Tento text napsal Jan Pelc s použitím materiálů prof. Štěpánka. Tato verze byla vygenerována programem LaTeX dne 04.09.2008 v 23:06:19 hodin.

Použití pouze na vlastní nebezpečí!

Obsah

Část I
Výroková logika

1 Úvod do výrokové logiky

Výroková logika zkoumá formule, které vzniknou pomocí logických spojek. To, co tyto spojky spojují, ale už není předmětem jejího zájmu. Tyto tzv. *prvotní formule* či *výrokové proměnné* bere jako nedělitelné celky, u kterých nás zajímá pouze to, zda jsou pravdivé nebo nepravdivé, a tuto vlastnost jim navíc většinou přiřazujeme sami.

1.1 Definice. Nechť P je neprázdná množina, jejíž prvky budeme nazývat *výrokové proměnné* nebo *prvotní formule*. *Jazyk* L_P výrokové logiky nad množinou P obsahuje:

- Prvky množiny P.
- Symboly pro *logické spojky* – unární $\neg$ (negace) a binární $\&$ (konjunkce), $\vee$ (disjunkce), $\to$ (implikace) a $\leftrightarrow$ (ekvivalence).
- *Pomocné symboly* – závorky a jiné symboly bez sémantického významu. Pomáhají přehledně a jednoznačně zapsat formule jazyka.

1.2 Definice. Nechť L_P je jazyk výrokové logiky nad množinou prvotních formulí P. Každá *výroková formule* vznikne konečným počtem použití těchto induktivních pravidel:

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

(ii) Jsou-li výrazy A, B formule, jsou formule i výrazy:

$$\neg A \qquad (A \,\&\, B) \qquad (A \vee B) \qquad (A \to B) \qquad (A \leftrightarrow B)$$

1.3 Definice. Nechť A je formule. Podslovo B formule A, které je samo formulí, nazveme *podformule* formule A.

1.4 Poznámka. Přestože uvedená definice výrokových formulí stanovuje jednoznačná pravidla psaní závorek, není zpravidla nutné psát závorky všude. Především krajní závorky se zpravidla vynechávají a řetězec stejných binárních logických spojek se chápe jako uzávorkován *zprava* (toto pravidlo se v tomto textu mlčky používá opravdu hodně). Tedy:

$$p_1 \to p_2 \to \ldots \to p_{n-1} \to p_n \qquad \text{znamená} \qquad (p_1 \to (p_2 \to \ldots (p_{n-1} \to p_n) \ldots))$$

2 Sémantika výrokové logiky

Sémantika zkoumá pravdivost formulí, jejich význam či interpretaci. Výrokové formule jsou konstruovány nad množinou prvotních formulí, které však sama výroková logika neanalyzuje. Proto musí být pravdivost těchto výrokových proměnných dána zvnějšku. Pravdivost formulí se pak určí z pravdivosti výrokových proměnných na základě významu logických spojek.

2.1 Definice. Nechť P je množina prvotních formulí jazyka L_P a F množina všech formulí jazyka L_P.

- *Množina pravdivostních hodnot* je dvouprvková a sestává se z hodnot 1 (true, pravda) a 0 (false, nepravda).
- *Pravdivostní ohodnocení* (valuace) prvotních formulí je zobrazení $v : P \to \{0, 1\}$, které každé prvotní formuli přiřadí pravdivostní hodnotu.
- *Pravdivostní hodnota formule A při ohodnocení v* je zobrazení $\bar{v} : F \to \{0, 1\}$, které jednoznačně rozšiřuje v na množinu všech formulí F a které je definováno induktivně:
  - Je-li A výroková proměnná, je $\bar{v}(A) = v(A)$.
  - Je-li A formule vzniklá z jiných formulí aplikací logické spojky, přiřadíme jí hodnotu podle následující tabulky:

A	B	$\neg A$	$A \,\&\, B$	$A \vee B$	$A \to B$	$A \leftrightarrow B$
0	0	1	0	0	1	1
0	1	1	0	1	1	0
1	0	0	0	1	0	0
1	1	0	1	1	1	1

  Formule A je *pravdivá* při ohodnocení v, pokud $\bar{v}(A) = 1$. Jinak je formule A *nepravdivá*.

2.2 Poznámka. Definice pravdivosti dává možnost o každé formuli snadno rozhodnout, zda je tautologie. S tím spojený algoritmus je však výpočtově exponenciálně složitý, protože pro n výrokových proměnných je nutné prozkoumat 2^n různých ohodnocení.

2.3 Pozorování (korektnost pravidla modus ponens). Z definice pravdivosti je zřejmé, že pokud jsou formule $A, A \to B$ při nějakém ohodnocení v pravdivé, není jiná možnost, než že i formule B je při v pravdivá. Tento fakt nám zaručí sémantickou korektnost odvozovacího pravidla *modus ponens*.

2.4 Definice. Nechť A je formule a v ohodnocení jejích výrokových proměnných.

- Je-li A pravdivá při ohodnocení v, říkáme, že v je *model formule* A a píšeme $v \vDash A$.
- Formule A je *splnitelná*, pokud pro ni existuje nějaký model v.

2.5 Definice. Nechť T je množina formulí a v ohodnocení jejích výrokových proměnných.

- Je-li každá formule $A \in T$ pravdivá při ohodnocení v, říkáme, že v je *model množiny formulí* T a píšeme $v \vDash T$.
- Množina formulí T je *splnitelná*, pokud pro ni existuje nějaký model v.

2.6 Definice. Nechť T je množina formulí a A je formule.

- Je-li každý model množiny T zároveň modelem formule A, říkáme, že A je *tautologický (sémantický) důsledek* T a píšeme $T \vDash A$.
- Je-li formule A pravdivá při každém ohodnocení výrokových proměnných, říkáme, že formule A je *tautologie* a píšeme $\vDash A$.

2.7 Poznámka. To, že A je tautologie, je zřejmě ekvivalentní tomu, že A je tautologický důsledek prázdné množiny formulí. Formálně vzato je totiž každé ohodnocení v modelem prázdné množiny formulí.

2.8 Poznámka. Když je množina formulí T nesplnitelná, nemá žádný model. Množina modelů množiny formulí T je tedy prázdná a libovolná formule A je pravdivá při každém prvku této prázdné množiny. Formálně tedy platí, že každá formule A je tautologickým důsledkem nesplnitelné množiny T. Jak později uvidíme, toto souvisí s tím, že nesplnitelná množina formulí je sporná a ze sporné množiny lze dokázat libovolnou formuli.

2.9 Pozorování. Pro libovolné (a tedy i prázdné) množiny formulí T_1, T_2 je:

$$T_1 \vDash A \quad \text{a} \quad T_2 \vDash A \to B \qquad \Rightarrow \qquad T_1 \cup T_2 \vDash B$$

Důkaz. Mějme libovolný model v množiny $T_1 \cup T_2$. Ten je zřejmě i modelem samostatných množin T_1 a T_2 a formule A a $A \to B$ jsou tedy při v pravdivé. Proto je podle pozorování 2.3 při v pravdivá i formule B. ☆

3 Formální systém výrokové logiky

Formální systém nějaké větve matematické logiky má několik částí:

- *Formální jazyk*, ve kterém jsou tvořeny formule systému.
- *Axiomy*, tedy formule, které přijímáme jako základní tvrzení.

- *Odvozovací pravidla*, které říkají, za jakých okolností můžeme z jiných formulí odvodit novou formuli jako jejich důsledek.

Dále nás při studiu formálních systémů bude zajímat, co je to *formální důkaz* formule, jaké formule se dají formálně dokázat a jaké prostředky se k důkazům dají využít, jsou-li všechny dokázané formule skutečně pravdivé (*korektnost* formálního systému), nedá-li se náhodou dokázat jakákoliv formule (*bezespornost* formálního systému) a jestli se dají dokázat právě všechny pravdivé formule (*úplnost* formálního systému).

3.1 Redukce jazyka. Abychom mohli axiomy a odvozovací pravidla zvolit co nejúsporněji, budeme budovat formální systém výrokové logiky pouze pro dvě logické spojky, a sice *negaci* $\neg$ a *implikaci* $\to$. Ostatní spojky budeme chápat jako odvozené a budeme je pokládat pouze za syntaktickou zkratku pro zjednodušení zápisu formulí využívajících pouze uvedených dvou spojek. Konkrétně:

$$\begin{array}{rll} (A \,\&\, B) & \text{je zkratka za formuli} & \neg(A \to \neg B) \\ (A \vee B) & \text{je zkratka za formuli} & (\neg A \to B) \\ (A \leftrightarrow B) & \text{je zkratka za formuli} & (A \to B) \,\&\, (B \to A) \end{array}$$

Dá se snadno ověřit, že ze sémantického hlediska jsou formule nalevo ekvivalentní formulím napravo (při jakémkoliv ohodnocení v mají obě formule stejnou pravdivostní hodnotu).

3.2 Volba axiomů a odvozovacích pravidel.

- Jako *axiomy* je vhodné volit takové formule, které jsou pravdivé nezávisle na interpretaci jazyka (v případě výrokové logiky na ohodnocení prvotních formulí). Proto budeme axiomy hledat mezi *tautologiemi*.
- Jako *odvozovací pravidla* je vhodné volit taková pravidla, která jsou *korektní*, tedy pro danou interpretaci (ohodnocení) odvodí z pravdivých formulí další pravdivou formuli.

Pokud zvolíme axiomy a pravidla podle uvedených zásad, budeme mít jistotu, že všechny věty dokázané v našem formálním systému budou tautologie. Naopak otázka, zda jsou všechny tautologie formálně dokazatelné, je těžší a budeme se jí zabývat v sekci o úplnosti výrokové logiky.

3.3 Definice. *Formální systém výrokové logiky* obsahuje:

- *Jazyk.* Použijeme redukovaný jazyk L'_P nad množinou prvotních formulí P.
- *Axiomy.* Jsou-li A, B, C formule, pak každá formule následujících tvarů je

axiom výrokové logiky:

$$A \to (B \to A) \tag{A1}$$
$$(A \to (B \to C)) \to [(A \to B) \to (A \to C)] \tag{A2}$$
$$(\neg B \to \neg A) \to (A \to B) \tag{A3}$$

- *Odvozovací pravidla.* Jediné odvozovací pravidlo výrokové logiky je pravidlo *modus ponens*:

$$\text{„Z formulí } A \text{ a } A \to B \text{ odvoď formuli } B.\text{“} \tag{MP}$$

Uvedené výrazy (A1), (A2) a (A3) jsou pouze *schémata axiomů*, podle kterých se dosazením za formule A, B, C vytvoří *instance axiomu*. Formální systém výrokové logiky má tedy nekonečně mnoho axiomů, ale pouze tři schémata axiomů.

3.4 Definice. Posloupnost formulí $(A_1, A_2, \ldots, A_n)$ je *formálním důkazem formule* A v daném formálním systému, pokud zároveň platí:

- $A_n = A$
- každá formule $A_i, i \in \{1, \ldots, n\}$ je buď:
  - *axiom* daného formálního systému
  - odvozena z určitých předchozích formulí $A_j, j \in \{1, \ldots, i-1\}$ použitím některého *odvozovacího pravidla* daného formálního systému

Formule A je v daném formálním systému *dokazatelná*, pokud existuje formální důkaz formule A. Říkáme také, že A je *větou* daného formálního systému a tuto skutečnost zapisujeme $\vdash A$.

3.5 Věta.

$$\vdash (A \to A) \tag{V1}$$

Důkaz. Větu dokážeme formálně ve smyslu předchozí definice:

(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)	$(A \to (A \to A)) \to (A \to A)$	(MP z (1) a (2))
(4)	$(A \to (A \to A))$	(A1)
(5)	$A \to A$	(MP z (3) a (4))

☆

Jak vidíme, formální důkaz i tak jednoduchého tvrzení má pět kroků. Lze očekávat, že důkazy složitějších formulí budou narůstat do délky. Pro zjednodušení proto můžeme formuli $A \to A$ od tohoto okamžiku pokládat za jakési „schéma axiomu“ a každou jeho „instanciaci“ pak v případě potřeby nahradit výše uvedenými pěti kroky. Toto je vlastně jediný formální důkaz, který uvedeme – všechny další důkazy budou spíše jakýmsi návodem, jak by bylo možné danou větu dokázat formálně, kdyby toho bylo zapotřebí, nebo budou s formálním důkazem manipulovat.

3.6 Definice. Nechť T je množina formulí. Posloupnost formulí $(A_1, A_2, \ldots, A_n)$ je *formálním důkazem formule A z předpokladů T* v daném formálním systému, pokud zároveň platí:

- $A_n = A$
- každá formule $A_i, i \in \{1, \ldots, n\}$ je buď:
  - *axiom* daného formálního systému
  - odvozena z určitých předchozích formulí $A_j, j \in \{1, \ldots, i-1\}$ použitím některého *odvozovacího pravidla* daného formálního systému
  - prvkem množiny T

Formule A je v daném formálním systému *dokazatelná z předpokladů T*, pokud existuje formální důkaz formule A z předpokladů T. Píšeme $T \vdash A$.

Od definice samotného formálního důkazu se tedy tato definice liší pouze tím, že jako prvek A_i posloupnosti lze použít i některý *předpoklad*, tedy některou formuli z T.

3.7 Poznámka ke značení. Obvykle nahrazujeme symbol T na levé straně zápisu $T \vdash A$ výčtem prvků množiny T nebo kombinujeme formule a množiny formulí, například:

$$\begin{array}{rcl} A, B \vdash C & \text{namísto} & \{A, B\} \vdash C \\ T, \neg A \vdash B & \text{namísto} & T \cup \{\neg A\} \vdash B \end{array}$$

3.8 Pozorování. Nechť T je množina formulí a A formule. Potom:

$$A \in T \quad \Rightarrow \quad T \vdash A \tag{DP}$$

Toto tvrzení je zřejmé (jednoprvková posloupnost (A) je důkazem formule A z předpokladů T, pokud $A \in T$). Uvádíme ho jen proto, abychom mohli některé kroky jiných důkazů komentovat písmeny DP („důkaz z předpokladů“).

3.9 Pozorování. Nechť T_1 a T_2 jsou množiny formulí takové, že $T_1 \subseteq T_2$, a A je formule. Potom zřejmě platí:

$$T_1 \vdash A \quad \Rightarrow \quad T_2 \vdash A$$

3.10 Důsledek. Nechť T_1, T_2 jsou libovolné množiny formulí a A, B formule. Platí:

$$T_1 \vdash A \quad \text{a} \quad T_2 \vdash A \to B \qquad \Rightarrow \qquad T_1 \cup T_2 \vdash B \tag{MP}$$

Důkaz. Spojíme formální důkazy formulí A a $A \to B$ a na konec zařadíme formuli B. Zřejmě tak vznikne formální důkaz formule B z předpokladů $T_1 \cup T_2$. ✯

3.11 Věta o dedukci pro výrokovou logiku. Nechť T je množina formulí a A, B jsou formule. Potom:

$$T \vdash A \to B \quad \Leftrightarrow \quad T \cup \{A\} \vdash B \tag{VD}$$

Důkaz.

$\Rightarrow$) Předpokládejme, že platí $T \vdash A \to B$. Potom existuje posloupnost formulí $(A_1, A_2, \ldots, A_{n-1}, A \to B)$, která je formálním důkazem formule $A \to B$ z předpokladů T. Doplníme-li k této posloupnosti formuli A, kterou přidáme i k množině předpokladů T, můžeme z této formule A a z formule $A \to B$ pravidlem *modus ponens* odvodit platnost formule B. Posloupnost $(A, A_1, A_2, \ldots, A_{n-1}, A \to B, B)$ se tak stane formálním důkazem formule B z předpokladů $T \cup \{A\}$. Skutečně tedy $T \cup \{A\} \vdash B$.

$\Leftarrow$) Nyní nechť $T \cup \{A\} \vdash B$ a $(A_1, A_2, \ldots, A_n = B)$ je formální důkaz formule B z předpokladů $T \cup \{A\}$. Indukcí podle délky formálního důkazu ukážeme, že pro $\forall i \in \{1, \ldots, n\}$ platí $T \vdash A \to A_i$. Tím budeme hotovi, neboť pro $i = n$ dostaneme $T \vdash A \to B$.

Předpokládejme, že pro všechna $j < i$ jsme již formální důkazy vět $T \vdash A \to A_j$ sestrojili (pro $i = 1$ tedy nepředpokládáme nic, což nevadí, protože varianta využívající indukční předpoklad nemůže pro $i = 1$ nastat). Pro dané i uvážíme tři případy:

- Formule A_i je formule A. Větu $\vdash A \to A$ máme již formálně dokázanou, stejně dokážeme $\vdash A \to A_i$ z předpokladů T.
- Formule A_i je axiom výrokové logiky nebo formule z množiny T. Potom posloupnost $(A_i, A_i \to (A \to A_i), A \to A_i)$ je formálním důkazem formule $A \to A_i$ z předpokladů T, neboť druhá formule je instancí axiomu (A1) a třetí formule vznikla z první a druhé pravidlem *modus ponens*.
- Formule A_i je odvozena pravidlem *modus ponens* z formulí A_j, A_k pro nějaká $j, k < i$, kde A_j je formule tvaru $A_k \to A_i$. Podle indukčního předpokladu jsme tedy již dříve museli dokázat $T \vdash A \to (A_k \to A_i)$ a

$T \vdash A \to A_k$. Postupujeme takto:

(1) $T \vdash A \to (A_k \to A_i)$

(2) $T \vdash A \to A_k$

(3) $T \vdash (A \to (A_k \to A_i)) \to [(A \to A_k) \to (A \to A_i)]$ (A2)

(4) $T \vdash (A \to A_k) \to (A \to A_i)$ (MP z (1) a (3))

(5) $T \vdash A \to A_i$ (MP z (2) a (4))

Formální důkaz věty (5) vznikne spojením předchozích důkazů vět (1) a (2) a formulí (3), (4) a (5).

☆

Důkaz věty o dedukci dává vlastně návod, jak lze přejít od formálního důkazu věty $T \vdash A \to B$ k formálnímu důkazu věty $T \cup \{A\} \vdash B$ a zpět. Při dokazování dalších vět výrokové logiky nebudeme již sestrojovat formální důkazy, ale budeme pouze ukazovat, že existují, a naznačovat, jak k nim lze v případě potřeby dojít.

3.12 Upozornění. Věta o dedukci nás může lákat zkrátit důkaz věty (V1) na pouhé dva kroky:

(1) $A \vdash A$ (DP)

(2) $\vdash A \to A$ (VD)

Věta (V1) však byla využita v důkazu věty o dedukci, proto nemůžeme použít větu o dedukci k důkazu věty (V1).[1]

Nyní si ukážeme dvě přímé aplikace věty o dedukci:

3.13 Věta o skládání implikací.

$$\vdash (A_1 \to A_2) \to (A_2 \to A_3) \to \ldots \to (A_{n-1} \to A_n) \to (A_1 \to A_n) \qquad \text{(SI)}$$

Důkaz.

(1) $A_1, A_1 \to A_2, \ldots, A_{n-1} \to A_n \vdash A_1$ (DP)

(2) $A_1, A_1 \to A_2, \ldots, A_{n-1} \to A_n \vdash A_1 \to A_2$ (DP)

(3) $A_1, A_1 \to A_2, \ldots, A_{n-1} \to A_n \vdash A_2$ (MP z (1) a (2))

(4) $A_1, A_1 \to A_2, \ldots, A_{n-1} \to A_n \vdash A_2 \to A_3$ (DP)

(5) $A_1, A_1 \to A_2, \ldots, A_{n-1} \to A_n \vdash A_3$ (MP z (3) a (4))

$\vdots$

(6) $A_1, A_1 \to A_2, \ldots, A_{n-1} \to A_n \vdash A_n$

Nyní postupnou aplikací věty o dedukci (postupně pro formule $A_1, A_{n-1} \to A_n, A_{n-2} \to A_{n-1} \ldots, A_1 \to A_2$) získáme konečně:

$\vdash (A_1 \to A_2) \to (A_2 \to A_3) \to \ldots \to (A_{n-1} \to A_n) \to (A_1 \to A_n)$

[1] Kdybychom však v důkazu věty o dedukci místo odkazu na (V1) rozvedli její formální důkaz (onu posloupnost pěti formulí), bylo by pak možné větu (V1) skutečně dokázat takto.

☆

3.14 Věta o záměně předpokladů. Nechť $A_1, A_2, \ldots, A_n, B$ jsou formule a π je permutace na množině $\{1, \ldots, n\}$. Potom:

$$\vdash (A_1 \to A_2 \to \ldots \to A_n \to B) \to (A_{\pi(1)} \to A_{\pi(2)} \to \ldots \to A_{\pi(n)} \to B) \qquad \text{(ZP)}$$

Důkaz. Vyjdeme z množiny předpokladů $(A_1 \to A_2 \to \ldots \to A_n \to B)$, A_1, A_2, …, A_n, kterou budeme pro zkrácení nazývat T:

(1)	$T \vdash A_1$	(DP)
(2)	$T \vdash A_1 \to A_2 \to \ldots \to A_n \to B$	(DP)
(3)	$T \vdash A_2 \to A_3 \to \ldots \to A_n \to B$	(MP z (1) a (2))
(4)	$T \vdash A_2$	(DP)
(5)	$T \vdash A_3 \to A_4 \to \ldots \to A_n \to B$	(MP z (3) a (4))
⋮		
(6)	$T \vdash B$	

A nyní již postupnou aplikací věty o dedukci v pořadí $A_{\pi(n)}$, $A_{\pi(n-1)}$, …, $A_{\pi(1)}$, $(A_1 \to A_2 \to \ldots \to A_n \to B)$:

$$\vdash (A_1 \to A_2 \to \ldots \to A_n \to B) \to (A_{\pi(1)} \to A_{\pi(2)} \to \ldots \to A_{\pi(n)} \to B)$$

☆

Nyní bude následovat několik vět a jejich variant, které budou (spolu s již uvedenými) *nenahraditelné* při důkazech složitějších formulí a tvrzení o nich.

3.15 Věta.

$$\vdash \neg A \to (A \to B) \qquad \text{(V2)}$$

Důkaz.

(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)	$\neg A \vdash (A \to B)$	(MP z (2) a (3))
(5)	$\vdash \neg A \to (A \to B)$	(VD)

Krok typu (3) budeme obvykle vynechávat a do komentáře následujícího řádku psát (A3, MP), což obvykle bude znamenat: „Použili jsme instanci axiomu 3 (který má tvar implikace) tak, aby předpoklad odpovídal předchozí formuli. Potom jsme použitím pravidla *modus ponens* odvodili tuto formuli, která je tvrzením axiomu.“ ☆

Uvědomme si intuitivní význam věty. Ten říká, že podaří-li se nám zároveň dokázat formuli A i její negaci $\neg A$, můžeme z toho odvodit *libovolnou* formuli

B. To poněkud ospravedlňuje definici spornosti, kterou uvedeme v následující kapitole.

3.16 Poznámka. Uvedený *neformální důkaz*[2] nám napovídá, jak sestrojit *formální důkaz* této věty. Vezmeme formuli $\neg A \to (\neg B \to \neg A)$, která je jakožto instance axiomu svým vlastním formálním důkazem. Důkaz věty o dedukci nám dává návod, jak tento důkaz transformovat na důkaz formule $\neg B \to \neg A$ z předpokladu $\neg A$. K tomuto důkazu přidáme axiom $(\neg B \to \neg A) \to (A \to B)$ a formuli $A \to B$, vznikne formální důkaz formule $A \to B$ z předpokladu $\neg A$. Věta o dedukci nám opět poví, jak od tohoto důkazu dospět k hledanému důkazu formule $\neg A \to (A \to B)$.

