Prednášky z Matematiky (4) — Logiky pre informatikov

Ján Kľuka, Jozef Šiška

Katedra aplikovanej informatiky
FMFI UK Bratislava

Letný semester 2017/2018

10. prednáška

Korektnosť tabiel pre logiku prvého rádu

30. apríla 2018

Obsah 10. prednášky

Oznamy

3 Logika prvého rádu
- Tablá pre logiku prvého rádu
- Korektnosť tablového kalkulu pre logiku prvého rádu
  - Ďalšie korektné pravidlá

Náhradné cvičenia

Náhradné cvičenia:

stredy 2. a 9. mája	2AIN1	14:50 ~~M–I~~ **H-6**
	2AIN2	16:30 M-IX
	2AIN3	16:30 M-XI
piatky 4. a 11. mája	3AIN$*$, ktorí nemôžu v stredu	
		9:50 F1-328

Organizácia skúšok

Termíny skúšok:

Termín	Písomná časť	Ústna časť
Riadny	pon 21. mája 13:00 posl. A	pia 25. mája 9:30 I-9
1. opravný	pia 1. júna 9:30 posl. B	pia 8. júna 9:30 I-9
2. opravný	uto 19. júna 9:30 posl. A	pia 22. júna 9:30 I-9

Ústna skúška:

- Poradie študentov je dané poradím zapísania sa v AIS.
- Paralelne traja skúšajúci.
- Príprava + odpoveď: 15 + 15 min.
- Počas odpovede jednej trojice študentov sa ďalšia trojica bude pripravovať.

Sémantika logiky prvého rádu

Štruktúry

Definícia 3.38

Nech $\mathcal{L}$ je jazyk logiky prvého rádu.
Štruktúrou pre jazyk $\mathcal{L}$ nazývame dvojicu $\mathcal{M} = (M, i)$, kde

doména M štruktúry $\mathcal{M}$ je ľubovoľná **neprázdna** množina;

interpretačná funkcia i štruktúry $\mathcal{M}$ je zobrazenie, ktoré

- každému symbolu konštanty c jazyka $\mathcal{L}$ priraďuje prvok $i(c) \in M$;
- každému funkčnému symbolu f jazyka $\mathcal{L}$ s aritou n priraďuje funkciu $i(f) : M^n \longrightarrow M$;
- každému predikátovému symbolu P jazyka $\mathcal{L}$ s aritou n priraďuje množinu $i(P) \subseteq M^n$.

Hodnota termu

Definícia 3.42

Nech $\mathcal{M} = (M, i)$ je štruktúra pre jazyk logiky prvého rádu $\mathcal{L}$,
nech e je ohodnotenie premenných.
Hodnotou termu t v štruktúre $\mathcal{M}$ pri ohodnotení premenných e
je prvok z M označovaný $\boldsymbol{t^{\mathcal{M}}[e]}$ a zadefinovaný induktívne nasledovne:

$$\begin{aligned} \boldsymbol{x^{\mathcal{M}}[e]} &= e(x), \text{ ak } x \text{ je premenná,} \\ \boldsymbol{a^{\mathcal{M}}[e]} &= i(a), \text{ ak } a \text{ je konštanta,} \\ \boldsymbol{\big(f(t_1, \ldots, t_n)\big)^{\mathcal{M}}[e]} &= i(f)(t_1^{\mathcal{M}}[e], \ldots, t_n^{\mathcal{M}}[e]), \text{ ak } t_1, \ldots, t_n \text{ sú termy.} \end{aligned}$$

Splnenie formuly v štruktúre

Definícia 3.44

Nech $\mathcal{M} = (M, i)$ je štruktúra, e je ohodnotenie premenných.
Relácia ***štruktúra $\mathcal{M}$ spĺňa formulu A pri ohodnotení e*** (skrátene $\mathcal{M} \models A[e]$) má nasledovnú induktívnu definíciu:

- $\mathcal{M} \models t_1 \doteq t_2[e]$ vtt $t_1^{\mathcal{M}}[e] = t_2^{\mathcal{M}}[e]$,
- $\mathcal{M} \models P(t_1, \ldots, t_n)[e]$ vtt $\left(t_1^{\mathcal{M}}[e], \ldots, t_n^{\mathcal{M}}[e]\right) \in i(P)$,
- $\mathcal{M} \models \neg A[e]$ vtt $\mathcal{M} \not\models A[e]$,
- $\mathcal{M} \models (A \wedge B)[e]$ vtt $\mathcal{M} \models A[e]$ a zároveň $\mathcal{M} \models B[e]$,
- $\mathcal{M} \models (A \vee B)[e]$ vtt $\mathcal{M} \models A[e]$ alebo $\mathcal{M} \models B[e]$,
- $\mathcal{M} \models (A \rightarrow B)[e]$ vtt $\mathcal{M} \not\models A[e]$ alebo $\mathcal{M} \models B[e]$,
- $\mathcal{M} \models \exists x\, A[e]$ vtt pre nejaký prvok $m \in M$ máme $\mathcal{M} \models A[e(x/m)]$,
- $\mathcal{M} \models \forall x\, A[e]$ vtt pre každý prvok $m \in M$ máme $\mathcal{M} \models A[e(x/m)]$,

pre všetky arity $n > 0$, všetky predikátové symboly P s aritou n,
všetky termy $t_1, t_2, \ldots, t_n$, všetky premenné x a všetky formuly A, B.

