

IB107 Vyčísitelnost a složitost

uzávěrové vlastnosti rekurzivních a r.e. množin, věta o projekci,
10. Hilbertův problém

Jan Strejček

Fakulta informatiky
Masarykova univerzita

Definice (obraz a vzor množiny)

Pro $f : \mathbb{N}^k \rightarrow \mathbb{N}$ a množiny $A \subseteq \mathbb{N}^k$ a $B \subseteq \mathbb{N}$ definujeme obraz množiny A při zobrazení f jako množinu

$$f(A) = \{f(a) \mid a \in \text{dom}(f) \cap A\}$$

a vzor množiny B při zobrazení f jako množinu

$$f^{-1}(B) = \{a \mid a \in \text{dom}(f) \text{ a } f(a) \in B\}.$$

uzávěrové vlastnosti rekurzivních množin

Třída rekurzivních množin je uzavřená na \cup , \cap a doplněk.

Věta

- 1 *Nechť $B \subseteq \mathbb{N}$ je rekurzivní množina a $f : \mathbb{N}^k \rightarrow \mathbb{N}$ je totálně vyčíslitelná funkce. Pak $f^{-1}(B)$ je rekurzivní množina.*
- 2 *Nechť $A \subseteq \mathbb{N}^k$ a $B \subseteq \mathbb{N}^l$ jsou rekurzivní množiny. Pak $A \times B \subseteq \mathbb{N}^{k+l}$ je rekurzivní množina.*

Důkaz:

$$W_i^{(j)} = \text{dom}(\varphi_i^{(j)})$$

Věta

Pro každé $k, l \geq 1$ existuje totálně vyčíslitelná funkce $h : \mathbb{N}^2 \rightarrow \mathbb{N}$ taková, že pro libovolné r.e. množiny $W_i^{(k)} \subseteq \mathbb{N}^k$ a $W_j^{(l)} \subseteq \mathbb{N}^l$ platí

$$W_i^{(k)} \times W_j^{(l)} = W_{h(i,j)}^{(k+l)}.$$

Důkaz:

Věta

Existují totálně vyčíslitelné funkce $h_1, h_2 : \mathbb{N}^2 \rightarrow \mathbb{N}$ takové, že pro každé r.e. množiny W_i, W_j platí:

1 $W_i \cup W_j = W_{h_1(i,j)}$

2 $W_i \cap W_j = W_{h_2(i,j)}$

Důkaz:

1 $W_i \cup W_j = W_{h_1(i,j)}$

2 $W_i \cap W_j = W_{h_2(i,j)}$

Věta

Existuje totálně vyčíslitelné funkce $f : \mathbb{N}^2 \rightarrow \mathbb{N}$ taková, že pro každou vyčíslitelnou funkci φ_i a každou r.e. množinu W_j platí

$$\varphi_i(W_j) = W_{f(i,j)}.$$

Důkaz: $\varphi_i(W_j) = \{\varphi_i(a) \mid a \in \text{dom}(\varphi_i) \cap W_j\}$

Víme, že existuje tot. vyčíslitelná funkce $t : \mathbb{N} \rightarrow \mathbb{N}$ taková, že $\text{range}(\varphi_k) = \text{dom}(\varphi_{t(k)})$. ■

Věta

Existuje totálně vyčíslitelné funkce $g : \mathbb{N}^2 \rightarrow \mathbb{N}$ taková, že pro každou vyčíslitelnou funkci φ_i a každou r.e. množinu W_j platí

$$\varphi_i^{-1}(W_j) = W_{g(i,j)}.$$

Důkaz: $\varphi_i^{-1}(W_j) = \{a \mid a \in \text{dom}(\varphi_i) \text{ a } \varphi_i(a) \in W_j\}$

Definice (projekce a řez)

Nechť $R \subseteq \mathbb{N}^k$ je k -ární relace pro $k \geq 2$. Množina

$$\{(a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_k) \mid \exists a_i \in \mathbb{N} \text{ tak, že } (a_1, \dots, a_k) \in R\}$$

se nazývá *i -tá projekce* relace R . Množina

$$\{(a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_k) \mid (a_1, \dots, a_{i-1}, b, a_{i+1}, \dots, a_k) \in R\}$$

se nazývá *i -tý řez* relace R pro pevně zvolené $b \in \mathbb{N}$.

Věta

- 1 *Libovolný řez rekurzivní množiny je rekurzivní množina.*
- 2 *Libovolný řez r.e. množiny je r.e. množina.*
- 3 *Libovolná projekce r.e. množiny je r.e. množina.*

Důkaz:

Předchozí tvrzení lze formulovat efektivně.

Tvrzení

- 1 *Projekce rekurzivní množiny nemusí být rekurzivní.*
- 2 *Libovolná projekce rekurzivní množiny je r.e. množina.*

Důkaz:



Věta (věta o projekci, věta o existenčním kvantifikátoru)

Nechť $A \subseteq \mathbb{N}^k$ je r.e. množina. Pak existuje rekurzivní množina $B \subseteq \mathbb{N}^{k+1}$ taková, že A je $(k + 1)$ -ní projekcí množiny B .

Důkaz:

- pro jednoduchost předpokládejme $k = 1$
- pro vhodné $i \in \mathbb{N}$ platí $A = W_i = \text{dom}(\varphi_i)$



Důsledek

Množina je r.e., právě když je projekcí rekurzivní relace.

Příklad: Dokažte, že množina $A = \{e \mid 7 \in \text{range}(\varphi_e)\}$ je r.e.

shrnutí uzávěrových vlastností

třída rekurzivních množin

- **je** uzavřená na:

- \cup, \cap aplikované na relace stejné arity
- doplněk, \times , vzor při totálně vyčíslitelném zobrazení f
- řez

- **není** uzavřená na:

- projekce

- obecně **není** uzavřená na:

- obraz při totálně vyčíslitelném zobrazení f
- vzor při vyčíslitelném zobrazení g

třída r.e. množin

- **je** uzavřená na:

- \cup, \cap aplikované na relace stejné arity
- \times , obraz i vzor při vyčíslitelném zobrazení f
- projekce, řez

- **není** uzavřená na:

- doplněk

10. Hilbertův problém

10. Hilbertův problém (1900)

Nalezněte algoritmus, který rozhodne, zda polynomičká rovnice s celočíselnými koeficienty má celočíselné řešení.



David Hilbert



Diofantos
z Alexandrie



Jurij Vladimirovič
Matijasevič

10. Hilbertův problém

Definice (diofantická relace)

Relace $R \subseteq \mathbb{N}^k$ se nazývá **diofantická**, právě když existuje polynom $P(x_1, \dots, x_k, y_1, \dots, y_l)$ s celočíselnými koeficienty a $k + l$ proměnnými splňující:

$$(a_1, \dots, a_k) \in R \iff \exists (b_1, \dots, b_l) \in \mathbb{N}^l \text{ takové, že } P(a_1, \dots, a_k, b_1, \dots, b_l) = 0$$

Věta (Matijasevič, 1970)

Relace je r.e., právě když je diofantická.