

15 → 19

## CS473 Algorithms: Lecture 16 (2022-03-22)

logistics: pset 6 due Fri

last lecture: randomized algo

today: randomized algo

Q: what is complexity of randomized algo?

I've been doing this

I've very experienced

runtime is a random variable

to see example

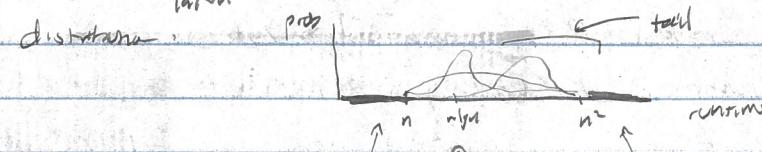
recall quicksort

given  $a = a_1, \dots, a_n$  integers, want to sort

$T(a) =$  runtime of quicksort on  $a$

as computer

$$t(n) = \max_{\text{partition}} \mathbb{E}[T(a)] \stackrel{\text{input fixed}}{\rightarrow} \stackrel{\text{random variable}}{\rightarrow} \stackrel{\text{also randomized}}{\rightarrow} \stackrel{\text{expected runtime}}{\rightarrow} = O(n \lg n) \quad \text{as computer}$$



is distribution?

$$\text{Q: } \Pr[T(a) \geq \gamma^2 n] \stackrel{\text{really bad runtime}}{\approx} \gamma^2 \quad \text{no guarantee} \quad \text{no guarantee}$$

$$\leq \gamma n \quad \text{small prob, acceptable} \quad \text{yes guarantee}$$

yes guarantee

I need more refined notion of probability?

$$\leq \gamma_2 n \quad \text{so small, essentially zero} \quad \text{yes guarantee}$$

yes guarantee

def: a randomized algo runs in time  $T(n)$  with probability  $1 - \delta(n)$  if

for all inputs of size  $n$ , the algorithm runs in time  $T(n)$ , and outputs the correct answer with probability  $\geq 1 - \delta(n)$

An algorithm runs in time  $T(n)$  with high probability if  $\delta(n) = \gamma_n$  ( $\gamma \rightarrow 0$  quickly)

rmk: two types of randomness: correctness vs random

next lesson will see algorithm whose response is not random, correctness only with high probability

Q:  $\Pr[X \geq \mathbb{E}[X]] \geq 1 - \delta$ ? (we've seen very  $\mathbb{E}[X]$  as measure of central tendency)

lem [Markov's inequality]:  $X \geq 0$  and  $\mathbb{E}[X] < \infty$  (non-negative is key!)

$$\text{for } a \geq 0, \Pr[X \geq a] \leq \frac{\mathbb{E}[X]}{a}$$

$$\Pr[X \geq a] = \frac{\Pr[X \geq a]}{a} \cdot a + \frac{\Pr[X \geq a] \cdot \mathbb{E}[X \geq a]}{a} \leq \frac{a}{a} = 1 \quad \text{probability}$$

aflo.

$$\geq a \cdot \Pr[X \geq a]$$

R

con:  $X \geq 0, k \geq 0$ .  $\Pr[X \geq k \cdot \mathbb{E}[X]] \leq \gamma_k$  (can't divide too far from expectation)

con:  $\Pr[T(a) \geq k \cdot \mathbb{E}[T(a)]] \leq \gamma_k$

$$\geq n^{3/10} \leq \Theta(\lg n) \quad \text{goes to zero quickly}$$

Q: do worse?

algo: quicksort - restart

- while

- run b = quicksort(a) for 2. O(n lg n) steps

to keep clock Z

that is O(n lg log Z)

expected runtime

Unspecified constant

- if b sorted, algo b

else [restart] Z

prop: quicksort - restart is always correct clear Z

prop: quicksort - restart runs in  $O(k n \lg n)$  time with probability  $1 - Y_{2^k}$  vs  $1 - Y_{n^k}$  Z

pf: chm: checking it b is sorted is  $O(n)$  time & single pass, look for violations Z

let L be number of keys

chm: runtime is  $L \cdot (2 \cdot O(R \lg r) + O(n))$  clear Z

$X_i = \begin{cases} 1 & \text{if attempt } i \text{ quicksort succeeds in } \\ 0 & \text{else} \end{cases}$  it has max steps? Z

chm:  $P[X_i = 0] = P[\text{quicksort runtime} \geq 2 \cdot \text{expected time}] \in Y_2$

co:  $\Pr[L > k] = \Pr[X_1 = \dots = X_k = 0] \in Y_2^k$  Marker

$\Rightarrow \Pr[\text{runtime} \geq k \cdot O(n \lg n)] \leq Y_2^k$  Z

cor: quicksort - restart runs in  $O(n \lg^2 n)$  time w.p.  $1 - Y_n$  why? Z

generic way to turn expected runtime into whp runtime  $O(n \lg^2 n)$  time w.p.  $1 - Y_n$ , any  $c = O(1)$  & probability of success

