Prednášky z Matematiky (4) – Logiky pre informatikov

Ján Kľuka, Jozef Šiška

Katedra aplikovanej informatiky
FMFI UK Bratislava

Letný semester 2015/2016

7. prednáška

Logika s rovnosťou

11. apríla 2016

Obsah 7. prednášky

Symboly jazyka logiky s rovnosťou

Definícia

Symbolmi jazyka logiky s rovnosťou $\mathcal{L}$ sú:

- *symboly* (*indivíduových*) *premenných* z nejakej nekonečnej spočítateľnej množiny $\mathcal{V}$ (označujeme ich x, y, ...);
- *mimologické* symboly:
  - *symboly konštánt* z nejakej spočítateľnej množiny $\mathcal{C}$ (a, b, ...);
  - *funkčné symboly* z nejakej spočítateľnej množiny $\mathcal{F}$ (f, g, ...);
  - *predikátové symboly* z nejakej spočít. množiny $\mathcal{P}$ (P, R, ...);
- *logické symboly*:
  - *logické spojky*: unárna $\neg$, binárne $\land$, $\lor$, $\to$;
  - *symbol rovnosti* $\doteq$ (niekedy zapisovaný priamo ako $=$);
- *pomocné symboly* (,) a , (ľavá, pravá zátvorka a čiarka);

Množiny $\mathcal{V}$, $\mathcal{C}$, $\mathcal{F}$ a $\mathcal{P}$ sú vzájomne disjunktné a neobsahujú logické a pomocné symboly.

Každému symbolu $S \in \mathcal{P} \cup \mathcal{F}$ je priradená *arita* $\mathrm{ar}(S) \in \mathbb{N}^+$.

Symboly jazyka logiky s rovnosťou

Poznámka

Symboly (konštánt, funkčné, predikátové) môžu byť nealfanumerické (1, $<$, $+$), či tvorené viacerými znakmi (empty, Even, push).

Dohoda

Aritu budeme niekedy písať ako horný index symbolov (pop^1, $<^2$).

Príklad

Jazyk grafov $\mathcal{L}_\mathsf{G}$ má dva predikátové symboly: unárny V a binárny E.
Jazyk usporiadania $\mathcal{L}_\mathsf{O}$ má dva binárne predikátové symboly: $<$, $\leq$.
Jazyk aritmetiky $\mathcal{L}_\mathsf{A}$ má symbol konštanty 0, funkčné symboly S^1, $+^2$, $\cdot^2$ a predikátové symboly $<^2$, $\leq^2$.
Jazyk zásobníkov $\mathcal{L}_\mathsf{S}$ by mohol mať napr. symbol konštanty empty, funkčné symboly push^2, top^1, pop^1 a predikátový symbol $\mathrm{is\_empty}^1$.

Termy jazyka logiky s rovnosťou

Definícia

Termy jazyka logiky s rovnosťou $\mathcal{L}$ sú postupnosti symbolov jazyka $\mathcal{L}$ definované rekurzívne nasledujúcimi pravidlami:

- Každý symbol premennej x je termom.
- Každý symbol konštanty c je termom.
- Ak f je funkčný symbol s aritou n a $t_1, \dots, t_n$ sú termy, tak aj $f(t_1, \dots, t_n)$ je termom.
- Nič iné nie je termom.

Dohoda

Termy označujeme písmenami t, s, r s prípadnými dolnými indexmi.

Termy jazyka logiky s rovnosťou

Príklad

Skonštruujme niekoľko termov v jazyku zásobníkov $\mathcal{L}$ so symbolmi premenných x, y, z, ..., symbolom konštanty empty, funkčnými symbolmi push^2, top^1, pop^1 a s predikátovým symbolom $\mathrm{is\_empty}^1$.

Formuly jazyka logiky s rovnosťou

Definícia

Formuly jazyka logiky s rovnosťou $\mathcal{L}$ sú postupnosti symbolov jazyka $\mathcal{L}$ definované rekurzívne nasledujúcimi pravidlami:

- Ak t_1 a t_2 sú termy, tak $t_1 \doteq t_2$ je formula (*rovnostný atóm*).
- Ak P je predikátový symbol s aritou n a t_1, ..., t_n sú termy, tak $P(t_1, \ldots, t_n)$ je formula (*predikátový atóm*).
- Ak A je formula, tak aj $\neg A$ je formula (*negácia* A).
- Ak A a B sú formuly, tak aj $(A \land B)$, $(A \lor B)$, $(A \to B)$ sú formuly (*konjunkcia*, *disjunkcia*, *implikácia* A a B).
- Nič iné nie je formula.

