GEMS OF TCS

RANDOMIZED ALGORITHMS

Sasha Golovnev
February 2, 2021
Randomized Algorithms

- Randomized algorithm may be faster and simpler
RANDOMIZED ALGORITHMS

- Randomized algorithm may be faster and simpler

- For some tasks randomness is necessary
RANDOMIZED ALGORITHMS

• Randomized algorithm may be faster and simpler

• For some tasks randomness is necessary

• We’ll use randomized algorithms in virtually all following topics
Review of Probability Theory

• Sample Space $\Omega$. 
**Review of Probability Theory**

- **Sample Space** $\Omega$.
  $\Omega = \{1, 2, 3, 4, 5, 6\}$;
Review of Probability Theory

• **Sample Space** $\Omega$.

  $\Omega = \{1, 2, 3, 4, 5, 6\}; \quad \Omega = \{HH, HT, TH, TT\}$
**Review of Probability Theory**

- **Sample Space** $\Omega$.

  $\Omega = \{1, 2, 3, 4, 5, 6\}; \quad \Omega = \{HH, HT, TH, TT\}$

- **Event** $A \subseteq \Omega$. 


Review of Probability Theory

• **Sample Space** $\Omega$.
  
  $\Omega = \{1, 2, 3, 4, 5, 6\}; \quad \Omega = \{HH, HT, TH, TT\}$

• **Event** $A \subseteq \Omega$. $A = \{2, 4, 6\};$
**Review of Probability Theory**

- **Sample Space** $\Omega$.
  $\Omega = \{1, 2, 3, 4, 5, 6\}$; $\Omega = \{HH, HT, TH, TT\}$

- **Event** $A \subseteq \Omega$. $A = \{2, 4, 6\}$; $A = \{TT, TH\}$
Review of Probability Theory

- **Sample Space** $\Omega$.
  $\Omega = \{1, 2, 3, 4, 5, 6\}; \quad \Omega = \{HH, HT, TH, TT\}$

- **Event** $A \subseteq \Omega$. $A = \{2, 4, 6\}; \quad A = \{TT, TH\}$

- **Probability measure**: $\forall A, \Pr(A) \in [0, 1]$
Review of Probability Theory

- **Sample Space** $\Omega$.
  
  $\Omega = \{1, 2, 3, 4, 5, 6\}; \quad \Omega = \{HH, HT, TH, TT\}$

- **Event** $A \subseteq \Omega$. $A = \{2, 4, 6\}; \quad A = \{TT, TH\}$

- **Probability measure**: $\forall A, \Pr(A) \in [0, 1]$
  
  - $\Pr(\Omega) = 1$
Review of Probability Theory

- **Sample Space** $\Omega$.
  $\Omega = \{1, 2, 3, 4, 5, 6\}; \quad \Omega = \{HH, HT, TH, TT\}$
- **Event** $A \subseteq \Omega$. $A = \{2, 4, 6\}; \quad A = \{TT, TH\}$
- **Probability measure**: $\forall A, \Pr(A) \in [0, 1]$
  - $\Pr(\Omega) = 1$
  - $A_1, A_2, \ldots$ are disjoint: $\Pr[\bigcup_i A_i] = \sum_i \Pr[A_i]$
**Review of Probability Theory**

- **Sample Space** $\Omega$.
  $\Omega = \{1, 2, 3, 4, 5, 6\}; \; \Omega = \{HH, HT, TH, TT\}$

- **Event** $A \subseteq \Omega$. $A = \{2, 4, 6\}; \; A = \{TT, TH\}$

- **Probability measure**: $\forall A, \Pr(A) \in [0, 1]$
  - $\Pr(\Omega) = 1$
  - $A_1, A_2, \ldots$ are disjoint: $\Pr[\bigcup A_i] = \sum_i \Pr[A_i]$
  - $A_1 = \{HH\}, \; A_2 = \{HT\}$,
    $\Pr[A_1 \cup A_2] = \Pr[A_1] + \Pr[A_2]$
INDEPENDENT EVENTS

- $A_1$ and $A_2$ are independent iff
  \[ \Pr[A_1 \cap A_2] = \Pr[A_1] \cdot \Pr[A_2] \]
  
  both happen
INDEPENDENT EVENTS

• $A_1$ and $A_2$ are independent iff
  \[ \Pr[A_1 \cap A_2] = \Pr[A_1] \cdot \Pr[A_2] \]
• $A_1 = \{1\text{st die is 6}\}, \; A_2 = \{2\text{nd die is 6}\}$
**Independent Events**

