Základy matematické logiky

Obsah

1 Úvod

1.1 Předmět matematiky

Ve 20. stol. se matematika stala konglomerátem teorií, které se zabývají studiem vlastností přesně charakterizovaných souhrnů objektů, jako jsou množiny, čísla, uspořádané množiny, grupy, okruhy, apod. Hovoříme pak o teorii množin, teorii čísel, teorii uspořádaných množin, terii grup, teorii okruhů, teorii těles, apod. Při rozvoji matematických teorií se klade důraz také na studium vztahů mezi jejich objekty (zobrazení mezi množinami, izotonní zobrazení mezi uspořádanými množinami, homomorfismy mezi grupami, apod.), takže předmětem moderní matematiky je cílevědomé studium tzv. matematických struktur.

Předmětem studia matematické logiky jsou právě matematické teorie, které jsou budovány formou definic, tvrzení a jejich důkazů. Tvrzení se dokazují dedukcí za použití přesného vymezení pojmů, tedy na základě formalizované logického systému. Stručně řečeno, *(matematickou) logikou* rozumíme

— analýzu metod správného usuzování a

— zkoumání matematických důkazů.

Hlavním úkolem logiky je studium zákonů, jimiž se řídíme při odvozování důsledků tak, abychom docházeli k závěrům vyplývajícím z výchozích předpokladů. Předmětem studia jsou matematické teorie, jejich jazyk a důkazové metody.

1.2 Nástin historie

Zakladatelem logiky je Aristoteles (který zkoumal tzv. kategorické úsudky). Ideu logického kalkulu poprvé formuloval G. W. Leibnitz. Prvky moderní matematické logiky se objevují v 19. stol. v souvislosti s přestavbou pojmů matematické analýzy na aritmetických základech a v souvislosti s objevem neeuklidovských geometrií. Matematická logika se zformulovala v polovině 19. století pracemi G. Boolea, k jejímu rozvoji významně přispěli také J. G. Frege, B. Russel, D. Hilbert. Silným impulsem byla Cantorova teorie množin a snaha o odstranění paradoxů teorie množin — vedla k nahrazení intuitivní teorie množin axiomatickými teoriemi (např. Zermelo-Fraenkelovou). Vzniklo však nebezpečí objevení nových paradoxů. Otázka bezespornosti axiomatických teorií vedla v r. 1920 D. Hilberta k formulaci tzv. programu formalizace matematiky.

1.3 Axiomatická výstavba matematických teorií

Je založena na *axiomech* — výchozích tvrzeních dané teorie, která se nedokazují, jejich platnost se předpokládá. Z axiomů se dedukcí odvozují další tvrzení — *důsledky*. Základním požadavkem je *bezespornost* — důsledkem axiomů nesmí být nějaké tvrzení a současně jeho negace. Vedlejším požadavkem je *nezávislost*

axiomů — žádný axiom není důsledkem zbývajících axiomů. Matematické teorie je pak možno formalizovat, tj. zapsat pomocí speciálních znaků — *symbolů*. Tvrzení dostanou podobu zvláštních *formulí* — slov sestavených určitým způsobem z daných symbolů. Pravidla odvozování důsledků pak přejdou v určité jednoduché operace s těmito formulemi. *Formalizovaná axiomatická teorie* je dána

symboly - tvoří abecedu dané teorie,

formulemi - určitá slova v této abecedě, která tvoří jazyk teorie,

axiomy - výchozí tvrzení dané teorie zapsaná pomocí abecedy jako jisté formule,

odvozovacími pravidly - pravidla pro manipulace s formulemi, pomocí kterých odvozujeme z axiomů důsledky.

Cílem Hilbertova programu bylo dokázat bezespornost silných matematických teorií pomocí kombinatorických manipulací s formulemi. K. Gödel však v r. 1931 svými větami o neúplnosti ukázal, že Hilbertův program nelze uskutečnit.

2 Výroková logika

Výroková logika (výrokový počet) zkoumá způsoby tvorby složených výroků z daných jednoduchých výroků, závislost pravdivosti (resp. nepravdivosti) složeného výroku na pravdivosti výroků, z nichž je složen. Tvorbu nejjednodušších výroků zde dále neanalyzujeme. Výroková logika je předstupeň k budování bohatších logických systémů.

Buď P neprázdná množina symbolů, které nazýváme *prvotní formule*. Zpravidla je značíme písmeny $p, q, \ldots$, případně s indexy $p_1, p_2, \ldots$. Prvotní formule hrají úlohu jednoduchých výroků. Složené výroky vytváříme z jednoduchých pomocí *logických spojek:*

$\neg$ negace,
$\wedge$ konjunkce,
$\vee$ disjunkce,
$\rightarrow$ implikace,
$\leftrightarrow$ ekvivalence.

Symboly jazyka L_P výrokové logiky (nad množinou P) jsou prvky množiny P, logické spojky a závorky (,). Úlohu složených výroků hrají *výrokové formule* jazyka L_P definované následovně:

(i) Každá prvotní formule $p \in P$ je výroková formule.

(ii) Jsou-li A, B výrokové formule, pak $(\neg A), (A \wedge B), (A \vee B), (A \rightarrow B), (A \leftrightarrow B)$ jsou také výrokové formule.

(iii) Každá výroková formule vznikne konečným počtem užití pravidel (i), (ii).

Každá výroková formule je konečná posloupnost symbolů jazyka L_P, která vznikne podle předchozích pravidel.

2.1 Závislost pravdivosti výrokových formulí na pravdivosti prvotních formulí

Pravdivostní ohodnocení prvotních formulí je lib. zobrazení $v : P \to \{0, 1\}$, tj. zobrazení, které každé prvotní formuli $p \in P$ přiřadí hodnotu 0 (nepravda) nebo 1 (pravda). Indukcí podle složitosti formule definujeme rozšíření $\overline{v}$ zobrazení v na množinu všech formulí jazyka L_P:

(i) $\overline{v}(p) = v(p)$ pro každé $p \in P$,

(ii) jsou-li A, B výrokové formule, pak $\overline{v}(\neg A), \overline{v}(A \wedge B), \overline{v}(A \vee B), \overline{v}(A \to B), \overline{v}(A \leftrightarrow B)$ v závislosti na $\overline{v}(A)$, $\overline{v}(B)$ se definuje podle následující tabulky:

$\overline{v}(A)$	$\overline{v}(B)$	$\overline{v}(\neg A)$	$\overline{v}(A \wedge B)$	$\overline{v}(A \vee B)$	$\overline{v}(A \to B)$	$\overline{v}(A \leftrightarrow B)$
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

Říkáme, že výroková formule A je *pravdivá při ohodnocení* v, jestliže $\overline{v}(A) = 1$. Říkáme, že výroková formule A je *tautologie*, jestliže $\overline{v}(A) = 1$ pro libovolné ohodnocení v. Píšeme $\models A$.

Následující výrokové formule jsou tautologie:

$A \vee \neg A$ **zákon vyloučeného třetího,**
$\neg\neg A \leftrightarrow A$ **zákon dvojí negace,**
$\neg(A \wedge \neg A)$ **vyloučení sporu.**

Tautologie jsou pravdivé bez ohledu na pravdivost svých prvotních formulí. Pravdivost tautologie je dána pouze jejím syntaktickým tvarem. Řekneme, že výrokové formule jsou *logicky ekvivalentní*, právě když $\overline{v}(A) = \overline{v}(B)$ při každém pravdivostním ohodnocení v. Formule A, B jsou logicky ekvivalentní, právě když formule $A \leftrightarrow B$ je tautologie.

Pro každé dvě výrokové formule A, B jsou následující dvojice logicky ekvivalentní formule:

$$\begin{aligned}
A \leftrightarrow B &\quad \dots \quad (A \to B) \wedge (B \to A) \\
A \to B &\quad \dots \quad \neg A \vee B \\
A \to B &\quad \dots \quad \neg(A \wedge \neg B) \\
A \vee B &\quad \dots \quad \neg(\neg A \wedge \neg B) \\
A \wedge B &\quad \dots \quad \neg(\neg A \vee \neg B) \\
A \vee B &\quad \dots \quad \neg A \to B \\
A \wedge B &\quad \dots \quad \neg(A \to \neg B)
\end{aligned}$$

Důsledek: Každá výroková formule je logicky ekvivalentní některé výrokové formuli, v níž se vyskytují pouze logické spojky $\neg, \to$. Totéž platí pro dvojice $\neg, \wedge$

a $\neg, \vee$. Je výhodné nepracovat se všemi spojkami, ale zvolit např. $\neg, \to$ za základní spojky a ostatní spojky pomocí nich dodefinovat.

Lze definovat nové logické spojky $\downarrow$ (Nicodova spojka) a $\mid$ (Shefferova spojka):

$\overline{v}(A)$	$\overline{v}(B)$	$\overline{v}(A \downarrow B)$	$\overline{v}(A \mid B)$
0	0	1	1
0	1	0	1
1	0	0	1
1	1	0	0

Pak	$A \downarrow B$	je log. ekvivalentní	$\neg A \wedge \neg B$
	$A \mid B$		$\neg A \vee \neg B$
	$\neg A$		$A \downarrow A$
	$\neg A$		$A \mid A$
	$A \wedge B$		$(A \downarrow A) \downarrow (B \downarrow B)$
	$A \vee B$		$(A \mid A) \mid (B \mid B)$.

Každá výroková formule je logicky ekvivalentní některé výrokové formuli sestrojené pouze pomocí log. spojky $\downarrow$ nebo pouze pomocí log. spojky $\mid$.

Definice pravdivosti přímo dává algoritmus k určení toho, zda daná formule A je tautologie. Pravdivost formule A při ohodnocení v závisí pouze na hodnotách $v(p)$ prvotních formulí, které se vyskytují v A. Množina P_A všech těchto prvotních formulí je konečná. Stačí tedy zkontrolovat jen konečný počet zobrazení $P_A \to \{0, 1\}$. Má-li P_A n prvků, pak těchto zobrazení je 2^n.

2.2 Dokazatelnost ve výrokové logice

Dále chceme studovat dokazatelnost ve výrokové logice. K tomuto účelu je výroková logika budována alternativním přístupem — jako formální axiomatická teorie (tzv. Hilbertova typu).

2.2.1 Formální axiomatický systém výrokové logiky

Abeceda - množina P prvotních formulí,
- symboly pro logické spojky $\neg, \to$,
- pomocné symboly $(,)$ pro závorky.

Formule - všechny prvotní formule jsou formule,
- jsou-li A, B formule, pak také $(\neg A)$ a $(A \to B)$ jsou formule,
- každá formule vznikne konečným počtem použití předchozích dvou pravidel.

Jazyk - abeceda a formule tvoří jazyk výrokové logiky.

Axiomy - nekonečně mnoho axiomů zadaných pomocí následujících tří schémat.

Pro libovolné formule A, B, C je každá formule některého z následujících tří tvarů axiomem výrokové logiky:

(A1) $A \to (B \to A)$
(A2) $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
(A3) $(\neg B \to \neg A) \to (A \to B)$

Odvozovací pravidlo – jediné pravidlo, které se nazývá *modus ponens* (pravidlo odloučení) a značí se MP: Z formulí $A, (A \to B)$ se odvodí formule B. Formule $A, (A \to B)$ se nazývají *předpoklady* a B *závěr* odvozovacího pravidla MP.

Definice 2.1. *Důkazem* ve formální výrokové logice rozumíme libovolnou konečnou posloupnost $A_1, \ldots, A_n$ výrokových formulí takovou, že pro každé $i \leq n$ formule A_i je buď axiomem nebo je závěrem pravidla modus ponens, jehož předpoklady jsou mezi $A_1, \ldots, A_{i-1}$. Řekneme, že formule A je *dokazatelná* ve výrokové logice, jestliže existuje důkaz, jehož poslední formulí je formule A; píšeme pak $\vdash A$.

Věta 2.1. (O korektnosti) *Libovolná dokazatelná formule výrokové logiky je tautologie.*

Důkaz: Nejprve se přesvědčíme, že všechny axiomy výrokové logiky jsou tautologie. Můžeme použít tabulkovou metodu. Mějme axiom (A1) a pro libovolné ohodnocení v uvažme všechny možnosti:

$\overline{v}(A)$	$\overline{v}(B)$	$\overline{v}(B \to A)$	$\overline{v}(A \to (B \to A))$
0	0	1	1
0	1	0	1
1	0	1	1
1	1	1	1

Takže $\overline{v}(A \to (B \to A)) = 1$ pro každé ohodnocení v, tedy (A1) je tautologie. Analogicky ověříme (A2),(A3).
Můžeme použít také nepřímou metodu. Uvažme axiom (A3): Kdyby v bylo ohodnocení takové, že $\overline{v}((\neg\, B \to \neg\, A) \to (A \to B)) = 0$, pak nutně $\overline{v}(A \to B) = 0$, odtud nutně $\overline{v}(A) = 1$, $\overline{v}(B) = 0$. Pak ovšem $\overline{v}(\neg A) = 0$, $\overline{v}(\neg B) = 1$, takže $\overline{v}(\neg B \to \neg A) = 0$. Potom ale $\overline{v}((\neg B \to \neg A) \to (A \to B)) = 1$, což je spor. Tedy (A3) je tautologie. Podobně lze ověřit, že (A1) a (A2) jsou tautologie.
Zbývá ukázat, že odvozovací pravidlo je korektní, tj. že jsou-li předpoklady A,$A \to B$ tautologie, je i B tautologie. Je-li ovšem v lib. ohodnocení, pak $\overline{v}(A) = 1, \overline{v}(A \to B) = 1$, odtud a z definice pravdivostního ohodnocení pro spojku $\to$ ihned plyne $\overline{v}(B) = 1$,tedy B je tautologie. Každá dokazatelná formule je proto tautologie.

□

Budeme potřebovat zobecnění pojmu dokazatelnosti. Nechť T je množina formulí výrokové logiky. Řekneme, že konečná posloupnost formulí $A_1, \ldots, A_n$ je *důkazem formule A z předpokladů T*, jestliže A_n je formule A a pro lib. $i \leq n$ platí: A_i je buď axiom výrokové logiky nebo formule z T nebo A_i je závěrem odvozovacího pravidla modus ponens, jehož předpoklady jsou mezi $A_1, \ldots, A_{i-1}$. Říkáme, že formule A je *dokazatelná z předpokladů T*, píšeme $T \vdash A$. Poznamenejme, že (v důsledku pravidla modus ponens) z $T \vdash A$ a $U \vdash A \to B$ vyplývá, že $T \cup U \vdash B$ (stačí důkaz formule $A \to B$ z předpokladů U napsat za důkaz formule A z předpokladů T a jako poslední člen připsat formuli B).
Směřujeme k důkazu toho, že axiomatický systém výrokové logiky je úplný, tj. že každá tautologie je dokazatelná.

Lemma 2.2. *Pro lib. fromuli A je dokazatelná formule $A \to A$, tj. $\vdash A \to A$.*

Důkaz: Následující posloupnost formulí je důkaz formule $A \to A$:

(1)	$A \to ((A \to A) \to A)$	(A1)
(2)	$(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A))$	(A2)
(3)	$(A \to (A \to A)) \to (A \to A)$	(1),(2) MP
(4)	$A \to (A \to A)$	(A1)
(5)	$A \to A$	(3),(4) MP

□

Pozn.:
(1) je (A1) pro volbu A, $A \to A$ za A,B
(2) je (A2) pro vlobu A, $A \to A$, A za A, B, C
(3) je závěr pravidla MP z předpokladů (1),(2)

Věta 2.3. (O dedukci) *Nechť T je množina formulí, nechť A,B jsou formule. Potom $T \vdash A \to B$, právě když $T \cup \{A\} \vdash B$.*

Pozn. Budeme stručně psát T, A místo $T \cup \{A\}$.

Důkaz: "$\Rightarrow$": Je-li $T \vdash A \to B$, potom existuje posloupnost formulí $A_1, \ldots, A_{n-1}, A \to B$, jež je důkazem formule $A \to B$ z předpokladů T. Pak $A, A_1, \ldots, A_{n-1}, A \to B, B$ je důkazem B z předpokladů T, A.