Dohoda

Formuly označujeme písmenami A, B, C, ... s prípadnými indexmi. Predikátové a rovnostné atómy súhrnne nazývame *atómy*, *atomické*

Formuly jazyka logiky s rovnosťou

Príklad

Skonštruujme niekoľko atómov a formúl v jazyku zásobníkov $\mathcal{L}$ so symbolmi premenných x, y, z, ..., symbolom konštanty empty, funkčnými symbolmi push^2, top^1, pop^1 a s predikátovým symbolom $\mathrm{is\_empty}^1$.

Zjednodušenie zápisu formúl

Dohoda

Zápis formúl môžeme zjednodušovať nasledujúcim spôsobom:

- Vonkajší pár zátvoriek môžeme vždy vynechať, teda napr. namiesto $(a \doteq b \to b \doteq a)$ môžeme písať $a \doteq b \to b \doteq a$.
- Binárnym spojkám priradíme prioritu:
  najvyššiu má $\land$, nižšiu $\lor$, najnižšiu $\to$.
  Ak $W = (A\, b_1\, B)$ je priamou podformulou $(X\, b_2\, Y)$ (teda $W = X$ alebo $W = Y$) a b_1 má vyššiu prioritu ako b_2, môžeme vynechať zátvorky okolo W. Napr. namiesto

  $$((P(x,y) \land (P(z,x) \lor P(y,z))) \to (P(x,z) \lor P(z,x)))$$

  môžeme písať

  $$P(x,y) \land (P(x,z) \lor P(y,z)) \to P(x,z) \lor P(z,x)$$

Štruktúry

Definícia

Nech $\mathcal{L}$ je jazyk logiky s rovnosťou.
Štruktúrou pre jazyk $\mathcal{L}$ nazývame dvojicu $\mathcal{M} = (M, \square^{\mathcal{M}})$, kde

- M je neprázdna množina, *doména* štruktúry $\mathcal{M}$;
- $\square^{\mathcal{M}}$ je zobrazenie, *interpretačná funkcia* štruktúry $\mathcal{M}$, ktoré
  - každému symbolu konštanty c jazyka $\mathcal{L}$ priraďuje prvok $c^{\mathcal{M}} \in M$;
  - každému funkčnému symbolu f jazyka $\mathcal{L}$ s aritou n priraďuje funkciu $f^{\mathcal{M}} \colon M^n \to M$;
  - každému predikátovému symbolu P jazyka $\mathcal{L}$ s aritou n priraďuje množinu $P^{\mathcal{M}} \subseteq M^n$.

Dohoda

Štruktúry označujeme veľkými kaligrafickými písmenami $\mathcal{M}$, $\mathcal{N}$, ...
Doménu označujeme rovnakým, ale tlačeným písmenom ako štruktúru.

Štruktúry

Štruktúra priraďuje symbolom jazyka význam: konštantám prvky domény, funkčným symbolom skutočné funkcie na doméne, a predikátom množiny tých n-tíc prvkov, pre ktoré predikát platí.

Príklad

Popíšme príklady štruktúr pre $\mathcal{L}_{\mathsf{G}}$, $\mathcal{L}_{\mathsf{O}}$, $\mathcal{L}_{\mathsf{A}}$, $\mathcal{L}_{\mathsf{S}}$.

Jazyk sa dá prirovnať k abstraktnej triede (alebo interfacu v Jave): deklaruje mená metód, ale neurčuje ich význam.
Štruktúra je potom ako konkrétna podtrieda takejto abstraktnej triedy, v ktorej majú všetky metódy implementáciu.

Ohodnotenie premenných, hodnota termov

Definícia

Nech $\mathcal{M} = (M, \square^{\mathcal{M}})$ je štruktúra pre jazyk $\mathcal{L}$.
Ohodnotenie (indivíduových) premenných je ľubovoľná funkcia $e\colon \mathcal{V} \to M$ (priraďuje premenným prvky domény).

Zápisom $e(x/v)$ označíme ohodnotenie premenných, ktoré priraďuje premennej x hodnotu v z domény M a všetkým ostatným premenným rovnakú hodnotu ako e.

Definícia

Nech $\mathcal{M} = (M, \square^{\mathcal{M}})$ je štruktúra, e je ohodnotenie premenných.
Hodnotou termu t v štruktúre $\mathcal{M}$ pri ohodnotení premenných e je prvok $t^{\mathcal{M}}[e]$ z M určený nasledovne:

- $x^{\mathcal{M}}[e] = e(x)$, ak x je premenná,
- $a^{\mathcal{M}}[e] = a^{\mathcal{M}}$, ak a je konštanta,
- $\big(f(t_1, \ldots, t_n)\big)^{\mathcal{M}}[e] = f^{\mathcal{M}}(t_1^{\mathcal{M}}[e], \ldots, t_n^{\mathcal{M}}[e])$, ak $t_1, \ldots, t_n$ sú termy.