- $A_1$ and $A_2$ are independent iff
  \[
  \Pr[A_1 \cap A_2] = \Pr[A_1] \cdot \Pr[A_2]
  \]
- $A_1 = \{1\text{st die is } 6\}, \ A_2 = \{2\text{nd die is } 6\}$

\[
\Pr[A_1] = 1/6;
\]
**INDEPENDENT EVENTS**

- $A_1$ and $A_2$ are independent iff
  \[ \Pr[A_1 \cap A_2] = \Pr[A_1] \cdot \Pr[A_2] \]
- $A_1 = \{1\text{st die is 6}\}, A_2 = \{2\text{nd die is 6}\}$

\[
\begin{align*}
\Pr[A_1] &= \frac{1}{6}; \quad \Pr[A_2] = \frac{1}{6}; \\
(1,1) &\quad (1,2) \quad (1,3) \quad \ldots \quad (6,6) \quad \frac{1}{36}
\end{align*}
\]
INDEPENDENT EVENTS

• $A_1$ and $A_2$ are independent iff
  \[ \Pr[A_1 \cap A_2] = \Pr[A_1] \cdot \Pr[A_2] \]

• $A_1 = \{1\text{st die is 6}\}, A_2 = \{2\text{nd die is 6}\}$

  \[
  \Pr[A_1] = \frac{1}{6}; \quad \Pr[A_2] = \frac{1}{6}; \quad \Pr[A_1 \cap A_2] = \frac{1}{36}
  \]

  \[
  \Pr[A_1 \cap A_2] = \Pr[A_1] \cdot \Pr[A_2] = \Pr[A_1 \cap A_2]
  \]
INDEPENDENT EVENTS

• $A_1$ and $A_2$ are independent iff
  \[ \Pr[A_1 \cap A_2] = \Pr[A_1] \cdot \Pr[A_2] \]
• $A_1 = \{1\text{st die is } 6\}$, $A_2 = \{2\text{nd die is } 6\}$

  \[ \Pr[A_1] = \frac{1}{6}; \quad \Pr[A_2] = \frac{1}{6}; \quad \Pr[A_1 \cap A_2] = \frac{1}{36} \]

• $A_1 = \{1\text{st die is } 1\}$, $A_2 = \{\text{sum of two dice is } 2\}$
INDEPENDENT EVENTS

• $A_1$ and $A_2$ are independent iff
  $$\Pr[A_1 \cap A_2] = \Pr[A_1] \cdot \Pr[A_2]$$
• $A_1 = \{1\text{st die is 6}\}, A_2 = \{2\text{nd die is 6}\}$

  $\Pr[A_1] = 1/6; \quad \Pr[A_2] = 1/6; \quad \Pr[A_1 \cap A_2] = 1/36$

• $A_1 = \{1\text{st die is 1}\}, A_2 = \{\text{sum of two dice is 2}\}$

  $\Pr[A_1] = 1/6; \quad \Pr[A_2] = 1/12$
**INDEPENDENT EVENTS**

- $A_1$ and $A_2$ are independent iff
  \[ \Pr[A_1 \cap A_2] = \Pr[A_1] \cdot \Pr[A_2] \]
- $A_1 = \{1\text{st die is 6}\}$, $A_2 = \{2\text{nd die is 6}\}$
  \[ \Pr[A_1] = 1/6; \quad \Pr[A_2] = 1/6; \quad \Pr[A_1 \cap A_2] = 1/36 \]

- $A_1 = \{1\text{st die is 1}\}$, $A_2 = \{\text{sum of two dice is 2}\}$
  \[ \Pr[A_1] = 1/6; \quad \Pr[A_2] = 1/36; \]
INDEPENDENT EVENTS

- $A_1$ and $A_2$ are independent iff
  \[ \Pr[A_1 \cap A_2] = \Pr[A_1] \cdot \Pr[A_2] \]
- $A_1 = \{1\text{st die is 6}\}, A_2 = \{2\text{nd die is 6}\}$
  \[ \Pr[A_1] = 1/6; \quad \Pr[A_2] = 1/6; \quad \Pr[A_1 \cap A_2] = 1/36 \]

- $A_1 = \{1\text{st die is 1}\}, A_2 = \{\text{sum of two dice is 2}\}$
  \[ \Pr[A_1] = 1/6; \quad \Pr[A_2] = 1/36; \quad \Pr[A_1 \cap A_2] = 1/36 \]

\[ \Pr[A_1, A_2] \neq \Pr[A_1] \cdot \Pr[A_2] \]
RANDOM VARIABLE

- Result of experiment is often not event but number
Random Variable

- Result of experiment is often not event but number
- Random variable $\mathbf{X} : \Omega \rightarrow \mathbb{R}$
Random Variable

- Result of experiment is often not event but number
- Random variable $X: \Omega \rightarrow \mathbb{R}$
- Toss three coins, $X =$ number of heads

$\Omega = \{000, 001, 010, 011, 100, 101, 110, 111\}$

$X = 3 \ 2 \ 2 \ 2 \ 1 \ 2 \ 1 \ 1 \ 1 \ 0$
Random Variable

- Result of experiment is often not event but number
- Random variable $X: \Omega \rightarrow \mathbb{R}$
- Toss three coins, $X = \text{number of heads}$
- Throw two dice:
  - $\overline{Y} = \text{sum of numbers, } \overline{Z} = \text{max of numbers}$
**Random Variable**

