Prírodovedecká fakulta UPJŠ Košice

Funkcionálne a logické programovanie

(poznámky z prednášok, verzia 2002/03)

prednáša: Prof. RNDr. Peter Vojtáš, DrSc.

Obsah

1 Teória množín **3**
1.1 Množiny . . . 3
1.1.1 Základné tvrdenia o množinách . . . 4
1.1.2 Základné definície a tvrdenia o reláciách . . . 4
1.2 Relácie a zobrazenia . . . 6
1.2.1 Matematická reprezentácia relácií . . . 6
1.2.2 Informatická reprezentácia relácií. . . . 9
1.3 Ordinálne čísla . . . 12
1.4 Stromy . . . 12

2 Výrokový počet **15**
2.1 Základné definície . . . 15
2.2 Ohodnotenie výrokov . . . 18
2.3 Tautológie . . . 19
2.4 Dôkaz a dokázateľnosť vo výrokovom počte . . . 21
2.5 Korektnosť výrokového počtu . . . 22

3 Predikátový počet **24**
3.1 Syntax predikátového počtu . . . 24
3.2 Sémantika predikátového počtu . . . 30

Literatúra

[1] Kolár, Štěpánková, Chytil – Logika, algebry a grafy. SNTL 89. Kap. 1. str. 17-21. Kap. 4. str. 92-123.

[2] Balcar, Štěpánek – Teórie množín. Kap. I §4, §5.

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

Funkcionálne a logické programovanie, Prírodovedecká fakulta UPJŠ Košice
Predmet: KMA/FLP1a/01
Prednáša: Prof. RNDr. Peter Vojtáš, DrSc.

V systéme LaTeX vysádzali: Ladislav Pálfi a Róbert Novotný (r.novotny@szm.sk)
Odborná korektúra: Marián Dvorský (marian@step.sk)
URL: http://skmi.science.upjs.sk/~novotnyr
Verzia 30. 5. 2003 (X_2)

1 Teória množín

1.1 Množiny

Množiny sú abstraktné dátové štruktúry, ktoré sa priamo fyzicky ťažko implementujú (konkrétne dátové nosiče sú usporiadané lepšie pre zoznamy postupnosti) - pre nás to bude teraz jazyk metamatematiky (rozpor DB relácie množina $\times$ fyzicky).

Príklady: $\begin{cases} \text{vymenovaním prvkov:} & \{a,b,c\} \quad \emptyset \\ \text{vlastnosťou:} & \{x : \varphi(x)\} \quad \{x : x \in A \,\&\, \varphi(x)\} \end{cases}$

V množine nezáleží na poradí, prvky sa neopakujú, množina $\{x,y\}$ označuje dvojprvkovú množinu, ak náhodou $x = y = a$ potom je $\{x,y\} = \{a\}$

Označenie 1.1

- množiny veľkými písmenami $(A, B, C, X, Y, \ldots)$
- systémy množín veľkými písanými písmenami $(\mathcal{A}, \mathcal{B}, \mathcal{C}, \ldots)$
- prvky množiny spravidla malými písmenami $(x, y, \ldots)$

Axióma 1.2 (extenzionality)

$$(\forall A, B)\ [(\forall x)(x \in A \longleftrightarrow x \in B) \longleftrightarrow (A = B)]$$

Táto axióma je základným prostriedkom pre rovnosť dvoch množín:
ak $A \subseteq B$, $A \supseteq B$, potom $A = B$ (dôkaz sa často rozdelí na dve časti).

Poznámka 1.3
$(\forall x)(x \in A \longleftrightarrow \varphi(x))$ vyjadríme ako $A = \{x \ : \ \varphi(x)\}$

Definícia 1.4
Zadefinujme nasledovné operácie na množinách:

- $A \cap B = \{x : x \in A \,\&\, x \in B\}$
- $A \cup B = \{x : x \in A \vee x \in B\}$
- $A - B = \{x : x \in A \,\&\, x \notin B\}$
- $\bigcup \mathcal{A} = \{x : (\exists A)(A \in \mathcal{A} \,\&\, x \in A)\} \qquad \bigcup\{A, B\} = A \cup B$
- $\bigcap \mathcal{A} = \{x : (\forall A)(A \in \mathcal{A} \longrightarrow x \in A)\} \qquad \bigcap\{A, B\} = A \cap B$
- $\mathcal{P}(A) = \{B : B \subseteq A\}$

Poznámka 1.5
Sme v metamatematike, ešte nemáme logiku; všetky spojky, kvantory sú skratky pre „slovenské“ výrazy.

1.1.1 Základné tvrdenia o množinách

Lemma 1.6
Pre ľubovoľné množiny X, Y, Z platí

(i) $X = X \cap X = X \cup X$ *(zákon idempotencie)*

(ii) $X \cup Y = Y \cup X$
$X \cap Y = Y \cap X$ *(komutatívnosť)*

(iii) $(X \cap Y) \cap Z = X \cap (Y \cap Z)$
$(X \cup Y) \cup Z = X \cup (Y \cup Z)$ *(asociatívnosť)*

(iv) $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$
$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$ *(distributívnosť)*

Lemma 1.7
$X \cap Y \subseteq X \subseteq X \cup Y$
$X \cap Y \subseteq Y \subseteq X \cup Y$
$X \subseteq Y \longleftrightarrow X \cup Y = Y$
$X \subseteq Y \longleftrightarrow X \cap Y = X$
Pre každé U také, že $X, Y \subseteq U$, platí $X \subseteq Y \longleftrightarrow U - Y \subseteq U - X$

De Morganove pravidlá:
$X - (Y_1 \cup Y_2) = (X - Y_1) \cap (X - Y_2)$
$X - (Y_1 \cap Y_2) = (X - Y_1) \cup (X - Y_2)$

Lemma 1.8
$(X - Y) - Z = X - (Y \cup Z)$
$X - (Y - Z) = (X - Y) \cup (X \cup Z)$
rozdiel nie je associatívny (ani komutatívny)

1.1.2 Základné definície a tvrdenia o reláciách

Definícia 1.9
Usporiadaná dvojica $\langle a, b\rangle$ je množina definovaná vzťahom

$$\langle a, b\rangle = \{\{a\}, \{a, b\}\}$$

Lemma 1.10
$\langle x, y\rangle = \langle u, v\rangle \longleftrightarrow (x = u \;\&\; y = v)$

Dôkaz.
$\longleftarrow$
ak $x = u$ a $y = v$ potom $\{x\} = \{u\}$ a $\{x, y\} = \{u, v\}$
$\longrightarrow$
$\{\{x\}, \{x, y\}\} = \{\{u\}, \{u, v\}\}$
vezmime $\{u\}$, to sa rovná $\begin{cases} \text{buď } \{u\} = \{x\} \longrightarrow x = u \\ \text{alebo } \{u\} = \{x, y\} \longrightarrow x = u \end{cases}$
a súčasne
vezmime $\{u, v\}$, to je tiež $\begin{cases} \text{buď } \{u, v\} = \{x\} \longrightarrow v = x \\ \text{alebo } \{u, v\} = \{x, y\} \longrightarrow v = x \vee v = y \end{cases}$

Ak $u = x$ a súčasne $v = y$ sme hotoví.
Ak $u = x$ a súčasne $v = x$ potom $\{u, v\} = \{x\}$. Odtiaľ

$$\{\{x\}, \{x, y\}\} = \{\{u\}, \{u, v\}\} = \{\{x\}, \{x\}\} = \{\{x\}\}$$

a teda $\{x, y\} = \{x\}$, z toho $y = x$. Na záver teda $u = v = y = x$. □

Definícia 1.11
Kartézsky súčin množín A a B je definovaný:

$$A \times B = \{\langle a, b\rangle : a \in A \,\&\, b \in B\}$$

Poznámka 1.12
Platí:

- $A \times B = \emptyset$ akk $(A = \emptyset \vee B = \emptyset)$
- Ak $A \times B \neq \emptyset$ potom $A \times B = C \times D \longrightarrow A = C \,\&\, B = D$
- $A \subseteq A_1$ a $B \subseteq B_1$ potom $A \times B \subseteq A_1 \times B_1$

Lemma 1.13
(i) $A \times (B_1 \cup B_2) = (A \times B_1) \cup (A \times B_2)$
$(A_1 \cup A_2) \times B = (A_1 \times B) \cup (A_2 \times B)$

(ii) $A \times (B_1 \cap B_2) = (A \times B_1) \cap (A \times B_2)$
$(A_1 \cap A_2) \times B = (A_1 \times B) \cap (A_2 \times B)$

(iii) $A \times (B_1 - B_2) = (A \times B_1) - (A \times B_2)$
$(A_1 - A_2) \times B = (A_1 \times B) - (A_2 \times B)$

Lemma 1.14

$$A \times B \subseteq \mathcal{P}(\mathcal{P}(A \cup B))$$

Dôkaz.
Nech $\langle u, v\rangle \in A \times B$.

Potom pre $\{\{u\}, \{u, v\}\} = \langle u, v\rangle$ platí: $\left\{ \begin{array}{l} u \in A \text{ a teda } \{u\} \subseteq A \subseteq A \cup B \\ \text{a zároveň} \\ v \in B \text{ a teda } \{u, v\} \subseteq A \cup B \end{array} \right.$.

Odtiaľ

$$\{u\} \in \mathcal{P}(A \cup B) \text{ a súčasne } \{u, v\} \in \mathcal{P}(A \cup B)$$

z toho

$$\begin{array}{rcl} \{\{u\}, \{u, v\}\} & \subseteq & \mathcal{P}(A \cup B) \\ \{\{u\}, \{u, v\}\} & \in & \mathcal{P}(\mathcal{P}(A \cup B)) \\ \langle u, v\rangle & \in & \mathcal{P}(\mathcal{P}(A \cup B)) \end{array}$$

□

Lemma 1.15
Ak $A \neq \emptyset$ a $B \neq \emptyset$ potom

$$A \cup B \subseteq \bigcup(\bigcup(A \times B))$$

Dôkaz.
Nech $u \in A$, $v \in B$ sú ľubovoľné, ale pevne zvolené.
Potom:

$$\begin{aligned} \{\{u\},\{u,v\}\} &\in A \times B \\ \{u\},\{u,v\} &\in \bigcup(A \times B) \\ u, v &\in \bigcup(\bigcup(A \times B)) \end{aligned}$$

□

1.2 Relácie a zobrazenia

Poznámka 1.16 (Motivácia)
Motivácia:

$$\text{Modelovanie moderného sveta} \begin{cases} \textit{relácie} \text{ (vzťahy medzi ľuďmi, organizáciami, štátmi, \ldots)} \\ \text{ale aj objekt a jeho vlastnosti (}\textit{atribúty}\text{).} \end{cases}$$

Napr. vzťah otec – matka – dieťa, alebo matematické relácie $2 \leq 3, (2+3)^2 = 25$

Rozvrhová akcia má hodnoty, parametre, atribúty – miesto, čas, učiteľ, skupina, predmet.
Zákazník banky - meno, adresa, číslo účtu, história stavu účtu.
Nákupný košík - zákazník, jeho atribúty, čo kúpil, ako platil, aké má auto.

$$\text{modelovanie sveta} \begin{cases} \text{v prirodzenom jazyku (vágne, subjektívne)} \\ \text{databázy, informačné systémy (DBS, IFS)} \\ \text{matematické a formálne modely} \\ \ldots \end{cases}$$

Džungľa elektronických dát, modelovanie znalostí (nekonkrétny SW alebo princípy, metódy a nové výsledky)
Znalosti, napr.

- ak má pacient horúčku, vysoké biele krvinky, RTG pozitívne, potom sa stanoví diagnóza Dg
- mladému nezamestnanému banka nedá úver – malá šanca, že ho splatí.

1.2.1 Matematická reprezentácia relácií

Definícia 1.17
Množina R je (*binárna matematická*) *relácia* ak existujú A a B také, že

$$R \subseteq A \times B.$$

Príklad 1.18
$R = \{\{\{a\},\{a,b\}\},\{\{a\},\{a,c\}\},\{\{b\},\{b,d\}\}\} \subseteq \{a,b\} \times \{b,c,d\}$
$S = \{a, \langle a,b\rangle, \langle a,c\rangle, d\}$ („pomiešaná“ množina)
Tieto množiny budeme využívať v príkladoch.

Poznámka 1.19
Poznamenajme, že niektoré relácie píšeme infixne, tj. $x \leq y$ akk $\langle x,y\rangle \in \leq$, $x = y$ akk $\langle x,y\rangle \in =$. Niekedy $\langle x,y\rangle \in R$ píšeme tiež $x\ R\ y$.

Definícia 1.20
Nech X je množina, potom

$$\begin{aligned}\mathrm{dom}(X) &= \{u : (\exists v)(\langle u, v\rangle \in X)\}\\ \mathrm{rng}(X) &= \{v : (\exists u)(\langle u, v\rangle \in X)\}\end{aligned}$$

Pozorovanie 1.21
Ak $R \subseteq A \times B$ *potom* $\mathrm{dom}(R) \subseteq A$ *a* $\mathrm{rng}(R) \subseteq B$. *Ak* R *je relácia, potom* $R \subseteq \mathrm{dom}(R) \times \mathrm{rng}(R)$.

Príklad 1.22
Pre množiny z príkladu 1.18 platí:

$$\begin{aligned}\mathrm{dom}(R) = \{a, b\}, &\qquad \mathrm{rng}(R) = \{b, c, d\}\\ \mathrm{dom}(S) = \{a\}, &\qquad \mathrm{rng}(S) = \{b, c\}\end{aligned}$$

Definícia 1.23
Nech X a Y sú množiny. Potom

$$\begin{aligned}X \,''\, Y &= \{z : (\exists y)(y \in Y \,\&\, \langle y, z\rangle \in X)\}\\ X \restriction Y &= \{\langle y, z\rangle : y \in Y \,\&\, \langle y, z\rangle \in X\}\end{aligned}$$

$X \,''\, Y$ čítame „obraz X na Y“.
$X \restriction Y$ čítame „X zúžené na Y“.

Príklad 1.24
Majme danú reláciu $\leq$ na množine $(0; 1)$. Nájdite

$$\leq \,''\, (0,5; 0,7), \qquad \leq \restriction (0,6; 0,9)$$

Pre množiny R a S z príkladu 1.18 platí:

$$S \,''\, \{d\} = \emptyset, R \,''\, \{a\} = \{b, c\}, S \restriction \{a\} = \{\langle a, b\rangle, \langle a, c\rangle\}, R \restriction \{b\} = \{\langle b, d\rangle\}$$

Lemma 1.25

$$\begin{array}{rcl} Y \subseteq Z & \textit{potom} & X \restriction Y \subseteq X \restriction Z\\ Y \subseteq Z & \textit{potom} & X \,''\, Y \subseteq X \,''\, Z\\ X \,''\, (Y \cup Z) & = & X \,''\, Y \cup X \,''\, Z\\ X \,''\, (X \cap Z) & \subseteq & X \,''\, Y \cap X \,''\, Z\\ X \,''\, Y - X \,''\, Z & \subseteq & X \,''\, (Y - Z)\end{array}$$

Úloha 1.26
Nájdite protipríklady na obrátené inklúzie a implikácie v predošlej lemme.

Definícia 1.27
Pre ľubovoľné relácie R a S definujeme

$$\begin{aligned}R^{-1} &= \{\langle u, v\rangle : \langle v, u\rangle \in R\}\\ R \circ S &= \{\langle u, v\rangle : (\exists w)(\langle u, w\rangle \in R \,\&\, \langle w, v\rangle \in S)\}\end{aligned}$$

Lemma 1.28
Pre ľubovoľné relácie R a S platí

$$\begin{array}{rcl}
\mathrm{dom}(R^{-1}) & = & \mathrm{rng}(R) \\
\mathrm{rng}(R^{-1}) & = & \mathrm{dom}(R) \\
R & = & (R^{-1})^{-1} \\
\mathrm{dom}(R \circ S) & \subseteq & \mathrm{dom}(R) \\
\mathrm{rng}(R \circ S) & \subseteq & \mathrm{rng}(S) \\
(R \circ S)^{-1} & = & S^{-1} \circ R^{-1} \\
R \circ (S \circ T) & = & (R \circ S) \circ T
\end{array}$$

Definícia 1.29
Relácia $F \subseteq A \times B$ sa nazýva *zobrazenie* (*funkcia*) z A do B, ak pre každé $a \in A$ a $b_1, b_2 \in B$ platí

$$(\langle a, b_1 \rangle \in F \;\; \& \;\; \langle a, b_2 \rangle \in F) \longrightarrow b_1 = b_2$$

Poznámka 1.30
Ak F je zobrazenie, potom fakt $\langle u, v \rangle \in F$ zapisujeme tiež $F(u) = v$.
Upozorňujeme, že pojem zobrazenie má iný význam v počítačovej grafike a funkcia môže mať v OOP tiež iný význam.

