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

Zimný semester 2012/13
3. prednáška

Ján Komara

Obsah 3. prednášky

Zopakovanie

Cieľ predmetu

- Vybudovať matematické základy deklaratívnych programovacích jazykov.

Stručná osnova predmetu

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

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

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

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

- 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.

Základný vývoj primitívne rekurzívnych funkcií

Veta

Primitívne rekurzívne funkcie sú uzavreté na operátor kompozície funkcií a primitívnej rekurzie.

Dôkaz.

Príklad:

$$
\begin{array}{rlrl}
 & & h(x,z,y) &= \mathsf{S}\,\mathsf{I}^3_2(x,z,y) \\
0+y &= y & 0+y &= \mathsf{I}(y) \\
x+1+y &= x+y+1 & \mathsf{S}(x)+y &= h(x,x+y,y) \\
 & & h_2(x,z,y) &= \mathsf{I}^3_2(x,z,y)+\mathsf{I}^3_3(x,z,y) \\
0\cdot y &= 0 & 0\cdot y &= \mathsf{Z}(y) \\
(x+1)\cdot y &= x\cdot y+y & \mathsf{S}(x)\cdot y &= h_2(x,x\cdot y,y).
\end{array}
$$

Základný vývoj primitívne rekurzívnych funkcií

Konštantné funkcie sú primitívne rekurzívne

- Unárne konštantné funkcie

$$\mathrm{C}_m(x) = m.$$

Primitívna rekurzívnosť C_m pomocou induktívneho argumentu

$$\mathrm{C}_0 = \mathrm{Z}$$
$$\mathrm{C}_{m+1}(x) = \mathrm{S}\,\mathrm{C}_m(x).$$

- Konštantné funkcie z ľubovolným počtom argumentov

$$\mathrm{C}^n_m(x_1, \ldots, x_n) = m.$$

Primitívnu rekurzívnosť C^n_m dostaneme z tohoto vyjadrenia

$$\mathrm{C}^n_m(x_1, \ldots, x_n) = \mathrm{C}_m\,\mathrm{I}^n_1(x_1, \ldots, x_n).$$

Základný vývoj primitívne rekurzívnych funkcií

Explicitné definície

Explicitné definície funkcií

Sú to definície v tvare

$$f(x_1, \ldots, x_n) = \tau[x_1, \ldots, x_n].$$

Veta

Primitívne rekurzívne funkcie sú uzavreté na explicitné definície.

Dôkaz.

Preklad definície induktívne podľa štruktúry termu τ. Napr.

$$f(x, y, z) = g_3\Big(x, g_2\big(z, g_1(x)\big), 2\Big).$$

Explicitné definície funkcií

Sú to definície v tvare

$$f(x_1, \ldots, x_n) = \tau[x_1, \ldots, x_n].$$

Veta

Primitívne rekurzívne funkcie sú uzavreté na explicitné definície.

Dôkaz.

Preklad definície induktívne podľa štruktúry termu τ. Napr.

$$\begin{aligned} h_1(x,y,z) &= g_1\, \mathrm{I}_1^3(x,y,z) \\ h_2(x,y,z) &= g_2\big(\mathrm{I}_3^3(x,y,z), h_1(x,y,z)\big) \\ f(x,y,z) &= g_3\big(\mathrm{I}_1^3(x,y,z), h_2(x,y,z), \mathrm{C}_2^3(x,y,z)\big). \end{aligned}$$

Primitívne rekurzívne definície

Sú to definície v tvare

$$f(\vec{y},0,\vec{z}) = \rho[\vec{y},\vec{z}]$$
$$f(\vec{y},x+1,\vec{z}) = \tau[\vec{y},x,f(\vec{y},x,\vec{z}),\vec{z}].$$

Špeciálne prípady:

- Iterácia unárnej funkcie

$$f^0(x) = x$$
$$f^{n+1}(x) = f\,f^n(x).$$

- Explicitná definícia s monadickou diskrimináciou

$$f(\vec{y},0,\vec{z}) = \rho[\vec{y},\vec{z}]$$
$$f(\vec{y},x+1,\vec{z}) = \tau[\vec{y},x,\vec{z}].$$

Základný vývoj primitívne rekurzívnych funkcií

Primitívne rekurzívne definície

Lema

Primitívne rekurzívne funkcie sú uzavreté na primitívne rekurzívne definície s aspoň jedným parametrom.

