Problémy a jazyky: přehled terminologie

Problém	**Jazyk**
Má objekt O vlastnost P?	$\{\langle O\rangle \mid O$ má vlastnost $P\}$
je **rozhodnutelný**	je **rekursivní**, tj. $\exists$ **úplný** TM, který ho **akceptuje**, tj. $\exists$ TM, který ho **rozhoduje**
je **nerozhodnutelný**	není rekursivní
je **částečně rozhodnutelný** neboli **semirozhodnutelný**	je **rekursivně spočetný**, tj. $\exists$ TM, který ho **akceptuje**

Redukce - Intuice

$A = \{w \in \{0,1\}^* \mid |w| \text{ je dělitelná } 26\}$

$B = \{w \in \{0,1\}^* \mid |w| \text{ je dělitelná } 13\}$

Redukce - Intuice

Turingovy stroje a funkce

Jednopáskový deterministický Turingův stroj lze vnímat jako funkci, jejíž hodnotou pro daný vstup je obsah pásky po skončení výpočtu. Přesněji, pokud stroj $\mathcal{M}$ na vstupu w zastaví s obsahem pásky $\triangleright y \sqcup^\omega$ (kde y nekončí na $\sqcup$), pak y označíme jako $\mathcal{M}(w)$.

Vyčíslitelné funkce

Definice. Funkce $f : \Sigma^* \to \Phi^*$ je **vyčíslitelná**, pokud existuje TM $\mathcal{M}$, který na vstupu w zastaví, právě když $f(w)$ je definovaná a navíc $f(w) = \mathcal{M}(w)$.

Funkce je **totálně vyčíslitelná**, pokud je vyčíslitelná a totální.

Příklady

- $f(x) = \begin{cases} 1 & \text{pokud } x = \langle \mathcal{M}, w \rangle \text{ a výpočet } \mathcal{M} \text{ na } w \text{ je konečný} \\ 0 & \text{jinak} \end{cases}$

- $g(x) = \begin{cases} 1 & \text{pokud } x = \langle \mathcal{M}, w \rangle \text{ a výpočet } \mathcal{M} \text{ na } w \text{ je konečný} \\ \perp & \text{jinak} \end{cases}$

- $h(x) = \begin{cases} 1 & \text{pokud } x = \langle \mathcal{M}, w \rangle \text{ a výpočet } \mathcal{M} \text{ na } w \text{ není konečný} \\ \perp & \text{jinak} \end{cases}$

- $k(x) = \begin{cases} 1 & \text{pokud } x = \langle \mathcal{M}, w \rangle \\ & \text{a výpočet } \mathcal{M} \text{ na } w \text{ skončí po nejvýše 100 krocích} \\ 0 & \text{jinak} \end{cases}$

Redukce

Definice. Nechť $A \subseteq \Sigma^*$ a $B \subseteq \Phi^*$ jsou jazyky. Řekneme, že A se **m-redukuje** na B, píšeme $A \leq_{\mathrm{m}} B$, 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.

A a B jsou **m-ekvivalentní**, psáno $A \equiv_{\mathrm{m}} B$, pokud $A \leq_{\mathrm{m}} B$ a $B \leq_{\mathrm{m}} A$.

$HALT \equiv_{\mathbf{m}} ACC$

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

$HALT \leq_{\mathrm{m}} ACC$:

$HALT \equiv_{\mathbf{m}} ACC$

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

$ACC \leq_{\mathrm{m}} HALT$:

Redukce a rozhodnutelnost

Věta. Nechť $A \leq_{\mathrm{m}} B$.

- B je rekursivní $\implies$ A je rekursivní.
- B je rekursivně spočetný $\implies$ A je rekursivně spočetný.

Důkaz.

Nechť f je redukce A na B a $\mathcal{M}_B$ je TM akceptující B.
Stroj $\mathcal{M}_A$ akceptující A na vstupu w

1. spočítá $f(w)$
2. spustí $\mathcal{M}_B$ na vstupu $f(w)$ a vrátí stejný výsledek jako $\mathcal{M}_B$

Je-li $\mathcal{M}_B$ úplný, pak je i $\mathcal{M}_A$ úplný. $\square$

Redukce a rozhodnutelnost

Důsledek. Nechť $A \leq_{\mathrm{m}} B$.

- A není rekursivní $\implies$ B není rekursivní.
- A není rekursivně spočetný $\implies$ B není rekursivně spočetný.

Důsledek. Nechť $A \equiv_{\mathrm{m}} B$.

- A je rekursivní $\iff$ B je rekursivní.
- A je rekursivně spočetný $\iff$ B je rekursivně spočetný.

Typické aplikace

- důkaz (částečné) rozhodnutelnosti A

- důkaz nerozhodnutelnosti B

Problém neprázdnosti

Problém neprázdnosti je problém rozhodnout, zda daný TM akceptuje neprázdný jazyk.

$$NONEMPTY = \{\langle \mathcal{M} \rangle \mid \mathcal{M} \text{ je TM a } L(\mathcal{M}) \neq \emptyset\}$$

Věta. Problém neprázdnosti není rozhodnutelný.

Důkaz. $ACC \leq_{\mathrm{m}} NONEMPTY$:

□

Postův systém

Definice. **Postův systém** P nad ebecedou Σ je konečná množina dvojic

$$P = \left\{ \left[\frac{\alpha_i}{\beta_i}\right] \mid \alpha_i, \beta_i \in \Sigma^*, 1 \leq i \leq n \right\}.$$

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. $P = \left\{ \left[\frac{c}{abc}\right], \left[\frac{ca}{b}\right], \left[\frac{a}{ca}\right], \left[\frac{ab}{a}\right] \right\}$

Postův korespondenční problém (PCP)

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

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

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

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

Věta. PCP není rozhodnutelný.

Důkaz. Postupně ukážeme $ACC \leq_{\mathrm{m}} inPCP \leq_{\mathrm{m}} PCP$. □

$\mathit{inPCP} \leq_{\mathbf{m}} \mathit{PCP}$

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

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

$ACC \leq_{\mathbf{m}} inPCP$

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