9. cvičení

Datové struktury I, 29. 11. 2022 https://iuuk.mff.cuni.cz/~chmel/2223/ds1/

Úloha 1 (Lineární systém)
Ukažte, že systém funkcí $\{h_{a,b}(x) = (ax + b \mod p) \mod m \colon a, b \in \mathbb{Z}_p\}$ je dokonce 1-univerzální, máme-li $0 < a < p$. Pro jak malé c je tento systém $(2, c)$-nezávislý?

Úloha 2 (Lineární systém bez konstanty)
Uvažme systém funkcí $\{h_a(x) = (ax \mod p) \mod m \colon a \in \mathbb{Z}_p \setminus \{0\}\}$. Je k-univerzální pro nějaké k? A co když dovolíme $a = 0$?

Úloha 3 (Lineární systém není 3-nezávislý)
Ukažte, že systém funkcí $\{h_{a,b}(x) = (ax + b \mod p) \mod m \colon a, b \in \mathbb{Z}_p\}$ není 3-nezávislý.

Úloha 4 (Vyloženě praktické systémy)
Uvažme systém funkcí $\mathcal{H}_1 = \{\mathrm{id}\}$, který obsahuje jedinou funkci, jež zobrazí x na x. Je $\mathcal{H}_1$ c-univerzální pro nějaké c? Je $\mathcal{H}_1$ (k, c)-nezávislý pro nějaká k a c?
Dále uvažme systém $\mathcal{H}_2 = \{h_a(x) = a \colon a \in [m]\}$. Dokažte (resp. zopakujte si z přednášky), že tento systém je (1,1)-nezávislý. Dále ukažte, že $\mathcal{H}_2$ není $(2, c)$-nezávislý ani c-univerzální pro žádné c.

Úloha 5 (Univerzální modulo může rozbít univerzalitu)
Ukažte, že pokud máme univerzální systém hešovacích funkcí $\mathcal{H}$, pak systém $\mathcal{H}'$, kde ke každé fci navíc přidáme modulo m, už nemusí být univerzální. Formálně: Dokažte, že pro každé c a $m > 1$ existuje univerzum $\mathcal{U}$ a systém $\mathcal{H}$ z $\mathcal{U}$ do $\mathcal{U}$ tak, že $\mathcal{H}$ je univerzální, ale $\mathcal{H}'$ už není c-univerzální.

Užitečné definice

Definice (c-univerzální systém fcí)**.** Systém $\mathcal{H}$ funkcí $h : \mathcal{U} \to [m]$ je c-univerzální pro $c > 0$, pokud pro všechna $x \neq y$ platí $\Pr_h[h(x) = h(y)] \leq \frac{c}{m}$.
Systém $\mathcal{H}$ je univerzální, pokud je c-univerzální pro nějaké $c > 0$.

Definice (k-nezávislý systém fcí)**.** Systém $\mathcal{H}$ funkcí $h : \mathcal{U} \to [m]$ je (k, c)-nezávislý pro nějaká $k \geq 1, c > 0$, pokud $\Pr_{h \in \mathcal{H}}[h(x_1) = a_1 \wedge \ldots \wedge h(x_k) = a_k] \leq \frac{c}{m^k}$ pro libovolná $x_1, \ldots, x_k$ různá, $a_1, \ldots, a_k$ ne nutně různá.
Sytém je k-nezávislý, pokud je (k, c)-nezávislý pro nějakou konstantu c.