IB107 Vyčíslitelnost a složitost

opakování, redukce, Turingovy stroje a redukce, Postův korespondenční problém

Jan Strejček

Fakulta informatiky
Masarykova univerzita

vyčíslitelnost funkcí

- funkce $f : \mathbb{N}^k \to \mathbb{N}$ je vyčíslitelná když

- funkce f je totálně vyčíslitelná, je-li vyčíslitelná a $dom(f) = \mathbb{N}^k$

numerace vyčíslitelných funkcí

- pro každé $k > 0$ lze všechny vyčíslitelné funkce typu $f^{(k)} : \mathbb{N}^k \to \mathbb{N}$ "očíslovat" jako

$$\varphi_0^{(k)}, \varphi_1^{(k)}, \varphi_2^{(k)}, \dots$$

tak, aby platily

1. věta o numeraci

2. věta o parametrizaci

vyčíslitelné vlastnosti množin

- množina $A \subseteq \mathbb{N}^k$ je rekurzivní, je-li její charakteristická funkce $\chi_A : \mathbb{N}^k \to \mathbb{N}$ vyčíslitelná, kde

- množina $A \subseteq \mathbb{N}^k$ je rekurzivně spočetná (r.e.), pokud $A = dom(f)$ pro nějakou vyčíslitelnou funkci $f : \mathbb{N}^k \to \mathbb{N}$

- problém zastavení K

- doplněk problému zastavení (problém nezastavení) $\overline{K}$

numerace r.e. množin a uzávěrové vlastnosti

- pro každé $k > 0$ lze všechny r.e. podmnožiny $\mathbb{N}^k$ "očíslovat" jako

$$W_0^{(k)}, W_1^{(k)}, W_2^{(k)}, \ldots$$

	třída rek. množin	**třída r.e. množin**
$\cup, \cap$ aplikované na relace stejné arity		
doplněk		
kartézský součin $\times$		
projekce		
řez		
vzor při tot. vyčíslitelném zobrazení		
vzor při vyčíslitelném zobrazení		
obraz při (tot.) vyčíslitelném zobrazení		

další vlastnosti r.e. množin

- věta o projekci

- 1. Riceova věta

- 2. a 3. Riceova věta

množiny a problémy: přehled terminologie

problém	**množina**
Má objekt O vlastnost V?	$A = \{\langle O \rangle \mid O \text{ má vlastnost } V\} \subseteq \mathbb{N}$
je rozhodnutelný	A je rekurzivní, tj. χ_A je totálně vyčíslitelná, tj. $\exists$ program rozhodující $x \overset{?}{\in} A$
je nerozhodnutelný	A není rekurzivní
je částečně rozhodnutelný neboli semirozhodnutelný	A je rekurzivně spočetná, tj. $A = dom(f)$ pro nějakou vyč. fci f, tj. $\exists$ program, který zastaví jen na vstupech z A, tj. $\exists$ program, který generuje A
je rozhodnutelný $\iff$ je částečně rozhodnutelný a jeho doplněk taky	A je rekurzivní $\iff$ A je rekurzivně spočetná a její doplněk taky

intuice pro redukci

$A = \{n \in \mathbb{N} \mid n \text{ je dělitelné } 13\}$

$B = \{n \in \mathbb{N} \mid n \text{ je dělitelné } 26\}$

intuice pro redukci

$K = \{i \in \mathbb{N} \mid \varphi_i(i) \text{ je definováno}\}$

$B = \{n \in \mathbb{N} \mid n \text{ je dělitelné } 26\}$

redukce

Definice (m-redukce, m-ekvivalence)

Nechť $A, B \subseteq \mathbb{N}$. Řekneme, že A se m-redukuje na B, píšeme $A \leq_m B$, právě když existuje totálně vyčíslitelná funkce $f : \mathbb{N} \to \mathbb{N}$ taková, že

$$x \in A \iff f(x) \in B.$$

Funkci f nazveme redukcí A na B.

