Michael Forbes
mforbes@illinois.edu

2018-02-12.1 → 2018-02-14.1
2018-02-14.2 ←
CS579

CS 579: Computational Complexity: Lecture 7

7/9

today: randomness

models of computation

- (deterministic) TMs] realistic
- nondeterministic TMs
- alternation TMs
- oracle TMs] hypothetical

Q: what is the "most" realistic model? what is its power?

randomness - coin toss [essentially unpredictable]
- quantum mechanics [truly random]
- rand() [random enough]

ex: how to estimate election outcome? ~323 million ppl in US
fact: a random sample of (46!) ~235 million voters] lots
ppl will estimate the vote ~126 million actually vote
- to error of 5%
- with probability of 95%

(46!) ← independent of # total voters

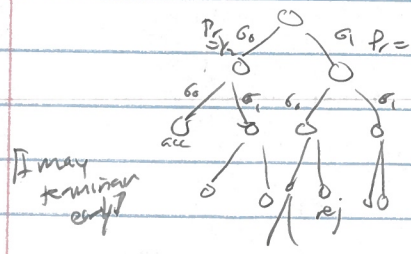
actual polls: - ~1000 for 3% error
- complex random sampling to fix biases

randomness in computation

- in inputs: algorithms work for "most" inputs ← "probabilistic algo" [machine learning]
- in algorithm: algorithm "mostly" works for all inputs ← "randomized algo" [complexity]

def: randomized TM

σ_0, σ_1 transition functions
states Q are all "randomized"



- each state branches w/ σ_0, σ_1 w/p $= 1/2$

$\Rightarrow$ any k-step computation branch occurs w/p $1/2^k$

$$\Pr[M \text{ acc } x] = \sum_{\substack{\text{branches } \ell \\ \text{ending in } q_{acc}}} \Pr[M \text{ on } x \text{ takes } \ell]$$

$$\Pr[\text{rej}] = \sum_{q_{rej}} \text{“}$$

M runs in time $t(n)$ if all branches terminate in $\leq t(|x|)$ steps on M on x

ichael Forbes
ziforbes@illinois.edu

eg: $L \subseteq \{0,1\}^*$ is in NP if

$x \in L \Rightarrow Pr[M \text{ acc } x] > 0$ ∃ accepting string

$x \notin L \Rightarrow$ " $= 0$

def: $L \subseteq \{0,1\}^*$ is in RP coRP BPP [bounded error polytime] P

if randomized poly(n) TM st

completeness: $x \in L \Rightarrow Pr[M \text{ acc } x] \geq 1/2$ [only false negatives] $= 1$ $\geq 2/3$ $= 1$

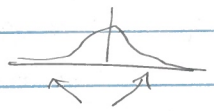
soundness: $x \notin L$ $= 0$ $\leq 1/2$ $\leq 1/3$ $= 0$

one sided error — "randomized polytime" — two sided error — "bounded error probabilistic polytime"

$\Rightarrow P \subseteq RP \subseteq BPP$

Q: robustness? $1/3$ vs $2/3$?

Central limit theorem: $X_1, X_2, \ldots X_n$ are independent identically distributed (iid) random variables $\Rightarrow \frac{X_1 + \cdots + X_n}{n} \xrightarrow{n \to \infty}$ Gaussian distribution



Thm [Chernoff Bound]: [not necessarily]

$X_1, \ldots X_n \in \{0,1\}$ independent random variables

$X = \frac{1}{n} \sum X_i$ [empirical average]

$Pr[|X - \mathbb{E}X| \geq \varepsilon] \leq 2 \exp\left(-\frac{\varepsilon^2 n}{4}\right)$ [in hw]

tail decays fast

lem [BPP amplification] $L \in BPP_\delta$ TM M s.t. $x \in L \Rightarrow Pr[\text{acc}] \geq 1/2 + \delta$; $x \notin L \Rightarrow \leq 1/2 - \delta$

then $BPP_{1/n} = BPP_{1/6} = BPP$ $= BPP_{1/2 - 1/2^n}$

Pf: $\supseteq$: clear

$BPP_{1/n} \subseteq BPP_{1/2 - 1/2^n}$ M for $L \in BPP_\delta$

algo M': on input x

1) run M on x t times

2) if $\geq t/2$ accepts $\Rightarrow$ acc

else $\Rightarrow$ rej

analysis: $X_i := \begin{cases} 1 & i\text{th run of } M \text{ on } x \text{ is correct, i.e. } M(x) = L(x) \\ 0 & \text{else} \end{cases}$