- Result of experiment is often not event but number
- **Random variable** $X$: $\Omega \rightarrow \mathbb{R}$
- Toss three coins, $X = \text{number of heads}$
- Throw two dice:
  - $Y = \text{sum of numbers}$, $Z = \text{max of numbers}$
- **Expected value** $\mathbb{E}[X] = \sum_i \Pr[x_i] \cdot x_i$
  
  $X \in \{x_1, \ldots, x_n\} \implies \mathbb{E}[X] = \sum_i \Pr[x_i] \cdot x_i$
Random Variable

- Result of experiment is often not event but number
- **Random variable** \( X: \Omega \rightarrow \mathbb{R} \)
- Toss three coins, \( X = \) number of heads
- Throw two dice:
  - \( Y = \) sum of numbers, \( Z = \max \) of numbers
- **Expected value** \( \mathbb{E}[X] = \sum_i \Pr[x_i] \cdot x_i \)
- Throw a die, \( X = \) the number you’re getting

\[
\mathbb{E}[X] = \frac{1}{6} \cdot 1 + \frac{1}{6} \cdot 2 + \ldots + \frac{1}{6} \cdot 6 = 3.5
\]
Cloud Sync
Cloud Sync

- Synchronize local files to the cloud
**Cloud Sync**

- Synchronize local files to the cloud
- Has file been changed? File length: $n$ bits
Cloud Sync

- Synchronize local files to the cloud
- Has file been changed? File length: $n$ bits
- Algorithm: send $n$ bits
Cloud Sync

- Synchronize local files to the cloud
- Has file been changed? File length: $n$ bits
- Algorithm: send $n$ bits
- Can send $n - 1$ bits?
Cloud Sync. Lower Bound

$n$ bits

| 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 |

$\log \eta$
CLOUD SYNC. LOWER BOUND

1 0 0 1 1 0 1 1 0 0
Cloud Sync. Lower Bound

1 0 0 1 1 1 0 1 1 0 0

changed this bit
Cloud Sync. Lower Bound

No algorithm can solve the problem by sending \( n - 1 \) bits
Cloud Sync. Lower Bound

No algorithm can solve the problem by sending $n - 1$ bits

Randomized algorithm can solve the problem by sending $\approx \log n$ bits!
**RANDOMIZED ALGORITHM**

- **Local file**
  - `n-bits`
  - 1 0 0 1 1 0 1 1 0 0 0

- **Cloud file**
  - `n-bits`
  - 1 0 0 1 1 1 1 1 1 1 1 1 0 0 0
RANDOMIZED ALGORITHM

local file

\[
\begin{array}{cccccccc}
1 & 0 & 0 & 1 & 1 & 1 & 0 & 1
\end{array}
\]

\[a \in \{0, \ldots, 2^n - 1\}\]

\[
\begin{array}{cccccccc}
1 & 0 & 0 & 1 & 1 & 1 & 1 & 1
\end{array}
\]

cloud file

\[
\begin{array}{cccccccc}
1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0
\end{array}
\]
**Randomized Algorithm**

local file

\[
\begin{array}{cccccccc}
1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
\end{array}
\]

\[a \in \{0, \ldots, 2^n - 1\}\]

\[
\begin{array}{cccccccc}
1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
\end{array}
\]

\[b \in \{0, \ldots, 2^n - 1\}\]

cloud file
**Randomized Algorithm**

**Local File**

| 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 |

\[a \in \{0, \ldots, 2^n - 1\}\]

Pick random prime \(p \in \{2, 3, \ldots, 100n^2 \log n\}\)

**Cloud File**

| 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 |

\[b \in \{0, \ldots, 2^n - 1\}\]
**Randomized Algorithm**

**Local file**

| 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 |

\[a \in \{0, \ldots, 2^n - 1\}\]

\[a \mod p\]

\[b \in \{0, \ldots, 2^n - 1\}\]

**Pick random prime** \(p \in \{2, 3, \ldots, 100n^2 \log n\}\)

**Cloud file**

| 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 |

**RANDOMIZED ALGORITHM**

local file

\[
a \in \{0, \ldots, 2^n - 1\}
\]

Pick random prime \( p \in \{2, 3, \ldots, 100n^2 \log n\} \)

EQ iff

\[
a \equiv b \mod p
\]

\[
b \in \{0, \ldots, 2^n - 1\}
\]

\[
\{0, \ldots, p-1\} \subseteq \{0, \ldots, 100n^2 \log n\}^3
\]

\[
\text{#bits} = \log (100n^2 \log n) + \log(\log(n))
\]
ANALYSIS

\[ a = b \quad \text{we want server to say } a = b \quad \text{almost always} \]

\[ a \neq b \quad \text{we want server to say } a = b \quad \text{almost never} \]

\[ a = b \quad \forall p \quad a = b \mod p \]

Files are same \(\rightarrow\) server says \(a = b\)


**Analysis**

- If \( a = b \), then for every \( p \), \( a = b \mod p \). We always output EQ!
 ANALYSIS

• If $a = b$, then for every $p$, $a = b \mod p$. We always output EQ!

