1-AIN-625 Úvod do matematickej logiky pre programátorov
1-INF-450 Logika pre informatikov

Zimný semester 2012/13

2. prednáška

Ján Komara

Obsah 2. prednášky

Zopakovanie

Cieľ predmetu

- Vybudovať matematické základy deklaratívnych programovacích jazykov.

Deklaratívne programovanie

- *Univerzum* je množina prirodzených čísel $\mathrm{N} = \{0, 1, 2, 3, \dots\}$.
- *Dátové štruktúry* kódujeme do N v štýle jazyka LISP s pomocou vhodnej párovacej funkcie.
- *Programy* sú vlastnosti totálnych funkcií nad oborom N spĺňajúce určité vstupné podmienky.
- *Formálny systém* je druhorádová formalizácia aritmetiky.
- Pri výučbe používame programovací jazyk a špecifikačno-verifikačný systém CL (Clausal Language).

Zopakovanie

Teória deklaratívneho programovania

- Primitívne rekurzívne funkcie
  - Aritmetizácia dátových štruktúr (Gödelizácia).
  - Regulárne rekurzívne definície s mierou:

    $$f(\vec{x}) = \tau[f; \vec{x}].$$

    Podmienka regularity $\Gamma_{f(\vec{\rho})} \to \mu[\vec{\rho}] < \mu[\vec{x}]$ pre rekurzívne volanie $f(\vec{\rho})$ funkcie f v terme τ.
- Obecne rekurzívne funkcie
  - Regulárne rekurzívne definície do dobre založených relácií:
    - Ackermannova funkcia (1928),
    - univerzálna funkcia pre primitívne rekurzívne funkcie.
- Čiastočne rekurzívne funkcie
  - Kleeneho prvá veta o rekurzii (veta o pevnom bode).
  - Kleeneho veta o normálnej forme.
  - Churchova téza a algoritmicky nerozhodnuteľné problémy (problém zastavenia).

Zopakovanie

Primitívne rekurzívne funkcie

- Základné funkcie:
  - konštantná funkcia $\mathrm{Z}(x) = 0$,
  - funkcia nasledovníka $\mathrm{S}(x) = x + 1$,
  - identity (projekcie):

    $$\mathrm{I}_i^n(x_1, \ldots, x_n) = x_i$$

    pre každé $1 \leq i \leq n$.
- Kompozícia (skladanie) funkcií:

  $$f(x_1, \ldots, x_n) = h\big(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)\big).$$

- Primitívna rekurzia:

  $$\begin{aligned} f(0, y_1, \ldots, y_n) &= g(y_1, \ldots, y_n) \\ f\big(\mathrm{S}(x), y_1, \ldots, y_n\big) &= h\big(x, f(x, y_1, \ldots, y_n), y_1, \ldots, y_n\big). \end{aligned}$$

Zopakovanie

Primitívne rekurzívne funkcie

- Základné funkcie:
  - konštantná funkcia $\mathrm{Z}(x) = 0$,
  - funkcia nasledovníka $\mathrm{S}(x) = x + 1$,
  - identity (projekcie):

    $$\mathrm{I}_i^n(\vec{x}) = x_i$$

    pre každé $1 \leq i \leq n$.
- Kompozícia (skladanie) funkcií:

  $$f(\vec{x}) = h\big(g_1(\vec{x}), \ldots, g_m(\vec{x})\big).$$

- Primitívna rekurzia:

  $$\begin{aligned} f(0, \vec{y}) &= g(\vec{y}) \\ f\big(\mathrm{S}(x), \vec{y}\big) &= h\big(x, f(x, \vec{y}), \vec{y}\big). \end{aligned}$$

Zopakovanie

Primitívne rekurzívne odvodenia

$$h_1(x,z,y) = \mathsf{S}\,\mathsf{I}^3_2(x,z,y)$$

$$0 + y = y \qquad 0 + y = \mathsf{I}(y)$$

$$x + 1 + y = x + y + 1 \qquad \mathsf{S}(x) + y = h_1(x, x+y, y)$$

$$h_2(x,z,y) = \mathsf{I}^3_2(x,z,y) + \mathsf{I}^3_3(x,z,y)$$

$$0 \cdot y = 0 \qquad 0 \cdot y = \mathsf{Z}(y)$$

$$(x+1) \cdot y = x \cdot y + y \qquad \mathsf{S}(x) \cdot y = h_2(x, x \cdot y, y)$$

