Logika I.

zpracoval Martin Kuba

16. května 1995

Obsah

1 Úvod **2**

1.1 Předmět matematiky 2

1.2 Nástin historie 2

1.3 Axiomatická výstavba matematických teorií 2

2 Výroková logika **3**

2.1 Závislost pravdivosti výrokových formulí na pravdivosti prvotních formulí 3

2.2 Dokazatelnost ve výrokové logice 4

2.2.1 FORMÁLNÍ AXIOMATICKÝ SYSTÉM LOGIKY HILBERTOVA TYPU 4

3 Predikátová logika **8**

3.1 Jazyk predikátové logiky 1. řádu 9

3.1.1 Termy 10

3.1.2 Atomické formule 10

3.1.3 Formule 11

4 Sémantika predikátové logiky **11**

4.1 Substituce termů za proměnné 14

5 Axiomy predikátové logiky **14**

5.1 schemata výrokových axiomů 14

5.2 schema axiomu kvantifikátoru 14

5.3 schema axiomů substituce 15

5.4 schemata axiomů rovnosti 15

5.5 odvozovací pravidla predikátové logiky 15

6 Věta o úplnosti **19**

7 Věta o kompaktnosti **22**

8 Prenexní tvary formulí **23**

8.1 Normální tvar formulí 23

8.1.1 Převedení formule na prenexní tvar 24

9 Herbrandova věta **25**

1 Úvod

1.1 Předmět matematiky

Jsou studovány abstraktní objekty (čísla, funkce, relace, plochy, grupy, tělesa ...). Ve 20. stol. se matematika stala konglomerátem teorií, z nichž každá studuje souhrn objektů charakterizovaný přesně formulovanými vztahy mezi nimi. Bourbaki: předmětem matematiky 20. století je cílevědomé studium matematických struktur.
Matematická tvrzení se dokazují dedukcí na základě přesného vymezení pojmů.
Co je logika ?

— analýza metod správného usuzování

— 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, důkazové metody.

1.2 Nástin historie

Zakladatelem logiky je Aristoteles (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 mat. analýzy na aritmetických základech a v souvislosti s objevem neeuklidovských geometrií. Matematická logika se zformulovala v polovině 19. století pracemi G. Boolea, k rozvoji přispěli 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. E. Zermelo). Vzniklo nebezpečí, zda se neobjeví nové paradoxy. Otázka bezespornosti axiom. teorií vedla ve 20. letech 20. století D. Hilberta k tzv. programu formalizace matematiky.

1.3 Axiomatická výstavba matematických teorií

Axiomy — výchozí tvrzení dané teorie, nedokazují se, 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.

Formalizace

Matematická tvrzení se zapíší 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

symboly — tvoří abecedu dané teorie

formule — určitá slova v této abecedě, tvoří jazyk teorie

axiomy — výchozí tvrzení dané teorie, jsou zapsány pomocí abecedy jako jisté formule

odvozovací pravidla — jisté manipulace s formulemi, pomocí nichž a axiomů odvozujeme důsledky

Cílem Hilbertova programu bylo dokázat bezespornost silných matematických teorií pomocí kombinatorických manipulací s formulemi. K. Gödel (1931) — věty o neúplnosti. Důsledek vět o neúplnosti — Hilbertův program nelze uskutečnit.

2 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 značíme písmeny $p, q, \ldots$ případně s indexy $p_1, p_2, \ldots$ hrají úlohu jednoduchých výroků. Složené výroky vytváříme z jednoduchých pomocí *logických spojek:*

$\neg$ negace

& konjunkce

$\vee$ disjunkce

$\rightarrow$ implikace

$\equiv$ 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 $(\neg A), (A \& B), (A \vee B), (A \rightarrow B), (A \equiv B)$ 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 $v : P \rightarrow \{0, 1\}$, tj. zobrazení, které každé prvotní formuli $p \in P$ přiřadí hodnotu 0 (tj. 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 $\overline{v}(\neg A), \overline{v}(A \& B), \overline{v}(A \vee B), \overline{v}(A \rightarrow B), \overline{v}(A \equiv B)$ v závislosti na $\overline{v}(A)$, $\overline{v}(B)$ se definuje podle tabulky.

$\overline{v}(A)$	$\overline{v}(B)$	$\overline{v}(\neg A)$	$\overline{v}(A \& B)$	$\overline{v}(A \vee B)$	$\overline{v}(A \rightarrow B)$	$\overline{v}(A \equiv B)$
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**

$\neg\neg A \equiv A$ **zákon dvojí negace**

$\neg(A \& \neg A)$ **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 $A \equiv B$ je tautologie.

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

$$\begin{array}{rcl} A \equiv B & \dots & (A \to B)\&(B \to A) \\ A \to B & \dots & \neg A \vee B \\ A \to B & \dots & \neg(A\&\neg B) \\ A \vee B & \dots & \neg(\neg A\&\neg B) \\ A\&B & \dots & \neg(\neg A \vee \neg B) \\ A \vee B & \dots & \neg A \to B \\ A\&B & \dots & \neg(A \to \neg B) \end{array}$$

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

$$\begin{array}{llll} \text{Pak} & A \downarrow B & \text{je log. ekvivalentní} & \neg A\&\neg B \\ & A \mid B & & \neg A \vee \neg B \\ & \neg A & & A \downarrow A \\ & \neg A & & A \mid A \\ & A\&B & & (A \downarrow A) \downarrow (B \downarrow B) \\ & A \vee B & & (A \mid A) \mid (B \mid B) \end{array}$$

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

Definice pravdivosti přímo dává algoritmus, 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 — a sice jako formální axiomatická teorie. K charakteristice dokazatelnosti byly vytvořeny 2 typy formálních systémů: Hilbertova typu a Gentzenova typu.

2.2.1 FORMÁLNÍ AXIOMATICKÝ SYSTÉM LOGIKY HILBERTOVA TYPU

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, zadány pomocí tří následujících schemat axiomů

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

$$\begin{array}{ll} \text{(A1)} & A \to (B \to A) \\ \text{(A2)} & (A \to (B \to C)) \to ((A \to B) \to (A \to C)) \\ \text{(A3)} & (\neg B \to \neg A) \to (A \to B) \end{array}$$

Odvozovací pravidlo – jediné pravidlo, nazývá se *modus ponens* (pravidlo odloučení), 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.

Definice 2.1

Důkazem ve formální výrokové logice rozumíme libovolnou konečnou posloupnost $A_1 \dots A_n$ 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 $A_1, \dots, A_{i-1}$. Řekneme, že formule A je *dokazatelná* ve výrokové logice, jestliže existuje důkaz, jehož poslední formulí je je formule A, píšeme $\vdash A$.

Věta 2.2 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

tedy $\overline{v}(A \to (B \to A)) = 1$ 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 $\overline{v}(\neg B \to \neg A) = 0$. Pak ale $\overline{v}((\neg B \to \neg A) \to (A \to B)) = 1$,což je spor. Tedy (A3) je tautologie. Podobně se ověří, že (A2) je 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 z definice pravdivostního ohodnocení pro spojku $\to$ ihned plyne $\overline{v}(B) = 1$,tedy B je tautologie. Každá dokazatelná formule je tautologie.

□

Budeme potřebovat zobecnění pojmu dokazatelnosti. Nechť T je množina formulí výrokové logiky. Řekneme, že konečná posloupnost $A_1, \dots, A_n$ 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 $A_1, \dots, A_{i-1}$. Říkáme, že formule A je dokazatelná z předpokladů T, píšeme $T \vdash A$.
Směřujeme k důkazu toho, že axiomatický systém výrokové logiky je úplný, tj. že každá tautologie je dokazatelná.

