Základy složitosti a vyčíslitelnosti

NTIN090

Petr Kučera

2021/22 (4. přednáška)

Algoritmicky vyčíslitelné funkce

Funkce — značení

Pro částečnou funkci $f : \Sigma^* \to \Sigma^*$ definujeme:

Doména f je množina vstupů, pro něž je hodnota f definovaná

$$\operatorname{dom} f = \{x \in \Sigma^* \mid f(x)\downarrow\}$$

Totální funkce f je definovaná pro každý vstup x, tedy $\operatorname{dom} f = \Sigma^*$

Obor hodnot f je množina možných hodnot f

$$\operatorname{rng} f = \{y \in \Sigma^* \mid (\exists x \in \Sigma^*)[f(x)\downarrow = y]\}$$

> Značení používáme i pro jiné než řetězcové funkce
>
> - například funkce $f : \mathbb{N} \to \mathbb{N}$

Algoritmicky vyčíslitelné funkce (definice)

Intuitivně

Algoritmicky vyčíslitelná funkce jsou právě ty, jejichž hodnoty lze vyčíslit nějakým algoritmem

Definice

Částečná funkce $f : \Sigma^* \to \Sigma^*$ je algoritmicky vyčíslitelná pokud existuje Turingův stroj M, který ji počítá.

Pro každý vstup $x \in \Sigma^*$ platí

- Je-li $f(x)\uparrow$, pak $M(x)\uparrow$
- Je-li $f(x)\downarrow = y$, pak
  - $M(x)\downarrow$ a
  - na výstupní pásce M je po ukončení výpočtu $M(x)$ řetězec y

Algoritmicky vyčíslitelné funkce

- Vyčíslitelné funkce = částečně rekurzivní funkce
- Totální vyčíslitelné funkce = obecně rekurzivní funkce
- Uvažujeme i funkce jiných typů, například
  - aritmetické funkce
  - funkce více parametrů

Příklad

Například funkce

$$f(x, y) = x^2 + y^2$$

může být realizována řetězcovou funkcí

$$f'(\langle x, y \rangle) = \langle x^2 + y^2 \rangle$$

Ne všechny funkce jsou vyčíslitelné

- Vyčíslitelných funkcí je jen spočetně mnoho
  $\Longrightarrow$ ne všechny funkce jsou vyčíslitelné

Příklad

Charakteristická funkce jazyka L_u

$$\chi_u(\langle M, x\rangle) = \begin{cases} 1 & x \in L(M) \\ 0 & x \notin L(M) \end{cases}$$

není algoritmicky vyčíslitelná, protože jazyk

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

je algoritmicky nerozhodnutelný

Vlastnosti (částečně) rozhodnutelných jazyků

Charakteristická funkce rozhodnutelného jazyka

Věta

Jazyk $L \subseteq \Sigma^*$ je rozhodnutelný, právě když jeho charakteristická funkce

$$\chi_L(x) = \begin{cases} 1 & x \in L \\ 0 & x \notin L \end{cases}$$

je algoritmicky vyčíslitelná.

Důkaz.

Důkaz ve dvou krocích

„$\Longrightarrow$“ L je rozhodnutelný $\Longrightarrow$ χ_L je algoritmicky vyčíslitelná

„$\Longleftarrow$“ χ_L je algoritmicky vyčíslitelná $\Longrightarrow$ L je rozhodnutelný

$\square$

Důkaz „ $\Longrightarrow$ “

- Předpokládáme, že L je rozhodnutelný jazyk
- Existuje Turingův stroj M, který
  - přijímá L ($L = L(M)$)
  - $M(x)\downarrow$ pro každý vstup $x \in \Sigma^*$
- Popíšeme Turingův stroj M', který počítá χ_L

Výpočet M' se vstupem x

Simuluj $M(x)$
if M přijal **then**
    Zapiš na výstup 1
else
    Zapiš na výstup 0