Někdy se nám bude hodit taky mírná varianta předchozí věty:

3.17 Důsledek.

$$\vdash A \to (\neg A \to B) \tag{V2'}$$

Důkaz. Plyne snadno z (V2) a věty o záměně předpokladů. ☆

3.18 Věta.

$$\vdash \neg\neg A \to A \tag{V3}$$

Důkaz.

(1)	$\vdash \neg\neg A \to (\neg A \to \neg\neg\neg A)$	(V2)
(2)	$\neg\neg A \vdash \neg A \to \neg\neg\neg A$	(VD)
(3)	$\neg\neg A \vdash \neg\neg A \to A$	(A3, MP)
(4)	$\neg\neg A \vdash A$	(VD)
(5)	$\vdash \neg\neg A \to A$	(VD)

Všiměme si použití (VD) v kroku (4) k eliminaci nadbytečného předpokladu. ☆

3.19 Věta.

$$\vdash A \to \neg\neg A \tag{V4}$$

Důkaz.

(1)	$\vdash \neg\neg\neg A \to \neg A$	(V3)
(2)	$\vdash A \to \neg\neg A$	(A3, MP)

☆

Následující věta je obdobou axiomu (A3):

3.20 Věta.

$$\vdash (A \to B) \to (\neg B \to \neg A) \tag{V5}$$

[2]Prof. Štěpánek používá ve svých skriptech pojem *demonstrace*.

Důkaz. Vyjdeme z věty o skládání implikací

$$\vdash (\neg\neg A \to A) \to (A \to B) \to (B \to \neg\neg B) \to (\neg\neg A \to \neg\neg B)$$

kterou pomocí věty o záměně předpokladů převedeme (prohozením druhého a třetího předpokladu) na:

$$\vdash (\neg\neg A \to A) \to (B \to \neg\neg B) \to (A \to B) \to (\neg\neg A \to \neg\neg B)$$

Protože první předpoklad je instance věty (V3) a druhý věty (V4), dostaneme po dvou (MP) znění prvního řádku:

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

☆

Pro úplnost zde uvedeme i ostatní varianty axiomu (A3) a věty (V5), které budeme později využívat a značit (V5'):

3.21 Důsledek.

(i)	$\vdash (A \to \neg B) \to (B \to \neg A)$	(V5')
(ii)	$\vdash (\neg A \to B) \to (\neg B \to A)$	(V5')

Důkaz. (i) Takto:

(1)	$A \to \neg B \vdash A \to \neg B$	(DP)
(2)	$A \to \neg B \vdash \neg\neg B \to \neg A$	(V5, MP)
(3)	$\vdash (B \to \neg\neg B) \to (\neg\neg B \to \neg A) \to (B \to \neg A)$	(SI)
(4)	$\vdash (\neg\neg B \to \neg A) \to (B \to \neg A)$	(V4, MP)
(5)	$A \to \neg B \vdash B \to \neg A$	(MP z (2) a (4))
(6)	$\vdash (A \to \neg B) \to (B \to \neg A)$	(VD)

(ii) Podobně, pouze bez mezikroku s větou o skládání implikací:

(1)	$\neg A \to B \vdash \neg A \to B$	(DP)
(2)	$\neg A \to B \vdash \neg B \to \neg\neg A$	(V5, MP)
(3)	$\neg A \to B, \neg B \vdash \neg\neg A$	(VD)
(4)	$\neg A \to B, \neg B \vdash A$	(V3, MP)
(5)	$\vdash (\neg A \to B) \to (\neg B \to A)$	(2× VD)

☆

3.22 Věta.

$$\vdash A \to \neg B \to \neg(A \to B) \qquad \text{(V6)}$$

Důkaz.

(1)	$A \to B \vdash A \to B$	(DP)
(2)	$A \vdash (A \to B) \to B$	(2× VD)
(3)	$A \vdash \neg B \to \neg(A \to B)$	(V5, MP)
(4)	$\vdash A \to \neg B \to \neg(A \to B)$	(VD)

☆

3.23 Věta.

$$\vdash (\neg A \to A) \to A \qquad \text{(V7)}$$

Důkaz.

(1)	$\vdash \neg A \to \neg A \to \neg(\neg A \to A)$	(V6)
(2)	$\vdash \neg A \to \neg(\neg A \to A)$	(3× VD)
(3)	$\vdash (\neg A \to A) \to A$	(A3, MP)

☆

Spíše pro úplnost než proto, že bychom to později potřebovali, uveďme, jak by se dokázala obdoba věty (V7):

3.24 Důsledek.

$$\vdash (A \to \neg A) \to \neg A \qquad \text{(V7')}$$

Důkaz.

(1)	$A \to \neg A \vdash A \to \neg A$	(DP)
(2)	$A \to \neg A \vdash \neg\neg A \to \neg A$	(V5, MP)
(3)	$\vdash (\neg\neg A \to \neg A) \to \neg A$	(V7)
(4)	$A \to \neg A \vdash \neg A$	(MP z (2) a (3))
(5)	$\vdash (A \to \neg A) \to \neg A$	(VD)

☆

4 Úplnost výrokové logiky

Nyní se budeme zabývat otázkou, zda jsou všechny tautologie opravdu dokazatelné. K tomu budeme potřebovat některé další pojmy, především pojem *spornosti*, *bezespornosti* a *maximální bezespornosti* množiny formulí.

Uvedený postup pochází ze slidů a přednášky prof. Štěpánka. V jeho skriptech je uveden postup jiný. Uvedený postup se taky do určité míry podobá postupu v predikátové logice.

4.1 Definice. Množina formulí T nějakého formálního systému je *sporná*, jestliže každá formule A daného formálního systému je dokazatelná z předpokladů T. V opačném případě řekneme, že T je *bezesporná*.

Bezespornost se někdy nazývá *konzistence* a spornost *inkonzistence*. Sémantickým ekvivalentem bezesporné množiny je pojem splnitelné množiny.

4.2 Věta o důkazu sporem. Pro každou formuli A a množinu formulí T platí:

$$T \vdash A \quad \Leftrightarrow \quad T \cup \{\neg A\} \text{ je sporná}$$

Důkaz.

$\Rightarrow$) Nechť B je libovolná formule a $T \vdash A$. Postupujeme takto:

(1)	$T \vdash A$	(předpoklad)
(2)	$\vdash A \to (\neg A \to B)$	(V2')
(3)	$T \vdash (\neg A \to B)$	(MP z (1) a (2))
(4)	$T, \neg A \vdash B$	(VD)

Množina $T \cup \{\neg A\}$ je tedy sporná, neboť z ní lze dokázat libovolnou formuli B.

$\Leftarrow$) Protože je $T \cup \{\neg A\}$ sporná, můžeme z ní dokázat libovolnou formuli, třeba A. Proto:

(1)	$T, \neg A \vdash A$	
(2)	$T \vdash \neg A \to A$	(VD)
(3)	$\vdash (\neg A \to A) \to A$	(V7)
(4)	$T \vdash A$	(MP z (2) a (3))

4.3 Věta o charakterizaci sporných množin. Množina formulí T je sporná, právě když pro nějakou formuli A lze dokázat $T \vdash A \,\&\, \neg A$.

Důkaz.

$\Rightarrow$) Protože je T sporná, lze z ní dokázat každou formuli, speciálně tedy i $A \,\&\, \neg A$ pro libovolnou A.

$\Leftarrow$) Nechť B je libovolná formule a platí $T \vdash A \,\&\, \neg A$ pro nějakou formuli A. Dokážeme $T \vdash B$:

(1)	$T \vdash \neg(A \to \neg\neg A)$	(přepsaná $A \,\&\, \neg A$)
(2)	$\vdash A \to (\neg B \to A)$	(A1)
(3)	$\vdash \neg B \to (A \to \neg\neg A)$	(2× VD, V4, MP, 2× VD)
(4)	$\vdash \neg(A \to \neg\neg A) \to \neg\neg B$	(V5, MP)
(5)	$T \vdash \neg\neg B$	(MP z (1) a (4))
(6)	$T \vdash B$	(V3, MP)

✯

4.4 Pozorování. Je-li množina formulí T bezesporná a $T \vdash A$, potom je také množina $T \cup \{A\}$ bezesporná.

Důkaz. Kdyby byla $T \cup \{A\}$ sporná, bylo by z ní možné podle věty 4.3 dokázat spor, tedy nějakou formuli tvaru $B \,\&\, \neg B$. Tento spor by potom byl dokazatelný pouze z předpokladů T, neboť bychom v jeho důkazu mohli případný výskyt formule A nahradit jejím důkazem z T. Množina T by tedy nemohla být bezesporná a došli bychom ke sporu. ✯

4.5 Definice. Řekneme, že množina formulí T je *maximální bezesporná*, jestliže je bezesporná a neexistuje žádná bezesporná množina T' taková, že $T \subset T'$.

4.6 Tvrzení. Nechť T je maximální bezesporná množina formulí. Potom:

$$T \vdash A \quad \Leftrightarrow \quad A \in T$$

Důkaz. Implikace $\Leftarrow$ je zcela triviální, soustřeďme se proto na implikaci $\Rightarrow$. Množina T je bezesporná a platí $T \vdash A$, proto je podle pozorování 4.4 bezesporná i množina $T \cup \{A\}$. Odtud nutně plyne $A \in T$, neboť v opačném případě by množina T nebyla maximální bezesporná. ✯

4.7 Tvrzení. Nechť T je maximální bezesporná množina formulí. Potom pro libovolnou formuli A je právě jedna z formulí A, $\neg A$ prvkem množiny T.

Důkaz. Mějme libovolnou formuli A. Předpokládejme, že obě formule A, $\neg A$ jsou prvky T. Potom lze z T snadno dokázat libovolnou formuli B:

(1)	$T \vdash \neg A$	(předpoklad $\neg A \in T$, tvrzení 4.6)
(2)	$T \vdash A$	(předpoklad $A \in T$, tvrzení 4.6)
(3)	$\vdash \neg A \to A \to B$	(V2)
(4)	$T \vdash B$	(2× MP)

Množina T je tedy podle definice sporná a to je spor.

Nyní předpokládejme, že žádná z formulí A, $\neg A$ není prvkem T. Protože by T měla být maximální bezesporná, je množina $T \cup \{\neg A\}$ sporná. Podle věty věty 4.2 je tedy $T \vdash A$, což podle tvrzení 4.6 znamená $A \in T$. Máme tedy opět spor. ✯

4.8 Lemma. Je-li T maximální bezesporná množina formulí a A, B formule, potom platí:

$$(A \to B) \in T \qquad \Leftrightarrow \qquad \neg A \in T \quad \text{nebo} \quad B \in T$$

Důkaz. Za daných předpokladů budeme dokazovat větu:

$$T \vdash (A \to B) \qquad \Leftrightarrow \qquad T \vdash \neg A \quad \text{nebo} \quad T \vdash B \tag{1}$$

Platnost lemmatu vyplyne z (1) díky tvrzení 4.6, neboť T je maximální bezesporná.

$\Leftarrow$) Dokážeme $T \vdash A \to B$ a to jak za předpokladu $T \vdash \neg A$, tak za předpokladu $T \vdash B$:

(1)	$T \vdash \neg A$	(předpoklad)
(2)	$\vdash \neg A \to (A \to B)$	(V2)
(3)	$T \vdash A \to B$	(MP z (1) a (2))
(4)	$T \vdash B$	(předpoklad)
(5)	$\vdash B \to (A \to B)$	(A1)
(6)	$T \vdash A \to B$	(MP z (4) a (5))

$\Rightarrow$) Dokážeme obměnu. Předpokládejme, že neplatí ani $T \vdash \neg A$, ani $T \vdash B$. Protože je T maximální bezesporná, musí podle tvrzení 4.7 platit $T \vdash A$ a $T \vdash \neg B$. Potom:

(1)	$T \vdash A$	(předpoklad)
(2)	$T \vdash \neg B$	(předpoklad)
(3)	$\vdash A \to \neg B \to \neg(A \to B)$	(V6)
(4)	$T \vdash \neg(A \to B)$	(2× MP)

Odtud plyne (opět podle tvrzení 4.7) neplatnost $T \vdash A \to B$. ☆

4.9 Lindenbaumova věta pro výrokovou logiku. Pro každou bezesporn-nou množinu T existuje maximální bezesporná možina S taková, že $T \subseteq S$.

Důkaz. Všechny formule jazyka libovolně uspořádáme do *prosté*[3] posloupnosti

$$A_1, A_2, A_3, \ldots \tag{1}$$

Dále vytvoříme „neklesající“ posloupnost bezesporných množin

$$T = T_0 \subseteq T_1 \subseteq T_2 \subseteq T_3, \ldots$$

tak, že pro $\forall i \in \mathbb{N}$ položíme

$$T_i = \begin{cases} T_{i-1} \cup \{A_i\}, & \text{je-li } T_{i-1} \cup \{A_i\} \text{ bezesporná} \\ T_{i-1} & \text{jinak.} \end{cases}$$

Nechť $S = T_\infty = \bigcup_{n=0}^{\infty} T_n$. Zřejmě $T \subseteq S$. Zbývá dokázat, že S je maximální bezesporná.

Pro spor nechť S není bezesporná. Potom podle věty 4.3 existuje formule A taková, že $S \vdash A\&\neg A$. Mějme tedy formální důkaz formule $A\&\neg A$ z předpokladů

[3] Bohužel se mi nepovedlo přijít na to, proč prof. Štěpánek požaduje prostou posloupnost. Dle mého názoru je důležité pouze to, aby se v posloupnosti vyskytla každá formule alespoň jednou...

S. Nechť C je množina všech formulí z S, které se v tomto důkazu vyskytují. Formuli $A \,\&\, \neg A$ lze tedy dokázat z předpokladů $C \subseteq S$, kterých je konečně mnoho, a proto pro nějaký dostatečně velký index k jsou všechny formule z C prvkem T_k. Množina T_k je ale bezesporná, a proto z ní žádnou formuli tvaru $A \,\&\, \neg A$ dokázat nelze. Máme tedy spor.

Pro spor nechť S není *maximální* bezesporná. Potom existuje nějaká bezesporná S', že $S \subset S'$, BÚNO taková, že $S' \setminus S = \{A\}$, tedy S' obsahuje oproti S navíc pouze formuli A. Nechť tato formule figuruje v posloupnosti (1) na místě k, tedy $A = A_k$. Neboť S' je bezesporná a máme $A_k \in S'$, $T_{k-1} \subseteq S \subset S'$ a tedy $T_{k-1} \cup \{A_k\} \subset S'$, je množina $T_{k-1} \cup \{A_k\}$ bezesporná. To ale znamená, že $T_k = T_{k-1} \cup \{A_k\}$ a tedy $A_k \in T_k \subseteq S$ a máme spor, protože jsme předpokládali $A_k \notin S$. ☆

4.10 Věta o bezespornosti a splnitelnosti. Je-li T množina formulí výrokové logiky, potom platí:

$$T \text{ je bezesporná} \quad \Leftrightarrow \quad T \text{ je splnitelná}$$

Důkaz.

$\Leftarrow$) Předpokládejme, že T je splnitelná a v je její model, tedy $v \vDash T$. Nejprve ukážeme, že každá formule dokazatelná z předpokladů T je pravdivá při ohodnocení v.

Buď tedy A libovolná formule dokazatelná z T a $(A_1, A_2, \ldots, A_n)$ její formální důkaz z předpokladů T. Indukcí dokážeme, že $\bar{v}(A_m) = 1$ pro $\forall m \in \{1, \ldots, n\}$:

- Formule A_m je axiom. Potom $\bar{v}(A_m) = 1$, neboť každý axiom je tautologie.
- Formule $A_m \in T$. Potom $\bar{v}(A_m) = 1$, neboť $v \vDash T$ podle předpokladu.
- Formule A_m je odvozena z formulí A_i, A_j, kde $i, j \in \{1, \ldots, m-1\}$, použitím pravidla *modus ponens*. Z indukčního předpokladu máme $\bar{v}(A_i) = \bar{v}(A_j) = 1$ a díky korektnosti pravidla *modus ponens* dostáváme $\bar{v}(A_m) = 1$.

Nyní uvažme libovolnou formuli tvaru $A \,\&\, \neg A$. Tato jistě není pravdivá při ohodnocení v, proto tedy nemůže být ani dokazatelná z T. Množina T je tedy bezesporná.

$\Rightarrow$) Nyní předpokládejme, že T je bezesporná. Potom ji lze podle Lindenbaumovy věty rozšířit do maximální bezesporné množiny S. Definujeme ohodnocení $v : P \to \{0, 1\}$, kde P je množina výrokových proměnných v S, následovně:

$$v(p) = 1 \quad \Leftrightarrow \quad p \in S$$

Nechť A je libovolná formule. Indukcí podle její složitosti dokážeme:

$$A \in S \quad \Leftrightarrow \quad \bar{v}(A) = 1 \tag{1}$$

Pro formuli A mohou nastat tyto případy:

- Formule A je výroková proměnná. Tvrzení (1) pak plyne přímo z definice ohodnocení v.
- Formule A je tvaru $\neg B$, kde B splňuje (1) jako indukční předpoklad. Potom

$$\neg B \in S \quad \overset{(1)}{\Leftrightarrow} \quad B \notin S \quad \overset{\text{(IP)}}{\Leftrightarrow} \quad \bar{v}(B) = 0 \quad \overset{(2)}{\Leftrightarrow} \quad \bar{v}(\neg B) = 1$$

  neboť S je maximální bezesporná množina a ekvivalence (1) tak plyne z tvrzení 4.7. Ekvivalence (2) plyne ze sémantického významu negace.
- Formule A je tvaru $B \to C$, kde B a C splňují (1) jako indukční předpoklad. Navíc můžeme předpokládat, že tento předpoklad splňuje i formule $\neg B$ (viz předchozí bod). Proto:

$$\begin{aligned}
(B \to C) \in S \quad &\Leftrightarrow \quad \neg B \in S \text{ nebo } C \in S && \text{(lemma 4.8)} \\
&\Leftrightarrow \quad \bar{v}(\neg B) = 1 \text{ nebo } \bar{v}(C) = 1 && \text{(indukční předpoklad)} \\
&\Leftrightarrow \quad \bar{v}(B) = 0 \text{ nebo } \bar{v}(C) = 1 && \text{(význam negace)} \\
&\Leftrightarrow \quad \bar{v}(B \to C) = 1 && \text{(význam implikace)}
\end{aligned}$$

Dokázali jsme, že $A \in S \Rightarrow \bar{v}(A) = 1$ a tedy $v \vDash S$. Protože $T \subseteq S$, je také $v \vDash T$. Množina T je tedy splnitelná. ✯

4.11 Lemma. Nechť T je množina formulí a A fomule. Platí:

$$T \vDash A \quad \Leftrightarrow \quad T \cup \{\neg A\} \text{ je nesplnitelná}$$

Důkaz.

$$\begin{aligned}
T \vDash A \quad &\Leftrightarrow \quad \text{každý model množiny } T \text{ je modelem formule } A \\
&\Leftrightarrow \quad \text{žádný model množiny } T \text{ není modelem formule } \neg A \\
&\Leftrightarrow \quad T \cup \{\neg A\} \text{ je nesplnitelná}
\end{aligned}$$

✯

4.12 Věta o úplnosti pro výrokovou logiku. Nechť T je množina formulí a A libovolná formule. Potom platí:

$$\begin{array}{lccc}
\text{(i)} & T \vdash A & \Leftrightarrow & T \vDash A \\
\text{(ii)} & \vdash A & \Leftrightarrow & \vDash A
\end{array}$$

Důkaz.

(i) Platí:

$$\begin{aligned}
T \vdash A \quad &\Leftrightarrow \quad T \cup \{\neg A\} \text{ je sporná} && \text{(věta 4.2)} \\
&\Leftrightarrow \quad T \cup \{\neg A\} \text{ je nesplnitelná} && \text{(věta 4.10)} \\
&\Leftrightarrow \quad T \vDash A && \text{(lemma 4.11)}
\end{aligned}$$

(ii) Toto tvrzení je speciálním případem tvrzení (i) pro $T = \varnothing$. ☆

4.13 Definice. Říkáme, že formální systém je *sporný*, je-li každá jeho formule dokazatelná. V opačném případě říkáme, že formální systém je *bezesporný*.

Formální systém je tedy sporný, právě když je v něm sporná prázdná množina formulí.

4.14 Důsledek (bezespornost výrokové logiky). Formální systém výrokové logiky je bezesporný.

Důkaz. Z věty o úplnosti plyne, že ve výrokové logice jsou dokazatelné právě tautologie. Žádná formule tvaru $A \,\&\, \neg A$ ale není tautologií, a proto není podle věty o úplnosti ani větou výrokové logiky. Dle definice je tedy výroková logika bezesporná. ☆

4.15 Věta o kompaktnosti výrokové logiky. Množina formulí T je splnitelná, právě když je splnitelná každá její *konečná* podmnožina $T' \subseteq T$.

Důkaz.

$\Rightarrow$) Triviální.

$\Leftarrow$) Dokážeme obměnu: je-li T nesplnitelná, potom existuje její konečná podmnožina T', která není splnitelná.

Nechť tedy T není splnitelná. Podle věty o splnitelnosti je T sporná. Existuje tedy formule A taková, že $T \vdash A \& \neg A$. Důkaz této formule je ale konečný a proto využívá jen konečný počet předpokladů množiny T, které zahrneme do konečné množiny $T' \subseteq T$. Množina T' je sporná, proto je podle věty o splnitelnosti nesplnitelná. ☆

4.16 Důsledek. Nechť T je množina formulí a A je formule taková, že $T \vDash A$. Potom existuje konečná podmnožina $T' \subseteq T$ taková, že $T' \vDash A$.

Důkaz. Předpokládejme $T \vDash A$, podle věty o úplnosti tedy $T \vdash A$. Důkaz ale využívá jen konečnou podmnožinu předpokladů $T' \subseteq T$, kde $T' \vdash A$. Opět podle věty o úplnosti dostaneme $T' \vDash A$.

Tato věta se však dá ukázat (opravdu) jako důsledek věty o kompaktnosti. Z $T \vDash A$ totiž plyne, že $T \cup \{\neg A\}$ je podle lemmatu 4.11 nesplnitelná. Potom podle věty o kompaktnosti existuje nesplnitelná podmnožina $T' \subseteq (T \cup \{\neg A\})$. Přitom však množina $T' \cup \{\neg A\}$ zůstane nesplnitelná, i kdyby T' formuli $\neg A$ neobsahovala. Proto tedy (opět podle lemmatu 4.11) $T' \vDash A$. ☆

5 Další užitečné výsledky výrokové logiky

5.1 Lemma. Pro libovolné formule A, B a množinu předpokladů T platí:

$$T \vdash A \,\&\, B \qquad \Leftrightarrow \qquad T \vdash A \quad \text{a} \quad T \vdash B \tag{KF}$$

Důkaz.

⇒) Postupujeme takto:

(1)	$T \vdash \neg(A \to \neg B)$	(přepsaná $A \,\&\, B$)
(2)	$\vdash \neg A \to (A \to \neg B)$	(V2)
(3)	$\vdash \neg(A \to \neg B) \to A$	(V5', MP)
(4)	$T \vdash A$	(MP z (1) a (3))
(5)	$\vdash \neg B \to (A \to \neg B)$	(A1)
(6)	$\vdash \neg(A \to \neg B) \to B$	(V5', MP)
(7)	$T \vdash B$	(MP z (1) a (6))

⇐) Dokážeme $T \vdash \neg(A \to \neg B)$, což je přepis $T \vdash A \,\&\, B$:

(1)	$T \vdash A$	(předpoklad)
(2)	$T \vdash B$	(předpoklad)
(3)	$T \vdash \neg\neg B$	(V4, MP)
(4)	$\vdash A \to (\neg\neg B \to \neg(A \to \neg B))$	(V6)
(5)	$T \vdash \neg\neg B \to \neg(A \to \neg B)$	(MP z (1) a (4))
(6)	$T \vdash \neg(A \to \neg B)$	(MP z (3) a (5))

☆

5.2 Důsledky.

(i)	$A \,\&\, B \vdash A$	(čili $\vdash (A \,\&\, B) \to A$)
(ii)	$A \,\&\, B \vdash B$	(čili $\vdash (A \,\&\, B) \to B$)
(iii)	$A, B \vdash A \,\&\, B$	(čili $\vdash A \to (B \to (A \,\&\, B))$)
(iv)	$A \leftrightarrow B \vdash A \to B$	(čili $\vdash (A \leftrightarrow B) \to (A \to B)$)
(v)	$A \leftrightarrow B \vdash B \to A$	(čili $\vdash (A \leftrightarrow B) \to (B \to A)$)
(vi)	$A \to B, B \to A \vdash A \leftrightarrow B$	

$$T \vdash A \leftrightarrow B \qquad \Leftrightarrow \qquad T \vdash A \to B \quad \text{a} \quad T \vdash B \to A \tag{KI}$$

Důkaz. (i) Protože zřejmě $(A \,\&\, B) \vdash (A \,\&\, B)$, máme $A \,\&\, B \vdash A$ jako jednoduchý důsledek lemmatu 5.1. Stejně tak i tvrzení (ii) a (iii).

