Gems of TCS

Randomness

Sasha Golovnev

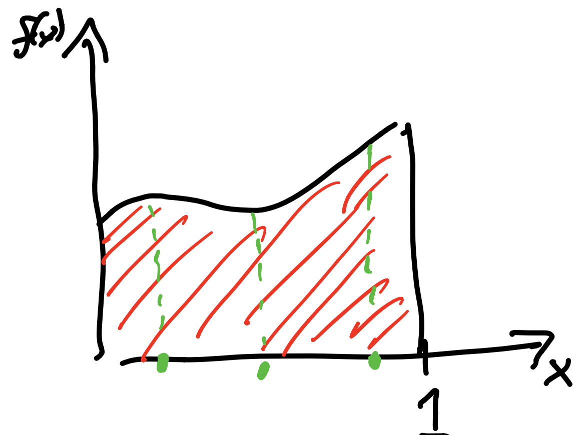
March 25, 2021

My opponent's move

My move

	R	P	S
R	T	L	W
P	W	T	L
S	L	W	T

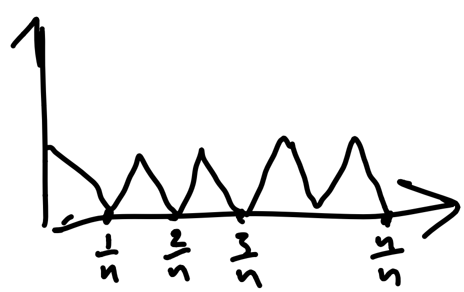
$$\int_0^1 f(x)\,dx \approx \frac{1}{K}\sum_{i=1}^{K} f(x_i)$$



x_i are random points in $[0,1]$

$x_1 = \frac{1}{n}$ $x_2 = \frac{2}{n}$ $x_3 = \frac{3}{n}$ ... $x_n = \frac{n}{n}$

What if $f(x)$



Deterministic Algorithms $\equiv$ non-randomized

Solve problem on most instances,
but may fail on some instances

$\underbrace{RPS}\underbrace{RPS}$

$$\int_0^1 f(x)\,dx \approx \frac{1}{n}\sum_{i=1}^{n} f\left(\frac{i}{n}\right)$$

Randomized Algorithms

Solve problem on all instances,
but fail on each instances
with some small prob. (2^{-n})

RRPSSRRPSS

$$\int_0^1 f(x)\,dx \approx \frac{1}{n}\sum_{i=1}^{n} f(x_i)$$

Maximum Cut

(Lecture 3)

- Undirected graph G, vertices V, edges E

Maximum Cut

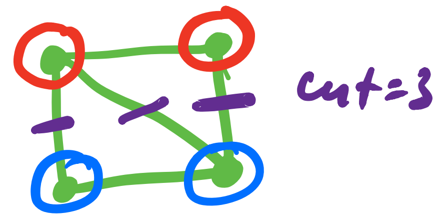
- Undirected graph G, vertices V, edges E
- Bipartition of V that maximizes the number of edges crossing the partition

Maximum Cut

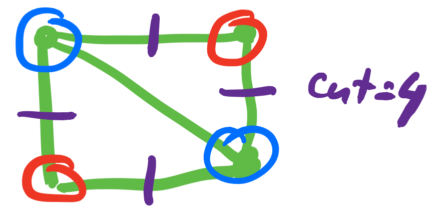
- Undirected graph G, vertices V, edges E
- Bipartition of V that maximizes the number of edges crossing the partition
- Bipartition: $S \subseteq V$, $\overline{S} \subseteq V$

Maximum Cut

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



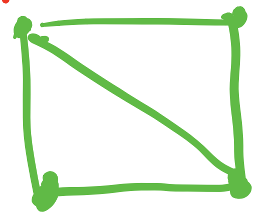
- Bipartition: $S \subseteq V$, $\overline{S} \subseteq V$
- Cut $\delta(S) = \{(u, v) \in E \colon u \in S, v \in \overline{S}\}$