Důkaz „ $\Longleftarrow$ “

- Předpokládáme, že funkce χ_L je algoritmicky vyčíslitelná
- Existuje Turingův stroj M, který počítá χ_L
- $M(x)\downarrow$ pro každý vstup $x \in \Sigma^*$
  - protože $\chi_L(x)\downarrow$ pro každý vstup $x \in \Sigma^*$
- $M(x)$ vypíše na výstup hodnotu $\chi_L(x)$ (1 pokud $x \in L$, jinak 0)
- Popíšeme Turingův stroj $M'(x)$, který
  - přijímá L ($L = L(M')$) a
  - $M'(x)\downarrow$ pro každý vstup $x \in \Sigma^*$

Výpočet M' se vstupem x

```
Simuluj M(x)
if M vypsal 1 then
│  přijmi
else
└  odmítni
```

Přijetí nebo zastavení

Věta

Jazyk L je částečně rozhodnutelný, právě když existuje Turingův stroj M splňující

$$L = \{x \in \Sigma^* \mid M(x)\downarrow\} \tag{1}$$

Důkaz.

Ve dvou krocích

„$\Longrightarrow$“ L je částečně rozhodnutelný $\Longrightarrow$ existuje M splňující (1)

„$\Longleftarrow$“ Existuje M splňující (1) $\Longrightarrow$ L je částečně rozhodnutelný

□

Důkaz „$\Longrightarrow$“

- Předpokládáme, že L je částečně rozhodnutelný
- Existuje Turingův stroj M', který přijímá L ($L = L(M')$)
- Popíšeme Turingův stroj M, který splňuje

$$L = \{x \in \Sigma^* \mid M(x)\downarrow\}$$

Výpočet M se vstupem x

1 Simuluj $M'(x)$
2 **if** $M'(x)$ odmítl **then**
3   vstup do nekonečného cyklu

- Pro každý řetězec $x \in \Sigma^*$

$$x \in L \Longleftrightarrow M'(x) \text{ přijme} \Longleftrightarrow M(x)\downarrow$$

Důkaz „ $\Longleftarrow$ “

- Předpokládejme, že M je Turingův stroj splňující

$$L = \{x \in \Sigma^* \mid M(x)\downarrow\}$$

- Popíšeme Turingův stroj M', který přijímá L ($L = L(M')$)

Výpočet M' se vstupem x

1. Simuluj $M(x)$
2. Přijmi

- Platí

$$x \in L \Longleftrightarrow M(x)\downarrow \Longleftrightarrow x \in L(M')$$

- Tedy $L = L(M')$

Domény algoritmicky vyčíslitelných funkcí

Věta

Jazyk L je částečně rozhodnutelný, právě když existuje algoritmicky vyčíslitelná funkce f splňující

$$L = \operatorname{dom} f = \{x \in \Sigma^* \mid f(x)\downarrow\} \tag{2}$$

Důkaz.

- L je částečně rozhodnutelný, právě když existuje TS M splňující

$$L = \{x \in \Sigma^* \mid M(x)\downarrow\} \tag{3}$$

(2) $\Longrightarrow$ (3) M počítá funkci f

(3) $\Longrightarrow$ (2) f je funkce počítaná strojem M

$\square$

Existenční kvantifikace

Věta

Jazyk L je částečně rozhodnutelný, právě když existuje rozhodnutelný jazyk B splňující

$$L = \{x \in \Sigma^* \mid (\exists y \in \Sigma^*)[\langle x, y \rangle \in B]\} \tag{4}$$

Důkaz.

Důkaz ve dvou krocích

„$\Longrightarrow$“ L je částečně rozhodnutelný $\Longrightarrow$ existuje rozhodnutelný jazyk B splňující (4)

„$\Longleftarrow$“ existuje rozhodnutelný jazyk B splňující (4) $\Longrightarrow$ L je částečně rozhodnutelný

$\square$

Důkaz „ $\Longrightarrow$ “

- Předpokládáme, že L je částečně rozhodnutelný
- Existuje Turingův stroj M přijímající L ($L = L(M)$)
- Platí

$$L = \{x \mid (\exists n \in \mathbb{N})[\underbrace{M(x) \text{ přijme do } n \text{ kroků}}_{\substack{\text{Rozhodnutelná podmínka,} \\ \text{stačí simulovat } M(x) \text{ po } n \text{ kroků}}}]\}$$

