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

Zimný semester 2012/13

12. prednáška

Ján Komara

Obsah 12. 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

Čiastočne rekurzívne funkcie

- Základné funkcie:
  - funkcia nasledovníka $\mathsf{S}(x) = x + 1$,
  - funkcia predchodcu $x \dot{-} 1$.
- Explicitné definície čiastočných funkcií:

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

- Rekurzívne definície čiastočných funkcií:

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

Funkcia je rekurzívna, ak je to totálna čiastočne rekurzívna funkcia.
Predikát je rekurzívny, ak taká je jeho charakteristická funkcia.

Zopakovanie

Veta

Trieda rekurzívnych funkcií je obecne rekurzívne uzavretá.

Dôsledok

- *Každá obecne rekurzívna funkcia je rekurzívna.*
- *Každý obecne rekurzívny predikát je rekurzívny.*
- *Trieda rekurzívnych funkcií je primitívne rekurzívne uzavretá.*
- *Rekurzívne predikáty sú uzavreté na explicitné definície predikátov s ohraničenými formulami.*
- *Rekurzívne funkcie sú uzavreté na definície funkcií ohraničenou minimalizáciou.*
- *Rekurzívne funkcie sú uzavreté na definície funkcií regulárnou minimalizáciou.*

Zopakovanie

Neohraničená minimalizácia

Sú to definície čiastočných funkcií v tvare

$$f(x_1, \ldots, x_n) \simeq \text{najmenšie číslo } y \text{ také, že platí } \varphi[x_1, \ldots, x_n, y],$$

kde φ je ohraničená formula. Skrátený zápis:

$$f(x_1, \ldots, x_n) \simeq \mu y \left[\varphi[x_1, \ldots, x_n, y]\right].$$

Regulárna minimalizácia:

$$f(\vec{x}) = \mu y \left[\varphi[\vec{x}, y]\right] \qquad \text{ak } \forall \vec{x} \exists y \varphi[\vec{x}, y],$$

je špeciálny prípad neohraničenej minimalizácie.

Veta

Trieda čiastočných rekurzívnych funkcií je uzavretá na definície čiastočných funkcií neohraničenou minimalizáciou.

Zopakovanie

Neohraničená minimalizácia

Sú to definície čiastočných funkcií v tvare

$$f(x_1, \ldots, x_n) \simeq y \leftrightarrow \varphi[x_1, \ldots, x_n, y] \wedge \forall z < y \, \neg\varphi[x_1, \ldots, x_n, z],$$

kde φ je ohraničená formula. Skrátený zápis:

$$f(x_1, \ldots, x_n) \simeq \mu y \left[\varphi[x_1, \ldots, x_n, y]\right].$$

Regulárna minimalizácia:

$$f(\vec{x}) = \mu y \left[\varphi[\vec{x}, y]\right] \qquad \text{ak } \forall \vec{x} \exists y \varphi[\vec{x}, y],$$

je špeciálny prípad neohraničenej minimalizácie.

Veta

Trieda čiastočných rekurzívnych funkcií je uzavretá na definície čiastočných funkcií neohraničenou minimalizáciou.

Zopakovanie

Veta o normálnej forme (Kleene)

Existuje unárna primitívne rekurzívna funkcia U *a pre každé* $n \geq 1$ *existuje* $(n+2)$*-árny primitívne rekurzívny predikát* T_n *taký, že pre každú* n*-árnu čiastočne rekurzívnu funkciu* f *existuje číslo* e *také, že pre všetky čísla* $x_1, \ldots, x_n$ *platí vzťah*

$$f(x_1, \ldots, x_n) \simeq \mathrm{U}\, \mu s[\mathrm{T}_n(e, x_1, \ldots, x_n, s)].$$

Idea dôkazu

Neformálny popis predikátu Kleeneho predikátu T_n a funkcie U:

- $\mathrm{T}_n(e, x_1, \ldots, x_n, s)$ platí práve vtedy, keď číslo e je kód nejakého programu a číslo s je kód výpočtu tohoto programu pre vstupy $x_1, \ldots, x_n$.
- Funkcia $\mathrm{U}(s)$ určí z kódu výpočtu výslednú hodnotu.

Zopakovanie

Čiastočne μ-rekurzívne funkcie

Je to najmenšia trieda čiastočných funkcií, ktorá obsahuje funkcie

$$\mathsf{Z}(x) = 0 \qquad \mathsf{S}(x) = x + 1 \qquad \mathsf{I}_i^n(\vec{x}) = x_i \quad \text{pre } 1 \leq i \leq n,$$

a je uzavretá na kompozíciu (skladanie) čiastočných funkcií:

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

primitívnu rekurziu čiastočných funkcií:

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

a minimalizáciu čiastočných funkcií:

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

Veta

Trieda čiastočne rekurzívnych funkcií je totožná s triedou čiastočne μ-rekurzívnych funkcií.

