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 Ω.

Review of Probability Theory

- Sample Space Ω.
  $\Omega = \{1, 2, 3, 4, 5, 6\};$

Review of Probability Theory

- Sample Space Ω.

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

Review of Probability Theory

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

Review of Probability Theory

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

Review of Probability Theory

- Sample Space Ω.

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

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

Review of Probability Theory

- Sample Space Ω.
  $\Omega = \{1, 2, 3, 4, 5, 6\}$; $\Omega = \{HH, HT, TH, TT\}$
- Event $A \subseteq \Omega$. $A = \{2, 4, 6\}$; $A = \{TT, TH\}$
- Probability measure: $\forall A, \Pr(A) \in [0, 1]$

Review of Probability Theory

- Sample Space Ω.
  $\Omega = \{1, 2, 3, 4, 5, 6\}$; $\Omega = \{HH, HT, TH, TT\}$
- Event $A \subseteq \Omega$. $A = \{2, 4, 6\}$; $A = \{TT, TH\}$
- Probability measure: $\forall A, \Pr(A) \in [0, 1]$
  - $\Pr(\Omega) = 1$

Review of Probability Theory

- Sample Space Ω.
  $\Omega = \{1, 2, 3, 4, 5, 6\}$; $\Omega = \{HH, HT, TH, TT\}$
- 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: $\Pr[\cup_i A_i] = \sum_i \Pr[A_i]$

Review of Probability Theory

- Sample Space Ω.
  $\Omega = \{1, 2, 3, 4, 5, 6\}$; $\Omega = \{HH, HT, TH, TT\}$
- 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: $\Pr[\cup_i A_i] = \sum_i \Pr[A_i]$
- $A_1 = \underline{\{HH\}}$, $A_2 = \underline{\{HT\}}$,
  $\Pr[A_1 \cup A_2] = \underline{\Pr[A_1]} + \underline{\Pr[A_2]}$

Independent Events

- A_1 and A_2 are independent iff $\Pr[\underbrace{A_1 \cap A_2}_{\text{both happen}}] = \Pr[\underline{A_1}] \cdot \Pr[\underline{A_2}]$

Independent Events

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

Independent Events

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

  $\Pr[A_1] = 1/6;$

Independent Events

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

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

(1, 1) (1, 2) (1, 3) ... (6, 6) $\frac{1}{36}$

Independent Events

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

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

$$\Pr[A_1] \cdot \Pr[A_2] = \Pr[A_1 \cap A_2]$$

Independent Events

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

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

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

Independent Events

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

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

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

1 1

$$\Pr[A_1] = 1/6;$$

Independent Events

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

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

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

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

Independent Events

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

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

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

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

$$\Pr[A_1 \cap A_2] \neq \Pr[A_1] \cdot \Pr[A_2] \quad \boxed{1} \quad \boxed{1}$$

Random Variable

- Result of experiment is often not event but number

Random Variable

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

Random Variable

- Result of experiment is often not event but number
- Random variable $X\colon \Omega \to \mathbb{R}$

zeros

- Toss three coins, $X =$ number of heads

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

$$X \qquad 3 \quad 2 \quad 2 \quad 1 \quad 2 \quad 1 \quad 1 \quad 0$$

Random Variable

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

Random Variable

- Result of experiment is often not event but number
- Random variable $X \colon \Omega \to \mathbb{R}$
- Toss three coins, $X =$ number of heads
- Throw two dice:
  $Y =$ sum of numbers, $Z = \max$ of numbers
- Expected value $\mathbb{E}[X] = \sum_i \underline{\Pr[x_i]} \cdot \underline{x_i}$

  $X \in \{x_1, \ldots, x_n\}$

Random Variable

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

$$\mathbb{E}[X] = \underbrace{\boxed{\frac{1}{6}}}_{\Pr[x_1]} \cdot \overbrace{\boxed{1}}^{x_1} + \frac{1}{6} \cdot 2 + \ldots + \frac{1}{6} \cdot 6 = \underline{\underline{3.5}}$$

