Kapitola 1

Teorie modelů

V této kapitole se trochu vzdálíme typickým aplikacím logiky v informatice[1] a nahlédneme o úroveň abstrakce výše, do oblasti *matematické* logiky. *Teorie modelů* se snaží popsat vztah mezi obecnými vlastnostmi teorií (predikátové logiky) a tříd jejich modelů. Nevyhneme se práci s nekonečnými teoriemi a s nekonečnými strukturami. Jde jen o ukázku několika vybraných výsledků, které jsou pro nás dostupné. Ani se nepokusíme obsáhnout všechny hlavní oblasti teorie modelů, která je velmi bohatá a hluboká. Do této kapitoly jsme také přidali materiál týkající se vlastností modelů, který se nehodil jinam.

1.1 Elementární ekvivalence

Nejprve se podíváme na několik vlastností souvisejících s pojmem *elementární ekvivalence*. Připomeňme, že L-struktury $\mathcal{A}$ a $\mathcal{B}$ jsou *elementárně ekvivalentní* ($\mathcal{A} \equiv \mathcal{B}$), pokud v nich platí tytéž L-sentence.

V teorii modelů nás často zajímá, jaké vlastnosti (sentence) platí v dané, konkrétní struktuře:

Definice 1.1.1 (Teorie struktury)**.** Mějme L-strukturu $\mathcal{A}$. *Teorie struktury* $\mathcal{A}$, značíme $\mathrm{Th}(\mathcal{A})$ je množina všech L-sentencí platných v $\mathcal{A}$:

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

Příklad 1.1.2. Jako důležitý příklad vezměme *standardní model aritmetiky*, strukturu $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$. Teorii $\mathrm{Th}(\underline{\mathbb{N}})$ říkáme *aritmetika přirozených čísel*. V následující kapitole si ukážeme, že je *(algoritmicky) nerozhodnutelná*.[2]

Několik jednoduchých vlastností teorie struktury shrneme v následujícím pozorování:

Pozorování 1.1.3. *Nechť $\mathcal{A}$ je L-struktura a T je L-teorie.*

(i) Teorie $\mathrm{Th}(\mathcal{A})$ *je kompletní.*

(ii) Je-li $\mathcal{A} \in \mathrm{M}_L(T)$*, potom* $\mathrm{Th}(\mathcal{A})$ *je (kompletní) jednoduchá extenze teorie* T*.*

[1] Například použití rezoluce k řešení otázky, zda v dané konečné teorii T platí daná sentence φ.

[2] Teorie T je *(algoritmicky) rozhodnutelná*, pokud existuje algoritmus, který pro každou vstupní sentenci φ doběhne a odpoví, zda $T \models \varphi$.

(iii) Pokud $\mathcal{A} \in \mathrm{M}_L(T)$ *a* T *je kompletní, potom je* $\mathrm{Th}(\mathcal{A})$ *ekvivalentní s* T*, v tom případě* $\mathrm{Th}(\mathcal{A}) = \mathrm{Csq}_L(T)$.

Pomocí pojmu *teorie struktury* můžeme také vyjádřit elementární ekvivalenci, pro L-struktury $\mathcal{A}, \mathcal{B}$ platí:

$$\mathcal{A} \equiv \mathcal{B} \text{ právě když } \mathrm{Th}(\mathcal{A}) = \mathrm{Th}(\mathcal{B}).$$

Příklad 1.1.4. Podívejme se standardní uspořádání reálných, racionálních, a celých čísel, tj. na struktury $\langle \mathbb{R}, \leq \rangle$, $\langle \mathbb{Q}, \leq \rangle$, $\langle \mathbb{Z}, \leq \rangle$. Jak jsme již zmínili v Příkladu **??**, není těžké ukázat, že $\langle \mathbb{R}, \leq \rangle \equiv \langle \mathbb{Q}, \leq \rangle$ (pomocí *hustoty* těchto uspořádání). Struktury $\langle \mathbb{Q}, \leq \rangle$ a $\langle \mathbb{Z}, \leq \rangle$ ale elementárně ekvivalentní nejsou: V $\langle \mathbb{Z}, \leq \rangle$ má každý prvek bezprostředního následníka, což v $\langle \mathbb{Q}, \leq \rangle$ neplatí. Pro následující sentenci φ tedy máme $\varphi \in \mathrm{Th}(\langle \mathbb{Z}, \leq \rangle)$ ale $\varphi \notin \mathrm{Th}(\langle \mathbb{Q}, \leq \rangle)$:

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

1.1.1 Kompletní jednoduché extenze

Máme-li teorii T, zajímá nás, jak vypadají její modely. Připomeňme, že:

- Teorie je *kompletní*, právě když má jediný model až na elementární ekvivalenci.[3]
- Modely teorie T až na elementární ekvivalenci jednoznačně odpovídají kompletním jednoduchým extenzím T.

Kompletní jednoduché extenze L-teorie T jsou tedy tvaru $\mathrm{Th}(\mathcal{A})$ pro $\mathcal{A} \in \mathrm{M}_L(T)$, a (jak jsme už zmínili výše) $\mathcal{A} \equiv \mathcal{B}$ právě když $\mathrm{Th}(\mathcal{A}) = \mathrm{Th}(\mathcal{B})$. Místo hledání všech modelů tedy stačí najít všechny kompletní jednoduché extenze.

Poznámka 1.1.5. Jednu z motivací, proč se zabývat kompletními jednoduchými extenzemi, je Tvrzení **??** z následující kapitoly, které říká, že pokud lze *efektivně (algoritmicky) popsat* všechny kompletní jednoduché extenze[4] *efektivně dané* teorie T,[5] potom je T *(algoritmicky) rozhodnutelná.*

Schopnost (efektivně) popsat všechny kompletní jednoduché extenze je poměrně vzácná, a vyžaduje silné předpoklady. Přesto to lze provést u mnoha důležitých teorií. Uveďme jeden příklad: *teorii hustého lineárního uspořádání (dense linear order).*

Příklad: DeLO*

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

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

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

- axiom *hustoty*

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

[3] Tedy všechny její modely jsou elementárně ekvivalentní.

[4] Představte si algoritmus, který pro daná vstupní i, j odpoví j-tý axiom i-té kompletní jednoduché extenze (v nějakém pevném očíslování); takový algoritmus ne vždy existuje!

[5] T může být nekonečná, ale musí existovat algoritmus, který postupně vygeneruje všechny axiomy T.

