COMPSCI 514: Algorithms for Data Science

Cameron Musco University of Massachusetts Amherst. Fall 2023. Lecture 3

Logistics

- Problem Set 1 has been posted on the course website and is due Friday 9/22 at 11:59pm.
- On the quiz feedback question, several people mentioned concerns about linear algebra background. The good news is you have some time – we will do essentially no linear algebra before the midterm. See resources on Lecture 15 for review material to get started on.
- For probability/problem solving practice beyond the quizzes/pset I highly recommend looking at the exercises in
- Foundations of Data Science and Probability and Computing. Feel free to ask for solutions to these on Piazza.
 - It is common to not catch everything in lecture. I strongly encourage going back to the slides to review/check your understanding after class. Also come to office hours for more in-depth discussion/examples.

Content Overview

Last Class:

Var(X+Y) = Var(X) + Var(Y)

- Linearity of variance.
- Markov's inequality: the most fundamental concentration bound. $Pr(X \ge t \cdot \mathbb{E}[X]) \le 1/t$.
- Algorithmic applications of Markov's inequality, linearity of expectation, and indicator random variables:
 - Counting collisions to estimate CAPTCHA database size.
 - Start on analyzing hash tables with random hash functions.
 - Collisions free hashing using a table with $O(m^2)$ slots to store *m* items.

Today:

- Finish up random hash functions and hash tables.
- 2-level hashing, 2-universal and pairwise independent hash functions.
- Application of random hashing to distributed load balancing.
- Through this application learn about Chebyshev's inequality, which strengthens Markov's inequality (maybe not until next class).

Quiz Questions



Quiz Questions

Hash Tables

We store *m* items from a large universe in a hash table with *n* positions.



- Want to show that when $h: U \rightarrow [n]$ is a fully random hash function, query time is O(1) with good probability.
- Equivalently: want to show that there are few collisions between hashed items.

Let
$$\mathbf{C} = \sum_{i,j \in [m], i < j} \mathbf{C}_{i,j}$$
 be the number of pairwise collisions between
items.
 $\mathbb{E}[\mathbf{C}] = \frac{m(m-1)}{2n}$ (via the Captcha analysis)

• For $n = 4m^2$ we have: $\mathbb{E}[\mathbf{C}] = \frac{m(m-1)}{8m^2} \leq \frac{1}{8}$.

اتلا

Let $C = \sum_{i,j \in [m], i < j} C_{i,j}$ be the number of pairwise collisions between items.

$$\mathbb{E}[\mathbf{C}] = \frac{m(m-1)}{2n}$$
 (via the Captcha analysis)

• For
$$n = 4m^2$$
 we have: $\mathbb{E}[\mathbf{C}] = \frac{m(m-1)}{8m^2} \leq \frac{1}{8}$.

Apply Markov's Inequality: $Pr[C \ge 1] \le \frac{\mathbb{E}[C]}{1} \le \frac{1}{8}$.

Let $C = \sum_{i,j \in [m], i < j} C_{i,j}$ be the number of pairwise collisions between items.

$$\mathbb{E}[\mathbf{C}] = \frac{m(m-1)}{2n}$$
 (via the Captcha analysis)

• For
$$n = 4m^2$$
 we have: $\mathbb{E}[\mathbf{C}] = \frac{m(m-1)}{8m^2} \leq \frac{1}{8}$.

Apply Markov's Inequality:
$$Pr[C \ge 1] \le \frac{\mathbb{E}[C]}{1} = \frac{1}{8}$$
.
 $Pr[C = 0] = 1 - Pr[C \ge 1] \ge 1 - \frac{1}{8} = \frac{7}{8}$

Let $C = \sum_{i,j \in [m], i < j} C_{i,j}$ be the number of pairwise collisions between items.

$$\mathbb{E}[\mathbf{C}] = \frac{m(m-1)}{2n}$$
 (via the Captcha analysis)

• For
$$n = 4m^2$$
 we have: $\mathbb{E}[\mathbf{C}] = \frac{m(m-1)}{8m^2} \le \frac{1}{8}$.

