

Predikátová (a výroková) logika

slidy k přednášce Logika a teorie množin (NUMP016, NMUE023) –
ZS 2011/12

Petr Glivický

petrglivicky@gmail.com

Katedra teoretické informatiky a matematické logiky
Univerzita Karlova v Praze

Ke stažení na <http://www.glivicky.cz>

Doporučená literatura

Elektronická:

- **tyto slidy :-)** a další materiály k přednášce dostupné na mém webu – **primární a požadavkům na zkoušku plně dostačující zdroj** (budou průběžně doplňovány)
- **skripta doc. Mlčka**
http://ktiml.mff.cuni.cz/~mlcek/PART_11.pdf – vhodné zejména sekce 1.1., 2. s výjimkou 2.4., 3. kromě 3.6., 3.7. (částečně přesahují náplň přednášky)
- **slidy Petra Pajase**
<http://ufal.mff.cuni.cz/~pajas/vyuka/logika.pdf> – trochu jiný styl výkladu, rovněž obsahově mírně posunuto

Tištěná: (značně přesahuje rámec přednášky)

- Vítězslav Švejdar, *Logika, neúplnost, složitost a nutnost*
- Wilfrid Hodges, *Model theory*

Matematická logika

Matematická logika

- objasňuje vztah jazyka (**syntaxe**) a významu (**sémantiky**)
- formalizuje a precizuje základní pojmy – tvrzení, axiom, teorie, důkaz, pravdivost, model
- **syntaxe** – je vybudována jako kalkulus konečných sekvencí symbolů (v rámci teorie množin; pro konečné jazyky stačí předpokládat aritmetiku přirozených čísel)
- **sémantika** – je založena na pojmu struktury, vybudována v rámci teorie množin

Předběžnosti

Kapitola 1: Předběžnosti

Předběžnosti

Uvedeme nyní základní pojmy, které nám umožní přesně formalizovat syntaxi a sémantiku logiky. Uvedený výklad lze chápat jako prováděný v rámci nějaké (i naivní) **teorie množin**.

Třída daná množinovým vztahem $\mathcal{V}$ je soubor všech objektů (množin) x , o nichž $\mathcal{V}(x)$ platí, zapisujeme ji jako $\{x; \mathcal{V}(x)\}$.
Není-li třída množinou, nazývá se **vlastní třída**. Například $V = \{x; x = x\}$ je **třída všech množin**. Skutečnost, že množina x je **prvkem** třídy Y resp. množiny y , zapisujeme jako $x \in Y$ resp. $x \in y$.

Symboly $\emptyset$, $\cup$, $\cap$, $-$ značí po řadě **prázdnou množinu** (danou vztahem $\emptyset = \{x; x \neq x\}$), **sjednocení**, **průnik** a **rozdíl** množin.

Zápis $\{x_0, \dots, x_{n-1}\}$ značí množinu obsahující právě n -prvků $x_0, \dots, x_{n-1}$, speciálně $\{x, y\}$ je **neuspořádaná dvojice** množin x, y a $\{x\}$ je **singleton** x , tj. množina s jediným prvkem x .

Předběžnosti

Množiny x, y jsou **disjunktní**, je-li $x \cap y = \emptyset$. Množina x je **podmnožinou** množiny y , je-li $z \in x$, pro každé $z \in y$; značíme to $x \subseteq y$. Množina všech podmnožin y se nazývá **potence** y a značí se $\mathcal{P}(y) = \{x; x \subseteq y\}$. **Sjednocením** (též **sumou**) množiny x je množina $\bigcup x = \{z; z \in y \text{ pro nějaké } y \in x\}$.

Uspořádaná dvojice množin x, y se značí (x, y) , definuje se jako $(x, y) = \{x, \{x, y\}\}$. Indukcí definujeme **uspořádanou n -tici** $(x_0, \dots, x_{n-1})$ pro $n > 2$: $(x_0, \dots, x_{n-1}) = ((x_0, \dots, x_{n-2}), x_{n-1})$.

Kartézský součin $X \times Y$ množin X, Y je množina $\{(x, y); x \in X, y \in Y\}$. **Kartézská mocnina** množiny X je definována induktivně $X^0 = \{0\}$, $X^1 = X$, $X^n = X^{n-1} \times X$. Pro $n \geq 2$ jsou pak prvky X^n právě n -tice $(x_0, \dots, x_{n-1})$ s $x_i \in X$.

Předběžnosti

Disjunkt ní sjednocení množin x, y značíme $x \uplus y$, je definováno jako množina $(\{\emptyset\} \times x) \cup (\{\{\emptyset\}\} \times y)$.

Relace je jakákoli množina uspořádaných dvojic (i prázdná). Místo $(x, y) \in R$ píšeme někdy $R(x, y)$ či $x R y$. **Definiční obor** relace R je množina $\text{dom}(R) = \{x; \text{pro nějaké } y \text{ je } (x, y) \in R\}$, **obor hodnot** relace R je množina $\text{rng}(R) = \{y; \text{pro nějaké } x \text{ je } (x, y) \in R\}$.

Extenze prvku x v relaci R je množina $R[x] = \{y; (x, y) \in R\}$.

Relace R je na množině X

- **reflexivní**, pokud $R(x, x)$ pro $x \in X$,
- **symetrická**, pokud $R(x, y)$ implikuje $R(y, x)$ pro $x, y \in X$,
- **tranzitivní**, pokud $R(x, y)$ a $R(y, z)$ implikuje $R(x, z)$ pro $x, y, z \in X$.

Předběžnosti

Relace R , která je reflexivní, symetrická a tranzitivní na X a $\text{dom}(R) = \text{rng}(R) = X$, se nazývá **ekvivalence** na X .

Je-li R ekvivalence na X , nazýváme množinu $R[x]$ **faktor** či **třída ekvivalence** prvku x dle R a $X/R = \{R[x]; x \in X\}$ **faktORIZACE** X dle R . Pro různé faktory $a, b \in X/R$ je $a \cap b = \emptyset$ a dále $\bigcup X/R = X$, říkáme, že X/R tvoří **rozklad** X dle R .

Existuje-li pro každé $x \in \text{dom}(R)$ jediné y s $R(x, y)$, říkáme, že R je **funkce**. Píšeme pak $R(x)$ místo y (pak $R(x) = y$ značí $R(x, y)$) a y nazýváme **hodnotou** funkce R v x . Zápis $f : X \rightarrow Y$ čteme **f je funkce z X do Y** a značí, že f je funkce s $\text{dom}(f) = X$ a $\text{rng}(f) \subseteq Y$. Funkce f je **prostá**, když pro $x \neq y$ z $\text{dom}(f)$ je $f(x) \neq f(y)$, a je **na** Y , když $\text{rng}(f) = Y$. Dále $f : X \rightarrow Y$ je **bijekce** X a Y , je-li prostá a na Y .

Předběžnosti

Pro prostou funkci $f : X \rightarrow Y$ je $f^{-1} = \{(y, x); (x, y) \in f\}$
inverzní funkce k f . Pro funkce $f : X \rightarrow Y$ a $g : Y \rightarrow Z$ je jejich
složení $f \circ g$ značené též gf definováno jako $(f \circ g)(x) = g(f(x))$.
Obraz množiny A přes funkci f je množina $f[A] = \{b; f(a) = b \text{ pro nějaké } a \in A\}$.

Množinu všech funkcí z X do Y značíme ${}^X Y$.

Někdy pro funkci f s $\text{dom}(f) = I$ píšeme f_i místo $f(i)$ a $\langle f_i \rangle_{i \in I}$
místo f ; říkáme pak, že f_i je i -tý člen souboru $\langle f_i \rangle_{i \in I}$ s indexovou
množinou I . Místo $\bigcup \text{rng}(f)$ pak píšeme $\bigcup_{i \in I} f_i$ či $\bigcup \{f_i; i \in I\}$.

Přirozená čísla jsou definována indukcí vztahem $n = \{0, \dots, n-1\}$,
tedy speciálně $0 = \emptyset$, $1 = \{0\} = \{\emptyset\}$, $2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}$.

Množinu všech přirozených čísel značíme $\mathbb{N}$ či též ω .

Předběžnosti

Konečná posloupnost neboli **sekvence** je každá funkce x s $\text{dom}(x) = n$ pro nějaké $n \in \mathbb{N}$. Sekvenci x zapisujeme nejčastěji jako soubor s indexovou množinou n , tj. $\langle x_i \rangle_{i \in n}$ či ekvivalentně $\langle x_0, \dots, x_{n-1} \rangle$ nebo jen $\bar{x}$. Je-li $\text{dom}(x) = n$, říkáme, že n je **délka** x a značíme ji $l(x)$. Dále **konkatenace** $x \cup y$ sekvencí x, y délek m, n je sekvence $\langle x_0, \dots, x_{m-1}, y_0, \dots, y_{n-1} \rangle$. Je-li z sekvence sekvencí, $l(z) = n$, je konkatenací z sekvence $\sqcup z = z_0 \cup \dots \cup z_{n-1}$.

x je **sekvence v množině** X , je-li $\text{rng}(x) \subseteq X$. **Množinu všech sekvencí v** X definujeme jako $X^* = \bigcup_{n \in \mathbb{N}} {}^n X$.

Sekvenci $\langle x_0, \dots, x_{n-1} \rangle \in {}^n X$ dále ztotožňujeme s ticí $(x_0, \dots, x_{n-1}) \in X^n$ a podobně ${}^n X$ ztotožňujeme s X^n .

Předběžnosti

Říkáme, že množina x má **menší nebo rovnou velikost** než y a značíme to $x \preceq y$, když existuje prostá funkce $f : x \rightarrow y$. Množina x má **stejnou velikost** jako y , značíme $x \approx y$, když existuje bijekce $f : x \rightarrow y$. Množina x má **menší velikost** než y , značíme $x \prec y$, když $x \preceq y$ a není $x \approx y$.

Dle **Cantor-Bernsteinovy věty** $x \preceq y$ a $y \preceq x$ implikuje $x \approx y$.

Ke každé množině x existuje tzv. **kardinální číslo** κ , pro něž $x \approx \kappa$, píšeme pak $|x| = \kappa$ a $|x|$ nazýváme **velikost** či **kardinalita** x . Je-li x konečná, je $|x|$ přirozené číslo.

Dále značíme $|\mathbb{N}| = \omega$ a říkáme, že x je **spočetná**, je-li $|x| = \omega$ (tj. $x \approx \mathbb{N}$). Není-li x spočetná, je **nespočetná**. Množina $\mathbb{R}$ je nespočetná, její velikost značíme $\mathfrak{c}$ a nazýváme ji **velikost kontinua** či jen **kontinuum**.

Předběžnosti

Na třídě $\mathbf{Cn}$ všech kardinálních čísel lze zavést lineární uspořádání $<$, pro $\kappa, \lambda \in \mathbf{Cn}$ pak platí $\kappa < \lambda \Leftrightarrow \kappa \in \lambda \Leftrightarrow \kappa \prec \lambda$ a každá neprázdná podmnožina $\mathbf{Cn}$ má nejmenší prvek. Nejmenší kardinální číslo větší než κ značíme κ^+ , je to **kardinální následník** κ .

Součet, **součin** a **mocnina** kardinálních čísel se definují jako $\kappa + \lambda = |\kappa \uplus \lambda|$, $\kappa \cdot \lambda = |\kappa \times \lambda|$ a $\kappa^\lambda = |\lambda^\kappa|$. Pak platí:

- ❶ $\kappa + \lambda = \kappa \cdot \lambda = \max(\kappa, \lambda)$, pokud (*),
- ❷ $\kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu$, $(\kappa^\lambda)^\mu = \kappa^{\lambda \cdot \mu}$, $|\mathcal{P}(x)| = 2^{|x|} > |x|$
- ❸ $\kappa^n = \kappa$ je-li $\kappa \geq \omega$ a $n > 0$, $|\bigcup_{i \in I} x_i| \leq |I| \cdot \sup\{|x_i|; i \in I\}$,
- ❹ $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = \omega < \mathfrak{c} = 2^\omega = |\mathbb{R}| = |\mathcal{P}(\omega)| = {}^\omega 2$.

(*) výše značí podmínku: jedno z κ, λ je nekonečné a $\kappa, \lambda > 0$.

Předběžnosti

Pro $n \in \mathbb{N}$ je **n -ární relace** neboli relace **arity** (**četnosti**) n na X jakákoli množina $R \subseteq X^n$. Speciálně tedy 1-ární relace na A je podmnožina A a 0-ární relace na A je podmnožina $A^0 = \{\emptyset\}$, tj. $\emptyset = 0$ nebo $\{\emptyset\} = 1$. 0-ární a 1-ární relace není tedy relace v dříve uvedeném smyslu, tj. není to množina uspořádaných dvojic.

Totální funkce arity (**četnosti**) n neboli **totální n -ární funkce** z X do Y je funkce $F : X^n \rightarrow Y$. Je-li v předchozím $X = Y$, nazýváme **F n -ární operace** nad X . Speciálně 0-ární funkce F je tvaru $\{(\emptyset, y)\}$ pro nějaké $y \in Y$, takovou funkci ztotožňujeme s y a říkáme, že F je **konstanta** y v Y .