Někdy se přidává i axiom *netriviality* $(\exists x)(\exists y)(\neg\, x = y)$ zakazující jednoprvkový model. Tato teorie není kompletní, umíme ale popsat všechny její kompletní jednoduché extenze:

Tvrzení 1.1.6. *Mějme sentence $\varphi = (\exists x)(\forall y)(x \leq y)$ a $\psi = (\exists x)(\forall y)(y \leq x)$ vyjadřující existenci minimálního resp. maximálního prvku. Následující čtyři teorie jsou právě všechny kompletní jednoduché extenze teorie DeLO*:*

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

Stačí ukázat, že tyto čtyři teorie jsou kompletní. Potom už je zřejmé, že žádná další kompletní jednoduchá extenze DeLO* nemůže existovat. Jak vysvětlíme v Sekci 1.3, jejich kompletnost plyne z faktu, že jsou *ω-kategorické*, tj. mají jediný spočetný model až na *izomorfismus*. Viz Důsledek 1.3.5.

1.1.2 Důsledky Löwenheim-Skolemovy věty

V Sekci **??** jsme dokázali tzv. Löwenheim-Skolemovu větu, konkrétně její variantu pro jazyky bez rovnosti:

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

Tato věta má následující jednoduchý důsledek:

Důsledek 1.1.7. *Je-li L spočetný jazyk bez rovnosti, potom ke každé L-struktuře existuje elementárně ekvivalentní spočetně nekonečná struktura.*

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

V jazyce bez rovnosti tedy nemůžeme vyjádřit například 'model má právě 42 prvků'.

V důkazu Löwenheim-Skolemovy věty jsme sestrojený model získali jako kanonický model pro bezespornou větev tabla z T pro položku $\mathrm{F}\bot$. Stejným způsobem se dokáže následující verze pro jazyky s rovností, stačí faktorizovat dle relace $=^A$:

Věta (Löwenheim-Skolemova s rovností)**.** *Je-li L spočetný jazyk s rovností, potom každá bezesporná L-teorie má spočetný model (tj. konečný, nebo spočetně nekonečný).*

I tato verze má snadný důsledek pro konkrétní struktury:

Důsledek 1.1.8. *Je-li L spočetný jazyk s rovností, potom ke každé* nekonečné *L-struktuře existuje elementárně ekvivalentní spočetně nekonečná struktura.*

Důkaz. Mějme nekonečnou L-strukturu $\mathcal{A}$. Stejně jako v důkazu Důsledku 1.1.7 najdeme spočetně nekonečnou strukturu $\mathcal{B} \equiv \mathcal{A}$. Protože v $\mathcal{A}$ neplatí pro žádné $n \in \mathbb{N}$ sentence vyjadřující 'existuje nejvýše n prvků' (což lze pomocí rovnosti snadno zapsat), neplatí tato sentence ani v $\mathcal{B}$, $\mathcal{B}$ tedy nemůže být konečná struktura. □

Tento důsledek použijeme, abychom ukázali, že existuje spočetné těleso, které je algebraicky uzavřené:

Spočetné algebraicky uzavřené těleso

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

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

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

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

Důsledek 1.1.9. *Existuje spočetné algebraicky uzavřené těleso.*

Důkaz. Dle Důsledku 1.1.8 existuje spočetně nekonečná struktura $\mathcal{A}$ elementárně ekvivalentní tělesu $\mathbb{C}$. Protože $\mathbb{C}$ je těleso a splňuje sentence ψ_n pro všechna $n > 0$, je i $\mathcal{A}$ algebraicky uzavřené těleso. □

1.2 Izomorfismus struktur

[TODO]

Podívejme se blíže na pojem *izomorfismu struktur*, který zobecňuje izomorfismus grafů, vektorových prostorů, apod. Neformálně řečeno, struktury jsou *izomorfní*, pokud se liší jen pojmenováním konkrétních prvků.

Definice 1.2.1. Mějme struktury $\mathcal{A}, \mathcal{B}$ jazyka $L = \langle \mathcal{R}, \mathcal{F} \rangle$. *Izomorfismus $\mathcal{A}$ a $\mathcal{B}$* (nebo '*$\mathcal{A}$ na $\mathcal{B}$*') je bijekce $h\colon A \to B$ splňující následující vlastnosti:

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

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

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

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

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

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

Všimněte si, že relace 'býti izomorfní' je ekvivalence. Ukažme si jeden příklad:

Příklad 1.2.2. Je-li $|X| = n$, je potenční algebra $\underline{\mathcal{P}(X)} = \langle \mathcal{P}(X), -, \cap, \cup, \emptyset, X \rangle$ izomorfní s Booleovou algebrou $\underline{2^n} = \langle \{0,1\}^n, -_n, \wedge_n, \vee_n, (0, \dots, 0), (1, \dots, 1) \rangle$ (kde operace aplikujeme po složkách) via $h(A) = \chi_A$, kde χ_A je charakteristický vektor podmnožiny $A \subseteq X$.

Nyní ukážeme, že izomorfismus je bijekce 'zachovávající sémantiku':

Tvrzení 1.2.3. *Mějme struktury $\mathcal{A}, \mathcal{B}$ jazyka $L = \langle \mathcal{R}, \mathcal{F} \rangle$. Bijekce $h\colon A \to B$ je izomorfismus $\mathcal{A}$ a $\mathcal{B}$, právě když platí následující:*

(i) pro každý L-term t a ohodnocení proměnných $e : \mathrm{Var} \to A$:

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

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

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

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

Jako okamžitý důsledek dostáváme fakt, že izomorfní struktury jsou elementárně ekvivalentní:

Důsledek 1.2.4. *Pokud $\mathcal{A} \simeq \mathcal{B}$, potom $\mathcal{A} \equiv \mathcal{B}$.*

Poznámka 1.2.5. Obrácená implikace ale obecně neplatí, například pro uspořádané množiny racionálních a reálných čísel platí $\langle \mathbb{Q}, \leq \rangle \equiv \langle \mathbb{R}, \leq \rangle$ ale $\langle \mathbb{Q}, \leq \rangle \not\simeq \langle \mathbb{R}, \leq \rangle$ neboť $\mathbb{Q}$ je spočetná množina zatímco $\mathbb{R}$ není (neexistuje tedy mezi nimi žádná bijekce).

