Michael Forbes
miforbes@illinois.edu

2019-02-21 → 2019-02-26.1
2019-02-26.2 ← cs579

Computational Complexity

cs579 lecture 13

admin: ps2 back [ps1 also] average 55

ps3 due Thurs

last lectures:

relativization

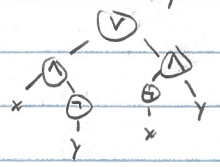
thm: any proof that P=NP or P≠NP must "notice" a lack of oracle

[how do we do this?]

circuits

$$f(x,y) = \begin{cases} 1 & x \neq y \\ 0 & x = y \end{cases} = x \oplus y \quad [\text{parity}]$$

=



[finite combinatorial object]

$$P/poly = \{ L : size(L|_{\{0,1\}^n}) \in poly(n) \}$$

[indicator function]

Q: can combinatorics prove $NP \not\subseteq P/poly \Rightarrow P \neq NP$?

$P \subseteq P/poly$ [Cook-Levin]

A: maybe yes! some combinatorial techniques "do not" support oracles [we'll see some]

A: maybe not?

P/poly contains undecidable languages [maybe P/poly is too strong?]

all functions $f: \{0,1\}^n \to \{0,1\}$ have $O(n 2^n)$ size ckts

[all langs]

$ALL = SIZE(O(n 2^n))$ [is weird]

but: $TIME(2^{2^n}) \not\subseteq TIME(n 2^n)$ [time hierarchy] [ckts too strong?]

today: - existence of hard functions

Q: are there languages which require large ckts?

$ALL = SIZE(n 2^n)$

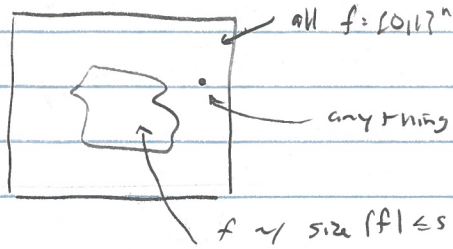
$\stackrel{?}{=} SIZE(poly(n))$?

[close ∀ vs ∃ in $n 2^n$]

thm [Shannon, Lupanov]: $\exists f: \{0,1\}^n \to \{0,1\}$ requires size $\Omega(2^n/n)$

Pf: idea: diagonalization? [naked for TMs]

combinatorics → non constructive counting argument



Michael Forbes
MForbes@illinois.edu
2019-02-26.2 ← → 2019-02-26.3
CS 579

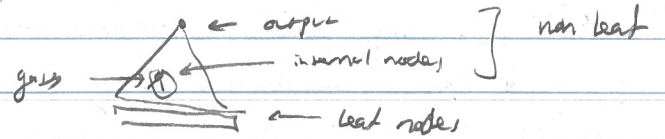
$\#\{f : \{0,1\}^n \to \{0,1\}\} = 2^{2^n}$

$\#\{f : \{0,1\}^n \to \{0,1\} \text{ s.t. } \text{size}(f) \le s\} \le ???$

$\le$ # ckts of size s

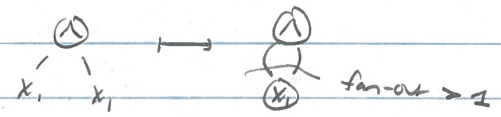
Clm: $s \ge \Omega(n)$. $\#\{\text{ckts size} \le s\} \le s^{O(s)}$

Pf: size s ckt =



s nodes. leaf nodes: wlog n leaf nodes labelled $x_1, \dots, x_n$

eg



non leaf - gate type = AND, OR, NOT (3 choices)

- ≤ 2 children (NOT gates have 1) $\} \le 5^2$ choices

$\le$

$\Rightarrow \underbrace{(35^2)^{s-n}}_{\le 35^2 \text{ choices each}}$ ckts $\le s^{O(s)}$ as $s \ge \Omega(n)$ ☒

If $s^{O(s)} < 2^{2^n} \Rightarrow \exists f$ not size s

[# size $\le s$] [# f]

take $s = \varepsilon \cdot \frac{2^n}{n}$

$s^{O(s)} = \underbrace{\left(\frac{\varepsilon 2^n}{n}\right)^{O(\varepsilon 2^n/n)}}_{\le 2^n} \le 2^{O(n \cdot \varepsilon 2^n/n)} = 2^{O(\varepsilon 2^n)} < 2^{2^n}$

