(predpoklad $\mathsf{Suble}(t, x, \psi)$ je splnený, lebo substituujeme konštantný term) Potom

$$T \vdash \forall x \psi(x) \rightarrow \psi(t)$$

Použitím modus ponens máme

$$T \vdash \psi(t)$$

V tomto prípade musíme indukciu podľa zložitosti robiť pre všetky konštantné inštancie formuly s voľnými premennými.
Máme $\mathfrak{M}_H \models \psi(t)$, kde $\psi(t)$ môžeme chápať ako slovo v abecede jazyka. To je však to isté ako to, pre každé ohodnotenie $e : \textsc{Var} \rightarrow \mathfrak{M}_H$ platí

$$\mathfrak{M}_H \models \psi[e]$$

lebo prvky nosnej množiny sú konštantné termy. To je však ekvivalentné tomu, že

$$\mathfrak{M}_H \models \forall x \psi$$

Teraz budeme ukazovať opačný smer implikácie[10]. Nech

$$T \not\vdash \forall x \psi(x)$$

Keďže T je úplná teória, tak

$$T \vdash \neg \forall x \psi(x)$$

Ale to je to isté ako

$$T \vdash \exists x \neg \psi(x)$$

Tu (a len tu) je potrebný predpoklad „henkinovskosti“ teórie T. Vieme, že pre $\neg\varphi$ existuje konštanta $c_{\neg\varphi}$ taká, že

$$T \vdash \exists x \neg\varphi(x) \longrightarrow \neg\psi(c_{\neg\psi})$$

Na predchádzajúce dve formule použijeme modus ponens a dostaneme

$$T \vdash \neg\psi(c_{\neg\psi})$$

Ale toto je opäť uzavretá formula, na ktorú sa vzťahuje indukčný predpoklad. Čiže

$$\mathfrak{M} \models \neg\psi(c_{\neg\psi})$$

čo je ekvivalentné tomu, že existuje ohodnotenie $e : \textsc{Var} \rightarrow \mathfrak{M}_H$ také, že $e(x) = c_{\neg\psi}$ a $\mathfrak{M} \models \neg\psi[e]$. Našli sme teda ohodnotenie, pre ktoré to neplatí a teda

$$\mathfrak{M} \not\models \forall x \psi(x)$$

$\square$

[10]Symbolicky povedané, ukázali sme, že $A \longrightarrow B$. Teraz chceme ukázať, že $B \longrightarrow A$ a to urobíme tak, že ukážeme $\neg A \longrightarrow \neg B$.

Prírodovedecká fakulta UPJŠ Košice

Teória funkcionálneho a logického programovania

(poznámky z prednášok z akademického roka 2002/2003)

prednáša: Prof. RNDr. Peter Vojtáš, DrSc.

Obsah

Literatúra

[1] Kolár, Štěpánková, Chytil – Logika, algebry a grafy. SNTL 1989.

[2] Štepánek, Petr – Predikátová logika, elektronický učebný text MFF UK, Praha 2000.

Materiál obsahuje sú definície, vety a dôkazy, ktoré odzneli na prednáškach predmetu Teória funkcionálneho a logického programovania (prednáša Prof. RNDr. Peter Vojtáš, DrSc.) v akademickom roku 2002/2003.

Na tvorbe tohto textu sa podieľali (v abecednom poradí):
Andrej Baran, Karol Buček, Maroš Budaj, Karol Čisárik, Michal Fečík, Martin Gold, Peter Grilli, Martin Jaroš, Konštantín Kan, Pavel Karady, Peter Komenský, Ľubomír Korenko, Helena Lengeňová, Michal Mati, Stanislav Nízky, Marián Novotný, Marián Novák, Róbert Novotný, Ondrej Pačay, Jana Pribolová, ? Pristáš, Matej Rehák, Peter Slaninka, Miroslav Sukeľ, Michal Ráček, Matej Rehák, Peter Zaremský.

Stačí nám matematická reprezentácia, pretože máme len jeden typ atribútu. Táto definícia je dobrá, lebo $p(t_1,\dots,t_n)$ je uzavretá formula a T je úplná teória.
Týmto sme nadefinovali štruktúru jazyka (všetko je fixované). Teraz potrebujeme dokázať, že

$$\mathfrak{M}_H \models T$$

Tento dôkaz vykonáme indukciou podľa zložitosti uzavretej formule

$$\mathfrak{M} \models \varphi \text{ akk } T \vdash \varphi$$

Opäť pripomeňme, že máme úplnú teóriu, teda buď formula alebo jej negácia je dokázateľná.

Krok 1. – konštantné atómy

$$\mathfrak{M} \models p(t_1,\dots,t_n) \text{ akk } T \vdash p(t_1,\dots,t_n)$$

Ľavá strana je ale z definície ekvivalentná $\langle t_1,\dots,t_n\rangle \in p_{\mathfrak{M}_H}$, čím dostávame tvrdenie $(\star)$.

Krok 2.

- negácia – nech tvrdenie platí pre φ

$$\mathfrak{M} \models \neg\varphi \text{ akk } \mathfrak{M} \not\models \varphi \text{ akk } T \not\vdash \varphi$$

  Posledný člen pre úplnú teóriu je ekvivalentný:

$$T \vdash \neg\varphi$$

- implikácia – nech tvrdenie platí pre φ a ψ

$$\mathfrak{M} \models \varphi \longrightarrow \psi \text{ akk } \begin{cases} \text{buď } \mathfrak{M} \models \neg\psi \\ \text{alebo } \mathfrak{M} \models \varphi \text{ a súčasne } \mathfrak{M} \models \psi \end{cases}$$

  – $\mathfrak{M} \models \neg\varphi$. Z indukčného predpokladu máme $T \vdash \neg\varphi$. Ďalej vo výrokovom počte $\vdash \neg\varphi \longrightarrow (\varphi \longrightarrow \psi)$ (napr. overíme, že je to tautológia „tabuľkovou metódou“). Teda aj v

$$T \vdash \neg\varphi \longrightarrow (\varphi \longrightarrow \psi)$$

  Použijeme modus ponens a získame $T \vdash \varphi \longrightarrow \psi$.

  – $\mathfrak{M} \models \varphi$ a súčasne $\mathfrak{M} \models \psi$. Pre obidve formule platí indukčný predpoklad a teda $T \vdash \varphi$ a $T \vdash \psi$. Vo výrokovom počte máme

$$\vdash \varphi \longrightarrow (\psi \longrightarrow (\varphi \longrightarrow \psi))$$

  (je to tautológia výrokového počtu, teda je to dokázateľné vo výrokovom počte a teda aj v predikátovom počte). Použijeme dvakrát modus ponens a dostávame požadovanú platnosť:

$$\begin{array}{lcl} \vdash \psi & \longrightarrow & (\varphi \longrightarrow \psi) \\ \vdash \varphi & \longrightarrow & \psi \end{array}$$

- použitie kvantifikátora.
  Ukážme najprv, že ak $T \vdash \varphi$, potom $\mathfrak{M} \models x$. Nech $\varphi = \forall x\varphi$. Formula φ je uzavretá, ale ψ uzavretá byť nemusí.
  Nech $T \vdash \forall x\psi$ (možno $T \vdash \forall x\psi(x)$?). Podľa axiómy 4:

$$\vdash \forall x\psi(x) \rightarrow \psi(t)$$

4.5 Úplnosť predikátového počtu

Našim ďalším cieľom je ukázať úplnosť predikátového počtu, teda že ak $T \vdash A$, potom $T \models A$, kde $T \models A$ znamená pravdivosť vo všetkých modeloch teórie. Myšlienka dôkazu:
Nech $T \models A$ a nech $T \not\vdash A$. Z Lindenbaumovej vety vieme, že

$$T \cup \{\neg A\}$$

je bezosporná. Trik dôkazu spočíva v tom, že stačí vedieť (t. j. v ďalšom dokázať), že každá bezosporná teória má model (nejaký) $\mathfrak{M}$. Ak $\mathfrak{M}$ je model teórie $T \cup \{\neg A\}$, potom zrejme $\mathfrak{M} \models \neg A$. Ale $\mathfrak{M}$ je aj modelom teórie T, čiže v $\mathfrak{M} \models A$. Ak je však teória T bezosporná, nemôžu nastať oba prípady naraz, čím získavame spor nášho dôkazu.
Z Lindenbaumovej vety vieme, že bezospornú teóriu vieme úplne rozšíriť. Z Henkinovej vety zase vieme každú teóriu rozšíriť do henkinovskej teórie. Symbolicky zapísané:

$$T \stackrel{\text{Lindenbaum}}{\longrightarrow} \underbrace{T'}_{\text{bezosporná, úplná}} \stackrel{\text{Henkin}}{\longrightarrow} \underbrace{T_H}_{\substack{\text{bezosporná, úplná} \\ \text{konzervatívne rozší-} \\ \text{rená, henkinovská}}}$$

Veta 4.28 (Henkin, Gödel)
Každá úplná (bezosporná) henkinovská teória má model.

Ako už vieme, sémantika predikátového počtu obsahuje

$$\mathfrak{I}, \mathfrak{A}, \mathfrak{C}, \mathfrak{V}, \mathfrak{P}, \mathfrak{F}$$

pričom sa zúžime na prípad, že $\mathfrak{A} = \{A\}$, teda máme len jeden typ premenných.
Model $\mathfrak{M}$ má

- nosnú množinu M
- každej konštante $c \in \mathfrak{C}$ zodpovedá nejaký $c_{\mathfrak{M}} \in M$
- pre $p \in \mathfrak{P}$ máme arita$(p) = \langle A_1, \ldots, A_n \rangle = n$ a zodpovedá jej nejaké $p_{\mathfrak{M}} \subset M^n$
- pre $f \in \mathfrak{F}$, kde arita$(f) = n + 1$ zodpovedá $f_{\mathfrak{M}} : M^n \to M$

Otázka je, z čoho vyrobiť nosnú množinu? Budeme ju vytvárať z konštantných termov. Z henkinovskosti sme pridali množstvo konštánt.

Dôkaz.
Majme úplnú henkinovskú teóriu T. Nech KT je množina konštantných termov jazyka teórie T. Náš model nazveme henkinovským $\mathfrak{M}_H$ a jeho nosnou množinou bude KT. Pre každú konštantu z jazyka teórie T máme priradiť $c_{\mathfrak{M}_H} = c$. Nech je to ona sama (konštanta je totiž konštantným termom).

$$c \in \mathfrak{C}_{\mathfrak{L}}(T) \rightsquigarrow c_{\mathfrak{M}_H} = c$$

Pre každý $f \in \mathfrak{F}$, pričom arita$(f) = n$ budeme mať

$$\begin{aligned} f_{\mathfrak{M}_H} &: \mathrm{KT}^n \to \mathrm{KT} \\ f_{\mathfrak{M}_H}(t_1, \ldots, t_n) &= f(t_1, \ldots, t_n) \end{aligned}$$

Táto operácia je syntaktická, k n slovám $(t_1, t_2, \ldots, t_n)$ priradíme nové slovo $f(t_1, \ldots, t_n)$ – toto slovo obsahuje teda naviac písmená f, (,) a čiarky ,. Takejto interpretácii konštánt sa hovorí Herbrandovo univerzum; ak nemáme funkčné symboly, tak konštantné termy sú iba konštanty.
Ešte treba interpretovať predikátové symboly. Ak arita$(p) = n$, potom máme $p_{\mathfrak{M}_H} \subseteq \mathrm{KT}^n$. Ale $p(t_1, \ldots, t_n)$ je uzavretá formula. Sme v úplnej teórii, kde je buď $\vdash p$ alebo $\vdash \neg p$. Toto nemôžeme hocijako interpretovať. Povieme, že nejaká n-tica

$$\langle t_1, \ldots, t_n \rangle \in p_{\mathfrak{M}_H} \quad \text{akk} \quad T \vdash p(t_1, \ldots, t_n) \tag{$\star$}$$

Dôležité vety a tvrdenia

[1] v literatúre sa možno stretnúť aj s označením „lema o neutrálnej formuli“

1 Úvod

V predchádzajúcej knihe sme si uviedli základné definície a vlastnosti výrokového a predikátového počtu. V predikátovom počte sme si zaviedli množinu axióm $\{\mathrm{Ax1}, \ldots \mathrm{Ax5}\}$, definovali pravdivosť a dokázateľnosť formule. V dokázateľnosti sme často používali vytvárajúcu postupnosť formule:

$$\varphi_0, \varphi_1, \varphi_k \equiv \varphi_n$$

Pripomeňme, že znamienkom $\equiv$ sme označovali syntaktickú rovnosť – rovnosť „písmenko po písmenku“. Používali sme pritom len dve logické spojky – negáciu $\neg$ a implikáciu $\longrightarrow$ a dve odvodzovacie pravidlá – modus ponens a generalizáciu.

