Randomness in Computing

CS 537

LECTURE 9

Last time

- Chebyshev's inequality
- Computing the median of an array

Today

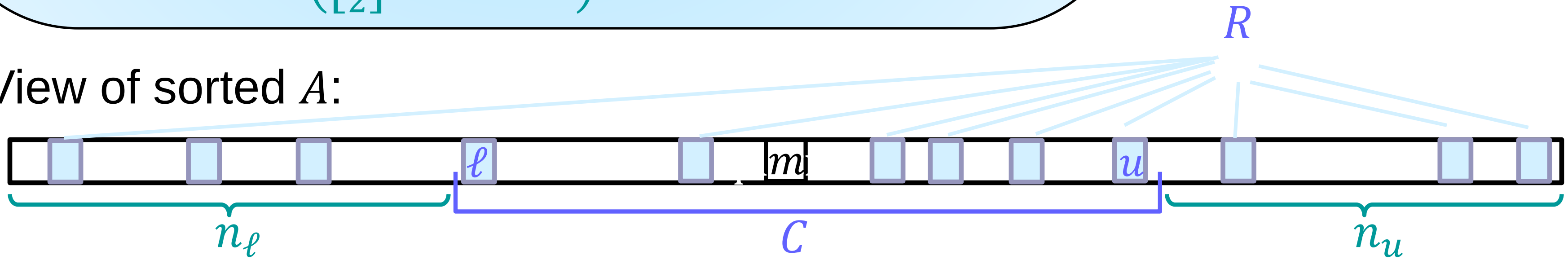
- Finish computing the median of an array
- Chernoff bounds

Randomized Median Algorithm

Input: array A of elements $a_1, \dots, a_n$
Output: median of A

1. Let R be an array $r_1, \dots, r_t$, where each r_i is chosen from A u.i.r. with replacement, where $t = \lceil n^{3/4} \rceil$.
2. Sort R.
3. Let ℓ be the $\left\lfloor \frac{n^{3/4}}{2} - \sqrt{n} \right\rfloor$-th smallest element in R.
4. Let u be the $\left\lceil \frac{n^{3/4}}{2} + \sqrt{n} \right\rceil$-th smallest element in R.
5. Use PARTITION from Quicksort to compute
$$C = \{a \in \mathrm{A} \mid \ell \le a \le u\},$$
$$n_\ell = |\{\, a \in A \mid a < \ell \,\}| \text{ and } n_u = |\{\, a \in A \mid a > u \,\}|$$
6. If $n_\ell > \left\lceil \frac{n}{2} \right\rceil$ or $n_u > \left\lceil \frac{n}{2} \right\rceil$ then **fail.**
7. If $|C| \le 4n^{3/4}$ then sort C; otherwise, **fail.**
8. Output the $\left(\left\lceil \frac{n}{2} \right\rceil - n_\ell + 1 \right)$-th smallest element in C.

View of sorted A:



Analysis: recall from last lecture

Theorem 1

Randomized Median Algorithm (RMA) terminates in $O(n)$ time.

It outputs either **fail** or the median.

Theorem 2

RMA outputs **fail** with probability at most $n^{-1/4}$.

Proof: Bad events $\mathcal{E}_1, \mathcal{E}_2$, and $\mathcal{E}_3$

$\mathcal{E}_3$: $|C| > 4n^{3/4}$

- RMA fails iff $\mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_3$ occurs