"$\Leftarrow$": Předpokládejme naopak, že $T, A \vdash B$. Nechť posloupnost $A_1, \ldots, A_{n-1}, B$ je důkaz formule B z předpokladů T, A. Označme také A_n formuli B. Ukážeme, jak tento důkaz přetvořit na důkaz $A \to B$ z předpokladů T. Indukcí ukážeme, že pro $j \leq n$ platí $T \vdash A \to A_j$. Tím pro $j = n$ dostaneme $T \vdash A \to B$.

Předpokládejme tedy, že pro všechna $i < j$ jsme již důkazy formulí $A \to A_i$ z předpokladů T sestrojili. Konstruujme důkaz formule $A \to A_j$ z předpokladů T. Mohou nastat 3 případy:

a) Je-li A_j axiom nebo formule z T, pak následující posloupnost
   (1) A_j (axiom nebo formule z T)
   (2) $A_j \to (A \to A_j)$ (A1)
   (3) $A \to A_j$ (1),(2) MP
   je důkazem $A \to A_j$ z předpokladů T.

b) Je-li $A_j = A$, pak dle předcházejícího lemmatu $\vdash A \to A$, tedy tím spíše $T \vdash A \to A$.

Poznamenejme, že pro $j = 1$ mohou nastat pouze předchozí dva případy.

c) Nechť nakonec A_j je závěrem pravidla modus ponens, jehož předpoklady jsou mezi formulemi A_i, $i < j$. Tyto předpoklady musí být tvaru A_r pro $r < j$, $A_r \to A_j$. Podle indukčního předpokladu máme $T \vdash A \to A_r$, $T \vdash A \to (A_r \to A_j)$.
   Dále, uvažujme axiom (A2) pro volbu A, A_r, A_j za formule A, B, C, tj. axiom
   $$\vdash (A \to (A_r \to A_j)) \to ((A \to A_r) \to (A \to A_j)).$$
   Dvojím použitím pravidla modus ponens dostaneme nejprve
   $$T \vdash (A \to A_r) \to (A \to A_j) \text{ a pak}$$
   $$T \vdash A \to A_j.$$

Věta o dedukci je dokázána.

□

Lemma 2.4. *Pro lib. formule A, B je*
(a) $\vdash \neg A \to (A \to B)$
(b) $\vdash \neg\neg A \to A$
(c) $\vdash A \to \neg\neg A$
(d) $\vdash (A \to B) \to (\neg B \to \neg A)$
(e) $\vdash A \to (\neg B \to \neg(A \to B))$
(f) $\vdash (\neg A \to A) \to A$

Důkaz:

(a)
(1)	$\vdash \neg A \to (\neg B \to \neg A)$	(A1)
(2)	$\neg A \vdash \neg B \to \neg A$	VD
(3)	$\vdash (\neg B \to \neg A) \to (A \to B)$	(A3)
(4)	$\neg A \vdash A \to B$	(2),(3) MP
(5)	$\vdash \neg A \to (A \to B)$	VD

(b)	(1)	$\vdash \neg\neg A \to (\neg A \to \neg\neg\neg A)$	podle (a)
	(2)	$\neg\neg A \vdash \neg A \to \neg\neg\neg A$	VD
	(3)	$\vdash (\neg A \to \neg\neg\neg A) \to (\neg\neg A \to A)$	(A3)
	(4)	$\neg\neg A \vdash \neg\neg A \to A$	(2),(3) MP
	(5)	$\neg\neg A \vdash A$	VD
	(6)	$\vdash \neg\neg A \to A$	VD

(c)	(1)	$\vdash \neg\neg\neg A \to \neg A$	podle (b)
	(2)	$\vdash (\neg\neg\neg A \to \neg A) \to (A \to \neg\neg A)$	(A3)
	(3)	$\vdash A \to \neg\neg A$	(1),(2) MP

(d)	(1)	$\neg\neg A \vdash A$	VD, podle (b)
	(2)	$A \to B \vdash A \to B$	
	(3)	$A \to B, \neg\neg A \vdash B$	(1),(2) MP
	(4)	$\vdash B \to \neg\neg B$	podle (c)
	(5)	$A \to B, \neg\neg A \vdash \neg\neg B$	(3),(4) MP
	(6)	$A \to B \vdash \neg\neg A \to \neg\neg B$	VD
	(7)	$\vdash (\neg\neg A \to \neg\neg B) \to (\neg B \to \neg A)$	(A3)
	(8)	$A \to B \vdash (\neg B \to \neg A)$	(6),(7) MP
	(9)	$\vdash (A \to B) \to (\neg B \to \neg A)$	VD

(e)	(1)	$A \vdash A$	
	(2)	$A \to B \vdash A \to B$	
	(3)	$A, A \to B \vdash B$	(1),(2) MP
	(4)	$A \vdash (A \to B) \to B$	VD
	(5)	$\vdash ((A \to B) \to B) \to (\neg B \to \neg(A \to B))$	podle (d)
	(6)	$A \vdash \neg B \to \neg(A \to B)$	(4),(5) MP
	(7)	$\vdash A \to (\neg B \to \neg(A \to B))$	VD

(f)	(1)	$\vdash \neg A \to (\neg A \to \neg(\neg A \to A))$	podle (e)
	(2)	$\neg A \vdash \neg(\neg A \to A)$	VD (2×)
	(3)	$\vdash \neg A \to \neg(\neg A \to A)$	VD
	(4)	$\vdash (\neg A \to \neg(\neg A \to A)) \to ((\neg A \to A) \to A)$	(A3)
	(5)	$\vdash (\neg A \to A) \to A$	(3),(4) MP

□

Lemma 2.5. (O neutrální formuli) *Nechť T je množina výrokových formulí, nechť A, B jsou formule. Jestliže $T, A \vdash B$ a $T, \neg A \vdash B$, pak $T \vdash B$.*

Důkaz: Ukážeme, jak se přesvědčit, že za daných předpokladů existuje důkaz B z předpokladů T.

(1)	$T, \neg A \vdash B$	předpoklad
(2)	$T \vdash \neg A \to B$	VD
(3)	$\vdash (\neg A \to B) \to (\neg B \to \neg\neg A)$	dle Lemmatu 2.4 (d)
(4)	$T \vdash \neg B \to \neg\neg A$	(2),(3) MP
(5)	$T, \neg B \vdash \neg\neg A$	VD
(6)	$\vdash \neg\neg A \to A$	dle Lemmatu 2.4 (b)
(7)	$T, \neg B \vdash A$	(5),(6) MP
(8)	$T, A \vdash B$	předpoklad
(9)	$T \vdash A \to B$	VD
(10)	$T, \neg B \vdash B$	(7),(9) MP
(11)	$T \vdash \neg B \to B$	VD
(12)	$\vdash (\neg B \to B) \to B$	dle Lemmatu 2.4 (f)
(13)	$T \vdash B$	(11),(12) MP

□

Zavedeme pomocné označení:
Je-li v lib. ohodnocení prvotních formulí, pak pro lib. formuli B klademe

$$B^v = \begin{cases} B & pro \quad \overline{v}(B) = 1 \\ \neg B & pro \quad \overline{v}(B) = 0 \end{cases}$$

Lemma 2.6. *Nechť všechny prvotní formule ve výrokové formuli A jsou obsaženy mezi $P_1, \ldots, P_n$. Pak pro lib. ohodnocení v prvotních formulí platí $P_1^v, \ldots, P_n^v \vdash A^v$.*

Důkaz: Indukcí podle složitosti formule A.

1) Je-li A některá z prvotních formulí, není co dokazovat.

2) Předpokládejme, že A je tvaru $\neg B$ a pro B je tvrzení již dokázáno. Jsou možné 2 případy:

   – Je-li $\overline{v}(B) = 0$, potom $B^v = \neg B$, čili B^v je A. Dále $\overline{v}(A) = 1$, takže A^v je A, čili A^v je rovno B^v a tvrzení pro A plyne z toho, že platí pro B.

   – Je-li $\overline{v}(B) = 1$, potom $B^v = B$ a máme $P_1^v, \ldots, P_n^v \vdash B$. Podle Lemmatu 2.4 (c) je dokazatelné $\vdash B \to \neg\neg B$. Odtud užitím pravidla MP: $P_1^v, \ldots, P_n^v \vdash \neg\neg B$. Zbývá si uvědomit, že $\neg\neg B$ je A^v, neboť $\neg B$ je A a $\overline{v}(A) = 0$.

3) Předpokládejme, že formule A je tvaru $C \to D$, kde pro C, D je tvrzení dokázáno. Jsou možné 4 případy:

   – Je-li $\overline{v}(C) = 1, \overline{v}(D) = 1$ nebo

   – je-li $\overline{v}(C) = 0, \overline{v}(D) = 1$, pak v obou případech $\overline{v}(A) = 1$. Dále, D^v je D, takže máme $P_1^v, \ldots, P_n^v \vdash D$ a dle (A1) $\vdash D \to (C \to D)$. Odtud užitím MP $P_1^v, \ldots, P_n^v \vdash C \to D$. Stačí si uvědomit, že $C \to D$ je A^v.

– Je-li $\overline{v}(C) = 0, \overline{v}(D) = 0$. Pak opět $\overline{v}(A) = 1$, dále C^v je $\neg C$, takže máme $P_1^v, \ldots, P_n^v \vdash \neg C$. Dle lemmatu 2.4 (a) $\vdash \neg C \to (C \to D)$ a užitím pravidla MP dostáváme $P_1^v, \ldots, P_n^v \vdash C \to D$. Stačí si uvědomit, že $C \to D$ je A^v.
– Je-li $\overline{v}(C) = 1, \overline{v}(D) = 0$, pak $\overline{v}(A) = 0$. Dále C^v je C, D^v je $\neg D$, takže máme $P_1^v, \ldots, P_n^v \vdash C$; $\quad P_1^v, \ldots, P_n^v \vdash \neg D$. Dle lemmatu 2.4 (e) máme $\vdash C \to (\neg D \to \neg(C \to D))$. Dvojím užitím pravidla MP dostáváme: $P_1^v, \ldots, P_n^v \vdash \neg(C \to D)$. Zbývá si uvědomit, že v tomto případě A^v je $\neg(C \to D)$.

□

Věta 2.7. (Postova věta o úplnosti) *Formule dokazatelné ve výrokové logice jsou právě tautologie. Jinými slovy — pro lib. výrokovou formuli A platí $\vdash A$, právě když $\models A$.*

Důkaz:

"⇒": Jestliže $\vdash A$, pak $\models A$ podle věty 2.1 (o korektnosti).

"⇐": Předpokládejme tedy naopak, že $\models A$.
Nechť $P_1, \ldots, P_n$ jsou všechny prvotní formule vyskytující se v A. Indukcí ukážeme, že pro každé $k \in \{0, \ldots n\}$ a každé každé ohodnocení u prvotních formulí platí vztah $P_1^u, \ldots, P_{n-k}^u \vdash A$.

Podle Lemmatu 2.6 pro libovolné ohodnocení u prvotních formulí máme: $P_1^u, \ldots, P_n^u \vdash A$, neboť A^u je A, jelikož $\overline{u}(A) = 1$ (A je tautologie). Tedy vztah platí pro $k = 0$.

Předpokládejme, že tvrzení platí pro $k \in \{0, \ldots, n-1\}$ a nechť u je libovolné ohodnocení prvotních formulí. Nechť v je ohodnocení prvotních formulí takové, že:

$$v(P_i) = u(P_i) \text{ pro } i = 1, \ldots, n-k-1,$$
$$v(P_{n-k}) \text{ je opačná oproti } u(P_{n-k}).$$

Podle indukčního předpokladu máme

$$P_1^u, \ldots, P_{n-k-1}^u, P_{n-k}^u \vdash A,$$
$$P_1^v, \ldots, P_{n-k-1}^v, P_{n-k}^v \vdash A$$

a platí $P_{n-k}^v = \neg P_{n-k}^u$. Podle Lemmatu 2.5 o neutrální formuli dostáváme: $P_1^v, \ldots, P_{n-k-1}^u \vdash A$. Tedy vztah platí pro $k+1$.

Ukázali jsme, že vztah platí pro libovolné $k \in \{0, \ldots, n\}$ a libovolné u. Volbou $k = n$ dostáváme $\vdash A$.

□

Postova věta o úplnosti ukazuje, že přirozený pojem tautologie se podařilo úplně charakterizovat ve formální výrokové logice pojmem dokazatelnosti, tj. volbou axiomů a odvozovacího pravidla.

3 Predikátová logika 1. řádu

Matematické teorie pracují s celými soubory objektů (čísla, body prostoru, prvky algebraických struktur). Pro označení lib. prvků z daného oboru používáme *proměnné* $(x, y, z, \ldots, x_1, x_2, \ldots)$.

Mezi prvky z daného oboru mohou být některé význačné objekty (0, neutrální prvek grupy,...), pro něž užíváme zvláštní symboly — *konstanty* (např. $0, 1, \ldots$).

S objekty daného oboru lze provádět různé operace (sčítání a násobení čísel, násobení v grupách,...). K označení operací užíváme *funkční symboly* ($f, g, h, \ldots$, $f_1, f_2, f_3, \ldots$). Ke každému funkčnímu symbolu je přiřazeno přirozené číslo, které vyjadřuje jeho *četnost*, tj. počet argumentů dané operace. Je-li četnost symbolu rovna n, říkáme, že symbol je n-ární. Je přirozené chápat konstanty jako nulární funkční symboly.

Matematika zkoumá vlastnosti objektů a vztahy mezi objekty. Vlastnosti a vztahy mezi objekty daného oboru, tzv. *predikáty*, ("být záporným číslem"(vlastnost), "být menší než", "být prvkem"(vztahy)) vyjadřujeme pomocí *predikátových symbolů* ($p, q, r, \ldots, p_1, p_2, \ldots$). Predikát znamená vztah mezi užitým počtem objektů. Tím je každému predikátovému symbolu přiřazeno přirozené číslo, jeho *četnost*, udávající počet jeho argumentů. Je-li četnost rovna n, říkáme, že symbol je n-*ární*. V mnoha případech používáme zvláštního označení $=$ pro binární predikátový symbol označující rovnost, tj. totožnost objektů z daného oboru.

Z proměnných, konstant, funkčních symbolů a predikátových symbolů sestavujeme jistým způsobem nejjednodušší tvrzení, vyjádřená tzv. *atomickými formulemi*. Z nich vytváříme složitější formule pomocí *logických spojek* (stejných jako ve výrokové logice) a pomocí *kvantifikace proměnných*.
Univerzální (obecný) kvantifikátor $\forall$ vyjadřuje platnost pro všechny objekty z daného oboru.
Existenční kvantifikátor $\exists$ vyjadřuje existenci požadovaného objektu v daném oboru.

Příklad 3.1.

a) $\forall x(x \cdot 0 = 0)$ v $\mathbf{R}$ vyjadřuje "pro každé reálné číslo x platí, že $x \cdot 0 = 0$".

b) $\exists x(\neg(x = 1) \wedge (x.x = 1))$ v $\mathbf{R}$ vyjadřuje "existuje reálné číslo x takové, že $x \neq 1$ a $x^2 = 1$".

c) $\forall x \exists y(x < y)$ vyjadřuje "pro každé x existuje y, které je větší než x".

Uvedené symboly spolu s logickými spojkami a *pomocnými symboly* (závorky, čárka) tvoří abecedu jazyka *predikátové logiky 1. řádu*. Proměnné jazyka 1. řádu jsou obecná jména pro objekty daného oboru, tj. pro individua (např. čísla). Jazyk neobsahuje proměnné pro množiny individuí (např. množiny čísel, relací,...). Kvantifikovat lze pouze proměnné pro individua; tím se jazyk 1. řádu liší od jazyků vyšších řádů, které dovolují kvantifikovat např. množiny, relace...

Příklad 3.2. V oboru $\mathbf{R}$ reálných čísel v logice 1. řádu nelze vyjádřit: $\forall A \subseteq \mathbf{R}; \forall f : \mathbf{R} \to \mathbf{R}$ ani $\forall_{n=1}^{\infty}$.

