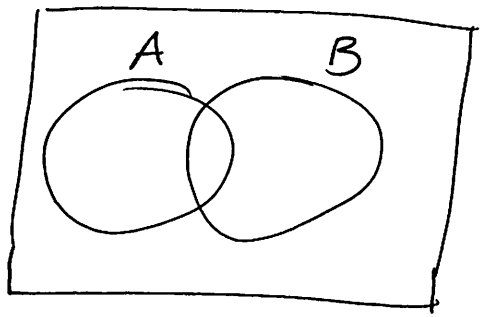
CS70
Fall 2013

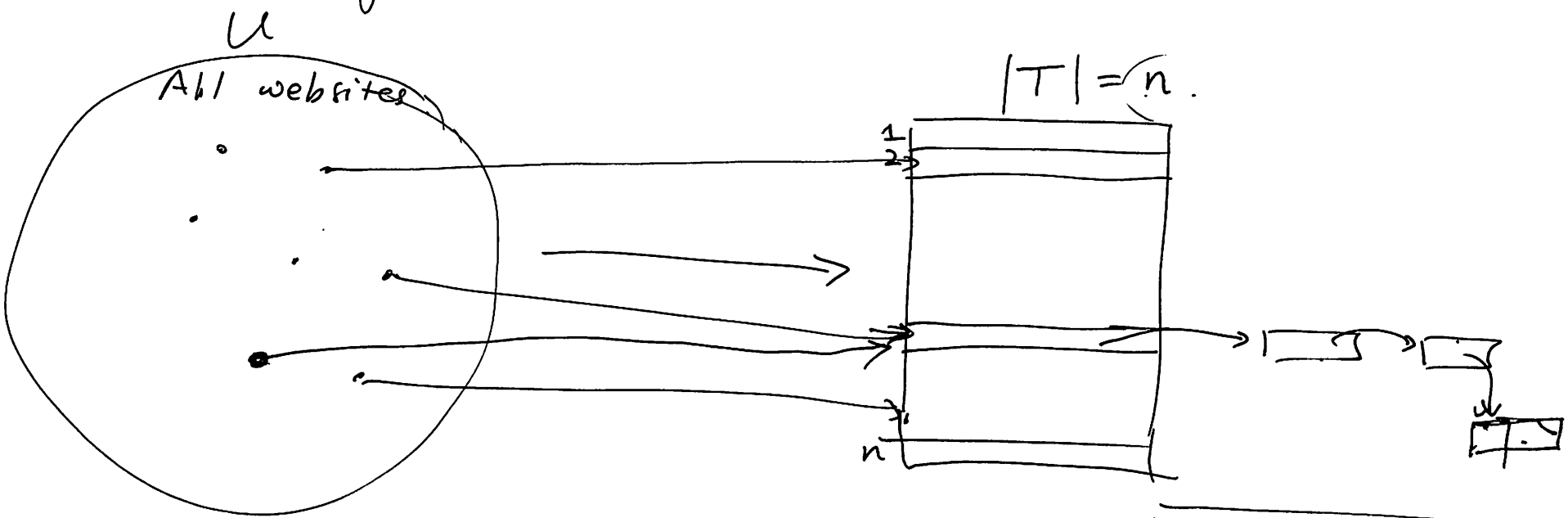
Two Killer Apps.

Union Bound:



$$P(A \cup B) \leq P(A) + P(B).$$

1. Hashing: Give a short name to an object.



Supports:
insert key
delete key
membership.

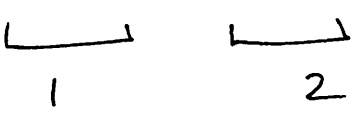
$S \subseteq U$ Store S.
$|S| = m$.

m balls in n bins.

Place m balls in n bins

How big can m be so that $P[\text{no collision}] \geq \frac{1}{2}$.

$P[\text{collision}] \leq \frac{1}{2}$.



$$P[\text{collision}] \leq \sum_{\{i,j\}} P[i,j \text{ same bin}]$$

$$\text{collision} = \bigcup_{\{i,j\}} (\text{Ball } i \text{ \& Ball } j \text{ placed in same bin})$$

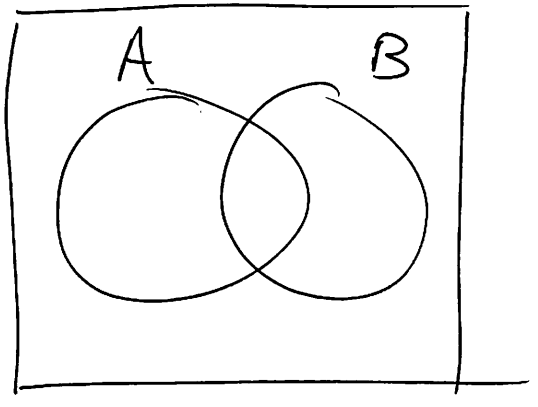
$$= \sum_{\{i,j\}} \frac{1}{n}$$

$$= \binom{m}{2} \frac{1}{n} = \frac{m(m-1)}{2n} \leq \frac{m^2}{2n} \leq \frac{1}{2}.$$

