí, aby z žádné 1 komponenty nevedla hrana do 0 komponenty.

$\Rightarrow$ literály ve stejné komponentě musí být ohodnoceny stejně

$\Leftarrow$: Ohodnocení vyrobené výše je model $\varphi$

- jednotková klauzule $l$ platí kvůli hraně $\bar{l} \to l$ a komponenta s $\bar{l}$ byla hodnocena dříve, tedy $0 \to 1$.
- $l_1 \vee l_2 \rightsquigarrow \bar{l}_1 \to l_2,\ \bar{l}_2 \to l_1$. Pokud jsme $l_1$ ohodnotili dříve, tak to musela být díky hraně $\bar{l}_1 \to l_2 \Rightarrow v(\bar{l}_1) = 0 \Rightarrow v(l_1) = 1$ a klauzule platí. Podobně pro l

Důsledek: 2-SAT je řešitelný lineárně ∵ komponenty a TU jsou $O(n+m)$.

• Horn-SAT a jednotková propagace

Def: Klauzule je hornovská ≡ má nejvýš 1 pozitivní literál.

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

→ Horn-SAT = splnitelnost hornovského výroku = CNF s horn. klauzulemi

👁 Jednotková propagace

→ jednotková klauzule $\ell$ vynucuje $v(\ell)=1$

⇒ všechny klauzule s $\ell$ se tím splní

⇒ z klauzulí s $\bar{\ell}$ lze $\bar{\ell}$ odstranit (je to 0)

$\varphi = (\neg p_1 \vee p_2) \wedge (\neg p_1 \vee \neg p_2 \vee p_3) \wedge (\neg p_2 \vee \neg p_3) \wedge (\neg p_5 \vee \neg p_4) \wedge \underline{p_4}$ ⇒ $p_4 = 1$

$\varphi^{p_4} = (\neg p_1 \vee p_2) \wedge (\neg p_1 \vee \neg p_2 \vee p_3) \wedge (\neg p_2 \vee \neg p_3) \wedge \underline{\neg p_5}$ ⇒ $p_5 = 0$

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

👁 Když hornovský výrok neobsahuje žádnou jednotkovou klauzuli, tak můžeme všechno ohodnotit 0 a bude to model.

Pž: klauzule: alespoň 2 literály, max. 1 pozitivní ⇒ alespoň 1 negativní. ☒

→ $\varphi$ má model $(0,0,0,1,0)$

Značení: $\varphi^{\ell}$ = výrok vzniklý jednotkovou propagací $\ell$ ve $\varphi$

? Co když $\varphi$ není splnitelný?

$$p \wedge (\neg p \vee q) \wedge (\neg q \vee r) \wedge \underline{\neg r} \sim p \wedge (\neg p \vee q) \wedge \underline{\neg q} \sim p \wedge \neg p \quad ↯$$

Algoritmus:

1. Pokud $\varphi$ obsahuje dvojici opačných jednotkových klauzulí $\ell, \bar{\ell}$, není splnitelný.
2. Pokud $\varphi$ neobsahuje žádnou jednotkovou klauzuli, nastav vše na 0 a toto je model.
3. $\varphi$ tedy obsahuje jednotkovou klauzuli $\ell$ → nahraď $\varphi$ výrokem $\varphi^{\ell}$ a goto 1.

Korektnost: zřejmě musíme nastavit jednotkovou klauzuli na 1.

👁 modely $\varphi^{\ell}$ jsou modely $\varphi$, ve kterých platí $\ell$.

Složitost: zřejmě nejhůř kvadratické, lze implementovat lineárně.

• Algoritmus DPLL pro řešení SAT

Def: Literál $l$ má čistý výskyt ve $\varphi \equiv l$ je ve $\varphi$, ale $\overline{l}$ se tam nevyskytuje.

👁 Literál s čistým výskytem lze vždy nastavit na 1 a odstranit tak všechny klauzule, kde se vyskytuje.

→ čistý výskyt nevyrobí nikdy jednotkovou kl., ale jednotková propagace může vyrobit č. výskyt ⇒ nejprve propagace

Algoritmus DPLL:

1. Pokud $\varphi$ obsahuje jednotkovou klauzuli $l$, nastav $v(l)=1$, proveď jednotkovou propagaci a nahraď $\varphi$ za výrok $\varphi^l$.
2. Pokud existuje literál $l$ s čistým výskytem ve $\varphi$, nastav $v(l)=1$ a odstraň klauzule obsahující $l$
3. Pokud $\varphi$ neobsahuje žádnou klauzuli, je splnitelný a tohle je model.
4. Pokud jednotková propagace vznikla prázdná klauzule $p \wedge \neg p \to \square$, je $\varphi$ nesplnitelný.
5. Jinak zvol dosud neohodnocenou proměnnou $p$, a zavolej algoritmus rekurzivně na $\varphi \wedge p$ a na $\varphi \wedge \neg p$ … zkusíme $p=1$ a $p=0$.

Složitost: Kvůli větvení to v nejhorším případě běží exponenciálně.

Příklad: $(\neg p \vee q \vee \neg r) \wedge (\neg p \vee \neg q \vee \neg s) \wedge (p \vee \neg r \vee \neg s) \wedge (q \vee \neg r \vee s) \wedge (p \vee s) \wedge (p \vee \neg s) \wedge (q \vee s)$

→ ∄ jednotková klauzule, ale $\neg r$ má čistý výskyt $r=0$

$(\neg p \vee \neg q \vee \neg s) \wedge (p \vee s) \wedge (p \vee \neg s) \wedge (q \vee s)$ → rekurze

$(p=1)$: $(\neg q \vee \neg s) \wedge (q \vee s)$

$(q=1)$: $\neg s$ ⇒ $s=0$ ⇒ model $\begin{matrix} p & q & r & s \\ (1, & 1, & 0, & 0) \end{matrix}$

→ pro ilustraci i ostatní větve – najdeme více modelů:

$(q=0)$: $s$ ⇒ $s=1$ ⇒ $(1,0,0,1)$

ale ne všechny ∵ čistý výskyt

$(p=0)$: $s \wedge \neg s \wedge (q \vee s)$

$s=0$: $\square \wedge q$ ⇒ tudy cesta nevede

• Formální dokazovací systémy

Def: Důkaz faktu, že v teorii T platí výrok φ je konečný syntaktický objekt, vycházející z axiomů T a výroku φ.
Pokud důkaz existuje, tak píšeme $T \vdash \varphi$.

Def: Dokazovací systém je

1) korektní $\equiv T \vdash \varphi \Rightarrow T \models \varphi$ ... dokazatelný výrok je pravdivý
2) úplný $\equiv T \models \varphi \Rightarrow T \vdash \varphi$ ... pravdivý výrok je dokazatelný

→ korektnost vyžadujeme vždy, také chceme, aby důkaz bylo možné algoritmicky sestrojit a ověřit jeho korektnost.

! nutný předpoklad: P musí být spočetný — potom je i T spočetná.

• Metoda analytického tabla

→ nejprve se zaměříme na případ $T = \emptyset$, tedy dokazujeme, že φ platí v logice.
→ tablo je strom představující hledání protipříkladu - modelu $v \not\models \varphi$
↳ basically ukážeme, že $\neg\varphi$ nemá model ⇒ φ je tautologie (dk. sporem)

→ vrcholy stromu mají label Tφ, Fφ ... platí / neplatí φ
→ do kořene stromu dáme Fφ a rozvíjíme tak, aby vždy platil následující invariant

Def: model se shoduje s nějakou položkou, pokud v něm platí(T) / neplatí(F) daný výrok
→ model se shoduje s větví ≡ se shoduje se všemi položkami v ní

Invariant: Každý model, který se shoduje s položkou v kořeni (platí v něm ¬φ) se shoduje i s některou větví tabla.

→ pokud je na větvi Tφ & Fφ, potom větev selhala (je sporná)
→ pokud selžou všechny větve, je tablo sporné a máme důkaz $T \vdash \varphi$
→ pokud nějaká větev neselhala a je dokončená (vše na ní je zredukované), lze z ní zkonstruovat model, ve kterém φ neplatí

## Příklad

$\varphi = ((p \to q) \to p) \to p$

$F((p \to q) \to p) \to p$

$T(p \to q) \to p$ — aby $F \to$

$F p$

buď $F\, p \to q$ nebo $T p$

- $F\, p \to q$
  - $T p$
  - $F q$ ⊗
- $T p$ ⊗

$\Rightarrow \varphi$ je tautologie

$\varphi = (\neg q \vee p) \to p$

$F(\neg q \vee p) \to p$

$T\, \neg q \vee p$

$F p$

buď $T \neg q$ nebo $T p$

- $T \neg q$
  - $F q$ ✓
- $T p$ ⊗

$\Rightarrow \varphi$ není tautologie

↳ $(0,0)$ není model $\quad 1 \vee 0 \to 0$

→ položky redukujeme pomocí atomických tabel

→ třeba pro ekvivalenci:

$T\, \varphi \leftrightarrow \psi$

- $T\varphi$
  - $T\psi$
- $F\varphi$
  - $F\psi$

$F\, \varphi \leftrightarrow \psi$

- $T\varphi$
  - $F\psi$
- $F\varphi$
  - $T\psi$

→ atomická tabla zachovávají invariant $\Rightarrow$ celé tablo ho zachovává

**Def:** Strom je $T \neq \emptyset$ s částečným uspořádáním – kořen je nejmenší prvek

↳ množina předků libovolného vrcholu je navíc dobře uspořádaná

Uspořádaný strom má navíc lineární uspořádání množiny synů $\forall$ vrcholu

Větev je maximální lineárně uspořádaná podmnožina $T$.

Označkovaný strom má navíc funkci label: $T \to$ Labels.

**Lemma (Königovo):** Nekonečný strom, kde mají všechny vrcholy konečný stupeň má nekonečnou větev.

Def: Položka je nápis $T\varphi$ nebo $F\varphi$, kde $\varphi$ je výrok.

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

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

Konvence: Kořen atomického tabla nepřipisujeme (už na té větvi je).

Def: Tablo z teorie $T$ je buď konečné, nebo i nekonečné; v tom případě je spočetné a definujeme ho jako

$T := \bigcup_{i \geq 0} T_i$, kde $T_0$ je jednoprvkové tablo a $T_{i+1}$ vzniklo z $T_i$ v jednom kroku

Def: Větev je sporná $\equiv$ obsahuje položky $T\varphi$ i $F\varphi$.

Tablo je sporné $\equiv$ $\forall$ jeho větev je sporná

Def: Položka $P$ na větvi $V$ je na této větvi redukovaná $\equiv$

- je tvaru $Tp$ nebo $Fp$ pro prvovýrok $p \in \mathbb{P}$
- nebo se na $V$ vyskytuje jako kořen atomického tabla

Def: Větev je dokončená $\equiv$ je sporná nebo

1) $\forall$ její položka je na této větvi redukovaná a
2) obsahuje položku $T\alpha$ pro $\forall \alpha \in T$

Tablo je dokončené $\equiv$ je každá jeho větev dokončená

Def: Tablo důkaz výroku $\varphi$ z teorie $T$ je sporné tablo z teorie $T$ s položkou $F\varphi$ v kořeni.

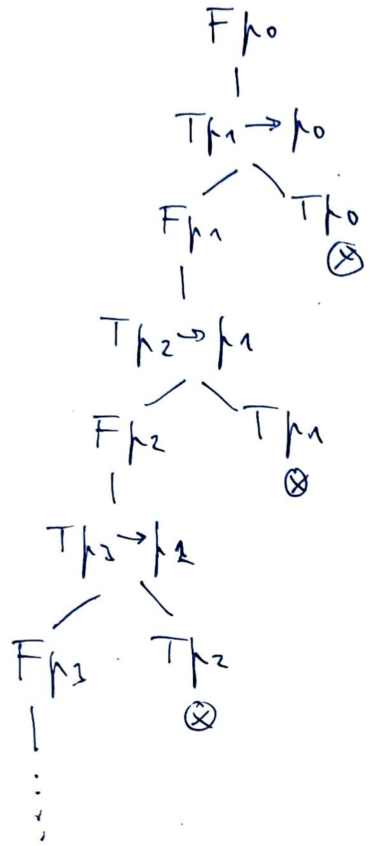
→ pokud existuje, je $\varphi$ tablo dokazatelný z $T$, píšeme $T \vdash \varphi$

Tablo zamítnutí je sporné tablo s $T\varphi$ v kořeni.

→ pokud existuje, je $\varphi$ tablo zamítnutelný z $T$, tedy platí $T \vdash \neg\varphi$.

Příklad: Dokončené nekonečné bezesporné tablo.

$T = \{p_{n+1} \to p_n \mid n \in \mathbb{N}\}$. $\varphi = p_0$




→ nejlevější větev je dokončená a bezesporná

↳ jsou tam všechny axiomy a jsou zredukované

→ shoduje se s modelem $v = (0,0,0,\dots 0)$

tedy $v: \mathbb{P} \to \{0,1\}$, $p_i \mapsto 0$.

⇒ $v$ je model $T$, ale není model $\varphi$

⇒ je to protipříklad ⇒ $T \nvDash p_0$.

- Korektnost a úplnost tablo metody

Věta (o korektnosti): Je-li $\varphi$ tablo dokazatelný z $T$, potom $T \models \varphi$.

Myšlenka důkazu: Protipříklad by se shodoval s některou z větví tablo důkazu, ale ty jsou všechny sporné.

Věta (o úplnosti): Pokud $T \models \varphi$, potom je $\varphi$ tablo dokazatelný z $T$.

Myšlenka důkazu: Libovolné dokončené tablo s $F\varphi$ v kořeni musí být sporné, takže je tablo důkazem $T \vdash \varphi$.

- Konečnost a systematičnost důkazů

→ ukážeme

1) existuje-li tablo důkaz, existuje i konečný tablo důkaz
2) existuje algoritmus, který umí vždy zkonstruovat dokončené tablo
   ↳ systematické tablo
3) pokud ∃ tablo důkaz, tak tento alg. zkonstruuje konečný tablo důkaz
   ↳ pokud ∄, tak se alg. nemusí zastavit

Pro konečnou $T$ je snadné zkonstruovat dokončené tablo.

↳ na začátku pověsíme všechny axiomy a pak redukujeme

Def (Systematické tablo): Myšlenka: na všechny se dostane, střídáme
- redukce následující položky na všech bezesporných větvích kde je
- přidání následujícího axiomu na všechny bezesporné větve

Systematické t. z teorie $T = \{\alpha_1, \alpha_2, \dots\}$ s položkou $R$ v kořeni je tablo $\tau := \bigcup_{i \geq 0} \tau_i$, kde $\tau_0$ je jednoprvkové t. s $R$ v kořeni a pro $i \geq 0$:

1) nechť $P$ je nejlevější položka v co nejmenší úrovni, která ještě není redukovaná na nějaké bezesporné větvi obsahující $P$.
   → definujme $\tau_i'$ jako tablo vzniklé z $\tau_i$ připojením atomického tabla pro $P$ na každou bezespornou větev obsahující $P$.
   → pokud $P$ neexistuje (vše je redukované), tak $\tau_i' := \tau_i$.
2) $\tau_{i+1}$ vznikne z $\tau_i'$ připojením $T\alpha_{i+1}$ na $\forall$ bezespornou větev $\tau_i'$
   → pokud $i \geq |T|$ ($T$ je konečná a pověsili jsme všechny axiomy), tak definujeme $\tau_{i+1} := \tau_i'$

Lemma: Systematické tablo je dokončené.

Dk: Jsou všechny větve dokončené?

- sporné větve jsou dokončené z definice
- bezesporná větev:
  - obsahuje $T\alpha_i$ pro všechna $i$ ... připojeno v $i$-tém kroku
  - každá položka je na ní zredukovaná – v nejhorším případě je tablo binární strom ⇒ pokud leží v hloubce $h$, tak na ní přišla řada nejpozději v kroku řádově $i = 2^h$.

Def: Kanonický model pro bezespornou větev $V$ dokončeného tabla je

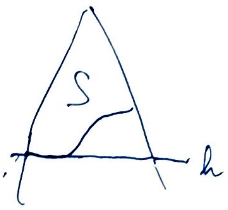
$$v : \mathbb{P} \to \{0,1\}, \quad v(p) := \begin{cases} 1, & \text{pokud se na } V \text{ vyskytuje } Tp \\ 0, & \text{jinak} \end{cases}$$

↳ pokud $Fp$ nebo není zmíněno vůbec

→ když $F\varphi$ má bezespornou větev, tak kanonický model této větve je (jeden z) protipříklad.

Věta (o konečnosti sporu): Je-li $T = \bigcup_{i \geq 0} T_i$ sporné (ne nutně systematické) tablo. Potom pro nějaké $n \in \mathbb{N}$ je $T_n$ sporné konečné tablo.

Dk: Definujme $S$ jako množinu vrcholů, nad kterými není spor, tedy dvojice položek $T\varphi$, $F\varphi$.



1, Kdyby $S$ byla nekonečná, tak podle Königova lemmatu pro podstrom $T$ na množině $S$ máme nekonečnou, bezespornou větev v $S$, tedy i v $T$. Ale $T$ je sporné ↯

2, Takže $S$ je konečná. ⇒ celá leží v hloubce $\leq h \in \mathbb{N}$.

→ ∀ vrchol na úrovni $h+1$ už má nad sebou spor

⇒ zvolíme $n$ tak, aby $T_n$ obsahovalo všechny vrcholy z prvních $h+1$ úrovní ⇒ ∀ větev $T_n$ je sporná ■

Důsledek: (konečnost důkazu): Pokud $T \vdash \varphi$, potom ∃ konečný tablo důkaz $\varphi$ z $T$.

Dk: Stačí neprodlužovat již sporné větve.

Důsledek (systematičnost důkazů): Pokud $T \vdash \varphi$, potom systematické tablo je konečným tablo důkazem $\varphi$ z $T$.

Dk: Věta o úplnosti říká, že libovolné dokončené tablo z $T$ s $F\varphi$ v kořeni je sporné, tedy tablo důkazem.

↳ platí to i pro systematické tablo, které je vždy dokončené

↳ navíc v systematickém tablu neprodlužujeme již sporné větve ⇒ je konečné ■

Důsledek: Tablo dokazatelnost $\vdash$ a platnost $\models$ jsou jedno a totéž.

⇒ v definicích je můžeme zaměňovat:

Teorie je sporná ⇔ je v ní dokazatelný spor

Teorie je kompletní ⇔ pro $\forall \varphi$: $T \vdash \varphi$ XOR $T \vdash \neg\varphi$.

Věta (o dedukci): $T, \varphi \vdash \psi \iff T \vdash \varphi \to \psi$.

Dk: stačí dokázat $T, \varphi \models \psi \iff T \models \varphi \to \psi$.

- Věta o kompaktnosti

Věta: Teorie má model $\iff$ $\forall$ její konečná část má model.