- modus ponens: ak existujú $j, k < i$ také, že $\varphi_j \equiv \varphi_k \longrightarrow \varphi_i$, resp.
- generalizácia:
$$\frac{\varphi}{(\forall x)\varphi}$$
Na záver sme si ukázali, že výrokový a predikátový počet je korektný, teda pre formulu φ platí:
$$\text{ak } \vdash \varphi \text{ potom } \models \varphi$$

2 Teórie a modely

Definícia 2.1
Množina formulí T jazyka $\mathfrak{J}$ sa nazýva *teória*. Štruktúra $\mathfrak{M}$ je *modelom teórie* T, ak pre každé $\varphi \in T$ platí

$$\mathfrak{M} \models \varphi$$

(teda pre každé ohodnotenie e platí, že $\mathfrak{M} \models \varphi[e]$)

Definícia 2.2
Povieme, že formula φ je dokázateľná v teórii[2] T (označujeme $T \vdash \varphi$), ak existuje postupnosť $\varphi_0, \ldots, \varphi_n \equiv \varphi$ taká, že pre každé $i \leq n$ platí, že

- φ_i je logická axióma alebo
- φ_i je axióma teórie T, t. j. $\varphi_i \in T$
- ex. $j, k < i : \varphi_j \equiv \varphi_k \longrightarrow \varphi_i$ (použitie modus ponens)
- ex. $j < i : \varphi_i \equiv \forall x \varphi_j$ (generalizácia)

Postupnosť formulí s takými vlastnosťami sa nazýva dôkaz v teórii T.

Definícia 2.3
Hovoríme, že φ je *sémantickým dôsledkom* teórie T, ak pre každý model $\mathfrak{M}$ teórie T ($\mathfrak{M} \models \varphi$) platí $\mathfrak{M} \models \varphi$ a označujeme

$$T \models \varphi$$

Poznámka 2.4

$$\emptyset \vdash \varphi \longrightarrow \emptyset \models \varphi$$

Veta 2.5 (o silnej korektnosti predikátového počtu)
Nech T je ľubovoľná teória jazyka $\mathfrak{J}$ a φ je formula. Potom

$$\textit{ak } T \vdash \varphi \textit{ tak aj } T \models \varphi$$

[2] alternatívne možno hovoriť, že φ je vetou teórie T

Otázkou je, či $T \vdash \varphi$. Táto otázka nie je triviálna, pretože sme do teórie pridávali nejaké axiómy. V dôkaze sme mohli použiť len konečne veľa špecializovaných axióm, máme teda:

$$T \cup \{\check{\mathrm{S}}\mathrm{pec}(\varphi_{n_1}^{i_1}), \ldots, \check{\mathrm{S}}\mathrm{pec}(\varphi_{n_k}^{i_k})\} \vdash \varphi, \qquad \text{pre } \varphi \in L_0$$

pričom môžeme predpokladať, že $i_1 \leq i_2 \leq \ldots i_k$.
Nasleduje trik. Môžeme pozorovať, že každá z špecializovaných axióm je uzavretá formula. Táto $\check{\mathrm{S}}\mathrm{pec}(\varphi_n^i)$ je uzavretá, lebo v $\varphi_n^i(x)$ bolo x kvantifikované a v $\varphi_n^i(x/c_n^i)$ už neostala žiadna voľná premenná. Pre ľubovoľnú špecializovanú axiómu platí veta o dedukcii (predikátového počtu), aplikujme ju na $\check{\mathrm{S}}\mathrm{pec}(\varphi_{n_k}^{i_k})$, čím dostaneme:

$$\underbrace{T \cup \{\check{\mathrm{S}}\mathrm{pec}(\varphi_{n_1}^{i_1}), \ldots, \check{\mathrm{S}}\mathrm{pec}(\varphi_{n_{k-1}}^{i_{k-1}})\}}_{A} \vdash \left(\underbrace{\left[(\exists x)\varphi_{n_k}^{i_k}(x) \longrightarrow \varphi_{n_k}^{i_k}(x/c_{n_k}^{i_k})\right]}_{\check{\mathrm{S}}\mathrm{pec}(\varphi_{n_k}^{i_k})} \longrightarrow \varphi\right)$$

pričom $i_1 \leq i_2 \leq \ldots i_k$.
Najprv sa chceme zbaviť tých konštánt, ktoré sme pridali ako posledné: pre každé $i < k$ sa konštanta $c_{n_k}^{i_k}$ nevyskytuje v $\check{\mathrm{S}}\mathrm{pec}(\varphi_{n_k}^{i_k})$. Taktiež sa nevyskytuje vo φ a jej výskyt vo $\check{\mathrm{S}}\mathrm{pec}(\varphi_{n_k}^{i_k})$ je jedine na mieste, kde ňou substituujeme x. Ďalej konštanta $c_{n_k}^{i_k}$ nie je v našom jazyku viazaná (nič o nej nevieme) a teda môžeme použiť vetu o konštantách.

$$A \vdash ((\exists x)\varphi_{n_k}^{i_k}(x) \longrightarrow \varphi_{n_k}^{i_k}(x/y)) \longrightarrow \varphi$$

kde y je nejaká celkom nová premenná. Použijeme generalizáciu:

$$A \vdash (\forall y)\Big(((\exists x)\varphi_{n_k}^{i_k}(x) \longrightarrow \varphi_{n_k}^{i_k}(x/y)) \longrightarrow \varphi\Big)$$

S kvantifikátorom môžeme vojsť dovnútra na 1. miesto:

$$A \vdash \Big((\exists y)\Big((\exists x)\varphi_{n_k}^{i_k}(x) \longrightarrow \varphi_{n_k}^{i_k}(y)\Big)\Big) \longrightarrow \varphi$$

Vojdime s kvantifikátorom na druhé miesto:

$$A \vdash \Big((\exists x)\varphi_{n_k}^{i_k}(x) \longrightarrow (\exists y)\varphi_{n_k}^{i_k}(y)\Big) \longrightarrow \varphi$$

Z výrokového počtu vieme, že $\vdash \varphi \longrightarrow \varphi$, čiže tiež

$$\vdash (\forall y)\neg\psi(y) \longrightarrow (\forall x)\neg\psi(x)$$

Teraz použijeme axiómu 3 po dosadení:

$$\vdash \Big((\forall y)\neg\psi(y) \longrightarrow (\forall x)\neg\psi(x)\Big) \longrightarrow \Big(\neg((\forall x)\neg\psi(x)) \longrightarrow \neg((\forall y)\neg\psi(y))\Big)$$

čo je ekvivalentné s:

$$\vdash \Big((\forall y)\neg\psi(y) \longrightarrow (\forall x)\neg\psi(x)\Big) \longrightarrow \Big((\exists x)\psi(x)) \longrightarrow (\exists y)\psi(y))\Big)$$

Ak dosadíme za ψ term $\varphi_{n_k}^{i_k}$, tak je to v poriadku a dostávame

$$A \vdash \varphi$$

Takto sme sa zbavili jednej konštanty a k nej prislúchajúcej špecializovanej axiómy. Analogicky sa budeme postupne zbavovať odzadu jednej konštanty za druhou, až sa zbavíme konštanty c^0 a ostane nám „holá“ teória T, t. j. dostaneme:

$$T \vdash \varphi$$

$\square$

4.4 Henkinovské teórie

Definícia 4.26 (henkinovská teória)
Nech T je teória v jazyku PP, povieme, že T je *henkinovská*, ak pre každú formulu $\varphi(x)$ s jednou voľnou premennou existuje konštanta $c_\varphi \in L$ taká, že

$$T \vdash (\exists x)\varphi(x) \longrightarrow \varphi(x/c_\varphi)$$

Veta 4.27 (Henkin)
Ku každej teórii T existuje jej rozšírenie T_h, také, že T_h je henkinovská a jazyk tejto teórie $\mathfrak{L}_{T_h}$ sa líši od $\mathfrak{L}$ len o nové konštanty t. j.

$$(\mathfrak{L}_{T_h}, T_h)$$

je konzervatívne rozšírenie $(\mathfrak{L}, T)$.

<u>*Dôkaz.*</u>
Majme jazyk $\mathfrak{L}_T = \mathfrak{L}_0$ a $T = T_0$. Očíslujme všetky formuly s jednou voľnou premennou

$$\mathrm{Fl}^0 = \{\varphi_n^0; n \in \omega\}$$

Zvoľme množinu:

$$\{c_n^0; n \in \omega\} \cap \mathfrak{L}_0 = \emptyset$$

Prienik je len symbolický, nie v striktne matematickom chápaní. Pri c je horný index úroveň, na ktorej sa nachádzame, dolný index je poradie. Podobné označenie zavedieme pre formuly.
Odkiaľ berieme nové konštanty? Predpokladáme, že v našom svete (môže byť formálne reprezentovaný napr. Gödelovými číslami) je dosť nevyužitých objektov (je nekonečný), ktoré možno využiť ako konštanty.
Položme:

$$\begin{aligned} \mathfrak{L}_1 &= \{\mathfrak{L}_0 \cup \{c_n^0; n \in \omega\}\} \\ \mathrm{Fl}^1 &= \{\varphi_n^1; n \in \omega\} \end{aligned}$$

kde Fl^1 sú všetky formuly v jazyku $\mathfrak{L}_1$ s jednou voľnou premennou.
Podobne rekurzívne zvolíme $\{c_n^1 : n \in \omega\} \cap L_1 = \emptyset$ a definujeme

$$\begin{aligned} \mathfrak{L}_2 &= L_1 \cup \{c_n^1 : n \in \omega\} \\ \mathrm{Fl}^2 &= \{\varphi_n^2; n \in \omega\} \\ &\vdots \end{aligned}$$

Potom budeme mať jazyk $\mathfrak{L}_\omega = \bigcup_{n\in\omega} L_n$ a $\mathrm{Fl}^\omega = \{\varphi_n^\omega : n \in \omega\}$ budú všetky formule v jazyku $\mathfrak{L}_\omega$ s jednou voľnou premennou, čiže

$$(\mathrm{Fl}^\omega = \bigcup_{n\in\omega} \mathrm{Fl}^n)$$

Teraz pre každé $\varphi_n^i \in \mathrm{Fl}^\omega$ pridajme do teórie T axiómy typu:

$$(\exists x)\varphi_n^i(x) \longrightarrow \varphi_n^i({}^x/_{c_n^i}) \coloneqq \check{\mathrm{S}}\mathrm{pec}(\varphi_n^i)$$

Axiómu tohto typu budeme nazývať *špecializovaná axióma*. Takto skonštruovanú teóriu označme ako T_h.
Je pomerne ľahko vidieť, že T_h je henkinovská, ostáva ešte dokázať, že $(\mathfrak{L}_{T_h}, T_h)$ je konzervatívne rozšírenie. Zaoberajme sa netriviálnym smerom dôkazu:
Nech φ je nejaká formula v pôvodnom jazyku teórie T tj. v $\mathfrak{L}_0$ a nech

$$T_h \vdash \varphi$$

<u>*Dôkaz.*</u>
Vykonáme indukciou pozdĺž dôkazu $\varphi_0, \ldots, \varphi_n$.
Zoberieme si ľubovoľný model $\mathfrak{M}$ teórie T a ukážeme, že $\forall i \le n$ platí $\mathfrak{M} \models \varphi_i$.

