Q: prime powers? ✓
is ppsr

Michael Forbes
mforbes@illinois.edu

2019-02-28.4 → 2019-03-05.1
2019-03-05.2 ← CS579

CS 579 Computational Complexity Lecture 15 18

last time: alternation
polynomial hierarchy

today: - NP vs P/poly
- randomness - def
- robustness
- examples

Q: $NP \subseteq P/poly$? [[circ version of P vs NP]] [["most" susceptible to relativization barrier]]

lem: $NP \subseteq P/poly$. $L = \{x \mid \exists y\ V(x,y)=1\} \in NP$. [[replaces '$\exists$' w/ circ]]

$x \xmapsto{f_L}$ { y w/ $V(x,y)=1$ if $x \in L$; $\perp$ if $x \notin L$ }

$\Rightarrow$ f_L has poly-size ckt.

Sketch: ps 1: $P=NP \Rightarrow$ can find satisfying assignments to $\varphi \in SAT$ [[search to decision reduction]]

Thm [Kap Lipton]: $NP \subseteq P/poly \Rightarrow \Pi^2 P \subseteq \Sigma^2 P$ [[extend to any NP problem w/ circ]]

$\equiv coNP^{NP} = NP^{NP} \Rightarrow PH = \Sigma^2 P$ [[last time]]

Pf: $L = \{x \mid \forall y \exists z\ P(x,y,z)=1\} \in \Pi^2 P$

$L' = \{(x,y) \mid \exists z\ P(x,y,z)=1\} \in NP \subseteq P/poly$

$\Rightarrow$ $f_{L'}: (x,y) \mapsto z$ s.t. $\nearrow$ has poly-size ckt C

$\equiv$ all $(x,y) \in L \Rightarrow P(x,y,C(x,y))=1$ ← any ckt $\hat{C}$

$(x,y) \notin L \Rightarrow \forall z\ P(x,y,z)=0 \Rightarrow P(x,y,\hat{C}(x,y))=0$

Clm: $x \in L$ iff $\exists \hat{C}$ [[poly size ckt]] $\forall y\ P(x,y,\hat{C}(x,y))=1$ ← $\Sigma^2 P$

Pf: $x \in L$: take $\hat{C} = C$. $\forall y \exists z\ P(x,y,z)=1$

$\Rightarrow \forall y\ P(x,y,C(x,y))=1$

$\Rightarrow \exists \hat{C} \forall y\ P(x,y,\hat{C}(x,y))=1$

$x \notin L$: $\exists y \forall z\ P(x,y,z)=0$

any $\hat{C}$, $\exists y\ P(x,y,\hat{C}(x,y))=0$

$\forall \hat{C} \exists y\ P(x,y,\hat{C}(x,y))=0$

$\neg \exists \hat{C} \forall y\ P(x,y,\hat{C}(x,y))=1$ ∎

Cor: $PH \neq \Sigma^k P$, any k [[PH infinite]] $\Rightarrow NP \not\subseteq P/poly$.

open: $NP \not\subseteq SIZE(O(n))$

= Questions

Q: what is the "most" realistic TM model?

realistic:
- deterministic
- (co)non-deterministic
- oracle
- w/ advice
- alternating

hypothetical [[useful in understanding problems we don't know how to solve]]

Michael Forbes
miforbes@illinois.edu
2019-03-05.2 ↔ 2019-03-05.1
2019-03-05.3
CS577

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

ex: how to estimate election outcome? ["computational" problem]
~328 million people in US
~235 million eligible voters
~135 million actual voters
} lots of ppl

fact: a truly random sample of 461 voters will estimate the vote
- to error 5%
- w probability 95%
[[real life: - sample size ~1000
- complex random sampling to fix biases]]

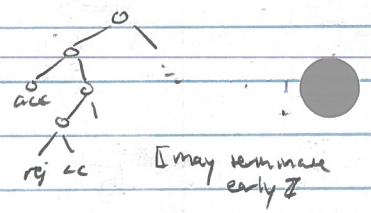
randomness in computation: [[machine learning]]
- inputs: algorithms work for "most" inputs [[worst case input]]
- algorithm: for every input, algorithm works "most" of the time ["probabilistic" "randomized"]

[[Q: how to model?]]

def: a randomized TM M is a TM w/ $\sigma: Q \times \Gamma \to 2^{Q \times \Gamma \times \{L,S,R\}}$ [[just like an NTM]]
w/ $|\sigma(q,\gamma)| = 2$ all q, γ

it computes by taking each transition with probability $1/2$
⇒ length k branch occurs w/p $1/2^k$

$\Pr[M \text{ acc } x] := \sum_{\text{acc branches}} \Pr[M \text{ on } x \text{ takes } \ell] \quad \leftarrow = 1/2^{|\ell|}$



$\Pr[M \text{ rej } x] := \sum_{\text{rej branch}}$ "

