Nerozhodnutelné problémy

Doposud jsme byli zvyklí na to, že ke každému problému můžeme nalézt algoritmus, který jej vyřeší.

(v nejhorším případě alespoň „hrubou silou“ – např. izomorfismus grafů)

Dnešní téma:

Existence problémů, které algoritmicky řešit nelze.

Poznatek z minula:

Pojem algoritmus můžeme ztotožnit s Turingovým strojem (Church-Turingova teze).

Rozhodovací problém

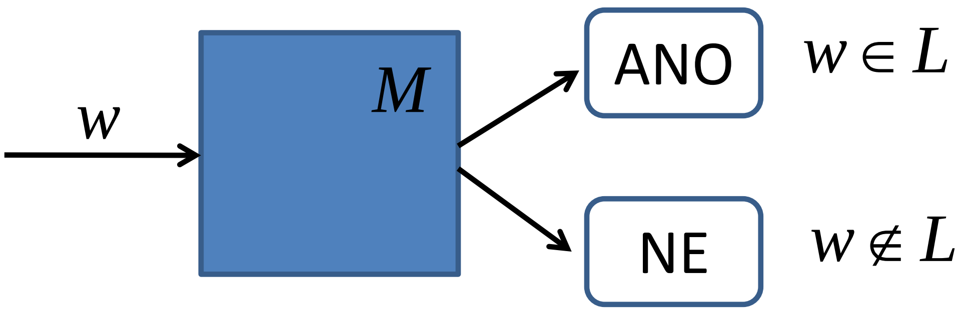
Rozhodovací problém P :

instance problému, odpověď **ANO** či **NE**

Ekvivalentně můžeme vzít jazyk L :

vstupní slovo w, situace $w \in L$ nebo $w \notin L$

TS M, jež rozhoduje jazyk L :



Problém zastavení Turingova stroje

<u>Vstup</u>: Turingův stroj M a slovo $w \in \{0,1\}^*$

<u>Otázka</u>: Zastaví se M, když dostane jako vstup w ?

Označení problému: HP (**H**alting **P**roblem)

Kódování Turingova stroje

$M = (Q, \Sigma, \Gamma, \delta, q_0, F)$

Libovolný TS M chceme reprezentovat pomocí slova.

- Stavy i symboly očíslujeme: $q_0, q_1, \ldots, q_k \qquad a_0, a_1, \ldots, a_l$
- Zakódujeme každou instrukci:

$$\boxed{10}\,B\,\boxed{111}\,B\,\boxed{10}\,B\,\boxed{1101}\,B\,\boxed{0}\,B \quad \cdots$$

$$(q, a) \to (\overline{q}, \overline{a}, D)$$

(a převedeme na binární tvar)

- Navíc vypíšeme všechny koncové stavy (a vyznačíme, jestli jsou přijímací nebo zamítací).

Označení kódu pro M: $Kod(M)$

Problém zastavení Turingova stroje

<u>Vstup</u>: Turingův stroj M a slovo $w \in \{0,1\}^*$
$Kod(M) \cdot w$

<u>Otázka</u>: Zastaví se M, když dostane jako vstup w ?

$$HP = \{u \mid \exists M : u = Kod(M) \cdot w \wedge !M(w)\}$$

$!M(w)$ … na vstup w se M zastaví

Nerozhodnutelnost HP

Důkaz sporem:

- Nechť H je TS, který rozhoduje HP (skončí ve stavu q_{ANO} nebo q_{NE})

- Sestrojíme stroj D s následujícím chováním:
  1. vstupní slovo $v \in \{0,1\}^*$ zdvojí na vv
  2. spustí jako podprogram stroj H
  3. jestliže (podprogram) H skončí ve stavu q_{ANO}, přejde D do nekonečného cyklu

     jestliže H skončí ve stavu q_{NE} , stroj D se zastaví

Skončí výpočet stroje D, když dostane jako vstup slovo $Kod(D)$? … <u>skončí právě tehdy, když neskončí</u> … spor

Paradox holiče

Holič holí právě všechny muže ve městě, kteří se neholí sami.
Holí holič sám sebe?