Príklad 1.31
Pre ľubovoľné A, B, je $\emptyset$ zobrazenie z A do B.

Dôkaz.
Zjavne $\emptyset \subseteq A \times B$. Keďže pre každé $a \in A, b \in B$ $\langle a, b \rangle \notin \emptyset$, potom je podmienka v definícií zobrazenia triviálne splnená (Ľavá časť implikácie je vždy nepravda, teda cela implikácia je vždy splnená.).

□

Definícia 1.32
Množina všetkých zobrazení z A do B je definovaná vzťahom

$${}^{A}B = \{f : f \text{ je zobrazenie z } A \text{ do } B \text{ také, že } \mathrm{dom}(f) = A\}$$

Definícia 1.33
Usporiadaná n-tica (kde n je metamatematické prirodzené číslo) sa definuje postupne pomocou operácie usporiadanej dvojice takto:

$$\begin{array}{rcl}
\langle x_1, x_2, x_3 \rangle & = & \langle \langle x_1, x_2 \rangle, x_3 \rangle \\
\langle x_1, x_2, x_3, x_4 \rangle & = & \langle \langle x_1, x_2, x_3 \rangle, x_4 \rangle \\
 & \ldots & \\
\langle x_1, \ldots, x_n \rangle & = & \langle \langle x_1, \ldots, x_{n-1} \rangle, x_n \rangle
\end{array}$$

Kartézsky súčin usporiadanej n-tice množín $\langle A_1, \ldots, A_n \rangle$ sa definuje podobne

$$\begin{array}{rcl}
(A_1 \times A_2 \times A_3) & = & (A_1 \times A_2) \times A_3 \\
 & \ldots & \\
\prod_{i=1}^{n} A_i & = & \prod_{i=1}^{n-1} A_i \times A_n
\end{array}$$

Množina je *n-árna relácia*, ak existujú $A_1, \ldots, A_n$ také, že

$$R \subseteq A_1 \times \ldots \times A_n$$

Poznámka 1.34
Tento striktne exaktný prístup má nevýhodu, že n-árna relácia je vlastne binárnou reláciou na množinách $(A_1 \times \ldots \times A_{n-1})$ a A_n. Preto niekedy abstrahujeme od poradia použitia operácie $\langle x, y\rangle$ a *stotožňujeme* všetky možné zátvorkovanie *pokiaľ sa zachováva poradie.*
Stotožňujeme:

- $\langle x_1, x_2, x_3\rangle \approx \langle x_1, \langle x_2, x_3\rangle\rangle \approx \langle\langle x_1, x_2\rangle, x_3\rangle$
- $\langle x_1, x_2, x_3, x_4\rangle \approx \langle\langle x_1, x_2, x_3\rangle, x_4\rangle \approx \langle\langle x_1, x_2\rangle, \langle x_3, x_4\rangle\rangle \approx \langle x_1, \langle x_2, x_3, x_4\rangle\rangle$
  $\approx \langle\langle\langle x_1, x_2\rangle, x_3\rangle, x_4\rangle \approx \langle\langle x_1, \langle x_2, x_3\rangle\rangle, x_4\rangle \approx \langle x_1, \langle x_2, \langle x_3, x_4\rangle\rangle\rangle$

Úloha 1.35
Koľko možných spôsobov zátvorkovania máme pre usporiadanú n-ticu?

1.2.2 Informatická reprezentácia relácií.

Príklad 1.36
Predpokladajme, že máme databázovú schému rozvrhu na našej fakulte

$$\textsc{Rozvrh}(\textit{miesto, čas, učiteľ, skupina, predmet})$$

a konkrétna realizácia rozvrhu obsahuje záznamy napr.

$$\begin{array}{rcl}
\langle \text{P8, Ut } 8^{45}\text{, PV, 2I, KMI/FLP1a}\rangle & \in & \textsc{Rozvrh} \\
\langle \text{P1, Št } 7^{00}\text{, VG, 2I, KMI/AFJ1a}\rangle & \in & \textsc{Rozvrh} \\
\langle \text{P8, Št } 9^{30}\text{, SK, 2I, KMI/DBS1b}\rangle & \in & \textsc{Rozvrh} \\
\langle \text{P1, Št } 15^{00}\text{, PE, 2I, KMI/OOP1e}\rangle & \in & \textsc{Rozvrh}
\end{array}$$

Potom tu platia funkčné závislosti:

- {miesto, čas} určuje {predmet, učiteľa}
- {predmet, skupina, učiteľ} určuje {poslucháreň, čas}

Potrebujeme modelovať viacárne relácie, ako tu 5-árne, ale potrebujeme zachovať aj „význam“. T.j. keď si predstavíme, že máme inú databázu technického vybavenia so schémou

$$\textsc{Technika}(\textit{poslucháreň, spätný projektor, dátový projektor})$$

so záznamami

$$\begin{array}{rcl}
\langle \text{P8, ÁNO, NIE}\rangle & \in & \textsc{Technika} \\
\langle \text{P1, ÁNO, ÁNO}\rangle & \in & \textsc{Technika}
\end{array}$$

a inú schému požiadaviek na predmet

$$\textsc{Požiadavky}(\textit{predmet, spätný projektor, dátový projektor})$$

so záznamami

$$\begin{array}{rcl}
\langle \text{KMI/DBS1b, ÁNO, ÁNO}\rangle & \in & \textsc{Požiadavky} \\
\langle \text{KMI/OOP1e, ÁNO, ÁNO}\rangle & \in & \textsc{Požiadavky}
\end{array}$$

S použitím matematickej reprezentácie relácií ťažko zistíme, či učiteľ má alebo nemá požadované vybavenie pre svoju prednášku.

Definícia 1.37
Nech I je množina indexov. Zobrazenie F také, že $\mathrm{dom}(F) = I$ nazývame indexovaným súborom množín $\{F(i) : i \in I\}$. V prípade, že $r(A_1, \dots, A_n)$ je relačná schéma a množina indexov $\mathcal{A} = \{A_1, \dots, A_n\}$ je množinou atribútov tejto schémy, potom je indexovaný súbor množín $\{D(A) : A \in \mathcal{A}\}$ nazývaný aj indexovaným súborom domén atribútov relačnej schémy $r(A_1, \dots, A_n)$.

Príklad 1.38
Majme schému

$$\textsc{Rozvrh}(\textit{miesto, čas, učiteľ, skupina, predmet})$$

potom

$$\begin{array}{rcl} \text{D(miesto)} & = & \{\text{P1, P2, \dots, P8, \dots, M5, \dots}\} \\ \text{D(čas)} & = & \{\text{Po } 7^{00}, \text{Po } 7^{15}, \dots, \text{Po } 18^{00}, \text{Ut } 7^{00}, \dots\} \\ \text{D(učiteľ)} & = & \{\text{GA, VG, SK, PV, \dots}\} \\ \text{D(skupina)} & = & \{\text{1I, 2I, 2MI, 2FI,\dots}\} \\ \text{D(predmet)} & = & \{\text{KMI/FLP1a, KMI/AFJ1a, KMI/DBS1b,\dots}\} \end{array}$$

je indexovaným súborom domén atribútov pre UPJŠ.

Definícia 1.39
Nech $r(A_1, \dots, A_n)$ je relačná schéma a $\{D(A) : A \in \mathcal{A}\}$ je indexovaný súbor domén jej atribútov ($D : \mathcal{A} \longrightarrow X$). Potom informatická reprezentácia relačnej schémy $r(A_1, \dots, A_n)$ je množina zobrazení

$$R \subseteq {}^{\mathcal{A}}(\bigcup \mathrm{rng}(D)) \text{ také, že } f \in R \text{ implikuje } (\forall A \in \mathcal{A}) \bigcup f(A) \in D(A)$$

Napr. $f.A$, rozvrh[2].čas

Definícia 1.40
Nech $r(A_1, \dots, A_n)$ je relačná schéma a $D : \mathcal{A} \longrightarrow \bigcup D(A)$ je indexovaný súbor domén atribútov (občas vyznačovaný $\{D(A) : A \in \mathcal{A}\}$). Potom informatická reprezentácia relačnej schémy $r(\mathcal{A})$ *vzhľadom k* D je množina zobrazení

$$R \subseteq {}^{\mathcal{A}}(\bigcup \mathrm{rng}(D))$$

taká, že

$$f \in R \text{ implikuje } (\forall A \in \mathcal{A})(f(A) \in D(A)).$$

Príklad 1.41
V Pascale definujeme napríklad

```
type Rozvrhová_akcia=record
       miesto : Mená_poslucharní
       čas : Časové_intervaly
       učiteľ : Mená_učiteľov
       skupina
       predmet
     end;

     Rozvrh=array[1...100] of Rozvrhová_akcia
     end;

var  Rozvrh0102 : Rozvrh
```

Príklad 1.42
V našom príklade relačnej schémy ROZVRH, množinová reprezentácia (relačná) obsahuje napríklad prvok

$$\langle \text{P8, Ut } 8^{45}\text{, PV, 2I, KMI/FLP1a} \rangle \in \textsc{Rozvrh}$$

V informatickej reprezentácii analogická informácia je reprezentovaná zobrazením (množinou usporiadaných dvojíc)

$$\{\langle \text{miesto, P8}\rangle, \langle \text{čas, RH } 8^{45}\rangle, \langle \text{učiteľ, PV}\rangle, \langle \text{skupina, 2I }\rangle, \langle \text{predmet, KMI/FLP1a}\rangle\}$$

Občas budeme túto informáciu (a ďalšie) reprezentovať graficky takto:

Rozvrh				
miesto	čas	učiteľ	skupina	predmet
P8	Ut 8^{45}	PV	2I	KMI/FLP1a
P1	Št 7^{00}	VG	2I	KMI/AFJ1a
...	...	...	...	...
P7	St 10^{00}	xy	3*	

Definícia 1.43
Nech R je ľubovoľná (ale pevne zvolená) relácia schémy $r(\mathcal{A})$ vzhľadom k D.
Nech $\mathcal{A}_1 \subseteq \mathcal{A}$. Potom *projekciu* R na $\mathcal{A}_1$ definujeme takto:

$$\prod_{\mathcal{A}_1}(R) = \{f \in {}^{\mathcal{A}_1}(\bigcup \text{rng}(D)) : \text{ex. } g \in R \text{ také, že } f \subseteq g\}$$

Definícia 1.44
Nech $\mathcal{A}_1, \mathcal{A}_2 \subseteq \mathcal{A}$ sú neprázdne. Povieme, že v relácii R platí *funkčná závislosť* $\mathcal{A}_1 \Rightarrow \mathcal{A}_2$, ak pre každé $f, g \in R$ také, že $f \restriction \mathcal{A}_1 = g \restriction \mathcal{A}_1$ platí, že $f \restriction \mathcal{A}_2 = g \restriction \mathcal{A}_2$

Definícia 1.45
Nech S je realizácia schémy $s(\mathcal{B})$ vzhľadom k doméne E. *Spojenie* realizácií R a S je realizácia:

$$\begin{aligned} R \bowtie S \quad = \quad & \{f : \mathcal{A} \cup \mathcal{B} \longrightarrow (\bigcup \text{rng}(D) \cup \bigcup \text{rng}(E)) : \\ & (\forall g \in R)(\exists h \in S) \text{ také, že } (\forall A \in \mathcal{A} \cap \mathcal{B})(g(A) = h(A)) \text{ a naviac } f = g \cup h\} \end{aligned}$$

Pre D a E definujeme $D \sqcap E$ zobrazenie s definičným oborom $\mathcal{A} \cup \mathcal{B}$ nasledovne:

$$(D \sqcap E)(A) = \begin{cases} D(A), & \text{ak } A \in \mathcal{A} - \mathcal{B} \\ E(A), & \text{ak } A \in \mathcal{B} - \mathcal{A} \\ D(A) \cap E(A), & \text{ak } A \in \mathcal{A} \cap \mathcal{B} \end{cases}$$

Pozorovanie 1.46
$R \bowtie S$ je realizáciou schémy $r \bowtie s(\mathcal{A} \cup \mathcal{B})$ vzhľadom k doménom $D \sqcap E$ a definícia je korektná, t.j. $f = g \cup h$ je zobrazením

Príklad 1.47
Prednášky so zabezpečeným technickým vybavením dostaneme ako realizáciu, ktorá je výsledkom operácií

$$\prod_{\{predmet,\ učitel\}} (\textsc{Rozvrh} \bowtie \textsc{Technika} \bowtie \textsc{Požiadavky})$$

(Poznamenajme, že z hľadiska výsledku nezáleží na poradí zátvorkovania operácie $\bowtie$, ale vzhľadom k efektívnosti je lepšie najprv zostrojiť join TECHNIKA $\bowtie$ POŽIADAVKY a až potom join s ROZVRH-om.) Vzhľadom k nášmu príkladu realizácia

$$\textsc{Technika} \bowtie \textsc{Požiadavky}$$

obsahuje napr. záznamy

$$\{\langle \textit{predmet}, \text{KMI/OOP1e}\rangle, \langle \textit{miesto}, \text{P1}\rangle, \langle \textit{spätný proj.}, \text{ÁNO}\rangle, \langle \textit{dátový proj.}, \text{ÁNO}\rangle\}$$

a vo výsledku „požadované technické vybavenie“

$$\{\langle \textit{predmet}, \text{KMI/OOP1e}\rangle, \langle \textit{učiteľ}, \text{PE}\rangle\}.$$

Všimnime si, že náš model ešte nie je dokonalý, neumožňuje dobre vyhodnotiť rozvrh, v ktorom je miestnosť vybavená lepšie než sa vyžaduje.

1.3 Ordinálne čísla

Neformálny prístup bez definície:

$$\begin{array}{rcl}
0 & = & \emptyset \\
1 & = & \{0\} = \{\emptyset\} \\
2 & = & \{0,1\} = \{\emptyset, \{\emptyset\}\} \\
3 & = & \{0,1,2\} = \ldots \\
n & = & \{0,1,\ldots,n-1\} \\
n+1 & = & \{0,1,\ldots,n\} = \{0,1,\ldots,n-1,n\} = \{0,1,\ldots,n-1\} \cup \{n\} = n \cup \{n\}
\end{array}$$

$$\begin{array}{rcl}
n < m & \text{akk} & n \in m \quad \text{akk} \quad n \subseteq m \\
n \cap m & = & \min\{n,m\} \\
n \cup m & = & \max\{n,m\}
\end{array}$$

Množina prirodzených čísel

$$\omega = \{0,1,2,\ldots,n,\ldots\}$$

v teórii rekurzívnych funkcií to je primitívny pojem – Peanova aritmetika, neznamená, čo konkrétne je n. Turingové stroje („paličky“) – na vstupe $n = I^{n+1}$, na výstupe fyzikálne – dvojková reprezentácia. Výhoda teórie množín oproti iným reprezentáciam je, že vieme povedať, čo sa deje „za“ ω, $\omega + 1 = \omega \cup \{\omega\}, \omega+2, \omega+3, \ldots, \omega+n, \ldots, \omega+\omega, \ldots$

1.4 Stromy

Definícia 1.48

$$^{n}m = \{f : f \text{ je zobrazenie z } n \text{ do } m \text{ také, že } \operatorname{dom}(f) = n\}$$

teda

$$(f \subseteq n \times m) \quad \& \quad (\operatorname{dom}(f) = n) \quad \& \quad (\forall x \in m)(\forall y_1, y_2 \in n)((f(x) = y_1 \,\&\, f(x) = y_2) \longrightarrow y_1 = y_2)$$

Keďže pre ľubovoľné n, m je $\emptyset$ zobrazenie z n do m (pozri príklad 1.31) a navyše $\mathrm{dom}(\emptyset) = \emptyset$, tak

$$^{\emptyset}\emptyset = {}^{\emptyset}m = \{\emptyset\}$$

lebo $\emptyset \subseteq \emptyset \times \emptyset = \emptyset \times m = \emptyset$.
Naproti tomu, pre $n \neq \emptyset$

$$^{n}\emptyset = \emptyset$$

lebo neexistuje také zobrazenie f z n do $\emptyset$, pre ktoré by navyše platilo $\mathrm{dom}(f) = n$.