Aritu relace R resp. funkce F značíme **$\text{ar}(R)$** resp. **$\text{ar}(F)$** . Relaci či funkci četnosti 0 resp. 1 resp. 2 nazýváme též **nulární** resp. **unární** resp. **binární**.

Základy syntaxe

Kapitola 2: Základy syntaxe

Základy syntaxe

Jazyk L predikátové logiky je tvořen logickými a mimologickými symboly, případně ještě symbolem rovnosti $=$.

Logické symboly jsou

- **proměnné** $v_0, v_1, \dots$ tvořící nekonečnou spočetnou množinu **Var** (značíme je často $x, y, z, \dots$)
- logické spojky $\neg$ (**negace**) a $\rightarrow$ (**implikace**)
- **obecné kvantifikace** $\forall_x$ pro všechny proměnné x

Ostatní logické spojky $\vee, \&, \leftrightarrow$ a existenční kvantifikace $\exists_x$ zavádíme jako zkratky.

Základy syntaxe

Mimologické symboly mohou být dvou typů:

- relační, tvořící množinu $\mathcal{R}_L$,
- funkční, tvořící množinu $\mathcal{F}_L$.

Přitom $\mathcal{R}_L$ a $\mathcal{F}_L$ jsou disjunktní (mohou být i prázdné) a neobsahují žádný logický symbol ani symbol $=$. Je-li jazyk L zřejmý z kontextu nebo nepodstatný, vynecháváme index L .

Každému mimologickému symbolu $S \in \mathcal{S}$, kde $\mathcal{S}$ je $\mathcal{R}$ či $\mathcal{F}$ je navíc jednoznačně přiřazena jeho četnost (arita) $\text{ar}_{\mathcal{S}}(S) \in \mathbb{N}$, máme tedy $\text{ar}_{\mathcal{S}} : \mathcal{S} \rightarrow \mathbb{N}$. Funkční symboly arity 0 nazýváme též konstantní symboly.

Základy syntaxe

Symbol = není logický ani mimologický. Pokládáme ho za relační symbol arity 2.

Je-li = symbolem jazyka L , říkáme, že jde o **jazyk s rovností**, jinak je **bez rovnosti**. Není-li dále výslovně uvedeno jinak, je každý jazyk s rovností. Postulujeme dále také, že každý jazyk obsahuje alespoň jeden relační symbol (mimologický nebo $=$).

Základy syntaxe

Signatura jazyka L je dvojice $(\underline{\mathcal{R}}_L, \underline{\mathcal{F}}_L)$, kde $\underline{\mathcal{R}}_L = (\mathcal{R}_L, \text{ar}_{\mathcal{R}_L})$ a $\underline{\mathcal{F}}_L = (\mathcal{F}_L, \text{ar}_{\mathcal{F}_L})$.

Jazyk je určen svojí signaturou a informací, zda je s rovností či bez rovnosti. Proto obvykle ztotožňujeme jazyk s jeho signaturou.

Často používáme volnější zápis signatury jazyka ve formě posloupnosti (v libovolném pořadí) jeho mimologických symbolů, k níž slovně dodáváme typy a arity uvedených symbolů.

Můžeme tak například definovat jazyk L následovně:

Příklad: Nechť $L = \langle 0, 1, +, \cdot, < \rangle$, kde symboly $0, 1$ jsou nulární funkční, $+, \cdot$ binární funkční a $<$ binární relační. Pak $\mathcal{R}_L = \{<\}$, $\mathcal{F}_L = \{0, 1, +, \cdot\}$, $\text{ar}_{\mathcal{R}_L}(<) = 2$, $\text{ar}_{\mathcal{F}_L}(0) = \text{ar}_{\mathcal{F}_L}(1) = 0$, $\text{ar}_{\mathcal{F}_L}(+) = \text{ar}_{\mathcal{F}_L}(\cdot) = 2$.

Základy syntaxe

Pojem jazyka je pojmem **čistě syntaktickým** (patřícím na stranu syntaxe). Významy (realizace) jednotlivých symbolů zde nejsou nijak stanoveny. Např. binární funkční symbol $+$ nemusí mít nutně význam sčítání.

Příklad: Aditivní jazyk teorie grup je definovaný jako $L^{g+} = \langle 0, -, + \rangle$, kde 0 je konstantní symbol, $-$ unární funkční a $+$ binární funkční symbol. Tento jazyk je jazykem grupy $\mathbb{Z}$ celých čísel, kde významy (neboli realizace) symbolů $0, -, +$ jazyka L^{g+} jsou po řadě „nula“, „opačný prvek“, „součet“.

Je však také jazykem multiplikativní grupy $\mathbb{R}^+$ kladných reálných čísel, kde významy symbolů $0, -, +$ jsou postupně 1 , „převrácená hodnota“ (tj. funkce $()^{-1}$), „součin“.

Základy syntaxe

Termy jsou (správně utvořené) funkční výrazy daného jazyka.

Definition: Množinu všech **termů** jazyka $L = (\mathcal{R}, \mathcal{F})$, též **L -termů**, (značíme Term_L) definujeme jako nejmenší množinu splňující:

- i. $\text{Var} \subseteq \text{Term}_L$ (každá proměnná je term)
- ii. $F(t_0, \dots, t_{n-1}) \in \text{Term}_L$ pro $t_i \in \text{Term}_L$ a $F \in \mathcal{F}$, $\text{ar}(F) = n$ (aplikací funkčních symbolů na termy vznikají termy)

Příklad: V jazyce $L = \langle 0, 1, +, \cdot, < \rangle$, kde symboly $0, 1$ jsou nulární funkční, $+, \cdot$ binární funkční a $<$ binární relační, jsou následující výrazy příklady termů: $x, 0, x + 1, (0 + 1) \cdot x + y \cdot z$.

Příklad: Termy $1, 1 + 0, 0 + 1, 1 \cdot 1$ jsou čtyři různé termy, jelikož jsou to různé posloupnosti symbolů.

Základy syntaxe

Poznámky k definici:

- Uvedená definice je příkladem tzv. **induktivní definice** – termy jsou vytvářeny z proměnných aplikací konečně mnoha funkčních symbolů.
- Dle ii. speciálně pro konstantní (tj. funkční arity 0) symbol c jazyka L plyne $c \in \text{Term}_L$.
- Použitý zápis $F(t_0, \dots, t_{n-1})$ je zkratkou za prefixní zápis v polské notaci $\langle F \rangle \cup t_0 \cup \dots \cup t_{n-1}$, který nepoužívá závorky, čárky ani žádné další nepovolené symboly.
- Mnohdy používáme volnější zápisy termů v infixní či jiné notaci (např. $x + y$ místo $+(x, y)$, formálně $\langle +, x, y \rangle$).

Základy syntaxe

Atomické formule jsou nejjednodušší tvrzení daného jazyka.

Definice: Atomická formule jazyka $L = (\mathcal{R}, \mathcal{F})$, také atomická L -formule, je tvaru $R(t_0, \dots, t_{n-1})$, kde $t_i \in \text{Term}_L$ a R je relační (tj. $R \in \mathcal{R}$ či R je $=$), $\text{ar}(R) = n$. Množinu všech atomických formulí jazyka L značíme AFm_L .

Příklad: V jazyce $L = \langle 0, 1, +, \cdot, < \rangle$ (s rovností), kde symboly $0, 1$ jsou nulární funkční, $+, \cdot$ binární funkční a $<$ binární relační, jsou následující výrazy příklady atomických formulí: $x < y$, $x = 0$, $1 < 0$, $x + y < y \cdot 1$, $x + 1 = (0 + 1) \cdot x + y \cdot z$.

Příklad: V jazyce $L = \langle p, U \rangle$ (s rovností), kde p je nulární relační a U unární relační symbol, jsou následující výrazy příklady atomických formulí: $x = y$, p , $U(x)$.

Základy syntaxe

Poznámky k definici:

- Dle definice je v každém jazyce L alespoň jeden relační symbol R . Pak $R(x_0, \dots, x_{\text{ar}(R)-1})$ je atomická formule L , tedy $AFm_L \neq \emptyset$.
- Speciálně pro nulární (tj. arity 0) relační symbol R jazyka L plyne $R \in AFm_L$.
- Použitý zápis $R(t_0, \dots, t_{n-1})$ je zkratkou za prefixní zápis v polské notaci $\langle R \rangle \cup t_0 \cup \dots \cup t_{n-1}$.
- Mnohdy používáme volnější zápisy atomických formulí v infixní či jiné notaci (např. $x + z < y$ místo $< (+ (x, z), y)$), formálně $\langle <, +, x, z, y \rangle$.

Základy syntaxe

Definice: Množinu všech **formulí** jazyka $L = (\underline{\mathcal{R}}, \underline{\mathcal{F}})$, též **L -formulí**, (značíme **Fm_L**) definujeme jako nejmenší množinu splňující

- i. $AFm_L \subseteq Fm_L$ (každá atomická formule je formule)
- ii. $\neg(\varphi), (\varphi) \rightarrow (\psi), \forall_x(\varphi) \in Fm_L$ jakmile $\varphi, \psi \in Fm_L$ a $x \in \text{Var}$ (negace a univerzální kvantifikace formule je formule, implikace dvou formulí je formule)

Příklad: V jazyce $L = \langle 0, 1, +, \cdot, < \rangle$ (s rovností), kde symboly 0, 1 jsou nulární funkční, $+$, $\cdot$ binární funkční a $<$ binární relační, jsou následující výrazy příklady formulí: $x < y$, $\neg(x = 0)$, $(1 < 0) \rightarrow (\forall_y(x + y < y \cdot 1))$.

Základy syntaxe

Poznámky k definici:

- Uvedená definice je opět **induktivní** – formule jsou vytvářeny z atomických aplikací konečně logických spojek a kvantifikátorů.
- Použité zápisy $\neg(\varphi)$, $(\varphi) \rightarrow (\psi)$, $\forall_x(\varphi)$ jsou zkratkou za prefixní zápis v polské notaci $\langle \neg \rangle \cup \varphi$, $\langle \rightarrow \rangle \cup \varphi \cup \psi$, $\langle \forall_x \rangle \cup \varphi$, který nepoužívá závorky, čárky ani žádné další nepovolené symboly. Při této formalizaci ztotožňujeme atomickou formuli φ se sekvencí $\langle \varphi \rangle$.
- Mnohdy vynecháváme některé závorky, symbol $\forall_x$ zapisujeme rovněž jako $(\forall x)$.

Příklad: Píšeme potom například $(\forall x)(\neg R(x) \rightarrow P(y))$ místo $\forall_x((\neg(R(x))) \rightarrow (P(y)))$, formálně $\langle \forall_x, \rightarrow, \neg, \langle R, x \rangle, \langle P, y \rangle \rangle$.

Základy syntaxe

Je-li L jazyk, **kardinalita** (neboli **velikost**) jazyka L je $\|L\| = \max(|\mathcal{R}_L \cup \mathcal{F}_L|, \omega)$. Tedy, má-li L jen konečně mnoho mimologických symbolů, je $\|L\| = \omega$, jinak je $\|L\|$ velikost množiny jeho mimologických symbolů.

Snadno se ukáže, že platí

- $\omega \leq |\text{Term}_L| \leq \|L\|$,
- $|AFm_L| \leq |Fm_L| \leq \|L\|$, přitom platí $=$ namísto $\leq$, je-li v L alespoň jeden relační symbol nenulové arity.

Základy syntaxe

Výskytem sekvence (symbolů) η v sekvenci η' je každá podsekvence η' , která je rovna η . Je-li $\eta = \langle s \rangle$, jde o **výskyt symbolu** s v η' .

Podterm termu t je každá jeho podsekvence, která je termem, **podformulí** formule φ každá její podsekvence, která je formulí.

Výskyt proměnné x ve formuli φ je **vázaný**, je-li výskytem v nějaké podformuli φ tvaru $(\forall x)\psi$. Není-li výskyt vázaný, je **volný**.

Proměnná je **volná** [**vázaná**] ve φ , má-li ve φ volný [**vázaný**] výskyt.

Příklad: Ve formuli $(\forall x)(x = y \rightarrow \neg x = z) \rightarrow (x = y)$ je proměnná x volná i vázaná, výskyty x jsou vázané, výskyt x volný. x není výskytem x , neboť $(\forall x)$ je pouhá zkratka za jediný symbol $\forall_x$.

Základy syntaxe

Formule φ je **otevřená** (bezkvantifikátorová), nemá-li v ní výskyt žádný symbol $\forall x$, je **uzavřená** (**sentence**), je-li v ní každý výskyt proměnné výskytem vázaným.

Příklad: $x < y + z$ je otevřená, není uzavřená

$(\forall x)(\forall y)(\forall z)(x < y + z)$ je uzavřená, není otevřená

$(\forall y)(\forall z)(x < y + z)$ není ani otevřená, ani uzavřená

$0 < 1 + 1$ je uzavřená i otevřená

Term t je **substituovatelný** za proměnnou x do formule φ , pokud x nemá volný výskyt v žádné podformuli φ tvaru $(\forall y)\psi$ takové, že y má výskyt v t (tj. tehdy, když nahrazením všech volných výskytů x ve φ termem t nevznikne nový vázaný výskyt nějaké proměnné).