Zopakovanie

Čiastočne μ-rekurzívne funkcie

Je to najmenšia trieda čiastočných funkcií, ktorá obsahuje funkcie

$$\mathsf{Z}(x) = 0 \qquad \mathsf{S}(x) = x + 1 \qquad \mathsf{I}_i^n(\vec{x}) = x_i \quad \text{pre } 1 \leq i \leq n,$$

a je uzavretá na kompozíciu (skladanie) čiastočných funkcií:

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

primitívnu rekurziu čiastočných funkcií:

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

a minimalizáciu čiastočných funkcií:

$$f(\vec{x}) \simeq y \leftrightarrow g(y, \vec{x}) \simeq 1 \wedge \forall z < y\big(g(z, \vec{x})\downarrow \wedge g(z, \vec{x}) \not\simeq 1\big).$$

Veta

Trieda čiastočne rekurzívnych funkcií je totožná s triedou čiastočne μ-rekurzívnych funkcií.

Enumerácia čiastočne rekurzívnych funkcií

Rekurzívny index operácie sčítania

Regulárna rekurzívna definícia

$$x + y = \textbf{if } x \neq 0 \textbf{ then } \mathsf{S}\big(\mathsf{P}(x) + y\big) \textbf{ else } y.$$

Tu $\mathsf{P}(x) = x \dot{-} 1$. Rekurzívna definícia so silnou rovnosťou

$$x_1 + x_2 \simeq \mathsf{D}\Big(x_1, \mathsf{S}\big(\mathsf{P}(x_1) + x_2\big), x_2\Big).$$

Rekurzívny funkčný symbol

$$\lambda_2.\mathsf{D}\Big(x_1, \mathsf{S}\,\mathfrak{f}_2\big(\mathsf{P}(x_1), x_2\big), x_2\Big).$$

Jeho aritmetizácia

$$\ulcorner \lambda_2.\mathsf{D}\Big(x_1, \mathsf{S}\,\mathfrak{f}_2\big(\mathsf{P}(x_1), x_2\big), x_2\Big) \urcorner$$

je rekurzívny index operácie sčítania.

Enumerácia čiastočne rekurzívnych funkcií

Rekurzívny index operácie sčítania

Regulárna rekurzívna definícia

$$x + y = \textbf{if } x \neq 0 \textbf{ then } \mathsf{S}\big(\mathsf{P}(x) + y\big) \textbf{ else } y.$$

Tu $\mathsf{P}(x) = x \dot{-} 1$. Rekurzívna definícia so silnou rovnosťou

$$x_1 + x_2 \simeq \mathsf{D}\Big(x_1, \mathsf{S}\big(\mathsf{P}(x_1) + x_2\big), x_2\Big).$$

Rekurzívny funkčný symbol

$$\lambda_2.\mathsf{D}\Big(x_1, \mathsf{S}\,\mathfrak{f}_2\big(\mathsf{P}(x_1), x_2\big), x_2\Big).$$

Jeho aritmetizácia

$$\boldsymbol{\lambda_2.\, D}\Big(x_1, \boldsymbol{S}\big(\boldsymbol{f}_2[0] \bullet \boldsymbol{P}(x_1) \bullet x_2\big), x_2\Big)$$

je rekurzívny index operácie sčítania.

Enumerácia čiastočne rekurzívnych funkcií

Rekurzívné funkčné symboly

Nech $\tau[\mathfrak{f}_n; x_1, \ldots, x_n]$ je term v premenných $x_1, \ldots, x_n$ a n-árnej funkčnej premennej $\mathfrak{f}_n$. Potom rekurzívny funkčný symbol $\lambda_n.\tau$ interpretujeme ako čiastočnú funkciu f definovanú vzťahom

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

Interpretáciu rekurzívneho funkčného symbolu $\lambda_n.\tau$ označujeme tým istým menom $\lambda_n.\tau$.

Aritmetizácia rekurzívnych funkčných symbolov

Pomocou párových konštruktorov, napr.

$$\boldsymbol{x}_i = \langle 0, i\rangle \quad \boldsymbol{0} = \langle 1, 0\rangle \quad \boldsymbol{S}(t) = \langle 2, t\rangle \quad \boldsymbol{P}(t) = \langle 3, t\rangle$$
$$\boldsymbol{D}(t_1, t_2, t_3) = \langle 4, t_1, t_2, t_3\rangle \quad \ldots \quad \boldsymbol{f}_n = \langle 7, n\rangle \quad \boldsymbol{\lambda}_n\boldsymbol{.}\, t = \langle 8, n, t\rangle.$$

Číslo $\ulcorner \lambda_n.\tau \urcorner$ označuje kód rekurzívneho funkčného symbolu $\lambda_n.\tau$.

Enumerácia čiastočne rekurzívnych funkcií

Rekurzívne indexy

Symbolom $\varphi_e^{(n)}$ označujeme n-árnu čiastočne rekurzívnu funkciu definovanú predpisom

$$\varphi_e^{(n)} = \begin{cases} \lambda_n.\tau & \text{ak } e = \ulcorner \lambda_n.\tau \urcorner \text{ pre nejaké } \lambda_n.\tau, \\ \emptyset^{(n)} & \text{ináč.} \end{cases}$$

Ak $f = \varphi_e^{(n)}$ tak číslo e nazveme rekurzívnym indexom čiastočnej funkcie f. Čísla v tvare $\ulcorner \lambda_n.\tau \urcorner$ sú dobre vytvorené indexy.

Veta

Čiastočná funkcia je rekurzívna práve vtedy, keď má rekurzívny index.