- Stačí tedy definovat

$$B = \{\langle x, \langle n \rangle \rangle \mid M(x) \text{ přijme do } n \text{ kroků}\}$$

- Jazyk B je rozhodnutelný a splňuje

$$L = \{x \in \Sigma^* \mid (\underbrace{\exists y \in \Sigma^*}_{y=\langle n \rangle})[\quad \underbrace{\langle x, y \rangle \in B}_{M(x) \text{ přijme do } n \text{ kroků}} \quad]\}$$

Důkaz „ $\Longleftarrow$ “

- Předpokládáme, že existuje rozhodnutelný jazyk B splňující

$$L = \{x \in \Sigma^* \mid (\exists y \in \Sigma^*)[\langle x, y \rangle \in B]\}$$

- Popíšeme Turingův stroj M přijímající L ($L = L(M)$)

Výpočet M se vstupem x

```
forall y ∈ Σ* v lexikografickém uspořádání do
    if ⟨x, y⟩ ∈ B then
        přijmi
```

- $x \in L \implies (\exists y \in \Sigma^*)[\langle x, y \rangle \in B] \implies M(x)$ přijme
- $x \notin L \implies (\forall y \in \Sigma^*)[\langle x, y \rangle \notin B] \implies M(x)\uparrow$
- Dohromady $L = L(M)$

Existenční kvantifikace (příklad)

Příklad

$$
\begin{aligned}
L_u &= \{\langle M, x\rangle \mid x \in L(M)\} \\
&= \{\langle M, x\rangle \mid (\exists n \in \mathbb{N})[\underbrace{M(x) \text{ přijme do } n \text{ kroků}}_{\substack{\text{Rozhodnutelná podmínka,} \\ \text{stačí simulovat } M(x) \text{ po } n \text{ kroků}}}]\}
\end{aligned}
$$

- Následující jazyk je rozhodnutelný

$$B = \{\langle M, x, n\rangle \mid M(x) \text{ přijme do } n \text{ kroků}\}$$

- Částečně rozhodnutelný jazyk L_u můžeme zapsat jako

$$L_u = \{\langle M, x\rangle \mid (\exists n \in \mathbb{N})[\langle M, x, n\rangle \in B]\}$$

Uzavřenost na existenční kvantifikaci

Důsledek

Je-li B částečně rozhodnutelný jazyk, pak jazyk

$$A = \{x \in \Sigma^* \mid (\exists y \in \Sigma^*)[\langle x, y \rangle \in B]\}$$

je též částečně rozhodnutelný.

Důkaz.

- Existuje rozhodnutelný jazyk C splňující

$$B = \{\langle x, y \rangle \in \Sigma^* \mid (\exists z \in \Sigma^*)[\langle x, y, z \rangle \in C]\}$$

- Platí $A = \{x \in \Sigma^* \mid (\exists \langle y, z \rangle \in \Sigma^*)[\langle x, y, z \rangle \in C]\}$
- A je částečně rozhodnutelný dle předchozí věty

$\square$

Uzavřenost na existenční kvantifikaci (příklad)

Příklad

$$\begin{aligned}\mathrm{NE} &= \{\langle M\rangle \mid L(M) \neq \emptyset\}\\ &= \{\langle M\rangle \mid (\exists x \in \Sigma^*)[x \in L(M)]\}\\ &= \{\langle M\rangle \mid (\exists x \in \Sigma^*)[\langle M, x\rangle \in L_u]\}\end{aligned}$$

- Jazyk L_u je částečně rozhodnutelný
- NE je tedy též částečně rozhodnutelný

Vyčíslitelnost jazyků

Enumerátor

Enumerátorem pro jazyk L je Turingův stroj E, který

- ignoruje svůj vstup,
- vypisuje řetězce $w \in L$ na vyhrazenou výstupní pásku
  - například oddělené $\#$
- každý řetězec $w \in L$ je někdy vypsán TS E
- Je-li L nekonečný, E svou činnost nikdy neskončí

