2-AIN-285 Symbolické programovanie a LISP

Letný semester 2017/18
6. prednáška

Ján Komara

Obsah 6. prednášky

Zopakovanie

Čiastočne rekurzívne funkcie

Výpočtový model pre čiastočne rekurzívne funkcie

Enumerácia čiastočne rekurzívnych funkcií

Rekurzívne nerozhodnuteľné problémy

Turingova úplnosť a totálne funkcionálne programovanie

Zopakovanie

Teória rekurzívnych funkcií

- Primitívne rekurzívne funkcie
  - Aritmetizácia dátových štruktúr.
  - Regulárne rekurzívne definície s mierou.
- Obecne rekurzívne funkcie
  - Regulárne rekurzívne definície do dobre založených relácií:
    - Ackermannova funkcia,
    - univerzálna funkcia pre primitívne rekurzívne funkcie.
  - Churchova téza.
- Čiastočne rekurzívne funkcie
  - Kleeneho prvá veta o rekurzii (veta o pevnom bode).
  - Kleeneho veta o normálnej forme.
  - Turing-Churchova téza.

Teória rekurzívnych funkcií umožňuje vybudovať matematické základy deklaratívnych programovacích jazykov.

Čiastočne rekurzívne funkcie

Definícia triedy čiastočne rekurzívnych funkcií

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

Rekurzívne odvodenia

Sčítanie

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

Odčítanie

$$x \mathbin{\dot{-}} y \simeq \textbf{if } x \neq 0 \textbf{ then if } y \neq 0 \textbf{ then } \mathsf{P}(x) \mathbin{\dot{-}} \mathsf{P}(y) \textbf{ else } x \textbf{ else } 0.$$

Násobenie

$$x \cdot y \simeq \textbf{if } x \neq 0 \textbf{ then } \mathsf{P}(x) \cdot y + y \textbf{ else } 0.$$

Umocňovanie

$$x^y \simeq \textbf{if } y \neq 0 \textbf{ then } x \cdot x^{\mathsf{P}(y)} \textbf{ else } 1.$$

Výpočtový model pre čiastočne rekurzívne funkcie

Rekurzívne termy a funkčné symboly (príklad)

Primitívne rekurzívna definícia

$$0 + y = y$$
$$S(x) + y = S(x + y).$$

Regulárna rekurzívna definícia

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

Rekurzívna definícia so silnou rovnosťou

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

Rekurzívny funkčný symbol

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

Výpočtový model pre čiastočne rekurzívne funkcie

Monadické numerály

Výpočet prebieha na monadických numeráloch:

$$0 \quad \mathsf{S}(0) \quad \mathsf{S}\,\mathsf{S}(0) \quad \mathsf{S}\,\mathsf{S}\,\mathsf{S}(0) \quad \mathsf{S}\,\mathsf{S}\,\mathsf{S}\,\mathsf{S}(0) \quad \ldots .$$

Označenie:

- Ak x je prirodzené číslo, potom $\underline{x}$ je monadický numerál, ktorý denotuje číslo x:

$$\underline{x} \equiv \overbrace{\mathsf{S}\ldots\mathsf{S}}^{x\text{-krát}}(0).$$

- Ak $x_1, \ldots, x_n$ sú prirodzené čísla, potom

$$\underline{x_1, \ldots, x_n} \equiv \underline{x_1}, \ldots, \underline{x_n} \equiv \overbrace{\mathsf{S}\ldots\mathsf{S}}^{x_1\text{-krát}}(0), \ldots, \overbrace{\mathsf{S}\ldots\mathsf{S}}^{x_n\text{-krát}}(0).$$

Výpočtový model pre čiastočne rekurzívne funkcie

Jeden krok výpočtu

Ak uzavretý rekurzívny term τ nie je numerál, tak musí obsahovať aspoň jeden podvýraz (*redex*) v tvare

$$\mathrm{D}(\underline{x}, \sigma_2, \sigma_3) \qquad \mathrm{P}(\underline{x}) \qquad (\lambda_n.\sigma)(\underline{\vec{x}}).$$

Jeden výpočtový krok spočíva v nájdení najľavejšieho redexu a jeho nahradením kontrakciou podľa nasledujúcich pravidiel

$$\begin{aligned} \mathrm{D}(\underline{0}, \sigma_2, \sigma_3) &\rhd_1 \sigma_3 \\ \mathrm{D}(\underline{x+1}, \sigma_2, \sigma_3) &\rhd_1 \sigma_2 \\ \mathrm{P}(\underline{x}) &\rhd_1 \underline{x \dot{-} 1} \\ (\lambda_n.\sigma[\mathfrak{f}_n; \vec{x}])(\underline{\vec{x}}) &\rhd_1 \sigma[\lambda_n.\sigma; \underline{\vec{x}}]. \end{aligned}$$

Tak dostaneme nový uzavretý rekurzívny term ρ a píšeme

$$\tau \rhd_1 \rho.$$

Výpočtový model pre čiastočne rekurzívne funkcie

Viac krokov výpočtu

Označenie:

- $\tau_1 \rhd_k \tau_2$, ak výraz τ_1 sa redukuje do výrazu τ_2 po k krokoch. To znamená, že existujú uzavreté rekurzívne termy $\rho_0, \rho_1, \ldots, \rho_k$ také, že

$$\tau_1 \equiv \rho_0 \rhd_1 \rho_1 \rhd_1 \cdots \rhd_1 \rho_k \equiv \tau_2.$$

  Umožníme tiež prípad $k = 0$. Vtedy $\tau_1 \rhd_0 \tau_2 \leftrightarrow \tau_1 \equiv \tau_2$.
- $\tau_1 \rhd \tau_2$, ak $\tau_1 \rhd_k \tau_2$ pre nejaké k.
- Ak $\tau \rhd \underline{x}$, tak vravíme, že výpočet skončil s výsledkom x.

Veta (Ekvivalentnosť definičnej a výpočtovej sémantiky)

Pre každý rekurzívny funkčný symbol f platí:

$$f(\vec{x}) \simeq y \leftrightarrow f(\underline{\vec{x}}) \rhd \underline{y}.$$

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.

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

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

  je enumerácia triedy n-árnych čiastočne rekurzívnych funkcií.
- Pre dobre vytvorené indexy n-árnych čiastočne rekurzívnych funkcií totiž platí:

$$\Psi_n(e, x_1, \ldots, x_n) \simeq \mathit{Dc}\ \mathit{Eval}\ e\big(\langle \ulcorner \underline{x_1} \urcorner, \ldots, \ulcorner \underline{x_n} \urcorner \rangle\big).$$

  Ψ_n je preto čiastočne rekurzívna funkcia.

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

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].

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^*:

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

Condition of regularity of the program:

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

where $t(x) = \mu k \left[\exists l\, P M^l(x) \to P M^k(x) \right]$ 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^*:

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

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 (zero for infinite loop).