Poznámka

Z dôkazu Kleeneho vety o normálnej forme vyplýva, že

$$\varphi_e^{(n)}(x_1, \ldots, x_n) \simeq \mathrm{U}\, \mu s[\mathrm{T}_n(e, x_1, \ldots, x_n, s)].$$

Enumerácia čiastočne rekurzívnych funkcií

Enumeračná čiastočná funkcia

Symbolom Ψ_n si označíme $(n+1)$-árnu čiastočnú funkciu definovanú predpisom

$$\Psi_n(e, x_1, \ldots, x_n) \simeq \varphi_e^{(n)}(x_1, \ldots, x_n).$$

Veta o enumerácií (Kleene)

Pre každé $n \geq 1$, čiastočná funkcia Ψ_n je čiastočne rekurzívna funkcia, ktorá enumeruje (z opakovaním) triedu n-árnych čiastočne rekurzívnych funkcií, t. j. postupnosť

$$\lambda x_1 \ldots x_n \,.\, \Psi_n(e, x_1, \ldots, x_n) \qquad \textit{pre } e = 0, 1, 2, \ldots$$

je enumerácia triedy n-árnych čiastočne rekurzívnych funkcií.

Enumerácia čiastočne rekurzívnych funkcií

Dôkaz vety o enumerácií

- Z vety charakterizujúcej rekurzívne indexy plynie, že nasledujúca postupnosť

$$\begin{array}{lccccc} & \lambda\vec{x}.\Psi_n(0,\vec{x}) & \lambda\vec{x}.\Psi_n(1,\vec{x}) & \lambda\vec{x}.\Psi_n(2,\vec{x}) & \dots \\ \text{t.j.} & \varphi_0^{(n)} & \varphi_1^{(n)} & \varphi_2^{(n)} & \dots \end{array}$$

  je enumerácia triedy n-árnych čiastočne rekurzívnych funkcií.

- Z dôkazu Kleeneho vety o normálnej forme vyplýva, že

$$\Psi_n(e,\vec{x}) \simeq \mathrm{U}\,\mu s[\mathrm{T}_n(e,\vec{x},s)].$$

  Rekurzívnosť čiastočnej funkcie Ψ_n plynie z tohoto vyjadrenia

$$f(e,\vec{x}) \simeq \mu s[\mathrm{T}_n(e,\vec{x},s)] \qquad \Psi_n(e,\vec{x}) \simeq \mathrm{U}\,f(e,\vec{x}).$$

Enumerácia čiastočne rekurzívnych funkcií

Enumeračná čiastočná funkcia je univerzálna (platí to aj naopak)

$(n+1)$-árna čiastočná funkcia Ψ_n spĺňa tieto dve podmienky:

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

$$\Psi_n(e, x_1, \ldots, x_n) \simeq f(x_1, \ldots, x_n).$$

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

$$f(x_1, \ldots, x_n) \simeq \Psi_n(e, x_1, \ldots, x_n)$$

  čiastočne rekurzívna.

Vravíme, že Ψ_n je univerzálnou pre triedu n-árnych čiastočne rekurzívnych funkcií.

Enumerácia čiastočne rekurzívnych funkcií

Zúplnenie unárnej enumeračnej čiastočnej funkcie nie je rekurzívna funkcia

Dôkaz sporom. Predpokladajme napr., že binárna funkcia f:

$$f(e,x) \simeq \begin{cases} \Psi_1(e,x) & \text{ak } \Psi_1(e,x)\downarrow \\ 0 & \text{ak } \Psi_1(e,x)\uparrow \end{cases} \tag{1}$$

je rekurzívna. Potom aj unárna funkcia g definovaná vzťahom

$$g(x) = f(x,x) + 1 \tag{2}$$

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

$$\Psi_1(e,x) \simeq g(x). \tag{3}$$

Odtiaľ $\Psi_1(e,e)\downarrow$. Postupnými úpravami odvodíme spor:

$$g(e) \overset{(2)}{=} f(e,e) + 1 \overset{(1)}{\simeq} \Psi_1(e,e) + 1 \overset{(3)}{\simeq} g(e) + 1.$$

Enumerácia čiastočne rekurzívnych funkcií

Zúplnenie enumeračnej čiastočnej funkcie nie je rekurzívna funkcia

Dôkaz sporom. Predpokladajme napr., že $(n+1)$-árna funkcia f:

$$f(e,\vec{x}) \simeq \begin{cases} \Psi_n(e,\vec{x}) & \text{ak } \Psi_n(e,\vec{x})\downarrow \\ 0 & \text{ak } \Psi_n(e,\vec{x})\uparrow \end{cases} \tag{1}$$

je rekurzívna. Potom aj n-árna funkcia g definovaná vzťahom

$$g(x_1,\ldots,x_n) = f(x_1,x_1,\ldots,x_n)+1 \tag{2}$$

je rekurzívna. Existuje teda číslo e také, že pre každé $x_1,\ldots,x_n$:

$$\Psi_n(e,x_1,\ldots,x_n) \simeq g(x_1,\ldots,x_n). \tag{3}$$

Odtiaľ $\Psi_n(e,e,\ldots,e)\downarrow$. Postupnými úpravami odvodíme spor:

$$g(e,..,e) \overset{(2)}{=} f(e,e,..,e)+1 \overset{(1)}{\simeq} \Psi_n(e,e,..,e)+1 \overset{(3)}{\simeq} g(e,..,e)+1.$$

