Michael Forbes
mforbes@illinois.edu

2018-04-20.4 → 2018-04-25.1
2018-04-25.2 ← CS579

CS579: Computational Complexity: Lecture 26

today: homogeneous depth 3 lbs
polynomial identity testing

homogeneous depth 3 - lbs

last time: det hom deg poly = all (nonzero) monomials have same degree
" ckt = all nodes compute homog poly

prop: size s ckt for f $\Rightarrow$ poly(s, deg f) homog ckt for $\{H_i(f)\}_i$
↳ depth increasing

prop: $\mathrm{esym}_{n,d} = \sum_{S \in \binom{[n]}{d}} \prod_{i \in S} x_i$ has $O(n^2)$ size $\underbrace{\Sigma\Pi\Sigma}_{\text{depth 3}}$

Thm: esym$_{n,d}$ requires $\Omega(n/d)^d$ size homog $\Sigma\Pi\Sigma$ [I didn't do]

Thm: det$_n$ requires $2^{\Omega(n)}$ "

idea: complexity measure μ
subadditive: $\mu(f+g) \le \mu(f) + \mu(g)$
submultiplicative: $\mu(f \cdot g) \le \mu(f) \cdot \mu(g)$
$\Rightarrow \mu(\Sigma^3 \Pi^d \Sigma) \le s \cdot 2^d$ [small]
↑ $\mu(\deg 1) \le 2$

$\mu(f) := \dim \underline{\partial}(f)$
$= \{\partial_{\bar{x}^{\bar{a}}} f\}_{\bar{a}}$ [partial derivatives]

Prop: $\mu(\det_n) \ge \binom{n}{n/2}^2 = \Theta(4^n/n)$
$\Rightarrow s \ge \Theta(2^n/n)$ as $d = n$

Pf: $\det(X) = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma)\, x_{1\sigma(1)} x_{2\sigma(2)} \cdots x_{n\sigma(n)}$

$\partial_{x_{ij}} \det = \sum_{\sigma \in S_n} \mathrm{sgn}\,\sigma\, \partial_{x_{ij}} x_{1\sigma(1)} \cdots x_{n\sigma(n)}$

$= \begin{cases} 0 & j \ne \sigma(i) \\ \prod_{k \ne i} x_{k\sigma(k)} & j = \sigma(i) \end{cases}$

$\partial_{x_{i_1 j_1}} \partial_{x_{i_2 j_2}} \det = \sum_{\sigma \in S_n} \mathrm{sgn}\,\sigma\, \partial\partial\, x_{1\sigma(1)} \cdots x_{n\sigma(n)}$

$= \begin{cases} \prod_{k \notin \{i_1, i_2\}} x_{k\sigma(k)} & j_1 = \sigma(i_1),\ j_2 = \sigma(i_2) \\ 0 & \text{else} \end{cases}$

$= x_{1\sigma(1)} \cdots x_{n\sigma(n)} \big|_\rho$ $\quad \rho = \begin{bmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & * \end{bmatrix}$

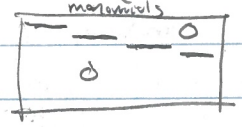
$= \det_n(X|_\rho) = \pm \det_{n-2}\left(x_{[n] \setminus \{i_1, i_2\},\, [n] \setminus \{j_1, j_2\}}\right)|_{\rho(x_{a,b})}$ $\quad \rho(x_{a,b}) = \begin{cases} 1 & a = i_k,\ b = j_k \\ x_{a,b} & a \notin \{i_1, i_2\},\ b \notin \{j_1, j_2\} \\ 0 & \text{else} \end{cases}$

Michael Forbes
MForbes@illinois.edu
2018-04-25.1 ← 2018-04-25.2 → 2018-04-25.3
cs579

$\Rightarrow \partial^{=1}(\det) = \{ \partial_{\bar{x}^{\bar{a}}} \det_n \}_{\deg \bar{x}^{\bar{a}} = k} = \{ \pm 1 \cdot \det_{n-k}(X|_{S \times T}) \}_{S,T \in \binom{[n]}{n-k}}$

Clm: $\dim \partial^{=1}(\det) = \binom{[n]}{n-k}^2$ ∎ linearly ind. deg ∎

Pf: idea:



ie: $\det_{n-k}(X|_{S \times T}) = \sum_{\sigma: S \to T} \operatorname{sgn}(\sigma) \prod_{i \in S} x_{i,\sigma(i)}$

$= x_{[\sigma(i_1)]} \cdots x_{i_{n-k}, \sigma(i_{n-k})}$

$= S \quad = T$

$\Rightarrow$ monomials in $\det_{n-k}(X|_{S' \times T'})$ do not overlap

$\Rightarrow$ triangular matrix

$\Rightarrow$ full rank. ∎

---

polynomial identity testing (PIT)

Q: given a polynomial is it zero? (by algebraic circuit)

lem: PIT ∈ coRP

Pf: Schwartz Zippel

Q: PIT ∈ P?

def: $\mathcal{C} \subseteq \mathbb{F}[\bar{x}]$ class of polynomials

$H \subseteq \mathbb{F}^n$ is a hitting set for $\mathcal{C}$ if $\forall f \in \mathcal{C}$,