• If $a \neq b$, how often do we output EQ?
**Analysis**

- If $a = b$, then for every $p$, $a = b \mod p$. We always output EQ!
- If $a \neq b$, how often do we output EQ?
- $a - b = 0 \mod p$. 

\[
\begin{align*}
a - b &= 0 \\ a &\equiv b \mod p
\end{align*}
\]
ANALYSIS

- If $a = b$, then for every $p$, $a = b \mod p$. We always output EQ!
- If $a \neq b$, how often do we output EQ?
- $a - b = 0 \mod p$
- $2^n \geq a - b$
Analysis

• If $a = b$, then for every $p$, $a = b \mod p$. We always output $EQ!$

• If $a \neq b$, how often do we output $EQ$?

• $a - b = 0 \mod p$.

$2^n \geq a - b = p_1 \cdot p_2 \cdots p_k$

\[ \underbrace{p; \geq 2} \]
ANALYSIS

- If $a = b$, then for every $p$, $a = b \mod p$. We always output EQ!
- If $a \neq b$, how often do we output EQ?
- $a - b = 0 \mod p$.

$$2^n \geq a - b = p_1 \cdot p_2 \cdots p_k \geq 2^k \implies k \leq n$$

$\underbrace{a = b \mod p} \implies (a-b) \text{ is a multiple of } p$

but there are $\leq n$ $p$ s.t. $(a-b)$ is a multiple of $p$
**Analysis**

- If $a = b$, then for every $p$, $a = b \mod p$. We always output EQ!
- If $a \neq b$, how often do we output EQ?
- $a - b = 0 \mod p$.
  $$2^n \geq a - b = p_1 \cdot p_2 \cdots p_k \geq 2^k$$
- Prime Number Theorem: there are $\approx \frac{N}{\log N}$ prime numbers in the interval $\{2, 3, \ldots, N\}$

$$N = 100n^2 \log n, \ \text{the \ # \ of \ primes \ } \geq \frac{100n^2}{n}$$

Only $n$ out of $100n^2$ will lead to error

$$\Rightarrow P[\text{error}] = \frac{n}{100n^2} = \frac{1}{100n}$$
**Analysis**

- If \( a = b \), then for every \( p \), \( a = b \mod p \). We always output EQ!
- If \( a \neq b \), how often do we output EQ?
- \( a - b = 0 \mod p \).
  
  \[ 2^n \geq a - b = p_1 \cdot p_2 \cdots p_k \geq 2^k \]

- Prime Number Theorem: there are \( \approx \frac{N}{\log N} \) prime numbers in the interval \( \{2, 3, \ldots, N\} \)
- With probability \( \approx 1 - \frac{1}{100n} \), the output is correct
Linearity of Expectation

\[ E[X + Y] = \sum \mathbb{P}(IX = \sum \mathbb{P}(IY) \cap \sum \mathbb{P}(I) \cap \sum \mathbb{P}(I\text{)} \cap \sum \mathbb{P}(I\text{)}) \]
LINEARITY OF EXPECTATION

\[ \mathbb{E}[X + Y] = \sum_{i,j} \Pr[X = x_i \cap Y = y_j] \cdot (x_i + y_j) \]
**LINEARITY OF EXPECTATION**

\[ E[X + Y] = \sum_{i, j} \left( \Pr[X = x_i \cap Y = y_j] \cdot (x_i + y_j) \right) \]

\[ = \sum_i x_i \sum_j \Pr[X = x_i \cap Y = y_j] \]

\[ + \sum_j y_j \sum_i \Pr[X = x_i \cap Y = y_j] \]

\[ = \Pr[X = x_i] \]

\[ + \Pr[Y = y_j] \]
LINEARITY OF EXPECTATION

\[ E[X + Y] \]

\[ E[X + Y] = \sum_{i,j} i, j \Pr[X = x_i \cap Y = y_j] \cdot (x_i + y_j) \]

\[ = \sum_i x_i \sum_j \Pr[X = x_i \cap Y = y_j] \]

\[ + \sum_j y_j \sum_i \Pr[X = x_i \cap Y = y_j] \]

\[ = \sum_i x_i \Pr[X = x_i] + \sum_j y_j \sum_i \Pr[Y = y_j] \]
Linearity of Expectation

\[ \mathbb{E}[X + Y] \]

\[ \mathbb{E}[X + Y] = \sum_{i,j} i, j \Pr[X = x_i \cap Y = y_j] \cdot (x_i + y_j) \]

\[ = \sum_{i} x_i \sum_{j} \Pr[X = x_i \cap Y = y_j] \]

\[ + \sum_{j} y_j \sum_{i} \Pr[X = x_i \cap Y = y_j] \]

\[ = \sum_{i} x_i \Pr[X = x_i] + \sum_{j} y_j \Pr[Y = y_j] \]

\[ = \mathbb{E}[X] + \mathbb{E}[Y] \]
LINEARITY OF EXPECTATION

• One die: $\mathbb{E}[X] = 3.5$
Linearity of Expectation

- One die: $\mathbb{E}[X] = 3.5$
- Five dice? $\mathbb{E}[X_1 + X_2 + X_3 + X_4 + X_5]$?
**Linearity of Expectation**

- One die: $\mathbb{E}[X] = 3.5$

- Five dice? $\mathbb{E}[X_1 + X_2 + X_3 + X_4 + X_5]$?