Enumerácia čiastočne rekurzívnych funkcií

Graf unárnej enumeračnej čiastočnej funkcie nie je rekurzívny predikát

Dôkaz sporom. Predpokladajme, že graf binárnej enumeračnej čiastočnej funkcie Ψ_1:

$$G_1(e, x, y) \leftrightarrow \Psi_1(e, x) \simeq y \tag{1}$$

je rekurzívny predikát. Potom je rekurzívny aj unárny predikát P:

$$P(x) \leftrightarrow G_1(x, x, 0). \tag{2}$$

Existuje teda číslo e také, že pre každé číslo x platí rovnosť

$$\Psi_1(e, x) \simeq P_*(x). \tag{3}$$

Postupnými úpravami teraz dostaneme spor:

$$P(e) \overset{(2)}{\Leftrightarrow} G_1(e, e, 0) \overset{(1)}{\Leftrightarrow} \Psi_1(e, e) \simeq 0 \overset{(3)}{\Leftrightarrow} P_*(e) \simeq 0 \Leftrightarrow \neg P(e).$$

Enumerácia čiastočne rekurzívnych funkcií

Graf enumeračnej čiastočnej funkcie nie je rekurzívny predikát

Dôkaz sporom. Predpokladajme, že graf $(n+1)$-árnej enumeračnej čiastočnej funkcie Ψ_n:

$$G_n(e, x_1, \ldots, x_n, y) \leftrightarrow \Psi_n(e, x_1, \ldots, x_n) \simeq y \tag{1}$$

je rekurzívny predikát. Potom je rekurzívny aj n-árny predikát P:

$$P(x_1, \ldots, x_n) \leftrightarrow G_n(x_1, x_1, \ldots, x_n, 0). \tag{2}$$

Existuje teda číslo e také, že pre každú n-ticu čísel $x_1, \ldots, x_n$ platí

$$\Psi_n(e, x_1, \ldots, x_n) \simeq P_*(x_1, \ldots, x_n). \tag{3}$$

Postupnými úpravami teraz dostaneme spor:

$$P(e, \ldots, e) \overset{(2)}{\Leftrightarrow} G_n(e, e, \ldots, e, 0) \overset{(1)}{\Leftrightarrow} \Psi_n(e, e, \ldots, e) \simeq 0 \overset{(3)}{\Leftrightarrow}$$
$$\Leftrightarrow P_*(e, \ldots, e) \simeq 0 \Leftrightarrow \neg P(e, \ldots, e).$$

Church-Turingova téza

Churchova téza (1936)

Trieda intuitívne vypočítateľných funkcií nad oborom N *je totožná s triedou obecne rekurzívnych funkcií.*

Turingova téza (1936-7)

Trieda intuitívne vypočítateľných funkcií nad oborom N *je totožná s triedou funkcií vypočítateľných na Turingových strojoch.*

Modely (čiastočne) vypočítateľných funkcií

- obecne rekurzívne funkcie [Herbrand-Gödel, 1931, 1934],
- λ-definovateľné funkcie [Church, 1932],
- (čiastočne) μ-rekurzívne funkcie [Kleene, 1935, 1952],
- Turingove stroje [Turing, 1936-7],
- čiastočne rekurzívne funkcie [Kleene, 1952],
- registrové stroje [napr. Minsky, 1961].

Turingova úplnosť a totálne funkcionálne programovanie

Euklidov algoritmus pre výpočet najväčšieho spoločného deliteľa

Implementácia

$$
\begin{aligned}
\gcd(x, y) = \textbf{if } & x \neq 0 \wedge y \neq 0 \textbf{ then} \\
& \textbf{case} \\
& \quad x > y \Rightarrow \gcd(x \dot{-} y, y) \\
& \quad x = y \Rightarrow x \\
& \quad x < y \Rightarrow \gcd(x, y \dot{-} x) \\
& \textbf{end} \\
& \textbf{else} \\
& \quad \max(x, y)
\end{aligned}
$$

Výpočet

Výpočet s argumentami klesajúcimi v miere $\max(x, y)$:

$$
\begin{array}{ccccccccc}
\gcd(9,12) & = & \gcd(9,3) & = & \gcd(6,3) & = & \gcd(3,3) & = 3 \\
12 & > & 9 & > & 6 & > & 3 &
\end{array}
$$

Turingova úplnosť a totálne funkcionálne programovanie

Euklidov algoritmus pre výpočet najväčšieho spoločného deliteľa

Implementácia

$$
\begin{aligned}
\gcd(x, y) = \textbf{if } & x \neq 0 \wedge y \neq 0 \textbf{ then} \\
& \textbf{case} \\
& \quad x > y \Rightarrow \gcd(x \dot{-} y, y) \\
& \quad x = y \Rightarrow x \\
& \quad x < y \Rightarrow \gcd(x, y \dot{-} x) \\
& \textbf{end} \\
\textbf{else} & \\
& \max(x, y)
\end{aligned}
$$

Výpočet

Podmienky regularity zaručujú, že výpočet vždy skončí:

$$x \neq 0 \wedge y \neq 0 \wedge x > y \rightarrow \max(x \dot{-} y, y) < \max(x, y)$$
$$x \neq 0 \wedge y \neq 0 \wedge x < y \rightarrow \max(x, y \dot{-} x) < \max(x, y).$$