Dk: $\Rightarrow$ zřejmé

$\Leftarrow$: Pro spor nechť $T$ nemá model, najdeme spornou konečnou $T' \subseteq T$. $T$ je sporná, tedy $T \models \bot$ a z úplnosti $T \vdash \bot$, tedy existuje i konečný tablo důkaz $\tau$ výroku $\bot$ z $T$. Protože $\tau$ je konečný, tak obsahuje jen konečně mnoho axiomů z $T$. Označíme

$$T' := \{\alpha \in T \mid T\alpha \text{ je položka v tablu } \tau\}$$

$\Rightarrow$ $\tau$ je také tablo důkaz výroku $\bot$ z konečné teorie $T'$, tedy $T' \vdash \bot$, dle korektnosti $T' \models \bot \Rightarrow T'$ je sporná ▨

- Aplikace kompaktnosti – dokazování vět typu

vlastnost nekonečného objektu $O$

$\Updownarrow$ ($\Downarrow$ easy, $\Uparrow$ kompaktnost)

vlastnost všech konečných podobjektů $O'$

1. vlastnost popíšeme pomocí nekonečné teorie $T$
2. ke každé konečné $T' \subseteq T$ sestrojíme konečný podobjekt $O'$
3. $O'$ splňuje danou vlastnost $\Rightarrow$ $T'$ má model
4. dle věty o kompaktnosti má i $T$ model $\Rightarrow$ $O$ splňuje vlastnost

Příklad: Spočetně nekonečný graf je bipartitní $\iff$ $\forall$ konečný podgraf je bipartitní

Dk: $\Rightarrow$ $\forall$ podgraf b.p. grafu je b.p.

$\Leftarrow$ $G$ je b.p. $\iff$ je 2-obarvitelný.

$\hookrightarrow$ udělám jazyk $\mathbb{P} := \{C_v \mid v \in V(G)\}$

teorii $T := \{C_v \to \neg C_u \mid \{u,v\} \in E(G)\}$

$\to$ zřejmě $G$ je b.p. $\iff$ $T$ má model

věta o kompaktnosti: stačí aby $\forall$ $T' \subseteq T$ (konečná) měla model

$\Rightarrow$ buď $G'$ podgraf $G$ indukovaný vrcholy o kterých $T'$ hovoří

$\to$ $\because$ $T'$ je konečná, je $G'$ také konečný, tedy dle předpokladu b.p. a 2-obarvitelný – to určuje model $T'$. ▨

- Rezoluční metoda

- mnohem efektivnější PC implementace
- rezoluční pravidlo:

$$(q \vee p_1 \vee p_2) \wedge (\neg q \vee p_1 \vee \neg p_3) \sim p_1 \vee p_2 \vee \neg p_3$$

→ obecně

$$\frac{\{p\} \cup C_1, \quad \{\neg p\} \cup C_2}{C_1 \cup C_2} \rightarrow \text{zápis} \quad \frac{\text{podmínky}}{\text{výsledek}}$$

- obecnější pravidlo řezu

$$\frac{\varphi \vee \psi, \quad \neg\varphi \vee \emptyset}{\psi \vee \emptyset}$$

- Množinová reprezentace CNF

$$(p_1 \vee p_2) \wedge (\neg p_1 \vee p_3) \wedge (p_1 \vee \neg p_2 \vee p_3)$$

$$\{\{p_1, p_2\}, \{\neg p_1, p_3\}, \{p_1, \neg p_2, p_3\}\} \rightarrow \text{ohodnocení } \{p_1, p_3, \neg p_2\} \text{ funguje}$$

$$(1, 1, 0)$$

↳ klauzule = konečná množina literálů

↳ CNF formule = množina klauzulí (klidně ∞)

→ Modely a množiny literálů

- ohodnocení = množina literálů, co neobsahuje žádnou dvojici $l, \bar{l}$
- úplné ohodnocení obsahuje $p$ nebo $\neg p$ pro každý prvovýrok
- ohodnocení $V$ splňuje formuli $S$, píšeme $V \models S \equiv$

  $V$ obsahuje nějaký literál z každé klauzule $S$:

$$\forall C \in S: V \cap C \neq \emptyset$$

→ v tom příkladu $\{p_1, p_3\}$ také splňuje $S$, ale není úplné

Def. Nechť $C_1, C_2$ jsou klauzule a $l$ literál splňující $l \in C_1$ & $\bar{l} \in C_2$.
Rezolventa klauzulí $C_1$ a $C_2$ přes literál $l$ je klauzule

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

Pokud $V \models C_1$ a $V \models C_2$, potom $V \models C$

**Def:** Rezoluční důkaz klauzule $C$ z formule $S$ je konečná posloupnost klauzulí $C_0, C_1, \dots C_n = C$ t.ž. pro $\forall i$:

1) $C_i \in S$ nebo
2) $C_i$ je rezolventou nějakých $C_j, C_k$, kde $j, k < i$.

→ pokud r.d. ∃, říkáme, že $C$ je rezolucí dokazatelná z $S$: $S \vdash_R C$

→ rezoluční zamítnutí formule $S$ je rezoluční důkaz $\square$ z $S$

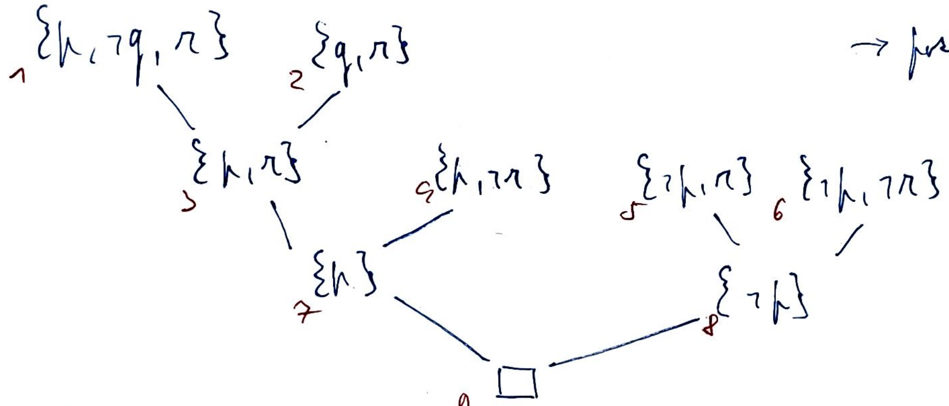
↳ v každém modelu $S$ musí platit $\square$ neboli spor $\perp$ → prázdná klauzule

⇒ tedy $S$ nemá model (spor nemá model)

**Příklad:** $S = \{\underset{1}{\{p, \neg q, r\}}, \underset{2}{\{p, \neg r\}}, \underset{3}{\{\neg p, r\}}, \underset{4}{\{\neg p, \neg r\}}, \underset{5}{\{q, r\}}\}$

↳ zamítnutí $1, 5, \{p, r\}, 2, \{p\}, 3, 4, \{\neg p\}, \square$

→ přirozená stromová struktura:




→ posloupnost zleva → doprava
↓
dolu

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

- v kořeni je $C$
- v listech jsou klauzule z $S$
- v každém vnitřním vrcholu je rezolventa klauzulí z jeho synů

$C$ má rezoluční strom z $S$ $\iff S \vdash_R C$.

**Def:** Rezoluční uzávěr $R(S)$ formule $S$ definujeme induktivně jako nejmenší množinu klauzulí splňující

1) $C \in R(S)$ pro $\forall C \in S$
2) $C_1, C_2 \in R(S) \Rightarrow$ rezolventa $C_1$ a $C_2 \in R(S)$

**Intuice:** $R(S)$ je množina všech klauzulí, co se dají z $S$ dokázat

• Korektnost a úplnost rezoluce

Věta (o korektnosti r.): Je-li CNF formule S rezolucí zamítnutelná, $S \vdash_R \square$, potom je S nesplnitelná.

Dk: Nechť $S \vdash_R \square$, tedy existuje nějaký rezoluční důkaz $C_0, C_1, \dots C_n = \square$. Pro spor nechť existuje ohodnocení $\mathcal{V} \models S$. Indukcí ukážeme, že $\mathcal{V} \models \square$, což bude spor. Zřejmě $\mathcal{V} \models C_0$, protože $C_0 \in S$. Pro $i > 0$:
↳ spor ⊥ nemá model

1, $C_i \in S$ ✓ 2, $C_i$ je rezolventou nějakých $C_j, C_k$, pro které to platí ✓

↳ $\mathcal{V} \models C_j$ & $\mathcal{V} \models C_k \Rightarrow \mathcal{V} \models C_i$

→ takto se dopracujeme k $\mathcal{V} \models C_n = \square$ ∎

• Strom dosazení

→ dosazení je množinový zápis jednotkové propagace

Def: Dosazení literálu $l$ do formule S je formule

$$S^l := \{C \setminus \{\bar{l}\} \mid C \in S,\ l \notin C\}$$

👁 $S^l$ je výsledek jednotkové propagace aplikované na $S \cup \{\{l\}\}$

👁 pokud S neobsahovala $l$ ani $\bar{l}$, tak $S^l = S$

pokud S obsahovala $\{\bar{l}\}$, → jednotková klauzule, tak $\square \in S^l$, tedy $S^l$ je sporná.

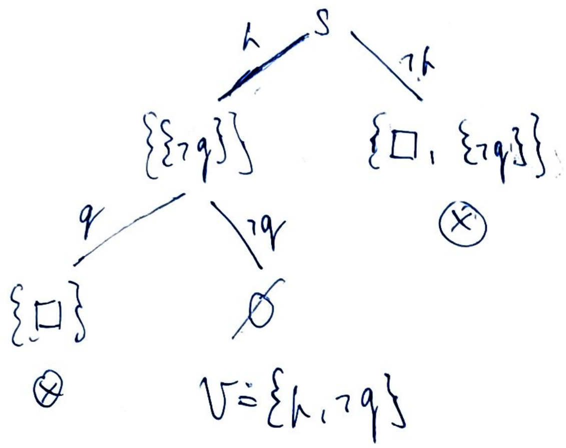
Lemma: S je splnitelná $\iff$ je splnitelná $S^l$ nebo $S^{\bar{l}}$.

Dk: $\Rightarrow$: Ohodnocení $\mathcal{V} \models S$ nemůže obsahovat $l$ i $\bar{l}$ $\Rightarrow$ BÚNO $\bar{l} \notin \mathcal{V}$.
Ukážeme $\mathcal{V} \models S^l$. Buď $C \in S^l$. Zřejmě $C = C' \setminus \{\bar{l}\}$ pro nějakou $C' \in S$.
Protože $\mathcal{V} \models C'$ a $\bar{l} \in \mathcal{V}$, tak $\mathcal{V}$ muselo splnit nějaký jiný literál a tento literál je i v C, čili $\mathcal{V} \models C$.

$\Leftarrow$: BÚNO nechť je $S^l$ splnitelná a $\mathcal{V}$ je její ohodnocení.
∵ se $l$ ani $\bar{l}$ nevyskytují v $S^l$, tak musí platit $\mathcal{V} \setminus \{\bar{l}\} \models S^l$
Plán: $S^l$ odebralo klauzule s $l$ $\Rightarrow$ musíme je splnit
$\Rightarrow$ z $\mathcal{V}$ dáme pryč $\bar{l}$ a přidáme tam $l$
$\mathcal{V}' := (\mathcal{V} \setminus \{\bar{l}\}) \cup \{l\}$ je ohodnocení S. ∎

To, zda je S splnitelná můžeme zjistit postupným dosazováním obou literálů pro nějaký prvovýrok p a rozvětvením na $S^p$ a $S^{\neg p}$
→ basically větvení z DPLL

$S = \{\{p\}, \{\neg q\}, \{\neg p, \neg q\}\}$

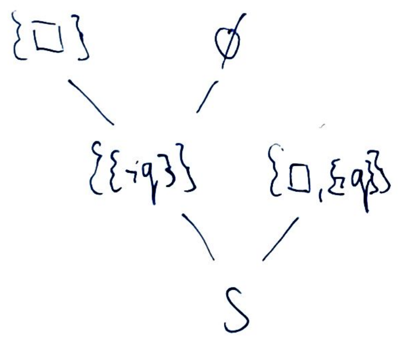



výsledný strom
||
STROM DOSAZENÍ

1) jakmile větev obsahuje □ je nesplnitelná
⇒ nepokračujeme v ní
2) pokud je v listu prázdná teorie, tak posloupnost dosazení určuje splňující ohodnocení

Důsledek: CNF formule je nesplnitelná ⟺ každá větev stromu dosazení obsahuje □.

Dk: Pro konečnou S indukcí podle $|Var(S)|$




→ pro $|Var(S)| = 0$ to triviálně platí $\begin{cases} S = \emptyset \\ S = \{\square\} \end{cases}$

→ pro 1 to platí ∵ podle lemmatu je $\{\{\neg q\}\}$ nesplnitelná
⟺ není splnitelná $\{\{\neg q\}\}^q$ ani $\{\{\neg q\}\}^{\neg q}$
→ tam už je 0 proměnných ⇒ už to máme dokázané

indukční krok: máme S, $|Var(S)| > 0$ → vybereme libovolný $l \in Var(S)$, aplikujeme lemma a řešíme úlohu pro $S^l$, $S^{\bar{l}}$, ale $|Var(S^l)| < |Var(S)|$

• Pro nekonečnou S: → její obměna

⇒: dle věty o kompaktnosti ∃ konečná $S' \subseteq S$, která je také nesplnitelná. pro $S'$ už to máme dokázané, čili po dosazení za všechny proměnné z $Var(S')$ bude v každé větvi □ ... konečně mnoho kroků.

⇐: Obměnou: Nechť je S splnitelná, potom ∃ větev co neobsahuje □.
S má splňující ohodnocení, tedy větev odpovídající tomuto ohodnocení ve stromu dosazení neobsahuje □.

↳ jinak by byla nesplnitelná, což je spor

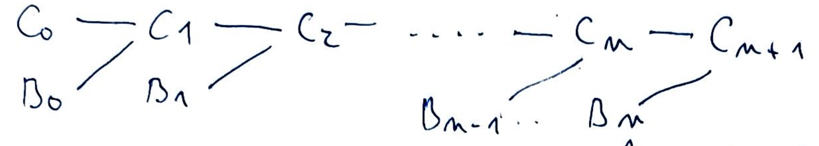
• Úplnost rezoluce

Věta (o úplnosti r.): Je-li S nesplnitelná, potom je rezolucí zamítnutelná $S \vdash_R \square$.

Dk: indukcí podle $|Var(S)|$

• LI rezoluce

– rezoluční důkaz můžeme reprezentovat i lineárně



axiom / nějaká stará $C_i$

Def: Lineární důkaz klauzule C z formule S je konečná posloupnost

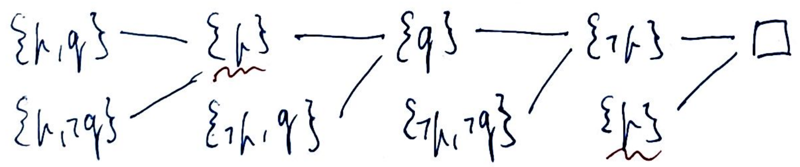
$$\begin{bmatrix}C_0\\B_0\end{bmatrix}, \begin{bmatrix}C_1\\B_1\end{bmatrix}, \dots \begin{bmatrix}C_n\\B_n\end{bmatrix}, C_{n+1},$$

kde $C_i$ jsou centrální klauzule, $B_i$ boční klauzule, $C_0$ je počáteční a $C_{n+1} = C$ koncová. Platí

- $C_0 \in S$, $C_{i+1}$ je rezolventou $C_i$ a $B_i$
- $B_0 \in S$, $B_i \in S$ nebo $B_i = C_j$ pro $j < i$.

Lineární zamítnutí S je lineární důkaz $\square$ z S.

Příklad: $S = \{\{p,q\}, \{p,\neg q\}, \{\neg p, q\}, \{\neg p, \neg q\}\}$



C má lineární důkaz z S $\Leftrightarrow$ C má rezoluční důkaz z S.

Def: LI-důkaz klauzule C z formule S je lineární důkaz, ve kterém jsou všechny boční klauzule axiomy z S.

→ pokud LI důkaz existuje, je C LI-dokazatelná z S $\quad S \vdash_{LI} C$

→ S je LI zamítnutelná $\equiv S \vdash_{LI} \square$.

LI důkaz odpovídá rezolučnímu stromu tvaru chlupaté cesty

Důsledek: LI důkaz je korektní, tedy $S \vdash_{LI} \square \Rightarrow$ S nemá ohodnocení.

→ ale ztrácíme úplnost pro obecné S

- Úplnost LI-rezoluce pro Hornovy formule

→ budeme umět dokazovat věci typu

$$\text{Hornova formule} \models p_1 \wedge p_2 \wedge \ldots \wedge p_n$$

→ sporem, tedy $H \wedge \underbrace{\neg(p_1 \wedge p_2 \wedge \ldots \wedge p_n)}_{\neg p_1 \vee \neg p_2 \vee \ldots \vee \neg p_n \;\leftarrow\; \text{cíl}} \vdash_{LI} \square$

<u>Def</u>: <u>Fakt</u> je pozitivní jednotková klauzule, tedy $\{p\}$ (hornovská)

<u>Pravidlo</u> je hornova klauzule tvaru $\neg p_1 \vee \neg p_2 \vee \ldots \vee \neg p_n \vee q \sim (p_1 \wedge \ldots \wedge p_n) \to q$

<u>Cíl</u> je neprázdná hornova klauzule bez pozitivního literálu $\neg p_1 \vee \neg p_2 \vee \ldots \vee \neg p_n$

<u>Příklad</u>: Máme splnitelnou hornovskou teorii

$$T = \{\{p, \neg r, \neg s\}, \{\neg q, r\}, \{q, \neg s\}, \{s\}\}$$, chceme dokázat $T \models p \wedge q$

$\Rightarrow$ cíl $G := \{\neg p, \neg q\}$ a ukážeme $T \cup \{G\} \vdash_{LI} \square$, z korektnosti $\models$

$$\begin{array}{ccccccccc}
G = \{\neg p, \neg q\} & — & \{\neg q, \neg r, \neg s\} & — & \{\neg q, \neg s\} & — & \{\neg s\} & — & \square \\
\{p, \neg r, \neg s\} & & \{\neg q, r\} & & \{q, \neg s\} & & \{s\} & &
\end{array}$$

<u>Věta</u>: Nechť je $T$ <u>splnitelná Hornova formule</u> a $G$ je <u>cíl</u>.
Pokud je $T \cup \{G\}$ <u>nesplnitelná</u>, potom je i <u>LI-zamítnutelná</u>,
a to zamítnutím, které začíná cílem $G$.

<u>Dk</u>: konstrukcí tohoto LI zamítnutí.