A a B jsou m-ekvivalentní, psáno $A \equiv_m B$, pokud $A \leq_m B$ a $B \leq_m A$.

Platí $A \leq_m B \implies \overline{A} \leq_m \overline{B}$.

Platí $A \leq_m B$ a $B \leq_m C \implies A \leq_m C$ (tj. $\leq_m$ je tranzitivní).

příklad redukce

$K = \{i \mid \varphi_i(i) \text{ je definováno}\}$
$J = \{i \mid \varphi_i(i) = 1\}$

$K \leq_m J$:

příklad redukce

$K = \{i \mid \varphi_i(i) \text{ je definováno}\}$
$J = \{i \mid \varphi_i(i) = 1\}$

$J \leq_m K$:

redukce a rozhodnutelnost

Věta

Nechť $A \leq_m B$.

1. *B je rekurzivní $\implies$ A je rekurzivní.*
2. *B je rekurzivně spočetná $\implies$ A je rekurzivně spočetná.*

Důkaz: $A \leq_m B$, tedy existuje tot. vyčíslitelná funkce f splňující

$$x \in A \iff f(x) \in B$$

1. B je rekurzivní, tedy χ_B je tot. vyčíslitelná

2. B je r.e., tedy $B = dom(g)$ pro nějakou vyčíslitelnou funkci g

■

redukce a rozhodnutelnost

Důsledek

Nechť $A \leq_m B$*.*

1. *A není rekurzivní* $\implies$ *B není rekurzivní.*
2. *A není rekurzivně spočetná* $\implies$ *B není rekurzivně spočetná.*

Důsledek

Nechť $A \equiv_m B$*.*

1. *A je rekurzivní* $\iff$ *B je rekurzivní.*
2. *A je rekurzivně spočetná* $\iff$ *B je rekurzivně spočetná.*

typické aplikace

- důkaz (částečné) rozhodnutelnosti A

- důkaz nerozhodnutelnosti B

r.e. množiny a K

Věta

Je-li $A \subseteq \mathbb{N}$ r.e., pak $A \leq_m K$.

Důkaz: Nechť g je vyčíslitelná funkce splňující $A = dom(g)$.

```
begin
   y := g(i);
   x1 := 1
end
```

■

těžká a úplná množina

Definice (těžká a úplná množina)

Nechť $\mathbb{C}$ *je třída podmnožin množiny* $\mathbb{N}$ *a* $A \subseteq \mathbb{N}$*. Řekneme, že* A *je* $\mathbb{C}$*-těžká, právě když pro každou množinu* $B \in \mathbb{C}$ *platí* $B \leq_m A$*. Je-li navíc* $A \in \mathbb{C}$*, pak* A *nazýváme* $\mathbb{C}$*-úplná nebo úplná v třídě* $\mathbb{C}$*.*

Důsledek

Množina K *je úplná v třídě všech rekurzivně spočetných množin.*

Turingův stroj

Definice (Turingův stroj)

(Deterministický) Turingův stroj (Turing Machine, TM) je devítice $\mathcal{M} = (Q, \Sigma, \Gamma, \triangleright, \sqcup, \delta, q_0, q_{acc}, q_{rej})$, kde

- *Q je konečná množina, jejíž prvky nazýváme stavy,*
- *Σ je konečná množina, tzv. vstupní abeceda,*
- *Γ je konečná množina, tzv. pracovní abeceda, $\Sigma \subseteq \Gamma$,*
- *$\triangleright \in \Gamma \setminus \Sigma$ je levá koncová značka,*
- *$\sqcup \in \Gamma \setminus \Sigma$ je symbol označující prázdné políčko,*
- *$\delta : (Q \setminus \{q_{acc}, q_{rej}\}) \times \Gamma \to Q \times \Gamma \times \{L, R\}$ je totální přechodová funkce,*
- *$q_0 \in Q$ je počáteční stav,*
- *$q_{acc} \in Q$ je akceptující stav,*
- *$q_{rej} \in Q$ je zamítající stav.*

Turingův stroj

Dále požadujeme, aby pro každé $q \in Q \smallsetminus \{q_{acc}, q_{rej}\}$ existoval $p \in Q$ takový, že $\delta(q, \rhd) = (p, \rhd, R)$ (tj. nelze sjet hlavou z pásky ani přepsat $\rhd$).