Lemma 2.3

Pro lib. fromuli A je dokazatelná formule $A \to A$. ($\vdash A \to A$)

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 2.4 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 předpokladu 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 pro $j \leq n$ ukážeme, že $T \vdash A \to A_j$. 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 $T \vdash A \to A$.

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 $r < j$, $A_r \to A_j$, dle indukčního předpokladu máme $T \vdash A \to A_r$, $T \vdash A \to (A_r \to A_j)$.

Dále axiom (A2) pro vobu A, A_r, A_j za formule A, B, C má tvar

$$(A \to (A_r \to A_j)) \to ((A \to A_r) \to (A \to A_j)).$$

Dvojím použitím pravidla modus ponens dostaneme

$$(A \to A_r) \to (A \to A_j)$$

$$A \to A_j$$

Připojením těchto posledních tří formulí k důkazům, které již máme podle ind. předpokladu, dostáváme $T \vdash A \to A_j$.

Věta o dedukci je dokázána. □

Lemma 2.5

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)	$\vdash (\neg\neg A \to \neg\neg B) \vdash (\neg B \to \neg A)$	(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
	(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 2.6 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 2.5 (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 2.5 (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 2.5 (f)
(13)	$T \vdash B$	(11),(12) MP

Zavedeme pomocné označení:

Je-li v lib. ohodnocení prvotních formulí, pak pro lib. formuli B klademe $B^v = \begin{cases} B & \textit{pro} \quad \overline{v}(B) = 1 \\ \neg B & \textit{pro} \quad \overline{v}(B) = 0 \end{cases}$

Lemma 2.7

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 2.5 (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 $\overline{v}(C) = 1, \overline{v}(D) = 1$

   ⋆ Je-li $\overline{v}(C) = 0, \overline{v}(D) = 1$ pak v obou případech $\overline{v}(A) = 1$, dále D^v je D, 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 $\neg C$, a máme $P_1^v, \ldots, P_n^v \vdash \neg C$. Dle lemmatu 2.5 (a) $\vdash \neg C \to (C \to D)$, odkud užitím pravidla MP $P_1^v, \ldots, P_n^v \vdash C \to D$. Stačí si uvědomit, že $C \to D$ je A^v.

   ⋆ Je-li $\overline{v}(C) = 1, \overline{v}(D) = 0$, pak $\overline{v}(A) = 0$. Dále C^v je C, D^v je $\neg D$, takže máme $P_1^v, \ldots, P_n^v \vdash C$; $P_1^v, \ldots, P_n^v \vdash D$. Dle lemmatu 2.5 (e) $\vdash C \to (\neg D \to \neg(C \to D))$. 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 2.8 POSTOVA VĚTA O ÚPLNOSTI
Formule dokazatelná ve výrokové logice jsou právě tautologie. Jinými slovy — pro lib. výrokovou formuli A platí $\vdash A$, právě když $\models A$.

Důkaz:

"$\Rightarrow$": Jestliže $\vdash A$, pak $\models A$ podle věty 2.2 (o korektnosti).

"$\Leftarrow$": Předpokládejme tedy naopak, že $\models A$.
Nechť $P_1, \ldots, P_n$ jsou všechny prvotní formule vyskytující se v A. Nechť w je lib. ohodnocení prvotních formulí.
Pak podle lemmatu 2.7 máme: $P_1^w, \ldots, P_n^w \vdash A$, neboť A^w je A poněvadž $\overline{w}(A) = 1$ (A je tautologie).
Nechť v je ohodnocení prvotních formulí takové, že:
$v(P_i) = w(P_i)$ pro $i = 1 \ldots n-1$
$v(P_n)$ je opačná oproti $w(P_n)$.
Pak opět podle lemmatu 2.7: $P_1^v, \ldots, P_n^v \vdash A$. Jinak napsáno, máme:

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

$$P_1^v, \ldots, P_{n-1}^v, \neg P_n^v \vdash A$$

. Podle lemmatu 2.6 dostáváme: $P_1^v, \ldots, P_{n-1}^v \vdash A$ pro lib. ohodnocení v. Opakujeme-li tento postup ještě $(n-1)$ krát, dokážeme $\vdash A$.

□

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

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 dané oblasti mohou být některé význačné objekty (0, neutrální prvek grupy,...) pro něž užíváme zvláštní symboly — ***konstanty***. (př. $0, 1, \ldots$).

S objekty daného oboru lze provádět různé operace (sčítání,násobení čísel, násobení v grupách,...). K označení operací užíváme *funkční symboly* $(f, g, h, \ldots, f_1, f_2, f_3, \ldots)$ Příklad: $+, ., \ldots$

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 nimi. Vlastnosti a vztahy mezi objekty daného oboru, tzv. *predikáty*, ("být záporným číslem" (vlastnost), "být menší než", "být prvkem" (vztahy)) vyjadřujeme pomocí *predikátových symbolů* $(p, q, r, \ldots, p_1, p_2, \ldots)$ Příklad: $\leq, \in$

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 rovnosti označující rovnost, tj. totožnost objektů z daného oboru.

Z uvedených 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.

Příklady:

- $\forall x(x.0 = 0)$ v $\mathbf{R}$ vyjadřuje "Pro každé reálné číslo x platí, že $x.0 = 0$"
- $\exists(\neg(x = 1)\&(x.x = 1))$ vyjadřuje "Existuje reálné číslo x takové, že $x \neq 1$ a $x^2 = 1$"
- $\forall x \exists y(x < y)$ vyjadřuje "Pro každé x existuje y, které je větší než x"

Uvedené symboly spolu s *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: 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 1. řádu

Specifiku jazyka určují jeho funkční a predikátové symboly (určují oblast, kterou jazyk popisuje).

logické symboly

$x, y, \ldots, x_1, x_2, \ldots$	proměnné
$\neg, \&, \vee, \to, \equiv$	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. Jazyk predikátové logiky je tedy určen výčtem svých speciálních symbolů.

Příklady:

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 . pro grupovou operaci násobení
3) Jazyk teorie okruhů
   - ⋆ jazyk s rovností =
   - ⋆ dvě konstanty $0, 1$
   - ⋆ dva binární funkční symboly $+, .$
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
     $+, .$ — 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.
Příklady: V jazyce elementární aritmetiky jsou následující výrazy termy:
x,y proměnné
0 konstanta
$S(0), S(x), S(S(0))$
$x + y, x + 0, x.y, x.S(x), (x + S(y)).y, (S(0) + (x.y)).S(x)$
Poznamenejme, že u vžitých funkčních symbolů místo $+(x, y)$ píšeme $x + y$, místo $.(x, y)$ píšeme $x.y$

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: jsou-li t_1, t_2 termy, pak $(t_1 = t_2)$ je atomická formule. Píšeme $(t_1 = t_2)$ místo $= (t_1, t_2)$.
Příklady:
V jazyce teorie uspořádání jsou atomické formule $x < x, x < y$.
V jazyce elementární aritmetiky je atomická formule $x.(y + z) = (x.y) + (x.z)$

3.1.3 Formule

(i) Každá atomická formule je formule

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

Příklady:
V jazyce teorie uspořádání je formule $\forall x\forall y(x < y \to \exists(x < z\&z < y))$
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 $(\forall x\varphi)$ nebo $\exists x\varphi$. V tom případě se podformule φ nazývá *obor kvantifikátoru* $\forall x$ nebo $\exists x$, proměnná x se vyskytuje v kvantifikátoru samém nebo ve formuli φ. V opačném případě (výskyt není vázaný) řekneme, že daný výskyt proměnné x ve formuli φ je volný. Proměnná x se nazývá *volnou proměnnou* ve formuli φ, existuje-li její volný výskyt v této formuli. Formule neobsahující žádnou volnou proměnnou se nazývá *uzavřená formule* nebo též *výrok*.