$\uparrow \varepsilon = \Theta(1)$, $\varepsilon \ll 1$

$\Rightarrow \exists f$ non size $\varepsilon 2^n/n$ for $\varepsilon \ll 1$.

equivalently size $\Omega(2^n/n)$ ☒

Rmk: - $\Rightarrow$ SIZE(n^2) ("ALL") $\not\subseteq$ P/poly $\Rightarrow$ NP $\not\subseteq$ P/poly "is possible" (non-constructive existence)

- can view this as probabilistic method

$\Pr_{f:\{0,1\}^n \to \{0,1\}}[f \text{ has size}(f) \le s] \le \frac{s^{O(s)}}{2^{2^n}}$ [equiv]

$\le \frac{2^{O(\varepsilon 2^n)}}{2^{2^n}}$ $s = \varepsilon 2^n/n$

$\le \frac{1}{2^{\Omega(2^n)}}$ $\varepsilon \ll 1$

$\le \frac{1}{100}$ $n \gg 1$

Michael Forbes
mforbes@illinois.edu

$\Rightarrow$ 99% of functions require $\Omega(2^n/n)$ size ckts

= Questions

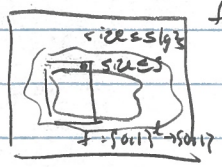
Q: $SIZE(n^2)$ vs $SIZE(n^3)$? [hierarchy thms]

thm [circuit size hierarchy]: $s: \mathbb{N} \to \mathbb{N}$ $\quad 2(n) \le s(n) \le O(2^n/n)$

$\to SIZE(s(n)) \subsetneq SIZE(s(n) \cdot \lg^2 s(n))$

Pf: parameter $\ell \in [0, n]$

idea: $f: \{0,1\}^n \to \{0,1\}$



$\#\{ f: \{0,1\}^n \to \{0,1\} \text{ w/ ckt size} \le s \} \le s^{O(s)}$

$\#\{ f: \{0,1\}^n \to \{0,1\} \text{ that only depend on first } \ell \text{ bits} \} \le 2^{2^\ell}$

If $f(x_1, \dots, x_n) = g(x_1, \dots, x_\ell) \to$ has circuit size $O(\ell \cdot 2^\ell)$

$g: \{0,1\}^\ell \to \{0,1\}$

pick smallest ℓ s.t. $s^{O(s)} < 2^{2^\ell}$

is $\ell = \lg(c \cdot s \lg s) = \Theta(\lg s)$

≥ 1 if $s \ge \Omega(n)$

$\le n$ if $s \le O(2^n/n)$

$\Rightarrow 2^\ell = c \cdot s \lg s$

$\Rightarrow 2^{2^\ell} = 2^{c \cdot s \lg s} = s^{c \cdot s} > s^{O(s)}$ if $c >> 1$

$\Rightarrow SIZE(s(n)) \subsetneq SIZE(\ell \cdot 2^\ell) = SIZE(s \lg^2 s)$

$\ell \cdot 2^\ell = \lg s \cdot O(s \lg s) = O(s \lg^2 s)$ ∎

Rmk: - "$\subsetneq$" is "diagonalization" [in some sense]

- "$\subsetneq$" is "padding" [proof]

- can sharpen, as $ALL = SIZE(2^n/n)$

= Questions?

Q: evidence that $NP \not\subseteq P/poly$?

A: open: prove $NP \not\subseteq SIZE(O(n))$ [few unconditional results]

↑ trivial lb to read all inputs!

A: open. $NP \subseteq P/poly \overset{?}{\Rightarrow} P = NP$ [collapse]

$\overset{?}{\Rightarrow} NP = coNP$ [surprising]

$\overset{?}{\Rightarrow} P^A = NP^A$ [might be interesting, depends on A]

Michael Forbes
miforbes@illinois.edu
2019-02-26.4 ← 2019-02-25.5
CS579 → 2019-02-28.1

- alternation

next lectures - $NP \subset P/poly \Rightarrow NP^{NP} = coNP^A$