Základy logiky a teorie množin

Petr Pajas

pajas@matfyz.cz

URL (slajdy): http://pajas.matfyz.cz/vyuka

Proč studovat matematickou logiku a teorii množin

- objasnění vztahu jazyka a významu (syntaxe a sémantiky)
- precizace klíčových matematických pojmů: axiom, teorie, důkaz, dokazatelnost, model, pravdivost
- teorie množin: axiomatická teorie tvořící rámec moderní matematiky
- zobecnění základních matematických postupů a konstrukcí
- objasnění pojmů jako konečnost/nekonečnost, zavedení základních matematických struktur
- hledání mezí (bezespornost, nedokazatelnost, nerozhodnutelnost)

Výroková logika

V logice důsledně odlišujeme jazyk od významu, tj. syntax od sémantiky, symboly a matematické objekty, které tyto symboly označují.

Přitom syntax i sémantiku popisujeme a studujeme obvyklými matematickými prostředky, v případě syntaxe velmi primitivními (práce s konečnými posloupnostmi, řetězci).

Syntax výrokové logiky

Začneme s nějakou neprázdnou (konečnou nebo nekonečnou) množinou $\mathcal{P}$ symbolů, jejíž prvky nazýváme *prvoformule*, či též *výrokové proměnné*. Budeme je značit $A, B, C, \ldots$

Prvoformule představují tvrzení, jejichž vnitřní strukturu dále nezkoumáme, zajímá nás pouze jejich pravdivost/nepravdivost a logické vztahy mezi nimi, jež zachycujeme *logickými spojkami*:

$\neg$	negace	*„není pravda, že“* či *„non“*
$\vee$	disjunkce	*„nebo“* či *„vel“*
$\wedge$	konjunkce	*„a“* či *„et“*
$\rightarrow$	implikace	*„jestliže . . . , pak . . . “* či *„implikuje“*
$\leftrightarrow$	ekvivalence	*„právě (tehdy) když“*

—5—

Definice: *Jazyk výrokové logiky* tvoří:

- logické spojky $\neg$, $\vee$, $\wedge$, $\rightarrow$, $\leftrightarrow$.
- pomocné symboly (závorky) $(,)$.
- neprázdná množina $\mathcal{P}$ výrokových proměnných neboli prvoformulí ($\mathcal{P}$ neobsahuje spojky ani pomocné symboly)

—6—

Definice: *Výroková formule nad $\mathcal{P}$*: Formuli získáme konečným počtem užití následujících pravidel:

1) každá výroková proměnná A z množiny $\mathcal{P}$ je formulí
2) jsou-li výrazy φ, ψ formule, pak výrazy $\neg\varphi$, $(\varphi \vee \psi)$, $(\varphi \wedge \psi)$, $(\varphi \rightarrow \psi)$, $(\varphi \leftrightarrow \psi)$ jsou také formulemi

➠ Definice tohoto typu se nazývají *induktivní definice*.

➠ Analogicky definujeme pojem *podformule* dané formule θ (všechny formule, jež při sestavování θ vznikly nebo byly užity v krocích 1 a 2).

➠ Formule značíme řeckými písmeny: $\varphi, \psi, \vartheta, \chi, \xi, \ldots$

➠ U složitějších formulí budeme v dalším textu vnější závorky někdy vynechávat.

Příklady formulí: A, $(A \wedge \neg A)$, $((A \rightarrow B) \wedge (\neg A \rightarrow B)) \leftrightarrow B$, atp.

—7—

Ověřování, že nějaký výraz vyhovuje definici formule, probíhá tzv. indukcí dle složitosti.

Příklad: Nechť $\mathcal{P} = \{A, B, C, D\}$.
Pak $((A \vee B) \rightarrow \neg C)$ je formule:

a) Výrazy A, B a C jsou formule dle 1),

b) Výrazy $(A \vee B)$ a $\neg C$ jsou formule dle a) a 2)

c) Výraz $((A \vee B) \rightarrow \neg C)$ je formule dle b) a 2)

Naopak, snadno se nahlédne, že AB, $\rightarrow$, $A \rightarrow B \rightarrow C$, $(A\wedge) \rightarrow B$, apod. formule nejsou.

—8—

Výroková logika – Sémantika

Prvoformule z množiny $\mathcal{P}$ ve výrokové logice dále neanalyzujeme, jejich pravdivost tedy musí být dána *„z vnějšku“*.

Množina pravdivostních hodnot je množina $\{0, 1\}$.

Definice: *Pravdivostní ohodnocení nad $\mathcal{P}$* (krátce ohodnocení) je zobrazení $e : \mathcal{P} \rightarrow \{0, 1\}$ přiřazující každé výrokové proměnné pravdivostní hodnotu 0 nebo 1.

Každé takové zobrazení můžeme jednoznačně rozšířit z oboru $\mathcal{P}$ výrokových proměnných na obor všech výrokových formulí nad $\mathcal{P}$ ...

. . . indukcí dle složitosti formule:

Definice: *Pravdivostní hodnota formule φ při ohodnocení $e : \mathcal{P} \to \{0,1\}$* (značíme $\varphi[e]$):

1. Je-li φ výroková proměnná A, je $\varphi[e] = e(A)$.
2. Je-li φ tvaru $\neg\psi$, je $\varphi[e] = 1$, když $\psi[e] = 0$, jinak $\varphi[e] = 0$.
3. Je-li φ tvaru $(\psi \wedge \vartheta)$, je $\varphi[e] = 1$, když $\psi[e] = \vartheta[e] = 1$, jinak $\varphi[e] = 0$.
4. Je-li φ tvaru $(\psi \vee \vartheta)$, je $\varphi[e] = 0$, když $\psi[e] = \vartheta[e] = 0$, jinak $\varphi[e] = 1$.
5. Je-li φ tvaru $(\psi \to \vartheta)$, je $\varphi[e] = 0$, když $\psi[e] = 1$ a $\vartheta[e] = 0$, jinak $\varphi[e] = 1$.
6. Je-li φ tvaru $(\psi \leftrightarrow \vartheta)$, je $\varphi[e] = 1$, když $\psi[e] = \vartheta[e]$, jinak $\varphi[e] = 0$.

Předchozí definici můžeme stručně vyjádřit pomocí tabulky:

ψ	ϑ	$\neg\psi$	$(\psi \wedge \vartheta)$	$(\psi \vee \vartheta)$	$(\psi \to \vartheta)$	$(\psi \leftrightarrow \vartheta)$
0	0	1	0	0	1	1
0	1	1	0	1	1	0
1	0	0	0	1	0	0
1	1	0	1	1	1	1

Jsou-li ψ a ϑ prvoformule, představují první dva sloupce všechna možná ohodnocení těchto dvou prvoformulí.

Z definice je patrné, že pravdivostní hodnota formule závisí pouze na ohodnocení výrokových proměnných, které se v ní vyskytují.

Terminologie:

- Formule φ je *pravdivá* při ohodnocení e, je-li $\varphi[e] = 1$. V opačném případě je při ohodnocení e *nepravdivá*.
- Je-li $\varphi[e] = 1$, říkáme též, že e je *model* formule φ a píšeme $e \models \varphi$.
- Je-li $\varphi[e] = 1$ pro **každé** e, říkáme, že φ je *tautologie*. Píšeme: $\models \varphi$.
- Je-li $\varphi[e] = 1$ pro **některé** e, říkáme, že φ je *splnitelná* (*má model*).
- Není-li φ splnitelná, je *nesplnitelná* (*nemá model*).

Na základě definice pravdivostní hodnoty formule lze vždy rozhodnout, při kterých ohodnoceních je daná formule pravdivá, zda je či není tautologií, atd. **Pro jednoduché formule lze užít tzv. tabulkovou metodu**.

Příklad: Formule $(B \to A) \vee \neg A$.

Postupně určujeme hodnoty jednotlivých podformulí a zapisujeme je do tabulky pravdivostních hodnot.

A	B	$(B \to A)$	$\neg A$	$(B \to A) \vee \neg A$
0	0	1	1	1
0	1	0	1	1
1	0	1	0	1
1	1	1	0	1

Vidíme, že uvedená formule je tautologie.

Některé důležité tautologie:

- Zákon dvojí negace: $\neg\neg A \leftrightarrow A$
- Obměna: $(A \to B) \leftrightarrow (\neg B \to \neg A)$
- Princip sporu: $\neg(A \wedge \neg A)$
- Zákon vyloučení třetího: $(A \vee \neg A)$
- Tranzitivita implikace: $((A \to B) \wedge (B \to C)) \to (A \to C)$
- Antisymetrie implikace: $((A \to B) \wedge (B \to A)) \leftrightarrow (A \leftrightarrow B)$
- Komutativita konjunkce: $(A \wedge B) \leftrightarrow (B \wedge A)$
- Komutativita disjunkce: $(A \vee B) \leftrightarrow (B \vee A)$

- Asociativita konjunkce: $((A \wedge B) \wedge C) \leftrightarrow (A \wedge (B \wedge C))$
- Asociativita disjunkce: $((A \vee B) \vee C) \leftrightarrow (A \vee (B \vee C))$
- Distributivita $\wedge$ vůči $\vee$: $(A \wedge (B \vee C)) \leftrightarrow ((A \wedge B) \vee (A \wedge C))$
- Distributivita $\vee$ vůči $\wedge$: $(A \vee (B \wedge C)) \leftrightarrow ((A \vee B) \wedge (A \vee C))$
- Vlastnost minima: $(A \wedge B) \to A$
- Vlastnost maxima: $A \to (A \vee B)$
- de Morganova pravidla: $\neg(A \wedge B) \leftrightarrow (\neg A \vee \neg B)$, $\neg(A \vee B) \leftrightarrow (\neg A \wedge \neg B)$
- Negace implikace: $\neg(A \to B) \leftrightarrow (A \wedge \neg B)$, $(A \vee B) \leftrightarrow (\neg A \to B)$, $(A \to B) \leftrightarrow (\neg A \vee B)$

Symbol $\top$ (*pravda*) chápeme jako zkratku za libovolnou tautologii, např. $(A \vee \neg A)$, a $\bot$ (*nepravda*, *spor*) jako zkratku za libovolnou nesplnitelnou formuli, např. $(A \wedge \neg A)$.

(V literatuře se někdy $\top$ a $\bot$ zavádějí jako nulární logické spojky.)

Pro každé ohodnocení e tedy platí $e(\top) = 1$ a $e(\bot) = 0$.

Platí např. (zákony absorpce):

$$\top \vee B \leftrightarrow \top, \quad \top \wedge B \leftrightarrow B$$
$$\bot \vee B \leftrightarrow B, \quad \bot \wedge B \leftrightarrow \bot.$$

Na základě známých tautologií a následující věty lze formule ekvivalentně upravovat, podobně jako se upravují algebraické výrazy.

Věta (*o nahrazení*): *Buďte φ, ψ, ϑ výrokové formule a A výroková proměnná. Pak platí*

1. *Je-li φ tautologie, pak nahrazením všech výskytů výrokové proměnné A ve formuli φ formulí ψ získáme opět tautologii.*
2. *Je-li $\psi \leftrightarrow \vartheta$ tautologie a φ' formule vzniklá z φ nahrazením některých výskytů podformule ψ formulí ϑ, pak $\varphi \leftrightarrow \varphi'$ je tautologie.*

Příklad: Uvažujme formuli $\neg(\neg(A \wedge \neg B) \vee A) \to C$.
Upravujme postupně její podformule (zápis $\varphi \leftrightarrow \psi \leftrightarrow \theta$ zde značí $\varphi \leftrightarrow \psi$ a $\psi \leftrightarrow \theta$):

- $\neg(A \wedge \neg B) \leftrightarrow (\neg A \vee \neg\neg B) \leftrightarrow (\neg A \vee B)$ dle de Morganova pravidla, pravidla dvojí negace a věty o nahrazení.
- $(\neg(A \wedge \neg B) \vee A) \leftrightarrow ((\neg A \vee B) \vee A) \leftrightarrow ((B \vee \neg A) \vee A) \leftrightarrow (B \vee (\neg A \vee A)) \leftrightarrow (B \vee \top) \leftrightarrow \top$ dle věty o nahrazení a komutativního a asociativního zákona pro $\vee$, a zákona absorpce.
- Původní formule je tedy ekvivalentní s $\neg\top \to C$, což je ekvivalentní $\top \vee C$, tedy i s $\top$.

Množiny formulí:

- Řekneme, že množina formulí T je *splnitelná*, existuje-li ohodnocení e takové, že $\varphi[e] = 1$ pro každé φ z množiny T.
  Píšeme pak $e \models T$ (čteme e je *model* T).
- Formule φ je *tautologickým důsledkem* množiny formulí T, pokud $e \models \varphi$ kdykoli $e \models T$. Píšeme $T \models \varphi$.

Zřejmě $T \models \varphi$ platí pro každé $\varphi \in T$.

Věta (*Modus ponens*): $\varphi, (\varphi \to \psi) \models \psi$.
Obecněji, je-li T množina formulí a formule φ, ψ jsou takové, že $T \models \varphi$ a $T \models (\varphi \to \psi)$, pak $T \models \psi$.

Věta (*o dedukci*): *Jsou-li φ, ψ výrokové formule a T množina výrokových formulí, pak*

$$T \models \varphi \to \psi \quad \text{právě když} \quad T, \varphi \models \psi$$

Příklad: Máme ukázat, že

$$\models (A \to (B \to (C \to D))) \to (C \to (B \to (A \to D)))$$

Důkaz. Několikanásobným užitím věty o dedukci převedeme úlohu na $(A \to (B \to (C \to D))), C, B, A \models D$. Několikanásobným užitím pravidla Modus ponens získáme postupně $(A \to (B \to (C \to D))), C, B, A \models (B \to (C \to D)), (C \to D), D$. □

Věta (*o důkazu sporem*): $T \models \varphi$ *právě tehdy když* $T, \neg\varphi \models \bot$
(tj. když množina formulí $T \cup \{\neg\varphi\}$ je nesplnitelná).

