IB107 Vyčíslitelnost a složitost

věta o parametrizaci, programovací systémy*, rekurzivní a r.e. množiny

Jan Strejček

Fakulta informatiky
Masarykova univerzita

věta o parametrizaci

- funkci lze definovat parametrizací, tj. zafixováním vybraných argumentů jiné funkce

Věta 5.20 (věta o parametrizaci, s_n^m věta (Kleene))

Pro každá $m, n \geq 1$ existuje totálně vyčíslitelná funkce $s_n^m : \mathbb{N}^{m+1} \to \mathbb{N}$ taková, že pro všechna $e, y_1, \ldots, y_{m+n} \in \mathbb{N}$ platí

$$\varphi^{(n)}_{s_n^m(e,y_1,\ldots,y_m)}(y_{m+1}, \ldots, y_{m+n}) = \varphi_e^{(m+n)}(y_1, \ldots, y_{m+n}).$$

důkaz věty o parametrizaci

$$\varphi^{(n)}_{s^m_n(e,y_1,\dots,y_m)}(y_{m+1},\dots,y_{m+n}) = \varphi^{(m+n)}_e(y_1,\dots,y_{m+n})$$

Důkaz: funkce $s^m_n(e, y_1, \dots, y_m)$ vrací index programu

begin

$x_{m+n} := x_n;$

$\vdots$

$x_{m+1} := x_1;$

$x_m := y_m;$

$\vdots$

$x_1 := y_1;$

P_e

end

■

využití věty o parametrizaci

Lemma 5.21

Existuje totálně vyčíslitelná funkce $h : \mathbb{N}^2 \to \mathbb{N}$ taková, že pro všechna $i, j, x \in \mathbb{N}$ platí

$$\varphi_{h(i,j)}(x) = (\varphi_i \circ \varphi_j)(x).$$

Důkaz:

- definujme funkci $f : \mathbb{N}^3 \to \mathbb{N}$ jako

$$f(i,j,x) = (\varphi_i \circ \varphi_j)(x) = \varphi_i(\varphi_j(x)) = \Phi(i, \Phi(j,x))$$

- f je vyčíslitelná a nechť e je její index
- věta o parametrizaci říká, že TVF s_1^2 splňující $\varphi_{s_1^2(e,i,j)}(x) = \varphi_e(i,j,x) = f(i,j,x)$
- klademe $h(i,j) = s_1^2(e,i,j)$ a tudíž h je totálně vyčíslitelná

$\blacksquare$

translační lemma

Důsledek 5.23 (translační lemma)

Ke každé vyčíslitené funkci $f : \mathbb{N}^2 \to \mathbb{N}$ existuje totálně vyčíslitelná funkce $r : \mathbb{N} \mapsto \mathbb{N}$ taková, že pro všechna $x, y \in \mathbb{N}$ platí

$$f(x, y) = \varphi_{r(x)}(y).$$

- nazývá se také neefektivní podoba věty o parametrizaci
- lze zobecnit na vyšší počty argumentů

Důkaz:

- nechť e je index f
- věta o parametrizaci říká, že existuje TVF s_1^1 splňující $\varphi_{s_1^1(e,x)}(y) = \varphi_e(x, y) = f(x, y)$
- klademe $r(x) = s_1^1(e, x)$ a tudíž r je totálně vyčíslitelná

$\blacksquare$

využití translačního lemmatu

- nechť $\psi : \mathbb{N} \to \mathcal{S}$ je (ne nutně totální) numerace podmnožiny unárních vyčíslitelných funkcí $\mathcal{S} \subseteq \mathcal{P}$, která splňuje větu o numeraci, tj. existuje vyčíslitelná funkce $\Phi_\psi : \mathbb{N}^2 \to \mathbb{N}$ taková, že pro všechna $x, y \in \mathbb{N}$ platí

$$\Phi_\psi(x, y) = \psi_x(y)$$

- dle translačního lemmatu pak existuje totálně vyčíslitelná funkce r splňující

$$\Phi_\psi(x, y) = \varphi_{r(x)}(y) = \psi_x(y)$$

- tedy r převádí numeraci ψ na standardní numeraci φ

programovací systém/jazyk

- while-programy nejsou jediným modelem algoritmů
- ukážeme nezávislost teorie na volbě formalismu

Definice (programovací systém/jazyk)

Programovací systém (či jazyk) pro $\mathcal{P}^{(j)}$ je dvojice $\mathcal{L}' = (T, \varphi')$, kde T je množina programů (syntaxe) a $\varphi' : T \mapsto \mathcal{P}^{(j)}$ je sémantika přiřazující každému programu j-ární vyčíslitelnou funkci.