# PREDIKÁTOVÁ LOGIKA (prvního řádu)

→ proměnné nemohou být množiny
→ pozn: proměnné mohou být množiny

příklad: chceme vyjádřit implikaci $x_1 \leq y_1$ & $x_2 \leq y_2 \Rightarrow (y_1 \cdot y_2) - (x_1 \cdot x_2) \geq 0$

$$\varphi = (x_1 \leq x_2) \wedge (y_1 \leq y_2) \rightarrow ((y_1 \cdot y_2) + (-(x_1 \cdot x_2)) \geq 0)$$

→ 2 binární relační symboly $\geq, \leq$

→ 2 binární funkční $+, \cdot$

1 unární funkční $-$

1 konstantní (= nulární funkční) $0$

→ model, ve kterém $\varphi$ platí: $\mathbb{N}$ s relacemi $\leq^{\mathbb{N}}, \geq^{\mathbb{N}}, +^{\mathbb{N}}, -^{\mathbb{N}}, \cdot^{\mathbb{N}}, 0^{\mathbb{N}}$

→ ale podobně v $\mathbb{Z}$ už neplatí: $-3 \leq -2$, $-5 \leq -2$, ale $4 - 15 \ngeq 0$.

- Struktury

Def: Signatura je dvojice $\langle R, F \rangle$ kde $R$ a $F$ jsou disjunktní množiny relačních a funkčních (ty zahrnují i konstantní) symbolů spolu s jejich aritami – tedy funkce $ar: R \cup F \rightarrow \mathbb{N}$. Symbol '=' je ovšem rezervovaný pro rovnost, tudíž zde není.

Ukázka: Pokud je arita a to, zda jsou r. nebo f. zřejmé z kontextu → jen symboly

$\langle E \rangle$ ... signatura grafů, $E$ je bin. rel. symbol "být hranou"

$\langle \leq \rangle$ ... signatura částečných uspořádání

$\langle +, -, 0 \rangle$ ... signatura grup

$\langle +, -, 0, \cdot, 1 \rangle$ ... signatura těles

$\langle Succ, +, \cdot, 0, \leq \rangle$ ... signatura aritmetiky

→ struktura je nějaká konkrétní „implementace" dané signatury na neprázdné doméně poté

↳ signatura ~ interface

↳ struktura ~ třída co to implementuje

Ukázka:

- struktura v prázdné signatuře $\langle \rangle$ je libovolná neprázdná množina
- struktura v signatuře grafů je $\langle V, E \rangle$, $V$ je doména, $E$ je bin. relace $V \neq \emptyset$, $E \subseteq V^2$ ... orientovaný graf

→ pokud je navíc $E$ reflexivní, tranzitivní a symetrická, tak to je částečné uspořádání

• signatura grup:

$\underline{\mathbb{Z}_n} = \langle \mathbb{Z}_n, +, -, 0 \rangle$ ... aditivní grupa $\mathbb{Z}_n$

$S_n = \langle \text{permutace}, \circ, ^{-1}, id \rangle$ je symetrická grupa všech permutací na $n$ prvcích.

$\underline{\mathbb{Q}^*} = \langle \mathbb{Q} \setminus 0, \cdot, ^{-1}, 1 \rangle$ ... multiplikativní grupa racionálních č. bez nuly

• signatura těles

$\underline{\mathbb{R}} = \langle \mathbb{R}, +, -, 0, \cdot, 1 \rangle$ ... reálná čísla

• signatura aritmetiky

$\underline{\mathbb{N}} = \langle \mathbb{N}, Succ, +, \cdot, 0, \leq \rangle$, kde $Succ(x) = x+1$ je standardní model aritmetiky

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

- $A$ je neprázdná množina ... doména / universum
- $\mathcal{R}^a = \{R^a \mid R \in \mathcal{R}\}$, kde $R^a \subseteq A^{ar(R)}$ je interpretace relačního symbolu $R$
- $\mathcal{F}^a = \{f^a \mid f \in \mathcal{F}\}$, kde $f: A^{ar(R)} \to A$ je interpretace funkčního symbolu $f$

↳ speciálně pro konstantní symbol $c \in \mathcal{F}$ máme $c^a \in A$.

• Syntaxe

Def: Jazyk je daný nějakou konkrétní signaturou a informací, zda je s rovností nebo ne.

→ rovnost '=' je identita prvků v konkrétní struktuře dané signatury.

Do jazyka patří:

1, spočetně mnoho proměnných $x_0, x_1, x_2, \ldots$ – množina všech prom. značíme Var.

2, relační a funkční symboly ze signatury, případně i symbol '='.

3, kvantifikátory $\underbrace{(\forall x)}_{1 \text{ symbol}}, (\exists x)$ pro každou proměnnou $x \in Var$

4, symboly logických spojek: $\neg, \vee, \wedge, \rightarrow, \leftrightarrow$, závorky '(', ')' a čárka ','

Vzorky:

$\langle \rangle$ s rovností ... jazyk čisté rovnosti

$\langle c_0, c_1, \ldots \rangle$ s rovností ... jazyk spočetně mnoha konstant

$\langle \leq \rangle$ s rovností ... jazyk uspořádání

$\langle E \rangle$ s rovností ... jazyk teorie grafů

$\langle \in \rangle$ s rovností ... jazyk teorie množin

**Def:** Termy jazyka $L$ jsou konečné nápisy definované induktivně

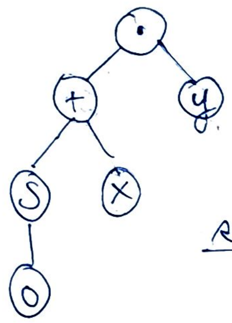
1) každá proměnná a každý konstantní symbol je term
2) je-li $f$ funkční symbol arity $n$ a jsou-li $t_1, \dots t_n$ termy, potom je nápis $f(t_1, t_2, \dots t_n)$ také term.

→ $\mathrm{Term}_L$ := množina všech termů jazyka $L$.

**Def:** $\mathrm{Tree}(t)$ pro term $t$: v listech proměnné / konstanty, vnitřní vrcholy – fční sym.

**Ukázka:** $(S(0)+x)\cdot y$ v jazyce aritmetiky

↳ formálně $\cdot(+(S(0),x),y)$ ... prefixový zápis, $\cdot$ a $+$ jsou funkce



strom tohoto termu

sémantika: proměnné ohodnotíme prvky, konst. a fční symboly nahradíme interpretacemi ze struktury ⇒ výsledek je prvek domény

**Def:** Atomická formule jazyka $L$ je nápis $R(t_1, \dots t_n)$, kde $R$ je $n$-ární relační symbol z $L$ (včetně '=') a $t_i \in \mathrm{Term}_L$.

$x \cdot y \leq (S(0)+x)\cdot y$ → $\leq$ opět píšeme infixově

**Def:** Formule jazyka $L$ jsou konečné nápisy definované induktivně:

1) každá atomická formule jazyka $L$ je formule
2) je-li $\varphi$ formule, je $(\neg\varphi)$ také formule
3) jsou-li $\varphi, \psi$ formule, je $(\varphi \square \psi)$ také formule ... $\square \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$
4) je-li $\varphi$ formule a $x$ proměnná, jsou $((\forall x)\varphi)$ a $((\exists x)\varphi)$ také formule.

**Konvence:** kvantifikátory mají stejnou prioritu jako $\neg$ (nejvyšší)

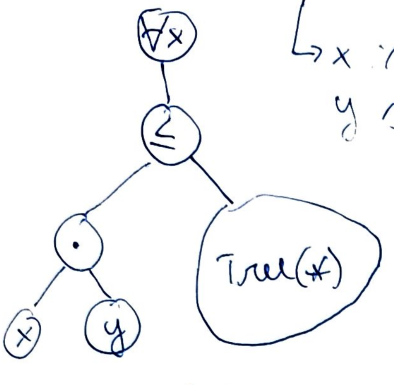
místo $((\forall x)\varphi)$ píšeme $(\forall x)\varphi$

→ jako ve výr. logice

**Def:** Strom formule $\mathrm{Tree}(\varphi)$ definujeme induktivně takto:

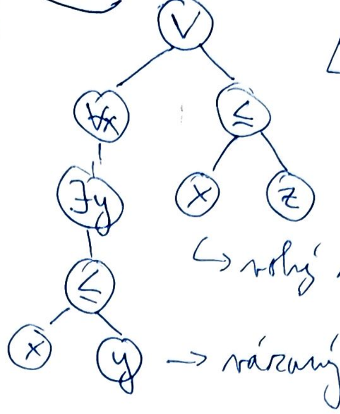
- je-li $\varphi$ atomická formule $R(t_1, \dots t_n)$, je v kořeni $R$ a připojíme stromy $\mathrm{Tree}(t_i)$
- je-li $\varphi$ tvaru $(\neg\varphi')$: v kořeni $\neg$, jediný syn: kořen $\mathrm{Tree}(\varphi')$
- je-li $\varphi$ tvaru $(\varphi' \square \psi)$: v kořeni $\square$, dva synové pro $\mathrm{Tree}(\varphi')$ a $\mathrm{Tree}(\psi)$
- je-li $\varphi$ tvaru $((Qx)\varphi')$ pro $Q \in \{\forall, \exists\}$: v kořeni $Qx$, jediný syn pro $\mathrm{Tree}(\varphi')$

Příklad: $\varphi = (\forall x)(x \cdot y \leq \underbrace{(S(0)+x)\cdot y)}_{*}$ | $\psi = (\forall x)(\exists y)(x \leq y) \vee (x \leq z)$




↳ x vázaná
y volná

$\varphi(y)$




↳ y vázaná, z volná
x volná i vázaná

$\psi(x, z)$

↳ volný výskyt

→ vázaný výskyt

Qx se nepočítá

- **Sémantika**

Def: Výskyt proměnné $x$ ve formuli $\varphi$ je list Tree($\varphi$) označený $x$. Výskyt je

1) vázaný ≡ je součástí nějaké podformule (podstromu) začínající $(Qx)$
2) volný ≡ není-li vázaný

Def: Proměnná $x$ je volná ve $\varphi$ ≡ má volný výskyt.
vázaná ve $\varphi$ ≡ má vázaný výskyt.

→ zápis $\varphi(x_1, x_2, \dots x_n)$ znamená, že $x_1, x_2, \dots x_n$ jsou volné proměnné ve $\varphi$

Poznámka: význam $\varphi$ bude záviset pouze na volných proměnných, proměnné v kvantifikátorech můžeme libovolně přejmenovat.

Def: Formule je

1) otevřená ≡ nemá žádný kvantifikátor
2) uzavřená ≡ nemá žádnou volnou proměnnou ← sentence

Ukázka:

- $x + y \leq 0$ ... otevřená
- $(\forall x)(\forall y)(x + y \leq 0)$ ... sentence = uzavřená
- $(\forall x)(x + y \leq 0)$ ... ani otevřená ani uzavřená
- $(0+1=1) \wedge (1+1=0)$ ... otevřená i uzavřená ⟺ nemá žádné proměnné
- atomické formule a jejich kombinace pomocí logických spojek jsou otevřené
- $(\forall x)\, 0=1$ ... formule bez vázané proměnné není nutně otevřená!

• Instance a varianty formulí

Neformálně: proměnná vázaná ke kvantifikátorem je lokální, volná ~ globální
- instance formule ~ dosazení nějakého termu za globální proměnnou
- varianta formule ~ přejmenování lokální proměnné

$P(x) \wedge (\forall x)(Q(x) \wedge (\exists x) R(x))$

1. volný 2. vázaný 3. vázaný

1) substituujeme za $x$ term $t = 1+1$
2) přejmenujeme $x$ na $y$
3) přejmenujeme $x$ na $z$

Instance: $P(1+1) \wedge (\forall x)(Q(x) \wedge (\exists x) R(x))$ ... značíme $\varphi(x/t)$

Varianta: $P(x) \wedge (\forall y)(Q(y) \wedge (\exists z) R(z))$

? Kdy je instance důsledek původní formule ?

$\varphi(x) = (\exists y)(x+y=1)$ ... existuje $1-x$

$\varphi(x/1) = (\exists y)(1+y=1)$ ... existuje $1-1$ ✓

$\varphi(x/y) = (\exists y)(y+y=1)$ ... existuje $2^{-1}$ ✗

Def: Term $t$ je substituovatelný za proměnnou $x$ ve formuli $\varphi$ $\equiv$ po nahrazení všech volných výskytů $x$ za $t$ nevznikne žádný nový vázaný výskyt.

→ vzniklá formule = instance, značíme ji $\varphi(x/t)$

👁 konstantní termy jsou vždy substituovatelné

Def: Nechť $\varphi$ obsahuje podformuli s kvantifikátorem $(Qx)\psi$ a pro $y \in Var$ platí
- $y$ je substituovatelná za $x$ do $\psi$,
- $y$ nemá volný výskyt ve $\psi$.

Varianta $\varphi$ vznikne nahrazením $(Qx)\psi$ za $(Qy)\psi(x/y)$.

Ukázka: $\varphi = (\exists x)(\forall y)(x \leq y)$
- $(\exists u)(\forall y)(u \leq y)$ ✓
- $(\exists y)(\forall y)(y \leq y)$ ✗ porušuje 1)
- $(\exists x)(\forall x)(x \leq x)$ ✗ porušuje 2) ... $x$ má volný výskyt ve $(\forall y)(x \leq y)$

## • Modely a pravdivostní hodnota

Neformálně:

• modely = struktury dané signatury

• formule platí ve struktuře ≡ platí při každém ohodnocení volných proměnných

prvky z domény

• hodnota termu se vyhodnocuje podle jeho stromu

• pravdivostní hodnoty atomických formulí získáme z hodnot termů

známe

$R(t_1 \dots t_n)$

• —— " —— složených formulí vyhodnocujeme pomocí jejich stromu.

$(\forall x)$ ~ konjunkce přes všechny prvky domény

$(\exists x)$ ~ disjunkce —— " ——

**Def:** Model jazyka $L$ nebo také $L$-struktura je libovolná struktura v signatuře jazyka $L$. Třídu všech modelů jazyka $L$ označíme $M_L$.

↳ doména = množina a množina všech množin neexistuje

**Ukázka:** modely jazyka $\langle \leq \rangle$ jsou například

• $\langle \mathbb{N}, \leq \rangle$, $\langle P(X), \subseteq \rangle$ ... částečná uspořádání

• $\langle \mathbb{Q}, > \rangle$, $G = \langle V, E \rangle$, $\langle \{0,1\}, \emptyset \rangle$ ... ne částečná uspořádání, ale modely ano

**Def:** Nechť $t$ je term jazyka $L = \langle \mathcal{R}, \mathcal{F} \rangle$ a nechť $\mathcal{A} = \langle A, \mathcal{R}^{\mathcal{A}}, \mathcal{F}^{\mathcal{A}} \rangle$ je $L$-struktura. Ohodnocení proměnných množinou $A$ je libovolná funkce $e: \mathrm{Var} \to A$.

**Def:** Hodnota termu $t$ ve struktuře $\mathcal{A}$ při ohodnocení $e$, značíme $t^{\mathcal{A}}[e]$, je dána:

1) $x^{\mathcal{A}}[e] := e(x)$ pro $x \in \mathrm{Var}$

2) $c^{\mathcal{A}}[e] := c^{\mathcal{A}}$ pro konstantní $c \in \mathcal{F}$

3) je-li $t = f(t_1, \dots t_n)$ pro $f \in \mathcal{F}$: $t^{\mathcal{A}}[e] := f^{\mathcal{A}}(t_1^{\mathcal{A}}[e], \dots t_n^{\mathcal{A}}[e])$.

**Ukázka:** $t = x + 1$, $L = \langle +, 1 \rangle$, struktura $\langle \mathbb{N}, \cdot, 3 \rangle$, $e(x) = 2$

$t^{\mathcal{A}}[e] = +(x, 1) = \cdot(2, 3) = 6$

**Def:** Nechť $\varphi$ je formule v jazyce $L$, $\mathcal{A}$ je model $L$ a $e$ je ohodnocení proměnných. Pravdivostní hodnota $\varphi$ v $\mathcal{A}$ při ohodnocení $e$, značíme $PH^{\mathcal{A}}(\varphi)[e]$, je dána:

1) pro atom. f: $PH^{\mathcal{A}}(R(t_1, \dots t_n))[e] := \begin{cases} 1 & \text{pokud } (t_1^{\mathcal{A}}[e], \dots t_n^{\mathcal{A}}[e]) \in R^{\mathcal{A}} \\ 0 & \text{jinak} \end{cases}$

2) $PH^{\mathcal{A}}(\neg\varphi)[e] := f_{\neg}(PH^{\mathcal{A}}(\varphi)[e])$

3) $PH^{\mathcal{A}}(\varphi \square \psi)[e] := f_{\square}(PH^{\mathcal{A}}(\varphi)[e], PH^{\mathcal{A}}(\psi)[e])$ ... $\square \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$

4) $PH^{\mathcal{A}}((\forall x)\varphi)[e] := \min_{m \in A} (PH^{\mathcal{A}}(\varphi)[e(x/m)])$

$PH^{\mathcal{A}}((\exists x)\varphi)[e] := \max_{m \in A} (PH^{\mathcal{A}}(\varphi)[e(x/m)])$

... $e(x/m)$ je ohodnocení vzniklé z $e$ změnou $e(x)$ na $m$

👁 p. hodnota formule závisí pouze na ohodnocení volných proměnných
$\Rightarrow$ p. hodnota sentence nezávisí na ohodnocení vůbec

• Platnost formule ve struktuře

Def: Nechť $\varphi$ je formule v jazyce $L$, $\mathcal{A}$ model $L$ (L-struktura) a $e$ ohodnocení.

1, $\mathcal{A} \models \varphi[e] \equiv PH^{\mathcal{A}}(\varphi)[e] = 1$ ... $\varphi$ platí v $\mathcal{A}$ při ohodnocení $e$
2, $\mathcal{A} \not\models \varphi[e] \equiv PH^{\mathcal{A}}(\varphi)[e] = 0$ ... $\varphi$ neplatí v $\mathcal{A}$ při ohodnocení $e$

→ globálně:
3, $\varphi$ je pravdivá v $\mathcal{A}$, $\mathcal{A} \models \varphi \equiv \forall e$ ohodnocení: $\mathcal{A} \models \varphi[e]$
4, $\varphi$ je lživá v $\mathcal{A} \equiv \forall e$ ohodnocení: $\mathcal{A} \not\models \varphi[e] \Leftrightarrow \mathcal{A} \models \neg\varphi$.

👁 sentence jsou vždy buď lživé nebo pravdivé.

Def: Generální uzávěr formule $\varphi(x_1, \dots x_n)$ (tedy $x_1, \dots x_n$ jsou volné proměnné) je sentence $(\forall x_1) \dots (\forall x_n)\varphi$.

👁 $A \models \varphi \Leftrightarrow A \models (\forall x)\varphi$
tedy děláme nyní pořádjeme aby $\forall m \in A$: $\mathcal{A} \models \varphi[e(x/m)]$
tedy pro volnou $x$: $\forall e$ ohodnocení $\mathcal{A} \models \varphi[e]$
$\Rightarrow$ pro libovolné ohodnocení $e$: $\mathcal{A} \models \varphi[e(x/m)]$

Důsledek: Formule platí ve struktuře $\Leftrightarrow$ tam platí její generální uzávěr.

• Teorie v predikátové logice

Def: Teorie jazyka $L$ je libovolná množina $L$-formulí $T \subseteq M_L$.
Def: Model teorie $T$ je $L$-struktura $\mathcal{A}$, ve které platí všechny axiomy $T$.