- ak φ_i je inštanciou logickej axiómy $Ax1 \ldots Ax5$, tak je pravdivosť tvrdenia zrejmá (*inštancie logických axióm sú pravdivé v každej štruktúre*).
- ak φ_i je z T, tak je pravdivosť tvrdenia zrejmá.
- posledné možnosti – generalizácia a modus ponens zachovávajú logickú pravdivosť a z toho je zrejmá pravdivosť tvrdenia.

□

Poznámka 2.6
V kurze Teórie algoritmov, resp. Teórie vypočítateľnosti sme sa zaoberali Turingovymi strojmi. Aritmetizáciou sme ukázali, že symboly jazyka Turingovych strojov môžeme kódovať ako prirodzené čísla. Rovnako bolo možné kódovať aj slová jazyka Turingovych strojov. Dôležitou vlastnosťou tohto kódovania bolo to, že „byť kódom“ musel byť (primitívne) rekurzívny predikát – teda tak ako bolo možné pre slovo nájsť jeho kód, aj pre každé číslo sa muselo dať nájsť slovo, ktorého kódom toto číslo bolo.
Analogickým spôsobom môžeme slová jazyka $\mathfrak{J}$ (formule a termy) kódovať do prirodzených čísel. Takisto musíme zabezpečiť, že „byť kódom formuly (termu)“ je primitívne rekurzívny predikát. Ak máme toto, potom môžeme takto kódovať aj dôkazy.
Problémom však môže byť overenie, či $\varphi_i \in T$. Treba vedieť, či $\{\lceil\varphi\rceil : \varphi \in T\}$ je PR. Ak existuje Turingov stroj, ktorý na vstup n vráti φ_n, potom je táto množina „dobrá“.
Problém však nastáva pri dokázateľnosti – je nekonštruktívna (rovnako ako „zastaví sa Turingov stroj na danom vstupe?“. Určiť dokázateľnosť nemusí byť efektívne, dokonca existujú teórie, kde dokázateľnosť nie je rekurzívne spočítateľná. Príčinou je použitie modus ponens a toho, že máme nekonečne veľa inštancií axióm.

Príklad 2.7
Na cvičeniach sa oboznámite s jazykom Prolog. Logický program je vlastne teória. Ukážeme si proces dôkazu (unifikácie). Majme pravidlá v teórii P. Chceme ukázať, že platí $B(t)$. Daný príklad ukazuje ako pracuje Prolog:
$P = \{B(x) \longleftarrow A(x), A(t)\}$
$?-\ B(t)$ $\qquad B(x_1) \longleftarrow A(x_1)$ – najprv substituujeme premenné v pravidle.
$?-\ A(t)$ $\qquad A(t)$ – dosadíme za x_1 premennú t a zunifikujeme.
$\emptyset$ pravidlá su unifikovateľné (prebehla unifikácia)
YES
Teraz uvažujme to isté, ale z hľadiska teórie. Skúsme urobiť dôkaz $B(t)$:

$$P = \{B(X) \longleftarrow A(X), A(t)\}$$

Máme formulu

$\varphi \coloneqq (\forall x_1)(B(x_1) \longleftarrow A(x_1)) \longrightarrow (B(t) \longleftarrow A(t))$	podľa axiómy 4
$(\forall x_1)(B(x_1) \longleftarrow A(x_1))$	v teórii je toto pravidlom
$B(t) \longleftarrow A(t)$	Modus Ponens (MP)
$A(t)$	pravidlo z teórie
$B(t)$	MP, teda je to dôkaz

Všimnime si, že v prvom kroku sme oindexovali premenné (podobne ako to robí Prolog). Tým sme zaistili, že $\mathrm{V\scriptstyle AR}(\varphi) \cap \mathrm{V\scriptstyle AR}(t) = \emptyset$ a teda, že $\mathsf{Suble}(t, x, \varphi)$.

Veta 2.8
Nech $\mathrm{V\scriptstyle AR}(t) \cap \mathrm{V\scriptstyle AR}(\varphi) = \emptyset$ a $x \in \mathrm{V\scriptstyle AR}(\varphi)$. *Potom platí, že*

$$\mathsf{Suble}(t, x, \varphi)$$

<u>*Dôkaz.*</u>
Musíme skontrolovať, či pre každú premennú $y \in \textsc{Var}(t)$ a pre každú podformulu tvaru $(\forall y)\psi$ formule φ platí, že neobsahuje výskyt x, ktorý je voľný z hľadiska celého φ.

$$(\forall y \in \mathcal{A})(\varphi) \text{ akk } (\forall y)(y \in \mathcal{A} \longrightarrow \varphi)$$

□

3 Výrokový počet *revisited*

Na zopakovanie uvedieme 3 základné axiómy výrokového počtu, z ktorých odvodíme ďalšie pravidlá.

Ax1 $\varphi \longrightarrow (\psi \longrightarrow \varphi)$

Ax2 $(\varphi \longrightarrow (\psi \longrightarrow \chi)) \longrightarrow ((\varphi \longrightarrow \psi) \longrightarrow (\varphi \longrightarrow \chi))$

Ax3 $(\neg\psi \longrightarrow \neg\varphi) \longrightarrow (\varphi \longrightarrow \psi)$

Zaviedli sme si ohodnotenie elementárnych výrokov

$$v : \mathrm{EV} \rightarrow \{0, 1\}$$

aj ohodnotenie formulí $\bar{v}$. Ak je toto ohodnotenie $\bar{v}(\varphi) = 1$, potom formula je tautológia. Ďalej je nám už vo výrokovom počte známa pravdivosť aj dokázateľnosť. Na záver sme si ukázali korektnosť výrokového počtu ($\vdash \varphi \longrightarrow \models \varphi$). Našim cieľom je teraz ukázať úplnosť výrokového počtu, teda, že z pravdivosti formule vyplýva aj jej dokázateľnosť. Na to však potrebujeme niekoľko pomocných tvrdení.

3.1 Niektoré vety výrokového počtu

Tvrdenie 3.1 (Tvrdenie 1)
Je dokázateľné, že $\varphi \longrightarrow \varphi$. V ďalšom to budeme zapisovať

$$\vdash \varphi \longrightarrow \varphi$$

<u>*Dôkaz.*</u>

1.	$\varphi \longrightarrow ((\varphi \longrightarrow \varphi) \longrightarrow \varphi)$	Ax1; $\{\varphi \longrightarrow \varphi/\psi\}$
2.	$(\varphi \longrightarrow ((\varphi \longrightarrow \varphi) \longrightarrow \varphi)) \longrightarrow ((\varphi \longrightarrow (\varphi \longrightarrow \varphi)) \longrightarrow (\varphi \longrightarrow \varphi))$	Ax2; $\{\varphi \longrightarrow \varphi/\psi, \varphi/\chi\}$
3.	$((\varphi \longrightarrow (\varphi \longrightarrow \varphi)) \longrightarrow (\varphi \longrightarrow \varphi))$	MP 1, 2
4.	$\varphi \longrightarrow (\varphi \longrightarrow \varphi)$	Ax1; $\{\varphi/\psi\}$
5.	$\varphi \longrightarrow \varphi$	MP 4, 3

□

Veta 3.2 (veta o dedukcii výrokového počtu)

$$T \cup \{\varphi\} \vdash \psi \Longleftrightarrow T \vdash \varphi \longrightarrow \psi$$

V teórii T s formulou φ je dokázateľné ψ, akk v teórii T je dokázateľné $\varphi \longrightarrow \psi$

<u>*Dôkaz.*</u>
$\Leftarrow$
Nech VPV $\varphi_0, \varphi_1, \ldots, \varphi_n$ je dôkaz výroku $\varphi \longrightarrow \psi$ v teórii T, pričom $\varphi_n \equiv \varphi \longrightarrow \psi$. Potom VPV

$$\varphi_0, \varphi_1, \ldots, \varphi_{n-1}, \varphi \longrightarrow \psi, \varphi, \psi$$

- Predpokladajme, že už máme skonštruovanú postupnosť až po T_n. Čomu sa rovná T_{n+1}?

$$T_{n+1} = \begin{cases} T_n \cup \{\varphi_n\} & \text{ak } T_n \nvdash \neg\varphi_n \\ T_n & \text{ináč} \end{cases}$$

Označme $\overline{T} = \bigcup_{n \in \omega} T_n$. Chceme overiť, či $\overline{T}$ je úplná teória. Všimnime si, že jazyk ostal ten istý, len sme niečo pridávali do teórie. Indukciou cez $i \in \omega$ dokážme, že T_i je bezosporná. Nech T_n je bezosporná, je aj T_{n+1} bezosporná?

- ak $T_{n+1} = T_n$ triviálne
- Nech $T_{n+1} = T_n \cup \varphi_n$ t.j. platí, že: $T_n \nvdash \neg\varphi_n$.
  Dokážme sporom, že je bezosporná:
  Nech
  $$T_{n+1} \vdash \psi \quad \text{a} \quad T_{n+1} \vdash \neg\psi$$
  Vo výrokovom počte platí
  $$\vdash \psi \longrightarrow (\neg\psi \longrightarrow \chi)$$
  takže platí aj:
  $$T_{n+1} \vdash \psi \longrightarrow (\neg\psi \longrightarrow \neg\varphi_n)$$
  a teda
  $$T_{n+1} \vdash \neg\varphi_n$$
  To však môžeme podľa toho, ako sme si stanovili T_{n+1} napísať ako
  $$T_n \cup \{\varphi_n\} \vdash \neg\varphi_n$$
  resp.
  $$T_n \cup \{\neg\varphi_n\} \vdash \neg\varphi_n$$
  a teda na základe vety o rozbore prípadov výrokového počtu je jedno, či je T_n rozšírená o φ alebo o $\neg\varphi$ a teda platí:
  $$T_n \vdash \neg\varphi_n$$
  čo je spor, teda T_{n+1} je bezosporná.

Z toho, ako sme si definovali $\overline{T} = \bigcup_{n \in \omega} T_n$ vieme, že $\overline{T} \supset T_i$ pre každé i. Chceme teraz overiť, že $\overline{T}$ je úplná teória, teda či pre každé n platí

$$T_n \vdash \varphi_n \quad \text{alebo} \quad T_n \vdash \neg\varphi_n$$

Buď $T_n \vdash \neg\varphi_n$ (čo je druhý prípad) alebo $T_{n+1} \equiv T_n \cup \{\varphi_n\}$ a tam je dokázateľné φ (čo je prvý prípad) – to znamená, že $\overline{T}$ je úplná.
Ostáva nám ešte overiť či je $\overline{T}$ bezosporná. Urobíme dôkaz sporom v metamatematike. Nech je $\overline{T}$ rozporuplná, čiže

$$\overline{T} \vdash \psi, \quad \overline{T} \vdash \neg\psi$$

Potom ale existuje n také, že všetky formule použité v dôkaze sporu sú z teórie T_n.

$$T_n \vdash \psi, T_n \vdash \neg\psi$$

Ale každá teória T_n je bezosporná, získavame teda „metaspor“. □

– alebo D_i je inštanciou axiómy 5. Potom

$$(\forall x)(\nu \longrightarrow \varphi) \longrightarrow (\nu \longrightarrow \forall x\varphi)$$

ak $x \notin \mathrm{FV}(\nu)$
Dôkaz je podobný prípadu axiómy 4, znovu $x \neq y$ atď.
Treba nám ale overiť či

$$x \notin \mathrm{FV}(\nu(c/y))$$

ale keďže $x \neq y$ a pred substitúciou platilo $x \notin \mathrm{FV}(\nu)$, tak to platí.