- By linearity of expectation:

  $\mathbb{E}[X_1 + X_2 + X_3 + X_4 + X_5]$

  $= \mathbb{E}[X_1] + \mathbb{E}[X_2] + \mathbb{E}[X_3] + \mathbb{E}[X_4] + \mathbb{E}[X_5]$

  $= 5 \cdot 3.5 = 17.5$
Break

- Alice and Bob have (unusual) dice
- Numbers on Alice’s die are 2, 2, 2, 2, 3, 3
- Numbers on Bob’s die are 1, 1, 1, 1, 6, 6
- Alice and Bob throw their dice; the one with the larger number on the die wins
- Whose die has larger expected number? Bob
- Who wins with higher probability? Alice
Maximum Cut (Max-CUT)
Maximum Cut

- Undirected graph $G$, vertices $V$, edges $E$
Maximum Cut

- Undirected graph $G$, vertices $V$, edges $E$
- Bipartition of $V$ that maximizes the number of edges crossing the partition
**Maximum Cut**

- Undirected graph $G$, vertices $V$, edges $E$
- Bipartition of $V$ that maximizes the number of edges crossing the partition
- Bipartition: $\overline{S} \subseteq V, \overline{\overline{S}} \subseteq V$
Maximum Cut

- Undirected graph $G$, vertices $V$, edges $E$
- Bipartition of $V$ that maximizes the number of edges crossing the partition
- Bipartition: $S \subseteq V$, $\overline{S} \subseteq V$
- Cut $\delta(S) = \{(u, v) \in E : u \in S, v \in \overline{S}\}$
**Maximum Cut**

- Undirected graph $G$, vertices $V$, edges $E$
- Bipartition of $V$ that maximizes the number of edges crossing the partition
- Bipartition: $S \subseteq V$, $\overline{S} \subseteq V$
- Cut $\delta(S) = \{(u, v) \in E : u \in S, v \in \overline{S}\}$
- Max-CUT: $\max_{S \subseteq V} \delta(S)$
Maximum Cut

- Undirected graph $G$, vertices $V$, edges $E$
- Bipartition of $V$ that maximizes the number of edges crossing the partition
- Bipartition: $S \subseteq V$, $\overline{S} \subseteq V$
- Cut $\delta(S) = \{(u, v) \in E: u \in S, v \in \overline{S}\}$
- Max-CUT: $\max_{S \subseteq V} \delta(S)$
- NP-hard to solve
Maximum Cut

- Undirected graph $G$, vertices $V$, edges $E$
- Bipartition of $V$ that maximizes the number of edges crossing the partition
- Bipartition: $S \subseteq V$, $\overline{S} \subseteq V$
- Cut $\delta(S) = \{(u, v) \in E : u \in S, v \in \overline{S}\}$
- Max-CUT: $\max_{S \subseteq V} \delta(S)$
- NP-hard to solve exactly
RANDOMIZED APPROXIMATION

• Output a random subset $S \subseteq V$
RANDOMIZED APPROXIMATION

- Output a random subset $S \subseteq V$
- In other words, add each vertex $v$ in $S$ independently with probability $1/2$
RANDOMIZED APPROXIMATION

• Output a random subset $S \subseteq V$

• In other words, add each vertex $v$ in $S$ independently with probability $1/2$

• Each edge $(u, v)$ is cut with probability $1/2$
\[ R \setminus \text{ANALYSIS} \]

- \( X_{u,v} = 1 \) if \((u, v)\) is cut, \( X_{u,v} = 0 \) otherwise
**Analysis**

- $X_{u,v} = 1$ if $(u, v)$ is cut, $X_{u,v} = 0$ otherwise
- $X_{u,v} = 1$ with probability $1/2$

$$E[X_{u,v}] = \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot 0 = \frac{1}{2}$$
ANALYSIS

- $X_{u,v} = 1$ if $(u, v)$ is cut, $X_{u,v} = 0$ otherwise
- $X_{u,v} = 1$ with probability 1/2
- $\mathbb{E}[X_{u,v}] = 1/2$
**Analysis**

- $X_{u,v} = 1$ if $(u, v)$ is cut, $X_{u,v} = 0$ otherwise
- $X_{u,v} = 1$ with probability $1/2$
- $\mathbb{E}[X_{u,v}] = 1/2$
- Number of cut edges

$$\sum_{(u,v) \in E} X_{u,v}$$
**Analysis**

- $X_{u,v} = 1$ if $(u, v)$ is cut, $X_{u,v} = 0$ otherwise
- $X_{u,v} = 1$ with probability 1/2
- $\mathbb{E}[X_{u,v}] = 1/2$
- Number of cut edges

\[
\sum_{(u,v) \in E} X_{u,v}
\]