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

assign red or blue color at random



NP-hard to find Maximum Cut

Randomized Approximation

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

Randomized Approximation

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

Randomized Approximation

- Pick independent uniform subsets $\boxed{S_1}, \ldots, \boxed{S_k} \subseteq V$ for $k = 100 \log n$
- Output the subset with maximum cut $\delta(S_i)$
- Lecture 3: With probability $\boxed{1 - \frac{1}{10^{10} n}}$, we cut at least $|E|/2.04$ edges

BPP

Definition

P—problems that can be solved in polynomial time (deterministic = don't use randomness)

BPP

Definition

P—problems that can be solved in polynomial time

Definition

NP—problems whose solution can be verified in polynomial time

BPP

Definition

$\boxed{\textbf{P}}$—problems that can be solved in polynomial time

Definition

NP—problems whose solution can be verified in polynomial time

Definition BPP – Bounded-error Probabilistic Poly-time

$\boxed{\textbf{BPP}}$—problems that can be solved in polynomial time using randomness with probability $\geq \boxed{2/3}$ $\quad \frac{1}{2} + \frac{1}{n^{100}} \quad 1 - \frac{1}{2^n}$

RPS

$\boxed{R\ R\ P\ P\ S\ S}$

P P S S R R

will not solve for strategies of opponent

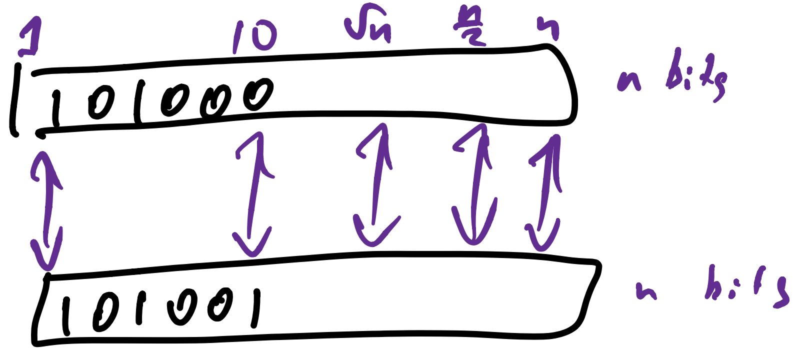
$\underline{P} \leq \underline{BPP}$

Cloud Sync

- Synchronize local files to the cloud

Cloud Sync

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



deterministic : compares all 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

n bits

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

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

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

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

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

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

$$\Big\downarrow\ a \mod p$$

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

$\boxed{a \mod p}$ $\in \{0, \ldots, n^3\}$

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

Files are same

- 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 ith probability $\approx 1 - \frac{1}{100n}$ we output NO!

One-sided error

RP

Definition

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

$\Uparrow$

If correct output 1
alg outputs 1 w.p. $\geq 2/3$

If correct output 1
alg outputs 1 w.p. $2/3$

RP

Definition

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

Definition (RP - randomized Poly-time)

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

- If correct answer is 1, then algorithm outputs 1 w. p. $\geq \boxed{2/3}$; $\frac{1}{n}$ $1 - \frac{1}{2^n}$
- If correct answer is 0, then algorithm outputs 0 always.

$$\boxed{P \subseteq RP \subseteq BPP}$$

Error Reduction for RP

Thm If there is an RP alg

If correct answer is 1, then alg outputs 1 w.p. $\boxed{\frac{1}{n}}$

If correct answer is 0, then alg outputs 0 always

$\Downarrow$

Then there is an RP alg s.t.

If correct answer is 1, then alg outputs 1 w.p. $\boxed{1 - \frac{1}{2^n}}$

If correct answer is 0, then alg outputs 0 always

Thm If there is an RP alg A
If correct answer is 1, then alg outputs 1 w.p. $\boxed{\frac{1}{n}}$
If correct answer is 0, then alg outputs 0 always

$\Downarrow$

Then there is an RP alg A'
If correct answer is 1, then alg outputs 1 w.p. $\boxed{1-\frac{1}{2^n}}$
If correct answer is 0, then alg outputs 0 always

Proof: A':

Run A n^3 times.
If we see at least one output 1, then A' output 1.
Else A' output 0.