& slight penalty in runtime

Q: avoid penalty turning expected runtime into whp runtime? A better probabilistic tool

fact: quicksort runs in  $O(n \lg n)$  time with probability  $1 - Y_n$ , any  $c = O(1)$  clear Z

$\geq n^{2/3}$  time w.p.  $Y_2^{O(n \lg n)}$

it better probabilistic tools?

Q: what is expectation?

why start at zero expectation Z

ex: distribution of human height, prob



avg = typical Z  
why? Z

Moments / Central Limit Theorem Z

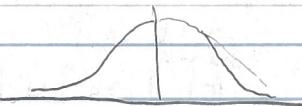
avg

height = height is sum of many small independent environmental factors  $\Rightarrow$  deviations "cancel out" Z

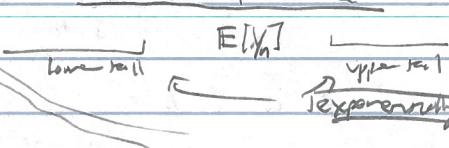
$X_1, \dots, X_n$  - random var over  $\mathbb{R}$ , identical and independent,  $\mathbb{E}[X_i]^2 < \infty$

then  $Y_n = \frac{X_1 + \dots + X_n}{\sqrt{n}} \rightarrow$  gaussian distribution

not too pathological Z



Q: (gaussian) reason? needed to also analyze



exponentially small & much less than Marker Z

then [Chernoff bound] [family of bounds]

$$X_1, \dots, X_n \in \{0, 1\}^{\text{dependent}} \text{, } \mathbb{E}[X_i] = p_i \quad \text{If may not be zero}$$

$$X = X_1 + \dots + X_n \quad \delta \geq 0 \quad \Pr[X \geq (1+\delta) \mathbb{E}[X]] \leq \left( \frac{e^\delta}{(1+\delta)^{1+\delta}} \right)^{\mathbb{E}[X]} \quad \begin{matrix} M = \mathbb{E}[X] \\ \text{messy - } \end{matrix}$$

$$\leq 20 \quad \Pr[|X - \mathbb{E}[X]| \geq \varepsilon \cdot n] \leq 2 \cdot e^{-\varepsilon^2 n / 4} \quad \begin{matrix} \text{sums} \\ \text{less general} \end{matrix}$$

If do applications, then prove rest on your own

e.g. (polling)

$$S \subseteq \Omega \text{ estimate } \frac{|S|}{|\Omega|} \quad \text{If fraction of voters for candidate I}$$

$$\text{algo: pick } \sigma_1, \dots, \sigma_t \in \Omega \text{ w/ random } \quad \text{I is parameter}$$

$$\text{return } \sum_i \frac{1_{\{\sigma_i \in S\}}}{t}$$

complexity:  $\Theta(t)$  [if there is +?]

$$\text{converges: } X_i = \mathbf{1}_{\{\sigma_i \in S\}} \quad \mathbb{E}[X_i] = \frac{|S|}{|\Omega|} = \mu$$

$$X = \sum_i X_i \quad \text{I also work} \quad \mathbb{E}[X] = \mu \cdot t$$

$$Y = \frac{1}{t} X \quad \text{I also work} \quad \mathbb{E}[Y] = \mu$$

$$\Pr[|Y - \mu| \geq \varepsilon] \leq 2e^{-\varepsilon^2 t / 4} \leq .05 \Rightarrow \varepsilon = .05$$

$$\frac{1}{t} |X - \mathbb{E}[X]|$$

if  $t \geq 8 \cdot 738$  & poly exp  
from back?

e.g. (balls into bins)

$m$  balls,  $n$  bins, each ball thrown into random bin. take (mean)

Q: what is the max load of bin  $j$ ?

$$X_{i,j} = \mathbf{1}_{\{\text{ball } i \rightarrow \text{bin } j\}} \quad \mathbb{E}[X_{i,j}] = \frac{1}{n}$$

$$Y_j = \sum_{i=1}^m X_{i,j} = \# \text{ balls in bin } j \quad \mathbb{E}[Y_j] = \text{linearity of expectation} \quad n \cdot Y_m = 1 \quad \begin{matrix} \text{Same as} \\ \text{hashing} \end{matrix}$$

$$\Pr[Y_j \geq c] \leq \left( \frac{e^{c-1}}{c^c} \right)^n = e^{-\Theta(c \ln c)} \quad \begin{matrix} \text{small!} \\ \text{and} \\ \text{linear} \end{matrix}$$

I was case when?

