Michael Forbes
Mforbes@illinois.edu
2018-04-18.4
2018-04-23.1 → 2018-04-23.4
CS 579

CS 579: Computational Complexity: Lecture 25

5, 6

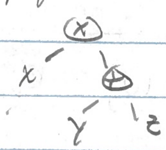
admin: ps6 due

projects: reports due 05-02

presentations next week

today: homogeneous polynomials — ubs — lbs

recall: algebraic circuits



compute polynomials $x^2 - x \neq 0$ over $\mathbb{F}_2$

$$P \text{ vs } NP \simeq VP \text{ vs } VNP \simeq \det \text{ vs } \mathrm{perm}$$

fact: exist polynomials hard to compute

Sketch: say over $\mathbb{F}_q$ — $\leq q^{\mathrm{poly}(s)}$ polynomials w/ size $\leq s$

— $= q^{\binom{n+d}{d}}$ polynomials degree $\leq d$ n-var

$\Rightarrow \quad s \geq \binom{n+d}{d}^{\Omega(1)}$

Rmk: can show $\{0,1\}$-coeff poly require $\binom{n+d}{d}^{\Omega(1)}$ size any $\mathbb{F}$

goal: lower bounds for explicit poly

↳ in restricted classes

---

def: $f(\bar{x}) = \sum_{\bar{a}} \alpha_{\bar{a}} \bar{x}^{\bar{a}}$ is *homogeneous* if all $\alpha_{\bar{a}} \bar{x}^{\bar{a}}$ $\begin{cases} = 0 \\ \deg = \deg f \end{cases}$

eg: $xy - x^2$ $\qquad = \sum_{i \leq \deg(f)} H_i(f)$ ← deg-i homogeneous part

not $xy - y$

det perm

def: a circuit is homogeneous if each node computes homogeneous polynomial

Q: homogeneous ckts vs general? // miraculous cancellation ?! eg $(x+1)^2 - x^2 = 2x+1$

Prop: size s fan-in 2 ckt for f // single output

$\Rightarrow$ poly(s,d)-size $\underbrace{\text{homog unbounded fanin}}_{\text{fan in 2}}$ ckt for $\{H_0(f), \ldots, H_d(f)\}$ $\quad d = \deg f$

$\Rightarrow$ "

if f homog get homog ckt for f

Pf: induction on gates

node v: computes f_v ← $\Theta(d)$ blowup

idea: split into $v_0, \ldots, v_d \mapsto$ computing $H_0(f_v), \ldots, H_d(f_v)$

$v = u + w$: $\quad f_v = \sum \underbrace{H_i(f_v)}_{\deg = i}$

$\quad \overset{\shortparallel}{f_u + f_w}$

$= \sum H_i(f_u) + \sum_i \underbrace{H_i(f_w)}_{\deg = i}$

$\Rightarrow H_i(f_v) = H_i(f_u) + H_i(f_w)$

hence: $v_i := u_i + w_i$ ← $\Theta(1)$ blowup

Michael Forbes
mforbes@illinois.edu
2018-04-23.2 ← 2018-04-23.1
→ 2018-04-23.3
cs579

$v = u \times w$: $f_u = \sum H_i(f_u)$ $f_w = \sum H_j(f_w)$

$$f_v = f_u \cdot f_w = \sum_i \sum_j \underbrace{H_i(f_u)}_{\deg i} \underbrace{H_j(f_w)}_{\deg j}$$

$$= \sum_k \underbrace{\sum_{i+j=k} H_i(f_u) H_j(f_w)}_{\deg k}$$

$$v_k := \underbrace{\sum_{i+j=k} u_i \times w_j}_{O(d) \text{ size}}$$

homogeneity: clear
correctness: clear
sizes: s nodes $\mapsto$ $s \cdot d$ nodes, $O(d)$ circuitry per node
$\rightarrow$ size $O(s \cdot d^2)$

