matrix_transpose:

- častou chybou byl „doslovný" transpose & swap, tedy rekurzivně si nechat transponovat matice a pak je prohodit
- to má horší časovou složitost
- $T(n)$ ... složitost transponování matice velikosti $n \times n$
- $T(n) = \underbrace{4\,T(\tfrac{n}{2})}_{\text{rekurze}} + \underbrace{O(n^2)}_{\text{swap}}$

master theorem:

- swap má časovou složitost $\Theta(n^{\lg_2 4}) = \Theta(n^2)$
- tím pádem má doslovný transpose & swap složitost $\Theta(n^2 \lg n)$

Def: Systém hash. fcí $\mathcal{H}$ je c-universální, pokud

$$\forall x \neq y \in \mathcal{U} : \Pr_{h \in_R \mathcal{H}} [h(x) = h(y)] \leq \frac{c}{m}.$$

Def: Systém hash. fcí $\mathcal{H}$ je (k,c)-nezávislý, pokud

$$\forall x_1 \neq x_2 \neq \dots \neq x_k \ \forall \underbrace{a_1, a_2, \dots, a_k}_{\text{ne nutně různá}} \in \{0, \dots, m-1\}$$

$$\Pr_{h \in_R \mathcal{H}} [h(x_1) = a_1 \wedge \dots \wedge h(x_k) = a_k] \leq \frac{c}{m^k}.$$

Př: Nechť $\mathcal{H}$ je (k,c)-nezávislý systém hash. fcí a $k>1$.

Dokažte, že $\mathcal{H}$ je $(k-1,c)$-nezávislý.

- z definice (k,c)-nezávislosti víme, že

$\forall x_1 \neq \dots \neq x_k \in \mathcal{U}, \forall a_1, \dots, a_k \in \{0, \dots, m-1\}$

$$\Pr_{h \in_R \mathcal{H}}[h(x_1) = a_1 \wedge \dots \wedge h(x_k) = a_k] \leq \frac{c}{m^k}$$

- zajímá nás

$$\Pr_{h \in_R \mathcal{H}}[h(x_1) = a_1 \wedge \dots \wedge h(x_{k-1}) = a_{k-1}]$$ pro $\forall x_1 \neq \dots \neq x_{k-1} \in \mathcal{U}$ $\forall a_1, \dots, a_k \in [m]$

- „nezajímá nás", co se děje s x_k

$\rightarrow \Pr_{h \in_R \mathcal{H}}[h(x_1) = a_1 \wedge \dots \wedge h(x_{k-1}) = a_{k-1}] =$

union bound a definice (k,c)-nezávislosti

$$= \Pr\Big[\bigcup_{p \in [m]} \Big(\bigwedge_{i=1}^{m-1} h(x_i) = a_i\Big) \wedge h(x_k) = p\Big] \leq m \sum \frac{c}{m^k} = \frac{c}{m^{k-1}} \quad \square$$

Př: Nechť $\mathcal{H}$ je $(2,c)$-nezávislý hash. systém. Ukažte, že $\mathcal{H}$ je c-universální systém.

- „kvantifikátory..." $\Pr[h(x_1) = a_1 \wedge h(x_2) = a_2] \leq \frac{c}{m^2}$.
- $\Pr[h(x) = h(y)]$ pro $x \neq y \in \mathcal{U}$?

- $\Pr[h(x) = h(y)] = \bigcup_{i \in [m]} \Pr[h(x) = i \wedge h(y) = i] \leq m \cdot \frac{c}{m^2} \leq \frac{c}{m}$ $\square$

→ „$\mathcal{H}$ je k-nezávislý $\Rightarrow$ $\mathcal{H}$ je 2-nezávislý"

→ „$\mathcal{H}$ je 2-nezávislý $\Rightarrow$ $\mathcal{H}$ je něco-univerzální"

Př: Ukažte, že konstantní fce jako systém hash. fcí je 1-nezávislý.

- $\Pr[h(x) = i]$ pro pevné $i \in [m]$?
- to nastane jen tehdy, vybereme-li jako h fci $h(x) = i$ pro $\forall x \in \mathcal{U}$.
- to nastane s pst $\frac{1}{m}$

→ „1-nezávislost" je zbytečný pojem :)