Q: what is the max load over all bins?

$$\Pr[\max_j Y_j \geq c] = \Pr[\exists j Y_j \geq c] \leq \sum_j \Pr[Y_j \geq c]$$

$$= n \cdot e^{-\Theta(c \ln c)}$$

$$= n \cdot \frac{1}{n^{\Theta(c)}} = \frac{1}{n^{\Theta(c)}} \quad \begin{matrix} \text{choose } c = k \cdot \ln n \\ \ln \ln n \end{matrix}$$

I w/ prob max  $\leq \Theta(\frac{\ln n}{\ln \ln n})$

$$\mathbb{E}[\max_j Y_j] = \underbrace{\mathbb{E}[Y_j | Y_j < k \frac{\ln n}{\ln \ln n}]}_{=: Y} \cdot \Pr[-] + \underbrace{\mathbb{E}[Y_j | Y_j \geq k \frac{\ln n}{\ln \ln n}]}_{\leq 1} \cdot \Pr[-] \leq n \cdot \frac{1}{n^{\Theta(c)}} = \frac{1}{n^{\Theta(c)}}$$

$$= O\left(\frac{\ln n}{\ln \ln n}\right) \text{ for } k = \Theta(1)$$

[Each bin has  $\mathbb{E}=1$  individually, but max load is expected to be higher]

thm [Chernoff].  $X_1, \dots, X_n \in \Sigma_{0,1}$  random variables, independent,  $\mathbb{E}[X_i] = p_i \in [0,1]$

$X = X_1 + \dots + X_n, \mathbb{E}[X] = \sum p_i$ ,  $\Pr[X \geq (1+\delta) \mathbb{E}[X]] \leq \left(\frac{e^\delta}{(1+\delta)^{1+\delta}}\right)^{\mathbb{E}[X]}$

pf: idea = Markov's inequality  $\frac{e^t - 1}{t} \text{ is strictly increasing}$

so transformed variable

$t > 0$  parameter.  $\Rightarrow x \mapsto e^{tx}$  is strictly increasing function

$$\Pr[X \geq (1+\delta) \mathbb{E}[X]] = \Pr[e^{tX} \geq e^{t(1+\delta)\mathbb{E}[X]}]$$

$$\mathbb{E}[e^{tX}] \leq \frac{\mathbb{E}[e^{tx}]}{e^{t(1+\delta)\mathbb{E}[X]}}$$

$$\mathbb{E}[e^{tx}] = \mathbb{E}[e^{t(x_1 + \dots + x_n)}] = \mathbb{E}[e^{tx_1 + \dots + tx_n}]$$

$$= \mathbb{E}[e^{tx_1}] \dots \mathbb{E}[e^{tx_n}] \quad [\text{Exp rule}]$$

$$= \mathbb{E}[e^{tx_i}] \dots \mathbb{E}[e^{tx_n}]$$

$$\mathbb{E}[e^{tx_i}] = e^{tx_i} \cdot \Pr[X_i = 1] + (e^0 \cdot \Pr[X_i = 0]) = 1 + p_i(e^t - 1) \leq e^{p_i(e^t - 1)}$$

$$p_i \underbrace{\left(\frac{e^t}{2}\right)}_{1-p_i} \underbrace{(1-p_i)}_{1+2 \leq e^2 \text{ (lucrative!)}}$$

$$\leq \prod_i e^{p_i(e^t - 1)} = e^{\sum p_i(e^t - 1)}$$

$$= e^{\mu(e^t - 1)}$$

$$\leq e^{\mu(e^{\delta t} - 1)} / e^{t(1+\delta)\mathbb{E}[X]}$$

choose  $t = \ln(1+\delta)$

$$= e^{\mu((1+\delta)-1)} / (1+\delta)^{(1+\delta)\mathbb{E}[X]} = \left(\frac{e^\delta}{(1+\delta)^{1+\delta}}\right)^\mu$$

today: randomized algo

- complexity of randomized algo

- expectation (probability)

- distribution (probability)

- tails (more realistic)

- tail bounds

- Markov

- quickest - easier to prove if "lucky"

$\rightarrow \infty$  for  $\mathbb{P}$

- tail bounds

- CLT

- Chernoff

- Hoeffding

- balls - n - bins

next lesson: randomized algo

logistics: per 6 due F17