Apply Markov's Inequality: $Pr[C \ge 1] \le \frac{\mathbb{E}[C]}{1} = \frac{1}{8}$.

$$\Pr[\mathsf{C} = 0] = 1 - \Pr[\mathsf{C} \ge 1] \ge 1 - \frac{1}{8} = \frac{7}{8}$$

I.e., with probability at least 7/8 we have no collisions and thus O(1) query time. But we are using $O(m^2)$ space to store *m* items...

Want to preserve O(1) query time while using O(m) space.

Want to preserve O(1) query time while using O(m) space.

Two-Level Hashing:



Want to preserve O(1) query time while using O(m) space.

Two-Level Hashing:



• For each bucket with s_i values, pick a collision free hash function mapping $[s_i] \rightarrow [s_i^2]$.



- For each bucket with s_i values, pick a collision free hash function mapping $[s_i] \rightarrow [s_i^2]$.
- Just Showed: A random function is collision free with probability $\geq \frac{7}{8}$ so can just generate a random hash function and check if it is collision free.

Query time for two level hashing is O(1): requires evaluating two hash functions.

Query time for two level hashing is O(1): requires evaluating two hash functions. What is the expected space usage?

Query time for two level hashing is O(1): requires evaluating two hash functions. What is the expected space usage?

Up to constants, space used is: $S = n + \sum_{i=1}^{n} S_i^2$



Query time for two level hashing is O(1): requires evaluating two hash functions. What is the expected space usage?

Up to constants, space used is: $\mathbb{E}[S] = n + \sum_{i=1}^{n} \mathbb{E}[S_i^2]$



Query time for two level hashing is O(1): requires evaluating two hash functions. What is the expected space usage? Up to constants, space used is: $\mathbb{E}[S] = n + \sum_{i=1}^{n} \mathbb{E}[S_i^2]$

Query time for two level hashing is O(1): requires evaluating two hash functions. What is the expected space usage?

Up to constants, space used is: $\mathbb{E}[S] = n + \sum_{i=1}^{n} \mathbb{E}[S_i^2]$

$$\mathbb{E}[\mathbf{s}_{i}^{2}] = \mathbb{E}\left[\left(\sum_{j=1}^{m} \mathbb{I}_{\mathbf{h}(x_{j})=i}\right)^{2}\right]$$

$$\mathbb{I}_{\mathbf{h}}(x_{j})=i = 1 \quad \text{if itom jheshey}$$

$$= 1 \quad \text{if to becket i}$$

$$= 0 \quad 0. \text{ w.}$$

Query time for two level hashing is O(1): requires evaluating two hash functions. What is the expected space usage?

Up to constants, space used is: $\mathbb{E}[S] = n + \sum_{i=1}^{n} \mathbb{E}[S_i^2]$

$$\mathbb{E}[\mathbf{s}_{i}^{2}] = \mathbb{E}\left[\left(\sum_{j=1}^{m} \mathbb{I}_{\mathbf{h}(x_{j})=i}\right)^{2}\right] \qquad \left(\mathbb{I}_{1} + \mathbb{I}_{2} + \mathbb{I}_{3}\right)\left(\mathbb{I}_{1} + \mathbb{I}_{2} + \mathbb{I}_{3}\right)$$
$$= \mathbb{E}\left[\sum_{j,k\in[m]}\mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right] \qquad \mathbb{Collisions again}$$

Collisions again!

 x_j, x_k : stored items, n: hash table size, **h**: random hash function, **S**: space usage of two level hashing, \mathbf{s}_i : # items stored in hash table at position *i*.

T. T.

Query time for two level hashing is O(1): requires evaluating two hash functions. What is the expected space usage?