Dôkaz.

Primitívne rekurzívna definícia s aspoň jedným parametrom $\vec{y}, \vec{z}$:

$$f(\vec{y}, 0, \vec{z}) = \rho[\vec{y}, \vec{z}] \qquad f(\vec{y}, x+1, \vec{z}) = \tau[\vec{y}, x, f(\vec{y}, x, \vec{z}), \vec{z}].$$

Primitívna rekurzívnosť funkcie f plynie z tohoto vyjadrenia

$$\begin{aligned}
g(\vec{y}, \vec{z}) &= \rho[\vec{y}, \vec{z}] \\
h(x, a, \vec{y}, \vec{z}) &= \tau[\vec{y}, x, a, \vec{z}] \\
f_1(0, \vec{y}, \vec{z}) &= g(\vec{y}, \vec{z}) \\
f_1(\mathrm{S}(x), \vec{y}, \vec{z}) &= h(x, f_1(x, \vec{y}, \vec{z}), \vec{y}, \vec{z}) \\
f(\vec{y}, x, \vec{z}) &= f_1(x, \vec{y}, \vec{z}).
\end{aligned}$$

Lema

Primitívne rekurzívne funkcie sú uzavreté na bezparametrické primitívne rekurzívne definície.

Dôkaz.

Bezparametrická primitívne rekurzívna definícia unárnej funkcie:

$$\begin{aligned} f(0) &= \rho \\ f(x+1) &= \tau[x, f(x)]. \end{aligned}$$

Primitívna rekurzívnosť funkcie f plynie podľa predošlej lemy z tohoto vyjadrenia

$$\begin{aligned} f_1(0, w) &= \rho \\ f_1(x+1, w) &= \tau[x, f_1(x, w)] \\ f(x) &= f_1(x, 0). \end{aligned}$$

Veta

Primitívne rekurzívne funkcie sú uzavreté na primitívne rekurzívne definície.

Dôsledok

Primitívne rekurzívne funkcie sú uzavreté na operátor iterácie unárnych funkcií:

$$f^0(x) = x \qquad\qquad f^{n+1}(x) = f\, f^n(x).$$

Dôsledok

Primitívne rekurzívne funkcie sú uzavreté na explicitné definície funkcií s monadickou diskrimináciou:

$$f(\vec{y}, 0, \vec{z}) = \rho[\vec{y}, \vec{z}] \qquad\qquad f(\vec{y}, x+1, \vec{z}) = \tau[\vec{y}, x, \vec{z}].$$

Príklady primitívne rekurzívnych funkcií

Násobenie

$$0 \cdot y = 0 \qquad (x+1) \cdot y = x \cdot y + y.$$

Umocňovanie

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

Sumačná funkcia

$$\sum_{i=0}^{0} i = 0 \qquad \sum_{i=0}^{n+1} i = \sum_{i=0}^{n} i + n + 1.$$

Modifikované odčítanie

Definícia

$$x \dot{-} y = \begin{cases} x - y & \text{ak } x \geq y, \\ 0 & \text{ak } x \leq y. \end{cases}$$

Príklady primitívne rekurzívnych funkcií

Funkcia predchodcu

$$0 \dot{-} 1 = 0 \qquad x + 1 \dot{-} 1 = x.$$

Modifikované odčítanie

$$x \dot{-} 0 = x \qquad x \dot{-} (y + 1) = x \dot{-} y \dot{-} 1.$$

Primitívne rekurzívne predikáty a ohraničená minimalizácia

Charakteristická funkcia predikátu

Charakteristická funkcia n-árneho predikátu P je n-árna funkcia P_* definovaná predpisom

$$P_*(x_1, \ldots, x_n) = \begin{cases} 1 & \text{ak platí } P(x_1, \ldots, x_n), \\ 0 & \text{ak neplatí } P(x_1, \ldots, x_n). \end{cases}$$

Notačná konvencia $x \; P_* \; y$ pre binárne predikáty s infixovou notáciou. Napr. $x =_* y$, $x \leq_* y$.

Primitívne rekurzívne predikáty

Predikát je primitívne rekurzívny, ak jeho charakteristická funkcia je primitívne rekurzívna funkcia.