Turingova úplnosť a totálne funkcionálne programovanie

Euklidov algoritmus pre výpočet najväčšieho spoločného deliteľa

Implementácia

$$
\begin{aligned}
\gcd(x, y) = \textbf{if } & x \neq 0 \wedge y \neq 0 \textbf{ then} \\
& \textbf{case} \\
& \quad x > y \Rightarrow \gcd(x \dot{-} y, y) \\
& \quad x = y \Rightarrow x \\
& \quad x < y \Rightarrow \gcd(x, y \dot{-} x) \\
& \textbf{end} \\
\textbf{else} & \\
& \max(x, y)
\end{aligned}
$$

Výpočet

Podmienka $x \neq 0 \wedge y \neq 0$ sa zbytočne opakovane vyhodnocuje

$$\gcd(9, 12) = \gcd(9, 3) = \gcd(6, 3) = \gcd(3, 3) = 3$$

Turingova úplnosť a totálne funkcionálne programovanie

Euklidov algoritmus pre výpočet najväčšieho spoločného deliteľa

Alternatívna implementácia so vstupnou podmienkou

$$x \neq 0 \wedge y \neq 0 \rightarrow \gcd(x, y) = \textbf{case}$$
$$x > y \Rightarrow \gcd(x \dot{-} y, y)$$
$$x = y \Rightarrow x$$
$$x < y \Rightarrow \gcd(x, y \dot{-} x)$$
$$\textbf{end}$$

Výpočet

Ten nemusí skončiť:

$$\gcd(1, 0) = \gcd(1 \dot{-} 0, 0) = \gcd(1, 0) = \cdots$$

Program počíta čiastočnú funkciu!

Turingova úplnosť a totálne funkcionálne programovanie

Euklidov algoritmus pre výpočet najväčšieho spoločného deliteľa

Alternatívna implementácia so vstupnou podmienkou

$$x \neq 0 \wedge y \neq 0 \rightarrow \gcd(x, y) = \textbf{case}$$
$$x > y \Rightarrow \gcd(x \dot{-} y, y)$$
$$x = y \Rightarrow x$$
$$x < y \Rightarrow \gcd(x, y \dot{-} x)$$
$$\textbf{end}$$

Výpočet

Rozšírené podmienky regularity pre mieru $\max(x, y)$:

$$x \neq 0 \wedge y \neq 0 \wedge x > y \rightarrow \max(x \dot{-} y, y) < \max(x, y) \wedge x \dot{-} y \neq 0 \wedge y \neq$$
$$x \neq 0 \wedge y \neq 0 \wedge x < y \rightarrow \max(x, y \dot{-} x) < \max(x, y) \wedge x \neq 0 \wedge y \dot{-} x \neq$$

Výpočet skončí pre vstupy spĺňajúce vstupnú podmienku.

Turing completeness and total functional programming

Interpreter for a programming language $\mathcal{L}$

Let M describe a single computation step of $\mathcal{L}$ and P its final configuration. Interpreter for $\mathcal{L}$ is the unlimited iteration of M s.t.

$$M^*(x) = \begin{cases} M^k(x) & \text{if } P\,M^k(x) \text{ and } k \text{ is the least such number,} \\ 0 & \text{if there is no such number.} \end{cases}$$

Program for evaluating of the interpreter M^*:

$$\exists k\, PM^k(x) \to M^*(x) = \textbf{if } P(x) \textbf{ then } x \textbf{ else } M^*\, M(x).$$

Condition of regularity of the program:

$$\exists k\, PM^k(x) \wedge \neg P(x) \to t\, M(x) < t(x) \wedge \exists k\, PM^k M(x),$$

where $t(x) = \mu k \left[\exists l\, PM^l(x) \to PM^k(x)\right]$ is the number of computation steps from the configuration x.

Turing completeness and total functional programming

Interpreter for a programming language $\mathcal{L}$

Let M describe a single computation step of $\mathcal{L}$ and P its final configuration. Interpreter for $\mathcal{L}$ is the unlimited iteration of M s.t.

$$M^*(x) = y \leftrightarrow \exists k\big(Pf^k(x) \wedge \forall l < k \neg PM^k(x) \wedge y = M^k(x)\big) \vee \neg\exists k\, PM^k(x) \wedge y = 0.$$

Program for evaluating of the interpreter M^*:

$$\exists k\, PM^k(x) \to M^*(x) = \textbf{if } P(x) \textbf{ then } x \textbf{ else } M^*\, M(x).$$

Condition of regularity of the program:

$$\exists k\, PM^k(x) \wedge \neg P(x) \to t\, M(x) < t(x) \wedge \exists k\, PM^k M(x),$$

where $t(x) = \mu k\big[\exists l\, PM^l(x) \to PM^k(x)\big]$ is the number of computation steps from the configuration x.

Nerozhodnuteľné problémy

Problém zastavenia

Aritmetizácia problému zastavenia pre n-árne čiastočne rekurzívne funkcie je $(n+1)$-árny predikát definovaný predpisom

$$\mathrm{W}_e^{(n)}(x_1, \ldots, x_n) \leftrightarrow \varphi_e^{(n)}(x_1, \ldots, x_n)\downarrow .$$

Veta

Problém zastavenia pre n-árne čiastočne rekurzívne funkcie je nerozhodnuteľný problém.

