1-AIN-470 Špecifikácia a verifikácia programov

Letný semester 2019/20

7. prednáška

Ján Komara

Obsah 7. prednášky

Primitívna rekurzia

- Umocňovanie:

$$x^0 = 1 \qquad x^{y+1} = x \cdot x^y.$$

Rekurzia s mierou

- Fibonacciho postupnosť:

$$f_0 = 0 \qquad f_1 = 1 \qquad f_{n+2} = f_{n+1} + f_n.$$

- Euklidov algoritmus.

Obecná rekurzia

- Ackermannova funkcia (1928).
- Univerzálna funkcia pre primitívne rekurzívne funkcie.

Primitívne rekurzívne funkcie

Definícia triedy primitívne rekurzívnych funkcií

- 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:

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

Primitívne rekurzívne funkcie

Definícia triedy primitívne rekurzívnych funkcií

- 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:

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

Primitívne rekurzívne funkcie

Definícia

- Základné funkcie: $\mathsf{Z}(x) = 0$, $\mathsf{S}(x) = x + 1$, $\mathsf{I}^n_i(\vec{x}) = x_i$.
- Kompozícia funkcií: $f(\vec{x}) = h(g_1(\vec{x}), \ldots, g_m(\vec{x}))$.
- Primitívna rekurzia:

$$f(0, \vec{y}) = g(\vec{y}) \qquad f(\mathsf{S}(x), \vec{y}) = h(x, f(x, \vec{y}), \vec{y}).$$

Sčítanie

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

Primitívne rekurzívne funkcie

Definícia

- Základné funkcie: $\mathrm{Z}(x) = 0$, $\mathrm{S}(x) = x + 1$, $\mathrm{I}_i^n(\vec{x}) = x_i$.
- Kompozícia funkcií: $f(\vec{x}) = h(g_1(\vec{x}), \ldots, g_m(\vec{x}))$.
- Primitívna rekurzia:

$$f(0, \vec{y}) = g(\vec{y}) \qquad f(\mathrm{S}(x), \vec{y}) = h(x, f(x, \vec{y}), \vec{y}).$$

Násobenie

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

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

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

Primitívne rekurzívne funkcie

Definícia

- Základné funkcie: $\mathrm{Z}(x) = 0$, $\mathrm{S}(x) = x + 1$, $\mathrm{I}^n_i(\vec{x}) = x_i$.
- Kompozícia funkcií: $f(\vec{x}) = h(g_1(\vec{x}), \dots, g_m(\vec{x}))$.
- Primitívna rekurzia:

$$f(0, \vec{y}) = g(\vec{y}) \qquad f(\mathrm{S}(x), \vec{y}) = h(x, f(x, \vec{y}), \vec{y}).$$

Umocňovanie

$$\begin{aligned} \mathrm{C}_1(x) &= \mathrm{S}\,\mathrm{Z}(x) \\ h_3(y, z, x) &= \mathrm{I}^3_3(y, z, x) \cdot \mathrm{I}^3_2(y, z, x) \\ f(0, x) &= \mathrm{C}_1(x) \end{aligned}$$

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

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

Primitívne rekurzívne funkcie

Primitívne rekurzívne odvodenia

$$
\begin{aligned}
& & h(x,z,y) &= \mathsf{S}\,\mathsf{I}^3_2(x,z,y) \\
0+y &= y & 0+y &= \mathsf{I}(y) \\
x+1+y &= x+y+1 & \mathsf{S}(x)+y &= h(x,x+y,y) \\
& & h_2(x,z,y) &= \mathsf{I}^3_2(x,z,y)+\mathsf{I}^3_3(x,z,y) \\
0{\cdot}y &= 0 & 0{\cdot}y &= \mathsf{Z}(y) \\
(x+1){\cdot}y &= x{\cdot}y+y & \mathsf{S}(x){\cdot}y &= h_2(x,x{\cdot}y,y) \\
& & \mathsf{C}_1(x) &= \mathsf{S}\,\mathsf{Z}(x) \\
& & h_3(y,z,x) &= \mathsf{I}^3_3(y,z,x){\cdot}\,\mathsf{I}^3_2(y,z,x) \\
& & f(0,x) &= \mathsf{C}_1(x) \\
x^0 &= 1 & f\big(\mathsf{S}(y),x\big) &= h_3\big(y,f(y,x),x\big) \\
x^{y+1} &= x{\cdot}x^y & x^y &= f\big(\mathsf{I}^2_2(x,y),\mathsf{I}^2_1(x,y)\big)
\end{aligned}
$$

Primitívne rekurzívne funkcie

Primitívne rekurzívne funkcie a deklaratívne programovanie

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

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

- 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.

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 $x_1, \ldots, x_n$ 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 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

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

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 primitívne rekurzívnych odvodení

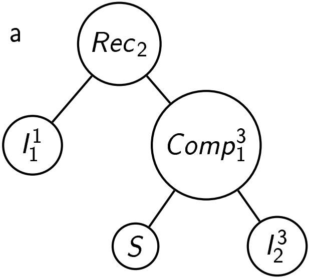
Príklad

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 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 $\mathrm{I}_i^n(\vec{x}) = x_i$.
- $\big(Comp_m^n(h, g_1, \ldots, g_m)\big)^{\mathcal{N}}$ je funkcia definovaná kompozíciou

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

- $\big(Rec_n(g, h)\big)^{\mathcal{N}}$ 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 $\ulcorner f \urcorner \in \mathrm{N}$ označuje kód (aritmetizáciu) primitívne rekurzívneho funkčného symbolu $f \in \mathrm{PR}$. Induktívna definícia:

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

Univerzálna funkcia pre primitívne rekurzívne funkcie

Aritmetizácia primitívne rekurzívnych odvodení

Príklad

Primitívne rekurzívne odvodenie operácie sčítania

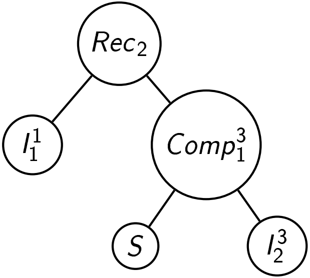
$$
\begin{aligned}
& & h(x,z,y) &= \mathrm{S}\,\mathrm{I}_2^3(x,z,y) \\
0 + y &= y & 0 + y &= \mathrm{I}(y) \\
x + 1 + y &= x + y + 1 & \mathrm{S}(x) + y &= h(x, x+y, y).
\end{aligned}
$$

Primitívne rekurzívny funkčný symbol

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

a jeho aritmetizácia

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



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.

Poznámka

Definícia univerzálnej funkcie U pre triedu n-árnych p.r. funkcií
$$U(e, x_1, \ldots, x_n) = e \bullet \langle x_1, \ldots, x_n \rangle.$$

Implementácia

Diskriminácia podľa konštruktorov p.r. funkčných symbolov:

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

Implementácia

Klauzálna forma rekurzívnej definície:

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

Univerzálna funkcia pre primitívne rekurzívne funkcie

Interpreter programovacieho jazyka

Dobré usporiadanie

Lexikografické usporiadanie dvojíc prirodzených čísel

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

Je to dobré usporiadanie: každá ostro klesajúca postupnosť

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

je konečná.

Transfinitná rekurzia

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

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

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 primitívne rekurzívnej funkcie, t.j. $e = \ulcorner f \urcorner$ pre nejaké $f \in \mathrm{PR}^n$.