(iv) Pokud si uvědomíme, že $A \leftrightarrow B$ je zkratka za $(A \to B) \,\&\, (B \to A)$, plyne (iv) ihned z (i) jako instance. Stejně tak i tvrzení (v) a (vi) plynou z (ii) a (iii). Tvrzení (vii) plyne jako instance z lemmatu 5.1. ☆

Tvrzení (vii) je docela důležité, neboť ukazuje, že k důkazu ekvivalence stačí z daných předpokladů postupně dokázat obě implikace. Také říká, že máme-li větu výrokové logiky ve tvaru ekvivalence, je možné z ní nezávisle použít kteroukoliv implikaci.

5.3 Lemma.

$$\vdash (A \leftrightarrow B) \leftrightarrow (\neg A \leftrightarrow \neg B)$$

Důkaz.

(1)	$A \leftrightarrow B \vdash B \to A$	(5.2 (ii))
(2)	$A \leftrightarrow B \vdash \neg A \to \neg B$	(V5, MP)
(3)	$A \leftrightarrow B \vdash A \to B$	(5.2 (i))
(4)	$A \leftrightarrow B \vdash \neg B \to \neg A$	(V5, MP)
(5)	$A \leftrightarrow B \vdash \neg A \leftrightarrow \neg B$	((KI) z (2) a (4))
(6)	$\vdash (A \leftrightarrow B) \to (\neg A \leftrightarrow \neg B)$	(VD)

Opačná implikace a tedy podle (KI) i celková ekvivalence se dokáže obdobně (tentokrát vyjdeme z předpokladu $\neg A \leftrightarrow \neg B$). ☆

5.4 Vlastnosti konjunkce.

(i)	$\vdash A \leftrightarrow (A \,\&\, A)$	(idempotence)
(ii)	$\vdash (A \,\&\, B) \leftrightarrow (B \,\&\, A)$	(komutativnost)
(iii)	$\vdash ((A \,\&\, B) \,\&\, C) \leftrightarrow (A \,\&\, (B \,\&\, C))$	(asociativita)

Důkaz. (i) Takto:

(1)	$\vdash (A \,\&\, A) \to A$	(5.2 (i))
(2)	$A, A \vdash A \,\&\, A$	(5.2 (iii))
(3)	$\vdash A \to (A \,\&\, A)$	(2× VD)
(4)	$\vdash A \leftrightarrow (A \,\&\, A)$	(5.2 (vii) z (1) a (3))

(ii) Takto:

(1)	$A \,\&\, B \vdash B$	(5.2 (ii))
(2)	$A \,\&\, B \vdash A$	(5.2 (i))
(3)	$A \,\&\, B \vdash B \,\&\, A$	(5.1 z (1) a (2))
(4)	$\vdash (A \,\&\, B) \to (B \,\&\, A)$	(VD)
(5)	$\vdash (B \,\&\, A) \to (A \,\&\, B)$	(instance (4))
(6)	$\vdash (A \,\&\, B) \leftrightarrow (B \,\&\, A)$	(5.2 (vii) z (4) a (5))

(iii) Takto:

(1)	$\vdash (A \,\&\, B) \to A$	(5.2 (i))
(2)	$\vdash (A \,\&\, B) \to B$	(5.2 (ii))
(3)	$(A \,\&\, B) \,\&\, C \vdash A \,\&\, B$	(5.2 (i))
(4)	$(A \,\&\, B) \,\&\, C \vdash A$	(MP z (1) a (3))
(5)	$(A \,\&\, B) \,\&\, C \vdash B$	(MP z (2) a (3))
(6)	$(A \,\&\, B) \,\&\, C \vdash C$	(5.2 (ii))
(7)	$(A \,\&\, B) \,\&\, C \vdash B \,\&\, C$	(5.1 z (5) a (6))
(8)	$(A \,\&\, B) \,\&\, C \vdash A \,\&\, (B \,\&\, C)$	(5.1 z (4) a (7))
(9)	$\vdash ((A \,\&\, B) \,\&\, C) \to (A \,\&\, (B \,\&\, C))$	(VD)
(10)	$\vdash (A \,\&\, (B \,\&\, C)) \to ((A \,\&\, B) \,\&\, C)$	(obdobně)
(11)	$\vdash ((A \,\&\, B) \,\&\, C) \leftrightarrow (A \,\&\, (B \,\&\, C))$	(5.2 (vii) z (9) a (10))

☆

5.5 Lemma. Pro libovolné formule $A_1, \ldots, A_n$ a množinu předpokladů T platí:

$$T \vdash A_1 \,\&\, \ldots \,\&\, A_n \quad \Leftrightarrow \quad T \vdash A_1 \text{ a } \ldots \text{ a } T \vdash A_n \qquad \text{(KF')}$$

Důkaz. Jde o zobecnění lemmatu 5.1, které použijeme opakovaně:

$$\begin{aligned} T \vdash A_1 \,\&\, \ldots \,\&\, A_n &\Leftrightarrow T \vdash A_1 \text{ a } T \vdash A_2 \,\&\, \ldots \,\&\, A_n \\ &\Leftrightarrow T \vdash A_1 \text{ a } T \vdash A_2 \text{ a } T \vdash A_3 \,\&\, \ldots \,\&\, A_n \\ &\;\;\vdots \\ &\Leftrightarrow T \vdash A_1 \text{ a } T \vdash A_2 \text{ a } \ldots \text{ a } T \vdash A_n \end{aligned}$$

☆

5.6 Důsledek. Pro libovolné formule $A_1, \ldots, A_n$ a $i \in \{1, \ldots, n\}$ platí:

$$\begin{array}{ll} A_1 \,\&\, \ldots \,\&\, A_n \vdash A_i & \vdash (A_1 \,\&\, \ldots \,\&\, A_n) \to A_i \\ A_1, \ldots, A_n \vdash A_1 \,\&\, \ldots \,\&\, A_n & \vdash A_1 \to \ldots \to A_n \to (A_1 \,\&\, \ldots \,\&\, A_n) \end{array}$$

Důkaz. Stejně jako důsledky 5.2 (i), (ii) a (iii), tentokrát z lemmatu 5.5. ☆

5.7 Tvrzení.

$$\vdash (A_1 \to A_2 \to \ldots \to A_n \to B) \leftrightarrow ((A_1 \,\&\, A_2 \,\&\, \ldots \,\&\, A_n) \to B)$$

Důkaz. Pro dopřednou implikaci vyjdeme z množiny předpokladů:

$$T = \{(A_1 \,\&\, \ldots \,\&\, A_n), (A_1 \to \ldots \to A_n \to B)\}$$

Protože zřejmě $T \vdash A_1 \,\&\, \ldots \,\&\, A_n$, máme díky lemmatu 5.5:

$$T \vdash A_1 \quad \text{a} \quad \ldots \quad \text{a} \quad T \vdash A_n$$

Skombinujeme-li to dohromady s $T \vdash A_1 \to \ldots \to A_n \to B$, dostaneme pomocí n-násobného použití pravidla (MP) větu $T \vdash B$. Odtud již pomocí věty o dedukci dojdeme k našemu cíli:

$$\vdash (A_1 \to \ldots \to A_n \to B) \to ((A_1 \,\&\, A_2 \,\&\, \ldots \,\&\, A_n) \to B)$$

U opačné implikace vyjdeme z tentokrát z těchto předpokladů:

$$T = \{((A_1 \,\&\, \ldots \,\&\, A_n) \to B), A_1, \ldots, A_n\}$$

Nyní platí $T \vdash A_1$, $T \vdash A_2$, …, $T \vdash A_n$ a proto opět podle lemmatu 5.5:

$$T \vdash A_1 \,\&\, \ldots \,\&\, A_n$$

A protože máme taky $T \vdash (A_1 \,\&\, \ldots \,\&\, A_n) \to B$, dostaneme pomocí pravidla (MP) větu $T \vdash B$. Nyní použijeme $(n{+}1)$-krát větu o dedukci a získáme konečně:

$$\vdash ((A_1 \,\&\, \ldots \,\&\, A_n) \to B) \to (A_1 \to \ldots \to A_n \to B)$$

5.8 Věta o ekvivalenci pro výrokovou logiku. Nechť formule A' vznikne z formule A nahrazením některých výskytů podformulí $A_1, A_2, \ldots, A_n$ po řadě formulemi $A'_1, A'_2, \ldots, A'_n$, kde pro $\forall i \in \{1, \ldots, n\}$ je $\vdash A_i \leftrightarrow A'_i$. Potom:

$$\vdash A \leftrightarrow A'$$

Důkaz. Indukcí podle složitosti formule A:

- Formule A je nějaká z formulí A_i a její výskyt byl nahrazen, čili $A' = A'_i$. Ekvivalence $\vdash A \leftrightarrow A'$ potom plyne přímo z příslušného předpokladu $\vdash A_i \leftrightarrow A'_i$.
- Formule A je nenahrazená výroková proměnná. V tom případě je $A = A'$ a ekvivalence $\vdash A \leftrightarrow A'$ plyne z (V1) a důsledku 5.2 (vii).
- Formule A je nenahrazená formule tvaru $\neg B$, přičemž $\vdash B \leftrightarrow B'$ bylo již dokázáno. Potom $A' = \neg B'$. Formuli $A \leftrightarrow A'$ neboli $\neg B \leftrightarrow \neg B'$ dokážeme takto:

(1)	$\vdash B \to B'$	(předpoklad)
(2)	$\vdash \neg B' \to \neg B$	(V5, MP)
(3)	$\vdash B' \to B$	(předpoklad)
(4)	$\vdash \neg B \to \neg B'$	(V5, MP)
(5)	$\vdash \neg B \leftrightarrow \neg B'$	(výsledek)

- Formule A je nenahrazená formule tvaru $B \to C$, přičemž $\vdash B \leftrightarrow B'$ a $\vdash C \leftrightarrow C'$ bylo již dokázáno. Potom $A' = B' \to C'$. První implikaci $A \to A'$ neboli $(B \to C) \to (B' \to C')$ dokážeme za použití věty o skládání implikací:

  $$(1) \qquad \vdash (B' \to B) \to (B \to C) \to (C \to C') \to (B' \to C') \qquad \text{(SI)}$$

  Pokračujeme takto:

  $$\begin{array}{lll} (2) & \vdash B' \to B & \text{(předpoklad)} \\ (3) & \vdash (B \to C) \to (C \to C') \to (B' \to C') & \text{(MP z (1) a (2))} \\ (4) & B \to C \vdash (C \to C') \to (B' \to C') & \text{(VD)} \\ (5) & \vdash C \to C' & \text{(předpoklad)} \\ (6) & B \to C \vdash B' \to C' & \text{(MP z (4) a (5))} \\ (7) & \vdash (B \to C) \to (B' \to C') & \text{(VD)} \end{array}$$

  Opačná implikace a tedy i celková formule $A \leftrightarrow A'$ se dokáže naprosto stejně, pouze zaměníme čárkované a nečárkované symboly pro formule.

  ☆

5.9 Věta (de Morganova pravidla).

$$\begin{array}{ll} \text{(i)} & \vdash \neg(A \,\&\, B) \leftrightarrow (\neg A \vee \neg B) \\ \text{(ii)} & \vdash \neg(A \vee B) \leftrightarrow (\neg A \,\&\, \neg B) \end{array}$$

Důkaz. (i) Z vět (V3), (V4) a (KI) plyne $\vdash \neg\neg A \leftrightarrow A$. Toto aplikujeme na formuli $\neg\neg(A \to \neg B)$, která je přepisem $\neg(A \,\&\, B)$, a dostaneme dle věty o ekvivalenci:

$$(1) \qquad \vdash \neg\neg(A \to \neg B) \leftrightarrow (A \to \neg B)$$

Totéž aplikujeme na formuli A v druhé závorce:

$$(2) \qquad \vdash \neg\neg(A \to \neg B) \leftrightarrow (\neg\neg A \to \neg B)$$

Podrobně řečeno jsme použitím věty o ekvivalenci získali ekvivalenci, která má na levé straně formuli (1) a na pravé (2). Z této ekvivalence jsme vybrali dopřednou implikaci (KI) a k získání (2) jsme aplikovali (MP) na (1) a tuto implikaci.

Formule (2) už není nic jiného než přepis dokazované (i).

(ii) Tato věta je ještě jednodušší. Ve formuli $\neg(\neg A \to B)$ (což je $\neg(A \vee B)$) stačí nahradit formuli B formulí $\neg\neg B$ a z věty o ekvivalenci dostaneme

$$\vdash \neg(\neg A \to B) \leftrightarrow \neg(\neg A \to \neg\neg B)$$

což je přepis dokazované (ii). ✯

5.10 Důsledek (zobecněná de Morganova pravidla).

$$\begin{aligned} &\text{(i)} && \vdash \neg(A_1 \,\&\, \ldots \,\&\, A_n) \leftrightarrow (\neg A_1 \vee \ldots \vee \neg A_n) \\ &\text{(ii)} && \vdash \neg(A_1 \vee \ldots \vee A_n) \leftrightarrow (\neg A_1 \,\&\, \ldots \,\&\, \neg A_n) \end{aligned}$$

Důkaz. Z de Morganových pravidel a věty o ekvivalenci:

$$\begin{aligned} \vdash \neg(A_1 \,\&\, \ldots \,\&\, A_n) &\leftrightarrow \neg A_1 \vee \neg(A_2 \,\&\, \ldots \,\&\, A_n) \\ &\leftrightarrow \neg A_1 \vee \neg A_2 \vee (A_3 \,\&\, \ldots \,\&\, A_n) \\ &\;\vdots \\ &\leftrightarrow \neg A_1 \vee \neg A_2 \vee \ldots \vee \neg A_n \end{aligned}$$

$$\begin{aligned} \vdash \neg(A_1 \vee \ldots \vee A_n) &\leftrightarrow \neg A_1 \,\&\, \neg(A_2 \vee \ldots \vee A_n) \\ &\leftrightarrow \neg A_1 \,\&\, \neg A_2 \,\&\, (A_3 \vee \ldots \vee A_n) \\ &\;\vdots \\ &\leftrightarrow \neg A_1 \,\&\, \neg A_2 \,\&\, \ldots \,\&\, \neg A_n \end{aligned}$$

✯

5.11 Vlastnosi disjunkce.

(i)	$\vdash A \to (A \vee B)$	(monotónnost)
(ii)	$\vdash B \to (A \vee B)$	(monotónnost)
(iii)	$\vdash A \leftrightarrow (A \vee A)$	(idempotence)
(iv)	$\vdash (A \vee B) \leftrightarrow (B \vee A)$	(komutativnost)
(v)	$\vdash ((A \vee B) \vee C) \leftrightarrow (A \vee (B \vee C))$	(asociativita)

Důkaz. (i) Uvědomíme-li si, že $A \vee B$ je pouze zkratka za $\neg A \to B$, je tvrzení (i) $(A \to (\neg A \to B))$ shodné s větou (V2') a tvrzení (ii) $(B \to (\neg A \to B))$ je axiomem (A1).

(iii) Podle věty 5.4 (i) je $\vdash \neg A \leftrightarrow (\neg A \,\&\, \neg A)$, z čehož aplikací věty o ekvivalenci a de Morganova pravidla získáme $\vdash \neg A \leftrightarrow \neg(A \vee A)$. Odtud již pomocí lemmatu 5.3 plyne dokazované tvrzení.

(iv) Opět vyjdeme z věty 5.4. Podle (ii) je $\vdash (\neg A \,\&\, \neg B) \leftrightarrow (\neg B \,\&\, \neg A)$, z čehož podobně získáme $\vdash \neg(A \vee B) \leftrightarrow \neg(B \vee A)$ a nakonec i dokazovanou větu.

(v) Taktéž obdobně z asociativity konjunkce. ✯

5.12 Lemma o důkazu rozborem případů. Nechť T je množina formulí a A, B, C jsou formule. Potom platí:

$$T, A \vee B \vdash C \qquad \Leftrightarrow \qquad T, A \vdash C \quad \text{a} \quad T, B \vdash C$$

Důkaz.

⇒) Snadno z monotónnosti disjunkce:

(1)	$T, A \vdash A \vee B$	(5.11 (i), VD)
(2)	$T, B \vdash A \vee B$	(5.11 (ii), VD)
(3)	$T \vdash (A \vee B) \to C$	(předpoklad, VD)
(4)	$T, A \vdash C$	(MP z (1) a (3))
(5)	$T, B \vdash C$	(MP z (2) a (3))

⇐) Takto:

(1)	$T, \neg C \vdash \neg A$	(předpoklad, VD, V5, MP, VD)
(2)	$T, \neg C \vdash \neg B$	(předpoklad, VD, V5, MP, VD)
(3)	$T, \neg C \vdash \neg A \,\&\, \neg B$	(KF)
(4)	$T, \neg C \vdash \neg(A \vee B)$	(de Morgan, KI, MP)
(5)	$T, A \vee B \vdash C$	(VD, A3, MP, VD)

✡

5.13 Distributivnost konjunkce a disjunkce.

(i)	$\vdash (A \vee (B \,\&\, C)) \leftrightarrow ((A \vee B) \,\&\, (A \vee C))$
(ii)	$\vdash (A \,\&\, (B \vee C)) \leftrightarrow ((A \,\&\, B) \vee (A \,\&\, C))$

Důkaz. (i) Z monotónnosti disjunkce, (VD) a (KF) dostaneme:

$$A \vdash (A \vee B) \,\&\, (A \vee C)$$

Totéž dokážeme z předpokladu $B \,\&\, C$:

(1)	$B \,\&\, C \vdash B$	(5.2 (i))
(2)	$B \,\&\, C \vdash A \vee B$	(5.11 (ii), MP)
(3)	$B \,\&\, C \vdash C$	(5.2 (i))
(4)	$B \,\&\, C \vdash A \vee C$	(5.11 (ii), MP)
(5)	$B \,\&\, C \vdash (A \vee B) \,\&\, (A \vee C)$	(KF)

Dohromady podle lemmatu o důkazu rozborem případů a (VD) dostáváme:

$$\vdash (A \vee (B \,\&\, C)) \to ((A \vee B) \,\&\, (A \vee C))$$

Pro opačnou implikaci vyjdeme z toho, že $A \vee B$ je pouze jinak zapsaná formule $\neg A \to B$:

(1)	$(A \vee B) \,\&\, (A \vee C), \neg A \vdash \neg A \to B$	(KF, přepis)
(2)	$(A \vee B) \,\&\, (A \vee C), \neg A \vdash \neg A \to C$	(KF, přepis)
(3)	$(A \vee B) \,\&\, (A \vee C), \neg A \vdash B$	(DP, MP)
(4)	$(A \vee B) \,\&\, (A \vee C), \neg A \vdash C$	(DP, MP)
(5)	$(A \vee B) \,\&\, (A \vee C), \neg A \vdash B \,\&\, C$	(KF)
(6)	$(A \vee B) \,\&\, (A \vee C) \vdash A \vee (B \,\&\, C)$	(VD, přepis)

A odtud již jedinou (VD):

$$\vdash ((A \vee B) \,\&\, (A \vee C)) \to (A \vee (B \,\&\, C))$$

(ii) Dokážeme z (i) pomocí de Morganových pravidel, věty o ekvivalenci a lemmatu 5.3:

$$\begin{aligned}
&\vdash (\neg A \vee (\neg B \,\&\, \neg C)) \leftrightarrow ((\neg A \vee \neg B) \,\&\, (\neg A \vee \neg C)) \\
&\vdash (\neg A \vee \neg(B \vee C)) \leftrightarrow (\neg(A \,\&\, B) \,\&\, \neg(A \,\&\, C)) \\
&\vdash \neg(A \,\&\, (B \vee C)) \leftrightarrow \neg((A \,\&\, B) \vee (A \,\&\, C)) \\
&\vdash (A \,\&\, (B \vee C)) \leftrightarrow ((A \,\&\, B) \vee (A \,\&\, C))
\end{aligned}$$

☆

5.14 Důsledek (zobecněná distributivnost).

(i) $\vdash (A \vee (B_1 \,\&\, \ldots \,\&\, B_n)) \leftrightarrow ((A \vee B_1) \,\&\, \ldots \,\&\, (A \vee B_n))$

(ii) $\vdash (A \,\&\, (B_1 \vee \ldots \vee B_n)) \leftrightarrow ((A \,\&\, B_1) \vee \ldots \vee (A \,\&\, B_n))$

Důkaz. Podobně jako důsledek 5.10 (zobecněná de Morganova pravidla). ☆

6 Normální formy výrokových formulí

6.1 Definice.

- *Literál* je výroková proměnná nebo její negace.
- *Klauzule* je disjunkce literálů.

6.2 Definice.

- Formule je v *konjunktivní normální formě* (CNF), má-li tvar konjunkce klauzulí.
- Formule je v *disjunktivní normální formě* (DNF), má-li tvar disjunkce konjunkcí literálů.

6.3 Věta o normálních tvarech. Ke každé formuli A výrokové logiky lze sestrojit formule A_k a A_d takové, že A_k je v konjunktivní normální formě, A_d je v disjunktivní normální formě a platí:

$$\vdash A \leftrightarrow A_k \qquad\qquad \vdash A \leftrightarrow A_d$$

Důkaz. Indukcí podle složitosti formule A:

- Je-li A prvotní formule, je podle definice v CNF i DNF.
- Je-li A tvaru $\neg B$, potom předpokládáme, že již máme sestrojeny B_k v CNF a B_d v DNF, obě ekvivalentní s B.

  Nechť B_d je tvaru $B_1 \vee \ldots \vee B_n$, kde B_i je tvaru $L^i_1 \,\&\, \ldots \,\&\, L^i_{m_i}$. Ze zobecněných de Morganových pravidel máme

  $$\vdash B \leftrightarrow B_d \quad \Rightarrow \quad \vdash \neg B \leftrightarrow \neg B_d \quad \Rightarrow \quad \vdash \neg B \leftrightarrow (\neg B_1 \,\&\, \ldots \,\&\, \neg B_n)$$

  kde $\neg B_i \leftrightarrow (\neg L^i_1 \vee \ldots \vee \neg L^i_{m_i})$. Nechť A_i vznikne z $\neg L^i_1 \vee \ldots \vee \neg L^i_{m_i}$ vynecháním dvojitých negací u literálů. Potom máme

  $$\vdash A \leftrightarrow (A_1 \,\&\, \ldots \,\&\, A_n)$$

  kde napravo máme konjunkci disjunkcí literálů a tedy formuli A_k v CNF. Uvedená ekvivalence platí díky větě o ekvivalenci.