3.1 Jazyk predikátové logiky

Logické symboly:

$x, y, \ldots, x_1, x_2, \ldots$	proměnné,
$\neg, \wedge, \vee, \to, \leftrightarrow$	logické spojky,
$\forall, \exists$	kvantifikátory,
$(,)$	závorky,
$=$	predik. symbol rovnosti.

Speciální symboly:

funkční symboly $f, g, \ldots, f_1, f_2, \ldots$, u každého symbolu je dáno nezáporné celé číslo — jeho četnost,

predikátové symboly $p, q, \ldots, p_1, p_2, \ldots$, u každého symbolu je dáno kladné celé číslo — jeho četnost.

Obsahuje-li jazyk symbol $=$ pro rovnost, mluvíme *o jazyku s rovností*. Specifiku jazyka určují jeho funkční a predikátové symboly (určují oblast, kterou jazyk popisuje).

Příklad 3.3.

1) Jazyk teorie uspořádání:
   - jazyk s rovností $=$
   - jediný predikátový (binární) symbol $<$
2) Jazyk teorie grup:
   - jazyk s rovností $=$
   - nulární funkční symbol 1 pro neutrální prvek
   - binární funkční symbol $\cdot$ pro grupovou operaci násobení
3) Jazyk teorie okruhů:
   - jazyk s rovností $=$
   - dvě konstanty $0, 1$
   - dva binární funkční symboly $+, \cdot$
4) Jazyk teorie množin:
   - jazyk s rovností

– binární predikátový symbol $\in$ být prvkem

5) Jazyk elementární aritmetiky:

– jazyk s rovností $=$

– funkční symboly :

0 — nulární symbol pro nulu

S — unární symbol pro vzetí následujícího čísla k danému číslu

$+, \cdot$ — binární symboly pro sčítání a násobení

3.1.1 Termy

(i) Každá proměnná je term.

(ii) Je-li f funkční symbol četnosti n a jsou-li $t_1, \ldots, t_n$ termy, pak také $f(t_1, \ldots, t_n)$ je term.

(iii) Každý term vznikne konečným počtem užití (i) a (ii).

Poznamenejme, že z (ii) plyne, že každá konstanta je term.

Příklad 3.4. V jazyce elementární aritmetiky jsou následující výrazy termy:
x, y proměnné,
0 konstanta,
$S(0), S(x), S(S(0)), x + y, x + 0, x \cdot y, x \cdot S(x), (x + S(y)) \cdot y, (S(0) + (x \cdot y)) \cdot S(x)$.

Poznamenejme, že u vžitých funkčních symbolů místo $+(x, y)$ píšeme $x + y$, místo $\cdot(x, y)$ píšeme $x \cdot y$ apod.

3.1.2 Atomické formule

Je-li p predikátový symbol četnosti n a jsou-li $t_1, \ldots, t_n$ termy, pak $p(t_1, \ldots, t_n)$ je *atomická formule.*
Speciálně, máme-li jazyk s rovností a jsou-li t_1, t_2 termy, pak $(t_1 = t_2)$ je atomická formule. Píšeme $(t_1 = t_2)$ místo $= (t_1, t_2)$. Podobný zápis používáme i pro jiné binární predikátové symboly, např. místo $< (t_1, t_2)$ píšeme $t_1 < t_2$.

Příklad 3.5.

a) V jazyce teorie uspořádání jsou atomické formule $x < x, x < y$.

b) V jazyce elementární aritmetiky je atomická formule $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

3.1.3 Formule

(i) Každá atomická formule je formule.

(ii) Jsou-li φ, ψ formule, pak také $(\neg\varphi), (\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \to \psi), (\varphi \leftrightarrow \psi)$ jsou formule.

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

(iv) Každá formule vznikne konečným počtem užití (i),(ii),(iii).

Příklad 3.6.

a) V jazyce teorie uspořádání je formule $\forall x \forall y(x < y \to \exists z(x < z \wedge z < y))$.

b) V jazyce elementární aritmetiky je formulí $\forall x(x \neq 0 \to \exists y(x = S(y)))$.

Poznamenejme, že píšeme $x \neq y$ místo $\neg(x = y)$, a také, pokud to nemůže narušit srozumitelnost, vynecháváme některé dvojice závorek.

Při tvorbě formule φ podle předchozí definice vytváříme určitou posloupnost formulí, která začíná atomickými formulemi a končí formulí φ a každá formule v této posloupnosti vzniká z některých předcházejících pomocí logických spojek a kvantifikátorů. Každá z těchto formulí se nazývá *podformule* formule φ.

Každá formule je konečnou posloupností symbolů. Každý symbol, zejména každá proměnná, se může ve formuli vyskytovat na jednom nebo více místech. Řekneme, že daný *výskyt* proměnné x ve formuli φ je *vázaný*, nachází-li se v nějaké podformuli tvaru $\forall x\psi$ nebo $\exists x\psi$. V tomto případě se proměnná x vyskytuje v kvantifikátoru samém nebo ve formuli ψ (podformule ψ se nazývá *obor kvantifikátoru* $\forall x$ nebo $\exists x$). V opačném případě (výskyt není vázaný) řekneme, že daný výskyt proměnné x ve formuli φ je *volný*. Proměnná x se nazývá *volnou (vázanou) proměnnou* ve formuli φ, existuje-li její volný (vázaný) výskyt v této formuli. Proměnná tedy může být ve formuli volná i vázaná. Formule neobsahující žádnou volnou proměnnou se nazývá *uzavřená formule* nebo též *výrok*. Naopak, formule neobsahující žádnou vázanou proměnnou se nazývá *otevřenou formulí*. Uzavřené a otevřené formule nazýváme *formulemi s čistými proměnnými*.

Příklad 3.7. Proměnná x má ve formuli $\underbrace{x}_{volný} = z \to (\exists\ \underbrace{x(x}_{vázaný} = z))$ dva vázané výskyty a jeden volný výskyt (a tato formule tedy není uzavřená ani otevřená).

4 Sémantika predikátové logiky

Chceme dát interpretaci symbolům jazyka predikátové logiky 1. řádu. Nejprve vymezíme obor, který bude určovat možné hodnoty proměnných, bude to určitý soubor M uvažovaných objektů. Funkčním symbolům budou odpovídat operace na M příslušných četností. Predikátovým symbolům budou odpovídat vztahy mezi objekty z M, které lze popsat jako relace na M příslušných četností. Máme-li jazyk s rovností, interpretujeme symbol $=$ jako rovnost objektů z M.

Definice 4.1. Nechť L je jazyk 1. řádu. *Realizací jazyka* L rozumíme algebraickou strukturu $\mathcal{M}$, která se skládá z

(i) neprázdné množiny M, kterou nazveme *univerzum*,

(ii) pro každý funkční symbol f četnosti n je dáno zobrazení $f_{\mathcal{M}} : M^n \to M$,

(iii) pro každý predikátový symbol p četnosti n, kromě rovnosti, je dána relace $p_{\mathcal{M}} \subseteq M^n$.

Poznamenejme, že pro nulární funkční symbol, tj. pro konstantu, je $M^0 = \{0\}$ a příslušné zobrazení $M^0 \to M$ lze chápat jako vyznačení určitého prvku z M odpovídajícího dané konstantě.

Příklad 4.1.

1. Neobsahuje-li jazyk L predikátové symboly, dostáváme známý pojem univerzální algebry.
2. Obsahuje-li jazyk L jediný binární predikátový symbol a žádný funkční symbol, dostáváme množinu vybavenou jedinou binární relací. (Lze chápat jako orientovaný graf.)
3. Obsahuje-li jazyk L jediný binární funkční symbol, dostáváme grupoid (tj. množinu vybavenou jednou binární operací).
4. Každá grupa, ale také každý grupoid s jedním vyznačeným prvkem, je realizací jazyka teorie grup.
5. Množina N všech přirozených čísel včetně nuly s obvyklými operacemi následníka, sčítání a násobení je realizací jazyka elementární aritmetiky.

Chceme-li zkoumat pravdivost formulí jazyka L v nějaké jeho realizaci $\mathcal{M}$, musíme volným proměnným přiřadit hodnoty, jimiž budou nějaké prvky množiny M.

Definice 4.2. Libovolné zobrazení e množiny všech proměnných do univerza M dané realizace $\mathcal{M}$ jazyka L budeme nazývat *ohodnocení proměnných*.

Je-li x proměnná, e ohodnocení proměnných a $m \in M$, potom ohodnocení proměnných, které proměnné x přiřazuje prvek m a pro všechny ostatní proměnné splývá s ohodnocením e, budeme značit $e(x/m)$.

Definice 4.3. *Hodnota termu* t v realizaci $\mathcal{M}$ jazyka L při daném ohodnocení e proměnných, označovaná $t[e]$, se definuje indukcí následovně:

(i) Je-li t proměnná x, potom $t[e]$ je $e(x)$,

(ii) je-li t term tvaru $f(t_1, \ldots, t_n)$, kde f je funkční symbol četnosti n a $t_1, \ldots, t_n$ jsou termy, potom $t[e]$ je $f_{\mathcal{M}}(t_1[e], \ldots, t_n[e])$.

Poznamenejme, že z (ii) plyne, že hodnotou konstanty je jí odpovídající vyznačený prvek z M.

Indukcí dle složitosti termu se ověří, že hodnota termu t závisí pouze na ohodnocení proměnných, které se v termu opravdu vyskytují. Hodnotou termu t s proměnnými $x_1, \ldots, x_n$ v prvcích $m_1, \ldots, m_n$ (tj. při ohodnocení splňujícím $e(x_1) = m_1, \ldots, e(x_n) = m_n$) je tedy jistý prvek z M, který získáme tak, že do termu t dosadíme prvky $m_1, \ldots, m_n$ za proměnné $x_1, \ldots, x_n$ a provedeme "naznačené"operace.

Definice 4.4. Nechť $\mathcal{M}$ je realizace jazyka L, nechť e je ohodnocení proměnných a nechť φ je formule jazyka L. Indukcí podle složitosti formule φ definujeme, co znamená, že *formule* φ *je pravdivá v* $\mathcal{M}$ *při ohodnocení* e . Tuto skutečnost budeme značit $\mathcal{M} \models \varphi[e]$.

(i) Je-li φ atomická formule tvaru $p(t_1, \ldots, t_n)$, kde p je predikátový symbol četnosti n a $t_1, \ldots, t_n$ jsou termy, pak $\mathcal{M} \models \varphi[e]$ právě když $(t_1[e], \ldots, t_n[e]) \in p_{\mathcal{M}}$.

(ii) Je-li φ atomická formule tvaru $t_1 = t_2$, kde t_1, t_2 jsou termy, pak $\mathcal{M} \models \varphi[e]$ právě když $t_1[e]$ je tentýž prvek jako $t_2[e]$ v M.

(iii) Je-li φ tvaru $\neg\psi$, kde ψ je formule jazyka L, pak $\mathcal{M} \models \varphi[e]$ právě když $\mathcal{M} \not\models \psi[e]$.

(iv) Je-li φ některého z tvarů $(\eta \wedge \psi), (\eta \vee \psi), (\eta \to \psi), (\eta \leftrightarrow \psi)$, kde η, ψ jsou formule, klademe:
$\mathcal{M} \models (\eta \wedge \psi)[e]$ právě když současně $\mathcal{M} \models \eta[e]$ a $\mathcal{M} \models \psi[e]$
$\mathcal{M} \models (\eta \vee \psi)[e]$ právě když platí alespoň jedno z $\mathcal{M} \models \eta[e]$ a $\mathcal{M} \models \psi[e]$ a podobně pro další logické spojky.

(v) Je-li φ tvaru $(\forall x\psi)$, kde ψ je formule jazyka L, pak $\mathcal{M} \models \varphi[e]$ právě když pro každý prvek $m \in M$ je $\mathcal{M} \models \psi[e(x/m)]$.

(vi) Je-li φ tvaru $(\exists x\psi)$, kde ψ je formule jazyka L, pak $\mathcal{M} \models \varphi[e]$ právě když existuje $m \in M$ takový, že $\mathcal{M} \models \psi[e(x/m)]$.

Indukcí dle složitosti formule lze ukázat, že pravdivost formule závisí pouze na ohodnocení jejích volných proměnných. Při zkoumání pravdivosti formule vystačíme s ohodnocením jen konečného počtu proměnných. Speciálně, pravdivost uzavřené formule v dané realizaci nezávisí na ohodnocení proměnných. Řekneme, že formule φ jazyka L je *splněna* v realizaci $\mathcal{M}$, jestliže φ je pravdivá v $\mathcal{M}$ při každém ohodnocení e. Pak píšeme $\mathcal{M} \models \varphi$. Je-li φ uzavřená formule, která je splněna v $\mathcal{M}$, říkáme, že φ je *pravdivá* v $\mathcal{M}$. Formule se nazývá *splnitelná*, je-li splněna v nějaké realizaci.

Definice 4.5. Řekneme, že formule φ jazyka L je *logicky platná*, jestliže pro každou realizaci $\mathcal{M}$ jazyka L je $\mathcal{M} \models \varphi$. Píšeme $\models \varphi$.

Příklad 4.2. Příklady logicky platných formulí:

1) Formule φ jazyka L, která vznikne tak, že do nějaké tautologie A výrokové logiky dosadíme za všechny prvotní formule $p_1, \ldots, p_n$ nějaké formule $\varphi_1, \ldots, \varphi_n$ jazyka L, je logicky platná formule jazyka L.

2) Pro libovolné formule φ a ψ jazyka L jsou zřejmě

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

$$(\exists x(\varphi \wedge \psi)) \to (\exists x\varphi) \wedge (\exists x\psi)$$

logicky platné formule jazyka L.

3) Jsou-li φ, ψ formule a je-li x proměnná, která nemá volný výskyt ve φ, pak je $(\forall x(\varphi \to \psi)) \to (\varphi \to (\forall x\psi))$ logicky platná formule. Nemá-li x volný výskyt ve ψ, je $(\forall x(\varphi \to \psi)) \to ((\exists x\varphi) \to \psi)$ logicky platná formule.

Naznačíme důkaz, že první formule z příkladu 3 je logicky platná. Máme ukázat, že v libovolné realizaci $\mathcal{M}$ při libovolném ohodnocení proměnných e je tato formule pravdivá.

- Jestliže $\mathcal{M} \not\models (\forall x(\varphi \to \psi))[e]$ jsme hotovi.
- Jestliže $\mathcal{M} \models (\forall x(\varphi \to \psi))[e]$, pak $\mathcal{M} \models (\varphi \to \psi)[e(x/m)]$ pro každé $m \in M$. Ovšem x není volná ve φ, takže pravdivost φ nezávisí na ohodnocení x.
  - Jestliže $\mathcal{M} \not\models \varphi[e]$, pak $\mathcal{M} \models (\varphi \to (\forall x\psi))[e]$ a jsme hotovi.
  - Jestliže $\mathcal{M} \models \varphi[e]$, pak $\mathcal{M} \models \varphi[e(x/m)]$ pro každé $m \in M$. Odtud $\mathcal{M} \models \psi[e(x/m)]$ pro každé $m \in M$, což znamená $\mathcal{M} \models (\forall x\psi)[e]$. Takže i v tomto případě máme $\mathcal{M} \models (\varphi \to (\forall x\psi)[e]$.

Definice 4.6. Řekneme, že formule φ, ψ jazyka L jsou *logicky ekvivalentní*, jestliže v libovolné realizaci $\mathcal{M}$ jazyka L a při libovolném ohodnocení e proměnných je $\mathcal{M} \models \varphi[e]$ právě tehdy, když $\mathcal{M} \models \psi[e]$.

Zřejmě formule φ, ψ jsou logicky ekvivalentní, právě když $(\varphi \leftrightarrow \psi)$ je logicky platná formule.

