Nerozhodnutelne problemy, redukce

13 October, 2020 07:52

<u>Def.:</u> • $L \subseteq \Sigma^*$, L je (Turingovsky) <u>rozhodnutelný</u>, pokud existuje TS M, který ho rozhoduje, tedy M se zastaví na všech vstupech a $L(M) = L$.

• $L \subseteq \Sigma^*$, L je (Turingovsky) <u>vyčíslitelný</u>, pokud existuje TS M taký, že pro každý vstup $w \in \Sigma^*$, M se zastaví na w právě tehdy, když $w \in L$.

<u>Pozorování:</u> L Turingovsky rozhodnutelný $\Rightarrow$ L Turingovsky vyčíslitelný.

<u>Pozorování:</u> L je vyčíslitelný $\Leftrightarrow$ existuje enumerator pro L.

<u>Dk.:</u> "$\Leftarrow$" na vstupu $\underline{w}$, pusť enumerátor pro L, čekej, zda někdy vytiskne $\underline{w}$. Jakmile ho vytiskne, zastav se.

"$\Rightarrow$" Nechť $w_0 = \varepsilon$, $w_1 = 0$, $w_2 = 1$, $w_3 = 00$, ... jsou řetězy v lexikografickém uspořádání nad Σ. Nechť M je TS vyčíslující L.

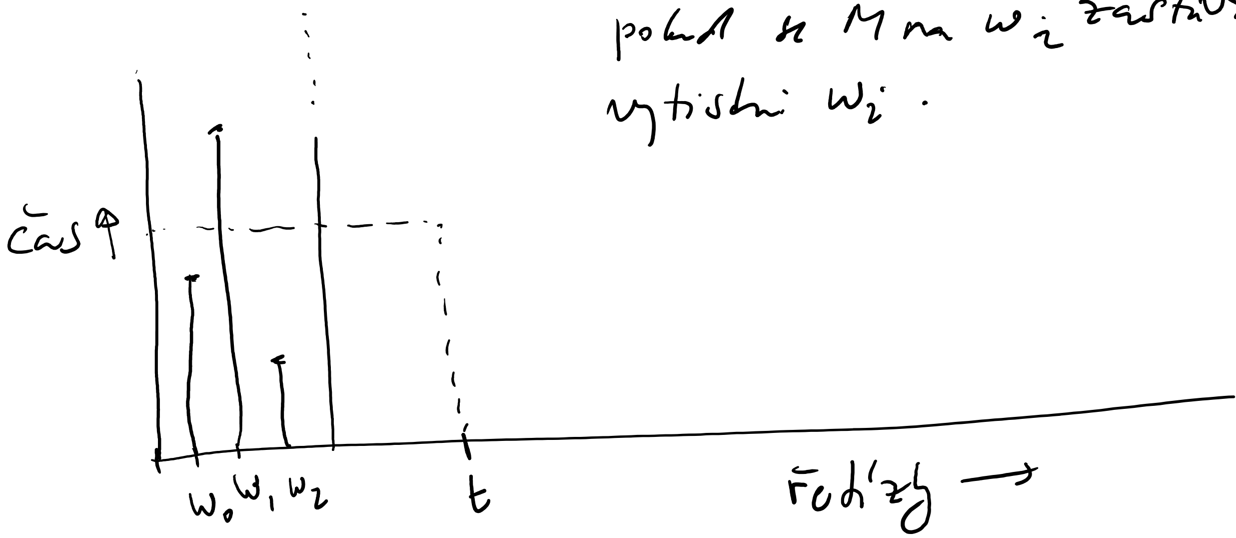
• Σ binární

Enumerátor pracuje takto:

Pro $t = 1, 2, \dots$

Pro $i = 0, 1, 2, \dots, t$

spusť M na w_i po t krocích,
pokud se M na w_i zastaví,
vytiskni w_i.



Tvrzení: $\exists L \subseteq \Sigma^*$, L není vyčíslitelný.

Dk: Každý TS lze popsat konečným řetězcem nad abecedou $\Sigma = \{0, 1\}$

$\Rightarrow$ # TS je spočetný.

Počet různých podmnožin Σ^* je nespočetný.

$\Rightarrow \exists L$ není vyčíslitelný $\boxtimes$

Def: $A_{TM} = \{ (\langle M \rangle, w)$, $\langle M \rangle$ je popis TS a w vstup a M přijímá $w \}$

Pozorování: A_{TM} je vyčíslitelný.

Dk: Simuluj M na w a zastav se, pokud M přijme w. $\boxtimes$

Věta: A_{TM} není rozhodnutelný

Dk: Sporem. Předpokládejme, že $\exists$ TS H, který se zastaví na všech vstupech a $L(H) = A_{TM}$

S použitím H zkonstruujeme následující TS D:

<u>D na vstupu $\langle M \rangle$:</u>

- vytvoří $(\langle M \rangle, \langle M \rangle)$
- spustí H na $(\langle M \rangle, \langle M \rangle)$
- pokud H přijme, D odmítne $\langle M \rangle$.
  pokud H odmítne, D přijme $\langle M \rangle$.