Pro konečné modely ale platí, že izomorfismus je totéž co elementární ekvivalence, máme-li jazyk s rovností, jak dokážeme v následujícím tvrzení:

Tvrzení 1.2.6. *Je-li L jazyk s rovností a $\mathcal{A}, \mathcal{B}$ konečné L-struktury, potom platí:*

$$\mathcal{A} \simeq \mathcal{B} \quad \textit{právě když} \quad \mathcal{A} \equiv \mathcal{B}$$

Důkaz. Jednu implikaci jsme dokázali v Důsledku 1.2.4. Předpokládejme, že $\mathcal{A} \equiv \mathcal{B}$ a ukažme, že existuje izomorfismus $\mathcal{A}$ na $\mathcal{B}$. Protože je jazyk s rovností, můžeme vyjádřit sentencí, že 'existuje právě n prvků'. Z toho plyne, že $|A| = |B|$.

Označme jako $\mathcal{A}'$ expanzi $\mathcal{A}$ o jména prvků z A; jde o strukturu v jazyce $L' = L \cup \{c_a \mid a \in A\}$. Ukážeme, že $\mathcal{B}$ lze expandovat na L'-strukturu $\mathcal{B}$ tak, že $\mathcal{A}' \equiv \mathcal{B}'$. Potom, jak lze snadno ověřit, je zobrazení $h(a) = c_a^{\mathcal{B}'}$ izomorfismem $\mathcal{A}'$ na $\mathcal{B}'$, a tedy i izomorfismem jejich L-reduktů a $\mathcal{A} \simeq \mathcal{B}$.

Stačí ukázat, že pro každé $c_a^{\mathcal{A}'} = a \in A$ existuje prvek $b \in B$ takový, že pro expanze o interpretaci konstantního symbolu c_a platí $\langle \mathcal{A}, a \rangle \equiv \langle \mathcal{B}, b \rangle$. Označme jako Ω množinu formulí $\varphi(x)$ takových, že $\langle \mathcal{A}, a \rangle \models \varphi(x/c_a)$, neboli $\mathcal{A} \models \varphi[e(x/a)]$. Protože je A konečná množina, existuje konečně mnoho formulí $\varphi_1(x), \ldots, \varphi_m(x)$ takových, že pro každou formuli $\varphi \in \Omega$ existuje i takové, že $\mathcal{A} \models \varphi \leftrightarrow \varphi_i$. Potom i $\mathcal{B} \models \varphi \leftrightarrow \varphi_i$ (neboť $\mathcal{A} \equiv \mathcal{B}$, stačí vzít generální uzávěr této formule, což je sentence).

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

Důsledek 1.2.7. *Pokud má kompletní teorie v jazyce s rovností konečný model, potom jsou všechny její modely izomorfní.*

1.2.1 Definovatelnost a automorfismy

Připomeňme si pojem definovatelné množiny, viz Sekce **??**. Ukážeme si užitečnou vlastnost definovatelných množin: jsou uzavřené ('invariantní') na automorfismy dané struktury.

Nikoho nepřekvapí, že při automorfismu se musí izolovaný vrchol daného grafu zobrazit na izolovaný vrchol, vrchol stupně 4 na vrchol stejného stupně, nebo třeba trojice vrcholů, která tvoří trojúhelník, na trojúhelník. To nám může pomoci například při hledání automorfismů.

Tvrzení 1.2.8. *Je-li $D \subseteq A^n$ definovatelná ve struktuře $\mathcal{A}$, potom pro každý automorfismus $h \in \mathrm{Aut}(\mathcal{A})$ platí $h[D] = D$ (kde $h[D]$ značí $\{(h(\overline{a}) \mid \overline{a} \in D\}$).*

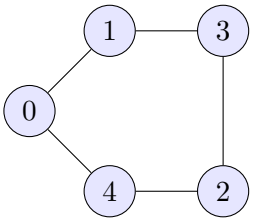
Je-li D definovatelná s parametry $\overline{b}$, platí totéž pro automorfismy identické na $\overline{b}$, tj. takové, že $h(\overline{b}) = \overline{b}$ (neboli $h(b_i) = b_i$ pro všechna i).

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

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

□

Příklad 1.2.9. Uvažme následující graf $\mathcal{G}$. Najděme všechny množiny definovatelné z $\mathcal{G}$ s parametrem 0, tj. množinu $\mathrm{Df}^1(\mathcal{G}, \{0\})$.



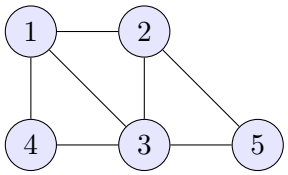
Tento graf má jediný netriviální automorfismus zachovávající vrchol 0: $h(i) = 5 - i$. Jeho *orbity* jsou $\{0\}$, $\{1, 4\}$, a $\{2, 3\}$. Tyto množiny jsou definovatelné:

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

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

$$\mathrm{Df}^1(\mathcal{G}, \{0\}) = \{\emptyset, \{0\}, \{1, 4\}, \{2, 3\}, \{0, 1, 4\}, \{0, 2, 3\}, \{1, 4, 2, 3\}, \{0, 1, 2, 3, 4\}\}$$

Cvičení 1.1. Uvažme následující graf. Najděte všechny automorfismy. Určete, které podmnožiny jsou definovatelné, uveďte definující formule. Které binární relace jsou definovatelné?



1.3 ω-kategorické teorie

Nyní se podíváme na teorie, které mají jediný spočetně nekonečný model (až na izomorfismus), říkáme jim *ω-kategorické*.[6]

Definice 1.3.1 (Izomorfní spektrum, κ-kategoricita)**.** *Izomorfní spektrum* teorie T je počet $I(\kappa, T)$ modelů T kardinality κ až na izomorfismus, pro každou kardinalitu κ (včetně *transfinitních*). Teorie T je *κ-kategorická*, pokud $I(\kappa, T) = 1$.