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

Cloud Sync. Lower Bound

1	0	0	1	1	0	1	1	0	0

Cloud Sync. Lower Bound

changed this bit

1	0	0	1	1	0	1	1	0	0

Cloud Sync. Lower Bound

1	0	0	1	1	0	1	1	0	0

deterministic ≡ non-randomized

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

Cloud Sync. Lower Bound

1	0	0	1	1	0	1	1	0	0

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

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

$n \longrightarrow \log n$

Randomized Algorithm

n-bits

local file

1	0	0	1	1	0	1	1	0	0

1	0	0	1	1	1	1	1	0	0

n-bits

cloud file

Randomized Algorithm

local file

1	0	0	1	1	0	1	1	0	0

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

1	0	0	1	1	1	1	1	0	0

cloud file

Randomized Algorithm

local file

1	0	0	1	1	0	1	1	0	0

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

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

1	0	0	1	1	1	1	1	0	0

cloud file

Randomized Algorithm

local file

1	0	0	1	1	0	1	1	0	0

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

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

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

1	0	0	1	1	1	1	1	0	0

cloud file

Randomized Algorithm

local file

1	0	0	1	1	0	1	1	0	0

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

$$\Big\downarrow {\scriptstyle a \bmod p}$$

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

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

1	0	0	1	1	1	1	1	0	0

cloud file

Randomized Algorithm

local file

1	0	0	1	1	0	1	1	0	0

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

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

$\underline{a \mod p}$

EQ iff

$a = b \mod p$

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

1	0	0	1	1	1	1	1	0	0

cloud file

$\{0, \ldots, p-1\} \subseteq \{0, \ldots, 100n^2 \log n\}$

$\# \text{bits} = \log(100n^2 \log n)$
$= \log 100 + 2 \log n + \log \log n$

Analysis

$a = b$ ~~we~~ we want server to say $a=b$ ~~almost~~ always

$a \neq b$ we want server to say $a=b$ almost never

$a = b$ $\forall p$ $a = b \mod p$

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?

  $a = b \mod p$
- $a - b = 0 \mod p$.

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?
- $a - b = 0 \mod p$.
  $2^n \geq a - b$

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?
- $a - b = 0 \mod p$.
  $2^n \geq a - b = \underbrace{p_1}_{p_i \geq 2} \cdot \underbrace{p_2} \cdots \underbrace{p_k}$

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?
- $a - b = 0 \mod p$.
  $2^n \geq a - b = p_1 \cdot p_2 \cdots p_k \geq 2^k$ $\Rightarrow k \leq n$

$a = b \mod p \Rightarrow (a-b)$ 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?
- $a - b = 0 \mod p$.
  $2^n \geq a - b = p_1 \cdot p_2 \cdots p_k \geq 2^k$

ct

$p \in \{2, 3, --, 100n^2 \log n\}$

- Prime Number Theorem: there are $\approx N/\log N$ prime numbers in the interval $\{2, 3, \ldots, N\}$

$N = 100n^2 \log n$, the # of primes $\gtrsim \underline{\underline{100n^2}}$

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

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

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 $\approx N / \log N$ prime numbers in the interval $\{2, 3, \ldots, N\}$
- With probability $\approx 1 - \frac{1}{100n}$ the output is correct

Linearity of Expectation

r.v.

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

Linearity of Expectation

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

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

Linearity of Expectation

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

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

$$= \sum_i x_i \boxed{\sum_j \Pr[X = x_i \cap Y = y_j]} = \Pr[X = x_i]$$

$$+ \sum_j y_j \boxed{\sum_i \Pr[X = x_i \cap Y = y_j]} = \Pr[Y = y_j]$$

Linearity of Expectation

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

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

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

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

$$= \sum_i x_i \Pr[X = x_i] + \sum_j y_j \cancel{\sum_i} \Pr[Y = y_j]$$

Linearity of Expectation

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

$$
\begin{aligned}
\underline{\mathbb{E}[X + Y]} &= \sum_i i, j \Pr[X = x_i \cap Y = y_j] \cdot (x_i + y_j) \\
&= \sum_i x_i \sum_j \Pr[X = x_i \cap Y = y_j] \\
&\quad + \sum_j y_j \sum_i \Pr[X = x_i \cap Y = y_j] \\
&= \sum_i x_i \Pr[X = x_i] + \sum_j y_j \cancel{\sum_i} \Pr[Y = y_j] \\
&= \underline{\mathbb{E}[X]} + \underline{\mathbb{E}[Y]}
\end{aligned}
$$