Neboli, formule platí právě tehdy, když z její negace lze vyvodit spor.

Věta (*o rozboru případů*): $T, \varphi \vee \psi \models \theta$ *právě tehdy když* $T, \varphi \models \theta$ *a současně* $T, \psi \models \theta$.

Neboli, je-li v předpokladu disjunkce, musíme prověřit obě alternativy zvlášť a z obou musí vyplývat závěr!

—21—

Věta (*o dualitě*): *Nechť φ je formule neobsahující jiné logické spojky než $\neg$, $\vee$ a $\wedge$. Pak $\models \neg\varphi \leftrightarrow \varphi^d$, kde φ^d je tzv. duální formule k φ.*
Ta vznikne z φ nahrazením prvoformulí jejich negacemi a nahrazením každé logické spojky $\square$ spojkou $\square^d$, přičemž $\wedge^d = \vee$, $\vee^d = \wedge$ a $\neg^d = \neg$.

- Větu o dualitě lze dokázat např. indukcí dle složitosti formule.
- Umožňuje *„zbavit se negace“* na začátku formule.
  (Víme *„není pravda, že ...“*, zajímá nás, *„co pravda je“*.)
- Speciálním případem této věty jsou De Morganova pravidla.

Co s formulemi, jež obsahují spojky $\rightarrow, \leftrightarrow$?

- Implikaci $(A \rightarrow B)$ lze nahradit formulí $(\neg A \vee B)$.
- Pro ekvivalenci platí: $\neg(A \leftrightarrow B) \leftrightarrow (A \leftrightarrow \neg B) \leftrightarrow (\neg A \leftrightarrow B)$

—22—

Literál je každá formule tvaru A a $\neg A$ pro $A \in \mathcal{P}$. Literály a konjunkce resp. disjunkce dvou nebo více literálů nazýváme *konjunktivní* resp. *disjunktivní formule*. Jedná se tedy o formule tvaru $\varphi_1 \wedge \varphi_2 \ldots \wedge \varphi_n$ resp. $\varphi_1 \vee \varphi_2 \ldots \vee \varphi_n$, kde $n \geq 1$ a každé φ_i je tvaru A nebo $\neg A$ pro nějaké $A \in \mathcal{P}$. (Vynechávání závorek je umožněno asociativitou $\vee$ a $\wedge$.)

Pro některé aplikace (např. databáze) je výhodné výrokové formule převést do jistého speciálního „normalizovaného“ tvaru:

- Formule je v tzv. *disjunktivním normálním tvaru (DNF)*, je-li disjunkcí konjunktivních formulí. Např. $(A \wedge B \wedge \neg C) \vee (\neg A \wedge B) \vee \neg D$, ale i samotné $(\neg A \wedge B)$ či jen $\neg D$.
- Formule je v tzv. *konjunktivním normálním tvaru (CNF)*: je-li konjunkcí disjunktivních formulí, např. $(A \vee D) \wedge (\neg A \vee \neg D) \wedge (B \vee \neg A \vee \neg C)$ (ale též libovolná disjunktivní formule či jen literál).

—23—

Věta (*o normálním tvaru*): *Ke každé výrokové formuli φ existuje formule ψ v DNF a formule θ v CNF tak, že $\psi \leftrightarrow \varphi \leftrightarrow \theta$.*

Důkaz. Ukážeme pouze existenci ψ (θ se najde podobně). Je-li φ nesplnitelná, položíme ψ rovno $(A \wedge \neg A)$. Nechť $\mathcal{P} = \{A_1, \ldots, A_n\}$ obsahuje všechny výrokové proměnné vyskytující se ve formuli φ. Pro každé ohodnocení $e : \mathcal{P} \rightarrow \{0,1\}$ buď ψ_e formule tvaru $A_1^e \wedge \ldots \wedge A_n^e$, kde A_i^e je A_i, pokud $e(A_i) = 1$, jinak $A_i^e = \neg A_i$. Zřejmě je ψ_e splněna právě ohodnocením e, tj. $\psi_e[e] = 1$ a $\psi_e[e'] = 0$ pro libovolné ohodnocení $e' : \mathcal{P} \rightarrow \{0,1\}$, $e \neq e'$. Buď nyní ψ disjunkcí formulí ψ_e příslušejících právě těm ohodnocením, pro něž $\varphi[e] = 1$ (takové existuje aspoň jedno). Pak zřejmě $\varphi[e] = \psi[e]$ pro každé e a ψ je v DNF. $\square$

Úkol: *dokažte obdobným způsobem existenci formule θ v CNF.*

—24—

V praxi je často jednodušší formuli převést do normálního tvaru na základě vět o nahrazení a o dualitě a základních tautologií (eliminace $\rightarrow$ a $\leftrightarrow$, distributivní zákon, atp.).

Příklad: Nalezení DNF ekvivalentu formule $\neg(A \wedge (B \vee \neg C)) \rightarrow C$: Nejprve se zbavíme $\rightarrow$ a formuli převedeme na $(A \wedge (B \vee \neg C)) \vee C$. Dále využijeme distributivitu a podformuli $(A \wedge (B \vee \neg C))$ nahradíme ekvivalentní formulí $((A \wedge B) \vee (A \wedge \neg C))$. Celkem (po odstranění závorek umožněném asociativitou) získáváme:

$$(A \wedge B) \vee (A \wedge \neg C) \vee C$$

$\wedge\vee$-tvar: vyjdeme z $(A \wedge (B \vee \neg C)) \vee C$ a distributivním zákonem pro $\vee$ získáme $(A \vee C) \wedge (B \vee \neg C \vee C)$. To je navíc ekvivalentní s $(A \vee C) \wedge (B \vee \top)$ a tedy i s $(A \vee C)$.

O výrokových funkcích a logických spojkách

Buď $\mathcal{P}$ libovolná *konečná* neprázdná množina prvovýroků.

- Označme $\mathcal{E}_\mathcal{P}$ množinu všech ohodnocení nad množinou prvoformulí $\mathcal{P}$. Zobrazením $F : \mathcal{E}_\mathcal{P} \to \{0,1\}$ říkáme *pravdivostní funkce* (nad $\mathcal{P}$).
- Každá výroková formule φ nad $\mathcal{P}$ určuje pravdivostní funkci $F_\varphi : e \mapsto \varphi[e]$.
- Řekneme, že obor $\mathcal{F}$ výrokových formulí nad $\mathcal{P}$ je *úplný*, pokud pro každou pravdivostní funkci F nad $\mathcal{P}$ existuje $\varphi \in \mathcal{F}$ tak, že $F = F_\varphi$.
- Z důkazu věty o normální formě plyne, že obory a) všech výrokových formulí, b) formulí v DNF, c) formulí v CNF, jsou úplné.
- Je-li σ množina logických spojek, značí $\mathcal{F}_\sigma$ obor formulí, v nichž se vyskytují pouze spojky z množiny σ. Jelikož $(A \wedge B) \leftrightarrow \neg(\neg A \vee \neg B)$, je obor $\mathcal{F}_{\{\neg,\vee\}}$ úplný. Z věty o dualitě plyne totéž pro $\mathcal{F}_{\{\neg,\wedge\}}$.

Zaveďme binární logickou spojku $(A|B)$ tak, že $(A|B) \leftrightarrow \neg(A \wedge B)$.

Úkol: *Ukažte, že obory formulí $\mathcal{F}_{\{\neg,\to\}}$ a $\mathcal{F}_{\{|\}}$ nad $\mathcal{P}$ jsou úplné.*

Formální metoda pro výrokový počet

K výrokovému počtu lze přistupovat též tzv. *formální metodou*, kdy vyjdeme z několika formulí (*axiomů*) a ostatní formule vyvozujeme prostřednictvím formálních důkazů na základě axiomů a odvozovacího pravidla (jímž bude pravidlo Modus Ponens).

Vyjdeme z redukovaného jazyka obsahujícího ze spojek pouze $\neg$ a $\to$.

Schémata axiomů výrokové logiky

V1 $\quad \varphi \to (\psi \to \varphi)$

V2 $\quad (\varphi \to (\psi \to \theta)) \to ((\varphi \to \psi) \to (\varphi \to \theta))$

V3 $\quad (\neg\psi \to \neg\varphi) \to (\varphi \to \psi)$

Axiomem výrokové logiky je každá formule tvaru V1, V2, nebo V3, kde φ, ψ, θ jsou výrokové formule. Konkrétní volbou formulí φ, ψ, θ získáme tzv. *instanci* schématu V1, V2, resp. V3.

Odvozovací pravidlo

Modus ponens – pravidlo odloučení – (čteme *„z formulí φ a $(\varphi \to \psi)$ odvod' ψ"*):

$$\frac{\varphi,\ (\varphi \to \psi)}{\psi}$$

Pojem formálního důkazu

Je-li T množina formulí, je *důkazem formule φ z předpokladů T* (či *v T*) konečná posloupnost formulí $\varphi_1, \ldots, \varphi_n$ taková, že $\varphi_n = \varphi$ a pro každé $i \in \{1, \ldots, n\}$ platí

- φ_i je axiom výrokového počtu, nebo
- $\varphi_i \in T$ (tj. φ_i je jeden z předpokladů, neboli axiom T), nebo
- φ_i lze získat aplikací pravidla Modus ponens na nějaké dvě formule, které v důkazu přecházejí formuli φ_i. To jest, existují $j, k < i$ tak, že φ_j je formule $(\varphi_k \to \varphi_i)$.

Existuje-li její důkaz formule φ v T, říkáme, že je *dokazatelná v T*, případně že je *větou* T a píšeme $T \vdash \varphi$.

Je-li T prázdná množina, říkáme jen *důkaz*, *dokazatelná* (ve výrokovém počtu), píšeme $\vdash \varphi$, atp.

Množina formulí T je *bezesporná*, pokud v T nelze dokázat spor, tj. formuli $\bot$, kde $\bot$ je např. $\neg(A \to A)$. Píšeme $T \nvdash \bot$. V opačném případě je T *sporná*, $T \vdash \bot$.

Příklad: dokážeme formuli $(A \to A)$

Následující posloupnost formulí je jejím formálním důkazem:

1. $A \to ((A \to A) \to A)$ instance V1
2. $(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A))$ instance V2
3. $(A \to (A \to A)) \to (A \to A)$ Modus ponens z 1),2)
4. $A \to (A \to A)$ instance V1
5. $(A \to A)$ Modus ponens z 4),3)

Úplnost výrokového počtu

Věta (*o bezespornosti a splnitelnosti*): *Je-li T množina výrokových formulí, pak T je bezesporná právě když T je splnitelná.*

Proč? $\Leftarrow$: stačí dokázat, že axiomy logiky jsou tautologie a že odvozovací pravidlo MP zachovává pravdivost. Ze splnitelné množiny tedy nelze dokázat spor. $\Rightarrow$: bezespornou množinu T lze rozšířit do maximální bezesporné množiny $T' \supseteq T$ (tzv. Lindenbaumova věta), tak že pro každé φ buď $\varphi \in T'$ nebo $\neg\varphi \in T'$. Ukáže se, že ohodnocení e takové, že pro prvoformuli A je $e(A) = 1$, když $A \in T'$, a $e(A) = 0$, když $\neg A \in T'$, je modelem T' a tedy i T.

DŮsledek (*Post*): *Pro výrokovou formuli φ a množinu výrokových formulí T platí:*

$$T \vdash \varphi \quad \textit{právě když} \quad T \models \varphi$$

Věta (*o kompaktnosti*): *Množina T je splnitelná, právě když každá konečná podmnožina $S \subseteq T$ je splnitelná.*

Neboli: existuje-li pro každou konečnou podmnožinu $S \subseteq T$ ohodnocení e_S splňující $e_S \models S$, pak existuje ohodnocení e tak, že $e \models T$.

Má řadu aplikací i mimo logiku, např. v teorii grafů.

Důkaz. 1. Je-li T splnitelná a $e \models T$, pak jistě $e \models S$ i pro každé konečné $S \subseteq T$.

2. Je-li naopak T nesplnitelná, je T sporná dle věty o bezespornosti a splnitelnosti. Tudíž v T existuje důkaz sporu, tj. formule $\neg(A \to A)$. Buď $\varphi_1, \ldots, \varphi_n$ důkaz sporu v T a nechť S je množina všech formulí z T, které se v tomto důkazu vyskytují. Pak $S \subseteq T$ je konečná a $\varphi_1, \ldots, \varphi_n$ je důkaz sporu v S. S je tedy sporná, tudíž nesplnitelná. Jsme hotovi. □

Predikátová logika (logika 1. řádu)

Jazyk výrokového počtu parametrizovala pouze množina výrokových proměnných $\mathcal{P}$ a její volba nebyla nijak zvlášť podstatná.

Jazyk predikátové logiky je daleko bohatší a volba parametrů (predikátových a funkčních symbolů a jejich četností) je často klíčová.

Základ jazyka predikátové logiky tvoří tzv. *logické symboly*:

- *Proměnné* (x, y, z, x_1, x_2, …, x', x'', …); dle potřeby jich je neomezeně mnoho. (Říká se též proměnné pro individua či individuální proměnné).
- Symboly pro *logické spojky*: $\neg$, $\wedge$, $\vee$, $\to$, $\leftrightarrow$
- Symboly pro *kvantifikátory*: $\forall$ univerzální (pro všechna), $\exists$ existenční (existuje)
- Pomocné symboly (závorky)

Kompletní jazyk logiky 1. řádu určuje až konkrétní volba *mimologických symbolů*:

- *Funkční symboly*, každý se svou četností (počet argumentů) $n \geq 0$.
- *Predikátové* neboli *relační symboly*, každý se svou četností $n \geq 0$.

Mimologických symbolů může být konečně ale i nekonečně mnoho.

