- also for balancing
- fix ps6.1 k(c) vs 1(a)
- clarity +1 leaf
- OR/4

2019-04-11.4 → 2019-04-16.1
2019-04-16.2 ←

Michael Forbes
miforbes@illinois.edu
2019-04-16.1
CS 579

+10 min
13 18

CS 579 Computational Complexity : Lecture 25

last week: unconditional results in
- query complexity
- communication complexity

this week:
- circuit complexity

[- weak computational models
- resolved P vs NP
- still had open questions
- unclear if really giving insight on Turing machine]
[more like computation]

today:
- intro
- balancing formulas
- random restrictions

⟹ **intro**

goal: $NP \not\subseteq P \Leftarrow NP \not\subseteq P/poly \equiv SAT$ requires $n^{\omega(1)}$-size ckts (> circuits)

rmk: avoids TMs, "only" combinatorics [pros and cons]

thm [Karp-Lipton]: $NP \subseteq P/poly \Rightarrow PH = \Sigma_2 P = NP^{NP}$ (infinite) [hence "reasonable"] (- it's hard)

fact: $EXP^{NP} \not\subseteq P/poly$ [big gap vs NP^{NP}]

similar to ps3: any k $PH \not\subseteq SIZE(n^k)$

open: $NEXP \overset{?}{\not\subseteq} P/poly$

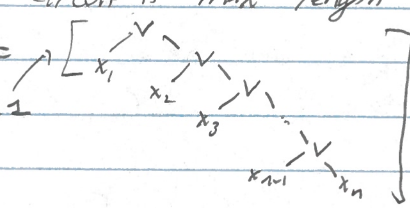
thm [...]: $\underbrace{(1+\Omega(1))\cdot n}$ ckt size lbs for "explicit" functions [best known] ($\in P, NP$)
↳ sensitive to gate set, eg $\{AND, \neg\}$ vs $\{NAND\}$

open: $\omega(n)$ ckt size lbs for "explicit" function

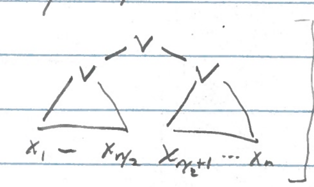
goal: ↳ for "interesting" restricted ckt classes [how to restrict?]

def. depth of a circuit is max length of input-output path

eg. $OR(x_1, \dots, x_n) =$



depth 1 ... depth n vs



depth $O(\lg n)$

def: (non-uniform) $NC^i = \{$ family $f_n : \{0,1\}^n \to \{0,1\}$ st

[can make uniform defn]

fan-in 2 ckt C_n computing f_n

$size(C_n) \le poly(n)$

$depth(C_n) \le O(\lg^i n)$

fact: "all" linear algebra is computable in (randomized, uniform) NC^2 [so NC^2 is nontrivial]

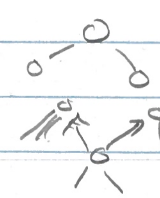
def. a formula is a circuit w/ fan-out 1 eg.

fact: fan-in 2 circuit depth d

$\Rightarrow$ formula size $2^{O(d)}$

$\Rightarrow$ $\le 2^{O(d)}$ (leaves)

not.



[reusing computation]

$\Rightarrow d \ge \Omega(\lg n)$ if function depends on all variables [NC^1 is first nontrivial case]

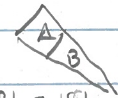
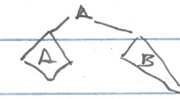
Cor. $NC^1 \subseteq \{ poly(n)$ size formulas $\}$

Michael Forbes
mforbes@illinois.edu
2019-04-16.2 ← 2019-04-16.1
→ 2019-04-16.3
cs579

[converse]