- Expected number of cut edges
\[
\mathbb{E}\left[ \sum_{(u,v) \in E} X_{u,v} \right] = \sum_{(u,v) \in E} \mathbb{E}[X_{u,v}] = \frac{|E|}{2}
\]
2-APPROXIMATION

• Max-CUT: $\text{OPT} \leq |E|$
2-APPROXIMATION

• Max-CUT: $\text{OPT} \leq |E|$

• Our algorithm: $\mathbb{E}[\delta(S)] \geq |E|/2$
2-APPROXIMATION

- Max-CUT: \( \text{OPT} \leq |E| \)
- Our algorithm: \( \mathbb{E}[\delta(S)] \geq |E|/2 \)
- \( \mathbb{E}[\delta(S)] \geq \text{OPT}/2 \)
2-APPROXIMATION

- Max-CUT: \( \text{OPT} \leq |E| \)
- Our algorithm: \( \mathbb{E}[\delta(S)] \geq |E|/2 \)
- \( \mathbb{E}[\delta(S)] \geq \text{OPT} / 2 \)
- Can we have algorithm that always outputs \( \delta(S) \geq \text{OPT} / 2 \)?
**Markov’s Inequality**

<table>
<thead>
<tr>
<th>Theorem</th>
<th>$X \geq 0$</th>
</tr>
</thead>
<tbody>
<tr>
<td>If $X$ is non-negative random variable, then</td>
<td></td>
</tr>
<tr>
<td>$\forall a$</td>
<td></td>
</tr>
<tr>
<td>$\Pr[X \geq a] \leq \frac{\mathbb{E}[X]}{a}$.</td>
<td></td>
</tr>
</tbody>
</table>
MARKOV’S INEQUALITY

Theorem

*If X is non-negative random variable*, then

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

\[ a = 2 \mathbb{E}[X] \]

Examples:

\[ \Pr[X \geq 2\mathbb{E}[X]] \leq \frac{1}{2}. \]
**Markov’s Inequality**

**Theorem**

If $X$ is non-negative random variable*, then

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

**Examples:**

$$
\Pr[X \geq 2\mathbb{E}[X]] \leq \frac{1}{2}.
$$  \quad a = 5 \in \mathbb{E}[X]

$$
\Pr[X \geq 5\mathbb{E}[X]] \leq \frac{1}{5}.
$$
<table>
<thead>
<tr>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>A lottery ticket costs 10 dollars. A 40% of a lottery budget goes to prizes. Show that the chances to win 500 dollars or more are less than 1%</td>
</tr>
</tbody>
</table>
# Lottery Budget

## Problem

A lottery ticket costs 10 dollars. A 40% of a lottery budget goes to prizes. Show that the chances to win 500 dollars or more are less than 1%

- Assume the contrary: the probability to win 500 dollars or more is at least 0.01
LOTTERY BUDGET

Problem
A lottery ticket costs 10 dollars. A 40% of a lottery budget goes to prizes. Show that the chances to win 500 dollars or more are less than 1%

- Assume the contrary: the probability to win 500 dollars or more is at least 0.01
- Denote the number of tickets sold by $n$
**Problem**

A lottery ticket costs 10 dollars. A 40% of a lottery budget goes to prizes. Show that the chances to win 500 dollars or more are less than 1%

- Assume the contrary: the probability to win 500 dollars or more is at least 0.01
- Denote the number of tickets sold by $n$
- Then the budget of the lottery is $10n$ dollars
A lottery ticket costs 10 dollars. A 40% of a lottery budget goes to prizes. Show that the chances to win 500 dollars or more are less than 1%

- Assume the contrary: the probability to win 500 dollars or more is at least 0.01
- Denote the number of tickets sold by $n$
- Then the budget of the lottery is $10n$ dollars
- $10n \times 0.4 = 4n$ dollars are spent on the prizes
**Lottery Budget**

**Problem**

A lottery ticket costs 10 dollars. A 40% of a lottery budget goes to prizes. Show that the chances to win 500 dollars or more are less than 1%

- Assume the contrary: the probability to win 500 dollars or more is at least 0.01
- Denote the number of tickets sold by $n$
- Then the budget of the lottery is $10n$ dollars
- $10n \times 0.4 = 4n$ dollars are spent on the prizes
- By our assumption at least $\frac{n}{100}$ tickets win at least 500 dollars
## Lottery Budget

### Problem

A lottery ticket costs 10 dollars. A 40% of a lottery budget goes to prizes. Show that the chances to win 500 dollars or more are less than 1%

- In total these tickets win $\frac{n}{100} \times 500 = 5n$ dollars
### Problem

A lottery ticket costs 10 dollars. A 40% of a lottery budget goes to prizes. Show that the chances to win 500 dollars or more are less than 1%

- In total these tickets win \( \frac{n}{100} \times 500 = 5n \) dollars
- This exceeds the total prize budget of \( 4n \)!
Problem
A lottery ticket costs 10 dollars. A 40% of a lottery budget goes to prizes. Show that the chances to win 500 dollars or more are less than 1%