Příklad 4.3. Příklad dvojic logicky ekvivalentních formulí pro libovolné formule φ, ψ a proměnnou x jsou

$$\begin{array}{rcl} (\exists x\varphi) & \text{a} & \neg(\forall x(\neg\varphi)), \\ (\forall x\varphi) & \text{a} & \neg(\exists x(\neg\varphi)), \\ (\forall x\varphi) \wedge (\forall x\psi) & \text{a} & \forall x(\varphi \wedge \psi), \\ (\exists x\varphi) \vee (\exists x\psi) & \text{a} & \exists x(\varphi \vee \psi). \end{array}$$

Důsledek 4.1. *Každá formule φ jazyka L je logicky ekvivalentní nějaké formuli ψ, v níž se nevyskytuje kvantifikátor $\exists$ (totéž platí i pro $\forall$).*

Každá formule jazyka L je logicky ekvivalentní nějaké formuli vytvořené z atomických formulí jen pomocí logických spojek $\neg, \rightarrow$ a kvantifikátoru $\forall$.

4.1 Substituce termů za proměnné

Je-li t term, pak výraz, který vznikne dosazením nějakých termů za proměnné do t je opět term.

Je-li φ formule, x proměnná, t term, potom výraz, který vznikne z formule φ nahrazením každého volného výskytu proměnné x termem t, je opět formule.

Ne každá substituce tohoto druhu je rozumná. Řekneme, že term t je *substituovatelný* za x do formule φ, jestliže žádný volný výskyt proměnné x ve formuli φ neleží v oboru některého kvantifikátoru $\forall y$ nebo $\exists y$, kde y je proměnná obsažená v termu t. Pak budeme značit $\varphi_x[t]$ formuli, která vznikne z φ nahrazením každého volného výskytu x termem t.

Příklad 4.4. V jazyce elementární aritmetiky term $S(S(y))$ není substituovatelný za x do formule $x \neq 0 \rightarrow \exists y(x = S(y))$.

Obecněji, je-li t_i term substituovatelný za proměnnou x_i do formule φ pro $i = 1 \ldots n$, pak budeme značit $\varphi_{x_1,\ldots,x_n}[t_1, \ldots, t_n]$ formuli, která vznikne z formule φ nahrazením každého volného výskytu proměnné x_i termem t_i pro $i = 1 \ldots n$. Formule $\varphi_{x_1,\ldots,x_n}[t_1, \ldots, t_n]$ se nazývá *instance* formule φ.

Tvrzení 4.2. *Je-li φ formule, x proměnná a t term substituovatelný za x do φ, pak $(\forall x\varphi) \rightarrow \varphi_x[t]$; $\varphi_x[t] \rightarrow \exists x\varphi$ jsou logicky platné formule.*

Důkaz: Pro první formuli: nechť $\mathcal{M}$ je libovolná realizace a nechť e je libovolné ohodnocení proměnných.
Jestliže $\mathcal{M} \not\models (\forall x\varphi)[e]$, pak $\mathcal{M} \models ((\forall x\varphi \rightarrow \varphi_x[t])[e]$.
Jestliže $\mathcal{M} \models (\forall x\varphi)[e]$, pak $\mathcal{M} \models \varphi[e(x/m)]$ pro každé $m \in M$. Pro $m = t[e]$ (hodnota termu t při ohodnocení e) je ale $\mathcal{M} \models \varphi[e(x/m)]$ totéž, co $\mathcal{M} \models (\varphi_x[t])[e]$ neboť term t je substituovatelný za x do φ. Takže máme $\mathcal{M} \models (\varphi_x[t])[e]$, a tedy $\mathcal{M} \models ((\forall x\varphi) \rightarrow \varphi_x[t])[e]$.

□

5 Formální systém predikátové logiky

Budujeme predikátovou logiku jako formální axiomatický systém. Jazyk L predikátové logiky přebíráme z předchozího s tím, že z logických spojek bereme jako základní $\neg$ a $\rightarrow$ (ostatní mohou být dodefinovány jako ve výrokovém počtu). Z kvantifikátorů bereme jako základní $\forall$, kvantifikátor $\exists$ je možno zavést takto: Je-li φ formule, pak $\exists x\varphi$ je zkratka pro $\neg(\forall x(\neg\varphi))$. Omezíme se tedy pouze na ty formule, které jsou vytvořeny z atomických formulí jen pomocí spojek $\neg, \rightarrow$ a kvantifikátoru $\forall$. Axiomy predikátové logiky lze rozdělit do čtyř skupin.

5.1 Schémata výrokových axiomů

Jsou-li φ, ψ, η formule jazyka L, pak

$$\varphi \rightarrow (\psi \rightarrow \varphi)$$

$$(\varphi \rightarrow (\psi \rightarrow \eta)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \eta))$$

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

jsou axiomy predikátové logiky.

5.2 Schéma axiomu kvantifikátoru

Jsou-li φ, ψ formule a je-li x proměnná, která nemá volný výskyt ve formuli φ, pak

$$(\forall x(\varphi \rightarrow \psi)) \rightarrow (\varphi \rightarrow (\forall x\psi))$$

je axiom predikátové logiky.
Předpoklad, že x nemá volný výskyt ve formuli φ, je podstatný, jak je zřejmé z následujícího příkladu:
Je-li $\varphi = p(x), \psi = p(x)$, pak x je volná ve φ. Axiom pak dává

$$(\forall x(p(x) \rightarrow p(x))) \rightarrow (p(x) \rightarrow (\forall x p(x))).$$

Je-li $\mathcal{M}$ taková realizace, že vlastnost p má aspoň jeden prvek a aspoň jeden prvek ji nemá, pak je implikace nepravdivá.

5.3 Schéma axiomu substituce

Je-li φ formule, x proměnná a t term substituovatelný za x do φ, pak

$$(\forall x\varphi) \rightarrow \varphi_x[t]$$

je axiom predikátové logiky. Předpoklad, že t je substituovatelný za x ve formuli φ, je podstatný, jak je zřejmé z následujícího příkladu:
Je-li $\varphi = \neg\forall y p(x, y), t = y$ (takže t není substituovatelný za x do φ), $cardM \geq 2$

a p je symbol rovnosti, pak axiom dává $(\forall x(\neg\forall y(x = y))) \to (\neg\forall y(y = y))$, což je zřejmě nepravdivá formule.

Jestliže $t = x$, pak schéma axiomu substituce má tvar

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

neboť $\varphi_x[x]$ je φ.

Je-li L jazyk s rovností, máme ještě následující skupinu axiomů:

5.4 Schémata axiomů rovnosti

Je-li x proměnná, pak $x = x$ je axiom. Jsou-li $x_1, \ldots, x_n, y_1, \ldots, y_n$ proměnné a je-li f funkční symbol četnosti n, pak

$$(x_1 = y_1 \to (x_2 = y_2 \to (\ldots (x_n = y_n \to f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)) \ldots))$$

je axiom. Jsou-li $x_1, \ldots, x_n, y_1, \ldots, y_n$ proměnné, je-li p predikátový symbol četnosti n, pak

$$(x_1 = y_1 \to (x_2 = y_2 \to (\ldots (x_n = y_n \to (p(x_1, \ldots, x_n) \to p(y_1, \ldots, y_n)) \ldots))$$

je axiom.

5.5 Odvozovací pravidla predikátové logiky

Pravidlo odloučení (modus ponens): Z formulí $\varphi, \varphi \to \psi$ se odvodí formule ψ.

Pravidlo zobecnění (generalizace): Pro libovolnou proměnnou x se z formule φ odvodí formule $(\forall x\varphi)$.

Důkazem v predikátové logice prvního řádu rozumíme libovolnou posloupnost $\varphi_1, \ldots, \varphi_n$ formulí jazyka L, v níž pro každý index i je formule φ_i buď axiom predikátové logiky nebo ji lze odvodit z některých předchozích formulí $\varphi_j, j < i$ použitím pravidla odloučení nebo zobecnění.

Řekneme, že formule φ je *dokazatelná* v predikátové logice 1. řádu, existuje-li důkaz, jehož poslední formulí je φ. Píšeme $\vdash \varphi$. Obecněji, buď T množina formulí jazyka L. Řekneme, že formule φ je *dokazatelná z předpokladů* T, jestliže existuje její důkaz z předpokladů T, tj. konečná posloupnost formulí jazyka L taková, že poslední formule je φ a každá formule v této posloupnosti je buď axiom predikátové logiky nebo prvek množiny T nebo ji lze odvodit z některých předchozích formulí užitím odvozovacích pravidel. Pak píšeme $T \vdash \varphi$.

Poznámka 5.1. a) Spolu se schematy výrokových axiomů a pravidlem odloučení přechází do predikátové logiky celá výroková logika. Je-li zejména A tautologie výrokové logiky a je-li φ formule jazyka L vzniklá dosazením formulí jazyka L za prvotní formule A, pak $\vdash \varphi$.

b) Jestliže formule φ je dokazatelná z předpokladů T jen použitím prostředků výrokové logiky, tj. jen pomocí formulí vzniklých dosazením do tautologií a použitím pravidla odloučení, říkáme, že φ je *tautologickým důsledkem* T. Tak např. formule $\neg\psi \to \neg\varphi$ je tautologickým důsledkem formule $\varphi \to \psi$. Skutečně, formuli $(\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$ obdržíme dosazením do tautologie $(A \to B) \to (\neg B \to \neg A)$. Stačí použít pravidlo odloučení. Podobně, složením implikací $\varphi \to \psi$ a $\psi \to \eta$ dostaneme formuli $\varphi \to \eta$ jako jejich tautologický důsledek. Skutečně, formuli $(\varphi \to \psi) \to ((\psi \to \eta) \to (\varphi \to \eta))$ obdržíme dosazením do tautologie, stačí užít dvakrát pravidlo odloučení.

Věta 5.2. (O korektnosti) *Libovolná formule jazyka L dokazatelná v predikátové logice 1. řádu je logicky platnou formulí, tj. je splněna v každé realizaci jazyka L.*

Důkaz: Nechť $\varphi_1, \ldots, \varphi_n$ je důkaz formule φ. Buď $\mathcal{M}$ libovolná realizace jazyka L. Abychom ukázali, že $\mathcal{M} \models \varphi$, ukážeme indukcí, že $\mathcal{M} \models \varphi_i$ pro každé $i = 1 \ldots n$. Předpokládejme tedy, že $\mathcal{M} \models \varphi_j$ pro $j = 1, \ldots, i-1$.

- Je-li φ_i výrokový axiom, je to zřejmé.
- Je-li φ_i axiom kvantifikátoru, pak viz. příklad 3 na straně 18.
- Je-li φ_i axiom substituce, pak viz tvrzení 4.2 na straně 19.
- Zřejmý je i případ axiomů rovnosti.
- Vznikla-li formule φ_i pravidlem odloučení z některých předchozích formulí $\varphi_j, \varphi_j \to \varphi_i$ pak $\mathcal{M} \models \varphi_j$, $\mathcal{M} \models \varphi_j \to \varphi_i$ podle indukčního předpokladu, čili pro libovolné ohodnocení proměnných e je $\mathcal{M} \models \varphi_j[e], \mathcal{M} \models (\varphi_j \to \varphi_i)[e]$, odkud ihned $\mathcal{M} \models \varphi_i[e]$, takže celkem $\mathcal{M} \models \varphi_i$.
- Jestliže φ_i vznikla z některé předchozí formule φ_j pravidlem zobecnění, pak φ_i je tvaru $(\forall x \varphi_j)$ pro nějakou proměnnou x a dle indukčního předpokladu $\mathcal{M} \models \varphi_j$. Je-li tedy e libovolné ohodnocení proměnných, pak $\mathcal{M} \models \varphi_j[e(x/m)]$ platí pro každý prvek m univerza realizace $\mathcal{M}$, takže $\mathcal{M} \models (\forall x \varphi_j)[e]$. Odtud $\mathcal{M} \models (\forall x \varphi_j)$, tj. je $\mathcal{M} \models \varphi_i$.

□

V následující kapitole dokážeme opak věty 5.2. Ukážeme tak, že formální systém predikátové logiky je úplný, tj., že formule dokazatelné v predikátové logice jsou právě logicky platné formule. Za tímto účelem nyní vybudujeme potřebné prostředky.

Lemma 5.3. (Pravidlo $\forall$) *Je-li $\vdash \varphi \to \psi$ a proměnná x nemá volný výskyt ve φ, pak $\vdash \varphi \to (\forall x \psi)$.*

Důkaz: Užitím pravidla zobecnění $\vdash \forall x(\varphi \to \psi)$. $\vdash (\forall x(\varphi \to \psi)) \to (\varphi \to (\forall x \psi))$ je axiom kvantifikátoru. Odtud užitím pravidla odloučení: $\vdash \varphi \to (\forall x \psi)$.

□

Lemma 5.4. (Pravidlo ∃) *Je-li* $\vdash \varphi \to \psi$ *a proměnná* x *nemá volný výskyt v* ψ, *pak* $\vdash (\exists x\varphi) \to \psi$.

Důkaz: $\neg\psi \to \neg\varphi$ je tautologický důsledek implikace $\varphi \to \psi$. Užitím pravidla $\forall$ dostaneme $\vdash \neg\psi \to (\forall x(\neg\varphi))$. Formule $\neg(\forall x(\neg\varphi)) \to \psi$ je nyní tautologický důsledek předchozí formule a můžeme ji přepsat na tvar $\vdash (\exists x\varphi) \to \psi$ dle definice zkratky ∃.

□

Pravidlo ∃ je duální pravidlu ∀.

Lemma 5.5. *Je-li* φ *formule,* x *proměnná,* t *term substituovatelný za* x *do* φ, *pak* $\vdash \varphi_x[t] \to (\exists x\varphi)$.

Důkaz: $\vdash (\forall x(\neg\varphi)) \to (\neg\varphi_x[t])$ je axiom substituce.
$\vdash \neg\neg(\forall x(\neg\varphi)) \to (\forall x(\neg\varphi)))$ dosazením do tautologie $\neg\neg A \to A$.
Složením obou implikací jako tautologický důsledek dostaneme
$\vdash \neg\neg(\forall x(\neg\varphi)) \to (\neg\varphi_x[t])$, což je
$\vdash \neg(\exists x\varphi) \to (\neg\varphi_x[t])$, odtud
$\vdash \varphi_x[t] \to (\exists x\varphi)$ jako tautologický důsledek.

□

Lemma 5.6. *Nechť* φ' *je instancí formule* φ, *tj. nechť* φ' *je tvaru* $\varphi_{x_1,\ldots,x_n}[t_1,\ldots,t_n]$ *pro nějaké termy* $t_1,\ldots,t_n$ *substituovatelné za* $x_1,\ldots,x_n$ *do* φ. *Jestliže* $\vdash \varphi$, *pak* $\vdash \varphi'$.

Důkaz: Jestliže $n = 1$, pak φ' je tvaru $\varphi_x[t]$. Z $\vdash \varphi$ pravidlem zobecnění $\vdash (\forall x\varphi)$. Dále (použijeme axiom substituce:) $\vdash (\forall x\varphi) \to \varphi_x[t]$ a pravidlem odloučení dostáváme $\vdash \varphi_x[t]$, tj. $\vdash \varphi'$. Jestliže $n > 1$, je nutno nejprve přeznačit proměnné. Nechť $z_1,\ldots,z_n$ jsou proměnné, které se nevyskytují v $t_1,\ldots,t_n$ ani ve formuli φ. Podobně jako výše postupně dostaneme: $\vdash \varphi_{x_1}[z_1]$, $\vdash \varphi_{x_1,x_2}[z_1,z_2],\ldots$ $\vdash \varphi_{x_1,\ldots,x_n}[z_1,\ldots,z_n]$. Označme poslední formuli ψ. Poněvadž proměnné $z_1,\ldots,z_n$ se nevyskytují v termech $t_1,\ldots,t_n$, dostáváme postupnou substitucí t_1 za z_1, pak t_2 za z_2, až t_n za z_n postupně formule $\psi_{z_1}[t_1]$, $\psi_{z_1,z_2}[t_1,t_2]$ až $\psi_{z_1,\ldots,z_n}[t_1,\ldots,t_n]$. Přitom podobně jako výše postupně odvodíme $\vdash \psi_{z_1}[t_1], \vdash \psi_{z_1,z_2}[t_1,t_2],\ldots,\vdash \psi_{z_1,\ldots,z_n}[t_1,\ldots,t_n]$. Poslední formule je totožná s $\varphi_{x_1,\ldots,x_n}[t_1,\ldots,t_n]$, tj. s φ'.