Enumerátor pro jazyk NE

$$\mathrm{NE} = \{\langle M \rangle \mid L(M) \neq \emptyset\}$$

- Enumerátor pro jazyk NE řeší následující úlohu:
  - Vypiš kódy Turingových strojů, které přijímají alespoň jedno slovo

---

Enumerátor pro jazyk NE

---

forall $\langle M, x, n \rangle \in \Sigma^*$ v lexikografickém uspořádání **do**
    Simuluj výpočet $M(x)$ po nejvýš n kroků
    if $M(x)$ přijal **then**
        Zapiš $\langle M \rangle$ na výstup

- Každý kód $\langle M \rangle \in \mathrm{NE}$ je vypsán nekonečný počet krát
- Stroje jsou vypisovány v neurčeném pořadí

Enumerátor pro jazyk NE

$$\mathrm{NE} = \{\langle M\rangle \mid L(M) \neq \emptyset\}$$

Upravíme enumerátor tak, aby každý kód stroje M s neprázdným jazykem byl vypsán právě jednou

Enumerátor jazyka NE

$S \leftarrow$ prázdný seznam řetězců
forall $\langle M, x, n\rangle \in \Sigma^*$ v lexikografickém uspořádání **do**
  Simuluj výpočet $M(x)$ po nejvýš n kroků
  if $M(x)$ přijal **and** $\langle M\rangle \notin S$ **then**
    Zapiš $\langle M\rangle$ na výstup
    Přidej $\langle M\rangle$ do seznamu S

Vyčíslitelnost částečně rozhodnutelných jazyků

Věta

Jazyk L je částečně rozhodnutelný, právě když pro něj existuje enumerátor E.

Důkaz.

Důkaz ve dvou krocích

„ $\Longrightarrow$ “ L je částečně rozhodnutelný $\Longrightarrow$ existuje enumerátor E pro L

„ $\Longleftarrow$ “ Existuje enumerátor E pro L $\Longrightarrow$ L je částečně rozhodnutelný

□

Důkaz „ $\Longrightarrow$ “

- L je částečně rozhodnutelný
- Existuje rozhodnutelný jazyk B splňující

$$L = \{x \in \Sigma^* \mid (\exists y \in \Sigma^*)[\langle x, y\rangle \in B]\}$$

Enumerátor E jazyka L

---

forall $\langle x, y\rangle \in \Sigma^*$ v lexikografickém uspořádání **do**
    if $\langle x, y\rangle \in B$ **then**
        Zapiš x na výstup

- Lze upravit tak, aby E vypsal každé slovo $x \in L$ právě jednou.
- Prvky L jsou vypisovány v neznámém pořadí

Důkaz „ $\Longleftarrow$ “

- Máme enumerátor E pro jazyk L
- Popíšeme Turingův stroj M přijímající L ($L = L(M)$)

Výpočet M se vstupem x

Simuluj E a sleduj výstup
if E vypsal x **then**
  přijmi

$x \in L \implies E$ někdy vypíše x a $M(x)$ přijme

$x \notin L \implies E$ nikdy nevypíše x a $M(x)$ nepřijme (zacyklí se)

Dohromady $L = L(M)$

Enumerátor pro jazyk prvočísel

$$\mathrm{PRIME} = \{\langle p \rangle \mid p \text{ je prvočíslo}\}$$

Úloha: vypisuj prvočísla v rostoucím pořadí

Enumerátor prvočísel

```
forall p ∈ ℕ v rostoucím pořadí do
    if p je prvočíslo then
        Zapiš ⟨p⟩ na výstup
```

Lze zkonstruovat díky tomu, že jazyk PRIME je rozhodnutelný.

Vyčíslitelnost rozhodnutelných jazyků

Věta

Jazyk L je rozhodnutelný, právě když pro něj existuje enumerátor E, který navíc vypisuje prvky L v lexikografickém pořadí.

Důkaz.