Příklad:
Proměnná x má ve formuli $\underbrace{x}_{voln} = z \to (\exists x(\underbrace{x(x}_{vzan} = z))$ dva vázané výskyty a jeden volý výskyt.

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, 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 odpovídající dané konstantě.

Příklady:

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 množiny vybavené jedinou binární relací. (Lze chápat jako orientované grafy.)

3. Obsahuje-li jazyk L jediný binární funkční symbol, dostáváme grupoidy (tj. množiny vybavené 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 a $m \in M$, potom ohodnocení proměnných, které proměnné x přiřazuje prvek m a na všech ostatních proměnných 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, označované $t[e]$, 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, $t_1, \ldots, t_n$ 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 splňující $e(x_1) = m_1, \ldots, e(x_n) = m_n$) 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; $t_1, \ldots, t_n$ 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 $(\eta \& \psi), (\eta \vee \psi), (\eta \rightarrow \psi), (\eta \equiv \psi)$, kde η, ψ jsou formule, klademe:
$\mathcal{M} \models (\eta \& \psi)$ právě když současně $\mathcal{M} \models \eta[e]$ a $\mathcal{M} \models \psi[e]$
$\mathcal{M} \models (\eta \vee \psi)$ 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 jejich 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 $\mathcal{M}$.

Definice 4.5

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

Otázku, zda daná formule φ je logicky platná, nelze rozhodnout konečnou procedurou.
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

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

$$(\exists x(\varphi \& \psi)) \rightarrow (\exists x\varphi)\&(\exists x\psi)$$

logicky platné formule jazyka L.

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

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

- Jestliže $\mathcal{M} \not\models (\forall x(\varphi \rightarrow \psi))[e]$ jsme hotovi.
- Jestliže $\mathcal{M} \models (\forall x(\varphi \rightarrow \psi))[e]$, pak $\mathcal{M} \models (\varphi \rightarrow \psi)[e(x/m)]$ 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 $\mathcal{M} \models (\varphi \rightarrow (\forall x\varphi))[e]$ 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 v tomto případě máme $\mathcal{M} \models (\forall x(\varphi \rightarrow \psi)) \rightarrow (\varphi \rightarrow (\forall x\psi))[e]$.

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 $(\varphi \equiv \psi)$ je logicky platná formule.
Příklady dvojic logicky ekvivalentních formulí pro libovolné formule φ, ψ a proměnnou x jsou

$(\exists x\varphi)$	$\neg(\forall x(\neg\varphi))$
$(\forall x\varphi)$	$\neg(\exists x(\neg\varphi))$
$(\forall x\varphi)\&(\forall x\psi)$	$\forall x(\varphi \& \psi)$
$(\exists x\varphi) \vee (\exists x\psi)$	$\exists x(\varphi \vee \psi)$

dvojice logicky ekvivalentních formulí.

Důsledek 4.7

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 log. 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 4.1
V jazyce elementární aritmetiky term $S(S(y))$ není substituovatelný za x do formule $x \neq 0 \to \exists y(x = S(y))$.

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

Tvrzení 4.1
Je-li φ formule, x proměnná a t term substituovatelný za x do φ, pak $(\forall x\varphi) \to \varphi_x[t]$; $\varphi_x[t] \to \exists x\varphi)$ 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 $\mathcal{M} \models ((\forall x\varphi \to \varphi_x[t])[e]$.
Jestliže $\mathcal{M}(\forall x\varphi)[e]$, 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 $\mathcal{M} \models ((\forall x\varphi) \to \varphi_x[t])[e]$. □

5 Axiomy predikátové logiky

Budujeme predikátovou logiku jako formální axiomatický systém. Jazyl L predikátové logiky přebíráme z předchozího s tím, že z logických spojek bereme jako základní $\neg$ a $\to$ (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 pouze na ty formule, které jsou vytvořeny z atomických formulí jen pomocí spojek $\neg$, $\to$ a kvantifikátoru $\forall$. Axiomy predikátové logiky lze rozdělit do čtyř skupin.

5.1 schemata výrokových axiomů

Jsou-li φ, ψ, η formule jazyka L, pak

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

$$(\varphi \to (\psi \to \eta)) \to ((\varphi \to \psi) \to (\varphi \to \eta))$$

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

jsou axiomy predikátové logiky.

5.2 schema axiomu kvantifikátoru

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

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

je axiom predikátové logiky.

5.3 schema axiomů substituce

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

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

je axiom predikátové logiky.

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

5.4 schemata 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

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

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 z formule φ se 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 každé i formule φ_i je 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, kde poslední formule je φ taková, že 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: Spolu se schematy výrokových axiomů a pravidlem odloučení přechází do predikátové logiky celá výroková logika. Zejména: je-li A tautologie výrokové logiky, a je-li φ formule jazyka L vzniklá dosazením formulí jazyka L za prvotní formule A, pak $\vdash \varphi$.

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.

Věta 5.1 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 $i = 1 \ldots n$.

- Je-li φ_i výrokový axiom, je to zřejmé.
- Je-li φ_i axiom kvantifikátoru, pak viz. příklad 3 na straně 13.
- Je-li φ_i axiom substituce, pak viz tvrzení 4.1 na straně 14
- Zřejmý je i případ axiomů rovnosti.
- Vznikla-li formule φ 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 $(\forall x\varphi_j)$ pro nějakou proměnnou x a dle indukčního předpokladu $\mathcal{M} \models \varphi_j$. To ale podle definice splňování ohodnocení dává: $\mathcal{M} \models (\forall x\varphi_j)$ a to je $\mathcal{M} \models \varphi_i$.

□

V následující kapitole dokážeme opak věty 5.1 (opačný směr). Ukážeme tak, že formule dokazatelné v predikátové logice jsou právě logicky platné formule — tzn. věta O úplnosti predikátové logiky: formální systém predikátové logiky je úplný — dovoluje odvodit právě všechny logicky platné formule.

K tomu účelu vybudujeme prostředky:

Lemma 5.2 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 5.3 PRAVIDLO $\exists$

Je-li $\vdash \varphi \to \psi$ a proměnná x nemá volný výskyt v ψ, pak $\vdash (\exists x\varphi) \to \psi$

Důkaz:

$\vdash \neg\psi \to \neg\varphi$ je tautologický důsledek $\varphi \to \psi$. Užitím pravidla $\forall$ dostaneme $\vdash \neg\psi \to (\forall x(\neg\varphi))$. $(\forall x(\neg\varphi)) \to \psi$ je tautologický důsledek předchozí formule, což je $\vdash (\exists x\varphi) \to \psi$ dle definice zkratky $\exists$. □

Pravidlo $\exists$ je duální pravidlu $\forall$.

Lemma 5.4

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.
$\vdash \neg\neg(\forall x(\neg\varphi))$ 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. □

Poznámka 5.5

Formule $\neg\psi \to \neg\varphi$ je tautologickým důsledkem formule $\varphi \to \psi$. Skutečně formule $(\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$ vznikla dosazením do tautologie $(A \to B) \to (\neg B \to \neg A)$. Stačí použít pravidlo odloučení.