$$\mathsf{C}_1(x) = \mathsf{S}\,\mathsf{Z}(x)$$

$$h_3(y,z,x) = \mathsf{I}^3_3(y,z,x) \cdot \mathsf{I}^3_2(y,z,x)$$

$$f(0,x) = \mathsf{C}_1(x)$$

$$x^0 = 1 \qquad f\left(\mathsf{S}(y), x\right) = h_3\left(y, f(y,x), x\right)$$

$$x^{y+1} = x \cdot x^y \qquad x^y = f\left(I^2_2(x,y), I^2_1(x,y)\right)$$

Zopakovanie

Primitívne rekurzívne funkcie

- Základný vývoj primitívne rekurzívnych funkcií.
- Primitívne rekurzívne predikáty a ohraničená minimalizácia.
- Párovacia funkcia a aritmetizácia (Gödelizácia).
- Vnorená jednoduchá rekurzia:

$$\begin{aligned} f(0,y) &= g(y) \\ f(x+1,y) &= h\Big(x, f(x, s_1(x,y)), f(x, s_2(x,y,f(x,s_1(x,y)))), y\Big). \end{aligned}$$

- Regulárne rekurzívne definície s mierou:

$$f(\vec{x}) = \tau[f;\vec{x}].$$

  Podmienka regularity $\Gamma_{f(\vec{\rho})} \rightarrow \mu[\vec{\rho}] < \mu[\vec{x}]$ pre rekurzívne volanie $f(\vec{\rho})$ funkcie f v terme τ.

Univerzálna funkcia pre primitívne rekurzívne funkcie

Definícia

Vravíme, že $(n+1)$-árna funkcia U je univerzálnou pre triedu n-árnych p.r. funkcií, ak sú splnené tieto podmienky:

- Pre každú n-árnu p.r. funkciu f existuje číslo e také, že pre každú n-ticu čísel $x_1, \ldots, x_n$ platí rovnosť

$$U(e, x_1, \ldots, x_n) = f(x_1, \ldots, x_n).$$

- Pre každé číslo e je n-árna funkcia f definovaná vzťahom

$$f(x_1, \ldots, x_n) = U(e, x_1, \ldots, x_n)$$

tiež primitívne rekurzívna.

Univerzálna funkcia pre primitívne rekurzívne funkcie

Veta

Žiadna univerzálna funkcia pre triedu n-árnych p.r. funkcií nie je primitívne rekurzívna.

Dôkaz sporom pre $n = 1$

Predpokladajme, že existuje p.r. funkcia U, ktorá je univerzálna pre triedu unárnych p.r. funkcií. Potom funkcia f definovaná vzťahom

$$f(x) = U(x, x) + 1 \tag{1}$$

je primitívne rekurzívna. Existuje číslo e také, že pre každé číslo x

$$U(e, x) = f(x). \tag{2}$$

Postupnými úpravami teraz dostaneme

$$f(e) \stackrel{(1)}{=} U(e, e) + 1 \stackrel{(2)}{=} f(e) + 1.$$

Spor.

Univerzálna funkcia pre primitívne rekurzívne funkcie

Aritmetizácia karteziánskeho súčinu

Cantorova párovacia funkcia (modifikovaná verzia)

$\langle x, y \rangle$	0	1	2	3	4	5	6	$\cdots$
0	1	2	4	7	11	16	22	$\cdots$
1	3	5	8	12	17	23	30	$\cdots$
2	6	9	13	18	24	31	39	$\cdots$
3	10	14	19	25	32	40	49	$\cdots$
4	15	20	26	33	41	50	60	$\cdots$
5	21	27	34	42	51	61	72	$\cdots$
6	28	35	43	52	62	73	85	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

$$\langle x, y \rangle = \sum_{i=0}^{x+y} i + 1 + x.$$

Vlastnosti párovacej funkcie

Modifikovaná verzia Cantorovej párovacej funkcie má tieto základné vlastnosti:

$$\langle x_1, x_2 \rangle = \langle y_1, y_2 \rangle \rightarrow x_1 = y_1 \wedge x_2 = y_2$$
$$x < \langle x, y \rangle \wedge y < \langle x, y \rangle$$
$$x = 0 \vee \exists y \exists z \, x = \langle y, z \rangle.$$

Projekcie

Unárne projekcie π_1 a π_2 spĺňajú tieto identity:

$$\pi_1 \langle x, y \rangle = x \qquad \pi_2 \langle x, y \rangle = y \qquad \pi_1(0) = 0 = \pi_2(0).$$

Univerzálna funkcia pre primitívne rekurzívne funkcie

Aritmetizácia karteziánskeho súčinu

Notácia

Pre $n \geq 3$ zapisujeme $\big\langle x_1, \langle x_2, \ldots, x_n \rangle \big\rangle$ skrátene $\langle x_1, x_2, \ldots, x_n \rangle$.