$\mathcal{A} \models T \equiv \forall \alpha \in T: \mathcal{A} \models \alpha$

$M_L(T) := \{\mathcal{A} \in M_L \mid \mathcal{A} \models T\}$

Def: Nechť je $T$ teorie v jazyce $L$. $L$-formule $\varphi$ je
1, pravdivá v $T$, $T \models \varphi \equiv M_L(T) \subseteq M_L(\varphi) \Leftrightarrow \forall \mathcal{A} \in M_L(T): \mathcal{A} \models \varphi$.
2, lživá v $T \equiv T \models \neg\varphi \Leftrightarrow M_L(T) \cap M_L(\varphi) = \emptyset$
3, nezávislá v $T \equiv$ není ani lživá ani pravdivá v $T$

Značení: Pokud $\emptyset \models \varphi$, tak píšeme $\models \varphi$ a říkáme, že $\varphi$ platí v logice. → je to tautologie

Def: Spor $\bot = R(x_1, \dots x_n) \wedge \neg R(x_1, \dots x_n)$, kde $R$ je libovolný relační symbol nebo rovnost, pokud daný jazyk neobsahuje žádné relační symboly.

Def: Teorie T je

1) sporná $\equiv T \models \bot$ ... platí v ní spor

<=> v ní platí každá formule

<=> nemá žádný model

2) bezesporná $\equiv$ není sporná <=> má aspoň 1 model

3) kompletní $\equiv$ je bezesporná & každá sentence je v ní buď pravdivá nebo lživá.

! neplatí, že má jediný model

Def: Důsledky teorie T jsou sentence pravdivé v T. Označíme

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

Def: Struktury $\mathcal{A}, \mathcal{B}$ v témže jazyce jsou elementárně ekvivalentní, píšeme $\mathcal{A} \equiv \mathcal{B}$, jestliže v nich platí tytéž sentence.

Teorie je kompletní <=> má právě 1 model až na elementární ekvivalenci

Ukázka: $\langle \mathbb{Q}, \leq \rangle$ a $\langle \mathbb{R}, \leq \rangle$ jsou el. ekvivalentní. Klíčová je hustota uspořádání. Problém by mohla být neúplnost $\mathbb{Q}$, ale úplnost hovoří o vlastnosti všech podmnožin, ale v logice prvního řádu nemohou být proměnné množiny.

Tvrzení: Nechť je T teorie a $\varphi$ sentence. Platí $T \models \varphi \iff T \cup \{\neg\varphi\}$ nemá model.

Dk: $T \cup \{\neg\varphi\}$ nemá model $\iff \neg\varphi$ neplatí v žádném modelu T

$\iff \varphi$ platí v každém modelu T ∎

Ukázka teorie: Teorie grafů $L = \langle E \rangle$ s rovností, axiomy ireflexibility a symetrie

$$T_G = \{\neg E(x,x),\ E(x,y) \to E(y,x)\}$$

→ modely $G = \langle V, E^G \rangle$, kde $E^G$ je libovolná iref. sym. relace

- $x \neq y \to E(x,y)$ platí v G <=> G je úplný.
  ↳ formálně $\neg x = y$

- $(\exists y_1)(\exists y_2)(y_1 \neq y_2 \wedge E(x,y_1) \wedge E(x,y_2) \wedge (\forall z)(E(x,z) \to z = y_1 \vee z = y_2))$
  platí v G <=> ∀ vrchol má stupeň 2

- Teorie uspořádání $L = \langle \leq \rangle$ s r. $T = \{x \leq x,\ x \leq y \wedge y \leq z \to x \leq z,\ x \leq y \wedge y \leq x \to x = y\}$
  - formule $x \leq y \vee y \leq x$ platí <=> model (ČUM) je lineární usp.

• Podstruktury

→ zobecnění podgrupy / vektorového podprostoru / indukovaného podgrafu

→ na podmnožině univerza vyrobíme strukturu, co zdědí všechny relace, funkce a konstanty

Def: Struktura $\mathcal{B} = \langle B, \mathcal{R}^{\mathcal{B}}, \mathcal{F}^{\mathcal{B}} \rangle$ je podstruktura struktury $\mathcal{A} = \langle A, \mathcal{R}^{\mathcal{A}}, \mathcal{F}^{\mathcal{A}} \rangle \equiv$

1) $\emptyset \neq B \subseteq A$ → kdyby $B = \emptyset$, tak $\mathcal{B}$ není struktura

2) $R^{\mathcal{B}} = R^{\mathcal{A}} \cap B^{ar(R)}$ pro $\forall R \in \mathcal{R}$

3) $f^{\mathcal{B}} = f^{\mathcal{A}} \cap (B^{ar(f)} \times B)$ pro $\forall f \in \mathcal{F}$

↳ speciálně pro konstantní $c \in \mathcal{F}$ máme $c^{\mathcal{B}} = c^{\mathcal{A}} \in B$.

Množina $\emptyset \neq B \subseteq A$ je univerzem podstuktury $\Leftrightarrow$ je uzavřená na všechny funkce struktury $\mathcal{A}$ včetně konstant.

$\Rightarrow$ je to restrikce $\mathcal{A}$ na množinu $B$, značíme $\mathcal{A} \restriction B$.

Ukázka: $\langle \mathbb{Z}, +, \cdot, 0 \rangle$ je podstukturou $\langle \mathbb{Q}, +, \cdot, 0 \rangle$, tedy $\underline{\mathbb{Z}} = \underline{\mathbb{Q}} \restriction \mathbb{Z}$

→ také $\underline{\mathbb{N}} = \underline{\mathbb{Z}} \restriction \mathbb{N} = \underline{\mathbb{Q}} \restriction \mathbb{N}$

→ ale $\mathbb{Z}^-$ není doménou žádné podstuktury ∵ není uzavřená na násobení.

Pokud $\mathcal{B} \subseteq \mathcal{A}$, $\varphi$ je otevřená formule ($\otimes$ kvantifikátory) a $e: \mathrm{Var} \to \underline{B}$, potom platí

$\mathcal{B} \models \varphi[e] \Leftrightarrow \mathcal{A} \models \varphi[e]$.

Důsledek: Otevřená formule platí ve struktuře $\mathcal{A} \Leftrightarrow$ platí v každé $\mathcal{B} \subseteq \mathcal{A}$.

Def: Teorie $T$ je otevřená $\equiv$ všechny její axiomy jsou otevřené

Modely otevřené teorie jsou uzavřené na podstuktury, tedy každá podstruktura modelu této teorie je také její model.

Ukázka: Teorie grafů je otevřená - indukovaný podgraf je grafem.

Def: Nechť $\mathcal{A} = \langle A, \mathcal{R}^{\mathcal{A}}, \mathcal{F}^{\mathcal{A}} \rangle$ a $\emptyset \neq X \subseteq A$. Buď $B \subseteq A$ nejmenší podmnožina obsahující $X$, která je uzavřená na všechny funkce $\mathcal{A}$ (tedy i konstanty). Potom podstruktura $\mathcal{A} \restriction B$ je generovaná $X$ a značíme ji $\mathcal{A}(X)$.

Ukázka: $\underline{\mathbb{Q}} = \langle \mathbb{Q}, +, \cdot, 0 \rangle$

$\underline{\mathbb{Q}}(\{1\}) = \underline{\mathbb{N}} = \langle \mathbb{N}, +, \cdot, 0 \rangle$, $\underline{\mathbb{Q}}(\{-1\}) = \underline{\mathbb{Z}}$

## • Expanze a redukt

**Def:** Nechť $L \subseteq L'$ jsou jazyky, $\mathcal{A}$ $L$-struktura a $\mathcal{A}'$ $L'$-struktura na stejné doméně. Je-li interpretace každého symbolu z $L$ stejná v $\mathcal{A}$ i $\mathcal{A}'$, potom:

1) $\mathcal{A}'$ je expanze $\mathcal{A}$ do $L'$ ... $L'$ expanze $\mathcal{A}$
2) $\mathcal{A}$ je redukt $\mathcal{A}'$ na $L$ ... $L$ redukt $\mathcal{A}'$

**Ukázka:** Mějme grupu $\underline{\mathbb{Q}} = \langle \mathbb{Q}, +, -, 0 \rangle$.

- $\langle \mathbb{Q}, + \rangle$ je její redukt
- $\langle \mathbb{Q}, +, -, 0, \cdot, 1 \rangle$ je její expanze na těleso

**Věta (o konstantách):** Nechť $\varphi$ je $L$-formule s volnými proměnnými $x_1, \dots x_n$. Označme jako $L'$ rozšíření $L$ o nové konstantní symboly $c_1, \dots c_n$ a $T'$ stejnou teorii jako $T$, ale v jazyce $L'$. Potom platí

$$T \models \varphi \iff T' \models \varphi(x_1/c_1, \dots x_n/c_n)$$

**Dk:** Stačí pro 1 volnou proměnnou, rozšíření indukcí.

$\Rightarrow$: Nechť $\varphi$ platí v každém modelu $T$. Chceme ukázat, že $\varphi(x/c)$ platí v každém modelu $T'$. Tedy buď $\mathcal{A}'$ model $T'$ a $e': Var \to A'$. Ukážeme $\mathcal{A}' \models \varphi(x/c)[e']$ pro libovolné ohodnocení $e'$.

$\rightarrow$ označme $\mathcal{A}$ redukt $\mathcal{A}'$ na $L$ (zapomeneme konstantu $c$).
zřejmě $\mathcal{A}$ je model $T$, tedy dle předpokladu $\mathcal{A} \models \varphi$, tedy $\mathcal{A} \models \varphi[e]$ pro libovolné $e: Var \to A' \overset{A}{=}$, speciálně i pro $e'(x/c^{\mathcal{A}'})$, kde $x$ ohodnotíme interpretací $c$ v $\mathcal{A}'$ (domény jsou stejné).
$\Rightarrow$ máme $\mathcal{A} \models \varphi[e'(x/c^{\mathcal{A}'})] \Rightarrow \mathcal{A}' \models \varphi(x/c)[e']$

$\Leftarrow$: Nechť $\varphi(x/c)$ platí v každém modelu $T'$. Chceme $\varphi$ platí v každém modelu $T$. Buď $\mathcal{A}$ model $T$ a $e: Var \to A$. Ukážeme $\mathcal{A} \models \varphi[e]$.

$\rightarrow$ označme $\mathcal{A}'$ expanzi $\mathcal{A}$ do $L'$, kde $c$ interpretujeme jako $c^{\mathcal{A}'} = e(x)$.
Dle předpokladu $\mathcal{A}' \models \varphi(x/c)[e]$. Protože v $\mathcal{A}'$ platí $c^{\mathcal{A}'} = e(x)$, tak $\mathcal{A}' \models \varphi[e]$. Formule $\varphi$ neobsahuje $c$, takže máme $\mathcal{A} \models \varphi[e]$. ■

• <u>Extenze teorií</u>

<u>Def</u>: Pro teorii $T$ jazyka $L$ je

1, <u>extenze</u>: $T'$ v jazyce $L' \supseteq L$ splňující $Csq_L(T) \subseteq Csq_{L'}(T')$.

→ extenze je

2, <u>jednoduchá</u> $\equiv L' = L$

3, <u>konzervativní</u> $\equiv Csq_L(T) = Csq_L(T') = Csq_{L'}(T') \cap \text{FORMULE}_L$

<u>Def</u>: Teorie $T$ a $T'$ ve stejném jazyce jsou <u>ekvivalentní</u> $\equiv$

$T'$ je extenze $T$ & $T$ je extenze $T'$.

Pro $T, T'$ ve stejném jazyce:

• $T'$ je extenze $T \iff M_L(T) \supseteq M_L(T')$

• $T'$ je ekvivalentní s $T \iff M_L(T) = M_L(T')$

→ rozšíříme-li jazyk

vektor modelu nezměníme

• výroková l.: přidáváme / zapomínáme hodnoty pro nové výrokové proměnné

• predikátová: děláme expanzi / redukt modelu.

<u>Tvrzení</u>: Nechť $L \subseteq L'$ jsou jazyky, $T$ je $L$-teorie a $T'$ je $L'$-teorie. Potom

(*) 1, $T'$ je extenze $T \iff$ $L$-redukt každého modelu $T'$ je model $T$.

2, $T'$ je konzervativní extenze $T \iff$ to je extenze a každý model $T$ lze expandovat do $L'$ na nějaký model $T'$.

• <u>Extenze o definice</u>

→ přidáme nový symbol, jehož význam popíšeme nějakou definicí

<u>Ukázka</u>: Teorii v jazyce s rovností lze rozšířit o symbol $\neq$ definovaný formulí

$x \neq y \leftrightarrow \neg x = y$

• Teorii uspořádání lze rozšířit o $<$ definovaný formulí $x \leq y \wedge \neg x = y$.

<u>Def</u>: Nechť $T$ je teorie a $\psi(x_1, \dots x_n)$ formule v jazyce $L$. Označíme jako $L'$ rozšíření $L$ o nový $n$-ární relační symbol $R$.

<u>Extenze teorie $T$ o definici $R$ formulí $\psi$</u> je $L'$-teorie

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

Tvrzení: 1, $T'$ je konzervativní extenze $T$
2, pro každou $L'$-formuli $\varphi'$ existuje $L$-formule $\varphi$ t.ž. $T' \models \varphi \Leftrightarrow \varphi'$

Dk: 1, Každý model $T$ lze jednoznačně expandovat na model $T'$
↳ $R$ interpretujeme podle jeho definice
⇒ podle tvrzení (*) je $T'$ konzervativní extenze $T$.

2, Pokud se ve $\varphi'$ nevyskytuje $R$, tak $\varphi := \varphi'$.
Jinak nahradíme atomické podformule tvaru $R(t_1, \dots t_n)$ za $\psi'(x_1/t_1, \dots x_n/t_n)$, kde $\psi'$ je variantou $\psi$ zaručující substituovatelnost všech termů $t_1, \dots t_n$ (všechny vázané proměnné ve $\psi$ přejmenujeme na nové) ■

→ teď přidáme nový funkční symbol
→ vztah $f(x_1, \dots x_n)$ definujeme formulí $\psi(x_1, \dots x_n, y)$
! aby to byla fce, tak pro $\forall x_1, \dots x_n \ \exists! \, y : \psi(x_1, \dots x_n, y)$

Ukázka: Teorie grup: binární funkční symbol $-$ pomocí $+$ a unárního $-$
$x - y = z \Leftrightarrow x + (-y) = z$.

Def: Nechť $T$ je teorie a $\psi(x_1, \dots x_n, y)$ formule v jazyce $L$. Označme jako $L'$ rozšíření $L$ o nový $n$-ární funkční symbol $f$. Nechť platí
i, $T \models (\exists y) \, \psi(x_1 \dots x_n, y)$ → existence
ii, $T \models \psi(x_1, \dots x_n, y) \wedge \psi(x_1, \dots x_n, z) \rightarrow y = z$ → jednoznačnost

Potom extenze teorie $T$ o definici $f$ formulí $\psi$ je $L'$ teorie
$$T' = T \cup \{ f(x_1, \dots x_n) = y \Leftrightarrow \psi(x_1, \dots x_n, y) \}$$

Tvrzení: 1, $T'$ je konzervativní extenzí $T$
2, pro každou $L'$-formuli $\varphi'$ existuje $L$-formule $\varphi$ t.ž. $T' \models \varphi \Leftrightarrow \varphi'$

Dk: 1, modely $T$ lze jednoznačně expandovat na modely $T'$!
2, stačí pro jediný výskyt symbolu $f$, potom indukcí.   proměnná
→ Označme $\varphi^*$ formuli vzniklou z $\varphi'$ nahrazením termu $f(t_1, \dots t_n)$ za novou p. $z$.
$\varphi := (\exists z)(\varphi^* \wedge \psi'(x_1/t_1, \dots x_n/t_n, y/z))$ ... $\psi'$ varianta $\psi$ aby šlo substituovat
→ ukážeme, že pro libovolný model $\mathcal{A} \models T'$ a ohodnocení $e$ platí $\mathcal{A} \models \varphi'[e] \Leftrightarrow \mathcal{A} \models \varphi[e]$.
→ Označme $a_e := (f(t_1, \dots t_n))^{\mathcal{A}}[e]$. Díky jednozn: $\mathcal{A} \models \psi'(x_1/t_1, \dots x_n/t_n, y/z)[e] \Leftrightarrow e(z) = a$.
⇒ $\mathcal{A} \models \varphi'[e] \Leftrightarrow \mathcal{A} \models \varphi^*[e(z/a)] \Leftrightarrow \mathcal{A} \models \varphi[e]$. ■

- Definice konstantního symbolu
  - → speciální případ: funkce arity 0
  - → extenze o definici konstantního symbolu $c$ formulí $\psi(y)$

$$T' = T \cup \{c = y \leftrightarrow \psi(y)\}$$

musí platit $T \models (\exists y)\psi(y)$ a $T \models \psi(y) \wedge \psi(z) \rightarrow y = z$.

Ukázka: Teorie aritmetiky: $1 = y \leftrightarrow y = S(0)$

- Teorie těles, symbol $\frac{1}{2}$: $\frac{1}{2} = y \leftrightarrow y \cdot (1+1) = 1$.

! není extenze o definici, neplatí existence v tělese char. 2 → tělesa $\mathbb{Z}_2$

→ ale v tělesech s char > 2 už to funguje

- Extenze teorie o definice

Def: $L'$-teorie $T'$ je extenzí $L$-teorie $T$ o definice ≡
vznikla postupnou extenzí o definice relačních a funkčních symbolů.

Tvrzení: 1) $T'$ je konzervativní extenze $\qquad 1 \Leftrightarrow 2$

2) každý model $T$ lze jednoznačně expandovat na model $T'$

3) pro $L'$-formuli $\varphi'$ existuje $L$-formule $\varphi$, t.ž. $T' \models \varphi \leftrightarrow \varphi'$.

Dk: indukcí.

- Definovatelnost ve struktuře

Def: Nechť $\varphi(x_1, \dots x_n)$ je formule a $\mathcal{A}$ struktura ve stejném jazyce.
Množina definovaná formulí $\varphi(x_1, \dots x_n)$ ve struktuře $\mathcal{A}$ je

$$\varphi^{\mathcal{A}}(x_1, \dots x_n) := \{(a_1, \dots a_n) \in A^n \mid \mathcal{A} \models \varphi(x_1/a_1, \dots x_n/a_n)\}$$

→ zkráceně $\varphi^{\mathcal{A}}(\underline{x}) := \{\underline{a} \in A^n \mid \mathcal{A} \models \varphi(\underline{x}/\underline{a})\}$.

Ukázka:

- $\neg(\exists y) E(x, y)$ definuje v daném grafu množinu všech izolovaných vrcholů.
- $(\exists y)(y \cdot y = x) \wedge (x \neq 0)$ definuje v tělese $\underline{\mathbb{R}}$ množinu $\mathbb{R}^+$

**Def:** Nechť $\varphi(\underline{x}, y)$ (kde $|\underline{x}| = n$, $|y| = k$) je $L$-formule, $\mathcal{A}$ $L$-struktura a $\underline{b} \in A^k$.