Dôkaz.

V opačnom prípade by takéto zúplnenie enumeračnej čiastočnej funkcie Ψ_n bola rekurzívna funkcia:

$$f(e, x_1, \ldots, x_n) \simeq \begin{cases} \varphi_e^{(n)}(x_1, \ldots, x_n) & \text{ak } \varphi_e^{(n)}(x_1, \ldots, x_n)\downarrow, \\ 0 & \text{ak } \varphi_e^{(n)}(x_1, \ldots, x_n)\uparrow. \end{cases}$$

Nerozhodnuteľné problémy

Problém zastavenia

Aritmetizácia problému zastavenia pre n-árne čiastočne rekurzívne funkcie je $(n+1)$-árny predikát definovaný predpisom

$$\mathrm{W}_e^{(n)}(x_1, \ldots, x_n) \leftrightarrow \varphi_e^{(n)}(x_1, \ldots, x_n)\downarrow .$$

Veta

Problém zastavenia pre n-árne čiastočne rekurzívne funkcie je nerozhodnuteľný problém.

Dôkaz.

V opačnom prípade by takéto zúplnenie enumeračnej čiastočnej funkcie Ψ_n bola rekurzívna funkcia:

$f(e, x_1, \ldots, x_n) \simeq$ **if** $\mathrm{W}_e^{(n)}(x_1, \ldots, x_n)$ **then** $\Psi_n(e, x_1, \ldots, x_n)$ **else** 0.

Nerozhodnuteľné problémy

Veta

Problém zastavenia pre enumeračnú čiastočnú funkciu je nerozhodnuteľný problém.

Dôkaz.

Nech e_n je rekurzívny index enumeračnej čiastočnej funkcie Ψ_n:

$$\Psi_n(e, x_1, \ldots, x_n) \simeq \Psi_{n+1}(e_n, e, x_1, \ldots, x_n).$$

Čiže

$$\varphi_e^{(n)}(x_1, \ldots, x_n)\downarrow \leftrightarrow \varphi_{e_n}^{(n+1)}(e, x_1, \ldots, x_n)\downarrow .$$

Odtiaľ dostaneme

$$\mathrm{W}_e^{(n)}(x_1, \ldots, x_n) \leftrightarrow \mathrm{W}_{e_n}^{(n+1)}(e, x_1, \ldots, x_n).$$

Z rozhodnuteľnosti problému zastavenia pre Ψ_n by sme dostali rozhodnuteľnosť všeobecného problému zastavenia.

Polorozhodnuteľné problémy

Čiastočne rekurzívne predikáty

n-árny predikát P je čiastočne rekurzívny, ak existuje n-árna čiastočne rekurzívna funkcia f taká, že

$$P(x_1, \ldots, x_n) \leftrightarrow f(x_1, \ldots, x_n)\downarrow .$$

Príklady

- Každý n-árny rekurzívny predikát P je čiastočne rekurzívny:

$$f(x_1, \ldots, x_n) \simeq \textbf{if } P(x_1, \ldots, x_n) \textbf{ then } 1 \textbf{ else } \emptyset^{(n)}(x_1, \ldots, x_n).$$

- Aritmetizácia problému zastavenia pre n-árne čiastočne rekurzívne funkcie je $(n+1)$-árny čiastočne rekurzívny predikát:

$$\mathrm{W}_e^{(n)}(x_1, \ldots, x_n) \leftrightarrow \Psi_n(e, x_1, \ldots, x_n)\downarrow .$$

Polorozhodnuteľné problémy

Čiastočne rekurzívne predikáty

n-árny predikát P je čiastočne rekurzívny, ak existuje n-árna čiastočne rekurzívna funkcia f taká, že

$$P(x_1, \ldots, x_n) \leftrightarrow f(x_1, \ldots, x_n)\downarrow .$$

Príklady

- Každý n-árny rekurzívny predikát P je čiastočne rekurzívny:

$$f(x_1, \ldots, x_n) \simeq \mu y[P(x_1, \ldots, x_n)].$$

- Aritmetizácia problému zastavenia pre n-árne čiastočne rekurzívne funkcie je $(n+1)$-árny čiastočne rekurzívny predikát:

$$\mathrm{W}_e^{(n)}(x_1, \ldots, x_n) \leftrightarrow \Psi_n(e, x_1, \ldots, x_n)\downarrow .$$

Polorozhodnuteľné problémy

Veta o normálnej forme (Kleene)

Pre každý n-árny čiastočne rekurzívny predikát P existuje číslo e také, že pre všetky čísla $x_1, \ldots, x_n$ platí vzťah

$$P(x_1, \ldots, x_n) \leftrightarrow \exists s \, \mathrm{T}_n(e, x_1, \ldots, x_n, s)$$

Dôkaz.