Ohodnotenie premenných, hodnota termov

Príklad

Vyhodnoťme v štruktúre $\mathcal{N} = (\mathbb{N}, \square^{\mathcal{N}})$ pre jazyk aritmetiky $\mathcal{L}_\mathsf{A}$ so štandardnou interpretáciou symbolov pri ohodnotení premenných $e = \{x \mapsto 4, y \mapsto 9, \ldots\}$ termy:

$$+(S(S(S(0))), S(S(0))) \qquad + (x, \cdot(S(S(0)), y))$$

Splnenie formuly v štruktúre

Definícia

Nech $\mathcal{M} = (M, \square^{\mathcal{M}})$ je štruktúra, e je ohodnotenie premenných. Relácia *formula A je splnená v štruktúre $\mathcal{M}$ pri ohodnotení e* (skrátene $\mathcal{M} \models \phi[e]$) má nasledovnú rekurzívnu 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 $(t_1^{\mathcal{M}}[e], \ldots, t_n^{\mathcal{M}}[e]) \in P^{\mathcal{M}}$,
- $\mathcal{M} \models \neg A[e]$ vtt $\mathcal{M} \not\models A[e]$,
- $\mathcal{M} \models (A \land B)[e]$ vtt $\mathcal{M} \models A[e]$ a zároveň $\mathcal{M} \models B[e]$,
- $\mathcal{M} \models (A \lor B)[e]$ vtt $\mathcal{M} \models A[e]$ alebo $\mathcal{M} \models B[e]$,
- $\mathcal{M} \models (A \to B)[e]$ vtt $\mathcal{M} \not\models A[e]$ alebo $\mathcal{M} \models B[e]$,

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

Splnenie formuly v štruktúre

Príklad

Sú v štruktúre $\mathcal{N} = (\mathbb{N}, \square^{\mathcal{N}})$ pre jazyk aritmetiky $\mathcal{L}_{\mathsf{A}}$ so štandardnou interpretáciou symbolov pri ohodnotení premenných $e = \{x \mapsto 4, y \mapsto 9, \ldots\}$ splnené atómy:

$$+(S(S(S(0))), S(S(0))) = +(x, \cdot(S(S(0)), y))$$
$$+(S(S(S(0))), S(S(0))) < +(x, \cdot(S(S(0)), y))\,?$$

Príklad

V akých štruktúrach pre jazyk grafov $\mathcal{L}_{\mathsf{G}}$ je pri *každom* ohodnotení e splnená formula

$$V(x) \land V(y) \land E(x, y) \to E(y, x)\,?$$

Kvázitautológie a kvázitautologické vyplývanie

Definícia

Nech X je formula v jazyku $\mathcal{L}$.
Formulu X nazveme *kvázitautológiou* vtt X je splnená v každej štruktúre $\mathcal{M}$ pre $\mathcal{L}$ pri každom ohodnotení e.

Definícia

Nech X je formula v jazyku $\mathcal{L}$, nech T je množina formúl v jazyku $\mathcal{L}$.
Formula X *kvázitautologicky vyplýva z* T (skrátene $T \models X$) vtt pre každú štruktúru $\mathcal{M}$ pre $\mathcal{L}$ a každé ohodnotenie e platí, že ak je každá formula Y z T splnená v $\mathcal{M}$ pri e, tak aj X je splnená v $\mathcal{M}$ pri e.

Tvrdenie

Nech X je formula v jazyku $\mathcal{L}$. Potom X je kvázitautológiou vtt X kvázitautologicky vyplýva z prázdej množiny formúl ($\{\} \models X$).

Kvázitautologická splniteľnosť

Definícia

Nech T je množina formúl v jazyku $\mathcal{L}$.
Množina T *kvázitautologicky splniteľná* vtt
pre každú štruktúru $\mathcal{M}$ pre $\mathcal{L}$ a každé ohodnotenie e platí, že
ak je každá formula Y z T je splnená v $\mathcal{M}$ pri e.
T je *kvázitautologicky nesplniteľná* vtt nie je splniteľná.

Tvrdenie

Nech X je formula v jazyku $\mathcal{L}$, nech T je množina formúl v jazyku $\mathcal{L}$.
Formula X kvázitautologicky vyplýva z T vtt
$T \cup \{X\}$ je kvázitautologicky nesplniteľná.

Kvázitautológie vs. tautológie

Ako sa líšia kvázitautológie od tautológií?

Príklad

Formula

$$x \doteq y \land g(f(z,x)) \doteq y \land \neg P(x) \to \neg P(g(f(z,x))) \tag{1}$$

je kvázitautológia.

Je (1) tautológia? Vo výrokovej logike sa na atómy logiky s rovnosťou pozeráme ako na výrokové premenné. Formulu (1) teda vidíme ako

$$p \land q \land \neg r \to \neg s\,,$$

čo určite nie je tautológia.

