FAKULTA MATEMATIKY, FYZIKY
A INFORMATIKY
UNIVERZITY KOMENSKÉHO
KATEDRA INFORMATIKY

VYBRANÉ PARTIE Z LOGIKY

poznámky z prednášok

martin florek

22. mája 2004

Predhovor

Vďaka nude a oprášeniu vedomostí z LaTeXu som sa rozhodol, že spíšem poznámky z prednášok *Vybrané partie z logiky*. Za prípadné chyby mi nenadávajte, ale pošlite mi mail, že čo, kde, ako, prečo a ja to opravím. Dúfam, že tieto mini skriptá budú pre vás užitočné a pomôžu vám zdolať skúšku.

Autor za správnosť neručí :), ale ked je niekde chyba, tak mi napíšte na *shelll@host.sk*

Tieto skriptá sú v rozrobenom štádiu a kúsok na koci chýba. Keď budem mať jedného pekné dňa čas, tak ich určite dopíšem.

Obsah

Kapitola 1

Úvod

Úvodom sa dozviete, o čom tento predmet vôbec je. Tak to síce ani srnka netuší, ale ináč o výrokovej logike a predikátovej logike.

Výroková logika

- jazyk výrokovej logiky
- sémantika a syntax výrokovej logiky
- formula, podforumla výrokovej logiky
- dôkaz, odvodenie, axiómy a pravidlá odvodenia
- niektoré teorémy
- Postove vety, bezospornosť výrokovej logiky
- úplnosť výrokovej logiky
- konjunktívny a disjunktívny normálny tvar

Predikátová logika

- jazyk predikátovej logiky
- vzťah výrokovej a predikátovej logiky
- axiómy a pravidlá odvodenia predikátovej logiky
- prenexný a Skolemov tvar formúl predikátovej logiky
- sémantika a syntax predikátovej logiky

Teória s rovnosťou
= binárny predikát rovnosti
axiómy rovnosti (sú tri)

Def 1.1.1. *Usporiadanú dvojicu* $(A, \cdot)$, *kde* $A \neq \emptyset$ *nazývame:*

1. *grupoid:* $\forall x, y \in A \implies x \cdot y \in A$
2. *pologrupa:* $\forall x, y, z \in A \implies (x \cdot y) \cdot z = x \cdot (y \cdot z)$

1. *a* 2. *sú špeciálne axiómy.*

Kapitola 2

Jazyk logiky

všeobecné názvy – čísla, množiny, body, priamky, geometrické útvary, relácie, zobrazenia
konštanty – 0, i, π, e, id ...
premenné – x, y, z ...
operácia – $f(x, y)$, $g(x, y, z)$ $\quad f, g$ – funkčné symboly
f_n – $n \in \mathbb{N}$, n-árny funkčný symbol, keď $n = 0$ – nulárny funkčný symbol (konštanta)

potrebujeme zachytiť vzťahy medzi objektami:

„číslo x je rovné dvojnásobku čísla y"	$=$	$x = 2y$
„číslo x je menšie ako číslo y"	$<$	$x < y$
„číslo x leží medzi číslami y a z"		

predikáty – P, Q, R ...
$n \geq 1$ „árnosť (arita) predikátového symbolu", keď $n = 0$, tak TRUE alebo FALSE
logické spojky – $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$

$\neg x = 2y$	„neplatí $x = 2y$"
$x = 2y \wedge x < 1$	„$x = 2y$ a $x < 1$"
$x = 2y \vee x < 1$	„$x = 2y$ alebo $x < 1$"
$x = 2y \rightarrow x < 1$	„$x = 2y$ implikuje $x < 1$", „ak $x = 2y$, tak $x < 1$"
$x = 2y \leftrightarrow x < 1$	„$x = 2y$ je ekvivalentné $x < 1$", „$x = 2y$ práve vtedy keď $x < 1$"

kvantifikátory:

- veľký, všeobecný $\forall$, „pre každé x platí ..."
- malý, existenčný $\exists$, „existuje také x, že ..."

$(\forall x)(x < 1)$	„pre každé x platí $x < 1$"
$(\exists x)(x = 2y)$	„existuje také x, že $x = 2y$"

pomocné symboly (zátvorky) – $(,), [,], \{, \}$
Všetky obraty môžeme zachytiť pomocou umelého symbolického jazyka.

2.1 Jazyk prvého, druhého a tretieho rádu

Def 2.1.1. *Jazyk prvého rádu obsahuje tieto symboly:*

1. *premenné $x, y, z \ldots, x_1, x_2 \ldots, y_1, y_2 \ldots$, ktorých je neohraničene veľa*
2. *funkčné symboly $f, g \ldots$, ku každému symbolu je priradené $n \in \mathbb{N}$, určujúce árnosť $(n \geq 0)$*

3. *predikátové symboly P, Q, R, ku každému je priradené $n \geq 1$, jeho árnosť*

4. *logické spojky $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$ (negácia, konjunkcia, disjunkcia, implikácia, ekvivalencia)*

5. *kvantifikátory $\forall, \exists$, všeobecný a existenčný*

6. *pomocné symboly (zátvorky)*

Poznámka. Niektoré symboly sú spoločné všetkým formálnym jazykom: premenné, logické spojky, kvantifikátory, pomocné symboly – nazývame logické symboly

Poznámka. Medzi logické symboly počítame aj symboly rovnosti $=$

Poznámka. Zostávajúce symboly $(2, 3)$ nazývame špeciálne symboly (Voľbou špeciálnych symbolov získavame špeciálne teórie)

$\in$ – binárny predikátový symbol patričnosti: $x \in M$, x patrí M (prináleží)

Def 2.1.2. *Termom nazývame dobre uzátvorkovaný výraz, ktorý predstavuje výsledok po uskutočnení naznačených oprácií. Term neobsahuje logické spojky.*
term: $f(g(x, y), h(x), x)$; x, y – premenné, f – ternárny funkčný symbol, g – binárny, h – unárny

Def 2.1.3. *Formulou nazývame matematické tvrdenie.*

Poznámka. termy a formuly – zložitejšie štruktúry poskladané zo symbolov

Poznámka. Premenné označujú všeobecné názvy pre individuá. Kvantifikovať môžeme iba individuá.

Def 2.1.4. *Jazyk druhého rádu obsahuje premenné pre množiny individuí.*

Def 2.1.5. *Jazyk tretieho rádu obsahuje premenné pre množiny množín individuí.*

2.2 Čiastočné usporiadanie

Def 2.2.1. *Usporiadanú dvojicu $(A; \leq)$, $A \neq \emptyset$ nazývame čiastočným usporiadaním práve vtedy, keď:*
$\leq$, D (relácia); $D \subseteq A \times A$

1.	$\forall x \in A:$	$(x, x) \in D$	*reflexívnosť*
2.	$\forall x, y \in A:$	$(x, y) \in D \wedge (y, x) \in D \rightarrow x = y$	*antisymetrickosť*
3.	$\forall x, y, z \in A:$	$(x, y) \in D \wedge (y, z) \in D \rightarrow (x, z) \in D$	*tranzitívnosť*

teória čiastočného usporiadania – je to teória s rovnosťou

Def 2.2.2. *Ostré čiastočné usporiadanie $(A; <)$, $A \neq \emptyset$.*

1.	$(\forall x)$	$\neg(x < x)$
2.	$(\forall x)(\forall y)(\forall z)$	$x < y \wedge y < z \rightarrow x < z$
3.	$(\forall x)(\forall y)$	$(x \neq y) \rightarrow (x < y) \vee (y < x)$
4.	$(\forall x)(\forall y)$	$(x = y) \vee (x < y) \vee (y < x)$

teória ostrého čiastočného usporiadania, 3. a 4. sú ekvivalentné

tautológia – $p \rightarrow q \leftrightarrow \neg p \vee q$

2.3 Telesá charakteristiky nula

Def 2.3.1. *Telesom nazývame usporiadanú trojicu $(A; +; \cdot)$, kde $+, \cdot$ sú také binárne operácie na A, že $(A; +)$ je komutatívna grupa, $(A^*; \cdot)$ je grupa (nie nutne komutatívna, ak $(A^*; \cdot)$ je komutatívna grupa, tak A nazývame pole) a $\cdot$ je distributívna vzhľadom na $+$. $A^* = A \setminus \{0\}$, kde 0 je neutrálny prvok grupy $(A; +)$.*
$0, 1, +, \cdot$ – špeciálne symboly jazyka teleso
$0, 1$ – konštanty

$x = 1 \times x,\ x + x = 2 \times x,\ x + (x + x) = 3 \times x\ \dots$
$p \times x,\ p \in \mathbb{N}^+$

Def 2.3.2. *Najmenšie $p \in \mathbb{N}^+$, pre ktoré platí $p \times 1 = 0$ nazývame charakteristikou telesa ($(A; +; \cdot)$ je teleso, 1 je neutrálny prvok grupy $(A^*; \cdot)$, char $A = p$). Ak $\forall p \in \mathbb{N}^+,\ p \times 1 \neq 0,$ char $A = 0$ (resp. ∞).*

Tvrdenie 1. *Každé konečná množina formúl, ktoré sú splnené vo všetkých telesách s char $= 0$, platí aj vo všetkých telesách dosť veľkej konečnej char.*

Predpoklad. Že telesá *char* 0 môžeme konečne axiomatizovať. M – konečná množina formúl.

Veta 2.3.1. *O kompaktnosti. Ak T je množina formúl jazyka L a ak je A formula jazyka L, potom:*
$T \models A \leftrightarrow T' \models A$ pre nejakú konečnú podmnožinu $T' \subseteq T$ (A je T platná práve vtedy, keď je T' platná).

Veta 2.3.2. *O kompaktnosti (2. tvar). Ak T je množina formúl jazyka L. Model teórie T existuje práve vtedy, keď každá konečná podmnožina T', $T' \subseteq T$ má model.*

- $p \times 1 \neq 0$
- $(\forall p)\ p \neq 0 \ \rightarrow\ p \times 1 \neq 0$

Ak zavedieme ďaší druh premenných, napr. prirodzené číslo, tak telesá char 0 môžeme konečne axiomatizovať. Veta o kompaktnosti neplatí v slabej logike druhého rádu.

Tvrdenie 2. *Žiadna množina formúl jazyka prvého rádu teórie telies neurčuje teleso reálnych čísel jednoznačne, až na izomorfizmus. (dôsledok vety Löwenheim - Skolem.)*

Veta 2.3.3. *Löwenheim - Skolem. Ak teória T prvého rádu má nejaký model, tak potom má aj spočítateľný model.*

Kapitola 3

Formálne systémy logiky

- popísali sme jazyk prvého rádu
- zoznámili sme sa s vyjadrovacími schopnosťami jazyka prvého rádu
- termy su individuá, ktoré sú výsledkom uskutočnenia naznačených operácií
- formuly sú matematické tvrdenia
- vieme definovať matematický dôkaz?
- čím je zastúpená vo formálnom jazyku logická úvaha?

Dôkaz vieme definovať ako konečnú postupnosť formúl, ktorej každý člen je buď nejaké základné tvrdenie – axióma alebo je z niektorých predchádzajúcich členov postupnosti odvodená jedným z odvodzujúcich pravidiel.

3.1 Formálny systém

Def 3.1.1. *Fromálny systém pozostáva z týchto troch zložiek:*

1. *jazyk z ktorého symbolov vytvárame konečné postupnosti, najmä termy a formuly*
2. *axiómy sú isté formuly, ktoré prijímame ako základné tvrdenia*
3. *odvodzovacie pravidlá sú syntaktické pravidlá, ktorými sa z jednej alebo viacej formúl vytvára ďalšia (odvodená) formula*

Def 3.1.2. *Dôkaz vo formálnom systéme je konečná postupnosť formúl, ktorej členmi sú niektoré axiómy a formuly odvodené z predchádzajúcich členov postupnosti pomocou odvodzovacích pravdiel.*

Def 3.1.3. *Hovoríme, že nejaka formula A je teoréma formálneho systému alebo, že je odvoditeľná, ak existuje dôkaz, teda konečná postupnosť formúl, ktorej posledným členom je formula A.*

Logická úvaha v intuitívnom poňatí. Voľbou axióm a pravidiel odvodenia určujeme triedu získaných tvrdení. V klasickej logike sa odvolávajú na sémantiku – všetky axiómy sú „univerzálne platné“ formuly, sú „pravdivé“ pri každej interpretácii symbolov. Pravidlá odvodenia volím tak, aby boli „korektné“.

výroková logika – axiómy a pravidlá odvodenia budú charakterizovať vlastnosti logických spojok

predikátová logika – pridáme axiómy a pravdilá odvodenia, ktoré charakaterizujú vlastnosti kvantifikátorov

predikátová logika s rovnosťou – uvedieme axiómy, ktoré prirodzeným spôsobom charakterizujú vlastnosti rovnosti

Kapitola 4

Výroková logika

- budeme sa zaoberať vlastnosťami logických spojok

4.1 Formuly

Def 4.1.1. *Nech P je neprázdna množina, jej prvky nazveme prvotné formuly. Môžu to byť vety prirodzeného jazyka, slová nejakého formálneho jazyka alebo len písmená: $p, q, r, s \ldots, p_1, p_2, \ldots$*

Def 4.1.2. *Jazyk L_P výrokovej logiky nad P obsahuje okrem prvkov množiny P aj symboly pre logické spojky: $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$ a pomocné symboly (zátvorky).*
Hovoríme, že P je množina prvotných formúl jazyka L_P.

Def 4.1.3. *Výrokové formuly jazyka L_P definujeme pomocou nasledujúcich syntaktických pravidiel:*

1. *každá prvotná formula $p \in P$ je výroková formula*
2. *ak sú výrazy A, B formuly, potom výrazy $(\neg A), (A \wedge B), (A \vee B), (A \rightarrow B), (A \leftrightarrow B)$ sú výrokové formuly*
3. *každá výroková formula vznikne konečným počtom použití pravidiel 1 a 2.*

Def 4.1.4. *Nech A je formula jazyku L_P, jej podformulou je:*

1. *ona sama, ak A je prvotná formula jazyka L_P*
2. *ona sama, a každá podformula formuly B, ak A je tvaru $(\neg B)$*
3. *ona sama, a každá podfurmula formúl B a C, ak A je tvaru $(B \wedge C), (B \vee C), (B \rightarrow C), (B \leftrightarrow C)$*
4. *žiadne iné podformuly okrem tých, čo sú opísané v 1, 2, 3 formula A nemá*

Príklad. majme $P = \{p, q, r, s\}$
p, q, r, s – sú formuly jazyka L_P podľa bodu 1.
$(p \vee q), (p \wedge s), (r \rightarrow q)$ – sú formuly jazyka L_P podľa bodu 3.
$((p \vee q) \rightarrow \underbrace{(q \wedge r)}_{\text{pod formula}})$
$(p \rightarrow (q \rightarrow (r \rightarrow s)))$
$\neg(p \rightarrow q)$
$\rightarrow p$ – nie je formula

4.2 Tautológia

Def 4.2.1.

1. *pravdivostné ohodnotenie (valuácia) prvotných formúl je každé zobrazenie* $p : P \to \{0,1\}$*, ktoré každej prvotnej formule* $p \in P$ *priradí hodnotu* 0 *alebo* 1 *(FALSE, TRUE).*

2. *indukcio podľa dĺžky formuly definujeme rozšírenie* $\overline{v}$ *zobrazenia* v *na množinu všetkých formúl jazyka* L_P*:*

   $\overline{v}(A) = v(A)$*, ak* A *je prvotná formula*
   $\overline{v}(\neg A) = 0$*, ak* $\overline{v}(A) = 1$
   $\overline{v}(\neg A) = 1$*, ak* $\overline{v}(A) = 0$
   $\overline{v}(A \wedge B) = 1$*, ak* $\overline{v}(A) = \overline{v}(B) = 1$*, inak* $= 0$
   $\overline{v}(A \vee B) = 0$*, ak* $\overline{v}(A) = \overline{v}(B) = 0$*, inak* $= 1$
   $\overline{v}(A \to B) = 0$*, ak* $\overline{v}(A) = 1$ *a* $\overline{v}(B) = 0$*, inak* $= 1$
   $\overline{v}(A \leftrightarrow B) = 1$*, ak* $\overline{v}(A) = \overline{v}(B)$*, inak* $= 0$

   Hovoríme, že $\overline{v}(A)$ *je pravdivostná hodnota formuly* A *pri ohodnotení* v*. Formula* A *je pravdivá pri ohodnotení* v*, ak* $\overline{v}(A) = 1$*, inak je formula* A *nepravdivá.*

Def 4.2.2.

