Základy složitosti a vyčíslitelnosti

NTIN090

Petr Kučera

2021/22 (3. přednáška)

Číslování Turingových strojů

Definice

Definice

Jazyk $L \subseteq \Sigma^*$ je …

částečně rozhodnutelný je-li přijímán nějakým Turingovým strojem M

- $L = L(M)$

rozhodnutelný je-li přijímán nějakým Turingovým strojem M, jehož výpočet s každým vstupem se zastaví

- $L = L(M)$ a
- $(\forall x \in \Sigma^*)[M(x)\downarrow]$

- Částečně rozhodnutelný jazyk = rekurzivně spočetný jazyk.
- Rozhodnutelný jazyk = rekurzivní jazyk.

Kolik je částečně rozhodnutelných jazyků?

Jsou všechny jazyky nad konečnou abecedou Σ částečně rozhodnutelné?

Kolik je jazyků nad abecedou Σ?

Kolik je částečně rozhodnutelných jazyků nad abecedou Σ?

Lexikografické uspořádání řetězců

- Uvažme abecedu Σ
- Předpokládejme, že $<$ je ostré uspořádání na znacích Σ
- $|u|$ označuje délku řetězce $u \in \Sigma^*$
- Řetězec $u \in \Sigma^*$ je lexikograficky menší než $v \in \Sigma^*$, pokud
  1. $|u| < |v|$ (u je kratší než v), nebo
  2. $|u| = |v|$ a je-li i první index s $u[i] \neq v[i]$, pak $u[i] < v[i]$
- Tento fakt označíme pomocí $u \prec v$.
- Tím je dané i značení $u \preceq v$, $u \succ v$ a $u \succeq v$

Příklad

$$\texttt{Bob} \prec \texttt{Alena} \prec \texttt{Alice} \prec \texttt{Cyril} \prec \texttt{Andrea}$$

Číslování řetězců

- Každému řetězci $w \in \Sigma^*$ přiřadíme číslo

$$\mathrm{index}(w) = |\{u \in \Sigma^* \mid u \prec w\}|$$

- Porovnáváme nejprve délku $\implies$ vždy konečné číslo
- $\mathrm{index}(w)$ je počet řetězců před w v lexikografickém uspořádání
- index je bijekcí mezi Σ^* a $\mathbb{N}$

Číslování binárních řetězců

- Uvažme binární abecedu $\Sigma = \{\texttt{0}, \texttt{1}\}$ a řetězec $w \in \Sigma^*$
- $\operatorname{index}(w) = i$, kde

$$\underbrace{(i+1)_B}_{\text{binární zápis } i+1} = \underbrace{\texttt{1}w}_{\text{konkatenace } \texttt{1} \text{ a } w}$$

w	$\texttt{1}w$	$\operatorname{index}(w)+1$	$\operatorname{index}(w)$
ε	1	1	0
0	10	2	1
1	11	3	2
00	100	4	3
⋮	⋮	⋮	
001011	1001011	75	74
⋮	⋮	⋮	

Lze spočítat jazyky?

Definice

Množina A je spočetná, pokud existuje prostá funkce $f : A \longrightarrow \mathbb{N}$, tj. pokud lze prvky A očíslovat.

- Jazyk $L \subseteq \Sigma^*$ odpovídá množině přirozených čísel

$$A = \{\mathrm{index}(w) \mid w \in L\}$$

- $\mathcal{P}(\mathbb{N})$ je nespočetná množina
  - Cantorova věta $\mathcal{P}(A)$ má větší mohutnost než A pro každou množinu A

Jazyků nad konečnou abecedou Σ není spočetně mnoho

Číslování Turingových strojů

Každému Turingovu stroji přiřadíme přirozené číslo

1. Turingův stroj popíšeme řetězcem nad malou abecedou
2. Řetězec nad touto abecedou převedeme do binární abecedy
3. Každému binárnímu řetězci w přiřadíme číslo $\mathrm{index}(w)$
4. Každému Turingovu stroji takto přiřadíme Gödelovo číslo

Převod do binární abecedy není pro číslování nutný, ale chceme, aby Univerzální Turingův stroj byl schopen simulovat sám sebe.