Rmk. never need to compute deg > deg f
only "efficient" if $d \le$ poly
increases depth: $O(1)$-depth unbounded fan in size s
$\mapsto$ $O(\lg s)$-depth fan-in 2 size poly(s)
$\mapsto$ " unbounded poly(s,d) homog
$\mapsto$ fan in 2

Q: homogeneous low depth formulas?

fact: $esym_{n,d}$ has poly(n) depth $O(d)$ by induct on d

Prop: $esym_{n,d} = \sum_{S \in \binom{[n]}{d}} \prod_{i \in S} x_i$ elementary symmetric poly

has $O(n^2)$ size depth 3 formula non homogeneous

Pf: by interpolation trick

$f(x_1, \ldots x_n) = \sum_i H_i(f)$

$f(tx_1, \ldots, tx_n) = \sum_i H_i(f) \cdot t^i \in \mathbb{F}[\bar{x}][t]$

Consider $f(\bar{x}) = (1+x_1) \cdots (1+x_n)$

$$f(t \cdot \bar{x}) = \sum_{i=0}^{n} esym_{n,i}(\bar{x})\, t^i$$

polynomial interpolation: extract coefficients from evaluations

any $d+1$ points $\alpha_0, \ldots \alpha_d \in \mathbb{F}$ any i, exist $\beta_0^{(i)}, \ldots \beta_d^{(i)}$ st any $\deg(f) = d$

$$H_i(f) = \sum_{j=0}^{d} \beta_j^{(i)} f(\alpha_j \cdot \bar{x})$$

$$\Rightarrow esym_{n,d}(\bar{x}) = \underbrace{\sum_{j=0}^{n} \beta_j^{(d)} \overbrace{\prod_{i=1}^{n} (1 + \alpha_j x_i)}^{\deg n > d}}_{\text{depth 3 size } \Theta(n^2)}$$

Michael Forbes
Miforbes@illinois.edu
2018-04-23.2 $\rightleftarrows$ 2018-04-23.3
2018-04-23.4
cs579

Rmk: surprising: $\underbrace{\text{esym}_{n,n/2}}_{\text{depth } 3} \approx \underbrace{\text{Majority}}_{\notin AC^0[p] \text{ any } p}$

Prop [NW96] $\text{esym}_{n,d}$ requires $\Omega(n/d)^d$ size depth 3 homogeneous [not show]

Rmk: homogeneity is restrictive in low depth

Prop: $\det_n$ requires $2^{\Omega(n)}$ " [will show]

def: $f \in \mathbb{F}[x_1, \ldots, x_n]$ $\quad \partial_{x_i} : \mathbb{F}[\bar{x}] \to \mathbb{F}[\bar{x}]$ formal derivative

$\partial_{x_i}\left(\sum \alpha_{\bar{a}} \bar{x}^{\bar{a}}\right) = \sum \alpha_{\bar{a}} \cdot a_i \cdot \bar{x}^{\bar{a} - \bar{e}_i}$

idea: $\mu : \mathbb{F}[\bar{x}] \to \mathbb{Z}$

$\mu(\det) \geq \text{large}$

$\mu(\text{ckt}) \leq \text{small}$

$\mu(f) = \dim \{\cdots\}$

eg: $\partial_x(1) = 0$

$\partial_x(x) = 1$

$\partial_x(x^2) = 2x$

lem: $\partial_{x_i}(\alpha f + \beta g) = \alpha \partial_{x_i}(f) + \beta \partial_{x_i}(g)$