Voľné premenné a splnenie formuly. Teórie

Tvrdenie 3.58

Nech $\mathcal{M}$ je štruktúra pre $\mathcal{L}$, nech e_1 a e_2 sú ohodnotenia,
nech X je formula jazyka $\mathcal{L}$, nech S je množina formúl jazyka $\mathcal{L}$.

- *Ak sa ohodnotenia e_1 a e_2 zhodujú na voľných premenných formuly X (teda $e_1(x) = e_2(x)$ pre každú $x \in \mathrm{free}(X)$), tak $\mathcal{M} \models X[e_1]$ vtt $\mathcal{M} \models X[e_2]$.*
- *Ak sa ohodnotenia e_1 a e_2 zhodujú na voľných premenných všetkých formúl z S, tak $\mathcal{M} \models S[e_1]$ vtt $\mathcal{M} \models S[e_2]$.*

Definícia 3.59

Formula A jazyka $\mathcal{L}$ je ***uzavretá*** vtt neobsahuje žiadne voľné výskyty premenných (teda $\mathrm{free}(x) = \emptyset$). ***Teóriou*** v jazyku $\mathcal{L}$ je každá spočítateľná množinu uzavretých formúl jazyka $\mathcal{L}$.

Splnenie množiny formúl, teórie

Definícia 3.61 (+ 3.46)

Nech S je množina formúl jazyka $\mathcal{L}$, nech A je formula jazyka $\mathcal{L}$,
nech $\mathcal{M}$ je štruktúra pre $\mathcal{L}$, nech e je ohodnotenie indiv. premenných.

Štruktúra $\mathcal{M}$ (súčasne) spĺňa množinu S pri ohodnotení e ($\mathcal{M} \models S[e]$) vtt
pre všetky formuly A z S platí $\mathcal{M} \models A[e]$.

Štruktúra $\mathcal{M}$ spĺňa formulu A ($\mathcal{M} \models A$) vtt
A je splnená v štruktúre $\mathcal{M}$ pri každom ohodnotení e.

Štruktúra $\mathcal{M}$ spĺňa množinu S ($\mathcal{M}$ je ***modelom*** S, $\mathcal{M} \models S$) vtt
pre všetky formuly A z S platí $\mathcal{M} \models A$.

Nezávislosť od ohodnotení

Dôsledok 3.62

Nech X je uzavretá formula jazyka $\mathcal{L}$, nech $\mathcal{M}$ je štruktúra pre $\mathcal{L}$.
Potom sú nasledujúce tvrdenia ekvivalentné:

a. $\mathcal{M} \models X$ *(teda* $\mathcal{M} \models X[e]$ *pre každé* e*),*
b. $\mathcal{M} \models X[e]$ *pri aspoň jednom ohodnotení* e*.*

Dôsledok 3.63

Nech T je teória v jazyku $\mathcal{L}$, nech $\mathcal{M}$ je štruktúra pre $\mathcal{L}$.
Potom sú nasledujúce tvrdenia ekvivalentné:

a. $\mathcal{M} \models T$,
b. $\mathcal{M} \models T[e]$ *pre všetky ohodnotenia* e,
c. $\mathcal{M} \models T[e]$ *pre aspoň jedno ohodnotenie* e.

Splniteľnosť, nesplniteľnosť, platnosť

Definícia 3.47

Nech X je formula jazyka $\mathcal{L}$ a nech S je množina formúl jazyka $\mathcal{L}$.

Formula X je ***splniteľná*** vtt aspoň jedna štruktúra $\mathcal{M}$ pre $\mathcal{L}$ spĺňa X pri aspoň jednom ohodnotení e.

Množina formúl S je ***splniteľná*** vtt aspoň jedna štruktúra $\mathcal{M}$ pre $\mathcal{L}$ spĺňa S pri aspoň jednom ohodnotení e.

Formula X (množina formúl S) je ***nesplniteľná*** vtt nie je splniteľná.