□

Poznámka 4.20 (interpretácia vety o konštantách)
Ak pridáme do jazyka konštantu a nič o nej nepovieme (nijak ju neviažeme), tak je tam zbytočná (neuškodí, ale ani nepomôže)

4.3 Konzervatívne rozšírenie teórie

Definícia 4.21 (konzervatívne rozšírenie)
Nech $\mathfrak{J}_1 \subseteq \mathfrak{J}_2$ sú jazyky predikátového počtu, pričom $T_1 \subseteq \mathrm{Fl}(\mathfrak{J}_1)$, $T_2 \subseteq \mathrm{Fl}(\mathfrak{J}_2)$, $T_1 \subseteq T_2$. Povieme, že $(T_2, \mathfrak{J}_2)$ je *konzervatívnym rozšírením* $(T_1, \mathfrak{J}_1)$, ak pre každú formulu $\varphi \in \mathrm{Fl}(\mathfrak{J}_1)$ platí:

$$T_1 \vdash_{\mathfrak{J}_1} \varphi \text{ akk } T_2 \vdash_{\mathfrak{J}_2} \varphi$$

Poznámka 4.22
Interpretácia tejto definície v smere zľava doprava je triviálna. V opačnom smere hovorí definícia asi toto:
Ak pridáme do teórie nejakú konštantu s nejakými vlastnosťami, aj tak môže ešte ísť o konzervatívne rozšírenie.
Ak máme napr. teóriu o reálnych čísel a pridáme k nej konštantu i (takú, že $i^2 = -1$), dostaneme teóriu o komplexných číslach. Potom ak pomocou komplexných čísel v tejto teórii dokážem nejakú vlastnosť (formulu φ) v ktorej sa však i nenachádza (teda všetky čísla vo φ sú reálne), potom sa táto vlastnosť dá dokázať aj v teórii reálnych čísel čiže existuje dôkaz v ktorom nemusím použiť i.

Pozorovanie 4.23
$(T, \mathfrak{J} \cup \{c\})$ *je konzervatívnym rozšírením* $(T, \mathfrak{J})$. *To sme dokázali pred chvíľou.*

Definícia 4.24 (úplná teória)
Teória T sa nazýva *úplná*, ak je bezosporná t.j. $T \nvdash \varphi \& \neg\varphi$ a pre každú uzavretú[9] formulu φ platí:

$$\text{buď } T \vdash \varphi \text{ alebo } T \vdash \neg\varphi$$

Veta 4.25 (Lindenbaumova)
Každá bezosporná teória T má úplné rozšírenie s tým istým jazykom.

<u>*Dôkaz.*</u>
Nech náš jazyk J je konečný. Potom môžeme všetky uzavreté formule jazyka zoradiť do (primitívne rekurzívnej) postupnosti:

$$\varphi_0, \varphi_1 \ldots, \varphi_n$$

Indukciou cez $n \in N$ skonštruujeme postupnosť teórií T_i takto:

- Na začiatku položíme $T_0 = T$, teóriu T chceme rozširovať.

[9] T. j. neobsahuje voľné premenné. Napríklad v teórii reálnych čísel formula $x+4 = 2$ uzavretá nie je. Iný príklad: teória grúp nie je úplná pretože nie je rozhodnuteľné či $x+y = y+x$ (existujú grupy komutatívne a nekomutatívne)

je dôkaz v teórii $T \cup \{\varphi\}$. Označme tieto formuly postupne $\psi_0, \psi_1, \ldots, \psi_{n-1}, \psi_n, \psi_{n+1}, \psi_{n+2}$. Potom platí nasledovné: $\psi_n = \psi_{n+1} \longrightarrow \psi_{n+2}$, Týmto ale máme $i = n+2$, $j = n$ a $k = n+1$, čiže $j, k < i$. Čiže ψ_{n+2} bolo zostrojené pomocou modus ponens použitím ψ_{n+1}, ψ_n. Z toho máme $T \cup \varphi \vdash \psi$.
$\Rightarrow$
Nech VPV $D_0, D_1, ..., D_n = \psi$ je dôkaz v $T \cup \{\varphi\}$. Indukciou cez všetky $i \leq n$ ukážeme, že $T \vdash \varphi \longrightarrow D_i$

1. Ak D_i je logická axióma z T, potom bez indukčného predpokladu platí, že $T \vdash \varphi \longrightarrow D_i$:

$D_i \longrightarrow (\varphi \longrightarrow D_i)$	Ax1 $\{D_i/\varphi, \varphi/\psi\}$
D_i	axióma teórie T
$\varphi \longrightarrow D_i$	MP 1, 2

2. Ak $D_i = \varphi$, potom musíme dokázať, že $T \vdash \varphi \longrightarrow \varphi$. Podľa predchádzajúceho tvrdenia však platí $\vdash \varphi \longrightarrow \varphi$, čo je silnejšie ako $T \vdash \varphi \longrightarrow \varphi$.

3. Použitím IP: Nech existujú také $j, k < i$, že $D_j = D_k \longrightarrow D_i$.
Z indukčného predpokladu máme:

$$T \vdash \varphi \longrightarrow D_k, \qquad T \vdash \varphi \longrightarrow D_j$$

1.	$(\varphi \longrightarrow (D_k \longrightarrow D_i)) \longrightarrow ((\varphi \longrightarrow D_k) \longrightarrow (\varphi \longrightarrow D_i))$	Ax2; $\{\psi/D_k, \chi/D_i\}$
2.	$(\varphi \longrightarrow D_k) \longrightarrow (\varphi \longrightarrow D_i)$	MP j, 1
3.	$\varphi \longrightarrow D_i$	MP k, 2

□

Tvrdenie 3.3 (Tvrdenie 2)

$$\vdash \neg\varphi \longrightarrow (\varphi \longrightarrow \psi)$$

<u>*Dôkaz.*</u>

1.	$\neg\varphi \longrightarrow (\neg\psi \longrightarrow \neg\varphi)$	Ax1; $\{\varphi/\neg\varphi, \psi/\neg\psi\}$
2.	$\{\neg\varphi\} \vdash \neg\psi \longrightarrow \neg\varphi$	veta o dedukcii
3.	$\{\neg\varphi\} \vdash (\neg\psi \longrightarrow \neg\varphi) \longrightarrow (\varphi \longrightarrow \psi)$	Ax3
4.	$\{\neg\varphi\} \vdash \varphi \longrightarrow \psi$	MP 3, 2
5.	$\vdash \neg\varphi \longrightarrow (\varphi \longrightarrow \psi)$	veta o dedukcii

□

Tvrdenie 3.4 (Tvrdenie 3)

$$\vdash \neg\neg\varphi \longrightarrow \varphi$$

<u>*Dôkaz.*</u>

1.	$\vdash \neg\neg\varphi \longrightarrow (\neg\varphi \longrightarrow \neg\neg\neg\varphi)$	tvrdenie 2; $\{\varphi/\neg\varphi, \psi/\neg\neg\neg\varphi\}$
2.	$\{\neg\neg\varphi\} \vdash \neg\varphi \longrightarrow \neg\neg\neg\varphi$	veta o dedukcii
3.	$\{\neg\neg\varphi\} \vdash (\neg\varphi \longrightarrow \neg\neg\neg\varphi) \longrightarrow (\neg\neg\varphi \longrightarrow \varphi)$	Ax3; $\{\varphi/\neg\neg\varphi, \psi/\varphi\}$
4.	$\{\neg\neg\varphi\} \vdash \neg\neg\varphi \longrightarrow \varphi$	MP 2, 3
5.	$\{\neg\neg\varphi\} \cup \{\neg\neg\varphi\} \vdash \varphi$	veta o dedukcii
6.	$\{\neg\neg\varphi\} \vdash \varphi$	$A \cup A = A$
7.	$\vdash \neg\neg\varphi \longrightarrow \varphi$	veta o dedukcii

□

Tvrdenie 3.5 (Tvrdenie 4)

$$\vdash \varphi \longrightarrow \neg\neg\varphi$$

<u>*Dôkaz.*</u>

1. $\vdash \neg\neg\neg\varphi \longrightarrow \neg\varphi$	tvrdenie 3; $\{\varphi/\neg\varphi\}$
2. $\vdash (\neg\neg\neg\varphi \longrightarrow \neg\varphi) \longrightarrow (\varphi \longrightarrow \neg\neg\varphi)$	Ax3; $\{\psi/\neg\neg\varphi, \psi/\varphi\}$
3. $\vdash \varphi \longrightarrow \neg\neg\varphi$	MP 1, 2

□

Tvrdenie 3.6 (Tvrdenie 5)

$$\vdash (\varphi \longrightarrow \psi) \longrightarrow (\neg\psi \longrightarrow \neg\varphi)$$

<u>*Dôkaz.*</u>

1. $\vdash \neg\neg\varphi \longrightarrow \varphi$	tvrdenie 3;
2. $\{\neg\neg\varphi\} \vdash \varphi$	veta o dedukcii
3. $\{\varphi \longrightarrow \psi, \neg\neg\varphi\} \vdash \varphi$	ak $T \vdash \varphi$, tak aj $T' \vdash \varphi,\ T' \supseteq T$
4. $\{\varphi \longrightarrow \psi, \neg\neg\varphi\} \vdash \psi$	veta o dedukcii + MP
5. $\{\varphi \longrightarrow \psi, \neg\neg\varphi\} \vdash \neg\neg\psi$	tvrdenie 4.
6. $\{\varphi \longrightarrow \psi\} \vdash \neg\neg\varphi \longrightarrow \neg\neg\psi$	veta o dedukcii
7. $\{\varphi \longrightarrow \psi\} \vdash \neg\psi \longrightarrow \neg\varphi$	MP Ax1, 6
8. $\vdash (\varphi \longrightarrow \psi) \longrightarrow (\neg\psi \longrightarrow \neg\varphi)$	veta o dedukcii

□

Tvrdenie 3.7 (Tvrdenie 6)

$$\vdash \varphi \longrightarrow (\neg\psi \longrightarrow \neg(\varphi \longrightarrow \psi))$$

<u>*Dôkaz.*</u>

1. $\{\varphi, \varphi \longrightarrow \psi\} \vdash \varphi$	v teórii s pravidlom φ je dokázateľné φ
2. $\{\varphi, \varphi \longrightarrow \psi\} \vdash \varphi \longrightarrow \psi$	obdobne
3. $\{\varphi, \varphi \longrightarrow \psi\} \vdash \psi$	MP 1, 2
4. $\{\varphi\} \vdash (\varphi \longrightarrow \psi) \longrightarrow \psi$	veta o dedukcii
5. $\{\varphi\} \vdash ((\varphi \longrightarrow \psi) \longrightarrow \psi) \longrightarrow (\neg\psi \longrightarrow \neg(\varphi \longrightarrow \psi))$	Ax3; $\{\neg\psi/\varphi \longrightarrow \psi, \neg\varphi/\psi\}$
6. $\{\varphi\} \vdash \neg\psi \longrightarrow \neg(\varphi \longrightarrow \psi)$	MP 4, 5
7. $\vdash \varphi \longrightarrow (\neg\psi \longrightarrow \neg(\varphi \longrightarrow \psi))$	veta o dedukcii

□

Tvrdenie 3.8 (Tvrdenie 7)

$$\vdash (\neg\varphi \longrightarrow \varphi) \longrightarrow \varphi$$

<u>*Dôkaz.*</u>
Najprv použijeme tvrdenie 6 v tvare

$$\vdash (\neg\varphi \longrightarrow \neg(\neg\varphi \longrightarrow \varphi)) \longrightarrow ((\neg\varphi \longrightarrow \varphi) \longrightarrow \varphi)$$

4.2 Rozšírenie jazyka o konštantu a dokázateľnosť

Veta 4.19 (o konštantách)
Nech $\mathfrak{J}_1$ je jazyk PP a nech $\mathfrak{J}_2 = \mathfrak{J}_1 \cup \{c\}$ ($\mathfrak{J}_2$ je jazyk rozšírený o novú konštantu). Nech T je teória, pričom $T \subset \mathrm{Fl}(\mathfrak{J}_1)$ a $\varphi \in \mathrm{Fl}(\mathfrak{J}_1)$ (t. j. φ je formula $\mathfrak{J}_1$).
Potom[8]

$$T \vdash_{\mathfrak{J}_1} \varphi \text{ akk } T \vdash_{\mathfrak{J}_2} \varphi$$

<u>*Dôkaz.*</u>

$\Rightarrow$ Triviálny. Keď si zoberieme ľubovoľný dôkaz konkrétnej formule, tak ostáva v platnosti aj keď máme zrazu viacej axióm.