$\partial_x(f \cdot g) = f \cdot \partial_x(g) + \partial_x(f) \cdot g$

def: $\bar{x}^{\bar{a}} = \prod x_i^{a_i}$

$\partial_{\bar{x}}^{\bar{a}} = \underbrace{\partial_{x_1} \cdots \partial_{x_1}}_{a_1} \cdots \underbrace{\partial_{x_n} \cdots \partial_{x_n}}_{a_n}$

lem: $\partial_{\bar{x}}^{\bar{a}}$ linear

$\partial_{\bar{x}}^{\bar{a}}(f \cdot g) = \sum_{\bar{b}+\bar{c}=\bar{a}} \binom{\bar{b}+\bar{c}}{\bar{b}} \partial_{\bar{x}}^{\bar{b}}(f)\, \partial_{\bar{x}}^{\bar{c}}(g)$, $\quad \binom{\bar{b}+\bar{c}}{\bar{b}} = \prod_i \binom{a_i}{b_i}$

def: $\underline{\partial}(f) = \{\partial_{\bar{x}}^{\bar{a}} f\}_{\bar{a}} \subseteq \mathbb{F}[\bar{x}]$

$\mu(f) := \dim \underline{\partial}(f) = \dim \operatorname{span} \underline{\partial}(f)$

lem: $\mu(f+g) \leq \mu(f) + \mu(g)$

$\mu(f \cdot g) \leq \mu(f) \cdot \mu(g)$

Pf: $\operatorname{span}\{\partial_{\bar{x}}^{\bar{a}} f \cdot g\}_{\bar{a}} \subseteq \operatorname{span}\{\partial_{\bar{x}}^{\bar{b}} f \cdot \partial_{\bar{x}}^{\bar{c}} g\}_{\bar{b},\bar{c}}$

$\subseteq \operatorname{span}\{\quad " \quad\}_{\bar{b} \in \mathcal{B},\, \bar{c} \in \mathcal{C}}$ basis for $\underline{\partial}(f)$

Prop: $f = \sum_{i=1}^{s} \prod_{j=1}^{d = \deg f} \underbrace{l_{ij}}_{\deg = 1} \Rightarrow \mu(f) \leq s \cdot 2^d$

Pf: $\mu(f) \leq \sum_i \mu\left(\prod_j l_{ij}\right)$

$\leq \sum_i \prod_j \mu(l_{ij})$

$\leq s\, 2^d$

$\hookrightarrow \quad = \sum_k \alpha_{ijk} x_k$

$\partial_{x_\ell} l_{ij} = \alpha_{ij\ell}$ $\quad \Big]$ dim $= 2$

Michael Forbes
miforbes@illinois.edu
2018-04-23.4 ← 2018-04-23.3
→ 2018-04-25.1
CS 579

Prop: $\mu(\det_n) \geq \binom{n}{n/2}^2$

$\Rightarrow$ thm: $\mu(\det) = \mu(\Sigma \Pi^n \Sigma) \leq s \cdot 2^n$

$\quad \vee\!\mid$

$\binom{n}{n/2}^2 \qquad \Rightarrow \quad s \geq \Omega(2^n/n)$

$\geq \Theta\left(\frac{2^n}{\sqrt{n}}\right)^2$

$= \Theta\left(\frac{4^n}{n}\right)$

Pf of prop: find $\binom{n}{n/2}^2$ linearly independent partial deriv

$\det_n\left(\boxed{}\right) = \sum \mathrm{sgn}(\sigma) \prod x_{i,\sigma(i)}$

$\partial_{x_{1,1}} \det_n = \det_n \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & \boxed{} & \\ & & & \end{pmatrix}$

$\partial_{x_{1,1} x_{2,2}} = \det \begin{pmatrix} 1 & 0 & & \\ 0 & 1 & & \\ & & \boxed{} & \end{pmatrix}$

$\Rightarrow$ degree-k derivatives $=$ $(n-k)\times(n-k)$ minors

$\binom{n}{k}^2$ of them

fact: fixed k linearly independent as triangular system

set $k = n/2$

Rmk: same proof for $esym_{n,d}$, argue $\mu(esym)$ more involved

$\mu(\Sigma\Pi\Sigma)$, $\mu(\det)$ both large

lbs for homog depth 4 only in 2014

5 ???