$X = \frac{1}{n} \sum X_i$

M' on x correct if $X > 1/2$

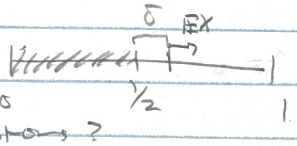
Michael Forbes
mforbes.illinois.edu

$$\Pr\left[X \le \tfrac{1}{2}\right] \le \Pr\left[|X - \underbrace{\mathbb{E}X}_{=\mathbb{E}\left[\frac{1}{n}\sum X_i\right]}| \ge \delta\right] \le 2\exp\left(-\frac{\delta^2 t}{4}\right) \le \frac{1}{2^n}$$

$$= \frac{1}{n}\sum \underbrace{\mathbb{E}[X_i]}_{\ge 1/2 + \delta} \qquad \delta = 1/n$$

[[linearity of expectation]]

$$\ge \tfrac{1}{2} + \delta$$



$\Rightarrow$ choose $t = \Theta(n^3)$

— questions?

Q: are more randomized algos powerful? [[and also easier to find]]

Thm [Solovay Strassen 77]: $PRIMES = \{p : p \in \mathbb{N} \text{ is prime}\} \in coRP \subseteq P$ — poly($\lg p$) time

Thm [Agrawal Kayal Saxena 04]

Rmk: Trial division takes poly(p) steps — $\Theta(\lg p)$ bits

Prop: $PRIMES \in BPP$

Pf: [[two parts]] [[simplest primality algo]]

algo: $k \in \mathbb{N}$ on input n:

1) pick $\alpha_1, \dots, \alpha_k \in \{0, \dots, n-1\}$ — uniformly at random — can simulate w/ rand bits

2) compute $\beta_i = \alpha_i^{\frac{n-1}{2}} \pmod n$ $\in \{0, \dots, n-1\}$

↳ modulo n: $m = qn + r$

↳ via repeated squaring $\alpha^{2^\ell} \bmod n = \left(\alpha^{2^{\ell-1}}\right)^2 \bmod n$

$\Rightarrow$ α^{2^ℓ} in ℓ multiplications mod n ↳ poly($\lg n$) work

$$\frac{n-1}{2} = \sum_{i=0}^{\lg n} b_i 2^\ell$$

α α ↖ $\lg n \cdot$ poly($\lg n$) work

3) if $\beta_1, \dots, \beta_k \notin \{\pm 1\}^k \Rightarrow$ not prime

$\in \{1\}^k \Rightarrow$ "not prime"

$\in \{\pm 1\}^k \setminus \{1\}^k \Rightarrow$ "prime"

[[also is simple, analysis less so]]

analysis: Prop: n prime $\Rightarrow$ acc w/p $1 - 1/2^k$; not prime $\Rightarrow$ w/p $1/2^k$ — [[rand one algo]] $k = 2$ suffices

Pf: Fact [number theory]:

n prime $\Rightarrow$ all $0 < \alpha < n$ $\alpha^{\frac{n-1}{2}} = \pm 1 \bmod n \Rightarrow$ "prime"

and half yield $+1$

" -1

Michael Forbes
miforbes@illinois.edu
2018-02-14.

n non-prime $\Rightarrow$ α, n share common factor $\Rightarrow$ $\alpha^{\frac{n-1}{2}} \neq \pm 1 \bmod n$
$\rightarrow$ "not prime"

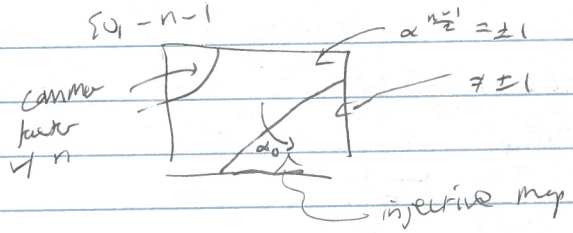
α, n no common factor

Fact: $\exists \alpha_0$ s.t. $\alpha_0^{\frac{n-1}{2}} = -1$
$\Rightarrow \exists \alpha_0$ s.t. $\alpha_0^{\frac{n-1}{2}} \neq \pm 1$

either
- $\alpha^{\frac{n-1}{2}} = 1$ all α $\Rightarrow$ "not prime"
- $\alpha_0^{\frac{n-1}{2}} \neq \pm 1$ some α.

If α, no factor w/ n $\quad \alpha^{\frac{n-1}{2}} = \pm 1 \bmod n$

$\Rightarrow$ $(\alpha_0 \alpha)^{\frac{n-1}{2}} = \underbrace{\alpha_0^{\frac{n-1}{2}}}_{\neq \pm 1} \underbrace{\alpha^{\frac{n-1}{2}}}_{= \pm 1} \neq \pm 1 \bmod n$



$\Rightarrow$ $\geq 1/2$ of α $\alpha^{\frac{n-1}{2}} \neq \pm 1 \Rightarrow$ "not prime"

next time: ps 2 due
randomness vs other resources