Nadále nás bude zajímat jen případ $\kappa = \omega$, totiž teorie s jediným spočetně nekonečným modelem (až na izomorfismus). Jako příklad uveďme teorii hustého lineárního uspořádání bez konců:

Tvrzení 1.3.2. *Teorie DeLO je ω-kategorická.*

Důkaz. Vezměme dva spočetně nekonečné modely $\mathcal{A}, \mathcal{B}$ a očíslujme jejich prvky: $A = \{a_i \mid i \in \mathbb{N}\}$, $B = \{b_i \mid i \in \mathbb{N}\}$. Indukcí podle n lze díky hustotě nalézt posloupnost $h_0 \subseteq h_1 \subseteq h_2 \subseteq \dots$ prostých (parciálních) funkcí z A do B, takových, že $\{a_0, \dots, a_{n-1}\} \subseteq \operatorname{dom} h_n$, $\{b_0, \dots, b_{n-1}\} \subseteq \operatorname{rng} h_n$,[7] a *zachovávají uspořádání*[8] Potom $\mathcal{A} \simeq \mathcal{B}$ via $h = \bigcup_{n\in\mathbb{N}} h_n$. □

Důsledek 1.3.3. *Izomorfní spektrum teorie DeLO* je následující:*

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

Spočetné modely až na izormofismus jsou například:

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

Důkaz. Husté uspořádání jistě nemůže být konečné. Izomorfismus musí zobrazit nejmenší prvek na nejmenší prvek, a největší na největší. □

Pojem *ω-kategoricity* lze chápat jako zeslabení pojmu *kompletnosti*. Platí následující užitečné kritérium:

Věta 1.3.4 (ω-kategorické kritérium kompletnosti)**.** *Mějme ω-kategorickou teorii T ve spočetném jazyce L. Je-li*

- *L bez rovnosti, nebo*
- *L s rovností a T nemá konečné modely,*

[6] Symbol ω se používá pro nejmenší nekonečné *ordinální* číslo, jinými slovy, pro množinu všech přirozených čísel.

[7] Zde dom značí *doménu* a rng značí *obor hodnot ('range')* funkce.

[8] Tj. je-li $a_i, a_j \in \operatorname{dom} h_n$, potom $a_i \leq^{\mathcal{A}} a_j$ právě když $h(a_i) \leq^{\mathcal{B}} h(b_j)$.

potom je teorie T kompletní.

Důkaz. Pro jazyk bez rovnosti víme z Důsledku 1.1.7 Löwenheim-Skolemovy věty, že každý model je elementárně ekvivalentní nějakému spočetně nekonečnému modelu. Ten je ale až na izomorfismus jediný, takže všechny modely jsou elementárně ekvivalentní, což je sémantická definice kompletnosti.

Máme-li jazyk s rovností, použijeme podobně Důsledek 1.1.8 a dostaneme, že všechny nekonečné modely jsou elementárně ekvivalentní. Mohly by existovat elementárně neekvivalentní konečné modely, to jsme ale zakázali. □

Důsledek 1.3.5. *Teorie* DeLO*,* DeLO^+*,* DeLO^-*, a* $\mathrm{DeLO}^\pm$ *jsou kompletní. Jsou to všechny (navzájem neekvivalentní) kompletní jednoduché extenze teorie DeLO***.*

Poznámka 1.3.6. Analogické kritérium platí i pro kardinality κ větší než ω.

1.4 Axiomatizovatelnost

Na závěr této kapitoly se podíváme, za jakých okolností lze 'popsat' (*axiomatizovat*) třídu modelů respektive teorii. Zajímat nás bude také kdy si vystačíme s konečně mnoha axiomy, a kdy to lze pomocí otevřených axiomů (kterých může být i nekonečně mnoho). Srovnejte s Tvrzením **??** z výrokové logiky.

Definice 1.4.1 (Axiomatizovatelnost)**.** Mějme třídu struktur $K \subseteq \mathrm{M}_L$ v nějakém jazyce L. Říkáme, že K je

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

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

Příklad 1.4.2. Uveďme několik příkladů:

- grafy nebo částečná uspořádání jsou konečně i otevřeně axiomatizovatelné,
- tělesa jsou konečně, ale ne otevřeně axiomatizovatelná,
- nekonečné grupy jsou axiomatizovatelné, ale ne konečně,
- konečné grafy nejsou axiomatizovatelné.

Proč tomu tak je ukážeme níže.

Začněme jednoduchým faktem:

Pozorování 1.4.3. *Je-li K axiomatizovatelná, musí být uzavřená na elementární ekvivalenci.*

Z věty o kompaktnosti snadno získáme následující tvrzení, pomocí kterého lze ukázat neaxiomatizovalnost např. konečných grafů, konečných grup, konečných těles.

Věta 1.4.4. *Pokud má teorie libovolně velké konečné modely, potom má i nekonečný model. V tom případě není třída všech jejích konečných modelů axiomatizovatelná.*

Důkaz. Je-li jazyk bez rovnosti, stačí vzít kanonický model pro některou bezespornou větev v tablu z T pro položku F$\bot$ (T je bezesporná, neboť má model(y), tedy tablo není sporné).

Mějme jazyk s rovností a označme jako T' následující extenzi teorie T' do jazyka rozšířeného o spočetně mnoho nových konstantních symbolů c_i:

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

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

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

Poznámka 1.4.5. Třída všech *nekonečných* modelů teorie ale je vždy axiomatizovatelná, máme-li jazyk s rovností: stačí k teorii přidat pro každé $n \in \mathbb{N}$ axiom vyjadřující 'existuje alespoň n prvků'.

1.4.1 Konečná axiomatizovatelnost

Ukážeme následující kritérium konečné axiomatizovatelnosti: jak třída struktur K tak i $\overline{K}$ musí být axiomatizovatelné.

Věta 1.4.6. *[O konečné axiomatizovatelnosti] Mějme třídu struktur $K \subseteq \mathrm{M}_L$ a uvažme také její doplněk $\overline{K} = \mathrm{M}_L \setminus K$. Potom K je konečně axiomatizovatelná, právě když K i $\overline{K}$ jsou axiomatizovatelné.*

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

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

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

Podle věty o kompaktnosti[9] existují konečné podteorie $T' \subseteq T$ a $S' \subseteq S$ takové, že:

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

Nyní si všimněme, že platí

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

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

Jako aplikaci si dokážeme, že tělesa charakteristiky 0 nejsou konečně axiomatizovatelná.

[9] Vidíte, jak je užitečná!

Příklad: tělesa charakteristiky 0

Nechť T je teorie těles. Charakteristika tělesa je nejmenší počet jedniček, které je třeba sečíst, abychom dostali nulu (v tom případě musí být charakteristika prvočíslo—dokažte si!), nebo, pokud nikdy nedostaneme sčítáním jedniček nulu, říkáme že je charakteristika 0. Trochu formálněji:

Definice 1.4.7 (Charakteristika tělesa)**.** Říkáme, že těleso $\mathcal{A} = \langle A, +, -, 0, \cdot, 1\rangle$ je

- *charakteristiky* p, je-li p nejmenší prvočíslo takové, že $\mathcal{A} \models p1 = 0$, kde $p1$ označuje term $1 + 1 + \cdots + 1$ s p jedničkami, nebo
- *charakteristiky 0*, pokud není charakteristiky p pro žádné prvočíslo p.