$\Leftarrow$ Nech $D_1, \ldots, D_n$ je dôkaz formule (budeme ho označovať D) φ z teórie T v jazyku J_2. Ak sa konštanta c v D nevyskytuje, tak niet čo riešiť. V opačnom prípade, ak sa konštanta c v dôkaze vyskytuje, tak nahraďme každý výskyt konštanty c v dôkaze D premennou y (takou, ktorá sa v D inde nevyskytuje).

$$D(c/y) = \{D_1(c/y), \ldots, D_n(c/y)\}$$

V tomto výraze nejde o pravú substitúciu (substitúcia za konštantu ani nebola definovaná), chceme tým len povedať, že v dôkaze každé písmeno „c“ nahradíme písmenom „y“, ktoré označuje premennú y.

Ukážeme, že $D(c/y)$ je dôkaz formule φ. (Vo φ sa c nevyskytuje, lebo $\varphi \in Fl(J_1)$)

$$D_n(c/y) = D_n = \varphi$$

Indukciou cez $i \leq n$ ukážeme, že $D(c/y)$ je dôkaz.

– buď D_i je inštanciou axiómy 1, 2 alebo 3. Potom $D_i(c/y)$ je opäť inštanciou axiómy 1, 2 alebo 3. Napríklad:

$$(\varphi \longrightarrow (\psi \longrightarrow \varphi))(c/y) = \varphi(c/y) \longrightarrow (\psi(c/y) \longrightarrow \varphi(c/y))$$

– alebo D_i je inštanciou axiómy 4. Teda $D_i = (\forall x)\varphi \longrightarrow \varphi(x/t)$, pričom platí $\mathsf{Suble}(t, x, \varphi)$ $y \neq x$, pretože také sme y vybrali.

$$D_i(c/y) = (\forall x)\varphi(c/y) \longrightarrow \varphi(x/t)(c/y)$$

pričom podľa vety z konca minulého semestra:

$$\varphi(x/t)(c/y) = \varphi(c/y)(x/_{t(c/y)})$$

teda:

$$D_i(c/y) = (\forall x)\varphi(c/y) \longrightarrow \varphi(c/y)(x/_{t(c/y)})$$

Treba však ešte overiť, že:

$$\mathsf{Suble}\big(t(c/y), x, \varphi(c/y)\big)$$

Keďže však $\textsc{Var}(t(c/y)) = \textsc{Var}(t) \cup \{y\}$ a je $\mathsf{Suble}(t, x, \varphi)$ tak to platí, pretože y nahradilo vo φ konštantu. Teda určite nikde vo formuli nie je $(\forall y)$

[8] $\vdash_{\mathfrak{J}_i}$ sme doteraz väčšinou písali ako $\vdash$ „z lenivosti“. Teória obsahuje schémy logických axióm (naša doteraz používaná T ich mala 5). Ak do ľubovoľnej z nich dosadíme (právoplatne: za všetky výskyty...) ľubovoľné formuly jazyka, dostaneme axiómu. Teda ak má jazyk naviac konštantu, tak naša teória má viacej axióm, lebo do schém môžeme dosadiť „viac“ vecí.

Tvrdenie 4.16 (dôsledok niektorých predchádzajúcich vlastností)
Nech $x \notin FV(\nu)$ a $\Box$ je ľubovoľný kvantifikátor a $\blacksquare$ je opačný kvantifikátor.
Potom platí:

- $(\Box x)(\nu \longrightarrow \varphi) \longleftrightarrow (\nu \longrightarrow (\Box x)\varphi)$
- $(\Box x)(\varphi \longrightarrow \nu) \longleftrightarrow ((\blacksquare x)\varphi \longrightarrow \nu)$

Poznámka 4.17
$\{P(x)\} \models (\forall x)P(x)$ nie je ekvivalentné s $\models P(x) \longrightarrow (\forall x)P(x)$

Veta 4.18 (o dedukcii v predikátovom počte)
Nech φ je uzavretá formula tj. $FV(\varphi) = \{\emptyset\}$ potom:

$$T \vdash \varphi \longrightarrow \psi \text{ akk } T \cup \{\varphi\} \vdash \psi$$

Dôkaz.
Dôkaz je podobný ako v prípade vety o dedukcii vo výrokovom počte:

$\Rightarrow$: Máme dôkaz $\varphi_0, \ldots, \varphi_{n-1}, \varphi_n = \varphi \longrightarrow \psi$ v teórii T
Zrazu sme v situácii, keď je dovolené používať ψ ako axiómu, dôkaz teda prepíšeme na:

$$\varphi_0, \ldots, \varphi_{n-1}, \varphi \longrightarrow \psi, \varphi, \psi$$

V dôkaze sa použil modus ponens v nasledujúcej podobe:

$$\varphi_n = \varphi_{n+1} \longrightarrow \varphi_{n+2}$$

$\Leftarrow$: Nech $D_0, \ldots, D_n = \psi$ je dôkaz v $T \cup \{\varphi\}$. Indukciou cez $i \leq n$ dokážeme, že $T \vdash \varphi \longrightarrow D_i$.

Vo VP bolo tvrdenie už dokázané pre D_i rovnajúce sa axiómam 1, 2, 3, axiómam T, φ, aj v prípade použitia modus ponens. Jediné, čo nám ešte zostalo, je generalizácia. To, že sme použili generalizáciu ako odvodzovacie pravidlo na kroku i znamená:

$$\text{existuje } j, j < i : D_i = (\forall x)D_j$$

Indukčný predpoklad hovorí, že:

$$T \vdash \varphi \longrightarrow D_j$$

Použijeme generalizáciu:

$$T \vdash (\forall x)(\varphi \longrightarrow D_j)$$

Máme predpoklad $\mathrm{FV}(\varphi) = \{\emptyset\}$, teda môžeme pokojne použiť axiómu predikátového počtu 5:

$$(\forall x)(\varphi \longrightarrow D_j) \longrightarrow (\varphi \longrightarrow (\forall x)D_j)$$

a teda

$$T \vdash (\varphi \longrightarrow (\forall x)D_j)$$

resp. ináč povedané:

$$T \vdash \varphi \longrightarrow D_i$$

□

1.	$\vdash \neg\varphi \longrightarrow (\neg\varphi \longrightarrow \neg(\neg\varphi \longrightarrow \varphi))$	tvrdenie 6; $\{\varphi/\neg\varphi, \psi/\varphi\}$
2.	$\{\neg\varphi\} \vdash \neg\varphi \longrightarrow \neg(\neg\varphi \longrightarrow \varphi)$	veta o dedukcii
3.	$\{\neg\varphi\} \cup \{\neg\varphi\} \vdash \neg(\neg\varphi \longrightarrow \varphi)$	veta o dedukcii
4.	$\{\neg\varphi\} \vdash \neg(\neg\varphi \longrightarrow \varphi)$	$A \cup A = A$
5.	$\vdash \neg\varphi \longrightarrow \neg(\neg\varphi \longrightarrow \varphi)$	veta o dedukcii
6.	$\vdash (\neg\varphi \longrightarrow \neg(\neg\varphi \longrightarrow \varphi)) \longrightarrow ((\neg\varphi \longrightarrow \varphi) \longrightarrow \varphi)$	Ax3; $\{\psi/\varphi, \varphi/\neg\varphi \longrightarrow \varphi\}$
7.	$\vdash (\neg\varphi \longrightarrow \varphi) \longrightarrow \varphi$	MP 5, 6

□

3.2 Ohodnotenie a dokázateľnosť

V minulom semestri sme si už ukázali, že vieme rozšíriť ohodnotenie elementárnych výrokov v na ohodnotenie všetkých výrokov (ohodnotenie $\bar{v}$). To vieme urobiť či už odspodu cez syntaktický strom výroku alebo pomocou vytvárajúcej postupnosti výroku.
Teda

$$v : \mathrm{EV} \rightarrow \{0, 1\}$$

vieme rozšíriť na

$$\bar{v} : \mathrm{V{\scriptsize YR}} \rightarrow \{0, 1\}$$

pričom sme používali funkciu $\mathrm{eval}(\varphi, v)$

Definícia 3.9
Nadefinujme si označenie φ^v kde φ je výrok a v je nejaké ohodnotenie elementárnych výrokov.

$$\varphi^v = \begin{cases} \varphi & \text{ak } \bar{v}(\varphi) = 1 \\ \neg\varphi & \text{ak } \bar{v}(\varphi) = 0 \end{cases}$$

Z letného semestra vieme, že

$$\mathrm{EV}(\varphi) = \{h(u) : u \text{ je list syntaktického stromu výroku } \varphi\}$$

Zaveďme si túto operáciu aj na množinu (elementárnych výrokov). Predpokladajme, že $\mathrm{EV}(\varphi) = \{p_1, \ldots, p_n\}$. Potom

$$\mathrm{EV}(\varphi)^v = \{p_1^v, \ldots, p_n^v\}$$

Inak povedané, keď výrok p_i má v našom svete hodnotu 1, tak ho ponecháme a ak mý hodnotu 0, tak ho znegujeme. Všimnime si, že ako dôsledok definície platí:

$$\bar{v}(\varphi^v) = 1$$

V nasledovnom tvrdení „miešame“ dokázateľnosť a chovanie sa v pravdivostných hodnotách.

Veta 3.10 (Post)
Nech φ je výrok a $v : EV \longrightarrow \{0, 1\}$. Potom

$$EV(\varphi)^v \vdash \varphi^v$$

To znamená, že keď si zoberieme množinu veľmi jednoduchých axióm $p_1, p_2, \ldots, p_n$ (prípadne niektoré podľa definície znegované, to záleží od „voľby“ ohodnotenia elementárnych výrokov v), tak z nich vieme dokázať φ^v.

