Hashing (contd.)

Weak universal hash functions:

Sometimes also called 2-universal.

A family of hash functions $H: U \to [m]$ is called a weak universal family if $\forall\ x \neq y$;

$$\Pr_{h \sim H}[h(x) = h(y)] \leq \frac{1}{m}.$$

// Strong universal if prob $\leq \frac{O(1)}{m^2}$.

By union bound,

$$\Pr[\exists h \in H \text{ s.t } h(x) = h(y)] \leq \frac{|H|}{m}.$$

$f_{a,b}(x) = ax + b \bmod p$

$g(y) = y \bmod m$

$h_{a,b}(x) = g(f_{a,b}(x))$.

Construction of ~~2-~~ weak universal family:

$U = \{0, \ldots, |U|-1\}$.

$$h_{a,b}(x) = ((ax + b) \bmod p) \bmod m$$

$|H| \leq p(p-1)$
$O(m^2)$

p is a prime $\geq m$

$$H = \{ h_{a,b}(x) \mid a, b \in \mathbb{Z}_p \wedge a \neq 0 \}.$$

$\mathbb{Z}/p\mathbb{Z}$ | a residue class of int wrt + and $\times$ modulo p.

Given a $h \in_R H$; $h(x) = h(y)$ for $x \neq y$ if

$$((ax + b) \bmod p) \bmod m = ((ay + b) \bmod p) \bmod m.$$

for some i, ← $i \in [0, \lfloor \frac{p-1}{m} \rfloor]$.

$u \equiv v \bmod m$,

$\Rightarrow \boxed{u = v + i \cdot m}$.

$$ax + b \equiv ay + b + i \cdot m \bmod p,$$

$$\Rightarrow a(x - y) \equiv i \cdot m \bmod p.$$

$p-1$ choices for a

$\lfloor \frac{p-1}{m} \rfloor$ choices for i.

Collision happens for $\frac{p-1}{m}$ choices out of $p-1$ choices.

→ Collision prob = $\left\lfloor \frac{p-1}{m} \right\rfloor \cdot \frac{1}{p-1} \le \frac{1}{m}$.

$a \cdot (x-y) \equiv i \cdot m \mod p$ | $x \not\equiv y \mod p$.

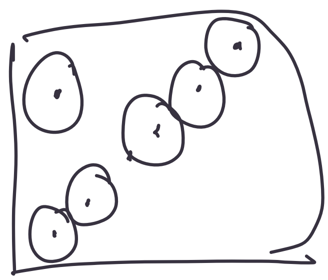
$a \equiv \frac{i \cdot m}{(x-y)} \mod p$

For every fixing of $i \in \left[0, \left\lfloor \frac{p-1}{m} \right\rfloor\right]$, a gets its value fixed.

⇒ $h_{a,b}(x) = h_{a,b}(y)$ for those values of a.

$ax + b \mod p$

$ax \mod p$



$h(x) = h(y)$.

2-wise ind and k-wise ind.

$$\Pr_{h \sim H}\left[h(x) = a \wedge h(y) = b \right] \le \frac{1}{m^2}.$$

$\downarrow$

b $[m]$

$$\Pr_{h \sim H}\left[\bigwedge_{i=1}^{k} h(x_i) = a_i \right] \le \frac{1}{m^k}.$$