Nechť T je teorie těles. Potom třída těles charakteristiky p je konečně axiomatizována teorií $T \cup \{p1 = 0\}$. Třída těles charakteristiky 0 je axiomatizována následující (nekonečnou) teorií:

$$T' = T \cup \{\neg\, p1 = 0 \mid p \text{ je prvočíslo}\}$$

Konečná axiomatizace ale neexistuje.

Tvrzení 1.4.8. *Třída K těles charakteristiky 0 není konečně axiomatizovatelná.*

Důkaz. Díky Větě 1.4.6 stačí ukázat, že $\overline{K}$ (tělesa nenulové charakteristiky) není axiomatizovatelná, což dokážeme sporem. Nechť existuje teorie S taková, že $\mathrm{M}(S) = \overline{K}$. Potom teorie $S' = S \cup T'$ má model, neboť každá její konečná část má model: stačí vzít těleso prvočíselné charakteristiky větší než jakékoliv p z axiomu T' tvaru $\neg\, p1 = 0$. Nechť $\mathcal{A}$ je model S'. Potom je i $\mathcal{A} \in \mathrm{M}(S) = \overline{K}$. Zároveň je ale $\mathcal{A} \in \mathrm{M}(T') = K$, což je spor. □

1.4.2 Otevřená axiomatizovatelnost

Pro otevřenou axiomatizovatelnost existuje jednoduché sémantické kritérium: třída jejích modelů být uzavřená na podstruktury. Platí dokonce ekvivalence, dokážeme ale jen jednu implikaci (důkaz druhé je obtížnější).

Věta 1.4.9. *Pokud je teorie T otevřeně axiomatizovatelná, potom je každá podstruktura modelu T také modelem T.*

Poznámka 1.4.10. Platí i obrácená implikace: Je-li každá podstruktura modelu T také modelem, potom je T otevřeně axiomatizovatelná. Důkaz zde ale neuvedeme.

Důkaz. Nechť T' je otevřená axiomatizace T. Mějme model $\mathcal{A} \models T'$ a podstrukturu $\mathcal{B} \subseteq \mathcal{A}$. Pro každou formuli $\varphi \in T'$ platí $\mathcal{B} \models \varphi$ (neboť φ je otevřená), tedy i $\mathcal{B} \models T'$. □

Příklad 1.4.11. Uveďme několik příkladů:

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

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

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

Kapitola 2

(draft) Nerozhodnutelnost a neúplnost

[TODO]

2.1 Rozhodnutelnost

[TODO]

Rekurzivní axiomatizace a rozhodnutelnost

- Intuitivní pojem *"algoritmus"* lze přesně formalizovat (např. pomocí TS).
- Teorie T je *rekurzivně axiomatizovaná*, pokud existuje algoritmus, který pro každou vstupní formuli φ skončí a oznámí, zda $\varphi \in T$.
- Teorie T je *rozhodnutelná*, pokud existuje algoritmus, který pro každou vstupní formuli φ skončí a oznámí, zda $\varphi \in Thm(T)$.
- Teorie T je *částečně rozhodnutelná*, pokud existuje algoritmus, který pro každou vstupní formuli φ skončí, právě když $\varphi \in Thm(T)$.

Tvrzení *Pro každou rekurzivně axiomatizovanou teorii T,*

(*i*) *T je částečně rozhodnutelná,*

(*ii*) *je-li navíc T kompletní, je T rozhodnutelná.*

Důkaz Konstrukce systematického tabla z T s $F\varphi$ v kořeni poskytuje algoritmus, který rozpoznává $T \vdash \varphi$. Je-li navíc T kompletní, paralelní konstrukce pro $F\varphi$ resp. $T\varphi$ v kořeni rozhoduje, zda $T \vdash \varphi$ či $T \vdash \neg\varphi$. □

Rekurzivně spočetná kompletace

Co když efektivně popíšeme všechny jednoduché kompletní extenze?

Řekneme, že množina všech (až na ekvivalenci) jednoduchých kompletních extenzí teorie T je *rekurzivně spočetná*, existuje-li algoritmus $\alpha(i, j)$, který generuje i-tý axiom j-té extenze (při nějakém očíslování), případně oznámí, že (takový axiom či extenze) neexistuje.

Tvrzení *Je-li teorie T rekurzivně axiomatizovaná a množina všech (až na ekvivalenci) jejích jednoduchých kompletních extenzí je rekurzivně spočetná, je T rozhodnutelná.*

Důkaz Díky rek. axiomatizaci poskytuje konstrukce systematického tabla z T s $F\varphi$ v kořeni algoritmus pro rozpoznání $T \vdash \varphi$. Pokud ale $T \nvdash \varphi$, pak $T' \vdash \neg\varphi$ v nějaké jednoduché kompletní extenzi T' teorie T. To lze rozpoznat paralelní postupnou konstrukcí systematických tabel pro $T\varphi$ z jednotlivých extenzí. V i-tém stupni se sestrojí tabla do i kroků pro prvních i extenzí. □

2.1.1 Rozhodnutelné teorie

[TODO]

Příklady rozhodnutelných teorií

Následující teorie jsou rozhodnutelné, ačkoliv jsou nekompletní.

- teorie čisté rovnosti; bez axiomů v jazyce $L = \langle\rangle$ s rovností,
- teorie unárního predikátu; bez axiomů v jazyce $L = \langle U\rangle$ s rovností, kde U je unární relační symbol,
- teorie hustých lineárních uspořádání $DeLO^*$,
- teorie algebraicky uzavřených těles v jazyce $L = \langle +, -, \cdot, 0, 1\rangle$ s rovností, s axiomy teorie těles a navíc axiomy pro každé $n \geq 1$,

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

  kde y^k je zkratka za term $y \cdot y \cdot \ \cdots \ \cdot y$ ($\cdot$ aplikováno $(k-1)$-krát).
- teorie komutativních grup,
- teorie Booleových algeber.

2.1.2 Rekurzivní axiomatizovatelnost

[TODO]

Rekurzivní axiomatizovatelnost

Dají se matematické struktury "efektivně" popsat?

- Třída $K \subseteq M(L)$ je *rekurzivně axiomatizovatelná*, pokud existuje rekurzivně axiomatizovaná teorie T jazyka L s $M(T) = K$.
- Teorie T je rekurzivně axiomatizovatelná, pokud $M(T)$ je rekurzivně axiomatizovatelná.