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

Rmk. - can consider $|\sigma(q,\gamma)| = 3, \ldots$ [[other models of randomness]] [[must acc or rej w/p ≥ 1]]
↳ doesn't change the complexity classes we'll define [[see book]]

eg $L \subseteq \Sigma^*$ [[$L \in NP$ if $x \in L \Rightarrow \Pr[M \text{ acc } x] > 0$ [[∃ acc string]]
$x \notin L \Rightarrow \Pr[M \text{ acc } x] = 0$ "
[[randomized polytime]] bounded error probabilistic polytime]]

def: $L \in$

	RP	coRP	BPP	P
if randomized polytime TM s.t. $x \in L \Rightarrow \Pr[M \text{ acc } x]$	$\ge 1/2$	$= 1$	$\ge 2/3$	1
$x \notin L \Rightarrow \Pr[M \text{ acc } x]$	$= 0$	$\le 1/2$	$\le 1/3$	0
	one sided error		two sided error	

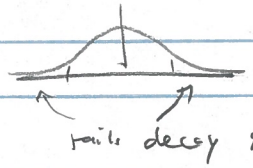
$\Rightarrow P \subseteq RP \subseteq BPP$

= Questions?

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

Central limit thm: $X_1, \ldots X_n$ independent identically distributed (iid) random variables w/ $\mathbb{E}[X_i] = 0$

$\Rightarrow \frac{X_1 + \cdots + X_n}{\sqrt{n}} \to$ Gaussian Distribution $n \to \infty$



Michael Forbes
mforbes@illinois.edu

Thm [Chernoff Bound] $X_1, \dots, X_n \in [0,1]$ independent [not necessarily iid] random variables. $X := \frac{\sum X_i}{n}$ [empirical average]

$$\Pr\left[|X - \underbrace{\mathbb{E}X}_{= \frac{\sum \mathbb{E}X_i}{n}}| \geq \varepsilon \right] \leq 2 e^{-\varepsilon^2 n/4}$$ [in practice] ← decays fast

Lem (BPP amplification): $L \in BPP_\delta$ if poly-time randomized TM M

$x \in L \Rightarrow \Pr[M \text{ acc } x] \geq \frac{1}{2} + \delta \geq 1 - \frac{1}{2^n}$

$x \notin \Rightarrow \leq \frac{1}{2} - \delta \leq \frac{1}{2^n}$

Then $BPP_{1/n} = \underbrace{BPP_{1/6}}_{= BPP} = BPP_{\frac{1}{2} - \frac{1}{2^n}}$

Pf: Suffices to show $BPP_{1/n} \subseteq BPP_{\frac{1}{2} - \frac{1}{2^n}}$

$L \in BPP_\delta$ w/ TM M

M' = "on input x:

1) run M on x t times ← fresh randomness

2) if $\geq t/2$ accepts ⇒ acc

else ⇒ rej

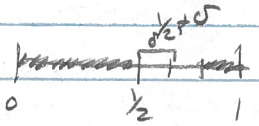
analysis: $X_i = \begin{cases} 1 & i\text{th run of } M \text{ on } x \text{ is correct, i.e. } M(x) = L(x) \\ 0 & \text{else} \end{cases}$

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

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

$$\Pr[M' \text{ errs}] \leq \Pr[X \leq 1/2] \leq \Pr[|X - \underbrace{\mathbb{E}[X]}_{= \frac{1}{t}\sum \mathbb{E}[X_i]}| \geq \delta] \leq 2\exp\left(-\frac{\delta^2 t}{4}\right)$$ [linearity of expectation]

$\geq 1/2 + \delta$



want $\leq \frac{1}{2^t} \leq \delta = 1/n$

⇒ take $t = \Theta(n^3)$ ∎

Rmk: RP, BPP capture "realistic" randomized computers closely.

Question

Q: are randomized algs more powerful than deterministic?

Thm [Solovay-Strassen 77]: $PRIMES = \{p : p \in \mathbb{N} \text{ is prime}\} \in co\,RP$ ← poly($\lg p$) time

Thm [Agrawal-Kayal-Saxena 04]: $\in P$

Rmk: obvious alg takes poly(p) steps [trial division].

Michael Forbes
MiForbes@illinois.edu
2019-03-05, 4 ← 2019-03-05.3
cs579 → 2019-03-07.1

Prop: PRIMES $\in$ BPP

Pf: "on input n: parameter k

can approximate w/ random bits

poly 0) deal w/ even n.
poly 1) pick $\alpha_1, \dots, \alpha_k \in \{0, \dots, n-1\}$ uniformly at random
poly 2) compute $\beta_i = \alpha_i^{\frac{n-1}{2}} \bmod n$
poly 3) if $(\beta_1, \dots, \beta_k) \in \{\pm 1\}^k \Rightarrow$ "not prime"
$\in \{1\}^k \Rightarrow$ "not prime"
$\in \{\pm 1\}^k \setminus \{1\}^k \Rightarrow$ "prime"

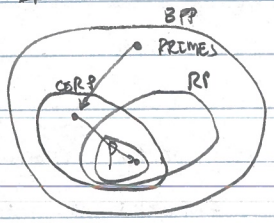
[Exposed by, psd.]

Complexity:

correctness: Prop. n prime $\Rightarrow$ acc $\geq 1 - 1/2^k$
n not prime $\Rightarrow$ $\leq 1/2^k$
[rand. or also]
$k=2$ suffices for BPP

Pf: Number theory [see Sipser]

Rmk:



next time: more randomness