Michael Forbes
miforbes@illinois.edu

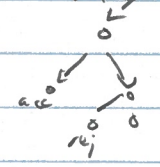
2019-03-05.4
2019-03-07.2 ⇄ 2019-03-07.1
CS579

CS579 Computational Complexity: Lecture 16 14 24

today: BPP vs DTIME
nonuniformity
alternation

Last time:

randomized TM $\Pr=1/2$ $\Pr=1/2$



	RP	coRP	NP
$L \in BPP$: $x \in L \Rightarrow \Pr_r[M \text{ acc } x] \geq 2/3$	$\geq 1/2$	$=1$	>0
$\rightsquigarrow$ rand poly time TM M $\notin$	$=0$	$\leq 1/2$	$=0$

$\leq 1/3$

$PRIMES = \{p : p \in \mathbb{N} \text{ prime}\} \in BPP$ ← saw algo, no analysis

$\in coRP \in BPP$ ← Solovay Strassen 77, Miller, Rabin

$\in P$ ← Agrawal Kayal Saxena 04 [breakthrough]

Q: what is power of randomized algos?

A: next time [beyond this course]: rand algos w/ no known matching det. algo [$P \neq BPP$?]

A: thm [Hardness vs Randomness] $L \in TIME(2^{O(n)})$ [eg SAT] requires $2^{\Omega(n)}$-size ckts [$\leq$ max size] $\Rightarrow P = BPP$ [plausible]

[nonuniformity doesn't help] [plausible]

Q: unconditional statements? [like NP verification]

goal: $BPP \subseteq PSPACE$

lem: $L \in BPP$ iff TM M st $M(x,r)$ runs in $poly(|x|)$ steps [only needs poly many rand bits]

$x \in L \Rightarrow \Pr_{r \in \{0,1\}^{poly(|x|)}}[M(x,r) \text{ acc}] \geq 2/3$

$\notin \leq 1/3$

Sketch: $\Leftarrow$: toss coins to get r, then run $M(x,r)$

$\Rightarrow$: $L \in BPP$ yields rand TM M running time $t(n)$

M' = "on input x, r:

1) simulate M on x, using r as source of randomness

succeeds if $|r| \geq t(n)$

Prop: L has rand algo time t, using m random bits $\Rightarrow m \leq t$

$\Rightarrow L$ has det. algo. time $poly(t, 2^m)$, space $poly(t, m)$

Pf: $M(x,r)$ algo for L

$r \in \{0,1\}^n \hookrightarrow \in \{0,1\}^m$

$x \in L \Rightarrow \Pr_{r \in \{0,1\}^m}[M(x,r) = 1] \geq 2/3$

$\notin \leq 1/3$

idea: compute ⟶ and decide

Michael Forbes
mforbes@illinois.edu
2019-03-07 ← 2019-03-07.1
2019-03-07.2 → 2019-03-07.3
cs579

algo compute $p = \frac{1}{2^m} \sum_{r \in \{0,1\}^m} M(x,r)$

$p \geq 2/3 \Rightarrow$ "$x \in L$"

$\leq 1/3$ " $\notin$ "

correctness: clear

complexity: poly$(t, 2^m)$ time

poly(t, m) space ∎

Cor: BPP ⊆ PSPACE ⊆ EXP

goal: BPP ⊆ P/poly ‖ P/poly ≟ P for "natural" problems like SAT ‖

Amplification Prop: $L \in BPP_\delta$ if $x \in L \Rightarrow \Pr[M \text{ acc}] \geq 1/2 + \delta \geq 1 - 1/2 - \frac{1}{2^n}$

$x \notin L \Rightarrow \Pr[M \text{ acc}] \leq 1/2 - \delta \leq 1/2 - 1/2^n$

then $BPP_{1/2^n} = BPP = BPP_{1/2 - \frac{1}{2^{n+1}}}$ ‖ run BPP$_\delta$ algo many times, take majority vote ‖

equiv: $L \in BPP \Rightarrow$ L rand poly-time algo $M(x,r)$ w/ error prob $\leq 1/2^n$ · $\frac{1}{2} \leq \frac{1}{2^n}$ (small!)

Pf: $L \in BPP \Rightarrow \exists r_0 \; \forall x \in \{0,1\}^n \quad x \in L \Rightarrow M(x,r_0) = 1$ (non-uniform)

$x \notin L \Rightarrow = 0$ (deterministic)

Pf: consider random r ‖ probabilistic method ‖

any x: $\Pr_r[L(x) \neq M(x,r)] < 2^{-n}$ ‖ indicator function ‖

$\Pr_r[\exists x \in \{0,1\}^n \; L(x) \neq M(x,r)] \leq 2^n \max_x \Pr_r[L(x) \neq M(x,r)]$ (union bound; $< 2^{-n}$)

$< 2^n \cdot 2^{-n} = 1$

$\Rightarrow \Pr_r[\forall x \; L(x) = M(x,r)] > 0$ ← what we want

$\Rightarrow r_0$ exists ∎

Cor: BPP ∈ P/poly

Pf: each input size n, give advice string r_n, run $M(x, r_{|x|})$ ← poly$|x|$ time; ← poly$|x|$ long

↳ works for all inputs length n.

= Questions

$M(x,r)$ rand poly-time TM: $x \in L \Rightarrow \Pr_r[M(x,r)=1] \geq 2/3 \geq 1/2 > 0$

$x \notin L \Rightarrow \leq 1/3 = 0 = 0$

BPP RP NP

$\Rightarrow$ RP ⊆ NP

Q: BPP vs NP?

ps: NP ⊆ BPP $\Rightarrow$ NP = RP

open: BPP ⊆ NP?