Príklad 1.49
Uvažujme pre dané n a m množinu všetkých zobrazení

$$^{<n}m = \bigcup_{i<n} {}^{i}m$$

a skúmajme reláciu $\subseteq$ na tejto množine

$$\begin{aligned} ^{<3}2 &= \bigcup_{i<3} {}^{i}2 = {}^{0}2 \cup {}^{1}2 \cup {}^{2}2 = \\ &= \{\emptyset, \{\langle 0,0\rangle\}, \{\langle 0,1\rangle\}, \{\langle 0,0\rangle, \langle 1,0\rangle\}, \{\langle 0,0\rangle, \langle 1,1\rangle\}, \{\langle 0,1\rangle, \langle 1,0\rangle\}, \{\langle 0,1\rangle, \langle 1,1\rangle\}\} \end{aligned}$$

$$\emptyset = \begin{cases} \subseteq \{\langle 0,0\rangle\} \begin{cases} \subseteq \{\langle 0,0\rangle, \langle 1,0\rangle\} \\ \subseteq \{\langle 0,0\rangle, \langle 1,1\rangle\} \end{cases} \\ \\ \subseteq \{\langle 0,1\rangle\} \begin{cases} \subseteq \{\langle 0,1\rangle, \langle 1,0\rangle\} \\ \subseteq \{\langle 0,1\rangle, \langle 1,1\rangle\} \end{cases} \end{cases}$$

Príklad 1.50 (stromy v XML)

```
<strom>0<strom>0<uzol>00</uzol><uzol>01</uzol></strom>
<strom>1<uzol>10</uzol><uzol>11</uzol></strom></strom>
```

Definícia 1.51
Pre $f \in {}^{<n}m$ a $i \in m$ definujeme

$$f^\frown i = f \cup \{\langle \mathrm{dom}(f), i\rangle\}$$

Definícia 1.52
Množina $T \subseteq {}^{<n}m$ sa nazýva *strom* (m-*árny strom*), ak

$$(\forall f \in T)(\forall i \in \mathrm{dom}(f))(f \restriction i \in T)$$

- $\emptyset \in T$ sa nazýva *koreň* stromu.
- $f \in T$ sa nazývajú *uzly* stromu T.
- Pre $f \in T$ a $i \in m$ sa $f^\frown i$ sa nazýva *potomok* (*následník*) uzla f.
- Pre $f \neq \emptyset$ sa uzol $f \restriction (\mathrm{dom}(f) - 1)$ nazýva *predok* (*bezprostredný predchodca*) uzla f.
- Pre $i < n$ je $T \cap {}^{i}m$ i-*tá hladina* stromu.
- *Dĺžka* (*výška*) stromu T je minimálne i také, že $T \cap {}^{i}m = \emptyset$.
- Uzol $f \in T$ sa nazýva *list* stromu, ak neexistuje $i \in m$ také, že $f^\frown i \in T$.

- $T_m^n = {}^{<n}m$ sa nazýva úplný m-árny strom dĺžky n.

Poznámka 1.53

- i-tú hladinu stromu pre $i < n$ je $\{f \in T : \mathrm{dom}(f) = i\}$. Podľa definície 1.52 je tiež zrejmé, že listy stromu ${}^{<n}m$ sú všetky zobrazenia ${}^{(n-1)}m$.

Definícia 1.54
Nech $T \subseteq {}^{<n}m$ je strom a H je množina hodnôt. Potom *ohodnotenie stromu* T hodnotami H je zobrazenie

$$h : T \to H.$$

Príklad 1.55
Nech H je množina všetkých možných rozložení dám na šachovnici – v zápise usporiadaná 8-tica (v stĺpci), napr.

$$\langle \text{Da1, Db3, Dc2, Dd4, De, Df, Dg, Dh} \rangle$$

$$\langle \text{Da5, Db8, Dc6, Dd4 } \rangle \text{ (ak dáma nie je uvedená, znamená to neobsadené pole)}$$

Pre $f \in {}^{<8}8$ položme $h(\emptyset) = \{\text{neobsadená žiadna}\}$

$$h(f) = \langle \text{Daf(0), Dbf(1), Dcf(2)}, \dots \rangle \text{ podľa dĺžky def. odboru.}$$

Nech $T_D \subseteq {}^{<9}8$ je množina tých $f \in {}^{<8}8$ pre ktoré $h(f)$ je rozloženie dám v prvých $\mathrm{dom}(f)$ stĺpcoch také, že žiadne dve z nich sa neohrozujú.

Úloha 1.56

- Dokážte, že T má dĺžku 9 (aj z uzlom $\emptyset$)
- Napíšte pascalovský program, ktorý nájde metódou backtracking rozloženie 8-dám.
- Dokážte, že
  $$f \in T_D \equiv (\forall i, j < \mathrm{dom}(f)) \left(\begin{array}{c} f(i) + |j-i| \neq f(j)) \\ f(i) - |j-i| \neq f(j) \end{array} \right\} \text{t.j. } |f(i) - f(j)| \neq |i-j| \right)$$

V tomto úvode do teórie množín sme prebrali základné konštrukcie (dátové štruktúry), pomocou ktorých budeme modelovať informatické procesy, objekty, atď.
Ďalší formalizmus, ktorý potrebujeme k informatike je logika. Logika je popis toho, čo má platiť medzi vstupom a výstupom

$$\varphi(\overline{x}, \overline{y})$$

Poznámka 1.57
Funkcionálne a logické programovanie

procedurálna stránka	deklaratívna stránka
algoritmus Pascal, TS	splnenie požiadaviek vzťah medzi $\overline{x}$ a $\overline{y}$
funkcionálne $f = \{\langle x, f(x)\rangle, x \in \mathrm{dom}\, f\}$	logické podminky
čierna skrinka	SQL dotaz
dôkaz $\vdash$ nedeterministický slepý algoritmus	pravdivosť $\models$ (v zmysle logiky)
vypočítaná odpoveď	správna odpoveď

Definícia 1.58 (neformálna)
Výrokový počet – výroky sú oznamovacie vety, na ktoré možno odpovedať pravda/nepravda (áno/nie). Nehľadáme vnútornú príčinu pravdivosti.
Predikátový počet – štruktúra objektov, hľadá vnútornú príčinu pravdivosti.

$$(x+y)^2 = x^2 + 2xy + y^2$$

$$\text{Logika} \begin{cases} \text{syntax - slová v abecede, axiómy, dokázateľnosť} \\ \text{sémantika - modely sveta, pravdivosť.} \end{cases}$$

Teplota $= 38.5°$C & … & pozitívny RTG $\longrightarrow$ diagnóza
žena: vek > 40 & príjem $\geq$ regionálny priemer $\longrightarrow$ dať pôžičku

2 Výrokový počet

2.1 Základné definície

Abeceda A výrokového počtu obsahuje

- množinu elementárnych výrokov $EV = \{p, q, r, s, p_1, r_1, \ldots\}$
- logické spojky $\neg, \longrightarrow$
- pomocné symboly ( ) ,

Slová v abecede A: $\quad p \quad \neg p \quad)p \quad p \longrightarrow q \quad p\neg \longrightarrow q \quad)($
Premenné na označovanie slov $\varphi, \psi, \chi, \varphi_0, \varphi_n, \ldots$

Definícia 2.1
Postupnosť slov $\varphi_0, \ldots, \varphi_n$ v abecede výrokového počtu sa nazýva *vytvárajúca postupnosť výroku*, ak pre každé $i \leq n$ platí, že

- buď φ_i je elementárny výrok
- alebo existujú $j, k < i$ také, že:
  - buď $\varphi_i \doteq \neg(\varphi_j)$
  - alebo $\varphi_i \doteq (\varphi_j) \longrightarrow (\varphi_k)$.

Poznámka 2.2
Rovnosť $\doteq$ je rovnosť syntaktická – „písmenko po písmenku“.

Definícia 2.3
Množina slov $\textsc{Vyr}_{\mathrm{VPV}} \subseteq A^*$ sa nazýva množinou výrokov definovaných „zdola“ pomocou vytvárajúcej postupnosti výroku, ak

$$\textsc{Vyr}_{\mathrm{VPV}} = \{\varphi : \text{ existuje vytvárajúca postupnosť výroku } \varphi_0, \ldots, \varphi_n \text{ taká, že } \varphi \doteq \varphi_n\}$$

Definícia 2.4
Množina slov $\mathcal{A} \subseteq A^*$ sa nazýva uzavretá, ak $EV \subseteq \mathcal{A}$ a pre každé $\varphi, \psi \in \mathcal{A}$ platí, že

$$\neg(\varphi) \in \mathcal{A} \quad \text{a} \quad (\varphi) \longrightarrow (\psi) \in \mathcal{A}$$

Definícia 2.5
Množina slov $\textsc{Vyr}_{\text{MUM}} \subseteq A^*$ sa nazýva množina výrokov definovaných „zhora" pomocou najmenšej (minimálnej) uzavretej množiny, ak

$$\textsc{Vyr}_{\text{MUM}} = \bigcap\{\mathcal{A} \subseteq A^* : \mathcal{A} \text{ je uzavretá množina}\}.$$

Definícia 2.6
Nech $H = EV \cup \{\neg, \longrightarrow\}$. Ohodnotený strom

$$h : T \to H$$

pre nejaké $T \subseteq {}^{<n}2$ sa nazýva *syntaktický strom výroku*, ak:

- každý uzol, pre ktorý $h(f) = \neg$, má práve jedného následníka $f^\frown 0$
- každý uzol, pre ktorý $h(f) =\longrightarrow$ má práve dvoch následníkov $f^\frown 0$, $f^\frown 1$
- f je *list stromu* T akk $h(f)$ je elementárny výrok (t.j. $h(f) \in \mathrm{EV}$).

Definícia 2.7
Nech $f \in T \subseteq {}^{<n}m$ je uzol stromu T. Potom podstrom T_f stromu T určený uzlom f je definovaný nasledovne:

$$T_f = \{g \in {}^{<(n-\text{dom}(f))}m : f^\frown g \in T\}$$

Pričom operácia $f^\frown g$ je definovaná nasledovne:

- Pre všetky $i < \text{dom}(f)$ je $(f^\frown g)(i) = f(i)$.
- Pre všetky $j < \text{dom}(g)$ je $(f^\frown g)(\text{dom}(f) + j) = g(j)$

Definícia 2.8
Nech $h : T \to H$ je syntaktický strom výroku. Rekurzívne „zdola nahor" definujeme pre $f \in T$ funkciu $\text{eval}(h, f)$ takto:

- ak $h(f) \in EV$ potom $\text{eval}(h, f) \coloneqq h(f)$.
- ak $h(f) = \neg$ potom $\text{eval}(h, f) \coloneqq \neg(\text{eval}(h, f^\frown 0))$
- ak $h(f) =\longrightarrow$ potom $\text{eval}(T_f) \coloneqq (\text{eval}(h, f^\frown 0)) \longrightarrow (\text{eval}(h, f^\frown 1))$

Definícia 2.9
Množina výrokov $\textsc{Vyr}_{\text{STR}} \subseteq A^*$ sa nazýva množina výrokov definovaných pomocou syntaktických stromov ak

$$\textsc{Vyr}_{\text{STR}} = \{\varphi : \text{ existuje syntaktický strom } h \text{ taký, že } \varphi \coloneqq \text{eval}(h, \emptyset)\}$$

Veta 2.10
Existuje Turingov stroj taký, že ak na páske vstupuje konfigurácia ϱ_0 pre $\varphi \in A^*$ tak vždy a dáva výsledok
$$\begin{cases} 1, \textit{ak } \varphi \textit{ je výrok} \\ 0, \textit{ak } \varphi \textit{ nie je výrok} \end{cases}$$

Veta 2.11
Množina Gödelovych čísel výrokov je rekurzívna.

Veta 2.12

$$\text{Vyr}_{\text{VPV}} = \text{Vyr}_{\text{MUM}} = \text{Vyr}_{\text{STR}} = \text{Vyr}$$

Dôkaz.
$\text{Vyr}_{\text{STR}} \subseteq \text{Vyr}_{\text{MUM}}$
Fixujeme $\mathcal{A}$ uzavretú. Nech h je syntaktický strom výroku. Potom indukciou cez uzly f od listov stromu ukážeme: $\text{eval}(h, \emptyset) \in \mathcal{A}$.

- $h(f) \in EV$, potom $\text{eval}(h, f) = h(f) \in EV \subseteq \mathcal{A}$
- Ak $h(f) = \longrightarrow$ a z indukčného predpokladu $\text{eval}(h, f^\frown 0) \in \mathcal{A}$ a $\text{eval}(h, f^\frown 1) \in \mathcal{A}$ potom

$$\text{eval}(h, f) = (\text{eval}(h, f^\frown 0)) \longrightarrow (\text{eval}(h, f^\frown 1)) \in \mathcal{A}.$$

- Ak $h(f) = \neg$ a $\text{eval}(h, f^\frown 0) \in \mathcal{A}$ potom

$$\text{eval}(h, f) = \neg(\text{eval}(h, f^\frown 0)) \in \mathcal{A}.$$

$\text{Vyr}_{\text{MUM}} \subseteq \text{Vyr}_{\text{VPV}}$.
Keďže Vyr_{MUM} je prienik všetkých uzavretých množín, stačí ukázať, že množina Vyr_{VPV} je uzavretá.

- $\text{EV} \subseteq \text{Vyr}_{\text{VPV}}$, lebo elementárny výrok je sám sebe VPV.
- Nech $\varphi, \psi \in \text{Vyr}_{\text{VPV}}$ a $\varphi_0, \ldots, \varphi_n \equiv \varphi$ je VPV φ a nech $\psi_0, \ldots, \psi_m \equiv \psi$ je VPV ψ. Potom

$$\varphi_0, \ldots, \varphi_n, \psi_0, \ldots, \psi_m, (\varphi_n) \longrightarrow (\psi_m)$$

  je VPV $(\varphi) \longrightarrow (\psi)$. Teda $(\varphi) \longrightarrow (\psi) \in \text{Vyr}_{\text{VPV}}$.
- Nech $\varphi \in \text{Vyr}_{\text{VPV}}$ a nech $\varphi_0, \ldots, \varphi_n \equiv \varphi$ je jeho VPV. Potom však aj $\neg(\varphi) \in \text{Vyr}_{\text{VPV}}$, lebo jeho VPV je $\varphi_0, \ldots, \varphi_n, \neg(\varphi_n)$. Teda Vyr_{VPV} je uzavretá množina.

$\text{Vyr}_{\text{VPV}} \subseteq \text{Vyr}_{\text{STR}}$
Definujeme operácie $\neg$ a $\longrightarrow$ na stromoch. Nech $h : T \to H, k : S \to H$ sú syntaktické stromy. Potom definujeme pre každé $u \in T$ a $v \in S$:

$$\begin{aligned}
(\neg h)(\emptyset) &= \neg \\
(\neg h)(\langle 0,0\rangle^\frown u) &= h(u) \\
\\
(h \longrightarrow k)(\emptyset) &= \longrightarrow \\
(h \longrightarrow k)(\langle 0,0\rangle^\frown u) &= h(u) \\
(h \longrightarrow k)(\langle 0,1\rangle^\frown v) &= k(v)
\end{aligned}$$

Ľahko vidieť, že $\text{eval}(\neg h, \emptyset) \equiv \neg(\text{eval}(h, \emptyset))$ a $\text{eval}(h \longrightarrow k, \emptyset) \equiv (\text{eval}(h, \emptyset)) \longrightarrow (\text{eval}(k, \emptyset))$.
Nech $\varphi_0, \ldots, \varphi_n \equiv \varphi$ je VPV φ. Indukciou cez $i \leq n$ ukážeme, že $\varphi_i \in \text{Vyr}_{\text{STR}}$.

