(roal: give you some of the understand #riday's paper. Focus on 4.1 tools to help universal hash expected value random var of income expected Focus on 4.1 U = 21,2,..., n3 Hash function

(add bater u  $h(u_{i})$ Li D > ->TUI S= Zu1, u2, u3) 4202  $h(u_2)$ us  $h(u_3)$ > [42[-]> [43] × 🚬

very large [ll] n buckets

all english words all phone numbers

want to store/query some SCU, 151<</ul>

want to use randomness to avoid collisions.

can I count on randomness in S? NO - randomness has to come in <u>Choosing</u> he hash Function h.

H is a universal family of hash functions if

for all X, y  $\in U$ ,  $x \neq y$ ,  $\Pr[h(x) = h(y)] \leq \pi$ 

h is universal pobabilin over random h is pairwise-indep. choice of h from H

Probability of a collision is low.  $\forall x, y \in U, x \neq y, | \geq h \in H : h(x) = h(y) > | \leq \frac{|H|}{n}$ There is no pair of elements that collide in more than 141/n of the hash functions. adversang chooses S we randomly choose h we get Pr (hlx) = h(y)] = h Mat does universality help us prove? Say miteurs have been hashed to n-bucket hask table. resolve willisions w/ maining (show on picture above) want to grong for XEU. let X = # items in h(x) (use picture above to show possible X values) say about X? What is something I'd like to  $\begin{cases} n/n \\ 1 + \frac{m-1}{n} \end{cases}$ if KSO let's divide  $E(X \in$ if x ESB cares expected have from svess litore Value of random var. our intrition is right here - but let's sectre prof.

let X; be an indicator variable S.t. X;=1 if it element of S is in same bucket as X and O otherwise.



by def. of X, X,

by linearity of expectation

bc h is universal

 Suppose X ∈ S.  $E[X] = E[X_i]$ by def of X, X: unere is x?  $= E \left[ 1 + \sum_{i=2}^{\infty} \chi_i \right]$ wlog, assume x is 1st eit of S = | + = E [X;] by linearly of expectation  $\leq 1 + \tilde{\Xi} + \tilde{L}$ bc h is universal check in w/ = 1+ m-1

mat have me chown?

If m=n, expect 1 item if x #S and 2 if x ES.

expect O(1) grenz time.

In practile, double table uneverer 1771. véhash ask trem: should I make new h?

What can I do if I can't store m pointers?





T 32 617