Důkaz ve dvou krocích

„$\Longrightarrow$“ L je rozhodnutelný $\Longrightarrow$ existuje enumerátor E pro L, který vypisuje prvky L v lexikografickém pořadí

„$\Longleftarrow$“ Existuje enumerátor E pro L, který vypisuje prvky L v lexikografickém pořadí $\Longrightarrow$ L je rozhodnutelný

□

Důkaz „ $\Longrightarrow$ “

- L je rozhodnutelný
- Popíšeme enumerátor E, který vypisuje slova L v lexikografickém pořadí

Enumerátor E jazyka L

```
// Podmínku lze ověřit díky rozhodnutelnosti L
forall x ∈ Σ* v lexikografickém uspořádání do
    if x ∈ L then
        Zapiš x na výstup
```

V případě, že L je konečný jazyk, E se po vypsání posledního slova z L zacyklí.

Důkaz „ $\Longleftarrow$ “

- Máme enumerátor E pro jazyk L
- E vypisuje prvky L v rostoucím lexikografickém pořadí
- Rozlišíme dva případy
  1. L je konečný jazyk $\Longrightarrow$ L je rozhodnutelný
     - Všechny konečné jazyky jsou rozhodnutelné
  2. L je nekonečný jazyk $\Longrightarrow$ popíšeme stroj M, který rozhoduje L

Výpočet M se vstupem x

Simuluj E a sleduj výstup
if E vypsal x **then**
    přijmi
if E vypsal řetězec $y > x$ **then**
    odmítni

L je nekonečný $\Longrightarrow$ vždy existuje $y > x$ $\Longrightarrow$ algoritmus skončí

Vyčíslitelnost jazyků a funkce

Důsledek

Nekonečný jazyk L je částečně rozhodnutelný, právě když je oborem hodnot nějaké totální algoritmicky vyčíslitelné funkce f (tj. $L = \operatorname{rng} f$).

„ $\Longrightarrow$ “ L částečně rozhodnutelný

- máme enumerátor E pro L
- Pro jednoduchost uvažujeme parametry f typu $\mathbb{N}$
- pro $i \in \mathbb{N}$ definujeme

$$f(i) = (i+1)\text{-ní řetězec vypsaný } E$$

- E vypisuje právě řetězce z L
- Možné hodnoty f jsou právě řetězce z L

Vyčíslitelnost jazyků a funkce

Důsledek

Nekonečný jazyk L je částečně rozhodnutelný, právě když je oborem hodnot nějaké totální algoritmicky vyčíslitelné funkce f (tj. $L = \operatorname{rng} f$).

„$\Longleftarrow$“ Máme funkci f

- Popíšeme enumerátor E pro L

Výpočet E

---

forall $y \in \Sigma^*$ v lexikografickém pořadí **do**
  Zapiš $f(y)$ na výstup

- $x \in L$

  $\Leftrightarrow$ existuje y pro nějž $f(y) = x$

  $\Leftrightarrow$ E vypíše x

Vyčíslitelnost rozhodnutelných jazyků a funkce

Definice

Funkce $f : \Sigma^* \to \Sigma^*$ je rostoucí, pokud platí, že $u < v$ implikuje $f(u) < f(v)$ pro každé dva řetězce $u, v \in \Sigma^*$, kde $f(u)\downarrow$ a $f(v)\downarrow$.

Důsledek

Nekonečný jazyk L je rozhodnutelný, právě když je oborem hodnot nějaké rostoucí totální algoritmicky vyčíslitelné funkce f (tj. $L = \operatorname{rng} f$).

Vyčíslitelnost rozhodnutelných jazyků a funkce

Důsledek

Nekonečný jazyk L je rozhodnutelný, právě když je oborem hodnot nějaké rostoucí totální algoritmicky vyčíslitelné funkce f (tj. $L = \operatorname{rng} f$).

