# IB107 Vyčíslitelnost a složitost

## rekurzivní a r.e. množiny, standardní numerace r.e. množin

Jan Strejček

Fakulta informatiky
Masarykova univerzita

# rekurzivní množiny

## Definice (rekurzivní množina)

*Množina* $A \subseteq \mathbb{N}^k$ *je rekurzivní, pokud existuje totálně vyčíslitelná funkce* $f : \mathbb{N}^k \to \mathbb{N}$ *taková, že*

$$A = f^{-1}(\{1\}) = \{(x_1, \ldots, x_k) \in \mathbb{N}^k \mid f(x_1, \ldots, x_k) = 1\}.$$

*Funkce $f$ se nazývá rozhodovací funkce pro $A$.*

- rekurzivní množině se také říká rozhodnutelná či řešitelná
- příklady rekurzivních množin:

# rekurzivní množiny

**Tvrzení**

*$A \subseteq \mathbb{N}^k$ je rekurzivní, právě když je její charakteristická funkce $\chi_A : \mathbb{N}^k \to \mathbb{N}$ definovaná vztahem*

$$\chi_A(x_1, \ldots, x_k) = \begin{cases} 1 & \textit{pokud } (x_1, \ldots, x_k) \in A \\ 0 & \textit{jinak} \end{cases}$$

*totálně vyčíslitelná.*

**Důkaz:**

■

# vlastnosti rekurzivních množin

**Tvrzení**

*Jestliže $A \subseteq \mathbb{N}^k$ je konečná množina nebo $\mathbb{N}^k \smallsetminus A$ je konečná, pak $A$ je rekurzivní.*

**Důkaz:**

$\blacksquare$

# vlastnosti rekurzivních množin

## Lemma

*Nechť $A, B \subseteq \mathbb{N}^k$ jsou rekurzivní množiny. Pak i množiny $\overline{A}$, $A \cup B$ a $A \cap B$ jsou rekurzivní.*

**Důkaz:**

$\blacksquare$

# rekurzivně spočetné množiny

### Definice (rekurzivně spočetná množina)

*Množina $B \subseteq \mathbb{N}$ je rekurzivně spočetná, právě když $B = \emptyset$ nebo existuje totálně vyčíslitelná funkce $f : \mathbb{N} \to \mathbb{N}$ taková, že $B = range(f)$. Funkce $f$ se nazývá numerující funkce pro $B$.*

- rekurzivně spočetné množině se také říká částečně rozhodnutelná, rekurzivně vyčíslitelná nebo jen r.e. (z anglického recursively enumerable).
- definici lze rozšířit na množiny $B \subseteq \mathbb{N}^k$

# vztahy rekurzivních a r.e. množin

**Věta**

*Každá rekurzivní množina* $A \subseteq \mathbb{N}$ *je také rekurzivně spočetná.*

**Důkaz:**

■

# vztahy rekurzivních a r.e. množin

## Věta

1. *Existuje množina* $A \subseteq \mathbb{N}$, *která není rekurzivní.*
2. *Existuje množina* $B \subseteq \mathbb{N}$, *která není r.e.*

**Důkaz: (pomocí mohutnosti)** Rekurzivních i r.e. množin je spočetně mnoho, ale $\mathbb{N}$ má nespočetně mnoho podmnožin.

**(diagonalizací)** $A = \{i \in \mathbb{N} \mid \varphi_i(i) \neq 1\}$

$B = \{i \in \mathbb{N} \mid i \notin range(\varphi_i)\}$

∎

# vztahy rekurzivních a r.e. množin

**Věta**

*Množina $A \subseteq \mathbb{N}$ je rekurzivní, právě když $A$ i $\overline{A}$ jsou r.e.*

**Důkaz:**

$\Longrightarrow$ je-li $A$ rekurzivní, pak je rekurzivní i $\overline{A}$ a každá rekurzivní množina je také r.e.