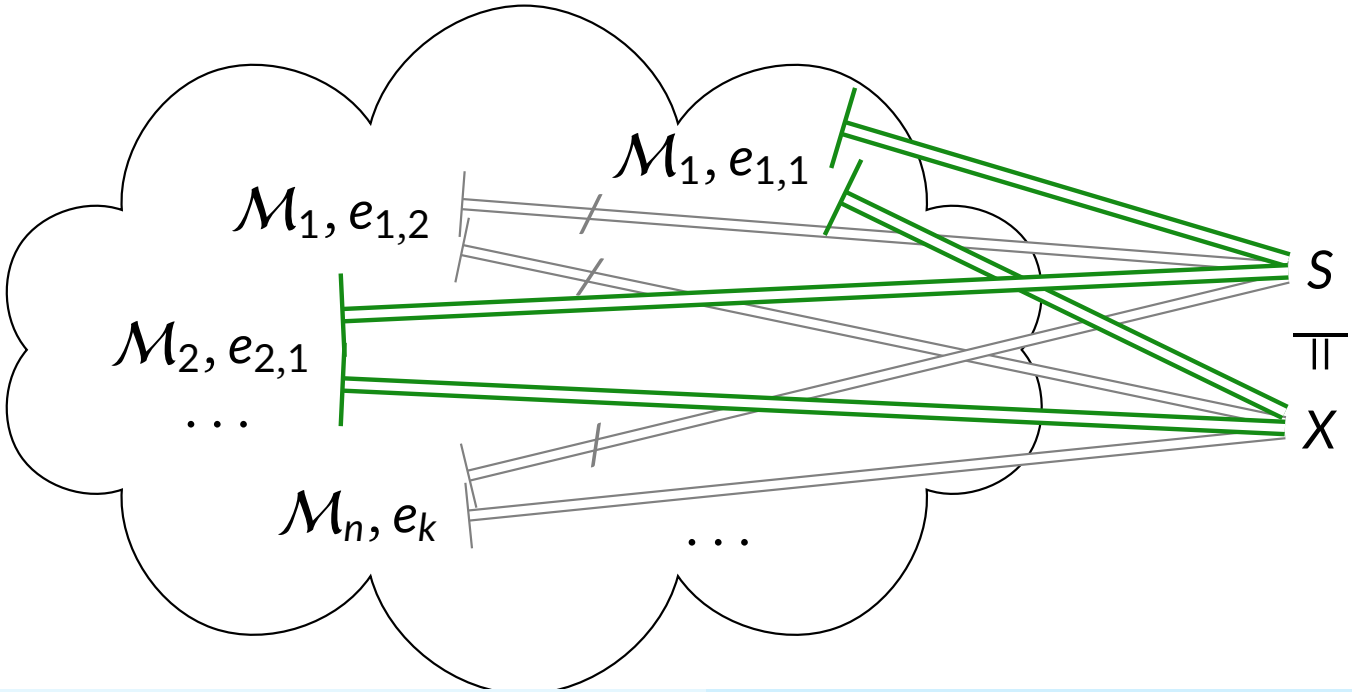
Definícia 3.48

Nech X je formula v jazyku $\mathcal{L}$.
Formula X je ***platná*** (skrátene $\models X$) vtt
každá štruktúra $\mathcal{M}$ pre $\mathcal{L}$ spĺňa X pri každom ohodnotení e.

Prvorádové vyplývanie

Definícia 3.49

Nech X je formula v jazyku $\mathcal{L}$, nech S je množina formúl v jazyku $\mathcal{L}$.
Formula X ***(prvorádovo) vyplýva*** z S
(tiež X je ***logickým dôsledkom*** S, skrátene $\boldsymbol{S \models X}$)
vtt pre každú štruktúru $\mathcal{M}$ pre $\mathcal{L}$ a každé ohodnotenie e platí, že
ak $\mathcal{M}$ spĺňa S pri e, tak $\mathcal{M}$ spĺňa X pri e.



Vzťah splniteľnosti a vyplývania

Podobne ako vo výrokovej logike platí:

Tvrdenie 3.51

Nech X je formula a S je množina formúl v jazyku $\mathcal{L}$.
Formula X prvorádovo vyplýva z S vtt
množina $S \cup \{\neg X\}$ je prvorádovo súčasne nesplniteľná.

Substitúcie

Substitúcia a aplikovateľnosť

Definícia 3.64 (Substitúcia)

Substitúciou (v jazyku $\mathcal{L}$) nazývame každé zobrazenie $\sigma : V \to \mathcal{T}_{\mathcal{L}}$
z nejakej množiny indivíduových premenných $V \subseteq \mathcal{V}_{\mathcal{L}}$ do termov jazyka $\mathcal{L}$.

Príklad 3.65

Napríklad $\sigma_1 = \{x \mapsto \mathtt{matka}(y), y \mapsto \mathtt{Adelka}\}$ je substitúcia.

Aplikovateľnosť substitúcie

Definícia 3.67 (Substituovateľnosť, aplikovateľnosť substitúcie)

Nech A postupnosť symbolov, nech t je term, x je premenná,
nech $\sigma = \{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$ je substitúcia.

Term t je ***substituovateľný*** za premennú x v A vtt
pre žiadnu premennú y vyskytujúcu sa v t
žiaden voľný výskyt premennej x v A
sa nenachádza v oblasti platnosti kvantifikátora $\exists y$ ani $\forall y$ v A.

Substitúcia σ je ***aplikovateľná*** na A vtt
term t_i je substituovateľný za x_i v A pre každé $i \in \{1, \ldots, n\}$.

Príklad 3.68

Ak $A = \exists y\ \mathtt{rodič}(y, x)$ a $\sigma_2 = \{x \mapsto \mathtt{matka}(y)\}$,
tak σ_2 **nie je aplikovateľná** na A.

Použitie substitúcie

Definícia 3.69 (Substitúcia do postupnosti symbolov)

Nech A je postupnosť symbolov,
nech $\sigma = \{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$ je substitúcia.
Ak σ je aplikovateľná na A, tak $A\sigma$ je postupnosť symbolov, ktorá vznikne *súčasným* dosadením t_i za každý *voľný* výskyt premennej x_i v A.

Príklad 3.70

Ak $A = (z \doteq \mathrm{Madga} \wedge \exists z\, \mathrm{rodič}(z, x))$
a $\sigma_3 = \{x \mapsto \mathrm{matka}(u), y \mapsto \mathrm{Adelka}, z \mapsto \mathrm{matka}(y)\}$,
tak σ_3 **je aplikovateľná** na A
a $A\sigma_3 = (\mathrm{matka}(y) \doteq \mathrm{Madga} \wedge \exists z\, \mathrm{rodič}(z, \mathrm{matka}(u)))$