<u>Množina definovaná formulí $\varphi(\underline{x}, y)$ s parametry</u> $\underline{b}$ ve struktuře $\mathcal{A}$ je

$$\varphi^{\mathcal{A}, \underline{b}} := \{ \underline{a} \in A^n \mid \mathcal{A} \models \varphi(\underline{x}/\underline{a}, y/\underline{b}) \}$$

→ pro $B \subseteq A$ označíme $Df^n(\mathcal{A}, B)$ množinu všech množin definovatelných v $\mathcal{A}$ s parametry pocházejícími z $B$.

$Df^n(\mathcal{A}, B)$ je uzavřená na doplněk, průnik, sjednocení a obsahuje $\emptyset$ a $A^n$.

$\Rightarrow$ je to podstruktura potenční algebry $\langle \mathcal{P}(A^n), \overline{\phantom{x}}, \cap, \cup, \emptyset, A^n \rangle$

<u>Ukázka</u>: $\varphi(x, y) = E(x, y)$ a $v \in V(G)$. $\Rightarrow$ $\varphi^{G, v} = \{ a \in V(G) \mid \mathcal{G} \models E(a, v) \}$

↳ sousedi vrcholu $v$.

## • Tablo metoda v predikátové logice – ZATÍM JAZYK BEZ =

Ukázka: $\varphi = (\exists x)\neg P(x) \rightarrow \neg(\forall x)P(x)$  $\psi = \neg(\forall x)P(x) \rightarrow (\exists x)\neg P(x)$

$F\,(\exists x)\neg P(x) \rightarrow \neg(\forall x)P(x)$
|
$T\,(\exists x)\neg P(x)$ ← svědek
|
$F\,\neg(\forall x)P(x)$
|
$T\,(\forall x)P(x)$ ← všichni
|
$T\,\neg P(c_0)$ ← substituce konstantního termu
|
$F\,P(c_0)$
|
$T\,(\forall x)P(x)$
|
$T\,P(c_0)$

⇓
jazyk rozšíříme o nové konstantní symboly

$F\,\neg(\forall x)P(x) \rightarrow (\exists x)\neg P(x)$
|
$T\,\neg(\forall x)P(x)$
|
$F\,(\exists x)\neg P(x)$ ← všichni
|
$F\,(\forall x)P(x)$ ← svědek
|
$F\,P(c_0)$
|
$F\,(\exists x)\neg P(x)$
|
$F\,\neg P(c_0)$
|
$T\,P(c_0)$
⊗

- $T(\exists x)\varphi(x)$, $F(\forall x)\varphi(x)$ → svědek ⇒ nová konstanta $c_i$ na větvi ještě není
- $T(\forall x)\varphi(x)$, $F(\exists x)\varphi(x)$ → všichni ⇒ libovolný konstantní term

  ↳ bezesporná větev je dokončená jen po dosazení všech termů do „všichni"

  ↳ musíme použít vše co víme

Konvence: kořeny atomických tabel nekreslíme kromě položek typu „všichni"
↳ po 1 dosazení ještě nejsme hotovi

→ spočetně mnoho axiomů, spočetně konstantních termů

Def: Nechť $L$ je spočetný jazyk bez rovnosti. Označme jako $L_C$ rozšíření $L$ o spočetně mnoho nových pomocných konstantních symbolů. $C = \{c_i \mid i \in \mathbb{N}\}$
→ konstantních termů v $L_C$ je jen spočetně mnoho → očíslujeme je $\{t_i \mid i \in \mathbb{N}\}$

Def: směrem k tablu:

- položka = nápis $T\varphi$ nebo $F\varphi$, kde $\varphi$ je $L_C$-sentence

  → $T(\exists x)\varphi(x)$ a $F(\forall x)\varphi(x)$ ... svědek

  → $F(\exists x)\varphi(x)$ a $T(\forall x)\varphi(x)$ ... všichni

- atomická tabla pro logické spojky jsou stejná jako ve výrokové logice

| $T(\forall x)\varphi(x)$ | $F(\exists x)\varphi(x)$ | $T(\exists x)\varphi(x)$ | $F(\forall x)\varphi(x)$ |
|---|---|---|---|
| \| | \| | \| | \| |
| $T\varphi(x/t_i)$ | $F\varphi(x/t_i)$ | $T\varphi(x/c_i)$ | $F\varphi(x/c_i)$ |

$t_i$ jakýkoli term    $c_i$ nový konstantní symbol

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

1, jednoprvkový strom s libovolnou položkou je tablo z teorie T

2, pro libovolnou položku P na libovolné větvi V můžeme na konec větve V připojit atomické tablo pro P

- je-li P typu svědek → pouze $c_i \in C$, který na V dosud není použitý
- je-li P typu všichni → jakýkoli konstantní $L_C$-term $t_i$

3, na konec libovolné větve můžeme připojit položku $T\alpha$ pro axiom $\alpha \in T$

Def: Tablo z teorie T je konečné, nebo i nekonečné. V tom případě je spočetné a definujeme ho jako

$\tau = \bigcup_{i \geq 0} \tau_i$ , kde $\tau_0$ je jednoprvkové tablo
$\tau_{i+1}$ vzniklo z $\tau_i$ v jednom kroku

→ tablo pro položku P má v kořeni položku P

Def: Tablo je sporné ≡ ∀ jeho větev je sporná
Větev je sporná ≡ obsahuje položky $T\varphi$ a $F\varphi$ pro nějakou sentenci $\varphi$

Def: Tablo je dokončené ≡ ∀ jeho větev je dokončená
Větev je dokončená ≡ je sporná nebo
1, každá její položka je na této větvi redukovaná a
2, obsahuje položku $T\alpha$ pro každý axiom $\alpha \in T$

Def: Položka P je redukovaná na větvi V procházející P (=obsahující) ≡ platí něco z následujícího
1, je tvaru $T\varphi$ nebo $F\varphi$ pro atomickou sentenci → tedy $R(t_1, \dots t_n)$ ← konst. $L_C$ termy
2, není typu všichni a vyskytuje se na V jako kořen atomického tabla
⇒ už došlo k jejímu rozvoji
3, je typu všichni a všechny její výskyty na větvi V jsou na V redukované

Def: Výskyt položky P typu všichni na větvi V je i-tý (=právě) ≡ má i-1 předků s labelem P.
→ i-tý výskyt je redukovaný na V ≡
- P má (i+1)-ní výskyt na V a
- na V je položka $T\varphi(x/t_i)$ pro $P = T(\forall x)\varphi(x)$ resp. $F\varphi(x/t_i)$ pro $P = F(\exists x)\varphi(x)$
← i-tý konstantní $L_C$-term

⇒ 'všichni' je redukovaná ⟺ má na V nekonečně výskytů a dosadili jsme do ní všechny $t_i$

→ jazyk bez rovnosti

Def: Tablo důkaz sentence $\varphi$ z teorie $T$ je sporné tablo z $T$ s položkou $F\varphi$ v kořeni

→ pokud existuje, je $\varphi$ (tablo) dokazatelný z $T$, píšeme $T \vdash \varphi$

Tablo zamítnutí je sporné tablo s $T\varphi$ v kořeni ... platí $T \vdash \neg\varphi$

• Konečnost a systematičnost důkazů

→ podobně jako ve výrokové logice uděláme systematické tablo

Def: systematické tablo z $T = \{\alpha_0, \alpha_1, \dots\}$ pro položku $R$ je $\tau = \bigcup_{i \geq 0} \tau_i$, kde $\tau_0$ je jednoprvkové s položkou $R$ a pro $i \geq 0$:

1) buď $P$ nejlevější položka v co nejmenší úrovni, která ještě není redukovaná na nějaké bezesporné větvi procházející $P$. — pro typ všichni znamená její výskyt redukovaný

2) definujeme $\tau_i'$ vzniklé z $\tau_i$ připojením atomického tabla pro $P$ na ∀ bezespornou větev procházející $P$, kde $P$ není redukovaná.

- je-li $P$ typu všichni: nechť má v daném vrcholu $k$-tý výskyt, potom dosadíme $k$-tý $L_C$-term $t_k$
- je-li $P$ typu svědek: dosadíme $c_k \in C$ pro nejmenší $k$, co na této větvi ještě není

→ pokud taková položka neexistuje: $\tau_i' = \tau_i$

3) $\tau_{i+1}$ vznikne z $\tau_i'$ připojením $T\alpha_{i+1}$ na všechny bezesporné větve.

→ pokud jsme již použili všechny axiomy: $\tau_{i+1} := \tau_i'$

Lemma: Systematické tablo je dokončené.

Dk: $k$-tý výskyt 'všichni' redukujeme když na něj narazíme

→ připojíme $(k+1)$-ní výskyt ... atomické tablo

→ dosadíme $k$-tý $L_C$-term

→ zbytek jako výroková logika: jsou všechny větve dokončené?

- sporné ✓
- jinak obsahují $T\alpha_i$ ✓

a všechny položky redukované v nějakém kroku $\sim 2^h$. ∎

→ teď všechny důkazy jako ve výrokové logice

VĚDY

Věta (o konečnosti sporu): Neprodlužujeme-li sporné větve, je sporné tablo konečné.

Důsledek (konečnost důkazu): Pokud $T \vdash \varphi$, potom $\exists$ konečný tablo důkaz $\varphi$ z $T$.

Důsledek (Systematičnost důkazu): Pokud $T \vdash \varphi$, potom systematické tablo je konečným důkazem $\varphi$ z $T$.

• Tablo metoda v jazyce s rovností

→ tablo je syntaktický objekt - velký nápis - ale '=' je identita prvků nějakého konkrétního modelu.

⇒ budeme se k $=^{a}$ chovat jako k nějakému relačnímu symbolu z $R$ struktury $a$

⇒ musíme přidat axiomy rovnosti, aby:

$c_1 = c_2 \rightarrow c_2 = c_1$
$f(c_1) = f(c_2)$
$c_1 \in P \leftrightarrow c_2 \in P$ ... $p$ je unární relační

} teď je $=$ kongruence na $a$

→ ale chceme, aby to byla identita, tedy $a = b \iff a, b$ jsou stejný prvek domény

⇒ uděláme unifikaci všech $=$ ekvivalentních prvků do jediného prvku

↳ faktorstruktura podle kongruence $=$ transitivita, symetrii

→ zajistí reflexivita,

Def: Nechť $\sim$ je ekvivalence na množině $A$, $f: A^n \rightarrow A$ funkce a $R \subseteq A^n$ relace.

• $\sim$ je kongruence pro $f \equiv \forall \underline{a}, \underline{b} \in A^n: (\forall i: a_i \sim b_i) \Rightarrow f(\underline{a}) = f(\underline{b})$.

• $\sim$ je kongruence pro $R \equiv \forall \underline{a}, \underline{b} \in A^n: (\forall i: a_i \sim b_i) \Rightarrow R(\underline{a}) \iff R(\underline{b})$

Def: Kongruence struktury $a$ je ekvivalence na $A$, co je kongruencí pro všechny fce a relace $a$.

Def: Nechť $a$ je struktura a $\sim$ její kongruence. Faktorstruktura $a$ podle $\sim$ je struktura $a/\sim$ v témže jazyce. Doména je množina ekvivalenčních tříd $A$ podle $\sim$, tedy $A/\sim$. Funkce a relace definujeme jako

• $f^{a/\sim}([a_1]_\sim, \dots [a_n]_\sim) := [f^{a}(a_1, \dots a_n)]_\sim$

• $R^{a/\sim}([a_1]_\sim, \dots [a_n]_\sim) \equiv R^{a}(a_1, \dots a_n)$

**Def:** Axiomy rovnosti pro jazyk $L$ s rovností jsou:

i) $x = x$

ii) pro každý n-ární funkční symbol $f$ jazyka $L$:

$$x_1 = y_1 \wedge x_2 = y_2 \wedge \dots \wedge x_n = y_n \rightarrow f(x_1, \dots x_n) = f(y_1, \dots y_n)$$

iii) pro každý n-ární relační symbol $R$ jazyka $L$ včetně rovnosti:

$$x_1 = y_1 \wedge x_2 = y_2 \wedge \dots \wedge x_n = y_n \rightarrow (R(x_1, \dots x_n) \rightarrow R(y_1, \dots y_n))$$

→ respektive jejich generální uzávěry – značení

pokud teorie $T$ obsahuje axiomy rovnosti a $\mathcal{A}$ je její model:

$=^{\mathcal{A}}$ je ekvivalence ... reflexivita z (i) a sym + tranz. ze (iii)

$$\forall x_1 x_2 y_1 y_2 : x_1 = y_1 \wedge x_2 = y_2 \rightarrow (x_1 = x_2 \rightarrow y_1 = y_2)$$

$$\Rightarrow x = y \wedge x = x \rightarrow (x = x \rightarrow y = x) \sim x = y \rightarrow y = x$$

$$\Rightarrow y = x \wedge y = z \rightarrow (y = y \rightarrow x = z) \sim x = y \wedge y = z \rightarrow x = z$$

$=^{\mathcal{A}}$ je kongruence ... díky (ii) a (iii)

**Def:** Nechť $T$ je teorie v jazyce $L$ s rovností. Označme jako $T^*$ rozšíření $T$ o generální uzávěry axiomů rovnosti pro $L$.

- Tablo důkaz z teorie $T$ je tablo důkaz z $T^*$ → podobně zamítnutí...

$\mathcal{A} \models T^* \Rightarrow \mathcal{A}/{=^{a}} \models T^*$ a v $\mathcal{A}/{=^{a}}$ je symbol $=$ interpretován jako identita

v každém modelu, kde je $=$ interpretován jako identita platí axiomy rovnosti

- Korektnost a úplnost tablo metody v predikátové logice

**Věta (o korektnosti):** Je-li sentence $\varphi$ tablo dokazatelná z $T$, potom je pravdivá v $T$

$$T \vdash \varphi \Rightarrow T \models \varphi$$

**Myšlenka důkazu:** Sporem: protipříklad by se po vhodné interpretaci shodoval s některou větví, ale ty jsou sporné.

**Věta (o úplnosti):** Je-li sentence $\varphi$ pravdivá v $T$, potom je tablo dokazatelná z $T$.

$$T \models \varphi \rightarrow T \vdash \varphi$$

**Myšlenka:** Ukážeme, že libovolné dokončené (např. systematické) tablo z $T$ s $F\varphi$ v kořeni je nutně sporné.

**Důsledek:** Dokazatelnost = platnost

- Kanonický model

→ opět bezesporná dokončená větev tabla pro položku $F\varphi$ vrací model $\neg\varphi$.

→ jaká bude jeho doména? trik: ze syntaktických objektů uděláme sémantické

Def: Nechť $L = \langle \mathcal{R}, \mathcal{F} \rangle$ je jazyk bez rovnosti. Pro bezespornou dokončenou větev $V$ definujeme kanonický model jako $L_C$-strukturu $\mathcal{A} := \langle A, \mathcal{R}^{\mathcal{A}}, \mathcal{F}^{\mathcal{A}} \cup C^{\mathcal{A}} \rangle$, kde

- $A$ je množina všech konstantních $L_C$-termů – takže to jsou nápisy
- pro $n$-ární relační symbol $R \in \mathcal{R}$ a "$s_1$", ... "$s_n$" $\in A$:

  ("$s_1$", ... "$s_n$") $\in R^{\mathcal{A}}$ $\equiv$ na $V$ je položka $T R(s_1, \dots s_n)$
- pro $n$-ární funkční symbol $f \in \mathcal{F}$ a "$s_1$", ... "$s_n$" $\in A$:

  $f^{\mathcal{A}}$("$s_1$", ... "$s_n$") := "$f(s_1, \dots s_n)$"
- speciálně: pro konstantní symbol $c$ máme $c^{\mathcal{A}}$ = "$c$".

Ukázka: $T = \{(\forall x) R(f(x))\}$, $L = \langle R, f, d \rangle$ bez rovnosti – $d$ je konstantní

$\varphi = \neg R(d)$ ... platí $T \models \varphi$?

$F \neg R(d)$
|
$T R(d)$
|
• $T (\forall x) R(f(x))$
|
$T R(f(d))$
|
• $T (\forall x) R(f(x))$
|
$T R(f(f(d)))$
|
• $T (\forall x) R(f(x))$
|
$T R(f(c_0))$
|
• $T (\forall x) R(f(x))$
|
$T R(f(c_1))$
|
⋮

$L_C = \langle R, f, d, c_0, c_1, \dots \rangle$

→ tablo se nikdy nerozvětví a nikdy nedojde ke sporu

⇒ platí $T \not\models \varphi$ ⇒ $\exists$ model, kde $\varphi$ neplatí

$A := \{$ "$d$", "$c_0$", "$c_1$", ...
"$f(d)$", "$f(c_0)$", "$f(c_1)$", ...
"$f(f(d))$", "$f(f(c_0))$", "$f(f(c_1))$", ...
⋱ $\}$

$d^{\mathcal{A}}$ := "$d$"

$c_i^{\mathcal{A}}$ := "$c_i$"

$f^{\mathcal{A}}$("$d$") := "$f(d)$", $f^{\mathcal{A}}$("$f(d)$") := "$f(f(d))$"

$R^{\mathcal{A}} = A \setminus C = \{$"$d$", "$f(d)$", "$f(c_0)$", ... $\}$ → ale "$c_i$" $\notin R^{\mathcal{A}}$

⇒ kanonický model: $L_C$ struktura $\mathcal{A} = \langle A, R^{\mathcal{A}}, f^{\mathcal{A}}, d^{\mathcal{A}}, c_0^{\mathcal{A}}, c_1^{\mathcal{A}}, \dots \rangle$

→ redukt na původní jazyk $L$: $\mathcal{A}' = \langle A, R^{\mathcal{A}}, f^{\mathcal{A}}, d^{\mathcal{A}} \rangle$

• Kanonický model v jazyce s rovností

Def: Pro jazyk $L$ s rovností:

→ tablo je nyní z teorie $T^*$ s axiomy rovnosti

1. vezmeme kanonický model $\mathcal{B}$ pro $V$ jako by byl $L$ bez rovnosti

↳ symbol $=$ interpretujeme jako obyčejnou binární relaci

⇒ relaci $=^{\mathcal{B}}$ definujeme stejně jako pro ostatní relační symboly:

$$\text{"}s_1\text{"} =^{\mathcal{B}} \text{"}s_2\text{"} \equiv \text{na } V \text{ je položka } T\, s_1 = s_2$$

2. Kanonický model pro $V$ je faktorstruktura $\mathcal{A} := \mathcal{B} /_{=^{\mathcal{B}}}$.

pro libovolnou $L_C$ formuli $\varphi$ platí $\mathcal{B} \models \varphi \iff \mathcal{A} \models \varphi$

- pro $\mathcal{B}$ interpretujeme '=' jako $=^{\mathcal{B}}$
- pro $\mathcal{A}$ interpretujeme '=' jako identitu prvků.

v jazyce bez rovnosti je kanonický model vždy spočetně nekonečný

~ jazyce s rovností může být i konečný

Ukázka: $T = \{(\forall x)\, R(f(x))\}$, $L = \langle R, f, d\rangle$, s rovností

$\varphi = \neg R(d)$

$F \neg R(d)$ $\quad L_C = \langle R, f, d, c_0, c_1, \dots\rangle$ s rovností

|

$T\, R(d)$ $\quad$ → sestrojíme kanonický model, jako by $L$ byl bez rovnosti

|

⋮ $\qquad \mathcal{B} = \langle B, R^{\mathcal{B}}, f^{\mathcal{B}}, d^{\mathcal{B}}, c_0^{\mathcal{B}}, c_1^{\mathcal{B}}, \dots\rangle$

tablo pro $T^*$ → včetně axiomů pro rovnost

→ '=' jako obyčejný symbol

⇒ kanonický model $\mathcal{A} = \langle A, R^{\mathcal{A}}, f^{\mathcal{A}}, d^{\mathcal{A}}, c_0^{\mathcal{A}}, c_1^{\mathcal{A}}, \dots\rangle$

- $A = B /_{=^{\mathcal{B}}}$
- $R^{\mathcal{A}}([s_i]_{\sim}) \equiv R^{\mathcal{B}}(s_i) \implies R^{\mathcal{A}} = B /_{=^{\mathcal{B}}} = A$
- $d^{\mathcal{A}} = [\text{"}d\text{"}]_{=^{\mathcal{B}}}$
- $c_i^{\mathcal{A}} = [\text{"}c_i\text{"}]_{=^{\mathcal{B}}}$
- $f^{\mathcal{A}}([\text{"}d\text{"}]_{=^{\mathcal{B}}}) = [\text{"}f(d)\text{"}]_{=^{\mathcal{B}}}$

  $f^{\mathcal{A}}([\text{"}f(d)\text{"}]_{=^{\mathcal{B}}}) = [\text{"}f(f(d))\text{"}]_{=^{\mathcal{B}}}$

## • Löwenheim-Skolemova věta a věta o kompaktnosti

<u>Věta</u> (<u>Löwenheim-Skolemova</u>): Je-li $L$ spočetný jazyk bez rovnosti, potom každá bezesporná $L$-teorie má spočetně nekonečný model.