„$\Longrightarrow$“ L je rozhodnutelný

- Máme enumerátor E, který vypisuje prvky L v rostoucím lexikografickém pořadí
- Pro jednoduchost uvažujeme parametry f typu $\mathbb{N}$
- Pro $i \in \mathbb{N}$ definujeme

$$f(i) = (i+1)\text{-ní řetězec vypsaný } E$$

- E vypisuje právě řetězce z L
- Možné hodnoty f jsou právě řetězce z L
- f je rostoucí, protože E vypisuje prvky L v rostoucím lexikografickém pořadí

Vyčíslitelnost rozhodnutelných jazyků a funkce

Důsledek

Nekonečný jazyk L je rozhodnutelný, právě když je oborem hodnot nějaké rostoucí totální algoritmicky vyčíslitelné funkce f (tj. $L = \operatorname{rng} f$).

„$\Longleftarrow$“ Máme funkci f

- Popíšeme enumerátor E pro L

Výpočet E

---

1 **forall** $y \in \Sigma^*$ v lexikografickém pořadí **do**
2 Zapiš $f(y)$ na výstup

- E vypisuje právě prvky L v lexikografickém pořadí, protože f je rostoucí
- E tedy ukazuje, že L je rozhodnutelný

Převoditelnost a úplnost

Jak ukazovat nerozhodnutelnost?

Intuitivní postup důkazu nerozhodnutelnosti

Chceme ukázat, že A je nerozhodnutelný jazyk.

1. Vybereme si jiný nerozhodnutelný jazyk B
   - například $B = L_u$
2. Sporem předpokládáme: Máme algoritmus D_A, který rozhoduje A
3. Popíšeme algoritmus D_B, který rozhoduje B
   - D_B může volat D_A jako podprogram
4. Dostáváme spor s nerozhodnutelností B
5. Ukázali jsme, že A není rozhodnutelný

Turingovská převoditelnost

Definice (Turingovská převoditelnost, lehce neformálně)

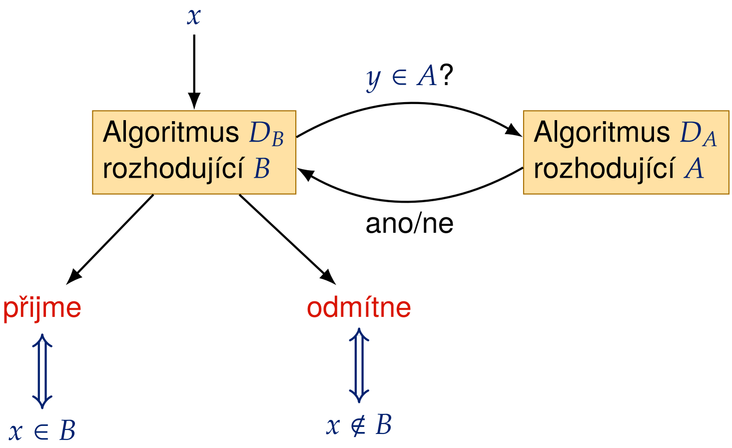
Jazyk $B \subseteq \Sigma^*$ je Turingovsky převoditelný na jazyk $A \subseteq \Sigma^*$, pokud existuje algoritmus (Turingův stroj) D_B, pro který platí

- D_B rozhoduje B
  - $B = L(D_B)$ a
  - $D_B(x)\downarrow$ pro každý vstup $x \in \Sigma^*$
- D_B může pokládat dotazy orákulu A, tedy
  - Kdykoli se D_B může o libovolném řetězci $y \in \Sigma^*$ zeptat, jestli $y \in A$
  - Tyto dotazy jsou okamžitě správně zodpovězeny (ano/ne)
  - Dotazovat se D_B může libovolný počet krát

- Označíme pomocí $B \leq_T A$.
- Je-li B nerozhodnutelný, je nerozhodnutelný i A
- Pro každý jazyk B platí, že $B \leq_T \overline{B}$
  - Stačí jeden dotaz a znegovat odpověď

Turingovská převoditelnost (princip)

$B \leq_T A$ = „pomocí A umíme rozhodnout B“



Problém zastavení

Problém zastavení (Halting problem)

Instance: Kód Turingova stroje M a vstup x.

Otázka: Zastaví se výpočet Turingova stroje M nad vstupem x, tedy $M(x)\downarrow$?