Aritmetizácia karteziánskeho súčinu

- Kódom n-tice $(x_1, \ldots, x_n) \in \mathrm{N}^n$ je číslo
$$\langle x_1, \ldots, x_n \rangle \in \mathrm{N}.$$
- Zobecnená projekcia $[x]_i^n$ operuje na kódoch n-tíc:
$$[\langle x_1, \ldots, x_n \rangle]_i^n = x_i \qquad \text{pre } 1 \leq i \leq n.$$

  Definícia:
$$[x]_i^n = \textbf{if } i \neq n \textbf{ then } \pi_1 \pi_2^{i \dot{-} 1}(x) \textbf{ else } \pi_2^{n \dot{-} 1}(x).$$

Univerzálna funkcia pre primitívne rekurzívne funkcie

Aritmetizácia primitívne rekurzívnych odvodení

Príklad

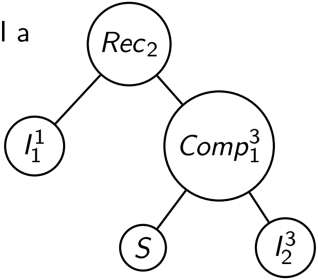
Primitívne rekurzívne odvodenie operácie sčítania

$$h(x,z,y) = \mathsf{S}\,\mathsf{I}^3_2(x,z,y)$$

$$\begin{aligned} 0 + y &= y & \qquad 0 + y &= \mathsf{I}(y) \\ x + 1 + y &= x + y + 1 & \qquad \mathsf{S}(x) + y &= h(x, x+y, y). \end{aligned}$$

Primitívne rekurzívny funkčný symbol a jeho syntaktický strom:

$$Rec_2(I^1_1, Comp^3_1(S, I^3_2))$$



Primitívne rekurzívne funkčné symboly

Trieda PR^n pozostáva z n-árnych p.r. funkčných symbolov:

- $Z \in \mathrm{PR}^1$, $S \in \mathrm{PR}^1$ a $I_i^n \in \mathrm{PR}^n$ pre $1 \leq i \leq n$.
- Ak $h \in \mathrm{PR}^m$ a $g_1, \ldots, g_m \in \mathrm{PR}^n$, potom
$$Comp_m^n(h, g_1, \ldots, g_m) \in \mathrm{PR}^n.$$
- Ak $g \in \mathrm{PR}^n$ a $h \in \mathrm{PR}^{n+2}$, potom
$$Rec_{n+1}(g, h) \in \mathrm{PR}^{n+1}.$$

Ich zjednotenie je množina všetkých p.r. funkčných symbolov

$$\mathrm{PR} = \bigcup_{n \geq 1} \mathrm{PR}^n.$$

Interpretácia primitívne rekurzívnych funkčných symbolov

Symbol $f \in \mathrm{PR}^n$ interpretujeme ako n-árnu funkciu $f^{\mathcal{N}}$ nad $\mathbb{N}$:

- $Z^{\mathcal{N}}$ je konštantná funkcia $\mathrm{Z}(x) = 0$.
- $S^{\mathcal{N}}$ je funkcia nasledovníka $\mathrm{S}(x) = x + 1$.
- $(I_i^n)^{\mathcal{N}}$ je identita $\mathrm{I}_i^n(\vec{x}) = x_i$.
- $\big(Comp_m^n(h, g_1, \dots, g_m)\big)^{\mathcal{N}}$ je funkcia definovaná kompozíciou

$$\big(Comp_m^n(h, g_1, \dots, g_m)\big)^{\mathcal{N}}(\vec{x}) = h^{\mathcal{N}}\big(g_1^{\mathcal{N}}(\vec{x}), \dots, g_m^{\mathcal{N}}(\vec{x})\big).$$

- $\big(Rec_n(g, h)\big)^{\mathcal{N}}$ je funkcia definovaná primitívnou rekurziou

$$\begin{aligned}\big(Rec_n(g, h)\big)^{\mathcal{N}}(0, \vec{y}) &= g^{\mathcal{N}}(\vec{y}) \\ \big(Rec_n(g, h)\big)^{\mathcal{N}}(x + 1, \vec{y}) &= h^{\mathcal{N}}\big(x, \big(Rec_n(g, h)\big)^{\mathcal{N}}(x, \vec{y}), \vec{y}\big).\end{aligned}$$

