1) $(2,c)$ – nezávislost $\Rightarrow$ c- univerzalita

c-univerzalita: $\forall x \neq y \quad P[h(x) = h(y)] \leq \frac{c}{m}$

$(2,c)$-nezávislost: $\forall x \neq y, \forall a,b \in [m]: P[h(x)=a \wedge h(y)=b)] \leq \frac{c}{m^2}$

$$P[h(x)=h(y)] = P\left[\bigcup_{a \in [m]} h(x)=h(y)=a\right] \underset{\text{union bound}}{\leq} \sum_{a \in [m]} P[h(x)=a=h(y)] \leq m \cdot \frac{c}{m^2} = \frac{c}{m}$$

↳ dokázali, že existuje jen m hashů, které můžou kolidovat.

(k,c) – nez. $\Rightarrow$ $(k-1,c)$ – nez.

– z kuličce vybereme jeden prvek, který nebude kolidovat.

– těchto výběrů máme m.

$\forall x_1 - x_k, \forall a_1 - a_{k-1}, fix$

$$= P[h(x_1)=a_1, \dots, h(x_{k-1})=a_{k-1}, h(x_k)=fix]$$

$$= P\left[\bigcup_{fix \in [m]} h(x_1)=a_1, \dots, h(x_{k-1})=a_{k-1}, h(x_k)=fix\right] \underset{\text{union bound}}{\leq} \sum_{fix \in [m]} \dots \leq \frac{c}{m^k} \cdot m = \frac{c}{m^{k-1}}$$

2)

$h_{a,b}(x) = (ax+b \bmod p)$ $a,b \in [p]$ je $(2,1)$-nez. Pro malou se stane $(2,4)$-nez.

a) Dokažte, že není 3-nezávislý.

$\forall x \neq y, \forall a,b \in [m]: P[h(x)=a \wedge h(y)=b)] \leq \frac{1}{m^2}$ $\rightarrow (2,1)$-nezávislost

$\forall x \neq y \quad P[h(x)=h(y)] \leq \frac{3}{m}$ $\rightarrow$ 3-nezávislost

$$\begin{aligned} ax+b &= r \\ ay+b &= s \\ az+b &= t \end{aligned} \quad \rightsquigarrow \text{upravíme} \quad \begin{aligned} ax+1 &= r \\ ay+1 &= s \\ az+1 &= t \end{aligned} \quad \rightsquigarrow$$

buď to není řešení, pak to nefunguje vůbec.
Nebo existuje p řešení.

Máme tedy celkem $\frac{p}{p^3}$ dosazení, tudíž celkem je to $\frac{1}{p^2}$.

rovnice $\rightarrow p+1$ proměnných má 0 řešení nebo jich má p.

nebo: $h(0)=0 \Rightarrow b=0$
$h(1)=0 \Rightarrow a=0$
$\Rightarrow P[h(0)=0 \wedge h(1)=0 \wedge h(2)=0] = \frac{1}{p^2} \gg \frac{c}{p^3}$

ze všech voleb a,b si vybere $0,0$

b) Uvažme pouze $(ax \bmod p) \bmod m \quad a \in \mathbb{Z}_p \setminus \{0\}$

Je 2-nez., c-univ pro nějaké c? A co $a=0$?

Když bude $a=0$, budou se všechny hodnoty rovnat 0.

Není 2-nezávislý: mám $ax = r$, $ay = s$ ⇝ tady mám šanci $\frac{p}{p^2}$ splnit jejich dosazení, kdežto mám $\frac{1}{p}$

nebo: $b=0$ vždy

$h(0)=0$ vždy $P[h(0)=1]=1 >> \frac{c}{m}$ => není to ani 1-nezávislé

Co c-univ.?

$\forall x \neq y : P[h(x)=h(y)] \leq \frac{2\lfloor\frac{p}{m}\rfloor}{p} \leq \frac{2}{m}$

⇕

$ax \bmod p \bmod m = ax \bmod p \bmod m$

⇓

$a \cdot (x-y) \bmod m \equiv l \cdot m$, $a \neq 0$, $(x-y) \neq 0$, $\in \mathbb{Z}_p$ — tímhle modulím do tabulky

$l \in -\lfloor\frac{p}{m}\rfloor, \dots -2,-1,1,2, \dots, +\lfloor\frac{p}{m}\rfloor$

tady chci získat 0, tudíž každé $l \cdot m \bmod m = 0$!

těchto voleb mám $2 \cdot \lfloor\frac{p}{m}\rfloor$

I když zafixuju b, tak sice ztratím nezávislost, ale univerzalitu úplně neztratím.