Příklad: Term $y + z$ není substituovatelný za x do $(\forall y)(x = x)$.

Základy syntaxe

Substitute termu t do formule φ za proměnnou x se provede simultánním nahrazením každého volného výskytu x ve φ termem t , **je-li** term t substituovatelný za x do φ . Výsledná formule se značí $\varphi(x/t)$.

Příklad: Term $y + z$ je substituovatelný za x do formule $x = y \rightarrow (\forall x)(x = x)$. $\varphi(x/y + z)$ je formule $y + z = y \rightarrow (\forall x)(x = x)$.

Teorií pro jazyk L (též **L -teorií**) nazýváme jakoukoli podmnožinu T množiny Fm_L . Prvky T nazýváme (**mimologické**) **axiomy** teorie T .

Příklad: Teorie grup je teorie G v jazyce $L^{g+} = \langle 0, -, + \rangle$ s mimo-logickými axiomy $x + (y + z) = (x + y) + z$, $x + 0 = x$, $0 + x = x$, $x + (-x) = 0$, $(-x) + x = 0$. Je tedy $G = \{x + (y + z) = (x + y) + z, x + 0 = x, 0 + x = x, x + (-x) = 0, (-x) + x = 0\}$.

Základy syntaxe

Hilbertovský kalkulus predikátové logiky je formální systém precizující pojem důkazu. Je dán soustavou logických axiomů — coby základních dokazatelných tvrzení — a odvozovacích pravidel umožňujících odvodit z dříve dokázaných formulí další formule.

Definice: **Odvozovací pravidla** jsou

- (modus ponens) (MP) $Z \varphi$ a $\varphi \rightarrow \psi$ odvod' ψ .
- (generalizace) (gen) $Z \varphi$ odvod' $(\forall x)\varphi$ pro $x \in \text{Var}$.

Pozor: Odvozovací pravidlo má jiný charakter než axiom ve tvaru implikace. Např. $\varphi \rightarrow (\forall x)\varphi$ dokonce obecně **není logicky pravdivá formule**.

Základy syntaxe

Definice: **Logické axiomy** hilbertovského kalkulu predikátové logiky pro jazyk L jsou

Axiomy o logických spojkách

$$(HK1) \quad \varphi \rightarrow (\psi \rightarrow \varphi)$$

$$(HK2) \quad (\varphi \rightarrow (\psi \rightarrow \chi)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \chi))$$

$$(HK3) \quad (\neg\varphi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \varphi)$$

kde $\varphi, \psi, \chi \in Fm_L$.

Axiomy o kvantifikátorech

- (substituce) $(\forall x)\varphi \rightarrow \varphi(x/t)$, je-li term t substituovatelný za x do φ
- ($\forall$ -zavedení) $(\forall x)(\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow (\forall x)\psi)$, pokud x není volná ve φ

kde $\varphi, \psi \in Fm_L$.

Základy syntaxe

Množinu všech **logických axiomů** jazyka L značíme LAx_L . Je-li L s rovností, zahrnujeme mezi logické axiomy též axiomy rovnosti:

Definice: **Axiomy rovnosti** pro jazyk L s rovností jsou

(E1) $x = x$ pro $x \in \text{Var}$

(E2) $x_0 = y_0 \rightarrow \dots \rightarrow x_{n-1} = y_{n-1} \rightarrow (R(x_0, \dots, x_{n-1}) \rightarrow R(y_0, \dots, y_{n-1}))$ pro R relační (tj. $R \in \mathcal{R}$ či $=$), $\text{ar}(R) = n$

(E3) $x_0 = y_0 \rightarrow \dots \rightarrow x_{n-1} = y_{n-1} \rightarrow (F(x_0, \dots, x_{n-1}) = F(y_0, \dots, y_{n-1}))$ pro $F \in \mathcal{F}$, $\text{ar}(F) = n$

Axiomy rovnosti říkají, že (realizace) $=$ má vlastnosti relace ekvivalence, která je kongruencí vůči všem relacím a funkcím R, F .

Základy syntaxe

Definice: **Důkaz** v L -teorii T je každá posloupnost $\langle \varphi_0, \dots, \varphi_{n-1} \rangle$ formulí jazyka L taková, že pro každé φ_i platí jedno z následujících

- $\varphi_i \in T \cup L\mathcal{A}_L$ (φ_i je logickým axiomem nebo vlastním axiomem teorie T) nebo
- φ_i je odvozeno z nějakých φ_j, φ_k s $j, k < i$ pomocí jednoho z odvozovacích pravidel.

Říkáme, že důkaz d je **důkazem formule** φ , je-li φ posledním členem důkazu d .

Má-li formule φ nějaký důkaz v teorii T , říkáme, že je **dokazatelná v T** či, že to je **teorém T** , píšeme pak $T \vdash \varphi$. Je-li $T = \emptyset$, říkáme, že φ je **dokazatelná v logice** a píšeme $\vdash \varphi$.

Základy syntaxe

Příklad: Formule $\varphi \rightarrow \varphi$ je dokazatelná v logice, příslušný důkaz následuje:

1. $\varphi \rightarrow ((\varphi \rightarrow \varphi) \rightarrow \varphi)$ (HK1) pro $\psi \equiv \varphi \rightarrow \varphi$
2. $(\varphi \rightarrow ((\varphi \rightarrow \varphi) \rightarrow \varphi)) \rightarrow$
 $\rightarrow ((\varphi \rightarrow (\varphi \rightarrow \varphi)) \rightarrow (\varphi \rightarrow \varphi))$ (HK2)
3. $(\varphi \rightarrow (\varphi \rightarrow \varphi)) \rightarrow (\varphi \rightarrow \varphi)$ (MP) na 1. a 2.
4. $\varphi \rightarrow (\varphi \rightarrow \varphi)$ (HK1)
5. $\varphi \rightarrow \varphi$ (MP) na 3. a 4.

Tvrzení, ke kterému sestavíme formální důkaz, nazýváme též **syntakticky dokázané**.

Základy syntaxe

Je-li $T \vdash \neg\varphi$, říkáme, že φ je **vyvratitelná** v T . Není-li φ dokazatelná ani vyvratitelná, nazývá se **nezávislá**, není-li vyvratitelná, pak je **konzistentní**.

Množinu všech teorémů teorie T značíme Thm_T . Lze ji definovat též **induktivně**.

Thm_T je nejmenší množina splňující

- i. $T \cup LA_{x_L} \subseteq Thm_T$ (každý axiom je teorémem)
- ii. $(\forall x)\varphi, \psi \in Thm_T$ jakmile $\varphi, \varphi \rightarrow \psi \in Thm_T$ (aplikací odvozovacího pravidla na teorém(y) získáme teorém)

Teorie T se nazývá **sporná**, je-li v ní dokazatelná každá formule, jinak je **bezesporná**. T je **kompletní** (úplná), je-li bezesporná a každá **sentence** je v ní dokazatelná či vyvratitelná.

Základy syntaxe

Další logické spojky $\&$, $\vee$, $\leftrightarrow$, existenční kvantifikaci $\exists_x$ a symboly pro spor/pravdu $\perp$, $\top$ zavádíme jako následující zkratky (tj. symboly $\&$, $\vee$, $\leftrightarrow$, $\exists_x$, $\perp$, $\top$ nepřidáváme do jazyka):

$\psi \vee \chi$	je zkratka za	$\neg\psi \rightarrow \chi$
$\psi \& \chi$	je zkratka za	$\neg(\psi \rightarrow \neg\chi)$
$\psi \leftrightarrow \chi$	je zkratka za	$(\psi \rightarrow \chi) \& (\chi \rightarrow \psi)$
$\exists_x(\psi)$	je zkratka za	$\neg(\forall_x(\neg\psi))$
$\perp$	je zkratka za	$\varphi \& \neg\varphi$ (φ libovolná formule)
$\top$	je zkratka za	$\varphi \vee \neg\varphi$ (φ libovolná formule)

Základy sémantiky

Kapitola 3: Základy sémantiky

Základy sémantiky

Významový obsah (sémantika) může být formálnímu pojmu jazyka přiřazen pomocí konceptu struktury.

Definice: **Struktura** pro signaturu $L = \langle \underline{\mathcal{R}}, \underline{\mathcal{F}} \rangle$, neboli **L -struktura**, je trojice $\mathcal{A} = \langle A, \mathcal{R}^A, \mathcal{F}^A \rangle$, kde

- $A \neq \emptyset$,
- $\mathcal{R}^A = \{R^A; R \in \mathcal{R}\}$, R^A je $\text{ar}(R)$ -ární relace na A ,
- $\mathcal{F}^A = \{F^A; F \in \mathcal{F}\}$, F^A je $\text{ar}(F)$ -ární funkce na A .

Říkáme, že R^A , F^A jsou **realizace** (též **interpretace**) symbolů R , F ve struktuře $\mathcal{A}$. Je-li navíc L s rovností, pak definujeme $=^A$ jako identitu na A .

Příklad: Pro jazyk $L = \langle 0, +, \leq \rangle$ je L -strukturou například struktura $\mathcal{A} = \langle \mathbb{Z}, 0^{\mathbb{Z}}, +^{\mathbb{Z}}, \leq^{\mathbb{Z}} \rangle$, kde $0^{\mathbb{Z}}$ je celé číslo 0, $+^{\mathbb{Z}}$ je funkce běžného sčítání celých čísel a $\leq^{\mathbb{Z}}$ je běžné uspořádání celých čísel.

Základy sémantiky

Příklad: Pro jazyk $L = \langle 0, +, \leq \rangle$ je L -strukturou rovněž struktura $\mathcal{F} = \langle F, \sin, \circ, \leq_{pw} \rangle$, kde F je množina všech spojitých reálných funkcí jedné proměnné, $\sin$ je funkce sinus, $\circ$ je skládání funkcí a $\leq_{pw}$ je relace porovnání dvou funkcí po složkách.

$\mathcal{B} = \langle B, \mathcal{R}^B, \mathcal{F}^B \rangle$ je **podstruktura** $\mathcal{A}$ (značíme $\mathcal{B} \subseteq \mathcal{A}$), je-li $B \subseteq A$ a $S^B = S^A \upharpoonright B$ pro $S \in \mathcal{R} \cup \mathcal{F}$. Nosič B podstruktury $\mathcal{B}$ je uzavřený na všechny funkce z $\mathcal{F}^A$ (speciálně obsahuje všechny konstanty z $\mathcal{F}^A$). $\mathcal{B}$ můžeme zapisovat také jako $\mathcal{A} \upharpoonright B$ a říkáme, že $\mathcal{B}$ je **redukt** struktury $\mathcal{A}$ na univerzum B .

Příklad: Nechť $\mathcal{A} = \langle \mathbb{Z}, 0^{\mathbb{Z}}, +^{\mathbb{Z}}, \leq^{\mathbb{Z}} \rangle$ je struktura pro jazyk $L = \langle 0, +, \leq \rangle$. Množina $\mathbb{N}$ je v $\mathcal{A}$ uzavřená na obě funkce $0^{\mathbb{Z}}$ a $+^{\mathbb{Z}}$ struktury $\mathcal{A}$, tedy je univerzem podstruktury $\mathcal{A} \upharpoonright \mathbb{N} = \langle \mathbb{N}, 0^{\mathbb{N}}, +^{\mathbb{N}}, \leq^{\mathbb{N}} \rangle$. Realizace $0^{\mathbb{N}}, +^{\mathbb{N}}, \leq^{\mathbb{N}}$ jsou restrikcemi odpovídajících funkcí $0^{\mathbb{Z}}, +^{\mathbb{Z}}, \leq^{\mathbb{Z}}$ na $\mathbb{N}$.

Základy sémantiky

Ohodnocení proměnných v množině A je každé $e : \text{Var} \rightarrow A$.

Definice: Hodnotu $t^A[e]$ termu $t \in \text{Term}_L$ v L -struktuře $\mathcal{A} = \langle A, \mathcal{R}^A, \mathcal{F}^A \rangle$ při ohodnocení proměnných e definujeme indukcí podle složitosti t :

- i. $x^A[e] = e(x)$
- ii. $(F(t_0, \dots, t_{n-1}))^A[e] = F^A(t_0^A[e], \dots, t_{n-1}^A[e])$

Speciálně pro konstantní symbol c je dle ii. $c^A[e] = c^A$.

Příklad: Hodnotou termu $(x + x) + 0$ ve struktuře $\mathcal{A} = \langle \mathbb{Z}, 0^{\mathbb{Z}}, +^{\mathbb{Z}}, \leq^{\mathbb{Z}} \rangle$ při ohodnocení e s $e(x) = 3$ je $((x+x)+0)^A[e] = 6$.

Příklad: Hodnotou téhož termu ve struktuře $\mathcal{F} = \langle F, \sin, \circ, \leq_{pw} \rangle$ z jednoho z předcházejících příkladů při ohodnocení e' s $e'(x) = \cos$ je funkce $t \mapsto \sin(\cos(\cos(t)))$.