Substitúcia do termov a formúl rekurzívne

Tvrdenie 3.71

Pre každú substitúciu $\sigma = \{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$, *každú premennú* $y \in \mathcal{V}_{\mathcal{L}} \setminus \{x_1, \ldots, x_n\}$, *každý symbol konštanty* $a \in \mathcal{C}_{\mathcal{L}}$, *každý funkčný symbol* $f^k \in \mathcal{P}_{\mathcal{L}}$, *každý predikátový symbol* $P^k \in \mathcal{P}_{\mathcal{L}}$, *každé* $i \in \{1, \ldots, n\}$, *každú spojku* $\diamond \in \{\wedge, \vee, \rightarrow\}$, *všetky formuly A a B a všetky termy* s_1, s_2, $\ldots$, $s_k \in \mathcal{T}_{\mathcal{L}}$ *platí:*

$$x_i\sigma = t_i \qquad y\sigma = y \qquad a\sigma = a \qquad (f(s_1, \ldots, s_k))\sigma = f(s_1\sigma, \ldots, s_k\sigma)$$

$$(s_1 \doteq s_2)\sigma = (s_1\sigma \doteq s_2\sigma) \qquad (P(s_1, \ldots, s_k))\sigma = P(s_1\sigma, \ldots, s_k\sigma)$$

$$(\neg A)\sigma = \neg(A\sigma) \qquad ((A \diamond B))\sigma = (A\sigma \diamond B\sigma)$$

$$(\forall y\, A)\sigma = \forall y\, (A\sigma) \qquad (\exists y\, A)\sigma = \exists y\, (A\sigma)$$

$$(\forall x_i\, A)\sigma = \forall x_i\, (A\sigma_i) \qquad (\exists x_i\, A)\sigma = \exists x_i\, (A\sigma_i),$$

kde $\sigma_i = \sigma \setminus \{x_i \mapsto t_i\}$.

Sémantika substitúcie

Tvrdenie 3.76 (+ 3.75)

Nech t je term a A je formula jazyka $\mathcal{L}$
a nech $\sigma = \{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$ je substitúcia aplikovateľná na A.
Nech $\mathcal{M}$ je štruktúra pre $\mathcal{L}$ a nech e je ohodnotenie indivíduových premenných.
Potom $(t\sigma)^{\mathcal{M}}[e] = t^{\mathcal{M}}[e(x_1/t_1^{\mathcal{M}}[e]) \cdots (x_n/t_n^{\mathcal{M}}[e])]$
a $\mathcal{M} \models A\sigma[e]$ vtt $\mathcal{M} \models A[e(x_1/t_1^{\mathcal{M}}[e]) \cdots (x_n/t_n^{\mathcal{M}}[e])]$.

Inak povedané:
Štruktúra spĺňa formulu $A\sigma$ po substitúcii pri ohodnotení e
vtt spĺňa pôvodnú formulu A pri takom ohodnotení e',
ktoré každej substituovanej premennej x_i priradí hodnotu za ňu
substituovaného termu t_i pri ohodnotení e
a ostatným premenným priraďuje rovnaké hodnoty ako e.

3.7

Tablá pre logiku prvého rádu

Splnenie označených formúl, vyplývanie

Podobne ako vo výrokovej logike môžeme zaviesť označovanie formúl logiky prvého rádu znamienkami **T** a **F**.

Definícia 3.78

Nech $\mathcal{M}$ je štruktúra pre jazyk $\mathcal{L}$, nech e je ohodnotenie indivíduových premenných, nech X je formula jazyka $\mathcal{L}$. Potom:

- $\mathcal{M} \models \mathbf{T}\,X[e]$ vtt $\mathcal{M} \models X[e]$;
- $\mathcal{M} \models \mathbf{F}\,X[e]$ vtt $\mathcal{M} \not\models X[e]$.

Splnenie množiny označených formúl a ***splniteľnosť*** ozn. formuly/množiny ozn. formúl definujeme analogicky ako pre neoznačené formuly.

Tvrdenie 3.79

Nech X je formula a S je množina formúl v jazyku $\mathcal{L}$.
Formula X prvorádovo vyplýva z S vtt
množina $\{\mathbf{T}\,Y \mid Y \in S\} \cup \{\mathbf{F}\,X\}$ je prvorádovo súčasne nesplniteľná.

Jednotný zápis označených formúl — α a β

Pre všetky definície odteraz zvoľme pevne ľubovoľný jazyk logiky prvého rádu $\mathcal{L}$.

Definícia 3.80 (Jednotný zápis označených formúl typu α)

Označená formula je ***typu*** $\boldsymbol{\alpha}$ vtt má jeden z tvarov v ľavom stĺpci tabuľky pre nejaké formuly A a B. Takéto formuly označujeme písmenom $\boldsymbol{\alpha}$; $\boldsymbol{\alpha_1}$ označuje príslušnú formulu zo stredného stĺpca a $\boldsymbol{\alpha_2}$ príslušnú formulu z pravého stĺpca.

α	α_1	α_2
$\mathbf{T}(A \wedge B)$	$\mathbf{T}A$	$\mathbf{T}B$
$\mathbf{F}(A \vee B)$	$\mathbf{F}A$	$\mathbf{F}B$
$\mathbf{F}(A \rightarrow B)$	$\mathbf{T}A$	$\mathbf{F}B$
$\mathbf{T}\neg A$	$\mathbf{F}A$	$\mathbf{F}A$
$\mathbf{F}\neg A$	$\mathbf{T}A$	$\mathbf{T}A$

Definícia 3.81 (Jednotný zápis označených formúl typu β)

Označená formula je ***typu*** $\boldsymbol{\beta}$ vtt má jeden z tvarov v ľavom stĺpci tabuľky pre nejaké formuly A a B. Takéto formuly označujeme písmenom $\boldsymbol{\beta}$; $\boldsymbol{\beta_1}$ označuje príslušnú formulu zo stredného stĺpca a $\boldsymbol{\beta_2}$ príslušnú formulu z pravého stĺpca.