1. *Výroková formula* A *je tautológia, ak* $\overline{v}(A) = 1$ *pre ľubovoľné ohodnotenie* v*.*

2. *Výroková formula* A *je splniteľná, ak* $\overline{v}(A) = 1$ *pre nejaké ohodnotenie* v*. Ohodnotenie* v *s touto vlastnosťou nazývame model formuly* A*.*

3. *Množina formúl* T *je splniteľná, ak existuje ohodnotenie* v *tak, že* $\overline{v}(A) = 1,\ \forall A \in T$*. Takéto ohodnotenie* v *nazývame model* T*.*

4. $T \models A$ *(*A *je tautologický dôsledok* T*), ak* $\overline{v}(A) = 1,\ \forall v$*, ktoré je modelom* T*.*

5. *Formulu* A *nazývame kontradikciou, ak* $\overline{v}(A) = 0,\ \forall v$*.*

$(A \vee \neg A)$ – zákon vylúčenia tretieho
$\neg(A \wedge \neg A)$ – vylúčenie kontradikcie
$\neg(A \wedge B) \leftrightarrow (\neg A \vee \neg B)$, $\neg(A \vee B) \leftrightarrow (\neg A \wedge \neg B)$ – de Morgan
$\neg\neg A \leftrightarrow A$ – zákon dvojitej negácie

Poznámka. Ak $T = \emptyset$, tak píšeme $\models A$, to znamená, že A je pravdivá. Platí pre ľubovoľné ohodnotenie (tautológia). $T \models A \wedge T \models A \to B$ potom $T \models B$.
$\overline{v}(A \to B) = 1$ a $\overline{v}(A) = 1$, tak aj $\overline{v}(B) = 1$ – modus ponens

T je množina formúl	
A je výroková formula	A je tautologický dôsledok možniny formúl T
v je model pre T	v model T, platí $\overline{v}(A) = 1$
$A_i \in T_i$, $\overline{v}(A_i) = 1$	$T \models A$

pre $\emptyset$ je ľubovoľné ohodnotenie v model
nech $A_i \in \emptyset$, tak $\overline{v}(A_i) = 1$

Poznámka.

1. Modelom $\emptyset$ formúl je ľubovoľné ohodnotenie v. Preto $\models A \leftrightarrow A$ je tautológia.

2. Ak nie je T splniteľná, potom ľubovoľná formula je jej tautologickým dôsledkom.
   $\forall A_i,\ \overline{v}(A_i) = 1,\ A_i \in T \to \overline{v}(A) = 1$, model neexistuje pre T.

3. Ak je T_0 nesplniteľná a $T_0 \subseteq T$, potom aj T je nesplniteľná.

4. (z vety o kompaktnosti) Pre splniteľnú ...

Cvičenie. Nech f je prosté zobrazenie množiny P všetkých prvotných formúl do množiny $\mathbb{N}$. Definujme zobrazenie f' na množine $P' = P \cup \{\wedge, \vee, \rightarrow, \leftrightarrow, \neg, (,)\}$ tak, že pre ľubovoľné $x \in P$ je $f'(x) = f(x) + 10$ a pre ostatné symboly platí priradenie definované nasledovne:

symbol	$\wedge$	$\vee$	$\rightarrow$	$\leftrightarrow$	$\neg$	(	)
f'(symbol)	1	2	3	4	5	6	7

Nech $\{a_i\}_{i \in \mathbb{N}}$ je nekonečná rastúca postupnosť prvočísiel. Ukážte, že zobrazenie F definované pre ľubovoľné slovo $s_1 \dots s_k$ abecedy P^* – prepisom $F(s_1, \dots, s_k) = a_1^{f'(s_1)} \cdot \dots \cdot a_k^{f'(s_k)} = \prod_1^k a_i^{f'(s_i)}$ platí $a_i > 1$, potom:

a) P je prosté zobrazebie množiny všetkých slov abecedy P' do množiny $\mathbb{N}$.

b) Pre ľubovoľné formuly A, B také, že $A \subseteq B$, platí $F(A) \leq F(B)$.

Cvičenie. Použitím *Cantor-Bernsteinovej* vety dokážte tieto tvrdenia:

a) Existuje prosté zobrazenie g množiny $\mathbb{N}$ na množinu všetkých formúl výrokového počtu s konečne prvotnými formulami P.

b) Množina všetkých výrokových formúl utvorených zo spočítateľnej množiny výrokových formúl je spočítateľná.

4.3 Veta o kompaktnosti

Veta 4.3.1. *O kompaktnosti (VK). Množina T formúl výrokového počtu je splniteľná práve vtedy, keď ľubovoľná konečná podmnožina $T_0 \subseteq T$ má model.*

Dôkaz.

„$\Rightarrow$“ T je splniteľná $\implies \forall T_0 \neq \emptyset,\ T_0 \subseteq T$ má model
triviálne platí

„$\Leftarrow$“ Predpokladajme, že $\forall T_0 \neq \emptyset,\ T_0 \subseteq T$ má model $\implies T$ je splniteľná.
Nech T množina formúl má model, t.j. v také ohodnotenie formúl, že platí $A \in T,\ \overline{v}(A) = 1$
$S = \{B, \overline{v}(B) = 1\}$ potom množina S má nasledovné vlastnosti:

1. $T \subseteq S$
2. každá konečná $S_0 \subseteq S$ je splniteľná
3. pre ľubovoľnú formulu A uvažovaného jazyka platí: buď $A \in S$ alebo $\neg A \in S$, ale nikdy nie súčasne

Dôkaz „$\Leftarrow$“ rozdelíme do dvoch častí:

1. najprv sa presvedčíme, že ak existuje S s uvedenými vlastnosťami, tak potom pomocou nej možno zostrojiť model pre T.
2. prevedieme konštrukciu požadovanej množiny

1. Nech v je také ohodnotenie, že pre každú prvotnú formulu p platí: $v(p) = 1 \leftrightarrow p \in S$
Indukciou podľa dĺžky formuly A dokážeme: $\overline{v}(A) = 1 \leftrightarrow A \in S$
Báza indukcie: platí podľa toho, ako máme v definované.
Indukčný krok: nech A_1, A_2 ($\overline{v}(A_i) = 1 \leftrightarrow A_i \in S$) sú formuly uvažovaného jazyka, na ktoré sa vzťahuje IP.

$\neg A_1$	$\overline{v}(\neg A_1) = 1 \leftrightarrow \overline{v}(A_1) = 0$	podľa IP $A_1 \notin S \implies \neg A_1 \in S$, z 3. vlastnosti S
$A_1 \wedge A_2$	$\overline{v}(A_i) = 1 \leftrightarrow A_i \in S,\ i \in \{1,2\}$	z IP
	$\overline{v}(A_1 \wedge A_2) = 1 \leftrightarrow A_1 \wedge A_2 \in S$	treba ukázať
	$\iff \overline{v}(A_1) = \overline{v}(A_2) = 1,\ A_1 \in S,\ A_2 \in S$	z IP

nech $A_1 \wedge A_2 \notin S$, ale $\neg(A_1 \wedge A_2) \in S$
$\implies \{\neg(A_1 \wedge A_2), A_1, A_2\}$
použijeme 2. vlastnosť, keďže A_1, A_2 sú splniteľné, tak $\neg(A_1 \wedge A_2)$ nie je splniteľná $\implies$ spor

$A_1 \wedge A_2 \in S$
$\overline{v}(A_1 \wedge A_2) = 1 \leftrightarrow \overline{v}(A_1) \wedge \overline{v}(A_2) = 1$
$\implies A_1 \in S \wedge A_2 \in S$

v je model pre S a teda aj pre T.

2. Zostáva nám nájsť množinu formúl S požadovaných vlastností. Na základe cvičenia sa môžeme presvedčiť, že existuje prosté zobrazenie množiny formúl výrokovej logiky na množinu $\mathbb{N}$. Takému zobrazeniu hovoríme enumerácia.
$A_0, A_1 \ldots$ mám zobrazenie formúl výrokovej logiky
$e(A_i) \to i$, e – enumerácia

$$\begin{aligned}
S_0 &= T \\
&\vdots \\
S_{i+1} &= \begin{cases} S_i \cup \{A_i\}, \text{ ak každá konečná podmnožina množiny } S_i \cup \{A_i\} \text{ je splniteľná} \\ S_i \cup \{\neg A_i\}, \text{ v opačnom prípade} \end{cases} \\
&\vdots \\
S &= \bigcup_{i \geq 0} S_i, \text{týmto sme získali množinu } S
\end{aligned}$$

Stačí ukázať, že spĺňa tie tri vlastnosti – platia, vyplýva to z konštrukcie S.

□

Dôsledok 4.3.2. *Ak je T množina formúl výrokovej logiky a A formula výrokovej logiky, potom:*
$T \models A \leftrightarrow T' \models A$ pre nejakú konečnú podmnožinu $T' \subseteq T$.

Dôkaz. Nech T je splniteľná množina formúl, potom $T \models A \leftrightarrow T \cup \{\neg A\}$ je splniteľná.
Nech v je model T, $\overline{v}(A) = 1 \to \overline{v}(\neg A) = 0 \to T \cup \{\neg A\}$ je splniteľná.
…teda aj obrátene :)

$T \cup \{\neg A\}$ – nesplniteľná množina, podľa vety o kompaktnosti, $\exists T_0 \subseteq T \cup \{\neg A\}$.
T_0 – konečná a nesplniteľná

nesplniteľná – $T_0 = T' \cup \{\neg A\} \leftrightarrow T' \models A, \quad T' = T_0 \setminus \{\neg A\}$

□

4.4 Grafy

Def 4.4.1. *Usporiadanú dvojicu (V, R) nazývame grafom, keď:*
V – množina vrcholov
R – binárna operácia na množine V
$R \subseteq V \times V$

R – je symterická a antireflexívna

$(\forall x)(\forall y)$	$(xRy \rightarrow yRx)$	*symetrickosť, neorientovaný*
	$((x,y) \in R \rightarrow (y,x) \in R)$	
$(\forall x)$	$\neg(xRx)$	*antireflexívnosť, nie sú tam slučky*
	$((x,x) \notin R)$	

Def 4.4.2. *Graf (V', R') je podgraf grafu (V, R), ak platí:*

$$V' \subseteq V \wedge R' \subseteq \{(x,y) | x \in V' \wedge y \in V' \wedge (xRy)\}$$

Def 4.4.3. *Regulárnym vrcholovím zafarbením grafu (V, R) n-farbami, nazývame zobrazenie $h : V \rightarrow \{1 \dots n\}$*

$$(\forall x)(\forall y)(xRy \rightarrow h(x) \neq h(y))$$

Príklad. Uvažujme tvrdenie: ak má každý konečný podgraf grafu (V, R) regulárne zafarbenie n-farbami, potom aj pre celý graf (V, R) existuje regulárne zafarbenie n-farbami.

Prevedieme uvedené tvrdenie na *vetu o kompaktnosti* vo výrokovej logike. Majme teda daný graf (V, R), potrebujeme zvoliť T – množinu výrokových formúl, dokonca zvolíme aj množinu P – prvotných formúl.

$P = \{p_{x,i} | x \in V \wedge 1 \leq i \leq n\}$ každá dvojica (x, i)
x – vrchol grafu, i – farba
$p_{x,i}$ reprezentuje tvrdenie, že vrcholu x je priradená farba i

T – zvolme zjednotenie nad množinou výrokových formúl:

$\{p_{x,1} \cup \dots \cup p_{x,n}, x \in V\}$, každý vrchol má farbu
$\{p_{x,i} \rightarrow \neg p_{x,j}, i \neq j\}$, ale len jednu
$\{p_{x,i} \rightarrow \neg p_{y,i}, xRy\}$, susedné vrcholy majú rôzne farby

v je ohodnotenie prvotných formúl, ktoré je model pre množinu T
h takto: $h(x) = i,\ v_{x,i} = 1$

Poznámka. Predpokladajme, že T je množina, ktorej graf má uzavreté podmnožiny intervalu $\langle 0, 1\rangle$ – toto chápeme ako podmnožinu $\mathbb{R}$

Ak má každý konečne veľa prvkov z T neprázdny prienik (t.j. $\cap F \neq \emptyset$, F je konečná podmnožina T, $F \subseteq T$). Potom existuje aspoň jedno reálne číslo $\cap T \neq \emptyset$

uzavretá podmnožina intervalu $\langle 0, 1\rangle$	– výroková formula
množina uzavretých množín	– množina výrokových formúl
prienik množiny je neprázdny	– množina je splniteľná

4.5 Formálny systém

- všetko pomocou $\neg$ a $\rightarrow$

$$\begin{aligned} A \wedge B &\iff \neg(A \rightarrow \neg B) \\ A \vee B &\iff (\neg A \rightarrow B) \\ A \leftrightarrow B &\iff (A \rightarrow B) \wedge (B \rightarrow A) \\ &\iff \neg((A \rightarrow B) \rightarrow \neg(B \rightarrow A)) \end{aligned}$$

Hilbert a Göntzen

Def 4.5.1.

1. *Hovoríme, že konečná postupnosť formúl $A_1, \dots A_n$ je odvodením (dôkazom) formuly A, ak A_n je formula A a pre ľubovoľné $i \leq n$, každá fomula A_i je buď axióma alebo vyplýva z predchádzajúcich formúl pomocou niektorých pravidiel odvodenia.*
2. *Ak existuje dôkaz (odvodenie) formuly A, hovoríme, že formula A je dokazateľná (odvoditeľná), nazývame ju teorémou.* $\vdash A$

Def 4.5.2. *Formálny systém výrokovej logiky pozostáva z nasledovných troch zložiek:*

1. *jazyk tvoria:*

   množina P – prvotných formúl

   symboly pre logické spojky – $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$

   pomocné symboly – zátvorky

2. *axiómy: Formulujeme tri schémy pre ľubovoľné formuly A, B, C. Každá z nasledujúcich schém je axióma výrokovej logiky.*

   (A1) $A \rightarrow (B \rightarrow A)$

   (A2) $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$

   (A3) $(\neg B \rightarrow \neg A) \rightarrow (A \rightarrow B)$

3. *pravidlo odvodenia máme: pravdilo modus ponens, MP* $\frac{A; A \rightarrow B}{B}$

Korektnosť pravidla MP, každá axióma je tautológia: $\overline{v}(A) = 1 \wedge \overline{v}(A \rightarrow B) = 1 \implies \overline{v}(B) = 1$

Teoréma 1. $\vdash A \rightarrow A$

Dôkaz.

1.	$\vdash A \rightarrow ((A \rightarrow A) \rightarrow A)$	$(A1)$
2.	$\vdash (A \rightarrow ((A \rightarrow A) \rightarrow A)) \rightarrow ((A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A))$	$(A2)$
3.	$\vdash (A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A)$	$(1)(2)(MP)$
4.	$\vdash A \rightarrow (A \rightarrow A)$	$(A1)$
5.	$\vdash A \rightarrow A$	$(3)(4)(MP)$

$\square$

Veta, ktorá umožňuje prejsť od dôkazu nejakej formuly k dôkazu inej formuly bez toho, že by sme ten dôkaz konštruovali.

Def 4.5.3. *Nech T je množina formúl výrokovej logiky, $A_1, \ldots, A_n$ sú formuly výrokovej logiky. Hovorím, že postupnosť formúl $A_1, \ldots, A_n$ je dôkazom formuly A s predpokladom T, ak A_n je formula A a pre ľubovoľné $i \leq n$, je A_i buď axióma, buď formula z T alebo A_i dostaneme z formúl $A_1, \ldots, A_{i-1}$ pomocou pravidiel odvodenia. Hovoríme, že A je dokazateľná (odvotieľná) z množiny T a píšeme $T \vdash A$, ak existuje dôkaz (odvodenie) z predpokladov T, číslo n nazývame dĺžkou odvodenia.*

Veta 4.5.1. *O dedukcii (VD). Nech T je množina formúl výrokovej logiky a A, B sú formuly výrokovej logiky. Potom* $T \vdash A \rightarrow B \iff T, A \vdash B,\ (T \cup \{A\} \vdash B)$

Dôkaz.

„$\Rightarrow$“ $T \vdash A \rightarrow B$

$A_1, \ldots, A_{n-1}, A \rightarrow B$, odvodenie z predpokladov T

$A, A_1, \ldots, A_{n-1}, A \rightarrow B, \underline{B}$

„$\Leftarrow$“ $T, A \vdash B$

Indukciou vzhľadom na dĺžku odvodenia formuly B z predpokladov $T \cup \{A\}$.