- In total these tickets win $\frac{n}{100} \times 500 = 5n$ dollars
- This exceeds the total prize budget of $4n$!
- Contradiction!
GEOMETRIC PROOF

$E[f] \geq a \times \Pr[f \geq a] \Leftrightarrow \Pr[f \geq a] \leq \frac{E[f]}{a}$
GEOMETRIC PROOF

$\mathbb{E}[f] \geq a \times \Pr[f \geq a]$

Suppose $f$ takes values $a_1, a_2, a_3, a_4$ with probabilities $p_1, p_2, p_3, p_4$
GEOMETRIC PROOF

$\mathbb{E}f \geq a \times \Pr[f \geq a]$  
Suppose $f$ takes values $a_1, a_2, a_3, a_4$ with probabilities $p_1, p_2, p_3, p_4$
GEOMETRIC PROOF

\[ \mathbb{E}f \geq a \times \Pr[f \geq a] \]
Suppose \( f \) takes values \( a_1, a_2, a_3, a_4 \) with probabilities \( p_1, p_2, p_3, p_4 \)
GEOMETRIC PROOF

\[ \mathbb{E}[f] \geq a \times \Pr[f \geq a] \]
Suppose \( f \) takes values \( a_1, a_2, a_3, a_4 \) with probabilities \( p_1, p_2, p_3, p_4 \)
$\mathbb{E}f \geq a \times \Pr[f \geq a]$

Suppose $f$ takes values $a_1, a_2, a_3, a_4$ with probabilities $p_1, p_2, p_3, p_4$
GEOMETRIC PROOF

\[ \mathbb{E}f \geq a \times \text{Pr}[f \geq a] \]

Suppose \( f \) takes values \( a_1, a_2, a_3, a_4 \) with probabilities \( p_1, p_2, p_3, p_4 \)

\( \mathbb{E}f \) is the area of the gray region
GEOMETRIC PROOF

\[ Ef \geq a \times \Pr[f \geq a] \]

Suppose \( f \) takes values \( a_1, a_2, a_3, a_4 \) with probabilities \( p_1, p_2, p_3, p_4 \)

\( Ef \) is the area of the gray region

\( a \times \Pr[f \geq a] \) is the area of the red region
\[ Ef \geq a \times \Pr[f \geq a] \]

Suppose \( f \) takes values \( a_1, a_2, a_3, a_4 \) with probabilities \( p_1, p_2, p_3, p_4 \)

\[ Ef \geq a \times \Pr[f \geq a] \]

\[ E[C \times \geq 3 \cdot E[C \times 1]] \leq \frac{1}{3} \]

\( Ef \) is the area of the gray region

\( a \times \Pr[f \geq a] \) is the area of the red region

The gray region is larger: the inequality follows
Approximation Guarantee

\[ \mathbb{E}[\# \text{cut edges}] = \frac{|E|}{2} \rightarrow \mathbb{E}[\# \text{uncut edges}] = \frac{|E|}{2} \]
APPROXIMATION GUARANTEE

\[ \varepsilon = 0.01 \]

\[ \mathbb{E}[\text{\#cut edges}] = |E|/2 \rightarrow \mathbb{E}[\text{\#uncut edges}] = \frac{|E|}{2} \]

\[ \text{Pr}[\text{\#uncut edges} \geq \frac{|E|}{2} (1 + \varepsilon)] \leq \frac{1}{1+\varepsilon} \]
**Approximation Guarantee**

- $\mathbb{E}[\#\text{cut edges}] = |E|/2 \rightarrow \mathbb{E}[\#\text{uncut edges}]
- $\Pr[\#\text{uncut edges} \geq \frac{|E|}{2} (1 + \varepsilon)] \leq \frac{1}{1+\varepsilon}$
- $\Pr[\#\text{cut edges} \leq \frac{|E|}{2} (1 - \varepsilon)] \leq \frac{1}{1+\varepsilon} \leq 1 - \varepsilon/2$
**Approximation Guarantee**

- $\mathbb{E}[\text{#cut edges}] = |E|/2 \rightarrow \mathbb{E}[\text{#uncut edges}]$
- $\Pr[\text{#uncut edges} \geq \frac{|E|}{2} (1 + \varepsilon)] \leq \frac{1}{1+\varepsilon}$
- $\Pr[\text{#cut edges} \leq \frac{|E|}{2} (1 - \varepsilon)] \leq \frac{1}{1+\varepsilon} \leq 1 - \varepsilon/2$
- With probability at least $\varepsilon/2$, we have $\frac{2}{1-\varepsilon}$-approximation

\[
\text{#cut edges} \geq |E|/2 (1-\varepsilon)
\]
Approximation Guarantee

- $\mathbb{E}[\# \text{cut edges}] = |E|/2 \rightarrow \mathbb{E}[\# \text{uncut edges}]
- \Pr[\# \text{uncut edges} \geq \frac{|E|}{2} (1 + \varepsilon)] \leq \frac{1}{1+\varepsilon}
- \Pr[\# \text{cut edges} \leq \frac{|E|}{2} (1 - \varepsilon)] \leq \frac{1}{1+\varepsilon} \leq 1 - \varepsilon/2
- With probability at least $\varepsilon/2$, we have $\frac{2}{1-\varepsilon}$-approximation
- Ex. $\varepsilon = 1/100$: with probability at least $1/200$, we have $2.03$-approximation
PROBABILITY AMPLIFICATION