  Stejným způsobem se dá z formule B_k v CNF sestrojit formule A_d v DNF.
- Je-li A tvaru $B \to C$, z indukčního předpokladu máme příslušné B_d, C_d, B_k a C_k. Zřejmě platí (což lze dokázat větou o ekvivalenci):

  $$\vdash (B \to C) \leftrightarrow (\neg B \vee C)$$

  a díky tomu stačí k sestrojení A_d v DNF sestrojit DNF D formule $\neg B_k$, což již umíme. Potom totiž bude formule $D \vee C_d$ hledanou formulí A_d.

  K sestrojení A_k v KNF vyjdeme z KNF tvaru $D_1 \,\&\, \ldots \,\&\, D_n$ formule $\neg B_d$, kde D_i jsou klauzule. Dostáváme:

  $$\vdash A \leftrightarrow ((D_1 \,\&\, \ldots \,\&\, D_n) \vee C_k)$$

  Odtud ze zobecněné distributivity plyne:

  $$\vdash A \leftrightarrow ((D_1 \vee C_k) \,\&\, \ldots \,\&\, (D_n \vee C_k)) \tag{1}$$

  Formule C_k je v CNF a proto má tvar $K_1 \,\&\, \ldots \,\&\, K_m$, kde K_i je klauzule. Pro každé $i \in SetN$ potom je, opět ze zobecněné distributivity:

  $$\vdash (D_i \vee C_k) \leftrightarrow ((D_i \vee K_1) \,\&\, \ldots \,\&\, (D_i \vee K_m))$$

  Formule napravo je v CNF a proto bude v CNF i formule A_c, která vznikne nahrazením příslušných $(D_i \vee C_k)$ na pravé straně (1).

  ✡

Část II
Predikátová logika

7 Úvod do predikátové logiky

Nyní, když už máme za sebou základy ve formě výrokové logiky, můžeme začít podrobněji zkoumat samotné prvotní formule. Ty zde bude představovat *predikát* aplikovaný na výrazy (*termy*), které mohou obsahovat *proměnné*. Proměnné mají jediný typ, universum dané interpretace jazyka, a lze je kvantifikovat.

7.1 Definice. *Jazyk prvního řádu* obsahuje následující symboly:

- *proměnné* – zastupují jednotlivá individua universa. Každý jazyk jich má k dispozici neomezené množství.
- *funkční symboly* – označují operace na n individuích, kde $n \in \mathbb{N}_0$ je *četnost* neboli počet parametrů dané funkce. Výsledkem operace je opět individuum. Funkční symboly s četností 0 budeme považovat za *konstanty*.
- *predikátové symboly* – označují relaci na n individuích, kde $n \in \mathbb{N}$ je *četnost* neboli počet parametrů daného predikátu[4].
- *logické spojky* – unární $\neg$ (negace) a binární $\&$ (konjunkce), $\vee$ (disjunkce), $\rightarrow$ (implikace) a $\leftrightarrow$ (ekvivalence).
- *kvantifikátory* – $\forall$ a $\exists$.
- *pomocné symboly* – závorky a jiné symboly bez sémantického významu. Tyto symboly nevystupují přímo v pomyslném syntaktickém stromu výrazů, pouze jej pomáhají přehledně a jednoznačně zapsat.

Někdy do jazyka zahrnujeme i speciální symbol $=$ pro predikát rovnosti. Pro tento predikát platí jistá speciální pravidla a potom hovoříme o *jazyku s rovností*.

7.2 Definice. Symboly jazyka prvního řádu dělíme do dvou skupin, a to:

- *logické symboly* – společné všem formálním jazykům bez ohledu na konkrétní účel jazyka. Jde o proměnné, logické spojky, kvantifikátory, pomocné symboly a predikát rovnosti, je-li v jazyku obsažen.
- *speciální symboly* – funkce a predikáty, které byly k jazyku přidány za účelem použití v konkrétní matematické disciplíně, která jazyk využívá.

[4] Predikátové symboly by teoreticky mohly mít i nulovou četnost, potom by plnily roli *logických konstant*. Přestože je nebudeme využívat, občas se s nimi lze setkat. Konstanta „pravda“ se zapisuje symbolem $\top$ (*top*) a „nepravda“ symbolem $\bot$ (*bottom*).

Jazyk je tedy jednoznačně určen výčtem svých speciálních symbolů a tím, zda obsahuje predikát rovnosti.

Ze symbolů jazyka se tvoří výrazy, které mohou být dvojího typu: *termy* a *formule*. Termy vzniknou postupnou aplikací funkcí na proměnné nebo konstanty a jejich hodnotou je objekt univresa, individuum. Formule vzniknou aplikací predikátu na termy, spojením jiných formulí logickými spojkami či kvantifikováním jiných formulí. Hodnotou formulí je pravdivostní hodnota.

7.3 Definice. *Term* vznikne konečným počtem použití těchto induktivních pravidel:

(i) Každá proměnná je term.

(ii) Je-li f n-ární funkční symbol a výrazy $t_1, t_2, \ldots, t_n$ jsou termy, potom je term i výraz:
$$f(t_1, t_2, \ldots, t_n)$$

7.4 Definice. *Formule* predikátové logiky vznikne konečným počtem použití těchto induktivních pravidel:

(i) Je-li p n-ární predikátový symbol a výrazy $t_1, t_2, \ldots, t_n$ jsou termy, potom je výraz
$$p(t_1, t_2, \ldots, t_n)$$
formule. Taková formule se navíc nazývá *atomická formule*.

(ii) Jsou-li výrazy A, B formule, jsou formule i výrazy:
$$\neg A \qquad (A \,\&\, B) \qquad (A \vee B) \qquad (A \to B) \qquad (A \leftrightarrow B)$$

(iii) Je-li x proměnná a A formule, jsou formule i výrazy:
$$(\forall x)A \qquad (\exists x)A$$

7.5 Definice. Nechť t je term a A formule.

- Podslovo s termu t, které je samo termem, nazveme *podterm* termu t.
- Podslovo B formule A, které je samo formulí, nazveme *podformule* formule A.

7.6 Definice. Nechť A je formule a x nějaká její proměnná. Řekneme, že proměnná x má ve formuli A *vázaný výskyt*, je-li tento výskyt součástí nějaké podformule A tvaru $(\forall x)B$ nebo $(\exists x)B$. V opačném případě je tento výskyt *volný*.

Řekneme, že má proměnná x je ve formuli A *volná*, pokud v ní má volný výskyt. Řekneme, že má proměnná x je ve formuli A *vázaná*, pokud v ní má vázaný výskyt.

7.7 Definice.

- Formule A je *otevřená*, pokud neobsahuje žádnou vázanou proměnnou.
- Formule A je *uzavřená*, pokud neobsahuje žádnou volnou proměnnou.

8 Sémantika predikátové logiky

V této kapitole se budeme zabývat pravdivostí formulí predikátové logiky. K tomu budeme potřebovat přiřadit použitému jazyku nějaký konkrétní význam, interpretaci.

8.1 Definice. *Interpretace (realizace)* jazyka L je relační struktura $\mathbb{M}$ obsahující:

- Neprázdnou množinu M, kterou nazýváme *universum (doména)* a její prvky *individua*.
- Pro každý n-ární funkční symbol f zobrazení $f_{\mathbb{M}} : M^n \to M$, které nazýváme *realizace funkčního symbolu* f.
- Pro každý n-ární predikátový symbol p (kromě případného symbolu pro predikát rovnosti) relaci $p_{\mathbb{M}} \subseteq M^n$, kterou nazýváme *realizace predikátového symbolu* p.

8.2 Definice. *Ohodnocení proměnných* (jazyka L při interpretaci $\mathbb{M}$) je zobrazení $e : P \to M$, kde P je množina všech proměnných jazyka L a M je doména $\mathbb{M}$.

8.3 Definice. *Interpretace termu* t při ohodnocení e (a při realizaci $\mathbb{M}$ jazyka L) se značí $t[e]$ (nebo $t[e, \mathbb{M}]$, není-li struktura $\mathbb{M}$ jasná z kontextu) a je definována takto:

$$t[e] = \begin{cases} e(x) & \text{je-li } t \text{ proměnná } x, \\ f_{\mathbb{M}}(t_1[e], t_2[e], \ldots, t_n[e]) & \text{je-li } t \text{ tvaru } f(t_1, t_2, \ldots, t_n). \end{cases}$$

8.4 Lemma. Nechť P je množina všech proměnných termu t a e, e' jsou dvě ohodnocení taková, že pro $\forall x \in P$ je $e(x) = e'(x)$. Potom $t[e] = t[e']$.

Důkaz. Indukcí podle složitosti termu t. Je-li t proměnná x, potom $x \in P$ a z předpokladu máme:

$$t[e] = e(x) = e'(x) = t[e']$$

Jinak je t tvaru $f(t_1, t_2, \ldots, t_n)$, přičemž pro $\forall t_i$ platí indukční předpoklad, potom:

$$t[e] = f_{\mathbb{M}}(t_1[e], t_2[e], \ldots, t_n[e]) = f_{\mathbb{M}}(t_1[e'], t_2[e'], \ldots, t_n[e']) = t[e']$$

☆

8.5 Definice. Nechť e je ohodnocení proměnných, $x_1, x_2, \ldots, x_n$ jsou proměnné a $m_1, m_2, \ldots, m_n \in M$ individua. Zápisem $e(x_1/m_1, x_2/m_2, \ldots, x_n/m_n)$ rozumíme *pozměněné ohodnocení* definované předpisem:

$$e(x_1/m_1, x_2/m_2, \ldots, x_n/m_n)(y) = \begin{cases} m_i & \text{je-li } y = x_i \text{ pro nějaké } i, \\ e(y) & \text{jinak.} \end{cases}$$

V ohodnocení e vlastně nahradíme hodnotu přiřazenou proměnné x individuem m.

8.6 Definice pravdivosti formule (Tarski). Nechť L je jazyk, $\mathbb{M}$ jeho interpretace, e ohodnocení proměnných a A formule jazyka L. Říkáme, že A je *splněna* v $\mathbb{M}$ při ohodnocení e, a píšeme $\mathbb{M} \vDash A[e]$ za některé z těchto podmínek:

- Formule A je atomická formule tvaru $p(t_1, t_2, \ldots, t_n)$, kde p není predikát rovnosti, a platí:
$$(t_1[e], t_2[e], \ldots, t_n[e]) \in p_{\mathbb{M}}$$
- Formule A je atomická formule tvaru $t_1 = t_2$ a platí:
$$t_1[e] = t_2[e]$$
- Formule A je tvaru $\neg B$ a $\mathbb{M} \nvDash B[e]$.
- Formule A je tvaru $B \to C$ a $\mathbb{M} \nvDash B[e]$ nebo $\mathbb{M} \vDash C[e]$.
- Formule A je tvaru $(\forall x)B$ a $\mathbb{M} \vDash B[e(x/m)]$ pro každé $m \in M$.
- Formule A je tvaru $(\exists x)B$ a $\mathbb{M} \vDash B[e(x/m)]$ pro nějaké $m \in M$.

Formule A je *pravdivá* v $\mathbb{M}$ (značeno $\mathbb{M} \vDash A$), je-li A splněna v $\mathbb{M}$ při každém ohodnocení proměnných.

8.7 Pozorování. Nechť P je množina všech volných proměnných formule A a e, e' jsou dvě ohodnocení taková, že pro $\forall x \in P$ je $e(x) = e'(x)$. Potom $\mathbb{M} \vDash A[e]$, právě když $\mathbb{M} \vDash A[e']$.

Důkaz. Indukcí podle složitosti formule A:

- Je-li A atomická formule tvaru $p(t_1, t_2, \ldots, t_n)$, jsou v ní všechny proměnné volné a podle předpokladu a lemmatu 8.4 je:
$$(t_1[e], t_2[e], \ldots, t_n[e]) \in p_{\mathbb{M}} \quad \Leftrightarrow \quad (t_1[e'], t_2[e'], \ldots, t_n[e']) \in p_{\mathbb{M}}$$
- Je-li A formule tvaru $\neg B$ nebo $B \to C$, kde pro B a C tvrzení platí, bude jistě platit i pro formuli A.
- Je-li A formule tvaru $(\forall x)B$ nebo $(\exists x)B$,

- TODO!

☆

Splnitelnost uzavřené formule tedy nezávisí na ohodnocení proměnných.

8.8 Definice. Formule A je *validní* (*platná*, *logicky pravdivá*), jestliže je pravdivá při každé interpretaci svého jazyka. Takovou formuli značíme $\vDash A$.

8.9 Definice. Jsou-li $x_1, \ldots, x_n$ různé proměnné, t term a $t_1, t_2, \ldots, t_n$ termy, potom výrazem

$$t_{x_1,x_2,\ldots,x_n}[t_1, t_2, \ldots, t_n]$$

označíme term, který vznikne z t (současným) nahrazením každého výskytu proměnné x_i termem t_i pro $\forall i \in \{1, \ldots, n\}$.

Protože nahrazujeme podterm jiným termem, je zřejmé, že takto vznikne opět term.

8.10 Definice. Jsou-li $x_1, \ldots, x_n$ různé proměnné, A formule a $t_1, t_2, \ldots, t_n$ termy, potom výrazem

$$A_{x_1,x_2,\ldots,x_n}[t_1, t_2, \ldots, t_n]$$

označíme formuli, která vznikne z A (současným) nahrazením každého volného výskytu proměnné x_i termem t_i pro $\forall i \in \{1, \ldots, n\}$.

Vzniklé formuli se říká *instance* formule A.

BAisahu

8.11 Definice. Term t je *substituovatelný* do formule A za proměnnou x, jestliže pro každou proměnnou y vyskytující se v termu t žádná podformule A tvaru $(\forall y)B$ a $(\exists y)B$ neobsahuje x jako volnou proměnnou z hlediska formule A.

Čili je-li term t je substituovatelný do formule A za proměnnou x, pak nahrazení volného výskytu proměnné x ve formuli A termem t nezpůsobí to, že by se nějaká proměnná termu t stala ihned po nahrazení vázanou.

Substituovatelnost je snadné rozpoznat za těchto okolností:

- Formule A je otevřená.
- Žádná proměnná substituovaných termů není vázaná v A.

8.12 Lemma. Nechť L je jazyk, $\mathbb{M}$ jeho interpretace, A formule, $t, t_1, t_2, \ldots, t_n$ termy, e ohodnocení a $m_1, m_2, \ldots, m_n$ individua $\mathbb{M}$ taková, že $\forall i \in \{1, \ldots, n\}$ je $m_i = t_i[e]$. Potom:

(i) $\quad t_{x_1,\ldots,x_n}[t_1, \ldots, t_n][e] \quad = \quad t[e(x_1/m_1, \ldots, x_n/m_n)]$

(ii) $\quad \mathbb{M} \vDash A_{x_1,\ldots,x_n}[t_1, \ldots, t_n][e] \quad \Leftrightarrow \quad \mathbb{M} \vDash A[e(x_1/m_1, \ldots, x_n/m_n)]$

Důkaz. (i) Indukcí podle složitosti termu t. Označme t' term $t_{x_1,\ldots,x_n}[t_1,\ldots,t_n]$.

- Je-li t jedna z proměnných x_i, je t' rovna t_i. Potom podle předpokladu máme $t'[e] = t_i[e] = m_i$, což je rovno $t[e(x_1/m_1,\ldots,x_n/m_n)]$.
- Je-li t jiná proměnná, potom zřejmě tvrzení platí.
- Je-li t tvaru $f(s_1,\ldots,s_r)$, z indukčního předpokladu máme pro $\forall i \in \{1,\ldots,r\}$:

  $$s_{ix_1,\ldots,x_n}[t_1,\ldots,t_n][e] = s_i[e(x_1/m_1,\ldots,x_n/m_n)]$$

  Individuum $t'[e]$ je rovno

  $$f_{\mathbb{M}}(s_{1x_1,\ldots,x_n}[t_1,\ldots,t_n][e],\ldots,s_{rx_1,\ldots,x_n}[t_1,\ldots,t_n][e])$$

  což je díky indukčním předpokladům rovno

  $$f_{\mathbb{M}}(s_1[e(x_1/m_1,\ldots,x_n/m_n)],\ldots,s_r[e(x_1/m_1,\ldots,x_n/m_n)])$$

  a to je rovno:

  $$t[e(x_1/m_1,\ldots,x_n/m_n)]$$

(ii) Indukcí podle složitosti formule A. Označme A' formuli $A_{x_1,\ldots,x_n}[t_1,\ldots,t_n]$.

- Je-li A atomická formule tvaru $p(s_1,\ldots,s_r)$, máme díky bodu (i) tohoto lemmatu:

  $$\begin{aligned}\mathbb{M} \vDash A'[e] &\Leftrightarrow (s_{1x_1,\ldots,x_n}[t_1,\ldots,t_n][e],\ldots,s_{rx_1,\ldots,x_n}[t_1,\ldots,t_n][e]) \in p_{\mathbb{M}}\\ &\Leftrightarrow (s_1[e(x_1/m_1,\ldots,x_n/m_n)],\ldots,s_r[e(x_1/m_1,\ldots,x_n/m_n)]) \in p_{\mathbb{M}}\\ &\Leftrightarrow \mathbb{M} \vDash A[e(x_1/m_1,\ldots,x_n/m_n)]\end{aligned}$$

- Je-li A tvaru $\neg B$, máme díky indukci a definici sémantiky negace:

  $$\begin{aligned}\mathbb{M} \vDash A'[e] &\Leftrightarrow \mathbb{M} \nvDash B'[e] && \text{(význam negace)}\\ &\Leftrightarrow \mathbb{M} \nvDash B[e(x_1/m_1,\ldots,x_n/m_n)] && \text{(indukční předpoklad)}\\ &\Leftrightarrow \mathbb{M} \vDash A[e(x_1/m_1,\ldots,x_n/m_n)] && \text{(význam negace)}\end{aligned}$$

- Je-li A binární logickou spojkou formulí B a C, postupujeme obdobně. Formule A' je splněna při $\mathbb{M}$ a e, právě když jsou za těchto okolností splněny či nesplněny formule B' a C' dle významu té které spojky. Splněnost těchto formulí je ale dle indukčního předpokladu ekvivalentní splněnosti těchto formulí při ohodnocení $e(x_1/m_1,\ldots,x_n/m_n)$. To je zase ekvivalentní splněnosti formule A' při ohodnocení $e(x_1/m_1,\ldots,x_n/m_n)$ dle významu dané spojky. Hotovo.
- Je-li A tvaru $(Qz)B$ a z je nějaká z proměnných x_i, potom A' je formule:

  $$(Qx_i)\overbrace{B_{x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n}[t_1,\ldots,t_{i-1},t_{i+1},\ldots,t_n]}^{B'}$$

Nahrazuje-li Q' slovo „libovolné“ nebo „nějaké“ podle kvantifikátoru Q, potom:

$$\begin{aligned}\mathbb{M} \vDash A'[e] &\Leftrightarrow \mathbb{M} \vDash B'[e(x_1/m)] \text{ pro } Q'\ m \in \mathbb{M} \\ &\Leftrightarrow \mathbb{M} \vDash B[e(x_1/m_1, \ldots, x_i/m, \ldots, x_n/m_n)] \text{ pro } Q'\ m \in \mathbb{M} \\ &\Leftrightarrow \mathbb{M} \vDash A[e(x_1/m_1, \ldots, x_n/m_n)]\end{aligned}$$

První ekvivalence plyne z významu kvantifikátoru Q, druhá z indukčního předpokladu a poslední z toho, že pravdivost formule A na ohodnocení proměnné x_i vůbec nezávisí.

- Je-li A tvaru $(Qz)B$ a z není žádná z proměnných x_i, potom máme obdobně:

$$\begin{aligned}\mathbb{M} \vDash A'[e] &\Leftrightarrow \mathbb{M} \vDash B'[e(z/m)] \text{ pro } Q'\ m \in \mathbb{M} \\ &\Leftrightarrow \mathbb{M} \vDash B[e(z/m, x_1/m_1, \ldots, x_n/m_n)] \text{ pro } Q'\ m \in \mathbb{M} \\ &\Leftrightarrow \mathbb{M} \vDash A[e(x_1/m_1, \ldots, x_n/m_n)]\end{aligned}$$

9 Formální systém predikátové logiky

9.1 Redukce jazyka. Podobně jako u výrokové logiky i zde budeme budovat formální systém pouze pro dvě logické spojky, a sice *negaci* $\neg$ a *implikaci* $\rightarrow$, a jeden kvantifikátor, *universální* $\forall$. Ostatní spojky budeme opět chápat jako odvozené a budeme je pokládat pouze za syntaktickou zkratku pro zjednodušení zápisu formulí využívajících pouze uvedených dvou spojek a kvantifikátoru. Konkrétně

$(A \,\&\, B)$	je zkratka za formuli	$\neg(A \rightarrow \neg B)$
$(A \vee B)$	je zkratka za formuli	$(\neg A \rightarrow B)$
$(A \leftrightarrow B)$	je zkratka za formuli	$(A \rightarrow B) \,\&\, (B \rightarrow A)$

a nově:

$(\exists x)A$	je zkratka za formuli	$\neg(\forall x)\neg A$

Není těžké nahlédnout, že ze sémantického hlediska je formule $(\exists x)A$ ekvivalentní formuli $\neg(\forall x)\neg A$, neboť pro každou interpretaci jazyka $\mathbb{M}$ a ohodnocení e je:

$$\begin{aligned}\mathbb{M} \vDash (\exists x)A[e] &\Leftrightarrow \text{existuje } m \in M \text{ takové, že } \mathbb{M} \vDash A[e(x/m)] \\ &\Leftrightarrow \text{není pravda, že pro každé } m \in M \text{ je } \mathbb{M} \nvDash A[e(x/m)] \\ &\Leftrightarrow \text{není pravda, že pro každé } m \in M \text{ je } \mathbb{M} \vDash \neg A[e(x/m)] \\ &\Leftrightarrow \mathbb{M} \nvDash (\forall x)\neg A[e] \\ &\Leftrightarrow \mathbb{M} \vDash \neg(\forall x)\neg A[e]\end{aligned}$$

9.2 Definice. Nechť L je jazyk prvního řádu. *Formální systém predikátové logiky bez rovnosti* obsahuje:

- *Jazyk.* Použijeme redukovaný jazyk L'.
- *Axiomy.* Jsou-li A, B, C formule, pak každá formule následujících tvarů je axiom predikátové logiky:

$$A \to (B \to A) \tag{A1}$$
$$(A \to (B \to C)) \to [(A \to B) \to (A \to C)] \tag{A2}$$
$$(\neg B \to \neg A) \to (A \to B) \tag{A3}$$

  Je-li A formule, x proměnná a t term, pak každá formule tvaru

$$(\forall x)A \to A_x[t] \tag{AS}$$

  je axiom predikátové logiky, tzv. *axiom specifikace*. Konečně jsou-li A, B formule a x proměnná, která nemá volný výskyt ve formuli A, potom je axiomem každá formule tvaru:

$$(\forall x)(A \to B) \to (A \to (\forall x)B) \tag{AP}$$

  Tomuto axiomu se říká *axiom přeskoku*.

- *Odvozovací pravidla.* Z výrokové logiky je zachováno pravidlo *modus ponens*:

  „Z formulí A a $A \to B$ odvoď formuli B.“ (MP)

  Navíc přidáme *pravidlo generalizace* (x je libovolná proměnná):

  „Z formule A odvoď formuli $(\forall x)A$.“ (PG)

9.3 Věta o přenositelnosti vět výrokové logiky. Nechť ve výrokové logice platí $T \vdash A$. Dále mějme zobrazení, které každé výrokové proměnné použité ve formulích množiny T a A přiřadí nějakou formuli predikátové logiky. Nechť množina T' a formule A' vznikne z množiny T a formule A tak, že v každé formuli nahradíme každý výskyt výrokové proměnné příslušnou formulí predikátové logiky. Potom bude v predikátové logice platit $T' \vdash A'$.