- Odpovídá jazyku $\mathrm{HALT} = \{\langle M, x\rangle \mid M(x)\downarrow\}$

Věta

Jazyk HALT je částečně rozhodnutelný, ale není rozhodnutelný.

Částečná rozhodnutelnost HALT

$$\mathrm{HALT} = \{\langle M, x\rangle \mid M(x)\downarrow\}$$

- Jazyk HALT je částečně rozhodnutelný
- Plyne z existence univerzálního stroje $\mathcal{U}$
- Stroj $\mathcal{H}$ přijímající HALT se vstupem $\langle M, x\rangle$
  1. Simuluje $M(x)$
  2. Po ukončení simulace přijme

Nerozhodnutelnost HALT

$$\mathrm{HALT} = \{\langle M, x\rangle \mid M(x)\downarrow\}$$

- Jazyk HALT je nerozhodnutelný
- Sporem: Nechť $\mathcal{H}$ je stroj rozhodující HALT
  - $\mathrm{HALT} = L(\mathcal{H})$ a
  - $\mathcal{H}(\langle M, x\rangle)\downarrow$ pro každý Turingův stroj M a vstup x
- Popíšeme Turingův stroj M_u, který rozhoduje $L_u = \{\langle M, x\rangle \mid x \in L(M)\}$

Stroj M_u rozhodující L_u s pomocí HALT

Výpočet stroje M_u se vstupem $\langle M, x\rangle$

Sestroj Turingův stroj M', který se řídí následujícím algoritmem
begin // Výpočet M' se vstupem y
  Pusť $M(y)$
  if M zamítl **then**
    vstup do nekonečné smyčky

// HALT je podle předpokladu rozhodnutelný
if $\langle M', x\rangle \in \mathrm{HALT}$ **then**
  přijmi
else
  odmítni

Stroj M_u rozhoduje L_u

Nerozhodnutelnost HALT

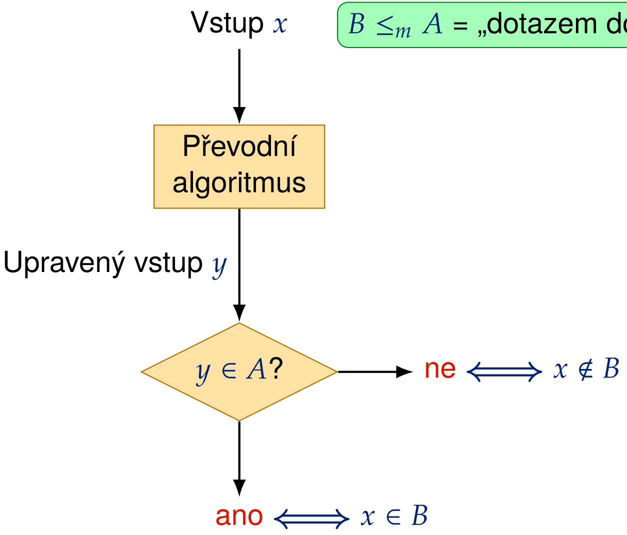
- Za předpokladu rozhodnutelnosti HALT jsme sestavili M_u, který rozhoduje L_u
- Víme, že L_u není rozhodnutelný
- Stroj M_u nemůže existovat
- Jazyk HALT tedy není rozhodnutelný

Ukázali jsme, že $L_u \leq_T \mathrm{HALT}$

- Program M_u je velmi specifický
  - Orákula HALT se ptá jen jednou na konec
  - Odpověď dotazu HALT je přímo odpovědí M_u
- Program ukazuje, že L_u je m-převoditelný na HALT

m-převoditelnost (princip)