Podobně: Složení implikací $\varphi \to \psi$ a $\psi \to \eta$ je formule $\varphi \to \eta$ jako jejich tautologický důsledek. Skutečně $(\varphi \to \psi) \to ((\psi \to \eta) \to (\varphi \to \eta))$ vzikne dosazením do tautologie, stačí užít dvakrát pravidlo odloučení.

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 $t_1,\ldots,t_n$ substituovatelný $x_1,\ldots,x_n$ 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 $t_1,\ldots,t_2$ 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 $\psi_{x_1,\ldots,x_n}[t_1,\ldots,t_n]$, tj. s φ'. □

Z axiomů substituce pro libovolnou formuli ψ a libovolnou proměnnou z speciálně dostaneme $\vdash (\forall z\psi) \to \psi$ neboť $\psi_z[z]$ je ψ.

Je-li nyní φ libovolná formule a $x_1, \ldots, x_n$ proměnné, pak odtud 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 5.7

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 5.8 O UZÁVĚRU

Je-li T množina formulí, je-li 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 5.9 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 $\vdash \varphi \to \psi$.
$\vdash (\forall x\varphi) \to (\forall x\psi)$ plyne odtud užitím pravidla $\forall$
$\vdash \psi \to (\exists x\psi)$ podle lemmatu 5.4
$\vdash \varphi \to (\exists x\psi)$ je tautologický důsledek předpokladu $\vdash \varphi \to \psi$ a předchozí formule (jejich složení)
$\vdash (\exists x\varphi) \to (\exists x\psi)$ plyne odtud užitím pravidla $\exists$ □

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

Věta 5.10 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, ψ. 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; $i < j$ pravidlem zobecnění. Tedy φ_j je tvaru $(\forall x\varphi_j)$ pro některou proměnnou x

Z indukčního předpokladu $T \vdash \varphi \to \varphi_i$. Poněvadž φ je uzavřená formule, neobsahuje volný výskyt proměnné x, 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 5.11 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.
Je-li $T \vdash \varphi_{x_1,\ldots,x_n}[c_1, \ldots, c_n]$:
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 ani 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 $\varphi_{x_1,\ldots,x_n}[c_1, \ldots, c_n]$ 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 lemmatu5.6. □

Odvodíme nyní několik důsledků axiomů rovnosti. První axiom rovnosti vyjadřuje reflexivitu rovnosti.

Lemma 5.12

Je-li L jazyk s rovností, pak

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

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

Důkaz: Použijeme 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) dostáváme symetrii rovnosti. Podobně z třetího axiomu rovnosti: $\vdash y = x \to (z = z \to (y = z \to x = z))$ Odtud užitím postupů výrokové logiky $\vdash z = z \to (y = x \to (y = z \to x = z))$ nyní s použitím prvního axiomu rovnosti pravidla odloučení $\vdash y = x \to (y = z \to x = z)$ složením této implikace se symetrií rovnosti vychází jako tautologický důsledek tranzitivita rovnosti. □

Lemma 5.13

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

Důkaz: Uvedené formule jsou instancemi axiomů rovnosti a formulí v lemmatu 5.12 stačí tedy užít lemma 5.6 □

Definice 5.14

Je-li L jazyk 1. řádu a T množina formulí jazyka L říkáme, že T je *teorie 1. řádu* s jazykem L. 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, jakmile pro nějakou formuli ψ jazyka L platí $T \vdash \psi$ a současně $T \vdash \neg\psi$. Pak totiž, poněvadž $\vdash (\neg\psi) \to (\psi \to \varphi)$ — vznik dosazením do tautologie $\neg A \to (A \to B))$ — užitím pravidla odloučení odvodíme $T \vdash \varphi$.

Důsledek 5.15

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 5.8 o uzávěru $T \vdash \varphi'$, 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: $T \cup \{\neg\varphi'\} \vdash \varphi'$, odkud z věty o dedukci (věta 5.10) $T \vdash (\neg\varphi') \to \varphi'$. 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. □

Poznámka 5.16

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 $\neg, \&, \exists$. (Spojka $\psi \to \eta$ se rozepíše $\neg(\psi \& \neg\eta)$, 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 & a kvantifikátor $\exists$ chápou jako zkratky obvyklým způsobem, takže vznikne opět formule obsahující jen logické spojky $\neg, \to$ a kvantifikátor $\forall$. Pak platí $\vdash \varphi \equiv \overline{\varphi}$, 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 5.9).

6 Věta o úplnosti

Definice 6.1
Buď L jazyk 1. řádu. Připomeňme, že lib. množinu T formulí jazyka L nazýváme teorií 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 6.2
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 6.3
Řekneme, že formule φ je *důsledkem teorie* T, jestliže pro každý model $\mathcal{M}$ teorie T je $\mathcal{M} \models \varphi$. Pak píšeme $T \models \varphi$.

Příklady:

1) Mějme jazyk teorie uspořádání. Speciální axiomy:
$\neg(x < x)$
$x < y \rightarrow (y < z \rightarrow x < z)$
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:
$x.(y.z) = (x.z).z$
$x.1 = x$ (pravý neutrální prvek)
$\forall x \exists y (x.y = 1)$ (pravý inverzní prvek)
již určují teorii grup. Modely této teorie jsou právě grupy. Je možno ukázat, že formule
$1.x = x$
$\forall x \exists y (y.x = 1)$
jsou důsledky této teorie.

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

Věta 6.4 O KOREKTNOSTI
Je-li T teorie s jazykem L, je-li 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 o korektnosti predikátové logiky v kapitole 5 na straně 14. □

Důsledek 6.5
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 6.4 to znamená, že $T \models \varphi$ i $T \models \neg\varphi$. Takže $\mathcal{M} \models \varphi$ i $\mathcal{M} \models \neg\varphi$, odkud $\mathcal{M} \models \varphi \& \neg\varphi$. To není možné. Tudíž T je bezesporná. □

Směřujeme k důkazu obrácení věty 6.4. Ukážeme, že syntax predikátové logiky je plně adekvátní její sémantice.

Věta 6.6 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 6.7 GÖDELOVA VĚTA O ÚPLNOSTI
Teorie T je bezesporná, právě když má nějaký model.

Důkaz: Věta 6.6 pomocí věty 6.7
Je-li T teorie a φ formule taková, že $T \vdash \varphi$, potom $T \models \varphi$ podle věty 6.4. 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 teorie T. To znamená, že teorie $T \cup \{\neg\varphi'\}$ nemá model. Podle věty 6.7 teorie $T \cup \{\neg\varphi'\}$ je sporná. Podle důsledku 5.15 to zamená $T \vdash$. □
Důkaz: samotné věty 6.7
S ohledem na důsledek 6.5 zbývá dokázat, že každá bezesporná teorie má nějaký model. Provedeme to nejprve ve speciálním případě. Pokračování důkazu je na straně 22. □

Definice 6.8
Řekneme, že teorie T s jazykem L je ***úplná***, jestliže T je bezesporná a pro každou uzavřenou formuli φ platí právě jedno: $T \vdash \varphi$ anebo $T \vdash \neg\varphi$.

Příklad 6.1
Buď $\mathcal{M}$ libovolná realizace jazyka L. Označme $Th(\mathcal{M})$ množinu všech uzavřených formulí jazyka L, které jsou pravdivé v $\mathcal{M}$. Pak $Th(\mathcal{M})$ je úplná teorie.

Definice 6.9
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 $T \vdash (\exists x\psi) \vdash \psi_x[c]$.