Pár technických omezení

Omezíme se na Turingovy stroje, které

1. mají jediný přijímající stav a
2. mají pouze binární vstupní abecedu $\Sigma_{in} = \{0, 1\}$.

- Vstupní řetězce budou zapsány jen pomocí znaků 0 a 1
- Pracovní abecedu nijak neomezujeme
  - Turingův stroj může během výpočtu zapisovat na pásku libovolné symboly
- Jakoukoli konečnou abecedu lze zakódovat do binární abecedy
- Každý TS M lze upravit tak, aby splňoval obě omezení

Zakódování přechodové funkce

$$M = (Q, \Sigma, \delta, q_0, F = \{q_1\})$$

$\downarrow$

δ zapíšeme řetězcem v_M v abecedě
$\Gamma = \{0, 1, L, N, R, |, \#, ;\}$

$\downarrow v_M$

Každý znak v_M zapíšeme pomocí 3 bitů

$\downarrow$

$\langle M \rangle$
Binární řetězec reprezentující M

Zápis přechodové funkce v abecedě Γ

- Předpokládejme, že
  - $Q = \{q_0, q_1, \ldots, q_r\}$ pro nějaké $r \geq 1$, kde q_0 je počáteční stav a q_1 je jediný přijímající stav.
  - $\Sigma = \{X_0, X_1, X_2, \ldots, X_s\}$ pro nějaké $s \geq 2$, kde $X_0 = \mathtt{0}$, $X_1 = \mathtt{1}$ a $X_2 = \lambda$
- Instrukci $\delta(q_i, X_j) = (q_k, X_l, Z)$, kde $Z \in \{L, N, R\}$ zakódujeme řetězcem

$$(i)_B|(j)_B|(k)_B|(l)_B|Z$$

- Jsou-li $C_1, \ldots, C_n$ kódy instrukcí TS M, pak přechodovou funkci δ zakódujeme řetězcem

$$C_1\#C_2\#\ldots\#C_n$$

Převod do binární abecedy

λ

$\delta(q_3, X_7) = (q_5, X_2, R)$

$11|111|101|10|R$

Γ	kód
0	000
1	001
L	010
N	011
R	100
|	101
#	110
;	111

Znaky abecedy Γ zakódujeme pomocí této tabulky

001001101001001001101001000001101001000101100

Gödelovo číslo

$\langle M \rangle$ binární řetězec kódující TS M

Gödelovo číslo jednoznačně přiřazené danému Turingovu stroji

- Definujeme jako $\mathrm{index}(\langle M \rangle)$

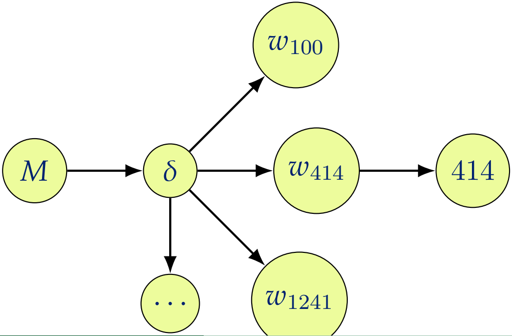
M_e Turingův stroj s Gödelovým číslem e

- $e = \mathrm{index}(\langle M_e \rangle)$

- Je-li w řetězec, který není syntakticky správným kódem Turingova stroje a je-li $e = \mathrm{index}(w)$, pak definujeme, že
  - přechodová funkce M_e není definovaná pro žádný vstup a
  - M_e okamžitě odmítne každý vstup, tedy $L(M_e) = \emptyset$

Nejednoznačnost kódu TS

- Kód TS není jednoznačný, protože nezáleží na
  - pořadí instrukcí,
  - na očíslování stavů kromě počátečního a přijímajícího,
  - znaků páskové abecedy kromě 0, 1, λ, a
  - binární zápis čísla stavu nebo znaku může být uvozen libovolným počtem 0.
- Každý TS má nekonečně mnoho různých kódů a potažmo nekonečně mnoho Gödelových čísel.