Odlišnosť kvázitautológií (a kvázitautologického vyplývania) od tautológií (a výrokovologického vyplývania) spočíva *práve v zohľadnení vlastností rovnosti*.

Axiómy rovnosti

Definícia

Nech $\mathcal{L}$ je jazyk logiky s rovnosťou.
Axiómami rovnosti sú všetky formuly vytvorené podľa nasledujúcich schém pre všetky arity $n > 0$, všetky funkčné symboly f s aritou n, všetky predikátové symboly P s aritou n, všetky termy t_1, t_2, t_3, $\ldots$, t_n, s_1, $\ldots$, s_n:

- $t_1 \doteq t_1$ (*reflexívnosť*),
- $t_1 \doteq t_2 \to t_2 \doteq t_1$ (*symetria*),
- $t_1 \doteq t_2 \wedge t_2 \doteq t_3 \to t_1 \doteq t_3$ (*tranzitívnosť*),
- $t_1 \doteq s_1 \wedge \cdots \wedge t_n \doteq s_n \to f(t_1, \ldots, t_n) \doteq f(s_1, \ldots, s_n)$ (*substitúcia pre funkčné symboly*),
- $t_1 \doteq s_1 \wedge \cdots \wedge t_n \doteq s_n \wedge P(t_1, \ldots, t_n) \to P(s_1, \ldots, s_n)$ (*substitúcia pre predikátové symboly*),

Množinu axióm rovnosti označíme Eq.

Výrokovologické a kvázitautologické vyplývanie

Veta

Všetky axiómy rovnosti sú kvázitautológie.

Dohoda

Vzťah výrokovologického vyplývania budeme odteraz označovať symbolom $\models_{\mathrm{p}}$.
Keď sa na formuly v jazyku $\mathcal{L}$ pozeráme z hľadiska výrokovej logiky, chápeme všetky atómy $\mathcal{L}$ ako výrokové premenné.

Veta

Nech X je formula v jazyku $\mathcal{L}$, nech T je množina formúl v jazyku $\mathcal{L}$. Potom $T \models X$ vtt existuje konečná *množina axióm rovnosti $E \subset \mathrm{Eq}$ taká, že $T \cup E \models_{\mathrm{p}} X$.*

Výrokovologické a kvázitautologické vyplývanie

Príklad

Nájdime množinu axióm rovnosti $E \subset \mathrm{Eq}$, z ktorej výrokovologicky vyplýva kvázitautológia

$$x \doteq y \wedge g(f(z,x)) \doteq y \wedge \neg P(x) \rightarrow \neg P(g(f(z,x))) \tag{1}$$

Tablový kalkul pre logiku s rovnosťou

Definícia

Pravidlami tablového kalkulu pre logiku s rovnosťou sú pravidlá typu α a β pre výrokovú logiku spolu s pravidlami:

$$\frac{}{\mathbf{T}\, t_1 \doteq t_1} \quad \text{(Refl)} \qquad\qquad \frac{\mathbf{T}\, t_1 \doteq t_2}{\mathbf{T}\, t_2 \doteq t_1} \quad \text{(Sym)}$$

$$\frac{\mathbf{T}\, t_1 \doteq t_2 \quad \mathbf{T}\, t_2 \doteq t_3}{\mathbf{T}\, t_1 \doteq t_3} \qquad \text{(Trans)}$$

$$\frac{\mathbf{T}\, t_1 \doteq s_1 \quad \cdots \quad \mathbf{T}\, t_n \doteq s_n}{\mathbf{T}\, f(t_1, \ldots, t_n) \doteq f(s_1, \ldots, s_n)} \qquad \text{(Fsub)}$$

$$\frac{\mathbf{T}\, t_1 \doteq s_1 \quad \cdots \quad \mathbf{T}\, t_n \doteq s_n \quad \mathbf{T}\, P(t_1, \ldots, t_n)}{\mathbf{T}\, P(s_1, \ldots, s_n)} \qquad \text{(Psub)}$$

Tablový kalkul pre logiku s rovnosťou

Doplnenie definície tabla

Vetvu tabla pre list y môžeme rozšíriť o jeden nový list obsahujúci dôsledok niektorého pravidla pre rovnosť, ak sa na vetve π_y nachádzajú *všetky* jeho predpoklady.

Označené formuly definujeme podobne ako vo výrokovej logike.

Veta (Korektnosť a úplnosť tablového kalkulu pre logiku s rovnosťou)

Nech S^+ je množina označených formúl v jazyku $\mathcal{L}$.
Množina S^+ je nesplniteľná vtt existuje uzavreté tablo $\mathcal{T}$ je pre S^+.

Literatúra