Primitívne rekurzívne predikáty a ohraničená minimalizácia

Jazyk formúl

Tvrdenia tvoríme z atomických formúl pomocou logických spojok a kvantifikátorov:

$\neg\varphi$	(negácia)
$\varphi \land \psi$	(konjunkcia)
$\varphi \lor \psi$	(disjunkcia)
$\varphi \to \psi$	(implikácia)
$\varphi \leftrightarrow \psi$	(ekvivalencia)
$\forall x \varphi$	(univerzálny kvantifikátor)
$\exists x \varphi$	(existenčný kvantifikátor)
$\forall x \leq \tau\, \varphi \equiv \forall x (x \leq \tau \to \varphi)$	(ohraničený kvantifikátor)
$\exists x \leq \tau\, \varphi \equiv \exists x (x \leq \tau \land \varphi)$	(ohraničený kvantifikátor)

Ohraničená formula obsahuje len ohraničené kvantifikátory.

Primitívne rekurzívne predikáty a ohraničená minimalizácia

Notačné konvencie pri zápise formúl

Od najvyššej priority k najmenšej:

- kvantifikátory,
- negácia,
- konjunkcia,
- disjunkcia,
- implikácia a ekvivalencia.

Príklad

Zadanie formuly v úplnej notácií

$$(\varphi_1 \rightarrow (\varphi_2 \leftrightarrow ((\neg\varphi_3) \vee ((\exists x \varphi_4) \wedge \varphi_5)))).$$

Jej skrátený zápis

$$\varphi_1 \rightarrow \varphi_2 \leftrightarrow \neg\varphi_3 \vee \exists x \varphi_4 \wedge \varphi_5.$$

Primitívne rekurzívne predikáty a ohraničená minimalizácia

Explicitné definície predikátov

Sú to definície v tvare

$$P(x_1, \ldots, x_n) \leftrightarrow \varphi[x_1, \ldots, x_n].$$

Nás zaujíma hlavne prípad, keď φ je ohraničená formula.

Príklad

Explicitná definícia predikátu deliteľnosti

$$x \mid y \leftrightarrow \exists z\, y = x \cdot z.$$

Iná definícia tentokrát s ohraničenou formulou

$$x \mid y \leftrightarrow \exists z \leq y\; y = x \cdot z.$$

Primitívne rekurzívne predikáty a ohraničená minimalizácia

Ohraničená minimalizácia

Sú to definície v tvare (φ je ohraničená formula)

$$f(x_1, \ldots, x_n) = \begin{cases} \text{najmenšie číslo } y \leq \tau[x_1, \ldots, x_n] \text{ také, že platí} \\ \qquad\qquad \varphi[x_1, \ldots, x_n, y]; \\ 0, \text{ ak také číslo neexistuje.} \end{cases}$$

Skrátený zápis $f(\vec{x}) = \mu y \leq \tau[\vec{x}]\big[\varphi[\vec{x}, y]\big]$.

Príklad

Neúplný podiel

$$x \div y = q \leftrightarrow y = 0 \land q = 0 \lor y \neq 0 \land \exists r(x = q{\cdot}y + r \land r < y).$$

Iná definícia tentokrát ohraničenou minimalizáciou

$$x \div y = \mu q \leq x[x < (q+1){\cdot}y].$$

Primitívne rekurzívne predikáty a ohraničená minimalizácia

Diskriminačná funkcia je primitívne rekurzívna

Ternárna diskriminačná funkcia D je definovaná predpisom

$$\mathrm{D}(x, y, z) = v \leftrightarrow x \neq 0 \land v = y \lor x = 0 \land v = z.$$

Notačná konvencia

$$D(\tau_1, \tau_2, \tau_3) \equiv \textbf{if } \tau_1 \neq 0 \textbf{ then } \tau_2 \textbf{ else } \tau_3$$
$$D\big(P_*(\vec{\tau}_1), \tau_2, \tau_3\big) \equiv \textbf{if } P(\vec{\tau}_1) \textbf{ then } \tau_2 \textbf{ else } \tau_3.$$

Primitívna rekurzívnosť funkcie D plynie z tohoto vyjadrenia

$$\mathrm{D}(0, y, z) = z$$
$$\mathrm{D}(x + 1, y, z) = y.$$

Je to explicitná definícia s monadickou diskrimináciou.