Jedno z Gödelových čísel M

Kolik je částečně rozhodnutelných jazyků?

- Je jen spočetně mnoho Turingových strojů
  - každý má Gödelovo číslo
  - každé číslo odpovídá jedinému Turingovu stroji
- Každý částečně rozhodnutelný jazyk je přijímán nějakým Turingovým strojem

Lemma

Částečně rozhodnutelných jazyků je spočetně mnoho.

- Všech jazyků nad konečnou abecedou je nespočetně mnoho

Musí proto existovat jazyky nad abecedou $\{0,1\}$, které nejsou částečně rozhodnutelné.

Kódování objektů (značení)

- Konečné objekty (např. číslo, řetězec, Turingův stroj, RAM, graf nebo formuli) můžeme kódovat binárními řetězci
- Podobně můžeme zakódovat i n-tice objektů

Definice

$\langle X \rangle$ binární řetězec kódující objekt X

$\langle X_1, \ldots, X_n \rangle$ binární řetězec kódující n-tici objektů $X_1, \ldots, X_n$

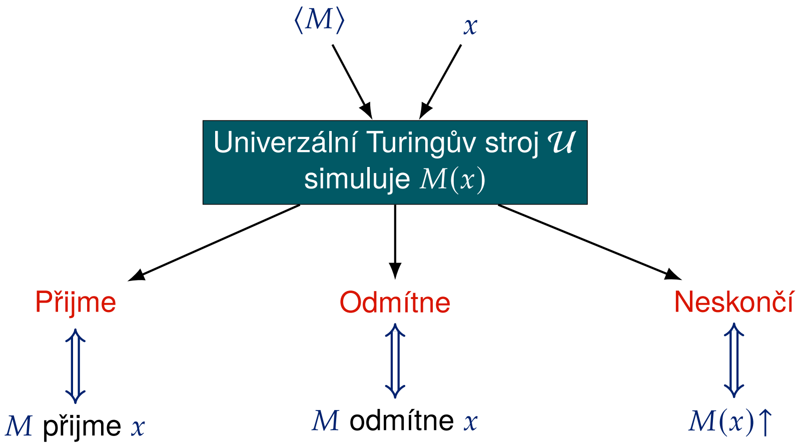
Příklad

$\langle M \rangle$ kód Turingova stroje M

$\langle M, x \rangle$ kód dvojice tvořené Turingovým strojem M a řetězcem x

Univerzální Turingův stroj

Univerzální Turingův stroj



Univerzální Turingův stroj

Vstup	$\langle M, x \rangle$ (M je Turingův stroj, x je vstup)
Univerzální Turingův stroj	simuluje práci stroje M nad vstupem x
Výsledek práce	zastavení/přijetí/zamítnutí vstupu a obsah výstupní pásky je dán výsledkem $M(x)$
Univerzální jazyk	jazyk univerzálního Turingova stroje

$$L_u = \{\langle M, x \rangle \mid x \in L(M)\}$$

Univerzální jazyk formalizuje problém PŘIJETÍ VSTUPUP

PŘIJETÍ VSTUPU

Instance: Kód Turingova stroje M a vstupní řetězec x

Otázka: Přijme M vstup x?

Struktura $\mathcal{U}$

Popíšeme 3-páskový Univerzální Turingův stroj $\mathcal{U}$

1. páska obsahuje vstup $\langle M, x\rangle$

$\langle M\rangle$	x

Na 2. pásce je uložen obsah pracovní pásky M
Symbol X_j zapsán jako $(j)_B$, bloky mají touž délku b bitů