Linearity of Expectation

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

Linearity of Expectation

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

11111
11112
11113

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:

$$\begin{aligned}
&\mathbb{E}[X_1 + X_2 + X_3 + X_4 + X_5] \\
&= \mathbb{E}[X_1] + \mathbb{E}[X_2] + \mathbb{E}[X_3] + \mathbb{E}[X_4] + \mathbb{E}[X_5] \\
&= 5 \cdot 3.5 = 17.5
\end{aligned}$$

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

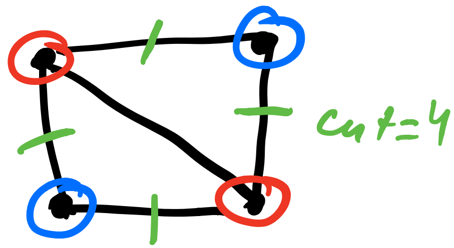
Maximum Cut (Max-CUT)

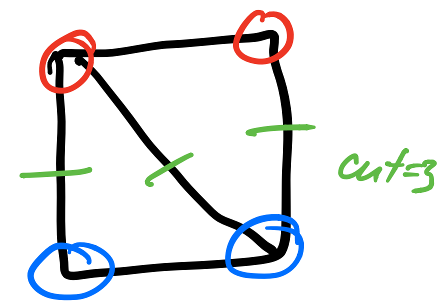
Maximum Cut

- 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: $S \subseteq V, \overline{S} \subseteq V$

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 $\delta(S) = \{(u, v) \in E \colon u \in S, v \in \overline{S}\}$
- 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 $\delta(S) = \{(u, v) \in E \colon u \in S, v \in \overline{S}\}$
- 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 $\delta(S) = \{(u, v) \in E\colon u \in S, v \in \overline{S}\}$
- Max-CUT: $\max_{S \subseteq V} \delta(S)$
- **NP**-hard to solve exactly

Randomized Approximation

- Output a random subset $\boxed{S} \subseteq V$

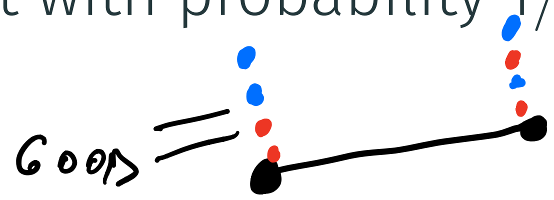
Randomized Approximation

- 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 $1/2$



Analysis

RV

$(u,v) \in E$

- $X_{u,v} = 1$ 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

- $\boxed{X_{u,v} = 1}$ 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 $1/2$
- $\boxed{\mathbb{E}[X_{u,v}] = 1/2}$
- Number of cut edges

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

Linearity of Expectation

- Expected number of cut edges

edges in the graph

$$\mathbb{E}[\sum_{(u,v)\in E} X_{u,v}] = \sum_{(u,v)\in E} \underline{\underline{\mathbb{E}[X_{u,v}]}} = \underline{\underline{|E|}}/2$$

2-APPROXIMATION

- Max-CUT: $\mathrm{OPT} \leq |E|$

2-APPROXIMATION

- Max-CUT: $\mathsf{OPT} \le |E|$
- Our algorithm: $\mathbb{E}[\delta(S)] \ge |E|/2$

2-APPROXIMATION

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

2-APPROXIMATION

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

probability

Markov's inequality

in expectation approximation is pretty good.

Markov's inequality

Theorem

$X \geq 0$

If X is non-negative random variable, then*

$\forall a$

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

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:

$$\Pr[X \geq 2\mathbb{E}[X]] \leq \frac{1}{2}.$$

$a = 5\,E[X]$

$$\Pr[X \geq 5\mathbb{E}[X]] \leq \frac{1}{5}.$$

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%

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

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

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
- $10n \times 0.4 = \boxed{4n}$ 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 $\boxed{\frac{n}{100}}$ tickets win at least $\boxed{500}$ 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

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
- This exceeds the total prize budget of $4n$!

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
- This exceeds the total prize budget of $4n$!
- Contradiction!