Nech f je n-árna čiastočne rekurzívna funkcia taká, že

$$P(x_1, \ldots, x_n) \leftrightarrow f(x_1, \ldots, x_n)\downarrow .$$

Z Kleeneho vety o normálnej forme pre n-árne čiastočne rekurzívne funkcie plynie, že existuje číslo e také, že

$$f(x_1, \ldots, x_n) \simeq \mathrm{U}\, \mu s[\mathrm{T}_n(e, x_1, \ldots, x_n, s)].$$

Polorozhodnuteľné problémy

Veta o normálnej forme (Kleene)

Pre každý n-árny čiastočne rekurzívny predikát P existuje číslo e také, že pre všetky čísla $x_1, \ldots, x_n$ platí vzťah

$$P(x_1, \ldots, x_n) \leftrightarrow \exists s \, \mathrm{T}_n(e, x_1, \ldots, x_n, s)$$

Dôkaz.

Nech f je n-árna čiastočne rekurzívna funkcia taká, že

$$P(x_1, \ldots, x_n) \leftrightarrow f(x_1, \ldots, x_n)\downarrow .$$

Z Kleeneho vety o normálnej forme pre n-árne čiastočne rekurzívne funkcie plynie, že existuje číslo e také, že

$$f(x_1, \ldots, x_n)\downarrow \leftrightarrow \exists s \, \mathrm{T}_n(e, x_1, \ldots, x_n, s).$$

Polorozhodnuteľné problémy

Veta (Post)

Predikát je rekurzívny práve vtedy, keď on a jeho negácia sú čiastočne rekurzívne predikáty.

Dôkaz.

Nech n-árny predikát P a jeho negácia sú čiastočne rekurzívne. Z vety o normálnej forme plynie, že existujú čísla e_1, e_2 také, že

$$P(x_1, \ldots, x_n) \leftrightarrow \exists s \, \mathrm{T}_n(e_1, x_1, \ldots, x_n, s)$$
$$\neg P(x_1, \ldots, x_n) \leftrightarrow \exists s \, \mathrm{T}_n(e_2, x_1, \ldots, x_n, s).$$

Regulárna minimalizácia definuje n-árnu rekurzívnu funkciu f:

$$f(x_1, \ldots, x_n) = \mu s[\mathrm{T}_n(e_1, x_1, \ldots, x_n, s) \vee \mathrm{T}_n(e_2, x_1, \ldots, x_n, s)].$$

Rekurzívnosť predikátu P plynie z tohoto vyjadrenia

$$P(x_1, \ldots, x_n) \leftrightarrow \mathrm{T}_n\big(e_1, x_1, \ldots, x_n, f(x_1, \ldots, x_n)\big).$$

Polorozhodnuteľné problémy

Projekcie rekurzívnych predikátov

Nech R je $(n+1)$-árny rekurzívny predikát a nech P je n-árny predikát definovaný predpisom

$$P(x_1, \ldots, x_n) \leftrightarrow \exists y \, R(y, x_1, \ldots, x_n).$$

Vravíme, že predikát P vznikol (existenčnou) projekciou rekurzívneho predikátu R.

Rekurzívne spočítateľné predikáty

n-árny predikát P je rekurzívne spočítateľný, ak jeho obor pravdivosti je prázdna množina alebo ak existuje unárna rekurzívna funkcia f taká, že

$$P(x_1, \ldots, x_n) \leftrightarrow \exists y \, f(y) = \langle x_1, \ldots, x_n \rangle.$$

Vravíme, že funkcia f enumeruje predikát P.

Polorozhodnuteľné problémy

Veta

Nech P je n-árny predikát. Potom nasledujúce podmienky sú ekvivalentné:

- *P je čiastočne rekurzívny predikát.*
- *P je projekcia rekurzívneho predikátu.*
- *P je rekurzívne spočítateľný predikát.*

Dôkaz.

Znenie vety plynie z nasledujúcich troch pomocných tvrdení.

Polorozhodnuteľné problémy

Lema

Každý čiastočne rekurzívny predikát je projekciou rekurzívneho predikátu.

Dôkaz.

Nech P je n-árny čiastočne rekurzívny predikát. Z Kleeneho vety o normálnej forme plynie, že existuje číslo e také, že

$$P(x_1, \ldots, x_n) \leftrightarrow \exists s \, \mathrm{T}_n(e, x_1, \ldots, x_n, s).$$

Nasledujúci vzťah definuje $(n+1)$-árny rekurzívny predikát R:

$$R(s, x_1, \ldots, x_n) \leftrightarrow \mathrm{T}_n(e, x_1, \ldots, x_n, s).$$

Predikát P je tak projekciou rekurzívneho predikátu

$$P(x_1, \ldots, x_n) \leftrightarrow \exists s \, R(s, x_1, \ldots, x_n).$$

Polorozhodnuteľné problémy

Lema

Každá projekcia rekurzívneho predikátu je rekurzívne spočítateľný predikát.

Dôkaz.

Nech R je $(n+1)$-árny rekurzívny predikát a nech P je jeho projekcia:

$$P(x_1, \ldots, x_n) \leftrightarrow \exists y \, R(y, x_1, \ldots, x_n)$$

Predpokladajme, že predikát P platí pre čísla $a_1, \ldots, a_n$. Uvažujme unárnu funkciu f definovanú vzťahom

$$f(z) = \begin{cases} \langle x_1, \ldots, x_n \rangle & \text{ak pre nejaké čísla } y, x_1, \ldots, x_n \text{ platí} \\ & z = \langle y, x_1, \ldots, x_n \rangle \text{ a } R(y, x_1, \ldots, x_n), \\ \langle a_1, \ldots, a_n \rangle & \text{ináč.} \end{cases}$$

f je rekurzívna funkcia, ktorá enumeruje predikát P:

$$P(x_1, \ldots, x_n) \leftrightarrow \exists z \, f(z) = \langle x_1, \ldots, x_n \rangle.$$

P je preto rekurzívne spočítateľný predikát.

