

1-INF-450 Logika pre informatikov
1-AIN-625 Úvod do matematickej logiky pre
programátorov
Zimný semester 2014/15
2. prednáška

Ján Komara

Obsah 2. prednášky

Zopakovanie

Univerzálna funkcia pre primitívne rekurzívne funkcie

- Aritmetizácia karteziánskeho súčinu

- Aritmetizácia primitívne rekurzívnych odvození

- Interpreter programovacieho jazyka

- Primitívne rekurzívne indexy

Záver

Zopakovanie

Cieľ predmetu

- ▶ Vybudovať matematické základy deklaratívnych programovacích jazykov.

Deklaratívne programovanie

- ▶ *Univerzum* je množina prirodzených čísel $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.
- ▶ *Dátové štruktúry* kódujeme do \mathbb{N} v štýle jazyka Lisp s pomocou vhodnej párovacej funkcie.
- ▶ *Programy* sú vlastnosti totálnych funkcií nad oborom \mathbb{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.
 - ▶ 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 .

- ▶ Obecné 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 $Z(x) = 0$,
- funkcia nasledovníka $S(x) = x + 1$,
- identity (projekcie):

$$I_i^n(x_1, \dots, x_n) = x_i$$

pre každé $1 \leq i \leq n$.

► Kompozícia (skladanie) funkcií:

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

► Primitívna rekurzia:

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

Zopakovanie

Primitívne rekurzívne odvodenia

$$0 + y = y$$

$$x + 1 + y = x + y + 1$$

$$0 \cdot y = 0$$

$$(x + 1) \cdot y = x \cdot y + y$$

$$x^0 = 1$$

$$x^{y+1} = x \cdot x^y$$

$$h(x, z, y) = S I_2^3(x, z, y)$$

$$0 + y = I(y)$$

$$S(x) + y = h(x, x + y, y)$$

$$h_2(x, z, y) = I_2^3(x, z, y) + I_3^3(x, z, y)$$

$$0 \cdot y = Z(y)$$

$$S(x) \cdot y = h_2(x, x \cdot y, y)$$

$$C_1(x) = S Z(x)$$

$$h_3(y, z, x) = I_3^3(y, z, x) \cdot I_2^3(y, z, x)$$

$$f(0, x) = C_1(x)$$

$$f(S(y), x) = h_3(y, f(y, x), x)$$

$$x^y = f(I_2^2(x, y), I_1^2(x, y))$$

Zopakovanie

Primitívne rekurzívne funkcie

- ▶ Základný vývoj primitívne rekurzívnych funkcií.
- ▶ Primitívne rekurzívne predikáty a ohraničená minimalizácia.
- ▶ Párovacia funkcia a aritmetizácia dátových štruktúr.
- ▶ Vnorená jednoduchá rekurzia:

$$f(0, y) = g(y)$$

$$f(x + 1, y) = h\left(x, f(x, s_1(x, y)), f(x, s_2(x, y, f(x, s_1(x, y)))), y\right).$$

- ▶ 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 primitívne rekurzívnych funkcií, ak sú splnené tieto podmienky:

- ▶ Pre každú n -árnu primitívne rekurzívnu funkciu f existuje číslo e také, že pre každú n -ticu čísel x_1, \dots, x_n platí rovnosť

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

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

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

tiež primitívne rekurzívna.

Univerzálna funkcia pre primitívne rekurzívne funkcie

Veta

Žiadna univerzálna funkcia pre triedu n -árnych primitívne rekurzívnych 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

$$f(x) = U(x, x) + 1 \quad (1)$$

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

$$U(e, x) = f(x). \quad (2)$$

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

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

Univerzálna funkcia pre primitívne rekurzívne funkcie

Aritmetizácia karteziánskeho súčinu

Vlastnosti párovacej funkcie

Modifikovaná verzia Cantorovej párovacej funkcie má tieto základné vlastnosti:

$$\begin{aligned}\langle x_1, x_2 \rangle = \langle y_1, y_2 \rangle &\rightarrow x_1 = y_1 \wedge x_2 = y_2 \\ x < \langle x, y \rangle &\wedge y < \langle x, y \rangle \\ x = 0 &\vee \exists y \exists z x = \langle y, z \rangle.\end{aligned}$$

Projekcie

Unárne projekcie π_1 a π_2 spĺňajú tieto identity:

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

Univerzálna funkcia pre primitívne rekurzívne funkcie

Aritmetizácia karteziánskeho súčinu

Notácia

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

Aritmetizácia karteziánskeho súčinu

- ▶ Kódom n -tice $(x_1, \dots, x_n) \in \mathbb{N}^n$ je číslo

$$\langle x_1, \dots, x_n \rangle \in \mathbb{N}.$$

- ▶ Zobecnená projekcia $[x]_i^n$ operuje na kódoch n -tíc:

$$[\langle x_1, \dots, x_n \rangle]_i^n = x_i \quad \text{pre } 1 \leq i \leq n.$$

Definícia:

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

Univerzálna funkcia pre primitívne rekurzívne funkcie

Aritmetizácia primitívne rekurzívnych odvození

Príklad

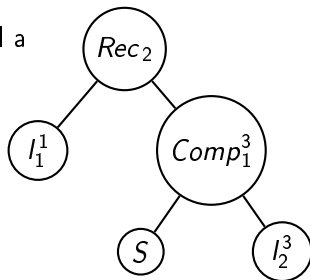
Primitívne rekurzívne odvozenie operácie sčítania

$$\begin{aligned}0 + y &= y \\ x + 1 + y &= x + y + 1\end{aligned}$$

$$\begin{aligned}h(x, z, y) &= S I_2^3(x, z, y) \\ 0 + y &= I(y) \\ S(x) + y &= h(x, x + y, y).\end{aligned}$$

Primitívne rekurzívny funkčný symbol a jeho syntaktický strom:

$$Rec_2(I_1^1, Comp_1^3(S, I_2^3))$$



Univerzálna funkcia pre primitívne rekurzívne funkcie

Aritmetizácia primitívne rekurzívnych odvození

Primitívne rekurzívne funkčné symboly

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

- ▶ $Z \in PR^1$, $S \in PR^1$ a $I_i^n \in PR^n$ pre $1 \leq i \leq n$.
- ▶ Ak $h \in PR^m$ a $g_1, \dots, g_m \in PR^n$, potom

$$Comp_m^n(h, g_1, \dots, g_m) \in PR^n.$$

- ▶ Ak $g \in PR^n$ a $h \in PR^{n+2}$, potom

$$Rec_{n+1}(g, h) \in PR^{n+1}.$$

Ich zjednotenie je množina všetkých p.r. funkčných symbolov

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

Univerzálna funkcia pre primitívne rekurzívne funkcie

Aritmetizácia primitívne rekurzívnych odvození

Interpretácia primitívne rekurzívnych funkčných symbolov

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

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

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

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

$$(Rec_n(g, h))^{\mathcal{N}}(0, \vec{y}) = g^{\mathcal{N}}(\vec{y})$$

$$(Rec_n(g, h))^{\mathcal{N}}(x + 1, \vec{y}) = h^{\mathcal{N}}(x, (Rec_n(g, h))^{\mathcal{N}}(x, \vec{y}), \vec{y}).$$

Univerzálna funkcia pre primitívne rekurzívne funkcie

Aritmetizácia primitívne rekurzívnych odvození

Aritmetizácia primitívne rekurzívnych funkčných symbolov

Pomocou párových konštruktorov z rôznymi rozlišovacími položkami:

$$\mathbf{Z} = \langle 1, 0 \rangle \quad (\text{konštantná funkcia})$$

$$\mathbf{S} = \langle 2, 0 \rangle \quad (\text{funkcia nasledovníka})$$

$$\mathbf{I}_i^n = \langle 3, n, i \rangle \quad (\text{identity})$$

$$\langle g, gs \rangle = \langle 4, g, gs \rangle \quad (\text{kontrakcia})$$

$$\mathbf{Comp}_m^n(h, gs) = \langle 5, n, m, h, gs \rangle \quad (\text{kompozícia})$$

$$\mathbf{Rec}_n(g, h) = \langle 6, n, g, h \rangle. \quad (\text{primitívna rekurzia})$$

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

Univerzálna funkcia pre primitívne rekurzívne funkcie

Aritmetizácia primitívne rekurzívnych odvození

Aritmetizácia primitívne rekurzívnych funkčných symbolov

Číslo $\ulcorner f \urcorner \in \mathbb{N}$ označuje kód (aritmetizáciu) primitívne rekurzívneho funkčného symbolu $f \in \text{PR}$. Induktívna definícia:

$$\ulcorner Z \urcorner = \mathbf{Z}$$

$$\ulcorner S \urcorner = \mathbf{S}$$

$$\ulcorner I_i^n \urcorner = \mathbf{I}_i^n$$

$$\ulcorner \text{Comp}_m^n(h, g_1, \dots, g_m) \urcorner = \mathbf{Comp}_m^n(\ulcorner h \urcorner, \langle \ulcorner g_1 \urcorner, \dots, \ulcorner g_m \urcorner \rangle)$$

$$\ulcorner \text{Rec}_n(g, h) \urcorner = \mathbf{Rec}_n(\ulcorner g \urcorner, \ulcorner h \urcorner).$$

Univerzálna funkcia pre primitívne rekurzívne funkcie

Aritmetizácia primitívne rekurzívnych odvození

Príklad

Primitívne rekurzívne odvozenie operácie sčítania

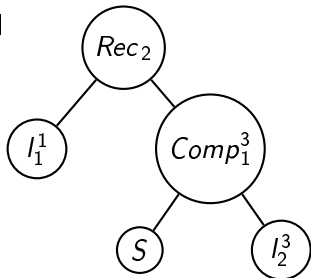
$$\begin{array}{ll} 0 + y = y & h(x, z, y) = S I_2^3(x, z, y) \\ x + 1 + y = x + y + 1 & 0 + y = I(y) \\ & S(x) + y = h(x, x + y, y). \end{array}$$