Co udělá D na vstupu $\langle D \rangle$?

$\hookrightarrow$ spor

$\boxed{QED}$

<u>Redukce</u> -- převedení jednoho problému na jiný.

(Řešení jednoho problému pomocí jiného.)

<u>Př:</u> 1) Matematik vaří čaj a dostane prázdnou konvici

2) — " — plnou konvici.

2) převede na 1) tím, že konvici vylije.

- $_M = \{ (\langle M \rangle, w), \ \langle M \rangle$ je TS, M se zastaví na $w \}$.

<u>Věta:</u> $HALT_{TM}$ není rozhodnutelný, ale je vyčíslitelný.

<u>Dk</u>: • vyčíslitelnost ... triv.

• (ne)rozhodnutelnost:

<u>Sporem:</u> nechť H rozhoduje $HALT_{TM}$, vyřešíme A_{TM} pomocí H.

alg pro A_{TM}:

- na vstupu $(\langle M \rangle, w)$
  - spusť H na $(\langle M \rangle, w)$

    pokud H přijme, simuluj M na w a udělej, co udělá.

    pokud H nepřijme, odmítni.

pokud se H vždy zastaví a dává správný výsledek, zastaví se vždy i tento alg. pro A_{TM} a dá správný výsledek. Spor s nerozhodnutelností A_{TM}. ∎

→ (vyřešili jsme $HALT_{TM}$ pomocí A_{TM})

- $E_{TM} = \{ \langle M \rangle, \langle M \rangle \text{ je TS a } L(M) = \emptyset \}$

Tvrzení: E_{TM} není rozhodnutelný.

Dk: převedeme A_{TM} na E_{TM}.

sporem. Nechť H rozhoduje E_{TM}

Alg pro A_{TM}:

- na vstupu $(\langle M \rangle, w)$:
  - sestroj TS M' takový, že na libovolném vstupu simuluje M na w a přijme, pokud M přijme w.
  - spusť H na $\langle M' \rangle$, pokud H přijme $\langle M' \rangle$, přijmi, jinak zamítni.

→ Takový alg. nemůže existovat

$\langle M \rangle$, přijmi, zamítni

$\Rightarrow$ Tato alg. nemůže existovat $\boxtimes$

E_{TM} není rozhodnutelný, $\overline{E_{TM}} = \Sigma^* \setminus E_{TM}$ je vyčíslitelný

- $EQ_{TM} = \{ (\langle M_1 \rangle, \langle M_2 \rangle)$, M_1 a M_2 jsou TS a $L(M_1) = L(M_2) \}$

Tvrzení: EQ_{TM} není rozhodnutelný.

E_{TM} zredukujeme na EQ_{TM}

alg pro E_{TM}:

- na vstupu $\langle M \rangle$, zkonstruujeme $M_\emptyset$ t.ž. $L(M_\emptyset) = \emptyset$

zeptáme se, zda $(\langle M \rangle, \langle M_\emptyset \rangle) \in EQ_{TM}$

$\boxtimes$

Otázka: Je $\overline{EQ_{TM}}$ vyčíslitelný?

Odpověď: není.

Věta: Nechť $L \subseteq \Sigma^*$ a $\overline{L} = \Sigma^* \setminus L$.

L je rozhodnutelný $\Leftrightarrow$ L i $\overline{L}$ jsou vyčíslitelné.

Dk: "$\Rightarrow$" triv. (z q_{acc} / q_{rej} přejdi do nekonečné smyčky)

"$\Leftarrow$" L je vyčíslitelný pomocí TS M_1

$\overline{L}$ je — " — TS M_2

<u>rozhodovací TS pro L:</u>

na vstupu w:

- simuluj paralelně (souběžně) M_1 i M_2 na w.
  (střídej kroky na nezávislých kopiích w.)
- pokud se M_1 zastaví → přijmi
  pokud se M_2 zastaví → odmítni.

jeden z M_1 a M_2 se musí na w zastavit.

⇒ alg. rozhoduje L $\boxed{}$

- A_{LBA}, E_{LBA}

- Postův korespondenční problém (Post Correspondence problem)

<u>Př</u>: $\left\{ \begin{bmatrix} a \\ ab \end{bmatrix}, \begin{bmatrix} b \\ ca \end{bmatrix}, \begin{bmatrix} ca \\ a \end{bmatrix}, \begin{bmatrix} abc \\ c \end{bmatrix} \right\}$ ← "kostičky"

$$\left| \begin{matrix} a \mid b \mid ca \mid a \mid abc \\ ab \mid ca \mid a \mid ab \mid c \end{matrix} \right|$$

lze sestavit stejné slovo dole i nahoře.

