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 (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

$\blacksquare$

využití věty o parametrizaci

Lemma

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 existuje tot. vyčíslitelná funkce 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 tot. vyčíslitelná ■

translační lemma

Důsledek (translační lemma)

Ke každé vyčíslitené funkci $f : \mathbb{N}^2 \to \mathbb{N}$ existuje tot. 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 tot. vyčíslitelná funkce 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 tot. vyčíslitelná ■

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 tot. 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 (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

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

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 jako 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 tot. 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 tot. 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 tot. 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 (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

Nechť ψ *je totální numerace všech unárních tot. 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

Neexistuje přípustná totální numerace všech totálních vyčíslitelných funkcí.

rekurzivní množiny

Definice (rekurzivní množina)

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

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

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

Tvrzení

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

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 (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 $B \subseteq \mathbb{N}^k$

Věta

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

Důkaz:

$\blacksquare$

vztahy rekurzivních a r.e. množin

Věta

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

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 $A = range(f)$ a $\overline{A} = range(g)$ pro nějaké totálně vyčíslitelné funkce $f, g : \mathbb{N} \to \mathbb{N}$
- platí $range(f) \cap range(g) = \emptyset$ a $range(f) \cup range(g) = \mathbb{N}$
- 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 ■

funkce Step counter

Lemma

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 ■

programy jako generátory

- rozšíříme jazyk while-programů o příkaz $output(x_i)$

Tvrzení

Množina A je r.e., právě když existuje program P (bez vstupních proměnných), který pomocí instrukce output během svého (potenciálně nekonečného) běhu dá na výstup právě všechny prvky A.

Důkaz:

$\Longleftarrow$

- pokud program P na výstup nic nedá, pak $A = \emptyset$ je r.e.
- nechť program generuje množinu výstupů $A \neq \emptyset$
- nechť $a \in A$, pak $A = range(f)$ pro

$$f(x) = \begin{cases} y & \text{pokud } P \text{ dá v } x\text{-tém kroku na výstup } y \\ a & \text{jinak} \end{cases}$$

- f je totálně vyčíslitelná

programy jako generátory

$\Longrightarrow$

- pro $A = \emptyset$ zřejmé
- nechť $A = range(f)$ pro tot. vyčíslitelnou funkci $f : \mathbb{N} \to \mathbb{N}$
- nechť f je počítána programem P_e
- pak A je generována tímto programem

begin
  $n := 0$;
  while *true* **do** **begin**
    $x := \pi_1(n)$;
    $y := \pi_2(n)$;
    if $Sc(e, x, y) = 1$ **then** **begin** $P_e(x)$; $output(x_1)$ **end**;
    $n := n + 1$;
  end
end

$\blacksquare$

množiny a problémy

Problém rozhodnout, zda dané x má vlastnost V ztotožníme s množinou $\{x \mid x \text{ má vlastnost } V\}$.

Příklad: problém, zda n je prvočíslo, ztotožníme s množinou

$$\{n \in \mathbb{N} \mid n \text{ je prvočíslo}\}$$

Terminologie

Nechť M je množina odpovídající danému problému. Tento problém je

- rozhodnutelný, právě když M je rekurzivní,
- částečně rozhodnutelný (semirozhodnutelný), právě když M je r.e.

Problém, který není rozhodnutelný, se nazývá nerozhodnutelný.

problém zastavení

Problém zastavení, tedy problém, zda program P_i zastaví na vstupu i, ztotožníme s množinou

$$\begin{aligned} K &= \{i \in \mathbb{N} \mid P_i \text{ zastaví nad vstupu } i\} \\ &= \{i \in \mathbb{N} \mid \varphi_i(i) \text{ je definováno}\}. \end{aligned}$$

Dříve jsme dokázali, že charakteristická funkce

$$\chi_K(i) = f(i) = \begin{cases} 1 & \text{jestliže } \varphi_i(i) \text{ je definováno} \\ 0 & \text{jestliže } \varphi_i(i) \text{ není definováno} \end{cases}$$

není vyčíslitelná. Proto K není rekurzivní a tedy problém zastavení je nerozhodnutelný.

problém zastavení

Věta

Množina $K = \{i \mid \varphi_i(i) \text{ je definováno}\}$ *je rekurzivně spočetná.*

Důkaz: Množina K je generována programem

begin
  $n := 0;$
  while *true* **do** **begin**
    $x := \pi_1(n);$
    $y := \pi_2(n);$
    if $Sc(x, x, y) = 1$ **then** $output(x);$
    $n := n + 1;$
  end
end

∎

Proto problém zastavení je částečně rozhodnutelný.

problém zastavení

Věta

Množina $\overline{K} = \{i \mid \varphi_i(i) = \bot\}$ *není rekurzivně spočetná.*

Důkaz:

- množina K je rekurzivně spočetná
- pokud by $\overline{K}$ byla také rekurzivně spočetná, tak by K bylo rekurzivní, což není ∎

Shrnutí:

rekurzivně spočetné množiny v rostoucím pořádku

Definice

Množina $A \subseteq \mathbb{N}$ je rekurzivně spočetná v rostoucím pořádku, právě když má rostoucí numerující funkci.

Lemma

Nekonečná množina $A \subseteq \mathbb{N}$ je rekurzivní, právě když je rekurzivně spočetná v rostoucím pořádku.

Důkaz:

$\Longleftarrow$

- nechť $A = range(f)$ pro rostoucí tot. vyčíslitelnou funkci f
- χ_A je počítána programem

<u>**begin**</u> $n := 0$;
   <u>**while**</u> $f(n) < x_1$ <u>**do**</u> $n := n + 1$;
   <u>**if**</u> $f(n) = x_1$ <u>**then**</u> $x_1 := 1$ <u>**else**</u> $x_1 := 0$
<u>**end**</u>

rekurzivně spočetné množiny v rostoucím pořádku

$\Longrightarrow$

- A je nekonečná a rekurzivní, tedy χ_A je vyčíslitelná
- A je generována v rostoucím pořádku programem

begin
  $n := 0$;
  while *true* **do** **begin**
    if $\chi_A(n) = 1$ **then** $output(n)$;
    $n := n + 1$;
  end
end

- funkce $f(i)$ vracející i-tý prvek z generovaného seznamu je totálně vyčíslitelná
- přitom f je rostoucí a $A = range(f)$
- tedy f je rekurzivně spočetná v rostoucím pořádku ■

rekurzivně spočetné množiny v rostoucím pořádku

Důsledek

Každá nekonečná r.e. množina A má nekonečnou rekurzivní podmnožinu B.

Důkaz:

- nechť f je numerující funkce pro A
- uvažme podmnožinu $B \subseteq A$, kterou generuje program

```
begin
   n := 0;  m := 0;
   while true do begin
            if f(n) > m then begin m := f(n);  output(m) end;
            n := n + 1;
   end
end
```

- B je nekonečná a generovaná v rostoucím pořádku
- tedy B je r.e. v rostoucím pořádku a tudíž rekurzivní ∎