Základy sémantiky

Definice: Hodnotu $H_{at}^A(\varphi, e)$ atomické formule $\varphi \equiv R(t_0, \dots, t_{n-1})$ ve struktuře $\mathcal{A} = \langle A, \mathcal{R}^A, \mathcal{F}^A \rangle$ při ohodnocení e definujeme následovně:

$$\bullet H_{at}^A(\varphi, e) = \begin{cases} 1 & \text{pro } (t_0^A[e], \dots, t_{n-1}^A[e]) \in R^A \\ 0 & \text{jinak} \end{cases}$$

Speciálně pro R nulární je $H^A(R, e) = 1 \Leftrightarrow \emptyset \in R^A$, tj. právě když $R^A = \{\emptyset\} = 1$.

Příklad: Pro atomickou formuli $\varphi \equiv (x + y) + 0 \leq x$ jazyka $\langle 0, +, \leq \rangle$ a ohodnocení e s $e(x) = 3$, $e(y) = 4$ ve struktuře $\mathcal{A} = \langle \mathbb{Z}, 0^{\mathbb{Z}}, +^{\mathbb{Z}}, \leq^{\mathbb{Z}} \rangle$ je $H_{at}^A(\varphi, e) = 0$, neboť v celých číslech neplatí $7 \leq 3$.

Základy sémantiky

Pro ohodnocení proměnných $e : \text{Var} \rightarrow A$, $x \in \text{Var}$ a $a \in A$ označme $e(x/a)$ ohodnocení proměnných shodující se s e mimo x a v x mající hodnotu a .

Operace $-_1, \rightarrow_1$ na množině $\{0, 1\}$ jsou dány následovně:

- $-_1 x = 1 - x$
- $x \rightarrow_1 y = \begin{cases} 0 & \text{pokud } x = 1 \text{ a } y = 0, \\ 1 & \text{jinak.} \end{cases}$

Definice: Hodnotu $H^A(\varphi, e)$ formule φ ve struktuře $\mathcal{A} = \langle A, \mathcal{R}^A, \mathcal{F}^A \rangle$ při ohodnocení e definujeme indukcí dle složitosti φ :

- $H^A(\varphi, e) = H_{at}^A(\varphi, e)$, je-li φ atomická
- $H^A(\neg\psi, e) = -_1 H^A(\psi, e)$
 - $H^A(\psi \rightarrow \chi, e) = H^A(\psi, e) \rightarrow_1 H^A(\chi, e)$
 - $H^A(\forall_x(\psi), e) = \min_{a \in A} H^A(\psi, e(x/a))$

Základy sémantiky

Platí (*):

$H^A(\neg\psi, e) = 1$	$\Leftrightarrow$	$H^A(\psi, e) = 0$
$H^A(\psi \rightarrow \chi, e) = 1$	$\Leftrightarrow$	$H^A(\psi, e) = 0$ nebo $H^A(\chi, e) = 1$.
$H^A(\psi \& \chi, e) = 1$	$\Leftrightarrow$	$H^A(\psi, e) = 1$ a $H^A(\chi, e) = 1$.
$H^A(\psi \vee \chi, e) = 1$	$\Leftrightarrow$	$H^A(\psi, e) = 1$ nebo $H^A(\chi, e) = 1$.
$H^A(\psi \leftrightarrow \chi, e) = 1$	$\Leftrightarrow$	$H^A(\psi, e) = H^A(\chi, e)$.
$H^A(\forall x(\psi), e) = 1$	$\Leftrightarrow$	pro každé $a \in A$ je $H^A(\psi, e(x/a)) = 1$.
$H^A(\exists x(\psi), e) = 1$	$\Leftrightarrow$	existuje $a \in A$, že $H^A(\psi, e(x/a)) = 1$.
$H^A(\perp, e) = 0$		vždy
$H^A(\top, e) = 1$		vždy
$H^A(x = y, e) = 1$	$\Leftrightarrow$	$e(x) = e(y)$ (je-li L s rovností)

Základy sémantiky

Říkáme, že φ **platí (je pravdivá)** ve struktuře $\mathcal{A}$ při ohodnocení e (píšeme $\mathcal{A} \models \varphi[e]$), pokud $H^A(\varphi, e) = 1$.

Dále φ **platí (je pravdivá)** ve struktuře $\mathcal{A}$ (píšeme $\mathcal{A} \models \varphi$), platí-li v $\mathcal{A}$ při každém ohodnocení e .

Platí-li φ v každé struktuře (pro daný jazyk), nazývá se **tautologie**.

Ne všechny vztahy (*) zůstanou pravdivé, nahradíme-li v nich platnost při ohodnocení platností ve struktuře. V následující tabulce $\nsubseteq, \not\models$ značí, že uvedená implikace obecně neplatí.

$\mathcal{A} \models \neg\psi$	$\nsubseteq, \Rightarrow$	$\mathcal{A} \not\models \psi$
$\mathcal{A} \models \psi \ \& \ \chi$	$\Leftrightarrow$	$\mathcal{A} \models \psi$ a $\mathcal{A} \models \chi$
$\mathcal{A} \models \psi \vee \chi$	$\Leftarrow, \not\models$	$\mathcal{A} \models \psi$ nebo $\mathcal{A} \models \chi$
$\mathcal{A} \models \varphi$	$\Leftrightarrow$	$\mathcal{A} \models (\forall x)\varphi$

Základy sémantiky

Definice: Struktura $\mathcal{A}$ se nazývá **model** teorie T (píšeme $\mathcal{A} \models T$), pokud $\mathcal{A} \models \psi$ pro každý axiom $\psi \in T$.

Říkáme, že formule φ **platí (je pravdivá)** v teorii T (píšeme $T \models \varphi$), pokud $\mathcal{A} \models \varphi$ pro každý model $\mathcal{A}$ teorie T .

Třidu všech modelů teorie T značíme $M(T)$.

Je-li $T = \emptyset$ teorie bez mimologických axiomů, píšeme $\models \varphi$ místo $\emptyset \models \varphi$. Jelikož každá L -struktura je modelem prázdné L -teorie, je $\models \varphi \Leftrightarrow \varphi$ je tautologie.

Struktury $\mathcal{A}, \mathcal{B}$ se nazývají **elementárně ekvivalentní** (značíme $\mathcal{A} \equiv \mathcal{B}$), platí-li v nich tytéž formule.

Základy sémantiky

Příklad: Teorie hustého lineárního uspořádání **DeLO*** je teorie v jazyce $L^O = \langle \leq \rangle$, kde $\leq$ je binární relační symbol, s axiomy:

- | | | |
|------|---|----------------------|
| (O1) | $x \leq x$ | (reflexivita) |
| (O2) | $(x \leq y \ \& \ y \leq x) \rightarrow x = y$ | (slabá antisymetrie) |
| (O3) | $(x \leq y \ \& \ y \leq z) \rightarrow x \leq z$ | (tranzitivita) |
| (LO) | $x \leq y \vee y \leq x$ | (linearita) |
| (De) | $x < y \rightarrow (\exists z)(x < z < y)$ | (hustota) |
| (nT) | $(\exists x, y)(x \neq y)$ | (netrivialita) |

Zde $x < y$ je zkratka za $x \leq y \ \& \ x \neq y$.

Teorie hustého lineárního uspořádání bez konců **DeLO** je L^O -teorie rozšiřující **DeLO*** o axiomy:

- | | | |
|------|---------------------------------|--------------------------------|
| (n+) | $(\forall x)(\exists y)(x < y)$ | (neexistence největšího prvku) |
| (n-) | $(\forall x)(\exists y)(y < x)$ | (neexistence nejmenšího prvku) |

Základy sémantiky

Příklad: Struktura $\underline{\mathbb{Q}} = \langle \mathbb{Q}, \leq \rangle$, kde $\leq$ je běžné uspořádání racionálních čísel, je modelem teorie DeLO. Jiné modely DeLO jsou např. $\underline{\mathbb{R}} = \langle \mathbb{R}, \leq \rangle$ či $\langle (0, 1), \leq \rangle$.

Příklad: Struktura $\mathcal{A} = \langle [0, 1], \leq \rangle$, kde $[0, 1]$ je polouzavřený interval reálných čísel, je modelem DeLO*, není však modelem DeLO, neboť $\mathcal{A} \not\models (n-)$.

Příklad: Struktury $\underline{\mathbb{R}}$ a $\mathcal{A}$ z předchozích příkladů nejsou elementárně ekvivalentní, platí totiž $\mathcal{A} \not\models (n-)$ a $\underline{\mathbb{R}} \models (n-)$.

Základy sémantiky

Zásadní význam pro vztah mezi syntaxí a sémantikou predikátové logiky má následující věta o kompletnosti.

Věta (o kompletnosti predikátové logiky – Gödel, 1929)

Nechť T je L -teorie, $\varphi \in Fm_L$. Pak

$$T \vdash \varphi \Leftrightarrow T \models \varphi$$

Důkaz: Bude později. □

Snadná implikace $\Rightarrow$ se nazývá **věta o korektnosti** predikátové logiky.

Základy sémantiky

Dle věty o kompletnosti formalizmus predikátové logiky vyhovuje Hilbertovu požadavku kompletnosti — tvrzení pravdivé v každém modelu T je dokazatelné v T .

Pokud je speciálně T kompletní teorie, tj. taková, která má jediný model $\mathcal{A}$ až na elementární ekvivalenci, platí $\mathcal{A} \models \varphi \Leftrightarrow T \vdash \varphi$. Pak (je-li navíc T dostatečně „bohatá“) může být model $\mathcal{A}$ považován za kompletní „svět matematiky“.

Výroková logika

Kapitola 4: Výroková logika

Výroková logika

Výroková logika může být chápána jako „redukt“ logiky predikátové, konkrétně pro jazyk $L^{\mathbb{P}} = \langle p \rangle_{p \in \mathbb{P}}$ bez rovnosti obsahující **pouze nulární relační symboly**, které tvoří množinu $\mathbb{P}$.

Prvky $p \in \mathbb{P}$ jsou ve všech strukturách realizovány jako $p^A \subseteq A^0 = \{\emptyset\}$, tj. jako $\emptyset = 0$ či $\{\emptyset\} = 1$; nazýváme je **prvovýroky** (**výrokové proměnné**).

$L^{\mathbb{P}}$ -formule neobsahují žádné termy (ani proměnné) a každá $\varphi \in Fm_L$ je ekvivalentní nějaké ψ otevřené (tj. $\models \varphi \leftrightarrow \psi$). Množinu všech otevřených $L^{\mathbb{P}}$ -formulí značíme $VF^{\mathbb{P}}$ a její prvky nazýváme **výroky** (či **výrokové formule**).

Vzhledem k výše uvedenému následujícím způsobem zužujeme pojem jazyka predikátové logiky. **Výrokový jazyk** nad $\mathbb{P}$ sestává z logických symbolů $\neg, \rightarrow$ a mimologických $p \in \mathbb{P}$.

Výroková logika

V souladu s výše popsaným zúžením pojmu jazyka redukuje pro výrokovou logiku také počet logických axiomů hilbertovského kalkulu. **Logické axiomy** hilbertovského kalkulu výrokové logiky jsou jen axiomy (HK1)–(HK3) o logických spojkách, **odvozovací pravidlo** je jen (MP).

Pro $L^{\mathbb{P}}$ -struktury $\mathcal{A}, \mathcal{B}$ je $\mathcal{A} \equiv \mathcal{B}$ právě když $p^{\mathcal{A}} = p^{\mathcal{B}}$ pro každé $p \in \mathbb{P}$, přičemž (jak řečeno výše) je $p^{\mathcal{A}}, p^{\mathcal{B}} \in \{0, 1\} = 2$.

Tedy modely jazyka $L^{\mathbb{P}}$ jsou (až na elementární ekvivalenci) v jednoznačné korespondenci s funkcemi $v : \mathbb{P} \rightarrow 2$. Taková v proto nazýváme **modely** výrokového jazyka nad $\mathbb{P}$ a jejich množinu značíme $\mathbb{P}^2$.

Výroková logika

Právě definované základní syntaktické a sémantické pojmy výrokové logiky popíšeme nyní pro přehlednost explicitně.

Výrokový jazyk nad množinou **prvovýroků** $\mathbb{P}$ sestává z logických symbolů $\neg, \rightarrow$ a mimologických $p \in \mathbb{P}$.

$\text{VF}^{\mathbb{P}}$ je nejmenší množina splňující:

- i. $\mathbb{P} \subseteq \text{VF}^{\mathbb{P}}$ (každý prvovýrok je výrok)
- ii. $\neg(\varphi), (\varphi) \rightarrow (\psi) \in \text{VF}^{\mathbb{P}}$ jakmile $\varphi, \psi \in \text{VF}^{\mathbb{P}}$ (negace výroku i implikace dvou výroků jsou výroky)

Výroková logika

Logické axiomy hilbertovského kalkulu výrokové logiky jsou

$$(HK1) \quad \varphi \rightarrow (\psi \rightarrow \varphi)$$

$$(HK2) \quad (\varphi \rightarrow (\psi \rightarrow \chi)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \chi))$$

$$(HK3) \quad (\neg\varphi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \varphi)$$

Odvozovací pravidlo je

- (MP) Z φ a $\varphi \rightarrow \psi$ odvod' ψ

Výroková teorie nad $\mathbb{P}$ je každá $T \subseteq VF^{\mathbb{P}}$, prvky T jsou její (mimologické) axiomy.