Geometric Proof

$$\mathbb{E}f \geq a \times \Pr[f \geq a] \quad \Longleftrightarrow \quad \Pr[f \geq a] \leq \frac{\mathbb{E}[f]}{a}$$

Geometric Proof

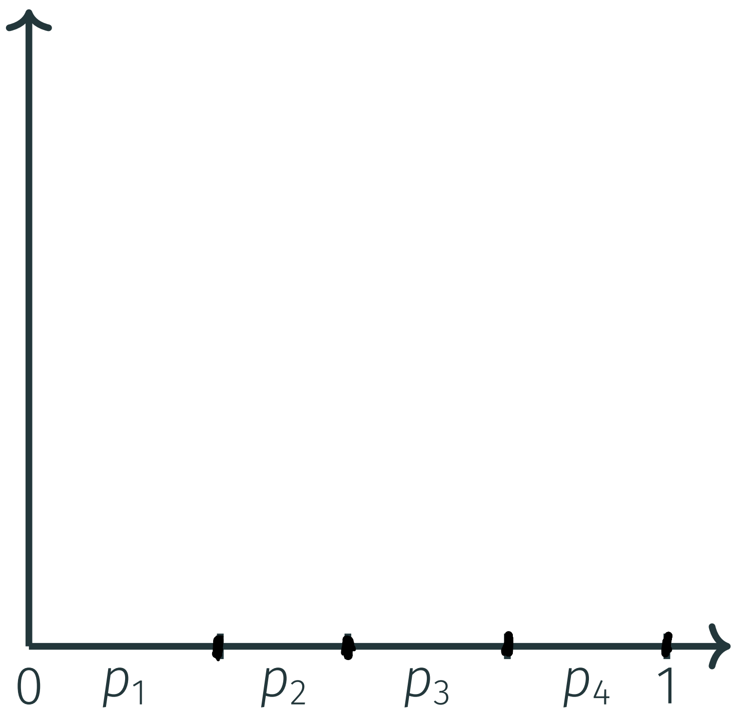
$\mathbb{E}f \geq a \times \Pr[f \geq a]$

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

Geometric Proof

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

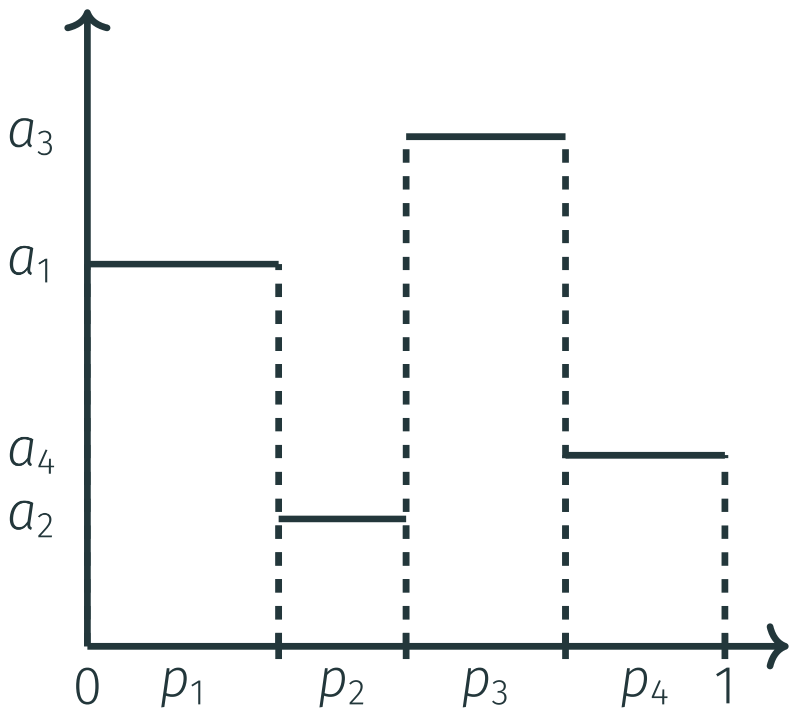
Suppose f takes values a_1, a_2, a_3, a_4 with probabilities p_1, p_2, p_3, p_4