Důkaz. Mějme formální důkaz formule A z předpokladů T. V tomto důkazu nahraďme všechny výrokové proměnné příslušnými formulemi. Pokud důkaz používá nějakou výrokovou proměnnou navíc, můžeme všechny její výskyty nahradit libovolnou, ale stejnou formulí predikátové logiky. Protože je každý použitý axiom a pravidlo *modus ponens* součástí predikátové logiky, získáme formální důkaz formule A' z předpokladů T'. ☆

9.4 Poznámka. Důkazové postupy výrokové logiky se přenáší jen potud, pokud rozumíme pojmem „dokazatelnosti“ pouze dokazatelnost ve výrokové logice, tedy pomocí (A1), (A2), (A3) a (MP). Například větu o dedukci jsme dokázali jen pro formální systém výrokové logiky a nepředpokládali jsme, že by důkazy, které transformuje, používaly i (AS), (AP) nebo (PG). Predikátová logika má sice vlastní větu o dedukci, ta má ale silnější předpoklady a není tak univerzální jako její obdoba ve výrokové logice.

9.5 Pozorování. Uvědomme si například, že i nadále můžeme z platnosti ekvivalence odvodit platnost obou směrů implikace a také můžeme ekvivalenci dokázat samostatným důkazem obou implikací. To je možné díky větám výrokové logiky ukázaných v pozorování 5.2, body (iv), (v) a (vi):

$$\vdash (p \leftrightarrow q) \to (p \to q)$$
$$\vdash (p \leftrightarrow q) \to (q \to p)$$
$$\vdash (p \to q) \to (q \to p) \to (p \leftrightarrow q)$$

Díky platnosti věty

$$\vdash \neg(p \to \neg\neg p) \to q$$

(viz důkaz věty 4.3) můžeme zase charakterizovat sporné množiny jako takové množiny T, u kterých pro nějakou formuli A platí $T \vdash A \,\&\, \neg A$. Díky větám

$$\vdash (p \,\&\, q) \to p$$
$$\vdash (p \,\&\, q) \to q$$
$$\vdash p \to q \to (p \,\&\, q)$$

(viz opět důsledek 5.2, (i), (ii) a (iii)) můžeme tvrdit, že množina T je sporná, právě když pro nějakou formuli A platí $T \vdash A$ a zároveň $T \vdash \neg A$.

Často budeme používat také větu o skládání implikací a větu o záměně předpokladů. Protože v predikátové logice nemáme k dispozici plnohodnotnou obdobu věty o dedukci, budou nám tyto dva její přímé důsledky velmi užitečné.

9.6 Věta (pravidlo substituce). Pro libovolnou formuli A, proměnnou x a term t platí:

$$\vdash A_x[t] \to (\exists x)A \qquad \text{(PS)}$$

Důkaz. Ve výrokové logice zřejmě platí věta $(p \to q) \to (\neg\neg p \to q)$, což lze jednoduše dokázat například z věty o skládání implikací, (V3) a (MP). Dosazením $(\forall x)\neg A$ za p a $\neg A_x[t]$ za q dostaneme:

(1) $\vdash ((\forall x)\neg A \to \neg A_x[t]) \to (\neg\neg(\forall x)\neg A \to \neg A_x[t])$

(2) $\vdash (\forall x)\neg A \to \neg A_x[t]$ (AS)

(3) $\vdash \neg\neg(\forall x)\neg A \to \neg A_x[t]$ (MP z (1) a (2))

(4) $\vdash A_x[t] \to \neg(\forall x)\neg A$ (A3, MP)

Poslední formule není nic jiného než rozepsaná $A_x[t] \to (\exists x)A$. ☆

Všimněme si, že pravidlo substituce tvoří jakýsi doplněk k axiomu specifikace. Kromě toho je užitečné si uvědomit, že $A_x[x] = A$ a obě pravidla lze tedy použít i takto:

$$\vdash (\forall x)A \to A$$
$$\vdash A \to (\exists x)A$$

9.7 Věta (pravidlo zavedení $\forall$). Nemá-li proměnná x volný výskyt ve formuli A, potom:

$$\vdash A \to B \quad \Rightarrow \quad \vdash A \to (\forall x)B \qquad (\mathrm{Z}\forall)$$

Důkaz.

(1)	$\vdash A \to B$	(předpoklad)
(2)	$\vdash (\forall x)(A \to B)$	(PG)
(3)	$\vdash (\forall x)(A \to B) \to (A \to (\forall x)B)$	(AP)
(4)	$\vdash A \to (\forall x)B$	(MP z (2) a (3))

Předpoklad o proměnné x jsme využili v kroku (3). Bez něj bychom nemohli použít axiom přeskoku. ☆

9.8 Věta (pravidlo zavedení $\exists$). Nemá-li proměnná x volný výskyt ve formuli B, potom:

$$\vdash A \to B \quad \Rightarrow \quad \vdash (\exists x)A \to B \qquad (\mathrm{Z}\exists)$$

Důkaz.

(1)	$\vdash A \to B$	(předpoklad)
(2)	$\vdash \neg B \to \neg A$	(V5, MP)
(3)	$\vdash \neg B \to (\forall x)\neg A$	(Z$\forall$)
(4)	$\vdash \neg(\forall x)\neg A \to B$	(V5', MP)

Poslední formule již je dokazovaná $(\exists x)A \to B$. Předpoklad o proměnné x jsme využili v kroku (3). ☆

9.9 Lemma o distribuci kvantifikátorů.

$$\vdash A \to B \qquad \Rightarrow \qquad \vdash (\forall x)A \to (\forall x)B \quad \text{a} \quad \vdash (\exists x)A \to (\exists x)B \qquad (\mathrm{DK})$$

Důkaz. Oba důsledky lze ukázat z věty o skládání implikací. Napřed ji použijeme ve tvaru

$$\vdash ((\forall x)A \to A) \to (A \to B) \to ((\forall x)A \to B)$$

kde první závorka je axiom specifikace a druhá náš předpoklad. Dvojím užitím pravidla (MP) získáme samostatnou třetí závorku, na kterou ještě aplikujeme pravidlo zavedení $\forall$ (což lze, neboť x je ve formuli $(\forall x)A$ vázaná) a získáme tak:

$$\vdash (\forall x)A \to (\forall x)B$$

Druhý důsledek se dokáže obdobně. Větu o skládání implikací napíšeme jako:

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

Zde je první závroka předpoklad a druhá pravidlo substituce. Po dvou (MP) aplikujeme na třetí závorku pravidlo zavedení $\exists$ (opět si uvědomme, proč to lze). Dostaneme:

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

$\bigstar$

9.10 Věta o instancích. Nechť A je formule, $x_1, \ldots, x_n$ proměnné a $t_1, \ldots, t_n$ termy. Potom:

$$\vdash A \quad \Rightarrow \quad \vdash A_{x_1,\ldots,x_n}[t_1, \ldots, t_n]$$

Důkaz. Napřed dokážeme pomocný krok, a sice pokud $\vdash A$, pak $\vdash A_x[t]$:

(1)	$\vdash A$	(předpoklad)
(2)	$\vdash (\forall x)A$	(PG)
(3)	$\vdash (\forall x)A \to A_x[t]$	(AS)
(4)	$\vdash A_x[t]$	(MP z (2) a (3))

Tento krok můžeme použít samostatně, pokud $n = 1$. Pokud $n \geq 2$, musíme postupovat opatrněji. Nemůžeme pouze opakovaně použít uvedený krok, protože nic nebrání například výskytu proměnné x_2 v termu t_1. Potom by totiž formule $A_{x_1}[t_1]_{x_2}[t_2]$ byla různá od formule $A_{x_1,x_2}[t_1, t_2]$. Dosazování totiž probíhá najednou, a my bychom takto dostali formuli, která by vznikala postupně. Pokud bychom ale dokázali zaručit, že term t_1 neobsahuje proměnnou x_2, potom by skutečně $A_{x_1}[t_1]_{x_2}[t_2] = A_{x_1,x_2}[t_1, t_2]$.

Proto nechť $z_1, \ldots, z_n$ jsou proměnné, které se nevyskytují ani ve formuli A, ani v termech $t_1, \ldots, t_n$. Postupným opakováním pomocného kroku skutečně dokážeme:

$$\vdash A \quad \Rightarrow \quad \vdash \overbrace{A_{x_1,\ldots,x_n}[z_1, \ldots, z_n]}^{B}$$

V takto vzniklé formuli B se nevyskytují proměnné $x_1, \ldots, x_n$, takže můžeme totéž zopakovat, tentokrát již pro termy $t_1, \ldots, t_n$ (svou substituovatelnost určitě neztratily, protože jinak by nebyly substituovatelné již předtím):

$$\vdash A \quad \Rightarrow \quad \vdash \overbrace{B_{z_1,\ldots,z_n}[t_1, \ldots, t_n]}^{A_{x_1,\ldots,x_n}[t_1,\ldots,t_n]}$$

✡

Věta říká, že je-li formule dokazatelná, je dokazatelná každá její instance. Také z ní plyne, že volné proměnné mohou být libovolně přejmenovány.

9.11 Lemma (zobecnění axiomu specifikace a pravidla substituce). Pro libovolnou formuli A, proměnné $x_1, \ldots, x_n$ a termy $t_1, \ldots, t_n$ platí:

$$\begin{array}{ll} \text{(i)} & \vdash (\forall x_1) \ldots (\forall x_n) A \to A_{x_1,\ldots,x_n}[t_1, \ldots, t_n] \\ \text{(ii)} & \vdash A_{x_1,\ldots,x_n}[t_1, \ldots, t_n] \to (\exists x_1) \ldots (\exists x_n) A \end{array}$$

Důkaz. (i) Z axiomu specifikace dostaneme formule:

$$\begin{array}{lll} (1) & \vdash (\forall x_n) A \to A & \text{(AS)} \\ (2) & \vdash (\forall x_{n-1})(\forall x_n) A \to (\forall x_n) A & \text{(AS)} \\ \vdots & & \\ (3) & \vdash (\forall x_1) \ldots (\forall x_n) A \to (\forall x_2) \ldots (\forall x_n) A & \text{(AS)} \end{array}$$

Nyní použitím věty o skládání implikací dostaneme ze všech těchto formulí postupnou aplikací pravidla (MP) implikaci:

$$(4) \qquad \vdash (\forall x_1) \ldots (\forall x_n) A \to A \qquad \text{(SI, MP)}$$

Dokazovaná formule není již nic jiného než instance této formule (první část instanciace neovlivní, neboť jsou v ní všechny výskyty proměnných $x_1, \ldots, x_n$ vázané), její platnost tedy plyne z věty o instancích.

(ii) Dokážeme obdobně:

$$\begin{array}{lll} (1) & \vdash A \to (\exists x_n) A & \text{(PS)} \\ (2) & \vdash (\exists x_n) A \to (\exists x_{n-1})(\exists x_n) A & \text{(PS)} \\ \vdots & & \\ (3) & \vdash (\exists x_2) \ldots (\exists x_n) A \to (\exists x_1) \ldots (\exists x_n) A & \text{(PS)} \\ (4) & \vdash A \to (\exists x_1) \ldots (\exists x_n) A & \text{(SI, MP)} \\ (5) & \vdash A_{x_1,\ldots,x_n}[t_1, \ldots, t_n] \to (\exists x_1) \ldots (\exists x_n) A & \text{(instance)} \end{array}$$

✡

9.12 Důsledek (záměna kvantifikací). Nechť A je formule a π permutace na množině indexů $\{1, \ldots, n\}$. Potom:

$$\begin{array}{ll} \text{(i)} & \vdash (\forall x_1) \ldots (\forall x_n) A \leftrightarrow (\forall x_{\pi(1)}) \ldots (\forall x_{\pi(n)}) A \\ \text{(ii)} & \vdash (\exists x_1) \ldots (\exists x_n) A \leftrightarrow (\exists x_{\pi(1)}) \ldots (\exists x_{\pi(n)}) A \end{array}$$

Důkaz. (i) Z předchozího lemmatu plyne:

$$\vdash (\forall x_1) \ldots (\forall x_n) A \to A$$

Opakovaným použitím pravidla zavedení $\forall$ postupně na proměnné $x_{\pi(n)}, \dots x_{\pi(1)}$ dostaneme:

$$\vdash (\forall x_1) \dots (\forall x_n) A \to (\forall x_{\pi(1)}) \dots (\forall x_{\pi(n)}) A$$

Opačná implikace vznikne z této přejmenováním proměnných a použitím inverzní permutace.

(ii) Opět z předchozího lemmatu plyne:

$$\vdash A \to (\exists x_{\pi(1)}) \dots (\exists x_{\pi(n)}) A$$

Opakovaným použitím pravidla zavedení $\exists$ dostaneme:

$$\vdash (\exists x_1) \dots (\exists x_n) A \to (\exists x_{\pi(1)}) \dots (\exists x_{\pi(n)}) A$$

Opačná implikace vznikne podobně jako v (i). ☆

9.13 Definice. Nechť A je formule a $x_1, \dots, x_n$ jsou právě všechny volné proměnné formule A. Formuli $(\forall x_1) \dots (\forall x_n) A$ nazveme *uzávěr* formule A.

Podle této definice má proměnná s alespoň dvěma volnými proměnnými více různých uzávěrů, nicméně díky důsledku 9.12 jsou všechny tyto uzávěry navzájem ekvivalentní.

9.14 Věta o uzávěru. Je-li A' uzávěr formule A, potom platí:

$$\vdash A \quad \Leftrightarrow \quad \vdash A'$$

Důkaz. Nechť je A' tvaru $(\forall x_1) \dots (\forall x_n) A$.

$\Rightarrow$) A' odvodíme postupným použitím pravidla generalizace:

(1)	$\vdash A$	(předpoklad)
(2)	$\vdash (\forall x_n) A$	(PG)
$\vdots$		
(3)	$\vdash (\forall x_1) \dots (\forall x_n) A$	(PG)

$\Leftarrow$) Podle zobecněného pravidla substituce (lemma 9.11) je:

$$\vdash (\forall x_1) \dots (\forall x_n) A \to A$$

Formule A se odtud dokáže z předpokladu A' pravidlem (MP). ☆

Věta o uzávěru ukazuje, že volné proměnné mají ve formuli stejný význam, jako kdyby byly uzavřeny obecným kvantifikátorem. Skutečně: ze sémantického hlediska (viz definice 8.6) je formule považována za pravdivou, je-li splněna pro *všechna* ohodnocení proměnných.

9.15 Věta o ekvivalenci pro predikátovou logiku. Nechť formule A' vznikne z formule A nahrazením některých výskytů podformulí $A_1, A_2, \ldots, A_n$ po řadě formulemi $A'_1, A'_2, \ldots, A'_n$, kde pro $\forall i \in \{1, \ldots, n\}$ je $\vdash A_i \leftrightarrow A'_i$. Potom:

$$\vdash A \leftrightarrow A'$$

Důkaz. Indukcí podle složitosti formule A podobně jako ve výrokové logice:

- Formule A je nějaká z formulí A_i a její výskyt byl nahrazen, čili $A' = A'_i$. Ekvivalence $\vdash A \leftrightarrow A'$ potom plyne přímo z příslušného předpokladu $\vdash A_i \leftrightarrow A'_i$.
- Formule A je nenahrazená atomická formule. V tom případě je $A = A'$ a ekvivalence $\vdash A \leftrightarrow A'$ plyne z věty výrokové logiky $p \leftrightarrow p$.
- Formule A je nenahrazená formule tvaru $\neg B$, přičemž $\vdash B \leftrightarrow B'$ bylo již dokázáno. Potom $A' = \neg B'$.

  Formuli $A \leftrightarrow A'$ neboli $\neg B \leftrightarrow \neg B'$ dokážeme takto:

(1)	$\vdash B \to B'$	(předpoklad)
(2)	$\vdash \neg B' \to \neg B$	(V5, MP)

  Implikaci v opačném směru obdržíme stejně, pouze zaměníme čárkované a nečárkované symboly pro formule.
- Formule A je nenahrazená formule tvaru $B \to C$, přičemž $\vdash B \leftrightarrow B'$ a $\vdash C \leftrightarrow C'$ bylo již dokázáno. Potom $A' = B' \to C'$.

  První implikaci $A \to A'$ neboli $(B \to C) \to (B' \to C')$ dokážeme za použití výrokové logiky (věty o skládání implikací a věty o záměně předpokladů):

(1)	$\vdash (B' \to B) \to (B \to C) \to (C \to C') \to (B' \to C')$	(SI)
(2)	$\vdash (B' \to B) \to (C \to C') \to (B \to C) \to (B' \to C')$	(ZP, MP)

  Protože $B' \to B$ a $C \to C'$ jsou předpoklady, dostaneme $(B \to C) \to (B' \to C')$ dvojím použitím pravidla (MP). Opačná implikace a tedy i celková formule $A \leftrightarrow A'$ se dokáže naprosto stejně, viz předchozí bod.
- Formule A je nenahrazená formule tvaru $(\forall x)B$ nebo $(\exists x)B$, přičemž $\vdash B \leftrightarrow B'$ bylo již dokázáno. Potom A' je tvaru $(\forall x)B'$ nebo $(\exists x)B'$.

  Z obou předpokladů $B \to B'$ i $B' \to B$ přitom plyne $A \to A'$ i $A' \to A$ a tedy celkově $A \leftrightarrow A'$ z lemmatu o distribuci kvantifikátorů (lemma 9.9).

☆

9.16 Značení. V následujícím textu bude symbol Q označovat některý kvantifikátor, buď $\forall$, nebo $\exists$. Symbol $\bar{Q}$ bude označovat kvantifikátor opačný.

9.17 Definice. Říkáme, že formule A' je *variantou* formule A, jestliže A' vznikne z A postupným nahrazením podformulí tvaru $(Qx)B$ formulemi $(Qy)B_x[y]$, kde y není volná proměnná v podformuli $(Qx)B$.

9.18 Věta o variantách. Je-li A' varianta formule A, potom $\vdash A \leftrightarrow A'$.

Důkaz. Stačí dokázat $(Qx)B \leftrightarrow (Qy)B_x[y]$, dokazovaná věta pak vyplyne z definice varianty a věty o ekvivalenci. Předpokládejme navíc, že $x \neq y$. Kdyby totiž $x = y$, bylo by $(Qx)B = (Qy)B_x[y]$ a protože $p \leftrightarrow p$ je věta výrokové logiky, byl by důkaz hotov.

Označme $C = B_x[y]$. Potom $C_y[x] = B_x[y]_y[x] = B$. Uvědomme si, že pokud byla y substituovatelná do B za x... TODO

Pro $Q = \forall$ postupujeme takto:

(1)	$\vdash (\forall x)B \to B_x[y]$	(AS)
(2)	$\vdash (\forall x)B \to (\forall y)B_x[y]$	(Z$\forall$)
(3)	$\vdash (\forall y)C \to C_y[x]$	(AS)
(4)	$\vdash (\forall y)C \to (\forall x)C_y[x]$	(Z$\forall$)
(5)	$\vdash (\forall y)B_x[y] \to (\forall x)B$	(přepis)

A pro $Q = \exists$ velmi podobně:

(6)	$\vdash B_x[y] \to (\exists x)B$	(PS)
(7)	$\vdash (\exists y)B_x[y] \to (\exists x)B$	(Z$\exists$)
(8)	$\vdash C_y[x] \to (\exists y)C$	(PS)
(9)	$\vdash (\exists x)C_y[x] \to (\exists y)C$	(Z$\exists$)
(10)	$\vdash (\exists x)B \to (\exists y)B_x[y]$	(přepis)

Krok (2) lze provést, neboť y není v $(\forall x)B$ volná dle předpokladu, stejně tak krok (4), neboť všechny volné výskyty x jsme ve formuli $C = B_x[y]$ nahradili proměnnou y. Obdobně ospravedlníme i kroky (7) a (9). ☆

9.19 Věta o dedukci pro predikátovou logiku. Nechť T je množina formulí, A je *uzavřená* fromule a B libovolná formule. Potom:

$$T \vdash A \to B \quad \Leftrightarrow \quad T, A \vdash B$$

Důkaz. Je skoro stejný jako ve výrokové logice.

$\Rightarrow$) Mějme posloupnost formulí $(A_1, A_2, \ldots, A_{n-1}, A \to B)$, která je formálním důkazem formule $A \to B$ z předpokladů T. Posloupnost $(A_1, A_2, \ldots, A_{n-1}, A \to B, A, B)$ je pak formálním důkazem formule B z předpokladů T, A.

$\Leftarrow$) Nyní mějme posloupnot $(A_1, A_2, \ldots, A_n = B)$, která je formálním důkazem formule B z předpokladů T, A. Indukcí podle délky formálního důkazu

ukážeme, že pro $\forall i \in \{1, \ldots, n\}$ platí $T \vdash A \to A_i$. Tím budeme hotovi, neboť pro $i = n$ dostaneme $T \vdash A \to B$. Pro dané i uvážíme tentokrát čtyři případy:

- Formule A_i je formule A. Použijeme větu výrokové logiky $\vdash p \to p$ a přidáme předpoklady T.
- Formule A_i je axiom predikátové logiky nebo formule z množiny T. Potom posloupnost $(A_i, A_i \to (A \to A_i), A \to A_i)$ je formálním důkazem formule $A \to A_i$ z předpokladů T.
- Formule A_i je odvozena pravidlem *modus ponens* z formulí A_j, A_k pro nějaká $j, k < i$, kde A_j je formule tvaru $A_k \to A_i$. Podle indukčního předpokladu jsme tedy již dříve museli dokázat $T \vdash A \to (A_k \to A_i)$ a $T \vdash A \to A_k$. Vyjdeme z instance axiomu (A2):

  $$\vdash (A \to (A_k \to A_i)) \to [(A \to A_k) \to (A \to A_i)]$$

  a k získání důkazu $T \vdash A \to A_i$ použijeme dvakrát pravidlo (MP).

A nově:

- Formule A_i je odvozena pravidlem generalizace z formule A_j pro nějaké $j < i$, čili $A_i = (\forall x)A_j$. Již dříve jsme museli dokázat $T \vdash A \to A_j$. Protože předpokládáme, že A je uzavřená, není v ní žádná proměnná volná a můžeme použít pravidlo zavedení obecného kvantifikátoru:

(1)	$T \vdash A \to A_j$	(indukční předpoklad)
(2)	$T \vdash A \to (\forall x)A_j$	(Z$\forall$)
(3)	$T \vdash A \to A_i$	(přepis)

☆

9.20 Poznámka. Jak vidíme, předpoklad uzavřenosti formule A jsme použili jenom k tomu, abychom se ujistili, že v důkazu věty $T, A \vdash B$ nebylo použito pravidlo generalizace na žádnou proměnnou, která je v A volná. Tato okolnost by se však univerzálně formulovala i ověřovala poněkud obtížně. Navíc předpoklad využíváme pouze ve směru $\Leftarrow$, opačný směr můžeme používat bez tohoto omezení.

9.21 Důsledek (důkaz sporem v predikátové logice). Nechť A' je uzávěr formule A a T je množina formulí. Potom:

$$T \vdash A \quad \Leftrightarrow \quad T \cup \{\neg A'\} \text{ je sporná}$$

Důkaz. Je stejný jako ve výrokové logice, pouze si musíme uvědomit oprávněnost použití věty o dedukci.