- ak $\varphi_i \in \text{EV}$, potom strom pre φ_i je $h_i(\emptyset) = \varphi_i$.
- ak existujú $j, k < i$, také, že $\varphi_i \equiv (\varphi_j) \longrightarrow (\varphi_k)$, potom strom h_i vznikne zo stromov h_j a h_k operáciou $\longrightarrow$ definovanou vyššie, $h_i = h_j \longrightarrow h_k$.
- ak existuje $j < i$, také, že $\varphi_i \equiv \neg(\varphi_j)$, potom $h_i = \neg h_j$

□

Každý logický systém má za cieľ popísať (modelovať) realitu - samozrejme s istým „zaokrúhlením“, z istej „perspektívy“, niečo musí zanedbať.

$$\text{logický systém} \begin{cases} \text{syntax} \\ \text{sémantika} \begin{cases} \text{možné svety} \\ \text{význam tvrdení} \\ \text{pravdivosť} \end{cases} \end{cases}$$

Výrokový počet - syntax - abeceda $A, A^*, \textsc{Vyr}_{\text{VPV}} = \textsc{Vyr}_{\text{MUM}} = \textsc{Vyr}_{\text{STR}}$ nepátra po vnútorných dôvodoch pravdivosti - možný svet je ohodnotenie elementárnych výrokov pravdivostnými hodnotami.

2.2 Ohodnotenie výrokov

Definícia 2.13
Ohodnotenie elementárnych výrokov je zobrazenie

$$v : \text{EV} \longrightarrow \{0, 1\}$$

Našou snahou je rozšíriť ohodnotenie $\textsc{Vyr}$. Musíme si ešte definovať pravdivostné funkcie logických spojok:

$$\begin{aligned} \neg^\bullet(x) &= 1 - x \\ \longrightarrow^\bullet(x, y) &= \min(1, 1 - x + y) \end{aligned}$$

alebo tabuľkou

$\longrightarrow^\bullet$	0	1
0	1	1
1	0	1

$\neg^\bullet$	
0	1
1	0

Už na strednej škole a v prvom ročníku vysokej školy sme počítali pravdivostnú hodnotu výroku takto: $p \longrightarrow (r \longrightarrow q)$

	p	q	$r \longrightarrow q$	$p \longrightarrow (q \longrightarrow p)$
$v1$	0	0	1	1
$v2$	0	1	0	1
$v3$	1	0	1	1
$v3$	1	1	1	1

Definícia 2.14
Nech $v : \text{EV} \longrightarrow \{0, 1\}$ je ohodnotenie elementárnych výrokov a nech $\varphi_0, \ldots, \varphi_n \equiv \varphi$ je vytvárajúca postupnosť výroku φ. Potom $\bar{v}_{\text{VPV}}(\varphi)$ definujeme indukciou pre $i \leq n$ takto:

- ak $\varphi_i \in \text{EV}$ potom $\bar{v}_{\text{VPV}}(\varphi_i) = v(\varphi_i)$
- ak ex. $j, k < i$ také, že
  - $\varphi_i \equiv \neg(\varphi_j)$ potom $\bar{v}_{\text{VPV}}(\varphi_i) = \neg^\bullet(\bar{v}_{\text{VPV}}(\varphi_j))$
  - $\varphi_i \equiv (\varphi_j) \longrightarrow (\varphi_k)$ potom $\bar{v}_{\text{VPV}}(\varphi_i) = \longrightarrow^\bullet (\bar{v}_{\text{VPV}}(\varphi_j), \bar{v}_{\text{VPV}}(\varphi_k))$.

Poznámka 2.15
Treba ukázať (odborníci na cvičeniach), že táto definícia je korektná – tj. že hodnota nezávisí na výbere vytvárajúcej postupnosti. Potom budeme mať korektne definované

$$\bar{v}_{\text{VPV}} : \textsc{Vyr} \rightarrow \{0, 1\}$$

Analogicky ako sme ukazovali viaceré možnosti syntakticky správnych slov – t.j. výrokov a dokázali, že $\mathrm{VYR}_{\mathrm{VPV}} = \mathrm{VYR}_{\mathrm{MUM}} = \mathrm{VYR}_{\mathrm{STR}} = \mathrm{VYR}$, aj pri definícii rozšírenia $\bar{v} : \mathrm{VYR} \longrightarrow \{0,1\}$ máme viacero možností. Uvedieme ešte $\bar{v}_{\mathrm{STR}}$.

Definícia 2.16
Nech $v : \mathrm{EV} \longrightarrow \{0,1\}$ a $h : T \longrightarrow H$ je syntaktický strom výroku φ a nech $\mathrm{evalTV}(h,f,v)$ je rekurzívna funkcia definovaná takto:

- ak $h(f) \in \mathrm{EV}$ potom $\mathrm{evalTV}(h,f,v)) = v(h(f))$
- ak $h(f) = \longrightarrow$ potom $\mathrm{evalTV}(h,f,v)) = \longrightarrow^{\bullet} (\mathrm{evalTV}(h, f^\frown 0, v), \mathrm{evalTV}(h, f^\frown 1, v))$
- ak $h(f) = \neg$ potom $\mathrm{evalTV}(h,f,v)) = \neg^{\bullet}(\mathrm{evalTV}(h, f^\frown 0))$

Potom $\bar{v}_{\mathrm{STR}}(\varphi)$ je definované nasledovne:

$$\bar{v}_{\mathrm{STR}}(\varphi) = \mathrm{evalTV}(h, \emptyset, v)$$

Poznámka 2.17
Dá sa ukázať, že $\bar{v}_{\mathrm{VPV}} = \bar{v}_{\mathrm{STR}} = \bar{v} : \mathrm{VYR} \longrightarrow \{0,1\}$ (odborníci na cvičeniach).

Príklad 2.18
Majme výrok $(p \longrightarrow (q \longrightarrow r)) \longrightarrow ((p \longrightarrow q) \longrightarrow (p \longrightarrow r))$.
Nech ohodnotenie $v(p) = 1, v(q) = 0 = v(r)$ („zdola“, od listov) Potom $\bar{v}(\varphi) = 1$

Syntaktické stromy sú jednoznačné, nevýhodou ale je, že pre každý možný svet to treba prepočítať zvlášť.

2.3 Tautológie

Definícia 2.19
Výrok φ je *tautológia*, ak pre každé ohodnotenie $v : \mathrm{EV} \to \{0,1\}$ elementárnych výrokov pravdivostnými hodnotami platí, že $\bar{v}(\varphi) = 1$.

označenie: $\models \varphi$

Označenie 2.20
$\mathrm{EV}(\varphi)$ označuje množinu všetkých elementárnych výrokov vyskytujúcich sa v φ (ako písmená abecedy v slove, alebo $\mathrm{rng}(h) \cap \mathrm{EV}$, ak h je syntaktický strom výroku φ).

Tvrdenie 2.21
Nech φ, ψ, χ sú ľubovoľné výroky. Potom nasledujúce výroky sú tautológie.

- $\varphi \longrightarrow (\psi \longrightarrow \varphi)$
- $(\varphi \longrightarrow (\psi \longrightarrow \varphi)) \longrightarrow ((\varphi \longrightarrow \psi) \longrightarrow (\varphi \longrightarrow \chi))$
- $(\neg\varphi \longrightarrow \neg\psi) \longrightarrow (\psi \longrightarrow \varphi)$

To, že $p \longrightarrow (q \longrightarrow p)$ je tautológia implikuje, že pre každé φ výrok

$$\varphi \longrightarrow (\varphi \longrightarrow \varphi)$$

je tautológia. Skúsime si to podrobnejšie rozanalyzovať a dokázať vo všeobecnosti.

Definícia 2.22
Nech $\mathrm{EV}(\psi) = \{p_1, \dots, p_n\}$ a nech $\varphi_1, \dots, \varphi_n$ sú výroky. Potom výrok

$$\psi(p_1/_{\varphi_1}, \dots, p_n/_{\varphi_n})$$

je výrok, ktorý z ψ vznikne simultánnym nahradením všetkých výskytov p_i za φ_i.
Presnejšie, nech

$$\psi = E_1 x_1 E_2 x_2 \dots E_k x_k E_{k+1}$$

kde platí, že $x_i, i = 1, \dots, k$ sú práve všetky výskyty elementárnych výrokov $(p_1, \dots, p_n)$ a E_i sú časti slova, ktoré neobsahujú elementárne výroky (a sú teda zložené z (,), $\longrightarrow$ a $\neg$).
Nech $\mathrm{ind}(x_i) \in \{1, \dots, n\}$ je index elementárneho výroku x_i tj. $x_i = p_{\mathrm{ind}(i)}$. Potom platí:

$$\psi(p_1/\varphi_1, \dots, p_n/\varphi_n) = E_1 \varphi_{\mathrm{ind}(1)} E_2 \varphi_{\mathrm{ind}(2)} E_3 \dots E_k \varphi_{\mathrm{ind}(k)} E_{k+1}.$$

Tvrdenie 2.23
Definícia je korektná, tj.

$$\psi(p_1/\varphi_1, \dots, p_n/\varphi_n)$$

je výrok.

Dôkaz.

- **Alternatíva 1.**
  Nech $\psi_1, \dots, \psi_m = \psi$ je VPV ψ a nech $\varphi_1^i, \dots, \varphi_{k_i}^i = \varphi_i$ je VPV φ_i. Potom

  $$\varphi_1^1, \dots, \varphi_{k_1}^1, \varphi_1^2, \dots, \varphi_{k_2}^2, \dots, \varphi_1^n, \dots, \varphi_{k_n}^n, \psi_1(p_1/\varphi_1, \dots, p_n/\varphi_n), \dots, \psi_m(p_1/\varphi_1, \dots, p_n/\varphi_n)$$

  je VPV $\psi(p_1/\varphi_1, \dots, p_n/\varphi_n)$.

- **Alternatíva 2.**
  Nech $h : T \to H$ je syntaktický strom výroku ψ a nech

  $$k_i : T_i \longrightarrow H$$

  sú syntaktické stromy výrokov φ_i. Potom syntaktický strom S výroku $\psi(p_1/\varphi_1, \dots, p_n/\varphi_n)$ definujeme nasledovne:
  Strom S vznikne tak, že na listy stromu T „zavesíme" stromy T_i podľa ohodnotenia:

  $S = \{f : f \in T \wedge h(f) \notin \{p_1, \dots, p_n\}$ alebo ex. $i \in \{1, \dots, n\}, u \in T, g \in T_i$, že $f = u^\frown g \wedge h(u) = p_i\}$

  Ohodnotenie $ch : S \longrightarrow H$ definujeme takto:

  - pre $f \in S$ ak $f \in T$ a $h(f) \notin \{p_1, \dots, p_n\}$, potom $ch(f) = h(f)$
  - pre $f^\frown g \in S$ také, že $h(f) = p_i$ platí, že $ch(f^\frown g) = k_i(g)$.

  Ľahko nahliadneme, že ak f je list stromu T a $h(f) = p_i$ pre $i \in \{1, \dots, n\}$, tak $\mathrm{eval}(ch, f) = T_i$ (z definície stromu S a podstromu). Teda

  $$\mathrm{eval}(ch, \emptyset) = \psi(p_1/\varphi_1, \dots, p_n/\varphi_n).$$

$\square$

Veta 2.24
Nech ψ je tautológia, $\mathrm{EV}(\psi) = \{p_1, \ldots, p_n\}$ *a* $\varphi_1, \ldots, \varphi_n$ *sú ľubovoľné výroky. Potom*

$$\psi(p_1/\varphi_1, \ldots, p_n/\varphi_n)$$

je tautológia.

Dôkaz.
Nech $v : \mathrm{EV} \to \{0,1\}$ je ľubovoľné (ale pevne zvolené) a nech $k : S \to H, h : T \to H, h_1 : T_1 \to H, \ldots, h_n : T_n \to H$ sú postupne syntaktické stromy výrokov $\psi(p_1/\varphi_1, \ldots, p_n/\varphi_n), \psi, \varphi_1, \ldots, \varphi_n$.
Definujme nové ohodnotenie $w : \mathrm{EV} \to \{0,1\}$, nasledovne:

$$w(p_i) = \bar{v}(\varphi_i) \text{ pre } i \in \{1, \ldots, n\}.$$

Ukážeme, že $\mathrm{evalTV}(k, \emptyset, v) = \mathrm{evalTV}(h, \emptyset, w)$. Indukciou podľa hladín stromu T:

- ak $u \in T$ je list a $h(u) = p_i$, pre $i \in \{1, \ldots, n\}$, potom $S_u = T_i$. Ale

  $$\mathrm{evalTV}(k, u, v) = \mathrm{evalTV}(h_i, \emptyset, v) = \bar{v}_{\mathrm{STR}}(\varphi_i) = \bar{v}(\varphi_i) = w(p_i) = w(h(u)) = \mathrm{evalTV}(h, u, w).$$

- ak $u \in T$ nie je list, potom podľa indukčného predpokladu pre každého potomka $u' \in T$ uzla u je $\mathrm{evalTV}(k, u', v) = \mathrm{evalTV}(h, u', w)$ a keďže $h(u) = k(u)$ potom $\mathrm{evalTV}(k, u, v) = \mathrm{evalTV}(h, u, w)$.

Z toho, že ψ je tautológia platí

$$\bar{v}(\psi(p_1/\varphi_1, \ldots, p_n/\varphi_n)) = \mathrm{evalTV}(k, \emptyset, v) = \mathrm{evalTV}(h, \emptyset, w) = \bar{w}(\psi) = 1.$$

□

Dôsledok 2.25
Nech φ, ψ, χ sú ľubovoľné výroky, potom

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

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

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

sú tautológie, nazveme ich „schémy logických axióm“. Pre každé konkrétne φ, ψ, χ sa daný výrok nazýva inštanciou logickej axiómy.

Úloha 2.26
Napíšte program v jazyku Pascal, resp. Turingov stroj rozoznávajúci, či daný výrok je inštanciou logickej axiómy. Ukážte, že množina Gödelovych čísel inštancií logických axióm je primitívne rekurzívna.

2.4 Dôkaz a dokázateľnosť vo výrokovom počte

Definícia 2.27
Postupnosť výrokov $\varphi_0, \ldots, \varphi_n = \varphi$ sa nazýva *dôkazom* výroku φ (dôkazom len z logických axióm), ak pre každé $i \leq n$ platí

- buď φ_i je inštanciou logickej axiómy
- alebo ex. $j, k < i$ také, že $\varphi_j = \varphi_k \longrightarrow \varphi_i$

Definícia 2.28
Výrok φ je *dokázateľný* vo VP (len z logických axióm), ak existuje dôkaz výroku φ.

$$\text{označenie: } \vdash \varphi$$

Poznámka 2.29
Poslednej podmienke hovoríme *použitie modus ponens*. Ak už vieme, že φ_k a $\varphi_k \longrightarrow \varphi_i$ sú dokázateľné výroky, potom je dokázateľný aj φ_i.

Príklad 2.30

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

Dôkaz.

$$\begin{aligned}
\varphi_0 &= \varphi \longrightarrow ((\varphi \longrightarrow \varphi) \longrightarrow \varphi) \\
\varphi_1 &= (\varphi \longrightarrow ((\varphi \longrightarrow \varphi) \longrightarrow \varphi)) \longrightarrow ((\varphi \longrightarrow (\varphi \longrightarrow \varphi)) \longrightarrow (\varphi \longrightarrow \varphi)) \\
\varphi_2 &= (\varphi \longrightarrow (\varphi \longrightarrow \varphi)) \longrightarrow (\varphi \longrightarrow \varphi) \\
\varphi_3 &= \varphi \longrightarrow (\varphi \longrightarrow \varphi) \\
\varphi_4 &= \varphi \longrightarrow \varphi
\end{aligned}$$

Komentár k dôkazu:
φ_0 je inštancia logickej axiómy 1:

$$(p \longrightarrow (q \longrightarrow p))(p/\varphi, q/(\varphi \longrightarrow \varphi))$$

φ_1 je inštancia logickej axiómy 2:

$$(p \longrightarrow (q \longrightarrow r)) \longrightarrow ((p \longrightarrow q) \longrightarrow (p \longrightarrow r))(p/\varphi, q/(\varphi \longrightarrow \varphi), r/\varphi)$$

φ_2 je výsledok použitia *modus ponens*, konkrétne pre

$$i = 2 \text{ ex. } j = 1, k = 0 \text{ (obe sú } < 2) \text{ také, že } \varphi_1 = \varphi_0 \longrightarrow \varphi_2$$

φ_3 je inštanciou logickej axiómy 1:

$$(p \longrightarrow (q \longrightarrow p))(p/\varphi, q/\varphi)$$

φ_4 je výsledok použitia *modus ponens*, pre

$$i = 4 \text{ ex. } j = 2, k = 3 \text{ také, že } \varphi_2 = \varphi_3 \longrightarrow \varphi_4$$

□

2.5 Korektnosť výrokového počtu

Veta 2.31 (o korektnosti výrokového počtu)
Nech φ je výrok, potom

$$\text{ak } \vdash \varphi, \text{ tak } \models \varphi.$$

(každý dokázateľný výrok je tautológia).