Predikátový symbol rovnosti, $=$ (četnost 2) má v logice speciální význam a proto se někdy zahrnujeme, na rozdíl od ostatních predikátových symbolů, mezi logické symboly. Mluvíme pak o logice s rovností.

Formálně:

Definice: *Jazyk 1. řádu* je zadán trojicí $\mathcal{L} = \langle \mathcal{F}, \mathcal{R}, \sigma \rangle$, kde $\mathcal{F}$ a $\mathcal{R}$ jsou vzájemně disjunktní množiny symbolů (různých od logických symbolů) zvaných *funkční* a *predikátové* a $\sigma : \mathcal{F} \cup \mathcal{R} \to \mathbb{N}$ je zobrazení, přiřazující každému z těchto symbolů přirozené číslo, které nazýváme jeho *četností*.

Trojici $\mathcal{L}$ nazýváme stručně *jazyk*.

Symboly četnosti 1 nazýváme *unární*, četnosti 2 *binární*, četnosti 3 *ternární*, četnosti n *n-ární*. Četnosti se proto též říká *arita*.

Jazykům bez predikátových symbolů ($\mathcal{R} = \emptyset$) se říká *algebraické jazyky*. Jejich sémantika se studuje v algebře.

Funkční symboly četnosti 0 nazýváme též *konstanty*. (Predikátové symboly četnosti 0 se užívají zřídka, odpovídají cca výrokovým proměnným.)

Příklady

- *Teorie množin* má jazyk s rovností a jedním mimologickým symbolem $\in$. Píšeme $\mathcal{L}^{TM} = \{\in\}$.
- *Teorie grup* má jazyk s rovností, binárním funkčním symbolem $\circ$ a nulárním funkčním symbolem (neboli konstantou) e. $\mathcal{L}^{G} = \{\circ, e\}$.
- *Jazyk aritmetiky* obsahuje vedle rovnosti násl. speciální symboly: konstantu 0, unární operaci S (následník), binární operace $+$ (sčítání) a $\cdot$ (násobení) a binární predikát $\leq$ (uspořádání). $\mathcal{L}^{Ar} = \{0, S, +, \cdot, \leq\}$.
- *Příklad nekonečného jazyka:* jazyk vektorových prostorů nad tělesem reálných čísel $\mathcal{L}^{V(\mathbb{R})} = \{0, +\} \cup \{r\cdot \ ; \ r \in \mathbb{R}\}$, kde 0 je konstanta (nulový vektor), $+$ je binární operace vektorového součtu a pro každé reálné číslo r je v jazyce unární funkční symbol $r\cdot$ pro násobení skalárem r.

Termy a formule

Pojmy termu a formule jazyka $\mathcal{L}$ definujeme induktivně.

Term je výraz určující individuum. **Definice:**

1. každá proměnná je term
2. je-li F n-ární a $t_1, \ldots, t_n$ jsou termy , pak $F(t_1, \ldots, t_n)$ je term
3. každý term vznikne konečným počtem užití pravidel 1) a 2).

Formule vyjadřují tvrzení o individuích. **Definice:**

i) je-li P n-ární predikátový symbol a $t_1, \ldots, t_n$ jsou termy, pak $P(t_1, \ldots, t_n)$ je (tzv. *atomická*) formule

ii) jsou-li φ, ψ formule, jsou formulemi rovněž výrazy $\neg\varphi$, $(\varphi \vee \psi)$, $(\varphi \wedge \psi)$, $(\varphi \to \psi)$, $(\varphi \leftrightarrow \psi)$

iii) je-li x proměnná a φ formule, jsou $(\forall x)\varphi$ a $(\exists x)\varphi$ formule.

iv) každá formule vznikne konečným počtem užití pravidel i), ii), iii).

Příklady

U binárních predikátových a funkčních symbolů užíváme infixní notace. Píšeme tedy např. $(x + y)$ resp. $x \leq y$ místo definicemi požadovaných $+(x, y)$ resp. $\leq(x, y)$. Z důvodů lepší čitelnosti budeme někdy vynechávat i vnější závorky termů a formulí.

- $(x \cdot (y \cdot z))$ a $(x + S(x)) + S(S(0) \cdot S(y))$ jsou termy jazyka aritmetiky $\mathcal{L}^{Ar}$
- $S(x, y)$ ani $(x + y + z)$ nejsou termy jazyka $\mathcal{L}^{Ar}$.
- $s \cdot (r \cdot x) + y$, kde $r, s \in \mathbb{R}$, je term jazyka $\mathcal{L}^{V(\mathbb{R})}$.
- $x \circ e = e \circ x$ je formule jazyka grup $\mathcal{L}^{G}$ (v logice s rovností)
- taktéž $(\forall x)(\exists y)(x \circ y = e \ \wedge \ y \circ x = e)$
- $\neg(\exists x)S(x) = 0$ a $(\forall x)(x \neq 0 \rightarrow (\exists y)S(y) = x)$ jsou formule jazyka $\mathcal{L}^{Ar}$, přičemž $t_1 \neq t_2$ je obvyklá zkratka za $\neg(t_1 = t_2)$.

Podtermy, podformule, výskyty proměnných

Nechť t je term a φ formule. Pak

i) podslovo s termu t, které je samo termem, nazveme *podtermem* termu t,

   podslovo ψ formule φ, které je samo formulí, nazveme *podformulí* formule φ.

ii) určitý výskyt proměnné x ve formuli φ nazveme *vázaným*, je-li součástí nějaké podformule tvaru $(\exists x)\psi$ nebo $(\forall x)\psi$.

Výskytům proměnné x, které nejsou vázané, říkáme *volné*.

Příklad: Ve formuli $x = x \wedge (\exists x)(0 \leq x)$ jsou první dva výskyty proměnné x volné, zatímco druhé dva vázané.

iii) *proměnná* x je ve formuli φ *volná*, má-li tam volný výskyt a je tam *vázaná*, má-li tam vázaný výskyt.

iv) Formule je *otevřená*, neobsahuje-li žádný vázaný výskyt proměnné. Formule je *uzavřená*, neobsahuje-li žádný volný výskyt proměnné.

Příklad: Ve formuli $x = y \wedge (x \neq 0 \rightarrow (\exists y)(S(y) = x))$ je x jen volná, zatímco y je tam jak volná tak vázaná.

Formule $y \neq x$ je otevřená, zatímco $(\forall x)(\exists y)(y \neq x)$ je uzavřená. Formule $0 + 0 = 0$ je současně uzavřená i otevřená.

Sémantika predikátové logiky

Abychom mohli formulím nějakého jazyka 1. řádu „vdechnout“ význam, musíme nejprve určit obor pro individuální proměnné a nad ním interpretovat jednotlivé mimologické symboly jazyka:

Definice: *Relační struktura* $\mathcal{M}$ pro jazyk $\mathcal{L}$ sestává z neprázdné množiny individuí M (zvané *univerzum* struktury $\mathcal{M}$) a zobrazení, které

- každému funkčnímu symbolu F jazyka $\mathcal{L}$ četnosti $n \geq 1$ přiřazuje funkci $F^{\mathcal{M}} : M^n \rightarrow M$,
- každé konstantě (funkčnímu symbol četnosti 0) c jazyka $\mathcal{L}$ prvek $c^{\mathcal{M}} \in M$,
- a každému predikátovému symbolu P jazyka $\mathcal{L}$ relaci $P^{\mathcal{M}} \subseteq M^n$

Říkáme, že struktura $\mathcal{M}$ je interpretací jazyka $\mathcal{L}$, píšeme $M \models \mathcal{L}$.

Příklady struktur

Struktury zadáváme zpravidla výčtem $\langle M, F_1^{\mathcal{M}}, F_2^{\mathcal{M}}, \ldots, P_1^{\mathcal{M}}, P_2^{\mathcal{M}}, \ldots\rangle$, přičemž $F_i^{\mathcal{M}}$ resp. $R_j^{\mathcal{M}}$ je funkce resp. relace odpovídající symbolu F_i resp. R_i daného jazyka.

- $\langle \mathbb{R}, <^{\mathbb{R}}\rangle$, kde $<^{\mathbb{R}}$ je obvyklá binární relace uspořádání reálných čísel, je struktura pro jazyk $\mathbb{R}$
- $\langle \mathbb{R}, \cdot^{\mathbb{R}}\rangle$, kde $\cdot^{\mathbb{R}}$ je obvyklá binární operace násobení reálných čísel, je struktura pro jazyk teorie grup
- $\langle \mathbb{N}, S^{\mathbb{N}}, +^{\mathbb{N}}, \cdot^{\mathbb{N}}, \leq^{\mathbb{N}}\rangle$, kde $S^{\mathbb{N}}(n) = n + 1$ pro každé $n \in \mathbb{N}$ a kde $+^{\mathbb{N}}, \cdot^{\mathbb{N}}$ značí obvyklé operace sčítání a násobení přirozených čísel a $\leq^{\mathbb{N}}$ značí jejich obvyklé (neostré) uspořádání je struktura pro jazyk $\mathcal{L}^{Ar}$

Nemůže-li dojít k mýlce, v těchto a podobných případech horní indexy zpravidla vynecháváme, symboly jazyka i jejich interpretace značíme stejně.

Hodnota termu ve struktuře

Nechť struktura $\mathcal{M}$ s univerzem M je interpretací jazyka $\mathcal{L}$. Ohodnocením ve struktuře $\mathcal{M}$ rozumíme zobrazení e přiřazující každé proměnné nějaký prvek $e(x) \in M$ univerza struktury $\mathcal{M}$.

Definice: Buď t term jazyka $\mathcal{L}$. *Hodnota termu* t ve struktuře $\mathcal{M}$ při ohodnocení e je prvek $t[e]$ (obšírně $t^{\mathcal{M}}[e]$) množiny M, definovaný indukcí dle složitosti termu t:

- je-li t proměnná, je $t[e] = e(t)$,
- je-li t tvaru $F(t_1, \ldots, t_n)$ a $F^{\mathcal{M}}$ je interpretace funkčního symbolu F ve struktuře $\mathcal{M}$, je $t[e] = F^{\mathcal{M}}(t_1[e], \ldots, t_n[e])$.

Neboli: hodnotu $t[e]$ vypočteme tak, že dosadíme za proměnné konkrétní prvky struktury $\mathcal{M}$ předepsané ohodnocením e a ve struktuře $\mathcal{M}$ na nich „provedeme“ předepsané operace (funkce).

Všimněme si, že hodnota $t[e]$ závisí pouze na ohodnocení proměnných, které se v termu t vyskytují.

Jsou-li všechny proměnné vyskytující se v termu t mezi $x_1, \ldots, x_n$, zapisujeme term t někdy jako $t(x_1, \ldots, x_n)$.

Je-li navíc e ohodnocení a pro $1 \leq i \leq n$ je $e(x_i) = m_i$, zapisujeme $t[e]$ jako $t(x_1, \ldots, x_n)[m_1, \ldots, m_n]$, případně jen $t[m_1, \ldots, m_n]$.

Je-li e ohodnocení v $\mathcal{M}$ a $m \in M$, značí $e(x/m)$ ohodnocení, jež proměnné x přiřadí m a na ostatních proměnných je shodné s e, tj. $e(x/m)(x) = m$ a $e(x/m)(y) = e(y)$ pro y různé od x.

Definice (*Tarského definice pravdy*): Formule φ je pravdivá ve struktuře $\mathcal{M}$ při ohodnocení e (značíme $\mathcal{M} \models \varphi[e]$), jestliže

- φ je atomická tvaru $t_1 = t_2$ a hodnotou $t_1[e]$ a $t_2[e]$ je týž prvek M,
- φ je atomická tvaru $P(t_1, \ldots, t_n)$ a $\langle t_1[e], \ldots, t_n[e]\rangle \in P^{\mathcal{M}}$, kde $P^{\mathcal{M}}$ je relace realizující mimologický predikátový symbol P v $\mathcal{M}$
- φ je tvaru $\neg\psi$ a formule ψ není v $\mathcal{M}$ pravdivá při ohodnocení e
- φ je tvaru $(\psi \wedge \theta)$ obě formule ψ, θ jsou v $\mathcal{M}$ při ohodnocení e pravdivé ... analogicky pro $(\psi \vee \theta)$, $(\psi \to \theta)$ a $(\psi \leftrightarrow \theta)$, jako ve výrokové logice
- φ je tvaru $(\forall x)\varphi$ a pro každý prvek $m \in M$ je formule φ pravdivá v $\mathcal{M}$ při ohodnocení $e(x/m)$
- φ je tvaru $(\exists x)\varphi$ a existuje prvek $m \in M$ tak, že formule φ je pravdivá v $\mathcal{M}$ při ohodnocení $e(x/m)$

Jinak je φ ve struktuře $\mathcal{M}$ při ohodnocení e *nepravdivá*, píšeme $\mathcal{M} \not\models \varphi[e]$.

—45—

Pravdivost formule φ ve struktuře $\mathcal{M}$ při ohodnocení e závisí pouze na ohodnocení volných proměnných ve formuli φ.

Formule φ je *splnitelná* v $\mathcal{M}$, platí-li $\mathcal{M} \models \varphi[e]$ pro nějaké ohodnocení e.

Formule φ je *pravdivá* v $\mathcal{M}$, platí-li $\mathcal{M} \models \varphi[e]$ pro každé ohodnocení e; píšeme pak $\mathcal{M} \models \varphi$ a čteme $\mathcal{M}$ je *model* φ.

Připomeňme, že formule je uzavřená, neobsahuje-li volnou proměnnou. Uzavřené formuli se někdy též říká *sentence*. Její pravdivost ve struktuře nezávisí na ohodnocení a je tedy splnitelná v $\mathcal{M}$ právě když je v $\mathcal{M}$ pravdivá.

Formule φ je *logicky pravdivá*, je-li pravdivá v libovolné struktuře $\mathcal{M}$ interpretující daný jazyk. Píšeme pak $\models \varphi$.