$f \equiv 0$ iff $f|_H \equiv 0$ ($\forall \bar{a} \in H \; f(\bar{a}) = 0$)

Rmk: poly-size explicit H for $\mathcal{C}_s = \{\text{size-}s \text{ circuits}\} \Rightarrow$ PIT ∈ P ∎ converse unclear ∎

exp-size explicit H exist, via Schwartz Zippel

poly-size H exist for $\mathcal{C}_s$, probabilistic method

constructing explicit small H for $\mathcal{C} \approx$ lbs against $\mathcal{C}$ ∎ hardness vs randomness ∎

Q: construct hitting sets? for deeper circuits? ∎ given how $\Sigma\Pi\Sigma$ known isn't det ∎

def: f is s-sparse if $f = \sum_{\bar{a} \in S} \alpha_{\bar{a}} \bar{x}^{\bar{a}}$ $|S| \leq s$.

Rmk: PIT is easy for this class

Q: hitting sets?

Michael Forbes
MForbes@mit.edu

2016-04-25.2 → 2016-04-25.3
2016-04-25.4 ← CS57

[Kliivers Spielman]

← qualitatively optimal

thm: explicit poly(s, n, d)-size hitting set for s-sparse poly in n-var deg ≤ d

idea: - $\mathcal{C} = \{ f \text{ univ deg} \le d \}$ is hit by any $d+1$ points
- reduce n-var s-sparse poly to ↑
  - ↳ via hashing

Rmk: pairwise hashing does not work
↳ not randomness efficient enough.

$f(\bar{x}) = \sum_{\bar{a} \in S} \alpha_{\bar{a}} \bar{x}^{\bar{a}}$ $|S| \le s$

$f(y^{b_1}, \dots, y^{b_n}) = \sum_{\bar{a} \in S} \alpha_{\bar{a}} y^{\langle \bar{a}, \bar{b} \rangle}$ ($= \sum a_i b_i$)

want low-degree ↑ univ ↑ then use univar hitting set

obs: $f \neq 0$, $\{\langle \bar{a}, \bar{b} \rangle\}_{\bar{a} \in S}$ distinct $\Rightarrow f(y^{\bar{b}}) \neq 0$ ∎ no cancellation

goal: construct $\mathcal{B}$ s.t. any $S \subseteq \{0, \dots, d\}^n$ $|S| \le s$ (small coeff's) some $\bar{b} \in \mathcal{B}$ s.t. $\{\langle \bar{a}, \bar{b} \rangle\}_{\bar{a} \in S}$ distinct

construction: p prime [don't need too large]

$\{(1, b \bmod p, b^2 \bmod p, \dots, b^{n-1} \bmod p)\}_{b \le p}$ $\subseteq \{0, \dots, p\}^n$

lem: $p > s^2 n$ works

pf: $\langle \bar{a}, \bar{b} \rangle = \sum_{0 \le i < n} a_i (b^i \bmod p) \equiv A(b) \bmod p$ (univar deg $< n$)

$\langle \bar{a}', \bar{b} \rangle \equiv A'(b) \bmod p$

$\langle \bar{a}, \bar{b} \rangle = \langle \bar{a}', \bar{b} \rangle \Rightarrow$

$\Rightarrow \equiv \bmod p$

$\Rightarrow$ [b root of $A - A' \bmod p$] $\le n$ such roots] $\le s^2$ such A, A'

putting it together:

$f(x_1, \dots, x_n) = \sum_{\bar{a} \in S} \alpha_{\bar{a}} \bar{x}^{\bar{a}}$ $|S| \le s$ some $\alpha_{\bar{a}} \neq 0$

$f(y^1, y^{b \bmod p}, \dots, y^{b^{n-1} \bmod p}) = \sum \alpha_{\bar{a}} y^{\langle \bar{a}, \bar{b} \rangle}$ $\neq 0$

($\le p$; $\le d \cdot p$; some $b \in \{0, \dots, p\}$)

$= f_{b,p}(y)$ ← not zero on $\alpha_0, \dots, \alpha_{dp}$

$\mathcal{H} = \{(\alpha_i^{1 \bmod p}, \alpha_i^{b \bmod p}, \dots, \alpha_i^{b^{n-1} \bmod p}) : p \text{ prime } > s^2 n,\ b \le p,\ p \le O(s^2 n),\ \alpha_0, \dots, \alpha_{dp} \text{ distinct}\}$

can be found in $\text{poly}(s, n)$ time

$\Rightarrow |\mathcal{H}| \le p \cdot (dp + 1) \le O(s^2 n) \cdot O(d s^2 n) = O(d s^4 n) \le \text{poly}(s, n, d)$ ∎

Bertrand's postulate

Michael Forbes
miforbes@illinois.edu
2015-04-25.4 ← 2015-04-25.3
↪|
CS579

Rmk: - hitting set for 2s sparse ⇒ interpolation set for s-sparse

$(f-g)|_H \neq 0 \Rightarrow f|_H \neq g|_H$ f,g s-sparse

- deterministic polytime also to interpolate s-sparse poly
[variations of the above]

next week: projects