1° $n = 1$, hneď to dostaneme

- $a)$ formula B je A, $(\vdash A \rightarrow A) \implies (T \vdash A \rightarrow A)$
- $b)$ formula $B \in T$, $T \vdash B$, $T \vdash B \rightarrow (A \rightarrow B)$ (A1) $\implies (MP)\ T \vdash A \rightarrow B$
- $c)$ B je axióma, $\vdash B$, $T \vdash B$, $T \vdash B \rightarrow (A \rightarrow B) \implies T \vdash A \rightarrow B$

2° IP – nech tvrdenie platí úre $n < s$

nech $n = s$

$B_1, \ldots, B_s = B$ – odvodenie (dôkaz) formuly B z predpokladov T, A.

$$B \text{ môže byť tvaru} \begin{cases} a) & B \text{ je } A \\ b) & B \in T \\ c) & B \text{ je axióma} \\ d) & B \text{ sa dostala z dôkazu pomocou formúl } B_i, B_j, \text{ pričom } i, j < s \text{ pomocou MP.} \end{cases}$$

a), b), c) – sa dokazujú ako v 1°

d) B_i, B_j; $B_j = B_i \rightarrow B$
na B_i, B_j sa vzťahuje IP:

$$T, A \vdash B_i \implies T \vdash A \rightarrow B_i$$
$$T, A \vdash B_j \implies T \vdash A \rightarrow B_j$$

1. $T \vdash A \rightarrow (B_i \rightarrow B)$
2. $T \vdash (A \rightarrow (B_i \rightarrow B)) \rightarrow ((A \rightarrow B_i) \rightarrow (A \rightarrow B))$ $(A2)$
3. $T \vdash (A \rightarrow B_i) \rightarrow (A \rightarrow B)$
4. $T \vdash A \rightarrow B_i$
5. $T \vdash A \rightarrow B$

□

Poznámka.
$\vdash B$
A je ľubovoľná formula výrokovej logiky

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

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

$A \rightarrow (B \rightarrow C)$
$T \vdash A \rightarrow (B \rightarrow C) \iff T, A, B \vdash C$ – nezáleží na poradí $(B \rightarrow (A \rightarrow C))$
$\vdash A \rightarrow (B \rightarrow C) \iff A, B \vdash C$

Teoréma 2. $\vdash \neg A \rightarrow (A \rightarrow B), \vdash A \rightarrow (\neg A \rightarrow B)$

Dôkaz.

1.		$\vdash \neg A \rightarrow (\neg B \rightarrow \neg A)$	$(A1)$
2.	$\neg A$	$\vdash \neg B \rightarrow \neg A$	(VD)
3.		$\vdash (\neg B \rightarrow \neg A) \rightarrow (A \rightarrow B)$	$(A3)$
4.	$\neg A$	$\vdash A \rightarrow B$	(2)(3)(MP)
5.		$\vdash \neg A \rightarrow (A \rightarrow B)$	(VD)

□

Teoréma 3. $\vdash \neg\neg A \rightarrow A$

Dôkaz.

1.		$\vdash \neg\neg A \rightarrow (\neg A \rightarrow \neg\neg\neg A)$	$(T2)$
2.	$\neg\neg A$	$\vdash \neg A \rightarrow \neg\neg\neg A$	(VD)
3.		$\vdash (\neg A \rightarrow \neg\neg\neg A) \rightarrow (\neg\neg A \rightarrow A)$	$(A3)$
4.	$\neg\neg A$	$\vdash \neg\neg A \rightarrow A$	(2)(3)(MP)
5.	$\neg\neg A$	$\vdash A$	(VD)
6.		$\vdash \neg\neg A \rightarrow A$	(VD)

□

Poznámka. ET: „to sa nesčituje ako jaternice“

Lema 1.

T4 $\vdash A \to \neg\neg A$

T5 $\vdash (A \to B) \to (\neg B \to \neg A)$

T6 $\vdash A \to (\neg B \to \neg(A \to B))$

T7 $\vdash (\neg A \to A) \to A$

Dôkaz.

T4

1.		$\vdash \neg\neg\neg A \to \neg A$	$(T3)$
2.		$\vdash (\neg\neg\neg A \to \neg A) \to (A \to \neg\neg A)$	$(A3)$
3.		$\vdash A \to \neg\neg A$	$(1)(2)(MP)$

$\square$

T5

1.		$\vdash \neg\neg A \to A$	$(T3)$
2.	$A \to B, \neg\neg A$	$\vdash A$	
3.	$A \to B, \neg\neg A$	$\vdash B$	
4.	$A \to B, \neg\neg A$	$\vdash \neg\neg B$	$(T4)(3)(MP)$
5.	$A \to B$	$\vdash \neg\neg A \to \neg\neg B$	(VD)
6.		$\vdash (\neg\neg A \to \neg\neg B) \to (\neg B \to \neg A)$	$(A3)$
7.	$A \to B$	$\vdash \neg B \to \neg A$	$(5)(6)(MP)$
8.		$\vdash (A \to B) \to (\neg B \to \neg A)$	(VD)

$\square$

T6

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

$\square$

T7

1.		$\vdash \neg A \to (\neg A \to \neg(\neg A \to A))$	$(T6)$
2.	$\neg A$	$\vdash \neg(\neg A \to A)$	$(VD, 2\times)$
3.		$\vdash \neg A \to \neg(\neg A \to A)$	(VD)
4.		$\vdash (\neg A \to \neg(\neg A \to A)) \to ((\neg A \to A) \to A)$	$(A3)$
5.		$\vdash (\neg A \to A) \to A$	$(3)(4)(MP)$

$\square$

T7 iný dôkaz, aby ste videli, že existujú rôzne dôkazy toho istého :)

1.	$\neg A, \neg A \to A$	$\vdash A$	(MP)
2.	$\neg A$	$\vdash (\neg A \to A) \to A$	(VD)
3.		$\vdash ((\neg A \to A) \to A) \to (\neg A \to \neg(\neg A \to A))$	$(T5)$
4.	$\neg A$	$\vdash \neg A \to \neg(\neg A \to A)$	$(2)(3)(MP)$
5.	$\neg A$	$\vdash \neg(\neg A \to A)$	(VD)
6.		$\vdash \neg A \to \neg(\neg A \to A)$	(VD)
7.		$\vdash (\neg A \to \neg(\neg A \to A)) \to ((\neg A \to A) \to A)$	$(A3)$
8.		$\vdash (\neg A \to A) \to A$	(MP)

$\square$

$\square$

Lema 2. *O neutrálnej formule. Ak T je množina formúl výrokovej logiky a A, B sú formuly výrokovej logiky. Ak $T, A \vdash B$ a $T, \neg A \vdash B$ potom $T \vdash B$.*

Dôkaz.

$T, \neg A$	$\vdash B$	(predpoklad 2)
T	$\vdash \neg A \to B$	(VD)
	$\vdash (\neg A \to B) \to (\neg B \to \neg\neg A)$	$(A3)$
T	$\vdash \neg B \to \neg\neg A$	(MP)
$T, \neg B$	$\vdash \neg\neg A$	(VD)
$T, \neg B$	$\vdash A$	$(T3)$ $(*)$
T, A	$\vdash B$	(predpoklad 1)
T	$\vdash A \to B$	(VD) $(**)$
$T, \neg B$	$\vdash B$	$(*)(**)(MP)$
T	$\vdash \neg B \to B$	(VD)
	$\vdash (\neg B \to B) \to B$	$(T7)$
T	$\vdash B$	(2 predošlé)(MP)

□

Def 4.5.4. *Nech v je valuácia, B je ľubovoľná formula. B^v označuje formulu B ak $\overline{v}(B) = 1$, formulu $\neg B$ ak $\overline{v}(B) = 0$.*

Lema 3. *Nech v je valuácia a nech všetky prvotné komponenty formuly A sú $p_1, \ldots p_n$. Potom:*

$$p_1^v, \ldots, p_n^v \vdash A^v$$

Dôkaz. Indukciou vzhľadom na zložitosť formuly A.

1° p_i
$p_i^v \vdash p_i^v$

2° A je tvaru $\neg B$ alebo $C \to D$. Na B, C, D sa vzťahuje IP.

$\neg B$

pre B je tvrdenie už dokázané, platí:

1. $\overline{v}(B) = 0 \implies B^v$ je $\neg B$ (to je A)
   počítajme $A^v = (\neg B)^v$, $\overline{v}(\neg B) = 1 \implies A^v$ je A
   platí toto: $p_1^v, \ldots, p_n^v \vdash B^v \implies p_1^v, \ldots, p_n^v \vdash A^v$, $(\overline{v}(B) = 0)$
   $\neg B, A, A^v$ je A
2. $\overline{v}(B) = 1 \implies B^v$ je B
   $p_1^v, \ldots, p_n^v \vdash B$
   použijeme $T4$: $\vdash B \to \neg\neg B$
   $p_1^v, \ldots, p_n^v \vdash \neg\neg B$
   A je $\neg B$, $\overline{v}(B) = 1 \implies \overline{v}(\neg B) = 0$
   $(\neg B)$ je A^v, lebo $(\neg B)^v$ je $\neg\neg B$ a to je A^v
   $p_1^v, \ldots, p_n^v \vdash A^v$

$C \to D$

1. $\overline{v}(C) = \overline{v}(D) = 1$
   D^v je D, C^v je C, $\overline{v}(C \to D) = 1$, $(C \to D)^v$ je $\overline{v}(C) \to \overline{v}(D)$
   $A1$: $\vdash D \to (C \to D)$
   $p_1^v, \ldots, p_n^v \vdash C \to D$
   $(C \to D)^v$ je $(C \to D)$ a to je A^v
2. $\overline{v}(C) = 1$, $\overline{v}(D) = 0$
   C^v je C, D^v je $\neg D$
   A^v, $(C \to D)^v$ $\overline{v}(C \to D)$ je $\overline{v}(C) \to \overline{v}(D) = 0$
   $\neg(C \to D)$

$p_1^v, \dots, p_n^v \vdash C$
$p_1^v, \dots, p_n^v \vdash \neg D$
$T6$: $\vdash C \rightarrow (\neg D \rightarrow \neg(C \rightarrow D))$
$p_1^v, \dots, p_n^v \vdash \neg(C \rightarrow D)$ a to je A^v (MP).

3. $\overline{v}(C) = 0 \wedge \overline{v}(D) = 0$
$\overline{v}(C) = 0 \wedge \overline{v}(D) = 1$
C^v je $\neg C$, D^v je $\neg D$
$p_1^v, \dots, p_n^v \vdash \neg C$
$p_1^v, \dots, p_n^v \vdash \neg D$
$(C \rightarrow D)^v$ je $C \rightarrow D$
$\overline{v}(C \rightarrow D) = \overline{v}(C) \rightarrow \overline{v}(D) = 1$
$T2$: $\vdash \neg C \rightarrow (C \rightarrow D)$
MP a je to (ale nie ako v tom seriáli :).

□

4.6 Postove vety, bezospornosť výrokovej logiky, úplnosť

Slabá forma vety o úplnosti

Veta 4.6.1. *Post. Pre ľubovoľnú formulu A výrokovej logiky platí:*

$$\vdash A \leftrightarrow \models A$$

Dôkaz.

„⇒“ – stačí preveriť, že všetky axiómy sú tautológie
– že pravidlo odvodenia MP je korektné v tom zmysle, že ak ho aplikujeme na tautológiu, tak odvodená formula bude tautológia

zoberme $A2$: $\vdash \underbrace{(A \rightarrow (B \rightarrow C))}_{1} \rightarrow \underbrace{((A \rightarrow B) \rightarrow (A \rightarrow C))}_{0}$

$\Longrightarrow$ keď $\overline{v}(A \rightarrow C) = 0 \quad \Longrightarrow \quad \overline{v}(A) = 1 \wedge \overline{v}(C) = 0$
$\overline{v}(A \rightarrow B) = 1 \quad \Longrightarrow \quad \overline{v}(A) = 1 \wedge \overline{v}(B) = 1$

$\Longrightarrow \quad A \rightarrow (B \rightarrow C) \neq 1 \quad \Longrightarrow$ je to tautológia

obdobne pre všetky axiómy

korektnosť MP: $\frac{A, A \rightarrow B}{B}$
$\overline{v}(A) = 1 \wedge \overline{v}(A \rightarrow B) = 1 \Longrightarrow \overline{v}(B) = 1$, pre ľubovoľnú valuáciu

„⇐“ nech $p_1, \dots, p_n$ sú všetky prvotné formuly v A
z $L3$ platí $p_1^v, \dots, p_n^v \vdash A$, $\overline{v}(A) = 1$ (lebo je to tautológia) $\Longrightarrow$

$$\left.\begin{array}{lcl} p_1^v, \dots, p_{n-1}^v, p_n^v & \vdash & A \\ p_1^v, \dots, p_{n-1}^v, \neg p_n^v & \vdash & A \end{array}\right\} \text{lema o neutrálnej formule} \Longrightarrow p_1^v, \dots, p_{n-1}^v \vdash A$$

použijeme to n-krát a dostaneme $\vdash A$

□

Def 4.6.1. *Hovoríme, že formálny systém je sporný, ak každá jeho formula je dokazateľná, v opačnom prípade hovoríme, že formálny systém je bezosporný.*

Def 4.6.2. *Ak je T množina formúl nejakého formálneho systému, tak hovoríme, že T je sporná ak je každá formula uvažovaného formálneho systému dokazateľná z predpokladov T. Ináč je T bezosporná.*

Poznámka. Sémantický ekvivalent pojmu bezospornosti množiny formúl je pojem splniteľnosti množiny formúl.

Dôsledok 4.6.2. *Postovej vety. Množina formúl výrokovej logiky je bezosporná práve vtedy, keď je splniteľná.*

Dôkaz.

„⇒“ existuje ohodnotenie v– model pre T, $\overline{v}(A) = 1\ \forall A \in T$
nejaké B dokazateľné z T, $\overline{v}(B) = 1$ a z korektnosti MP
treba nájsť kontradikciu B, $\overline{v}(B) = 0\ \forall v$ – toto stačí

„⇐“ existuje konečná podmnožina formúl (podľ VK) $\{A_1, \dots, A_n\} \subseteq T$, ktorá nie je splniteľná

$\neg A_1 \vee \cdots \vee \neg A_n$ je splniteľná pre $\forall v$, označme ju B
B je tautológia a je dokazateľná vo výrokovej logike
$A_1 \wedge \cdots \wedge A_n$ (z *de Morgana* → je to negácia toho predošlého), $\neg B$

$$\begin{array}{lll} T & \vdash B & \\ T & \vdash \neg B & \\ & \text{nech } C \text{ je ľubovoľná formula} & \\ & \vdash \neg B \rightarrow (B \rightarrow C) & (T2) \\ T & \vdash C & (MP, 2\times) \end{array}$$

□

Silná forma vety o úplnosti

Veta 4.6.3. *Nech T je ľubovoľná množina formúl výrokovej logiky a A je formula výrokovej logiky. Potom platí:*

$$T \models A \leftrightarrow T \vdash A$$

Dôkaz.

„⇒“ $T \models A$, podľa dôsledku VK, že existuje konečná podmnožina $T_0 \subseteq T$
$T_0 = \{A_1, \dots, A_n\}$, $T_0 \models A$ (A je tautologický dôsledok T_0)
$T_0 \models A \iff \models (A_1 \rightarrow (A_2 \rightarrow \dots (A_n \rightarrow A) \dots))$
buď indukciou cez n alebo priamo
nech v je model T_0 ($\overline{v}(A) = 1$), všetky implikácie sú pravdivé
$T_0 \models A \implies \models (A_1 \rightarrow \dots (A_n \rightarrow A) \dots)$
a keď v nie je model $\implies$ aspoň pre jedno A_i, $\overline{v}(A_i) = 0$, je to opäť tautológia
$T \models A \implies T_0 \models A \iff \models (A_1 \rightarrow \dots (A_n \rightarrow A) \dots)$
$\vdash A_1 \rightarrow (A_2 \rightarrow \dots (A_n \rightarrow A) \dots)$
použijeme VD n-krát $\implies A_1, \dots, A_n \vdash A \implies T \vdash A$

„⇐“ $A_1, \dots, A_n = A$
A_i je buď axióma, formula z T ...

$$\left.\begin{array}{l} \overline{v}(B) = 1 \\ B \in T \end{array}\right\} \implies \overline{v}(A) = 1$$

□

Poznámka. Výroková logika je rozhodnuteľná a predikátová logika nie je rozhodnuteľná.

Lema 4.

T8 $A \wedge B \vdash A,\ A \wedge B \vdash B$

T9 $A, B \vdash A \wedge B$

Dôkaz.

T8 $A \wedge B \iff \neg(A \to \neg B)$

$$\begin{array}{rll}
 & \vdash \neg A \to (A \to \neg B) & (T2) \\
 & \vdash (\neg A \to (A \to \neg B)) \to (\neg(A \to \neg B) \to \neg\neg A) & (T5) \\
 & \vdash \neg(A \to \neg B) \to \neg\neg A & (T2)(T5)(MP) \\
\neg(A \to \neg B) & \vdash \neg\neg A & (VD) \\
 & \vdash \neg\neg A \to A & (T3) \\
\neg(A \to \neg B) & \vdash A & (\text{2 predošlé})(MP) \\
A \wedge B & \vdash A & (\text{prepis } \wedge) \\
\hline
\end{array}$$

$$\begin{array}{rll}
 & \vdash \neg B \to (A \to \neg B) & (A1) \\
 & \vdash (\neg B \to (A \to \neg B)) \to (\neg(A \to \neg B) \to \neg\neg B) & (T5) \\
 & \vdash \neg(A \to \neg B) \to \neg\neg B & (A1)(T5)(MP) \\
\neg(A \to \neg B) & \vdash \neg\neg B & (VD) \\
 & \vdash \neg\neg B \to B & (T3) \\
\neg(A \to \neg B) & \vdash B & (\text{2 predošlé})(MP) \\
A \wedge B & \vdash B & (\text{prepis } \wedge)
\end{array}$$

□

T9

$$\begin{array}{rll}
A, B & \vdash \neg\neg B & (T4) \\
 & \vdash A \to (\neg\neg B \to \neg(A \to \neg B)) & (T6) \\
A, \neg\neg B & \vdash \neg(A \to \neg B) & (VD, 2\times) \\
A, B & \vdash A \wedge B & (T3)(\text{prepis } \wedge)
\end{array}$$

□

□

Dôsledok 4.6.4. $(A \leftrightarrow B) \leftrightarrow ((A \to B) \wedge (B \to A))$

1. $A \leftrightarrow B \vdash A \to B$
2. $A \leftrightarrow B \vdash B \to A$
3. $A \to B, B \to A \vdash (A \to B) \wedge (B \to A)$
4. *ak* $\vdash A \leftrightarrow B$, *tak* $T \vdash A \iff T \vdash B$

Dôkaz. 1, 2, 3 sú triviálne záležitosti

4. $\vdash A \leftrightarrow B$
   $\vdash A \to B, \quad T \vdash A \implies T \vdash B$
   $\vdash B \to A, \quad T \vdash B \implies T \vdash A$
   $T \vdash A \iff T \vdash B$

□

Dôsledok 4.6.5.