Příkladem takové formule v logice s rovností je např. $(\forall x)(x = x)$.

—46—

Teorie

Množinu formulí T jazyka $\mathcal{L}$ nazveme teorií v jazyce $\mathcal{L}$.
Přesněji: *Teorií* nazýváme dvojici $(\mathcal{L}, T)$, kde $\mathcal{L}$ je jazyk a T je množina formulí v jazyce $\mathcal{L}$. Značit ji budeme ale jen symbolem T.

Prvky množiny T nazýváme *axiomy teorie* T. Struktura $\mathcal{M}$ interpretující jazyk $\mathcal{L}$ je *modelem* teorie T (píšeme $\mathcal{M} \models T$), jestliže pro každou formuli $\varphi \in T$ platí $\mathcal{M} \models \varphi$.

Formule φ je *logickým důsledkem* T (píšeme $T \models \varphi$), je-li φ pravdivá v každém modelu teorie T. Říkáme též, že φ *vyplývá* z T.

Příklad (*princip generalizace*):

$$\varphi \models (\forall x)\varphi$$

—47—

Věta (*o vyloučení třetího*): *Nechť $\mathcal{M}$ je struktura pro jazyk $\mathcal{L}$ a φ formule jazyka $\mathcal{L}$. Pak*

1. *Jestliže $\mathcal{M} \models \varphi$, pak $\mathcal{M} \not\models \neg\varphi$.*
2. *Je-li φ navíc uzavřená, pak $\mathcal{M} \models \varphi$ nebo $\mathcal{M} \models \neg\varphi$.*

Důkaz. Je-li $\mathcal{M} \models \varphi$, pak $\mathcal{M} \models \varphi[e]$ pro každé ohodnocení e, přičemž aspoň jedno ohodnocení e vždy existuje, neboť M je z definice neprázdná. Pro toto e je dle definice pravdy $\mathcal{M} \not\models (\neg\varphi)[e]$, tudíž $\mathcal{M} \not\models \neg\varphi$.

Když $\mathcal{M} \not\models \varphi$, pak $\mathcal{M} \not\models \varphi[e]$ pro nějaké e, tudíž $\mathcal{M} \models \neg\varphi[e]$. Je-li tedy φ (tedy i $\neg\varphi$) uzavřená, platí to nutně při všech ohodnoceních, čili $\mathcal{M} \models \neg\varphi$. □

—48—

Různé teorie a jejich modely

Teorie grup v jazyce $\{\cdot, e\}$ má axiomy:

$x \cdot (y \cdot z) = (x \cdot y) \cdot z$	(asociativita)
$x \cdot e = x \wedge x = e \cdot x$	(e je oboustranný neutrální prvek)
$(\exists y)(x \cdot y = e \wedge y \cdot x = e)$	(ke každému prvku existuje prvek oboustranně inverzní)

Z nich například již plyne:
$(\forall x)(x \cdot x = x \to x = e)$,
$(x \cdot y = e \wedge x \cdot z = e) \to z = y$, atp.

Příklady grup (tj. modelů teorie grup):

- celá, racionální, reálná, komplexní, atp. čísla s operacemi sčítání a nulou jakožto interpretací symbolu e
- nenulová racionální, reálná či komplexní čísla, příp. jen kladná racionální či kladná reálná s násobením a neutrálním prvkem 1
- množina permutací (bijekcí) na množině X (např. $X = \{1, \ldots, n\}$) s operací skládání zobrazení a identickým zobrazením jakožto neutrálním prvkem
- množina regulárních matic s operací násobení matic a jednotkovou maticí

Osmiprvková nekomutativní *grupa kvaternionů* $Q_8 = \{1, i, j, k, -1, -i, -j, -k\}$ (nalezená W.R.Hamiltonem). Jedná se o zobecnění grupy $\{1, -1, i, -i\}$, kde i je komplexní jednotka. V kvaternionech jsou komplexní jednotky 3. Grupová operace násobení je definována následující tabulkou a vztahem $-1 \cdot x = x \cdot (-1) = -x$ pro $x = i, j, k$.

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Základní rovnice pro kvaterniony: $i^2 = j^2 = k^2 = ijk = -1$.

Uplatňují se s výhodou všude tam, kde se popisuje rotace a orientace objektů v 3-dimenzionálním prostoru.

Teorie neostrého uspořádání $\{\leq\}$ má axiomy:

$x \leq x$ (reflexivita), $x \leq y \wedge y \leq x \to x = y$ (slabá antisymetrie),
$x \leq y \wedge y \leq z \to x \leq z$ (tranzitivita)

Lineární uspořádání: navíc axiom $x \leq y \vee y \leq x$

$x < y$ užíváme jako zkratku za formuli $(x \neq y \wedge x \leq y)$.

Diskrétní uspořádání: má navíc axiom

$$(\exists y)(x < y) \to (\exists y)(x < y \wedge \neg(\exists z)(x < z \wedge z < y)$$
$$\wedge(\exists y)(y < x) \to (\exists y)(y < x \wedge \neg(\exists z)(y < z \wedge z < x)$$

Husté uspořádání: má navíc axiom $x < y \to (\exists z)(x < z \wedge z < y)$

Jediné uspořádání, jež je současně husté a diskrétní je jednoprvkové.

Další často přidávané axiomy vyjadřují *„(ne)existuje největší/nejmenší prvek.“*

DeLO: Teorie hustého lineárního uspořádání bez nejmenšího a největšího prvku

DiLO: Teorie diskrétního lineárního uspořádání bez nejmenšího a největšího prvku

Definice: Teorie T v jazyce $\mathcal{L}$ je úplná, jestliže má model a pro každou formuli φ jazyka $\mathcal{L}$ platí buď $T \models \varphi$ nebo $T \models \neg\varphi$.

Jak DeLO tak DiLO jsou *úplné* teorie v jazyce $\{<\}$ (později si ukážeme proč).

Modelem DeLO jsou např. struktury $\langle \mathbb{Q}, < \rangle$ či $\langle \mathbb{R}, < \rangle$, modelem DiLO je např. $\langle \mathbb{Z}, < \rangle$.

Robinsonova aritmetika v jazyce $\mathcal{L}^{Ar} = \{0, S, +, \cdot, \leq\}$ s axiomy

- $0 \neq S(x)$
- $S(x) = S(y) \to x = y$
- $x + 0 = x$
- $x + S(y) = S(x + y)$
- $x \cdot 0 = 0$
- $x \cdot S(y) = x \cdot y + x$
- $x \neq 0 \to (\exists y)(x = S(y))$
- $x \leq y \leftrightarrow (\exists z)(z + x = y)$

Peanova aritmetika: přidává navíc nekonečnou množinu axiomů, tzv. schéma axiomů indukce. Pro každou formuli φ jazyka $\mathcal{L}^{Ar}$ přidáme axiom:

$$(\varphi(x/0) \wedge (\forall x)(\varphi \to \varphi(x/S(x)))) \to (\forall x)\varphi(x/S(x)).$$

Modelem Peanovy aritmetiky (tzv. *standardním modelem*) je $\mathbb{N}$ (při obvyklé interpretaci jazyka). Existují i jiné modely, tzv. nestandardní.

Teorie lze zadávat též implicitně, příkladem je třeba *teorie sentencí dané struktury*: každá struktura $\mathcal{M}$ určuje úplnou teorii

$$\mathrm{Thm}(\mathcal{M}) = \{\varphi\ ;\ \varphi \text{ je uzavřená a } \mathcal{M} \models \varphi\}$$

Říkáme, že struktury $\mathcal{M}$ a $\mathcal{N}$ jsou *elementárně ekvivalentní*, jestliže v nich platí stejné sentence, tj. $\mathrm{Thm}(\mathcal{M}) = \mathrm{Thm}(\mathcal{N})$. Značíme $\mathcal{M} \equiv \mathcal{N}$.

Z úplnosti DeLO např. ihned plyne $(\mathbb{Q}, \leq) \equiv (\mathbb{R}, \leq)$.

Ukážeme si později, že $(\mathbb{Q}, +) \equiv (\mathbb{R}, +)$.

Rozmyslete si, proč $(\mathbb{Q}, \cdot) \not\equiv (\mathbb{R}, \cdot)$ či $(\mathbb{Z}, +) \not\equiv (\mathbb{Q}, +)$

Vyjadřování v jazycích 1. řádu

Pro procvičení si zkuste formulemi jazyka 1. řádu zapsat různé vlastnosti prvků běžných matematických struktur, tj. pro danou vlastnost prvků nějaké konkrétní struktury $\mathcal{M}$ zkuste nalézt formuli φ daného jazyka tak, aby φ platila v $\mathcal{M}$ právě o prvcích s danou vlastností. Několik příkladů:

Uvažujme strukturu $\mathcal{N}$ tvořenou množinou přirozených čísel $\mathbb{N}$ a přirozenými interpretacemi jazyka aritmetiky $\mathcal{L}^{Ar} = \{0, S, +, \cdot, \leq\}$, případně jen určitého podjazyka např. $\{+, \cdot\}$, atp. Připomeňme, že S je operace následníka, interpretovaná funkcí $S^{\mathcal{N}} : n \mapsto n + 1, n \in \mathbb{N}$.

- *„x je číslo 2“* lze vyjádřit např. formulí $x = S(S(0))$, ale taktéž jen v jazyce $\{\leq\}$, jako

$$(\exists u)(\exists v)(u \leq v \wedge v \leq x \wedge u \neq v \wedge v \neq x \wedge (\forall w)(w \leq x \to (w = x \vee w = v \vee w = u))),$$

totéž jen v jazyce $\{+\}$ pomocí sčítání:

$$(\exists w)(x = w + w \wedge x \neq w \wedge (\forall y)(\forall z)(y + z = w \to w = y \vee w = z))$$

- *„x je sudé“* — $(\exists y)(x = y \cdot S(S(0)))$.
  Lze rovněž jen pomocí sčítání: $(\exists y)(x = y + y)$.
- *„x je liché“* — $\neg(\exists y)(x = y + y)$.
- *„x a y jsou nesoudělná“* —

$$(\forall u)(\forall v)(\forall w)(u \cdot v = x \wedge u \cdot w = y \to u = S(0)),$$

atp.

Je vhodné cvičení zkusit u těchto a podobných vlastností prozkoumat, které symboly jazyka jsou pro zachycení dané vlastnosti ve struktuře $\mathbb{N}$ nezbytné či naopak postačují.

—57—

Příklady s dalšími jazyky:

Jazyk teorie množin $\{\in\}$: Formule $\neg(\exists y)(y \in x)$ stejně jako třeba $(\forall y)(y \in x \to y \neq y)$ vyjadřují, že x je prázdná množina.

Jazyk čisté rovnosti (bez mimologických symbolů): formule $(\forall x)(\forall y)(x = y)$ je splněna právě v jednoprvkových strukturách. Jejími modely jsou tedy právě všechny jednoprvkové množiny. Totéž ovšem platí i o formuli $(\exists x)(\forall y)(x = y)$. Naopak formule $(\forall x)(\exists y)(x = y)$ platí v každé struktuře.

Podobně formule $(\exists x_1)(\exists x_2)(x_1 \neq x_2 \wedge (\forall y)(y = x_1 \vee y = x_2))$ je splněna právě ve 2-prvkových strukturách. Analogicky lze pro každé n sestavit formule φ_n resp. ψ_n vyjadřující vlastnosti struktury *„mít právě n prvků“* resp. *„mít aspoň n prvků“*, atp. (Zkuste si to!)

—58—

Možnost vyjádřit určitou vlastnost prvků struktury podstatně závisí na volbě jazyka (a interpretace).

Některé vlastnosti struktur v daném jazyce jednou formulí (případně konečně mnoha) vyjádřit nelze, např. *„mít nekonečně mnoho prvků“* nelze vyjádřit v jazyce čisté rovnosti; je k tomu potřeba nekonečná množina formulí $T = \{\psi_n\ ;\ n \in \mathbb{N}\}$.

Ne vždy to ovšem znamená, že to danou vlastnost nelze popsat jednou formulí v nějakém bohatším jazyce (např. jazyce uspořádání $\leq$, viz dále).

Některé vlastnosti struktur však není možno vyjádřit ani nekonečnou množinou formulí (dokonce v žádném jazyce 1. řádu): např. *„mít konečně mnoho prvků“* (pochopitelně aniž bychom nějak konkrétně shora omezili jejich počet). Platí totiž: je-li T množina formulí, která má libovolně velké konečné modely, má T i nekonečný model (vyplývá z věty o kompaktnosti v predikátové logice).

—59—

Nahrazování (substituce) Slovo, které vznikne ze slova (např. termu či formule) σ nahrazením všech výskytů podslov $\alpha_1, \ldots, \alpha_n$ slovy $\beta_1, \ldots, \beta_n$, značíme

$$\sigma(\alpha_1/\beta_1, \ldots, \alpha_n/\beta_n).$$

Věta (*o nahrazení*): *a) Je-li φ tautologie výrokového počtu nad množinou výrokových proměnných $\mathcal{P} = \{A_1, \ldots, A_n\}$ a $\theta_1, \ldots, \theta_n$ jsou libovolné formule jazyka $\mathcal{L}$, pak $\varphi(A_1/\theta_1, \ldots, A_n/\theta_n)$ je logicky platnou formulí jazyka $\mathcal{L}$.*

b) Je-li φ je formule, $\theta_1, \ldots, \theta_n$ nějaké její podformule, a $\theta'_1, \ldots, \theta'_n$ formule takové, že pro každé $1 \leq i \leq n$ je $\models \theta_i \leftrightarrow \theta'_i$, pak

$$\models \varphi \leftrightarrow \varphi(\theta_1/\theta'_1, \ldots, \theta_n/\theta'_n)$$

Důkaz indukcí dle složitosti formule, část a) dále porovnáním definic pravdivosti výrokového a predikátového počtu.