…	|	0	1	0	|	0	1	0	|	1	0	1	|	1	1	0	|	…

3. páska obsahuje $(i)_B$ reprezentující aktuální stav q_i stroje M

…	1	0	0	1	1	λ	λ	λ	λ	λ	λ	λ	λ	λ	λ	λ	λ	…

Výpočet $\mathcal{U}$

- Předpokládáme, že

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

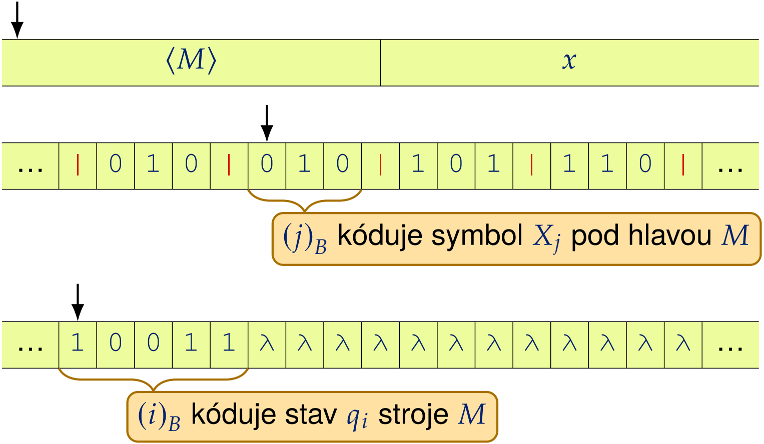
- Vstup $\mathcal{U}$ má dvě části $\langle M \rangle$ a x
  - $\mathcal{U}$ umí číst každou zvlášť
- $\langle M \rangle$ kóduje přechodovou funkci δ dle dřívějšího popisu
- Výpočet $\mathcal{U}(\langle M \rangle, x)$ má 3 fáze
  1. Inicializace
  2. Simulace
  3. Zakončení

Inicializace

1. Syntaktická kontrola
   - Pokud první část vstupu není syntakticky správným kódem Turingova stroje, odmítni
2. Určení délky bloku b pro znak na 2. pásce
   - Maximální délka znaku X_i v rámci nějaké instrukce
   - Abeceda Σ obsahuje alespoň $\mathtt{0}$, $\mathtt{1}$ a λ, tedy $b \geq 2$
   - Pracovní abeceda není jinak omezená
3. Přepis vstupu na 2. pásku
   - Překódování vstupu do bloků délky b oddělených $\mathtt{|}$
   - $\mathtt{0}$ je přepsáno na $\mathtt{0}^b$ ($X_0 = \mathtt{0}$)
   - $\mathtt{1}$ je přepsáno na $\mathtt{0}^{b-1}\mathtt{1}$ ($X_1 = \mathtt{1}$)
4. Zapiš $\mathtt{0}$ na 3. pásku
   - Počáteční stav je q_0
5. Návrat všech tří hlav na začátky slov na příslušných páskách

Polohy hlav na začátku simulace kroku M

1. páska na začátku kódu $\langle M\rangle$
2. páska nad blokem symbolu X_j, nad nímž je hlava M
3. páska na začátku čísla stavu q_i



Simulace kroku M

1. Hledej v $\langle M \rangle$ instrukci pro displej (q_i, X_j)
   - Instrukce není nalezena $\Longrightarrow$ simulace končí
   - Jinak označme nalezenou instrukci $\delta(q_i, X_j) = (q_k, X_l, Z)$
2. Na 3. pásce přepiš číslo stavu na $(k)_B$
3. Na 2. pásce přepiš blok pod hlavou na $(l)_B$ (b bitů)
4. Na 2. pásce přesuň hlavu
   - o blok vlevo (je-li $Z = L$)
   - o blok vpravo (je-li $Z = R$)
   - na začátek stávajícího bloku (je-li $Z = N$)
5. Pokud se hlava přesunem dostala mimo použitou část pásky, $\mathcal{U}$ přidá další blok tvaru $\mathtt{0}^{b-2}\mathtt{10}$ ($X_2 = \lambda$)
6. Vrať hlavy do předpokládaných pozic a pokračuj simulací dalšího kroku M

Zakončení

- $\mathcal{U}$ přijme, pokud na 3. pásce je číslo 1 jediného přijímajícího stavu q_1, jinak odmítne
- Pokud chceme simulovat výpočet funkce M, pak je potřeba přepsat pracovní pásku do řetězce z Σ^*