<u>Dk</u>: V $T$ není dokazatelný spor, takže tablo z $T$ s $F\bot$ v kořeni musí mít bezespornou větev. Hledaný model je $L$-redukt kanonického modelu pro tuto větev. ■

<u>Poznámka</u>: Později dokážeme něco silnějšího pro jazyky s rovností.

<u>Věta</u> (<u>o kompaktnosti</u>): Teorie má model $\Leftrightarrow$ $\forall$ její konečná část má model.

<u>Dk</u>: Stejný jako ve výrokové logice. $\Rightarrow$: zřejmě platí

$\Leftarrow$: pro spor nechť $T$ je sporná, tedy $T \vdash \bot$ $\qquad T' \vdash \bot$ ↯

↳ vezmeme konečný tablo důkaz $\bot$ z $T$.

$\Rightarrow$ obsahuje jen konečně mnoho axiomů $T$ $\Rightarrow$ tvoří konečnou $T' \subseteq T$ ■

## • Nestandardní model přirozených čísel

→ aplikace věty o kompaktnosti

$\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$ ... standardní model

$\Rightarrow$ $Th(\underline{\mathbb{N}}) :=$ množina všech sentencí pravdivých v $\underline{\mathbb{N}}$

→ $n$-tý <u>numerál</u> je term $\underline{n} := (\underbrace{S \circ S \circ \ldots \circ S}_{n})(0)$

$\Rightarrow$ přidáme nový konstantní symbol $C$, větší než každý numerál

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

$\forall$ <u>konečná</u> část $T$ má model

$\Rightarrow$ $T$ má model ... z věty o kompaktnosti

↳ <u>nestandardní model přirozených čísel</u>

↳ platí v něm tytéž sentence jako v $\underline{\mathbb{N}}$

ale navíc obsahuje konstantu větší než $\forall n \in \mathbb{N}$

## • Rezoluce v predikátové logice

→ opět důkaz sporem $S \vdash_R \square$ ... ale co je CNF?

$T \models \varphi$? ⇝ $T \cup \{\neg\varphi\} =: S$ ⇝ ukážeme $S \vdash_R \square \Rightarrow T \models \varphi$.

↑ sentence

Def: Literál je atomická formule $R(t_1, \dots t_n)$ nebo její negace.

Klauzule je konečná množina literálů.

CNF formule je množina klauzulí. – klidně ∞

$\vee, \wedge, \neg$ jsou minimální

👁 otevřenou formuli (bez kvantifikátorů) je vždy možné převést do CNF

👁 pokud je na začátku $(\forall x)$, tak to tam jde ∵ $\varphi \sim$ generální uzávěr $\varphi$

$$(\forall x)(P(x) \vee \neg Q(x)) \sim P(x) \vee \neg Q(x) \rightsquigarrow \{P(x), \neg Q(x)\}$$

• pro existenční kv. zavedeme nové svědky

$$(\exists x)(P(x) \vee \neg Q(x)) \rightsquigarrow \{P(C), \neg Q(C)\} \quad \dots \text{skolemizace}$$

↳ není ekvivalentní, ale zachovává (ne)splnitelnost

• rezoluční krok

$$\{P(x), \neg Q(x)\}, \{Q(f(c))\} \rightsquigarrow \{P(f(c))\}$$

↳ uděláme substituci $x/f(c)$ ... unifikace

Ukázka:

• $T = \{(\forall x)P(x), (\forall x)(P(x) \to Q(x))\}$, $\varphi = (\exists x)Q(x)$

→ $\neg\varphi = \neg(\exists x)Q(x) \sim (\forall x)\neg Q(x) \rightsquigarrow \{\neg Q(x)\}$

$T \cup \{\neg\varphi\} \sim S = \{\{P(x)\}, \{\neg P(x), Q(x)\}, \{\neg Q(x)\}\}$

👁 na $P(x)$ se můžu dívat jako $p$, $Q(x)$ jako $q$

⇒ $S = \{\{p\}, \{\neg p, q\}, \{\neg q\}\}$ ← grounding

$q$ — $\square$ → řešení jako ve výrokové logice

• $T = \{(\forall x)(\exists y)R(x,y), R(x,y) \to Q(x)\}$, $\varphi = (\exists x)Q(x)$  $\neg\varphi \sim (\forall x)\neg Q(x) \sim \neg Q(x)$

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

↳ nahradíme za $R(x, f(x))$, kde $f$ je nový funkční symbol, reprezentuje výběr svědka

→ $S = \{\{R(x, f(x))\}, \{\neg R(x,y), Q(x)\}, \{\neg Q(x)\}\}$ → pole obě nesplnitelné

↳ není ekvivalentní $T \cup \{\neg\varphi\}$, ale je ekvisplnitelná

→ unifikace $y/f(x)$ : $\{R(x, f(x))\}$ a $\{\neg R(x,y), Q(x)\}$ ⇝ $\{Q(x)\}$ → $\square$
$\{\neg Q(x)\}$ ↗

**!** ale tedy grounding nefunguje
$\{\{r\}, \{\neg p, q\}, \{\neg q\}\}$ není splnitelná

⇒ musíme vyřešit, že $R(x, f(x))$ a $R(x,y)$ mají podobnou strukturu

- <u>Skolemizace</u>

<u>Def</u>: L-teorie T a L'-teorie T' jsou ekvisplnitelné ≡ T má model ⟺ T' má model.

→ pro převod do CNF potřebujeme otevřené formule

⇒ <u>cíl</u>: Ke každé teorii T sestrojíme ekvisplnitelnou, otevřenou teorii T'!
1. axiomy T převedeme do PNF ... vytknutí kvantifikátorů
2. nahradíme generálními uzávěry ⇒ sentence
3. sentence nahradíme Skolemovými variantami ... odstranění ∃
4. odstraníme zbývající ∀ ⇒ otevřené formule

- <u>Prenexní normální forma</u> – PNF

<u>Def</u>: Formule φ je v <u>PNF</u> ≡ je tvaru $\underbrace{(Q_1 x_1) \cdots (Q_n x_n)}_{\text{kvantif. prefix}} \underbrace{\varphi'}_{\text{otevřené jádro}}$, $Q_i \in \{\forall, \exists\}$, φ' otevřená

- univerzální formule: PNF & všechny kvant. jsou ∀

<u>Tvrzení</u>: Ke každé formuli φ existuje ekvivalentní formule v PNF.
<u>Dk</u>: Nahrazujeme podformule ekvivalentními a posouváme kvantifikátory blíž ke kořeni Tree(φ), dle pravidel z následujícího lemmatu. ■

<u>Důsledek</u>: Existuje i ekvivalentní PNF sentence (uzávěr).

<u>Lemma</u>: Označme $\overline{Q}$ opačný kvantifikátor ke Q. Pro formule φ, ψ, <u>kde x není volná</u>:

$\neg(Qx)\varphi \sim (\overline{Q}x)\neg\varphi$ $\qquad (Qx)\varphi \to \psi \sim (\overline{Q}x)(\varphi \to \psi)$
$(Qx)\varphi \wedge \psi \sim (Qx)(\varphi \wedge \psi)$ $\qquad \varphi \to (Qx)\psi \sim (Qx)(\varphi \to \psi)$
$(Qx)\varphi \vee \psi \sim (Qx)(\varphi \vee \psi)$

<u>Dk</u>: Třeba tablo metodou. Konkrétně: $(Qx)\varphi \to \psi \sim \neg(Qx)\varphi \vee \psi \sim (\overline{Q}x)\neg\varphi \vee \psi$
$\sim (\overline{Q}x)(\neg\varphi \vee \psi) \sim (\overline{Q}x)(\varphi \to \psi)$ ■

x ~~má~~ nemá být volná ve ψ aby to bylo ekvivalentní
$((\exists x)\, x=2) \wedge x=4 \not\sim (\exists x)(x=2 \wedge x=4)$ | $(\exists y)\, y=2 \wedge x=4 \sim (\exists y)(y=2 \wedge x=4)$
↳ přejmenuju to na y

Ukázka: převod do PNF

→ volná

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

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

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

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

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

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

PNF není jednoznačná, je lepší vytknout nejprve $\exists$:

$(\exists y)(\forall x)\varphi$ je lepší než $(\forall x)(\exists y)\varphi$

↳ $y$ nezávisí na $x$ ↳ $y$ závisí na $x$

- **Skolemova varianta**

- pokud je PNF sentence univerzální, tedy $(\forall x_1)\dots(\forall x_n)\psi$, tak hledaná ekvisplnitelná otevřená formule je $\psi$.

→ jinak musíme provést skolemizaci = odstranění $\exists$

Def: Nechť $\varphi$ je $L$-sentence v PNF, všechny vázané proměnné různé. Nechť

1) existenční kvantifikátory jsou $(\exists y_1)\dots(\exists y_n)$
2) pro každé $i$ jsou $(\forall x_1)\dots(\forall x_{n_i})$ univerzální kv. předcházející $(\exists y_i)$.

⇒ označme jako $L'$ rozšíření $L$ o nové funkční symboly $f_1,\dots f_n$, kde $f_i$ má aritu $n_i$.

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

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

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

Věta (Skolemova): Každá teorie má otevřenou konzervativní extenzi.

Tvrzení: Sentence $\varphi$ a její s.v. $\varphi_S$ jsou ekvisplnitelné.

Důsledek: Ke každé teorii můžeme skolemizací najít ekvisplnitelnou otevřenou teorii, kterou už snadno převedeme do CNF.

# • Grounding a Herbrandova věta

→ když máme otevřenou nesplnitelnou teorii, tak její nesplnitelnost lze dokázat pomocí konkrétních prvků

**Def:** Nechť $\varphi(x_1, \dots x_n)$ je otevřená formule. Řekneme, že <u>instance</u> $\varphi(x_1/t_1, \dots x_n/t_n)$ je <u>základní</u> (ground) ≡ termy $t_1, \dots t_n$ jsou konstantní

**Def:** Nechť $L = \langle R, F \rangle$ je jazyk s aspoň jedním konstantním symbolem. L-struktura $\mathcal{A} = \langle A, R^{\mathcal{A}}, F^{\mathcal{A}} \rangle$ je <u>Herbrandův model</u> ≡

tohle často jako kanonický model

- $A$ je množina všech konstantních L-termů ... <u>Herbrandovo univerzum</u>
- pro $f \in F$ arity $n$ a "$t_1$", ... "$t_n$" $\in A$: → nápisy

  $f^{\mathcal{A}}(\text{"}t_1\text{"}, \dots \text{"}t_n\text{"}) = \text{"}f(t_1, \dots t_n)\text{"}$
- na relační symboly neklademe podmínky

**Věta (<u>Herbrandova</u>):** Je-li $T$ otevřená, v jazyce bez rovnosti a s aspoň jedním konstantním symbolem, potom:

- buď má $T$ Herbrandův model ⇒ je splnitelná
- nebo existuje konečně mnoho základních instancí axiomů $T$, jejichž konjunkce je nesplnitelná

  ⇒ $T$ je nesplnitelná

**Důsledek:** Nesplnitelnost $T$ lze dokázat na konkrétních prvcích.

**Ukázka:** $T = \{P(x,y) \vee R(x,y), \neg P(c,y), \neg R(x, f(x))\}$

→ substituujeme konstantní termy $x/c$ a $y/f(c)$

⇒ $\{P(c, f(c)) \vee R(c, f(c)), \neg P(c, f(c)), \neg R(c, f(c))\}$

$R(c, f(c))$ —— $\square$

→ když tyto základní instance axiomů chápeme jako prvýroky $\{p \vee r, \neg p, \neg r\}$, tak to umíme zamítnout výrokovou rezolucí

**Důsledek:** Je-li $T$ otevřená v jazyce bez rovnosti s konstantním symbolem, potom má $T$ model ⟺ má model $T_{ground} := \{\varphi \mid \varphi \text{ je zákl. instance } \alpha \in T\}$

**Dk:** ⇒: V modelu $T$ platí i všechny základní instance axiomů → je to model $T_{ground}$.

⇐: Pro spor nechť $T$ nemá model. Potom je podle H. věty nějaká konečná $T' \subseteq T_{ground}$ nesplnitelná, tedy $T_{ground}$ je taky nesplnitelná ↯ ∎

• __Unifikace:__

→ místo všech základních instancí použijeme nějaké vhodné substituce

__Ukázka:__ $\{P(x), Q(x,z)\}$ a $\{\neg P(y), \neg Q(f(y), y)\}$

1) $\{x/f(a), y/a, z/a\}$ : $\{P(f(a)), Q(f(a), a)\}$ a $\{\neg P(a), \neg Q(f(a), a)\}$
$\Rightarrow \{P(f(a)), \neg P(a)\}$

2) $\{x/f(z), y/z\}$: $\{P(f(z)), Q(f(z), z)\}$ a $\{\neg P(z), \neg Q(f(z), z)\}$
$\Rightarrow \{P(f(z)), \neg P(z)\}$

2) je lepší než 1) ... je to obecnější, dozvíme se více

__Def:__ __Substituce__ je konečná množina $\sigma = \{x_1/t_1, \dots x_n/t_n\}$, kde $x_i$ jsou navzájem různé proměnné a $t_i$ jsou termy různé od $x_i$ $(t_i \neq x_i)$.

__Def:__ Substituce $\sigma = \{x_1/t_1, \dots x_n/t_n\}$ je

1) __základní__ ≡ všechny termy $t_i$ jsou konstantní

2) __přejmenování proměnných__ ≡ všechny termy $t_i$ jsou navzájem různé proměnné

__Def:__ Výraz je term nebo literál (at. formule / její negace).

__Def:__ Instance výrazu $E$ při substituci $\sigma = \{x_1/t_1, \dots x_n/t_n\}$ je
$E\sigma := E(x_1/t_1, \dots x_n/t_n)$ ⇝ výskyty $x_i$ nahradíme za $t_i$

Pro množinu výrazů $S$ je $S\sigma := \{E\sigma \mid E \in S\}$

__Ukázka:__ $S = \{P(x), R(y,z)\}$, $\sigma = \{x/f(y,z), y/x, z/c\}$
$\Rightarrow S\sigma = \{P(f(y,z)), R(x,c)\}$

→ substituce lze skládat: $\sigma\tau$ znamená nejprve $\sigma$, potom $\tau$
$\Rightarrow$ chceme aby $E(\sigma\tau) = (E\sigma)\tau$

__Def:__ Složení substitucí $\sigma = \{x_1/t_1, \dots x_n/t_n\}$ a $\tau = \{y_1/s_1, \dots y_m/s_m\}$ je substituce $\sigma\tau$ definovaná následovně.

Označme $X := \{x_1, \dots x_n\}$ a $Y := \{y_1, \dots y_m\}$

1) pokud $y_j \in Y \setminus X$, potom $y_j/s_j \in \sigma\tau$

2) pokud $x_i \in X$ a $x_i = t_i\tau$, tak nemusíme dělat nic

3) pokud $x_i \in X$ a $x_i \neq t_i\tau$, potom $x_i/t_i\tau \in \sigma\tau$

Tvrzení: Platí 1) $(E\sigma)\tau = E(\sigma\tau)$

2) $(\sigma\tau)\varrho = \sigma(\tau\varrho)$

Dk: 1) Stačí postupně pro $E = x_1, \dots x_n, y_1, \dots y_m$ ... triviálně ✓

↳ substituce nemění ostatní symboly

2) $E((\sigma\tau)\varrho) = (E(\sigma\tau))\varrho = ((E\sigma)\tau)\varrho = (E\sigma)(\tau\varrho) = E(\sigma(\tau\varrho))$ ∎

• Unifikační algoritmus

Def: Unifikace pro $S = \{E_1, \dots E_n\}$ je substituce $\sigma$ t.ž. $E_1\sigma = E_2\sigma = \dots = E_n\sigma$, tedy $S\sigma$ obsahuje jediný výraz.

→ unifikace $\sigma$ je nejobecnější ≡ ∀ jinou unifikaci $\tau$ pro $S$ lze získat jako $\tau = \sigma\lambda$ pro nějakou substituci $\lambda$.

Ukázka: $S = \{P(f(x), y), P(f(a), w)\}$ (konst. → $a$)

• $\sigma = \{x/a, y/w\}$ je nejobecnější unifikace ⇒ $\{P(f(a), w)\}$ (proměnná → $w$)

• $\tau = \{x/a, y/b, w/b\}$ je unifikace $\{P(f(a), b)\}$ (konstanta → $b$) ale není nejobecnější

↳ nelze z ní získat $\sigma$ nebo ani $\{x/a, y/c, w/c\}$

• $\tau = \sigma\lambda$ pro $\lambda = \{w/b\}$ : $\{x/a, y/w\}\lambda = \{x/a, y/b, w/b\}$

Algoritmus:

Vstup: $S = \{E_1, \dots E_n\} \neq \emptyset$

Výstup: nejobecnější unifikace $\sigma$ nebo info, že $S$ není unifikovatelná

0. $S_0 \leftarrow S$, $\sigma_0 \leftarrow \emptyset$, $k \leftarrow 0$

1. Pokud $|S_k| = 1$ : return $\sigma = \sigma_0\sigma_1 \cdots \sigma_k$ → konec

→ teď budeme postupně procházet výrazy $E_1, \dots E_n$ jako řetězce zleva doprava a když narazíme na neshodu dvou řetězců, tak je unifikujeme

$D(S)$ := množina všech podvýrazů začínajících na pozici první neshody v $S$

$S = \{P(x, y), P(f(x), z), P(z, f(x))\}$ ... $p = 3$ ⇒ $D(S) = \{x, f(x), z\}$

2. Pokud je v $D(S_k)$ proměnná $x$ a term $t$ neobsahující $x$: $f(x), z$

3. $\sigma_{k+1} \leftarrow \{x/t\}$ , $S_{k+1} \leftarrow S_k\sigma_{k+1}$

$k \leftarrow k+1$ , goto 1.