—60—

I v predikátové logice tedy můžeme formule *„upravovat“* podobně, jako se upravují aritmetické výrazy, tak, že jednotlivé podformule nahrazujeme formulemi s nimi ekvivalentními, přičemž takovou úpravou získáme formuli logicky ekvivalentní s původní formulí.

Uvedená věta platí pro libovolné formule.

Na **uzavřené** formule, jejichž pravdivost závisí pouze na zvolené interpretaci a nezávisí již na ohodnocení individuálních proměnných, se navíc vztahují všechny obecné zákony tautologické odvoditelnosti zkoumané ve výrokovém počtu, např. věta o dedukci.

Podmínka substituovatelnosti — term t je *substituovatelný* do formule φ za proměnnou x, jestliže se po substituci nestane žádná proměnná vyskytující se v t vázanou. Jinými slovy, žádný výskyt proměnné x ve formuli φ se nenachází v podformuli tvaru $(\forall y)\psi$ nebo $(\exists y)\psi$ takové, že y má výskyt v termu t.

Příklad: Term $x + 1$ není substituovatelný za y do $(\exists x)(x = y)$.

Příklad (*princip specifikace*): Je-li φ formule a term t je substituovatelný do φ za x, pak $\models (\forall x)\varphi \to \varphi(x/t)$.

Napíšeme-li v dalším $\varphi(x/t)$, budeme vždy předpokládat splnění podmínky substituovatelnosti, tj. že term t je substituovatelný do φ za x.

Formuli $\varphi(x_1/t_1, \ldots, x_n/t_n)$ vzniklé substitucí termů $t_1, \ldots, t_n$ za (navzájem různé) proměnné $x_1, \ldots, x_n$ se někdy říká *instance* formule φ. Instance vyjadřuje nějaký zvláštní případ tvrzení formule.

Jak zajistit podmínku substituovatelnosti?

Je-li to potřeba, můžeme vhodně přejmenovat vázané proměnné (získáme tzv. variantu).

Definice: *Bezprostřední variantou* formule $(\forall x)\psi$ je každá formule tvaru $(\forall y)\psi(x/y)$, kde proměnná y nemá v ψ žádný výskyt.
Bezprostřední variantou formule $(\exists x)\psi$ je každá formule tvaru $(\exists y)\psi(x/y)$, kde proměnná y nemá v ψ žádný výskyt.
Variantou formule φ je každá formule, jež vznikne z φ konečným počtem nahrazení podformulí tvaru $(\forall x)\psi$ či $(\exists x)\psi$ jejich bezprostředními variantami.

Věta (*o variantách*): *Je-li φ' variantou φ, pak $\models \varphi' \leftrightarrow \varphi$.*

Základní prostředky dedukce v predikátovém počtu

- věta o tautologiích
- věty výrokového počtu aplikované na uzavřené formule predikátového počtu, např. věta o důkazu sporem, o rozboru případů, zejména však
- věta o dedukci: Je-li φ uzavřená, pak $T \models \varphi \to \psi$ právě když $T, \varphi \models \psi$
- Modus ponens: $\varphi, \varphi \to \psi \models \psi$
- generalizace: $\varphi \models (\forall x)\varphi$
- specifikace: $\models (\forall x)\varphi \to \varphi(x/t)$ a speciálně $\models (\forall x)\varphi \to \varphi$
- a duálně: $\models \varphi(x/t) \to (\exists x)\varphi$

Věta (*o dualitě*): *Nechť formule φ neobsahuje jiné logické spojky než $\neg$, $\vee$ a $\wedge$. Pak $\models \neg\varphi \leftrightarrow \varphi^d$, kde φ^d je tzv. duální formule k φ, získaná z φ nahrazením atomických formulí jejich negacemi, nahrazením každého kvantifikátoru či spojky $\square$ symbolem $\square^d$, kde $\exists^d = \forall$, $\forall^d = \exists$, $\wedge^d = \vee$, $\vee^d = \wedge$ a $\neg^d = \neg$.*

Podmínka uzavřenosti formule ve větě o dedukci je velmi podstatná (pro implikaci zprava doleva, opačná implikace plyne z pravidla Modus ponens, jež platí zcela obecně).

V predikátové logice již musíme důsledně rozlišovat $\to$ a $\models$.

Příklad: Pravidlo generalizace nelze formulovat jako implikaci $\varphi \to (\forall x)\varphi$. Např. formule $x = 1 \to (\forall x)x = 1$ totiž neplatí ve struktuře $\langle \mathbb{N}, 1\rangle$ přirozených čísel při ohodnocení $e : x \mapsto 1$.

Příklad (*Záměnnost stejných kvantifikátorů*): Jsou-li x, y jediné volné proměnné ve formuli φ, pak $\models (\forall x)(\forall y)\varphi \to (\forall y)(\forall x)\varphi$.

$(\forall x)(\forall y)\varphi$ je uzavřená, dle věty o dedukci stačí tedy dokázat:

$$(\forall x)(\forall y)\varphi \models (\forall y)(\forall x)\varphi \qquad (1)$$

Platí:

$(\forall x)(\forall y)\varphi \models (\forall y)\varphi$	specifikace
$(\forall y)\varphi \models \varphi$	specifikace
$\varphi \models (\forall x)\varphi$	generalizace
$(\forall x)\varphi \models (\forall y)(\forall x)\varphi$	generalizace

(3) vyplývá z předchozího a tranzitivity relace $\models$.

Příklad: Jsou-li φ a $(\forall x)\psi$ uzavřené, pak

$$\models (\forall x)(\varphi \to \psi) \to (\varphi \to (\forall x)\psi)$$

Pomocí věty o dedukci úlohu převedeme na

$$(\forall x)(\varphi \to \psi) \models (\varphi \to (\forall x)\psi)$$

a odtud dále na

$$(\forall x)(\varphi \to \psi), \varphi \models (\forall x)\psi$$

Postupně dostáváme:

$(\forall x)(\varphi \to \psi), \varphi \models \varphi \to \psi$	specifikace
$\varphi \to \psi, \varphi \models \psi$	Modus ponens
$\psi \models (\forall x)\psi$	generalizace

Uvedené implikace ovšem platí i pro formule, které nejsou uzavřené. Předpoklad uzavřenosti nám pouze umožnil aplikovat větu o dedukci. Řešení nabízí věta o konstantách, zachycující význam postupu který používáme v matematickém důkazu, když říkáme *„zvolme x libovolně, avšak pevně...“*

Věta (*o konstantách*): *Nechť $c_1, \ldots, c_n$ jsou konstanty, které se nevyskytují ve formuli φ ani v žádné z formulí z množiny T. Nechť $T \models \varphi(x_1/c_1, \ldots x_n/c_n)$. Pak $T \models \varphi$.*

Smysl: konstanty, o nichž nic nepředpokládáme, se chovají jako volné proměnné.

Použití: na začátku důkazu nahradíme volné proměnné, jejichž přítomnost brání užití věty o dedukci, novými konstantami. Tím se formule stane uzavřenou. Na konci důkazu konstanty nahradíme zpátky proměnnými.

Příklad: $\models (\forall x)(\forall y)\varphi \to (\forall y)(\forall x)\varphi$, tentokrát bez omezení množství volných proměnných ve φ.

Nechť všechny volné proměnné formule φ jsou mezi $x, y, x_1, \ldots, x_n$ a nechť $c_1, \ldots, c_n$ jsou konstanty nevyskytující se v φ. Z toho, co jsme ukázali dříve, plyne, že uvedená implikace platí, dosadíme-li za formuli φ formuli $\varphi(x_1/c_1, \ldots, x_n/c_n)$, neboli

$$\models (\forall x)(\forall y)\varphi(x_1/c_1, \ldots, x_n/c_n) \to (\forall y)(\forall x)\varphi(x_1/c_1, \ldots, x_n/c_n)$$

Z věty o konstantách ihned dostáváme, že to platí i pro samotné φ.

Příklad: $\models (\forall x)(\varphi \to \psi) \to (\varphi \to (\forall x)\psi)$, za předpokladu, že x nemá ve formuli φ volný výskyt.

Zcela analogicky.

Důkaz věty o konstantách.

Nechť $T \models \varphi(x_1/c_1, \ldots, x_n/c_n)$. Máme ukázat, že $T \models \varphi$, čili, že pro libovolnou strukturu $\mathcal{M}$ splňující $\mathcal{M} \models T$ a libovolné ohodnocení e v $\mathcal{M}$ platí $\mathcal{M} \models \varphi[e]$. Zvolme $\mathcal{M}$ a e libovolně, avšak pevně.

Na základě relační struktury $\mathcal{M}$ definujme relační strukturu $\mathcal{N}$, jež je totožná s $\mathcal{M}$, liší se pouze realizacemi konstant $c_1, \ldots, c_n$, pro něž platí $c_i^N = e(x_i)$, $1 \leq i \leq n$. Speciálně, neobsahuje-li formule ψ konstanty $c_1, \ldots, c_n$, je $\mathcal{M} \models \psi$ právě když $\mathcal{N} \models \psi$.

Jelikož formule z množiny T neobsahují konstanty $c_1, \ldots, c_n$, platí $\mathcal{N} \models T$, tudíž $\mathcal{N} \models \varphi(x_1/c_1, \ldots, x_n/c_n)$ dle předpokladu. Pak ovšem $\mathcal{N} \models \varphi[e]$, neboť $c^N = e(x_i)$. Ani φ však neobsahuje uvedené konstanty, tudíž $\mathcal{M} \models \varphi[e]$, což bylo dokázati. □

Aby se to nepletlo, dokončíme repertoár tvrzení o pravdivosti tzv. větou o *zavedení konstant*. Dokazuje se obdobně, jako věta o konstantách.

Věta (*o zavedení konstant*): *Nechť formule z množiny T ani formule φ, ψ neobsahují konstanty $c_1, \ldots, c_n$ a nechť φ nemá jiné volné proměnné než $x_1, \ldots, x_n$. Nechť dále*

$$T \models (\exists x_1) \ldots (\exists x_n)\varphi. \tag{2}$$

Jestliže $T, \varphi(x_1/c_1, \ldots, x_n/c_n) \models \psi$, pak $T \models \psi$.

Věta zachycuje běžně užívaný obrat: *„... existují tedy (čísla) x, y, taková že ... Označme je a a b. Pak ...“*

Použití: odvodíme-li existenční formuli tvaru (4), rozšíříme jazyk o nové konstanty a k předpokladům přidáme formuli $\varphi(x_1/c_1, \ldots, x_n/c_n)$. Vyvodíme-li nyní nějaké ψ, jež neobsahuje nové konstanty, vyplývá toto ψ již z původní množiny předpokladů.

Příklad: Odvodíme: $\models (\exists x)(\forall y)\varphi \to (\forall y)(\exists x)\varphi$

Můžeme předpokládat, že φ neobsahuje jiné volné proměnné než x, y. V opačném případě je po zbytek důkazu nahradíme novými konstantami a v závěru aplikujeme větu o konstantách.

Lze tudíž použít větu o dedukci a dokazovat pouze

$$(\exists x)(\forall y)\varphi \models (\forall y)(\exists x)\varphi$$

Buď c nová konstanta. Pak

- $(\forall y)\varphi(x/c) \models \varphi(x/c)$ specifikace
- $\ldots \models (\exists x)\varphi$ duální specifikace
- $\ldots \models (\forall y)(\exists x)\varphi$ generalizace

Odtud již dokazovaný vztah plyne dle věty o zavedení konstant (roli množiny T zde hraje jediná formule $(\exists x)(\forall y)\varphi$).

Příklad: Pozor, opačně to neplatí: $\not\models (\forall y)(\exists x)\varphi \to (\exists x)(\forall y)\varphi$

Zvolme totiž za φ např. $x = y$. Pak uvedená implikace neplatí v žádné struktuře s alespoň dvěma prvky. Je zajímavé si též všimnout, kde selže pokus o důkaz vedený stejným způsobem jako pro opačnou implikaci. Dokazujeme $(\forall y)(\exists x)\varphi \models (\exists x)(\forall y)\varphi$. Ze specifikace plyne $(\forall y)(\exists x)\varphi \models (\exists x)\varphi$. Toto x označíme konstantou c a pokračujeme:

- $\varphi(x/c) \models (\forall y)\varphi(x/c)$ generalizace
- $(\forall y)\varphi(x/c) \models (\exists x)(\forall y)\varphi$ duální specifikace

Vyplývá z dokázaného dle věty o zavedení konstant vztah

$$(\forall y)(\exists x)\varphi \models (\exists x)(\forall y)\varphi?$$

Ne, protože není splněn její předpoklad: formule φ může obsahovat kromě x ještě volné y! Jinými slovy, udělali jsme chybu v tom, že c nebyla *„konstanta“*, závisela totiž na y.

Prenexní tvar formule

Formule je v *prenexním tvaru*, je-li tvaru $(Q_1x_1)(Q_2x_2)\dots(Q_nx_n)\psi$, kde ψ je otevřená formule a každé Q_i je symbol $\forall$ nebo $\exists$, $(n \geq 0)$.