$\Longleftarrow$

- je-li $A = \emptyset$ nebo $\overline{A} = \emptyset$, pak $A$ je rekurzivní
- nechť $A \neq \emptyset \neq \overline{A}$ jsou r.e., pak $A = \mathit{range}(f)$ a $\overline{A} = \mathit{range}(g)$ pro nějaké totálně vyčíslitelné funkce $f, g : \mathbb{N} \to \mathbb{N}$
- platí $\mathit{range}(f) \cap \mathit{range}(g) = \emptyset$ a $\mathit{range}(f) \cup \mathit{range}(g) = \mathbb{N}$
- charakteristickou funkci $\chi_A(x)$ počítáme takto:
  1. počítáme $f(0), g(0), f(1), g(1), \ldots$ dokud nedostaneme $x$
  2. pokud $x = f(n)$ pro nějaké $n$, pak vrátíme 1
  3. pokud $x = g(n)$ pro nějaké $n$, pak vrátíme 0
- $\chi_A$ je vyčíslitelná, tedy $A$ je rekurzivní

∎

# funkce Step counter

**Lemma**

*Funkce*

$$Sc(x,y,z) = \begin{cases} 1 & \textit{jestliže program } P_x \textit{ zastaví pro vstup } y \\ & \textit{během } z \textit{ kroků} \\ 0 & \textit{jinak} \end{cases}$$

*je totálně vyčíslitelná.*

**Důkaz:** interpreter z důkazu věty o numeraci rozšíříme o počítání instrukcí

∎

# programy jako generátory

- rozšíříme jazyk while-programů o příkaz *output*$(x_i)$

**Tvrzení**

*Množina $A$ je r.e., právě když existuje program $P$ (bez vstupních proměnných), který pomocí instrukce output během svého (potenciálně nekonečného) běhu dá na výstup právě všechny prvky $A$.*

**Důkaz:**

$\Longleftarrow$

- pokud program $P$ na výstup nic nedá, pak $A = \emptyset$ je r.e.
- nechť program generuje množinu výstupů $A \neq \emptyset$
- nechť $a \in A$, pak $A = range(f)$ pro

$$f(x) = \begin{cases} y & \text{pokud } P \text{ dá v } x\text{-tém kroku na výstup } y \\ a & \text{jinak} \end{cases}$$

- $f$ je totálně vyčíslitelná

# programy jako generátory

$\Longrightarrow$

- pro $A = \emptyset$ zřejmé
- nechť $A = \mathit{range}(f)$ pro tot. vyčíslitelnou funkci $f : \mathbb{N} \to \mathbb{N}$
- nechť $f$ je počítána programem $P_e$
- pak $A$ je generována tímto programem

**begin**
  $n := 0;$
  **while** *true* **do** **begin**
    $x := \pi_1(n);$
    $y := \pi_2(n);$
    **if** $Sc(e, x, y) = 1$ **then** **begin** $P_e(x);\ \mathit{output}(x_1)$ **end**;
    $n := n + 1;$
  **end**
**end**

$\blacksquare$

# množiny a problémy

Problém rozhodnout, zda dané $x$ má vlastnost $V$ ztotožníme s množinou $\{x \mid x \text{ má vlastnost } V\}$.

**Příklad:** problém, zda $n$ je prvočíslo, ztotožníme s množinou

$$\{n \in \mathbb{N} \mid n \text{ je prvočíslo}\}$$

## Terminologie

Nechť $M$ je množina odpovídající danému problému. Tento problém je

- rozhodnutelný, právě když $M$ je rekurzivní,
- částečně rozhodnutelný (semirozhodnutelný), právě když $M$ je r.e.

Problém, který není rozhodnutelný, se nazývá nerozhodnutelný.