□

Poznamenejme, že důkaz předchozího lemmatu pro $n > 1$ nelze provádět n-násobným opakováním postupu, který byl užit v důkazu pro $n = 1$, neboť obecně formule $\varphi_{x_1,\ldots,x_n}[t_1,\ldots,t_n]$ a $(\ldots((\varphi_{x_1}[t_1])_{x_2}[t_2])\ldots)_{x_n}[t_n]$ jsou různé, jak je ukázáno

v následujícím příkladu: Nechť φ je formule $x < y$ a nechť $t = y$ a $s = x$. Pak $\varphi_{x,y}[t, s]$ je formule $y < x$, zatímco $(\varphi_x[t])_y[s]$ je formule $(y < y)_y[s]$, tj. formule $x < x$.

Je-li nyní φ libovolná formule a $x_1, \ldots, x_n$ proměnné, pak z axiomu substituce postupně dostáváme
$\vdash (\forall x_n \varphi) \to \varphi$,
$\vdash (\forall x_{n-1} \forall x_n \varphi) \to (\forall x_n \varphi)$,
$\vdots$
$\vdash (\forall x_1 \forall x_2 \ldots \forall x_n \varphi) \to (\forall x_2 \ldots \forall x_n \varphi)$.
Odtud složením jako tautologický důsledek plyne: $\vdash (\forall x_1 \ldots \forall x_n \varphi) \to \varphi$.
Je-li nyní π libovolná permutace na množině indexů $\{1, \ldots, n\}$, pak n-násobným užitím pravidla $\forall$ odtud odvodíme $\vdash (\forall x_1 \ldots \forall x_n \varphi) \to (\forall x_{\pi_1} \ldots \forall x_{\pi_n} \varphi)$. Analogicky se odvodí i opačná implikace. Nezáleží tedy na pořadí v bloku stejných kvantifikátorů. To ospravedlňuje následující definici.

Definice 5.1. Jsou-li $x_1, \ldots, x_n$ všechny volné proměnné ve formuli φ v nějakém pořadí, pak formuli $(\forall x_1 \ldots \forall x_n \varphi)$ nazveme *uzávěrem formule* φ.

Věta 5.7. (O uzávěru) *Je-li T množina formulí a φ' uzávěr formule φ, pak $T \vdash \varphi$ právě když $T \vdash \varphi'$.*

Důkaz: Je-li $T \vdash \varphi$, pak užitím pravidla zobecnění dostaneme $T \vdash \varphi'$.
Je-li $T \vdash \varphi'$, podle předchozí úvahy máme $\vdash \varphi' \to \varphi$. Odtud pravidlem odloučení odvodíme $T \vdash \varphi$.

□

Lemma 5.8. (Distribuce kvantifikátorů) *Je-li $\vdash \varphi \to \psi$, potom $\vdash (\forall x \varphi) \to (\forall x \psi)$, $\vdash (\exists x \varphi) \to (\exists x \psi)$*

Důkaz: Nejprve $\vdash (\forall x \varphi) \to \varphi$ podle axiomu substituce. $\vdash (\forall x \varphi) \to \psi$ je tautologický důsledek předchozí formule a předpokladu $\vdash \varphi \to \psi$. Tedy užitím pravidla $\forall$ dostáváme $\vdash (\forall x \varphi) \to (\forall x \psi)$. Podle lemmatu 5.5 máme $\vdash \psi \to (\exists x \psi)$. Formule $\vdash \varphi \to (\exists x \psi)$ je nyní tautologický důsledek předpokladu $\vdash \varphi \to \psi$ a předchozí formule (jejich složení). Takže užitím pravidla $\exists$ dostáváme $\vdash (\exists x \varphi) \to (\exists x \psi)$.

□

Větu o dedukci z výrokové logiky nelze beze změny převést do predikátové logiky.

Věta 5.9. (O dedukci) *Nechť T je množina formulí jazyka L, nechť φ je uzavřená formule, ψ je libovolná formule jazyka L. Potom $T \vdash \varphi \to \psi$, právě když $T, \varphi \vdash \psi$.*

Důkaz: Je naprosto analogický jako ve výrokové logice. Pouze v důkazu toho, že $T, \varphi \vdash \psi$ má za následek $T \vdash \varphi \to \psi$, je nutno uvážit navíc jednu možnost.

Nechť $\varphi_1, \ldots, \varphi_n$ je důkaz formule ψ z předpokladů T, φ. Dokazujeme indukcí pro $j \leq n$, že $T \vdash \varphi \to \varphi_j$. Navíc je nutno uvažovat případ, kdy formule φ_j vznikla z některé formule φ_i, $i < j$, pravidlem zobecnění. Tedy φ_j je tvaru $\forall x \varphi_i$ pro některou proměnnou x. Z indukčního předpokladu máme $T \vdash \varphi \to \varphi_i$. Poněvadž φ je uzavřená formule, neobsahuje volný výskyt proměnné x, takže pravidlem $\forall$ dostaneme $T \vdash \varphi \to (\forall x \varphi_i)$, to jest $T \vdash \varphi \to \varphi_j$. Věta je dokázána.

□

Následující věta umožní řešit některé případy, na které nelze aplikovat větu o dedukci.

Věta 5.10. (O konstantách) *Nechť T je množina formulí jazyka L, nechť φ je formule. Nechť $x_1, \ldots, x_n$ jsou proměnné a nechť $c_1, \ldots, c_n$ jsou nové konstanty, jejichž přidáním k L vznikne jazyk L'. Potom $T \vdash \varphi_{x_1,\ldots,x_n}[c_1, \ldots, c_n]$, právě když $T \vdash \varphi$.*

Důkaz: Je-li $T \vdash \varphi$, potom $T \vdash \varphi_{x_1,\ldots,x_n}[c_1, \ldots, c_n]$ podle lemmatu 5.6.
Nechť $T \vdash \varphi_{x_1,\ldots,x_n}[c_1, \ldots, c_n]$ a nechť $\varphi'_1, \ldots, \varphi'_m$ je důkaz formule $\varphi_{x_1,\ldots,x_n}[c_1, \ldots, c_n]$ z předpokladu T. Nechť $y_1, \ldots, y_n$ jsou proměnné, které se nikde v tomto důkazu ani ve formuli φ nevyskytují. Nahradíme-li ve všech formulích $\varphi'_1, \ldots, \varphi'_m$ každý výskyt konstanty c_i proměnnou y_i pro $i = 1, \ldots, n$, obdržíme tak zřejmě důkaz $\varphi_1, \ldots, \varphi_m$ formule $\varphi_{x_1,\ldots,x_n}[y_1, \ldots, y_n]$ z předpokladů T. Skutečně, každý axiom v důkazu přejde v axiom téhož typu, odvozovací pravidla budou použitelná stejně (tj. bude to důkaz). Formule φ je instancí formule $\varphi_{x_1,\ldots,x_n}[y_1, \ldots, y_n]$. Tedy $T \vdash \varphi$ podle lemmatu 5.6.

□

Odvodíme nyní několik důsledků axiomů rovnosti. První axiom rovnosti vyjadřuje reflexivitu rovnosti. Ukážeme, že rovnost splňuje i symetrii a tranzitivitu.

Lemma 5.11. *Je-li L jazyk s rovností, pak*

$$\vdash x = y \to y = x$$

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

Důkaz: Použijeme třetí axiom rovnosti, v němž jako predikátový symbol p vezmeme predikát rovnosti $=$. Takto máme $\vdash x = y \to (x = x \to (x = x \to y = x))$, odtud užitím postupů výrokové logiky $\vdash x = x \to (x = x \to (x = y \to y = x))$, což spolu s prvním axiomem rovnosti (tj. $x = x$) užitím pravidla odloučení (2x) dává symetrii rovnosti. Podobně podle třetího axiomu rovnosti máme $\vdash y = x \to (z = z \to (y = z \to x = z))$. Odtud užitím postupů výrokové logiky dostáváme

$\vdash z = z \to (y = x \to (y = z \to x = z))$ a nyní s použitím prvního axiomu rovnosti a pravidla odloučení obdržíme $\vdash y = x \to (y = z \to x = z)$. Složením této implikace se symetrií rovnosti vychází jako tautologický důsledek tranzitivita rovnosti.

□

Lemma 5.12. *Je-li f funkční symbol četnosti n, je-li p predikátový symbol četnosti m jazyka L a jsou-li $u, v, w, s_1, \ldots, s_n, t_1, \ldots, t_n$ termy jazyka L, pak*

(i) $\vdash u = u$

(ii) $\vdash u = v \to v = u$

(iii) $\vdash u = v \to (v = w \to u = w)$

(iv) $\vdash s_1 = t_1 \to (s_2 = t_2 \to \ldots (s_n = t_n \to f(s_1, \ldots, s_n) = f(t_1, \ldots, t_n)) \ldots)$

(v) $\vdash s_1 = t_1 \to (s_2 = t_2 \to \ldots (s_n = t_n \to (p(s_1, \ldots, s_n) \to p(t_1, \ldots, t_n)) \ldots)$

Důkaz: Uvedené formule jsou instancemi axiomů rovnosti a formulí v lemmatu 5.11. Stačí tedy užít lemma 5.6

□

Poznámka 5.13. Buď φ formule jazyka L, tj. formule, v níž se vyskytují pouze logické spojky $\neg, \to$ a kvantifikátor $\forall$. Nechť φ' je formule, která vznikne z formule φ rozepsáním spojky $\to$ a kvantifikátoru $\forall$, takže se v ní vyskytují pouze $\neg, \wedge, \exists$. (Spojka $\psi \to \eta$ se rozepíše $\neg(\psi \wedge \neg\eta)$, kvantifikátor $(\forall x\psi)$ se rozepíše $\neg(\exists x(\neg\psi))$). Nechť $\overline{\varphi}$ je formule, která vznikne rozepsáním φ' tak, že se v ní spojka $\wedge$ a kvantifikátor $\exists$ chápou jako zkratky obvyklým způsobem, takže vznikne opět formule obsahující jen logické spojky $\neg, \to$ a kvantifikátor $\forall$. Pak platí $\vdash \varphi \leftrightarrow \overline{\varphi}$, tj. platí $\vdash \varphi \to \overline{\varphi}$ a $\vdash \overline{\varphi} \to \varphi$. Důkaz lze provést indukcí vzhledem ke složitosti formule φ s využitím prostředků výrokové logiky a distribuce kvantifikátorů (lemma 5.8).

6 Prenexní tvary formulí

Soustředíme se na to, abychom dokázali, že existuje základní tvar formulí predikátové logiky a prostředky, jak libovolnou formuli převést do tohoto tvaru.

Připomeňme, že z úvah prováděných v 5. kapitole vyplývá:

Lemma 6.1. *Buď $i_1, \ldots, i_n$ libovolná permutace čísel $\{1, \ldots, n\}$. Nechť $x_1, \ldots, x_n$ jsou proměnné a A formule predikátové logiky. Pak platí:*

a) $\vdash (\forall x_1) \ldots (\forall x_n)A \leftrightarrow (\forall x_{i_1}) \ldots (\forall x_{i_n})A$,

b) $\vdash (\exists x_1) \ldots (\exists x_n)A \leftrightarrow (\exists x_{i_1}) \ldots (\exists x_{i_n})A$.

Z věty 5.7 (o uzávěru) ihned dostáváme:

Věta 6.2. *Buď A formule taková, že proměnné $x_1, \ldots, x_n$ jsou jediné proměnné s volným výskytem v A. Pak $\vdash A$, právě když $\vdash \forall x_1 \ldots \forall x_n A$.*

Budeme potřebovat ještě následující tvrzení:

Věta 6.3. (O ekvivalenci) *Nechť formule A' vznikne z formule A nahrazením některých výskytů podformulí $B_1, \ldots, B_n$ po řadě formulemi $B'_1, \ldots, B'_n$. Je-li $\vdash B_i \leftrightarrow B'_i$ pro všechna $i = 1, \ldots, n$, pak platí $\vdash A \leftrightarrow A'$.*

Důkaz: (Indukcí vzhledem ke složitosti formule A.) Mohou nastat následující 4 případy:

a) A je atomická formule. Potom buď A' je A (pokud k nahrazení nedojde) nebo A' je B'_1 (pokud A je B_1). Tedy tvrzení plyne z lemmatu 2.2 nebo z předpokladů věty.

b) A je tvaru $\neg B$ a pro B bylo již tvrzení dokázáno. Tedy $\vdash B \leftrightarrow B'$, takže $\vdash B \to B'$ a užitím lemmatu 2.4(d) dostáváme $\vdash \neg B' \to \neg B$, tj. $\vdash A' \to A$. Podobně se ukáže $\vdash A \to A'$.

c) A je tvaru $B \to C$ a pro formule B a C již bylo tvrzení dokázáno, tj. $\vdash B \leftrightarrow B'$ a $\vdash C \leftrightarrow C'$. Tedy $\vdash B' \to B$ a $\vdash C \to C'$. Dále máme $\vdash (B' \to B) \to ((B \to C) \to (B' \to C))$ a $\vdash (B' \to C) \to ((C \to C') \to (B' \to C'))$ (obě formule jsou zřejmě tautologie), takže složením dostáváme $\vdash (B' \to B) \to ((B \to C) \to ((C \to C') \to (B' \to C')))$. Odtud $\vdash (B' \to B) \to ((C \to C') \to ((B \to C) \to (B' \to C')))$ a po dvojím užití pravidla modus ponens máme $\vdash (B \to C) \to (B' \to C')$, tj. $\vdash A \to A'$. Analogicky dokážeme opačnou implikaci.

d) A je tvaru $\forall x B$ a pro B bylo již tvrzení dokázáno. Potom A' je tvaru $\forall x B'$ a z indukčního předpokladu pro formuli B dostáváme $\vdash B \leftrightarrow B'$. Tedy $\vdash B \to B'$ a $\vdash B' \to B$, takže máme $\vdash A \to A'$ a $\vdash A' \to A$ podle lemmatu 5.8 (distribuce kvantifikátorů). Odtud plyne tvrzení věty jako tautologický důsledek.

□

Věta o ekvivalenci nás teoreticky vybavila možností upravit formule predikátové logiky podle momentálních potřeb na ekvivalentní tvar, který dává čitelnější a přehlednější zápis nebo ve kterém je rozsah platnosti kvantifikátorů v podformulích buď minimalizován nebo naopak ve kterém mají všechny kvantifikátory co největší rozsah. Praktickým prostředkem k takovým úpravám jsou ekvivalence mezi formulemi uvedené v následující větě, kterým se často zkráceně říká *prenexní operace*, protože se výrazně uplatňují při převodu formulí do tzv. prenexního tvaru.

Věta 6.4. *Buďte A,B formule a x proměnná. Pak*

$$(1) \quad \vdash (\exists x)\neg A \leftrightarrow \neg(\forall x)A \text{ a podobně } \vdash (\forall x)\neg A \leftrightarrow \neg(\exists x)A.$$

Jestliže x není volná ve formuli A a $\circ$ značí některou z výrokových spojek $\wedge, \vee, \rightarrow$, pak platí:

$$(2) \quad \vdash \forall x(A \circ B) \leftrightarrow (A \circ \forall x B) \text{ a podobně } \vdash \exists x(A \circ B) \leftrightarrow (A \circ \exists x B);$$

pro opačnou implikaci $B \rightarrow A$ platí:

$$(3) \quad \vdash \forall x(B \rightarrow A) \leftrightarrow (\exists x B \rightarrow A) \text{ a podobně } \vdash \exists x(B \rightarrow A) \leftrightarrow (\forall x B \rightarrow A).$$

Důkaz: (1) Protože formule A a $\neg\neg A$ jsou ekvivalentní, máme

$$\vdash \neg(\forall x)A \leftrightarrow \neg(\forall x)\neg\neg A.$$

Formuli na pravé straně lze psát ve tvaru $(\exists x)\neg A$.
Předpokládejme dále, že x není volná ve formuli A.