- jazyk while-programů:
- můžeme předpokládat, že $T = \mathbb{N}$
- programovací jazyk by měl být
  - univerzální – existuje univerzální program
  - efektivní – programy lze jednoduše skládat

redukce a ekvivalence numerací

Definice 6.1 (redukce a ekvivalence numerací)

Numerace ψ množiny M se redukuje na numeraci ψ' množiny M' (píšeme $\psi \leq \psi'$), právě když existuje totálně vyčíslitelná funkce $r : \mathbb{N} \to \mathbb{N}$ taková, že pro všechna $i \in dom(\psi)$ platí

$$\psi_i = \psi'_{r(i)}.$$

Numerace ψ, ψ' jsou ekvivalentní (píšeme $\psi \equiv \psi'$), právě když $\psi \leq \psi'$ a $\psi' \leq \psi$.

- jsou-li ψ, ψ' dvě totální numerace množiny $\mathcal{P}^{(j)}$, pak $\psi \leq \psi'$ znamená, že jazyk $(\mathbb{N}, \psi)$ lze efektivně přeložit do jazyka $(\mathbb{N}, \psi')$

vztahy numerací

Věta 6.2

Nechť pro každé $j \geq 1$ jsou $\psi^{(j)}, \psi'^{(j)}$ totální numerace množiny $\mathcal{P}^{(j)}$. Pokud ψ splňuje větu o numeraci a ψ' větu o parametrizaci, pak $\psi^{(j)} \leq \psi'^{(j)}$ pro každé $j \geq 1$.

Důkaz: pro $j = 1$

- ψ má vyčíslitelnou univerzální funkci

$$\Phi_\psi(i, x) = \psi_i(x)$$

- translační lemma pro ψ' říká, že existuje totální vyčíslitelná funkce r taková, že

$$\Phi_\psi(i, x) = \psi'_{r(i)}(x)$$

- tedy $\psi \leq \psi'$

■

vztahy ke standardní numeraci

Věta 6.2 (pokračování)

Nechť pro každé $j \geq 1$ je $\psi^{(j)}$ totální numerací množiny $\mathcal{P}^{(j)}$ a $\varphi^{(j)}$ její standardní numerací. Pak ψ splňuje věty o numeraci a parametrizaci, právě když pro každé $j \geq 1$ platí $\psi^{(j)} \equiv \varphi^{(j)}$.

Důkaz:

$\Longrightarrow$ plyne z předchozí věty

$\Longleftarrow$ ukážeme, že ψ splňuje větu o numeraci

- pro každé $j \geq 1$ je univerzální funkce $\Phi_\psi : \mathbb{N}^{j+1} \to \mathbb{N}$ pro ψ definovaná vztahem
$$\Phi_\psi(i, x_1, \ldots, x_j) = \psi_i^{(j)}(x_1, \ldots, x_j)$$
- z $\psi^{(j)} \leq \varphi^{(j)}$ plyne existence totálně vyčíslitelné funkce $r : \mathbb{N} \to \mathbb{N}$ splňující $\psi_i^{(j)} = \varphi_{r(i)}^{(j)}$

  $\Phi_\psi(i, x_1, \ldots, x_j) =$
- tedy Φ_ψ je vyčíslitelná

vztahy ke standardní numeraci

$\Longleftarrow$ ukážeme, že ψ splňuje větu o parametrizaci

- nechť $m, n \geq 1$
- z $\psi^{(m+n)} \leq \varphi^{(m+n)}$ plyne existence totálně vyčíslitelné funkce $r : \mathbb{N} \to \mathbb{N}$ splňující $\psi_i^{(m+n)} = \varphi_{r(i)}^{(m+n)}$
- z $\varphi^{(n)} \leq \psi^{(n)}$ plyne existence totálně vyčíslitelné funkce $s : \mathbb{N} \to \mathbb{N}$ splňující $\varphi_i^{(n)} = \psi_{s(i)}^{(n)}$

$$\psi_i^{(m+n)}(y_1, \ldots, y_{m+n}) \ =$$

- jelikož $g(i, y_1, \ldots, y_m) = s(s_n^m(r(i), y_1, \ldots, y_m))$ je totálně vyčíslitelná funkce, ψ splňuje větu o parametrizaci ■

přípustná numerace

Definice 6.3 (přípustná numerace)

Totální numerace vyčíslitelných funkcí je přípustná (efektivní), pokud pro ni platí věty o numeraci a parametrizaci.

věty o numeraci a parametrizaci jsou nezávislé, tedy

- existuje numerace, pro kterou platí věta o numeraci, ale neplatí věta o parametrizaci
- existuje numerace, pro kterou neplatí věta o numeraci, ale platí věta o parametrizaci

numerace totálně vyčíslitelných funkcí

Věta 6.5

Nechť ψ je totální numerace všech unárních totálně vyčíslitelných funkcí. Pak univerzální funkce $\Phi_\psi : \mathbb{N}^2 \to \mathbb{N}$ definovaná jako

$$\Phi_\psi(i, x) = \psi_i(x)$$

není vyčíslitelná.

