Gems of TCS

Randomness

Sasha Golovnev

Novmeber 3, 2025

Deterministic Algorithms

Randomized Algorithms

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 $\delta(S) = \{(u, v) \in E \colon u \in S, v \in \overline{S}\}$

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: $\max_{S \subseteq V} \delta(S)$

Randomized Approximation

- Pick independent uniform subsets $S_1, \ldots, S_k \subseteq V$ for $k = 100 \log n$

Randomized Approximation

- Pick independent uniform subsets $S_1, \dots, S_k \subseteq V$ for $k = 100 \log n$
- Output the subset with maximum cut $\delta(S_i)$

Randomized Approximation

- Pick independent uniform subsets $S_1, \dots, S_k \subseteq V$ for $k = 100 \log n$

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

- Lecture 3: With probability $1 - \frac{1}{10^{10} n}$, we cut at least $|E|/2.04$ edges

BPP

Definition

P—problems that can be solved in polynomial time

BPP

Definition

P—problems that can be solved in polynomial time

Definition

NP—problems whose solution can be verified in polynomial time

BPP

Definition

P—problems that can be solved in polynomial time

Definition

NP—problems whose solution can be verified in polynomial time

Definition

BPP—problems that can be solved in polynomial time using randomness with probability $\geq 2/3$

Cloud Sync

- Synchronize local files to the cloud

Cloud Sync

- Synchronize local files to the cloud

- Has file been changed? File length: n bits

Randomized Algorithm

local file

1	0	0	1	1	0	1	1	0	0

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

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

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

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

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

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

$$a \bmod p \Big\downarrow$$

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

$a \mod p$

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

Analysis

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*!

- Lecture 3: If $a \neq b$, then with probability $\approx 1 - \frac{1}{100n}$ we output NO!

RP

Definition

BPP—problems that can be solved in polynomial time using randomness with probability $\geq 2/3$

RP

Definition

BPP—problems that can be solved in polynomial time using randomness with probability $\geq 2/3$

Definition

RP—problems that can be solved in polynomial time using randomness s.t.

- If correct answer is 1, then algorithm outputs 1 w. p. $\geq 2/3$;
- If correct answer is 0, then algorithm outputs 0 always.

Error Reduction for RP

Error Reduction for BPP

Chernoff Bound

Las Vegas Algorithms

$\mathsf{BPP} \subseteq \mathsf{P}/_{\textsf{POLY}}$