Michael Forbes
MiForbes@illinois.edu

2019-03-07.2 → 2019-03-07.3
2019-03-07.4 ←
CS 579

Prop: $NP \subseteq BPP \subseteq P/poly \Rightarrow \Sigma_2 P = \Pi_2 P$ [using Karp Lipton]
[get something more direct?]

Thm [Sipser Gacs Lautemann 83]: $BPP \subseteq \Sigma_2 P$

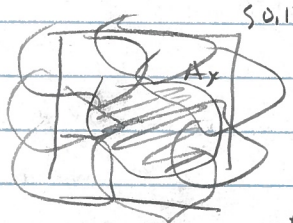
Cor: $P = NP \Rightarrow P = NP = NP^{NP} = NP^{NP^{NP}} = \cdots \Rightarrow P = BPP$. [so if SAT easy $\Rightarrow P = BPP$; if SAT hard $\Rightarrow P = BPP$]
$\Sigma_2 P$ $\Sigma_3 P$

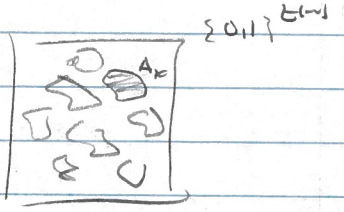
Pf: $M(x,r)$ BPP algo w/ error prob $\leq 2^{-n}$ time $t(n)$

want: $P(x,y,z)$ deterministic poly$|x|$ time

$x \in L$ iff $\exists y \forall z \; P(x,y,z) = 1$
(poly$|x|$ size)

idea: probabilistic method via "randomized covering argument"

$x \in L$: 

$x \notin L$: 

$A_x = \{ r \in \{0,1\}^{t(n)} : M(x,r) = 1 \}$

random translations of A_x cover $\{0,1\}^{t(n)}$ [they don't]

$s \in \{0,1\}^{t(n)}$ $A_x \oplus s = \{ r \oplus s, r \in A_x \}$ [shift A_x around]
(XOR, addition mod 2)

$\Rightarrow |A_x \oplus s| = |A_x|$ (poly(n) bits)

Clm: $x \in L \Rightarrow \underbrace{\exists s_1, \ldots, s_{t(n)} \in \{0,1\}^{t(n)} \; \forall r \in \{0,1\}^{t(n)}}_{\Sigma_2 P} \; r \in \bigcup_{i=1}^{t(n)} (A_x \oplus s_i)$

$\equiv \underbrace{\bigvee_{i=1}^{t(n)} M(x, r \oplus s_i)}_{\in P}$

$x \notin L \Rightarrow$ not

$\equiv \forall s_1, \ldots, s_{t(n)} \; \exists r \; r \notin \bigcup_{i=1}^{t(n)} \cdots$

Pf: $x \in L$: idea probabilistic method

$\Pr_{s_1,\ldots,s_t}[\exists r : r \notin \bigcup (A_x \oplus s_i)] \leq 2^t \max_r \Pr_{s_1,\ldots,s_t}[r \notin \bigcup (A_x \oplus s_i)]$
[bad event]

$= \Pr_{s_1,\ldots,s_t}[\bigwedge_i \underbrace{r \notin (A_x \oplus s_i)}_{\equiv s_i \oplus r \notin A_x}]$

[indep]

$= (\underbrace{\Pr_s[s \oplus r \notin A_x]}_{\leq 2^{-n}})^t$

$\leq 2^{-nt}$

$< 2^t (2^{-n})^t \leq 1$ ($n \geq 1$)

$\Rightarrow \Pr_{s_1,\ldots,s_t}[\forall r : r \in \bigcup_i (A_x \oplus s_i)] > 0$

$\Rightarrow \exists s_1, \ldots, s_t \; \forall r \; r \in \bigcup_i (A_x \oplus s_i)$

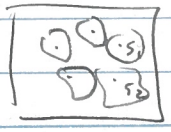
Michael Forbes
m.forbes@illinois.edu
2019-03-07.4 ← 2019-03-07.3 → 2019-03-12.1
CS 574

$x \notin L$: idea: volume argument

want: all $s_1, \dots, s_t$ $\exists r$ $r \notin \bigcup_i (A_x \oplus s_i)$

fix $s_1, \dots, s_t$ $\Pr_r[r \in \bigcup_{i=1}^t (A_x \oplus s_i)] \le t \cdot \underbrace{\Pr_r[r \in A_x \oplus s]}_{< 2^{-n}}$ ← union bound

$< \frac{t}{2^n} < 1$ ← larger n can fix so t all n w/ more careful parameters



$\Rightarrow \Pr_r[r \notin \bigcup (A_x \oplus s_i)] > 0$

$\Rightarrow$ r exists

$\Rightarrow \forall s_1, \dots, s_t \; \exists r \; r \notin \bigcup (A_x \oplus s_i)$

$\equiv \neg \exists s_1, \dots, s_t \; \forall r \; r \in \bigcup (A_x \oplus s_i)$

digest: $x \in L \Rightarrow A_x$ large $\Rightarrow$ exist small # shifts cover $[q]^t$ ($\exists$ small # shifts, $\forall$ cover $[q]^t$)

$x \notin$ small; all ($\forall$) small # shifts; exist ($\exists$) cover $[q]^t$

today: - BPP $\subseteq$ PSPACE $\subseteq$ EXP — ∥ enumeration ∥
- BPP $\subseteq$ P/poly — ∥ non-uniformity ∥
- BPP $\subseteq \Sigma^2 P \subseteq$ PSPACE — ∥ alternation ∥

next time: randomized algs