Lemma 1. $\Pr[\mathcal{E}_1] \leq \frac{1}{4} \cdot \frac{1}{n^{1/4}}$

Lemma 2. $\Pr[\mathcal{E}_2] \leq \frac{1}{4} \cdot \frac{1}{n^{1/4}}$

Analysis

Lemma 3. $\Pr[\mathcal{E}_3] \le \frac{1}{2} \cdot \frac{1}{n^{1/4}}$

$\mathcal{E}_3$: $|C| > 4n^{3/4}$

Proof: Define events

$\mathcal{E}_{3,1}$: $\ge 2n^{3/4}$ elements of C are greater than the median m

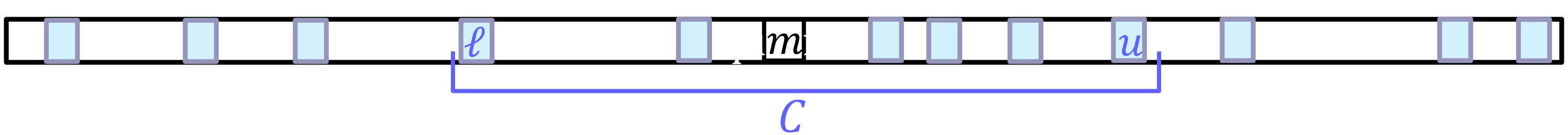
$\mathcal{E}_{3,2}$: $\ge 2n^{3/4}$ elements of C are smaller than the median m

By a union bound, $\Pr[\mathcal{E}_3] \le \Pr[\mathcal{E}_{3,1}] + \Pr[\mathcal{E}_{3,2}] = 2\Pr[\mathcal{E}_{3,1}]$

$\mathcal{E}_{3,1}$ holds $\Leftrightarrow$ rank of u in A is $\ge \left\lceil \frac{n}{2} \right\rceil + 2n^{3/4}$

but we threw out $\frac{n^{3/4}}{2} - \sqrt{n}$ samples in R with a larger value than u

$\ge \frac{n^{3/4}}{2} - \sqrt{n}$ samples in R are among $\left\lceil \frac{n}{2} \right\rceil - 2n^{3/4}$ largest in A



Analysis

Lemma 3. $\Pr[\mathcal{E}_3] \le \frac{1}{2} \cdot \frac{1}{n^{1/4}}$

$\mathcal{E}_3$: $|C| > 4n^{3/4}$

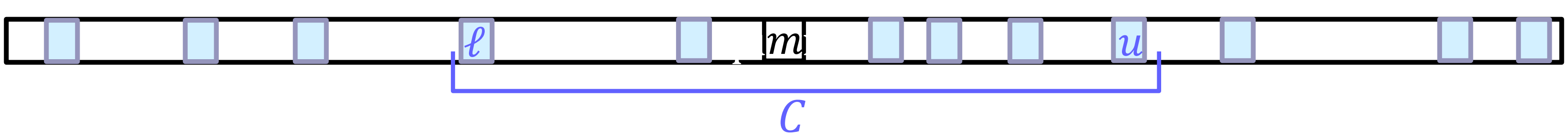
Proof: $\mathcal{E}_{3,1}$: $\ge 2n^{3/4}$ elements of C are greater than the median m

$\mathcal{E}_{3,1}$ holds $\Leftrightarrow \ge \frac{n^{3/4}}{2} - \sqrt{n}$ samples in R are among $\frac{n}{2} - 2n^{3/4}$ largest in A

Recall: $t = n^{3/4}$. For all $i \in [t]$, define

$$X_i = \begin{cases} 1 & \text{if } r_i \text{ isamong } \frac{n}{2} - 2n^{3/4} \text{ largest in } A \\ 0 & \text{otherwise} \end{cases}$$

$$X = \sum_{i \in [t]} X_i$$



Monte Carlo vs. Las Vegas

- Monte Carlo: a randomized algorithm that may fail or produce an incorrect answer.
- Las Vegas: a randomized algorithm that always returns the right answer.

- We can get a Las Vegas algorithm from a Monte Carlo algorithm that may fail by repeating until it succeeds.