$\Rightarrow$ poly(s) size

Prop: f has size s formula $\Rightarrow$ f has depth $O(\lg s)$ formula

idea - balance a formula $C =$  $\longmapsto$ 

[I need more refined notion of size] $|A|, |B| \approx \frac{|C|}{2}$ $D(s) \le D(\approx s/2) + \Theta(1) = O(\lg s)$

def: the *size* of a formula is the number of leaves

ps: in formula where all gates have ≥ 2 children, # gates, # edges $\le O(\#\text{ leaves})$

and any formula size s is equiv to formula size $s' \le s$ w/ ie all negations are at the bottom $\neg(x \vee y) \equiv \neg x \wedge \neg y$

put negation into leaf [not "gate"]

lem: F fan-in 2 formula w/ $L(F)$ leaves, all gates w/ ≥ 2 children
$\Rightarrow$ exists gate v in F w/ subformula F_v rooted at v
w/ $L(F_v) \le 2/3 \cdot L(F)$, $> 1/3 \cdot L(F)$

Pf: idea: traverse down tree

key fact: $L(u \text{ op } w) = L(u) + L(w)$ each >0

$\vee$ $2/3\, L(F)$ $\Rightarrow$ ≥ 1 of these is $\ge \frac{1}{2} \cdot (> 2/3\, L(F)) > 1/3\, L(F)$

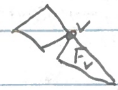
follow the child

stop when $L(v) \le 2/3\, L(F)$, $> 1/3\, L(F)$ ← by previous step ☒

Pf of prop: F fan-in 2 all gates 2 children
v node w/ $L(F_v) \le 2/3\, L(F)$, $> 1/3\, L(F)$

$F =$ 

key obs: F formula $\Rightarrow$ F_v only used to compute value of F
↳ partial computations not reused

ie = 

define $F|_{v \leftarrow b} = F$ w/ - all children of v deleted
- v replaced w/ leaf labelled by b

$$\Rightarrow L(F|_{v\leftarrow b}) = L(F) \underbrace{- L(F_v)}_{> 1/3 \cdot L(F)} + 1 < 2/3\, L(F) + 1$$

$$\Rightarrow \le \lceil 2/3\, L(F) \rceil$$

obs: $F = \begin{cases} F|_{v\leftarrow 0} & \text{if } F_v = 0 \\ F|_{v\leftarrow 1} & \text{if } F_v = 1 \end{cases}$

$F = (\neg F_v \wedge F|_{v\leftarrow 0}) \vee (F_v \wedge F|_{v\leftarrow 1})$] depth $\le \lceil 2/3\, L(F) \rceil$

$$\Rightarrow D(L(F)) \le D(\lceil 2/3\, L(F) \rceil) + O(1) \le O(\lg L(F))$$

Michael Forbes
mforbes@illinois.edu

2019-04-16.2 → 2019-04-16.3
2019-04-16.4 ← cs579

Q?

Q: lbs for formulas? for which function? SAT? [too hard to prove lbs]

def: $\text{parity}_n : \{0,1\}^n \to \{0,1\}$ is $x_1 \oplus \cdots \oplus x_n = \sum x_i \bmod 2$

fact: ↳ has $O(n^2)$ size formula using AND, OR, ¬

thm [Subbotovskaya 60's]: requires $\Omega(n^{1.5})$ size

thm [Krapchenko]: n^2

idea: small formulas can be simplified under substitution — very simple: $OR(x,1) = 1$, $OR(x,0) = x$

- parity cannot: $\oplus(x,0) = x$, $\oplus(x,1) = \neg x$

goal: find restriction $\rho : [n] \to \{0,1,*\}$ st
- $\rho(x_i) = *$ "most" i [alive] [retain hardness of parity]
- $F|_\rho$ simplifies to much smaller formula

[all negations at bottom]

lem: formula F w/ ℓ leaves, fan-in $= 2$ ⇒ exists variable x_i appearing in $\geq \ell/n$ leaves
⇒ pick ρ w/ $\rho(x_i) \in \{0,1\}$, $\rho(x_j) = *$, then $|F|_\rho| \leq \ell - \ell/n = (1-\frac{1}{n})\ell$ (under simplification)