Up to constants, space used is: $\mathbb{E}[S] = n + \sum_{i=1}^{n} \mathbb{E}[S_i^2]$

$$\underline{\mathbb{E}[\mathbf{s}_{i}^{2}]} = \mathbb{E}\left[\left(\sum_{j=1}^{m} \mathbb{I}_{\mathbf{h}(x_{j})=i}\right)^{2}\right]$$
$$= \mathbb{E}\left[\sum_{j,k\in[m]} \mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right] = \sum_{j,k\in[m]} \mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right].$$

Query time for two level hashing is O(1): requires evaluating two hash functions. What is the expected space usage?

Up to constants, space used is: $\mathbb{E}[S] = n + \sum_{i=1}^{n} \mathbb{E}[S_i^2]$

$$\mathbb{E}[\mathbf{s}_{i}^{2}] = \mathbb{E}\left[\left(\sum_{j=1}^{m} \mathbb{I}_{\mathbf{h}(x_{j})=i}\right)^{2}\right]$$
$$= \mathbb{E}\left[\sum_{j,k\in[m]} \mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right] = \sum_{j,k\in[m]} \mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right].$$
$$\cdot \text{ For } j = k,$$

Query time for two level hashing is O(1): requires evaluating two hash functions. What is the expected space usage?

Up to constants, space used is: $\mathbb{E}[S] = n + \sum_{i=1}^{n} \mathbb{E}[S_i^2]$

$$\mathbb{E}[\mathbf{s}_{i}^{2}] = \mathbb{E}\left[\left(\sum_{j=1}^{m} \mathbb{I}_{\mathbf{h}(x_{j})=i}\right)^{2}\right]$$
$$= \mathbb{E}\left[\sum_{j,k\in[m]} \mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right] = \sum_{j,k\in[m]} \mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right].$$
$$\cdot \text{ For } j = k,$$
$$\mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right] = \mathbb{E}\left[\left(\mathbb{I}_{\mathbf{h}(x_{j})=i}\right)^{2}\right]$$
$$= \mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{j})=i} \int_{\Omega}^{2} \frac{1}{n}\right]$$

Query time for two level hashing is O(1): requires evaluating two hash functions. What is the expected space usage?

Up to constants, space used is: $\mathbb{E}[S] = n + \sum_{i=1}^{n} \mathbb{E}[S_i^2]$

$$\mathbb{E}[\mathbf{s}_{i}^{2}] = \mathbb{E}\left[\left(\sum_{j=1}^{m} \mathbb{I}_{\mathbf{h}(x_{j})=i}\right)^{2}\right]$$
$$= \mathbb{E}\left[\sum_{j,k\in[m]} \mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right] = \sum_{j,k\in[m]} \mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right].$$
$$\cdot \text{ For } j = k,$$
$$\mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right] = \mathbb{E}\left[\left(\mathbb{I}_{\mathbf{h}(x_{j})=i}\right)^{2}\right] = \Pr[\mathbf{h}(x_{j})=i]$$

Query time for two level hashing is O(1): requires evaluating two hash functions. What is the expected space usage?

Up to constants, space used is: $\mathbb{E}[\mathbf{S}] = n + \sum_{i=1}^{n} \mathbb{E}[\mathbf{s}_{i}^{2}]$

$$\mathbb{E}[\mathbf{s}_{i}^{2}] = \mathbb{E}\left[\left(\sum_{j=1}^{m} \mathbb{I}_{\mathbf{h}(x_{j})=i}\right)^{2}\right]$$
$$= \mathbb{E}\left[\sum_{j,k\in[m]} \mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right] = \sum_{j,k\in[m]} \mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right].$$
$$\cdot \text{ For } j = k,$$
$$\mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right] = \mathbb{E}\left[\left(\mathbb{I}_{\mathbf{h}(x_{j})=i}\right)^{2}\right] = \Pr[\mathbf{h}(x_{j}) = i] = \frac{1}{n}.$$

Query time for two level hashing is O(1): requires evaluating two hash functions. What is the expected space usage?