New algorithm

- Pick independent uniform subsets
  \( S_1, \ldots, S_k \subseteq V \)
Probability Amplification

- Pick independent uniform subsets $S_1, \ldots, S_k \subseteq V$
- Output the subset with maximum cut $\delta(S_i)$
Probability Amplification

- Pick independent uniform subsets $S_1, \ldots, S_k \subseteq V$
- Output the subset with maximum cut $\delta(S_i)$
- $\Pr[\max \delta(S_i) \leq \frac{|E|}{2} (1 - \varepsilon)]$
**Probability Amplification**

- Pick independent uniform subsets $S_1, \ldots, S_k \subseteq V$
- Output the subset with maximum cut $\delta(S_i)$
- $\Pr[\max \delta(S_i) \leq \frac{|E|}{2}(1 - \varepsilon)] = \Pr[\text{all } \delta(S_i) \leq \frac{|E|}{2}(1 - \varepsilon)]$
PROBABILITY AMPLIFICATION

• Pick independent uniform subsets $S_1, \ldots, S_k \subseteq V$

• Output the subset with maximum cut $\delta(S_i)$

• $\Pr[\max \delta(S_i) \leq \frac{|E|}{2}(1-\varepsilon)] = \Pr[\text{all } \delta(S_i) \leq \frac{|E|}{2}(1-\varepsilon)]$

  $\leq (1 - \varepsilon/2)^k$

$$\leq 0.99$$
PROBABILITY AMPLIFICATION

• Pick independent uniform subsets $S_1, \ldots, S_k \subseteq V$

• Output the subset with maximum cut $\delta(S_i)$

• $\Pr[\max \delta(S_i) \leq \frac{|E|}{2}(1-\varepsilon)] = \Pr[\text{all } \delta(S_i) \leq \frac{|E|}{2}(1-\varepsilon)] \\ \leq (1-\varepsilon/2)^k \leq e^{-\varepsilon k/2}$

$$e^x = 1 + x + \frac{x^2}{2} + \cdots$$

$$e^{\frac{\varepsilon}{2}} \geq 1 + \frac{\varepsilon}{2} \quad \Rightarrow \quad \left(1 - \frac{\varepsilon}{2}\right)^k \leq e^{-\varepsilon k/2}$$
PROBABILITY AMPLIFICATION

\[ \mathbb{E} \text{ [Mach's in}] \text{ w small p. output good approx] } \]

- Pick independent uniform subsets \( S_1, \ldots, S_k \subseteq V \)

- Output the subset with maximum cut \( \delta(S_i) \)

\[ \Pr[\max \delta(S_i) \leq \frac{|E|}{2} (1 - \varepsilon)] = \Pr[\text{all } \delta(S_i) \leq \frac{|E|}{2} (1 - \varepsilon)] \]
\[ \leq (1 - \varepsilon/2)^k \leq e^{-\varepsilon k/2} \leq \frac{1}{10^{10} n} \text{ for } k = \frac{2 \ln n + 50}{\varepsilon} \]

\[ e^{-\varepsilon k/2} = \frac{1}{10^{10} \cdot n} \]

\[ \Rightarrow \text{ outputs } \frac{2}{1 - \varepsilon} \text{ w.p. } 1 - \frac{1}{10^{10} n} \]
Probability Amplification

- Pick independent uniform subsets $S_1, \ldots, S_k \subseteq V$

- Output the subset with maximum cut $\delta(S_i)$

- \[ \Pr[\max \delta(S_i) \leq \frac{|E|}{2} (1 - \varepsilon)] = \Pr[\text{all } \delta(S_i) \leq \frac{|E|}{2} (1 - \varepsilon)] \leq (1 - \varepsilon/2)^k \leq e^{-\varepsilon k/2} \leq \frac{1}{10^{10} n} \] for $k = \frac{2 \ln n + 50}{\varepsilon}$

- We have $\frac{2}{1 - \varepsilon}$-approximation with probability $1 - \frac{1}{10^{10} n}$
SUMMARY

- Randomized algorithm may be faster and simpler
SUMMARY

- Randomized algorithm may be faster and simpler
- For some tasks randomness is necessary
SUMMARY

- Randomized algorithm may be faster and simpler
- For some tasks randomness is necessary
- We can go from expectation to probability via Markov’s inequality
SUMMARY

- Randomized algorithm may be faster and simpler
- For some tasks randomness is necessary
- We can go from expectation to probability via Markov’s inequality
- We can amplify probability of success by independent repetitions