Nerozhodnutelnost Univerzálního jazyka

Vlastnosti univerzálního jazyka

Věta

Jazyk $L_u = \{\langle M, x\rangle \mid x \in L(M)\}$ *je částečně rozhodnutelný, ale není rozhodnutelný.*

- Částečná rozhodnutelnost plyne z existence univerzálního Turingova stroje
- Nerozhodnutelnost ukážeme diagonalizací, plán:
  1. Univerzální jazyk reprezentujeme jako matici A
  2. Jazyk daný doplňkem diagonály A není částečně rozhodnutelný
  3. Z toho dovodíme, že L_u není rozhodnutelný

Univerzální jazyk jako matice

$L_u = \{\langle M, x\rangle \mid x \in L(M)\}$ lze reprezentovat nekonečnou maticí A

Odpovídá j-tému binárnímu řetězci $\mathbf{w}_j$ s indexem j

$\mathbf{w}_i$ označuje binární řetězec s indexem i

M_i označuje TS s Gödelovým číslem i

Platí: $\mathbf{w}_i = \langle M_i\rangle$

indexy binárních řetězců

Gödelova čísla

$\mathbf{A}$	0	1	2	…	i	…	j	…
0	0	1	0	…	0	…	1	…
1	1	1	0	…	1	…	0	…
2	1	1	0	…	0	…	1	…
⋮								
i	0	0	1	…	1	…	0	…
⋮								

$\mathbf{w}_i \in L(M_i)$

$\mathbf{w}_j \notin L(M_i)$

Odpovídá Turingovu stroji M_i s Gödelovým číslem i

Matice univerzálního jazyka

- Každý Turingův stroj M má nekonečně mnoho Gödelových čísel

$\Longrightarrow$ Každému Turingovu stroji M odpovídá nekonečně mnoho řádků v matici A

$\Longrightarrow$ Každému částečně rozhodnutelnému jazyku odpovídá nekonečně mnoho řádků v matici A

Doplněk diagonály matice A určuje diagonální jazyk

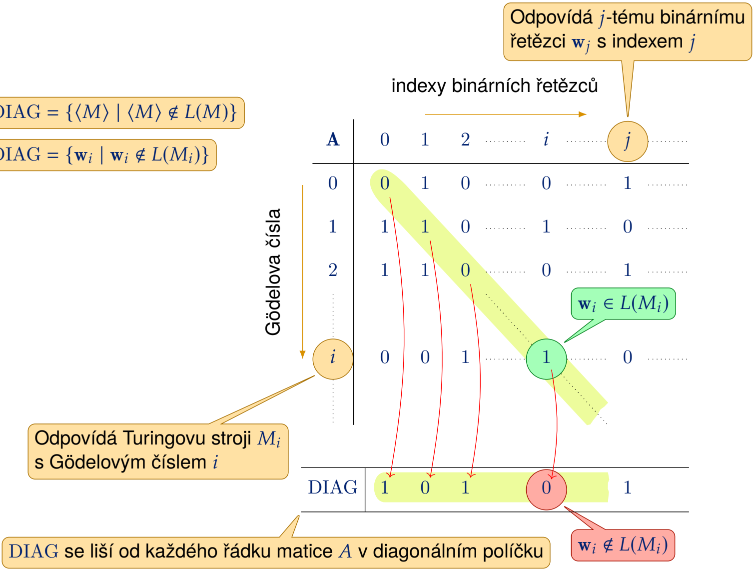
$$\mathrm{DIAG} = \{\langle M\rangle \mid \langle M\rangle \notin L(M)\}$$

- DIAG nemá svůj řádek v matici A
- DIAG není částečně rozhodnutelný

Diagonální jazyk

$\mathrm{DIAG} = \{\langle M \rangle \mid \langle M \rangle \notin L(M)\}$

$\mathrm{DIAG} = \{\mathbf{w}_i \mid \mathbf{w}_i \notin L(M_i)\}$



Diagonální jazyk není částečně rozhodnutelný

Věta

Jazyk $\mathrm{DIAG} = \{\langle M\rangle \mid \langle M\rangle \notin L(M)\}$ *není částečně rozhodnutelný*

Důkaz.