Up to constants, space used is: $\mathbb{E}[\mathbf{S}] = n + \sum_{i=1}^{n} \mathbb{E}[\mathbf{s}_{i}^{2}]$

$$\mathbb{E}[\mathbf{s}_{i}^{2}] = \mathbb{E}\left[\left(\sum_{j=1}^{m} \mathbb{I}_{\mathbf{h}(x_{j})=i}\right)^{2}\right]$$
$$= \mathbb{E}\left[\sum_{j,k\in[m]} \mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right] = \sum_{j,k\in[m]} \mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right]$$
$$\cdot \text{ For } j = k,$$
$$\mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right] = \mathbb{E}\left[\left(\mathbb{I}_{\mathbf{h}(x_{j})=i}\right)^{2}\right] = \Pr[\mathbf{h}(x_{j}) = i] = \frac{1}{n}.$$

• For $j \neq k$,

 x_j, x_k : stored items, *n*: hash table size, **h**: random hash function, **S**: space usage of two level hashing, **s**_i: # items stored in hash table at position *i*.

10

Query time for two level hashing is O(1): requires evaluating two hash functions. What is the expected space usage?

Up to constants, space used is: $\mathbb{E}[\mathbf{S}] = n + \sum_{i=1}^{n} \mathbb{E}[\mathbf{s}_{i}^{2}]$

$$\mathbb{E}[\mathbf{s}_{i}^{2}] = \mathbb{E}\left[\left(\sum_{j=1}^{m} \mathbb{I}_{\mathbf{h}(x_{j})=i}\right)^{2}\right]$$
$$= \mathbb{E}\left[\sum_{j,k\in[m]} \mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right] = \sum_{j,k\in[m]} \mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right].$$
$$\cdot \text{ For } j = k,$$
$$\mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right] = \mathbb{E}\left[\left(\mathbb{I}_{\mathbf{h}(x_{j})=i}\right)^{2}\right] = \Pr[\mathbf{h}(x_{j}) = i] = \frac{1}{n}.$$
$$\cdot \text{ For } j \neq k, \mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{k})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right] = \mathbb{E}\left[\left(\mathbb{I}_{\mathbf{h}(x_{k})=i}\right)^{2}\right] = \Pr[\mathbf{h}(x_{j}) = i] = \frac{1}{n}.$$
$$\cdot \text{ For } j \neq k, \mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{k})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right] = \mathbb{E}\left[\mathbb{E}\left[\mathbb{E}\left[\mathbb{E}\left[\mathbf{h}(x_{k})=i\right] + \mathbb{E}\left[\mathbf{h}(x_{k})=i\right] + \mathbb{E}\left[\mathbf{h}(x_{k})=i\right]\right] = \mathbb{E}\left[\mathbb{E}\left[\mathbb{E}\left[\mathbf{h}(x_{k})=i\right] + \mathbb{E}\left[\mathbf{h}(x_{k})=i\right]\right] = \mathbb{E}\left[\mathbb{E}\left[\mathbf{h}(x_{k})=i\right] + \mathbb{E}\left[\mathbf{h}(x_{k})=i\right] = \frac{1}{n}.$$

Query time for two level hashing is O(1): requires evaluating two hash functions. What is the expected space usage?

Up to constants, space used is: $\mathbb{E}[\mathbf{S}] = n + \sum_{i=1}^{n} \mathbb{E}[\mathbf{s}_{i}^{2}]$

$$\mathbb{E}[\mathbf{s}_{i}^{2}] = \mathbb{E}\left[\left(\sum_{j=1}^{m} \mathbb{I}_{\mathbf{h}(x_{j})=i}\right)^{2}\right]$$
$$= \mathbb{E}\left[\sum_{j,k\in[m]} \mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right] = \sum_{j,k\in[m]} \mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right]$$
$$\cdot \text{ For } j = k,$$
$$\mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right] = \mathbb{E}\left[\left(\mathbb{I}_{\mathbf{h}(x_{j})=i}\right)^{2}\right] = \Pr[\mathbf{h}(x_{j}) = i] = \frac{1}{n}.$$
$$\cdot \text{ For } j \neq k, \mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right] = \Pr[\mathbf{h}(x_{j}) = i \cap \mathbf{h}(x_{k}) = i]$$

Query time for two level hashing is O(1): requires evaluating two hash functions. What is the expected space usage?