Dôkaz.
Indukciou cez $i \leq n$ pomocou VPV. Vezmime si VPV $\varphi_0, \ldots, \varphi_n = \varphi$.
Vo VPV je φ:

- buď elementárny výrok

- alebo existuje $j < i$ také, že $\varphi_i = \neg\varphi_j$
- alebo existuje $j, k < i$ také, že $\varphi_i = \varphi_j \longrightarrow \varphi_k$

Indukciou cez $i \leq n$ dokážeme, že $\mathrm{EV}(\varphi)^v \vdash \varphi_i^v$

1. Nech $\varphi_i \in \mathrm{EV}(\varphi)$.
Potom samozrejme $\varphi_i^v \in \mathrm{EV}(\varphi)^v$, čiže φ_i^v je axiómou v teórii ($\mathrm{EV}(\varphi)^v$ je naša teória). Dá sa teda dokázať jednoducho (jej dôkaz je totiž dĺžky 1)
A teda v tomto prípade platí $\mathrm{EV}(\varphi)^v \vdash \varphi_i^v$

2. nech existuje $j < i : \varphi_i = \neg\varphi_j$
Tu už budeme potrebovať indukčný predpoklad; ten hovorí, že $\mathrm{EV}(\varphi)^v \vdash \varphi_j^v$. V závislosti od ohodnotenia v môžu nastať dva prípady:

   - buď $\bar{v}(\varphi_j) = 0$. Potom ale $\varphi_j^v = \neg\varphi_j = \varphi_i$. Keď $\bar{v}(\varphi_j) = 0$, tak $\bar{v}(\varphi_i) = 1$ a z toho $\varphi_i^v = \varphi_i$ S využitím týchto rovností:
   $$\mathrm{EV}(\varphi)^v \vdash \varphi_j^v, \text{ z toho } \mathrm{EV}(\varphi)^v \vdash \varphi_i, \text{ z toho } \mathrm{EV}(\varphi)^v \vdash \varphi_i^v$$
   - alebo $\bar{v}(\varphi_j) = 1$. Potom $\varphi_j^v = \varphi_j$. Keď $\bar{v}(\varphi_i) = 0$, tak $\varphi_i^v = \neg\varphi_i = \neg\neg\varphi_j$. Podľa tohto a indukčného predpokladu: $\mathrm{EV}(\varphi)^v \vdash \varphi_j^v$ a teda a teda $EV(\varphi)^v \vdash \varphi_j$. Ďalej podľa už dokázanej vlastnosti 4 je
   $$\vdash \varphi_j \longrightarrow \neg\neg\varphi_j$$
   bez akýchkoľvek dodatočných axióm. Z toho vyplýva, že:
   $$EV(\varphi)^v \vdash \neg\neg\varphi_j = \varphi_i^v$$

3. Zostáva nám prípad, že existujú $j, k < i : \varphi_i = \varphi_j \longrightarrow \varphi_k$. Rozoberme si všetky možnosti pomocou tabuľky:

	$v(\varphi_j)$	$v(\varphi_k)$	φ_j^v	φ_k^v	$\varphi_i^v = (\varphi_j \longrightarrow \varphi_k)^v$
v_1	0	0	$\neg\varphi_j$	$\neg\varphi_k$	$\varphi_j \longrightarrow \varphi_k$
v_2	0	1	$\neg\varphi_j$	φ_k	$\varphi_j \longrightarrow \varphi_k$
v_3	1	0	φ_j	$\neg\varphi_k$	$\neg(\varphi_j \longrightarrow \varphi_k)$
v_4	1	1	φ_j	φ_k	$\varphi_j \longrightarrow \varphi_k$

   - Prípady 2 a 4:
   Máme indukčný predpoklad $\mathrm{EV}(\varphi)^v \vdash \varphi_k$. Axióma číslo 1 výrokového počtu nám hovorí, že
   $$\varphi_k \longrightarrow (\varphi_j \longrightarrow \varphi_k)$$
   Využijeme odvodzovacie pravidlo modus ponens:
   $$EV(\varphi)^v \vdash (\varphi_j \longrightarrow \varphi_k) = \varphi_i^v$$
   - Prípad 1:
   Využijeme indukčný predpoklad
   $$EV(\varphi)^v \vdash \neg\varphi_j$$
   (druhý IP nám tu netreba)
   Tvrdenie 2 nám hovorí, že
   $$\vdash \neg\varphi_j \longrightarrow (\varphi_j \longrightarrow \varphi_k)$$
   Použijeme modus ponens a máme
   $$EV(\varphi)^v \vdash (\varphi_j \longrightarrow \varphi_k) = \varphi_i^v$$

A ak v tomto substituujeme
$$p/\neg\nu, \quad q/(\exists x)(\nu \longrightarrow \varphi), \quad r/(\exists x)\varphi$$
získavame požadované tvrdenie. □

Tvrdenie 4.13 (vlastnosť 11)

$$(\exists x)(\varphi \longrightarrow \nu) \longrightarrow ((\forall x)\varphi \longrightarrow \nu)$$
ak $x \notin FV(\nu)$.

Dôkaz.
Máme axiómu:
$$\vdash (\varphi \longrightarrow \nu) \longrightarrow (\neg\nu \longrightarrow \neg\varphi)$$
To implikuje:
$$(\exists x)(\vdash (\varphi \longrightarrow \nu) \longrightarrow (\neg\nu \longrightarrow \neg\varphi))$$
S kvantifikátorom môžeme vojsť dnu na obidve miesta:
$$\vdash (\exists x)(\varphi \longrightarrow \nu) \longrightarrow (\exists x)(\neg\nu \longrightarrow \neg\varphi)$$
Využijem vlastnosť 9:
$$(\exists x)(\neg\nu \longrightarrow \neg\varphi) \longrightarrow (\neg\nu \longrightarrow (\exists x)\neg\varphi)$$
Môžeme obrátiť poslednú implikáciu, čím dostaneme:
$$(\exists x)(\neg\nu \longrightarrow \neg\varphi) \longrightarrow \underbrace{\neg(\exists x)\neg\varphi \longrightarrow \nu}_{((\forall x)\varphi \longrightarrow \nu)}$$
□

Veta 4.14 (vlastnosť 12 (obrátená 11))

$$\vdash ((\forall x)\varphi \longrightarrow \nu) \longrightarrow (\exists x)(\varphi \longrightarrow \nu)$$
ak $x \notin FV(\nu)$

Dôkaz.
$$((\forall x)\varphi \longrightarrow \nu)) \longrightarrow (\neg\nu \longrightarrow (\exists x)\neg\varphi)$$
Pomocou vlastnosti 10:
$$(\neg\nu \longrightarrow (\exists x)\neg\varphi) \longrightarrow (\exists x)(\neg\nu \longrightarrow \neg\varphi)$$
a stačí už len obrátiť implikáciu:
$$(\exists x)(\neg\nu \longrightarrow \neg\varphi) \longrightarrow (\exists x)(\varphi \longrightarrow \nu)$$
□

Veta 4.15 (vlastnosť 13)

$$\vdash \neg(\forall x)\varphi \longrightarrow (\exists x)\neg\varphi$$
Dôkaz.
$$\vdash \neg(\forall x)\varphi \longrightarrow \neg(\forall x)\neg\neg\varphi \quad \longrightarrow (\exists x)\neg\varphi$$
□

Ak dosadíme za p term $(\nu \longrightarrow \varphi)$, za q term ν, za r term φ a za s term $(\exists x)\varphi$, potom vieme, že platí:

$$\vdash (\nu \longrightarrow \varphi) \longrightarrow (\nu \longrightarrow (\exists x)\varphi)$$

Použitím generalizácie:

$$(\forall x)[(\nu \longrightarrow \varphi) \longrightarrow (\nu \longrightarrow (\exists x)\varphi)]$$

Všimnime si, že x nie je voľné (nemá voľný výskyt) v ν, ani v $((\exists x)\varphi)$, preto s ním môžeme vojsť na prvé miesto (z vlastnosti č. 7 vieme, že sa mení na $(\exists x)$):

$$(\exists x)(\nu \longrightarrow \varphi) \longrightarrow (\nu \longrightarrow (\exists x)\varphi)$$

čím získavame požadované tvrdenie. □

Veta 4.12 (vlastnosť 10)

$$(\nu \longrightarrow (\exists x)\varphi) \longrightarrow (\exists x)(\nu \longrightarrow \varphi)$$

ak $x \notin FV(\nu)$

Dôkaz.
Axióma 1 nám hovorí, že

$$\vdash \neg\nu \longrightarrow (\neg\varphi \longrightarrow \neg\nu)$$

Použitím vety o dedukcii výrokového počtu, môžeme s $\neg\nu$ „vyjsť von“:

$$\neg\nu \vdash \neg\varphi \longrightarrow \neg\nu$$

resp. ekvivalentne:

$$\neg\nu \vdash \nu \longrightarrow \varphi$$

opäť použitím vety o dedukcii sa môžeme „vrátiť dnu“:

$$\vdash \neg\nu \longrightarrow (\nu \longrightarrow \varphi)$$

použijeme generalizáciu:

$$\vdash (\forall x)(\neg\nu \longrightarrow (\nu \longrightarrow \varphi))$$

Vojdeme s kvantifikátorom na druhé miesto:

$$\vdash \neg\nu \longrightarrow (\forall x)(\nu \longrightarrow \varphi)$$

Uvedomme si, že

$$(\nu \longrightarrow \varphi) \longrightarrow (\exists x)(\nu \longrightarrow \varphi)$$

takže sme dokázali, že

$$\vdash \neg\nu \longrightarrow (\exists x)(\nu \longrightarrow \varphi)$$

Máme polovicu dôkazu, pokúsme sa teraz napojiť z druhej strany:
Axióma 1 hovorí:

$$\vdash \varphi \longrightarrow (\nu \longrightarrow \varphi)$$

To nám implikuje nasledujúce tvrdenie:

$$\vdash (\exists x)(\varphi \longrightarrow (\nu \longrightarrow \varphi))$$

Vojdime s kvantifikátorom dovnútra na obidve miesta:

$$\vdash (\exists x)\varphi \longrightarrow (\exists x)(\nu \longrightarrow \varphi)$$

Vo výrokovom počte je nasledujúca formula tautológia:

$$(\neg p \longrightarrow q) \longrightarrow ((r \longrightarrow q) \longrightarrow ((p \longrightarrow r) \longrightarrow q))$$

- Prípad 3:
  Využijeme dva indukčné predpoklady:

$$\begin{array}{lcl} \mathrm{EV}(\varphi)^v & \vdash & \varphi_j \\ \mathrm{EV}(\varphi)^v & \vdash & \neg\varphi_k \end{array}$$

  Tvrdenie 6 hovorí: $\vdash \varphi_j \longrightarrow (\neg\varphi_k \longrightarrow \neg(\varphi_j \longrightarrow \varphi_k))$. Dvojnásobným použitím modus ponens dostávame

$$\mathrm{EV}(\varphi)^v \vdash \neg(\varphi_j \longrightarrow \varphi_k) = \varphi_i^v$$

□

Veta 3.11 (o dôkaze rozborom prípadov[3])

$$\left.\begin{array}{r} T \cup \{\varphi\} \vdash \psi \\ T \cup \{\neg\varphi\} \vdash \psi \end{array}\right\} \textit{potom } T \vdash \psi$$

Inak povedané, ak máme dané dva dôkazy výroku ψ (ako sú uvedené), potom vieme nájsť dôkaz φ v teórii T (bez použitia φ alebo $\neg\varphi$)

Dôkaz.
Vďaka vete o dedukcii môžeme preformulovať zápis na

$$T \vdash \varphi \longrightarrow \psi \quad (1)$$

$$T \vdash \neg\varphi \longrightarrow \psi \quad (2)$$

Čiže v podstate prestáva záležať na T, stačí ukázať, že keď sa nám podarilo ukázať (1) a (2), tak by sme mali vedieť dokázať ψ aj bez axióm teórie T.
Vieme, že (ukázali sme to v jednom z pomocných tvrdení):

$$\vdash (\varphi \longrightarrow \psi) \longrightarrow (\neg\psi \longrightarrow \neg\varphi) \quad (\star)$$

Aplikovaním modus ponens:

$$\vdash \neg\psi \longrightarrow \neg\varphi \quad (\Box)$$

Pridajme do teórie T ďalšie formule:

$$T \cup \{\neg\psi, \neg\psi \longrightarrow \neg\varphi, \neg\varphi \longrightarrow \psi\}$$

Formulu ψ v tejto teórii by sme dokázali jednoducho dvojnásobným použitím modus ponens. Teraz ale vetu o dedukcii.

$$T \cup \{\neg\psi \longrightarrow \neg\varphi, \neg\varphi \longrightarrow \psi\} \vdash \neg\psi \longrightarrow \psi \quad (\circ)$$

Aplikujme MP na $(\Box)$ a $(\circ)$.

$$T \cup \{\neg\varphi \longrightarrow \psi\} \vdash \neg\psi \longrightarrow \psi$$

Opäť použime vetu o dedukcii

$$T \vdash (\neg\varphi \longrightarrow \psi) \longrightarrow (\neg\psi \longrightarrow \psi) \quad (\bullet)$$

Ďalší MP na (2) a $(\bullet)$.

$$T \vdash \neg\psi \longrightarrow \psi \quad (\cdot)$$

Vo výrokovom počte platí tvrdenie 7 – to však znamená, že platí aj v našej teórii T:

$$T \vdash (\neg\psi \longrightarrow \psi) \longrightarrow \psi$$

A posledným MP na $(\cdot)$ a toto dostávame:

$$T \vdash \psi$$

□

[3] v literatúre sa možno stretnúť aj s označením „lema o neutrálnej formuli“

3.3 Úplnosť výrokového počtu

Veta 3.12 (o úplnosti výrokového počtu)
Ak $\models \varphi$ *potom* $\vdash \varphi$.