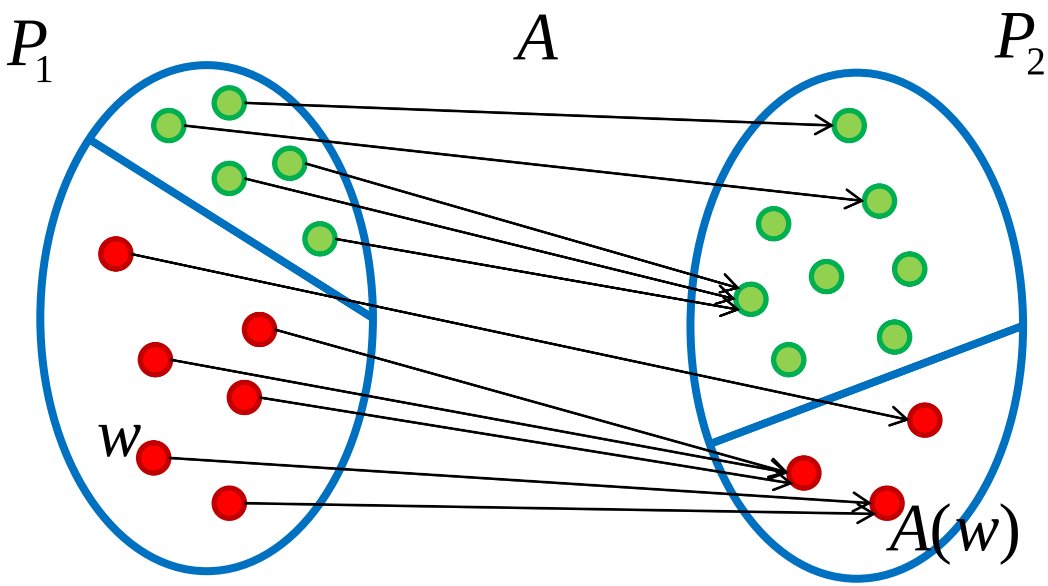
- Pokud se holič holí, porušuje uvedené pravidlo.
- Pokud se holič neholí, měl by se podle pravidla holit.

Logický spor, uvedený holič nemůže existovat.

Muž	Turingův stroj
Holí se	Zastaví se na svůj kód
Holič (holí toho, kdo se neholí)	Stroj D (zastaví se pro stroj, který se nezastaví)

Algoritmická převeditelnost

Problém P_1 je algoritmicky převeditelný na problém P_2, jestliže existuje algoritmus A, který pro každé zadání w problému P_1 sestrojí zadání $A(w)$ problému P_2 takové, že odpověď pro w je v P_1 **ANO** právě tehdy, když je i odpověď pro $A(w)$ v P_2 **ANO**.



Definice pro jazyky

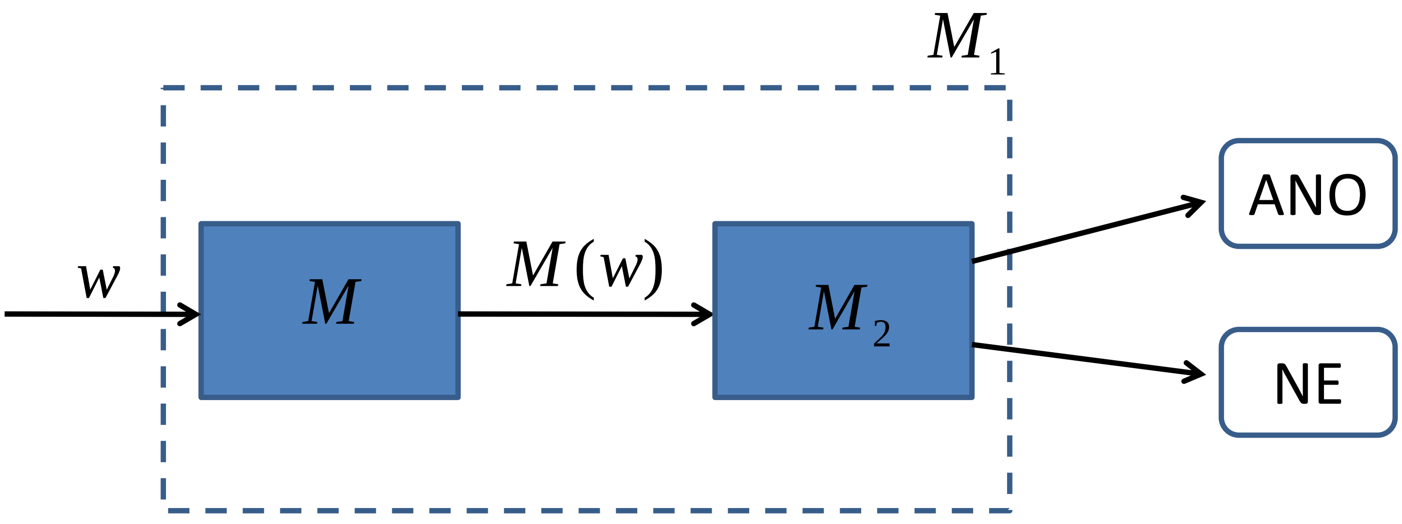
Jazyk L_1 nad abecedou Σ_1 je algoritmicky převeditelný na jazyk L_2 nad Σ_2, jestliže existuje Turingův stroj M, který se vždy zastaví a pro vstupní slovo $w \in \Sigma_1^*$ je jeho výstupem slovo $M(w) \in \Sigma_2^*$ splňující:

$$w \in L_1 \Leftrightarrow M(w) \in L_2$$

Využití převeditelnosti I

Označení (L_1 je převeditelný na L_2): $L_1 \to L_2$

Mějme TS M_2, který rozhoduje L_2.
Platí-li $L_1 \to L_2$, můžeme sestrojit TS M_1 rozhodující L_1:



Využití převeditelnosti II

Věta: Nechť L_1 je nerozhodnutelný a $L_1 \to L_2$. Potom je také L_2 nerozhodnutelný.

Uniform Halting Problem (UHP):

Vstup: Turingův stroj M.

Otázka: Zastaví se M na každý vstup?

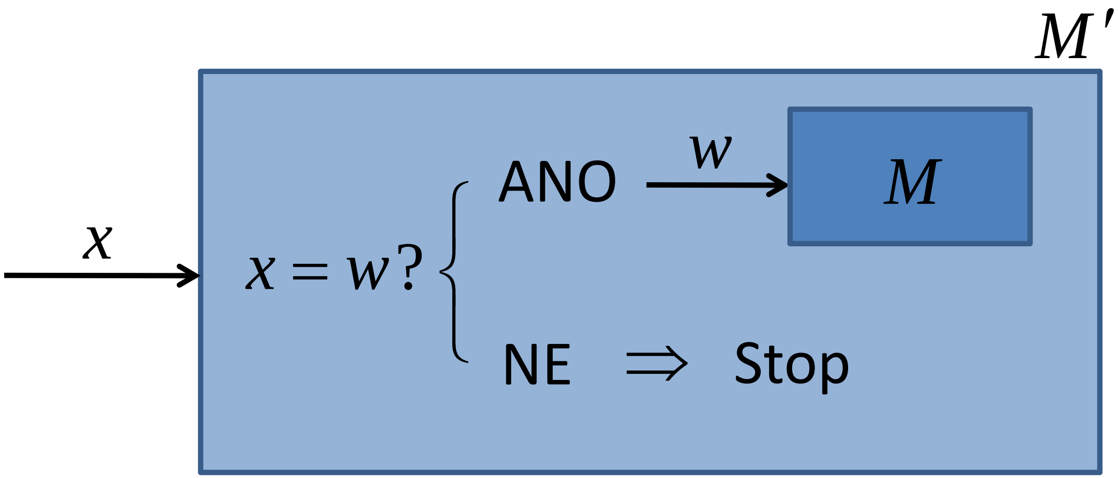
$$UHP = \left\{ Kod\left(M\right) | \ \forall u \in \{0,1\}^* \ !M(u) \right\}$$

Nerozhodnutelnost UHP

Ukážeme, že $HP \rightarrow UHP$

Cíl: $Kod(M) \cdot w \quad \Rightarrow \quad Kod(M')$

$$!M(w) \quad \Leftrightarrow \quad \forall x\, !M'(x)$$



- slovo w si M' „zapamatuje“ ve svých stavech

Důsledky nerozhodnutelnosti UHP

Nemůžeme automaticky testovat, zda je zdrojový kód validní v tom smyslu, že se nikdy (nechtěně) „nezacyklí“.

```
public static int factorial(int n) {
   int result = 1;
   while (n > 1) {
     result *= n;
     // n--;
   }
   return result;
}
```

Další příklady nerozhodnutelných problémů

<u>Vstup</u>: Dvě bezkontextové gramatiky G_1 a G_2.