Polorozhodnuteľné problémy

Lema

Každá projekcia rekurzívneho predikátu je rekurzívne spočítateľný predikát.

Dôkaz.

Nech R je $(n+1)$-árny rekurzívny predikát a nech P je jeho projekcia:

$$P(x_1, \ldots, x_n) \leftrightarrow \exists y\, R(y, x_1, \ldots, x_n)$$

Predpokladajme, že predikát P platí pre čísla $a_1, \ldots, a_n$. Uvažujme unárnu funkciu f definovanú vzťahom

$$f(z) = \begin{cases} \langle x_1, \ldots, x_n \rangle & \text{ak pre nejaké čísla } y, x_1, \ldots, x_n \text{ platí} \\ & z = \langle y, x_1, \ldots, x_n \rangle \text{ a } R(y, x_1, \ldots, x_n), \\ \langle a_1, \ldots, a_n \rangle & \text{ináč.} \end{cases}$$

$$\langle R \rangle(z) \leftrightarrow R([z]_1^{n+1}, [z]_2^{n+1}, \ldots, [z]_{n+1}^{n+1})$$

$$f(z) = \textbf{if } \mathit{Tuple}(n+1, z) \wedge \langle R \rangle(z) \textbf{ then } \pi_2(z) \textbf{ else } \langle a_1, \ldots, a_n \rangle.$$

f je rekurzívna funkcia, ktorá enumeruje predikát P:

Polorozhodnuteľné problémy

Lema

Každý rekurzívne spočítateľný predikát je čiastočne rekurzívny predikát.

Dôkaz.

Nech f je unárna rekurzívna funkcia, ktorá enumeruje n-árny predikát P:

$$P(x_1, \ldots, x_n) \leftrightarrow \exists y\, f(y) = \langle x_1, \ldots, x_n \rangle.$$

Potom neohraničená minimalizácia

$$g(x_1, \ldots, x_n) \simeq \mu y[f(y) = \langle x_1, \ldots, x_n \rangle]$$

definuje čiastočne rekurzívnu funkcia g takú, že

$$P(x_1, \ldots, x_n) \leftrightarrow g(x_1, \ldots, x_n)\downarrow .$$

Polorozhodnuteľné problémy

Uniformný problém zastavenia

Aritmetizácia uniformného problému zastavenia pre n-árne čiastočne rekurzívne funkcie je unárny predikát definovaný predpisom

$$\mathrm{Tot}_n(e) \leftrightarrow \forall x_1 \cdots \forall x_n \, \varphi_e^{(n)}(x_1, \ldots, x_n)\downarrow .$$

Veta

Uniformný problém zastavenia pre n-árne čiastočne rekurzívne funkcie nie je ani polorozhodnuteľný problém.

Polorozhodnuteľné problémy

Uniformný problém zastavenia

Aritmetizácia uniformného problému zastavenia pre n-árne čiastočne rekurzívne funkcie je unárny predikát definovaný predpisom

$$\mathrm{Tot}_n(e) \leftrightarrow \forall x_1 \cdots \forall x_n \mathrm{W}_e^{(n)}(x_1, \ldots, x_n).$$

Veta

Uniformný problém zastavenia pre n-árne čiastočne rekurzívne funkcie nie je ani polorozhodnuteľný problém.

Polorozhodnuteľné problémy

Dôkaz pre $n = 1$.

Sporom. Predpokladajme. že predikát Tot je čiastočne rekurzívny. Potom existuje unárna rekurzívna funkcia k, ktorá ho enumeruje:

$$\mathrm{Tot}(e) \leftrightarrow \exists x\, k(x) = e.$$

Nasledujúci vzťah definuje unárnu čiastočne rekurzívnu funkciu f:

$$f(x) \simeq \Psi\big(k(x), x\big) + 1 \ \big(\simeq \varphi_{k(x)}(x) + 1\big). \tag{1}$$

Pretože $\varphi_{k(x)}(x)\downarrow$, f je totálna. Existujú preto čísla e_0, x_0 také, že

$$\forall x\, \Psi(e_0, x) \simeq f(x) \tag{2}$$

$$e_0 = k(x_0). \tag{3}$$

Postupnými úpravami odvodíme spor:

$$f(x_0) \overset{(1)}{\simeq} \Psi\big(k(x_0), x_0\big) + 1 \overset{(3)}{\simeq} \Psi(e_0, x_0) + 1 \overset{(2)}{\simeq} f(x_0) + 1.$$

Záver

Skúšobné obdobie

- Na riadne termíny sa zapisujte cez AIS2. Požiadavka: priebežné semestrálne hodnotenie aspoň 20 bodov (podľa AIS2).
- Ďalšie informácie sú na webovej stranke predmetu:
  - konzultácie počas skúšobného obdobia,
  - súbor obsahujúci otázky na skúšku.