Tail Bounds So Far

Markov Inequality

For all nonnegative random variables X and all $a > 0$,

$$\Pr[X \geq a] \leq \frac{\mathbb{E}[X]}{a}.$$

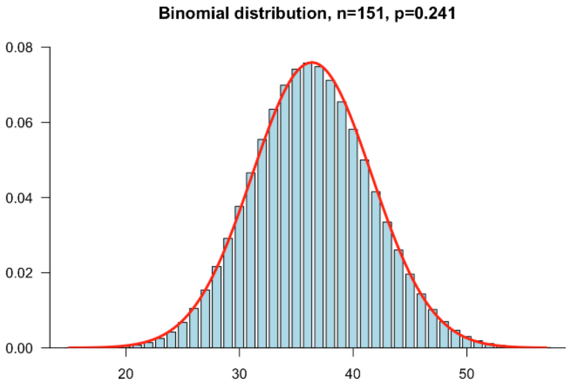
Chebyshev's Inequality

For all random variables X and all $a > 0$,

$$\Pr(|X - \mathbb{E}[X]| \geq a) \leq \frac{\mathrm{Var}(X)}{a^2}.$$

Sums of independent RVs

- Bernoulli trials:
  $X_1, \dots, X_n$ are mutually independent 0-1 RVs.
  $$\Pr[X_i = 1] = p$$
- Poisson trials (generalization): **≠ Poisson RVs**
  $X_1, \dots, X_n$ are mutually independent 0-1 RVs.
  $$\Pr[X_i = 1] = p_i$$



Generalization of binomial RVs

- Let $X = X_1 + \cdots + X_n$ and $\mu = \mathbb{E}[X]$. Then μ is
  $$\mathbb{E}[X_1 + \cdots + X_n] = \mathbb{E}[X_1] + \cdots + \mathbb{E}[X_n] = p_1 + \cdots + p_n$$
- Want to bound $\Pr[X \geq (1+\delta)\mu]$ for $\delta > 0$ ***upper tail***
  and $\Pr[X \leq (1-\delta)\mu]$ for $\delta \in (0,1)$ ***lower tail***
  in terms of μ and δ.

Sums of Independent Bernoullis

Chernoff Bound (Upper Tail)

Let $X_1, \ldots, X_n$ be independent Bernoulli RVs.
Let $X = X_1 + \cdots + X_n$ and $\mu = \mathbb{E}[X]$. Then

- (stronger) for all $\delta > 0$,

$$\Pr[X \geq (1+\delta)\mu] \leq \left(\frac{e^{\delta}}{(1+\delta)^{1+\delta}}\right)^{\mu}.$$

- (easier to use) for all $\delta \in (0,1]$,

$$\Pr[X \geq (1+\delta)\mu] \leq e^{-\mu\delta^2/3}.$$

Obtaining the bounds

Ideas:

- Consider RV e^{tX}, where t is a parameter.
- Apply Markov for e^{tX}.
- Use independence of X_i (and hence e^{tX_i})
- Pick the value of t to get the best bound.

Aside:

- $\mathbb{E}[X^k]$ is called the k-th moment of X.
- $\mathbb{E}[e^{tX}] = \sum_{k=0}^{\infty} \frac{t^k \, \mathbb{E}[X^k]}{k!}$ (power series)
- $\mathbb{E}[e^{tX}]$ is the moment-generating function of X.

Proof of (stronger) Chernoff Bound

- For all real $t > 0$,

  by Markov

  $\Pr[X \geq (1+\delta)\mu] \quad = \Pr\left[e^{tX} \geq e^{t(1+\delta)\mu}\right] \leq \frac{\mathbb{E}[e^{tX}]}{e^{t(1+\delta)\mu}}$

- $\mathbb{E}[e^{tX}] \quad = \mathbb{E}\left[e^{t(X_1+\cdots+X_n)}\right] = \mathbb{E}[e^{tX_1} \cdot e^{tX_2} \cdot \ldots \cdot e^{tX_n}]$

  $= \mathbb{E}[e^{tX_1}] \cdot \mathbb{E}[e^{tX_2}] \cdot \ldots \cdot \mathbb{E}[e^{tX_n}]$

  X_i are mutually independent , so are e^{tX_i}

- $e^{tX_i} = \begin{cases} e^t & \text{w.p.} \quad p_i \\ 1 & \text{w.p.} \quad 1-p_i \end{cases}$
- $\mathbb{E}[e^{tX_i}] =$
- Then $\mathbb{E}[e^{tX}] \leq$

Proof of (stronger) Chernoff Bound

- For all real $t > 0$,

  by Markov

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

  $$\leq \frac{e^{(e^t-1)\mu}}{e^{t(1+\delta)\mu}}$$

  $$= \left[\frac{e^{e^t-1}}{e^{t(1+\delta)}}\right]^{\mu}$$

  $$\mathbb{E}[e^{tX}] \leq e^{(e^t-1)\mu}$$

- To minimize $\frac{e^{e^t-1}}{e^{t(1+\delta)}} = e^{e^t-1-t(1+\delta)}$
  we minimize $\mathbf{e}^{t} - \mathbf{1} - t(\mathbf{1}+\boldsymbol{\delta})$

