1-AIN-470 Špecifikácia a verifikácia programov

Letný semester 2016/17

12. prednáška

Ján Komara

Obsah 12. prednášky

Čiastočne rekurzívne funkcie

Kleeneho veta o normálnej forme

Enumerácia čiastočne rekurzívnych funkcií

Rekurzívne nerozhodnuteľné problémy

Turingova úplnosť a totálne funkcionálne programovanie

Čiastočne rekurzívne funkcie

Definícia triedy čiastočne rekurzívnych funkcií

- Základné funkcie:
  - funkcia nasledovníka $S(x) = x + 1$,
  - 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.

Čiastočne rekurzívne funkcie

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:

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

Veta

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

Čiastočne rekurzívne funkcie

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:

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

Veta

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

Čiastočne rekurzívne funkcie

Dôkaz.

V odvodení f použijeme túto čiastočne rekurzívnu funkciu:

$$g(y,\vec{x}) \simeq \begin{cases} y & \text{ak platí } \varphi[\vec{x},y], \\ g(y+1,\vec{x}) & \text{ak neplatí } \varphi[\vec{x},y]. \end{cases}$$

Rekurzívnosť čiastočnej funkcie f plynie z tohoto vyjadrenia

$$\begin{aligned} P(\vec{x},y) &\leftrightarrow \varphi[\vec{x},y] \\ g(y,\vec{x}) &\simeq \textbf{if } P(\vec{x},y) \textbf{ then } y \textbf{ else } g(y+1,\vec{x}) \\ f(\vec{x}) &\simeq g(0,\vec{x}). \end{aligned}$$

Korektnosť implementácie plynie z tejto vlastnosti čiastočne rekurzívnej funkcie g:

$$g(y,\vec{x}) \simeq z \leftrightarrow y \leq z \wedge \varphi[\vec{x},z] \wedge \forall z_1 \big(y \leq z_1 < z \rightarrow \neg\varphi[\vec{x},z_1]\big).$$

Kleeneho veta o normálnej forme

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 prirodzené čísla* $x_1, \ldots, x_n$ *platí vzťah:*

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

Zopakovanie

Nasledujúce témy boli prebraté na predošlej prednáške:

- výpočtový model pre čiastočne rekurzívne funkcie,
- aritmetizácia výpočtového modelu.

Kleeneho veta o normálnej forme

Idea dôkazu

Neformálny popis predikátu T_n a funkcie U:

- Kleeneho predikát T_n má túto základnú vlastnosť:

  $\mathrm{T}_n(e, x_1, \ldots, x_n, s)$ *platí práve vtedy, keď* e *je kód programu a* s *je kód výpočtu tohoto programu pre vstupy* $x_1, \ldots, x_n$.

  Tu programom rozumieme čiastočne rekurzívne odvodenie nejakej čiastočnej funkcie a výpočtom proces vyhodnotenia tejto čiastočnej rekurzívnej funkcie.
- Funkcia $\mathrm{U}(s)$ určí z kódu výpočtovej postupnosti výslednú hodnotu.

Ukážeme, že Kleeneho predikát T_n i funkciu U môžeme zvoliť ako primitívne rekurzívne.

Kleeneho veta o normálnej forme

Aritmetizácia redukčnej relácie

Binárny primitívne rekurzívny predikát $t \rhd_1^\bullet r$ je aritmetizáciou jednokrokovej redukčnej relácie $\tau \rhd_1 \rho$:

> *$t \rhd_1^\bullet r$ platí práve vtedy, keď existujú uzavreté rekurzívne termy τ, ρ také, že $t = \ulcorner \tau \urcorner$, $r = \ulcorner \rho \urcorner$ a $\tau \rhd_1 \rho$.*

Primitívna rekurzívnosť predikátu plynie z tohoto vyjadrenia

$$t \rhd_1^\bullet r \leftrightarrow Ctm(t) \wedge \neg Nm(t) \wedge Ctm(r) \wedge Rd(t) = r.$$