Up to constants, space used is: $\mathbb{E}[\mathbf{S}] = n + \sum_{i=1}^{n} \mathbb{E}[\mathbf{S}_{i}^{2}]$

$$\mathbb{E}[\mathbf{s}_{i}^{2}] = \mathbb{E}\left[\left(\sum_{j=1}^{m} \mathbb{I}_{\mathsf{h}(x_{j})=i}\right)^{2}\right] \xrightarrow{\mathbb{E}}\left[\left(\sum_{j=1}^{n} \mathbb{I}_{\mathsf{h}(x_{j})=i}\right)^{2}\right] \xrightarrow{\mathbb{E}}\left[\left(\sum_{j,k\in[m]}^{n} \mathbb{I}_{\mathsf{h}(x_{k})=i}\right)^{2}\right] \xrightarrow{\mathbb{E}}\left[\left(\sum_{j,k\in[m]}^{n} \mathbb{I}_{\mathsf{h}(x_{k})=i}\right)^{2}\right] \xrightarrow{\mathbb{E}}\left[\left(\sum_{j,k\in[m]}^{n} \mathbb{I}_{\mathsf{h}(x_{k})=i}\right)^{2}\right] \xrightarrow{\mathbb{E}}\left[\left(\sum_{j,k\in[m]}^{n} \mathbb{I}_{\mathsf{h}(x_{k})=i}\right)^{2}\right] \xrightarrow{\mathbb{E}}\left[\left(\sum_{j,k\in[m]}^{n} \mathbb{E}\left[\mathbb{I}_{\mathsf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathsf{h}(x_{k})=i}\right]\right] \xrightarrow{\mathbb{E}}\left[\left(\sum_{j,k\in[m]}^{n} \mathbb{E}\left[\mathbb{I}_{\mathsf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathsf{h}(x_{k})=i}\right]\right] \xrightarrow{\mathbb{E}}\left[\left(\sum_{j,k\in[m]}^{n} \mathbb{E}\left[\mathbb{E$$

• For
$$j = k$$
,

$$\mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_j)=i} \cdot \mathbb{I}_{\mathbf{h}(x_k)=i}\right] = \mathbb{E}\left[\left(\mathbb{I}_{\mathbf{h}(x_j)=i}\right)^2\right] = \Pr[\mathbf{h}(x_j)=i] = \frac{1}{n}.$$

• For
$$j \neq k$$
, $\mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_j)=i} \cdot \mathbb{I}_{\mathbf{h}(x_k)=i}\right] = \Pr[\mathbf{h}(x_j)=i \cap \mathbf{h}(x_k)=i] = \frac{1}{n^2}$.

.

•

$$\mathbb{E}[\mathbf{s}_{i}^{2}] = \sum_{j,k\in[m]} \mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right]$$

$$\mathbb{E}[\mathbf{s}_{i}^{2}] = \sum_{j,k\in[m]} \mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{j})=i}\right] + \mathbb{E}[\mathbf{x}_{k} \in [\mathbf{m}]]$$

$$\mathbb{E}[\mathbf{x}_{k} \in [\mathbf{m}]]$$

$$\mathbb{E}[\mathbf{x}_{k} \in [\mathbf{m}]]$$

$$\mathbb{E}[\mathbb{E}[\mathbf{x}_{k}] = i \cdot \mathbb{E}[\mathbf{x}_{k}] = \frac{1}{n}.$$

$$\mathbb{E}[\mathbb{E}[\mathbf{x}_{k}] = i \cdot \mathbb{E}[\mathbf{x}_{k}] = \frac{1}{n^{2}}.$$

$$\mathbb{E}[\mathbf{s}_i^2] = \sum_{j,k \in [m]} \mathbb{E}\left[\mathbb{I}_{\mathsf{h}(x_j)=i} \cdot \mathbb{I}_{\mathsf{h}(x_k)=i}\right]$$
$$= \underbrace{m \cdot \frac{1}{n}}_{n} + 2 \cdot \binom{m}{2} \cdot \frac{1}{n^2}$$

• For
$$j = k$$
, $\mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_j)=i} \cdot \mathbb{I}_{\mathbf{h}(x_k)=i}\right] = \frac{1}{n}$.