Pojmy **důkaz**, **dokazatelnost**, **vyvratitelnost**, **nezávislost**, **konzistence**, **spornost**, **bezespornost**, **kompletnost** zůstávají stejné jako v predikátové logice.

Výroková logika

Jako zkratky (stejnými definicemi jako v predikátové logice) zavádíme logické spojky $\vee$, $\&$, $\leftrightarrow$ a symboly sporu/pravdy $\perp$, $\top$.

Definition: **Model** (výrokového jazyka) nad $\mathbb{P}$ (také **ohodnocení výrokových proměnných**) je každá funkce $v : \mathbb{P} \rightarrow 2$. Množinu všech modelů nad $\mathbb{P}$ značíme $\mathbb{P}^2$.

Definition: **Hodnotu** $\bar{v}(\varphi)$ výroku φ v modelu v definujeme indukcí dle složitosti φ :

- i. $\bar{v}(p) = v(p)$, je-li $p \in \mathbb{P}$
- ii. a) $\bar{v}(\neg\psi) = -_1 \bar{v}(\psi)$
b) $\bar{v}(\psi \rightarrow \chi) = \bar{v}(\psi) \rightarrow_1 \bar{v}(\chi)$

Často píšeme $v(\varphi)$ místo $\bar{v}(\varphi)$.

Výroková logika

Výrok φ je **pravdivý (platí)** v modelu v (značíme $v \models \varphi$), je-li $v(\varphi) = 1$. Platí-li φ ve všech modelech, nazýváme jej (výroková) **tautologie**.

Model teorie T je takové $v \in \mathbb{P}^2$, že $v \models \varphi$ pro každé $\varphi \in T$ (značíme $v \models T$).

Výrok φ je **pravdivý (platí)** v teorii T (značíme $T \models \varphi$), jestliže $v \models \varphi$ pro každý model v teorie T . Je-li $T = \emptyset$ píšeme $\models \varphi$.

Jsou-li φ, φ' výroky nad $\mathbb{P}$ a T nějaká $\mathbb{P}$ -teorie, nazýváme φ a φ' (**sémanticky**) **ekvivalentní** v T a píšeme $\varphi \sim_T \varphi'$, platí-li $T \models \varphi \leftrightarrow \varphi'$. Je-li $T = \emptyset$, říkáme, že φ, φ' jsou **ekvivalentní logicky** a píšeme $\varphi \sim \varphi'$.

Výroková logika

Tvrzení: (o sémantické ekvivalenci)

Nechť T je teorie, $\varphi \in VF^{\mathbb{P}}$ a ψ podformule φ . Nechť dále φ' vznikne z φ nahrazením nějakých výskytů ψ výrokem ψ' . Potom $\psi \sim_T \psi' \Rightarrow \varphi \sim_T \varphi'$.

Důkaz: Indukcí dle složitosti φ . □

Zřejmě pro výroky φ, φ' a teorii T platí $\varphi \sim_T \varphi' \Leftrightarrow \Leftrightarrow M(T, \varphi) = M(T, \varphi')$. Zde T, φ je zkratka za teorii $T \cup \{\varphi\}$.

Výrok l se nazývá **literál**, je-li to prvovýrok nebo negace prvovýroku.

Výrok φ je v **konjunktivně/disjunktivně normálním tvaru (CNF/DNF)**, je-li konjunkcí disjunktí literálů/disjunktí konjunktí literálů, tj. je-li tvaru $\bigwedge_i \bigvee_j l_{i,j}$ resp. $\bigvee_i \bigwedge_j l_{i,j}$ s $l_{i,j}$ literály.

Výroková logika

Tvrzení: Každý výrok je logicky ekvivalentní výroku v CNF i výroku v DNF.

Důkaz: Necht' $\varphi \in \mathcal{VF}^{\mathbb{P}}$, označme P (konečnou) množinu všech prvovýroků, které mají výskyt ve φ . Volme $\psi_D = \bigvee_{v \in M^P(\varphi)} \bigwedge_{p \in P} p^{v(p)}$, kde p^0 je zkratka za $\neg p$ a p^1 za p . Evidentně ψ_D je v DNF. Zřejmě $w \models \psi_D \Leftrightarrow w = v$ na P pro nějaké $v \in M^P(\varphi) \Leftrightarrow w \models \varphi$, tedy $\varphi \sim \psi_D$. Podobně $\psi_C = \bigwedge_{v \notin M^P(\varphi)} \bigvee_{p \in P} p^{-1v(p)}$ je v CNF a ekvivalentní φ . $\square$

Příklad: Výrok $p \& (q \rightarrow r)$ má nad množinou svých prvovýroků $P = \{p, q, r\}$ tři modely: $\langle 1, 0, 0 \rangle, \langle 1, 0, 1 \rangle, \langle 1, 1, 1 \rangle$. Dle důkazu předchozího tvrzení je tedy ekvivalentní výroku $(p \& \neg q \& \neg r) \vee (p \& \neg q \& r) \vee (p \& q \& r)$ v DNF.

Výroková logika

Výroky můžeme převádět na DNF/CNF taktéž pomocí tzv. **ekvivalentních úprav**:

Příklad: Nechť φ je výrok $(p \vee q) \rightarrow \neg((p \& r) \rightarrow q)$ (nad nějakou množinou prvovýroků $\mathbb{P}$ obsahující p, q, r).

Pak platí: $\varphi \sim \neg(p \vee q) \vee (p \& r \& \neg q) \sim (\neg p \& \neg q) \vee (p \& r \& \neg q)$, poslední formule je v DNF.

Dále je $\varphi \sim (\neg p \vee p) \& (\neg p \vee r) \& (\neg p \vee \neg q) \& (\neg q \vee p) \& (\neg q \vee r) \& (\neg q \vee \neg q) \sim (\neg p \vee r) \& \neg q$, což je v CNF.

Výroková logika

Následující **věta o dedukci** je jednou ze základních metod syntaktického dokazování.

Tvrzení: (věta o dedukci)

Pro teorii T a výroky φ, ψ platí $T \vdash \psi \rightarrow \varphi \Leftrightarrow T, \psi \vdash \varphi$.

Důkaz: „ $\Rightarrow$ “ plyne z (MP).

„ $\Leftarrow$ “ se dokáže indukcí na teorémech $T \cup \{\psi\}$ (tj. indukcí dle složitosti důkazu φ v $T \cup \{\psi\}$). Je-li φ axiom (logický či mimologický) teorie T , plyne $T \vdash \psi \rightarrow \varphi$ z (HK1) a (MP), je-li φ rovno ψ , je $T \vdash \psi \rightarrow \psi$ dle dříve uvedeného syntaktického důkazu. Nakonec, je-li φ odvozeno v $T \cup \{\psi\}$ pomocí (MP) z tamtéž dokazatelných $\chi, \chi \rightarrow \varphi$, máme z indukčního předpokladu $T \vdash \psi \rightarrow \chi$, $T \vdash \psi \rightarrow (\chi \rightarrow \varphi)$. Dle (HK2) $T \vdash (\psi \rightarrow (\chi \rightarrow \varphi)) \rightarrow ((\psi \rightarrow \chi) \rightarrow (\psi \rightarrow \varphi))$ a tedy $T \vdash \psi \rightarrow \varphi$ dvojím užitím (MP). $\square$

Výroková logika

Dále již směřujeme k důkazu věty o kompletnosti výrokové logiky.

Věta (o kompletnosti výrokové logiky – Post)

Nechť T je výroková teorie nad $\mathbb{P}$, $\varphi \in VF^{\mathbb{P}}$. Pak

$$T \vdash \varphi \Leftrightarrow T \models \varphi$$

Její lehčí implikaci „ $\Rightarrow$ “ formulujeme dále jako samostatné **tvrzení o korektnosti**.

Uvedená věta je důsledkem (zatím nedokázané) věty o kompletnosti predikátové logiky, přesto ji zde z ilustrativních důvodů dokážeme přímo.

Výroková logika

Tvrzení: (o korektnosti výrokové logiky)

Nechť T je výroková teorie nad $\mathbb{P}$, $\varphi \in \text{VF}^{\mathbb{P}}$. Pak $T \vdash \varphi \Rightarrow T \models \varphi$

Důkaz: Indukcí na teoremech T : Je-li $\varphi \in T$, z definice $T \models \varphi$. Je-li φ logický axiom, platí dokonce $\models \varphi$, jak se snadno ověří rozбором případů. Je-li φ odvozena v T z ψ a $\psi \rightarrow \varphi$ pomocí (MP), je z indukčního předpokladu $T \models \psi, \psi \rightarrow \varphi$ a odtud snadno $T \models \varphi$. $\square$

Tvrzení: (o spornosti)

- 1) Teorie T je sporná $\Leftrightarrow T \vdash \perp$.
- 2) (o důkazu sporem) $T, \neg\varphi \vdash \perp \Leftrightarrow T \vdash \varphi$

Důkaz: Je technický avšak snadný. $\square$

Výroková logika

Následující tvrzení je jádrem důkazu věty o kompletnosti.

Tvrzení: (o existenci modelu) Teorie T je bezesporná, právě když má model.

Důkaz: „ $\Leftarrow$ “: Pokud je T sporná, pak $T \vdash \perp$ a tedy $v \models \perp$, kdykoli $v \models T$. Pro případný model $v \models T$ tedy $v(\perp) = 1$, což není možné.

„ $\Rightarrow$ “: Dle Zornova lemmatu (viz teorie množin) lze bezespornou T rozšířit do maximální bezesporné $T' \supseteq T$ (tj. takové, že pro $\varphi \notin T'$ je $T' \cup \{\varphi\}$ sporná).

Pak platí pro každé φ, ψ : ($\varphi \in T' \Leftrightarrow \neg\varphi \notin T'$) a ($\varphi \rightarrow \psi \in T' \Leftrightarrow \psi \in T'$ nebo $\neg\varphi \in T'$). Proto $v : \mathbb{P} \rightarrow 2$ definované jako $v(p) = 1$ pro $p \in T'$ a $v(p) = 0$ pro $p \notin T'$ je model T' a tedy i T , neboť $v \models \varphi \Leftrightarrow \varphi \in T'$, což se dokáže indukcí dle složitosti φ . $\square$

Výroková logika

Nyní již můžeme dokázat větu o kompletnosti.

Věta (o kompletnosti výrokové logiky – Post)

Nechť T je výroková teorie nad $\mathbb{P}$, $\varphi \in \text{VF}^{\mathbb{P}}$. Pak

$$T \vdash \varphi \Leftrightarrow T \models \varphi$$

Důkaz: Zbývá už dokázat jen „ $\Leftarrow$ “. Nechť $T \models \varphi$ a $T \not\vdash \varphi$. Dle tvrzení o spornosti je pak $T \cup \{\neg\varphi\}$ bezesporná. Podle tvrzení o existenci modelu má tedy model $v \models T, \neg\varphi$. Ovšem z $v \models T$ a $T \models \varphi$ zřejmě plyne $v \models \varphi$, což je spor s $v \models \neg\varphi$. $\square$

Výroková logika

Snadným důsledkem věty o kompletnosti (resp. tvrzení o existenci modelu) je věta o kompaktnosti.

Věta (o kompaktnosti výrokové logiky)

*Teorie T má model $\Leftrightarrow$ každá **konečná** $S \subseteq T$ má model.*

Důkaz: „ $\Rightarrow$ “ je zřejmá. „ $\Leftarrow$ “: Nechť T nemá model. Pak je dle tvrzení o existenci modelu sporná, tedy dle tvrzení o spornosti $T \vdash \perp$. Nechť d je nějaký důkaz $\perp$ v T . V d se vyskytuje jen konečně mnoho axiomů T , označme jejich množinu S . Pak d je rovněž důkazem $\perp$ v S , tedy S je sporná a nemá proto model. $\square$

Výroková logika

Věta o kompaktnosti výrokové logiky má řadu aplikací v různých oblastech matematiky — umožňuje totiž přenášet vlastnosti konečných systémů na nekonečné.

Příklad: Slavná věta o čtyřech barvách říká, že každý konečný rovinný graf lze obarvit čtyřmi barvami tak, aby žádné dva sousední (tj. hranou spojené) vrcholy neměly stejnou barvu. Pomocí věty o kompaktnosti dokážeme, že stejné tvrzení platí i pro nekonečné rovinné grafy.

Nechť $G = \langle V, E \rangle$ je (nekonečný) rovinný graf s množinou vrcholů (univerzem) V a binární relací E obsahující právě dvojice vrcholů spojené hranou.

Definujme výrokový jazyk $\mathbb{P} = \{c_{w,i}; w \in V, i < 4\}$; výrok $c_{w,i}$ interpretujeme jako „vrchol w je obarven i -tou barvou“.