<u>Otázka</u>: Dán seznam kostiček a výchozí kostička, lze sestavit kostičky tak, aby dole i nahoře bylo stejné slovo?

→ Algoritmicky nerozhodnutelné

↳ <u>Dk</u>.: A_{TM} zredukujeme na Postův koresp. problém

$$\begin{bmatrix} \# \\ \# q_0 w_1 w_2 \dots w_n \# \end{bmatrix}$$ výchozí kostička

δ .. přechodová fce M — krok výpočtu

δ ... přechodová fce M krok výpočtu

Γ ... pracovní abeceda

$\forall a,b,c \in \Gamma$
$\forall q,r \in Q$
$q \neq q_{rej}$

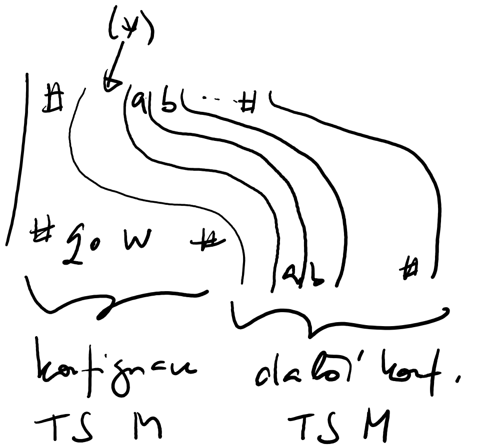
$\delta(q,a) = (r,b,R) \Rightarrow \begin{bmatrix} q & a \\ b & r \end{bmatrix}$ kostička (*)

$\delta(q,a) = (r,b,L) \Rightarrow \begin{bmatrix} c & q & a \\ r & c & b \end{bmatrix}$ kostička (**)

$\forall a \in \Gamma$ $\begin{bmatrix} a \\ a \end{bmatrix}$ kostička

$\begin{bmatrix} \# \\ \# \end{bmatrix}$ kostičky

} kopíruje shora dolů



. . .

$\forall a \in \Gamma$ $\begin{bmatrix} a & q_{acc} \\ & q_{acc} \end{bmatrix}$ $\begin{bmatrix} q_{acc} & a \\ q_{acc} & \end{bmatrix}$ požere obsah pásky

$\begin{bmatrix} q_{acc} & \# & \# \\ & & \# \end{bmatrix}$ . . . . $\# \; q_{acc} \; \# \; \#$ / $\# \; q_{acc} \; \# \; \#$ ukončí

$\boxtimes$

- Lze modifikovat tak, že se nemusí začínat s první kostičkou.

Redukce many-one

- $F : \Sigma^* \to \Sigma^*$, F je spočitatelná, pokud existuje

TS M, který se zastaví na každém vstupu w a na konci výpočtu je na jeho pásce zapsáno $f(w)$.

Př: 1) $f(m+n) = m+n$

2) $f(m \times n) = m \times n$

3) $f(\langle M \rangle) = \langle M' \rangle$ kde M' má místo q_{REJ} smyčku

Def: Nechť $A, B \subseteq \Sigma^*$. Řekneme, že se A redukuje (many-one) na B, $A \leq_m B$, pokud existuje spočitatelná fce f t.ž. $\forall w \in \Sigma^*$

$$w \in A \Leftrightarrow f(w) \in B$$

Př: $A_{TM} \leq_m HALT_{TM}$

f z př. 3)

$g(\langle M \rangle, w) = (f(\langle M \rangle), w)$

$$(\langle M \rangle, w) \in A_{TM} \Leftrightarrow g(\langle M \rangle, w) \in HALT_{TM}$$

$\boxtimes$

Věta: Pokud $A \leq_m B$ a B je rozhodnutelná, pak A je rozhodnutelné.

Důs: Pokud $A \leq_m B$ a A je nerozhodnutelné, pak B je nerozhodnutelné.

Př: $A_{TM} \leq_m \overline{E_{TM}}$.

Věta: Pokud $A \leq_m B$ a B je vyčíslitelná, pak A je vyčíslitelné.

Důs: Pokud $A \leq_m B$ a A není vyčíslitelné, pak B není vyčíslitelné.

- $L \subseteq \Sigma^*$, L je rozhodnutelný $\Rightarrow \exists^\infty$ TS M, $L(M) = L$.

- $ID_L = \{\langle M \rangle;\ M \text{ je TS } \& \ L(M) = L\}$.

- $E_{TM} = ID_\emptyset$

$\Rightarrow$ není rozhodnutelný pro žádný jazyk.

- $\mathcal{L} \subsetneq \mathcal{P}(\Sigma^*)$ $\qquad \mathcal{L} \neq \emptyset$

$\Rightarrow$ $ID_{\mathcal{L}}$ nerozhodnutelný

$$ID_{\mathcal{L}} = \bigcup_{L \in \mathcal{L}} ID_L$$