Notace: $\sqcup^\omega = \sqcup\sqcup\sqcup\sqcup\sqcup\sqcup\ldots$

Definice (konfigurace Turingova stroje)

Konfigurace Turingova stroje je trojice $(q, z, n) \in Q \times \{y\sqcup^\omega \mid y \in \Gamma^*\} \times \mathbb{N}_0$, *kde*

- q *je stav,*
- $y\sqcup^\omega$ *je obsah pásky,*
- n *značí pozici hlavy na pásce.*

Počáteční konfigurace pro vstup $w \in \Sigma^*$ *je trojice* $(q_0, \rhd w\sqcup^\omega, 0)$.

Akceptující konfigurace je každá trojice tvaru (q_{acc}, z, n).

Zamítající konfigurace je každá trojice tvaru (q_{rej}, z, n).

krok výpočtu Turingova stroje

Definice (krok výpočtu)

Na množině všech konfigurací stroje $\mathcal{M}$ definujeme binární relaci

krok výpočtu $\vdash_{\mathcal{M}}$ *jako*

$$(p, z, n) \quad \vdash_{\mathcal{M}} \quad \begin{cases} (q, z', n+1) & \text{pokud } \delta(p, z_n) = (q, b, R) \\ (q, z', n-1) & \text{pokud } \delta(p, z_n) = (q, b, L) \end{cases}$$

kde z_n je n-tý znak z (příčemž z_0 je nejlevější znak z) a z' vznikl ze z nahrazením znaku z_n znakem b.

výpočet Turingova stroje

Definice (výpočet)

Výpočet TM $\mathcal{M}$ na vstupu w je maximální (konečná nebo nekonečná) posloupnost konfigurací $K_0, K_1, K_2, \ldots$, kde K_0 je počáteční konfigurace pro w a $K_i \vdash_{\mathcal{M}} K_{i+1}$ pro všechna $i \geq 0$.

- stroj $\mathcal{M}$ akceptuje slovo w, právě když výpočet $\mathcal{M}$ na w je konečný a jeho poslední konfigurace je akceptující
- stroj $\mathcal{M}$ zamítá slovo w, právě když výpočet $\mathcal{M}$ na w je konečný a jeho poslední konfigurace je zamítající
- stroj $\mathcal{M}$ pro vstup w cyklí, právě když výpočet $\mathcal{M}$ na w je nekonečný
- jazyk akceptovaný strojem $\mathcal{M}$ definujeme jako množinu $L(\mathcal{M}) = \{w \in \Sigma^* \mid \mathcal{M} \text{ akceptuje } w\}$

vícepáskový Turingův stroj

Věta

Pro každý vícepáskový Turingův stroj existuje (jednopáskový) Turingův stroj akceptující stejný jazyk.

nedeterministický Turingův stroj

Definice (nedeterministický Turingův stroj)

Nedeterministický Turingův stroj $\mathcal{M}$ *je definován stejně jako det. TM s výjimkou přechodové funkce* δ*, která je definována jako totální funkce* $\delta : (Q \smallsetminus \{q_{acc}, q_{rej}\}) \times \Gamma \to 2^{Q \times \Gamma \times \{L,R\}}$.

- většina pojmů se definuje stejně jako u deterministického TM
- v definici kroku výpočtu $\underset{\mathcal{M}}{\vdash}$ píšeme $(q, b, R) \in \delta(p, z_n)$ namísto $\delta(p, z_n) = (q, b, R)$ a podobně pro (q, b, L)
- stroj $\mathcal{M}$ akceptuje slovo w, právě když existuje výpočet $\mathcal{M}$ na w, který je konečný a jeho poslední konfigurace je akceptující

Věta

Pro každý nedeterministický TM existuje deterministický TM akceptující stejný jazyk.