• For
$$j \neq k$$
, $\mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_j)=i} \cdot \mathbb{I}_{\mathbf{h}(x_k)=i}\right] = \frac{1}{n^2}$

$$\mathbb{E}[\mathbf{s}_i^2] = \sum_{j,k \in [m]} \mathbb{E}\left[\mathbb{I}_{\mathsf{h}(x_j)=i} \cdot \mathbb{I}_{\mathsf{h}(x_k)=i}\right]$$
$$= m \cdot \frac{1}{n} + 2 \cdot \binom{m}{2} \cdot \frac{1}{n^2}$$

• For
$$j = k$$
, $\mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_j)=i} \cdot \mathbb{I}_{\mathbf{h}(x_k)=i}\right] = \frac{1}{n}$.

• For
$$j \neq k$$
, $\mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_j)=i} \cdot \mathbb{I}_{\mathbf{h}(x_k)=i}\right] = \frac{1}{n^2}$

$$\mathbb{E}[\mathbf{s}_i^2] = \sum_{j,k \in [m]} \mathbb{E}\left[\mathbb{I}_{\mathsf{h}(x_j)=i} \cdot \mathbb{I}_{\mathsf{h}(x_k)=i}\right]$$
$$= m \cdot \frac{1}{n} + 2 \cdot \binom{m}{2} \cdot \frac{1}{n^2}$$

• For
$$j = k$$
, $\mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_j)=i} \cdot \mathbb{I}_{\mathbf{h}(x_k)=i}\right] = \frac{1}{n}$

• For
$$j \neq k$$
, $\mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_j)=i} \cdot \mathbb{I}_{\mathbf{h}(x_k)=i}\right] = \frac{1}{n^2}$

$$\mathbb{E}[\mathbf{s}_{i}^{2}] = \sum_{j,k \in [m]} \mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right]$$
$$= m \cdot \frac{1}{n} + 2 \cdot \binom{m}{2} \cdot \frac{1}{n^{2}}$$
$$= \frac{m}{n} + \frac{m(m-1)}{n^{2}} + \gamma$$
$$\cdot \text{ For } j = k, \mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right] = \frac{1}{n}.$$
$$\cdot \text{ For } j \neq k, \mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right] = \frac{1}{n^{2}}.$$

$$\mathbb{E}[\mathbf{s}_{i}^{2}] = \sum_{j,k \in [m]} \mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right]$$
$$= m \cdot \frac{1}{n} + 2 \cdot \binom{m}{2} \cdot \frac{1}{n^{2}}$$
$$= \underbrace{\frac{m}{n}}_{} + \underbrace{\frac{m(m-1)}{n^{2}}}_{} \leq 2 \text{ (If we set } n = m.)$$
$$\cdot \text{ For } j = k, \mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right] = \frac{1}{n}.$$
$$\cdot \text{ For } j \neq k, \mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right] = \frac{1}{n^{2}}.$$

$$\mathbb{E}[\mathbf{s}_{i}^{2}] = \sum_{j,k \in [m]} \mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right]$$

$$\mathcal{Q} = m \cdot \frac{1}{n} + 2 \cdot \binom{m}{2} \cdot \frac{1}{n^{2}}$$

$$= \frac{m}{n} + \frac{m(m-1)}{n^{2}} \leq 2 \text{ (If we set } n = m.)$$

$$\cdot \text{ For } j = k, \mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right] = \frac{1}{n}.$$

$$\cdot \text{ For } j \neq k, \mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_{j})=i} \cdot \mathbb{I}_{\mathbf{h}(x_{k})=i}\right] = \frac{1}{n^{2}}.$$

