Cvičení z Úvodu do aproximačních a pravděpodobnostních algoritmů

ZS2324 - 7. cvičení

1

Mějme funkci $F : \{0, \ldots, n-1\} \to \{0, \ldots, m-1\}$.
Víme, že pro každé $x, y \in \{0, \ldots, n-1\}$ platí $F((x+y) \mod n) = (F(x) + F(y)) \mod m$.
Jediný způsob, kterým umíme vyhodnocovat F, je pomocí tabulky, ve které jsou hodnoty F uloženy.
V této tabulce je ale $1/5$ všech hodnot špatně a my nevíme, které to jsou.
Popište jednoduchý randomizovaný algoritmus, který pro libovolnou danou hodnotu z vrátí $F(z)$ s pravděpodobností alespoň $1/2$.

Následně vám dovolím spustit tento algoritmus pro dané z hned třikrát. Tudíž dostanete tři (ne nutně různé) hodnoty, které by měly být $F(z)$. **S jakou pravděpodobností umíte určit $F(z)$ nyní?**

2

Ukažte, že pro libovolnou diskrétní nahodnou veličinu X která nabývá pouze hodnot v intervalu $[0, 1]$ platí $\text{var}(X) \leq 1/4$.

3

Na přednášce jste viděli, že pro libovolné $p \geq n$ (kde p je prvočíslo) rodina hashovacích funkcí

$$\mathcal{H} = \{h_{a,b} \mid 1 \leq a \leq p-1, 1 \leq b \leq p\}$$

kde

$$h_{a,b}(x) = ((ax + b) \mod p) \mod n$$

je 2-univarzální.

Uvažme nyní rodinu hashovacích funkcí

$$\mathcal{H}' = \{h_a \mid 1 \leq a \leq p-1\}$$

kde

$$h_a(x) = (ax \mod p) \mod n.$$

Ukažte, že tato rodina není 2-univerzální.
Následně ukažte, že je téměř 2-univerzální v tom smyslu, že pro libovolné $x, y \in \{0, \ldots, p-1\}$ a pro uniformně náhodně vybranou $h \in \mathcal{H}'$ platí $\Pr(h(x) = h(y)) \leq 2/n$.