Tvrzení *Pro každou konečnou strukturu $\mathcal{A}$ v konečném jazyce s rovností je* $\mathrm{Th}(\mathcal{A})$ *rekurzivně axiomatizovatelná. Tedy,* $\mathrm{Th}(\mathcal{A})$ *je rozhodnutelná.*

Důkaz Nechť $A = \{a_1, \ldots, a_n\}$. Teorii $\mathrm{Th}(\mathcal{A})$ axiomatizujeme jednou sentencí (tedy rekurzivně) kompletně popisující $\mathcal{A}$. Bude tvaru *"existuje právě n prvků $a_1, \ldots, a_n$ splňujících právě ty základní vztahy o funkčních hodnotách a relacích, které platí ve struktuře $\mathcal{A}$."* □

Příklady rekurzivní axiomatizovatelnosti

Následující struktury $\mathcal{A}$ mají rekurzivně axiomatizovatelnou teorii $\mathrm{Th}(\mathcal{A})$.

- $\langle \mathbb{Z}, \leq \rangle$, teorií diskrétních lineárních uspořádání,
- $\langle \mathbb{Q}, \leq \rangle$, teorií hustých lineárních uspořádání bez konců ($DeLO$),
- $\langle \mathbb{N}, S, 0 \rangle$, teorií následníka s nulou,
- $\langle \mathbb{N}, S, +, 0 \rangle$, tzv. Presburgerovou aritmetikou,
- $\langle \mathbb{R}, +, -, \cdot, 0, 1 \rangle$, teorií reálně uzavřených těles,
- $\langle \mathbb{C}, +, -, \cdot, 0, 1 \rangle$, teorií algebraicky uzavřených těles charakteristiky 0.

Důsledek *Pro uvedené struktury je* $\mathrm{Th}(\mathcal{A})$ *rozhodnutelná.*

Poznámka *Uvidíme, že ale* $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$ *rekurzivně axiomatizovat* nelze. *(Vyplývá to z první Gödelovy věty o neúplnosti).*

2.2 Aritmetika

[TODO]

2.2.1 Robinsonova a Peanova aritmetika

[TODO]

Robinsonova aritmetika

Jak efektivně a přitom co nejúplněji axiomatizovat $\underline{\mathbb{N}} = \langle \mathbb{N}, S, +, \cdot, 0, \leq \rangle$*?*

Jazyk aritmetiky je $L = \langle S, +, \cdot, 0, \leq \rangle$ s rovností.

Robinsonova aritmetika Q má axiomy (konečně mnoho)

$$\begin{array}{ll} S(x) \neq 0 & x \cdot 0 = 0 \\ S(x) = S(y) \to x = y & x \cdot S(y) = x \cdot y + x \\ x + 0 = x & x \neq 0 \to (\exists y)(x = S(y)) \\ x + S(y) = S(x + y) & x \leq y \leftrightarrow (\exists z)(z + x = y) \end{array}$$

Poznámka Q *je velmi slabá, např. nedokazuje komutativitu či asociativitu operací* $+, \cdot$ *ani tranzitivitu* $\leq$*. Nicméně postačuje například k důkazu existenčních tvrzení o numerálech, která jsou pravdivá v* $\underline{\mathbb{N}}$*.*

Např. pro $\varphi(x, y)$ *tvaru* $(\exists z)(x + z = y)$ *je*

$$Q \vdash \varphi(\underline{1}, \underline{2}), \quad \textit{kde } \underline{1} = S(0) \textit{ a } \underline{2} = S(S(0)).$$

Peanova aritmetika

Peanova aritmetika PA má axiomy

(a) Robinsonovy aritmetiky Q,

(b) schéma indukce, tj. pro každou formuli $\varphi(x, \overline{y})$ jazyka L axiom

$$(\varphi(0, \overline{y}) \wedge (\forall x)(\varphi(x, \overline{y}) \to \varphi(S(x), \overline{y}))) \to (\forall x)\varphi(x, \overline{y}).$$

Poznámka PA *je poměrně dobrou aproximací* $\mathrm{Th}(\underline{\mathbb{N}})$*, dokazuje všechny základní vlastnosti platné v* $\underline{\mathbb{N}}$ *(např. komutativitu* $+$*). Na druhou stranu existují sentence pravdivé v* $\underline{\mathbb{N}}$ *ale nezávislé v* PA*.*

Poznámka V jazyce 2. řádu lze axiomatizovat $\underline{\mathbb{N}}$ *(až na izomorfismus), vezmeme-li místo schéma indukce přímo axiom indukce (2. řádu)*

$$(\forall X)\ ((X(0) \wedge (\forall x)(X(x) \to X(S(x)))) \to (\forall x)\ X(x)).$$

2.2.2 Hilbertův desátý problém

[TODO]

Hilbertův 10. problém

- Nechť $p(x_1, \ldots, x_n)$ je polynom s celočíselnými koeficienty.

  Má *Diofantická rovnice* $p(x_1, \ldots, x_n) = 0$ celočíselné řešení?

- Hilbert (1900) *"Nalezněte algoritmus, který po konečně mnoha krocích určí, zda daná Diofantická rovnice s libovolným počtem proměnných a celočíselnými koeficienty má celočíselné řešení."*

Poznámka *Ekvivalentně lze požadovat algoritmus rozhodující, zda existuje řešení v přirozených číslech.*

Věta (DPRM, 1970) *Problém existence celočíselného řešení dané Diofantické rovnice s celočíselnými koeficienty je alg. nerozhodnutelný.*

Důsledek *Neexistuje algoritmus rozhodující pro dané polynomy* $p(x_1, \ldots, x_n)$, $q(x_1, \ldots, x_n)$ *s přirozenými koeficienty, zda*

$$\underline{\mathbb{N}} \models (\exists x_1) \ldots (\exists x_n)(p(x_1, \ldots, x_n) = q(x_1, \ldots, x_n)).$$

2.3 Nerozhodnutelnost predikátové logiky

[TODO]

Nerozhodutelnost predikátové logiky

Existuje algoritmus, rozhodující o dané sentenci, zda je logicky pravdivá?