Buďte φ, θ formule a x proměnná, která nemá volný výskyt v θ. Pak jsou všechny následující (tzv. *prenexní*) formule logicky platné:

$$\neg(\forall x)\varphi \leftrightarrow (\exists x)\neg\varphi \qquad \neg(\exists x)\varphi \leftrightarrow (\forall x)\neg\varphi$$
$$(\theta \to (\forall x)\varphi) \leftrightarrow (\forall x)(\theta \to \varphi) \qquad (\theta \to (\exists x)\varphi) \leftrightarrow (\exists x)(\theta \to \varphi)$$
$$((\exists x)\varphi \to \theta) \leftrightarrow (\forall x)(\varphi \to \theta) \qquad ((\forall x)\varphi \to \theta) \leftrightarrow (\exists x)(\varphi \to \theta)$$
$$(\theta \vee (\forall x)\varphi) \leftrightarrow (\forall x)(\theta \vee \varphi) \qquad (\theta \vee (\exists x)\varphi) \leftrightarrow (\exists x)(\theta \vee \varphi)$$
$$(\theta \wedge (\forall x)\varphi) \leftrightarrow (\forall x)(\theta \wedge \varphi) \qquad (\theta \wedge (\exists x)\varphi) \leftrightarrow (\exists x)(\theta \wedge \varphi)$$

Věta (*o prenexním tvaru*): *Každá formule je logicky ekvivalentní s nějakou formulí v prenexním tvaru.*

Příklad: Převedeme následující formuli do prenexního tvaru:

$$(\forall x)(P(x) \to (\exists y)Q(x,y)) \vee \neg(\forall x)P(x)$$

Postupujeme *„zevnitř ven“*:

1. $(P(x) \to (\exists y)Q(x,y)) \leftrightarrow (\exists y)(P(x) \to Q(x,y))$, tedy
   $(\forall x)(P(x) \to (\exists y)Q(x,y)) \leftrightarrow (\forall x)(\exists y)(P(x) \to Q(x,y))$
2. $\neg(\forall x)P(x) \leftrightarrow (\exists x)\neg P(x)$
3. $(\forall x)(\exists y)(P(x) \to Q(x,y)) \vee (\forall x)\neg P(x) \leftrightarrow$
   $(\forall x)(\exists y)((P(x) \to Q(x,y)) \vee (\forall x)\neg P(x))$
4. $((P(\underline{x}) \to Q(\underline{x},y)) \vee (\forall x)\neg P(x)) \leftrightarrow$
   $((P(x) \to Q(x,y)) \vee (\forall w)\neg P(w)) \leftrightarrow$
   $(\forall w)((P(x) \to Q(x,y)) \vee \neg P(w))$
5. $(\forall x)(P(x) \to (\exists y)Q(x,y)) \vee \neg(\forall x)P(x) \leftrightarrow$
   $(\forall x)(\exists y)(\forall w)((P(x) \to Q(x,y)) \vee \neg P(w))$

Příklad: Víme, že obecně neplatí

$$\not\models (\forall y)(\exists x)\varphi \to (\exists x)(\forall y)\varphi.$$

Je-li však φ tvaru $\theta(y) \to \chi(x)$, kde $\theta(y)$ neobsahuje x volně a $\chi(x)$ neobsahuje y volně, implikace platí. Z prenexních formulí totiž plyne:

$$(\forall y)(\exists x)(\theta(y) \to \chi(x)) \leftrightarrow$$
$$(\forall y)(\theta(y) \to (\exists x)\chi(x)) \leftrightarrow$$
$$((\exists y)\theta(y) \to (\exists x)\chi(x)) \leftrightarrow$$
$$(\exists x)((\exists y)\theta(y) \to \chi(x)) \leftrightarrow$$
$$(\exists x)(\forall y)(\theta(y) \to \chi(x))$$

Formální metoda pro predikátový počet
Hilbertovský kalkulus

Stručně popíšeme formální systém pro logiku 1. řádu navržený Davidem Hilbertem. (Existují i jiné formální systémy, např. Gentzenovský kalkulus založený na pojmu sekventu.)

Podobně jako u výrokového počtu, vyjdeme z několika formulí (*axiomů*) z nichž vyvozujeme další formule prostřednictvím formálních důkazů na základě axiomů a odvozovacích pravidel Modus Ponens a generalizace.

Užijeme redukovaného jazyka obsahujícího ze spojek pouze $\neg$ a $\to$ a jediný kvantifikátor $\forall$.

Napíšeme-li formuli $(\exists x)\varphi$, chápeme ji jako zkratku za $\neg(\forall x)\neg\varphi$.

Axiomy predikátové logiky

Zavádíme je jako schémata axiomů.

Každá z následujících formulí je axiomem predikátové logiky při libovolné volbě formulí φ, ψ, θ a termu t (u P1, P2 musí φ a t vyhovovat uvedené podmínce):

V1) $\varphi \to (\psi \to \varphi)$

V2) $(\varphi \to (\psi \to \theta)) \to ((\varphi \to \psi) \to (\varphi \to \theta))$

V3) $(\neg\psi \to \neg\varphi) \to (\varphi \to \psi)$

P1) $(\forall x)(\varphi \to \psi) \to (\varphi \to (\forall x)\psi)$,
neobsahuje-li φ proměnnou x volně

P2) $(\forall x)\varphi \to \varphi(x/t)$,
je-li t je substituovatelný do φ za x

Axiomy rovnosti

V logice s rovností přidáváme k uvedeným axiomům ještě následující schémata axiomů charakterizující naše chápání identity:

R1) $x = x$

R2) $(x_1 = y_1 \to (x_2 = y_2 \to \ldots (x_n = y_n \to$
$\to F(x_1, \ldots, x_n) = F(y_1, \ldots, y_n)) \ldots))$,
kde F je libovolný funkční symbol četnosti $n \geq 0$ a $x_1, \ldots, x_n$, $y_1, \ldots, y_n$ ne nutně různé proměnné,

R3) $(x_1 = y_1 \to (x_2 = y_2 \to \ldots (x_k = y_k \to$
$\to (P(x_1, \ldots, x_k) \to P(y_1, \ldots, y_k))) \ldots))$,
kde P je libovolný predikátový symbol (včetně predikátu $=$) četnosti $k \geq 1$ a $x_1, \ldots, x_k, y_1, \ldots, y_k$ ne nutně různé proměnné

Odvozovací pravidla

Na rozdíl od výrokového počtu jsou dvě.

Modus ponens:

$$\frac{\varphi,\ (\varphi \to \psi)}{\psi}$$

Pravidlo generalizace:

$$\frac{\varphi}{(\forall x)\varphi}$$

Důkaz v teorii

Je-li T teorie 1. řádu, je *důkazem formule φ v teorii T* konečná posloupnost formulí $\varphi_1, \ldots, \varphi_n$ jazyka teorie T taková, že $\varphi_n = \varphi$ a pro každé $i \in \{1, \ldots, n\}$ platí

- φ_i je axiom logiky (případně rovnosti), nebo
- $\varphi_i \in T$ (tj. φ_i je axiom teorie T), nebo
- φ_i plyne z $\varphi_1, \ldots, \varphi_i$ pomocí některého odvozovacího pravidla

Existuje-li důkaz formule φ v T, říkáme, že je *dokazatelná v T*, případně že je *větou* T a píšeme $T \vdash \varphi$.

φ je *dokazatelná v logice*, má-li důkaz v teorii s prázdnou množinou axiomů (v libovolném jazyce). Píšeme $\vdash \varphi$.

Teorie T je *sporná*, pokud pro nějakou formuli φ platí $T \vdash \varphi$ a současně $T \vdash \neg\varphi$. Jinak je T *bezesporná*, neboli *konzistentní*.

Ve sporné teorii je dokazatelná libovolná formule
(viz následující příklad $\vdash \neg\varphi \to (\varphi \to \theta)$ dokazatelný už ve výrokovém počtu).

Formule φ jazyka teorie T je:

- *vyvratitelná* v T, pokud $T \vdash \neg\varphi$,
- *nezávislá* na T, není-li dokazatelná ani vyvratitelná

Teorie T je *úplná*, je-li bezesporná a každá formule jazyka T je buď dokazatelná nebo vyvratitelná v T.

Příklad: $\vdash \neg\varphi \to (\varphi \to \theta)$

---

1. $\vdash \neg\varphi \to (\neg\theta \to \neg\varphi)$ — instance V1,
2. $\neg\varphi \vdash (\neg\theta \to \neg\varphi)$ — věta o dedukci (VD)
3. $\neg\varphi \vdash (\neg\theta \to \neg\varphi) \to (\varphi \to \theta)$ — instance V3,
4. $\neg\varphi \vdash (\varphi \to \theta)$ — MP
5. $\vdash \neg\varphi \to (\varphi \to \theta)$ — VD

Z právě dokázaného speciálně plyne $\vdash \neg\varphi \to (\varphi \to \bot)$ odkud lze pomocí VD odvodit **větu o důkazu sporem** pro $\vdash$:

$$T \vdash \varphi \quad \text{právě když} \quad T, \neg\varphi \vdash \bot.$$

Pro Hilbertovský kalkulus, tj. pro dokazatelnost ($\vdash$), platí podobná základní pravidla dedukce, jako pro pravdivost ($\models$), zejména věta o dedukci pro uzavřené formule, věta o důkazu sporem a věta o konstantách (v jejichž znění nahradíme symbol $\models$ symbolem $\vdash$).

(Větu o dedukci, případně skrytě i větu o konstantách, jsme užili už v předchozím příkladu).

Ověření platnosti těchto vět pro dokazatelnost se věnovat nebudeme. Poznamenejme jen, že se při něm pochopitelně pracuje s definicí důkazu (nikoli modelu jako u $\models$).

Např. u věty o dedukci *„$\varphi \vdash \psi$ právě když $\vdash \varphi \to \psi$“* jde o to, přepracovat existující důkaz ψ z axiomu φ na důkaz požadované implikace v prázdné teorii.

Příklad: Dokážeme symetrii rovnosti: $\vdash x = y \to y = x$. Dle věty o konstantách převedeme úlohu na $\vdash c = d \to d = c$, kde c, d jsou konstanty.

Formule $x = y \to (x = x \to (x = x \to y = x))$ je instance axiomu rovnosti R3, kde roli predikátu P hraje $=$ a roli proměnných x_1, x_2, y_1, y_2 hrají po řadě proměnné x, x, y, x. Platí tudíž:

$\vdash (\forall x)(\forall y)(x = y \to (x = x \to (x = x \to y = x)))$ (gener.)
$\vdash (c = d \to (c = c \to (c = c \to d = c)))$ (axiom P2 a pravidlo MP)
$\vdash c = c$ (axiom R1, dále P2 a pravidlo MP)
$c = d \vdash d = c$ (z předchozího 3x MP)
$\vdash c = d \to d = c$ (věta o dedukci)
$\vdash x = y \to y = x$ (věta o konstantách)

Zákon identity

Z axiomů rovnosti dále plyne její tranzitivita:

$$x = y \to (y = z \to x = z)$$

a zákon identity:

$$(t_1 = s_1 \to (t_2 = s_2 \to \ldots (t_n = s_n \to \\ \to (\varphi(x_1/t_1, \ldots, x_n/t_n) \to \varphi(x_1/s_1, \ldots, x_n/s_n)) \ldots))$$

kde φ je libovolná formule a termy $t_1, \ldots, t_n$ resp. $s_1, \ldots, s_n$ jsou substituovatelné do φ za $x_1, \ldots, x_n$.

Klíčovou roli hraje následující věta, jež je analogií Postovy věty z výrokového počtu.

Věta (*o úplnosti a bezespornosti*):

Nechť T je teorie a φ formule jejího jazyka. Pak:

1. *T je bezesporná právě když má model.*
2. *$T \vdash \varphi$ právě když $T \models \varphi$.*

Důkaz je technicky složitý, nám bude stačit vysvětlit si jeho princip.

Princip důkazu

Implikaci $\Rightarrow$ bodu 2. lze ověřit poměrně snadno: každý axiom (logiky nebo T) platí v každém modelu T a odvozovací pravidla modus ponens a generalizace pravdivost neporušují. Dokazatelná tvrzení jsou tedy pravdivá.

Implikace $\Leftarrow$ bodu 1. plyne ihned z 2. $\Rightarrow$.

Implikace $\Leftarrow$ bodu 2. plyne z 1. $\Rightarrow$ dle věty o důkazu sporem.

Zbývá **klíčová implikace: *bezesporná teorie má model***.

Pro danou bezespornou teorii T v jazyce $\mathcal{L}$ musíme sestrojit její model. Trik: model sestrojíme přímo z (rozšířeného) jazyka teorie T.

Jazyk postupně rozšíříme tak, aby byl uzavřený na tzv. henkinovské konstanty a současně teorii T přidáním vhodných axiomů zúplníme...

Příprava

A) *Henkinovské rozšíření* teorie T v jazyce $\mathcal{L}$ získáme takto:

pro každou formuli φ jazyka $\mathcal{L}$ s jedinou volnou proměnnou x přidáme do jazyka novou (tzv. *henkinovskou*) konstantu c_φ a dále přidáme nový axiom $(\exists x)\varphi \to \varphi(x/c_\varphi)$.

Takto zbohacenou teorii a jazyk označme T^H a $\mathcal{L}^H$. Je-li T bezesporná, je taková i T^H (plyne z věty o zavedení konstant pro dokazatelnost).

B) *Zúplnění bezesporné teorie* T je teorie $\overline{T}$ taková, že $T \subseteq \overline{T}$ a pro každou sentenci φ jazyka $\mathcal{L}$ je buď $\varphi \in T$, nebo $\neg\varphi \in T$. Získáme je takto: všechny formule jazyka $\mathcal{L}$ seřadíme do posloupnosti $\{\varphi_n\}_{n\in\mathbb{N}}$ (aby šlo všechny formule očíslovat prvky $\mathbb{N}$, musí jít takto očíslovat množina symbolů jazyka $\mathcal{L}$. Neboli, množina symbolů jazyka $\mathcal{L}$ musí být konečná nebo „spočetná“. Pro nespočetný jazyk lze postupovat velmi podobně, formule pak indexujeme prvky nějakého *„transfinitního ordinálního čísla“*. K těmto pojmům se vrátíme v teorii množin.) Dále vytvoříme posloupnost teorií $\{T_n\}_{n\in\mathbb{N}}$ takto:

1. $T_0 = T$,
2. $T_{n+1} = \begin{cases} T_n \cup \{\varphi_n\}, & \text{je-li } T_n \cup \{\varphi_n\} \text{ bezesporná,} \\ T_n \cup \{\neg\varphi_n\}, & \text{jinak.} \end{cases}$

Pak $\overline{T} = \bigcup_{n\in\mathbb{N}} T_n$ je (bezesporné) úplné rozšíření teorie T.