Primitívne rekurzívne predikáty a ohraničená minimalizácia

Rovnosť je primitívne rekurzívny predikát

Pretože $x = y \leftrightarrow x \dot{-} y + (y \dot{-} x) = 0$, primitívna rekurzívnosť funkcie $x =_* y$ plynie z tohoto vyjadrenia

$$(x =_* y) = \mathrm{D}\big(x \dot{-} y + (y \dot{-} x), 0, 1\big).$$

Boolovské funkcie sú primitívne rekurzívne

Základné boolovské funkcie

$$\begin{aligned}(\neg_* x) = y &\leftrightarrow x \neq 0 \land y = 0 \lor x = 0 \land y = 1\\ (x \land_* y) = z &\leftrightarrow x \neq 0 \land y \neq 0 \land z = 1 \lor (x = 0 \lor y = 0) \land z = 0.\end{aligned}$$

Primitívna rekurzívnosť bool. funkcií plynie z tohoto vyjadrenia

$$\begin{aligned}(\neg_* x) &= \mathrm{D}(x, 0, 1)\\ (x \land_* y) &= \mathrm{D}\big(x, \mathrm{D}(y, 1, 0), 0\big).\end{aligned}$$

Primitívne rekurzívne predikáty a ohraničená minimalizácia

Operátor ohraničenej minimalizácie

Je to definícia v tvare

$$f(x, \vec{y}) = \mu z \leq x\, [g(z, \vec{y}) = 1].$$

Veta

Primitívne rekurzívne funkcie sú uzavreté na operátor ohraničenej minimalizácie.

Dôkaz.

Primitívna rekurzívnosť funkcie f plynie z tohoto vyjadrenia

$$f(0, \vec{y}) = 0$$

$$f(x+1, \vec{y}) = \begin{cases} f(x, \vec{y}) & \text{ak } g\big(f(x, \vec{y}), \vec{y}\big) = 1, \\ x+1 & \text{ak } g\big(f(x, \vec{y}), \vec{y}\big) \neq 1 \text{ a } g(x+1, \vec{y}) = 1, \\ 0 & \text{ináč.} \end{cases}$$

Primitívne rekurzívne predikáty a ohraničená minimalizácia

Veta

Primitívne rekurzívne predikáty sú uzavreté na explicitné definície predikátov s ohraničenými formulami.

Dôkaz.

Explicitná definícia predikátu s ohraničenou formulou:

$$P(x_1, \ldots, x_n) \leftrightarrow \varphi[x_1, \ldots, x_n].$$

Primitívna rekurzívnosť predikátu P_* plynie z tohoto vyjadrenia

$$P_*(x_1, \ldots, x_n) = \varphi_*[x_1, \ldots, x_n].$$

Tu φ_* je charakteristický term formuly φ:

$$(\varphi \to \varphi_* = 1) \land (\neg\varphi \to \varphi_* = 0).$$

Primitívne rekurzívne predikáty a ohraničená minimalizácia

Konštrukcia φ_* induktívne podľa štruktúry formuly φ:

$$\begin{aligned}
(\rho = \tau)_* &\equiv (\rho =_* \tau) \\
(R(\vec{\tau}))_* &\equiv R_*(\vec{\tau}) \\
(\neg\psi)_* &\equiv (\neg_* \psi_*) \\
(\psi \land \chi)_* &\equiv (\psi_* \land_* \chi_*) \\
(\exists y \le \tau\, \psi[y])_* &\equiv \psi_*\Big[\mu y \le \tau\big[\psi_*[y] = 1\big]\Big].
\end{aligned}$$

Primitívne rekurzívne predikáty a ohraničená minimalizácia

Veta

Primitívne rekurzívne funkcie sú uzavreté na definície funkcií ohraničenou minimalizáciou.

Dôkaz.

Definícia funkcie ohraničenou minimalizáciou:

$$f(\vec{x}) = \mu y \leq \tau[\vec{x}]\big[\varphi[\vec{x}, y]\big].$$

Primitívna rekurzívnosť funkcie f plynie z tohoto vyjadrenia

$$\begin{aligned} P(y, \vec{x}) &\leftrightarrow \varphi[\vec{x}, y] \\ g(z, \vec{x}) &= \mu y \leq z[P_*(y, \vec{x}) = 1] \\ f(\vec{x}) &= g(\tau[\vec{x}], \vec{x}). \end{aligned}$$

Záver

2. cvičenie

- Výsledky s komentárom nájdete na webe.

3. cvičenie

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

4. prednáška

- Párovacia funkcia a aritmetizácia dátových štruktúr (Gödelizácia).