(2) Formule $A \rightarrow B$ vznikne složením implikací $A \rightarrow (\forall x)B$ a $(\forall x)B \rightarrow B$. Tedy implikace $((\forall x)B \rightarrow B) \rightarrow ((A \rightarrow (\forall x)B) \rightarrow (A \rightarrow B))$ je tautologickým důsledkem předchozích tří formulí. Protože formule $(\forall x)B \rightarrow B$ je axiom (substituce), užitím pravidla modus ponens odvodíme $\vdash (A \rightarrow (\forall x)B) \rightarrow (A \rightarrow B)$. Odtud pravidlem $\forall$ dostaneme $\vdash (A \rightarrow (\forall x)B) \rightarrow (\forall x)(A \rightarrow B)$ (jelikož formule v antecedentu implikace nemá volný výskyt proměnné x). Protože opačná implikace je axiomem, je pro případ, kdy $\circ$ je spojka $\rightarrow$, tvrzení $\vdash \forall x(A \circ B) \leftrightarrow (A \circ \forall x B)$ dokázáno. Dokážeme pro tento případ i druhé tvrzení. Podle lemmatu 5.5 máme

$$\vdash B \rightarrow (\exists x)B.$$

Dále máme

$$\vdash (B \rightarrow (\exists x)B) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow (\exists x)B)),$$

neboť formule vznikla dosazením do tautologie. Z posledních dvou formulí pravidlem modus ponens odvodíme

$$\vdash (A \rightarrow B) \rightarrow (A \rightarrow (\exists x)B)$$

a odtud dostaneme

$$\vdash (\exists x)(A \rightarrow B) \rightarrow (A \rightarrow (\exists x)B)$$

užitím pravidla $\forall$ (neboť formule $A \rightarrow (\exists x)B$ neobsahuje volně proměnnou x). K důkazu obrácené implikace nejprve odvodíme $\vdash (\exists x)B \rightarrow (\exists x)(A \rightarrow B)$ distribucí kvantifikátoru $\exists$ z prvního axiomu výrokové logiky. Dále dostaneme $\vdash (A \rightarrow B) \rightarrow (\exists x)(A \rightarrow B)$ podle lemmatu 5.5. Složením této formule s tautologií $\neg A \rightarrow (A \rightarrow B)$ dostaneme $\vdash \neg A \rightarrow (\exists x)(A \rightarrow B)$ jako jejich tautologický důsledek. Nyní dosadíme A, $(\exists x)B$, $(\exists x)(A \rightarrow B)$ postupně za D, E, F do tautologie

$$(\neg D \rightarrow F) \rightarrow ((E \rightarrow F) \rightarrow ((D \rightarrow E) \rightarrow F))$$

a pak pravidlem modus ponens pomocí odvozených formulí $(\exists x)B \rightarrow (\exists x)(A \rightarrow B)$ a $\vdash \neg A \rightarrow (\exists x)(A \rightarrow B)$ dostaneme

$$\vdash (A \rightarrow (\exists x)B) \rightarrow (\exists x)(A \rightarrow B).$$

Tím jsou obě tvrzení (2) pro případ, kdy $\circ$ je spojka $\rightarrow$, dokázána.

(3) Platí

$$\vdash ((\forall x)B \rightarrow A) \leftrightarrow (\neg A \rightarrow \neg(\forall x)B),$$

neboť formule vznikla dosazením do tautologie. Ovšem

$$\vdash (\neg A \rightarrow \neg(\forall x)B) \leftrightarrow (\neg A \rightarrow \neg(\forall x)\neg\neg B)$$

podle věty o ekvivalenci, tedy

$$\vdash (\neg A \rightarrow \neg(\forall x)\neg\neg B) \leftrightarrow (\neg A \rightarrow (\exists x)\neg B).$$

Dále, podle dokázaného tvrzení (2) máme

$$\vdash (\neg A \rightarrow (\exists x)\neg B) \leftrightarrow (\exists x)(\neg A \rightarrow \neg B).$$

Konečně, věta o ekvivalenci dává

$$\vdash (\exists x)(\neg C \rightarrow \neg B) \leftrightarrow (\exists x)(B \rightarrow C).$$

Složením předchozích ekvivalencí dostaneme první z obou tvrzení (3). Druhé tvrzení se dokáže analogicky.

Zbývá dokázat tvrzení (2) po případ, kdy $\circ$ je spojka $\wedge$ nebo $\vee$. To se snadno provede rozepsáním příslušné spojky pomocí negace a implikace a užitím již dokázaných tvrzení (1)-(3).

□

Z různých oblastí matematiky jsme zvyklí nepovažovat za rozdílné formule lišící se jen ve jménu vázané proměnné, např. $\forall x(x^2 + y^2 > 0)$ a $\forall z(z^2 + y^2 > 0)$ představují totéž tvrzení. Proto zavádíme následující definice.

Definice 6.1. Nechť A je formule predikátové logiky. Formule A' je *variantou* formule A, jestliže vznikne z A postupným nahrazením podformulí tvaru $(Qx)B$ podformulemi $(Qy)B_x[y]$, kde Q je obecný nebo existenční kvantifikátor a y je proměnná, která není volná v B.

Příklad 6.1. Uvažujme formuli $\forall x\exists y(x \neq y)$. Pak např. $\forall x\exists z(x \neq z)$ je její variantou, zatímco formule $\forall x\exists x(x \neq x)$ není.

Z věty 6.3 nyní plyne:

Důsledek 6.5. *Je-li A' variantou formule A, pak je dokazatelné, že obě formule jsou ekvivalentní* ($\vdash A \leftrightarrow A'$).

Důkaz: Podle věty 6.3 stačí ukázat, že formule $(Qx)B$ a $(Qy)B_x[y]$ jsou ekvivalentní. Provedeme důkaz pro případ, kdy Q je $\forall$. Případ, kdy Q je $\exists$, se dokáže podobně. Předpokládejme, že ve formuli $(\forall y)B_x[y]$ jsou x, y různé proměnné (v opačném případě není co dokazovat). Z axiomu substituce $\vdash (\forall x)B \rightarrow B_x[y]$

a z pravidla $\forall$ ihned plyne $\vdash (\forall x)B \to (\forall y)B_x[y]$. Abychom dokázali opačnou implikaci, označme B' formuli $B_x[y]$. Pak proměnná x nemá volný výskyt v B' a je substituovatelná za y do B'. Stejně jako v první části důkazu dostaneme $\vdash (\forall y)B' \to (\forall x)B'_y[x]$. Ale $B'_y[x]$ je formule B. Tím je důkaz hotov.

□

Definice 6.2. Formule A je v *prenexním tvaru*, jestliže má tvar $Q_1x_1 \dots Q_nx_nB$, kde

(i) $n \geq 0$ a pro každé $i = 1, \dots, n$ je Q_i buď $\forall$ nebo $\exists$,

(ii) $x_1, \dots, x_n$ jsou navzájem různé proměnné,

(iii) B je otevřená formule (neobsahuje kvantifikátory).

Na základě věty 6.4 lze nyní snadno dokázat následující tvrzení:

Věta 6.6. *Ke každé formuli A lze sestrojit formuli A' v prenexním tvaru tak, že $\vdash A \leftrightarrow A'$.*

Důkaz: (Indukcí podle složitosti formule A). Mohou nastat následující 4 případy:

a) A je atomická formule. Pak A je v prenexním tvaru a za A' volíme A.

b) A je tvaru $\neg B$ a již umíme sestrojit prenexní tvar B' formule B. Pak A' vznikne z $\neg B'$ přesunutím negace "dovnitř"(tj. bezprostředně před atomickou formuli) užitím ekvivalencí (1) z věty 6.4.

c) Pokud A je ve tvaru $B \to C$ a již umíme sestrojit prenexní tvary B' a C' formulí B a C, potom $A \leftrightarrow (B' \to C')$. Sestrojme varianty B'', C'' formulí B', C' takové, že žádná volná proměnná formule C' (a tedy ani C'') není vázaná ve formuli B'' a také žádná volná proměnná ve formuli B' (a tedy ani v B'') není vázaná ve formuli C''. Podle důsledku 6.5 máme $A \leftrightarrow (B'' \to C'')$ a prenexní tvar formule $B'' \to C''$ (a tedy i formule A) odvodíme z této formule pomocí vztahů (2) a (3) věty 6.4.

d) A je tvaru $(\forall x)B$ a B' je prenexní tvar formule B. Pak $(\forall x)B'$ je prenexní tvar formule A, jestliže x není vázaná ve formuli B', jinak je prenexním tvarem formule B formule B'.

□

6.1 Převedení formule na prenexní tvar

Návod explicitně vyjádříme jako výčet transformací, jejichž postupné užití dovolí získat prenexní tvar libovolné formule predikátové logiky. Abychom se v prenexním tvaru nemuseli vyhýbat použití spojek $\vee$ a $\wedge$, zahrneme mezi uvedené transformace i pravidla pro práci s těmito spojkami.

1. **Vyloučení zbytečných kvantifikátorů** – vynecháme všechny kvantifikátory $\forall x$, resp. $\exists x$ v podformulích tvaru $\forall x B$ nebo $\exists x B$, pokud se proměnná x nevyskytuje volně v B.

2. **Přejmenování proměnných** – vyhledáme podformuli QxA nejvíc vlevo takovou, že proměnná x se vyskytuje volně v A. Pokud x má ještě další výskyt ve výchozí formuli, nahradíme podformuli QxA její variantou $Qx'A'$, kde x' je proměnná různá od všech proměnných vyskytujících se v převáděné formuli. Tento proces opakujeme do té doby, až všechny kvantifikátory mají různé proměnné a žádná proměnná není v získané formuli současně volná i vázaná (formule s čistými proměnnými).

3. **Eleminace spojky** $\leftrightarrow$ – provede se podle následujícího schematu:

$$A \leftrightarrow B \ldots (A \to B) \wedge (B \to A)$$

4. **Přesun negace dovnitř** – provádíme postupně náhrady podformulí podle schémat

$\neg(\forall x A) \quad \ldots \exists x \neg A$
$\neg(\exists x A) \quad \ldots \forall x \neg A$
$\neg(A \to B) \ldots A \wedge \neg B$
$\neg(A \vee B) \ \ldots \neg A \wedge \neg B$
$\neg(A \wedge B) \ \ldots \neg A \vee \neg B$
$\neg(\neg A) \quad \ldots A$

tak dlouho, až se spojka negace vyskytne nejvýše bezprostředně před atomickými formulemi.

5. **Přesun kvantifikátorů doleva** – pro podformuli B, ve které se nevyskytuje proměnná x, provádíme náhrady podle schémat

$(QxA) \vee B \ \ldots Qx(A \vee B)$
$(QxA) \wedge B \ \ldots Qx(A \wedge B)$
$(QxA) \to B \ldots \overline{Q}x(A \to B)$
$B \to (QxA) \ldots Qx(B \to A)$,

kde $\overline{Q}$ je kvantifikátor "opačný"ke Q. Někdy lze snížit počet kvantifikátorů použitím schémat

$(\exists x A) \vee (\exists y B) \ldots \exists x(A \vee B_y[x])$
$(\forall x A) \wedge (\forall y B) \ldots \forall x(A \wedge B_y[x])$

Příklad 6.2. Hledejme prenexní tvar formule $\forall y(\exists x P(x,y) \to \exists u R(y,u)) \to \forall x S(x,y)$, kde P, R, S jsou binární predikáty. Transformace 1. se neuplatní, transformace 2. se uplatní nejprve na druhý a pak na první kvantifikátor. Dostáváme postupně tyto formule:

$A_1 : \forall y_2(\exists x_1 P(x_1, y_2) \to \exists u R(y_2, u)) \to \forall x S(x, y)$
$A_2 : \forall x(\forall y_2(\exists x_1 P(x_1, y_2) \to \exists u R(y_2, u)) \to S(x, y))$
$A_3 : \forall x \exists y_2((\exists x_1 P(x_1, y_2) \to \exists u R(y_2, u)) \to S(x, y))$
$A_4 : \forall x \exists y_2 \exists x_1((P(x_1, y_2) \to \exists u R(y_2, u)) \to S(x, y))$
$A_5 : \forall x \exists y_2 \exists x_1 \forall u((P(x_1, y_2) \to R(y_2, u)) \to S(x, y))$.

Prenexní tvar pro danou formuli není určen jednoznačně. Odlišnosti mohou nastat nejen v označení nových vázaných proměnných, ale i v pořadí kvantifikátorů v prefixu formule nebo ve tvaru jádra.

7 Věta o úplnosti

Definice 7.1. Je-li L jazyk 1. řádu a T množina formulí jazyka L, říkáme, že T je *teorie 1. řádu* s jazykem L.

Formule z T jsou tzv. *speciální axiomy*, které spolu s axiomy predikátové logiky tvoří soustavu všech axiomů teorie T.

Definice 7.2. Říkáme, že teorie T je *sporná*, jestliže pro každou formuli φ jazyka L platí $T \vdash \varphi$. V opačném případě je teorie *bezesporná*.

Je vidět, že T je sporná teorie, právě když pro nějakou formuli ψ jazyka L platí $T \vdash \psi$ a současně $T \vdash \neg\psi$. Pak totiž, poněvadž $\vdash (\neg\psi) \to (\psi \to \varphi)$ (získáno dosazením do tautologie $(\neg A \to (A \to B))$), užitím pravidla odloučení odvodíme $T \vdash \varphi$.

Důsledek 7.1. *Nechť T je množina formulí a nechť φ' je uzávěr formule φ. Potom $T \vdash \varphi$, právě když $T \cup \{\neg\varphi'\}$ je sporná teorie.*

Důkaz: Je-li $T \vdash \varphi$, pak podle věty 5.7 o uzávěru máme $T \vdash \varphi'$, takže $T \cup \{\neg\varphi'\} \vdash \neg\varphi'$ a $T \cup \{\neg\varphi'\} \vdash \varphi'$, čili $T \cup \{\neg\varphi'\}$ je sporná teorie. Je-li naopak teorie $T \cup \{\neg\varphi'\}$ sporná, pak lze z ní dokázat libovolnou formuli, tedy i formuli φ'. Takže $T \cup \{\neg\varphi'\} \vdash \varphi'$ a podle věty o dedukci (věta 5.9) $T \vdash (\neg\varphi') \to \varphi'$. Dále máme $\vdash (\neg\varphi' \to \varphi') \to \varphi'$ (formule vznikla dosazením do tautologie $(\neg A \to A) \to A$). Pravidlem odloučení $T \vdash \varphi'$, odkud $T \vdash \varphi$ podle věty o uzávěru (věta 5.7).

□

Definice 7.3. Buď T teorie s jazykem L a nechť $\mathcal{M}$ je nějaká realizace jazyka L. Řekneme, že $\mathcal{M}$ je *model teorie T*, jestliže $\mathcal{M} \models \varphi$ pro každou formuli $\varphi \in T$. Pak píšeme $\mathcal{M} \models T$.

Definice 7.4. Řekneme, že formule φ je *důsledkem teorie T*, jestliže pro každý model $\mathcal{M}$ teorie T je $\mathcal{M} \models \varphi$. Pak píšeme $T \models \varphi$.

Příklad 7.1.

1) Mějme jazyk teorie uspořádání. Pak speciální axiomy
$\neg(x < x)$
$x < y \to (y < z \to x < z)$
zadávají teorii částečného uspořádání. Každý model této teorie je částečně uspořádaná množina. Přidáme-li další speciální axiom
$x < y \vee x = y \vee y < x$,
dostaneme teorii lineárního uspořádání. Modely této teorie jsou právě lineárně uspořádané množiny.

2) Mějme jazyk teorie grup. Lze ukázat, že speciální axiomy
$x \cdot (y \cdot z) = (x \cdot y) \cdot z$
$x \cdot 1 = x$ (pravý neutrální prvek)
$\forall x \exists y(x \cdot y = 1)$ (pravý inverzní prvek)
již určují teorii grup. Modely této teorie jsou právě grupy. Je možno ukázat, že formule
$1 \cdot x = x$
$\forall x \exists y(y \cdot x = 1)$
jsou důsledky této teorie.