1. $\vdash (A \wedge B) \leftrightarrow (B \wedge A)$
2. $\vdash ((A \wedge B) \wedge C) \leftrightarrow (A \wedge (B \wedge C))$
3. $\vdash (A_1 \to \dots (A_n \to B) \dots) \leftrightarrow ((A_1 \wedge \dots \wedge A_n) \to B)$

Dôkaz.

1.
$$\begin{array}{rcl} A \wedge B & \vdash & A, B \\ A \wedge B & \vdash & B \wedge A \\ \vdash (A \wedge B) & \to & (B \wedge A) \end{array} \qquad \begin{array}{rcl} B \wedge A & \vdash & A, B \\ B \wedge A & \vdash & A \wedge B \\ \vdash (B \wedge A) & \to & (A \wedge B) \end{array}$$

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

2. analogicky
$(A \wedge B) \wedge C \vdash (A \wedge B), C \qquad (A \wedge B) \wedge C \vdash A, B, C$
$A, B, C \vdash A \wedge (B \wedge C)$
$\vdash (A \wedge B) \wedge C \to A \wedge (B \wedge C)$
druhá implikácia obdobne

3. len myšlienka
$A_1 \wedge \cdots \wedge A_n,\ A \to (A_2 \to \ldots (A_n \to B) \ldots) \vdash B$ $\quad n$-násobným použitím MP
$A_1, \ldots, A_n$
$A_1 \to \ldots (A_n \to B) \vdash (A_1 \wedge \cdots \wedge A_n) \to B$
$\underline{\vdash (A_1 \to \ldots (A_n \to B)) \to ((A_1 \wedge \cdots \wedge A_n) \to B)}$ $\quad (VD)$

$A_1, \ldots, A_n, (A_1 \wedge \cdots \wedge A_n) \to B \vdash B$ $\quad$ (jasné :) MP)
$(A_1 \wedge \cdots \wedge A_n) \to B \vdash A_1 \to (\ldots (A_n \to B) \ldots)$
$\underline{\vdash ((A_1 \wedge \cdots \wedge A_n) \to B) \to (A_1 \to (\ldots (A_n \to B) \ldots))}$

$\square$

Veta 4.6.6. *O ekvivalentnej zámene. Nech fomula A' vznikne z formuly A nahradením niektorých podformúl $A_1, \ldots, A_n$ formulami $A'_1, \ldots, A'_n$. Keď platí $\vdash A_i \iff \vdash A'_i$ pre $i = \overline{1, n}$, potom $\vdash A \leftrightarrow A'$.*

Dôkaz. Indukciou podľa zložitosti formuly A.

1° A je prvotná formula
A je niektoré z podformúl $A_1, \ldots, A_n$
A je p, z $T1 : \vdash p \to p$ dostávame: $\vdash p \leftrightarrow p$
$\vdash A_i \leftrightarrow A'_i$ z IP

2° A je tvaru $\neg B$ alebo $B \to C$. Na B, C sa vzťahuje IP.

$\neg B$

$\vdash B \leftrightarrow B'$ // nahradené, nie negácia

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

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

$\vdash \neg B' \to \neg B$
$\vdash \neg B \to \neg B'$

$\vdash A \leftrightarrow A'$

$B \to C$

$$\begin{array}{rll}
 & \vdash B \leftrightarrow B' & \\
 & \vdash B \to B' & \\
 & \vdash B' \to B & \\
 & & \\
 & \vdash C \leftrightarrow C' & \\
 & \vdash C \to C' & \\
 & \vdash C' \to C & \\
 & & \\
B', B' \to B, B \to C, C \to C' & \vdash C' & (MP) \\
B' \to B, B \to C, C \to C' & \vdash B' \to C' & (VD) \\
B' \to B, C' \to C & \vdash (B \to C) \to (B' \to C') & \\
 & \vdash (B \to C) \to (B' \to C') & \\
 & \vdash A \to A' &
\end{array}$$

dôkaz $\vdash A' \to A$ je analogický

□

Lema 5. *de Morganove pravidlá (DM).*

1. $\vdash \neg(A \wedge B) \leftrightarrow (\neg A \vee \neg B)$
2. $\vdash \neg(A \vee B) \leftrightarrow (\neg A \wedge \neg B)$

Dôkaz.

1.
$$\begin{array}{rlll}
\vdash \neg(A \wedge B) & \leftrightarrow & \neg\neg(A \to \neg B) & \\
 & \leftrightarrow & \neg\neg A \to \neg B & \\
 & \leftrightarrow & \neg A \vee \neg B & ((A \vee B) \leftrightarrow (\neg A \to B))
\end{array}$$

2.
$$\begin{array}{rlll}
\vdash \neg(A \vee B) & \leftrightarrow & \neg(\neg A \to B) & \\
 & \leftrightarrow & \neg(\neg A \to \neg\neg B) & \\
 & \leftrightarrow & \neg A \wedge \neg B & ((A \wedge B) \leftrightarrow \neg(A \to \neg B))
\end{array}$$

□

Dôsledok 4.6.7.

1. $\vdash A \to (A \vee B), \vdash B \to (A \vee B)$
2. $\vdash (A \vee B) \leftrightarrow (B \vee A)$
3. $\vdash (A \vee (B \vee C)) \leftrightarrow ((A \vee B) \vee C)$

Dôkaz.

1. týmto dôkazom som si nie istý, v zošite mám nejaký xaos, takže kto to má, nex ma opraví
   $A \wedge B \vdash A,\ \ A \wedge B \vdash B$
   $\neg A \wedge \neg B \vdash \neg A$
   $\neg A \wedge \neg B \vdash \neg B$
   $\vdash (\neg A \wedge \neg B) \to \neg A$
   $\vdash (\neg A \wedge \neg B) \to \neg B$
   $\vdash (A \to B) \to (\neg A \to \neg B)$
   $\vdash \neg\neg A \to \neg(\neg A \wedge \neg B) \Longleftrightarrow \vdash A \to (A \vee B) \qquad (MP)$

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

2. $(\neg A \wedge \neg B) \vdash (\neg B \wedge \neg A)$ $(VD)(T5)(T3)(T4)$ a postupujem rovnako[1]

3. $(\neg A \wedge (\neg B \wedge \neg C)) \vdash ((\neg A \wedge \neg B) \wedge \neg C)$ $(VD)(T5)(T3)(T4)$ a postupujem rovnako[2]

□

Veta 4.6.8. *O dôkaze rozborov prípadov (DRP). Nech T je množina formúl výrokovej logiky a A, B, C sú formuly výrokovej logiky. Potom:*

$$T, (A \vee B) \vdash C \iff T, A \vdash C \wedge T, B \vdash C$$

Dôkaz.

„⇒“ $T, A \vee B \vdash C$

$A \vdash A \vee B \quad (DM \to D1)$

$T, A \vdash A \vee B \implies T, A \vdash C$

$B \vdash A \vee B \quad (DM \to D1)$

$T, B \vdash A \vee B \implies T, B \vdash C$

„⇐“ $T, A \vdash C \wedge T, B \vdash C$

$$\begin{array}{rcll}
T & \vdash & A \to C & \\
T & \vdash & B \to C & \\
T & \vdash & (A \to C) \to (\neg C \to \neg A) & (T5) \\
T & \vdash & (B \to C) \to (\neg C \to \neg B) & (T5) \\
T & \vdash & \neg C \to \neg A & (MP) \\
T & \vdash & \neg C \to \neg B & (MP) \\
T, \neg C & \vdash & \neg A & (VD) \\
T, \neg C & \vdash & \neg B & (VD) \\
T, \neg C & \vdash & \neg A \wedge \neg B & \text{(predošlé dve)} \\
T, \neg C & \vdash & \neg(A \vee B) & (DM) \\
T & \vdash & \neg C \to \neg(A \vee B) & (VD) \\
T & \vdash & (\neg C \to \neg(A \vee B)) \to (\neg\neg(A \vee B) \to \neg\neg C) & \\
T & \vdash & \neg\neg(A \vee B) \to \neg\neg C & \\
T & \vdash & (A \vee B) \to C & \\
T, A \vee B & \vdash & C &
\end{array}$$

□

Dôsledok 4.6.9. *Distributívnosť* $\vee$, $\wedge$.

1. $\vdash (A \vee (B \wedge C)) \leftrightarrow ((A \vee B) \wedge (A \vee C))$

2. $\vdash (A \wedge (B \vee C)) \leftrightarrow ((A \wedge B) \vee (A \wedge C))$

[1] ak niekto xce, tak mi to može poslať a pridám to sem

[2] ak niekto xce, tak mi to može poslať a aj toto sem pridám

Dôkaz.

1. „$\Rightarrow$“

$$
\begin{array}{rll}
 & \vdash & A \rightarrow (A \vee B) \\
 & \vdash & A \rightarrow (A \vee C) \\
A & \vdash & A \vee B \\
A & \vdash & A \vee C \\
A & \vdash & (A \vee B) \wedge (A \vee C) \qquad \text{(predošlé dve)} \\
B \wedge C & \vdash & B \\
B \wedge C & \vdash & C \\
 & \vdash & B \rightarrow (B \vee A) \\
 & \vdash & C \rightarrow (C \vee A) \\
B \wedge C & \vdash & A \vee B \\
B \wedge C & \vdash & A \vee C \\
B \wedge C & \vdash & (A \vee B) \wedge (A \vee C) \\
A \vee (B \wedge C) & \vdash & (A \vee B) \wedge (A \vee C) \qquad (DRP) \\
 & \vdash & (A \vee (B \wedge C)) \rightarrow ((A \vee B) \wedge (A \vee C)) \qquad \text{//ešte obrátene :)}
\end{array}
$$

„$\Leftarrow$“

$$
\begin{array}{rll}
(A \vee B) \wedge (A \vee C) & \vdash & A \vee B \\
(A \vee B) \wedge (A \vee C) & \vdash & A \vee C \\
 & & A \vee B \Longleftrightarrow \neg A \rightarrow A \\
 & & A \vee C \Longleftrightarrow \neg A \rightarrow C \\
A \vee B, \neg A & \vdash & B \\
A \vee C, \neg A & \vdash & C \\
(A \vee B) \wedge (A \vee C), \neg A & \vdash & B \wedge C \\
(A \vee B) \wedge (A \vee C) & \vdash & \neg A \rightarrow (B \wedge C) \\
(A \vee B) \wedge (A \vee C) & \vdash & A \vee (B \wedge C) \\
 & \vdash & ((A \vee B) \wedge (A \vee C)) \rightarrow (A \vee (B \wedge C))
\end{array}
$$

2. „$\Rightarrow$“ na základe 1. platí:

$$
\begin{array}{ll}
\vdash & (\neg A \vee (\neg B \wedge \neg C)) \leftrightarrow ((\neg A \vee \neg B) \wedge (\neg A \vee \neg C)) \\
\vdash & (\neg A \vee (\neg B \wedge \neg C)) \rightarrow ((\neg A \vee \neg B) \wedge (\neg A \vee \neg C)) \\
\vdash & \neg((\neg A \vee \neg B) \wedge (\neg A \vee \neg C)) \rightarrow \neg(\neg A \vee (\neg B \wedge \neg C)) \qquad (T5) \\
\vdash & ((A \wedge B) \vee (A \wedge C)) \rightarrow (A \wedge (B \vee C)) \qquad (DM)
\end{array}
$$

„$\Leftarrow$“ úplne analogicky

$\square$

4.7 Konjunktívny a disjunktívny normálny tvar

Def 4.7.1. *Literál je prvotná formula alebo jej negácia.*

Veta 4.7.1. *Každá formula A výrokovej logiky je ekvivalentná istej formule $A_1 \wedge \cdots \wedge A_n$ (1), kde každá A_i, $i = 1, \ldots, n$ je disjunkcia literálov. Tvar (1) nazývame* konjunktívny normálny tvar. *Formula A je taktiež ekvivalentná istej formule tvaru $B_1 \vee \cdots \vee B_m$ (2), kde každá B_i, $i = 1, \ldots, m$ je konjunkcia literálov. Tvar (2) nazývame* disjunktívny normálny tvar.

Dôkaz. indukciou vzhľadom na zložitosť formuly A

1° A je prvotná formula, teda je napísaná v konjunktívnom aj disjunktívnom normálnom tvare.

2° A môže byť tvaru $\neg B$ alebo $B \rightarrow C$.

$\neg B$ pre B platí IP, teda B je vyjadrená v B_d aj v B_k

$$
\begin{array}{lll}
\vdash B \leftrightarrow B_d & \vdash \neg B \leftrightarrow \neg B_d & \vdash A \leftrightarrow \neg B_d \\
\vdash B \leftrightarrow B_k & \vdash \neg B \leftrightarrow \neg B_k & \vdash A \leftrightarrow \neg B_k
\end{array}
$$

B_d je v tvare $B_1 \vee \cdots \vee B_m$

$\neg B_d$ je v tvare $\neg B_1 \wedge \cdots \wedge \neg B_m$
B_i je konjunkcia literálov
$\neg B_i$ je disjunkcia literálov

$\neg\neg L \leftrightarrow L$ //literál
$\vdash A \leftrightarrow \neg B_d$
$\vdash A \leftrightarrow A_k$
$\vdash A \leftrightarrow \neg B_k$

$B \rightarrow C$ $\vdash B \leftrightarrow B_d$
$\vdash B \leftrightarrow B_k$
$\vdash C \leftrightarrow C_d$
$\vdash C \leftrightarrow C_k$

$\vdash (B \rightarrow C) \leftrightarrow (\neg B \vee C)$
disjunktívny normálny tvar formuly A
$B_k,\ C_d$
$\vdash (B \rightarrow C) \leftrightarrow (\neg B_k \vee C_d)$
$\neg B_k \vee C_d$ je A_d
$\vdash (B \rightarrow C) \leftrightarrow (\neg B \vee C)$

$B,\ B_d$
$\vdash A \leftrightarrow (\neg B_d \vee C_k)$
$\neg B_d$ je konjunktívny normálny tvar formuly B
$\neg B_d \leftrightarrow B_1 \wedge \cdots \wedge B_n$
$C_k \leftrightarrow D_1 \wedge \cdots \wedge D_m$
D_j – disjunkcia literálov
B_i – disjunkcia literálov
$B_i,\ i = 1, \ldots n$
$(B_j \vee C_k)$
$(B_1 \wedge \cdots \wedge B_n) \vee C_k$
$(C_i \vee C_k) \leftrightarrow (B_i \vee D_i) \wedge \cdots \wedge (B_i \vee D_m)$
Keďže B_i aj D_j je disjunkcia literálov, tak dostávam konjunktívny normálny tvar.

□

4.8 Zopár viet na záver

Veta 4.8.1. *Nech $A, A_1, \ldots, A_n$ sú formuly výrokovej logiky, nech $p_1, \ldots, p_n$ sú navzájom rôzne prvotné formuly, ktoré sa vyskytujú vo formuly A. Nech A' vznikne z formuly A tak, že nahradíme každý výskyt prvotnej formuly p_i formulou A_i, $i = 1, \ldots, n$. Potom ak $\vdash A$, tak $\vdash A'$.*

Dôkaz. $\vdash A \implies \models A$
v je ľubovoľné ohodnotenie prvotných formúl, $\overline{v}(A) = 1$, nezáleží to od $v(p_i)$.
$\overline{v}(A')$ – počítame rovnakým spôsobom ako $\overline{v}(A)$
$v(p_i)$ – namiesto toho berieme hodnoty $\overline{v}(A_i)$
Kedže nezávisí od $v(p_i)$, tak $\overline{v}(A') = 1$ □

Poznámka. Veta je metateória – o vlastnostiach teórie.