$B \leq_m A$ = „dotazem do A rozhodneme B“

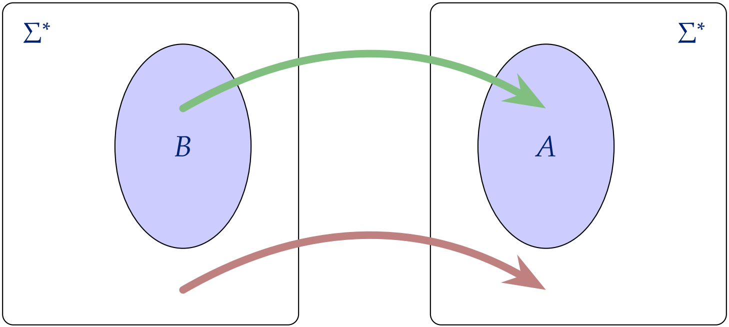


m-převoditelnost (definice)

Definice

Jazyk B je m-převoditelný na jazyk A, pokud existuje totální vyčíslitelná funkce f splňující

$$(\forall x \in \Sigma^*)[x \in B \Leftrightarrow f(x) \in A]$$



m-převoditelnost (definice)

Definice

Jazyk B je m-převoditelný na jazyk A, pokud existuje totální vyčíslitelná funkce f splňující

$$(\forall x \in \Sigma^*)[x \in B \Leftrightarrow f(x) \in A]$$

- Označíme pomocí $B \leq_m A$
- $\leq_m$ je reflexivní a tranzitivní relace (kvaziuspořádání).
- Pokud $A \leq_m B$ a B je (částečně) rozhodnutelný jazyk, pak totéž lze říct o A.

$$\underbrace{\overline{L_u}}_{\text{není částečně rozhodnutelný}} \quad \not\leq_m \quad \underbrace{L_u}_{\text{částečně rozhodnutelný}}$$

m-převoditelnost (reflexivita)

Lemma (Reflexivita m-převoditelnosti)

Pro každý jazyk A platí $A \leq_m A$

Důkaz.

- Identita $\mathrm{id}(x) = x$ je totální algoritmicky vyčíslitelná funkce
- Pro každý řetězec $x \in \Sigma^*$ platí

$$x \in A \Leftrightarrow \mathrm{id}(x) \in A$$

$\square$

m-převoditelnost (tranzitivita)

Lemma (Tranzitivita m-převoditelnosti)

Pro každé jazyky A, B a C platí $A \leq_m B \wedge B \leq_m C \implies A \leq_m C$

- $A \leq_m B$ pomocí funkce g
- $B \leq_m C$ pomocí funkce h
- Definujme funkci $f(x) = h(g(x))$
  - f je totální algoritmicky vyčíslitelná funkce
- Pro každý řetězec $x \in \Sigma^*$ platí

$$x \in A \underbrace{\iff}_{A \leq_m B} g(x) \in B \underbrace{\iff}_{B \leq_m C} h(g(x)) \in C \quad \underbrace{\iff}_{f(x)=h(g(x))} \quad f(x) \in C$$

- $A \leq_m C$ pomocí funkce f

m-převoditelnost porovnává obtížnost

Lemma

Nechť B a A jsou dva jazyky, pro něž platí, že $B \leq_m A$.

1. *A rozhodnutelný $\Longrightarrow$ B je rozhodnutelný*
2. *A částečně rozhodnutelný $\Longrightarrow$ B je částečně rozhodnutelný*

- Předpokládejme, že M_A je TS, který přijímá/rozhoduje A
- Popíšeme TS M_B, který přijímá/rozhoduje B

Výpočet stroje M_B se vstupem x

```
y ← f(x)                    // f ukazuje, že B ≤_m A
Pusť M_A(y)
if M_A přijal then
    přijmi
else
    odmítni
```

m-převoditelnost a nerozhodnutelnost

Lemma

Nechť B a A jsou dva jazyky, pro něž platí, že $B \leq_m A$.

1. *A je rozhodnutelný $\Longrightarrow$ B je rozhodnutelný*
2. *A je částečně rozhodnutelný $\Longrightarrow$ B je částečně rozhodnutelný*

Důsledek

Nechť B a A jsou dva jazyky, pro něž platí, že $B \leq_m A$.

1. *B je nerozhodnutelný $\Longrightarrow$ A je nerozhodnutelný*
2. *B není částečně rozhodnutelný $\Longrightarrow$ A není částečně rozhodnutelný*