Lemma 6.10
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 5.13 (i),(ii),(iii) na straně 18) 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 $\tilde{t} = \{s \in C; s \sim t\}$. 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 $f_\mathcal{M}(\tilde{t}_1, \ldots, \tilde{t}_n) = \tilde{f}(t_1, \ldots, t_n)$,[1] $\tilde{t}_1, \ldots, \tilde{t}_n \in p_\mathcal{M}$ právě když $T \vdash p(t_1, \ldots, t_n)$. Z lemmatu 5.13 (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 $\mathcal{M} \models \varphi$ (je splněn). 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 $\mathcal{M} \models \varphi$. Stačí tedy dokážeme-li následující vlastnost: Pro libovolnou uzavřenou formuli φ jazyka L platí: $\mathcal{M} \models \varphi$ právě když $T \vdash \varphi$ (silnější tvrzení).

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 $\neg, \&$ a kvantifikátoru $\exists$ (to lze ospravedlnit poznámkou na konci kapitoly 5).

Indukce:

(i). 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 $T \vdash p(t_1, \ldots, t_n)$.

[1] to je třída !

(ii). 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 $T \vdash t_1 = t_2$.

(iii). 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 $T \vdash \neg\psi$, čili $T \vdash \varphi$.

(iv). Je-li φ formule tvaru $\psi \& \eta$, 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 totéž jako $T \vdash \psi \& \eta$ čili $T \vdash \varphi$ užitím postupů výrokové logiky.

(v). 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 $(\exists x \psi)$. $\mathcal{M} \models (\exists x \psi)[e]$ právě když existuje $\tilde{t} \in M$ takové, že $\mathcal{M} \models \psi[e(x/\tilde{t})]$, což je totéž jako $\mathcal{M} \models \psi_x[t][e]$ a to je $\mathcal{M} \models \psi_x[t]$ 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 toto nastane právě když $T \vdash (\exists x \psi)$, čili $T \vdash \varphi$. Je-li $T \vdash \psi_x[t]$, pak $T \vdash (\exists x \psi)$ (podle lemmatu 5.4 na straně 16 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 ukončen. □

Lemma 6.11

Pro libovolné formule φ, ψ a libovolnou proměnnou x, je-li $\vdash (\varphi \to (\exists x \psi))$ pak také $\vdash \exists x(\varphi \to \psi)$.

Důkaz: Užitím distribuce kvantifikátorů (lemma 5.9) na první výrokový axiom dostáváme $\vdash (\exists x \varphi) \to (\exists x(\varphi \to \psi))$. Podle lemmatu 5.4 máme $\vdash (\varphi \to \psi) \to (\exists x(\varphi \to \psi))$ Odtud spolu s tautologií $\neg\varphi \to (\varphi \vdash \psi)$ složením vychází $\vdash \neg\varphi \to (\exists x(\varphi \to \psi))$. Jako tautologický důsledek této a první formule důkazu dostaneme $\vdash (\varphi \to (\exists x \psi)) \to (\exists x(\varphi \to \psi))$. Zbývá použít pravidlo odloučení. □

Definice 6.12

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 φ jazyka L takovou, že $T' \vdash \psi$ je již $T \vdash \psi$.

Poznámka 6.13

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

Lemma 6.14 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 (že je rozšířením, je jasné).

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 5.3) odtud $T \vdash (\exists w((\exists x \eta) \to \eta_x[w]) \to (\varphi_1 \ldots \to (\varphi_n \to \psi)\ldots)$. Podle lemmatu 5.4 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 podle lemmatu 6.11 (aplikováno na formule $(\exists x \eta)$, $\eta_x[w]$ místo φ, ψ) máme $\vdash \exists w((\exists x \eta) \to \eta_x[w])$. Toto spolu s poslední dlouhou formulí užitím pravidla odloučení dává $T \vdash (\varphi_2 \to \ldots(\varphi_n \to \psi)\ldots)$. Opakováním tohoto postupu nakonec $T \vdash \psi$. □

Lemma 6.15
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 6.16 Linderbaum
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 6.15) 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 lib. uzavřená formule jazyka L. Připusťme, že $T' \nvdash \varphi$ a $T' \nvdash \varphi'$. Poněvadž $T' \nvdash \varphi$, podle důsledku 5.15 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: Pokračování důkazu Gödelovy věty 6.7 na straně 20
Máme ukázat, že bezesporná teorie T jazyka L má nějaký model. Podle lemmatu 6.14 existuje Henkinova teorie T_H tak, že je bezesporná, její jazyk L' je rozšířením jazyka L o množinu konstant. Podle věty 6.16 existuje úplné rozšíření T' teorie T_H s jazykem L'. Teorie T' je úplná a současně zůstává i Henkinova. Podel lemmatu 6.10 má teorie T' nějaký model $\mathcal{M}'$. Model $\mathcal{M}'$ je realizací jazyka L'. Nebudeme-li v $\mathcal{M}'$ vyznačovat prvky odpovídající přidaným konstantám z L', dostaneme tak realizaci $\mathcal{M}$ jazyka L, která je zřejmě modelem teorie T. □

7 Věta o kompaktnosti

Věta 7.1 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, viz. věta 6.7 a z lemmatu 6.15. □
Jako ukázku aplikace této věty uvedeme příklad o neaxiomatizovatelnosti.

Aplikace:
Uvažujme jazyk z teorie grup a teorii abelovských grup. Tuto teorii lze zadat konečným počtem speciálních axiomů: Grupa se nazývá periodickou grupou, jestliže je v ní splněno: $\forall x \exists n \geq 1 : x^n = 1$ kde x^n je zkratka pro term $\underbrace{x \cdot \ldots x}_{n}$. 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 7.1
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. 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 S má model, podle věty 7.1 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 není konečného řádu. □

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

Věta 7.2
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 6.7. Rozšíření L' jazyka L je konstruováno v lemmatu 6.14. 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 6.10. Poněvadž už množina termů jazyka L' nemá větší mohutnost než $max\{\aleph_0, |L|\}$, je vidět, že ani model nebude větší mohutnosti. □

Věta 7.3 LÖWONHEIN,SHOLLN
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 lib. 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 7.1 o kompaktnosti má tedy sama teorie S model, a tedy je bezesporná. Podle věty 7.2 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. □

Aplikace:
Existuje nestandardní model Peanovy aritmetiky. Skutečně, standardní model Peanovy aritmetiky je spočetný (tedy nekonečný). Podle věty 7.3 existuje model Peanovy aritmetiky libovolné mohutnosti $n \geq \aleph_0$. Je-li $n > \aleph_0$, je tento model nestandardní.

8 Prenexní tvary formulí

8.1 Normální tvar formulí

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

Lemma 8.1
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) $\vdash (\exists x_1) \ldots (\exists x_n) A \leftrightarrow (\exists x_{i_1}) \ldots (\exists x_{i_n}) A$

Věta 8.2 O UZÁVĚRU
Buď A formule taková, že proměnné $x_1, \ldots, x_n$ jsou jediné proměnné s volným výskytem v A.
Pak $\vdash A$ právě když $\vdash \forall x_1 \ldots \forall x_n A$.

Věta 8.3 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 $\vdash A \leftrightarrow A'$.

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 následující ekvivalence mezi formulemi, kterým se často zkráceně říká *prenexní operace*, protože se výrazně uplatňují při převodu formulí do tzv. prenexní formy.