3) V jazyce elementární aritmetiky speciální axiomy
$\neg S(x) = 0$
$S(x) = S(y) \to x = y$
$x + 0 = x$
$x + S(y) = S(x + y)$
$x \cdot 0 = 0$
$x \cdot S(y) = x \cdot y + x$
určují teorii nazvanou *elementární aritmetika*. Je-li φ formule elementární aritmetiky a je-li x proměnná, pak $\varphi_x[0] \to ((\forall x(\varphi \to \varphi_x[S(x)])) \to (\forall x \varphi))$ je axiom indukce. Dostaneme teorii nazývanou Peanova aritmetika. Přirozená čísla včetně 0 s obvyklými operacemi následníka, sčítání a násobení tvoří tzv. standardní model Peanovy aritmetiky.

Věta 7.2. (O korektnosti) *Je-li T teorie s jazykem L a φ formule taková, že $T \vdash \varphi$, pak $T \models \varphi$*

Důkaz: Buď $\varphi_1, \ldots, \varphi_n$ důkaz formule φ z předpokladů T. Buď $\mathcal{M}$ libovolný model teorie T. Indukcí pro $i = 1, \ldots, n$ dokážeme, že $\mathcal{M} \models \varphi_i$. Je-li φ_i speciální axiom, pak $\mathcal{M} \models \varphi_i$, neboť $\mathcal{M}$ je model teorie T. S tímto dodatkem se důkaz provede stejně jako důkaz věty 5.2 o korektnosti predikátové logiky na str. 22.

□

Důsledek 7.3. *Má-li teorie T s jazykem L nějaký model, potom je bezesporná.*

Důkaz: Nechť $\mathcal{M}$ je model teorie T. Připusťme, že teorie T je sporná. Nechť φ je nějaká uzavřená formule jazyka L. Pak $T \vdash \varphi$ a $T \vdash \neg\varphi$. Pak podle věty 7.2 to znamená, že $T \models \varphi$ i $T \models \neg\varphi$. Takže $\mathcal{M} \models \varphi$ i $\mathcal{M} \models \neg\varphi$, odkud $\mathcal{M} \models \varphi \wedge \neg\varphi$. To není možné. Tudíž T je bezesporná.

□

Směřujeme k důkazu obrácení věty 7.2. Ukážeme, že syntax predikátové logiky je plně adekvátní její sémantice.

Věta 7.4. (Gödelova věta o úplnosti) *Je-li T teorie s jazykem L a je-li φ lib. formule jazyka L, pak $T \vdash \varphi$ právě když $T \models \varphi$.*

Tato věta je důsledkem následující věty, která nese tentýž název.

Věta 7.5. (Gödelova věta o úplnosti) *Teorie T je bezesporná, právě když má nějaký model.*

Důkaz: (Dokazujeme větu 7.4 pomocí věty 7.5.) Je-li T teorie a φ formule taková, že $T \vdash \varphi$, potom $T \models \varphi$ podle věty 7.2. Předpokládejme, že $T \models \varphi$. Tedy pro každý model $\mathcal{M}$ teorie T je $\mathcal{M} \models \varphi$. Buď φ' uzávěr formule φ. Podle definice splňování také $\mathcal{M} \models \varphi'$ pro každý model $\mathcal{M}$ teorie T. To znamená, že teorie $T \cup \{\neg\varphi'\}$ nemá model. (Kdyby totiž teorie $T \cup \{\neg\varphi'\}$ měla nějaký model $\mathcal{M}'$, pak by $\mathcal{M}'$ byl také model teorie T, takže bychom měli $\mathcal{M}' \models \varphi'$. Protože $\mathcal{M}' \models \neg\varphi'$, dostali bychom spor.) Podle věty 7.5 je teorie $T \cup \{\neg\varphi'\}$ sporná. Podle důsledku 7.1 to zamená, že $T \vdash \varphi$.

□

Abychom dokázali samotnou větu 7.5, s ohledem na důsledek 7.3 zbývá dokázat, že každá bezesporná teorie má nějaký model. Za tím účelem se budeme nejprve věnovat vyšetřování speciální teorie a získané výsledky pak využijeme ve zmíněném důkazu, který je uveden na straně 37.

Definice 7.5. Řekneme, že teorie T s jazykem L je *úplná*, jestliže T je bezesporná a pro každou uzavřenou formuli φ platí $T \vdash \varphi$ nebo $T \vdash \neg\varphi$ (v důsledku bezespornosti nemůže platit $T \vdash \varphi$ i $T \vdash \neg\varphi$ současně). V opačném případě říkáme, že T je *neúplná*.

Příklad 7.2. Buď $\mathcal{M}$ libovolná realizace jazyka L. Označme $Th(\mathcal{M})$ množinu všech uzavřených formulí jazyka L, které jsou splněny v $\mathcal{M}$. Pak $Th(\mathcal{M})$ je úplná teorie.

Definice 7.6. Řekneme, že teorie T s jazykem L je *Henkinova*, jestliže pro libovolnou uzavřenou formuli tvaru $(\exists x\psi)$ jazyka L existuje konstanta c jazyka L taková, že $T \vdash (\exists x\psi) \to \psi_x[c]$.

Lemma 7.6. *Libovolná úplná Henkinova teorie má model.*

Důkaz: Buď T úplná Henkinova teorie s jazykem L. Nechť C je množina všech termů jazyka L bez proměnných. Je-li L jazyk s rovností, definujeme relaci $\sim$ na C následovně: pro každá $t_1, t_2 \in C$ klademe $t_1 \sim t_2$, právě když $T \vdash t_1 = t_2$. Z reflexivity, symetrie a tranzitivity rovnosti (viz. lemma 5.12 (i),(ii),(iii) na straně 26) plyne, že relace $\sim$ je ekvivalence na C. Položme $M = C$ nebo $M = C/_\sim$ (v případě, že L je jazyk s rovností). Pro každé $t \in C$ značíme $\tilde{t} = \{s \in C; s \sim t\}$. Tedy v případě jazyka bez rovnosti je $\tilde{t}$ jednoprvkovou množinou $\{t\}$, kterou ztotožníme s termem t. Definujme realizaci $\mathcal{M}$ jazyka L s univerzem M následovně: Pro každý funkční symbol f četnosti n a pro každý predikátový symbol p četnosti n kromě rovnosti a pro každá $\tilde{t}_1, \ldots, \tilde{t}_n \in M$ klademe jednak $f_{\mathcal{M}}(\tilde{t}_1, \ldots, \tilde{t}_n) = f(t_1, \ldots, t_n)$, jednak $(\tilde{t}_1, \ldots, \tilde{t}_n) \in p_{\mathcal{M}}$, právě když $T \vdash p(t_1, \ldots, t_n)$. Z lemmatu 5.12 (iv),(v) plyne, že tyto definice jsou korektní. Navíc indukcí vzhledem ke složitosti termů lze ukázat, že je-li $t \in C$, pak $\tilde{t}$ je hodnota termu t v realizaci $\mathcal{M}$.

Ukážeme, že $\mathcal{M}$ je modelem teorie T. Chceme ukázat, že pro každý speciální axiom $\varphi \in T$ je $\mathcal{M} \models \varphi$. Buď φ' uzávěr formule φ. Podle věty o uzávěru pak $T \vdash \varphi'$. Ukážeme-li, že $\mathcal{M} \models \varphi'$, pak podle definice splňování odtud ihned plyne $\mathcal{M} \models \varphi$. Stačí tedy, dokážeme-li následující vlastnost: Pro libovolnou uzavřenou formuli φ jazyka L platí: $\mathcal{M} \models \varphi$, právě když $T \vdash \varphi$.

Dokážeme to indukcí vzhledem ke složitosti uzavřené formule φ. Pro jednoduchost budeme předpokládat, že každá formule jazyka L je vytvořena z atomických formulí jen pomocí logických spojek $\neg, \wedge$ a kvantifikátoru $\exists$ (což je možné podle poznámky na konci kapitoly 5).

Indukce:

1. Je-li φ atomická formule tvaru $p(t_1, \ldots, t_n)$, pak termy $t_1, \ldots, t_n$ jsou bez proměnných. Podle definice splňování a podle definice relace $p_{\mathcal{M}}$ dostáváme $\mathcal{M} \models p(t_1, \ldots, t_n)$, právě když $(\tilde{t}_1, \ldots, \tilde{t}_n) \in p_{\mathcal{M}}$, a to je právě když $T \vdash p(t_1, \ldots, t_n)$.

2. Je-li φ atomická formule tvaru $t_1 = t_2$, pak $\mathcal{M} \models t_1 = t_2$, právě když $\tilde{t}_1 = \tilde{t}_2$, a to je právě když $t_1 \sim t_2$, to jest právě když $T \vdash t_1 = t_2$.

3. Je-li φ tvaru $\neg\psi$, pak $\mathcal{M} \models \varphi$, právě když $\mathcal{M} \not\models \psi$, což podle indukčního předpokladu je právě když $T \not\vdash \psi$. Ale T je úplná teorie, takže $T \not\vdash \psi$, právě když $T \vdash \neg\psi$, tj. $T \vdash \varphi$.

4. Je-li φ formule tvaru $\psi \wedge \eta$, pak $\mathcal{M} \models \varphi$, právě když $\mathcal{M} \models \psi$ a $\mathcal{M} \models \eta$, což podle indukčního předpokladu je právě když $T \vdash \psi$ a $T \vdash \eta$, což je dle postupů výrokové logiky totéž jako $T \vdash \psi \wedge \eta$, tj. $T \vdash \varphi$.

5. Je-li φ tvaru $(\exists x\psi)$, pak formule ψ obsahuje nejvýše jednu volnou proměnnou x. Přitom $\mathcal{M} \models \varphi$ znamená, že $\mathcal{M} \models \varphi[e]$ pro jakékoliv ohodnocení proměnných e. Ovšem φ je $(\exists x\psi)$. Máme $\mathcal{M} \models (\exists x\psi)[e]$, právě když existuje $\tilde{t} \in M$ takové, že $\mathcal{M} \models \psi[e(x/\tilde{t})]$, což je totéž, jako $\mathcal{M} \models \psi_x[t][e]$, tedy jako

$\mathcal{M} \models \psi_x[t]$, neboť formule $\psi_x[t]$ je uzavřená. Podle indukčního předpokladu to nastane, právě když $T \vdash \psi_x[t]$, pro nějaký term $t \in C$.

Ukážeme, že tato situace nastane, právě když $T \vdash (\exists x\psi)$, tj. $T \vdash \varphi$. Je-li $T \vdash \psi_x[t]$, pak $T \vdash (\exists x\psi)$ (podle lemmatu 5.5 na straně 23 užitím pravidla odloučení).

Je-li $T \vdash (\exists x\psi)$, pak protože teorie T je Henkinova, existuje konstanta c jazyka L taková, že $T \vdash (\exists x\psi) \to \psi_x[c]$. Odtud pravidlem odloučení $T \vdash \psi_x[c]$.

Důkaz je hotov.

□

Definice 7.7. Jazyk L' je *rozšířením jazyka* L, jestliže každý speciální symbol jazyka L je obsažen v jazyce L'. Teorie T' jazyka L' je *rozšířením teorie* T jazyka L, jestliže pro libovolnou formuli φ jazyka L takovou, že $T \vdash \varphi$, je také $T' \vdash \varphi$. Teorie T' je *konzervativním rozšířením teorie* T, jestliže navíc pro každou formuli ψ jazyka L takovou, že $T' \vdash \psi$, je již $T \vdash \psi$.

Poznámka 7.7. *Je-li T' konzervativní rozšíření teorie T, je ihned vidět, že T je bezesporná, právě když T' je bezesporná.*

Lemma 7.8. (Henkin) *K libovolné teorii T lze sestrojit Henkinovu teorii T_H, která je konzervativním rozšířením teorie T.*

Důkaz: Buď L jazyk teorie T. Sestrojme jazyk L_1, který bude rozšířením jazyka L, a teorii T_1 s tímto jazykem, která bude rozšířením teorie T, následovně: Pro každou uzavřenou formuli jazyka L tvaru $(\exists x\varphi)$ přidejme novou, tzv. *Henkinovu konstantu* označenou c_φ a nový speciální axiom $(\exists x\varphi) \to \varphi_x[c_\varphi]$. V jazyku L_1 vznikají nové uzavřené formule $(\exists x\varphi)$. Tímtéž způsobem sestrojíme k teorii T_1 jazyka L_1 její rozšíření T_2 v rozšířeném jazyce L_2, atd. Vzniká tak posloupnost $L_1, L_2, \ldots$ jazyků a posloupnost $T_1, T_2, \ldots$ teorií, z nichž každá je rozšířením předchozí. Henkinovy konstanty, které jsme přidávali při tvorbě jazyka L_n, nazveme konstantami řádu n.

Nechť nyní L_H je jazyk vzniklý z jazyka L přidáním všech Henkinových konstant všech řádů, tzn. $L_H = \cup_{i=1}^{\infty} L_i$. Nechť T_H je teorie vzniklá z teorie T přidáním všech uvedených axiomů příslušných všem konstantám, tj. $T_H = \cup_{i=1}^{\infty} T_i$ (T_H je Henkinova teorie). Dokážeme, že T_H je konzervativním rozšířením teorie T.

T_H je zřejmě rozšířením teorie T. Nechť ψ je libovolná formule jazyka L taková, že $T_H \vdash \psi$. Nechť $\varphi_1, \ldots, \varphi_n$ jsou všechny Henkinovské axiomy použité v důkazu formule ψ z předpokladu T_H. Můžeme navíc předpokládat, že φ_1 je axiom obsahující Henkinovu konstantu maximálního řádu mezi všemi axiomy $\varphi_1, \ldots, \varphi_n$. Tedy $T, \varphi_1, \ldots, \varphi_n \vdash \psi$. Z věty o dedukci z kapitoly 5 dostáváme $T \vdash (\varphi_1 \to (\varphi_2 \to (\ldots(\varphi_n \to \psi))\ldots))$. Nechť axiom φ_1 je tvaru $(\exists x\eta) \to \eta_x[e_\eta]$. Protože c_n je konstanta maximálního řádu, není obsažena v $\varphi_2, \ldots, \varphi_n$ ani v ψ. Nyní užitím věty

o kostantách z kapitoly 5 odvodíme $\vdash ((\exists x\eta) \to \eta_x[w]) \to (\varphi_2 \to \ldots \to (\varphi_n \to \psi)\ldots)$, kde w je nová proměnná nevyskytující se ve $\varphi_1, \ldots, \varphi_n$ ani v ψ. Užitím pravidla $\exists$ (lemma 5.4) odtud $T \vdash (\exists w((\exists x\eta) \to \eta_x[w]) \to (\varphi_2 \ldots \to (\varphi_n \to \psi)\ldots)$. Podle lemmatu 5.5 máme $\vdash \eta \to (\exists w\ \eta_x[w])$. Odtud užitím pravidla $\exists$ vychází $\vdash (\exists x\eta) \to (\exists w\eta_x[w])$, takže po provedení prenexní operace (viz větu 6.4(2)) máme $\vdash \exists w((\exists x\eta) \to \eta_x[w])$. Toto spolu s formulí uvedenou o tři řádky výše užitím pravidla odloučení dává $T \vdash (\varphi_2 \to \ldots (\varphi_n \to \psi)\ldots)$. Opakováním tohoto postupu nakonec dostaneme $T \vdash \psi$.

□

Lemma 7.9. *Teorie T je bezesporná, právě když každá její konečná podmnožina $Q \subseteq T$ je bezesporná.*

Důkaz: Plyne z toho, že každý důkaz v predikátové logice z předpokladů T obsahuje jen konečný počet formulí.