Geometric Proof

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

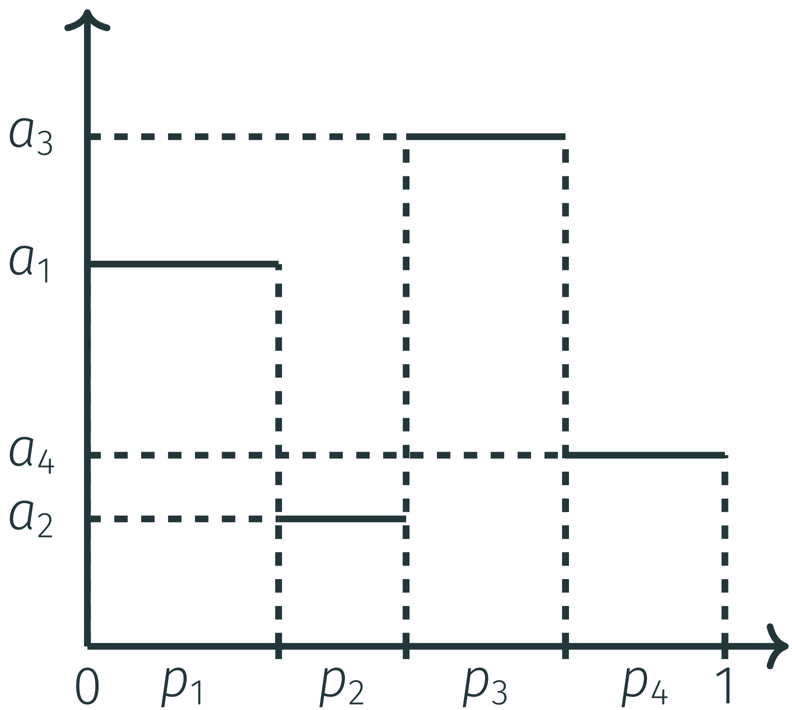
Suppose f takes values a_1, a_2, a_3, a_4 with probabilities p_1, p_2, p_3, p_4



Geometric Proof

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

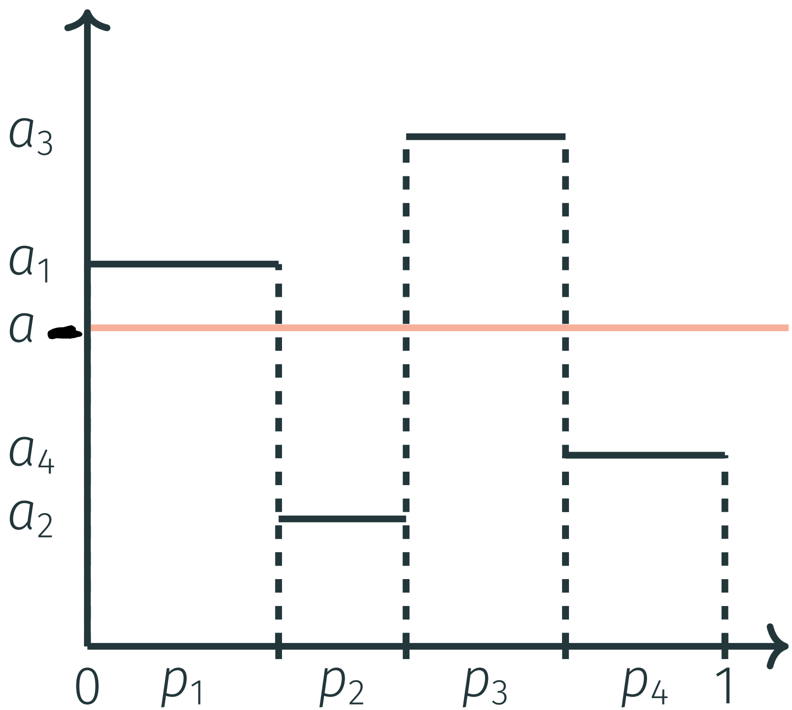
Suppose f takes values a_1, a_2, a_3, a_4 with probabilities p_1, p_2, p_3, p_4