β	β_1	β_2
$\mathbf{F}(A \wedge B)$	$\mathbf{F}A$	$\mathbf{F}B$
$\mathbf{T}(A \vee B)$	$\mathbf{T}A$	$\mathbf{T}B$
$\mathbf{T}(A \rightarrow B)$	$\mathbf{F}A$	$\mathbf{T}B$

Jednotný zápis označených formúl — γ a δ

Definícia 3.82 (Jednotný zápis označených formúl typu γ)

Označená formula je ***typu*** $\boldsymbol{\gamma}$ vtt má jeden z tvarov v ľavom stĺpci tabuľky pre nejakú formulu A a indivíduovú premennú x.
Takéto formuly označujeme $\boldsymbol{\gamma(x)}$ a pre ľubovoľný term t substituovateľný za x v A príslušnú formulu z pravého stĺpca označujeme $\boldsymbol{\gamma_1(t)}$.

$\gamma(x)$	$\gamma_1(t)$
$\mathbf{F}\,\exists x\,A$	$\mathbf{F}A\{x \mapsto t\}$
$\mathbf{T}\,\forall x\,A$	$\mathbf{T}A\{x \mapsto t\}$

Definícia 3.83 (Jednotný zápis označených formúl typu δ)

Označená formula je ***typu*** $\boldsymbol{\delta}$ vtt má jeden z tvarov v ľavom stĺpci tabuľky pre nejakú formulu A a indivíduovú premennú x.
Takéto formuly označujeme $\boldsymbol{\delta(x)}$ a pre ľubovoľnú premennú y substituovateľnú za x v A príslušnú formulu z pravého stĺpca označujeme $\boldsymbol{\delta_1(y)}$.

$\delta(x)$	$\delta_1(y)$
$\mathbf{T}\,\exists x\,A$	$\mathbf{T}A\{x \mapsto y\}$
$\mathbf{F}\,\forall x\,A$	$\mathbf{F}A\{x \mapsto y\}$

Rovnosť

- Pravidlá pre α a β formuly umožňujú pracovať s logickými spojkami
- Pravidlá pre γ a δ formuly umožňujú pracovať s kvantifikátormi.
- V jazyku je ešte jeden logický symbol — rovnosť ($\doteq$)
- Žiadne pravidlo s ňou zatiaľ nepracuje
- Čo potrebujeme, aby rovnosť mala očakávané vlastnosti?

Axiomatizácia rovnosti

- Rovnosť by sme mohli popísať teóriou — *axiomatizovať* ju
- Je reflexívna, symetrická a tranzitívna:

$$\forall x\, x \doteq x$$

$$\ldots$$

- Navyše má vlastnosť substitúcie alebo *kongruencie*:
  Pre každý pár rovnajúcich sa k-tic argumentov:
  - hodnota každého funkčného symbolu f^k je rovnaká,
  - každý predikátový symbol P^k je
    na oboch k-tiach splnený alebo na oboch nesplnený.

$$\forall x_1\, \forall y_1 \ldots \forall x_k\, \forall y_k \big(x_1 \doteq y_1 \wedge \cdots \wedge x_k \doteq y_k \rightarrow \cdots\big)$$

Dôkazy s axiomatizovanou rovnosťou

- Skúsme niečo dokázať:

1. $\mathbf{T}\ \mathrm{matka}(\mathrm{Oliverko}) \doteq \mathrm{Magda}$ S^+
2. $\mathbf{T}\ \exists x\, \mathrm{prvé\_dieťa}(\mathrm{matka}(\mathrm{Oliverko}), x) \doteq \mathrm{Adelka}$ S^+
3. $\mathbf{F}\ \exists x\, \mathrm{prvé\_dieťa}(\mathrm{Magda}, x) \doteq \mathrm{Adelka}$ S^+

...

Eulerovo pravidlo

- Dôkazy s axiómami rovnosti sú prácne aj v jednoduchých prípadoch
- Vlastnosť kongruencie sa však dá induktívne zovšeobecniť na ľubovoľné formuly
- ***Eulerovo pravidlo***: V každej formule môžeme nahradiť rovné rovným

1.	$\mathbf{T}\,\mathtt{matka}(\mathtt{Oliverko}) \doteq \mathtt{Magda}$	S^+
2.	$\mathbf{T}\,\exists x\,\mathtt{prvé\_dieťa}(\mathtt{matka}(\mathtt{Oliverko}), x) \doteq \mathtt{Adelka}$	S^+
3.	$\mathbf{T}\,\exists x\,\mathtt{prvé\_dieťa}(\mathtt{Magda}, x) \doteq \mathtt{Adelka}$	Euler 1, 2

- Ale **naozaj**?

$$\mathbf{T}\,\mathtt{matka}(\mathtt{Oliverko}) \doteq x$$

$$\mathbf{T}\,\exists x\,\mathtt{prvé\_dieťa}(\mathtt{matka}(\mathtt{Oliverko}), x) \doteq \mathtt{Adelka}$$

$$\mathbf{T}\,\exists x\,\mathtt{prvé\_dieťa}(x, x) \doteq \mathtt{Adelka}$$

partenogenéza?!?

