Michael Forbes
Mforbes@illinois.edu
2015-03-25.4
2015-04-02.2 → 2015-04-02.1
cs 579

cs 579: Computational Complexity: Lecture 20

admin: project topics due

today: circuit lower bounds - intro
- balancing formulas
- random restrictions

intro:

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

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

Thm [Karp Lipton]: $NP \subseteq P/poly \Rightarrow PH = \Sigma_2^P$ [hence "reasonable"]

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

↳ similar to hw: any k, $PH \not\subseteq Size(n^k)$

open: $NEXP \not\subseteq P/poly$ ($\in P, NP$?)

Thm [...] $(1+\Omega(1)) \cdot n$ ckt size lbs for "explicit" functions

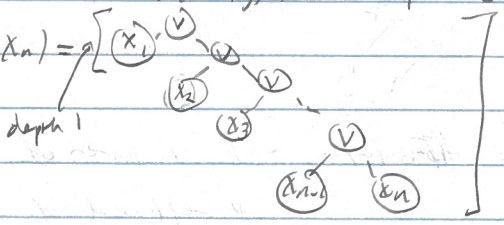
↳ sensitive to gate set eg $\{AND, \neg\}$ vs $\{NAND\}$

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

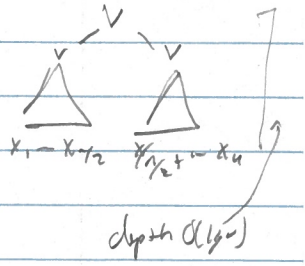
goal: $\omega(n)$ size lb for "interesting" restricted ckt classes

def: depth of circuit is max length of input-output path

eg: $OR(x_1, \dots, x_n) = g[(x_1), (x_2), (x_3), \dots, (x_{n-1}), (x_n)]$ depth 1



depth n =



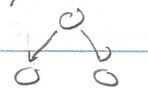
depth $O(\lg n)$

non uniform

def: $NC^i = \{$ family $f_n : \{0,1\}^n \to \{0,1\}$ s.t.
fan-in-2 ckt C_n computing f_n
$size(C_n) \le poly(n)$
$depth(C_n) \le O(\lg^i n)$ $\}$

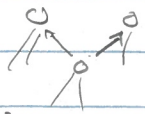
Fact: "all" linear algebra computable in (randomized, uniform) NC^2

def: a formula is a ckt w/ fan-out 1 eg [reuse of computation]



hw: fan-in 2 ckt depth d
$\Rightarrow$ formula size $2^{O(d)}$

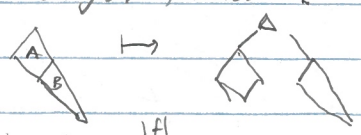
not:



Cor: $NC^1 \subseteq$ polysize formulas

Prop: f size s formula $\Rightarrow$ depth $O(\lg s)$ formula [& size $poly(s)$]

idea: balance a formula



$|A|, |B| \le \frac{|f|}{2}$

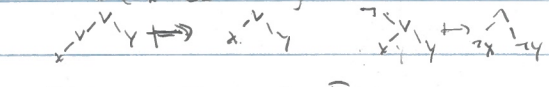
$D(s) \le D(\le s/2) + O(1)$
$\le O(\lg n)$

Michael Forbes
mforbes@illinois.edu
2015-04-02.2 ← 2015-04-02.1
2015-04-02.3 →
CS579

[[recall "basic" version of size]]

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

hw: in formula (, # gates, # edges ≤ O(# leaves)

no gates w/ 1 child ← fan-in 2 ← can collapse eg 

lem: F a formula w/ $L(F)$ leaves. Then some gate v in F w/ subformula F_v rooted at v has $L(F_v) \leq 2/3\, L$ and $> 1/3\, L$.

Pf: traverse down tree

key fact: $L(u \vee w) = L(u) + L(w)$ each > 0.

$\vee$ $2/3\, L(F)$ ↖ one is $> 1/3\, L(F)$, follow that gate

stop when: $L(v) \leq 2/3\, L(F)$

$> 1/3\, L(F)$ ← by previous step. □

Pf of prop: F fan-in 2, no gates w/ 1 child

v node w/ $L(F_v)$ $\leq 2/3\, L(F)$ $> 1/3\, L(F)$

F = 

key fact: F formula ⇒ all gates in F_v influence F via value at v

ie 

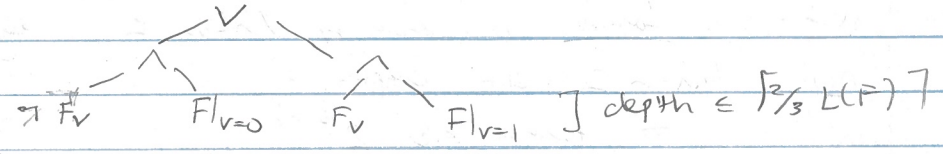
define $F|_{v=b}$ = F w/ - all children of v deleted
- v replaced w/ leaf labelled w/ b