$f : \{0,1\}^n \rightarrow \{0,1\}$
$f(x_1, \ldots, x_n) \in \{0,1\},\ x_i \in \{0,1\}$ – funkcia algebry logiky (boolovská funkcia)

Def 4.8.1. *Nech $A = A(p_1, \ldots, p_n)$ je formula výrokovej logiky. Pravdivostnou funkcio $h(x_1, \ldots, x_n)$ zodpovedajúcou formule A nazývame funkciou algebry logiky, ktorá je realizovaná formulou A, t.j. funkcia vzniká podľa nasledovných pravidiel:*

a) ak $A = p_i$*, potom* $h_A(x_i) = x_i$

b) ak $A = \neg B$*, potom* $h_A(x_1, \ldots, x_n) = \overline{h}_B(x_1, \ldots, x_n) = \neg h_B(x_1, \ldots, x_n)$
„$\overline{\ }$“, „$\neg$“ – *negácia v zmysle algebry logiky*

c) ak $A = B_1 \;\rightarrow\; B_2$*, potom* $h_A(x_1, \ldots, x_n) = h_{B_1}(x_{i_1}, \ldots, x_{i_{n_1}}) \;\rightarrow\; h_{B_2}(x_{j_1}, \ldots, x_{j_{n_2}})$
$\{x_1, \ldots, x_n\} = \{x_{i_1}, \ldots, x_{i_{n_1}}\} \cup \{x_{j_1}, \ldots, x_{j_{n_2}}\}$
„$\rightarrow$“ – *v zmysle algebry logiky*

Kapitola 5

Predikátová logika

- jazyk a jeho syntax a sémantika

5.1 (žeby) Syntax predikátovej logiky

Def 5.1.1. *Jazyk prvého rádu obsahuje:*

a) neohraničene mnoho symbolov pre premenné, označujeme: $x, y, z, \dots, x_1, x_2, \dots, y_1, y_2, \dots$

b) symboly pre logické spojky: $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$

c) symboly pre kvantifikátory: $\exists, \forall$

d) symboly pre predikáty $P, Q, R, \dots$ *ku každému symbolu je priradené prirodzené číslo* $n \geq 1$ *(árnosť), ak je medzi symbolmi symbol „=“, hovoríme o jazyku s rovnosťou*

e) symboly pre funkcie $f, g, \dots,$ *ku každému symbolu je priradené prirodzené číslo* $n \geq 1$ *(árnosť)*

f) pomocné symboly – zátvorky

Príklad. Jazyk teórie usporiadania je jazyk prvého rádu s rovnosťou a obsahuje jediný špeciálny symbol $<$, binárny predikátový symbol

Príklad. Jazyk teórie grúp je jazyk prvého rádu s rovnosťou, ktorý obsahuje dva špeciálne symboly „1“ – nulárny[1] konštantný symbol pre jedntokový prvok a „$\circ$“ binárny funkčný symbol pre grupovú operáciu

Príklad. Jazyk teórie telies je jazyk prvého rádu s rovnosťou, ktorý obsahuje dva binárne funkčné symboly „+“ (pre sčítanie) a „$\circ$“ (pre násobenie) a dva nulárne symboly „0“ a „1“ pre 0 a jednotkový prvok.

Príklad. Jazyk teórie množín je jazyk prvého rádu s rovnosťou a má jediný špeciálny symbol $\in$, binárny predikátovy symbol pre patričnosť.

Príklad. Jazyk elementárnej aritmetiky je jazyk prvého rádu s rovnosťou, ktorý obsahuje:

„0“ nulárny funkčný symbol

„S“ unárny funkčný symbol pre funkciu nasledovníka

„+“ binárny funkčný symbol pre operáciu sčítania

„$\cdot$“ binárny funkčný symbol pre operáciu násobenia

Def 5.1.2. *Term:*

1. každá premenná a každá konštanta je term

[1] 0 - árny

2. *ak sú výrazy $t_1, \ldots, t_n$ termy a f je je n-árny funkčný symbol, tak aj výraz $f(t_1, \ldots, t_n)$ je term*

3. *každý term vznikne konečným počtom použitím bodov* 1 *a* 2

Príklad. uvažujme jazyk elementárnej aritmetiky. 0, $S(0)$, $S(S(0))$ sú termy
$+, \ \cdot$
$+(x, y), \ \cdot(x, y), \ x + y, \ x \cdot y$
$((x + y) \cdot 0), \ (S(0) + (x \cdot y)) \cdot S(0)$
f – n-árny funkčný symbol
$f((x \cdot y), y_1, \ldots, y_{n-1})$
toto všetko sú termy

Def 5.1.3. *Formula:*

1. *ak je P n-árny predikátový funkčný symbol a ak sú výrazy $t_1, \ldots, t_n$ termy, tak potom výraz $P(t_1, \ldots, t_n)$ je atomická formula*

2. *ak sú výrazy A, B formuly, tak potom výrazy $\neg A$, $A \wedge B$, $A \vee B$, $A \rightarrow B$, $A \leftrightarrow B$ sú formuly*

3. *ak je x premenná a A je formula, potom výrazy $(\forall x)A$ a $(\exists x)A$ sú formuly*

4. *každá formula vznikne konečným počtom použitím bodov* 1, 2, 3

Poznámka.
$x = y \quad = (x, y)$
$x < y \quad < (x, y)$
$x \neq y \quad \neg(x = y)$

Príklad.

1. $S(0) = (0 \cdot x) + S(0)$

2. $(\exists x)(y = x \cdot z)$

3. $(\forall x)(x \neq 0 \rightarrow (\exists x)(x = S(y)))$

1. je atomická formula, 2. a 3. nie sú atomické formuly, všetko sú to formuly elementárnej aritmetiky

Def 5.1.4. *Nech Aje formula, jej podformulou sa nazýva:*

1. *len ona sama, ak A je atomická formula*

2. *ona sama a každá podformula formuly B, ak $A = \neg B$, $A = (\forall x)B$, $A = (\exists x)B$*

3. *ona sama a každá podformula formuly B a C, ak $A = B \rightarrow C$, $A = B \wedge C$, $A = B \vee C$, $A = B \rightarrow C$, $A = B \leftrightarrow C$*

4. *žiadne iné podformuly okrem tých, ktoré sú opísané v bodoch* 1, 2, 3 *formula A nemá*

Def 5.1.5. *Slová A, B, zreťazením týchto slov nazývame slovo AB. C je podslovo slova A, ak A je tvaru BCD, kde B, D sú slová.*

Príklad. t je term $f(x, g(x, y))$
$g(x, y)$ je podlsovo slova t, x je tiež podslovo
sú to aj podtermy termu t
)) nie je podterm
$(\forall x)(x \neq 0 \rightarrow (\exists y)(x = S(y)))$
$(\forall x)$ je podslovo, ale nie je podformula

Def 5.1.6. *Nech t je term a A je formula.*

1a) *Hovoríme, že term s je podtermom termu t, ak s je podslovom slova t.*

1b) Hovoríme, že formula B je podformulou formuly A, ak slovo B je podslovom slova A.

2) Hovoríme, že daný výskyt premennej x vo formule A je viazaný, ak je súčasťou nejakej podformuly tvaru $(\exists x)B$ alebo $(\forall x)B$ formuly A. Ak nie je daný výskyt premennej x viazaný tak hovoríme, že je voľný.

3) Hovoríme, že premenná x je voľná vo formule A, ak tam má voľný výskyt. Hovoríme, že premenná x je viazaná vo formule A, ak tam má viazaný výskyt.

4) Hovoríme, že formula A je otvorená, ak neobsahuje žiadnu viazanú premennú. Hovoríme, že formula A je uzavretá, ak neobsahuje žiadnu voľnú premennú.

Poznámka. $(x = y) \rightarrow (\exists x)(x = z)$, x je voľná aj viazaná
formuly s čitými premennými toto nemajú

5.2 Sémantika predikátovej logiky

- term, formula
- pravdivostná hodnota formuly

x, y, f, p
$\forall$, $\exists$, $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$
obor x, y, z
$M \neq \emptyset$
M – univerzum, jej prvky nazývame indivíduá

f – n-árny funkčný symbol
$f_M : M^n \to M$
$f_M : M \times \cdots \times M \to M$
$f_M(i_1, \ldots, i_n) = j$
$i_1, \ldots, i_n \in M,\ j \in M$
$\mathcal{M},\ f_{\mathcal{M}}$

P – n-árny predikátový symbol
$P_M \subseteq M^n$
$P_M \subseteq M \times \cdots \times M$
$\mathcal{M},\ P_{\mathcal{M}}$– konkrétna realizácia

M, $P_{\mathcal{M}}$, $f_{\mathcal{M}}$ – relačné štruktúry

Def 5.2.1. *Nech L je jazyk prvého rádu. Relačna štruktúra $\mathcal{M}$, ktorá obsahuje*

1. *neprázdnu množinu M*
2. *zobrazenie $f_{\mathcal{M}} : M^n \to M$ pre ľubovoľný n-árny funkčný symbol f z L*
3. *n-árnu reláciu $P_{\mathcal{M}} \subseteq M^n$ pre ľubovoľný n-árny predikátový symbol P z L, okrem binárneho predikátu pre rovnosť „=“*

sa nazýva realizácia jazyka L. Prvky univerza M nazývame indivíduá, zobrazenie $f_{\mathcal{M}}$ prislúchajúce k symbolu f nazývame realizácia funkčného symbolu a reláciu $P_{\mathcal{M}}$ realizáciou predikátového symbolu P.

Príklad. $\mathbb{N}$, množina prirodzených čísel
$< \mathbb{N}, \mathbb{N} \times \mathbb{N} >$ – relácia
štruktúra pre jazyk teórie čiastočného usporiadania

Príklad. $< \mathbb{N}^+, 0, S, \oplus, \odot >$ $\quad \mathbb{N}^+ = \{x \in \mathbb{N}, x > 0\}$
S – funkcia nasledovníka
relačná štruktúra pre jazyk elementárnej aritmetiky

Príklad. $< \mathbb{N}, 0, 1, \oplus, \odot >$
relačná štruktúra pre jazyk teórie telies[2]

[2]nemusí to byť teleso

0, 1 – sú nulárne funkčné symboly, teda musia byť z univerza

5.3 (žeby) Pravdivosť

$e(x) = m \in M$
$e(x/m)$
e – ohodnotenie premenných
t – term[3]
x – premenná
$t[\mathcal{M}, e] = t[e] = m \in M$
$e(x/m) = t[e]$
f n-árny funkčný symbol, $t_1, \ldots, t_n$ – termy, tak term $t[e] = f_{\mathcal{M}}(t_1[e], \ldots, t_n[e])$
$t_i[e] \in M \implies t[e] \in M$

Lema 1. *Nech t je term a $x_1, \ldots, x_n$ sú premenné, ktoré sa vyskytujú v terme t. Nech e, e' sú ohodnotenia premenných jazyka L, nech platí $e(x_i) = e'(x_i)$, $i = 1, \ldots, n$, potom:*

$$t[e] = t[e']$$

Dôkaz. MI vzhľadom na zložitosť termu t.

1° keď je to konštanta, tak je to už realizácia
keď je to premenná, tak z predpokladu platí $e(x) = e'(x)$

2° t je $f_{\mathcal{M}}(x_1, \ldots, x_n)$, $x_1, \ldots, x_n$ sú všetky premmené, ktoré sa vyskytujú v t
$e(x_i) = e'(x_i)$, $i = 1, \ldots, n$
$t_i[e] = t_i[e']$, $i = 1, \ldots, n$
$\implies f_{\mathcal{M}}(t_1[e], \ldots, t_n[e]) = f_{\mathcal{M}}(t_1[e'], \ldots, t_n[e'])$
pravdivosť formuly A pre konkrétne ohodnotenie premenných

□

Def 5.3.1. *Tarski*

1. *Nech $\mathcal{M}$ je realizácia jazyka L, e je ohodnotenie premenných formuly A. Indukciou podľa zložitosti formuly A budeme definovať pravdivosť formuly A v $\mathcal{M}$ pri ohodnotení e a označovať $\mathcal{M} \models A[e]$. Pravdivosť formuly A pri ohodnotení e v relačnej štruktúre $\mathcal{M}$.*

   a1) *ak A je atomická formula tvaru $P(t_1, \ldots, t_n)$, kde P je n-árny predikátový symbol rôzny od „=“ a $t_1, \ldots, t_n$ sú termy, potom $\mathcal{M} \models A[e] \iff (t_1[e], \ldots, t_n[e]) \in P_{\mathcal{M}}$*

   a2) *ak A je atomická formula $t_1 = t_2$, potom $\mathcal{M} \models A[e]$ práve vtedy, ak termy t_1, t_2 sú realizované pri ohodnotení e, jedným a tým istým indivíduom, t.j. $t_1[e] = t_2[e]$*

   b) *ak A je tvaru $\neg B$, potom $\mathcal{M} \models A[e]$ práve vtedy, ak $\mathcal{M} \not\models B[e]$*

   c) *ak A je tvaru $B \to C$, potom $\mathcal{M} \models A[e] \iff \mathcal{M} \not\models B[e] \lor \mathcal{M} \models C[e]$*

   d) *ak A je tvaru $(\forall x)B$, potom $\mathcal{M} \models A[e] \iff$ pre prekždé indivídum $m \in M$ platí $\mathcal{M} \models B[e(x/m)]$*

   d’) *ak A je tvaru $(\exists x)B$, potom $\mathcal{M} \models A[e] \iff$ pre isté indivídum $m \in M$ platí $\mathcal{M} \models B[e(x/m)]$*

2. *Hovoríme, že formula A je splnená v $\mathcal{M}$ a píšeme $\mathcal{M} \models A$, ak pre ľubovoľné e platí $\mathcal{M} \models A[e]$*

Poznámka. časť d' môžeme vynechať z dôvodu, že $(\exists x)$ vieme vyjadriť pomocou $(\forall x)$, $\neg$

Poznámka. obdobne v prípade termov aj v prípade formúl platí, ak $x_1, \ldots, x_n$ sú všetky premenné, ktoré sa vyskytujú v A a e, e' sú ohodnotenia, pre ktoré $e(x_i) = e'(x_i)$, $i = 1, \ldots, n$ potom $\mathcal{M} \models A[e] \iff \mathcal{M} \models A[e']$

Def 5.3.2. *Ak je uzavretá formula A splnená na relačnej štruktúre $\mathcal{M}$, tak hovoríme, že je pravdivá na $\mathcal{M}$, teda $\mathcal{M} \models A[e] \implies \mathcal{M} \models A$*

Def 5.3.3. *Nech A je formula. A' nazveme uzáverom formuly A, ak každá voľná premenná vo formule A je vo formule A' viazaná veľkým kvantifikátorom $(\forall)$.*

Tvrdenie 3. *Formula A je splnená na $\mathcal{M}$ vtedy a len vtedy, ak jej uzáver A' je pravdivý na $\mathcal{M}$.*

Dôkaz. ET: „Odporúčam spraviť na domácu úlohu“[4] □

5.4 Substitúcia termov za premenné

$x_1, \ldots, x_n$ sú rôzne premenné
$t, t_1, \ldots, t_n$ sú termy
$t_{x_1,\ldots,x_n}[t_1, \ldots, t_n]$ – term, ktorý vznikne z termu t dosadením termov t_i za premenné x_i naraz, $i = 1, \ldots, n$

Príklad.
$t = (x + y)$
$t_1 = (x + x)$
$t_2 = (z \cdot y)$
$t_3 = w$
$t_{x,y}[t_1, t_2] = ((x + x) + (z \cdot y))$
$t_{x,w}[t_1, t_3] = ((x + x) + y)$[5]
$t_{x,y,z}[t_1, t_2, t_3] = t_{x,y}[t_1, t_2]$

dosadením vždy vznikne term

A – formula
t – term
x – voľná premenná v A

$A_x[t]$ – substitúcia každého voľného výskytu premennej x za term t
$A_x[t]$ – je formula, je to **inštancia formuly** A (špeciálny prípad A)

Def 5.4.1. *Hovoríme, že term t je substituovateľný za x[6] do formuly A, ak pre každú premennú y obsiahnutú v t, žiadna podformula tvaru $(\forall y)B$ a $(\exists y)B$ formuly A neobsahuje (z hľadiska A) voľný výskyt premennej x. V ďalšom budeme označovať znakom $A_x[t]$ len tú skutočnosť, že term t je substiovateľný za x do A.*

Príklad. formula A je otvorená – žiadna premenná nemá viazaný výskyt

Príklad. žianda premenná $y \in t$ nie je viazaná v A, tiež môžem za ľubovoľnú premennú $x \in A$ substituovať term t

Príklad. z je premenná
term $t = z$
formula $A : (x = 0) \ \rightarrow \ \neg(\exists z)(z \neq 0)$
formula $A_x[t] : (z = 0) \ \rightarrow \ \neg(\exists z)(z \neq 0)$

$A_{x_1,\ldots,x_n}[t_1, \ldots, t_n]$ – tiež to robím naraz, hovorí nám to, že t_i, $i = 1, \ldots, n$ sú substituovateľné

Lema 2. *Nech $\mathcal{M}$ je realizácia jazyka L, A je formula, $t, t_1, \ldots, t_n$ sú termy jazyka L a e je ohodnotenie premenných $x_1, \ldots, x_n$ také, že platí $t_i[e] = m_i$, pre $i = 1, \ldots, n$. Potom:*

a) $t_{x_1,\ldots,x_n}[t_1, \ldots, t_n][e]$ *je indivídum* $t[e(x_1/m_1, \ldots, x_n/m_n)]$