Eulerovo pravidlo presne

- ***Eulerovo pravidlo***: V každej formule môžeme nahradiť rovné rovným
- Čo znamená „nahradiť“? A kedy to môžeme urobiť *bez zmeny významu* formuly?
- Substitúcia $\{x \mapsto t\}$ nahrádza premennú termom
- Eulerovo pravidlo potrebuje nahradiť jeden term t_1 druhým t_2
- Dá sa to popísať substitúciami? Áno:
- Chceme nahradiť term $t_1 = \mathtt{matka}(\mathtt{Oliverko})$ termom $t_2 = \mathtt{Magda}$ vo formule:

$$
\begin{aligned}
A_1^+ &= \mathbf{T}\,\exists x\, \mathtt{prvé\_dieťa}(\mathtt{matka}(\mathtt{Oliverko}), x) \doteq \mathtt{Adelka} \\
&= A^+\{q \mapsto \mathtt{matka}(\mathtt{Oliverko})\} \\
A^+ &= \mathbf{T}\,\exists x\, \mathtt{prvé\_dieťa}(q, x) \doteq \mathtt{Adelka} \\
A_2^+ &= A^+\{q \mapsto \mathtt{Magda}\} \\
&= \mathbf{T}\,\exists x\, \mathtt{prvé\_dieťa}(\mathtt{Magda}, x) \doteq \mathtt{Adelka}
\end{aligned}
$$

Eulerovo pravidlo — obmedzenia

- Vyjadrenie Eulerovho pravidla pomocou substitúcií:

$$\frac{\mathbf{T}\, t_1 \doteq t_2 \qquad A^+\{q \mapsto t_1\}}{A^+\{q \mapsto t_2\}}$$

- Automaticky dostávame aj **rozumné obmedzenia**
- **Nemôžeme** nahradiť term $t_1 = \mathtt{matka(Oliverko)}$ termom $t_2 = \underline{x}$ vo formule:

$$\begin{aligned} A_1^+ &= \mathbf{T}\,\exists \underline{x}\, \mathtt{prvé\_dieťa}(\mathtt{matka(Oliverko)}, \underline{x}) \doteq \mathtt{Adelka} \\ &= A^+\{q \mapsto \mathtt{matka(Oliverko)}\} \\ A^+ &= \mathbf{T}\,\exists \underline{x}\, \mathtt{prvé\_dieťa}(q, \underline{x}) \doteq \mathtt{Adelka} \end{aligned}$$

lebo substitúcia $\{q \mapsto \underline{x}\}$ **nie je aplikovateľná** na A^+ ($\underline{x}$ je viazané v mieste voľného výskytu q)

Vlastnosti rovnosti

- Eulerovo pravidlo odvodí symetriu, tranzitivitu aj kongruenciu
- Ale potrebuje pomocníčku — reflexivitu:

$$\frac{}{\mathbf{T}\, t_0 \doteq t_0}$$

- Symetriu potom odvodíme v table postupnosťou krokov:

1.	$\mathbf{T}\, t_1 \doteq t_2$		
2.	$\mathbf{T}\, t_1 \doteq t_1$	reflexivita	$A^+\{q \mapsto t_1\}$ pre $A^+ = \mathbf{T}\, q \doteq t_1$
3.	$\mathbf{T}\, t_2 \doteq t_1$	Euler 1 a 2	$A^+\{q \mapsto t_2\}$

- Tranzitivitu odvodíme:

1.	$\mathbf{T}\, t_1 \doteq t_2$		$A^+\{q \mapsto t_2\}$ pre $A^+ = \mathbf{T}\, t_1 \doteq q$
2.	$\mathbf{T}\, t_2 \doteq t_3$		
3.	$\mathbf{T}\, t_2 \doteq t_1$	Euler 2 a 1	$A^+\{q \mapsto t_3\}$

Tablové pravidlá pre logiku prvého rádu

Definícia 3.84

Tablovými pravidlami pre logiku prvého rádu sú:

$$\frac{\alpha}{\alpha_1} \qquad \frac{\alpha}{\alpha_2} \qquad\qquad \frac{\beta}{\beta_1 \mid \beta_2}$$

$$\frac{\gamma(x)}{\gamma_1(t)} \qquad\qquad \frac{\delta(x)}{\delta_1(y)}$$

$$\frac{}{\mathbf{T}\, t_0 \doteq t_0} \qquad\qquad \frac{\mathbf{T}\, t_1 \doteq t_2 \quad A^+\{x \mapsto t_1\}}{A^+\{x \mapsto t_2\}}$$

pre všetky ozn. formuly $\alpha, \beta, \gamma(x), \delta(x)$ príslušných typov a všetky im zodpovedajúce $\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1(t)$ a $\delta_1(y)$, všetky termy t_0, všetky ozn. formuly A^+, všetky termy t_1 a t_2 substituovateľné za x do príslušnej A^+.

Tablo pre množinu označených formúl

Definícia 3.85

Analytické tablo pre množinu označených formúl S^+ (skrátene ***tablo pre S^+***) je binárny strom, ktorého vrcholy obsahujú označené formuly a ktorý je skonštruovaný induktívne podľa nasledovných pravidiel:

- Strom s jediným vrcholom (koreňom) obsahujúcim niektorú označenú formulu A^+ z S^+ je tablom pre S^+.
- Nech $\mathcal{T}$ je tablo pre S^+ a ℓ je nejaký jeho list. Potom tablom pre S^+ je aj každé ***priame rozšírenie*** $\mathcal{T}$ ktoroukoľvek z operácií:
  - **A** Ak sa na vetve π_ℓ (ceste z koreňa do ℓ) vyskytuje nejaká označená formula α, tak ako jediné dieťa ℓ pripojíme nový vrchol obsahujúci α_1 alebo α_2.
  - **B** Ak sa na vetve π_ℓ vyskytuje nejaká označená formula β, tak ako deti ℓ pripojíme dva nové vrcholy, pričom ľavé dieťa bude obsahovať β_1 a pravé β_2.
  - **S^+** Ako jediné dieťa ℓ pripojíme nový vrchol obsahujúci ľubovoľnú označenú formulu $A^+ \in S^+$.