⇒) Nechť B je libovolná formule a $T \vdash A$. Potom je podle věty o uzávěru i $T \vdash A'$. Dále postupujeme stejně jako ve výrokové logice:

(1)	$T \vdash A'$	(předpoklad)
(2)	$\vdash \neg A' \to (A' \to B)$	(V2)
(3)	$\vdash A' \to (\neg A' \to B)$	(ZP z (2))
(4)	$T \vdash \neg A' \to B$	(MP z (1) a (3))
(5)	$T, \neg A' \vdash B$	(VD)

⇐) Protože je $T \cup \{\neg A'\}$ sporná, můžeme z ní dokázat libovolnou formuli, třeba A. Proto:

(1)	$T, \neg A' \vdash A'$	
(2)	$T \vdash \neg A' \to A'$	(VD)
(3)	$\vdash (\neg A' \to A') \to A'$	(V7)
(4)	$T \vdash A'$	(MP z (2) a (3))

Odtud opět díky vetě o uzávěru $T \vdash A$. ☆

9.22 Věta o konstantách. Nechť T je množina formulí a A je formule jazyka L a $x_1, \ldots, x_n$ jsou proměnné. Dále nechť jazyk L' vznikne rozšířením jazyka L o nové symboly $c_1, \ldots, c_n$ pro konstanty (funkční symboly s nulovou aritou). Potom platí:

$$T \vdash A_{x_1,\ldots,x_n}[c_1, \ldots, c_n] \text{ v jazyce } L' \quad \Leftrightarrow \quad T \vdash A \text{ v jazyce } L$$

Důkaz.

⇐) Tato implikace plyne přímo z věty o instancích (věta 9.10).

⇒) Označme $A' = A_{x_1,\ldots,x_n}[c_1, \ldots, c_n]$. Mějme posloupnost $(A'_1, \ldots, A'_m)$, která je formálním důkazem formule A' z předpokladů T. Nechť $y_1, \ldots, y_n$ jsou nové proměnné, které se nevyskytují ani v žádné formuli důkazu, ani v A. Pokud by se nám podařilo dokázat formuli $A'' = A_{x_1,\ldots,x_n}[y_1, \ldots, y_n]$ z předpokladů T tak, že žádná formule důkazu nebude obsahovat žádnou konstantu c_i, máme důkaz formule A v jazyce L, neboť A je instancí A''.

Nechť pro $\forall i \in \{1, \ldots, m\}$ vznikne formule A_i z formule A'_i nahrazením každého výskytu konstanty c_i proměnnou y_i. Zřejmě $A_m = A''$ a navíc se nikde nevyskytuje žádná konstanta c_i. Posloupnost $(A_1, \ldots, A_m)$ je tedy hledaným důkazem formule A'' z předpokladů T, neboť vždy, když je formule A'_i instancí axiomu, prvek T nebo odvozena odvozovacími pravidly, je formule A_i instancí stejného axiomu, prvkem T nebo odvozena stejným pravidlem. ☆

9.23 Důsledek (věta o dedukci a konstanty). Chceme-li z $T, A \vdash B$ odvodit $T \vdash B$, stačí pro všechny volné proměnné $x_1, \ldots, x_n$ formule A zavést nové konstanty $c_1, \ldots, c_n$ a dokázat:

$$T, A_{x_1,\ldots,x_n}[c_1, \ldots, c_n] \vdash B_{x_1,\ldots,x_n}[c_1, \ldots, c_n]$$

Důkaz. Formule $A_{x_1,\dots,x_n}[c_1,\dots,c_n]$ je uzavřená a proto dostaneme z věty o dedukci

$$T \vdash A_{x_1,\dots,x_n}[c_1,\dots,c_n] \to B_{x_1,\dots,x_n}[c_1,\dots,c_n]$$

z čehož plyne $T \vdash A \to B$ pomocí věty o konstantách. ☆

10 Prenexní tvary formulí

Podobně jako jsme ve výrokové logice měli normální tvary formulí, i zde můžeme každou formuli převést do ekvivalentního tvaru, který splňuje určitá užitečná pravidla.

10.1 Definice. Řekneme, že formule A je v *prenexním tvaru*, pokud má tvar

$$(Q_1x_1)(Q_2x_2)\dots(Q_nx_n)B$$

kde B je otevřená formule a $x_1,\dots,x_n$ jsou navzájem různé proměnné.

Formule B se nazývá *otevřené jádro* a posloupnost kvantifikací před B se nazývá *prefix*.

10.2 Lemma (prenexní operace).

(i) $\vdash (\bar{Q}x)\neg B \leftrightarrow \neg(Qx)B$

(ii) $\vdash (Qx)(B \to C) \leftrightarrow (B \to (Qx)C)$, pokud x není volná v B

(iii) $\vdash (\bar{Q}x)(B \to C) \leftrightarrow ((Qx)B \to C)$, pokud x není volná v C

(iv) $\vdash (Qx)(B \,\&\, C) \leftrightarrow ((Qx)B \,\&\, C)$, pokud x není volná v C

(v) $\vdash (Qx)(B \vee C) \leftrightarrow ((Qx)B \vee C)$, pokud x není volná v C

Důkaz. (i) Pro $Q = \forall$ máme $\vdash B \leftrightarrow \neg\neg B$, proto podle věty o ekvivalenci je

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

což je přepis formule $(\exists x)\neg B \leftrightarrow \neg(\forall x)B$. Pro $Q = \exists$ dosadíme do $\vdash p \leftrightarrow \neg\neg p$ přímo:

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

To je přepis formule $(\forall x)\neg B \leftrightarrow \neg(\exists x)B$.

(ii) Nechť x není volná v B. Nejprve dokážeme formuli pro $Q = \forall$. Implikace

$$\vdash (\forall x)(B \to C) \to (B \to (\forall x)C)$$

je axiom přeskoku. Pro druhý směr použijeme větu o skládání implikací, záměně předpokladů, axiom specifikace a pravidlo zavedení $\forall$ (x není volná v B a tedy

ani v $B \to (\forall x)C$):

(1)	$\vdash (B \to (\forall x)C) \to ((\forall x)C \to C) \to (B \to C)$	(SI)
(2)	$\vdash ((\forall x)C \to C) \to (B \to (\forall x)C) \to (B \to C)$	(ZP, MP)
(3)	$\vdash ((\forall x)C \to C)$	(AS)
(4)	$\vdash (B \to (\forall x)C) \to (B \to C)$	(MP z (2) a (3))
(5)	$\vdash (B \to (\forall x)C) \to (\forall x)(B \to C)$	(Z$\forall$)

Pro $Q = \exists$ dokážeme dopřednou implikaci obdobně jako obrácenou pro $Q = \forall$:

(1)	$\vdash (B \to C) \to (C \to (\exists x)C) \to (B \to (\exists x)C)$	(SI)
(2)	$\vdash (C \to (\exists x)C) \to (B \to C) \to (B \to (\exists x)C)$	(ZP, MP)
(3)	$\vdash (C \to (\exists x)C)$	(PS)
(4)	$\vdash (B \to C) \to (B \to (\exists x)C)$	(MP z (2) a (3))
(5)	$\vdash (\exists x)(B \to C) \to (B \to (\exists x)C)$	(Z$\exists$)

Obrácená implikace bude složitější[5]. Nejprve ukážeme, že ve výrokové logice platí:

$$\vdash (\neg p \to r) \to (q \to r) \to (p \to q) \to r \tag{1}$$

Potom do této formule dosadíme postupně za výrokové proměnné p, q, r formule B, $(\exists x)C$, $(\exists x)(B \to C)$. Dostaneme tak:

$$\vdash (\neg B \to (\exists x)(B \to C)) \to ((\exists x)C \to (\exists x)(B \to C)) \to X \tag{2}$$

kde X je dokazovaná implikace. K jejímu důkazu bude tedy nutné dokázat formule

$$\vdash \neg B \to (\exists x)(B \to C) \tag{3}$$
$$\vdash (\exists x)C \to (\exists x)(B \to C) \tag{4}$$

neboť pak X vyplyne z (1) dvěma pravidly (MP).

K důkazu formule (1) ve výrokové logice vyjdeme z věty o skládání implikací (místo výrokových proměnných p, q, r používám symboly A, B, C, protože mi přijdou přehlednější):

(1)	$\vdash (\neg C \to A) \to (A \to B) \to (B \to C) \to (\neg C \to C)$	(SI)
(2)	$\neg A \to C \vdash (\neg C \to A)$	(V5', VD)
(3)	$\neg A \to C \vdash (A \to B) \to (B \to C) \to (\neg C \to C)$	(MP)

[5]Motivaci tohoto postupu lze nalézt ve slidech prof. Štěpánka, tamní postup se mi ale po formální stránce moc nezamlouvá. Je však velmi podobný, taktéž dojde na dílčí důkazy vět (3) a (4). Uvedený postup pochází ze skript prof. Štěpánka, až na důkaz formule (1), který je vlastní.

Dále máme:

$$\begin{array}{lll} (4) & \neg A \to C, A \to B, B \to C \vdash \neg C \to C & (2\times \text{ VD}) \\ (5) & \vdash (\neg C \to C) \to C & (\text{V7}) \\ (6) & \neg A \to C, A \to B, B \to C \vdash C & (\text{MP}) \end{array}$$

Použitím věty o dedukci dostaneme finální:

$$\vdash (\neg A \to C) \to (B \to C) \to (A \to B) \to C$$

Nyní konečně k důkazu formulí (3) a (4). Z věty o skládání implikací máme

$$\vdash [\neg B \to (B \to C)] \to [(B \to C) \to (\exists x)(B \to C)] \to [\neg B \to (\exists x)(B \to C)]$$

přičemž první hranatá závorka je instancí (V2) a druhá substitučního pravidla. Odtud plyne dvojím (MP) platnost formule (3). Formule (4) plyne z instance $C \to (B \to C)$ axiomu (A1) distribucí existenčního kvantifikátoru.

(iii) Bude se nám hodit věta výrokové logiky, která vznikne kombinací (A3) a (V5):

$$\vdash (p \to q) \leftrightarrow (\neg q \to \neg p) \tag{1}$$

Pro $Q = \forall$ postupujeme, zkráceně zapsáno, takto:

$$\begin{array}{lll} \vdash ((\forall x)B \to C) \leftrightarrow (\neg C \to \neg(\forall x)B) & & (\text{instance (1)}) \\ \leftrightarrow (\neg C \to \neg(\forall x)\neg\neg B) & & (\text{věta o ekvivalenci}) \\ \leftrightarrow (\neg C \to (\exists x)\neg B) & & (\text{zkratka za } \exists) \\ \leftrightarrow (\exists x)(\neg C \to \neg B) & & (\text{případ (ii) lemmatu}) \\ \leftrightarrow (\exists x)(B \to C) & & (\text{věta o ekvivalenci}) \end{array}$$

a pro $Q = \exists$ velmi podobně:

$$\begin{array}{lll} \vdash ((\exists x)B \to C) \leftrightarrow (\neg C \to \neg(\exists x)B) & & (\text{instance (1)}) \\ \leftrightarrow (\neg C \to \neg\neg(\forall x)\neg B) & & (\text{zkratka za } \exists) \\ \leftrightarrow (\neg C \to (\forall x)\neg B) & & (\text{věta o ekvivalenci}) \\ \leftrightarrow (\forall x)(\neg C \to \neg B) & & (\text{případ (ii) lemmatu}) \\ \leftrightarrow (\forall x)(B \to C) & & (\text{věta o ekvivalenci}) \end{array}$$

(iv) Pomocí již dokázaných případů, definice konjunkce a věty o ekvivalenci:

$$\begin{array}{lll} \vdash ((Qx)B \,\&\, C) \leftrightarrow \neg((Qx)B \to \neg C) & & (\text{zkratka za \&}) \\ \leftrightarrow \neg(\bar{Q}x)(B \to \neg C) & & (\text{případ (iii), VE}) \\ \leftrightarrow (Qx)\neg(B \to \neg C) & & (\text{případ (i)}) \\ \leftrightarrow (Qx)(B \,\&\, C) & & (\text{zkratka za \&}) \end{array}$$

(v) Obdobně jako (iv):

$$\begin{aligned}
\vdash ((Qx)B \vee C) &\leftrightarrow (\neg(Qx)B \to C) && \text{(zkratka za } \vee\text{)}\\
&\leftrightarrow ((\bar{Q}x)\neg B \to C) && \text{(případ (i), VE)}\\
&\leftrightarrow (Qx)(\neg B \to C) && \text{(případ (iii))}\\
&\leftrightarrow (Qx)(B \vee C) && \text{(zkratka za } \vee\text{)}
\end{aligned}$$

☆

10.3 Věta o prenexním tvaru. Ke každé formuli A lze sestrojit formuli A' v prenexním tvaru takovou, že $\vdash A \leftrightarrow A'$.

Důkaz. Indukcí podle složitosti formule A:

- Formule A je atomická formule. Potom je v prenexním tvaru sama o sobě.
- Formule A je tvaru $\neg B$, přičemž z indukčního předpokladu existuje prenexní formule B' ekvivalentní s B. Formuli A' obdržíme z formule $\neg B'$ postupnou aplikací operace (i) předchozího lemmatu na všechny kvantifikace v prefixu formule B':

  $$\vdash A \leftrightarrow \neg B \leftrightarrow \neg B' \leftrightarrow A'$$

  První ekvivalence plyne z rovnosti obou formulí, druhá z předpokladu a věty o ekvivalenci a třetí z předchozího lemmatu. Navíc je A' v prenexním tvaru.
- Formule A je tvaru $B \to C$, přičemž k B i C máme ekvivalentní formule B' a C' v prenexním tvaru. Z nich sestrojíme varianty B'' a C'' tak, aby žádná volná proměnná formule B'' nebyla vázaná ve formuli C'' a naopak. Potom z implikace $B'' \to C''$ sestrojíme formuli A' postupnou aplikací operace (ii) předchozího lemmatu na všechny kvantifikace v prefixu formule C'' a operace (iii) na všechny kvantifikace v prefixu formule B''. Formule A' pak bude v prenexním tvaru a navíc:

  $$\vdash A \leftrightarrow (B \to C) \leftrightarrow (B' \to C') \leftrightarrow (B'' \to C'') \leftrightarrow A'$$

  První ekvivalence plyne opět z rovnosti obou formulí, druhá z předpokladu a věty o ekvivalenci, třetí z věty o variantách a čtvrtá z předchozího lemmatu.
- Formule A je tvaru $(\forall x)B$, přičemž k B máme opět ekvivalentní formuli B' v prenexním tvaru. Položíme-li

  $$A' = \begin{cases} B' & \text{je-li } x \text{ v } B \text{ již vázaná,}\\ (\forall x)B' & \text{jinak,}\end{cases}$$

  pak jsme zřejmě hotovi.

☆

Ruční převod formule do prenexního tvaru spočívá v postupné aplikaci operací naznačených v lemmatu 10.2 a v případném přejmenování vázaných proměnných. Poněkud komplikovanějším případem je ekvivalence, kterou je nutné rozepsat na konjunkci implikací, což má za následek „zdvojení“ kvantifikátorů[6].

11 Predikátová logika s rovností

Chceme-li k jazyku prvního řádu přidat predikát pro rovnost, je vhodné pro něj zavést jisté axiomy, které by zaručily, že se bude chovat tak, jak to od rovnosti intuitivně očekáváme.

11.1 Definice. *Formální systém predikátové logiky s rovností* obsahuje vše, co obsahuje formální systém predikátové logiky bez rovnosti, a navíc tyto axiomy:

- Je-li x proměnná, je následující formule *axiomem identity*:

$$x = x \tag{R1}$$

- Jsou-li $x_1, \ldots, x_n$ a $y_1, \ldots, y_n$ proměnné a je-li f n-ární funkční symbol, potom je následující formule *axiomem rovnosti pro funkce*:

$$x_1 = y_1 \to x_2 = y_2 \to \ldots \to x_n = y_n \to f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n) \tag{R2}$$

- Jsou-li $x_1, \ldots, x_n$ a $y_1, \ldots, y_n$ proměnné a je-li p n-ární predikátový symbol, potom je následující formule *axiomem rovnosti pro predikáty*:

$$x_1 = y_1 \to x_2 = y_2 \to \ldots \to x_n = y_n \to p(x_1, \ldots, x_n) \to p(y_1, \ldots, y_n) \tag{R3}$$

Tyto axiomy vyjadčují přirozené požadavky, které matematika klade na rovnost: aby byla reflexivní a aby sobě rovná individua měla stejné vlastnosti vůči každému predikátu jazyka a dávala stejné výsledky při použití libovolné operace jazyka.

Protože rovnost běžně chápeme jako ekvivalenci, je přirozené po ní kromě reflexivity požadovat i další vlastnosti ekvivalence, které mezi uvedenými axiomy chybí: symetrii a tranzitivitu. Jak ale ukážeme, tyto vlastnosti se ze zavedených axiomů dají odvodit. Použijeme k tomu skutečnost, že rovnost je predikát a proto může v axiomu (R3) figurovat i na místě predikátu p.

11.2 Tvrzení (symetrie rovnosti). Pro libovolné proměnné x, y platí:

$$\vdash x = y \to y = x \tag{SR}$$

[6] Příklady viz skripta a slidy prof. Štěpánka.

Důkaz. Vyjdeme z axiomu rovnosti pro binární predikáty

$$\vdash x_1 = y_1 \to x_2 = y_2 \to p(x_1, x_2) \to p(y_1, y_2)$$

do kterého dosadíme za x_1, y_1, x_2, y_2 po řadě x, y, x, x a za predikát p dosadíme predikát rovnosti:

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

Nyní použijeme větu o záměně předpokladů a první předpoklad posuneme o dvě místa doprava:

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

Jak je vidět, první dva předpoklady jsou axiomem identity, proto dvojím (MP) dostaneme konečně:

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

☆

11.3 Tvrzení (tranzitivita rovnosti). Pro libovolné proměnné x, y, z platí:

$$\vdash x = y \to y = z \to x = z \tag{TR}$$

Důkaz. Je podobný. Opět vyjdeme z axiomu rovnosti pro binární predikáty

$$\vdash x_1 = y_1 \to x_2 = y_2 \to p(x_1, x_2) \to p(y_1, y_2)$$

do kterého tentokrát dosadíme za x_1, y_1, x_2, y_2 po řadě x, x, y, z a za predikát p opět predikát rovnosti:

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

Nyní opět použijeme větu o záměně předpokladů, tentokrát prohodíme druhý a třetí předpoklad:

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

První předpoklad je opět axiomem identity, proto pravidlem (MP) dostaneme:

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

☆

11.4 Poznámka. Uvědomme si, že ačkoliv všechny tři axiomy pro rovnost i předchozí dvě tvrzení hovoří pouze o proměnných, není problém nahradit slovo „proměnná“ slovem „term“. Můžeme totiž vyjít z dané formule s proměnnými a vytvořit instanci této formule, kde nahradíme proměnné příslušnými termy. Z věty o instancích potom plyne platnost takto upravené formule.

Nyní uvedeme větu, která je obdobou věty o ekvivalenci.

11.5 Věta o rovnosti. Nechť $t_1, \ldots, t_n$ a $s_1, \ldots, s_n$ jsou termy takové, že pro $\forall i \in \{1, \ldots, n\}$ platí $\vdash t_i = s_i$.

(i) Je-li t term a s term, který vznikne z t záměnou některých výskytů termů t_i odpovídajícími termy s_i, potom:

$$\vdash t = s$$

(ii) Je-li A formule a A' formule, která vznikne z A záměnou některých výskytů termů t_i odpovídajícími termy s_i[7], potom:

$$\vdash A \leftrightarrow A'$$

Důkaz. (i) Indukcí podle složitosti termu t:

- Je-li t zaměněný term t_i, potom s je s_i a rovnost $\vdash t = s$ plyne ihned z předpokladu $\vdash t_i = s_i$.
- Je-li t nezaměněná proměnná, potom s je t a rovnost $\vdash t = s$ plyne ihned z axiomu identity.
- Je-li t nezaměněná funkce $f(r_1, \ldots, r_k)$, potom s je $f(r'_1, \ldots, r'_k)$, přičemž z indukčního předpokladu máme $\vdash r_i = r'_i$ pro $\forall i \in \{1, \ldots, k\}$. Vyjdeme z axiomu rovnosti pro funkce:

  $$\vdash r_1 = r'_1 \to \ldots \to r_k = r'_k \to f(r_1, \ldots, r_k) = f(r'_1, \ldots, r'_k)$$

  Formule $\vdash f(r_1, \ldots, r_k) = f(r'_1, \ldots, r'_k)$ neboli $\vdash t = s$ zbude po k-násobné aplikaci pravidla (MP) na indukční předpoklad.

(ii) Protože se termy vyskytují pouze v atomických formulích, stačí, když dokážeme, že všechny atomické podformule formule A tvaru $p(r_1, \ldots, r_k)$ jsou ekvivalentní svým transformovaným variantám $p(r'_1, \ldots, r'_k)$. Tvrzení věty potom vyplyne z věty o ekvivalenci.

Z části (i) této věty víme, že pro $\forall i \in \{1, \ldots, k\}$ je $\vdash r_i = r'_i$. Použijeme-li axiom rovnosti pro predikáty

$$\vdash r_1 = r'_1 \to \ldots \to r_k = r'_k \to p(r_1, \ldots, r_k) \to p(r'_1, \ldots, r'_k) \tag{1}$$

dostaneme implikaci $p(r_1, \ldots, r_k) \to p(r'_1, \ldots, r'_k)$ použitím k pravidel (MP).

Opačnou implikaci odvodíme podobně. Ve formuli (1) nejprve prohodíme čárkované a nečárkované symboly pro termy. Protože použitím symetrie rovnosti (tvrzení 11.2) a pravidla (MP) snadno dojdeme od věty $\vdash r_i = r'_i$ k větě $\vdash r'_i = r_i$, dostaneme opačnou implikaci opět k-násobným (MP). ☆

Následující důsledek je pouze jinou formou věty o rovnosti.

[7] Zde prof. Štěpánek dodává: „kromě případů, kdy je term t_i proměnná x, která je součástí kvantifikace (Qx)“. To však nepovažuji za nutné, neboť ono „x“ v kvantifikaci neznačí *term*, ale *kvantifikovanou proměnnou* a té se záměna *termů* netýká.

11.6 Důsledek. Jsou-li $t_1, \ldots, t_n, s_1, \ldots, s_n$ termy, term s vznikne z termu t záměnou některých výskytů termů t_i odpovídajícími termy s_i a formule A' vznikne z formule A taktéž záměnou některých výskytů termů t_i odpovídajícími termy s_i, potom platí:

(i) $\vdash t_1 = s_1 \to \ldots \to t_n = s_n \to t = s$

(ii) $\vdash t_1 = s_1 \to \ldots \to t_n = s_n \to (A \leftrightarrow A')$

Důkaz. TODO! ☆

11.7 Tvrzení. Nechť A je formule, t term a x proměnná neobsažená v termu t. Potom:

(i) $\vdash A_x[t] \leftrightarrow (\forall x)(x = t \to A)$

(ii) $\vdash A_x[t] \leftrightarrow (\exists x)(x = t \,\&\, A)$

Důkaz. (i)

(1)	$\vdash (\forall x)(x = t \to A) \to (t = t \to A_x[t])$	(AS)
(2)	$\vdash t = t \to (\forall x)(x = t \to A) \to A_x[t]$	(ZI, MP)
(3)	$\vdash (\forall x)(x = t \to A) \to A_x[t]$	(R1, MP)

TODO! ☆

12 Úplnost predikátové logiky

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

Formulím z množiny T říkáme *speciální axiomy* teorie T.

12.2 Definice. Nechť T je teorie s jazykem L a $\mathbb{M}$ je interpretace jazyka L.

- $\mathbb{M}$ je *modelem* teorie T (psáno $\mathbb{M} \vDash T$), je-li v $\mathbb{M}$ pravdivý každý speciální axiom teorie T.
- Formule A je *sémantickým důsledkem* teorie T (psáno $T \vDash A$), je-li A pravdivá v každém modelu teorie T.

12.3 Lemma (korektnost axiomů predikátové logiky). Všechny axiomy predikátové logiky jsou validní formule.

Důkaz. Nechť $\mathbb{M}$ je libovolná interpretace a e ohodnocení proměnných. Rozebereme všechny axiomy A predikátové logiky s rovností a u každého ukážeme $\mathbb{M} \vDash A[e]$. Tím podle definice dokážeme, že A je validní formule.

- A je axiom výrokové logiky. Nechť A' je formule výrokové logiky, která má stejnou strukturu jako A a výrokové proměnné $p_1, \ldots, p_n$ v ní zastupují podformule $A_1, \ldots, A_n$ tak, že dosazením všech A_i za p_i dostaneme původní formuli A.