Geometric Proof

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

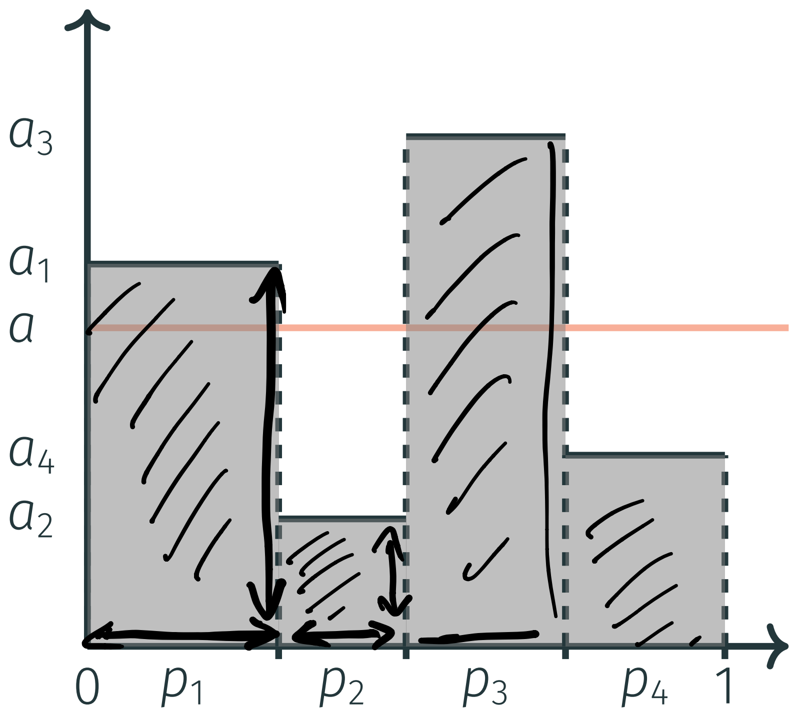
Suppose f takes values a_1, a_2, a_3, a_4 with probabilities p_1, p_2, p_3, p_4



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



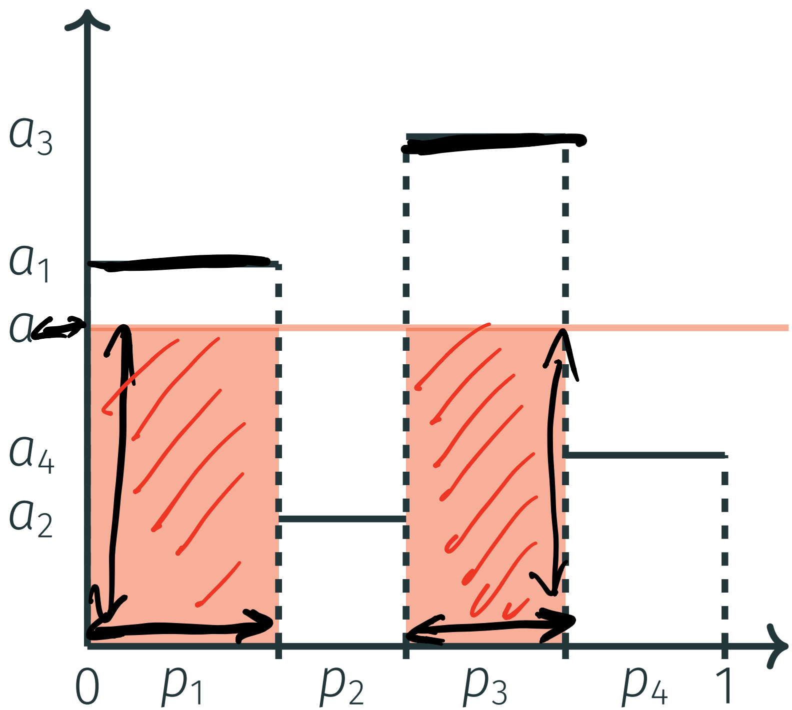
$\mathbb{E}f$ is the area of the gray region

Geometric Proof

area of gray region

$\boxed{\mathbb{E}f} \ge \boxed{\boxed{a} \times \boxed{\Pr[f \ge a]}}$ = area of red regions