4. jinak $S$ není unifikovatelná → konec

Ukázka:

$S_0 = \{P(f(y, g(z)), h(t)),\ P(f(h(w), g(a)), s),\ P(f(h(t), g(z)), y)\}$

$\to$ $k = 5$: $D(S_0) = \{y, h(w), h(t)\}$ ... $y$ není v $h(w)$ $\Rightarrow \sigma_1 = \{y/h(w)\}$

$S_1 = \{P(f(h(w), g(z)), h(t)),\ P(f(h(w), g(a)), s),\ P(f(h(t), g(z)), h(w))\}$

$\to$ $D(S_1) = \{w, t\} \Rightarrow \sigma_2 = \{w/t\}$

$S_2 = \{P(f(h(t), g(z)), h(t)),\ P(f(h(t), g(a)), s),\ \cancel{P(f(h(t), g(z)), h(t))}\}$

$\to$ $D(S_2) = \{z, a\} \Rightarrow \sigma_3 = \{z/a\}$

$S_3 = \{P(f(h(t), g(a)), h(t)),\ P(f(h(t), g(a)), s)\}$

$\to$ $D(S_3) = \{h(t), s\} \Rightarrow \sigma_3 = \{s/h(t)\}$

$S_4 = \{P(f(h(t), g(a)), h(t))\}$

$\Rightarrow$ nejobecnější unifikace: $\sigma = \sigma_1\sigma_2\sigma_3\sigma_4 = \{y/h(t), w/t, z/a, s/h(t)\}$

Tvrzení: Unifikační alg. najde nejobecnější unifikaci $\sigma$, která splňuje $\sigma\tau = \tau$ pro libovolnou unifikaci $\tau$.

Dk: Zjevně najde unifikaci, obecnost z vlastnosti nosič – indukcí.

- Rezoluční pravidlo

$\to$ chceme-li ukázat $T \models \varphi$, skolemizací najdeme ekvisplnitelnou otevřenou formuli, kterou převedeme do CNF a najdeme rezoluční zamítnutí $T \cup \{\neg\varphi\}$.

Ukázka: $C_1 = \{P(x), Q(x,y), Q(x, f(z))\}$ a $C_2 = \{\neg P(u), \neg Q(f(u), u)\}$

$\to$ chceme rezolucí odstranit $Q(x, f(z))$ a $\neg Q(f(u), u)$

$\Rightarrow$ $S = \{Q(x,y), Q(x, f(z)), Q(f(u), u)\}$ ... $Q$ a zapomeneme na $\neg$

unifikace $\sigma = \{x/f(f(z)), y/f(z), u/f(z)\}$

$S\sigma = \{\underbrace{Q(f(f(z)), f(z))}_{\bullet}\}$

rezolventa: $C_1\sigma = \{P(f(f(z))), \bullet\}$ $\Rightarrow$ $C = \{P(f(f(z))), \neg P(f(z))\}$

$C_2\sigma = \{\neg P(f(z)), \neg\bullet\}$

Def: Nechť $C_1$ a $C_2$ jsou klauzule s disjunktními množinami proměnných.

Nechť $C_1 = C_1' \sqcup \{A_1, \dots A_n\}$ $n \geq 1$

$C_2 = C_2' \sqcup \{\neg B_1, \dots \neg B_m\}$ $m \geq 1$ … $\sqcup$ značí disjunktní sjednocení

a nechť $S = \{A_1, \dots A_n, B_1, \dots B_m\}$ lze unifikovat. Označme $\sigma$ nejobecnější unifikaci $S$ a $E$ výsledek $S\sigma$. Máme

$$C_1\sigma = C_1'\sigma \sqcup \{E\}$$
$$C_2\sigma = C_1'\sigma \sqcup \{\neg E\}$$

Rezolventou $C_1$ a $C_2$ myslíme klauzuli $C_1'\sigma \cup C_2'\sigma$.

Pokud $C_1$ a $C_2$ nemají disjunktní proměnné, tak proměnné z $C_1$ přejmenujeme.

→ děláme to proto, aby unifikační algoritmus fungoval

• Rezoluční důkaz

Def: Rezoluční důkaz klauzule $C$ z formule $S$ je konečná posloupnost klauzulí $C_0, C_1, \dots C_n = C$ t.ž.

1) $C_i$ je nějaká klauzule z $S$ až na $\underbrace{\text{přejmenování proměnných}}^{\text{druh substituce}}$

2) nebo $C_i$ je rezolventou nějakých $C_k, C_j$, kde $j,k < i$.

→ existuje-li, píšeme $S \vdash_R C$

Rezoluční zamítnutí $S$ je rezoluční důkaz $\square$ z $S$

Ukázka: $S = \{\underbrace{\{\neg P(x,y), \neg P(y,z), P(x,z)\}}_{1}, \underbrace{\{\neg P(x,x)\}}_{2}, \underbrace{\{\neg P(x,y), P(y,x)\}}_{3}, \underbrace{\{P(x,f(x))\}}_{4}\}$

→ rezoluční zamítnutí $S$:

$\overset{1}{\{\neg P(x,y), \neg P(y,z), P(x,z)\}}$ $\overset{4}{\{P(x',f(x'))\}}$ $\overset{3}{\{\neg P(x,y), P(y,x)\}}$ $\overset{4}{\{P(x',f(x'))\}}$

$y/f(x),\ x'/x$ $\qquad$ $x/x',\ y/f(x')$

$\{\neg P(f(x),z), P(x,z)\}$ $\qquad$ $\{P(f(x'),x')\}$

$z/x,\ x'/x$

$\{P(x,x)\}$ $\quad$ $\overset{2}{\{\neg P(x',x')\}}$

$x/x'$

$\square$

$S \vdash_R \square$

• **Korektnost a úplnost rezoluce**

Tvrzení: Pokud je $C$ rezolventou klauzulí $C_1$ a $C_2$ & $\mathcal{A}$ je model $C_1$ a $C_2$, tak $\mathcal{A}$ je i modelem $C$. Tedy $\mathcal{A} \models C_1$ & $\mathcal{A} \models C_2 \Rightarrow \mathcal{A} \models C$.

Dk: Rozepišme si to. $C$ je rezolventou $C_1$ a $C_2$, tedy

$C_1 = C_1' \sqcup \{A_1, \dots A_n\}$
$C_2 = C_2' \sqcup \{\neg B_1, \dots \neg B_m\}$ a máme nejobecnější unifikaci $\sigma$

$C = C_1'\sigma \cup C_2'\sigma$ a označíme $E$ výsledek unifikace $\{A_1, \dots A_n, B_1, \dots B_m\}$ $\Rightarrow E = A_1\sigma$

$\Rightarrow$ máme $C_1\sigma = C_1'\sigma \cup \{E\}$
$C_2\sigma = C_2'\sigma \cup \{\neg E\}$.

Nechť $\mathcal{A}$ je model $C_1$ a $C_2$. Tudíž platí i $\mathcal{A} \models C_1\sigma$ a $\mathcal{A} \models C_2\sigma$.
$\rightarrow$ musíme ukázat, že při libovolném ohodnocení proměnných $e$ je v klauzuli $C = \underbrace{C_1'\sigma}_{1} \cup \underbrace{C_2'\sigma}_{2}$ nějaký splněný literál.

1, pokud $\mathcal{A} \models E[e]$, tak $\mathcal{A} \not\models \neg E[e]$, tudíž aby mohlo být $\mathcal{A} \models C_2\sigma$, tak musí platit $\mathcal{A} \models \underbrace{C_2'\sigma[e]}_{2}$, což splňuje $C$.

2, pokud $\mathcal{A} \not\models E[e]$, tak musí být $\mathcal{A} \models \underbrace{C_1'\sigma[e]}_{1}$, což splňuje $C$. ∎

Věta (o korektnosti r.): Pokud je CNF formule rezolučně zamítnutelná, potom je nesplnitelná.

Dk: Víme, že $S \vdash_R \square$, vezmeme tedy nějaký r. důkaz $\square$ z $S$. : $C_0, C_1, \dots C_n = \square$
Kdyby existoval model $\mathcal{A} \models S$, tak indukcí podle délky důkazu platí i $\mathcal{A} \models S$ ... protože $C_0$ je nějaká klauzule z $S$ a $C_i$ je buď klauzule z $S$ nebo rezolventa nějakých $C_k$ a $C_l$, $k, l < i$.
Podle předchozího tvrzení musí být $\mathcal{A} \models C_i$, tudíž i $\mathcal{A} \models \square$.
Ale spor nemá žádný model, SPOR. ∎

Věta (o úplnosti r.): Je-li CNF formule nesplnitelná, potom je rezolučně zamítnutelná.

Myšlenka důkazu: Přes grounding převedeme na výrokovou logiku.

• LI-rezoluce

Def: Lineární důkaz: $\begin{bmatrix} C_0 \\ B_0 \end{bmatrix}, \begin{bmatrix} C_1 \\ B_1 \end{bmatrix}, \dots \begin{bmatrix} C_n \\ B_n \end{bmatrix}, C_{n+1}$ klauzule $C$ z $S$.

- $B_0$ a $C_0$ jsou varianty klauzulí z $S$ (varianta = přejmenování proměnné v kvantifikátorem)
- $C_{n+1} = C$
- $C_{i+1}$ je rezolventa $C_n$ a $B_n$
- $B_i$ je buď varianta klauzule z $S$ nebo $B_i = C_j$, $j < i$

→ lineární zamítnutí $S$ je lineární důkaz □ z $S$.

Def: LI-důkaz je lin. důkaz, kde $\forall B_i$ je varianta nějaké klauzule z $S$.

→ pokud existuje: $S \vdash_{LI} C$

→ LI zamítnutí $S$ je $S \vdash_{LI} \square$.

Korektnost LI rezoluce plyne z korektnosti rezoluce.

Věta (o úplnosti lin. r.): $C$ má lineární důkaz z $S$ $\Leftrightarrow$ má rezoluční důkaz z $S$.

Dk: převodem na výrokovou logiku.

Věta (o úplnosti LI pro Hornovy formule): Je-li Hornova formule $T$ splnitelná, a $T \cup \{G\}$ nesplnitelná pro cíl $G$, potom $T \cup \{G\} \vdash_{LI} \square$, a to LI-zamítnutím, které začíná v $G$.

Dk: Převod na výrokovou logiku.

# POKROČILÉ PARTIE

**Def:** Teorie struktury $\mathcal{A}$ v jazyce $L$ je množina
$$Th(\mathcal{A}) := \{\varphi \mid \varphi \text{ je } L\text{-sentence a } \mathcal{A} \models \varphi\}$$

**Ukázka:** Budeme pracovat s $Th(\underline{\mathbb{N}})$, kde $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$ ... std. model arit.

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

- $Th(\mathcal{A})$ je kompletní teorie = je bezesporná a $\forall$ sentence je v ní pravdivá nebo lživá
  $\Rightarrow$ pravdivá $(\Leftrightarrow)$ $\in Th(\mathcal{A})$, jinak lživá
- $\mathcal{A} \in M_L(T) \Rightarrow Th(\mathcal{A})$ je jednoduchá extenze $T$
- $\mathcal{A} \in M_L(T)$ & $T$ je kompletní $\Rightarrow Th(\mathcal{A}) = Csq_L(T) \sim T$

**Připomenutí:** Struktury $\mathcal{A}, \mathcal{B}$ jsou elementárně ekvivalentní $\mathcal{A} \equiv \mathcal{B}$ $\Leftrightarrow$ v nich platí tytéž $L$-sentence, neboli $Th(\mathcal{A}) = Th(\mathcal{B})$.

**Ukázka:** $\langle \mathbb{R}, \leq \rangle \equiv \langle \mathbb{Q}, \leq \rangle$
$\langle \mathbb{Q}, \leq \rangle \not\equiv \langle \mathbb{Z}, \leq \rangle$ ... $\mathbb{Z}$ není husté

**Def:** Teorie je rozhodnutelná $\equiv$ existuje algoritmus, který dokáže rozhodnout o platnosti každé sentence : $T \models \varphi$?

Teorie je kompletní $\equiv$ má až na el. ekvivalenci právě 1 model.

**Důsledek:** Nechť $T$ je libovolná teorie. Protože $\mathcal{A} \in M_L(T) \Rightarrow Th(\mathcal{A})$ je jednoduchá ex. $T$, tak model $\mathcal{A}$ odpovídá kompletní extenzi $T$ : $Th(\mathcal{A})$.
Navíc pokud $\mathcal{A} \equiv \mathcal{B}$, tak $Th(\mathcal{A}) = T(\mathcal{B})$, tedy jim odpovídají stejné kompletní extenze $T$.

**Motivace:** Ukážeme, že pokud lze efektivně popsat všechny kompletní jednoduché extenze dané teorie, potom je rozhodnutelná.

## • Kompletní jednoduché extenze DeLO*

<u>Def</u>: Teorie hustého lin. uspořádání (DeLO*) je extenze teorie uspořádání o linearitu, hustotu a netriviálitu:

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

→ značení: $x < y$ je zkratka za $x \leq y \wedge \neg x = y$

- $x < y \rightarrow (\exists z)(x < z \wedge z < y)$
- $(\exists y)(\exists x)(\neg x = y)$ ... alespoň 2 prvky

<u>Tvrzení</u>: DeLO* má právě 4 kompletní jednoduché extenze (až na ekvivalenci).

Označme $\varphi := (\exists x)(\forall y)(x \leq y)$ a $\psi := (\exists x)(\forall y)(y \leq x)$.

→ v každém modelu $\mathcal{A}$ musí $\varphi$ a $\psi$ buď platit nebo neplatit.

→ protože modely určují kompletní extenze, tak

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

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

pokud tohle jsou kompletní extenze, tak jsou jediné možné.

<u>Pz</u>: To, že jsou kompletní vyplyne z něčeho, co dokážeme později.

• Löwenheim – Skolemova věta pro jazyk s rovností

→ pomocí kanonického modelu tabla jsme dokázali

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

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

Dk: Buď $\mathcal{A}$ L-struktura. Teorie $Th(\mathcal{A})$ je bezesporná (má model $\mathcal{A}$), tedy dle L-S věty má spočetně nekonečný model $\mathcal{B} \models Th(\mathcal{A})$. Ale $Th(\mathcal{A})$ je kompletní, takže musí platit $\mathcal{A} \equiv \mathcal{B}$. ■

Důsledek: Bez rovnosti tedy nelze specifikovat například počet prvků modelu dané teorie.

Věta (L-S s '='): Ve spočetném jazyce s rovností má každá bezesporná teorie spočetný model.

Dk: Podobně jako bez '=', tam použijeme kanonický model pro bezespornou větev tabla z T pro F⊥.
→ pro jazyk s '=' stačí tento model faktorovat podle $=^{\mathcal{A}}$.
↳ výsledná faktorstruktura může být i konečná. ■

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

Dk: K nekonečné L-struktuře $\mathcal{A}$ najdeme stejně jako v minulém důkazu spočetnou $\mathcal{B} \equiv \mathcal{A}$.
→ protože v $\mathcal{A}$ neplatí pro žádné $n \in \mathbb{N}$ sentence vyjadřující 'model má nejvýše n prvků' – to je s rovností easy
tak neplatí ani v $\mathcal{B}$. Tedy $\mathcal{B}$ nemůže být konečná. ■

- Spočetné algebraicky uzavřené těleso

Def: Těleso je algebraicky uzavřené $\equiv$ v něm má $\forall$ polynom stupně $> 0$ kořen.

→ $\mathbb{Q}, \mathbb{R}$ nejsou alg. uzavřené: $x^2+1$

→ $\mathbb{C}$ je algebraicky uzavřené, ale není spočetné

→ algebraickou uzavřenost vyjádříme pro polynom stupně $n > 0$ sentencí

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

→ $y^k$ je zkratka za $y \cdot y \cdot \dots \cdot y$

Tvrzení: Existuje algebraicky uzavřené spočetné těleso.

Dk: Dle důsledku L-S. věty o rovnosti existuje spočetně nekonečná struktura $\mathcal{A} \equiv \mathbb{C}$. Protože $Th(\mathcal{A}) = Th(\mathbb{C})$ a $\mathbb{C}$ splňuje $\psi_n$ pro všechna $n$, tak je i $\mathcal{A}$ algebraicky uzavřené. ■

- Izomorfismus struktur

Def: Izomorfismus struktur $\mathcal{A}, \mathcal{B}$ jazyka $L = \langle \mathcal{R}, \mathcal{F} \rangle$ je bijekce $h: A \to B$ t.ž.

i) pro každý $f \in \mathcal{F}$ arity $n$ a $\underset{\sim}{a} \in A^n$:

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

$\to$ speciálně pro konstantní $c \in \mathcal{F}$: $h(c^{\mathcal{A}}) = c^{\mathcal{B}}$

ii) pro každý $R \in \mathcal{R}$ arity $n$ a $\underset{\sim}{a} \in A^n$:

$$R^{\mathcal{A}}(\underset{\sim}{a}) \Leftrightarrow R^{\mathcal{B}}(h(a_1), \dots h(a_n))$$

$\to$ existuje-li, jsou izomorfní $\mathcal{A} \simeq \mathcal{B}$.

$\to$ automorfismus $\mathcal{A}$ je izomorfismus $\mathcal{A}$ s $\mathcal{A}$.

$\to$ izomorfismus $\sim$ liší se jen pojmenováním prvků (mají stejně velké domény)

Relace 'být izomorfní' je ekvivalence.

