

Problémy jako jazyky

Problém rozhodnout, zda daný řetězec w má vlastnost P lze ztotožnit s množinou $\{w \mid w \text{ má vlastnost } P\}$.

Objekty O lze kódovat jako slova $\langle O \rangle$. Problém, zda O má vlastnost P ztotožníme s jazykem $\{\langle O \rangle \mid O \text{ má vlastnost } P\}$.

Příklad. Problém rozhodnout, zda daný konečný graf je souvislý, ztotožníme s jazykem $\{\langle G \rangle \mid G \text{ je konečný souvislý graf}\}$.

Rozhodnutelnost problémů

Definice. Problém P odpovídající jazyku $L = \{\langle O \rangle \mid O \text{ má vlastnost } P\}$ je

- **rozhodnutelný**, právě když L je rekursivní
- **nerozhodnutelný**, právě když L není rekursivní
- **částečně rozhodnutelný (semirozhodnutelný)**, právě když L je rekursivně spočetný

Problém akceptování

Problém akceptování (problém příslušnosti pro Turingovy stroje) 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 částečně rozhodnutelný.

Důkaz. Plyne z existence univerzálního Turingova stroje. □

Věta. Problém akceptování je nerozhodnutelný.

Důkaz. (Sporem:) Předpokládejme, že existuje TM \mathcal{A} rozhodující problém akceptování. Tedy \mathcal{A} akceptuje $\langle \mathcal{M}, w \rangle$, právě když \mathcal{M} akceptuje w .

S využitím \mathcal{A} zkonstruujeme TM \mathcal{D} : dostane-li \mathcal{D} na vstupu zakódovaný stroj $\langle \mathcal{M} \rangle$, zeptá se stroje \mathcal{A} , zda \mathcal{M} akceptuje svůj vlastní kód $\langle \mathcal{M} \rangle$ a následně odpověď otočí. Tedy

\mathcal{D} akceptuje $\langle \mathcal{M} \rangle$, pokud \mathcal{M} neakceptuje $\langle \mathcal{M} \rangle$ a
 \mathcal{D} neakceptuje $\langle \mathcal{M} \rangle$, pokud \mathcal{M} akceptuje $\langle \mathcal{M} \rangle$.

Nyní spustíme \mathcal{D} na vstupu $\langle \mathcal{D} \rangle$:

\mathcal{D} akceptuje $\langle \mathcal{D} \rangle$, pokud \mathcal{D} neakceptuje $\langle \mathcal{D} \rangle$ a
 \mathcal{D} neakceptuje $\langle \mathcal{D} \rangle$, pokud \mathcal{D} akceptuje $\langle \mathcal{D} \rangle$.

To je spor. Stroj \mathcal{A} tedy neexistuje a problém akceptování je nerozhodnutelný. □

Diagonalizace

Problémy a jazyky: přehled terminologie

Problém	Jazyk
Má objekt O vlastnost P ?	$\{\langle O \rangle \mid O \text{ má vlastnost } P\}$
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
je rozhodnutelný \iff je částečně rozhodnutelný a jeho doplněk taky	je rekursivní \iff je rekursivně spočetný a jeho doplněk taky

Ne-semirozhodnutelné problémy

Věta. Doplněk problému akceptování není ani částečně rozhodnutelný, tedy $co-ACC$ není rekursivně spočetný.

Důkaz.



Důsledek. Třída rekursivně spočetných jazyků není uzavřená na doplněk.

Problém zastavení

Problém zastavení (halting problem) je problém rozhodnout, zda daný TM \mathcal{M} má na daném slově w nad jeho vstupní abecedou konečný výpočet (tedy zda \mathcal{M} na vstupu w zastaví). 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.

Důkaz. Pomocí univerzálního Turingova stroje simulujeme \mathcal{M} na w . Pokud simulovaný výpočet skončí, akceptujeme. □

Věta. Problém zastavení je nerozhodnutelný.

Důkaz. (Sporem:) Předpokládejme, že existuje úplný TM \mathcal{H} rozhodující problém zastavení. Pak ovšem umíme sestrojít TM \mathcal{A} rozhodující problém akceptování. Stroj \mathcal{A} dekoduje dvojici $\langle \mathcal{M}, w \rangle$ ze vstupu a změní \mathcal{M} tak, že místo přechodů do zamítajícího stavu začne cyklit. Modifikovaný stroj \mathcal{M}' zastaví, právě když \mathcal{M} akceptuje. Nyní stačí spustit \mathcal{H} na vstupu $\langle \mathcal{M}', w \rangle$. Dostáváme tedy úplný TM \mathcal{A} rozhodující problém akceptování. To je spor. Úplný stroj \mathcal{H} tedy neexistuje. □

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 $f : \Sigma^* \rightarrow \Phi^*$ 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. Necht' $A \subseteq \Sigma^*$ 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 $f : \Sigma^* \rightarrow \Phi^*$ taková, že

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

Funkci f nazveme **redukcí** A na B .

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

$$HALT \equiv_m ACC$$

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

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

$HALT \leq_m ACC$:

$$HALT \equiv_m ACC$$

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

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

$ACC \leq_m HALT$:

Redukce a rozhodnutelnost

Věta. Necht' $A \leq_m B$.

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

Důkaz.

Neht' 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. □

Redukce a rozhodnutelnost

Důsledek. Necht' $A \leq_m B$.

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

Důsledek. Necht' $A \equiv_m B$.

- 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. $ACC \leq_m NONEMPTY$:



Postův systém

Definice. Postův systém P nad abecedou 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, \dots, i_k taková, že $1 \leq i_j \leq n$ a

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

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 $ACC \leq_m inPCP \leq_m PCP$. □

$$\text{inPCP} \leq_m \text{PCP}$$

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

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

$ACC \leq_m inPCP$

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