Sporem: existuje TS M_D, který přijímá DIAG (tj. $\mathrm{DIAG} = L(M_D)$)

$$\begin{tikzcd}
 & \langle M_D\rangle \notin L(M_D) \arrow[dd, Leftrightarrow, "\times" description, "\text{Spor}"] \\
\langle M_D\rangle \in \mathrm{DIAG} \arrow[ur, Leftrightarrow, "\text{definice } \mathrm{DIAG}"] \arrow[dr, Leftrightarrow, "\mathrm{DIAG} = L(M_D)"'] & \\
 & \langle M_D\rangle \in L(M_D)
\end{tikzcd}$$

□

Nerozhodnutelnost univerzálního jazyka

Věta

Jazyk $L_u = \{\langle M, x\rangle \mid x \in L(M)\}$ *není rozhodnutelný.*

Důkaz.

- Sporem: Existuje Turingův stroj M_u, který rozhoduje L_u
  - $L_u = L(M_u)$ a $M_u(\langle M, x\rangle)\downarrow$ pro každý vstup $\langle M, x\rangle$
- Pro každý Turingův stroj M platí

$$\langle M\rangle \in \mathrm{DIAG} \quad \overbrace{\Longleftrightarrow}^{\text{definice } \mathrm{DIAG}} \quad \langle M\rangle \notin L(M) \quad \overbrace{\Longleftrightarrow}^{\text{definice } L_u} \quad \langle M, \langle M\rangle\rangle \notin L_u$$

- Stroj M_u lze použít k rozhodování DIAG
- Spor s nerozhodnutelností DIAG

$\square$

Vlastnosti (částečně) rozhodnutelných jazyků

Uzavřenost na jazykové operace

Doplněk jazyka L označíme pomocí $\overline{L} = \Sigma^* \setminus L$.

Konkatenací dvou jazyků L_1 a L_2 vznikne jazyk

$$L_1 \cdot L_2 = \{w_1 w_2 \mid w_1 \in L_1, w_2 \in L_2\}.$$

Kleeneho uzávěrem jazyka L je jazyk

$$L^* = \{w \mid (\exists k \in \mathbb{N})(\exists w_1, \ldots, w_k \in L)[w = w_1 w_2 \ldots w_k]\}.$$

Věta

Jsou-li L_1 a L_2 (částečně) rozhodnutelné jazyky, pak $L_1 \cup L_2$, $L_1 \cap L_2$, $L_1 \cdot L_2$, L_1^* jsou (částečně) rozhodnutelné jazyky.

Jsou (částečně) rozhodnutelné jazyky uzavřené na doplněk?

Postova věta

Věta (Postova věta)

Jazyk L je rozhodnutelný, právě když L i $\overline{L}$ jsou částečně rozhodnutelné jazyky.

Důkaz.

Dva kroky

„ $\Longrightarrow$ “ L je rozhodnutelný $\Longrightarrow$ L i $\overline{L}$ jsou částečně rozhodnutelné

„ $\Longleftarrow$ “ L i $\overline{L}$ jsou částečně rozhodnutelné $\Longrightarrow$ L je rozhodnutelný

$\square$

Postova věta (důkaz „ $\Longrightarrow$ “)

- Předpokládáme, že $L \subseteq \Sigma^*$ je rozhodnutelný jazyk

$\Longrightarrow$ Existuje Turingův stroj M rozhodující L
  - $L = L(M)$ a $M(x)\downarrow$ pro každý vstup $x \in \Sigma^*$
- Sestavíme Turingův stroj M', který se vstupem x
  1. Pustí $M(x)$
  2. Na závěr zneguje odpověď
     - $M'(x)$ přijme $\Longleftrightarrow$ $M(x)$ odmítne
- M' přijímá $\overline{L}$
- $M'(x)\downarrow$ pro každý vstup $x \in \Sigma^*$

