L15 Hashing + Backwards analysis 10/12/23

H is a 2-Universal hash function family

$f \in H \quad f:\{0,\dots,p-1\} \to \{0,\dots,m-1\}$

$\forall x,y \in \mathbb{Z}_p \quad x \neq y \quad P_{f\in H}[f(x)=f(y)] = \frac{1}{m}$

p: is a "large" prime

$h(x) = ((ax+b) \bmod p) \bmod m$

$a, b \in \mathbb{Z}_p = \{0,1,2,\dots,p-1\} \quad a \neq 0$

$\boxed{p \text{ is a prime}}$

$x \equiv_p y$ this is

$(x \bmod p) = (y \bmod p)$

Lemma

For $\alpha, \beta \in \mathbb{Z}_p \quad \alpha \neq 0$ and $\beta \neq 0$

$\Rightarrow \alpha\beta \not\equiv_p 0$

proof $\alpha\beta \equiv_p 0 \Rightarrow \exists i > 0$ s.t.

$\alpha\beta = ip$

$\alpha = p_1 \cdot p_2 \cdots p_k \quad \beta = p_{k+1} p_{k+2} \cdots p_t$

p_is are all prime

$p_i < p$

$p_1 \cdot p_2 \cdots p_k p_{k+1} p_{k+2} \cdots p_t \neq ip$

$p \nmid$

$x \mid y \iff x$ divides y. ▨

Lemma

$\alpha, \beta, i \in \{1,2,\dots,p-1\} \quad \alpha \neq \beta$

$\Rightarrow \alpha i \not\equiv_p \beta i$

Proof

$\alpha i \equiv_p \beta i$ assume $\alpha > \beta \iff$

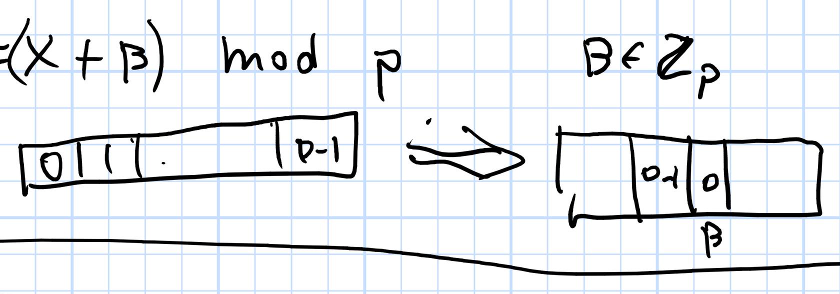
$(\alpha-\beta) i \equiv_p 0 \bmod p$ impossible by previous lemma

▨

$g(x) = \alpha x \bmod p \quad \alpha \neq 0 \quad \alpha \in \mathbb{Z}_p$

$g: \mathbb{Z}_p \to \mathbb{Z}_p$ one to one.

$g(x) = (x+\beta) \bmod p \quad \beta \in \mathbb{Z}_p$



$\alpha \neq 0, \beta$

$f(x) = \alpha x + \beta$ one-to-one function

Lemma

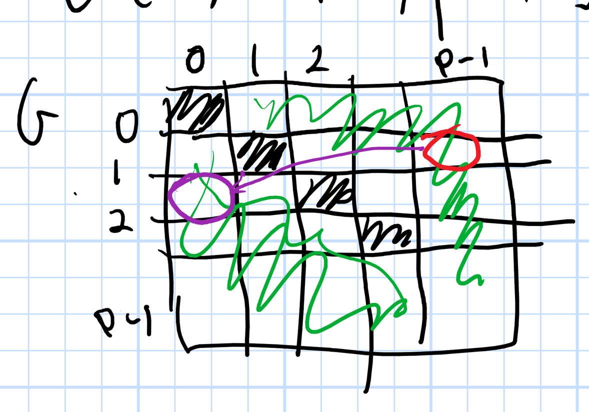
Consider the mapping

$F(x,y) = (f(x), f(y))$ [f as defined above]

$F: G \to G$. one to one.

$f(r) \stackrel{?}{=} f(s)$

$G = \{(r,s) \in \mathbb{Z}_p \times \mathbb{Z}_p \mid r \neq s\}$



Proof

pick any $(r,s) \in G$, and (x,y) there is exactly one function f s.t.

$F(r,s) = (x,y)$.

Proof

$f(r) = x \quad f(s) = y \iff \begin{cases} \alpha r + \beta \equiv_p x \\ \alpha s + \beta \equiv_p y \end{cases}$

$\alpha(r-s) + \beta - \beta \equiv_p x - y$

$\alpha(r-s) \equiv_p x - y$ multiply by $\frac{1}{r-s}$

$\alpha \equiv_p \frac{x-y}{r-s}$

$\beta \equiv_p x - \alpha r \equiv x - \frac{x-y}{r-s} r$

Lemma

For any $x \in \mathbb{Z}_p \quad x \neq 0$ there exist a unique value y s.t.