Total Expected Space Usage: (if we set n = m) $\underbrace{\mathbb{E}[S]}_{i=1} = n + \sum_{j=1}^{n} \mathbb{E}[s_{j}^{2}]$

Total Expected Space Usage: (if we set n = m)

$$\mathbb{E}[\mathbf{S}] = n + \sum_{i=1}^{n} \mathbb{E}[\mathbf{s}_i^2] \le n + n \cdot 2 = 3n = 3m.$$

.

$$\mathbb{E}[\mathbf{s}_i^2] = \sum_{j,k \in [m]} \mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_j)=i} \cdot \mathbb{I}_{\mathbf{h}(x_k)=i}\right]$$
$$= m \cdot \frac{1}{n} + 2 \cdot \binom{m}{2} \cdot \frac{1}{n^2}$$
$$= \frac{m}{n} + \frac{m(m-1)}{n^2} \le 2 \text{ (If we set } n = m.)$$
For $j = k$, $\mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_j)=i} \cdot \mathbb{I}_{\mathbf{h}(x_k)=i}\right] = \frac{1}{n}$.
For $j \neq k$, $\mathbb{E}\left[\mathbb{I}_{\mathbf{h}(x_j)=i} \cdot \mathbb{I}_{\mathbf{h}(x_k)=i}\right] = \frac{1}{n^2}$.

Total Expected Space Usage: (if we set n = m)

$$\mathbb{E}[\mathbf{S}] = n + \sum_{i=1}^{n} \mathbb{E}[\mathbf{s}_i^2] \le n + n \cdot 2 = 3n = 3m.$$

Near optimal space with O(1) query time!

So Far: we have assumed a fully random hash function $\underline{h}(x)$ with $Pr[\mathbf{h}(x) = i] = \frac{1}{n}$ for $i \in 1, ..., n$ and $\mathbf{h}(x), \mathbf{h}(y)$ independent for $x \neq y$.

So Far: we have assumed a fully random hash function h(x) with $Pr[h(x) = i] = \frac{1}{n}$ for $i \in 1, ..., n$ and h(x), h(y) independent for $x \neq y$.

To compute a random hash function we have to store a table of x values and their hash values. Would take at least O(m) space and O(m) query time to look up h(x) if we hash m values.
 Making our whole quest for O(1) query time pointless!



12

What properties did we use of the randomly chosen hash function?

What properties did we use of the randomly chosen hash function?

Pairwise Independent Hash Function. A random hash function from $\mathbf{h} : U \rightarrow [n]$ is pairwise independent if for all $i, j \in [n]$:

$$\Pr[\mathbf{h}(x) = i \cap \mathbf{h}(y) = j] = \frac{1}{n^2}.$$

What properties did we use of the randomly chosen hash function?

Pairwise Independent Hash Function. A random hash function from $\mathbf{h} : U \rightarrow [n]$ is pairwise independent if for all $i, j \in [n]$:

$$\Pr[\mathbf{h}(x) = i \cap \mathbf{h}(y) = j] = \frac{1}{n^2}.$$

Exercise 1: Check the two-level hashing proof to confirm that this property is all that was needed.

What properties did we use of the randomly chosen hash function?

Pairwise Independent Hash Function. A random hash function from $\mathbf{h} : U \rightarrow [n]$ is pairwise independent if for all $i, j \in [n]$:

$$Fr[\mathbf{h}(\mathbf{x}) = i \cap \mathbf{h}(\mathbf{y}) = j] = \frac{1}{n^2}.$$

Exercise 1: Check the two-level hashing proof to confirm that this property is all that was needed.

When $\mathbf{h}(x)$ and $\mathbf{h}(y)$ are chosen independently at random from [n], $\Pr[\mathbf{h}(x) = i \cap \mathbf{h}(y) = j] = \frac{1}{n^2}$ (so a fully random hash function is pairwise independent).

What properties did we use of the randomly chosen hash function?