Věta 8.4
Buď z proměnná, která není volná ve formuli A. Nechť $\circ$ je některá z výrokových spojek $\&, \vee, \rightarrow$. Pak platí

$$\vdash \forall z(A \circ B) \leftrightarrow (A \circ \forall zB)$$

$$\vdash \exists z(A \circ B) \leftrightarrow (A \circ \exists zB)$$

Pro implikaci $B \rightarrow A$, tj. v opačném pořadí (kvůli tomu, že z není volná v A, o vztahu z a B se nic nepředpokládá - pozn. makuba), naopak platí:

$$\vdash \forall z(B \rightarrow A) \leftrightarrow (\exists zB \rightarrow A)$$

$$\vdash \exists z(B \rightarrow A) \leftrightarrow (\forall zB \rightarrow A)$$

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 8.5
Nechť A je formule predikátové logiky. Formule A' je *variantou* formule A, jestliže vznikne z A postupným nahrazením podformulí tvaru (QxB) podformulemi $(QyB_x[y])$, kde Q je obecný nebo existenční kvantifikátor a y je proměnná nevyskytující se v B.

Příklad 8.1
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.

Věta 8.6
Je-li A' variantou formule A, pak je dokazatelné, že jsou ekvivalentní ($\vdash A \leftrightarrow A'$).

Definice 8.7
Formule A je v *prenexní formě*, 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)

Věta 8.8 PŘEKVAPIVÁ VĚTA
Ke každé formuli A lze sestrojit formuli A' v prenexní formě tak, že $\vdash A \leftrightarrow A'$.

8.1.1 Převedení formule na prenexní tvar

Návod explicitně vyjádříme jako výčet transformací, jejichž postupné užívání dovolí získat prenexní formu libovolné formule predikátové logiky. Abychom se v prenexní formě nemuseli vyhýbat použití spojek $\vee$ a $\&$, 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 $\forall xB$ nebo $\exists xB$, pokud se proměnná 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:

$$A \leftrightarrow B \dots (A \rightarrow B) \& (B \rightarrow A)$$

.

4. **Přesun negace dovnitř** — provádíme postupně náhrady podformulí podle schémat:
   $\neg(\forall xA) \quad \ldots \exists x \neg A$
   $\neg(\exists xA) \quad \ldots \forall x \neg A$
   $\neg(A \to B) \ldots A \& \neg B$
   $\neg(A \vee B) \ldots \neg A \& \neg B$
   $\neg(A \& B) \ldots \neg A \vee \neg B$
   $\neg(\neg A) \quad \ldots A$
   tak dlouho, až se spojka negace vyskytne nejvýše bezprostředně před atomickými formulemi.

5. **Přesun kvantifikátorů doleva** — pro B, ve které se nevyskytuje proměnná x, provádíme náhrady podle schémat:
   $(QxA) \vee B \ldots Qx(A \vee B)$
   $(QxA) \& B \ldots Qx(A \& B)$
   $(QxA) \to B \ldots \overline{Q}x(A \to B)$
   $B \to (QxA) \ldots Qx(B \to A)$

   kde $\overline{Q}$ je kvantifikátor "opačný" ke Q. Někdy lze snížit počet kvantifikátorů použitím schémat
   $(\exists xA) \vee (\exists yB) \ldots \exists x(A \vee B_y[x])$
   $(\forall xA) \& (\forall yB) \ldots \forall x(A \& B_y[x])$

Příklad 8.2
Hledejme prenexní formu formule $\forall y(\exists xP(x,y) \to \exists uR(y,u)) \to \forall xS(x,y)$, 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:
$A_1 : \forall y_2(\exists x_1 P(x_1,y_2) \to \exists uR(y_2,u)) \to \forall xS(x,y)$
$A_2 : \forall x(\forall y_2(\exists x_1 P(x_1,y_2) \to \exists uR(y_2,u)) \to S(x,y))$
$A_3 : \forall x \exists y_2((\exists x_1 P(x_1,y_2) \to \exists uR(y_2,u)) \to S(x,y))$
$A_4 : \forall x \exists y_2 \exists x_1((P(x_1,y_2) \to \exists uR(y_2,u)) \to S(x,y))$
$A_5 : \forall x \exists y_2 \exists x_1 \forall u((P(x_1,y_2) \to R(y_2,u)) \to S(x,y))$

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

9 Herbrandova věta

V celé kapitole 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 lib. ohodnocení proměnných e je $\mathcal{M} \not\models \varphi[e]$. Formule 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 $\varphi(t_1, \ldots, t_n)$.

Věta 9.1 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 $t_1^1, \ldots, t_n^1, \ldots, t_1^{\mathcal{M}}, \ldots, t_n^{\mathcal{M}}$ takové, že $\varphi(t_1^1, \ldots, t_n^1) \& \ldots \& \varphi(t_1^{\mathcal{M}}, \ldots, t_n^{\mathcal{M}})$ je kontradikce.

Buď L jazyk obsahující alespoň jednu konstantu. Pak označme H neprázdnou množinu všech termů bez proměnných jazyka L. *Herbrandova realizace* jazyka L je každá realizace $\mathcal{H}$ vyhovující podmínkám

1. její univerzum je množina H
2. pro každý funkční symbol f četnosti n příslušná operace $f_{\mathcal{H}} : H_n \to H$ je dána tak, že pro každá $t_1, \ldots, t_n \in H$ je $f_{\mathcal{H}}(t_1, \ldots, t_n) = f(t_1, \ldots, t_n)$.

Relace na H odpovídající predikátovým symbolům jazyka L přitom nepodléhají žádným omezením.

Buď Q množina všech atomických formulí bez proměnných jazyka L, tj. množina všech formulí tvaru $p(t_1, \ldots, t_n)$, kde p je predikátový symbol četnosti n a $t_1, \ldots, t_n \in H$. Existuje vzájemně jednoznačná korespondence mezi Herbrandovými realizacemi jazyka L a pravdivostními ohodnoceními množiny Q. Přitom Herbrandově realizaci H odpovídá pravdivostní ohodnocení v, které popisuje interpretaci predikátových symbolů v realizaci H takto: pro každou formuli $p(t_1, \ldots, t_n)$ z Q je $v(p(t_1, \ldots, t_n)) = 1$ právě když $(t_1, \ldots, t_n) \in P_{\mathcal{H}}$, kde $P_{\mathcal{H}} \subseteq H^n$ je relace příslušející predikátovému symbolu P. Pak zřejmě pro každou otevřenou formuli ψ jazyka L bez proměnných je $\overline{v}(\psi) = 1$ právě když $\mathcal{H} \models \psi$. (ψ je splněna v realizaci $\mathcal{H}$).

Lemma 9.2

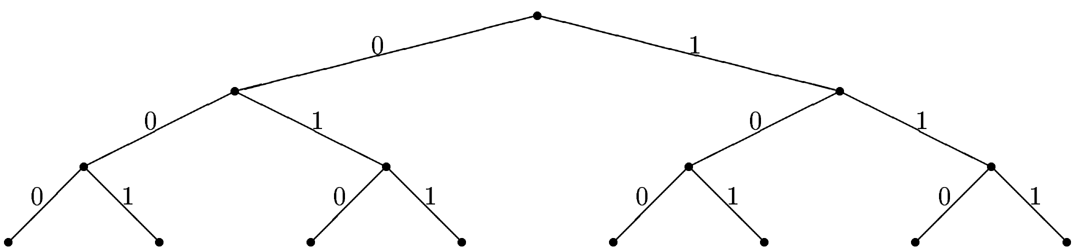
Je-li $\varphi(x_1, \ldots, x_n)$ otevřená formule jazyka L obsahujícího alespoň jednu konstantu, pak uzávěr formule $(\forall x_1 \ldots \forall x_n \varphi(x_1, \ldots, x_n))$ je sporný právě když pro každou Herbrandovu realizaci $\mathcal{H}$ jazyka L je $\mathcal{H} \not\models (\forall x_1 \ldots \forall x_n \varphi(x_1 \ldots x_n))$.