[4] ak to niekto máte, tak mi to pošlite a ja to sem pridám
[5] v t neexistuje w, teda y a nie w!
[6] teda x môžem nahradiť termom t, teda snáď :)

b) $\mathcal{M} \models A_{x_1,\dots,x_n}[t_1,\dots,t_n][e] \iff \mathcal{M} \models A[e(x_1/m_1,\dots,x_n/m_n)]$

za x_i *dosadíme* $t_i[e]$, $i = 1,\dots,n$

Dôkaz.

a) indukciou podľa zložitosti termu t

1° t' je $t_{x_1,\dots,x_n}[t_1,\dots,t_n]$
nech t je premenná x, potom t je t' ak x sa nenachádza medzi $x_1,\dots,x_n$
ak je x niektoré x_i, tak potom t' je $t_i[e]$ (je indivídum m_i)
v tomto prípade tvrdenie platí

2° t je tvaru $f(s_1,\dots,s_n)$
IP: $s_i[t_1,\dots,t_n][e] = s_i[e(x_1/m_1,\dots,x_n/m_n)]$, $i = 1,\dots,n$
$t'[e] =?$ je indivídum $f_{\mathcal{M}}(s_1[e(x_1/m_1,\dots,x_n/m_n)],\dots,s_n[e(x_1/m_1,\dots,x_n/m_n)])$
indivídum $t[e(x_1/m_1,\dots,x_n/m_n)]$

b) indukciou vzhľadom na zložitosť t formuly A

1° A' je inštancia $A_{x_1,\dots,x_n}[t_1,\dots,t_n]$
A je $P(s_1,\dots,s_n)$, P je rôzny od „=“

$$\begin{aligned}
\mathcal{M} \models A'[e] &\iff (s_1[t_1,\dots,t_n][e],\dots,s_r[t_1,\dots,t_n][e]) \in P \iff \\
&\iff (s_1[e(x_1/m_1,\dots,x_n/m_n)],\dots,s_r[e(x_1/m_1,\dots,x_n/m_n)]) \in P_{\mathcal{M}} \iff \\
&\iff \mathcal{M} \models A[e(x_1/m_1,\dots,x_n/m_n)]
\end{aligned}$$

ak A je tvaru $t = s$
$A' : t[t_1,\dots,t_n] = s[t_1,\dots,t_n]$

$$\begin{aligned}
\mathcal{M} \models A[e] &\iff t_{x_1,\dots,x_n}[t_1,\dots,t_n][e] = s_{x_1,\dots,x_n}[t_1,\dots,t_n][e] \iff \\
&\iff t[e(x_1/m_1,\dots,x_n/m_n)] = s[e(x_1/m_1,\dots,x_n/m_n)] \iff \\
&\iff \mathcal{M} \models A[e(x_1/m_1,\dots,x_n/m_n)]
\end{aligned}$$

2° rozdelíme na prípady, čomu sa rovná formula A

$\neg B$, $B \to C$ – analogický postup, **ET povedal, že to treba na skúšku, teda ak to niekto viete, tak mi to pošlite**
– vychádza z IP a Tarského definície

$(\forall z)B$

1. $z \in \{x_1,\dots,x_n\}$
   Potom píšeme $A_{x_1,\dots,x_n}[t_1,\dots,t_n]$, $(\forall x_1)B_{x_1,\dots,x_n}[t_1,\dots,t_n]$
   nech z je x_1

$$\begin{aligned}
\mathcal{M} \models A'[e] &\iff \forall k \in M : \mathcal{M} \models B_{x_2,\dots,x_n}[t_2,\dots,t_n][e/(x_1/k)] \iff \\
&\iff \forall x \in M : \mathcal{M} \models B[e(x_1/k, x_2/m_2,\dots,x_n/m_n)] \iff \\
&\iff \mathcal{M} \models A[e(x_2/m_2,\dots,x_n/m_n)]^7 \iff \\
&\iff \mathcal{M} \models A[e(x_1/m_1,\dots,x_n/m_n)]
\end{aligned}$$

2. $z \notin \{x_1,\dots,x_n\}$
   – dôkaz v tomto prípade je zjednodušením zápisu predchádzajúceho dôkazu!

□

[7] pretože podľa definície pravdivosť A nezáleží na ohodnotení viazenej premennej x_1

5.5 Axiómy predikátovej logiky

$(\exists x)A$, skrátený zápis pre $\neg(\forall x)\neg A$

Def 5.5.1. *Nech A, B, C sú ľubovoľné formuly, potom*

(A1) $A \to (B \to A)$

(A2) $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$

(A3) $(\neg B \to \neg A) \to (A \to B)$

P – množina prvotných formúl, ktoré vo výrokovej logike nemôžeme ďalej rozkladať. Ak za P zvolíme všetky atomické formuly jazyka L, všetky formuly tvaru $(\forall x)B$, $(\exists x)B$, kde x je premenná jazyka L. Potom každá formula jazyka L vznikne z formúl len pomocou logických spojok. Ak si za pravidlo odvodenia zvolíme MP, tak dostávame vzťah medzi predikátovou a výrokovou logikou, ktroý je vyjadrený v nasledujúcej vete.

Veta 5.5.1. *Ak A je formula jazyka L – predikátovej logiky. Nech P je množina všetkých atomických formúl jazyka L a všetkých formúl tvaru $(\forall x)B$ a $(\exists x)B$, kde x je ľubovoľná premenná jazyka L a B je ľubovoľná formula jazyka L. Ak A je tautológia výrokovej logiky nad P, tak potom A je teorémou predikátovej logiky.*

Dôkaz. A je tautológia, $\models A \implies \vdash A$
predikátová logika je viac, teda A je dokázateľná aj v nej ... ???[8]
$A_1, \ldots, A_n \models$ □

Dôsledok 5.5.2. *Všetky teorémy výrokovej logiky prechádzajú do predikátovej logiky.*

Def 5.5.2. *Axióma špecifikácie: Ak A je formula, x premenná a t term substituovateľný za premennú x do formuly A, potom formula*

(A4) $(\forall x)A \to A_x[t]$

je axióma predikátovej logiky.

Táto axióma má názorný zmysel: Ak A platí pre ľubovoľné x, potom platí aj pre každý špeciálny prípad $A_x[t]$.

Formula A vyjadrená v prenexnom (prefixovom) tvare.

$$A : \underbrace{(Q_1x_1)\ldots(Q_nx_n)}_{prefix} B(x_1, \ldots, x_n)$$

kde Q_i, $i = 1, \ldots, n$ je $\exists$ alebo $\forall$ a B je jadro (formula bez kvantifikátorov)

Def 5.5.3. *Ak má A, B formuly a ak x je premenná, ktorá nemá voľný výskyt v A, tak potom formula*

(A5) $(\forall x)(A \to B) \to (A \to (\forall x)B)$

je axióma predikátovej logiky.

5.6 Pravidlá odvodenia

Def 5.6.1. *Modus ponens:*

$$\frac{A, A \to B}{B}$$

Def 5.6.2. *Pravidlo zovšeobecnenia (PZ): Hovorí o vlastnostiach voľných premenných.*
Pre ľubovoľnú premennú x a formulu A odvodíme formulu pre $(\forall x)A$. x je voľná vo formuly A, potom je dokázateľná formula $(\forall x)A$.

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

[8] tuto je nejaký chaos

Lema 1. *Pravdilo zavedenia veľkého kvantifikátora: Ak* $\vdash A \rightarrow B$ *a premenná* x *nemá voľný výskyt v* A*, potom* $\vdash A \rightarrow (\forall x)B$

Dôkaz.

$\vdash A \rightarrow B$
$\vdash (\forall x)(A \rightarrow B)$
$\vdash (\forall x)(A \rightarrow B) \rightarrow (A \rightarrow (\forall x)B)$ ($A5$, môžeme ju použiť)
$\vdash A \rightarrow (\forall x)B$ (MP)

□

Lema 2. *Pre ľubovoľné formuly* A, B *a term* t *platí:*

a) $\vdash A_x[t] \rightarrow (\exists x)A$ [9]

b) ak $\vdash A \rightarrow B$ *a premenná* x *nemá voľný výskyt v* B*, potom* $\vdash (\exists x)A \rightarrow B$ [10]

Dôkaz.

a)

$\vdash (\forall x)\neg A \rightarrow \neg A_x[t]$	($A4$)
$\vdash \neg\neg(\forall x)\neg A \rightarrow (\forall x)\neg A$	platí aj obrátene
$\vdash \neg(\exists x)A \rightarrow (\forall x)\neg A$	nahradenie $\forall$ s $\exists$
$\vdash (\neg(\exists x)A \rightarrow (\forall x)\neg A) \rightarrow (((\forall x)\neg A \rightarrow \neg A_x[t]) \rightarrow (\neg(\exists x)A \rightarrow \neg A_x[t]))$[11]	
$\vdash (\neg(\exists x)A \rightarrow \neg A_x[t]) \rightarrow (A_x[t] \rightarrow (\exists x)A)$	($A3$)($MP, 2\times$)
$\vdash A_x[t] \rightarrow (\exists x)A$	

b)

$\vdash A \rightarrow B$	
$\vdash (A \rightarrow B) \rightarrow (\neg B \rightarrow \neg A)$	($A3$)
$\vdash \neg B \rightarrow \neg A$	(MP)
$\vdash \neg B \rightarrow (\forall x)\neg A$	($L1$)
$\vdash (\neg B \rightarrow (\forall x)\neg A) \rightarrow (\neg(\forall x)\neg A \rightarrow \neg\neg B)$	
$\vdash \neg(\forall x)\neg A \rightarrow \neg\neg B$	
$\vdash (\exists x)A \rightarrow \neg\neg B$	
$\vdash (\exists x)A \rightarrow B$	

□

Lema 3. *Nech* A' *je inštancia formuly* A*, to znamená, že* A' *je tvaru* $A_{x_1,\ldots,x_n}[t_1,\ldots,t_n]$*, potom*

$$\vdash A \Longrightarrow \vdash A'$$

Dôkaz. Ak je dokázateľná formula A, tak je dokázateľný aj každý špeciálny tvar (inštancia) formuly A. Indukciou podľa počtu substituovaných termov.

1° $n = 1$, A' je tvaru $A_x[t]$
prepoklad: $\vdash A$

$\vdash (\forall x)A$	(PZ)[12]
$\vdash (\forall x)A \rightarrow A_x[t]$	($A4$)
$\vdash (A_x[t])$	(MP)

2° Nasledujúci príklad hovorí že, že v prípade $n > 1$ nemožno priamočiaro použiť dokázaného prípadu pre $n = 1$.
Príklad. Nech A je formula $x < y$, nech term t je premenná y a term s nech je premenná x. Uvažujme

[9] duálny tvar k a axióme špecifikácie
[10] duálny tvar k Leme 1, zavedenie malého kvantifikátora
[11] to je ako $(a \rightarrow b) \rightarrow ((b \rightarrow c) \rightarrow (a \rightarrow c))$, pravidlo jednoduchého sylogizmu
[12] pravidlo zovšeobecnenia

$A_{x,y}[s,t]$, to je formula $t < s$ a teda je $y < x$. Ale po dosadzovaní po jednej premennej dostaneme formulu $x < x$ ak najprv dosadíme t za x a potom s za y. V obrátenom poradí substituovania dostaneme $y < y$.

Nech $z_1, \ldots, z_n$ sú premenné, ktoré sa nevyskytujú vo formule A ani v termoch $t_1, \ldots, t_n$. Potom z predpokladu, že $\vdash A$ dostávame

$\vdash A \implies \vdash A_{x_1}[z_1]$
$\vdash A_{x_1,x_2}[z_1, z_2]$ ľahko sa o tom presvedčíme
$\vdots$
$\vdash A_{x_1,\ldots,x_n}[t_1, \ldots, t_n]$ označme ju B ($\vdash B$)
$\vdash B$
$\vdash B_{z_1}[t_1]$
$\vdots$
$\vdash B_{z_1,\ldots,z_n}[t_1, \ldots, t_n]$ toto je A'

□

Poznámka. voľné premenné môžu byť zamené

Dôsledok 5.6.1. *Nech $x_1, \ldots, x_n$ sú všetky voľné premenné vo formule A. Nech $z_1, \ldots, z_n$ sú navzájom rôzne premenné také, že z_i je substituovateľná za x_i, $i = 1, \ldots, n$ do formuly A. Potom $\vdash A \implies \vdash A'$, kde A' je inštanciou formuly A tvaru $A_{z_1,\ldots,z_n}[x_1, \ldots, x_n]$.*

Dôkaz. Vyplýva z ($L3$). □

Lema 4. *Pre ľubovoľnú formulu A, premenné $x_1, \ldots, x_n$ a termy $t_1, \ldots, t_n$ platí:*

a) $\vdash (\forall x_1) \ldots (\forall x_n) A \rightarrow A_{x_1,\ldots,x_n}[t_1, \ldots, t_n]$ [13]

b) $\vdash A_{x_1,\ldots,x_n}[t_1, \ldots, t_n] \rightarrow (\exists x_1) \ldots (\exists x_n) A$ [14]

Dôkaz. ľubovoľná formula C, ľubovoľná premenná x, potom $C_x[x]$ je C
$\vdash (\forall x) C \rightarrow C$ ($A4$)

a)

$\vdash (\forall x_n) A \rightarrow A$
$\vdash (\forall x_{n-1})(\forall x_n) A \rightarrow (\forall x_n) A$
$\vdots$
$\vdash (\forall x_1) \ldots (\forall x_n) A \rightarrow (\forall x_2) \ldots (\forall x_n) A$
$\vdots$
$\vdash (\forall x_1) \ldots (\forall x_n) A \rightarrow A$ označme A', pravidlo sylogizmu

a) je inštanciou A' a A' je pravdivá $\implies$ platí to z ($L3$).

b)

$\vdash C \rightarrow (\exists x) C$ ($L2a$)
$\vdots$
$\vdash A \rightarrow (\exists x_1) \ldots (\exists x_n) A$ označme A'', analogicky ako v a)

b) je inštanciou A'' a A'' je pravdivá $\implies$ paltí to z ($L3$).

□

Poznámka. Z formúl $(\forall x_1) \ldots (\forall x_n) A \rightarrow A$, $A \rightarrow (\exists x_1) \ldots (\exists x_n) A$ môžeme dokázať pomocou zavedenia $\forall$, $\exists$

$$\vdash (\forall x_1) \ldots (\forall x_n) A \leftrightarrow (\forall x_{\pi(1)}) \ldots (\forall x_{\pi(n)}) A$$

[13] zovšeobecnený tvar ($A4$)
[14] zovšeobecnený tvar duálneho tvaru ($A4$)

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

kde π je ľubovoľná permutácia na množine $\{1,\dots,n\}$

$\Longrightarrow$ nezáleží na ich poradí

Def 5.6.3. *Nech sú $x_1,\dots,x_n$ všetky premenné s voľným výskytom vo formule A v nejakom usporiadaní. Potom formula $(\forall x_1)\dots(\forall x_n)A$ nazveme uzáverom formuly A.*

Veta 5.6.2. *O uzávere (VU). Ak A' je uzáver formuly A, potom*

$$\vdash A \Longleftrightarrow \vdash A'$$

Dôkaz.

„⇒“ $\vdash A$, potom pravdilom zovšeobecnenia je $\vdash A'$

„⇐“

$\vdash A'$
$\vdash A' \to A$ $(L4a)$
$\vdash A$ (MP)

□

Poznámka. Veta o uzávere charakterizuje voľné premenné. Vo formálnej aritmetike platí:

$$\vdash x = 0 \Longrightarrow \vdash (\forall x)x = 0$$

Lema 5. *O distribúcii kvantifikátorov.*

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

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

Dôkaz.

a)

$\vdash A \to B$
$\vdash (\forall x)A \to A$ $(A4)$
$\vdash (\forall x)A \to B$ (*jednoduchý sylogizmus*)
$\vdash (\forall x)A \to (\forall x)B$ $(L1)$[15]

b)

$\vdash A \to B$
$\vdash B \to (\exists x)B$ $(L2a)$
$\vdash A \to (\exists x)B$ (*jednoduchý sylogizmus*)
$\vdash (\exists x)A \to (\exists x)B$ (*zavedenie* $\exists$)

□

Veta 5.6.3. *O ekvivalencii (VE). Nech formula A' vznikne z formuly A nahradením niektorých výskytov podformúl $B_1,\dots,B_n$ v uvedenom poradí formulami $B'_1,\dots,B'_n$.*

$$\vdash B_i \leftrightarrow B'_i,\ i = 1,\dots,n \Longrightarrow \vdash A \leftrightarrow A'$$

[15] lema o zavedení $\forall$, podmienky sú splnené

Dôkaz.
A má tvar $(\forall x)B$ alebo $(\exists x)B$
A' má tvar $(\forall x)B'$ alebo $(\exists x)B'$

$\vdash B \leftrightarrow B'$ $\qquad$ $(z\ IP)$
$\vdash B \rightarrow B' \wedge \vdash B' \rightarrow B$

aplikujeme lemu o distribúcii kvantifikátorov □

Def 5.6.4. *Hovoríme, že formula A' je variant formuly A, ak A' vznikne z A postupným nahradením podformúl tvaru $(Qx)B$ formulami $(Qy)B_x[y]$, kde y nie je voľná v B a Q je $\exists$ alebo $\forall$.*

Veta 5.6.4. *Ak A' je variant formuly A, tak potom*

$$\vdash A \leftrightarrow A'$$

Dôkaz. Podľa vety o ekvivalencii nám stačí dokázať, že formuly $(Qx)B$ a $(Qy)B_x[y]$ sú ekvivalentné.