Dôkaz.
Nech $\varphi_0, \ldots, \varphi_n = \varphi$ je (nejaký) dôkaz výroku φ (nie je jednoznačne určený, jeden výrok môže mať viacero dôkazov). Indukciou pozdĺž dôkazu ukážeme, že platí $\models \varphi_i$. Pre $i \leq n$ platí

- buď φ_i je inštancia logickej axiómy, potom $\models \varphi_i$.
- alebo ex. $j, k < i$ také, že $\varphi_j \equiv \varphi_k \longrightarrow \varphi_i$ a z indukčného predpokladu $\models \varphi_j$ a $\models \varphi_k$. Chceme ukázať, že pre ľubovoľné $v : \mathrm{EV} \to \{0,1\}$ je $\bar{v}(\varphi_i) = 1$.
  Z IP vieme, že $\bar{v}(\varphi_k) = 1$ a $\bar{v}(\varphi_j) = 1$. Keďže $\varphi_j \equiv (\varphi_k \longrightarrow \varphi_i)$, tak $\bar{v}(\varphi_k \longrightarrow \varphi_i) = 1$. Máme teda:
  $1 = \bar{v}(\varphi_j) = \bar{v}(\varphi_k \longrightarrow \varphi_i) = \longrightarrow^\bullet (\bar{v}(\varphi_k), \bar{v}(\varphi_i)) =$
  $\min(1, 1 - \underbrace{\bar{v}(\varphi_k)}_{1} + \bar{v}(\varphi_i)) = \min(1, 1 - 1 + \bar{v}(\varphi_i)) = \min(1, \bar{v}(\varphi_i))$
  Z tejto rovnosti vyplýva, že $\bar{v}(\varphi_i) = 1$. □

Poznámka 2.32
Iný náhľad na dôkaz:
Vezmime možné ohodnotenie a v ňom jediný riadok, kde je $\bar{v}(\varphi_k) = 1$ a $\bar{v}(\varphi_k \longrightarrow \varphi_i) = 1$. Tam je potom $\bar{v}(\varphi_i) = 1$.

φ_k	φ_i	$\varphi_j \equiv \varphi_k \longrightarrow \varphi_i$	
0	0	1	
0	1	1	
1	0	0	
1	1	1	v tomto riadku platí IP: $\bar{v}(\varphi_k) = 1$ a súčasne $\bar{v}(\varphi_j) = 1$. Z toho teda $\bar{v}(\varphi_i) = 1$

Poznámka 2.33 (alebo úloha)
Napíšte pascalovský program, resp. Turingov stroj, ktorý overuje, či postupnosť slov je dôkaz daného výroku. Ukážte, že „Gödelove číslo postupnosti slov je kódom správneho dôkazu“ je primitívne rekurzívny predikát.

Poznámka 2.34
Náš prístup k budovaniu výrokového počtu je minimalistický (minimálna množina axióm, jedno odvodzovacie pravidlo, jazyk iba s $\longrightarrow$ a $\neg$ (bez &, $\vee$, $\leftrightarrow, \ldots$)) a sleduje úsporný spôsob dôkazu vety o úplnosti.

3 Predikátový počet

$$\text{Predikátový počet}\left\{\begin{array}{l}
\text{syntax – abeceda, jazyk} \\[1em]
\text{sémantika}\left\{\begin{array}{l}
\text{modely sveta}\left\{\begin{array}{l}
\text{domény atribútov} \\
\text{mená indivíduí, objektov} \\
\text{výrazy, ktoré nadobúdajú hodnoty na objektoch} \\
\text{konštrukcie, vzorčeky, algoritmy, funkčné závis-} \\
\text{losti – termy}
\end{array}\right. \\[1em]
\text{možné svety – tvrdenia o termoch, pravdivosť}
\end{array}\right.
\end{array}\right.$$

3.1 Syntax predikátového počtu

Poznámka 3.1
Predikátový počet - abeceda jazyka

$$\text{Jazyk } J\left\{\begin{array}{l}
\text{metadáta - atribúty } \mathcal{A} \\[1em]
\text{„doménová“ časť jazyka}\left\{\begin{array}{l}
\text{premenné}\left\{\begin{array}{l}
\text{pre každé } A \in \mathcal{A} \\
\textsc{Var}^A = \{x^A, y^A, x_1^A, \ldots\} \\
\textsc{Var}_J = \{\textsc{Var}^A : A \in \mathcal{A}\}
\end{array}\right. \\[1em]
\text{konštanty}\left\{\begin{array}{l}
\mathcal{C}^A = \{c^A, d^A, c_1^A, \ldots\} \\
\mathcal{C}_J = \{\mathcal{C}^A : A \in \mathcal{A}\}
\end{array}\right. \\[1em]
\text{funkčné symboly}\left\{\begin{array}{l}
\text{písmená abecedy } f, g, \ldots \\
\text{metadáta } f(\underbrace{A_1, \ldots, A_n}_{\text{vstup}}) = \underbrace{A_{n+1}}_{\text{výstup}} \\
\mathcal{F}_J = \{\{\mathcal{F}^{\bar{A}} : \bar{A} \in {}^{n+1}\mathcal{A}\}; n \in \omega \setminus \{0\}\}
\end{array}\right.
\end{array}\right. \\[1em]
\begin{array}{l}\text{„pravdivostná“} \\ \text{časť jazyka}\end{array}\left\{\begin{array}{l}
\text{predikátové symboly}\left\{\begin{array}{l}
\text{písmená abecedy } p, +, \ldots \\
\text{metadátová časť } \underbrace{p(A_1, \ldots, A_n)}_{\substack{\text{predikát } p \text{ má atri-} \\ \text{búty } A_1, \ldots, A_n}} \\
\mathcal{P}_J = \{\{\mathcal{P}^{\bar{A}} : \bar{A} \in {}^{n}\mathcal{A}\}; n \in \omega \setminus \{0\}\}
\end{array}\right. \\[1em]
\text{spojky } \neg, \longrightarrow \\
\text{kvantifikátor } \forall \\
\text{pomocné symboly } ()
\end{array}\right.
\end{array}\right.$$

$$\text{metadátové funkcie}\left\{\begin{array}{rcl}
\text{typ}(x) & = & A \in \mathcal{A} : x \in \textsc{Var}^A \\
\text{typ}(c) & = & A \in \mathcal{A} : c \in \mathcal{C}^A \\
\text{typ}(f) & = & \langle A_1, \ldots, A_n; A_{n+1}\rangle : f \in \mathcal{F}^{\langle A_1, \ldots, A_n; A_{n+1}\rangle} \\
\text{typ}(p) & = & \langle A_1, \ldots, A_n\rangle : p \in \mathcal{P}^{\langle A_1, \ldots, A_n\rangle}
\end{array}\right.$$

Príklad 3.2
Príklad jazyka „Rozvrh PF UPJŠ 0102“ (AIS subsystém ŠTUDENT)

- $\mathcal{A}_{\text{ROZ}} = \{$Študent, Posluchářeň, Skupina, Čas, Učiteľ, Predmet$\}$
- $\textsc{Var}_{\text{ROZ}} = \{\textsc{Var}^A : A \in \mathcal{A}\}$
- $\mathcal{C}_{\text{ROZ}} = \{\mathcal{C}^A : A \in \mathcal{A}\}$

- $\mathcal{C}^{Stud}$ = {mená študentov
  - ⋄ terajších
  - ⋄ prerušené
  - ⋄ minulí
  - ⋄ prihlásení

  }
- $\mathcal{C}^{\mathrm{Posl}}$ = {M5, D1, P8, BZ1,...}
- $\mathcal{C}^{\mathrm{Predm}}_{\mathrm{ROZ0102}}$ = {KMI/FLP1, KMI/AFJ, KMI/TAL, KMI/UM}
- ($\mathcal{C}^{\mathrm{Predm}}_{\mathrm{ROZ0203}}$ = {UI/FLP1, UI/TVY, UI/UI,...})

* $\mathcal{F}_{\mathrm{ROZ}}$: napr. počet_zapísaných_kreditov(študent) = počet_kreditov

Príklad 3.3
Príklad jazyka „Peanova aritmetika, rekurzívne funkcie“:
$0, +1, +, \cdot, <, =$
rozšírenie jazyka: ( ) ^{2}, x^y, „je prvočíslo“, „je kódom výpočtu Turingovho stroja“, ... „je kódom dôkazov VP“,...

Logika je o modelovaní sveta, o pravdivosti, dokázateľnosti (odvodzovanie – deduktívne a – reduktívne) Modelovanie môže byť viac alebo menej verné, buď vedome rozhodneme o tom, čo zanedbáme – alebo nie sme schopní modelovať.

Príklady:
Výrokový počet, predikátový počet, temporálne, modálne logiky, ...
Aj v predikátovom počte môžem viac rozvinúť stavbu metadát, napr.

* množina atribútov $\mathcal{A}$
* množina typov domén $D = \{\texttt{char}, \texttt{boolean}, \texttt{real}, \texttt{integer}, \texttt{ascii}, \texttt{string}, \texttt{LATIN2}\}$

Rôzne významy – hlavne v programovacích jazykoch a SQL. (napr. SQL formálne umožňuje dotazy typu: „nájdi zamestnancov, ktorí v roku 2002 majú mesačný plat 2002$“).
Takže aj v predikátovom počte môžeme nasadiť rôznu úroveň presnosti modelovania – my chceme byť „o krok“ presnejší než matematická logika, aby sme mohli modelovať informatické fenomény.

Príklad 3.4

* Analýza: $x, +, *, x^y, \log, \ln, \sin, \cos, \mathrm{e}, \pi, 0, 1, <, =$, čo je to $\int \sin(x)\mathrm{d}x$, $\frac{d\cos x}{\mathrm{d}x}$, ..., miera μ
* Algebra: matice, sústavy rovníc, grupy, okruhy, telesá, ...
* Grafy,...
* Teória množín

Definícia 3.5
Postupnosť slov $t_0, \ldots, t_n$ v abecede predikátového počtu J sa nazýva *vytvárajúca postupnosť termu* ak pre každé $i \leq n$ platí, že

* buď t_i je konštanta (term t_i je typu typ(t_i), t.j. typh(t_i) = typ(t_i))
* alebo t_i je premenná (term t_i je typu typ(t_i), t.j. typh(t_i) = typ(t_i))

- alebo existujú m a $j_1, \ldots, j_m < i$ a funkčný symbol $f \in \bigcup \mathcal{F}_J$ taký, že

$$\mathrm{typ}(f) = \langle A_1, \ldots, A_m; A_{m+1} \rangle \text{ a } \mathrm{typh}(t_{j_k}) = A_k \quad (k \in \{1, \ldots, m\}) \text{ a } t_i \doteq f(t_{j_1}, \ldots, t_{j_m}).$$

(Potom povieme, že term t_i je typu A_{k+1}, t.j. $\mathrm{typh}(t_i) = A_{k+1}$)

Definícia 3.6
Nech $T \subseteq {}^{<n}m$ je strom. Ohodnotený strom

$$h : T \to \bigcup \mathrm{V{\scriptsize AR}}_J \cup \bigcup \mathcal{C}_J \cup \bigcup \mathcal{F}_J$$

sa nazýva *syntaktický strom termu*, ak:

- každý uzol u, pre ktorý $h(u) \in \bigcup \mathcal{F}_J$ a $\mathrm{typ}(h(u)) = \langle A_1, \ldots, A_k; A_{k+1} \rangle$ má práve k následníkov: $u^\frown 0, \ldots, u^\frown (k-1)$ a $\mathrm{typh}(h(u^\frown i)) = A_i$. Potom $\mathrm{typh}(h(u)) = A_{k+1}$.
- u je list stromu T akk $(h(u) \in \bigcup \mathrm{V{\scriptsize AR}}_J$ alebo $h(u) \in \bigcup \mathcal{C}_J)$. Potom $\mathrm{typh}(h(u)) = \mathrm{typ}(h(u))$.

Definícia 3.7
Nech h je syntaktický strom termu. Rekurzívne definujeme funkciu $\mathrm{eval}(h, u)$ takto:

- ak u je list potom $\mathrm{eval}(h, u) \doteq h(u)$
- ak $h(u) = f \in \bigcup \mathcal{F}_J$ a $\mathrm{typ}(f) = \langle A_1, \ldots, A_k; A_{k+1} \rangle$ potom

$$\mathrm{eval}(h, u) \doteq f(\mathrm{eval}(h, u^\frown 0, \ldots, \mathrm{eval}(h, u^\frown (k-1))))$$

Definícia 3.8
Množina slov $\mathrm{T{\scriptsize ERM}}_{\mathrm{VPT}} \subseteq J^*$ sa nazýva množinou termov definovaných pomocou vytvárajúcej postupnosti, ak

$$t \in \mathrm{T{\scriptsize ERM}}_{\mathrm{VPT}} \quad \text{akk} \quad \text{ex. VPT } t_1, \ldots, t_n \text{ také, že } t \doteq t_n.$$

Množina slov $\mathrm{T{\scriptsize ERM}}_{\mathrm{STR}} \subseteq J^*$ sa nazýva množinou termov definovaných pomocou syntaktických stromov termu ak

$$t \in \mathrm{T{\scriptsize ERM}}_{\mathrm{STR}} \quad \text{akk} \quad \text{ex. } h \text{ také, že } t \doteq \mathrm{eval}(h, \emptyset).$$

Veta 3.9

$$\mathrm{T{\scriptsize ERM}}_{\mathrm{VPT}} = \mathrm{T{\scriptsize ERM}}_{\mathrm{STR}} = \mathrm{T{\scriptsize ERM}}$$

Úloha 3.10
Úloha – programy, prim. rekurzie, TS – syntaktická analýza ako u výrokov.

Definícia 3.11
(Pokiaľ nepovieme ináč, platí „rezervácia označenia" v jazyku (napr. x, c, f, p, u, T, J,...) použitého v predošlých definíciách.)

- množina $\mathrm{V{\scriptsize AR}}(t) = \{h(u) : u$ je list syntaktického stromu termu t a $h(u) \in \bigcup \mathrm{V{\scriptsize AR}}_J\}$.
  Ak $\mathrm{V{\scriptsize AR}}(t) = \emptyset$, hovoríme, že t je *konštantný term*.
- slovo $p(t_1, \ldots, t_n) \in J^*$ sa nazýva *atomárna formula* (niekedy len *atóm*) ak p je predikátový symbol – $p \in \bigcup \mathcal{P}_J$, $\mathrm{typ}(p) = \langle A_1, \ldots, A_n \rangle$ a pre $i \in \{1, \ldots, n\}$: $\mathrm{typh}(t_i) = A_i$, $\mathrm{V{\scriptsize AR}}(p(t_1, \ldots, t_n)) = \bigcup \{\mathrm{V{\scriptsize AR}}(t_i) : i \leq n\}$
  Ak $\mathrm{V{\scriptsize AR}}(p(t_1, \ldots, t_n))$ je prázdne, hovoríme, že p je *konštantný atóm*.

- Množina voľných premenných $\mathrm{FV}(p(t_1,\ldots,t_n)) = \textsc{Var}(p(t_1,\ldots,t_n))$
  Množina viazaných premenných $\mathrm{BV}(p(t_1,\ldots,t_n)) = \emptyset$.
- Nech x je premenná, ktorá má výskyt v $p(t_1,\ldots,t_n) = E_1xE_2$, potom tento *výskyt je voľný*.