C) Buď nyní T bezesporná teorie v jazyce $\mathcal{L}$. Teorii $T' = \bigcup_{n\in\mathbb{N}} T^{(n)}$ v jazyce $L' = \bigcup_{n\in\mathbb{N}} L^{(n)}$ sestrojíme takto:

1. $T^{(0)} = T$, $\mathcal{L}^{(0)} = \mathcal{L}$,
2. $T^{(n+1)} = \overline{(T^{(n)})^H}$, $\mathcal{L}^{(n+1)} = (\mathcal{L}^{(n)})^H$.

Výsledkem je úplná, *henkinovská* teorie, tj. taková, že pro každou formuli φ jazyka $\mathcal{L}'$ s jedinou volnou proměnnou x existuje konstanta c_φ jazyka $\mathcal{L}'$ tak, že platí $T' \vdash (\exists x)\varphi \to \varphi(x/c_\varphi)$. Volně řečeno, vše co existuje dokazatelně v T'), je označeno nějakou henkinovskou konstantou.

V následujícím již na základě teorie T' a množiny C jejích henkinovských konstant popíšeme konstrukci tzv. *kanonické struktury* $\mathcal{M}$ pro teorii T.

1. Univerzum M struktury $\mathcal{M}$ je množina $M = \{[t] \,;\, t \in C\}$, kde C je množina konstantních termů jazyka $\mathcal{L}'$ a $[t] = t$ pro logiku bez rovnosti resp. $[t] = \{t' \in C \,;\, T' \vdash t' = t\}$ pro logiku s rovností.

2. Predikátový symbol P jazyka $\mathcal{L}$ četnosti $n \geq 0$ interpretujeme relací $P^M = \{\langle [t_1], \ldots, [t_n]\rangle \,;\, [t_1], \ldots, [t_n] \in C \text{ a } T \vdash P(t_1 \ldots t_n)\}$.

3. Funkční symbol F jazyka $\mathcal{L}$ četnosti $n \geq 0$ interpretujeme funkcí $F^M : M^n \to M$, kde klademe $F^M([t_1], \ldots, [t_n]) = [F(t_1, \ldots, t_n)]$.

Korektnost těchto definic pro logiku s rovností vyplývá z axiomů rovnosti.

Poměrně snadno (indukcí podle počtu spojek a kvantifikátorů) se nyní ověří, že pro každou formuli φ jazyka $\mathcal{L}(T')$ platí $M \models \varphi$ právě když $\varphi \in T'$. Speciálně $\mathcal{M} \models T$. Získali jsme tedy model bezesporné teorie T. Z důkazu navíc plyne, že bezesporná teorie ve **spočetném** jazyce má **spočetný** model.

Poznámka: Výše uvedená metoda nalezení úplného rozšíření $\overline{T}$ bezesporné teorie T slouží v zásadě pouze jako teoretický prostředek. Problematický je krok:

$$T_{n+1} = \begin{cases} T_n \cup \{\varphi_n\}, & \text{je-li } T_n \cup \{\varphi_n\} \text{ bezesporná,} \\ T_n \cup \{\neg\varphi_n\}, & \text{jinak.} \end{cases}$$

S výjimkou některých *„krotkých“* teorií bychom v praxi měli velký problém s rozšířením T byť i o jedinou složitější formuli.

Lze dokázat, že u některých teorií (například už u Robinsonovy aritmetiky) nedokáže v konečném čase bezespornost rozhodnout ani žádný algoritmus běžící na ideálním počítači s neomezeným množstvím paměti (Turingově stroji).

Následující věta je klíčovým prostředkem při zkoumání různých teorií.

Věta (*o kompaktnosti*): *Teorie T má model právě když každá konečná podteorie $S \subseteq T$ má model.*

Důkaz. Implikace zleva doprava je zřejmá (model T je jistě modelem libovolné konečné $S \subseteq T$).

Naopak, využijeme větu o úplnosti a bezespornosti. Stačí ukázat, že T je bezesporná. Kdyby nebyla, existoval by důkaz sporu v T. Ten by využíval jen nějakou konečnou mnoho axiomů S teorie T. Pak by ovšem S byla konečná **sporná** podteorie T, což není možné, neboť S má dle předpokladu model. □

Příklad: Má-li T libovolně velké konečné modely, má nekonečný model (vlastnost modelu *„být konečný“* tedy nejde vyjádřit žádnou množinou axiomů).

Důkaz. Nechť $C = \{c_n \ ; \ n \in \mathbb{N}\}$ je množina nových konstant. Teorii T rozšíříme o axiomy $\{c_n \neq c_m \ ; \ n, m \in \mathbb{N}, n \neq m\}$. Výsledná teorie T' má model dle věty o kompaktnosti, neboť je-li $S \subseteq T'$ její konečná podteorie, obsahují axiomy S jen konečně mnoho konstant c_n. Dostatečně velký konečný model $\mathcal{M}$ teorie T lze tedy rozšířit o interpretace konstant c_n tak, aby $\mathcal{M} \models S$.

T' má tedy model. Ten je nutně nekonečný, neboť interpretuje nekonečnou množinu konstant C a to nevyhnutelně navzájem různými prvky. Každý model T' je však současně modelem teorie T. □

Příklad: Z jiného soudku.

Co se stane, rozšíříme-li teorii $\mathrm{Thm}(\langle \mathbb{N}, 0, S, +, \cdot, \leq \rangle)$ (tzv. pravdivá aritmetika) do teorie T přidáním nové konstanty c a axiomů $\{\underline{n} < c \ ; \ n \in \mathbb{N}\}$, kde $\underline{n}$ je term $\underbrace{S \ldots S}_{n\text{-krát}}(0)$ (takzvaný n-tý numerál, vyjadřující v jazyce aritmetiky přirozené číslo n)?

Z věty o kompaktnosti plyne, že T je bezesporná (jelikož každá konečná podmnožina má za model strukturu $\mathbb{N}$, v níž c interpretujeme dostatečně velkým přirozeným číslem).

Modely T jsou tzv. *nestandardní modely* (pravdivé) aritmetiky. Platí v nich všechny pravdivé věty o přirozených číslech, obsahují však prvky větší, než je každé konkrétní přirozené číslo, tzv. *nestandardní prvky*. Tyto prvky nelze od ostatních prvků *„zevnitř“*, tj. prostředky jazyka 1. řádu, odlišit.

Podobný trik má velmi praktické využití v tzv. nestandardním přístupu k matematické analýze, při popisu pojmů jako je spojitost funkce a dalších. Lze totiž takto v matematice korektně zavést nekonečně velké a nekonečně malé veličiny, něco, s čím běžně intuitivně pracovali matematici jako Newton, Leibniz, či Euler, co však pozdější generace odmítli, nahradili neohrabaným kalkulem dnešní matematické analýzy, aby to bylo na skloknu 60. let znovu přivedeno na svět A. Robinsonem (a nezávisle P. Vopěnkou).

Izomorfizmus modelů

Relační struktury $\mathcal{M}$ a $\mathcal{N}$ pro jazyk $\mathcal{L}$ jsou *izomorfní*, existuje-li vzájemně jednoznačné zobrazení $h : M \to N$ takové, že pro každé $a_1, \ldots, a_n \in M, n \geq 0$ platí:

1. pro každý funkční symbol F jazyka $\mathcal{L}$ je
$$h(F^M(a_1, \ldots, a_n)) = F^N(h(a_1), \ldots, h(a_n)),$$
2. pro každý predikátový symbol P jazyka $\mathcal{L}$ je $\langle a_1, \ldots, a_n \rangle \in P^M$ právě když $\langle h(a_1), \ldots, h(a_n) \rangle \in P^N$.

Existuje-li izomorfismus struktur $\mathcal{M}$ a $\mathcal{N}$, říkáme, že $\mathcal{M}$ a $\mathcal{N}$ jsou izomorfní, značíme $\mathcal{M} \cong \mathcal{N}$. Zřejmě platí: je-li h izomorfismus struktur $\mathcal{M}$ a $\mathcal{N}$, je h^{-1} izomorfismus struktur $\mathcal{N}$ a $\mathcal{M}$.

Izomorfní struktury jsou de facto totožné, liší se pouze volbou množiny individuí.

Věta: *Je-li h izomorfismus struktur $\mathcal{M}$ a $\mathcal{N}$, pak pro libovolnou formuli φ s volnými proměnnými $x_1, \ldots, x_n$ a pro libovolné $a_1, \ldots, a_n \in M$ platí $\mathcal{M} \models \varphi[a_1, \ldots, a_n]$ právě když $\mathcal{N} \models \varphi[h(a_1), \ldots, h(a_n)]$*[1)].

Speciálně, je-li φ sentence, je $\mathcal{N} \models \varphi$ právě když $\mathcal{M} \models \varphi$.

[1)] $\mathcal{M} \models \varphi[a_1, \ldots, a_n]$ značí pravdivost φ při ohodnocení přiřazujícím proměnné x_i prvek a_i, $1 \leq i \leq n$

Připomeňme: *Teorie sentencí struktury $\mathcal{M}$* je (úplná) teorie

$$\mathrm{Thm}(\mathcal{M}) = \{\varphi \,;\, \varphi \text{ je uzavřená a } \mathcal{M} \models \varphi\}$$

Struktury $\mathcal{M}$ a $\mathcal{N}$ jsou *elementárně ekvivalentní* (značíme $\mathcal{M} \equiv \mathcal{N}$), jestliže $\mathrm{Thm}(\mathcal{M}) = \mathrm{Thm}(\mathcal{N})$.

Podobně, je-li T teorie, píšeme

$$\mathrm{Thm}(T) = \{\varphi \,;\, \varphi \text{ je uzavřená a } T \vdash \varphi\}.$$

Je-li T úplná teorie a $\mathcal{M} \models T$, je $\mathrm{Thm}(T) = \mathrm{Thm}(M)$. Každé dva modely úplné teorie jsou tudíž elementárně ekvivalentní.

Z předchozí věty mj. plyne:

$$\text{je-li } \mathcal{M} \cong \mathcal{N}, \text{ pak } \mathcal{M} \equiv \mathcal{N}.$$

Platí i opačná implikace?

Vsuvka o mohutnostech množin

Pojmem *mohutnost množiny* se budeme podrobněji zabývat v teorii množin, nyní tedy trochu předběhneme.

Množiny X a Y mají *stejnou mohutnost* (píšeme $X \approx Y$), existuje-li vzájemně jednoznačné (tj. prosté a na) zobrazení $f : X \to Y$. Říkáme též, že X *má mohutnost množiny* Y. Tento vztah je symetrický, reflexivní a tranzitivní.

Existuje-li prosté zobrazení $f : X \to Y$, říkáme že X má mohutnost *menší nebo rovnu* mohutnosti Y, píšeme $X \preccurlyeq Y$. Je-li $X \preccurlyeq Y$, ale $X \not\approx Y$, má X *(ostře) menší mohutnost* než Y, píšeme $X \prec Y$. Platí: Je-li $X \preccurlyeq Y$ a $Y \preccurlyeq X$, je $X \approx Y$ (tzv. Cantorova věta).

Množina je *konečná*, pokud $X \approx \{k \in \mathbb{N} \,;\, k \leq n\}$, pro nějaké $n \in \mathbb{N}$, jinak je *nekonečná* (tyto pojmy budeme později definovat maličko jinak, ovšem v zásadě ekvivalentně). Je-li $\mathbb{N} \approx X$, je X tzv. *spočetná*. Příkladem spočetných množin jsou $\mathbb{Z}$ či $\mathbb{Q}$. Množina $\mathbb{R}$ je nekonečná, není však spočetná. Říkáme, že je *nespočetná*.

Mohutností nekonečných množin existuje mnoho. Ke každé množině X lze totiž najít Y tak, že $X \prec Y$ (a to i tehdy, je-li X nekonečná)! Není tedy jen jedno nekonečno.

Zpátky k otázce $\mathcal{M} \equiv \mathcal{N} \stackrel{?}{\Rightarrow} \mathcal{M} \cong \mathcal{N}$. Obecně to **neplatí**!

Na základě věty o kompaktnosti lze totiž ukázat, že má-li teorie nekonečný model, má model libovolné nekonečné mohutnosti větší něž je mohutnost jazyka (tj. množiny symbolů). Každá teorie, jež má nekonečný model, má tudíž neizomorfní modely (neboť má modely různých mohutností).

Původní otázku můžeme ovšem položit lépe: Nechť $\mathcal{M} \equiv \mathcal{N}$, přičemž $M \approx N$. Je pak již $\mathcal{M} \cong \mathcal{N}$?

Bohužel, i zde je odpověď obecně **záporná**.

Kategorické teorie

Teorie T je *kategorická* v mohutnosti X, jsou-li každé dva modely teorie T mohutnosti X izomorfní.

Věta (*test úplnosti*): *Nechť T nemá konečné modely a nechť $\mathcal{M} \models T$, přičemž M má alespoň mohutnost jazyka teorie T. Je-li T kategorická v mohutnosti M, je úplná.*

Důkaz. Ukážeme, že $\mathrm{Thm}(T) = \mathrm{Thm}(\mathcal{M})$. Nechť $\mathcal{M} \models \varphi, T \not\vdash \varphi$. Pak $T \cup \{\neg\varphi\}$ je bezesporná a má tedy nějaký model $\mathcal{N}$, přičemž lze předpokládat, že N a M mají stejnou mohutnost (tzv. Löwenheim-Skolemova věta, bez důkazu). Jelikož $\mathcal{N} \models \neg\varphi$, nejsou $\mathcal{M}$ a $\mathcal{N}$ izomorfní, spor s kategoričností. □

Příklad: DeLO (teorie hustého lineárního uspořádání bez nejmenšího a největšího prvku) je úplná.