  Protože A' je tautologie, na splněnosti jednotlivých $A_1, \ldots, A_n$ při $\mathbb{M}$ a e nezáleží a $\mathbb{M} \models A[e]$ platí vždy.

- A je axiom specifikace tvaru $(\forall x)B \to B_x[t]$. Není-li předpoklad $(\forall x)B$ při $\mathbb{M}$ a e splněn, je implikace splněna.

  Nechť tedy platí $\mathbb{M} \models (\forall x)B[e]$. Podle definice pravdivosti to znamená, že pro každé individuum $m \in \mathbb{M}$ je $\mathbb{M} \models B[e(x/m)]$, speciálně tedy i pro $m = t[e]$. Díky lemmatu 8.12 (ii) je tedy $\mathbb{M} \models B_x[t][e]$ a implikace je splněna.

- A je axiom přeskoku tvaru $(\forall x)(B \to C) \to (B \to (\forall x)C)$. Opět zkoumejme případ, kdy je předpoklad $(\forall x)(B \to C)$ při $\mathbb{M}$ a e splněn. Podle definice pravdivosti potom máme pro libovolné individuum $m \in \mathbb{M}$:

  $$\mathbb{M} \models (B \to C)[e(x/m)]$$

  To znamená, že při ohodnocení $e(x/m)$ buď není splněna B, nebo je splněna C.

  Protože B neobsahuje proměnnou x volně, je $\mathbb{M} \models B[e(x/m)]$, právě když $\mathbb{M} \models B[e]$. To znamená, že B je buď vždy splněna, nebo ne, nezávisle na m. Pokud tedy B není při $e(x/m)$ splněna, není splněna ani při e a v implikaci $B \to (\forall x)C$ není splněn předpoklad. Implikace tedy splněna je, stejně jako celá formule A.

  Pokud naopak B je při $e(x/m)$ splněna, je splněna pro jakékoliv m a proto musí být pro jakékoliv m při $e(x/m)$ splněna i formule C. Je tedy $\mathbb{M} \models C[e(x/m)]$ pro libovolné $m \in \mathbb{M}$ a to podle definice znamená $\mathbb{M} \models (\forall x)C[e]$. Proto je v implikaci $B \to (\forall x)C$ při $\mathbb{M}$ a e splněno tvrzení, a tedy implikace samotná, a tedy celá formule A.

Ještě zbývá rozebrat axiomy pro rovnost. Uvědomme si, že binární predikát rovnosti je v každé interpretaci $\mathbb{M}$ realizován pro $\forall m_1, m_2 \in \mathbb{M}$ jako

$$(m_1, m_2) \in =_{\mathbb{M}} \quad \Leftrightarrow \quad m_1 = m_2$$

čili sobě rovná jsou právě identická individua.

- A je axiom identity tvaru $x = x$ pro proměnnou x. Při ohodnocení e je proměnná x realizována individuem $m = e(x)$, platí $m = m$ a formule A je splněna.

- A je axiom rovnosti pro funkce tvaru

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

kde $x_1, \ldots, x_n$ a $y_1, \ldots, y_n$ jsou proměnné a f je n-ární funkční symbol daného jazyka. Opět rozebereme pouze případ, kdy jsou splněny všechny předpoklady, jinak je totiž A splněna.

Nechť tedy v daném ohodnocení platí $x_i = y_i$ pro $\forall i \in \{1, \ldots, n\}$. To znamená, že je $e(x_i) = e(y_i)$. Proto

$$f(x_1, \ldots, x_n)[e] = f_{\mathbb{M}}(e(x_1), \ldots, e(x_n)) = \\ = f_{\mathbb{M}}(e(y_1), \ldots, e(y_n)) = f(y_1, \ldots, y_n)[e]$$

a skutečně tedy platí $\mathbb{M} \vDash (f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n))[e]$.

- A je axiom rovnosti pro predikáty tvaru

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

kde $x_1, \ldots, x_n$ a $y_1, \ldots, y_n$ jsou proměnné a p je n-ární predikátový symbol daného jazyka. Postupujeme obdobně. Opět rozebereme pouze případ, kdy jsou splněny všechny předpoklady (a tedy opět $e(x_i) = e(y_i)$ pro $\forall i \in \{1, \ldots, n\}$), navíc i predikát $p(x_1, \ldots, x_n)$:

$$\mathbb{M} \vDash p(x_1, \ldots, x_n)[e] \Rightarrow (e(x_1), \ldots, e(x_n)) \in p_{\mathbb{M}} \\ \Rightarrow (e(y_1), \ldots, e(y_n)) \in p_{\mathbb{M}} \\ \Rightarrow \mathbb{M} \vDash p(y_1, \ldots, y_n)[e]$$

☆

12.4 Lemma (korektnost odvozovacích pravidel predikátové logiky). Mějme interpretaci $\mathbb{M}$.

(i) Je-li formule B odvozena z formulí A a $A \to B$ pravidlem *modus ponens*, potom:

$$\mathbb{M} \vDash A \quad \text{a} \quad \mathbb{M} \vDash (A \to B) \qquad \Rightarrow \qquad \mathbb{M} \vDash B$$

(ii) Je-li formule $(\forall x)A$ odvozena z formule A pravidlem generalizace, potom:

$$\mathbb{M} \vDash A \quad \Rightarrow \quad \mathbb{M} \vDash (\forall x)A$$

Důkaz. (i) Plyne přímo z definice významu implikace. Mějme libovolné ohodnocení e. Pokud by platilo $\mathbb{M} \vDash A[e]$ a přitom neplatilo $\mathbb{M} \vDash B[e]$, nemohlo by ani platit $\mathbb{M} \vDash (A \to B)[e]$ a měli bychom spor, neboť dle předpokladů platí $\mathbb{M} \vDash A[e]$ a $\mathbb{M} \vDash (A \to B)[e]$ při každém ohodnocení. Proto při každém ohodnocení platí i $\mathbb{M} \vDash B[e]$ a je tedy $\mathbb{M} \vDash B$.

(ii) Předpoklad $\mathbb{M} \vDash A$ znamená, že $\mathbb{M} \vDash A[e]$ platí při každém ohodnocení e. Pro libovolné individuum $m \in \mathbb{M}$ a ohodnocení e je tedy $\mathbb{M} \vDash A[e(x/m)]$, což dle definice znamená $\mathbb{M} \vDash (\forall x)A[e]$. Dokázali jsme tedy $\mathbb{M} \vDash (\forall x)A$. ☆

12.5 Věta o korektnosti. Je-li T teorie s jazykem L a A formule jazyka L, potom:

$$T \vdash A \quad \Rightarrow \quad T \vDash A$$

neboli každá věta teorie T (každá formule dokazatelná z předpokladů T) je pravdivá ve všech modelech (je sémantickým důsledkem teorie T). Speciálně pro $T = \varnothing$ dostaneme

$$\vdash A \quad \Rightarrow \quad \vDash A$$

neboli každá věta predikátové logiky je logicky validní.

Důkaz. Indukcí podle délky formálního důkazu formule A z předpokladů T. Mějme posloupnost $(A_1, \ldots, A_n)$, která je formálním důkazem $T \vdash A$. Pro $\forall i \in \{1, \ldots, n\}$ postupně dokážeme $T \vDash A_i$. Tím budeme hotovi, neboť pro $i = n$ dostaneme $T \vDash A$.

Mějme $i \in \{1, \ldots, n\}$. Pokud pro libovolný model $\mathbb{M}$ teorie T dokážeme $\mathbb{M} \vDash A_i$, budeme mít $T \vDash A_i$. Nechť je tedy $\mathbb{M}$ libovolný model teorie T. Rozebereme všechny úlohy, které může formule A_i v důkazu mít:

- Formule A_i je axiomem predikátové logiky. A_i je potom podle lemmatu 12.3 validí formule a proto $\mathbb{M} \vDash A_i$.
- Formule A_i je speciálním axiomem teorie T. Potom $\mathbb{M} \vDash A_i$, neboť $\mathbb{M} \vDash T$ dle předpokladu a $A_i \in T$.
- Formule A_i je odvozena z formulí A_j a A_k $(j, k < i)$ pravidlem *modus ponens*, přičemž z indukčního předpokladu máme $\mathbb{M} \vDash A_j$ a $\mathbb{M} \vDash A_k$. Odtud díky lemmatu 12.4 (i) také $\mathbb{M} \vDash A_i$.
- Formule A_i je odvozena z formule A_j $(j < i)$ pravidlem generalizace. Opět máme $\mathbb{M} \vDash A_j$ a díky lemmatu 12.4 (ii) také $\mathbb{M} \vDash A_i$.

☆

12.6 Definice. Nechť T je teorie nad jazykem L. Řekneme, že struktura $\mathbb{M}$ je *kanonický model* teorie T, pokud:

- Universum $\mathbb{M}$ tvoří právě všechny termy jazyka L bez proměnných.
- Je-li $t_1, \ldots, t_n \in \mathbb{M}$ a f je n-ární funkční symbol jazyka L, je jeho realizace $f_{\mathbb{M}}$ definována jako:

$$f_{\mathbb{M}}(t_1, \ldots, t_n) = f(t_1, \ldots, t_n) \in \mathbb{M}$$

- Je-li $t_1, \ldots, t_n \in \mathbb{M}$ a p je n-ární predikátový symbol jazyka L, je jeho realizace $p_{\mathbb{M}}$ definována jako:

$$(t_1, \ldots, t_n) \in p_{\mathbb{M}} \quad \Leftrightarrow \quad T \vdash p(t_1, \ldots, t_n)$$

12.7 Poznámka. S uvedenou definicí kanonického modelu $\mathbb{M}$ je řada nesnází:

1) Je-li L jazyk s rovností, může se stát, že dva různé termy t, s bez proměnných splňují $T \vdash t = s$. V interpretaci $\mathbb{M}$ ale nebude tato rovnost splněna, neboť t a s jsou různá individua.

2) Je-li A uzavřená formule, musí být při interpretaci $\mathbb{M}$ pravdivá jedna z formulí A nebo $\neg A$. Žádná z nich přitom nemusí být větou teorie T.

3) Neobsahuje-li jazyk L žádné konstanty, potom neexistují žádné termy bez proměnných a universum $\mathbb{M}$ je prázdné. $\mathbb{M}$ tedy není podle definice interpretací jazyka L.

4) Je-li formule tvaru $(\exists x)A$ větou teorie T, nemusí být pravdivá v interpretaci $\mathbb{M}$. Nemusíme totiž najít individuum (term bez proměnných) t, který by pravdivost formule „dosvědčilo“ (kdybychom takové individuum t nalezli, znamenalo by to, že i formule $B_x[t]$ je větou teorie T).

Nesnáz 1 vyřešíme tak, že budeme považovat všechna individua t, s splňující $T \vdash t = s$ za identická. Zavedeme ekvivalenci $\sim$ na univerzu $\mathbb{M}$, kterou definujeme takto:

$$t \sim s \quad \Leftrightarrow \quad T \vdash t = s \tag{1}$$

Neboť jsme o predikátu rovnosti dokázali, že je reflexivní, symetrický a tranzitivní, je takto definovaná relace skutečně ekvivalencí.

Místo celého univerza $\mathbb{M}$ budeme uvažovat jeho třídy ekvivalence $\mathbb{M}/\sim$. Je-li t individuum, budeme zápisem $[t]$ rozumět takovou třídu, do které individuum t „padne“:

$$[t] = \{s \in \mathbb{M} \mid t \sim s\}$$

Funkční symboly potom realizujeme jako

$$f_{\mathbb{M}}([t_1], \ldots, [t_n]) = [f(t_1, \ldots, t_n)]$$

a predikátové jako:

$$([t_1], \ldots, [t_n]) \in p_{\mathbb{M}} \quad \Leftrightarrow \quad T \vdash p(t_1, \ldots, t_n)$$

Zbývá ukázat, že taková definice realizace je korektní, tedy že platí-li pro nějaké $n \in \mathbb{N}$ identity $[t_1] = [s_1], \ldots, [t_n] = [s_n]$, máme pro n-ární funkční symbol f

$$[f(t_1, \ldots, t_n)] = [f(s_1, \ldots, s_n)] \tag{2}$$

a pro n-ární predikátový symbol p:

$$T \vdash p(t_1, \ldots, t_n) \quad \Leftrightarrow \quad T \vdash p(s_1, \ldots, s_n) \tag{3}$$

Z $[t_i] = [s_i]$ plyne $t_i \sim s_i$ a tedy podle definice (1) $T \vdash t_i = s_i$. Uvážíme-li ale axiom rovnosti pro funkce

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

vyplyne nám $T \vdash f(t_1, \ldots, t_n) = f(s_1, \ldots, s_n)$, což opět dle definice (1) znamená $f(t_1, \ldots, t_n) \sim f(s_1, \ldots, s_n)$, z čehož plyne (2).

Podobným způsobem plyne z axiomu rovnosti pro predikáty (a pro obrácenou implikaci navíc ze symetrie rovnosti)

$$T \vdash p(t_1, \ldots, t_n) \leftrightarrow p(s_1, \ldots, s_n)$$

odkud snadno dostaneme (3).

12.8 Lemma. Nechť $x_1, \ldots, x_n$ jsou právě všechny proměnné termu t, případně právě všechny volné proměnné formule A, a mějme ohodnocení e takové, že $e(x_i) = [t_i]$ pro $\forall i \in \{1, \ldots, n\}$ a nějaké termy bez proměnných $t_1, \ldots, t_n$. Potom platí:

$$\begin{array}{lrcl} \text{(i)} & t[e] & = & [t_{x_1,\ldots,x_n}[t_1, \ldots, t_n]] \\ \text{(ii)} & \mathbb{M} \vDash A[e] & \Leftrightarrow & \mathbb{M} \vDash A_{x_1,\ldots,x_n}[t_1, \ldots, t_n] \end{array}$$

Důkaz. TODO Revize! Platí-li $e(x_i) = [t_i]$ pro $\forall i \in \{1, \ldots, n\}$, je jistě:

$$e = e(x_1/[t_1], \ldots, x_n/[t_n]) \tag{1}$$

Odtud dostáváme:

$$\begin{aligned} t[e] &= t[e(x_1/[t_1], \ldots, x_n/[t_n]] && (2) \\ &= t_{x_1,\ldots,x_n}[t_1, \ldots, t_n][e] && (3) \\ &= [t_{x_1,\ldots,x_n}[t_1, \ldots, t_n]] && (4) \end{aligned}$$

$$\begin{aligned} \mathbb{M} \vDash A[e] &\Leftrightarrow \mathbb{M} \vDash A[e(x_1/[t_1], \ldots, x_n/[t_n])] && (5) \\ &\Leftrightarrow \mathbb{M} \vDash A_{x_1,\ldots,x_n}[t_1, \ldots, t_n][e] && (6) \\ &\Leftrightarrow \mathbb{M} \vDash A_{x_1,\ldots,x_n}[t_1, \ldots, t_n] && (7) \end{aligned}$$

První ekvivalence (2) a (5) plynou z rovnosti (1), druhé (3) a (6) z lemmatu 8.12 (kde máme $m_i = t_i[e] = [t_i]$) a třetí (4) a (7) z toho faktu, že všechny proměnné termu t, případně volné proměnné formule A nahradili termy bez proměnných a proto nezáleží na ohodnocení e. ☆

12.9 Tvrzení. Nechť $\mathbb{M}$ je kanonický model teorie T nad jazykem L. Potom pro každou *atomickou* formuli A *bez proměnných* platí:

$$\mathbb{M} \vDash A \quad \Leftrightarrow \quad T \vdash A$$

Důkaz. Nechť A je tvaru $p(t_1, \ldots, t_n)$. Je-li t_i term bez proměnných, potom pro libovolné ohodnocení e je $t_i[e] = [t_i]$. Máme:

$$\begin{aligned} \mathbb{M} \vDash A &\Leftrightarrow \mathbb{M} \vDash A[e] \text{ pro všechna ohodnocení } e \\ &\Leftrightarrow (t_1[e], \ldots, t_n[e]) \in p_{\mathbb{M}} \text{ pro všechna ohodnocení } e \\ &\Leftrightarrow ([t_1], \ldots, [t_n]) \in p_{\mathbb{M}} \\ &\Leftrightarrow T \vdash p(t_1, \ldots, t_n) \\ &\Leftrightarrow T \vdash A \end{aligned}$$

☆

12.10 Definice. Nechť T je teorie s jazykem L.

- T je *úplná* teorie, je-li bezesporná a pro libovolnou uzavřenou formuli A jazyka L je právě jedna z formulí A a $\neg A$ dokazatelná v T.
- T je *Henkinova* teorie, jestliže pro libovolnou uzavřenou formuli tvaru $(\exists x)A$ existuje konstanta c taková, že platí:

$$T \vdash (\exists x)A \to A_x[c]$$

Uvědomme si, že je-li teorie úplná a Henkinova, potom odpadá nesnáz 2 (díky úplnosti) i nesnáze 3 a 4 (díky Henkinově vlastnosti).

12.11 Věta o kanonickém modelu. Je-li T *úplná Henkinova* teorie nad jazykem L, potom je kanonický model teorie T skutečně modelem teorie T.

Důkaz. Napřed dokážeme, že pro každou *uzavřenou* formuli A redukovaného jazyka L platí

$$\mathbb{M} \vDash A \quad \Leftrightarrow \quad T \vdash A \tag{1}$$

a to indukcí podle složitosti formule A:

- Je-li A atomická formule, plyne (1) z tvrzení 12.9.
- Je-li A tvaru $\neg B$, kde B je taktéž uzavřená formule. Potom:

$$\begin{aligned} \mathbb{M} \vDash A &\Leftrightarrow \mathbb{M} \nvDash B && \text{(význam negace)} \\ &\Leftrightarrow T \nvdash B && \text{(indukční předpoklad)} \\ &\Leftrightarrow T \vdash \neg B && (T \text{ je úplná}) \\ &\Leftrightarrow T \vdash A \end{aligned}$$

- Je-li A tvaru $B \to C$, kde B a C jsou taktéž uzavřené formule. Potom:

$$\begin{aligned} \mathbb{M} \vDash A &\Leftrightarrow \mathbb{M} \nvDash B \text{ nebo } \mathbb{M} \vDash C && \text{(význam implikace)} \\ &\Leftrightarrow T \nvdash B \text{ nebo } T \vdash C && \text{(indukční předpoklad)} \\ &\Leftrightarrow T \vdash \neg B \text{ nebo } T \vdash C && (T \text{ je úplná}) \\ &\Leftrightarrow T \vdash B \to C && \text{(viz níže)} \\ &\Leftrightarrow T \vdash A \end{aligned}$$

  Předposlední ekvivalence si zaslouží vysvětlení. Ve výrokové logice máme věty

$$\begin{aligned} &\vdash \neg B \to (B \to C) && \text{(V2)} \\ &\vdash C \to (B \to C) && \text{(A1)} \end{aligned}$$

ze kterých lze platnost $T \vdash B \to C$ odvodit snadno z platností alespoň jedné z vět $T \vdash B$ nebo $T \vdash C$ pravidlem (MP). Kdyby naopak $T \vdash B \to C$, musela by díky úplnosti T a uzavřenosti B platit buď $T \vdash B$, nebo $T \vdash \neg B$. V prvním případě by se pavidlem (MP) odvodilo $T \vdash C$, druhý vyhovuje. Srovnej s důkazem lemmatu 4.8.

- Je-li A tvaru $(\forall x)B$, potom:

$$\begin{aligned}
\mathbb{M} \vDash A &\Leftrightarrow \mathbb{M} \vDash (\forall x)B[e] \text{ pro libovolné ohodnocení } e && (1)\\
&\Leftrightarrow \mathbb{M} \vDash B[e(x/[t])] \text{ pro libovolné } e \text{ a term bez proměnných } t && (2)\\
&\Leftrightarrow \mathbb{M} \vDash B_x[t] \text{ pro libovolný term bez proměnných } t && (3)\\
&\Leftrightarrow T \vdash B_x[t] \text{ pro libovolný term bez proměnných } t && (4)\\
&\Leftrightarrow T \vdash A && (5)
\end{aligned}$$

Ekvivalence (1) a (2) plynou z definic, (4) z indukčního předpokladu, neboť formule $B_x[t]$ je uzavřená (formule A uzavřená byla a B obsahuje jedinou volnou proměnnou, x, kterou jsme nahradili termem bez proměnných, t). Ekvivalence (3) plyne z lemmatu 12.8 (ii).

Poslední ekvivalence (5) je složitější. Směr „zdola nahoru“ je instancí axiomu specifikace. Pro opačný směr nechť platí pro libovolný term bez proměnných t věta $T \vdash B_x[t]$. To, že potom musí platit $T \vdash (\forall x)B$ neboli $T \vdash A$ dokážeme sporem:

$$\begin{aligned}
&T \nvdash (\forall x)B && \text{(pro spor)}\\
&T \vdash \neg(\forall x)B && (\text{úplnost } T)\\
&T \vdash \neg(\forall x)\neg\neg B && \text{(VE)}\\
&T \vdash (\exists x)\neg B && \text{(přepis)}\\
&T \vdash (\exists x)\neg B \to \neg B_x[c] \text{ pro nějakou konstantu } c && (\text{Henkinova } T)\\
&T \vdash \neg B_x[c] \text{ pro nějakou konstantu } c && \text{(MP)}\\
&T \nvdash B_x[c] \text{ pro nějakou konstantu } c && (\text{úplnost } T)
\end{aligned}$$

Jak vidíme, došli jsme ke sporu, neboť předpokládáme $T \vdash B_x[t]$ pro libovolný term bez proměnných t, tedy i pro danou konstantu c. Proto musí platit $T \vdash (\forall x)B$ neboli $T \vdash A$.

Nyní již k důkazu samotné věty. Mějme libovolný speciální axiom A teorie T a jeho uzávěr A'. Podle věty o uzávěru je i A' větou teorie T, proto je podle první části důkazu A' při $\mathbb{M}$ pravdivá. A protože je A' uzávěr A, je při $\mathbb{M}$ pravdivá i formule A (viz definice pravdivosti). ☆

12.12 Definice. Nechť T je teorie s jazykem L a T' teorie s jazykem L'.

- Jazyk L' je *rozšířením* jazyka L, je-li každý n-ární speciální symbol (případně i predikát rovnosti) jazyka L také n-árním symbolem jazyka L'.

- Teorie T' je *rozšířením* teorie T, je-li jazyk L' rozšířením jazyka L a každý speciální axiom teorie T je větou teorie T'.
- Teorie T' je *konzervativním rozšířením* teorie T, je-li T' rozšířením T a navíc pro každou formuli A jazyka L platí:

$$T' \vdash A \quad \Rightarrow \quad T \vdash A$$

12.13 Pozorování (ekvivalentní definice rozšíření teorie). Teorie T' je rozšíření teorie T s jazykem L, právě když pro každou formuli A jazyka L platí:

$$T \vdash A \quad \Rightarrow \quad T' \vdash A$$

Důkaz.

$\Rightarrow$) Dle definice rozšiřování teorií je každý speciální axiom teorie T dokazatelný v teorii T', zkombinujme proto jejich formální důkazy do jedné veliké posloupnosti formulí P. Dále uvažme posloupnost formulí Q, která vznikne z formálního důkazu $T \vdash A$ vypuštěním všech formulí, které patří do T.

Není těžké si uvědomit, že zřetězením posloupností P a Q vznikne formální důkaz $T' \vdash A$, neboť vždy, když v důkazu $T \vdash A$ použijeme odvozovací pravidlo na nějakou formuli z T, je tato formule, i když jsme ji v Q odstranili, součástí posloupnosti P.