# problém zastavení

Problém zastavení, tedy problém, zda program $P_i$ zastaví na vstupu $i$, ztotožníme s množinou

$$\begin{aligned} K &= \{i \in \mathbb{N} \mid P_i \text{ zastaví nad vstupu } i\} \\ &= \{i \in \mathbb{N} \mid \varphi_i(i) \text{ je definováno}\}. \end{aligned}$$

Dříve jsme dokázali, že charakteristická funkce

$$\chi_K(i) = f(i) = \begin{cases} 1 & \text{jestliže } \varphi_i(i) \text{ je definováno} \\ 0 & \text{jestliže } \varphi_i(i) \text{ není definováno} \end{cases}$$

není vyčíslitelná. Proto $K$ není rekurzivní a tedy problém zastavení je nerozhodnutelný.

# problém zastavení

**Věta**

*Množina* $K = \{i \mid \varphi_i(i)$ *je definováno*$\}$ *je rekurzivně spočetná.*

**Důkaz:** Množina $K$ je generována programem

```
begin
   n := 0;
   while true do begin
         x := π1(n);
         y := π2(n);
         if Sc(x, x, y) = 1 then output(x);
         n := n + 1;
   end
end
```

∎

Proto problém zastavení je částečně rozhodnutelný.

# problém zastavení

**Věta**

*Množina* $\overline{K} = \{i \mid \varphi_i(i) = \bot\}$ *není rekurzivně spočetná.*

**Důkaz:**

- množina $K$ je rekurzivně spočetná
- pokud by $\overline{K}$ byla také rekurzivně spočetná, tak by $K$ bylo rekurzivní, což není $\blacksquare$

**Shrnutí:**

# rekurzivně spočetné množiny v rostoucím pořádku

## Definice

*Množina $A \subseteq \mathbb{N}$ je rekurzivně spočetná v rostoucím pořádku, právě když má rostoucí numerující funkci.*

## Lemma

*Nekonečná množina $A \subseteq \mathbb{N}$ je rekurzivní, právě když je rekurzivně spočetná v rostoucím pořádku.*

**Důkaz:**

$\Longleftarrow$

- nechť $A = range(f)$ pro rostoucí tot. vyčíslitelnou funkci $f$
- $\chi_A$ je počítána programem

**begin** $n := 0$;
  **while** $f(n) < x_1$ **do** $n := n + 1$;
  **if** $f(n) = x_1$ **then** $x_1 := 1$ **else** $x_1 := 0$
**end**

# rekurzivně spočetné množiny v rostoucím pořádku

$\Longrightarrow$

- $A$ je nekonečná a rekurzivní, tedy $\chi_A$ je vyčíslitelná
- $A$ je generována v rostoucím pořádku programem

<u>**begin**</u>
    $n := 0$;
    <u>**while**</u> *true* <u>**do**</u> <u>**begin**</u>
            <u>**if**</u> $\chi_A(n) = 1$ <u>**then**</u> $\mathit{output}(n)$;
            $n := n + 1$;
    <u>**end**</u>
<u>**end**</u>

- funkce $f(i)$ vracející $i$-tý prvek z generovaného seznamu je totálně vyčíslitelná
- přitom $f$ je rostoucí a $A = \mathit{range}(f)$
- tedy $A$ je rekurzivně spočetná v rostoucím pořádku ■

# rekurzivně spočetné množiny v rostoucím pořádku

## Důsledek

*Každá nekonečná r.e. množina $A$ má nekonečnou rekurzivní podmnožinu $B$.*

**Důkaz:**

- nechť $f$ je numerující funkce pro $A$
- uvažme podmnožinu $B \subseteq A$, kterou generuje program

```
begin
   n := 0;  m := 0;
   while true do begin
         if f(n) > m then begin m := f(n); output(m) end;
         n := n + 1;
   end
end
```

- $B$ je nekonečná a generovaná v rostoucím pořádku
- tedy $B$ je r.e. v rostoucím pořádku a tudíž rekurzivní ■

# alternativní charakterizace r.e. množin

**Věta**

1. *Množina* $A \subseteq \mathbb{N}$ *je rekurzivně spočetná, právě když* $A = dom(g)$ *pro nějakou vyčíslitelnou funkci* $g : \mathbb{N} \to \mathbb{N}$.
2. *Množina* $A \subseteq \mathbb{N}$ *je rekurzivně spočetná, právě když* $A = range(g)$ *pro nějakou vyčíslitelnou funkci* $g : \mathbb{N} \to \mathbb{N}$.