Definícia 3.12
Postupnosť slov $\varphi_0,\ldots,\varphi_n$ v abecede predikátového počtu J sa nazýva *vytvárajúca postupnosť formuly* (VPF), ak pre každé $i \le n$ platí, že

- buď φ_i je atomárna formula
- alebo existujú $j, k < i$ také, že
  - buď $\varphi_i \equiv (\varphi_j) \longrightarrow (\varphi_k)$
    potom

$$\begin{aligned}\textsc{Var}(\varphi_i) &= \textsc{Var}(\varphi_j) \cup \textsc{Var}(\varphi_k)\\ \mathrm{FV}(\varphi_i) &= \mathrm{FV}(\varphi_j) \cup \mathrm{FV}(\varphi_k)\\ \mathrm{BV}(\varphi_i) &= \mathrm{BV}(\varphi_j) \cup \mathrm{BV}(\varphi_k)\end{aligned}$$

    ak BUNV $\varphi_j \equiv E_1xE_2$ bol voľný (viazaný) výskyt x vo φ_j, potom

$$\varphi_i \equiv \underbrace{(E_1}_{E_1'}\, x\, \underbrace{E_2) \longrightarrow (\varphi_k)}_{E_2'}$$

    je voľný (viazaný) výskyt x vo φ_i.
    analogicky pre výskyty vo φ_k
  - alebo $\varphi_i \equiv \neg(\varphi_j)$
    Potom

$$\begin{aligned}\textsc{Var}(\varphi_i) &= \textsc{Var}(\varphi_j)\\ \mathrm{FV}(\varphi_i) &= \mathrm{FV}(\varphi_j)\\ \mathrm{BV}(\varphi_i) &= \mathrm{BV}(\varphi_j)\end{aligned}$$

    a „kvalita" výskytov sa nezmenila.
  - alebo existuje $x \in \bigcup \textsc{Var}_J$ také, že $\varphi_i \equiv (\forall x)(\varphi_j)$.
    (V tom prípade sa φ_j volá *oblasť pôsobenia kvantifikátora* $\forall x$)
    - ⋄ $\textsc{Var}(\varphi_i) = \textsc{Var}(\varphi_j) \cup \{x\}$,
    - ⋄ $\mathrm{FV}(\varphi_i) = \mathrm{FV}(\varphi_j) - \{x\}$,
    - ⋄ $\mathrm{BV}(\varphi_i) = \mathrm{BV}(\varphi_j) \cup \{x\}$.

    Každý výskyt premennej x vo φ_i je viazaný. Všetky výskyty premenných rôznych od x „nezmenili kvalitu", tj. ak boli voľné vo φ_j zostali voľné vo φ_i a ak boli viazané vo φ_j zostali viazané vo φ_i.

Definícia 3.13
Nech $T \subseteq {}^{<n}m$ je strom. Ohodnotený strom

$$h : T \longrightarrow \bigcup \textsc{Var}_J \cup \bigcup \mathcal{C}_J \cup \bigcup \mathcal{F}_J \cup \bigcup \mathcal{P}_J \cup \{\longrightarrow, \neg\} \cup (\{\forall\} \times \bigcup \textsc{Var}_J)$$

sa nazýva *syntaktický strom formuly*, ak pre každý uzol $u \in T$ platí:

- ak $h(u) \in \bigcup \mathcal{P}_J$, $\mathrm{typ}(h(u)) = \langle A_1, \ldots, A_n \rangle$, potom u má práve n nasledníkov $u^\frown 0, \ldots u^\frown (n-1)$ takých, že $\mathrm{typh}(h(u^\frown (i-1))) = A_i$ (pre $i \in \{1, \ldots, n\}$).
Potom
$$\mathrm{eval}(h, u) \doteq p(\mathrm{eval}(h, u^\frown 0), \ldots, \mathrm{eval}(h, u^\frown (n-1)))$$
- ak $h(u) = \neg$, potom u má práve jedného nasledníka $u^\frown 0$
$$\mathrm{eval}(h, u) \doteq \neg(\mathrm{eval}(h, u^\frown 0))$$
- ak $h(u) = \longrightarrow$, potom u má práve dvoch nasledníkov $u^\frown 0$ a $u^\frown 1$
$$\mathrm{eval}(h, u) \doteq (\mathrm{eval}(h, u^\frown 0)) \longrightarrow (\mathrm{eval}(h, u^\frown 1))$$
- ak $h(u) = \forall x$, potom u má práve jedného nasledníka $u^\frown 0$
$$\mathrm{eval}(h, u) \doteq (\forall x)(\mathrm{eval}(h, u^\frown 0)).$$

Analogicky ako v prípade VPF definujeme množiny $\textsc{Var}(h)$, $\mathrm{FV}(h)$, $\mathrm{BV}(h)$. Výskyty v zmysle slov $\mathrm{eval}(h, \emptyset)$ sú tiež rovnaké. Strom nám umožňuje definovať výskyty ako uzly stromu takto:

Definícia 3.14
Voc – *Variable Occurence* – všetky uzly ohodnotené premennou

$$\textsc{Voc}(h) = \{u \in \mathrm{dom}(h) : h(u) \in \bigcup \textsc{Var}_J\}$$

Foc – *Free Variable Occurence*

$$\textsc{Foc}(h) = \{u \in \textsc{Voc}(h) : \text{ pre každé } i \in \mathrm{dom}(u) \text{ také, že } h(u \restriction i) = \forall x \text{ platí } x \neq h(u)\}$$

$$\textsc{Foc}(h, x) = \{u \in \textsc{Foc}(h) : h(u) = x\}$$

Boc – *Bounded Variable Occurence*

$$\textsc{Boc}(h) = \{u \in \textsc{Voc}(h) : \text{ existuje } i \in \mathrm{dom}(u) \text{ také, že } h(u \restriction i) = \forall h(u)\}$$

Definícia 3.15
Množina slov $\textsc{Form}_{\mathrm{VPF}} \subseteq J^*$ sa nazýva *množinou formúl definovaných pomocou vytvárajúcej postupnosti formuly*, ak

$$\varphi \in \textsc{Form}_{\mathrm{VPF}} \qquad \text{akk} \qquad \text{ex. VPF } \varphi_0, \ldots, \varphi_n \text{ také, že } \varphi \doteq \varphi_n$$

Definícia 3.16
Množina slov $\textsc{Form}_{\mathrm{STR}} \subseteq J^*$ sa nazýva *množinou formúl definovaných pomocou syntaktického stromu formuly*, ak platí:

$$\varphi \in \textsc{Form}_{\mathrm{STR}} \qquad \text{akk} \qquad \text{ex. } h \text{ také, že } \varphi \doteq \mathrm{eval}(h, \emptyset).$$

Veta 3.17

$$\textsc{Form}_{\mathrm{VPF}} = \textsc{Form}_{\mathrm{STR}} = \textsc{Form}$$

Úloha 3.18
Programy, prim. rekurz, TS – syntaktická analýza ako u výrokov a termov.

Označenie 3.19
Nech φ je formula a $\{x_1, \ldots, x_n\}$ sú navzájom rôzne premenné. Potom všetky voľné výskyty premenných $\{x_1, \ldots, x_n\}$ vo formule φ označíme

$$\varphi = E_1{}^{x_{i_1}} E_2{}^{x_{i_2}} E_3{}^{x_{i_3}} \ldots E_l{}^{x_{i_l}} E_{l+1}$$

pričom platí, že $i_1, \ldots, i_l$ je usporiadaná postupnosť čísel od 1 do n (s opakovaním) a pre $j \leq l$ každý

$$\operatorname{ind}(i_j) \in \{1, \ldots, n\}$$

označuje index premennej (t.j. $x_{i_j} = x_{\operatorname{ind}(i_j)}$), a každý výskyt

$$\varphi = \underbrace{(E_1{}^{x_{i_1}} E_2{}^{x_{i_2}} \ldots E_j)}_{E_1'}{}^{x_{i_j}} \underbrace{(E_{j+1}{}^{x_{i_{j+1}}} \ldots E_l{}^{x_{i_l}} E_{l+1})}_{E_2'}$$

je voľným výskytom premennej $x_{\operatorname{ind}(i,j)}$ v zmysle predošlej definície a sú to práve všetky výskyty.
Analogicky všetky viazané výskyty označíme

$$\varphi = F_1{}_{x_{i_1}} F_2{}_{x_{i_2}} \ldots F_l{}_{x_{i_e}} F_{l+1}$$

Definícia 3.20
Nech φ je formula a $\langle x_1, \ldots, x_n\rangle$ sú navzájom rôzne premenné typu $\langle A_1, A_2, \ldots, A_n\rangle$ a $\langle t_1, \ldots, t_n\rangle$ sú termy také, že $\operatorname{typh}(t_i) = A_i$. Potom substitúcia termov t_i za premenné x_i vo formule φ je syntaktická operácia definovaná na slove z abecedy J^* nasledovne:
Nech $\varphi = E_1{}^{x_{i_1}} E_2{}^{x_{i_2}} E_3{}^{x_{i_3}} \ldots E_l{}^{x_{i_l}} E_{l+1}$ sú všetky voľné výskyty premenných $\{x_1, \ldots, x_n\}$. Potom výsledok substitúcie

$$\varphi(x_1/t_1, \ldots, x_n/t_n) = E_1\ t_{\operatorname{ind}(i_j)}\ E_2\ t_{\operatorname{ind}(i_j)}\ E_3\ \ldots\ E_e\ t_{\operatorname{ind}(i_e)}\ E_{e+1}.$$

Simultánne nahradíme všetky voľné výskyty.

Definícia 3.21
Nech $h : T \to H$ je syntaktický strom formuly, $\langle x_1, \ldots, x_n\rangle$ sú navzájom rôzne premenné typu $\langle A_1, \ldots, A_n\rangle$ a $k_1, \ldots, k_n$ sú syntaktické stromy termov typu $\langle A_1, \ldots, A_n\rangle$.
Potom definujeme syntaktický strom formuly

$$ch = h(x_1/k_1, \ldots, x_n/k_n)$$

takto: $u \in \operatorname{dom}(ch)$ akk

- buď $u \notin \bigcup_{i=1}^{n} \textsc{Foc}(h, x_i)$ (u nie je ohodnotený premennou, a ak je, nie premennou $x_1, \ldots, x_n$) a $u \in \operatorname{dom}(h)$.
  Potom
  $$ch(u) = h(u)$$
- alebo existuje $l_u \in \bigcup_{i=1}^{n} \textsc{Foc}(h, x_i)$ a $h(l_u) = x_i$ a existuje uzol $w_u \in \operatorname{dom}(k_i)$ taký, že $u = l_u{}^\frown w_u$.
  Potom
  $$ch(u) = k_i(w_u)$$

Tvrdenie 3.22
Definícia $h(x_1/k_1, \ldots, x_n/k_n)$ je korektná a

$$\operatorname{eval}(h, \emptyset)(x_1/\operatorname{eval}(k_1, \emptyset), \ldots, x_n/\operatorname{eval}(k_n, \emptyset)) = \operatorname{eval}(h(x_1/k_1, \ldots, x_n/k_n), \emptyset)$$

Poznámka 3.23
Majme formulu $(\exists y)(x + y = z)$. Táto formula je pravdivá v $\mathbb{R}$, nie však v $\mathbb{N}$.
Substituovaním:

$$\varphi(y/u) \coloneqq (\exists u)(x + u = z)$$

sa význam zachová.
Ale

$$\varphi(x/x \cdot u) \coloneqq (\exists u)((x \cdot u) + u = z)$$

„hovorí niečo iné“, dokonca aj v $\mathbb{R}$.
Operácia môže meniť význam formuly, my by sme však chceli „dobrú“ substitúciu.

Definícia 3.24
Term t je substituovateľný za premennú x vo formule φ ($\varphi \coloneqq \mathrm{eval}(h, \emptyset)$),

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

ak pre každé $y \in \textsc{Var}(t)$ a pre každé $u \in \textsc{Foc}(h)$ také, že $h(u) = x$ platí:

$$\text{pre každé } i < \mathrm{dom}(i) : h(u \restriction i) \neq \forall y$$

alebo ekvivalentne:
Ak pre každé y, v, u platí, že ak $y \in \textsc{Var}(t)$ a $h(v) = \forall y$, potom

$$\text{ak } v \subseteq u \text{ a } h(u) = x, \text{ tak } u \notin \textsc{Foc}(h)$$

alebo ekvivalentne:
Pre každé y, v, u, ak $h(v) = \forall y$ a $v \subseteq u$ a $h(u) = x$ a $u \in \textsc{Foc}(h)$, potom

$$y \notin \textsc{Var}(t).$$

3.2 Sémantika predikátového počtu

$$\begin{array}{l} \text{Logický systém} \\ \text{(VP, PP, \dots)} \end{array} \begin{cases} \text{syntax} \begin{cases} \text{abeceda} \\ \text{termy} \\ \text{formuly} \\ \text{gramatika} \end{cases} \\ \\ \text{sémantika} \begin{cases} \text{možné svety} \begin{cases} \models \text{ formula je dokázateľná v štruktúre} \\ \text{tautológie} \end{cases} \\ \text{štruktúry jazyka} \end{cases} \end{cases}$$

„možné svety“ - štruktúry jazyka odzrkadľujú samotný jazyk, každá súčasť jazyka má vplyv na štruktúru jazyka.

Definícia 3.25
Majme jazyk predikátového počtu

$$J = \langle \mathcal{A}, \textsc{Var}_J = \{\textsc{Var}^A : A \in \mathcal{A}\}, \mathcal{C}_J = \{\mathcal{C}^A : A \in \mathcal{A}\}, \mathcal{P}_J, \mathcal{F}_J, \dots \rangle$$

potom $\mathfrak{M}$ sa nazýva *štruktúra jazyka* J, ak

$$\begin{aligned} \mathfrak{M} \quad = \quad & \langle \mathcal{D}_J^{\mathfrak{M}} = \{D(A) : A \in \mathcal{A}\}, \mathcal{C}_J^{\mathfrak{M}} = \{\mathcal{C}_{\mathfrak{M}}^A : A \in \mathcal{A}\}, \\ & \mathcal{P}_J^{\mathfrak{M}} = \{\mathcal{P}_{\mathfrak{M}}^{\bar{A}} : \bar{A} \in \bigcup_{n=1}^{\infty} {}^n\mathcal{A}\}, \mathcal{F}_J^{\mathfrak{M}} = \{\mathcal{F}_{\mathfrak{M}}^{\bar{A}} : \bar{A} \in \bigcup_{n=1}^{\infty} {}^{n+1}\mathcal{A}\} \rangle \end{aligned}$$

pričom

- D je indexovaný súbor množín a pre každé $A \in \mathcal{A}$ je $D(A) \neq \emptyset$ (nazývaná doména atribútu A)
- pre každé $A \in \mathcal{A}$ je $\mathcal{C}^A_{\mathfrak{M}} = \{c_{\mathfrak{M}} : c \in \mathcal{C}^A\}$ a každé $c_{\mathfrak{M}} \in D(\mathrm{typ}(c))$
- pre každé $\bar{A} \in \bigcup_{n=1}^{\infty} {}^n\mathcal{A}$ je ${}^I\mathcal{P}^{\bar{A}}_{\mathfrak{M}} = \{p^I_{\mathfrak{M}} : p \in \mathcal{P}^{\bar{A}}\}$ a ak $\bar{A} = (A_1, \ldots, A_n) = \mathrm{typ}(p)$, potom $p^I_{\mathfrak{M}}$ je *informatická reprezentácia* relačnej schémy $p(A_1, \ldots, A_n)$ vzhľadom k D, t.j.

$$p^I_{\mathfrak{M}} \subseteq {}^{\{A_1,\ldots,A_n\}}\bigcup \mathrm{rng}(D) \text{ také, že } z \in p_{\mathfrak{M}}; z(A_i) \in D(A_i)$$

- pre každé $\bar{A} = \langle A_1, \ldots, A_n; A_{n+1}\rangle$ je je $\mathcal{F}^{\bar{A}}_{\mathfrak{M}} = \{f_{\mathfrak{M}} : f \in \mathcal{F}^{\bar{A}}\}$ a $f_{\mathfrak{M}} : D(A_1) \times \ldots \times D(A_n) \to D(A_{n+1})$.

Definícia 3.26
Nech $\mathfrak{M}$ je štruktúra jazyka J a pre každé $A \in \mathcal{A}$ nech

$$e^A : \mathrm{V{\scriptstyle AR}}^A \to D(A)$$

je ohodnotenie premenných. Ďalej nech $e = \{e^A : A \in \mathcal{A}\}$. Nech $t_1, \ldots, t_n = t$ je vytvárajúca postupnosť termu t. Potom indukciou cez $i \leq n$ definujeme $t_i[e]$ hodnotu termu t_i pri ohodnotení premenných e takto:

- ak $t_i \in \bigcup \mathcal{C}_J$, potom $t_i[e] = (t_i)_{\mathfrak{M}}$
- ak $t_i \in \bigcup \mathrm{V{\scriptstyle AR}}_J$, potom $t_i[e] = e^{\mathrm{typ}(t_i)}(t_i)$
- ak existuje $j_1, \ldots, j_k < i$ a $\langle A_1, \ldots, A_k; A_{k+1}\rangle = \bar{A}$ a $f \in \mathcal{F}^{\bar{A}}$ také, že $t_i = f(t_{j_1}, \ldots, t_{j_k})$ potom

$$t_i[e] = f_{\mathfrak{M}}(t_{j_1}[e], \ldots, t_{j_k}[e])$$

Poznámka 3.27 (odborníci dokážu sami alebo na cvičení)
Táto definícia nezávisí od výberu vytvárajúcej postupnosti. Analogicky možno definovať pre syntaktický strom termu rekurzívnu procedúru

$$\mathrm{evalTV}(h, u, e)$$

Definícia 3.28
Nech $\mathfrak{M}$ je štruktúra jazyka J a $e = \{e^A : A \in \mathcal{A}\}$ je ohodnotenie premenných a nech $\varphi_1, \ldots, \varphi_n = \varphi$ je VPF φ. Potom indukciou cez $i \leq n$ definujeme

$$\mathfrak{M} \models \varphi_i[e]$$

t.j. či v štruktúre $\mathfrak{M}$ pri ohodnotení e je pravdivé φ_i.