Turingovy stroje a třídy jazyků

Věta

Jazyk L je rekurzivně spočetný neboli r.e. (tj. generovaný gramatikou typu 0) $\iff$ L je akceptovaný nějakým Turingovým strojem.

Definice (úplný Turingův stroj, rekurzivní jazyk)

Turingův stroj se nazývá úplný, je-li každý jeho výpočet konečný (akceptující nebo zamítající). Jazyk se nazývá rekurzivní, pokud je akceptovaný nějakým úplným Turingovým strojem.

Terminologie

- (obecný) TM $\mathcal{M}$ akceptuje/rozpoznává/přijímá jazyk $L(\mathcal{M})$
- úplný TM $\mathcal{M}$ rozhoduje jazyk $L(\mathcal{M})$

uzávěrové vlastnosti rekurzivních a r.e. jazyků

	třída rek. jazyků	**třída r.e. jazyků**
$\cup, \cap$		
zřetězení, mocniny		
(pozitivní) iterace		
doplněk		

Věta

Jazyk L je rekurzivní, právě když jsou jazyky L a $\overline{L}$ r.e.

kódování a univerzální Turingův stroj

- každý TM $\mathcal{M}$ lze zakódovat do řetězce $\langle \mathcal{M} \rangle \in \{0, 1\}^*$
- každé slovo w lze zakódovat do řetězce $\langle w \rangle \in \{0, 1\}^*$
- dvojice $(\mathcal{M}, w)$ lze zakódovat jako $\langle \mathcal{M}, w \rangle = \langle \mathcal{M} \rangle \# \langle w \rangle$

Věta

Existuje univerzální Turingův stroj $\mathcal{U}$, který dokáže simulovat libovolný zadaný TM na zadaném vstupu w:

$$\mathcal{U} \text{ akceptuje } \langle \mathcal{M}, w \rangle \iff \mathcal{M} \text{ akceptuje } w$$

problém zastavení (halting problem)

Definice (problém zastavení)

Problém zastavení je problém rozhodnout, zda daný TM $\mathcal{M}$ má na daném slově w nad jeho vstupní abecedou konečný výpočet. Problém ztotožníme s jazykem

$$HALT = \{\langle \mathcal{M}, w \rangle \mid \mathcal{M} \text{ je TM a výpočet } \mathcal{M} \text{ na } w \text{ je konečný}\}.$$

Věta

Problém zastavení je částečně rozhodnutelný.

Věta

Problém zastavení je nerozhodnutelný.

Turingovy stroje a funkce

- obsah pásky jednopáskového deterministického Turingova stroje po skončení výpočtu lze vnímat jako jeho výstup
- pokud stroj $\mathcal{M}$ na vstupu w zastaví s obsahem pásky $\triangleright y \sqcup^\omega$ (kde y nekončí na $\sqcup$), pak y je jeho výstupem značeným $\mathcal{M}(w)$

Definice ((totálně) vyčíslitelná funkce)

Funkce $f : \Sigma^* \to \Phi^*$ je vyčíslitelná, pokud existuje TM $\mathcal{M}$, který zastaví právě na vstupech z $dom(f)$ a pro každé slovo $w \in dom(f)$ platí $\mathcal{M}(w) = f(w)$.

Funkce je totálně vyčíslitelná, pokud je vyčíslitelná a totální.

redukce jazyků

Definice (m-redukce)

Nechť $A \subseteq \Sigma^*$ a $B \subseteq \Phi^*$ jsou jazyky. Řekneme, že A se m-redukuje na B, píšeme $A \leq_m B$, právě když existuje totálně vyčíslitelná funkce $f : \Sigma^* \to \Phi^*$ taková, že

$$w \in A \iff f(w) \in B.$$

Funkci f nazveme redukcí A na B.