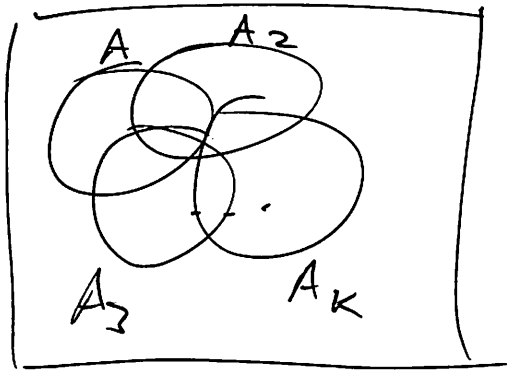
$$m^2 \leq n$$

$$m \leq \sqrt{n}.$$

Review session: Sunday 4-7pm 155 Dwinelle.



$$P[A \cup B] \leq P[A] + P[B].$$



$$P[A_1 \cup A_2 \cup \cdots \cup A_K] \leq P[A_1] + \cdots + P[A_K]$$

$$\| \quad \text{"}$$

$$P\left[\bigcup_{i=1}^{K} A_i\right] \leq \sum_{i=1}^{K} P[A_i].$$

Birthday Paradox.

$m = 23$ with prob $\geq \frac{1}{2}$ two have same birthday.

$m = 60$ prob $\geq 99\%$ two " " ".

$n = 365$ bins

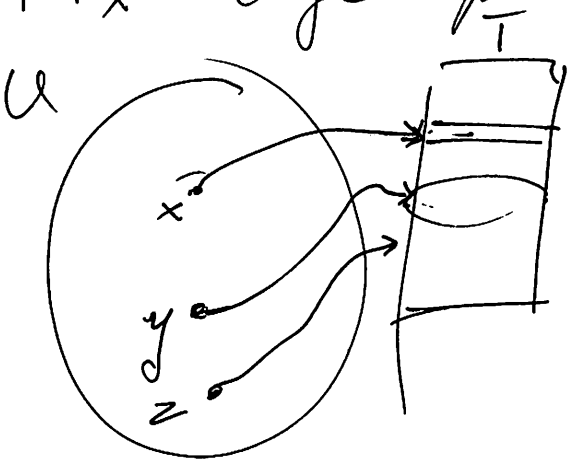
as long as $m \leq \sqrt{365} \approx 18$ prob $\leq \frac{1}{2}$ two have same birthday.

$$\rightarrow P[\text{no two have same birthday}] = \frac{365 \times 364 \times 363 \times \cdots \times (365-m+1)}{365^m}$$

$m = 23 \approx \frac{1}{2}$.

How to choose pick a "random-looking" function?

Fix large prime $p \geq |U|$.



$x \longrightarrow \underline{\underline{a}}x + \underline{\underline{b}} \pmod p$

a, b are random $(\bmod p)$

Hash table of size $N = 2^n$.

$$h(x) = \left[ax + b \pmod p \right] \pmod N$$

Pairwise Independent:

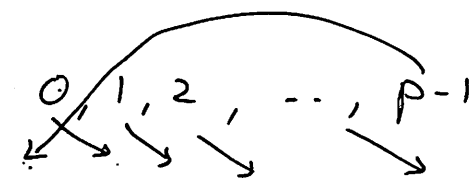
$u = ax + b \pmod p$

$v = ay + b \pmod p$

$b \bmod p$

$b+1 \bmod p$.

$b+2 \pmod p$



$$\frac{1}{p} = P\left[\underline{\underline{v}} = ay + b \pmod p \;\middle|\; \underline{\underline{u}} = ax + b \pmod p \right]$$

$$P\left[\underbrace{v - u}_{\text{random.}} = \underline{\underline{a}}(y - x) \bmod p \;\middle|\; \text{——} \right]$$

$$P\left[2\textcircled{a} = 5 \bmod p \right]$$

$$\text{"} \quad \frac{1}{p}.$$

$(\mathrm{mod}\ p)$ $\qquad P(0)$.

$\deg \le 2 \qquad a_2 x^2 + a_1 x + a_0 \quad (\mathrm{mod}\ p)$.

~~Pick~~ Select $P(x)$ at random.

1st way: Pick a_0, a_1, a_2 randomly $(\mathrm{mod}\ p)$.