Důkaz: Přímý směr je zřejmý. Abychom dokázali opačný směr, předpokládejme, že formule není sporná. Tedy existuje realizace $\mathcal{M}$ jazyka L taková, že $\mathcal{M} \models \varphi$. Pro každý term $t \in H$ nechť $\chi(t)$ je hodnota termu t v realizaci $\mathcal{M}$. Tím je dáno zobrazení $\chi : H \to M$, kde M je univerzum realizace $\mathcal{M}$. Definujme dále pravdivostní ohodnocení v formulí z Q takto: Je-li p n-ární predikátový symbol a $t_1, \ldots, t_n \in H$ klademe $v(p(t_1, \ldots, t_n)) = 1$ právě když $\chi(t_1), \ldots, \chi(t_n) \in p_{\mathcal{M}}$. Nechť nyní $\mathcal{H}$ je Herbrandova realizace jazyka L odpovídající pravdivostnímu ohodnocení v. Ukážeme, že $\mathcal{H} \models \varphi$. Pro libovolné ohodnocení proměnných e v $\mathcal{H}$ máme ukázat, že $\mathcal{H} \models \varphi[e]$. Je-li $e(x_1) = t_1, \ldots, e(x_n) = t_n$, znamená to zřejmě totéž jako $\mathcal{H} \models \varphi(t_1, \ldots, t_n)$. To je ekvivalentní $\overline{v}(\varphi(t_1, \ldots, t_n)) = 1$ (viz poznámka před lemmatem). To je s ohledem na definici ohodnocení v ekvivalentní $\mathcal{M} \models \varphi(t_1, \ldots, t_n)$ což je totéž jako $\mathcal{M} \models \varphi[\overline{e}]$, kde $\overline{e}$ je ohodnocení proměnných v $\mathcal{M}$ takové, že $\overline{e}(x_1) = \chi(t_1), \ldots, \overline{>}e(x_n) = \chi(t_n)$. To je ale splněno, neboť $\mathcal{M} \models \varphi$. Takže $\mathcal{H} \models \varphi$ — spor. □

Poznámka 9.3

Z důkazu je vidět, že otevřená formule $\varphi(x_1, \ldots, x_n)$ je splněna v Herbrandově realizaci $\mathcal{H}$ právě tehdy, když pro každá $t_1, \ldots, t_n \in H$ je $\mathcal{H} \models \varphi(t_1, \ldots, t_n)$, a to je právě když $\overline{v}(\varphi(t_1, \ldots, t_n)) = 1$, kde v je pravdivostní ohodnocení odpovídající realizaci $\mathcal{H}$.

Zavedeme pomocný pojem: Řekneme, že jazyk L predikátové logiky je *standardní*, obsahuje-li alespoň jeden, ale nanejvýš konečný počet predikátových symbolů a dále buď alespoň jeden funkční symbol kladné četnosti a alespoň jednu konstantu, dohromady však nanejvýš konečný počet funkčních symbolů a nebo pouze spočetnou množinu konstant. Standartní jazyk má spočetnou množinu H termů bez proměnných a také spočetnou množinu Q atomických formulí bez proměnných. Všechny atomické formule bez proměnných standardního jazyka lze tedy nějakým způsobem uspořádat do nekonečné posloupnosti $\pi_1, \pi_2, \ldots$.



Nekonečný strom, uzly rozděleny do úrovní $0, 1, 2, \ldots$, každá hrana je označena číslem $0, 1$. Každý uzel má dva následníky, každý uzel vyjma jediného uzlu úrovně 0, má jediného předchůdce. Větev stromu π je nekonečná posloupnost uzlů $U = U_0 U_1 U_2 \ldots$, kde uzel U je úrovně i pro $i = 0, 1, 2, \ldots$ a pro každé $i > 0$ uzly U_{i-1} a U_i jsou spojeny hranou. Větve stromu $\mathcal{A}$ vzájemně jednoznačně odpovídají nekonečným posloupnostem $\underline{\alpha} = \alpha_1 \alpha_2 \ldots$ čísel $0, 1$; příslušná větev

$U = U_1U_1\ldots$ je dána tak, že U_0 je jediný uzel úrovně 0 a pro každé $i > 0$ je U_i ten z následníků uzlu U_{i-1}, který je s ním spojen hranou označenou číslem α_i.

Buď Q spočetná množina všech atomických formulí bez proměnných standardního jazyka L uspořádaná do nekonečné posloupnosti $\pi_1, \pi_2, \ldots$ pak existuje vzájemně jednoznačná korespondence mezi pravdivostními ohodnoceními v množině Q a nekonečnými posloupnostmi $\underline{\alpha} = \alpha_1\alpha_2\ldots$ čísel $0, 1$; totiž posloupnosti $\underline{\alpha}$ odpovídá ohodnocení v, v němž pro každé ß $= 1, 2, \ldots$ je $V(\pi_i) = 1$ právě když $\alpha_i = 1$. Poněvadž pravdivostním ohodnocením množiny Q odpovídají Herbrandovy realizace jazyka L a posloupnostem čísel $0, 1$ odpovídají větve binárního stromu $\mathcal{A}$, dostáváme vzájemně jednoznačnou korespondenci mezi Herbrandovými realizacemi jazyka L a větvemi binárního stromu $\mathcal{A}$. Je-li N větev binárního stromu $\mathcal{A}$, označme w_N příslušné pravdivostní ohodnocení množiny Q.

Buď V uzel stromu $\mathcal{A}$ úrovně 0. Pak pro každý uzel U stromu $\mathcal{A}$ úrovně j existuje jediná posloupnost uzlů $U_0, U_1, \ldots, U_j$ taková, že $U_0 = V, U_j = U$ a pro každé $i = 1, \ldots, j$ uzly U_{i-1} a U_i jsou spojeny hranou. Tato poslounost uzlů určuje posloupnost $\alpha_1, \ldots, \alpha_j$ čísel $0, 1$ tak, že pro každé $i = 1, \ldots, j$ je α_i označení hrany spojující uzly U_{i-1}, U_i tím je dána jednoznačná korespondence mezi uzly úrovně j a posloupnostmi čísel $0, 1$ délky j.

Pro každé $j \geq 0$ je *částečné pravdivostní ohodnocení* hloubky j libovolné zobrazení $w : \{\pi_1, \pi_2, \ldots, \pi_j\} \to \{0, 1\}$. Na ostatních formulích z Q není zobrazení w definováno. Existuje vzájemně jednoznačná korespondence mezi těmito částečnými ohodnoceními a posloupnostmi $\alpha_1, \ldots, \alpha_2$ čísel $0, 1$. Těmto posloupnostem jednoznačně odpovídají uzly stromu $\mathcal{A}$. Dostáváme vzájemně jednoznačnou korespondenci mezi částečnými pravdivostními ohodnoceními hloubky j a uzly binárního stromu $\mathcal{A}$ úrovně j.

Označme w_U částečné pravdivostní ohodnocení odpovídající uzlu U. Poznámka: Je-li N některá větev stromu $\mathcal{A}$ a je-li U některý její uzel, pak částečné ohodnocení w_U splývá s w_N na těch formulích z Q, pro něž je definováno.

Buď $\varphi(x_1, \ldots, x_n)$ otevřená formule standardního jazyka L. Řekneme, že uzel U binárního stromu $\mathcal{A}$ je *vyvracejícím uzlem* formule φ, existují-li termy $t_1, \ldots, t_n \in H$ takové, že pro každou atomickou formuli π obsaženou ve formuli $\varphi(t_1, \ldots, t_n)$ je definováno $w_u(\pi)$, takže je definováno $\overline{w_u}(\varphi(t_1, \ldots, t_n))$ a přitom vychází $\overline{w_u}(\varphi(t_1, \ldots, t_n)) = 0$.