If correct answer $=0$, then A' always outputs zero

If correct answer $=1$, what's probability A outputs 0 n^3 times

$$\underbrace{\left(1-\frac{1}{n}\right)\left(1-\frac{1}{n}\right)\cdots\left(1-\frac{1}{n}\right)}_{n^3}$$

$$1+x \le e^x \;\; \forall x \Rightarrow \left(1-\frac{1}{n}\right) < e^{-\frac{1}{n}}$$

$$\left(1-\frac{1}{n}\right)^{n^3} \leq \left(e^{-\frac{1}{n}}\right)^{n^3} = \frac{1}{e^{n^2}} \ll \frac{1}{2^n}$$

$\Rightarrow$ A' will output 1 w.p. $1-\frac{1}{2^n}$

$\square$

Error Reduction for BPP

Useless alg for all problems:
doesn't look input
it outputs 0/1 at random.

solves every problem correctly w.p. $\boxed{\frac{1}{2}}$.

We want (for BPP) prob. success $> \frac{1}{2}$

Thm If $\exists$ BPP alg A that is correct
w.p. $\boxed{\frac{1}{2} + \frac{1}{n}}$, then
$\exists$ BPP alg A' that is correct
w.p. $1 - \frac{1}{2^n}$

A': Run A n^3 times

$$\underbrace{0\,1\,0\,0\,0\,1\,1\,0\,0\,0\,1\,0\,0\,1\,1}_{n^3}$$

A' outputs Majority of these answers

A' will be correct w.p. $1 - \frac{1}{2^n}$

---

wlog correct answer $= 1$.

A solves problem $\boxed{\frac{1}{2} + \frac{1}{n}}$

We expect to see $\boxed{\geq \left(\frac{1}{2} + \frac{1}{n}\right) n^3 \text{ ones}}$

$\leq \left(\frac{1}{2} - \frac{1}{n}\right) n^3$ zeros

Chernoff bound $\Rightarrow$ w.p. $\boxed{1 - \frac{1}{2^n}}$

we'll see more ones than zeros in the output. $\delta = \frac{1}{2^n}$ $\square$

Chernoff Bound

Estimate # vaccinated people in US

Pick n random People

k out of n are vaccinated

$\Rightarrow$ $\frac{k}{n}$ - fraction is vaccinated.

$(\frac{k}{n} \pm \varepsilon)$ - fraction

w.p. $1-\delta$, $(\frac{k}{n} \pm \varepsilon)$ - fraction vaccinated

w.p. $\boxed{0.99}$ $\boxed{(\frac{k}{n} \pm 0.01)}$

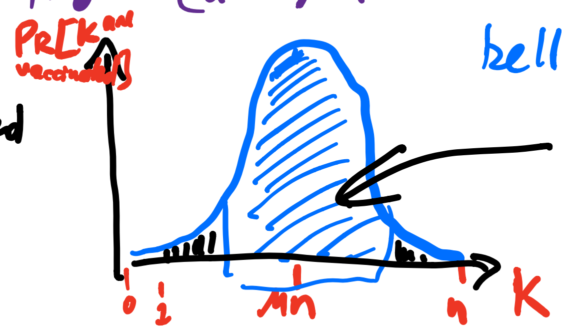
you fix ε, δ.
smallest n?