Setting the derivative w.r. t ***to 0*** gives

$$\mathbf{e}^{t} = \mathbf{1} + \boldsymbol{\delta}$$

Sums of Independent Bernoullis

Chernoff Bound (Upper Tail)

Let $X_1, \dots, X_n$ be independent Bernoulli RVs.
Let $X = X_1 + \cdots + X_n$ and $\mu = \mathbb{E}[X]$. Then

- (stronger) for all $\delta > 0$,

$$\Pr[X \geq (1+\delta)\mu] \leq \left(\frac{e^{\delta}}{(1+\delta)^{1+\delta}}\right)^{\mu}.$$

- (easier to use) for all $\delta \in (0,1]$,

$$\Pr[X \geq (1+\delta)\mu] \leq e^{-\mu\delta^2/3}.$$

Proof of weaker Chernoff Bound

- For all real $t > 0$,

  $$\Pr[X \geq (1+\delta)\mu] = \Pr\left[\mathrm{e}^{tX} \geq \mathrm{e}^{t(1+\delta)\mu}\right] \underset{\text{by Markov}}{\leq} \frac{\mathbb{E}[\mathrm{e}^{tX}]}{\mathrm{e}^{t(1+\delta)\mu}}$$

  $$\leq \left[\frac{\mathrm{e}^{\mathrm{e}^{t}-1}}{\mathrm{e}^{t(1+\delta)}}\right]^{\mu}$$

- To minimize $\frac{\mathrm{e}^{\mathrm{e}^{t}-1}}{\mathrm{e}^{t(1+\delta)}} = \mathrm{e}^{\mathrm{e}^{t}-1-t(1+\delta)}$

  we minimize $\mathbf{e}^{t} - \mathbf{1} - t(\mathbf{1}+\boldsymbol{\delta})$

  Setting the derivative w.r.t. t ***to 0*** gives

  $$\boxed{\mathbf{e}^{t} = \mathbf{1}+\boldsymbol{\delta}}$$

- To derive the easier Chernoff bound, we need to show $\forall\delta \in (0,1]$:

  $\mathbf{e}^{t} - \mathbf{1} - t(\mathbf{1}+\boldsymbol{\delta}) \leq -\delta^{2}/\mathbf{3}$, where $t = ln(\mathbf{1}+\boldsymbol{\delta})$

Sums of Independent Bernoullis

Chernoff Bound (Upper Tail)

Let $X_1, \ldots, X_n$ be independent Bernoulli RVs.
Let $X = X_1 + \cdots + X_n$ and $\mu = \mathbb{E}[X]$. Then

- (stronger) for all $\delta > 0$,

$$\Pr[X \geq (1+\delta)\mu] \leq \left(\frac{e^{\delta}}{(1+\delta)^{1+\delta}}\right)^{\mu}.$$

- (easier to use) for all $\delta \in (0,1]$,

$$\Pr[X \geq (1+\delta)\mu] \leq e^{-\mu\delta^2/3}.$$

Sums of Independent Bernoullis

Chernoff Bound (Lower Tail)

Let $X_1, \ldots, X_n$ be independent Bernoulli RVs.
Let $X = X_1 + \cdots + X_n$ and $\mu = \mathbb{E}[X]$. Then

- (stronger) for all $\delta \in (0,1)$,

$$\Pr[X \le (1-\delta)\mu] \le \left(\frac{e^{-\delta}}{(1-\delta)^{1-\delta}}\right)^{\mu}.$$

- (easier to use) for all $\delta \in (0,1)$,

$$\Pr[X \le (1-\delta)\mu] \le e^{-\mu\delta^2/2}.$$

Exercise 2

- The Halting Problem Team wins each hockey game they play with probability 1/3. Assuming outcomes of the games are independent, derive an upper bound on the probability that they have a winning season in n games.

- The Halting Problem Team hires a new coach, and critics revise their probability of winning each game to 3/4. Derive an upper bound on the probability they suffer a losing season.