Najprv dokazujeme keď Q je $\forall$. Predpokladajme, že x a y sú rôzne premenné (ináč by nebolo čo dokazovať).

1. $\vdash (\forall y)B_x[y] \rightarrow (\forall x)B$
   Označme B' formulu $B_x[y]$. Vidíme, že x nemá voľný výskyt v B', teda je substituovateľné z, aj do B'.

   $\vdash (\forall y)B' \rightarrow B'_y[x]$ $\qquad$ $(A4)$
   $\vdash (\forall y)B' \rightarrow (\forall y)B'_y[x]$ $\qquad$ $(zavedenie\ \forall)$
   $B'_y[x]$ je B
   $\vdash (\forall y)B_x[y] \rightarrow (\forall x)B$

2. $\vdash (\forall x)B \rightarrow (\forall y)B_x[y]$

   $\vdash (\forall x)B \rightarrow B_x[y]$ $\qquad$ $(A4)$
   $\vdash (\forall x)B \rightarrow (\forall y)B_x[y]$ $\qquad$ $(zavedenie\ \forall)$

Ďalej dokazujeme, keď Q je $\exists$. Predpokladajme, že x a y sú rôzne premenné.

1. $\vdash (\exists y)B_x[y] \rightarrow (\exists x)B$

   $\vdash B_x[y] \rightarrow (\exists x)B$ $\qquad$ $(duálny\ tvar\ A4)$
   $\vdash (\exists y)B_x[y] \rightarrow (\exists x)B$ $\qquad$ $(zavedenie\ \exists)$

2. $\vdash (\exists x)B \rightarrow (\exists y)B_x[y]$
   B' označme $B_x[y]$

   $\vdash B'_y[x] \rightarrow (\exists y)B'$
   $\vdash (\exists x)B'_y[x] \rightarrow (\exists y)B'$
   $\vdash (\exists x)B \rightarrow (\exists y)B_x[y]$

□

Def 5.6.5. *Nech A je niektorá formula z množiny formúl T a nech $A_1, \ldots, A_n$ je lubovoľné odvodenie z predpokladov (hypotéz) T. Hovoríme, že formula A_i je v tomto odvodení závislá od A, ak platí:*

1. *formula A_i je A a objavila sa v dôkaze ako prvok množiny T*
2. *A_i je formula, ktorú sme dostali podľa pravidla zovšeobecnenia formuly A_j, $(j < i)$ a formula A_j závisí od formuly A*
3. *formulu A_i sme dostali pomocou pravidla MP z formúl A_{j_1}, A_{j_2}, $(j_1 < i \wedge j_2 < i)$ a aspoň jedna z formúl A_{j_1}, A_{j_2} závisí v tomto odvodení od formuly A*

4. A_i je schéma axióm, ktorá obsahuje podfomulu závislú od A

Veta 5.6.5. O dedukcii (VD). *Nech T je množina formúl a A, B sú formuly predikátovej logiky, tak potom platí:*

a) $T \vdash A \rightarrow B \implies T, A \vdash B$

b) $T, A \vdash B$ *a existuje také odvodenie B z predpokladov $\{T, A\}$, že v ňom pri aplikácii pravidla zovšeobecnenia na formuly, ktoré v tomto odvodení závisia od A, sa veľkým kvantifikátorom neviaže žiadna premenná voľná v A, potom* $T \vdash A \rightarrow B$

Dôkaz.

a) $A_1, \ldots, A_n(A \rightarrow B)$
rozšírime množinu predpokladov – T, A

$$\begin{array}{rll} T & \vdash A \rightarrow B & \\ T, A & \vdash A \rightarrow B & \\ T, A & \vdash B & (MP) \end{array}$$

b) indukciou vzhľadom na dĺžku odvodenia formuly B

1° $n = 1$

1. $B \in T$

$$\begin{array}{rll} & \vdash B \rightarrow (A \rightarrow B) & \\ & B \in T \implies T \vdash B & \\ T & \vdash A \rightarrow B & (MP) \end{array}$$

2. B je A

$$\begin{array}{rl} & \vdash A \rightarrow A \\ T & \vdash A \rightarrow A \end{array}$$

3. B je axióma

$$\begin{array}{rll} & \vdash B & \\ T & \vdash B & \\ & \vdash B \rightarrow (A \rightarrow B) & \\ T & \vdash A \rightarrow B & (MP) \end{array}$$

2° $A_1, \ldots, A_s(B)$ – postupnosť formúl z predpokladov T, A
T, A – skúmame ako sa $A_s(B)$ tam mohlo dostať

1. $B \in T$, ako v 1°
2. B je A, ako v 1°
3. B je axióma, ako v 1°
4. B sa dostalo tak: A_j, A_i (MP) pričom $i, j < s$

$$\text{nech } i < j: \left.\begin{array}{l} A_j = A_i \rightarrow B \\ A_i \end{array}\right\} \text{MP} \ldots \rightarrow B$$

na A_i, A_j sa vzťhuje IP

$$\begin{array}{rll} T & \vdash A \rightarrow A_i & \\ T, A & \vdash A_i & \\ T & \vdash A \rightarrow A_j & \\ T, A & \vdash A_j & \\ T & \vdash A \rightarrow (A_i \rightarrow B) & \\ & \vdash (A \rightarrow (A_i \rightarrow B)) \rightarrow ((A \rightarrow A_i) \rightarrow (A \rightarrow B)) & (A2) \\ T & \vdash (A \rightarrow A_i) \rightarrow (A \rightarrow B) & \\ T & \vdash A \rightarrow B & \end{array}$$

A_i, $i < s$
$B = (\forall x)A_i$

možné su dva prípady

a) A_i nezávisí od formuly A v odvodení

$$T \vdash A_i \implies T \vdash \underbrace{(\forall x)A_i}_{B} \quad (PZ)$$

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

na základe IP platí: $T, A \vdash A_i \implies T \vdash A \to A_i$, lebo $i < s$

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

b) formula A neobsahuje voľné výskyty premennej x
$\implies$ tým sme splnili podmienky tvrdenia $T, A \vdash B \implies T \vdash A \to B$

□

Dôsledok 5.6.6. *Ak $T, A \vdash B$ a formula A je uzavretá, tak $T \vdash A \to B$*

Dôsledok 5.6.7. *Ak $T, A \vdash B$ a existuje také odvodenie B z predpokladov $\{T, A\}$, že v ňom neaplikujeme pravidlo zovšeobecnenia, tak $T \vdash A \to B$.*

Poznámka. Z dôkazu VD je zréjme, že ak v odvodení B z predpokladov $\{T, A\}$ nebolo použité pravidlo zovšeobecnenia na žiadnu voľnú premennú v A (inými slovami: žiadna voľná premenná formuly A nebola v uvedenom dôkaze použitá), tak $T \vdash A \to B$.

Veta 5.6.8. *O konštantách (VK). Nech T je množina formúl jazyka L a nech A je formula jazyka L. Nech L' je jazyk, ktorý vznikne z L rozšírením o nové symboly pre konšanty*[16]*. Ak sú $c_1, \ldots, c_m$ nové konštanty, potom*

$$T \vdash A[c_1, \ldots, c_m] \iff T \vdash A$$

Dôkaz.

„$\Leftarrow$“ Vyplýva z ($L3$).

„$\Rightarrow$“ $T \vdash A[c_1, \ldots, c_m]$ a nech $A'_1, \ldots, A'_m$ je odvodenie formuly $A[c_1, \ldots, c_m]$ z predpokladu T, nech $y_1, \ldots, y_m$ sú premenné, ktoré sa nevyskytujú v dôkaze A'_i ani vo formule A.

$A'_i \to A_i$, $i = 1, \ldots, n$
$c_j - y_i$, v $\forall A'_i$ konštantu c_j nahradíme y_i, $j = 1, \ldots, m$, dostaneme:
$A_1, \ldots, A_n$ – bez konštánt, je dôkazom formuly $A[y_1, \ldots, y_m]$ z predpokladov T

$T \vdash A[y_1, \ldots, y_m]$

- A', $C' \to (D' \to C')$ napríklad je to axióma tohoto typu, dostaneme
  $C \to (D \to C)$ ...toho istého
- A je inštancia formuly $A[y_1, \ldots, y_m]$ a tá je dokázateľná: $T \vdash A[y_1, \ldots, y_m] \implies T \vdash A$

[16]konštanty sú špecálne termy

□

Poznámka. nech formula A nie je uzavretá
nech $y_1, \ldots, y_n$ sú voľné premenné formuly A
$T \vdash A \rightarrow B$
L rozšírime o nové konštanty $c_1, \ldots, c_m$
$T \vdash A \rightarrow B$, potom podľa (VK)[17]:

$$T \vdash A \rightarrow B \iff T \vdash A[c_1, \ldots, c_m] \rightarrow B[c_1, \ldots, c_m] \iff T, A[c_1, \ldots, c_m] \vdash B[c_1, \ldots, c_m]$$

Veta 5.6.9. *Všeobecnejší tvar VD. Ak je A formula a T, S sú množiny formúl, potom $T \vee S \vdash A \iff \exists n \in \mathbb{N}$ a formuly $B_1, \ldots, B_n$ z ktorých každá je uzáverom nejakej formuly z S a $T \vdash B_1 \rightarrow (\ldots(B_n \rightarrow A)\ldots)$*

Dôkaz. Nech formuly $B_1, \ldots, B_n$ spĺňajú podmienky vety
$S \vdash B_i$, $i = 1, \ldots, n$
B_i je uzáver $A_i \in S$, $S \vdash A_i$
na základe (VU): $T \vee S \vdash A$
$T, B_1, \ldots, B_n \vdash A \implies T \vdash B_1 \rightarrow (\ldots(B_n \rightarrow A)\ldots)$ □

Dôsledok 5.6.10. *Nech A' je uzáver formuly A, nech T je množina formúl, potom $T \vdash A \iff T \cup \{\neg A'\}$ je sporná teória.*

Dôkaz.
$\vdash A \rightarrow (\neg A \rightarrow B)$
$\vdash \neg A \rightarrow (A \rightarrow B)$
A aj $\neg A \implies$ platí tam ľubovoľná formula[18], teda je to sporná teória

„⇒“ Nech formula A je dokázateľná z T, podľa (VU) to isté platí aj v A'

$$\left.\begin{array}{l} T \vdash A' \\ T \cup \{\neg A'\} \vdash \neg A' \end{array}\right\} \implies T \cup \{\neg A'\} \text{ je sporná}$$

„⇐“ $T \cup \{\neg A'\}$ je sporná teória, to znamená, že je v nej dokázateľná každá formula a teda aj A'

$$\begin{array}{rll} T \cup \{\neg A'\} & \vdash A' & \\ T & \vdash \neg A' \rightarrow A' & (VD) \\ & \vdash (\neg A' \rightarrow A') \rightarrow A' & (\textit{teoréma}) \\ T & \vdash A' & (MP) \\ T & \vdash A & (VU) \end{array}$$

□

5.7 Prenexné tvary formúl

– tiež prefixové

Def 5.7.1. *Hovoríme, že formula A je v prenexnom tvare, ak A má tvar:*

$$(Q_1 x_1)\ldots(Q_n x_n)B$$

kde $n \geq 0$ a pre každé $i = 1, \ldots, n$, Q_i je buď $\forall$ alebo $\exists$. B je otvorená formula (nemá žiadnu viazanú formulu) a $x_1, \ldots, x_n$ sú navzájom rôzne premenné. Formula B sa nazýva jadro formuly A a postupnosť kvantifikácii, ktoré predchádzajú B sa nazýva prefix formuly A.

[17] všeobecnejší tvar (VK)
[18] teda každá

Def 5.7.2. *Prenexné operácie (PO):*
Q *– kvantifikátor* $\forall$, $\exists$
ak Q *je* $\forall$, *tak* $\overline{Q}$ *je* $\exists$
ak Q *je* $\exists$, *tak* $\overline{Q}$ *je* $\forall$

a) podformulu B nahradíme nejakým jej variantom B'

b) podformulu $\neg(Qx)B$ nahradíme formulou $(\overline{Q}x)\neg B$

c) ak premenná x nie je voľná vo formule B, tak podformulu $B \rightarrow (Qx)C$ nahradíme formulou $(Qx)(B \rightarrow C)$

d) ak premenná x nie je voľná vo formule C, tak podformulu $(Qx)B \rightarrow C$ nahradíme formulou $(\overline{Q}x)(B \rightarrow C)$

e) ak symbol $\square$ označuje $\wedge$, $\vee$ a premenná x nie je voľná v B, tak podformulu $B\square(Qx)C$ nahradíme formulou $(Qx)(B\square C)$[19]

Treba dokázať, že v $a), \ldots, e)$ nahrádzame ekvivalentnou formulou.

Lema 6. *Pre ľubovoľné formuly B, C a každú premennú x platí:*

a) $\vdash B \leftrightarrow B'$

b) $\vdash (\overline{Q}x)\neg B \leftrightarrow \neg(Qx)B$

c) $\vdash (Qx)(B \rightarrow C) \leftrightarrow (B \rightarrow (Qx)C)$, *ak x nie je voľná v B*

d) $\vdash (\overline{Q}x)(B \rightarrow C) \leftrightarrow ((Qx)B \rightarrow C)$, *ak x nie je voľná v C*

e) $\vdash (Qx)(B\square C) \leftrightarrow (B\square(Qx)C)$, *ak x nie je voľna v B*

Dôkaz.

a) vyplýva z vety o variantoch

b)

Q je $\forall$
$\vdash \neg(\forall x)\neg\neg B \leftrightarrow \neg(\forall x)B$
$\vdash (\exists x)\neg B \leftrightarrow \neg(\forall x)B$

Q je $\exists$
$\vdash \neg(\exists x)B \leftrightarrow \neg(\exists x)\neg\neg B \leftrightarrow (\forall x)\neg B$

c)

Q je $\forall$

Q je $\exists$

d)

Q je $\forall$

Q je $\exists$

e) rozpísaním $\square$ pomocou $\neg$ a $\rightarrow$ a použitím predošlích prenexných operácií

$\square$

Veta 5.7.1. *Ku každej formuly A môžeme zostrojiť formulu A' v prenexnom tvare tak, že platí*

$$\vdash A \leftrightarrow A'$$

[19] aj $(Qx)C\square B$ – je to komutatívne

Dôkaz. A' získame z A pomocou prenexných operácií.
indukciou vzhľadom na zložitosť formuly A

1° A – atomická formula (bez kvantifikátorov)
A' je A
$\vdash A \leftrightarrow A'$

2° A môže byť: $\neg B$, $B \rightarrow C$, $(\forall x)B$. Na formuly B, C sa vzťahuje IP.

$\neg B$

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

$B \rightarrow C$

B', C' sú prenexné tvary B, C
$\vdash B \leftrightarrow B'$
$\vdash C \leftrightarrow C'$
Potrbujeme zostrojiť A'
C'' je variant C', že prefix neobsahuje premenné, ktoré sa vyskytujú v prefixe B'
pomocou (POa) $C' \rightarrow C''$
$\vdash (B \rightarrow C) \leftrightarrow (B' \rightarrow C'')$
pomocou (POc), (POd) $B' \rightarrow C''$

$(\forall x)B$

$\vdash B \leftrightarrow B'$
A' je v tvare $(\forall x)B'$, ak x nie je v prefixe B'
ak x je v prefixe B', tak B' je prenexný tvar A

□

Poznámka. Prenexné operácie pre $\leftrightarrow$ musím rozpísať: $A \leftrightarrow B \qquad (A \rightarrow B) \wedge (B \rightarrow A)$

Def 5.7.3. *Ak prefix uzavretej formuly má tvar $(\exists x_1) \dots (\exists x_k)(\forall x_{k+1}) \dots (\forall x_m)$, kde $k \geq 1$. Prípad $k = m$ nevylučujeme. Potom hovoríme, že formula A je vyjadrená v Skolemovom tvare (prenexný normálny tvar).*

Def 5.7.4. *Hodnosťou formuly A nazývame počet veľkých kvantifikátorov, ktoré v prefixe predchádzajú poslednému malému kvantifikátoru (počítame z ľava do prava).*

Veta 5.7.2. *Každú formulu možno zapísať v Skolemovom tvare. Ku každej formule A predikátového počtu, môžeme zostrojiť formulu A' v Skolemovom tvare, tak že*

$$\vdash A \Longleftrightarrow \vdash A'$$

Dôkaz. Predpokladajme, že formula A je vyjadrená v uzavretom tvare a v prenexnom tvare.
indukciou na hodnosť formuly A

1° Ak hodnosť formuly A je rovná 0, tak formula A je vyjadrená v Skolemomovom tvare.