Nechť nyní $\mathcal{A}_\varphi$ je množina všech uzlů stromu $\mathcal{A}$, které nejsou vyvracejícími uzly formule φ. Uzel V úrovně 0 leží v $\mathcal{A}_\varphi$ ($\overline{w}$ není definováno). Je-li U uzel úrovně j ležící v $\mathcal{A}_\varphi$ a je-li $U_0U_1\ldots U_j$ jediná posloupnost uzlů spojující uzly V a U, pak také každý z uzlů této posloupnosti leží v $\mathcal{A}_\varphi$. Tvoří tedy $\mathcal{A}_\varphi$ jakýsi "začátek" ve stromu $\mathcal{A}$, který sám je stromem. Je-li U některý uzel stromu $\mathcal{A}_\varphi$ úrovně j, označme $[U]_\varphi$ množinu všech těch uzlů U' stromu $\mathcal{A}_\varphi$ úrovní $k \geq j$, které leží pod uzlem U, tj. takových, že existuje posloupnost $U_jU_{j+1}\ldots U_k$ uzlů spojujících U s U'.

Lemma 9.4

Je-li $\varphi(x_1, \ldots, x_n)$ otevřená formule standardního jazyka L taková, že formule $\forall x_1 \ldots \forall x_n \varphi(x_1, \ldots, x_n))$ je sporná, pak strom $\mathcal{A}_\varphi$ je konečný.

Poznámka 9.5

Platí i obrácené tvrzení — nebudeme potřebovat.

Důkaz: sporem

Připusťme, že strom $\mathcal{A}_\varphi$ je nekonečný, má nekonečně mnoho uzlů. Indukcí sestrojíme nekonečnou větev $U = U_0U_1\ldots$ stromu $\mathcal{A}$ ležící v $\mathcal{A}_\varphi$ takovou, že pro každé $i = 0, 1, \ldots$ bude množina $[U_i]_\varphi$ nekonečná. Za U_0 vezmeme uzel úrovně 0. Pak množina $[U_0]_\varphi \mathcal{A}_\varphi$ je nekonečná. Máme-li již sestrojen uzel U_i, pak množina $[U_i]_\varphi$ je nekonečná, takže alespoň jeden z obou následníků uzlu U_i, označme ho W, musí mít tu vlastnost, že leží v $\mathcal{A}_\varphi$ a množina $[W]_\varphi$ je nekonečná. Vezmeme W a U_{i+1}. Takto dostáváme větev $U = U_0U_1\ldots$. Jí odpovídá jistá Herbrandova realizace $\mathcal{H}$ jazyka L. Poněvadž formule $\forall x_1 \ldots \forall x_n \varphi(x_1, \ldots, x_n))$ je sporná, není splněna v $\mathcal{H}$ a tedy existují termy $t_1, \ldots, t_n \in H$ takové,že $\mathcal{H} \not\models \varphi(t_1, \ldots, t_n)$, To znamená, že $\overline{w_U}(\varphi(t_1, \ldots, t_n)) = 0$. Formule $\varphi(t_1, \ldots, t_n)$ obsahuje konečně mnoho atomických formulí, tedy jistě existuje uzel U_i větve U takový, že pro každou tuto atomickou formuli π je definováno $w_{U_i}(\pi)$. Pak ovšem $\overline{w_{U_i}}(\varphi(t_1, \ldots, t_n)) = 0$. To znamená, že U_i je vyvracejícím uzlem formule φ. To je spor, neboť větev U celá leží v $\mathcal{A}_\varphi$. □

Důkaz: věty 9.1

Nechť nejprve formule $\forall x_1 \ldots \forall x_n \varphi(x_1, \ldots, x_n))$ je sporná. Buď L_φ jazyk obsahující jen ty funkční a predikátové symboly, které se vyskytují ve φ. Z L_φ je možno přidáním nejvýše spočetně mnoha konstant vytvořit standardní jazyk $\overline{L}_\varphi$. Pak φ je formule jazyka $\overline{L}_\varphi$. Podle lemmatu 9.4 je strom $\mathcal{A}\varphi$ konečný. Buď $\{V_1, \ldots, V_m\}$ konečná množina všech těch vyvracejících uzlů formule φ, jejichž předchůdci leží v $\mathcal{A}_\varphi$. Pak pro každý z těchto uzlů V_i existují termy $t'_1, \ldots, t'_n \in H$ jazyka $\overline{L}_\varphi$ takové, že $\overline{w}_{V_i}(\varphi(t'_1, \ldots, t'_n))$ je definováno a rovno 0. Ukážeme, že pak $\varphi(t^1_1, \ldots, t^1_n) \& \ldots \& \varphi(t^m_1, \ldots, t^m_n)$ je kontradikce. Buď v libovolné pravdivostní ohodnocení množiny Q a nechť U je větev stromu $\mathcal{A}$ pro niž $w_U = v$. Tato větev musí obsahovat jeden z uzlů $V_1, \ldots, V_n$, nechť je to uzel V_i. Pak $\overline{w}_{V_i}(\varphi(t'_1, \ldots, t'_n)) = 0$, odkud plyne

$\overline{v}(\varphi(t'_1,\ldots,t'_n)) = 0$, tím spíše $\overline{v}(\varphi(t_1^1,\ldots,t_n^1)\&\ldots\&\varphi(t_1^m,\ldots,t_n^m)) = 0$, jde tedy o kontradikci. Nakonec, obsahují-li uvedené termy některé nově přidané konstanty, získáme z nich termy jazyka L_φ tak, že v nich každou novou konstantu nahradíme některou proměnnou; přitom vlastnost kontradikce zůstává zachována.

Nechť naopak termy $t_1^1,\ldots,t_n^1,\ldots,t_1^m,\ldots,t_n^m$ jazyka L jsou takové, že $\varphi(t_1^1,\ldots,t_n^1)\&\ldots\&\varphi(t_1^m,\ldots,t_n^m)$ je kontradikce. Můžeme předpokládat, že termy jsou bez proměnných, tedy i formule je bez proměnných. V opačném případě bychom rozšířili jazyk L přidáním nových konstant a nahradili bychom v termech proměnné konstantami. Tím se vlastnost kontradikce neporuší. Buď nyní $\mathcal{H}$ libovolná Herbrandova realizace jazyka L. Nechť v je odpovídající pravdivostní ohodnocení formulí z Q. Pak $\overline{v}(\varphi(t_1^1,\ldots,t_n^1)\&\ldots\&\varphi(t_1^m,\ldots,t_n^m)) = 0$ odkud plyne, že pro některé $i = 1,\ldots,m$ je $\overline{v}(\varphi(t_1^i,\ldots,t_n^i)) = 0$. Takže $\mathcal{H} \not\models \varphi(t_1^i,\ldots,t_n^i)$, což znamená, že $\mathcal{H} \not\models (\forall x_1\ldots\forall x_n\varphi(x_1,\ldots,x_n))$. Podle lemmatu 9.2 je tedy formule $(\forall x_1\ldots\forall x_n\varphi(x_1,\ldots,x_n))$ sporná. □

Negováním formulí v obou částech věty 9.1 dostáváme tento obvyklý tvar Herbrandovy věty:

Věta 9.6 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. Skolemovských funkcí. A jestli neumřeli, tak tam šťastně žijí až dodnes ...