<u>Otázka č.1</u>: Generují obě gramatiky stejný jazyk?

<u>Otázka č.2</u>: Generují gramatiky G_1, G_2 alespoň jedno **stejné** slovo?

Rozhodnutelné je:

<u>Otázka č.3</u>: Generuje gramatika G_1 alespoň jedno slovo?

Otázka ekvivalence dvou programů

Vstup: Dva konečné automaty A_1 a A_2 .

Otázka: Přijímají oba automaty stejný jazyk?

$L_1 = L_2 \Leftrightarrow \left(L_1 \cap \overline{L_2}\right) \cup \left(\overline{L_1} \cap L_2\right) = \emptyset$ … je rozhodnutelné

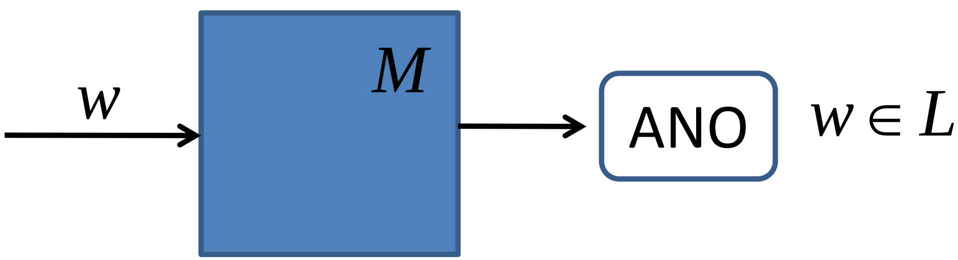
Vstup: Dva Turingovy stroje M_1 a M_2.

Otázka: Přijímají oba stroje stejný jazyk?

Není rozhodnutelné.

Částečná rozhodnutelnost

Jazyk (problém) je částečně rozhodnutelný, pokud existuje TS M, který se zastaví právě na slova náležící do daného jazyka.



$w \notin L$ M se nezastaví

<u>Jiná terminologie</u>:

- rekurzivní jazyk (rozhodnutelný)
- rekurzivně spočetný jazyk (částečně rozhodnutelný)

Univerzální TS

Univerzální Turingův stroj (UTS):

- vstup: $Kod(M) \cdot w$
- UTS simuluje činnost stroje M
- skončí právě tehdy, když skončí M a výsledek výpočtu je totožný s výsledkem stroje M

Důsledek: HP je částečně rozhodnutelný

Částečná rozhodnutelnost

Věta (Postova): Jazyk L je rozhodnutelný právě tehdy, když je L i jeho doplněk $\overline{L}$ částečně rozhodnutelný.

Důsledek: $\overline{HP}$ není částečně rozhodnutelný.

$\overline{HP}$: $Kod(M) \cdot w$, kde M se na w nezastaví
a též všechna slova, která nekódují TS a jeho vstup

Diagonalizační metoda

Georg Cantor – neexistuje bijekce mezi množinou přirozených a reálných čísel (publikováno 1891)

$$
\begin{array}{lllllll}
r_1 = & \boxed{0} & 0 & 0 & 1 & 1 & 0 & \cdots \\
r_2 = & 1 & \boxed{1} & 0 & 0 & 1 & 0 & \cdots \\
r_3 = & 1 & 0 & \boxed{0} & 1 & 0 & 1 & \cdots \\
r_4 = & 0 & 0 & 1 & \boxed{0} & 0 & 0 & \cdots \\
\vdots
\end{array}
$$

$$r_0 = 1 \quad 0 \quad 1 \quad 1 \quad \cdots$$

Diagonalizační metoda

$$DHP = \{Kod(M) \mid \neg ! M(Kod(M))\}$$

- Diagonal Halting Problem
- Neexistuje TS, který přijímá DHP (tj. DHP není částečně rozhodnutelný)

	$Kod(M_1)$	$Kod(M_2)$	$Kod(M_3)$	$\cdots$
M_1	$\boxed{0}$	0	1	
M_2	1	$\boxed{1}$	1	
M_3	0	1	$\boxed{0}$	
$\vdots$				
M_{DHP}	1	0	1	Neodpovídá žádnému řádku v tabulce.

… slovo v příslušném sloupci patří do *DHP*