Věta

Nechť $A \subseteq \Sigma^*$ a $B \subseteq \Phi^*$ jsou jazyky a $A \leq_m B$.

1. *B je rekurzivní $\implies$ A je rekurzivní.*
2. *B je rekurzivně spočetný $\implies$ A je rekurzivně spočetný.*

problém akceptování

Definice (problém akceptování)

Problém akceptování je problém rozhodnout, zda daný TM $\mathcal{M}$ akceptuje dané slovo w nad jeho vstupní abecedou. Problém ztotožníme s jazykem

$$ACC = \{\langle \mathcal{M}, w \rangle \mid \mathcal{M} \text{ je TM a } \mathcal{M} \text{ akceptuje } w\}.$$

Věta

Problém akceptování je nerozhodnutelný.

Důkaz: $HALT \leq_m ACC$

nerozhodnutelnost problému akceptování

HALT $\leq_m$ *ACC*:

$$\begin{aligned} HALT &= \{\langle \mathcal{M}, w\rangle \mid \mathcal{M} \text{ je TM a výpočet } \mathcal{M} \text{ na } w \text{ je konečný}\} \\ ACC &= \{\langle \mathcal{M}, w\rangle \mid \mathcal{M} \text{ je TM a } \mathcal{M} \text{ akceptuje } w\} \end{aligned}$$

■

Platí také $ACC \leq_m HALT$ a tudíž $HALT \equiv_m ACC$.

Postův systém

Definice (Postův systém)

Postův systém P nad ebecedou Σ je konečná množina dvojic

$$P = \left\{ \begin{bmatrix} \dfrac{\alpha_i}{\beta_i} \end{bmatrix} \mid \alpha_i, \beta_i \in \Sigma^*, 1 \leq i \leq n \right\}.$$

Řešením systému P je konečná neprázdná posloupnost přirozených čísel $i_1, i_2, \ldots, i_k$ taková, že $1 \leq i_j \leq n$ a

$$\alpha_{i_1} \alpha_{i_2} \ldots \alpha_{i_k} = \beta_{i_1} \beta_{i_2} \ldots \beta_{i_k}.$$

Příklad:

$$P = \left\{ \begin{bmatrix} \dfrac{c}{abc} \end{bmatrix}, \begin{bmatrix} \dfrac{ca}{b} \end{bmatrix}, \begin{bmatrix} \dfrac{a}{ca} \end{bmatrix}, \begin{bmatrix} \dfrac{ab}{a} \end{bmatrix} \right\}$$

Postův korespondenční problém (PCP)

Definice (Postův korespondenční problém (PCP))

Postův korespondenční problém (PCP) je problém rozhodnout, zda má Postův systém P nějaké řešení.

$$PCP = \{\langle P\rangle \mid P \text{ je Postův systém, který má nějaké řešení}\}$$

Definice (iniciální Postův korespondenční problém (inPCP))

Iniciální Postův korespondenční problém (inPCP) je problém rozhodnout, zda má Postův systém P řešení začínající číslem 1.

$$inPCP = \{\langle P\rangle \mid P \text{ je Postův systém a má řešení začínající číslem } 1\}$$

nerozhodnutelnost PCP

Věta

PCP není rozhodnutelný.

Důkaz: Postupně ukážeme $ACC \leq_m inPCP \leq_m PCP$.

$inPCP \leq_m PCP$:

Zkonstruujeme totálně vyčíslitelnou funkci f tak, že $f(\langle P \rangle) = \langle P' \rangle$, kde P' má řešení $\iff$ P má řešení začínající 1.

$$P = \left\{ \left[\frac{ba}{b}\right], \left[\frac{b}{bb}\right], \left[\frac{b}{abb}\right], \left[\frac{bab}{a}\right] \right\}$$

nerozhodnutelnost PCP

$ACC \leq_m inPCP$:

$\#q_0 \triangleright w \# \triangleright q' w \# \;\; \ldots \;\; \# \triangleright \ldots q_{acc} \ldots \#$