2° Nech A má hodnosť w.
$A = (\exists x_1) \dots (\exists x_n)(\forall y)B(x_1, \dots, x_n, y)$
formula B obsahuje len voľné premenné $x_1, \dots, x_n, y$
formula B má hodnosť $m - 1$

A priradíme A^*
$\vdash A \Longleftrightarrow \vdash A^*$

$P^{(n+1)}$ – $n+1$-árny predikátový symbol, ktorý sa nenachádza v B
$A^* = (\exists x_1)\dots(\exists x_n)[(\forall y)(B(x_1,\dots,x_n,y) \to P^{(n+1)}(x_1,\dots,x_n,y)) \to (\forall y)P^{(n+1)}(x_1,\dots,x_n,y)]$
treba dokázať $\vdash A \iff \vdash A^*$

„$\Rightarrow$“

$$\vdash \underbrace{(B \to P^{(n+1)})}_{a} \to (\underbrace{B}_{b} \to \underbrace{P^{(n+1)}}_{c})$$

$\vdash (a \to (b \to c)) \to (b \to (a \to c))$ (*zámena predpokladov*)
$\vdash (b \to (a \to c))$ (MP)
$\vdash B \to ((B \to P^{(n+1)}) \to P^{(n+1)})$ (*teda*)
$\vdash (\forall y)(B \to ((B \to P^{(n+1)}) \to P^{(n+1)}))$ $(PZ, 2\times)$(*distribúcia* $\forall$)
n-krát použijeme pravidlo zovšeobecnenia podľa premenných $x_n,\dots,x_1$
a n-krát teorému $\vdash (\forall x)(a \to b) \to ((\exists x)a \to (\exists x)b)$ (POd)
$\vdash (\forall x_n)[(\forall y)B \to ((\forall y)(B \to P^{(n+1)}) \to (\forall y)P^{(n+1)})]$

$$\vdash \underbrace{(\exists x_1)\dots(\exists x_n)(\forall y)B(x_1,\dots,x_n,y)}_{A} \to A^*$$

$\vdash A \to A^*$
$\vdash A \Longrightarrow \vdash A^*$

„$\Leftarrow$“

$$\vdash A^*, \text{ tak je } \vdash (\exists x_1)\dots(\exists x_n)(\underbrace{(\forall y)(B \to B)}_{a} \to \underbrace{(\forall y)B)}_{b} \quad (PO)$$

$\vdash (\exists x)(a \to b) \leftrightarrow ((\forall x)a \to (\exists x)b)$ (POd)
$\vdash (\exists x_1)\dots(\exists x_{n-1})((\forall x_n)(\forall y)(B \to B) \to (\exists x_n)(\forall y)B)$ (PO)
$\vdots$
$\vdash (\forall x_1)\dots(\forall x_n)(\forall y)(B \to B) \to (\exists x_1)\dots(\exists x_n)(\forall y)B$
$\vdots$
$\vdash B \to B$ $(PZ, n\times)$

ideme skúmať A^*
$B = (Q_1 z_1)\dots(Q_l z_l)C$, kde C je formula bez kvantifikátorov

$$\begin{aligned}
A^* &= (\exists x_1)\dots(\exists x_n)((\forall y)[(Q_1 z_1)\dots(Q_l z_l)C \to P^{(n+1)}] \to (\forall y)P) \leftrightarrow \\
&\vdots \quad l\text{-krát } (POd) \\
&\leftrightarrow (\exists x_1)\dots(\exists x_n)((\forall y)(\overline{Q}_1 z_1)\dots(\overline{Q}_l z_l)[C \to P^{(n+1)}] \to (\forall u)P^{(n+1)}) \leftrightarrow \\
&\vdots \quad (POd) \\
&\leftrightarrow (\exists x_1)\dots(\exists x_n)(\exists y)((\overline{Q}_1 z_1)\dots(\overline{Q}_l z_l)[C \to P^{(n+1)}] \to (\forall u)P^{(n+1)}) \leftrightarrow \\
&\leftrightarrow (\exists x_1)\dots(\exists x_n)(\exists y)(Q_1 z_1)\dots(Q_l z_l)(\forall u)([C \to P^{(n+1)}] \to P^{(n+1)})
\end{aligned}$$

□

Kapitola 6

Axiómy rovnosti, logika s rovnosťou

$\mathcal{M} \models A[e]$ $\quad = \quad$ $P^{(2)}$ – binárny predikát rovnosti
$\mathcal{M} \models A$
Každé indivídum musí byť rovné samo sebe.

6.1 Axiómy

Def 6.1.1.

(R1) Ak x je premenná, potom formula $x = x$ je axióma identity.[1]

(R2) Ak sú $x_1, \dots x_k$, $y_1, \dots, y_k$ premenné a ak f je ľubovoľný k-árny funkčný symbol, potom formula

$$(x_1 = y_1 \rightarrow (x_2 = y_2 \rightarrow \dots \rightarrow (x_k = y_k \rightarrow (f(x_1, \dots, x_k) = f(y_1, \dots, y_k))) \dots)$$

je axióma.

(R3) Ak sú $x_1, \dots x_k$, $y_1, \dots, y_k$ premenné a ak P je ľubovoľný k-árny predikátový symbol, potom formula

$$(x_1 = y_1 \rightarrow (x_2 = y_2 \rightarrow \dots \rightarrow (x_k = y_k \rightarrow (P(x_1, \dots, x_k) \rightarrow P(y_1, \dots, y_k))) \dots)$$[2]

je axióma.

Veta 6.1.1. *Nech $t_1, \dots, t_n$, $s_1, \dots, s_n$ sú termy také, že platí*

$$(8) \quad \vdash t_i = s_i, \quad i = 1, \dots, n$$

i) Ak t je term a s je term, ktorý vznikne z t zámenou niektorých výskytov t_i zodpovedajúcimi termami s_i, potom platí

$$(9) \quad \vdash t = s$$

ii) Ak a je formula a A' vznikne z A zámenou niektorých výskytov termov t_i zodpovedajúcimi termami s_i, okrem prípadu keď t_i je premenná x, ktorá je súčasťou kvantifikácie $(\forall x)$ alebo $(\exists x)$ potom platí

$$(10) \quad \vdash A \leftrightarrow A'$$

Dôkaz.

i) indukciou vzhľadom na zložitosť termu

1° Ak t je premenná alebo niektorý z termov t_i, tak potom (9) je jeden prípad (8).

[1] $(R1)$ postuluje reflexívnosť rovnosti
[2] platí aj $P(y_1, \dots, y_k) \rightarrow P(x_1, \dots, x_k)$

2° Nech t je tvaru $f(r_1, \ldots, r_k)$ pre $r_1, \ldots, r_k$ platí IP. Ak je s v tvare $f(r'_1, \ldots, r'_k)$ kde r'_j pre $j = 1, \ldots, k$ vznikne z r_j zámenou niektorých t_i za s_i, podľa IP platí $r_j = r'_j$ (11), $j = 1, \ldots, k$

(12) $\vdash r_1 = r'_1 \ \rightarrow \ \ldots \ \rightarrow \ r_k = r'_k \ \rightarrow \ f(r_1, \ldots, r_k) = f(r'_1, \ldots, r'_k)$ (*inštancia (R2)*)
$\vdots$ k-krát (MP)
$\vdash f(r_1, \ldots, r_k) = f(r'_1, \ldots, r'_k)$

ii) – prechádzame od formuly A k formule A'
– zámena sa robí len v atomických formulách (P je rôzne od „=“)
$P(r_1, \ldots, r_k)$, dostávam $P(r'_1, \ldots, r'_k)$ podľa (11) platí $r_j = r'_j$
$\vdash r_1 = r'_1 \ \rightarrow \ \ldots \ \rightarrow \ r_k = r'_k \ \rightarrow \ P(r_1, \ldots, r_k) \ \rightarrow \ P(r'_1, \ldots, r'_k)$ (*inštancia (R3)*)
$\vdots$
$\vdash P(r_1, \ldots, r_k) \ \rightarrow \ P(r'_1, \ldots, r'_k)$
potrebujeme to aj opačne
keď platí (11), tak to platí aj naopak, teda opačná implikácia je úplne analogicky

nech P je „=“
nech formula $A : r_1 = r_2$, $A' : r'_1 = r'_2$
$\vdash A \ \leftrightarrow \ A'$ treba dokázať, teda $\vdash r_1 = r_2 \ \leftrightarrow \ r'_1 = r'_2$
využijeme tranzitívnosť
$\vdash r_1 = r'_1$
$\vdash r_2 = r'_2$
$\vdash r_1 = r'_1 \implies \vdash r'_1 = r_1$
$\vdash r_1 = r_2 \implies \vdash r'_1 = r_2$
$\vdash r_2 = r'_2 \implies \vdash r'_1 = r'_2$
$\vdash r_1 = r_2 \ \rightarrow \ r'_1 = r'_2$

□

Veta 6.1.2. *Ak sú $t, t_1, \ldots, t_n$, $s_1, \ldots, s_n$ termy a ak A je formula potom platí*

(i) $\vdash t_1 = s_1 \ \rightarrow \ \ldots \ \rightarrow \ t_n = s_n \ \rightarrow \ t[t_1, \ldots, t_n] = t[s_1, \ldots, s_n]$

(ii) $\vdash t_1 = s_1 \ \rightarrow \ \ldots \ \rightarrow \ t_n = s_n \ \rightarrow \ (A[t_1, \ldots, t_n] \ \leftrightarrow \ A[s_1, \ldots, s_n])$

ak je naviac x premenná, ktorá sa nevyskytuje v terme t, tak potom platí

(iii) $\vdash A_x[t] \ \leftrightarrow \ (\forall x)(x = t \ \rightarrow \ A)$

(iv) $\vdash A_x[t] \ \leftrightarrow \ (\exists x)(x = t \wedge A)$

Dôkaz. Ak termy $t_1, \ldots, t_n$, $s_1, \ldots, s_n$ neobsahujú žiadne premenné, tak tvrdenia (i), (ii) vyplývajú z príslušných tvrdení predošlej vety. Vo všeobecnom prípade premenné v termoch $t_1, \ldots, t_n$, $s_1, \ldots, s_n$ nahradíme novými konštantami, potom (i), (ii) vyplývajú z predošlej vety, (VD) a (VK).

(iii) „⇒“
$\vdash A_x[t] \ \rightarrow \ (\forall x)(x = t \ \rightarrow \ A)$
$\vdash x = t \ \rightarrow \ (A \ \leftrightarrow \ A_x[t])$ (ii)
$\vdash x = t \ \rightarrow \ (A_x[t] \ \rightarrow \ A)$
$\vdash A_x[t] \ \rightarrow \ (x = t \ \rightarrow \ A)$
$\vdash A_x[t] \ \rightarrow \ (\forall x)(x = t \ \rightarrow \ A)$

„⇐“
$\vdash (\forall x)(x = t \ \rightarrow \ A) \ \rightarrow \ (t = t \ \rightarrow \ A_x[t])$ $(A4)$
$\vdash t = t \ \rightarrow \ ((\forall x)(x = t \ \rightarrow \ A) \ \rightarrow \ A_x[t])$
$\vdash (\forall x)(x = t \ \rightarrow \ A) \ \rightarrow \ A_x[t]$ (MP)

(iv)

$\vdash (\forall x)(x = t \rightarrow \neg A) \leftrightarrow \neg A_x[t] \qquad (iii)$
$\vdash \neg(\forall x)(x = t \rightarrow \neg A) \leftrightarrow \neg\neg A_x[t]$
$\vdash (\exists x)(x = t \wedge A) \leftrightarrow A_x[t]$

□

6.2 Pravdivosť a dokázateľnosť, veta o úplnosti

6.2.1 Veta o korektnosti

Zhrnieme, čo sa zatiaľ udialo v predikátovej logike.

- jazyky logiky prvého rádu
- termy, formuly, podformuly
- relačná štruktúra $\mathcal{M} \models A[e]$, A je pravdivá v $\mathcal{M}$ pri ohodnotení e
- $\mathcal{M} \models A$, A je splnená v $\mathcal{M}$ pri ľubovoľnom ohodnotení
- axiómy
- odvodzovacie pravidlá

Def 6.2.1. *Nech L je jazyk prvého rádu, A je formula jazyka L. Hovoríme, že formula A je logicky platná a označujeme $\models A$ ak A je splnená v každej realizácii jazyka L.*

Poznámka. Logicky platné sú teda tie formuly, ktore sú splnené bez ohľadu na realizáciu jazyka, teda pri ľubovoľnej interpretácii špeciálnych symbolov.

Def 6.2.2. *Ak L je jazyk prvého rádu a T je nejaká množina formúl jazyka L, hovríme, že T je teória prvého rádu (v predikátovej logiky) s jazykom L.*

Def 6.2.3. *Ak je T teória s jazykom L a $\mathcal{M}$ realizácia jazyka L, hovoríme, že $\mathcal{M}$ je modelom teórie T a píšeme $\mathcal{M} \models T$, ak je v $\mathcal{M}$ splnená každá formula patriaca T. Hovoríme, že formula A je sémantickým dôsledkom teórie T, alebo že A je T-platná, ak je splnená v každom modeli teórie T, píšeme $T \models A$.*

Príklad. TODO :(

Veta 6.2.1. *O korektnosti. Ak je T teória s jazykom L a ak A je formula taká, že $T \vdash A$, potom $T \models A$.*

Poznámka. Ak formula A je dokázateľná z predpokladov T, tak potom je splnená v každom modeli teórie T.

Dôkaz. TODO :(□

Poznámka. Z vety o korektnosti vyplýva, že v predikátovej logike platí

$$\vdash A \Longrightarrow \models A$$

Poznámka. Veta o korektnosti nám dáva metódu, ako určiť, či daná formula A je teorémou danej teórie. Stačí nám uviesť model teórie T a také ohodnotenie premenných e, že $A[e]$ nie je pravdivá (tým pádom nie je teoréma).

Dôsledok 6.2.2. *Ak má teória T nejaký model, potom T je bezosporná.*

Dôkaz. T je bezosporná ak existuje formula teórie T, ktorá nie je teorémou teórie T. Nech $\mathcal{M}$ je model teórie T.
$\mathcal{M} \models A$, $A \in T$
B, B' je jej uzáver na jazyku L
$\left.\begin{array}{l}\mathcal{M} \models B' \\ \mathcal{M} \models \neg B'\end{array}\right\}$ len jedno z nich
$\mathcal{M} \not\models B'$, B' nie je teoréma v T □

Veta 6.2.3. O úplnosti.[3] *Nech T je teória s jazykom L a A je ľubovoľná formula jazyka L, potom*

$$T \vdash A \iff T \models A$$

Teda A je vetou teórie T práve vtedy, keď A je splnená v ľubovoľnom modeli teórie T.

Veta 6.2.4. O úplnosti - druhá formulácia. *Teória T je bezosporná práve vtedy, keď T má model.*

Dôkaz.

„$\Leftarrow$“ Dôsledok nejakej vety.[4]

„$\Rightarrow$“ T je bezosporná, ideme k nej zostrojiť model.

Formula A teórie T s jazykom L, A' je uzáver A.
$T \vdash A \iff T \cup \{\neg A'\}$ je sporná teória (dôsledok VD)
$\implies$ táto teória nemá model, to znamená, že v každom modeli teórie T je uzáver A' pravdivý a podľa definície splňovania, je formula A splnená v každom modeli teórie $T \implies T \models A$
$T \vdash A \iff T \models A$, teda táto veta implikuje tú hornú!

Existuje relačná štruktúra $\mathcal{M}$, $\mathcal{M} \models A$, $A \in T$
Henkinova metóda dôkazu.
Teória T s jazykom L, T je bezosporná.
Máme ukázať, že existuje relačná štruktúra $\mathcal{M}$, ktorá je modelom T.
ľubovoľná $A \in T$, $\mathcal{M} \models A$, $\mathcal{M} \models A[e]$

musíme nájsť:

- množinu indivíduí – univerzum M
- relácie a zobrazenia, ktoré vhodne realizujú funkčné a predikátové symobly jazyka L

K dispozícii máme len syntaktické prostriedky teórie T – jazyk a axiómy teórie.

Základná myšlienka konštrukcie modelu $\mathcal{M}$ teórie T: Objekty teórie T, ktoré sa hodia za prvky univerza sú iba termy bez premenných, teda konštanty. Termy bez premenných budú indivíduá.

splňovanie: formula A bude splnená v modeli práve vtedy, keď A bude vetou T

Tento dôkaz ešte pokračuje časťou, že nedostatky, ale je toho už na mňa trochu moc. Nabudúce ;)

□

Potom tu ešte chýba zopár definícií, nejaká lema, vety: Henkinova, Lindenbaumova a veta o kompaktnosti.

[3]dokázal ju Kurt Gödel
[4]nechce sa mi to hľadať, tak ak sa niekomu chce, tak nech mi to pošle