- Víme, že Robinsonova aritmetika Q má konečně axiomů, má za model $\underline{\mathbb{N}}$ a stačí k důkazu existenčních tvrzení o numerálech, která platí v $\underline{\mathbb{N}}$.
- Přesněji, pro každou existenční formuli $\varphi(x_1, \ldots, x_n)$ jazyka aritmetiky

  $$Q \vdash \varphi(x_1/\underline{a_1}, \ldots, x_n/\underline{a_n}) \quad \Leftrightarrow \quad \underline{\mathbb{N}} \models \varphi[e(x_1/a_1, \ldots, x_n/a_n)]$$

  pro každé $a_1, \ldots, a_n \in \mathbb{N}$, kde $\underline{a_i}$ značí a_i-tý numerál.

- Speciálně, pro φ tvaru $(\exists x_1)\dots(\exists x_n)(p(x_1,\dots,x_n) = q(x_1,\dots,x_n))$, kde p, q jsou polynomy s přirozenými koeficienty (numerály), platí

$$\underline{\mathbb{N}} \models \varphi \quad \Leftrightarrow \quad Q \vdash \varphi \quad \Leftrightarrow \quad \vdash \psi \to \varphi \quad \Leftrightarrow \quad \models \psi \to \varphi,$$

  kde ψ je konjunkce (uzávěrů) všech axiomů Q.

- Tedy, pokud by existoval algoritmus rozhodující logickou pravdivost, existoval by i algoritmus rozhodující, zda $\underline{\mathbb{N}} \models \varphi$, což není možné.

2.4 Gödelovy věty

[TODO]

2.4.1 První věta o neúplnosti

[TODO]

Gödelova 1. věta o neúplnosti

Věta (Gödel) *Pro každou bezespornou rekurzivně axiomatizovanou extenzi T Robinsonovy aritmetiky existuje sentence pravdivá v $\underline{\mathbb{N}}$ a nedokazatelná v T.*

Poznámky

- *"Rekurzivně axiomatizovaná" znamená, že je* "efektivně zadaná".
- *"Extenze R. aritmetiky" znamená, že je* "základní aritmetické síly".
- *Je-li navíc $\underline{\mathbb{N}} \models T$, je teorie T nekompletní.*
- *V důkazu sestrojená sentence vyjadřuje* "nejsem dokazatelná v T".
- *Důkaz je založen na dvou principech:*

  (*a*) *aritmetizaci syntaxe,*

  (*b*) *self-referenci.*

Aritmetizace dokazatelnosti

Aritmetizace - predikát dokazatelnosti

- Konečné objekty syntaxe (symboly jazyka, termy, formule, konečná tabla, tablo důkazy) lze vhodně zakódovat přirozenými čísly.

- Nechť $\lceil\varphi\rceil$ značí kód formule φ a nechť $\underline{\varphi}$ značí numerál (term jazyka aritmetiky) reprezentující $\lceil\varphi\rceil$.
- Je-li T rekurzivně axiomatizovaná, je relace $\mathrm{Prf}_T \subseteq \mathbb{N}^2$ rekurzivní.

$$\mathrm{Prf}_T(x,y) \quad \Leftrightarrow \quad \textit{(tablo) } y \textit{ je důkazem (sentence) } x \textit{ v } T.$$

- Je-li T navíc extenze Robinsonovy aritmetiky Q, dá se dokázat, že Prf_T je reprezentovatelná nějakou formulí $Prf_T(x,y)$ tak, že pro každé $x, y \in \mathbb{N}$

$$\begin{array}{ll} Q \vdash Prf_T(\underline{x},\underline{y}), & \textit{je-li} \quad \mathrm{Prf}_T(x,y), \\ Q \vdash \neg Prf_T(\underline{x},\underline{y}), & \textit{jinak.} \end{array}$$

- $Prf_T(x,y)$ vyjadřuje *"y je důkaz x v T"*.
- $(\exists y)Prf_T(x,y)$ vyjadřuje *"x je dokazatelná v T"*.
- Je-li $T \vdash \varphi$, pak $\underline{\mathbb{N}} \models (\exists y)Prf_T(\underline{\varphi},y)$ a navíc $T \vdash (\exists y)Prf_T(\underline{\varphi},y)$.

Self-reference

Princip self-reference

- *Tato věta má 16 písmen.*

  Self-reference ve formálních systémech většinou není přímo k dispozici.

- *Následující věta má 24 písmen "Následující věta má 24 písmen".*

  Přímá reference obvykle je k dispozici, stačí, když umíme "mluvit" o posloupnostech symbolů. Uvedená věta ale není self-referenční.

- *Následující věta zapsaná jednou a ještě jednou v uvozovkách má 116 písmen "Následující věta zapsaná jednou a ještě jednou v uvozovkách má 116 písmen".*

  Pomocí přímé reference lze dosáhnout self-reference. Namísto *"má x písmen"* může být jiná vlastnost.

- `main(){char *c="main(){char *c=%c%s%c; printf(c,34, c,34);}"; printf(c,34,c,34);}`

Věta o pevném bodě

Věta *Nechť T je bezesporné rozšíření Robinsonovy aritmetiky. Pro každou formuli $\varphi(x)$ jazyka teorie T existuje sentence ψ taková, že $T \vdash \psi \leftrightarrow \varphi(\underline{\psi})$.*

Poznámka *Sentence ψ je self-referenční, říká* "splňuji podmínku φ".

Důkaz (idea) Uvažme *zdvojující* funkci d takovou, že pro každou formuli $\chi(x)$

$$d(\ulcorner \chi(x) \urcorner) = \ulcorner \chi(\underline{\chi(x)}) \urcorner$$

- Platí, že d je reprezentovatelná v T. Předpokládejme *(pro jednoduchost)*, že nějakým termem, který si označme d, stejně jako funkci d.
- Pak pro každou formuli $\chi(x)$ jazyka teorie T platí

$$T \vdash d(\underline{\chi(x)}) = \underline{\chi(\underline{\chi(x)})} \tag{2.1}$$

- Za ψ vezměme sentenci $\varphi(d(\underline{\varphi(d(x))}))$. Stačí ověřit $T \vdash d(\underline{\varphi(d(x))}) = \underline{\psi}$.
- To plyne z (2.1) pro $\chi(x)$ tvaru $\varphi(d(x))$, neboť v tom případě

$$T \vdash d(\underline{\varphi(d(x))}) = \underline{\varphi(d(\underline{\varphi(d(x))}))} \quad \square$$

Nedefinovatelnost pravdy

Nedefinovatelnost pravdy

Řekneme, že formule $\tau(x)$ *definuje pravdu* v aritmetické teorii T, pokud pro každou sentenci φ platí $T \vdash \varphi \leftrightarrow \tau(\underline{\varphi})$.