Tablo pre množinu označených formúl

Definícia 3.85 (pokračovanie)

C Ak sa na vetve π_ℓ vyskytuje nejaká označená formula $\gamma(x)$, tak ako jediné dieťa ℓ pripojíme nový vrchol obsahujúci $\gamma_1(t)$ pre ľubovoľný term t substituovateľný za x v $\gamma_1(x)$.

D Ak sa na vetve π_ℓ vyskytuje nejaká označená formula $\delta(x)$, tak ako jediné dieťa ℓ pripojíme nový vrchol obsahujúci $\delta_1(y)$ pre ľubovoľnú premennú y, ktorá je substitovateľná za x v $\delta_1(x)$ a **nemá voľný výskyt** v žiadnej formule na vetve π_ℓ.

E Ak sa na vetve π_ℓ vyskytuje $\mathbf{T}\, t_1 \doteq t_2$ pre nejaké termy t_1 a t_2 a označená formula $A^+\{x \mapsto t_1\}$ pre nejakú A^+, v ktorej sú t_1 a t_2 substituovateľné za x, tak ako jediné dieťa ℓ pripojíme nový vrchol obsahujúci $A^+\{x \mapsto t_2\}$.

R Ako jediné dieťa ℓ pripojíme nový vrchol obsahujúci označenú formulu $\mathbf{T}\, t \doteq t$ pre ľubovoľný term t.

3.8

Korektnosť tablového kalkulu pre logiku prvého rádu

Korektnosť tablových pravidiel

Tvrdenie 3.86

Nech S je množina označených formúl v jazyku $\mathcal{L}$, nech x a y sú premenné, nech s, t sú termy, nech α, β, γ, δ sú ozn. formuly príslušného typu, A je ozn. formula.

- *Ak $\alpha \in S$, tak S je splniteľná vtt $S \cup \{\alpha_1, \alpha_2\}$ je splniteľná.*
- *Ak $\beta \in S$,*
  tak S je splniteľná vtt $S \cup \{\beta_1\}$ je splniteľná alebo $S \cup \{\beta_2\}$ je splniteľná.
- *Ak $\gamma(x) \in S$ a τ je term substituovateľný za x v $\gamma_1(x)$,*
  tak S je splniteľná vtt $S \cup \{\gamma_1(\tau)\}$ je splniteľná.
- *Ak $\delta(x) \in S$, y je substituovateľná za x v $\delta_1(x)$*
  a y sa nemá voľný výskyt v S,
  tak S je splniteľná vtt $S \cup \{\delta_1(y)\}$ je splniteľná.
- *S je splniteľná vtt $S \cup \{\mathbf{T}\, t \doteq t\}$ je splniteľná.*
- *Ak $\{\mathbf{T}\, t_1 \doteq t_2, A^+\{x \mapsto t_1\}\} \subseteq S$, tak $S \cup \{A^+\{x \mapsto t_2\}\}$ je splniteľná.*

Korektnosť tablových pravidiel — dôkaz

Dôkaz (čiastočný, pre pravidlo δ v smere $\Longrightarrow$).

Zoberme ľubovoľné S, x, y, t a $\delta(x)$ spĺňajúce predpoklady tvrdenia. Nech S je splniteľná, teda existuje štruktúra $\mathcal{M}$ a ohodnotenie e také, že $\mathcal{M} \models S[e]$. Preto aj $\mathcal{M} \models \delta(x)[e]$. Podľa tvaru $\delta(x)$ môžu nastať nasledujúce dva prípady.

- Ak $\delta(x) = \mathbf{T}\,\exists x A$ pre nejakú formulu A, tak podľa def. 3.78 $\mathcal{M} \models \exists x A[e]$ a podľa def. spĺňania máme nejakého *svedka* $m \in M$ takého, že $\mathcal{M} \models A[e(x/m)]$. Podľa tvr. 3.76 potom $\mathcal{M} \models A\{x \mapsto y\}[e(x/m)(y/m)]$. Prem. x nie je voľná v $A\{x \mapsto y\}$, preto podľa tvr. 3.58 $\mathcal{M} \models A\{x \mapsto y\}[e(y/m)]$, teda $\mathcal{M} \models \mathbf{T}\,A\{x \mapsto y\}[e(y/m)]$, teda $\mathcal{M} \models \delta_1(y)[e(y/m)]$.
- Ak $\delta(x) = \mathbf{F}\,\forall y A$ pre nejakú formulu A, tak podľa def. 3.78 $\mathcal{M} \not\models \forall x A[e]$ a podľa def. spĺňania neplatí, že $\mathcal{M} \models A[e(x/m)]$ pre každé $m \in M$. Preto máme nejaký *kontrapríklad* $m \in M$ taký, že $\mathcal{M} \not\models A[e(x/m)]$. Podľa tvr. 3.76 potom $\mathcal{M} \not\models A\{x \mapsto y\}$ $[e(x/m)(y/m)]$. Prem. x nie je voľná v $A\{x \mapsto y\}$, preto podľa tvr. 3.58 $\mathcal{M} \not\models A\{x \mapsto y\}[e(y/m)]$, teda $\mathcal{M} \models \mathbf{F}\,A\{x \mapsto y\}[e(y/m)]$, čiže $\mathcal{M} \models \delta_1(y)[e(y/m)]$.