Tu $Rd(t)$ je unárna primitívne rekurzívna funkcia taká, že platí:

$$\text{ak } \tau \rhd_1 \rho, \text{ potom } Rd(\ulcorner \tau \urcorner) = \ulcorner \rho \urcorner$$
$$Rd(\ulcorner \underline{x} \urcorner) = \ulcorner \underline{x} \urcorner.$$

Kleeneho veta o normálnej forme

Kleeneho predikát

Primitívne rekurzívny predikát $Computation(s)$ platí, ak číslo s je kódom (ukončenej) výpočtovej postupnosti:

$$Computation(s) \leftrightarrow s \neq 0 \wedge \forall i < L(s) \dot{-} 1 \ (s)_i \rhd_1^{\bullet} (s)_{i+1} \wedge$$
$$\wedge Nm\left((s)_{L(s)\dot{-}1}\right).$$

Primitívne rekurzívna funkcia $\mathrm{U}(s)$ vyberie z výpočtovej postupnosti s výslednú hodnotu:

$$\mathrm{U}(s) = Dc\left((s)_{L(s)\dot{-}1}\right).$$

Kleeneho predikát T_n je $(n{+}2)$-árny primitívne rekurzívny predikát definovaný explicitne predpisom

$$\mathrm{T}_n(e, x_1, \ldots, x_n, s) \leftrightarrow Rf(n, e) \wedge Computation(s) \wedge$$
$$\wedge (s)_0 = e(\langle \ulcorner \underline{x_1} \urcorner, \ldots, \ulcorner \underline{x_n} \urcorner \rangle).$$

Kleeneho veta o normálnej forme

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 prirodzené čísla* $x_1, \ldots, x_n$ *platí vzťah:*

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

Poznámka

Z dôkazu Kleeneho vety o normálnej forme vyplýva, že pre každý n-árny rekurzívny funkčný symbol f platí

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

Kleeneho veta o normálnej forme

Churchova téza (1936)

Trieda intuitívne vypočítateľných funkcií nad oborom prirodzených čísel je totožná s triedou obecne rekurzívnych funkcií.

Turingova téza (1936-1937)

Trieda intuitívne vypočítateľných funkcií nad oborom prirodzených čísel 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, 1936-1937],
- čiastočne rekurzívne funkcie [Kleene, 1952],
- registrové stroje [napr. Minsky, 1961].

Enumerácia čiastočne rekurzívnych funkcií

Rekurzívne indexy

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

$$\varphi_e^{(n)} = \begin{cases} f & \text{ak } e = \ulcorner f \urcorner \text{ pre nejaký } n\text{-árny rek. fun. symbol } f, \\ \emptyset^{(n)} & \text{ináč.} \end{cases}$$

Ak $f = \varphi_e^{(n)}$ tak číslo e nazveme rekurzívnym indexom čiastočnej funkcie f. Čísla v tvare $\ulcorner f \urcorner$ 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 (s 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

$$\lambda\vec{x}.\Psi_n(0,\vec{x}) \quad \lambda\vec{x}.\Psi_n(1,\vec{x}) \quad \lambda\vec{x}.\Psi_n(2,\vec{x}) \quad \ldots$$

$$\text{t.j.} \qquad \varphi_0^{(n)} \qquad \varphi_1^{(n)} \qquad \varphi_2^{(n)} \qquad \ldots$$

  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 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

Graf 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:

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

Rekurzívne 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:

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

Rekurzívne 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:

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

Rekurzívne 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.

Turing completeness and total functional programming

Evaluator of a programming language $\mathcal{L}$

Let M describe a single computation step of $\mathcal{L}$ and P its final configuration. Evaluator of $\mathcal{L}$ 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 computing the evaluator 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 (zero for infinite loop).

Turing completeness and total functional programming

Evaluator of a programming language $\mathcal{L}$

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

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

Program for computing the evaluator M^*:

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

Condition of regularity of the program:

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

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