Výroková logika

Následující výroková teorie T popisuje, že každý vrchol grafu G je obarven jednou ze čtyř barev $i < 4$ a přitom sousední vrcholy mají různou barvu. Její axiomy jsou:

$$\begin{aligned} \bigvee_{i < 4} c_{w,i} & \quad \text{pro každé } w \in V, \\ \neg(c_{w,i} \ \& \ c_{w,j}) & \quad \text{pro každé } w \in V \text{ a } i \neq j, \\ \neg(c_{w,i} \ \& \ c_{w',i}) & \quad \text{pro vrcholy } w, w' \in V \text{ s } (w, w') \in E \text{ a } i < 4. \end{aligned}$$

Model $v \models T$ pak určuje hledané obarvení grafu G následovně:

$$w \in V \text{ má barvu } i \Leftrightarrow v(c_{w,i}) = 1. \quad (\#)$$

Potřebujeme ukázat, že T má model — užijeme k tomu větu o kompaktnosti.

Výroková logika

Nechť S je nějaká konečná podmnožina T — chceme ukázat, že má model.

Označme V_S množinu vrcholů w , pro něž nějaký axiom S obsahuje výskyt nějakého prvovýroku $c_{w,i}$, a $G_S = G \upharpoonright V_S$ buď podstruktura G vzniklá zúžením G na univerzum V_S .

G_S je konečný graf, dle věty o čtyřech barvách tedy existuje obarvení G_S čtyřmi barvami $i < 4$. Vztah $(\#)$ pak určuje model $v \models S$.

Výroková logika

Kapitola 5: Věta o kompletnosti predikátové logiky

Predikátová logika

V této kapitole dokážeme větu o kompletnosti predikátové logiky.

Věta (o kompletnosti predikátové logiky – Gödel, 1929)

Nechť T je L -teorie, $\varphi \in Fm_L$. Pak

$$T \vdash \varphi \Leftrightarrow T \models \varphi$$

Podobně jako u výrokové logiky, nejprve dokážeme několik pomocných tvrzení:

Tvrzení: (věta o dedukci)

Pro teorii T formulí φ a sentenci ψ platí $T \vdash \psi \rightarrow \varphi \Leftrightarrow T, \psi \vdash \varphi$.

Důkaz: „ $\Rightarrow$ “ plyne z (MP) (dokonce bez předpokladu, že ψ je sentence). □

Predikátová logika

Důkaz: „ $\Leftarrow$ “ se dokáže indukcí na teorémech $T \cup \{\psi\}$.

Je-li φ axiom (logický či mimologický) teorie T , plyne $T \vdash \psi \rightarrow \varphi$ z (HK1) a (MP).

Je-li φ rovno ψ , je $T \vdash \psi \rightarrow \psi$ dle jednoho z předcházejících příkladů.

Je-li φ odvozeno v $T \cup \{\psi\}$ pomocí (MP) z tamtéž dokazatelných $\chi, \chi \rightarrow \varphi$, máme z indukčního předpokladu $T \vdash \psi \rightarrow \chi$, $T \vdash \psi \rightarrow (\chi \rightarrow \varphi)$. Dle (HK2) $T \vdash (\psi \rightarrow (\chi \rightarrow \varphi)) \rightarrow ((\psi \rightarrow \chi) \rightarrow (\psi \rightarrow \varphi))$ a tedy $T \vdash \psi \rightarrow \varphi$ dvojím užitím (MP).

Nakonec, je-li φ odvozeno pravidlem (gen) z χ (tj. $\varphi \equiv (\forall x)\chi$) a pro χ tvrzení platí, pak z předpokladu $T, \psi \vdash \varphi$ máme díky axiomu substituce a (MP) $T, \psi \vdash \chi$, tedy dle indukčního předpokladu $T \vdash \psi \rightarrow \chi$ a dle axiomu $\forall$ -zavedení (ψ je sentence) také $T \vdash \psi \rightarrow \varphi$.

□

Predikátová logika

Příklad: Předpoklad, že ψ je sentence je ve větě o dedukci podstatný. Např. pro $\psi \equiv x = y$ a $\varphi \equiv x = z$ je $\psi \vdash \varphi$ ale $\not\vdash \psi \rightarrow \varphi$.

Tvrzení: (o spornosti)

1) Teorie T je sporná $\Leftrightarrow T \vdash \perp$.

2) (o důkazu sporem) Je-li φ sentence, pak $T, \neg\varphi \vdash \perp \Leftrightarrow T \vdash \varphi$

Důkaz: Je technický avšak snadný. □

Predikátová logika

Podobně jako ve výrokové logice je **věta o kompletnosti** snadným důsledkem **tvrzení o existenci modelu**.

Připomeňme, že kardinalitou $\|L\|$ jazyka L rozumíme počet mimologických symbolů jazyka L , je-li L nekonečný, a ω , je-li konečný.

Tvrzení: (o existenci modelu) Je-li T bezsporná L -teorie, má model. Navíc má model nějaké velikosti $\lambda \leq \|L\|$.

Hlavní kroky důkazu tvrzení můžeme rozdělit do dvou skupin – dokazujeme jednak, že pro T určitých dodatečných vlastností lze model sestavit a dále, že pro každou T existuje její extenze $T' \supseteq T$, která má tyto dodatečné vlastnosti.

Predikátová logika

Dále je T bezesporná teorie v jazyce $L = \langle \mathcal{R}, \mathcal{F} \rangle$. Předpokládáme, že L obsahuje nějaký konstantní symbol.

Konstantní struktura pro T je struktura $\mathcal{A} = \langle A, \mathcal{R}^A, \mathcal{F}^A \rangle$, kde A je množina všech **konstantních termů** (tj. termů neobsahujících proměnné) jazyka L , $F^A(t_0, \dots, t_{n-1}) = \langle F \rangle \cup t_0 \cup \dots \cup t_{n-1}$ a $R^A(t_0, \dots, t_{n-1}) \Leftrightarrow T \vdash R(t_0, \dots, t_{n-1})$.

Tvrzení: Je-li L **bez rovnosti** a $\mathcal{A}$ **konstantní struktura** pro T , pak pro **atomickou** L -sentenci φ je $\mathcal{A} \models \varphi \Leftrightarrow T \vdash \varphi$.

Důkaz: φ je tvaru $R(t_0, \dots, t_{n-1})$, kde $t_i \in A$. Tvrzení proto plyne přímo z definice R^A . □

Predikátová logika

Příklad: Konstantní struktura $\mathcal{A}$ pro Peanovu aritmetiku (P) (ta je v jazyce $L = \langle 0, S, +, \cdot, \leq \rangle$ s rovností) obsahuje například dva různé konstantní termy $S(S(0))$ a $S(0) + S(0)$. Pro formuli $\varphi: S(S(0)) = S(0) + S(0)$ tedy $\mathcal{A} \not\models \varphi$, ovšem jistě $PA \vdash \varphi$.

Chceme-li obdržet analogii předchozího tvrzení i pro jazyk s rovností, musíme místo konstantní struktury použít strukturu kanonickou.

Je-li L bez rovnosti, je **kanonická struktura** pro T definována jako konstantní struktura pro T .

Predikátová logika

Kanonickou strukturu pro teorii T v jazyce L s rovností definujeme následovně:

Nechť $\mathcal{A}$ je konstantní struktura pro T a A její univerzum. Definujeme ekvivalenci $\sim$ na A takto $t \sim s \Leftrightarrow T \vdash t = s$ a označíme $[t]_\sim = [t] = \{s; t \sim s\}$.

Dále definujeme $K = A / \sim = \{[t]_\sim; t \in A\}$ a

$$R^K([t_0]_\sim, \dots, [t_{n-1}]_\sim) \Leftrightarrow R^A(t_0, \dots, t_{n-1}),$$

$$F^K([t_0]_\sim, \dots, [t_{n-1}]_\sim) = [F^A(t_0, \dots, t_{n-1})]_\sim \text{ pro } R \in \mathcal{R}, F \in \mathcal{F}.$$

Definice je zřejmě korektní.

Kanonická struktura pro T je struktura $\mathcal{K} = \langle K, \mathcal{R}^K, \mathcal{F}^K \rangle$.

Tvrzení: Je-li $\mathcal{K}$ **kanonická struktura** pro T , pak pro **atomickou** L -sentenci φ je $\mathcal{K} \models \varphi \Leftrightarrow T \vdash \varphi$.

Predikátová logika

Indukcí dle složitosti φ plyne, že je-li $\mathcal{K}$ kanonická struktura pro T , platí $\mathcal{K} \models \varphi \Leftrightarrow T \vdash \varphi$ pro každou otevřenou sentenci φ .

Chceme totéž tvrzení pro libovolnou sentenci φ . Ukazuje se, že v tom případě musí být T navíc maximální bezesporná a henkinovská.

Definice: Teorie T je **henkinovská**, jestliže pro každou formuli φ teorie T s nejvýše jednou volnou proměnnou x existuje konstantní symbol $h = h_\varphi$ jazyka T tak, že $T \vdash (\exists x)\varphi(x) \rightarrow \varphi(x/h_\varphi)$. Konstantní symbol h_φ se pak nazývá **henkinovská konstanta** pro φ v T .

Tvrzení: Je-li T maximální bezesporná henkinovská teorie a $\mathcal{K}$ kanonická struktura pro T , pak pro libovolnou L -sentenci φ je $\mathcal{K} \models \varphi \Leftrightarrow T \vdash \varphi$. Tedy speciálně $\mathcal{K} \models T$.

Důkaz: Nevádíme. □

Predikátová logika

Tvrzení: Každou L -teorii T lze rozšířit do **maximální bezesporné henkinovské** teorie T' v jazyce $\|L'\|$ kardinality $\|L\|$.

Důkaz: Indukcí sestojíme L_i -teorie T_i pro $i \in \omega$ tak, že $T_0 = T$ a pro každou $\varphi \in Fm_{L_i}$ existuje $h_\varphi \in L_{i+1}$ splňující $T_{i+1} \vdash (\exists x)\varphi(x) \rightarrow \varphi(x/h_\varphi)$.

V indukčním kroku z i na $i+1$ přidáme nejprve k jazyku L_i pro každou $\varphi \in Fm_{L_i}$ jeden konstantní symbol h_φ a výsledný jazyk označíme L_{i+1} . Nakonec položíme $T_{i+1} = T_i \cup \{(\exists x)\varphi(x) \rightarrow \varphi(x/h_\varphi); \varphi \in Fm_{L_i}\}$.

Pak zřejmě $T'' = \bigcup_{i \in \mathbb{N}} T_i$ je henkinovská a je-li bezesporná, libovolné její maximální bezesporné rozšíření T' (to existuje dle Zornova lemmatu) má požadované vlastnosti.

Klíčový krok důkazu: bezespornost T'' , je technický, proto ho neuvádíme. □

Predikátová logika

Tvrzení: (o existenci modelu) Je-li T bezesporná L -teorie, má model. Navíc má model nějaké velikosti $\lambda \leq \|L\|$.

Důkaz: Nechť T je dána, L její jazyk. Volme $T' \supseteq T$ nějakou její maximální bezespornou henkinovskou extenzi.

Pak kanonická struktura $\mathcal{K}'$ pro T' splňuje $\mathcal{K}' \models \varphi \Leftrightarrow T' \vdash \varphi$ pro každou $L_{T'}$ -formuli φ . Proto speciálně $\mathcal{K}' \models \varphi$, kdykoli $T \vdash \varphi$, a tedy reduct $\mathcal{K}$ struktury $\mathcal{K}'$ do jazyka L je model T . Navíc $|\mathcal{K}'| \leq \|L_{T'}\| = \|L\|$. $\square$

Predikátová logika

Věta (o kompletnosti predikátové logiky – Gödel, 1929)

Nechť T je L -teorie, $\varphi \in Fm_L$. Pak $T \vdash \varphi \Leftrightarrow T \models \varphi$.

Důkaz: Je snadným důsledkem tvrzení o existenci modelu - důkaz je totožný s případem výrokové logiky. $\square$

Věta (Věta o kompaktnosti)

Teorie T má model, právě když má každá konečná $S \subseteq T$ model. Navíc zmíněný model T lze volit velikosti $\leq \|L_T\|$.

Důkaz: Plyne z věty o kompletnosti zcela stejně jako ve výrokové logice. $\square$

Predikátová logika

Příklad: Má-li teorie T libovolně velký konečný model, má i model nekonečný. Speciálně neexistuje teorie, jejímiž modely by byly právě všechny konečné struktury daného jazyka, tj. teorie vyjadřující vlastnost „být konečnou strukturou“.

Uvedené tvrzení je důsledkem věty o kompaktnosti. Má-li totiž T libovolně velký konečný model, ukážeme, že také teorie $T \cup \{ \text{„existuje alespoň } n \text{ prvků“} ; n \in \mathbb{N} \}$ má model $\mathcal{A}$. Pak zřejmě $\mathcal{A}$ je nekonečný a $\mathcal{A} \models T$.

Předpokládejme bez újmy na obecnosti, že T je v jazyce s rovností a označme α_n formulí vyjadřující „existuje alespoň n prvků“. Nechť $S \subseteq T \cup \{ \alpha_n ; n \in \mathbb{N} \}$ je konečná, chceme ukázat, že má model. S obsahuje jen konečně mnoho axiomů α_n ; nechť n_0 je takové, že $\alpha_n \in S \Rightarrow n \leq n_0$. Dle předpokladu existuje libovolně velký a tedy i alespoň n_0 prvkový model $\mathcal{B} \models T$, zřejmě pak $\mathcal{B} \models S$.