Důkaz: diagonalizací ■

Důsledek 6.6

Neexistuje přípustná totální numerace všech totálních vyčíslitelných funkcí.

rekurzivní množiny

Definice 7.1 (rekurzivní množina)

Množina $A \subseteq \mathbb{N}^k$ je rekurzivní, pokud existuje totálně vyčíslitelná funkce $f : \mathbb{N}^k \to \mathbb{N}$ taková, že

$$A = f^{-1}(\{1\}) = \{(x_1, \dots, x_k) \in \mathbb{N}^k \mid f(x_1, \dots, x_k) = 1\}.$$

Funkce f se nazývá rozhodovací funkce pro A.

- rekurzivní množině se také říká rozhodnutelná či řešitelná
- příklady rekurzivních množin:

rekurzivní množiny

Tvrzení

$A \subseteq \mathbb{N}^k$ je rekurzivní, právě když je její charakteristická funkce $\chi_A : \mathbb{N}^k \to \mathbb{N}$ definovaná vztahem

$$\chi_A(x_1, \ldots, x_k) = \begin{cases} 1 & \textit{pokud } (x_1, \ldots, x_k) \in A \\ 0 & \textit{jinak} \end{cases}$$

totálně vyčíslitelná.

Důkaz:

vlastnosti rekurzivních množin

Věta 7.4

Jestliže $A \subseteq \mathbb{N}^k$ je konečná množina nebo $\mathbb{N}^k \smallsetminus A$ je konečná, pak A je rekurzivní.

Důkaz:

$\blacksquare$

vlastnosti rekurzivních množin

Lemma 7.5

Nechť $A, B \subseteq \mathbb{N}^k$ jsou rekurzivní množiny. Pak i množiny $\overline{A}$, $A \cup B$ a $A \cap B$ jsou rekurzivní.

Důkaz:

$\blacksquare$

rekurzivně spočetné množiny

Definice 7.1 (rekurzivně spočetná množina)

Množina $B \subseteq \mathbb{N}$ je rekurzivně spočetná, právě když $B = \emptyset$ nebo existuje totálně vyčíslitelná funkce $f : \mathbb{N} \to \mathbb{N}$ taková, že $B = range(f)$. Funkce f se nazývá numerující funkce pro B.

- rekurzivně spočetné množině se také říká částečně rozhodnutelná, rekurzivně vyčíslitelná nebo jen r.e. (z anglického recursively enumerable).
- definici lze rozšířit na množiny $B \subseteq \mathbb{N}^k$

vztahy rekurzivních a r.e. množin

Věta 7.6

Každá rekurzivní množina $A \subseteq \mathbb{N}$ je také rekurzivně spočetná.

Důkaz:

■

vztahy rekurzivních a r.e. množin

Věta 7.7

1. *Existuje množina $A \subseteq \mathbb{N}$, která není rekurzivní.*
2. *Existuje množina $B \subseteq \mathbb{N}$, která není r.e.*

Důkaz: (pomocí mohutnosti) Rekurzivních i r.e. množin je spočetně mnoho, ale $\mathbb{N}$ má nespočetně mnoho podmnožin.

(diagonalizací) $A = \{i \in \mathbb{N} \mid \varphi_i(i) \neq 1\}$

$B = \{i \in \mathbb{N} \mid i \notin range(\varphi_i)\}$

■

vztahy rekurzivních a r.e. množin

Věta 7.8

Množina $A \subseteq \mathbb{N}$ je rekurzivní, právě když A i $\overline{A}$ jsou r.e.

Důkaz:

$\Longrightarrow$ je-li A rekurzivní, pak je rekurzivní i $\overline{A}$ a každá rekurzivní množina je také r.e.

$\Longleftarrow$

- je-li $A = \emptyset$ nebo $\overline{A} = \emptyset$, pak A je rekurzivní
- nechť $A \neq \emptyset \neq \overline{A}$ jsou r.e., pak $A = \mathit{range}(f)$ a $\overline{A} = \mathit{range}(g)$ pro nějaké totálně vyčíslitelné funkce $f, g : \mathbb{N} \to \mathbb{N}$
- platí $\mathit{range}(f) \cap \mathit{range}(g) = \emptyset$ a $\mathit{range}(f) \cup \mathit{range}(g) = \mathbb{N}$
- charakteristickou funkci $\chi_A(x)$ počítáme takto:

  1. počítáme $f(0), g(0), f(1), g(1), \ldots$ dokud nedostaneme x
  2. pokud $x = f(n)$ pro nějaké n, pak vrátíme 1
  3. pokud $x = g(n)$ pro nějaké n, pak vrátíme 0

- χ_A je vyčíslitelná, tedy A je rekurzivní

$\blacksquare$

funkce Step counter

Lemma 7.9

Funkce

$$Sc(x,y,z) = \begin{cases} 1 & \textit{jestliže program } P_x \textit{ zastaví pro vstup } y \\ & \textit{během } z \textit{ kroků} \\ 0 & \textit{jinak} \end{cases}$$

je totálně vyčíslitelná.

Důkaz: interpreter z důkazu věty o numeraci rozšíříme o počítání instrukcí ■