Aritmetizácia primitívne rekurzívnych funkčných symbolov

Pomocou párových konštruktorov z rôznymi rozlišovacími položkami:

$$\begin{aligned}
\boldsymbol{Z} &= \langle 1, 0 \rangle && \text{(konštantná funkcia)} \\
\boldsymbol{S} &= \langle 2, 0 \rangle && \text{(funkcia nasledovníka)} \\
\boldsymbol{I}_i^n &= \langle 3, n, i \rangle && \text{(identity)} \\
\boldsymbol{\langle} g \boldsymbol{,} gs \boldsymbol{\rangle} &= \langle 4, g, gs \rangle && \text{(kontrakcia)} \\
\boldsymbol{Comp}_m^n(h, gs) &= \langle 5, n, m, h, gs \rangle && \text{(kompozícia)} \\
\boldsymbol{Rec}_n(g, h) &= \langle 6, n, g, h \rangle. && \text{(primitívna rekurzia)}
\end{aligned}$$

Pre konštruktor $\boldsymbol{\langle} g \boldsymbol{,} gs \boldsymbol{\rangle}$ používame podobné notačné konvencie ako pre párovaciu funkciu $\langle x, y \rangle$.

Aritmetizácia primitívne rekurzívnych funkčných symbolov

Číslo $\ulcorner f \urcorner \in \mathrm{N}$ je kódom p.r. funkčného symbolu $f \in \mathrm{PR}$:

$$\begin{aligned}
\ulcorner Z \urcorner &= \boldsymbol{Z} \\
\ulcorner S \urcorner &= \boldsymbol{S} \\
\ulcorner I_i^n \urcorner &= \boldsymbol{I}_i^n \\
\ulcorner Comp_m^n(h, g_1, \ldots, g_m) \urcorner &= \boldsymbol{Comp}_m^n\big(\ulcorner h \urcorner, \langle \ulcorner g_1 \urcorner, \ldots, \ulcorner g_m \urcorner \rangle\big) \\
\ulcorner Rec_n(g, h) \urcorner &= \boldsymbol{Rec}_n(\ulcorner g \urcorner, \ulcorner h \urcorner).
\end{aligned}$$

Univerzálna funkcia pre primitívne rekurzívne funkcie

Aritmetizácia primitívne rekurzívnych odvodení

Príklad

Primitívne rekurzívne odvodenie operácie sčítania

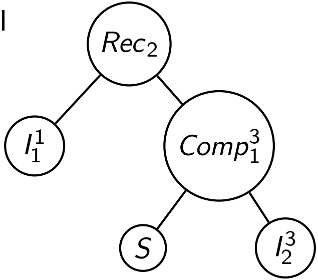
$$
\begin{aligned}
& & h(x,z,y) &= \mathsf{S}\,\mathsf{I}^3_2(x,z,y)\\
0+y &= y & 0+y &= \mathsf{I}(y)\\
x+1+y &= x+y+1 & \mathsf{S}(x)+y &= h(x,x+y,y).
\end{aligned}
$$

Primitívne rekurzívny funkčný symbol

$$Rec_2(I^1_1, Comp^3_1(S, I^3_2))$$

a jeho aritmetizácia

$$\boldsymbol{Rec}_2(\boldsymbol{I}^1_1, \boldsymbol{Comp}^3_1(\boldsymbol{S}, \boldsymbol{I}^3_2)).$$



Univerzálna funkcia pre primitívne rekurzívne funkcie

Špecifikácia

Interpreter programovacieho jazyka p.r. odvodení je binárna funkcia $e \bullet x$, ktorá má tieto dve základné vlastnosti:

- Pre každé $f \in \mathrm{PR}^n$ a $x_1, \ldots, x_n \in \mathrm{N}$ platí rovnosť

$$\ulcorner f \urcorner \bullet \langle x_1, \ldots, x_n \rangle = f^{\mathcal{N}}(x_1, \ldots, x_n).$$

- Pre každé číslo $e \in \mathrm{N}$, unárna funkcia f definovaná vzťahom

$$f(x) = e \bullet x$$

  je primitívne rekurzívna funkcia.