Pf: $\rho(x_i) \in \{0,1\}$, $F|_\rho$ still has ℓ leaves: $x_i \vee x_j \to 0 \vee x_j$

simplification rules:
- absorb constants, eg $AND(x,1) = x$ ⇒ all leaves are literals
- short circuiting: eg $x \wedge G \longmapsto x \wedge G|_{x=1}$ [OR similar]

($G|_{x=1}$: recursively simplify, does not depend on x)

⇒ all leaves w/ x_i get absorbed ⇒ $\leq \ell - \ell/n$ remaining leaves

Cor: parity requires $\Omega(n)$ size lbs

Pf: restrict 1 bit: $\ell \mapsto \leq (1-\frac{1}{n})\ell$ [under simplification]

2 bits $\mapsto (1-\frac{1}{n})(1-\frac{1}{n-1})\cdot\ell$

...

$\underbrace{n-1 \text{ bits}}$ $\longmapsto \underbrace{(1-\frac{1}{n})}_{\frac{n-1}{n}}\underbrace{(1-\frac{1}{n-1})}_{\frac{n-2}{n-1}} \cdots \underbrace{(1-\frac{1}{3})}_{2/3}\underbrace{(1-\frac{1}{2})}_{1/2}\cdot\ell = \ell/n$

↳ 1 bit parity function remains $= \begin{cases} x \\ \neg x \end{cases}$ ⇒ ≥ 1 leaf ⇒ $\ell/n \geq 1$ ∎

Q: how to do better?

A: $x \wedge G \underset{x=0}{\longmapsto} 0$ ← gets absorbed ⇒ kills ≥ 2 leaves

Prop: F simplified formula, pick 1 variable at random (random restrict) and set it randomly from $\{0,1\}$. ⇒ $\mathbb{E}\,|F|_\rho| \leq |F|(1-\frac{1.5}{n})$ (under simplification)

Michael Forbes
Mforbes@illinois.edu
2019-04-16.4 $\leftrightarrows$ 2019-04-16.3 / 2019-04-18.1
CS 579

let x occur in s leaves, eg $\wedge(x, G)$, $\wedge(\neg x, G)$, $\vee(x, G)$, $\vee(\neg x, G)$

in each case:

no double counting for G's

w/p $\frac{1}{2}$: replace w/ G $\leftarrow$ elim 1 leaf — simplification $\Rightarrow$ G has no x leaves

" w/ $\underbrace{\text{constant}}$ $\leftarrow$ elim 2 leaves

$\uparrow$ gets absorbed

$\mathbb{E}[\#\text{ leaves removed} \mid x \text{ chosen}] \geq \frac{3}{2} \cdot s$

$\Rightarrow \mathbb{E}[\quad " \quad] \geq \frac{3}{2} \cdot \frac{|F|}{n}$ $\blacksquare$

Cor: parity requires $\Omega(n^{1.5})$ size AND, OR, NOT formulas.

Pf. restrict 1 bit $\ell \mapsto \leq (1 - \frac{1.5}{n}) \cdot \ell \leq (1 - \frac{1}{n})^{1.5} \cdot \ell$

2 bits $\leq ((1-\frac{1}{n})(1-\frac{1}{n-1}))^{1.5} \cdot \ell$ $\nwarrow$ bernoulli ineq.

$\vdots$

n-1 bits $\leq (\underbrace{(1-\frac{1}{n})(1-\frac{1}{n-1})\cdots(1-\frac{1}{2})}_{=1/n})^{1.5} \ell = \ell/n^{1.5}$

1 bit parity requires ≥ 1 leaf $\Rightarrow \ell/n^{1.5} \geq 1$

$\Rightarrow \ell \geq n^{1.5}$ $\blacksquare$

Rmk: - can improve "shrinkage exponent" from $1.5 \to 2 - o(1)$ [more advanced simplification]

- best explicit lb for AND/OR/NOT formula is $\tilde{\Omega}(n^3)$ [how to do more?]

next time: constant depth unbounded fanin ckts