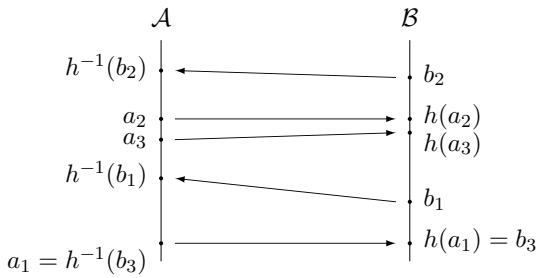
DeLO nemá konečný model neboť konečná lineární uspořádání mají nejmenší a největší prvek.

Zřejmě $\langle \mathbb{Q}, \leq \rangle \models$ DeLO.

DeLO je kategorická v mohutnosti množiny $\mathbb{Q}$, jak nyní dokážeme.

Předně: prvky $\mathbb{Q}$ lze očíslovat přirozenými čísly, množina $\mathbb{Q}$ je tedy spočetná.

Jsou-li $\mathcal{A}$, $\mathcal{B}$ dva spočetné modely teorie DeLO, $A = \{a_n \ ; \ n \in \mathbb{N}\}$ a $B = \{b_n \ ; \ n \in \mathbb{N}\}$, sestrojíme izomorfismus jejich uspořádání tzv. *„cik-cak“* metodou, kterou znázorňuje následující obrázek...



Hodnoty h definujeme prvek po prvku, kdy střídavě vždy nejvýše o jeden prvek rozšiřujeme zobrazení h a h^{-1}. Jsou-li $X \subseteq A$ a $Y \subseteq B$ konečné takové, že $\langle X, \leq^A \rangle \cong \langle Y, \leq^B \rangle$ a $a \in A$, lze díky hustotě uspořádání $\langle B, \leq^B \rangle$ najít prvek $b \in B$ tak, že $\langle X \cup \{a\} \rangle \cong \langle Y \cup \{b\} \rangle$. V našem případě je v $2n$-tém kroku $X = \{a_0, \ldots, a_{n-1}, h^{-1}(b_0), \ldots h^{-1}(b_{n-1})\}$ a $Y = \{h(a_0), \ldots, h(a_{n-1}), b_0, \ldots, b_{n-1}\}$. V $2n+1$-ním kroku naopak analogicky rozšíříme h^{-1} na b_n. □

DŮsledek: $\langle \mathbb{Q}, \leq \rangle \equiv \langle \mathbb{R}, \leq \rangle$.

Důkaz. Každá z uvedených struktur je modelem teorie DeLO, tudíž v obou z nich dle věty o úplnosti a bezespornosti platí všechny sentence dokazatelné v DeLO, čili

$$\mathrm{Thm}(\text{DeLO}) \subseteq \mathrm{Thm}(\langle \mathbb{Q}, \leq \rangle) \quad \text{a} \tag{3}$$

$$\mathrm{Thm}(\text{DeLO}) \subseteq \mathrm{Thm}(\langle \mathbb{R}, \leq \rangle). \tag{4}$$

DeLO je úplná. Uvedené inkluze tedy nemohou být ostré; v obou případech tudíž platí rovnost:

$$\mathrm{Thm}(\mathbb{Q}, \leq) = \mathrm{Thm}(\text{DeLO}) = \mathrm{Thm}(\mathbb{R}, \leq).$$

Kdyby totiž např. $\varphi \in \mathrm{Thm}(\langle \mathbb{Q}, \leq \rangle) - \mathrm{Thm}(\text{DeLO})$, pak $\neg\varphi \in \mathrm{Thm}(\text{DeLO})$ z úplnosti. Z inkluze (3) pak ovšem dostáváme $\{\varphi, \neg\varphi\} \subseteq \mathrm{Thm}(\langle \mathbb{Q}, \leq \rangle)$, spor. Analogicky pro $\langle \mathbb{R}, \leq \rangle$. □

—105—

Příklad: Platí $\langle \mathbb{Q}, + \rangle \equiv \langle \mathbb{R}, + \rangle \equiv \langle \mathbb{C}, + \rangle$

Nežli to dokážeme, připomeňme, že *vektorový prostor nad tělesem* $\mathcal{K} = \langle K, +^K, .^K, 1^K, 0^K \rangle$ je struktura v jazyce $\{+, 0\} \cup \{r\cdot\,; r \in K\}$ v níž platí následující axiomy *teorie vektorových prostorů nad tělesem* K:

1. axiomy teorie grup:

$$x + (y + z) = (x + y) + z, \qquad x + 0 = x \wedge 0 + x = x,$$
$$(\exists y)(x + y = 0 \wedge y + x = 0)$$

2. komutativita: $x + y = y + x$
3. vlastnosti násobení skalárem: pro každé $r, s \in K$ axiomy

$$(r +^K s) \cdot x = r \cdot x + s \cdot x, \quad r \cdot (x + y) = r \cdot x + r \cdot y$$
$$0^K \cdot x = 0, \quad 1^K \cdot x = x, \quad (r \cdot^K s) \cdot x = r \cdot (s \cdot x)$$

—106—

Všimněme si, že struktury $\langle \mathbb{Q}, +, 0, r\cdot \rangle_{r\in\mathbb{Q}}$, $\langle \mathbb{R}, +, 0, r\cdot \rangle_{r\in\mathbb{Q}}$ a $\langle \mathbb{C}, +, 0, r\cdot \rangle_{r\in\mathbb{Q}}$ v nichž je pro každé racionální číslo r dána unární operace $r\cdot$ *„násobení racionálním číslem r“.* jsou vektorové prostory nad tělesem $\mathbb{Q}$; všechny mají zjevně nenulovou dimenzi (prostor nulové dimenze sestává pouze z nulového vektoru). Dokážeme, že jsou elementárně ekvivalentní. Elementární ekvivalence $\langle \mathbb{Q}, + \rangle \equiv \langle \mathbb{R}, + \rangle \equiv \langle \mathbb{C}, + \rangle$ je speciální případ pro jazyk zredukovaný na $+$.

Stačí, když dokážeme, že teorie vektorových prostorů nenulové dimenze nad tělesem $\mathbb{Q}$ je úplná. K tomu nám opět poslouží test založený na pojmu kategoričnosti, tentokrát ovšem využijeme kategoričnosti pro nespočetné modely.

—107—

Základní fakta o vektorových prostorech, která nejspíš znáte

- Každý vektorový prostor $\mathcal{V}$ má *bázi*, tj. existuje minimální množina $B \subseteq V$ taková, že každý nenulový prvek $v \in V$ je lineární kombinací nějakých prvků z B (z minimality plyne, že prvky báze jsou lin. nezávislé).
- Mohutnosti báze se říká *dimenze* prostoru $\mathcal{V}$; dimenze vektorového prostoru je určena jednoznačně, tj. všechny jeho báze mají stejnou mohutnost.
- Vektorové prostory stejné dimenze jsou izomorfní (libovolné vzájemně jednoznačné zobrazení jejich bází lze rozšířit do izomorfismu celých prostorů).
- Je-li $\mathcal{V}$ vektorový prostor nad tělesem $\mathbb{Q}$ nenulové dimenze, je V nekonečná množina.
- Je-li navíc množina V nespočetná, je díky spočetnosti $\mathbb{Q}$ i každá báze B prostoru $\mathcal{V}$ nespočetná (ze spočetné báze nagenerují lineární kombinace s koeficienty z $\mathbb{Q}$ jen spočetně mnoho vektorů) a má dokonce stejnou mohutnost jako V, neboli $B \approx V$ (objasníme později).

—108—

DĹŽsledek: *Každé dva vektorové prostory nad $\mathbb{Q}$ stejné nespočetné mohutnosti jsou izomorfní.*

Teorie vektorových prostorů nenulové dimenze nad tělesem $\mathbb{Q}$ je proto kategorická v každé nespočetné mohutnosti, nemá konečné modely, a je tedy úplná dle testu úplnosti.

Stoji za zmínku, že teorii vektorových prostorů nad tělesem $\mathbb{Q}$ lze axiomatizovat pouze v jazyce $\{+, 0\}$ (případně jen $\{+\}$) jakožto teorii tzv. *„abelovských (tj. komutativních) divizibilních grup bez torze“*:

1. axiomy teorie grup:

$$x + (y + z) = (x + y) + z, \qquad x + 0 = x \wedge 0 + x = x,$$
$$(\exists y)(x + y = 0 \wedge y + x = 0)$$

2. komutativita: $x + y = y + x$

3. axiom *„beztorznosti“*: pro libovolné přirozené $n \geq 1$

$$x \neq 0 \to \underbrace{x + x + \ldots + x}_{n\text{-krát}} \neq 0$$

4. axiom *divizibility*: pro libovolné přirozené $n \geq 1$

$$(\forall x)(\exists y)x = \underbrace{y + y + \ldots + y}_{n\text{-krát}}$$

Máme-li naopak dokázat, že dvě struktury nejsou elementárně ekvivalentní, stačí najít sentenci, jež platí v jedné z těchto struktur, ale neplatí ve druhé.

Příklady:

1. $\langle \mathbb{Q}, + \rangle \not\equiv \langle \mathbb{Z}, + \rangle$, neboť formule $(\forall x)(\exists y)(x = y + y)$ neplatí v $\langle \mathbb{Z}, + \rangle$.

2. $\langle \mathbb{C}, \cdot \rangle \not\equiv \langle \mathbb{R}, \cdot \rangle$. V $\mathbb{C}$ má totiž každý prvek druhou odmocninu, v $\mathbb{R}$ nikoli (např. -1), tj. formule $(\forall x)(\exists y)(x = y \cdot y)$ platí v $\mathbb{C}$, ne však v $\mathbb{R}$.

3. $\langle \mathbb{Q}, \cdot, \leq, 0 \rangle \not\equiv \langle \mathbb{R}, \cdot, \leq, 0 \rangle$ je podobné: v $\mathbb{R}$ mají právě všechna nezáporná čísla druhou odmocninu. V $\mathbb{Q}$ nemá odmocninu např. číslo 5. Struktury lze odlišit třeba sentencí $(\forall x)(0 \leq x \to (\exists y)(x = y \cdot y))$.

4. $\langle \mathbb{Q}, \cdot, \leq \rangle \not\equiv \langle \mathbb{R}, \cdot, \leq \rangle$ je stejné jako předchozí případ, nyní však nemáme k dispozici konstantu 0. Vlastnost $z = 0$ lze však v uvedených strukturách vyjádřit pouze pomocí násobení třeba formulí

$$(\forall y)(y \cdot z = z),$$

čili v původní formuli

$$(\forall x)(0 \leq x \to (\exists y)(x = y \cdot y))$$

pouze nahradíme podformuli $0 \leq x$ formulí

$$(\exists z)((\forall y)(y \cdot z = z) \wedge z \leq x)$$

a jsme hotovi.

5. $\langle \mathbb{Q}, \cdot \rangle \not\equiv \langle \mathbb{R}, \cdot \rangle$

Tentokrát nemáme v jazyce ani uspořádání, nemůžeme tedy tak snadno vyjádřit vlastnost *„x je nezáporné“* společně pro obě struktury. Můžeme to však využít toho, že reálná nezáporná čísla mají odmocninu k následujícímu triku: je-li $r \in \mathbb{R}$, je r^2 je nezáporné a má tedy čtvrtou odmocninu (což je totéž, jako že $|r|$ má druhou odmocninu). Toto neplatí v $\mathbb{Q}$ např. pro $r = 2$. Použijeme tedy např. formuli

$$(\forall x)(\exists y)(x \cdot x = y \cdot y \cdot y \cdot y).$$

Otázka: platí $\langle \mathbb{C} - \{0\}, \cdot \rangle \equiv \langle \mathbb{Q}, + \rangle$?

Nejde o překlep. Řekněme, že obě struktury chápeme jako interpretace jazyka s jednou binární operací $\circ$, přičemž v $\mathbb{C} - \{0\}$ tuto operaci interpretujeme jako násobení komplexních čísel a v $\mathbb{Q}$ jako sčítání racionálních čísel...

Návod: ověřte, že $\langle \mathbb{C} - \{0\}, \cdot, 1 \rangle$ je abelovská divizibilní grupa bez torze.

Tímto končíme exkurzi do predikátové logiky. Seznámili jsme se s

- výrokovou pravdivostí, zejm. tabulkovou metodou a normálními tvary formulí
- jazykem predikátové logiky
- její sémantikou (relační struktury)
- základními pravidly odvozování v predikátové logice
- principy (Hilbertova) formálního kalkulu dokazatelnosti
- vztahem sémantiky a formální dokazatelnosti
- některými základními pojmy z teorie modelů (úplnost, elementární ekvivalence, kategoričnost) včetně několika elementárních příkladů

Literatura

Volně dostupné texty:

- Stručné, srozumitelné: *Úvod do matematické logiky a teorie množin*, Petr Kůrka
- Podrobněší: *Základy logického kalkulu*, Karel Čuda
- Detailní: *Predikátová logika*, skripta, Petr Štěpánek

(ke stažení z http://pajas.matfyz.cz/vyuka, případně http://ufal.mff.cuni.cz/~pajas/vyuka)

Výborná je též kniha:
Logika - neúplnost, složitost a nutnost, V. Švejdar, Academia, Praha 2002

Z ní jsou případně vhodné zejména (pod)kapitoly 1.1, 1.2, informativně 1.3, dále 3.1, informativně 3.2 a 3.4. Kniha obsahuje příklady a velkou řadu cvičení.

Další materiály dostupné na webu (příklady a cvičení):
http://vychodil.inf.upol.cz/courses/cs2ml/doc/mlcviceni.pdf
http://math.feld.cvut.cz/demlova/teaching/dml/prikl_vyr.pdf
http://math.feld.cvut.cz/demlova/teaching/dml/prikl_pred.pdf