Pairwise Independent Hash Function. A random hash function from $\mathbf{h} : U \rightarrow [n]$ is pairwise independent if for all $i, j \in [n]$:

$$\Pr[\mathbf{h}(x) = i \cap \mathbf{h}(y) = j] = \frac{1}{n^2}.$$

Exercise 1: Check the two-level hashing proof to confirm that this property is all that was needed.

When $\mathbf{h}(x)$ and $\mathbf{h}(y)$ are chosen independently at random from [n], $\Pr[\mathbf{h}(x) = i \cap \mathbf{h}(y) = j] = \frac{1}{n^2}$ (so a fully random hash function is pairwise independent).

Efficient Implementation: Let *p* be a prime with $p \ge |U|$. Choose random $\mathbf{a}, \mathbf{b} \in [p]$ with $\mathbf{a} \neq 0$. Represent *x* as an integer and let

 $\mathbf{h}(x) = (\underline{\mathbf{a}x} + \mathbf{b} \mod p) \mod n.$

Another common requirement for a hash function:

2-Universal Hash Function (low collision probability). A random hash function from $h: U \rightarrow [n]$ is two universal if:

$$\Pr[\mathbf{h}(x) = \mathbf{h}(y)] \le \frac{1}{n}$$

Another common requirement for a hash function:

2-Universal Hash Function (low collision probability). A random hash function from $h: U \rightarrow [n]$ is two universal if:

$$\Pr[\mathbf{h}(x) = \mathbf{h}(y)] \le \frac{1}{n}.$$

Think-Pair-Shair: Which is a more stringent requirement? 2-universal or pairwise independent?

Another common requirement for a hash function:

2-Universal Hash Function (low collision probability). A random hash function from $h: U \rightarrow [n]$ is two universal if:

$$\Pr[\mathbf{h}(x) = \mathbf{h}(y)] \le \frac{1}{n}.$$

Think-Pair-Shair: Which is a more stringent requirement? 2-universal or pairwise independent?

Pairwise Independent Hash Function. A random hash function from $\mathbf{h} : U \rightarrow [n]$ is pairwise independent if for all $i, j \in [n]$:

$$\Pr[\mathbf{h}(x) = i \cap \mathbf{h}(y) = j] = \frac{1}{n^2}.$$

Another common requirement for a hash function:

2-Universal Hash Function (low collision probability). A random hash function from $h: U \rightarrow [n]$ is two universal if:

 $\Pr[\mathbf{h}(x) = \mathbf{h}(y)] \le \frac{1}{n}.$

Think-Pair-Shair: Which is a more stringent requirement? 2-universal or pairwise independent?



Another common requirement for a hash function:

2-Universal Hash Function (low collision probability). A random hash function from $h: U \rightarrow [n]$ is two universal if:

$$\Pr[\mathbf{h}(x) = \mathbf{h}(y)] \le \frac{1}{n}.$$

Think-Pair-Shair: Which is a more stringent requirement? 2-universal or pairwise independent?

$$\Pr[\mathbf{h}(x) = \mathbf{h}(y)] = \sum_{i=1}^{n} \Pr[\mathbf{h}(x) = i \cap \mathbf{h}(y) = i] = n \cdot \frac{1}{n^2} = \frac{1}{n}.$$

Remember: A fully random hash function is both 2-universal and pairwise independent. But it is not efficiently implementable.

Another common requirement for a hash function:

2-Universal Hash Function (low collision probability). A random hash function from $h: U \rightarrow [n]$ is two universal if:

$$\Pr[\mathbf{h}(x) = \mathbf{h}(y)] \le \frac{1}{n}.$$

Think-Pair-Shair: Which is a more stringent requirement? 2-universal or pairwise independent?

$$\Pr[\mathbf{h}(x) = \mathbf{h}(y)] = \sum_{i=1}^{n} \Pr[\mathbf{h}(x) = i \cap \mathbf{h}(y) = i] = n \cdot \frac{1}{n^2} = \frac{1}{n}.$$

Remember: A fully random hash function is both 2-universal and pairwise independent. But it is not efficiently implementable. Exercise 2: Rework the two-level hashing proof to show that 2-universality is in fact all that is needed.

14