BPP — Monte Carlo alg

Chernoff bound gives you n s.t.

w.p. $1-\delta$ $(\frac{k}{n} \pm \varepsilon)$ - fraction vaccinated

Say, $\mu \in [0,1]$ - true fraction of vaccinated



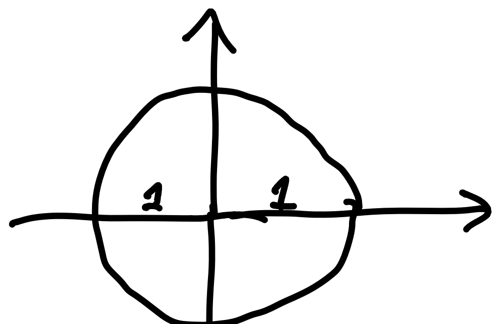
bell curve

w.p. $1-\delta$
$k \in (\mu \pm \varepsilon) n$

Las Vegas Algorithms

Randomized algs that <u>always</u> output correct answers, but their running in expectation is poly

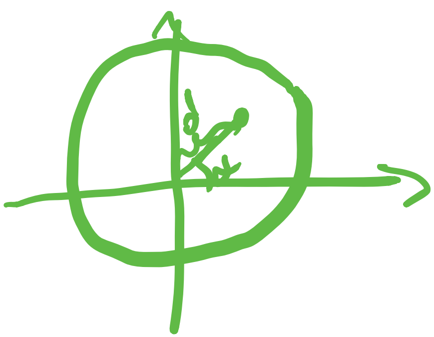
Sample a random point in a circle



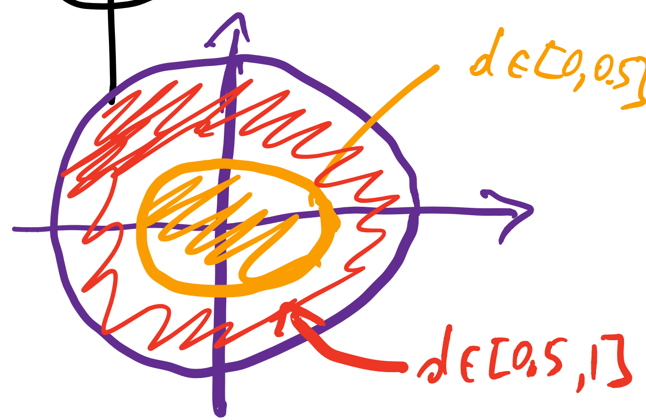
Wrong way:

d ∈ [0,1] random

angle α ∈ [0,2π] random



Why not uniform random?



Las Vegas Alg.

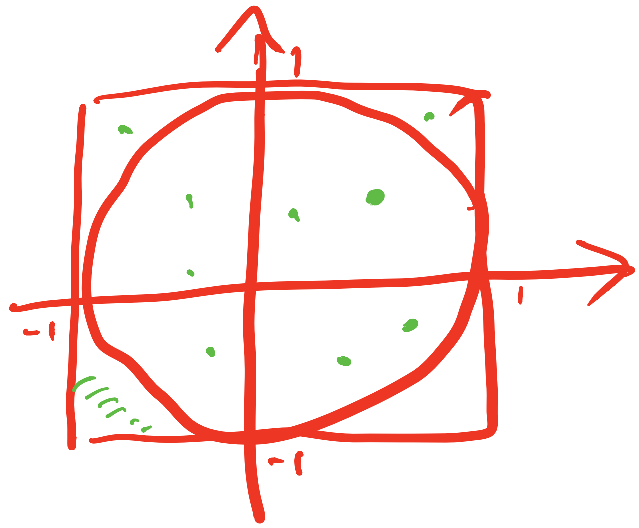
$x \in [-1; 1]$

$Y \in [-1; -1]$

If $x^2+y^2<1$

Then output (x, Y)

Else REPEAT



Area of square $= 4$

Area of ball $= \pi$

w.p. $\pi/4$ each time point in the circle

Exp to sample $\frac{4}{\pi} < 2$ points until we get a point in the circle.

	Correctness	Run-time
Monte Carlo Algs	probabilistic	certain
Las Vegas Algs	certain	probabilistic

If there is a Las Vegas Alg

$\implies \exists$ a Monte Carlo Alg

Complexity ZOO

class of poly-time LAS VEGAS

circuits of poly size

$$P \subseteq ZPP \subseteq RP \subseteq BPP \subseteq P/poly$$

$$RP \subseteq NP$$