$\Longrightarrow$ $\overline{L}$ je rozhodnutelný jazyk

$\Longrightarrow$ L i $\overline{L}$ jsou částečně rozhodnutelné jazyky

Postova věta (důkaz „ $\Longleftarrow$ “)

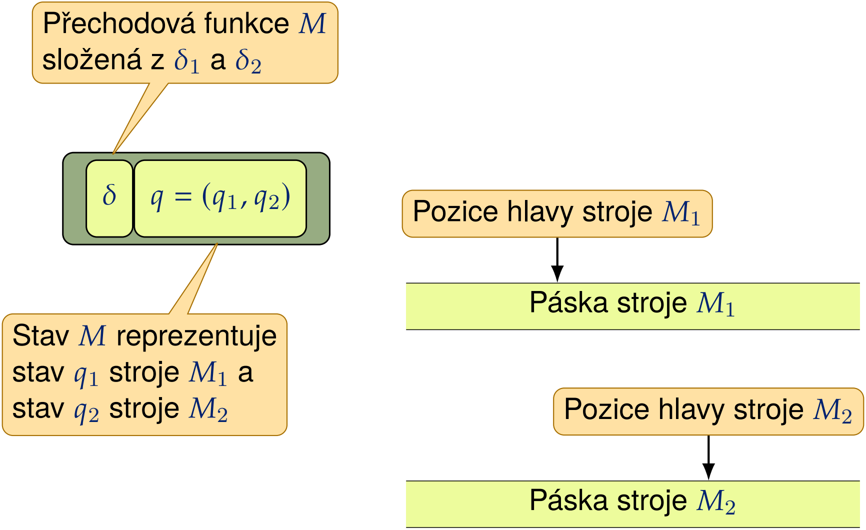
- Předpokládáme, že
  - $L = L(M_1)$ pro nějaký Turingův stroj $M_1 = (Q_1, \Sigma, \delta_1, q_0^1, F_1)$
  - $\overline{L} = L(M_2)$ pro nějaký Turingův stroj $M_2 = (Q_2, \Sigma, \delta_2, q_0^2, F_2)$
- Sestavíme Turingův stroj M, který rozhoduje L, tedy
  - $L = L(M)$ a
  - $M(x)\downarrow$ pro každý vstup x
- Idea:
  - Pokud $M_1(x)$ přijme, pak $x \in L$
  - Pokud $M_2(x)$ přijme, pak $x \notin L$

Postova věta (důkaz „ $\Longleftarrow$ “)

Práce M se vstupem x

```
Pusť M₁(x) a M₂(x) paralelně a čekej až jeden z nich přijme
if M₁(x) přijal then
    přijmi
if M₂(x) přijal then
    odmítni
```

Možná implementace M



Uzavřenost na doplněk

Důsledek

- *Třída rozhodnutelných jazyků je uzavřená na operaci doplňku*
- *Třída částečně rozhodnutelných jazyků není uzavřená na operaci doplňku*

- Jazyk L_u je částečně rozhodnutelný, ale není rozhodnutelný
- Dle Postovy věty $\overline{L_u}$ není částečně rozhodnutelný
- $\mathrm{DIAG} = \{\langle M\rangle \mid \langle M\rangle \notin L(M)\}$ není částečně rozhodnutelný
- $\overline{\mathrm{DIAG}} = \{\langle M\rangle \mid \langle M\rangle \in L(M)\}$ je částečně rozhodnutelný
  - Plyne z existence univerzálního Turingova stroje

Vztahy tříd jazyků

PD částečně rozhodnutelné jazyky

- *partially decidable*

co-PD doplňky částečně rozhodnutelných jazyků

- $L \in \text{co-PD} \Leftrightarrow \overline{L} \in \mathrm{PD}$
- *co-partially decidable*

DEC rozhodnutelné jazyky

- *decidable*

Postova věta: $\mathrm{DEC} = \mathrm{PD} \cap \text{co-PD}$