$\Leftarrow$) Pro každý speciální axiom $A \in T$ je zřejmě $T \vdash A$ a tedy díky předpokladu i $T' \vdash A$. Teorie T' je tedy rozšířením T dle definice. ☆

12.14 Důsledek (ekvivalentní definice konzervativního rozšíření teorie). Teorie T' je konzervativní rozšíření teorie T s jazykem L, právě když pro každou formuli A jazyka L platí:

$$T \vdash A \quad \Leftrightarrow \quad T' \vdash A$$

Důkaz. Zřejmé. ☆

Čili je-li T' s jazykem L' rozšířením teorie T s jazykem L, pak každá věta, kterou lze dokázat v teorii T, je dokazatelná i v teorii T'. Konzervativní rozšíření teorie je takové rozšíření, ve kterém neplatí oproti původní teorii žádné věty jazyka L navíc.

12.15 Pozorování.

(i) Je-li T' rozšířením teorie T, potom:

$$T' \text{ je bezesporná} \quad \Rightarrow \quad T \text{ je bezesporná}$$

(ii) Je-li T' konzervativním rozšířením teorie T, potom:

$$T' \text{ je bezesporná} \quad \Leftrightarrow \quad T \text{ je bezesporná}$$

Důkaz.

(i) Pro spor nechť T není bezesporná, potom pro nějakou formuli A platí $T \vdash A \,\&\, \neg A$. Protože je T' rozšířením T, platí podle pozorování 12.13 i $T' \vdash A \,\&\, \neg A$ a teorie T' je sporná, což je spor.

(ii) Směr $\Rightarrow$ plyne z bodu (i), opačný směr se dokáže naprosto stejně (spor se u konzervativního rozšíření přenáší popsaným způsobem oběma směry). ☆

12.16 Henkinova věta. Ke každé teorii T lze sestrojit její konzervativní rozšíření T_H, které je Henkinovou teorií.

Důkaz. Teorii T_H sestrojíme z teorie T konzervativním rozšířením, které přidá nové konstanty a speciální axiomy tak, aby výsledná teorie měla Henkinovu vlastnost.

Mějme teorii T_n s jazykem L_n. Pro nějakou uzavřenou formuli jazyka L_n tvaru $(\exists x)A$ uvažme konstantu

$$c_{(\exists x)A} \tag{1}$$

a speciální axiom tvaru:

$$(\exists x)A \to A_x[c_{(\exists x)A}] \tag{2}$$

Budeme říkat, že konstanta (1) přísluší k axiomu (2) a naopak.

Teorie T_{n+1} s jazykem L_{n+1} vznikne pak z teorie T_n s jazykem L_n tak, že pro všechny uzavřené formule jazyka L_n tvaru $(\exists x)A$ přidáme do jazyka L_{n+1} všechny výše naznačené konstanty do teorie T_{n+1} všechny výše naznačené speciální axiomy. Přidané konstanty nazveme „Henkinovými konstantami $(n+1)$-tého řádu“ a přidané speciální axiomy „Henkinovými axiomy $(n+1)$-tého řádu“.

Označme původní teorii T jako T_0 a její jazyk L jako L_0. Sestrojíme-li naznačeným postupem teorii T_1 jazyka L_1, stále ještě nemusí mít Henkinovu vlastnost. V novém jazyce L_1 totiž existuje oproti L_0 větší množství (uzavřených) formulí (formule obsahující nějakou konstantu, která je v L_1 oproti L_0 navíc) a k takovým formulím nemáme příslušné Henkinovy konstanty ani axiomy.

Proto musíme naznačený postup „do nekonečna“ iterovat a vytvořit posloupnost jazyků a teorií:

$$L_0 \subset L_1 \subset L_2 \subset \ldots \qquad\qquad T_0 \subset T_1 \subset T_2 \subset \ldots$$

Označíme-li

$$L_H = L_\infty = \bigcup_{n=0}^{\infty} L_n \qquad\qquad T_H = T_\infty = \bigcup_{n=0}^{\infty} T_n$$

tvrdíme, že teorie T_H s jazykem L_H je Henkinovou teorií a konzervativním rozšířením teorie T.

Kdyby T_H nebyla Henkinova teorie, existovala by v jazyce L_H uzavřená formule tvaru $(\exists x)A$, ale pro žádnou konstantu c jazyka L_H by neplatilo:

$$T_H \vdash (\exists x)A \to A_x[c]$$

Formule $(\exists x)A$ je ale konečná (jako každá jiná formule) a proto obsahuje jen konečný počet Henkinových konstant. Nechť k je řád takové Henkinovy konstanty maximálního řádu. Proto již teorie T_{k+1} a jazyk L_{k+1} musí obsahovat konstantu $c_{(\exists x)A}$ a axiom $(\exists x)A \to A_x[c_{(\exists x)A}]$. Protože tato dvojice je jistě součástí teorie T_H s jazykem L_H, dostáváme spor. Teorie T_H je tedy Henkinova.

Zbývá dokázat, že teorie T_H je konzervativním rozšířením teorie T. Protože je $T \subset T_H$, je teorie T_H jistě *rozšířením* teorie T. Dále mějme v jazyce L libovolnou formuli A, která je větou teorie T_H. Abychom dokázali, že T_H je *konzervativním* rozšířením teorie T, musíme ukázat $T \vdash A$.

Nechť formule $B_1, \ldots, B_n$ jsou právě všechny Henkinovy axiomy použité ve formálním důkazu $T_H \vdash A$ seřazené podle řádu sestupně (B_1 tedy odpovídá Henkinově axiomu nejvyššího řádu a B_n nejnižšího řádu, pozor, některé můžou mít i stejný řád). Potom jistě:

$$T, B_1, \ldots, B_n \vdash A$$

Protože každý Henkinův axiom je uzavřená formule, z věty o dedukci dostáváme:

$$T \vdash B_1 \to \ldots \to B_n \to A \tag{3}$$

Nechť je axiom B_1 tvaru:

$$(\exists x)C \to C_x[c_{(\exists x)C}]$$

Protože konstanta $c_{(\exists x)C}$ není obsažena ve formulích $B_2, \ldots, B_n$ (díky jejich seřazení) a už vůbec ne v teorii T, máme díky větě o konstantách pro *novou* proměnnou y:

$$T \vdash (((\exists x)C \to C_x[y]) \to (B_2 \to \ldots \to B_n \to A))_y[c_{(\exists x)C}] \quad \Rightarrow \tag{4}$$

$$\Rightarrow \quad T \vdash ((\exists x)C \to C_x[y]) \to (B_2 \to \ldots \to B_n \to A) \tag{5}$$

Předpoklad (4) je vlastně jiný zápis formule (3), odtud dostáváme platnost tvrzení (5). Toto tvrzení dále upravíme (uvědomme si, že se proměnná y ve formulích $B_2, \ldots, B_n, A$ nevyskytuje):

$$\begin{aligned}
&T \vdash (\exists y)((\exists x)C \to C_x[y]) \to (B_2 \to \ldots \to B_n \to A) && \text{(zavedení } \exists) \\
&T \vdash ((\exists x)C \to (\exists y)C_x[y]) \to (B_2 \to \ldots \to B_n \to A) && \text{(prenexní operace)} \\
&\quad \vdash (\exists x)C \to (\exists y)C_x[y] && \text{(věta o variantách)} \\
&T \vdash B_2 \to \ldots \to B_n \to A && \text{(modus ponens)}
\end{aligned}$$

Celkový výsledek $T \vdash A$ získáme iterací tohoto postupu. ☆

12.17 Lindenbaumova věta pro predikátovou logiku. Každou bezespornou teorii T lze rozšířit do úplné teorie S se stejným jazykem L.

Důkaz. Je podobný, jako ve výrokové logice. BÚNO předpokládejme, že všechny speciální axiomy teorie T jsou uzavřené formule. Vznikne-li totiž T'

uzávěrem všech axiomů T, je T' rozšířením T (každý speciální axiom T je v T' dokazatelný pomocí věty o uzávěru) a rozšíření je vlastnost tranzitivní, takže i S postavená z T' bude rozšířením původní teorie T.

Uspořádejme *všechny uzavřené* formule jazyka L do libovolné *prosté*[8] posloupnosti

$$A_1, A_2, A_3, \ldots$$

Vytvoříme „neklesající“ posloupnost bezesporných množin

$$T = T_0 \subseteq T_1 \subseteq T_2 \subseteq T_3, \ldots$$

tak, že pro $\forall i \in \mathbb{N}$ položíme

$$T_i = \begin{cases} T_{i-1} \cup \{A_i\}, & \text{je-li } T_{i-1} \cup \{A_i\} \text{ bezesporná} \\ T_{i-1} & \text{jinak.} \end{cases}$$

Nechť $S = T_\infty = \bigcup_{n=0}^{\infty} T_n$. Naprosto stejně jako ve výrokové logice se dokáže, že S je maximální bezesporná množina, tentokrát ale pouze *uzavřených* formulí. Zbývá dokázat, že S je úplná teorie.

Teorie S je bezesporná (a proto se z ní nedá dokázat uzavřená formule A a zároveň $\neg A$), ale pro spor předpokládejme, že existuje uzavřená formule A taková, že je zároveň:

$$S \nvdash A \quad \text{a} \quad S \nvdash \neg A$$

Protože A není dokazatelná z S, je množina $T \cup \{\neg A\}$ bezesporná a S je její vlastní podmnožinou (protože $\neg A$ není větou S, nemůže být ani prvkem S). Máme tedy spor s maximalitou S a S je úplná teorie. ✯

12.18 Definice. Nechť je jazyk L' rozšířením jazyka L, $\mathbb{M}$ je interpretací jazyka L a $\mathbb{M}'$ je interpretací jazyka L'.

- *Redukce struktury* $\mathbb{M}'$ do jazyka L je struktura $\mathbb{M}' \mid L$, která vznikne ze struktury $\mathbb{M}'$ vynecháním funkcí a relací, které realizují takové funkční a predikátové symbolům, které jsou v jazyce L', ale nejsou v jazyce L.
- $\mathbb{M}'$ je *expanzí struktury* $\mathbb{M}$, jestliže $\mathbb{M} = \mathbb{M}' \mid L$.

12.19 Lemma. Nechť T' je rozšíření teorie T s jazykem L a $\mathbb{M}'$ je model teorie T'. Potom $\mathbb{M}' = \mathbb{M} \mid L$ je model teorie T.

Důkaz. Struktury $\mathbb{M}$ a $\mathbb{M}'$ mají stejné univerzum a také stejně realizují všechny speciální symboly jazyka L. Proto pro libovolné ohodnocení proměnných e a term t jazyka L je hodnota $t[e]$ stejná v obou strukturách a pro libovolnou formuli A jazyka L platí:

$$\mathbb{M} \vDash A[e] \quad \Leftrightarrow \quad \mathbb{M}' \vDash A[e]$$

[8] Ani zde se mi nepodařilo předpoklad prostosti odůvodnit. Že by opět proto, aby posloupnost obsahovala *každou* (uzavřenou) formuli?

Formálně by se obě tvrzení dala dokázat indukcí podle složitosti termu t či formule A. Dále máme:

$$\mathbb{M} \vDash A \quad \Leftrightarrow \quad \mathbb{M}' \vDash A \tag{1}$$

Je-li $A \in T$, potom je podle definice rozšíření formule A větou teorie T' a dle věty o korektnosti máme $\mathbb{M}' \vDash A$. To díky (1) znamená, že $\mathbb{M} \vDash A$. Struktura $\mathbb{M} = \mathbb{M}' \mid L$ je tedy skutečně modelem teorie T. ☆

12.20 Věta o úplnosti predikátové logiky prvního řádu (Gödel). Nechť T je teorie s jazykem L.

(i) Je-li A libovolná formule jazyka L, potom:

$$T \vdash A \quad \Leftrightarrow \quad T \vDash A$$

(ii) Teorie T je bezesporná, právě když má model.

Důkaz. Napřed dokážeme bod (ii) a bod (i) z něj pak vyplyne jako důsledek.

⇐) Nechť $\mathbb{M}$ je model teorie T a A je nějaká uzavřená formule jazyka L. Podle definice pravdivosti je v modelu $\mathbb{M}$ pravdivá právě jedna z formulí A a $\neg A$. Druhá, nepravdivá formule nemůže být podle věty o korektnosti dokazatelná v teorii T. Teorie T je tedy bezesporná.

⇒) Mějme bezespornou teorii T. Podle Henkinovy věty k ní lze sestrojit její konzervativní rozšíření T_H s jazykem L_H, které je Henkinovou teorií. Díky pozorování 12.15 navíc víme, že T_H je také bezesporná, a proto podle Lindenbaumovy věty existuje rozšíření T' teorie T_H, které je úplné a navíc má stejný jazyk jako teorie T_H, tedy L_H.

Obě teorie T_H a T' se tedy vztahují ke stejnému jazyku, proto je i úplná teorie T' teorií Henkinovou (každá uzavřená formule A jazyka teorie T' je i formulí jazyka teorie T_H a protože je T' rozšířením T_H, dá se v T' dokázat Henkinův axiom pro formuli A).

Teorie T' je tedy úplná a Henkinova, proto pro ni podle věty o kanonickém modelu existuje model $\mathbb{M}'$. Protože je T' rozšířením teorie T s jazykem L, podle lemmatu 12.19 je struktura $\mathbb{M} = \mathbb{M}' \mid L$ modelem teorie T. Nalezli jsme tedy model $\mathbb{M}$ teorie T.

Nyní zpět k bodu (i). Kromě toho, že směr ⇒ je vlastně tvrzení věty o korektnosti, je celá ekvivalence důsledkem bodu (ii) (symbolem A' značíme uzávěr formule A):

$T \vdash A \Leftrightarrow T \cup \{\neg A'\}$ je sporná	(důsledek 9.21)
$\Leftrightarrow T \cup \{\neg A'\}$ nemá model	(dokázaný bod (ii))
$\Leftrightarrow$ žádný model T není modelem $\neg A'$	(sporem)
$\Leftrightarrow$ každý model T je modelem A'	(význam negace)
$\Leftrightarrow T \vDash A'$	(definice)
$\Leftrightarrow T \vDash A$	(definice)

☆

Uvědomme si, že idea důkazu věty o úplnosti predikátové logiky je velmi podobná důkazu věty o úplnosti výrokové logiky. Bod (ii) věty je vlastně obdoba věty o bezespornosti a splnitelnosti a bod (i), samotná úplnost, se dokáže velmi podobně. Nejinak je tomu i v případě následující věty o kompaktnosti.

12.21 Věta o kompaktnosti predikátové logiky. Teorie T má model, právě když má model každá *konečná* teorie $T' \subseteq T$.

Důkaz.

$\Rightarrow$) Zřejmé

$\Leftarrow$) Nechť pro spor nemá teorie T žádný model. To podle věty o úplnosti, bod (ii) znamená, že je sporná, a proto pro nějakou formuli A existuje formální důkaz věty $T \vdash A \,\&\, \neg A$. Tento důkaz ale využívá jen konečné množství speciálních axiomů teorie T, proto musí platit $T' \vdash A \,\&\, \neg A$ i pro nějakou *konečnou* podmnožinu $T' \subseteq T$. To ale znamená, že tato podmnožina T' je sporná a nemá tedy žádný model, což podle předpokladu nelze. Došli jsme ke sporu. ☆

12.22 Důsledek. TODO!!!

Důkaz. ☆

13 Vývoj teorií

Formální systémy matematických teorií začínají axiomy, které jsou formulovány úsporně a v co nejjednodušším jazyku. S rozvíjením teorie přibývají nové pojmy (konstanty, operace, predikáty), které definujeme pomocí již známých pojmů. V této části ukážeme, že tyto definice mají pouze pomocný charakter, definované symboly lze eliminovat a vrátit se tak k původnímu jazyku a rozšíření teorie, které definicemi vznikne, je konzervativní.

13.1 Lemma (charakterizace rozšíření pomocí modelů). Nechť T je teorie s jazykem L a T' je teorie s jazykem L', který je rozšířením jazyka L. Potom:

(i) T' je rozšířením teorie T, právě když pro každý model $\mathbb{M}'$ teorie T' je jeho redukt $\mathbb{M} = \mathbb{M}' \mid L$ modelem teorie T.

(ii) T' je konzervativním rozšířením teorie T, pokud je T' rozšířením T a každý model $\mathbb{M}$ teorie T lze expandovat do modelu $\mathbb{M}'$ teorie T'.

Důkaz. (i) $\Rightarrow$) Lemma 12.19.

$\Leftarrow$) Nechť redukt každého modelu teorie T' do jazyka L je modelem teorie T. Mějme libovolný speciální axiom A teorie T.

Dále mějme libovolný model $\mathbb{M}'$ teorie T'. Protože $\mathbb{M} = \mathbb{M}' \mid L$ je dle předpokladu modelem teorie T, je $\mathbb{M} \vDash A$. Potom také $\mathbb{M}' \vDash A$ (viz důkaz lemmatu 12.19).

Dokázali jsme, že A je pravdivá v každém modelu teorie T', a proto $T' \vDash A$. Z věty o úplnosti potom máme $T' \vdash A$. Teorie T' je tedy rozšířením teorie T.

(ii) Nechť $\mathbb{M}$ je libovolný model teorie T a jeho expanze $\mathbb{M}'$ je modelem teorie T'. Dále nechť formule A jazyka L je větou teorie T'. Podle věty o korektnosti a opět podle důkazu lemmatu 12.19 je potom

$$T' \vdash A \quad \Rightarrow \quad T' \vDash A \quad \Rightarrow \quad \mathbb{M}' \vDash A \quad \Rightarrow \quad \mathbb{M} \vDash A$$

což platí pro libovolný model $\mathbb{M}$ teorie T, proto $T \vDash A$. A tedy protože T' je rozšířením teorie T, je to také konzervativní rozšíření. ✯

13.2 Věta o definici predikátového symbolu. Nechť T je teorie s jazykem L, rozšíření L' jazyka L vznikne přidáním nového n-árního predikátového symbolu p a rozšíření T' teorie T vznikne přidáním speciálního axiomu

$$p(x_1, \ldots, x_n) \leftrightarrow D$$

kde D je formule jazyka L taková, že $x_1, \ldots, x_n$ jsou právě všechny její volné proměnné.

Potom teorie T' s jazykem L' je konzervativním rozšířením teorie T. Navíc pro libovolnou formuli B' jazyka L' lze sestrojit formuli B jazyka L takovou, že:

$$T' \vdash B \leftrightarrow B'$$

Důkaz. Napřed dokážeme, že definovaný symbol lze eliminovat. Nechť B' je libovolná formule jazyka L' a D' je taková varianta definující formule D, že žádná proměnná formule B' není vázaná v D' (potom můžeme libovolný term formule B' substituovat do formule D). Z věty o variantách máme:

$$T' \vdash p(x_1, \ldots, x_n) \leftrightarrow D' \tag{1}$$

Formule B vznikne z formule B' naznačeným nahrazením všech výskytů definovaného predikátu p:

$$p(t_1, \ldots, t_n) \qquad \longrightarrow \qquad D'_{x_1,\ldots,x_n}[t_1, \ldots, t_n]$$

Z věty o instancích a z (1) potom pro takové nahrazení platí

$$T' \vdash p(t_1, \ldots, t_n) \leftrightarrow D'_{x_1,\ldots,x_n}[t_1, \ldots, t_n]$$

a proto podle věty o ekvivalenci máme:

$$T' \vdash B \leftrightarrow B'$$

Nyní ukážeme konzervativnost popsaného rozšíření teorie T na T'. Dokážeme poněkud silněji, že pro libovolnou formuli B' jazyka L' platí

$$T' \vdash B' \quad \Rightarrow \quad T \vdash B \tag{2}$$

kde formule B jazyka L vznikla z B' eliminováním definovaného predikátu. Potom speciálně je-li formule B' pouze z jazyka L, jsou B a B' totožné formule a (2) má tvar

$$T' \vdash B \quad \Rightarrow \quad T \vdash B$$

čímž bude konzervativnost rozšíření dokázána.

Nechť $(B'_1, \ldots, B'_m)$ je formální důkaz $T' \vdash B'$ a každá formule B_i vznikne z B'_i eliminací definovaného predikátu. Indukcí podle tohoto formálního důkazu dokážeme, že každá taková B_i je větou teorie T, a to speciálně pro $i = m$ znamená, že $T \vdash B$.

- B'_i je axiom predikátové logiky kromě axiomu rovnosti pro definovaný predikát p. B_i je potom axiomem stejného druhu.
- B'_i je axiom rovnosti pro definovaný predikát p, tedy:

  $$y_1 = z_1 \to \ldots \to y_n = z_n \to p(y_1, \ldots, y_n) \to p(z_1, \ldots, z_n)$$

  Potom B_i je tvaru

  $$y_1 = z_1 \to \ldots \to y_n = z_n \to D_{x_1,\ldots,x_n}[y_1, \ldots, y_n] \to D_{x_1,\ldots,x_n}[z_1, \ldots, z_n]$$

  a to je důsledek 11.6 věty o rovnosti.
- Je-li B'_i odvozena odvozovacím pravidlem, je B_i odvozena stejným pravidlem z odpovídajících formulí.
- Je-li B'_i speciálním axiomem T', pak je buď $B'_i = B_i \in T$ a není co dokazovat, nebo je to definující axiom a B_i je tvaru $D' \leftrightarrow D$ a to plyne z věty o variantách.

☆

13.3 Věta o zavedení funkčního symbolu. Nechť T je teorie s jazykem L a platí

$$T \vdash (\exists y)A \tag{1}$$

kde formule $(\exists y)A$ jazyka L má všechny volné proměnné mezi $x_1, \ldots, x_n$. Dále nechť T' vznikne z T rozšířením jazyka o nový n-ární funkční symbol f a axiom

$$A_y[f(x_1, \ldots, x_n)] \tag{2}$$

Potom T' je konzervativní rozšíření teorie T.

Důkaz. K důkazu budeme potřebovat jistý výsledek teorie množin:

- Množina M je *dobře uspořádaná* relací $\prec$, má-li každá neprázdná podmnožina M' množiny M nejmenší prvek vzhledem k uspořádání $\prec$.
- Na každé množině existuje relace dobrého uspořádání.

Teorie T' je jistě rozšířením T. Konzervativnost rozšíření dokážeme tak, že každý model $\mathbb{M}$ teorie T expandujeme do modelu $\mathbb{M}'$ teorie T' (viz lemma 13.1).

Nechť je tedy $\mathbb{M}$ libovolný model T a $\prec$ relace dobrého uspořádání na universu $\mathbb{M}$. Dále mějme libovolné ohodnocení e. Díky (1) a definici pravdivosti platí pro nějaké individuum $m \in \mathbb{M}$:

$$\mathbb{M} \vDash A[e(y/m)]$$

Toto m závisí na individuích $m_1, \ldots, m_n$, kde $m_i = e(x_i)$. Množinu všech takových m označme:

$$F(m_1, \ldots, m_n) = \{m \mid \mathbb{M} \vDash A[e(y/m)]\}$$

Jde o neprázdnou množinu individuí a protože uspořádání $\prec$ je dobré, má vzhledem k němu nejmenší prvek. Interpretaci $f_{\mathbb{M}}$ nového funkčního symbolu potom zvolíme předpisem

$$f_{\mathbb{M}}(m_1, \ldots, m_n) = \min\left(F(m_1, \ldots, m_n)\right)$$

a takto vytvoříme expanzi $\mathbb{M}'$ modelu $\mathbb{M}$. Nový model $\mathbb{M}'$ je modelem teorie T', neboť nový axiom (2) je při $\mathbb{M}'$ pravdivý. ☆

13.4 Definice.

- Formule A je *univerzální* (*existenční*), je-li v prenexním tvaru a všechny kvantifikátory prefixu jsou univerzální (existenční).
- Dvě teorie T, S se stejným jazykem jsou *ekvivalentní*, jestliže mají stejné věty. Píšeme $T \equiv S$.
- Teorie T je *otevřená*, jestliže jsou všechny její axiomy otevřené formule.