Implementácia

Diskriminácia podľa konštruktorov p.r. funkčných symbolov:

$$
\begin{array}{l}
e \bullet x = \textbf{case} \\
\qquad\qquad e = \boldsymbol{Z} \Rightarrow 0 \\
\qquad\qquad e = \boldsymbol{S} \Rightarrow x + 1 \\
\qquad\qquad e = \boldsymbol{I}_i^n \Rightarrow [x]_i^n \\
\qquad\qquad e = \langle g, gs \rangle \Rightarrow \langle g \bullet x, gs \bullet x \rangle \\
\qquad\qquad e = \boldsymbol{Comp}_m^n(h, gs) \Rightarrow h \bullet (gs \bullet x) \\
\qquad\qquad e = \boldsymbol{Rec}_n(g, h) \Rightarrow \\
\qquad\qquad\quad \textbf{case} \\
\qquad\qquad\qquad x = \langle 0, y \rangle \Rightarrow g \bullet y \\
\qquad\qquad\qquad x = \langle z + 1, y \rangle \Rightarrow h \bullet \langle z, \boldsymbol{Rec}_n(g, h) \bullet \langle z, y \rangle, y \rangle \\
\qquad\qquad\qquad \textbf{otherwise} \Rightarrow 0 \\
\qquad\qquad\quad \textbf{end} \\
\qquad\qquad \textbf{otherwise} \Rightarrow 0 \\
\qquad\quad \textbf{end}.
\end{array}
$$

Univerzálna funkcia pre primitívne rekurzívne funkcie

Interpreter programovacieho jazyka

Implementácia

Klauzálna forma rekurzívnej definície:

$$
\begin{aligned}
\boldsymbol{Z} \bullet x &= 0 \\
\boldsymbol{S} \bullet x &= x + 1 \\
\boldsymbol{I}_i^n \bullet x &= [x]_i^n \\
\langle g, gs \rangle \bullet x &= \langle g \bullet x, gs \bullet x \rangle \\
\boldsymbol{Comp}_m^n(h, gs) \bullet x &= h \bullet (gs \bullet x) \\
\boldsymbol{Rec}_n(g, h) \bullet \langle 0, y \rangle &= g \bullet y \\
\boldsymbol{Rec}_n(g, h) \bullet \langle x + 1, y \rangle &= h \bullet \langle x, \boldsymbol{Rec}_n(g, h) \bullet \langle x, y \rangle, y \rangle.
\end{aligned}
$$

Univerzálna funkcia pre primitívne rekurzívne funkcie

Interpreter programovacieho jazyka

Dobré usporiadanie

Lexikografické usporiadanie dvojíc prirodzených čísel

$$(a, b) >_{\mathrm{lex}} (c, d) \leftrightarrow a > c \lor a = c \land b > d.$$

Každá ostro klesajúca postupnosť je konečná

$$(a_1, b_1) >_{\mathrm{lex}} (a_2, b_2) >_{\mathrm{lex}} (a_3, b_3) >_{\mathrm{lex}} (a_4, b_4) >_{\mathrm{lex}} \cdots .$$

Transfinitná rekurzia

Podmienky regularity pre interpreter $e \bullet x$ sú triviálne splnené, napr.

$$\begin{aligned}
&\big(\boldsymbol{Rec}_n(g, h), \langle x + 1, y\rangle\big) >_{\mathrm{lex}} \big(\boldsymbol{Rec}_n(g, h), \langle x, y\rangle\big) \\
&\big(\boldsymbol{Rec}_n(g, h), \langle x + 1, y\rangle\big) >_{\mathrm{lex}} \big(h, \big\langle x, \boldsymbol{Rec}_n(g, h) \bullet \langle x, y\rangle, y\big\rangle\big).
\end{aligned}$$

Univerzálna funkcia pre primitívne rekurzívne funkcie

Primitívne rekurzívne indexy

Definícia

Prirodzené číslo e také, že

$$\forall x_1 \ldots \forall x_n\, f(x_1, \ldots, x_n) = e \bullet \langle x_1, \ldots, x_n \rangle,$$

sa nazýva primitívne rekurzívny index funkcie f.

Veta

Funkcia je primitívne rekurzívna práve vtedy, keď má primitívne rekurzívny index.

Definícia

Predikát $Prf(n, e)$ platí, ak číslo e je *dobre vytvorený* primitívne rekurzívny index nejakej n-árnej p.r. funkcie, t.j. $e = \ulcorner f \urcorner$ pre nejaké $f \in \mathrm{PR}^n$.

Záver

1. cvičenie

- Výsledky s komentárom nájdete na webe.

2. cvičenie

- Začína hneď po prednáške v miestnosti F1-248.
- Pracujte vo dvojiciach.
- Úlohy odovzdať najneskôr do 12:00 v pondelok budúci týždeň.

3. prednáška

- Základný vývoj primitívne rekurzívnych funkcií.
- Primitívne rekurzívne predikáty a ohraničená minimalizácia.