Věta *V žádném bezesporném rozšíření Robinsonovy aritmetiky neexistuje definice pravdy.*

Důkaz Dle věty o pevném bodě pro $\neg\tau(x)$ existuje sentence φ taková, že

$$T \vdash \varphi \leftrightarrow \neg\tau(\underline{\varphi}).$$

Kdyby formule $\tau(x)$ definovala pravdu v T, bylo by

$$T \vdash \varphi \leftrightarrow \neg\varphi,$$

což v bezesporné teorii není možné. $\square$

Poznámka *Důkaz je založen na paradoxu lháře, sentence φ by vyjadřovala "nejsem pravdivá v T".*

1. věta o neúplnosti

Důkaz 1. věty o neúplnosti

Věta (Gödel) *Pro každou bezespornou rekurzivně axiomatizovanou extenzi T Robinsonovy aritmetiky existuje sentence pravdivá v $\underline{\mathbb{N}}$ a nedokazatelná v T.*

Důkaz Nechť $\varphi(x)$ je $\neg(\exists y)Prf_T(x,y)$, vyjadřuje *"$x$ není dokazatelná v T"*.

- Dle věty o pevném bodě pro $\varphi(x)$ existuje sentence ψ_T taková, že

$$T \vdash \psi_T \leftrightarrow \neg(\exists y)Prf_T(\underline{\psi_T}, y). \tag{2.2}$$

  ψ_T říká *"nejsem dokazatelná v T"*. Přesněji, ψ_T je ekvivalentní sentenci vyjadřující, že ψ_T není dokazatelná v T. (Ekvivalence platí v $\underline{\mathbb{N}}$ i v T).

- Nejprve ukážeme, že ψ_T *není dokazatelná v T*. Kdyby $T \vdash \psi_T$, tj. ψ_T je lživá v $\underline{\mathbb{N}}$, pak $\underline{\mathbb{N}} \models (\exists y)Prf_T(\underline{\psi_T}, y)$ a navíc $T \vdash (\exists y)Prf_T(\underline{\psi_T}, y)$. Tedy z (2.2) plyne $T \vdash \neg\psi_T$, což ale není možné, neboť T je bezesporná.

- Zbývá dokázat, že ψ_T je pravdivá v $\underline{\mathbb{N}}$. Kdyby ne, tj. $\underline{\mathbb{N}} \models \neg\psi_T$, pak $\underline{\mathbb{N}} \models (\exists y)Prf_T(\underline{\psi_T}, y)$. Tedy $T \vdash \psi_T$, což jsme již dokázali, že neplatí. □

2.4.2 Důsledky první věty

[TODO]

Důsledky a zesílení 1. věty

Důsledek *Je-li navíc $\underline{\mathbb{N}} \models T$, je teorie T nekompletní.*

Důkaz Kdyby byla T kompletní, pak $T \vdash \neg\psi_T$ a tedy $\underline{\mathbb{N}} \models \neg\psi_T$, což je ve sporu s $\underline{\mathbb{N}} \models \psi_T$. □

Důsledek Th($\underline{\mathbb{N}}$) *není rekurzivně axiomatizovatelná.*

Důkaz Th($\underline{\mathbb{N}}$) je bezesporná extenze Robinsonovy aritmetiky a má model $\underline{\mathbb{N}}$. Kdyby byla rekurzivně axiomatizovatelná, dle předchozího důsledku by byla nekompletní, ale Th($\underline{\mathbb{N}}$) je kompletní. □

Gödelovu 1. větu o neúplnosti lze následovně zesílit.

Věta (Rosser) *Pro každou bezespornou rekurzivně axiomatizovanou extenzi T Robinsonovy aritmetiky existuje nezávislá sentence. Tedy T je nekompletní.*
Poznámka Tedy předpoklad, že $\underline{\mathbb{N}} \models T$, je v prvním důsledku nadbytečný.

2.4.3 Druhá věta o neúplnosti

[TODO]

Gödelova 2. věta o neúplnosti

Označme Con_T sentenci $\neg(\exists y)Prf_T(\underline{0=1}, y)$. Platí $\underline{\mathbb{N}} \models Con_T \Leftrightarrow T \nvdash 0 = \underline{1}$. Tedy Con_T vyjadřuje, že *"T je bezesporná"*.

Věta (Gödel) *Pro každou bezespornou rekurzivně axiomatizovanou extenzi T Peanovy aritmetiky platí, že Con_T není dokazatelná v T.*

Důkaz (náznak) Nechť ψ_T je Gödelova sentence *"nejsem dokazatelná v T"*.

- V první části důkazu 1. věty o neúplnosti jsme ukázali, že

$$\text{"Je-li } T \text{ bezesporná, pak } \psi_T \text{ není dokazatelná v } T\text{."} \tag{2.3}$$

  Jinak vyjádřeno, platí $Con_T \to \psi_T$.

- Je-li T extenze Peanovy aritmetiky, důkaz tvrzení (2.3) lze formalizovat v rámci T. Tedy $T \vdash Con_T \to \psi_T$.
- Jelikož T je bezesporná dle předpokladu věty, podle (2.3) je $T \nvdash \psi_T$.
- Z předchozích dvou bodů vyplývá, že $T \nvdash Con_T$. □

Poznámka Taková teorie T tedy neumí dokázat vlastní bezespornost.

2.4.4 Důsledky druhé věty

[TODO]

Důsledky 2. věty

Důsledek *Existuje model $\mathcal{A}$ Peanovy aritmetiky t.ž. $\mathcal{A} \models (\exists y)Prf_{PA}(\underline{0=1}, y)$.*

Poznámka $\mathcal{A}$ musí být nestandardní model PA, svědkem musí být nestandardní prvek (jiný než hodnoty numerálů).

Důsledek *Existuje bezesporná rekurzivně axiomatizovaná extenze T Peanovy aritmetiky taková, že $T \vdash \neg Con_T$.*

Důkaz Nechť $T = PA \cup \{\neg Con_{PA}\}$. Pak T je bezesporná, neboť $PA \nvdash Con_{PA}$. Navíc $T \vdash \neg Con_{PA}$, tj. T dokazuje spornost $PA \subseteq T$, tedy i $T \vdash \neg Con_T$. □

Poznámka $\underline{\mathbb{N}}$ nemůže být modelem teorie T.

Důsledek *Je-li teorie množin ZFC bezesporná, není Con_{ZFC} dokazatelná v ZFC.*