- ak $\varphi_i = p(t_1, \ldots, t_n)$ je atomárna formula (t.j. $\mathrm{typ}(p) = \langle A_1, \ldots, A_n\rangle$ a $\mathrm{typh}(t_i) = A_i$) platí

$$\begin{array}{rll} \mathfrak{M} \models p(t_1, \ldots, t_n)[e] & \text{akk} & \{\langle A_i, t_i[e]\rangle : i \in \{1, \ldots, n\}\} \in p^I_{\mathfrak{M}} \quad \text{(informatická reprezentácia)} \\ \text{resp.} & \text{akk} & \langle t_1[e], \ldots, t_n[e]\rangle \in p^M_{\mathfrak{M}} \quad \text{(matematická reprezentácia)} \end{array}$$

- ak ex. $j < i$, také, že $\varphi_i = \neg(\varphi_j)$ potom

$$\mathfrak{M} \models \neg(\varphi_j)[e] \quad \text{akk} \quad \text{nie je pravda, že } \mathfrak{M} \models \varphi_j[e]$$

  (značíme $\mathfrak{M} \not\models \varphi_j[e]$)

- ak ex. $j, k < i$, také, že $\varphi_i \coloneqq (\varphi_j) \longrightarrow (\varphi_k)$ potom

$$\mathfrak{M} \models (\varphi_j \longrightarrow \varphi_k)[e] \quad \text{akk} \quad \text{z } \mathfrak{M} \models \varphi_j[e] \text{ plynie, že } \mathfrak{M} \models \varphi_k[e]$$

alebo ekvivalentne:

$$\text{nie je pravda, že } \mathfrak{M} \models \varphi_j[e] \text{ a súčasne } \mathfrak{M} \not\models \varphi_k[e]$$

Definícia 3.29
Nech $e = \{e^A : A \in \mathcal{A}\}$ je ohodnotenie premenných a nech $x \in \mathrm{VAR}^A$ a $m \in D(A)$. Potom

$$e(x/m) = \{e^A(x/m)\} \cup \{e^{A'} : A' \in \mathcal{A} \setminus \{A\}\}$$

pričom $e^A(x/m)$ je ohodnotenie premenných typu A prvkami z $D(A)$ tj. $e^A(x/m) : \mathrm{VAR}^A \longrightarrow D(A)$ definované nasledovne:

$$\begin{array}{rcl} e^A(x/m)(y) & = & e^A(y), \text{ ak } y \neq x \\ e^A(x/m)(x) & = & m \end{array}$$

Definícia 3.30 (pokračovanie definície 3.28)

- ak ex. $j < i$ a $x \in \bigcup \mathrm{VAR}_J$, také, že $\varphi_i \coloneqq (\forall x)\varphi_j$ potom

$$\mathfrak{M} \models ((\forall x)(\varphi_j))[e] \text{ akk pre každé } m \in D(A) \text{ platí } \mathfrak{M} \models \varphi_j[e(x/m)]$$

Definícia 3.31
Nech $t_0, \ldots, t_n \coloneqq t$ je vytvárajúca postupnosť termu a nech $x_1, \ldots, x_k$ sú navzájom rôzne premenné a $r_1, \ldots, r_k$ sú termy.
Potom $t(x_1/r_1, \ldots, x_k/r_k)$ definujeme indukciou podľa $i \leq n$ takto:

- ak $t_i \in \bigcup \mathrm{VAR}_J$ a $t_i = x_j$, pričom $j \in \{1, \ldots, k\}$ potom $t_i(x_1/r_1, \ldots, x_k/r_k) = r_j$
- $t_i \in (\bigcup \mathrm{VAR}_J \cup \bigcup \mathcal{C}_J) \setminus \{x_1, \ldots, x_k\}$ potom $t_i(x_1/r_1, \ldots, x_k/r_k) = t_i$
- ak $t_i = f(t_{i_1}, \ldots, t_{i_m})$, kde $i_1, \ldots, i_m < i$ potom

$$t_i(x_1/r_1, \ldots, x_k/r_k) = f(t_{i_1}(x_1/r_1, \ldots, x_k/r_k), \ldots, t_{i_m}(x_1/r_1, \ldots, x_k/r_k))$$

Veta 3.32 (pre odborníkov aj pre učiteľov)
Nech $t, r_1, \ldots, r_k$ sú termy a $\{x_1, \ldots, x_k\}$ navzájom rôzne premenné a e je ohodnotenie premenných, potom

$$t(x_1/r_1, \ldots, x_k/r_k)[e] = t[e(x_1/r_1[e], \ldots, x_k/r_k[e])]$$

Príklad 3.33
Nech $t = x^2 + 2xy + y^2$, $D = \mathbb{R}$, $r_1 = \sin z$, $r_2 = \cos z$ a $e(z) = \pi$, potom podľa vety:

$$\begin{array}{rcl} r_1[e] & = & \sin(\pi) = 0 \\ r_2[e] & = & \cos(\pi) = -1 \end{array}$$

a platí:

$$\begin{array}{rcl} e(x/r_1[e], y/r_2[e])(x) & = & 0 \\ e(x/r_1[e], y/r_2[e])(y) & = & -1 \end{array}$$

teda:

$$(x^2 + 2xy + y^2)[e(x/r_1[e], y/r_2[e])] = 0^2 + 2 \cdot 0 \cdot (-1) + (-1)^2 = 1$$

a

$$(x^2 + 2xy + y^2)(x/r_1, y/r_2)[e] = (\sin^2 z + 2 * \sin z + \cos z + \cos^2 z)[e] =$$
$$= (\sin^2 \pi + 2 * \sin \pi + \cos \pi + \cos^2 \pi) = 0^2 + 2 \cdot 0 \cdot (-1) + (-1)^2 = 1$$

<u>*Dôkaz.*</u>
Nech $t_1, \ldots, t_n \equiv t$ je vytvárajúca postupnosť termu t. Tvrdenie dokážeme indukciou cez $i \leq n$:

- ak $t_i \in \bigcup \mathrm{VAR}_J$ a $t_i = x_j$ potom:

  ľavá strana rovnosti: $t_i(x_1/r_1, \ldots, x_k/r_k) = r_j$ a
  $t_i(x_1/r_1, \ldots, x_k/r_k)[e] = r_j[e]$
  pravá strana rovnosti: $e^{\mathrm{typ}(x_j)}(x_1/r_1[e], \ldots, x_k/r_k[e])(x_j) = r_j[e]$
  $t_i[e(x_1/r_1[e], \ldots, x_k/r_k[e])] = r_j[e]$

- ak $t_i \in (\bigcup \mathrm{VAR}_J \cup \bigcup \mathcal{C}_J) - \{x_1, \ldots, x_k\}$, tak

  $$e \restriction \mathrm{VAR}(t_i) = e(x_1/r_1[e], \ldots, x_k/r_k[e]) \restriction \mathrm{VAR}(t_i)$$

  ľavá strana rovnosti: $t_i(x_1/r_1, \ldots, x_k/r_k)[e] = t_i[e]$
  pravá strana rovnosti: $t_i[e] = t_i[e(x_1/r_1[e], \ldots, x_k/r_k[e])]$

- existujú $i_1, \ldots, i_m < i$ a $f \in \bigcup \mathcal{F}_J$ také, že $\mathrm{typ}(f) = \langle A_1, \ldots, A_m; A_{m+1} \rangle$ a $\mathrm{typh}(t_{i_j}) = A_j$ a $t_i \equiv f(t_{i_1}, \ldots, t_{i_m})$ a platí indukčný predpoklad, potom

  ľavá strana rovnosti: $t_i(x_1/r_1, \ldots, x_k/r_k)[e] =$
  $f(t_{i_1}(x_1/r_1, \ldots, x_k/r_k), \ldots, t_{i_m}(x_1/r_1, \ldots, x_k/r_k))[e] =$
  $f_{\mathfrak{M}}(t_{i_1}(x_1/r_1, \ldots, x_k/r_k)[e], \ldots, t_{i_m}(x_1/r_1, \ldots, x_k/r_k)[e]) =$
  z IP: $f_{\mathfrak{M}}(t_{i_1}[e(x_1/r_1[e], \ldots, x_k/r_k[e])], \ldots, t_{i_m}[e(x_1/r_1, \ldots, x_k/r_k[e])]) =$
  (z def. ohodnot. termu) $f(t_{i_1}, \ldots, t_{i_m})[e(x_1/r_1[e], \ldots, x_k/r_k[e])] =$
  $t_i[e(x_1/r_1[e], \ldots, x_k/r_k[e])]$

□

Lemma 3.34
Nech t je term, $\{x_1, \ldots, x_k\}$ sú navzájom rôzne premenné, $\mathfrak{M}$ je štruktúra jazyka a e je ohodnotenie premenných a $m_i \in D(\mathrm{typ}(x_i))$, $i = 1, \ldots, k$.
Potom ak $\mathrm{VAR}(t) \cap \{x_1, \ldots, x_k\} = \emptyset$, tak $t[e] = t[e(x_1/m_1, \ldots, x_k/m_k)]$

<u>*Dôkaz.*</u>
Nech $t_1, \ldots, t_n \equiv t$ je vytvárajúca postupnosť termu.

- ak $t_i \in \bigcup \mathcal{C}_J$, potom $t_i[e] = (t_i)_{\mathfrak{M}} = t_i[e(x_1/m_1, \ldots, x_k, m_k)]$

- ak $t_i \in \bigcup \mathrm{VAR}_J$, potom $\mathrm{VAR}(t_i) = \{t_i\}$

- ak $t_i \notin \{x_1, \ldots, x_k\}$, potom

  $$t_i[e] = e^{\mathrm{typ}(t_i)}(t_i) = e(x_1/m_1, \ldots, x_k, m_k)^{\mathrm{typ}(t_i)}(t_i) = t_i[e(x_1/m_1, \ldots, x_k, m_k)].$$

- ak ex. $i_1, \ldots, i_m < i$ také, že $t_i = f(t_{i_1}, \ldots, t_{i_m})$, $\textsc{Var}(t_i) = \bigcup_{j=1}^{m} \textsc{Var}(t_{i_j}) \cap \{x_1, \ldots, x_m\} = \emptyset$. Potom

$$\begin{array}{rcl} t_i[e] & = & f(t_{i_1}, \ldots, t_{i_m})[e] \\ & = & f_{\mathfrak{M}}(t_{i_1}[e], \ldots, t_{i_m}[e] \\ \text{z IP} & = & f_{\mathfrak{M}}(t_{i_1}[e(x_1/m_1, \ldots, x_k, m_k)], \ldots, t_{i_m}[e(x_1/m_1, \ldots, x_k, m_k)]) \\ & = & f_{\mathfrak{M}}(t_{i_1}, \ldots, t_{i_m})[e(x_1/m_1, \ldots, x_k, m_k)] \end{array}$$

□

Poznámka 3.35
Všimnime si, že premenné v predpoklade sú disjunktné. Keďže vytvárajúca postupnosť termu nie je jednoznačná, keby sa použila nadbytočná časť, ktorá využije niektoré premenné, mohol by nastať problém.

Definícia 3.36
Nech t je term a $h : T \to H$ je syntaktický strom termu t (t.j. $\mathrm{eval}(h, \emptyset) = t$). *Kanonickou vytvárajúcou postupnosťou* termu t nazývame takú vytvárajúcu postupnosť, ktorá vznikne z usporiadania[1] ohodnotenia uzlov stromu T takto:

- ak $\mathrm{dom}(u_1) < \mathrm{dom}(u_2)$, potom $\mathrm{eval}(h, u^\frown 0) < \mathrm{eval}(h, u^\frown 1)$
- na rovnakej hladine platí: $\mathrm{eval}(h, u^\frown i) < \mathrm{eval}(h, u^\frown j)$, ak $i < j$.

Definícia 3.37
Nech $h : T \to H$ je syntaktický strom formuly $\varphi = \mathrm{eval}(h, \emptyset)$. Pre $u \in T$ označíme

$$\begin{array}{rcl} \varphi_u & = & \mathrm{eval}(h, u) \\ T^{-(\forall x)} & = & \{u \in T : (\forall v \subsetneq u)(h(v) \neq \forall x)\} \end{array}$$

Pre $u \in T$, $x \in \bigcup \textsc{Var}_J$ povieme, že voľné výskyty premennej x vo formule φ_u súhlasia s výskytmi, ktoré sú voľné aj z hľadiska celého φ (označenie $\mathsf{VVS}(u, x, \varphi)$) ak

$$\{u^\frown w : u^\frown w \in \textsc{Foc}(h, x)\} = \{u^\frown w : w \in \textsc{Foc}(h \restriction {T_u}^2, x)\}$$

Tvrdenie 3.38
Nech $u \in T^{-(\forall x)}$ potom platí $\mathsf{VVS}(u, x, \varphi)$ a $\mathrm{eval}(h(x/t), u) = \mathrm{eval}(h, u)(x/t)$.

<u>*Dôkaz.*</u>
Indukciou cez strom $T^{-(\forall x)}$.

- Ak u je list stromu $T^{-(\forall x)}$ potom môžu nastať dve možnosti:
  - „u je novým listom“ – tj. $h(u) = \forall x$ a $\varphi_u = (\forall x)(\varphi_{u^\frown 0})$. Potom žiaden výskyt x vo φ_u nie je voľný (ako z hľadiska φ_u, tak z hľadiska φ).
  - „u je list pôvodného stromu“ – ak $h(u) \in \bigcup \mathcal{C}$, tak tam nie je žiaden výskyt. Ak $h(u) = x$ tak tento výskyt je voľný aj z hľadiska φ lebo $u \in T^{-(\forall x)}$ a teda neexistuje nad ním uzol $v \subsetneq u$ taký, že by menil kvalitu výskytu t.j. $h(v) = \forall x$.

[1] Treba si uvedomiť, že relácia $<$ medzi „výsledkami“ funkcie eval je čosi ako lexikografické porovnanie, a nie v zmysle relácie $<$ pre prirodzené čísla.

[2] $h \restriction T_u$ treba rozumieť tak, že to je ohodnotenie podstromu T_u. Treba si uvedomiť, že to nie je len obyčajné zúženie zobrazenia, lebo napr. $(h \restriction T_u)(\emptyset) = h(u)$.

- Indukciou cez strom $T^{-(\forall x)}$ neexistuje uzol ohodnotený kvantifikátorom $\forall x$ a ten jediný môže meniť kvalitu výskytu premennej x.