□

Věta 7.10. (Lindenbaum) *Je-li T bezesporná teorie s jazykem L, pak existuje úplné rozšíření T' teorie T se stejným jazykem L.*

Důkaz: Buď $\mathcal{S}$ množina všech uzavřených formulí jazyka L. Nechť $\mathcal{B} = \{S; S \subseteq \mathcal{S}$ a $T \cup S$ je bezesporná teorie$\}$. Množina $\mathcal{B}$ je částečně uspořádaná inkluzí a je neprázdná, neboť $\emptyset \in \mathcal{B}$, protože T je bezesporná. Mějme libovolnou podmnožinu $\mathcal{D} \subseteq \mathcal{B}$, která je řetězcem vzhledem k inkluzi. Pak $T \cup (\cup\mathcal{D})$ je bezesporná teorie (podle lemmatu 7.9), neboť každá konečná podmnožina $\cup\mathcal{D}$ je podmnožinou některé množiny $S \in \mathcal{D}$ a $T \cup S$ je bezesporná teorie. Takže $\cup\mathcal{D} \in \mathcal{B}$. Podle Zornova lemmatu existuje v částečně uspořádané množině $\mathcal{B}$ maximální prvek, nechť je to S_0. Pak teorie $T \cup S_0 = T'$ je rozšířením teorie T, je bezesporná a ukážeme, že je to úplná teorie.

Buď φ libovolná uzavřená formule jazyka L. Připusťme, že $T' \nvdash \varphi$ a $T' \nvdash \neg\varphi$. Poněvadž $T' \nvdash \varphi$, podle důsledku 7.1 je $T' \cup \{\neg\varphi\}$ bezesporná teorie. To znamená, že $S_0 \cup \{\neg\varphi\} \in \mathcal{B}$. Přitom $\neg\varphi \notin S_0$, dokonce $\neg\varphi \notin T'$, neboť $T' \nvdash \neg\varphi$. To je spor s maximalitou množiny S_0.

□

Důkaz Gödelovy věty 7.5 ze strany 34: Jak již bylo uvedeno, vzhledem k důsledku 7.3 zbývá ukázat, že bezesporná teorie T jazyka L má nějaký model. Podle poznámky 7.7 a lemmatu 7.8 existuje Henkinova teorie T_H tak, že je bezesporná a její jazyk L' je rozšířením jazyka L o množinu Henkinových konstant. Podle věty 7.10 existuje úplné rozšíření T' teorie T_H s jazykem L'. Teorie T' je úplná a současně zůstává i Henkinova. Podle lemmatu 7.6 má teorie T' nějaký model $\mathcal{M}'$. Model $\mathcal{M}'$ je realizací jazyka L'. Nebudeme-li v $\mathcal{M}'$ vyznačovat prvky odpovídající přidaným Henkinovým konstantám z L', dostaneme tak realizaci $\mathcal{M}$ jazyka L, která je zřejmě modelem teorie T.

□

8 Věta o kompaktnosti a věta Herbrandova

Věta 8.1. (O kompaktnosti) *Nechť T je množina formulí jazyka L. Pak teorie T má nějaký model, právě když každá její konečná podmnožina $Q \subseteq T$ má model.*

Důkaz: Plyne z Gödelovy věty o úplnosti (věta 7.5) a z lemmatu 7.9.

□

Jako ukázku aplikace této věty uvedeme příklad o neaxiomatizovatelnosti.

Aplikace:
Uvažujme jazyk teorie grup a teorii abelovských grup. Tuto teorii lze zadat konečným počtem speciálních axiomů. Grupa se nazývá periodickou grupou, jestliže každý její prvek x má konečný řád n ($n \in \mathbb{N}$), tj. jestliže je v ní splněno: $\forall x \exists n \geq 1 : x^n = 1$ kde x^n je zkratka pro term $\underbrace{x \cdot \ldots \cdot x}_{n}$. Ale tento výraz není formulí predikátové logiky 1. řádu. Je to tvrzení tzv. slabé logiky 2. řádu, neboť se v něm kvantifikuje přes přirozená čísla. Vidíme tedy, že periodické abelovské grupy lze axiomatizovat ve slabé logice 2. řádu. Ukážeme, že je však nelze axiomatizovat v predikátové logice 1. řádu.

Tvrzení 8.2. *Buď P množina všech formulí jazyka 1. řádu teorie grup, které jsou splněny ve všech periodických abelovských grupách. Potom existuje abelovská grupa $\mathcal{A}$ taková, že $\mathcal{A}$ není periodická abelovská grupa a přitom $\mathcal{A} \models P$.*

Důkaz: Rozšiřme jazyk teorie grup o nový konstantní symbol c. Uvažme množinu formulí $S = P \cup \{\neg(c = 1), \neg(c^2 = 1), \neg(c^3 = 1), \ldots\}$. Mějme nyní libovolnou konečnou podmnožinu $Q \subseteq S$. Vezměme největší n takové, že formule $\neg(c^n = 1)$ je obsažena v Q (pokud $Q \subseteq P$, volíme $n = 0$). Uvažujme jakoukoliv cyklickou grupu C řádu $n+1$. Je to periodická abelovská grupa a interpretujeme-li v ní navíc symbol c kterýmkoliv prvkem řádu $n + 1$, je jasné, že pak C se stane modelem teorie Q. Takže každá konečná podmnožina množiny S má model, podle věty 8.1 pak i S má model $\mathcal{A}$. Tento model $\mathcal{A}$ je abelovská grupa, neboť $\mathcal{A} \models P$, ale není to periodická grupa, neboť prvek a z $\mathcal{A}$, který interpretuje konstantu c, nemá konečný řád.

□

Označme $|L|$ mohutnost množiny všech speciálních symbolů jazyka L.

Věta 8.3. *Buď T bezesporná teorie jazyka L. Pak T má model mohutnosti nejvýše $max\{\aleph_0, |L|\}$.*

Důkaz: Plyne z důkazu věty o úplnosti, viz důkaz věty 7.5. Rozšíření L' jazyka L je konstruováno v lemmatu 7.8. Přitom mohutnost množiny formulí v žádném kroku konstrukce, a tedy mohutnost množiny Henkinových konstant lib. řádu, nikdy nepřevýší $max\{\aleph_0, |L|\}$. Model úplné teorie T' jazyka L' se konstruuje v lemmatu 7.6. Poněvadž už množina termů jazyka L' nemá větší mohutnost než $max\{\aleph_0, |L|\}$, je vidět, že ani model nebude větší mohutnosti.

□

Věta 8.4. (Löwenheim,Skolem) *Má-li teorie T s jazykem L nekonečný model, pak má model libovolné mohutnosti $n \geq max\{\aleph_0, |L|\}$.*

Důkaz: Buď $\mathcal{M}$ nekonečný model teorie T. Rozšiřme jazyk L přidáním množiny $\{c_i; i \in I\}$ nových konstantních symbolů, kde mohutnost I je rovna n. Uvažme množinu formulí $S = T \cup \{\neg(c_i = c_j); i, j \in I, i \neq j\}$. Máme-li libovolnou konečnou podmnožinu $Q \subseteq S$, pak ve formulích z Q je jen konečný počet nových konstantních symbolů. Poněvadž $\mathcal{M}$ je struktura s nekonečným univerzem, můžeme těmto konstantním symbolům přiřadit navzájem různé prvky z $\mathcal{M}$ a je jasné, že tím se $\mathcal{M}$ stává modelem teorie Q. Podle věty 8.1 o kompaktnosti má tedy sama teorie S model, a tedy je bezesporná. Podle věty 8.3 ovšem má teorie S model mohutnosti nejvýše $max\{\aleph_0, |L| + |I|\} = n$. Na druhé straně, poněvadž v tomto modelu je splněno $\neg(c_i = c_j)$ pro $i \neq j; i, j \in I$, má tento model mohutnost právě n. Opomeneme-li interpretaci konstantních symbolů $c_i; i \in I$, dostaneme model teorie T.

□

Příklad 8.1. Existuje nestandardní model Peanovy aritmetiky. Skutečně, standardní model Peanovy aritmetiky je spočetný (tedy nekonečný). Podle věty 8.4 existuje model Peanovy aritmetiky libovolné mohutnosti $n \geq \aleph_0$. Je-li $n > \aleph_0$, je tento model nestandardní.

Ve zbytku kapitoly se omezíme na jazyky predikátové logiky 1. řádu bez rovnosti.

Herbrandova věta charakterizuje některé logicky platné formule predikátové logiky pomocí jistých tautologií. Často bývá formulována v negativní podobě, tj. jako charakterizace některých sporných formulí pomocí jistých kontradikcí.

Řekneme, že výroková formule A je *kontradikce*, jestliže $\overline{v}(A) = 0$ pro lib. pravdivostní ohodnocení v prvotních formulí. Zřejmě A je kontradikce, právě když $\neg A$ je tautologie. Buď L jazyk predikátové logiky. V dalším budeme jako množinu P prvotních formulí pro výrokovou logiku brát množinu všech atomických formulí jazyka L. Výrokové formule budou tedy formule vytvořené z atomických formulí pomocí logických spojek, tj. otevřené formule.

Řekneme, že formule φ jazyka L je *sporná*, jestliže pro každou realizaci $\mathcal{M}$ jazyka L při libovolném ohodnocení proměnných e je $\mathcal{M} \not\models \varphi[e]$. Formule φ je sporná, právě když $\neg\varphi$ je logicky platná formule.

Zavedeme následující označení: zápisem $\varphi(x_1, \ldots, x_n)$ budeme označovat formuli φ, jejíž všechny volné proměnné jsou mezi $x_1, \ldots, x_n$. Jsou-li $t_1, \ldots, t_n$ termy substituovatelné za $x_1, \ldots, x_n$ do φ, pak instanci $\varphi_{x_1,\ldots,x_n}[t_1, \ldots, t_n]$ budeme značit $\varphi(t_1, \ldots, t_n)$.

Herbrandova věta se obvykle dokazuje ve svém negativním tvaru (z důvodu náročnosti tento důkaz neuvádíme):

Věta 8.5. (Herbrandova věta – negativní tvar.) *Je-li $\varphi(x_1, \ldots, x_n)$ otevřená formule jazyka L, pak formule $(\forall x_1 \ldots \forall x_n \varphi(x_1, \ldots, x_n))$ je sporná, právě když existují termy $t_1^1, \ldots, t_n^1, \ldots, t_1^m, \ldots, t_n^m$ takové, že $\varphi(t_1^1, \ldots, t_n^1) \wedge \ldots \wedge \varphi(t_1^m, \ldots, t_n^m)$ je kontradikce.*

Negováním formulí v obou částech věty 8.5 dostáváme tento obvyklý tvar Herbrandovy věty:

Věta 8.6. (Herbrandova věta - pozitivní tvar) *Je-li $\varphi(x_1, \ldots, x_n)$ otevřená formule jazyka L, pak formule $(\exists x_1 \ldots \exists x_n \varphi(x_1, \ldots, x_n))$ je logicky platná, právě když existují termy $t_1^1, \ldots, t_n^1, \ldots, t_1^m, \ldots, t_n^m$ takové, že $\varphi(t_1^1, \ldots, t_n^1) \vee \ldots \vee \varphi(t_1^m, \ldots, t_n^m)$ je tautologie.*

Vzhledem ke Gödelově větě o úplnosti je Herbrandova věta současně charakterizací některých formulí dokazatelných v predikátové logice 1. řádu. Jde o uzavřené formule v prenexním tvaru, jejichž prefix obsahuje jen existenční kvantifikátor. Tento výsledek je možno rozšířit na libovolné formule zavedením tzv. Skolemových funkcí. Pomocí těchto funkcí je možno upravit prenexní tvar formule tak, že neobsahuje existenční kvantifikátory. Idea úpravy spočívá v transformaci formule $\forall x_1, \ldots \forall x_n \exists x_{n+1} \varphi(x_1, \ldots x_n, x_{n+1})$ na formuli $\forall x_1, \ldots \forall x_n \varphi(x_1, \ldots x_n, f(x_1, \ldots x_n))$, tzv. Skolemův normální tvar, kde f je tzv. Skolemova funkce. Skolemův normální tvar dané formule obecně není logicky ekvivalentní s touto formulí, je však splnitelný, právě když daná formule je splněnitelná (obecně ale ne pro stejnou realizaci).

Příklad 8.2.

1) Skolemův normální tvar formule $\forall x \exists y \forall z \exists w(\varphi(x, y) \vee \neg\psi(z, w))$ je zřejmě $\forall x \forall z(\varphi(x, f(x)) \vee \neg\psi(z, g(x, z)))$.

2) Formule $\forall x \exists y p(x, y)$ má Skolemův normální tvar $\forall x p(x, f(x))$, což v realizaci s univerzem $\mathbb{Z}$ a symbolem $p(x, y)$ interpretovaným relací $x + y = 0$ znamená, že formule $\forall x \exists y(x + y = 0)$ má Skolemův normální tvar $\forall x(x + f(x) = 0)$. Pak zřejmě $f(x) = -x$.

Je-li nyní φ libovolná formule, převedeme formuli $\psi = \neg\varphi$ na Skolemův normální tvar a aplikujeme negativní tvar Herbrandovy věty. Tím rozhodneme o spornosti formule ψ a tedy o dokazatelnosti formule φ.

9 Věty o neúplnosti

Roku 1931 dokázal Kurt Gödel dvě významné věty, které jsou dnes známy jako První a Druhá věta o neúplnosti predikátové logiky. Tyto věty mají zcela výsadní postavení v moderní matematice, neboť hrají důležitou roli nejen v logice, ale také v mnoha dalších oblastech matematiky, zejména v teorii modelů, aritmetice a teorii množin. Gödelovy věty jsou ovšem významné i z hlediska filozofie, neboť stanovují hranice „axiomatického“ uvažování. Plyne z nich mj. neproveditelnost tzv. Hilbertova programu, který si kladl za cíl zachytit celou matematiku jako systém určitých fixních axiomů a odvozovacích pravidel, ze kterých by bylo možno vyvozovat všechna platná tvrzení, tj. věty. Tento systém měl být bezesporný a úplný a Kurt Gödel ukázal, že toho dosáhnout nelze. V této kapitole uvádíme obě věty nikoliv v původním, méně srozumitelném tvaru, nýbrž v mírně zesíleném tvaru převedeném do srozumitelnější terminologie. Tyto věty byly zobecněny mnoha autory, příslušná zobecnění však přesahují rámec tohoto textu, proto je neuvádíme. Ze stejného důvodu vynecháváme důkazy obou vět.

V následující větě užíváme pojem rekurzivní teorie. Přesná matematická definice tohoto pojmu je poněkud komplikovaná, proto použijeme následující „informatickou“ definici: Teorie je rekurzivní, právě když existuje algoritmus, který umožní stroji rozhodnout o libovolné formuli, zda je či není axiomem této teorie. Tedy teorie je rekurzivní, právě když stroj umí rozhodnout o každé posloupnosti formulí, zda je či není důkazem v této teorii. Všechny běžně uvažované matematické teorie jsou rekurzivní.

Věta 9.1. (První věta o neúplnosti.) *Je-li T bezesporná rekurzivní teorie, která je rozšířením Peanovy aritmetiky, pak je neúplná (přesněji, pak existuje uzavřená formule φ v jazyce teorie T taková, že platí $T \nvdash \varphi$ a $T \nvdash \neg\varphi$).*

První věta o neúplosti stanovuje hranici každého formálního systému zahrnujícího (Peanovu) aritmetiku. Hraje tedy významnou roli nejen v matematice a filozofii, ale také v informatice, kde omezuje výpočetní sílu užitou pro algoritmizaci nejrůznějších úloh. Věta totiž ukazuje omezenost algoritmizace a nenahraditelnost člověka strojem.

Věta 9.2. (Druhá věta o neúplnosti.) *Nechť T je bezesporná rekurzivní teorie, která je rozšířením Peanovy aritmetiky, a nechť Con_T značí formuli „T je bezesporná“. Pak platí $T \nvdash Con_T$.*

Podle Druhé věty o neúplnosti tedy nemůže žádná bezesporná rekurzivní teorie obsahující Peanovu aritmetiku vlastními prostředky dokázat svoji bezespornost. Zatímco První věta o neúplnosti říká, že v žádné rozumné teorii přirozených čísel není dokazatelné vše, Druhá věta je konkrétní příklad takového nedokazatelného tvrzení.