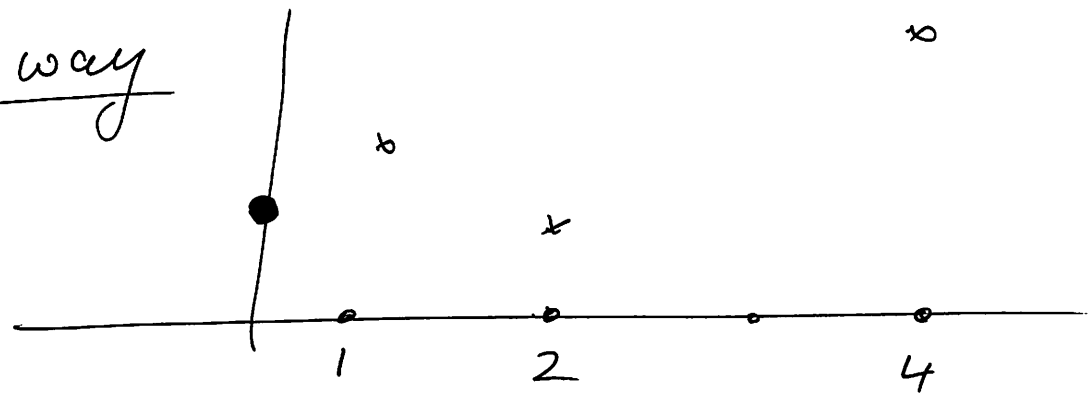
p^3 choices.

$$\Pr\left[P[0] = \cdot \,\middle|\, P(1)=y_1, P_2(2)=y_2 \cdots P(k)=y_k\right]$$

$$= \begin{cases} \frac{1}{p} : \text{if } k \le d. \\ \underline{0 \text{ or } 1} \quad k \ge d+1 \end{cases}$$

knew $P(0)$.

2nd way



$P[1] = y_1 \quad P[2] = y_2 \quad P[4] = y_4$.

Pick y_1, y_2, y_4 uniformly $(\mathrm{mod}\ p)$.

$P[0]$ = secret. Pick $P(1), \ldots, P(d)$ at random.

Load Balancing

m tasks

$P[\text{max load} \geq K] \leq \cdot \frac{1}{2}$.

$P[\text{max load} \leq K] \geq \frac{1}{2}$.

$m = n$

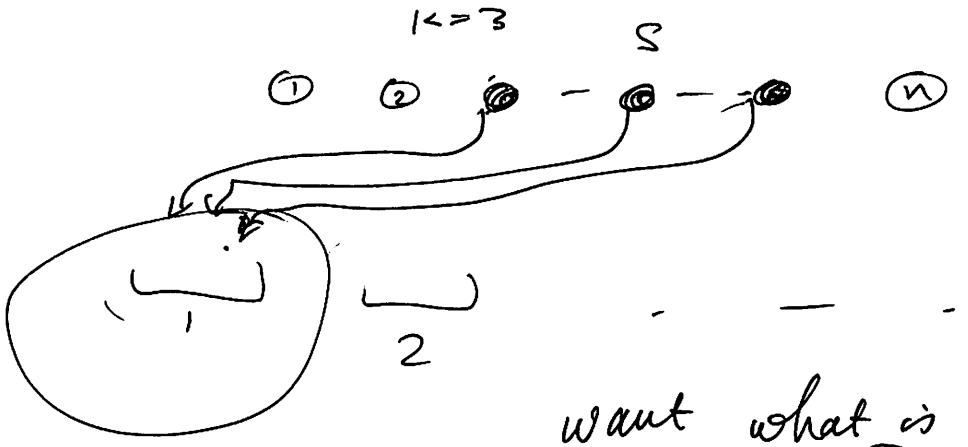
$\text{Ans} \approx \frac{\ln n}{\ln \ln n} = K$

I. $P[\text{bin 1 has} \geq K \text{ balls}] \leq \frac{1}{2n}$.

(some bin $\geq K$ balls) $= \bigcup_{i=1}^{n}$ (bin i has $\geq K$ balls).

$P[\text{some bin has} \geq K \text{ balls}] \leq \sum_{i=1}^{n} P[\text{bin } i \text{ has} \geq K \text{ balls}]$

$\leq n \cdot \frac{1}{2n} \leq \frac{1}{2}$.



want what is value of k: $\leq \frac{1}{2n}$.

$P[\geq k \text{ balls in bin } 1]$

$[\geq k \text{ balls in bin } 1] = \bigcup_{|S|=k} [S \text{ ended up in bin } 1]$ (all balls in S ended up in bin 1)

$P[\geq k \text{ balls in bin } 1] \leq \sum_{|S|=k} P[\text{all balls in } S \text{ ended up in bin } 1]$.

$= \binom{n}{k} \frac{1}{n^k}$

$= \frac{n!}{(n-k)!\,k!} \frac{1}{n^k}$.

$= \frac{n(n-1)\cdots(n-k+1)}{k!} \frac{1}{n^k} \leq \frac{1}{k!} \leq \frac{1}{2n}$.

what value of k

Roughly: $k! = n$.

$$\left(\frac{k}{e}\right)^k = n.$$

$e = 2.7\ldots$

$$k(\ln k - 1) = \ln n.$$

$$k \approx \ln n.$$

$$k \approx \frac{\ln n}{\ln \ln n}.$$