Dôkaz.
Myšlienka dôkazu:
Budeme to dokazovať pre každé φ zvlášť. Každé φ má nejakú množinu elementárnych výrokov $\{p_1, \ldots, p_n\}$. Vieme, že je všetkých možných ohodnotení týchto výrokov je 2^n.
Zoberme si najskôr také ohodnotenie, že všetky $p_1, \ldots, p_n$ majú hodnotu 1. Potom

$$\mathrm{EV}(\varphi)^v = \{p_1, \ldots, p_n\} \vdash \varphi^v \equiv \varphi$$

lebo $\models \varphi$
Teraz si zoberieme také ohodnotenie, že $p_1, \ldots, p_{n-1}$ majú hodnotu 1 a p_n má hodnotu 0. Podobne máme

$$\{p_1, \ldots, p_{n-1}, \neg p_n\} \vdash \varphi$$

Na základe vety o dôkaze rozborom prípadov vieme, že:

$$\{p_1, \ldots, p_{n-1}\} \vdash \varphi$$

Analogicky môžeme postupovať a odstrániť p_{n-1} atď.
Samotný dôkaz:
Nech $\mathrm{EV}(\varphi) = \{p_1, \ldots, p_n\}$ a nech

$$S = \bigcup_{k<n} {}^k 2 = {}^{<n}2,$$

teda S je úplný binárny strom. Pre každé $f \in {}^n 2$ máme nejaké v_f a $v_f(p_i) = f(i-1) \quad i < n$. Takisto pre každé $g \in {}^k 2$ máme v_g také, že $v_g(p_i) = g(i-1) \quad i < k$. Churchova (Postova) veta nám hovorila o listoch stromu S a „nahor“ sa dostaneme pomocou vety o rozbore prípadov. Keď už budeme mať dokázaný indukčný predpoklad pre uzol v strome S, tak ho dokážeme aj pre uzol nad ním.
Reformulujme si Churchovu vetu:

$$\mathrm{EV}(\varphi)^v \vdash \varphi^v$$

V našom prípade to znamená, že pre každé $f \in {}^n 2$ platí

$$\mathrm{EV}(\varphi)^{v_f} \vdash \varphi$$

(lebo $\varphi \equiv \varphi^{v_f}$). Takže pre listy stromu S to už máme dokázané, a teraz sa potrebujeme dostať vyššie.
Uveďme najprv indukčný predpoklad pre uzol $g \in {}^k 2$ kde $k < n$:

$$\begin{aligned} \{p_1^{v_g}, \ldots, p_k^{v_g}, p_{k+1}\} &\vdash \varphi \\ \{p_1^{v_g}, \ldots, p_k^{v_g}, \neg p_{k+1}\} &\vdash \varphi \end{aligned}$$

Pre ostatné uzly:

$$\begin{aligned} p_{k+1} &= p_{k+1}^{v_g \frown 1} \\ \neg p_{k+1} &= p_{k+1}^{v_g \frown 0} \end{aligned}$$

Pre indukciu musíme ešte overiť 2 veci:

1. že vieme indukciu naštartovať, teda že indukčný predpoklad platí pre zobrazenia dĺžky $k = n-1$. Ale $n-1$ je predposledná hladina stromu S. Pre listy to platí podľa Churchovej vety, čiže je to v poriadku.

Tvrdenie 4.10 (vlastnosť 8, obrátená vlastnosť 7)
Ak $x \notin FV(\nu)$*, potom platí:*

$$\vdash ((\exists x)\varphi \longrightarrow \nu) \longrightarrow (\forall x)(\varphi \longrightarrow \nu)$$

Dôkaz.
Z vlastnosti číslo 6:

$$\vdash \underbrace{(\neg\nu \longrightarrow (\forall x)\neg\varphi)}_{(\neg(\forall x)\neg\varphi \longrightarrow \neg\neg\nu)} \longrightarrow (\forall x)(\neg\nu \longrightarrow \neg\varphi)$$

Platí:

$$(\neg(\forall x)\neg\varphi \longrightarrow \neg\neg\nu) \quad \equiv \quad ((\exists x)\varphi \longrightarrow \nu)$$

Teraz chceme ukázať, že:

$$(\forall x)(\neg\nu \longrightarrow \neg\varphi) \longrightarrow (\forall x)(\varphi \longrightarrow \nu)$$

Axióma VP číslo 3 hovorí:

$$(\neg\nu \longrightarrow \neg\varphi) \longrightarrow (\varphi \longrightarrow \nu)$$

Použijeme generalizáciu (tj. dáme pred to celé $(\forall x)(\ldots)$, a potom vojdeme s kvantifikátorom dovnútra na obe miesta, čím dostaneme:

$$((\forall x)\neg\nu \longrightarrow \neg\varphi) \longrightarrow ((\forall x)\varphi \longrightarrow \nu)$$

Keď to všetko dáme dokopy:

$$((\exists x)\varphi \longrightarrow \nu) \longrightarrow (\forall x)\neg\nu \longrightarrow \neg\varphi) \longrightarrow (\forall x)(\varphi \longrightarrow \nu)$$

Tvrdenie potom vyplýva z tranzitívnosti implikácie. □

Veta 4.11 (vlastnosť 9)

$$(\exists x)(\nu \longrightarrow \varphi) \longrightarrow (\nu \longrightarrow (\exists x)\varphi),$$

ak $x \notin FV(\nu)$

Dôkaz.
Vďaka vlastnosti č.1 máme, že

$$\varphi \longrightarrow (\forall x)\varphi$$

lebo $\varphi \equiv \varphi(x/x)$ quad a x sa dá vždy substituovať samo za seba. Logicky z toho vyplýva, že:

$$\varphi \longrightarrow (\exists x)\varphi$$

Vo výrokovom počte sme mali

$$\varphi \longrightarrow \varphi$$

teda nasledovná formula je tautológia.

$$\vdash (\nu \longrightarrow \varphi) \longrightarrow (\nu \longrightarrow \varphi)$$

Treba nám overiť nasledujúcu formulu:

$$(p \longrightarrow (q \longrightarrow r)) \longrightarrow (r \longrightarrow s) \longrightarrow (p \longrightarrow (q \longrightarrow s))$$

To však platí, jej dôkaz vo výrokovom počte získame dvojnásobným použitím modus ponens na axiómy výrokového počtu. Formula sa dá prepísať na:

$$\Big((p \longrightarrow (q \longrightarrow r)) \wedge (r \longrightarrow s)\Big) \longrightarrow (p \longrightarrow (q \longrightarrow s))$$

$\vdash (\forall x)\varphi \longrightarrow \varphi$	
$\vdash (\nu \longrightarrow \varphi) \longrightarrow (\nu \longrightarrow \varphi)$	
$\vdash (\nu \longrightarrow (\forall x)\varphi) \longrightarrow (\nu \longrightarrow \varphi)$	dá sa overiť vo VP
$\vdash (\forall x)((\nu \longrightarrow (\forall x)\varphi) \longrightarrow (\nu \longrightarrow \varphi))$	generalizácia
$\vdash (\nu \longrightarrow (\forall x)\varphi) \longrightarrow (\forall x)(\nu \longrightarrow \varphi)$	axióma 5

□

Ukázali sme si teda, že ak máme nejakú tautológiu výrokového počtu φ, kde $\mathrm{EV}(\varphi) = \{p_1, \ldots, p_n\}$, potom pre ľubovoľné formuly predikátového počtu $\varphi_1, \ldots, \varphi_n$ je formula $\varphi(p_1/\varphi_1, \ldots, p_n/\varphi_n)$ tautológia, a naviac dôkaz z výrokového počtu sa dá prepísať do predikátového počtu – stačí zobrať dôkaz z výrokového počtu a všetky p_i nahradiť φ_i pre každé i. Ak bol nejaký člen dôkazu axiómou výrokového počtu, potom aj po substitúcii je axiómou predikátového počtu, lebo všetky axiómy výrokového počtu sú axiómami aj v predikátovom počte.
Z úplnosti výrokového počtu vieme, že ak je φ tautológia, tak jej dôkaz existuje.

Tvrdenie 4.9 (vlastnosť 7)
Ak $x \notin FV(\nu)$, potom

$$(\forall x)(\varphi \longrightarrow \nu) \longrightarrow ((\exists x)\varphi \longrightarrow \nu)$$

Dôkaz.
Už sme si ukázali korektnosť tvrdenia

$$(\forall x)(\neg\nu \longrightarrow \neg\varphi) \longrightarrow (\neg\nu \longrightarrow (\forall x)\neg\varphi)$$

To môžeme ekvivalentne napísať ako

$$(\forall x)(\neg\nu \longrightarrow \neg\varphi) \longrightarrow \underbrace{(\neg(\forall x)\neg\varphi \longrightarrow \nu)}_{((\exists x)\varphi\longrightarrow\nu)}$$

Máme už pravú časť tvrdenia, už stačí len ukázať, že

$$(\forall x)(\varphi \longrightarrow \nu) \longrightarrow (\forall x)(\neg\nu \longrightarrow \neg\varphi)$$

Vo výrokovom počte máme axiómu:

$$(\varphi \longrightarrow \nu) \longrightarrow (\neg\nu \longrightarrow \neg\varphi)$$

My sme ale v predikátovom počte, kde môžeme používať odvodzovacie pravidlo generalizácie:

$$(\forall x)((\varphi \longrightarrow \nu) \longrightarrow (\neg\nu \longrightarrow \neg\varphi))$$

Podľa 3. vlastnosti môžeme vojsť s kvantifikátorom dovnútra (pritom nás nezaujíma, či tam sú nejaké výskyty):

$$(\forall x)(\varphi \longrightarrow \nu) \longrightarrow (\forall x)(\neg\nu \longrightarrow \neg\varphi)$$

Čiže máme:

$$(\forall x)(\varphi \longrightarrow \nu) \longrightarrow (\forall x)(\neg\nu \longrightarrow \neg\varphi) \longrightarrow ((\exists x)\varphi \longrightarrow \nu)$$

a tvrdenie vyplýva z tranzitívnosti implikácie □

Niekoľkými vlastnosťami sa tu ukazuje, že ak máme $(\heartsuit x)(\varphi \longrightarrow \psi)$ kde $\heartsuit$ je kvantifikátor, potom:

- môžeme ním vojsť dovnútra na obe miesta, pričom sa nemusíme starať o výskyty x vo formuliach φ, ψ.
- môžeme vojsť iba na jedno miesto, pokiaľ druhá formula neobsahuje voľné x, pričom:
  - ak vchádzame na druhé miesto kvantifikátor sa nemení
  - ak vchádzame na prvé miesto kvantifikátor je opačný

2. že vždy keď sa dostaneme do tejto situácie pri nejakom (ďalšom) k, vieme ukázať (pomocou vety o dôkaze rozborom prípadov), že

$$\{p_1^{v_g}, \ldots, p_k^{v_g}\} \vdash \varphi$$

Pre $k = n - 1$ je indukčný predpoklad splnený a ďalej

$$\{p_1\} \;\vdash\; \varphi$$
$$\{\neg p_1\} \;\vdash\; \varphi$$

čiže $\vdash \varphi$. □

Dôkaz je exponenciálnej zložitosti.