# alternativní charakterizace r.e. množin

**Důkaz:**

1. $A$ je r.e. $\iff$ $\exists$ vyčíslitelná funkce $g$ tak, že $A = dom(g)$

$\Longrightarrow$
- $A = \emptyset$
- $A \neq \emptyset$ je r.e., pak $A = range(f)$ pro tot. vyčíslitelnou funkci $f$

# alternativní charakterizace r.e. množin

1. $A$ je r.e. $\iff$ $\exists$ vyčíslitelná funkce $g$ tak, že $A = dom(g)$

$\Longleftarrow$

- $A = dom(g) = \emptyset$
- $A = dom(g) \neq \emptyset$, pak nechť $a_0 \in A$

# alternativní charakterizace r.e. množin

2. $A$ je r.e. $\iff$ $\exists$ vyčíslitelná funkce $g$ tak, že $A = range(g)$

$\Longrightarrow$
- $A = \emptyset$
- $A \neq \emptyset$ je r.e., pak $A = range(f)$ pro tot. vyčíslitelnou funkci $f$
- položíme $g = f$

$\Longleftarrow$
- $A = range(g) = \emptyset$
- $A = range(g) \neq \emptyset$, pak nechť $a_0 \in A$

# možné numerace r.e. množin

$$dom(\varphi_0), dom(\varphi_1), dom(\varphi_2), \ldots$$

$$range(\varphi_0), range(\varphi_1), range(\varphi_2), \ldots$$

**Věta**

*Existují totálně vyčíslitelné funkce $f, g : \mathbb{N} \to \mathbb{N}$ takové, že pro všechna $i \in \mathbb{N}$ platí vztahy:*

1. $dom(\varphi_i) = range(\varphi_{f(i)})$
2. $range(\varphi_i) = dom(\varphi_{g(i)})$

**Důkaz:**

1. $\mathit{dom}(\varphi_i) = \mathit{range}(\varphi_{f(i)})$

2. $\mathit{range}(\varphi_i) = \mathit{dom}(\varphi_{g(i)})$

$\blacksquare$

# standardní numerace r.e. množin

**Definice (standardní numerace r.e. množin)**

*Standardní numerací r.e. množin nazveme funkci* $W : \mathbb{N} \to \{A \subseteq \mathbb{N} \mid A \text{ je r.e.}\}$ *definovanou vztahem*

$$W(i) = dom(\varphi_i).$$

*Index r.e. množiny* $A \subseteq \mathbb{N}$ *je číslo* $i$ *splňující* $A = W(i)$.

- místo $W(0), W(1), \ldots$ píšeme $W_0, W_1, \ldots$
- množinu $W_i$ lze chápat jako akceptovanou programem $P_i$: program $P_i$ akceptuje $n \in \mathbb{N}$, jestliže $P_i$ zastaví pro vstup $n$

# r.e. relace a standardní numerace r.e. relací

**Definice (rekurzivně spočetná relace)**

*Relace $A \subseteq \mathbb{N}^j$ je rekurzivně spočetná (r.e.), právě když existuje vyčíslitelná funkce $f : \mathbb{N}^j \to \mathbb{N}$ taková, že $A = dom(f)$.*

**Definice (standardní numerace r.e. relací)**

*Standardní numerací j-árních r.e. relací nazveme funkci $W^{(j)} : \mathbb{N} \to \{A \subseteq \mathbb{N}^j \mid A \text{ je r.e.}\}$ definovanou vztahem*

$$W^{(j)}(i) = dom(\varphi_i^{(j)}).$$

*Index r.e. relace $A \subseteq \mathbb{N}^{(j)}$ je číslo i splňující $A = W^{(j)}(i)$.*

Místo $W^{(j)}(0), W^{(j)}(1), \ldots$ píšeme $W_0^{(j)}, W_1^{(j)}, \ldots$.