Primitívne rekurzívny funkčný symbol

$$Rec_2(I_1^1, Comp_1^3(S, I_2^3))$$

a jeho aritmetizácia

$$Rec_2(I_1^1, Comp_1^3(S, I_2^3)).$$



Univerzálna funkcia pre primitívne rekurzívne funkcie

Interpreter programovacieho jazyka

Špecifikácia

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

- ▶ Pre každé $f \in PR^n$ a $x_1, \dots, x_n \in \mathbb{N}$ platí rovnosť

$$\lceil f \rceil \bullet \langle x_1, \dots, x_n \rangle = f^{\mathcal{N}}(x_1, \dots, x_n).$$

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

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

je primitívne rekurzívna funkcia.

Poznámka

Definícia univerzálnej funkcie U pre triedu n -árnych p.r. funkcií

$$U(e, x_1, \dots, x_n) = e \bullet \langle x_1, \dots, x_n \rangle.$$

Univerzálna funkcia pre primitívne rekurzívne funkcie

Interpreter programovacieho jazyka

Implementácia

Diskriminácia podľa konštruktorov p.r. funkčných symbolov:

$e \bullet x = \text{case}$

$$e = Z \Rightarrow 0$$

$$e = S \Rightarrow x + 1$$

$$e = I_i^n \Rightarrow [x]_i^n$$

$$e = \langle g, gs \rangle \Rightarrow \langle g \bullet x, gs \bullet x \rangle$$

$$e = \text{Comp}_m^n(h, gs) \Rightarrow h \bullet (gs \bullet x)$$

$$e = \text{Rec}_n(g, h) \Rightarrow$$

case

$$x = \langle 0, y \rangle \Rightarrow g \bullet y$$

$$x = \langle z + 1, y \rangle \Rightarrow h \bullet \langle z, \text{Rec}_n(g, h) \bullet \langle z, y \rangle, y \rangle$$

$$\text{otherwise} \Rightarrow 0$$

end

$$\text{otherwise} \Rightarrow 0$$

end.

Univerzálna funkcia pre primitívne rekurzívne funkcie

Interpreter programovacieho jazyka

Implementácia

Klauzálna forma rekurzívnej definície:

$$Z \bullet x = 0$$

$$S \bullet x = x + 1$$

$$I_i^n \bullet x = [x]_i^n$$

$$\langle g, gs \rangle \bullet x = \langle g \bullet x, gs \bullet x \rangle$$

$$Comp_m^n(h, gs) \bullet x = h \bullet (gs \bullet x)$$

$$Rec_n(g, h) \bullet \langle 0, y \rangle = g \bullet y$$

$$Rec_n(g, h) \bullet \langle x + 1, y \rangle = h \bullet \langle x, Rec_n(g, h) \bullet \langle x, y \rangle, y \rangle.$$

Univerzálna funkcia pre primitívne rekurzívne funkcie

Interpreter programovacieho jazyka

Dobré usporiadanie

Lexikografické usporiadanie dvojíc prirodzených čísel

$$(a, b) <_{\text{lex}} (c, d) \leftrightarrow a < c \vee a = c \wedge b < d.$$

Je to dobré usporiadanie: každá ostro klesajúca postupnosť

$$(a_1, b_1) >_{\text{lex}} (a_2, b_2) >_{\text{lex}} (a_3, b_3) >_{\text{lex}} (a_4, b_4) >_{\text{lex}} \dots$$

je konečná.

Transfinitná rekúzia

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

$$\begin{aligned} (\mathbf{Rec}_n(g, h), \langle x, y \rangle) &<_{\text{lex}} (\mathbf{Rec}_n(g, h), \langle x + 1, y \rangle) \\ (h, \langle x, \mathbf{Rec}_n(g, h) \bullet \langle x, y \rangle, y \rangle) &<_{\text{lex}} (\mathbf{Rec}_n(g, h), \langle x + 1, y \rangle). \end{aligned}$$

Univerzálna funkcia pre primitívne rekurzívne funkcie

Primitívne rekurzívne indexy

Definícia

Prirodzené číslo e také, že

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

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 *dobře vytvorený* primitívne rekurzívny index nejakej n -árnej primitívne rekurzívnej funkcie, t.j. $e = \ulcorner f \urcorner$ pre nejaké $f \in PR^n$.

Záver

1. cvičenie

- ▶ Výsledky s komentárom nájdete na webe.

2. cvičenie

- ▶ Začína v stredu o 09:50 v miestnosti F1-248.
- ▶ Pracujte vo dvojiciach.
- ▶ Úlohy odovzdať najneskôr do 12:00 v pondelok budúci týždeň.

3. prednáška

- ▶ Základný vývoj primitívne rekurzívnych funkcií:
 - ▶ explicitné definície,
 - ▶ primitívne rekurzívne definície.