$L(F|_{v=b}) = L(F) - L(F_v) + 1 \leq 2/3\, L(F) + 1$

$> 1/3\, L(F)$

⇒ $L_v \leq \lceil 2/3\, L(F) \rceil$

obs: $F = \begin{cases} F|_{v=0} & \text{if } F_v = 0 \\ F|_{v=1} & \text{if } F_v = 1 \end{cases}$ $x \Rightarrow y$ $\neg x \vee y$

F = 

⇒ $D(L(F)) \leq D(\lceil 2/3\, L(F) \rceil) + O(1)$

$\leq O(\lg L(F))$

= Q

Q: lower bounds for formulas?

hard function $\stackrel{?}{=}$ SAT [[hardness makes this hard]]

parity

Michael Forbes
mforbes@illinois.edu

hw: parity $(\bar{x}) = x_1 \oplus \cdots \oplus x_n$ has $O(n^2)$ size formula in AND, OR, NOT basis

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

Thm [Krapchenko]: $\Omega(n^2)$ size

idea: small formulas can be simplified $OR(x,1) = 1$, $OR(x,0) = x$ (simplified)

under substitution

parity generalizes: $\oplus(x,0) = x$, $\oplus(x,1) = \neg x$

goal: find restriction $\rho : [n] \to \{0,1,*\}$ s.t.

- $\rho(x_i) = *$ "most i" ⇒ retain hardness of parity
- $F|_\rho$ "much" simpler than F

lem: formula F of ℓ leaves ↦ variable x_i appearing in $\geq \ell/n$ leaves

⇒ $\exists \rho$ s.t. $\rho(x_i) \in \{0,1\}$, $\rho(x_j) = *$ ⇒ $|F|_\rho| \leq \ell - \ell/n \leq (1-1/n)\ell$

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

simplification rules:

- absorb constants: eg $A \wedge 0 = 0$, $A \wedge 1 = x$ ⇒ all leaves are variables
- push negations to bottom: $\neg(x \vee y) = \neg x \wedge \neg y$ ⇒ all leaves are literals
- short circuiting: $x \wedge F \mapsto x \wedge F|_{x=1}$ (recursively simplify); OR is similar

⇒ all leaves of x_i are absorbed ⇒ $\leq \ell - \ell/n$ remaining leaves

cor: parity requires $\Omega(n)$ size circuits

Pf: restrict 1 bit: $\ell \mapsto (1-\frac{1}{n})\ell$

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

$\vdots$

$n-1$ bits: $\ell \mapsto (1-\frac{1}{n})(1-\frac{1}{n-1})\cdots(1-\frac{1}{3})(1-\frac{1}{2})\ell$

$\frac{n-1}{n} \cdot \frac{n-2}{n-1} \cdots \frac{2}{3} \cdot \frac{1}{2} \ell = \ell/n$

↳ 1 bit parity function ⇒ ≥ 1 leaf

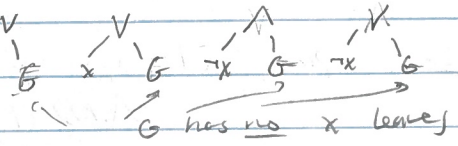
Q: how to do better?

A: $x \wedge g \mapsto 0$ ($x=0$) kills $\geq$ two leaves

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

Richard Farber
rfarber2@illinois.edu
2018-04-02-4 ← 2018-04-02.3
2018-04-04.1 →
cs579

let x occur in s leaves eg x.



in each case:

no double counting

- w/p 1/2: replace w/ G ← elim ≥1 leaf
- 1/2: w/ constant ≥2 leafs

$\mathbb{E}$[# leaves removed | x chosen] $\geq \frac{3}{2} \cdot s$ ← gets absorbed

$\Rightarrow \mathbb{E}$[# leaves removed] $\geq \frac{3}{2} \frac{1}{n} \cdot |F|$ ☐

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

pf: restrict 1 bit: $\ell \mapsto \leq \ell\left(1 - \frac{1.5}{n}\right) \leq \ell\left(1 - \frac{1}{n}\right)^{1.5}$ ← Bernoulli's inequality

$\vdots$

$\underbrace{n-1 \text{ bits}}_{1 \text{ bit parity}}$ $\ell \mapsto$ $\underbrace{\leq \ell \cdot \frac{1}{n^{1.5}}}_{\geq 1}$ $\Rightarrow \ell \geq n^{1.5}$

Rmk: Can improve "shrinkage exponent" $1.5 \mapsto 2 - o(1)$

best explicit lb for AND/OR/NOT formula is $\tilde{\Omega}(n^3)$

next time: constant depth circuits