Navyše y nie je voľná v žiadnej formule z S, preto $\mathcal{M} \models S[e(y/m)]$. Teda $\mathcal{M} \models (S \cup \{\delta_1(y)\})[e(y/m)]$. Preto je $S \cup \{\delta_1(y)\}$ splniteľná. □

Korektnosť prvorádových tabiel

Otvorené a uzavreté vetvy a tablá sú definované rovnako ako pri tablách pre výrokovú logiku.

Veta 3.87 (Korektnosť tablového kalkulu)

Nech S^+ je množina označených formúl.
Ak existuje uzavreté tablo $\mathcal{T}$ pre S^+, tak je množina S^+ nesplniteľná.

Dôkaz (nepriamy).

Nech S^+ je množina označených formúl.
Nech S^+ je splniteľná. Dokážeme, že každé tablo $\mathcal{T}$ pre S^+ je otvorené, úplnou indukciou na počet vrcholov tabla $\mathcal{T}$.
...

□

3.8.1

Ďalšie korektné pravidlá

Pohodlnejšie verzie pravidiel γ a δ

Tvrdenie 3.88

Nasledujúce pravidlá sú korektné:

$$\gamma^* \quad \frac{\mathbf{T}\,\forall x_1 \ldots \forall x_n\, A}{\mathbf{T}\,A\{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}} \qquad \frac{\mathbf{F}\,\exists x_1 \ldots \exists x_n\, A}{\mathbf{F}\,A\{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}}$$

$$\delta^* \quad \frac{\mathbf{F}\,\forall x_1 \ldots \forall x_n\, A}{\mathbf{F}\,A\{x_1 \mapsto y_1, \ldots, x_n \mapsto y_n\}} \qquad \frac{\mathbf{T}\,\exists x_1 \ldots \exists x_n\, A}{\mathbf{T}\,A\{x_1 \mapsto y_1, \ldots, x_n \mapsto y_n\}}$$

kde A je formula, $x_1, \ldots, x_n$ sú premenné,
$t_1, \ldots, t_n$ sú termy substituovateľné za príslušné $x_1, \ldots, x_n$ v A
a $y_1, \ldots, y_n$ sú premenné substituovateľné za príslušné $x_1, \ldots, x_n$ v A
*pričom $y_1, \ldots, y_n$ sa **nevyskytujú voľné** vo vetve, v liste ktorej je pravidlo použité.*

Pravidlá pre ekvivalenciu

Tvrdenie 3.89

Nasledujúce pravidlá sú korektné:

$$ESTT \quad \frac{\mathbf{T}(A_1 \leftrightarrow A_2) \quad \mathbf{T}\,A_i}{\mathbf{T}\,A_{3-i}} \qquad ESTF \quad \frac{\mathbf{T}(A_1 \leftrightarrow A_2) \quad \mathbf{F}\,A_i}{\mathbf{F}\,A_{3-i}}$$

$$ESFT \quad \frac{\mathbf{F}(A_1 \leftrightarrow A_2) \quad \mathbf{T}\,A_i}{\mathbf{F}\,A_{3-i}} \qquad ESFF \quad \frac{\mathbf{F}(A_1 \leftrightarrow A_2) \quad \mathbf{F}\,A_i}{\mathbf{T}\,A_{3-i}}$$

kde A_1 a A_2 sú formuly, $i \in \{1, 2\}$.

Dokazovanie s rovnosťou a explicitnými definíciami

- Využime nové pravidlá na dôkaz vlastnosti množín.
- Zoberme jazyk $\mathcal{L}$, kde $C_{\mathcal{L}} = \{\emptyset\}$, $\mathcal{P}_{\mathcal{L}} = \{\in^2, \subseteq^2\}$ a $\mathcal{F}_{\mathcal{L}} = \{\cup^2, \cap^2, \setminus^2, \complement^1\}$.
- Binárne symboly budeme zapisovať infixovo, napr. namiesto $\in(t_1, t_2)$ napíšeme $t_1 \in t_2$, namiesto $\cup(t_1, t_2)$ napíšeme $(t_1 \cup t_2)$, ...

Príklad 3.90

Dokážme tablom, že $T \models X$ pre

$$T = \left\{ \begin{array}{c} \forall x\, \forall y (x \subseteq y \leftrightarrow \forall z (z \in x \rightarrow z \in y)) \\ \forall x\, \forall y\, \forall z (z \in (x \cup y) \leftrightarrow (z \in x \vee z \in y)) \end{array} \right\}$$

$$X = \forall x\, \forall y ((x \cup y) \doteq x \rightarrow y \subseteq x)$$

Literatúra

Martin Davis and Hillary Putnam. A computing procedure for quantification theory. *J. Assoc. Comput. Mach.*, 7:201–215, 1960.

Martin Davis, George Logemann, and Donald Loveland. A machine program for theorem-proving. *Communications of the ACM*, 5(7):394–397, 1962.

Michael Genesereth and Eric Kao. *Introduction to Logic*. Morgan & Claypool, 2013. ISBN 9781627052481.

Christos H. Papadimitriou. *Computational complexity*. Addison-Wesley, 1994. ISBN 978-0-201-53082-7.

Raymond M. Smullyan. *Logika prvého rádu*. Alfa, 1979. Z angl. orig. *First-Order Logic*, Berlin-Heidelberg: Springer-Verlag, 1968 preložil Svätoslav Mathé.

Vítězslav Švejdar. *Logika: neúplnost, složitost, nutnost*. Academia, 2002. Prístupné aj na http://www1.cuni.cz/~svejdar/book/LogikaSve2002.pdf.