$x \cdot y \equiv_p 1$

Proof $\left|\{x\cdot 1, x\cdot 2, x\cdot 3, \dots x\cdot\tau \dots x\cdot(p-1)\}_p\right| = p-1$

does not contain

must contain $1 \Rightarrow \exists \tau \quad x\tau \equiv_p 1$ ▨

$h(x) = ((\alpha x + \beta) \bmod p) \bmod m$

H is 2-Universal

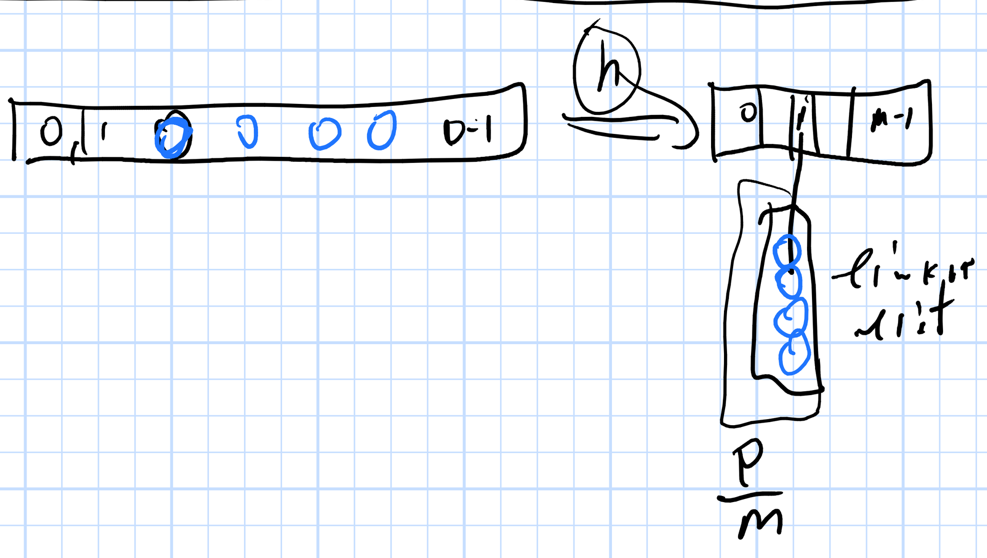
x, y, z

$h(x)$

$h(y)$

$h(z)$

$h(x) = (\alpha x^2 + \beta x + \gamma \bmod p) \bmod m$

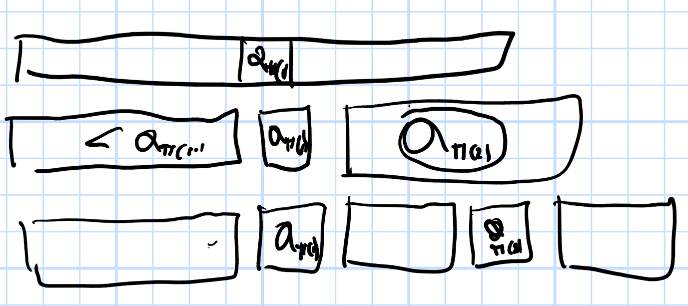


Backwards analysis

Quick Sort

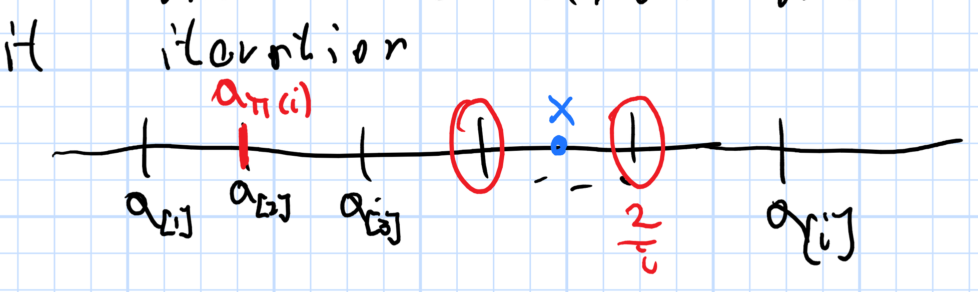
$a_1, a_2, \dots, a_n$

$a_{\pi(1)}, a_{\pi(2)}, \dots, a_{\pi(n)}$



Q: Expected # of comparisons involving item x.

Consider the state after the ith iteration



Q: What is the probability that x participated in a comp in the ith iteration

$Z_i = 1 \iff x$ participated in comp

$P[Z_i = 1] \leq \frac{2}{i}$

$E\left[\text{\# of comp involving } x \text{ in QS}\right] = \sum_{i=1}^{n} E[Z_i] \leq \sum_{i=1}^{n} \frac{2}{i} = O(\log n)$.

$V_1, V_2, \dots, V_n$ n distinct values

π random permutation

$X_i := \max_{l=1}^{i} V_{\pi(l)}$

$\{X_1, X_2, \dots, X_n\}$: How many distinct values.

$P[X_i \neq X_{i-1}] = \frac{1}{i}$

$E\left[\text{\# times the maximum changes}\right] = \sum_{i=1}^{n} \frac{1}{i} = O(\log n)$.