$\square$

Tvrdenie 3.39
V predošlom označení, nech $u \in T^{-(\forall x)}$ je taký, že $h(u) = \forall x$. Nech $x \in \bigcup \mathrm{VAR}_J$, t je term, $\mathfrak{M}$ je štruktúra jazyka, $n \in D(\mathrm{typ}(x))$ a e je ohodnotenie premenných. Potom

$$\varphi_u(x/t) \quad = \quad \varphi_u \tag{1}$$
$$\mathfrak{M} \models \varphi_u[e] \quad \textit{akk} \quad \textit{pre každé } n \in D(\mathrm{typ}(x)) \quad \mathfrak{M} \models \varphi_u[e(x/n)]. \tag{2}$$

Dôkaz.
Ad 1: treba si uvedomiť, že x nemá vo φ_n voľný výskyt, teda niet za čo dosadzovať
Ad 2:
Označme $\varphi_{u^\frown 0} = \psi$, potom $\varphi_u = (\forall x)\psi$.
Nech

$$\mathfrak{M} \models ((\forall x)\psi)[e(x/n)].$$

To je však práve vtedy, keď

$$\text{pre každé } m \in D(\mathrm{typ}(x)) \text{ platí, že } \mathfrak{M} \models \psi[(e(x/n))(x/m)]$$

Keďže ale z dvoch po sebe idúcich zmien hodnôt $e^{\mathrm{typ}(x)}(x)$ „platí“ tá posledná, máme ekvivalentne

$$\mathfrak{M} \models \psi[e(x/m)] \quad \text{akk} \quad \mathfrak{M} \models (\forall x)\psi[e]$$

$\square$

Veta 3.40
Nech φ je formula, x premenná, t term, $\mathfrak{M}$ štruktúra jazyka a e je ohodnotenie premenných. Potom ak $\mathsf{Suble}(t, x, \varphi)$, *t.j. term t je substituovateľný za premennú x vo formule φ, tak*

$$\mathfrak{M} \models \varphi(x/t)[e] \quad \textit{akk} \quad \mathfrak{M} \models \varphi[e(x/t[e])].$$

Dôkaz.
Indukciou po hladinách stromu $T^{-(\forall x)}$ zdola nahor. Vieme už, že kvalita výskytov premennej x vo formulách φ_v pre $v \in T^{-(\forall x)}$ je tá istá ako ich kvalita z hľadiska celého φ. (z vety 3.38)
Indukčný predpoklad, ktorý budeme overovať je nasledovný:

- (IP-ŽVV) Pre $v \in T^{-(\forall x)}$ dokážeme, že platí:
  Ak x nemá vo φ_v žiaden voľný výskyt, potom pre každé $n \in D(\mathrm{typ}(x))$ a pre každé ohodnotenie e platí, že
  $$\mathfrak{M} \models \varphi_v[e] \quad \text{akk} \quad \mathfrak{M} \models \varphi_v[e(x/n)]$$
  a súčasne
- (IP-MVV)
  Ak x má vo φ_v voľný výskyt, potom pre každé ohodnotenie e platí:
  $$\mathfrak{M} \models \varphi_v(x/t)[e] \quad \text{akk} \quad \mathfrak{M} \models \varphi_v[e(x/t[e])]$$

1°) Indukciu naštartujeme na listoch stromu $T^{-(\forall x)}$. Môžu nastať dva prípady:

- list – prípad 1 – x nemá vo φ_v nemá žiaden voľný výskyt. Tu môžu nastať dve možnosti:

- $h(v) = \forall x$ – bolo dokázané v predchádzajúcom tvrdení 3.39
- $h(v) = p(t_1, \dots, t_n)$, kde $x \notin \textsc{Var}(h(v))$ (inak by bol voľný výskyt). Potom z vety 3.32 vieme, že pre každé $i = 1, \dots, n$ platí:
$$t_i(x/t)[e] = t_i[e(x/t[e])]$$
ale keďže x sa tam nevyskytuje, tak $t_i = t_i(x/t)$. Naviac jednoduchou modifikáciou pôvodného dôkazu dostaneme, že
$$\text{ak } x \notin \textsc{Var}(t_i) \text{ potom } t_i \equiv t_i(x/t)[e] \equiv t_i[e(x/n)],$$
lebo v rozbore prípadov vo vytvárajúcej postupnosti výroku nemôže nastať prípad, že sa tam vyskytne premenná x – overili sme IP-ŽVV.

- list – prípad 2 – x má vo φ_v voľný výskyt, potom $\varphi_v \equiv p(t_1, \dots, t_k)$ a všetky výskyty x vo φ_v sú voľné a sú voľné aj z hľadiska celého φ a
$$\varphi_v(x/t) = p(t_1(x/t), \dots, t_k(x/t))$$
(To je dôležité si uvedomiť, lebo do termu substituujeme vždy, ale do formuly len za voľné výskyty.) Potom platí:
$$\begin{array}{lccl} & \mathfrak{M} & \models & (p(t_1, \dots, t_k))(x/t)[e] \\ \text{akk} & \mathfrak{M} & \models & p(t_1(x/t), \dots, t_k(x/t))[e] \\ \text{akk} & & & \langle t_1(x/t)[e], \dots, t_k(x/t)[e]\rangle \in p^M_{\mathfrak{M}}, \text{ resp. } \{\langle A_j, t_j(x/t)[e]\rangle : j \leq k\} \in p^I_{\mathfrak{M}}) \\ \text{akk} & & & \langle t_1[e(x/t[e])], \dots, t_k[e(x/t[e])]\rangle \in p^M_{\mathfrak{M}}, \text{ resp. } \{\langle A_j, t_j[e(x/t[e])]\rangle : j \leq k\} \in p^I_{\mathfrak{M}}) \\ \text{akk} & \mathfrak{M} & \models & p(t_1, \dots, t_k)[e(x/t[e])], \end{array}$$
čím sme overili IP-MVV.

2°) ostatné uzly

- prípad $h(v) = \neg$
Potom sa kvalita výskytov x sa nezmenila a tvrdenie platí z jedného či druhého prípadu podľa definície splňovania formuly s negáciou.

- prípad $h(v) = \longrightarrow$
  - Ak sa stretli formuly s rovnakou kvalitou výskytov x, platí to na základe definície splňovania $\longrightarrow$ a rovnakého indukčného predpokladu.
  - Môže sa ale stať, že x má vo φ voľný výskyt, ak napríklad vo $\varphi_{v\frown 0}$ nemá žiaden voľný výskyt (platí IP-ŽVV) a vo $\varphi_{v\frown 1}$ má voľný výskyt (IP-MVV). Pre $\varphi_v \equiv (\varphi_{v_0}) \longrightarrow (\varphi_{v_1})$ potrebujeme overiť či platí IP-MVV, teda či
  $$\mathfrak{M} \models \varphi_v(x/t)[e] \text{ akk } \mathfrak{M} \models \varphi_v[e(x/t[e])].$$
  Nech $\mathfrak{M} \models \varphi_v(x/t)[e]$. To je vtedy a len vtedy keď (vieme, že $(\varphi_{v\frown 0})(x/t) = \varphi_{v\frown 0}$) z platnosti
  $$\mathfrak{M} \models \varphi_{v\frown 0}[e] \qquad \text{plynie} \qquad \mathfrak{M} \models (\varphi_{v\frown 1})(x/t)[e]$$
  Ľavá strana je na základe IP-ŽVV pre každé $n \in D(\text{typ}(x))$ a teda pre $n = t[e]$ ekvivalentná s $\mathfrak{M} \models \varphi_{v\frown 0}[e(x/t[e])]$.

Pravá strana je na základe IP-MVV ekvivalentná s $\mathfrak{M} \models \varphi_{v^\frown 1}[e(x/t[e])]$.
Týmito ekvivalenciami „po zložkách“ máme overené, že to celé je ekvivalentné tým, že z

$$\mathfrak{M} \models \varphi_{v^\frown 0}[e(x/t[e])] \qquad \text{plynie} \qquad \mathfrak{M} \models \varphi_{v^\frown 1}[e(x/t[e])]$$

a to opäť ekvivalentné s

$$\mathfrak{M} \models (\varphi_{v^\frown 0} \longrightarrow \varphi_{v^\frown 1})[e(x/t[e])].$$

- prípad $h(v) = \forall y$
  Keďže $v \in T^{-(\forall x)}$, vieme, že $x \neq y$.
  - **Možnosť 1:** φ_v a teda aj $\varphi_{v^\frown 0}$ nemá voľný výskyt premennej x
    Potom pre každé $n \in D(typ(x))$:

    $$\begin{array}{lll} \mathfrak{M} \models \varphi_v[e] & & \\ \text{akk} & \mathfrak{M} \models & (\forall y)(\varphi_{v^\frown 0})[e] \\ \text{akk} & \multicolumn{2}{l}{\text{pre každé } m \in D(\text{typ}(y)) \text{ platí:}} \\ & \mathfrak{M} \models & \varphi_{v^\frown 0}[e(y/m)] \end{array}$$

    Teraz z indukčného predpokladu IP-ŽVV pre ohodnotenie $e(y/m)$ to je ekvivalentné s

    $$\mathfrak{M} \models \varphi_{v^\frown 0}[(e(y/m))(x/n)]$$

    Keďže $x \neq y$ (lebo $v \in T^{-(\forall x)}$), tieto dve zmeny hodnôt sa dajú „prehodiť“ a teda máme ekvivalentne s

    $$\begin{array}{lll} & \mathfrak{M} \models & \varphi_{v^\frown 0}[(e(x/n))(y/m)] \\ \text{akk} & \mathfrak{M} \models & \varphi_v[e(x/n)], \end{array}$$

    čím sme overili IP-ŽVV.
  - **Možnosť 2**. Nech φ_v má voľný výskyt premennej x (a teda aj $\varphi_{v^\frown 0}$).
    Teraz sú splnené predpoklady definície o substituovateľnosti t za premennú x vo formule φ, lebo ak $u \in \textsc{Foc}(\varphi_v, x)$ tak určite $v \subsetneq u$, lebo v nie je list. Platí teda $y \notin \textsc{Var}(t)$.
    Potom:

    $$\begin{array}{lll} & \mathfrak{M} \models & \varphi_v(x/t)[e] \\ \text{akk} & \mathfrak{M} \models & (\forall y)(\varphi_{v^\frown 0})(x/t)[e] \\ \text{akk} & \multicolumn{2}{l}{\text{pre každé } m \in D(\text{typ}(y))} \\ & \mathfrak{M} \models & \varphi_{v^\frown 0}(x/t)[e(y/m)] \end{array}$$

    Teraz na základe IP-MVV pre ohodnotenie $e(y/m)$ platí

    $$\mathfrak{M} \models \varphi_{v^\frown 0}[(e(y/m))(x/t[e(y/m)])]$$

    Teraz prichádza kľúčový moment, keď použijeme predpoklad substituovateľnosti, keďže $y \notin \textsc{Var}(t)$ (zo substituovateľnosti) platí, že $t[e(y/m)] = t[e]$, a teda je to ekvivalentné s

    $$\mathfrak{M} \models \varphi_{v^\frown 0}[(e(y/m))(x/t[e])]$$

    opäť použitím $x \neq y$ prehodíme dve zmeny

    $$\begin{array}{lll} & \mathfrak{M} \models & \varphi_{v^\frown 0}[(e(x/t[e]))(y/m)] \\ \text{akk} & \mathfrak{M} \models & (\forall y)(\varphi_{v^\frown 0})[e(x/t[e])] \\ \text{akk} & \mathfrak{M} \models & \varphi_v[e(x/t[e])], \end{array}$$

    čím sme overili IP-MVV.

$\square$

Veta 3.41
Nech $\mathsf{Suble}(t, x, \varphi)$*. Potom pre každé* $\mathfrak{M}$ *a* e *platí*

$$\mathfrak{M} \models ((\forall x)\varphi \longrightarrow \varphi(x/t))[e].$$

Dôkaz.
Treba overiť, že ak $\mathfrak{M} \models (\forall x)\varphi[e]$ tak potom aj $\mathfrak{M} \models \varphi(x/t)[e]$.
$\mathfrak{M} \models (\forall x)\varphi[e]$ znamená, že pre každé $m \in D(\text{typ}(x))$ platí, že $\mathfrak{M} \models \varphi[e(x/m)]$. Keď pre každé m, potom aj pre $m = t[e]$ (lebo term substituujeme, ak typh(t) = typ(x)). Teda $\mathfrak{M} \models \varphi[e(x/t[e])]$. Z predchádzajúcej vety potom platí $\mathfrak{M} \models \varphi(x/t)[e]$. □

Veta 3.42
Nech φ *je také, že* x *v nej nemá žiaden voľný výskyt. Potom pre každé* $\mathfrak{M}$ *a* e *platí:*

$$\mathfrak{M} \models ((\forall x)(\varphi \longrightarrow \psi) \longrightarrow (\varphi \longrightarrow (\forall x)\psi))[e].$$

Dôkaz.
Treba overiť, či z platnosti $\mathfrak{M} \models (\forall x)(\varphi \longrightarrow \psi)[e]$ plynie $\mathfrak{M} \models (\varphi \longrightarrow (\forall x)\varphi)[e]$.
Nech $\mathfrak{M} \models (\forall x)(\varphi \longrightarrow \psi)[e]$ potom, pre každé $n \in D(\text{typ}(x))$ platí $\mathfrak{M} \models (\varphi \longrightarrow \psi)[e(x/n)]$ a to znamená, že z platnosti $\mathfrak{M} \models \varphi[e(x/n)]$ plynie platnosť $\mathfrak{M} \models \psi[e(x/n)]$, a to pre každé $n \in D(\text{typ}(x))$.
Teraz potrebujeme overiť, či z platnosti $\mathfrak{M} \models \varphi[e]$ plynie pre každé $n \in D(\text{typ}(x))$ aj $\mathfrak{M} \models \psi[e(x/n)]$.
Použijeme predpoklad, že x nemá vo φ žiadny voľný výskyt. Potom z predošlého tvrdenia o substituovateľnosti a overovania indukčného predpokladu IP-ŽVV platí, že pre každé $n \in D(\text{typ}(x))$

$$\mathfrak{M} \models \varphi[e] \text{ akk } \mathfrak{M} \models \varphi[e(x/n)].$$

Môžeme použiť predpoklad, že z $\mathfrak{M} \models \varphi[e(x/n)]$ plynie $\mathfrak{M} \models \psi[e(x/n)]$ pre každé n a teda $\mathfrak{M} \models (\varphi \longrightarrow (\forall x)\psi)[e]$. □

Definícia 3.43
Povieme, že φ je *pravdivé* v $\mathfrak{M}$ ($\mathfrak{M} \models \varphi$), ak pre každé e platí, že

$$\mathfrak{M} \models \varphi[e].$$

Definícia 3.44
Povieme, že φ je tautológia predikátového počtu ($\models \varphi$), ak pre každé $\mathfrak{M}$ platí, že

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

Veta 3.45
Nech φ, ψ *sú formuly,* x *premenná a* t *term. Potom nasledujúce formuly sú tautológie predikátového počtu:*

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

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

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

Ax. 4 *Ak* $\mathsf{Suble}(t, x, \varphi)$ *potom* $((\forall x)\varphi \longrightarrow \varphi(x/t))$ *je tautológia*

Ax. 5 *Ak* x *nemá vo* φ *žiaden voľný výskyt, potom*

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

je tautológia.

Tvrdenie 3.46
Ak $\models \varphi$ *potom* $\models (\forall x)\varphi$.

Dôkaz.
Nech $\mathfrak{M}$ a e sú ľubovoľné. Overíme, či platí

$$\mathfrak{M} \models (\forall x)\varphi[e].$$

To je ale ekvivalentné s tým, že pre každé $n \in D(\text{typ}(x))$ platí

$$\mathfrak{M} \models \varphi[e(x/n)].$$

To je však pravda, lebo $\models \varphi$ znamená, že pre každé $\mathfrak{M}$ a každé ohodnotenie e (t.j. špeciálne pre ohodnotenie $e(x/n)$) platí

$$\mathfrak{M} \models \varphi[e(x/n)].$$

□

Definícia 3.47 (dôkaz v predikátovom počte)
Postupnosť formúl $\varphi_0, \ldots, \varphi_n$ sa nazýva *dôkaz*, ak pre každé $i \leq n$ platí, že

- buď φ_i je jedna z logických axióm (Ax. 1) až (Ax. 5)
- alebo existujú $j, k < i$ také, že
  - buď $\varphi_j = \varphi_k \longrightarrow \varphi_i$ (*modus ponens*)
  - alebo $\varphi_i = (\forall x)\varphi_j$ (*generalizácia*)

Definícia 3.48
Formula φ je dokázateľná (označujeme $\vdash \varphi$), ak existuje dôkaz $\varphi_0, \ldots, \varphi_n = \varphi$.

Veta 3.49 (korektnosť predikátového počtu)
Ak $\vdash \varphi$ *potom* $\models \varphi$.

Dôkaz.
Dôkaz je podobný ako vo výrokovom počte – indukciou pozdĺž dôkazu dokážeme, že $\models \varphi_i$.

- každá axióma je tautológia,
- *modus ponens* zachováva tautologičnosť (veta 3.45)
- *generalizácia* zachováva tautologičnosť (veta 3.46)

□

V systéme LaTeXvysádzali: Ladislav Pálfi a Róbert Novotný (`r.novotny@szm.sk`)
Odborná korektúra: Marián Dvorský (`marian@step.sk`)
URL: `http://skmi.science.upjs.sk/~novotnyr`
Verzia 30. 5. 2003 (X_2)