Predikátová logika

Příklad: **Peanova aritmetika (P)** je teorie v aritmetickém jazyce $L^a = \langle 0, S, +, \cdot, \leq \rangle$, kde 0 je konstantní symbol, S unární funkční a $+, \cdot$ binární funkční symboly, $\leq$ je binární relační symbol. Symbol S se nazývá následník a jeho zamýšlená interpretace je „přičítání jedničky“. Axiomy PA jsou:

$$\begin{array}{ll}
 (Q1) & S(x) \neq 0 \\
 (Q2) & S(x) = S(y) \rightarrow x = y \\
 (Q3) & x + 0 = x \\
 (Q4) & x + S(y) = S(x + y) \\
 (Q5) & y \neq 0 \rightarrow (\exists x)S(x) = y \\
 (Q6) & x \leq y \leftrightarrow (\exists z)z + x = y \\
 (Q7) & x \cdot 0 = 0 \\
 (Q8) & x \cdot S(y) = x \cdot y + x
 \end{array}$$

$(ind_\varphi) (\varphi(0) \& (\forall x)(\varphi(x) \rightarrow \varphi(S(x)))) \rightarrow (\forall x)\varphi(x)$ pro $\varphi \in Fm_L$

Teorie v jazyce L^a s axiomy (Q1)–(Q8) se nazývá **Robinsonova aritmetika (Q)**, teorie v jazyce $L^{a+} = \langle 0, S, +, \leq \rangle$ s axiomy (Q1)–(Q6) a schématem indukce (ind_φ) pro $\varphi \in Fm_{L^{a+}}$ je **Presburgerova aritmetika (Pr)**.

Predikátová logika

Příklad: Struktura přirozených čísel $\underline{\mathbb{N}} = \langle \mathbb{N}, 0^{\mathbb{N}}, S^{\mathbb{N}}, +^{\mathbb{N}}, \cdot^{\mathbb{N}}, \leq^{\mathbb{N}} \rangle$ je modelem P i Q , nazývá se **standardní model**. Každé $n \in \mathbb{N}$ je v $\underline{\mathbb{N}}$ realizací termu tvaru $S(S(\dots S(0)\dots))$ s n výskyty S ; takový term značíme $\underline{n}$ a nazýváme ho **n -tý numerál**.

Z věty o kompaktnosti predikátové logiky plyne existence i jiných modelů P , tzv. nestandardních modelů. Rozšířme aritmetický jazyk L^a o nový konstantní symbol c a přidejme k P nové axiomy $\underline{n} \neq c$ pro $n \in \mathbb{N}$. Výslednou teorii označme T .

Každá konečná podteorie $S \subseteq T$ obsahuje jen konečně mnoho nových axiomů, a tedy má model vzniklý realizací c v $\underline{\mathbb{N}}$ různě od všech n vyskytujících se v nových axiomech S . Dle věty o kompaktnosti má tedy T nějaký model $\mathcal{M}_c$. V $\mathcal{M}_c$ je c realizováno jako prvek různý od všech $n \in \mathbb{N}$. Redukt $\mathcal{M}_c$ na jazyk L^a je model P neizomorfní s modelem $\underline{\mathbb{N}}$, nazýváme ho **nestandardní model** P .

Predikátová logika

Dalším důsledkem věty o kompaktnosti je následující tvrzení:

Tvrzení: Necht' T je bezesporná L -teorie, která má nějaký nekonečný model. Pak T má model každé velikosti $\kappa \geq \|L\|$.

Důkaz: Necht' $\kappa \geq \|L\|$ je dáno. Buď T' teorie T rozšířená o axiomy $c_i \neq c_j$ pro $i < j < \kappa$, v jazyce L' rozšiřujícím L o κ nových konstantních symbolů c_i , $i \in \kappa$. T' je bezesporná dle věty o kompaktnosti.

Dle tvrzení o existenci modelu má T' model velikosti $\leq \|L'\| = \kappa$. Zřejmě však každý model T' má velikost alespoň κ . $\square$

Výroková logika

Kapitola 6: Základy teorie modelů

Predikátová logika

Připomeňme, že $\bar{a}$ značí n -sekvenci $\langle a_0, \dots, a_{n-1} \rangle$ s nějakým n .
Dále $f(\bar{a})$ značí $\langle f(a_0), \dots, f(a_{n-1}) \rangle$ pro $a_i \in \text{dom}(f)$.

Definice: Necht' $\mathcal{A}, \mathcal{B}$ jsou dvě struktury pro jazyk $L = \langle \mathcal{R}, \mathcal{F} \rangle$.
Zobrazení $f : A \rightarrow B$ se nazývá **homomorfismus**, jestliže „zachovává všechny relace i funkce“, tj.

- a) $R^{\mathcal{A}}(\bar{a}) \Rightarrow R^{\mathcal{B}}(f(\bar{a}))$ pro každé $R \in \mathcal{R}$
- b) $f(F^{\mathcal{A}}(\bar{a})) = F^{\mathcal{B}}(f(\bar{a}))$ pro každé $F \in \mathcal{F}$

Je-li f prostý homomorfismus takový, že navíc v a) platí $\Leftrightarrow$ místo $\Rightarrow$, je to **izomorfní vnoření**, je-li navíc surjektivní (tj. bijekce), pak je to **izomorfismus**.

Existuje-li mezi $\mathcal{A}$ a $\mathcal{B}$ nějaký izomorfismus, nazýváme $\mathcal{A}$ a $\mathcal{B}$ **izomorfní**, píšeme $\mathcal{A} \cong \mathcal{B}$.

Predikátová logika

Příklad: Bud' $L^O = \langle \leq \rangle$ jazyk teorie uspořádání a $\mathcal{A}, \mathcal{B}, \mathcal{C}$ následující L^O -struktury: $\mathcal{A} = \langle \mathbb{Q}, \leq \rangle$, $\mathcal{B} = \langle \mathbb{R}, \leq \rangle$ a $\mathcal{C} = \langle (-1, 1), \leq \rangle$, kde $(-1, 1)$ je otevřený interval reálných čísel a $\leq$ značí vždy obvyklé uspořádání.

Je $\mathcal{B} \cong \mathcal{C}$, izomorfismem je například funkce $x \mapsto (2/\pi) \cdot \arctg(x)$.

Dále $\mathcal{B} \not\cong \mathcal{A} \not\cong \mathcal{C}$, neboť univerzum $\mathcal{A}$ je spočetné, narozdíl od univerz struktur $\mathcal{B}, \mathcal{C}$. Mezi spočetnou a nespočetnou množinou neexistuje bijekce, tedy ani izomorfismus.

Identita $\text{id}_{\mathbb{Q}} : \mathbb{Q} \rightarrow \mathbb{R}$ (tj. zobrazení $q \mapsto q$ pro $q \in \mathbb{Q}$) je izomorfní vnoření $\mathcal{A}$ do $\mathcal{B}$, které však není surjektivní. Složením $\text{id}_{\mathbb{Q}}$ s nějakým izomorfismem $\mathcal{B}$ a $\mathcal{C}$ získáme izomorfní vnoření $\mathcal{A}$ do $\mathcal{C}$.

Predikátová logika

Příklad: Teorie vektorových prostorů nad tělesem $F = \langle F, 0^F, 1^F, +^F, -^F, \cdot^F \rangle$ je teorie $VS(F)$ v jazyce $L^{m,F} = \langle 0, +, -, \underline{r} \rangle_{r \in F}$, kde 0 je konstantní symbol, $-$ unární funkční a $+$ binární funkční symbol, $\underline{r}$ je unární funkční symbol pro každé $r \in F$. Axiomy $VS(F)$ jsou:

$$\begin{array}{ll}
 (G1) & x + (y + z) = (x + y) + z & (Mo1) & \underline{r}(x + y) = \underline{r}(x) + \underline{r}(y) \\
 (G2) & x + 0 = x = 0 + x & (Mo2) & (\underline{r} +^F \underline{s})(x) = \underline{r}(x) + \underline{s}(x) \\
 (G3) & x + (-x) = 0 = (-x) + x & (Mo3) & (\underline{r} \cdot^F \underline{s})(x) = \underline{r}(\underline{s}(x)) \\
 (AG) & x + y = y + x & (Mo4) & \underline{1^F}(x) = x
 \end{array}$$

kde $r, s \in F$.

Predikátová logika

Příklad: Buďte $\mathbb{R}$ a $\mathbb{R}^2$ euklidovské vektorové prostory nad tělesem $\mathbb{R}$ dimenzí 1 resp. 2. Pak zobrazení $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ definované jako $f : (x, y) \mapsto x$ je (surjektivní) homomorfismus mezi $\mathbb{R}^2$ a $\mathbb{R}$.

Naopak každé zobrazení $f_v : \mathbb{R} \rightarrow \mathbb{R}^2$, kde v je nenulový vektor z $\mathbb{R}^2$, dané jako $f_v(r) = r(v)$, je izomorfní vnoření $\mathbb{R}$ do $\mathbb{R}^2$.

Příklad: Nechtě $\mathcal{A}, \mathcal{B} \models \text{VS}(F)$ jsou vektorové prostory nad F téže dimenze κ a $\langle a_\alpha; \alpha \in \kappa \rangle$ resp. $\langle b_\alpha; \alpha \in \kappa \rangle$ jsou báze $\mathcal{A}$ resp. $\mathcal{B}$.

Každý vektor $v \in \mathcal{A}$ lze jednoznačně zapsat ve tvaru $v = \sum_{i \in I} \underline{r}_i(a_i)$, kde I je konečná podmnožina κ a $r_i \in F$ pro každé $i \in I$. Zobrazení $f: \sum_{i \in I} \underline{r}_i(a_i) \mapsto \sum_{i \in I} \underline{r}_i(b_i)$ je pak izomorfismus $\mathcal{A}$ a $\mathcal{B}$.

Naopak, je-li f izomorfismus nějakých vektorových prostorů $\mathcal{C}, \mathcal{D}$, je f -obraz báze prostoru $\mathcal{C}$ bází $\mathcal{D}$. Tedy dva vektorové prostory jsou izomorfní, právě když mají stejnou dimenzi.

Predikátová logika

Příklad: Budte $\mathcal{A}, \mathcal{B}$ spočetné modely teorie DeLO. Ukážeme, že $\mathcal{A} \cong \mathcal{B}$.

Nechť $\langle a_i; 0 < i \in \omega \rangle$ resp. $\langle b_i; 0 < i \in \omega \rangle$ je prostá posloupnost všech prvků A resp. B . Taková „očíslování“ A, B lze najít díky předpokladu spočetnosti.

Sestrojíme izomorfismus $f : A \rightarrow B$ takzvanou metodou „cik-cak“, tj. indukci tak, že v n -tém kroku definujeme hodnoty $f(a_n)$ a $f^{-1}(b_n)$ takovým způsobem, aby f bylo izomorfismem $\mathcal{A} \upharpoonright \text{dom}(f)$ a $\mathcal{B} \upharpoonright \text{rng}(f)$.

Predikátová logika

V kroku 0 buď f prázdné zobrazení.

Krok $n > 0$: Předpokládejme, že $f(a_n)$, $f^{-1}(b_n)$ ještě nejsou definována (v opačném případě neprovádíme nic). Nechť a_- resp. a_+ je největší prvek $\text{dom}(f)$ pod a_n resp. nejmenší prvek $\text{dom}(f)$ nad a_n ; a_- resp. a_+ je $-\infty$ resp. ∞ , pokud takový prvek neexistuje. Protože $\mathcal{B}$ je husté a bez konců, leží v intervalu $(f(a_-), f(a_+))$ nějaký prvek $b \in \mathcal{B}$. Definujme $f(a_n) = b$. Hodnotu $f^{-1}(b_n)$ definujeme analogicky. Pak f je zřejmě izomorfismus $\mathcal{A} \upharpoonright \text{dom}(f)$ a $\mathcal{B} \upharpoonright \text{rng}(f)$.

Z konstrukce f zřejmě plyne, že f je izomorfismus $\mathcal{A}$ a $\mathcal{B}$.

Tedy každé dva spočetné modely teorie DeLO jsou izomorfní a speciálně izomorfní modelu $\langle \mathbb{Q}, \leq \rangle$.

Predikátová logika

Z věty o kompletnosti zřejmě plyne, že bezesporná teorie T je kompletní, právě když každé dva její modely jsou elementárně ekvivalentní.

Říkáme, že teorie T je κ -kategorická, pokud T má model velikosti κ a každé dva její modely velikosti κ jsou izomorfní.

Tvrzení: (kategorické kritérium kompletnosti) Nechť L -teorie T nemá konečné modely a je κ -kategorická pro nějaké $\kappa \geq \|L\|$. Pak T je kompletní.