4 Predikátový počet *revisited*

Poznámka 4.1
V ďalšom sa budeme snažiť získať základy na formalizáciu deklaratívnej stránky výpočtových procesov. Cieľom ďalších úvah bude ukázať, že platí

$$\emptyset \vdash \varphi \;\text{ akk }\; \emptyset \models \varphi$$

Pripomenieme najprv množinu axióm výrokového počtu:

Ax. 1 $\varphi \longrightarrow (\psi \longrightarrow \varphi)$

Ax. 2 $(\varphi \longrightarrow (\psi \longrightarrow \chi)) \longrightarrow ((\varphi \longrightarrow \psi) \longrightarrow (\varphi \longrightarrow \chi))$

Ax. 3 $(\neg\psi \longrightarrow \neg\varphi) \longrightarrow (\varphi \longrightarrow \psi)$

Za základ našich úvah by sme mohli zobrať inú množinu axióm. Napríklad množinu

$$\mathrm{LA}_2 = \{\varphi : \models \varphi\}$$

Je to množina všetkých tautológií výrokového počtu. Overenie je možné v čase 2^n, kde n je počet výrokov. Túto množinu je možné generovať a zostaviť pre ňu syntaktický analyzátor[4]. Dokázateľnosť výrokov pri takejto množine axióm je triviálna[5]. Čitateľ ľahko vidí, že tento systém nie je efektívny. Naša množina axióm je efektívna v tom zmysle, že overenie tautologičnosti má lineárnu časovú zložitosť vzhľadom na dĺžku výroku. Vždy musíme o množine axióm uvažovať ako o vstupnom parametre systému.
Prejdime však k predikátovému počtu, ktorý je pre nás dôležitejší[6]. Axiomatiku vybudujeme na množine axióm výrokového počtu, ktorú rozšírime o 2 axiómy:

Ax. 4 ak $\mathsf{Suble}(t, x, \varphi)$, tak $\forall x\varphi \longrightarrow \varphi(x/t)$[7]

Ax. 5 ak $x \notin \mathrm{FV}(\nu)$, tak $(\forall x)(\nu \longrightarrow \varphi) \longrightarrow (\nu \longrightarrow \forall x\varphi)$

Pripomeňme ešte, že $\models \varphi$ znamená, že formula φ je pravdivá v každom modeli, pri každom ohodnotení premenných. Z uvedeného ľahko vidno, že v prípade predikátového počtu nemôžeme vytvoriť množinu axióm zo všetkých tautológií, pretože nestačí uvažovať všetky ohodnotenia, ale aj všetky modely. Vetu o korektnosti predikátového počtu sme už dokázali, chceli by sme ukázať aj druhý pohľad – úplnosť. V ďalších úvahách je dôležité si uvedomiť, že vlastnosti a dôkazy z výrokového počtu sú správne aj v predikátovom počte, lebo nemeníme štruktúru zloženia formúl. Začneme nasledujúcim tvrdením:

[4] t.j. možno zostrojiť Turingov stroj, ktorý rozpoznáva tautológie
[5] dôkaz má dĺžku 1
[6] to je totiž teória databáz
[7] je to vlastne volanie procedúry

4.1 Niektoré vety predikátového počtu

Tvrdenie 4.2 (vlastnosť 1)
Ak $\mathsf{Suble}(t, x, \varphi)$, *tak*

$$\vdash \varphi(x/t) \longrightarrow (\exists x)\varphi$$

<u>Dôkaz.</u>

$\exists x\varphi \equiv \neg\forall\neg\varphi$	zrejme platí
$\vdash \neg\neg\underbrace{(\forall x)\neg\varphi} \longrightarrow \underbrace{(\forall x)\neg\varphi}$	vlastnosť VP
$\vdash (\forall x)\neg\varphi \longrightarrow \neg\varphi(x/t)$	axióma 4, ak $\mathsf{Suble}(t, x, \varphi)$, tak $\mathsf{Suble}(t, x, \neg\varphi)$ - SSF
$\vdash \neg\underbrace{\neg(\forall x)\neg\varphi}_{(\exists x)\varphi} \longrightarrow \neg\varphi(x/t)$	tranzitívnosť $\longrightarrow$
$\vdash \varphi(x/t) \longrightarrow (\exists x)\varphi$	axióma 3

□

Poznámka 4.3
Axióma 4 hovorí, že ak formula φ platí pre každé x, tak platí aj pre objekty, ktoré nemajú meno. Musíme si dať pozor na substituovateľnosť! Ak máme premenné v terme, musíme ich „rozdisjunktniť“.

Tvrdenie 4.4 (vlastnosť 2)

$$\vdash (\forall x)\varphi \longrightarrow (\exists x)\varphi$$

<u>Dôkaz.</u>

$\vdash (\forall x)\varphi \longrightarrow \varphi(x/x)$	zrejme platí $\mathsf{Suble}(x, x, \varphi)$, Axióma 4
$\vdash \varphi(x/x) \longrightarrow (\exists x)\varphi$	podľa lemmy 1
$\vdash (\forall x)\varphi \longrightarrow (\exists x)\varphi$	z tranzitívnosti $\longrightarrow$

□

Tvrdenie 4.5 (vlastnosť 3)

$$\vdash (\forall x)(\varphi \longrightarrow \psi) \longrightarrow ((\forall x)\varphi \longrightarrow (\forall x)\psi)$$

<u>Dôkaz.</u>

$\vdash (\forall x)(\varphi \longrightarrow \psi) \longrightarrow (\varphi \longrightarrow \psi)$	axióma 4
$\vdash (\forall x)\varphi \longrightarrow \varphi$	axióma 4

Tieto formule sú (z hľadiska výrokového počtu) tvaru:

$$p \longrightarrow (\varphi \longrightarrow \psi)$$

$r \longrightarrow \varphi$
$?\{p \longrightarrow (\varphi \longrightarrow \psi), r \longrightarrow \varphi\} \vdash p \longrightarrow (r \longrightarrow \psi)$
$?\{p \longrightarrow (\varphi \longrightarrow \psi), r \longrightarrow \varphi\} \vdash ((p \longrightarrow (\varphi \longrightarrow \psi)) \longrightarrow (r \longrightarrow \varphi)) \longrightarrow (p \longrightarrow (r \longrightarrow \psi))$
Je možné, aby výrok mal hodnotu 0? Skúsme nájsť také ohodnotenie elementárnych výrokov, aby mal hodnotu 0: $\underbrace{((p \longrightarrow (\varphi \longrightarrow \psi)) \longrightarrow (r \longrightarrow \varphi))}_{1} \longrightarrow \underbrace{(p \longrightarrow (r \longrightarrow \psi))}_{0}$
$\underbrace{((p \longrightarrow (\varphi \longrightarrow \psi)) \longrightarrow (r \longrightarrow \varphi))}_{1} \longrightarrow (\underbrace{p}_{1} \longrightarrow \underbrace{(r \longrightarrow \psi)}_{0})$

$$\underbrace{((p \longrightarrow (\varphi \longrightarrow \psi)) \longrightarrow (r \longrightarrow \varphi))}_{1} \longrightarrow (\underbrace{p}_{1} \longrightarrow (\underbrace{r}_{1} \longrightarrow \underbrace{\psi}_{0}))$$

$$\underbrace{((\underbrace{p}_{1} \longrightarrow (\varphi \longrightarrow \underbrace{\psi}_{0})) \longrightarrow (\underbrace{r}_{1} \longrightarrow \varphi))}_{1} \longrightarrow \underbrace{(\underbrace{p}_{1} \longrightarrow (\underbrace{r}_{1} \longrightarrow \underbrace{\psi}_{0}))}_{0}$$

$$\underbrace{\underbrace{((\underbrace{p}_{1} \longrightarrow (\underbrace{\varphi}_{1} \longrightarrow \underbrace{\psi}_{0}))}_{0} \longrightarrow \underbrace{(\underbrace{r}_{1} \longrightarrow \underbrace{\varphi}_{1}))}_{1}}_{1} \longrightarrow \underbrace{(\underbrace{p}_{1} \longrightarrow (\underbrace{r}_{1} \longrightarrow \underbrace{\psi}_{0}))}_{0}$$

Výrok $p \longrightarrow (\varphi \longrightarrow \psi)$ má hodnotu 0, čo je v spore s predpokladom. Platí

$$\{p \longrightarrow (\varphi \longrightarrow \psi), r \longrightarrow \varphi\} \vdash p \longrightarrow (r \longrightarrow \psi)$$

$\vdash (\forall x)(\varphi \longrightarrow \psi) \longrightarrow ((\forall x)\varphi \longrightarrow \psi)$	$p \eqcirc (\forall x)(\varphi \longrightarrow \psi), r \eqcirc (\forall x)\varphi$
$\vdash (\forall x)((\forall x)(\varphi \longrightarrow \psi) \longrightarrow ((\forall x)\varphi \longrightarrow \psi))$	generalizácia
$\vdash (\forall x)(\varphi \longrightarrow \psi) \longrightarrow (\forall x)((\forall x)\varphi \longrightarrow \psi)$	Ax5
$\vdash (\forall x)(\varphi \longrightarrow \psi) \longrightarrow ((\forall x)\varphi \longrightarrow (\forall x)\psi)$	Ax5

□

Tvrdenie 4.6 (vlastnosť 4)

$$\vdash (\forall x)(\varphi \longrightarrow \psi) \longrightarrow ((\exists x)\varphi \longrightarrow (\exists x)\psi)$$

<u>Dôkaz.</u>

$\vdash (\varphi \longrightarrow \psi) \longrightarrow (\neg\psi \longrightarrow \neg\varphi)$	tvrdenie z výrokového počtu
$\vdash (\forall x)((\varphi \longrightarrow \psi) \longrightarrow (\neg\psi \longrightarrow \neg\varphi))$	generalizácia
$\vdash (\forall x)(\varphi \longrightarrow \psi) \longrightarrow (\forall x)(\neg\psi \longrightarrow \neg\varphi)$	
$\vdash (\forall x)(\varphi \longrightarrow \psi) \longrightarrow (\forall x\neg\psi \longrightarrow \forall x\neg\varphi)$	
$\vdash (\forall x)(\varphi \longrightarrow \psi) \longrightarrow (\neg\forall x\neg\varphi \longrightarrow \neg\forall x\neg\psi)$	
$\vdash (\forall x)(\varphi \longrightarrow \psi) \longrightarrow ((\exists x)\varphi \longrightarrow (\exists x)\psi)$	

□

Tvrdenie 4.7 (vlastnosť 5)
Ak $x \notin FV(\nu)$, *tak:*

$$\vdash (\forall x)\nu \equiv \nu$$

<u>Dôkaz.</u>
$\Rightarrow$:

$$\vdash (\forall x)\nu \longrightarrow \nu(x/x) \eqcirc \nu$$

$\Leftarrow$:

$\vdash \nu \longrightarrow \nu$	tvrdenie z výrokového počtu
$\vdash (\forall x)(\nu \longrightarrow \nu)$	generalizácia
$\vdash \nu \longrightarrow (\forall x)\nu$	Ax5

□

Tvrdenie 4.8 (vlastnosť 6)
Ak $x \notin FV(\nu)$, *tak:*

$$\vdash (\nu \longrightarrow (\forall x)\varphi) \longrightarrow (\forall x)(\nu \longrightarrow \varphi)$$

<u>Dôkaz.</u>