Ukázka: Potenční algebra $\underline{P(X)} = \langle P(X), \bar{\ }, \cap, \cup, \emptyset, X \rangle$ $|X| = n$

je izomorfní s $\underline{2^n} = \langle \{0,1\}^n, \text{NOT}, \text{AND}, \text{OR}, (0,\dots 0), (1, \dots 1) \rangle$

0-1 vektory — pro složkách jako na počítači

$\to$ izomorfismus $h(A) =$ charakteristický vektor podmnožiny $A \subseteq X$

Tvrzení: Bijekce $h: A \to B$ je izomorfismus $\mathcal{A}$ a $\mathcal{B}$ $\Leftrightarrow$ pro $\forall$ ohodnocení $e: \text{Var} \to A$

(*) i) pro $\forall$ term $t$: $h(t^{\mathcal{A}}[e]) = t^{\mathcal{B}}[e \circ h]$

ii) pro $\forall$ formuli $\varphi$: $\mathcal{A} \models \varphi[e] \Leftrightarrow \mathcal{B} \models \varphi[e \circ h]$

Dk: $\Rightarrow$: indukcí podle stromu termu / formule

$\hookrightarrow$ pro konstanty a proměnné triviálně $\Rightarrow$ pak i pro složené

$\hookrightarrow$ pro atomické formule triviálně $\Rightarrow$

$\Leftarrow$: Je-li $h$ bijekce splňující i) a ii), tak dosadíme $e: x_i \mapsto a_i$

$t = f(x_1, \dots x_n) \Rightarrow t^{\mathcal{A}}[e] = f^{\mathcal{A}}(a_1, \dots a_n) = f^{\mathcal{A}}(\underset{\sim}{a})$

i): $h(f^{\mathcal{A}}(\underset{\sim}{a})) = t^{\mathcal{B}}[e \circ h] = f^{\mathcal{B}}(h(a_1), \dots h(a_n))$

$\to$ definice $\simeq$

$\varphi = R(x_1, \dots x_n)$

ii) $\mathcal{A} \models R(\underset{\sim}{a}) \Leftrightarrow \mathcal{B} \models R(h(a_1), \dots h(a_n)) \Rightarrow R^{\mathcal{A}}(\underset{\sim}{a}) \Leftrightarrow R^{\mathcal{B}}(\dots)$ ∎

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

$\to Th(\mathcal{A}) = Th(\mathcal{B})$

Dk: Pro každou sentenci $\varphi$ máme z ii) $\mathcal{A} \models \varphi \iff \mathcal{B} \models \varphi$ ■

Tvrzení: Nechť je $L$ jazyk s rovností a $\mathcal{A}, \mathcal{B}$ konečné $L$-struktury. Platí
$$\mathcal{A} \simeq \mathcal{B} \iff \mathcal{A} \equiv \mathcal{B}.$$

Dk: $\Rightarrow$: už víme

$\Leftarrow$: $|A| = |B|$ protože díky '=' můžeme vyjádřit "existuje právě n prvků"

... pak jen ukázat, že existuje izomorfismus (bijekce existuje).

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

Dk: Kompletní teorie má všechny modely el. ekvivalentní ■

- Vztah definovatelných množin a automorfismů

Připomenutí: Množina definovaná formulí $\varphi(x_1, \dots x_n)$ ve struktuře $\mathcal{A}$ je
$$\varphi^{\mathcal{A}}(\underline{x}) := \{\underline{a} \in A^n \mid \mathcal{A} \models \varphi(\underline{x}/\underline{a})\}.$$

Množina definovaná formulí $\varphi(x_1, \dots x_n, y_1, \dots y_m)$ s parametry $\underline{b} \in A^m$ je
$$\varphi^{\mathcal{A}, \underline{b}}(\underline{x}) := \{\underline{a} \in A^n / \mathcal{A} \models \varphi(\underline{x}/\underline{a}, \underline{y}/\underline{b})\}$$

Když mám graf a udělám automorfismus, tak se musí zachovat všechny vlastnosti (je to jen přejmenování vrcholů)

$\Rightarrow$ $\Delta$ se zobrazí na $\Delta$, izolovaný vrchol na izolovaný vrchol atd.

$\Rightarrow$ množina všech $\Delta$ se zobrazí na množinu všech $\Delta$

Tvrzení: Je-li $D \subseteq A^n$ definovatelná v $\mathcal{A}$, potom pro každý automorfismus $h$ na $\mathcal{A}$ platí, že obraz $D$ v $h$, $h[D] = D$.

→ Je-li navíc definovatelná s parametry $\underline{b}$, tak to platí pro automorfismy identické na $\underline{b}$: tedy $h(b_i) = b_i$.

Dk: Ukážeme jen verzi s parametry. Nechť $D = \varphi^{\mathcal{A}, \underline{b}}(\underline{x}, \underline{y})$. Potom pro $\forall \underline{a} \in A^n$:

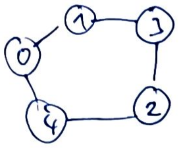
$\underline{a} \in D \iff \mathcal{A} \models \varphi(\underline{x}/\underline{a}, \underline{y}/\underline{b}) \iff \mathcal{A} \models \varphi[e(\underline{x}/\underline{a}, \underline{y}/\underline{b})]$, kde $e$ je libovolné ohodnocení

$\overset{(*)}{\iff} \mathcal{A} \models \varphi[(e \circ h)(\underline{x}/\underline{a}, \underline{y}/\underline{b})]$

$\iff \mathcal{A} \models \varphi[e(\underline{x}/h(\underline{a}), \underline{y}/h(\underline{b}))]$

$\iff \mathcal{A} \models \varphi[e(\underline{x}/h(\underline{a}), \underline{y}/\underline{b})] \iff h(\underline{a}) \in D.$ ■

Ukázka: Mějme graf $G$ a parametr $y = 0$




Množiny definovatelné s $y = 0$:

$\{0\}$ formulí $y = x$

$\{1,4\}$ formulí $E(x,y)$

$\{2,3\}$ formulí $\neg E(x,y) \wedge x \neq y$

$\emptyset$, $\{0,1,2,3,4\}$

→ a $\cap$, $\cup$, doplňky, ...

→ jediný netriviální automorfismus $G$ zachovávající $0$ je $h(i) = (5-i) \bmod 5$.

$\Rightarrow h[\{2,3\}] = \{3,2\}$ ...

- $\omega$-kategorické teorie

Def: Izomorfní spektrum $T$: $I(\kappa,T) :=$ # modelů $T$ kardinality $\kappa$ až na $\cong$.

$T$ je $\kappa$-kategorická $\equiv I(\kappa,T) = 1$.

Speciálně: $T$ je $\omega$-kategorická $\Leftrightarrow$ má jediný spočetně nekonečný model až na $\cong$.

Tvrzení: DeLO je $\omega$-kategorická.

Dk: Nechť $\mathcal{A}, \mathcal{B}$ jsou spočetné nekonečné modely. Ukážeme $\mathcal{A} \cong \mathcal{B}$. Označme

$A = \{a_i \mid i \in \mathbb{N}\}$
$B = \{b_i \mid i \in \mathbb{N}\}$ DeLO má axiom hustoty, tedy induktivně postupně

najdeme funkce $h_0 \subseteq h_1 \subseteq h_2 \subseteq \dots$ takové, že jsou prosté a

$h_i : A_i \subseteq A \to B$ je definovaná pro $\{a_0, \dots a_{i-1}\}$ a její obor hodnot obsahuje $\{b_0, \dots b_{i-1}\}$.

→ dále $h_i$ zachovávají axiomy uspořádání

$\Rightarrow \mathcal{A} \cong \mathcal{B}$ pomocí izomorfismu $h := \bigcup_{i \geq 0} h_i$

Důsledek: Izomorfní spektrum teorie DeLO*:

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

$I(\omega, \text{DeLO}^*) = 4$.

Dk: Husté uspořádání nemůže být konečné.

Proč 4? Viz ty modely z úvodu o DeLO*

↳ min se musí zobrazit na min a max na max. ∎

• $\omega$-kategorické kritérium kompletnosti.

Věta: Buď T $\omega$-kategorická ve spočetném jazyce L. Je-li
1) bez rovnosti nebo
2) s rovností a T nemá konečné modely,
potom je T kompletní.

Dk: 1) L-S věta bez rovnosti: $\forall$ model je $\equiv$ k nějakému spočetně nekonečnému
→ ale ten je z $\omega$-kat. jediný (až na $\simeq$). a $\simeq \Rightarrow \equiv$.
2) L-S věta o rovnosti: podobně $\forall$ model je $\equiv$ k nějakému spočetnému
→ ale ten je jen 1, protože jsme konečné zakázali ■

Důsledek: DeLO, DeLO$^+$, DeLO$^-$, DeLO$^\pm$ jsou kompletní, takže to jsou jediné kompletní jednoduché extenze DeLO$^*$.

• Axiomatizovatelnost

Def: Třída struktur $K \subseteq M_L$ je
1) axiomatizovatelná $\equiv \exists$ teorie T t.ž. $M_L(T) = K$.
2) konečně axiom. $\equiv$ je axiom. konečnou teorií
3) otevřeně axiom. $\equiv$ je axiom. otevřenou teorií

Def: Teorie T je konečně resp. otevřeně axiom. $\equiv$
třída jejích modelů $K = M_L(T)$ je konečně resp. otevřeně axiom.

Aby K mohla být axiom., tak musí být uzavřená na el. ekvivalenci.

Ukázka:
• grafy a částečná usp. jsou konečně i otevřeně ax.
• tělesa jsou konečně, ale ne otevřeně ax.

Věta: Má-li T libovolně velké konečné modely, má i nekonečný model.
Navíc není třída jejích modelů axiomatizovatelná.

Důsledek: Třídy konečných modelů nejsou axiomatizovatelné
• konečné grafy nejsou axiomatizovatelné

**Věta** (o konečné ax.): $K \subseteq M_L$ je konečně axiomatizovatelná $\iff$

$K$ i $\overline{K} = M_L \setminus K$ jsou obě konečně axiomatizovatelné.

- Tělesa char. 0 nejsou konečně ax.

→ odteď značí $T$ teorii těles

tělesa char $p$ jsou konečně ax. jako

$$T_p = T \cup \{\underbrace{1+1+\dots+1}_{p} = 0\}$$

tělesa char 0 jsou ax., ale ne konečně

$$T_0 = T \cup \{\underbrace{1+1+\dots+1}_{p} \neq 0 \mid p \text{ je prvočíslo}\}$$

**Tvrzení:** Třída $K$ těles char. 0 není konečně ax.

**Dk:** Stačí dokázat, že $\overline{K}$ (tělesa nenulové char. a netělesa) není ax.

Pro spor nechť $\overline{K} = M(S)$ pro nějakou (ne nutně konečnou) teorii $S$.

Definujme $S' := S \cup T_0$.

každá konečná část $S'$ má model – těleso dostatečně velké char.

$\Rightarrow$ z věty o kompaktnosti má i $S'$ model – označme ho $\mathcal{A}$.

Protože $\mathcal{A} \models S' = S \cup T_0$, tak $\mathcal{A} \models S \Rightarrow \mathcal{A} \in M(S) = \overline{K}$

$\mathcal{A} \models T_0 \rightarrow \mathcal{A} \in M(T_0) = K$. ↯ ∎

- Otevřená axiomatizovatelnost

**Věta:** Je-li $T$ otevřeně ax. potom je každá podstruktura modelu $T$ také model $T$.

**Dk:** Nechť $T'$ je otevřená ax. $T$, $\mathcal{A}$ model $T'$ (tedy i $T$) a $\mathcal{B} \subseteq \mathcal{A}$.

Pro $\forall \alpha \in T'$ platí $\mathcal{B} \models \alpha$, tudíž $\mathcal{B} \models T'$ (tedy i $T$).

↑ $\alpha$ je otevřená = bez kvant. → nezáleží na doméně

**Poznámka:** Platí i opačná implikace ∎

**Ukázka:**

- DeLO není otevřeně ax. $\because$ třeba $\mathbb{N} \subseteq$ DeLO není hustá
- teorie těles není otevřeně ax. $\because$ $\mathbb{Z} \subseteq \mathbb{Q}$ není těleso

• **Nerozhodnutelnost a neúplnost**

→ Gödelovy věty

• Rekurzivní axiomatizace → neúplnost

Def: T je rekurzivně axiomatizovaná ≡ ∃ algoritmus, který pro ∀ formuli $\varphi$ doběhne a odpoví, zda $\varphi \in T$.

Def: Teorie T je

1) rozhodnutelná ≡ ∃ algoritmus, který pro ∀ formuli $\varphi$ doběhne a odpoví, zda $T \models \varphi$.

2) částečně rozhodnutelná ≡ ∃ algoritmus, který

- pokud $T \models \varphi$ doběhne a odpoví "ano"
- pokud $T \not\models \varphi$ buď nedoběhne, nebo doběhne a odpoví "ne".

Tvrzení: Je-li T rekurzivně ax., potom

1) T je částečně rozh.

2) pokud je navíc kompletní, tak je rozhodnutelná.

Dk: 1) Algoritmus konstruuje systematický tablo z T pro $F\varphi$.
T je rekurzivně ax. takže postupně dostaneme všechny axiomy
→ pokud $T \models \varphi$, je tablo konečné a sporné

2) Víme, že buď $T \vdash \varphi$ nebo $T \vdash \neg\varphi$
⇒ paralelně konstruujeme systematická tabla z T pro $F\varphi$ a $T\varphi$.
↪ jedno z nich bude konečné. ∎

• **Rekurzivně spočetná kompletace**

Def: T má rekurzivně spočetnou kompletaci ≡ → až na ekvivalenci
množina všech jednoduchých kompletních extenzí T je rekurzivně spočetná
→ tedy ∃ algoritmus, který pro vstup $(i, j)$ vypíše $i$-tý axiom $j$-té extenze nebo odpoví, že neexistuje.

Věta: Je-li T rekurzivně ax. a má rekurzivně spočetnou kompletaci, potom je rozhodnutelná.

Dk: Algoritmus paralelně konstruuje tablo důkaz $\varphi$ z T a postupně tablo důkazy $\neg\varphi$ ze všech kompletních jednoduchých extenzí $T_1, T_2, \dots$ Aspoň 1 z tabel je sporné ∎

Ukázka: Následující teorie jsou rekurzivní ax. a mají rekurzivní spoč. kompletaci

$\Rightarrow$ jsou rozhodnutelné

- Teorie hustých lineárních uspořádání ReLO
- Teorie Booleových algeber $\langle -, \wedge, \vee, \bot, \top \rangle$
- Teorie algebraicky uzavřených těles

- Rekurzivní axiomatizovatelnost

Def: Třída modelů $K \subseteq M_L$ je rek. axiomatizovatelná $\equiv$

$\exists$ rekurzivní axiomatizovaná $T$ t.ž. $K = M_L(T)$.

$\to T'$ je rek. axiomatizovatelná $\equiv$ to platí pro třídu jejích modelů

$\iff$ je ekvivalentní nějaké rek. ax. teorii

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

Dk: Označme doménu $A = \{a_1, \dots a_n\}$.. $Th(\mathcal{A})$ axiomatizujeme sentencí

"existuje právě $n$ prvků $a_1, \dots a_n$ splňujících právě ty základní vztahy o funkčních hodnotách a relacích, které platí v $\mathcal{A}$"

$\to$ třeba když $f^{\mathcal{A}}(a_4, a_2) = a_{17}$, tak přidáme $f(x_4, x_2) = x_{17}$.

$(a_3, a_3, a_1) \notin R^{\mathcal{A}}$, přidej $\neg R(x_3, x_3, x_1)$. ∎

Důsledek: $Th(\mathcal{A})$ konečné struktury $\mathcal{A}$ v konečném jazyce s '=' je rozhodnutelná.

Dk: je rek. ax. & $Th(\mathcal{A})$ je vždy kompletní $\Rightarrow$ rozhodnutelná ∎

Ukázka: Pro následující struktury je $Th(\mathcal{A})$ rekurzivně axiomatizovatelná

$\Downarrow$ tedy i rozhodnutelná

- $\langle \mathbb{Z}, \leq \rangle$ ... teorie diskrétních lin. usp.
- $\langle \mathbb{Q}, \leq \rangle$ ... teorie ReLO
- $\langle \mathbb{N}, S, 0 \rangle$ ... teorie následníka s nulou
- $\langle \mathbb{C}, +, -, \cdot, 0, 1 \rangle$ ... teorie algebraicky uzavřených těles char. 0

! teorie standardního modelu aritmetiky

$\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$

není rekurzivně ax.

• Gödelovy věty o neúplnosti

Věta (o nerozhodnutelnosti predikátové l.): Neexistuje algoritmus, který pro vstupní formuli $\varphi$ rozhodne, zda platí v logice, tedy $\models \varphi$.

→ neboli $T = \emptyset$ není rozhodnutelná

• Aritmetika

→ jazyk je $L = \langle S, +, \cdot, 0, \leq \rangle$ s rovností

→ standardní model $\underline{\mathbb{N}}$ nemá rekurzivně axiomatizovatelnou teorii (viz 1. věta o neúplnosti)

→ používáme rekurzivně ax. teorie, které vlastnosti $\mathbb{N}$ popisují částečně

• Robinsonova aritmetika – Q

$$S(x) \neq 0 \qquad x \cdot 0 = 0$$
$$S(x) = S(y) \rightarrow x = y \qquad x \cdot S(y) = x \cdot y + x$$
$$x + 0 = x \qquad x \neq 0 \rightarrow (\exists y)(x = S(y))$$
$$x + S(y) = S(x+y) \qquad x \leq y \leftrightarrow (\exists z)(z + x = y)$$

→ velmi slabá, nelze dokázat ani asociativita/komutativita + a ·

• Peanova aritmetika – PA

→ extenze Q o schéma axiomů indukce.

↳ pro každou L-formuli $\varphi(x, \bar{y})$ přidáme axiom

$$(\varphi(0,\bar{y}) \wedge (\forall x)(\varphi(x,\bar{y}) \rightarrow \varphi(S(x),\bar{y}))) \rightarrow (\forall x)\, \varphi(x,\bar{y})$$

→ mnohem silnější aproximace $Th(\underline{\mathbb{N}})$

Věta (1. Gödelova): Je-li $T$ bezesporná rekurzivně axiomatizovatelná extenze Q, potom $\exists$ sentence pravdivá v $\underline{\mathbb{N}}$, ale nedokazatelná v $T$.

⇒ $\forall$ efektivní popis aritmetiky přirozených čísel je neúplný

Důsledek: Je-li $T$ bezesporná, rek. ax. extenze Q & $\underline{\mathbb{N}}$ je model $T$, potom $T$ není kompletní.

Dk: Pro spor nechť je $T$ kompletní. Vezmeme sentenci $\varphi$, garantovanou 1. větou, která je $\underline{\mathbb{N}} \models \varphi$, ale $T \nvdash \varphi$.

→ $T$ je kompletní, tedy $T \vdash \neg\varphi$, tedy $T \models \neg\varphi$, tedy $\underline{\mathbb{N}} \models \neg\varphi$. ■

Věta (nedefinovatelnost pravdy): V žádném bezesporném rozšíření Robinsonovy aritmetiky nemůže existovat definice pravdy

→ to se dá nějak formálně definovat

→ myšlenka: paradox lháře … je pravdivá $\varphi$ = "nejsem pravdivá v T"?

- Druhá věta o neúplnosti

Neformálně: Efektivně daná, dostatečně bohatá T nedokáže svou bezespornost.

Věta (2. Gödelova): Je-li T bezesporná rekurzivně axiomatizovatelná extenze PA, potom $\varphi$ = "T je bezesporná" není dokazatelná v T.

Důsledek: Je-li ZFC bezesporná, nelze to v ní dokázat.

Pz.: ZFC není extenze PA, ale je v ní možné PA interpretovat.

Důsledek: Kdyby někdo v rámci ZFC dokázal, že je bezesporná, znamenalo by to, že je sporná.