Důkaz: Nechť φ je nezávislá sentence v T . Pak teorie T, φ a $T, \neg\varphi$ jsou bezesporné a mají tedy po řadě nějaké modely $\mathcal{A}, \mathcal{B}$ velikosti κ . Z předpokladu κ -kategoričnosti je $\mathcal{A} \cong \mathcal{B}$, tedy speciálně $\mathcal{A} \equiv \mathcal{B}$ — spor. $\square$

Predikátová logika

Příklad: Teorie $VS(F, \infty)$ nekonečných vektorových prostorů nad tělesem F je extenze teorie $VS(F)$ o axiomy ε_n : $(\exists x_0, \dots, x_{n-1}) \bigwedge_{i \neq j} (x_i \neq x_j)$ s $n \in \omega$ vyjadřující „existuje nekonečně mnoho prvků“.

$VS(F, \infty)$ nemá konečné modely a kdykoli jsou $\mathcal{A}, \mathcal{B}$ dva její modely velikosti $\kappa > |F| = \|L^{m,F}\|$, je $\dim(\mathcal{A}) = \kappa = \dim(\mathcal{B})$, tedy $\mathcal{A} \cong \mathcal{B}$. Teorie $VS(F, \infty)$ je tedy kompletní.

Příklad: Teorie DeLO nemá konečné modely a každé dva její spočetné modely jsou izomorfní. Je tedy DeLO kompletní.

Predikátová logika

Definice: L -struktura $\mathcal{A}$ je **elementární podstruktura** L -struktury $\mathcal{B}$ resp. $\mathcal{B}$ je **elementární extenze** $\mathcal{A}$ (značíme $\mathcal{A} \prec \mathcal{B}$.), je-li $\mathcal{A} \subseteq \mathcal{B}$ a $\mathcal{A} \models \varphi(\bar{a}) \Leftrightarrow \mathcal{B} \models \varphi(\bar{a})$ platí pro každá $\bar{a} \in A$ a každou L -formuli $\varphi(\bar{x})$.

Je-li $\mathcal{A} \prec \mathcal{B}$, je speciálně $\mathcal{A} \equiv \mathcal{B}$.

Tvrzení: (Tarski-Vaughtův test) $\mathcal{A} \prec \mathcal{B}$ platí, právě když pro každou formuli $\varphi(y, \bar{x})$ a $\bar{a} \in A$ je: $\mathcal{B} \models (\exists y)\varphi(y, \bar{a}) \Rightarrow$ existuje $a \in A$ takové, že $\mathcal{B} \models \varphi(a, \bar{a})$.

Důkaz: Indukcí dle složitosti φ . □

Predikátová logika

Věta (Löwenheim-Skolemovy věty)

Nechť $\mathcal{A}$ je nekonečná L -struktura. Pak

- ① *(nahoru) je-li $\kappa \geq \max(|A|, \|L\|)$, existuje $\mathcal{B}$ mohutnosti κ tak, že $\mathcal{A} \prec \mathcal{B}$,*
- ② *(dolů) je-li $\|L\| \leq \kappa \leq |A|$, existuje $\mathcal{C}$ mohutnosti κ tak, že $\mathcal{C} \prec \mathcal{A}$.*

Důkaz: „Dolů“: Dokáže se užitím Tarski-Vaughtova testu. Volme $\mathcal{C} = \mathcal{A} \upharpoonright C$, kde $C = \bigcup_{i \in \omega} C_i$ pro $C_i \subseteq A$ sestrojená rekurzí:

Nechť $C_0 \subseteq A$ je libovolná velikosti κ . Je-li C_i sestrojeno, definujeme C_{i+1} jako $C_i \cup \{a_{\varphi, \bar{c}}; \varphi(y, \bar{x}) \text{ je } L\text{-formule}, \bar{c} \in C_i\}$, kde $a_{\varphi, \bar{c}} \in A$ je takové, že platí $\mathcal{A} \models (\exists y)\varphi(y, \bar{c}) \Rightarrow \mathcal{A} \models \varphi(a_{\varphi, \bar{c}}, \bar{c})$.

Pak zřejmě $\mathcal{C} \prec \mathcal{A}$ dle Tarski-Vaughtova testu a $|C| = \kappa$. □

Predikátová logika

Důkaz: „Nahoru“: Přidejme do jazyka konstantní symboly c_a pro $a \in A$ a položme jejich realizace v A takto: $c_a^A = a$. Vzniklou $L \cup \langle c_a; a \in A \rangle$ -strukturu označme $\mathcal{A}_A$. Volme $T = Th(\mathcal{A}_A)$; pak kdykoli $\mathcal{B} \models T$, je (až na izomorfismus) $\mathcal{A} \prec \mathcal{B}$.

Označme L' jazyk $L \cup \langle c_a; a \in A \rangle \cup \langle d_\alpha; \alpha < \kappa \rangle$ s κ novými konstantními symboly d_α a položme $T' = T \cup \{d_\alpha \neq d_\beta; \alpha < \beta < \kappa\}$. Dle věty o kompaktnosti má T' model $\mathcal{B}$ velikosti $\leq \|L'\| = \max(\|L\|, |A|, \kappa) = \kappa$ avšak zřejmě není $|B| < \kappa$ (d_α^B , $\alpha < \kappa$ je κ různých prvků B). $\square$

Predikátová logika

Příklad: Bud' $\underline{\mathbb{C}} = \langle \mathbb{C}, 0, 1, -, +, \cdot \rangle$ těleso komplexních čísel. Je $|\mathbb{C}| = 2^\omega$.

Podle Löwenheim-Skolemovy věty směrem dolů existuje spočetné těleso $\mathcal{C}$ takové, že $\mathcal{C} \prec \underline{\mathbb{C}}$.

Tedy například každá soustava polynomiálních rovnic s koeficienty z $\mathcal{C}$ má řešení v $\mathcal{C}$ právě když ho má v $\mathbb{C}$. Speciálně má každý polynom jedné proměnné nenulového stupně s koeficienty z $\mathcal{C}$ kořen v $\mathcal{C}$, tj. $\mathcal{C}$ je algebraicky uzavřené.

Výroková logika

Kapitola 7: Gödelovy věty o neúplnosti

Neúplnost

Formulujeme zde bez důkazu dvě zásadní Gödelovy věty o neúplnosti a některá jejich zobecnění.

L -teorie T je **rekurzivně axiomatizovaná**, existuje-li „algorithmus“, který o každé L -formuli rozhodne, zda je či není mimologickým axiomem T . Pojem algoritmu je možné definovat precizně, zde to z časových důvodů neděláme.

Věta (1. Gödelova věta o neúplnosti)

Je-li T bezesporná rekurzivně axiomatizovaná teorie rozšiřující Robinsonovu aritmetiku Q , pak existuje sentence ν pravdivá v $\mathbb{N}$ ale nedokazatelná v T .

Je-li navíc T tzv. **korektní**, tj. platí-li $\mathbb{N} \models T$, je ν nezávislá sentence v T , tedy T není kompletní.

Neúplnost

První Gödelovu větu lze zesílit následovně:

Věta (Rosserova věta o neúplnosti)

Je-li T bezsporná rekurzivně axiomatizovaná teorie rozšiřující Robinsonovu aritmetiku Q , pak existuje sentence ρ nezávislá v T . Tedy speciálně není T kompletní.

Lze ukázat, že pro rekurzivně axiomatizovanou T existuje sentence Con_T jazyka L^a aritmetiky taková, že $\mathbb{N} \models Con_T \Leftrightarrow T$ je bezsporná teorie. Con_T tedy čteme jako „ T je bezsporná“.

Věta (2. Gödelova věta o neúplnosti)

Je-li T bezsporná rekurzivně axiomatizovaná teorie rozšiřující Peanovu aritmetiku P , pak $T \not\models Con_T$.

Taková T tedy „neumí dokázat vlastní bezspornost“.

Neúplnost

Z druhé Gödelovy věty plyne důležitý důsledek, totiž že axiomatická teorie množin není schopna dokázat vlastní bezespornost. Tím spíše pak není možné dokázat bezespornost teorie množin finitárními metodami, jak požadoval Hilbertův program.

Speciálně je axiomatická teorie množin nekompletní teorie.

Podle Rosserovy věty jsou Robinsonova i Peanova aritmetika nekompletní teorie. Navíc je nelze zkompletizovat přidáním žádné „algoritmicky“ popsatelné množiny axiomů. Speciálně teorie $Th(\mathbb{N})$, jejímiž axiomy jsou všechny sentence pravdivé ve struktuře $\mathbb{N}$, není ekvivalentní rekurzivně axiomatizované teorii.

Neúplnost

Důkazy vět o neúplnosti využívají existenci tzv. aritmetického kódingu logické syntaxe. Každému syntaktickému pojmu σ , který je konečnou sekvencí symbolů (symbol jazyka, term, formule, důkaz) lze přiřadit přirozené číslo $\overline{\sigma}$ — jeho **kód**. Říkáme dále, že formule φ jazyka aritmetiky **popisuje** množinu syntaktických pojmů S , je-li $\mathbb{N} \models \varphi(n) \Leftrightarrow n = \overline{\sigma}$ pro nějaké $\sigma \in S$. Tedy $\varphi(x)$ vyjadřuje „ x je v množině S “.

Popisuje-li L^a -formule $\lambda(x)$ množinu mimologických symbolů nějakého jazyka L , existují L^a -formule $Term_L(x)$, $Fm_L(x)$ popisující po řadě množiny $Term_L$, Fm_L (tj. vyjadřující „ x je L -term“ resp. „ x je L -formule“). Popisuje-li navíc $\tau(x)$ množinu mimologických axiomů L -teorie T , existují formule $Prf_T(x, y)$, $Pr_T(x)$, Con_T vyjadřující po řadě „ y je důkaz x v T “, „ x je dokazatelná v T “, „ T je bezesporná“.

Neúplnost

Pro L -formuli φ značí $\underline{\varphi}$ „ φ -tý numerál“ (přesněji numerál $\underline{\varphi} = SSS \dots S(0)$, kde S je $\underline{\varphi}$ -krát). Podobně definujeme $\underline{\sigma}$ pro σ symbol jazyka, term, důkaz.

Kromě kódingu je klíčovým prvkem důkazu první Gödelovy věty tzv. **Gödelovo autoreferenční (též diagonální) lemma**:

Tvrzení: (Gödelovo autoreferenční lemma) Nechť $T \supseteq Q$ (Robinsonova aritmetika). Pak pro každou formuli $\varphi(x)$ s jednou volnou proměnnou x existuje sentence ψ taková, že $T \vdash \psi \leftrightarrow \varphi(\underline{\psi})$.

Ekvivalenci $\psi \leftrightarrow \varphi(\underline{\psi})$ je možné číst tak, že ψ říká „já mám vlastnost φ “ (odtud autoreference).

Neúplnost

Aplikací lemmatu na různé formule φ je možné získat řadu zajímavých důsledků.

Důsledek: (neexistence definice pravdy) Je-li $T \supseteq Q$ bezesporná, pak v T **neexistuje definice pravdy**, tj. formule τ taková, že pro každou sentenci ψ je $T \vdash \psi \leftrightarrow \tau(\underline{\psi})$.

Důkaz: Sporem – aplikací autoreferenčního lemmatu na formuli $\varphi \equiv \neg\tau$ získáme sentenci ψ takovou, že $T \vdash \psi \leftrightarrow \neg\tau(\underline{\psi}) \leftrightarrow \neg\psi$, tedy T je sporná. $\square$

Neúplnost

Věta (1. Gödelova věta o neúplnosti)

Je-li T bezesporná rekurzivně axiomatizovaná teorie rozšiřující Robinsonovu aritmetiku Q , pak existuje sentence ν pravdivá v $\mathbb{N}$ ale nedokazatelná v T .

Důkaz: (náznak) Dokážeme větu za nadbytečného, ovšem zjednodušujícího předpokladu, že $\mathbb{N} \models T$. Aplikujeme autoreferenční lemma na formuli $\varphi(x) \equiv \neg Pr_T(x)$ (taková formule existuje díky rekurzivní axiomatizovatelnosti T) a získáme sentenci ν takovou, že $T \vdash \nu \leftrightarrow \neg Pr_T(\underline{\nu})$.

Pak $T \not\vdash \nu$. Dokažme to sporem. Nechť $T \vdash \nu$, pak $T \vdash \neg Pr_T(\underline{\nu})$, tedy $\mathbb{N} \models \neg(\exists \delta)(Prf_T(\delta, \underline{\nu}))$. Zároveň však dle $T \vdash \nu$ existuje důkaz d sentence ν v T , tedy $\mathbb{N} \models Prf_T(\underline{d}, \underline{\nu})$ – spor. $\square$

Nerozhodnutelnost

L -teorie T je **rozhodnutelná**, existuje-li „algoritmus“, který o každé L -formuli rozhodne, zda je či není dokazatelná v T . V opačném případě je T **nerozhodnutelná**.

Platí následující kritéria (ne)rozhodnutelnosti:

Tvrzení: Rekurzivně axiomatizovaná kompletní teorie T je rozhodnutelná.

Tvrzení: Bezesporná teorie T rozšiřující Robinsonovu aritmetiku Q je nerozhodnutelná.

Příklad: Teorie DeLO či $VS(\mathbb{Q})$ jsou kompletní a rekurzivně axiomatizované, tedy jsou rozhodnutelné.

Příklad: Peanova aritmetika P a Robinsonova aritmetika Q jsou nerozhodnutelné teorie.