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

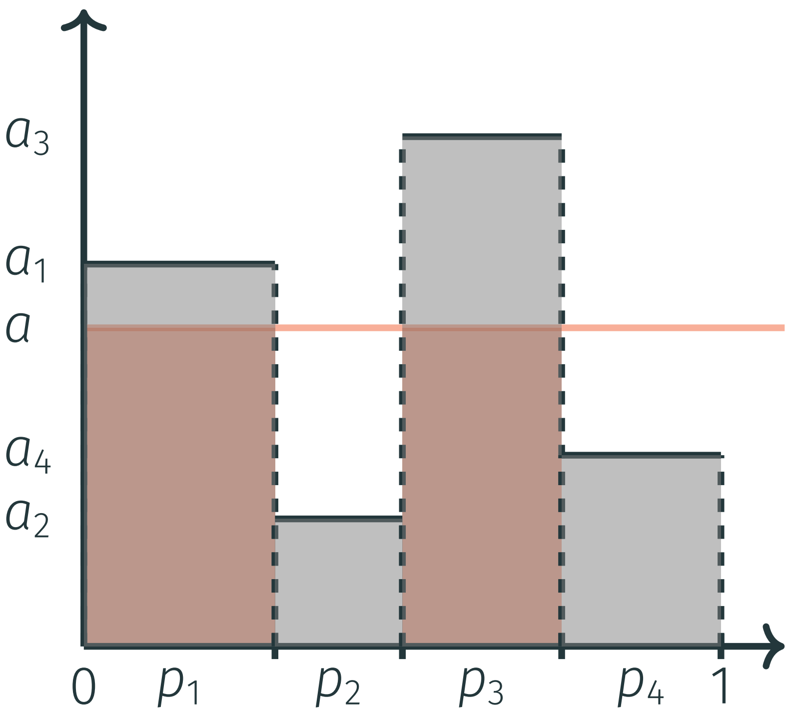
$a \times \Pr[f \ge a]$ is the area of the red region

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

$E[X \geq \boxed{3} \cdot E[X]] \leq \frac{1}{\boxed{3}}$



$\mathbb{E}f$ 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

- $\mathbb{E}[\#\text{cut edges}] = |E|/2 \to \mathbb{E}[\#\text{uncut edges}] = |E|/2$

Approximation Guarantee

$\varepsilon = 0.01$

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

Approximation Guarantee

- $\mathbb{E}[\#\text{cut edges}] = |E|/2 \to \mathbb{E}[\#\text{uncut edges}]$
- $\Pr[\#\underline{\text{uncut}}\text{ edges} \geq \frac{|E|}{2}(1+\varepsilon)] \leq \frac{1}{1+\varepsilon}$
- $\Pr[\#\underline{\text{cut}}\text{ edges} \overset{!!!}{\leq} \frac{|E|}{2}(1-\varepsilon)] \leq \boxed{\frac{1}{1+\varepsilon}} \leq \underline{1-\varepsilon/2}$

Approximation Guarantee

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

#cut edges $\geq \frac{|E|}{2}(1-\varepsilon)$

Approximation Guarantee

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

Probability Amplification

New algorithm

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

Probability Amplification

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

looks at the graph

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

Probability Amplification

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

Probability Amplification

- Pick independent unifrom subsets $S_1, \ldots, S_k \subseteq V$
- Output the subset with maximum cut $\delta(S_i)$
- $\Pr[\max \delta(S_i) \leq \frac{|E|}{2}(1-\varepsilon)] = \Pr[\text{all } \delta(S_i) \leq \frac{|E|}{2}(1-\varepsilon)]$ $\leq \underbrace{(1-\varepsilon/2)}_{0.99}{}^k$

Probability Amplification

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

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

$$e^x \geq 1 + x \qquad x = -\frac{\varepsilon}{2}$$

$$\left(1 - \frac{\varepsilon}{2}\right) \leq e^{-\varepsilon/2} \implies \left(1 - \frac{\varepsilon}{2}\right)^k \leq e^{-\varepsilon k/2}$$

Probability Amplification

$\mathbb{E} \xrightarrow{\text{Markov's in}}$ w small p. output good apx

repeat

w large p output good apx

- Pick independent unifrom 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 $\boxed{k = \frac{2 \ln n + 50}{\varepsilon}}$

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

$\Rightarrow$ outputs $\frac{2}{1-\varepsilon}$-apx w.p. $1 - \frac{1}{10^{10} n}$

Probability Amplification

- Pick independent unifrom 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