Lecture 3: Lower Bounds in Algebraic Complexity

Rafael Oliveira

University of Waterloo
Cheriton School of Computer Science

rafael.oliveira.teaching@gmail.com

January 18, 2021

Overview

- “Natural” lower bound strategies
- Lower Bounds for Homogeneous Depth-3 Circuits
- Shifted Partial Derivatives and Depth-4 Circuits
- Conclusion
- Acknowledgements

How to prove lower bounds?

1. *Computation Progresses Slowly:* complexity of $f + g$ or $f \times g$ shouldn't be so different from complexity of f, g

How to prove lower bounds?

1. *Computation Progresses Slowly:* complexity of $f + g$ or $f \times g$ shouldn't be so different from complexity of f, g
2. *Complexity Measure:* find complexity measure $\mu : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{N}$ which captures this slow progress

How to prove lower bounds?

1. *Computation Progresses Slowly:* complexity of $f + g$ or $f \times g$ shouldn't be so different from complexity of f, g
2. *Complexity Measure:* find complexity measure $\mu : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{N}$ which captures this slow progress
   - $\mu(x_i), \mu(\alpha) = O(1)$ for all variables and constants from $\mathbb{F}$

How to prove lower bounds?

1. *Computation Progresses Slowly:* complexity of $f + g$ or $f \times g$ shouldn't be so different from complexity of f, g
2. *Complexity Measure:* find complexity measure $\mu : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{N}$ which captures this slow progress
   - $\mu(x_i), \mu(\alpha) = O(1)$ for all variables and constants from $\mathbb{F}$
   - μ is sub-additive and sub-multiplicative

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

not so important

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

$$\boxed{\mu(f) + \mu(g)}$$

How to prove lower bounds?

1. *Computation Progresses Slowly:* complexity of $f + g$ or $f \times g$ shouldn't be so different from complexity of f, g
2. *Complexity Measure:* find complexity measure $\mu : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{N}$ which captures this slow progress
   - $\mu(x_i), \mu(\alpha) = O(1)$ for all variables and constants from $\mathbb{F}$
   - μ is sub-additive and sub-multiplicative

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

$$\mu(f \cdot g) \leq \mu(f) + \mu(g) + 1$$

   - μ is "easy" to compute or estimate } useful
3. For instance $\boxed{S(f)}$ is a valid complexity measure, but we don't know how to estimate it, let alone compute it

How to prove lower bounds?

1. *Computation Progresses Slowly:* complexity of $f + g$ or $f \times g$ shouldn't be so different from complexity of f, g
2. *Complexity Measure:* find complexity measure $\mu : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{N}$ which captures this slow progress
   - $\mu(x_i), \mu(\alpha) = O(1)$ for all variables and constants from $\mathbb{F}$
   - μ is sub-additive and sub-multiplicative

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

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

   - μ is "easy" to compute or estimate
3. For instance $S(f)$ is a valid complexity measure, but we don't know how to estimate it, let alone compute it
4. *Open problem:* what is the complexity of computing $S(f)$, if I give f in dense representation? (algebraic minimum circuit size problem)

f deg d n vars $\binom{n+d}{d}$ poly$\left(\binom{n+d}{d}\right)$ time

How have we usually proved lower bounds?

$s_n : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{N}$

1. Define class of simple polynomials $\mathcal{S}$
2. *Normal form:* every circuit from circuit class $\mathcal{C}$ can be expressed as small sum of simple polynomials in $\mathcal{S}$

problem: given circuit class $\mathcal{C}$, parameter h_n

find explicit polynomial $\{P_n\}_{n \geq 1}$ s.t. P requires

size h_n in class $\mathcal{C}$

$$\Phi \in \mathcal{C} \qquad \Phi = P \Rightarrow s(\Phi) \geq h$$

$$\{\mathrm{Det}_n\}_{n \geq 1} \qquad \{\mathrm{Per}_n\}_{n \geq 1} \qquad \{E_{n,d}\}_{n,d \geq 1}$$

$d = d(n)$

$\mathcal{C}$ = poly-sized formulas } we choose

$\mathcal{G}$ = $f \cdot g$ where

$$\frac{1}{3}\deg(fg) \le \deg(f), \deg(g) \le \frac{2}{3}\deg(fg)$$

} we choose

$\Phi \in \mathcal{C}$ $\quad s(\Phi) = s$

$$\Phi = \sum_{i=1}^{s} f_i g_i$$

any formula of size s can be written as sum of $\le s$ "simple" polynomials

Hyafil '70s

How have we usually proved lower bounds?

1. Define class of simple polynomials $\mathcal{S}$
2. *Normal form:* every circuit from circuit class $\mathcal{C}$ can be expressed as <u>small sum of simple polynomials</u> in $\mathcal{S}$
3. *Complexity Measure:* find sub-additive complexity measure $\mu : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{N}$ which captures the simplicity of $\mathcal{S}$

How have we usually proved lower bounds?

1. Define class of simple polynomials $\mathcal{S}$
2. *Normal form:* every circuit from circuit class $\mathcal{C}$ can be expressed as small sum of simple polynomials in $\mathcal{S}$
3. *Complexity Measure:* find sub-additive complexity measure $\mu : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{N}$ which captures the simplicity of $\mathcal{S}$
   - $\mu(f)$ small for all polynomials in $\mathcal{S}$

$f \in S \Rightarrow \mu(f)$ small $(\leq U)$

How have we usually proved lower bounds?

1. Define class of simple polynomials $\mathcal{S}$
2. *Normal form:* every circuit from circuit class $\mathcal{C}$ can be expressed as small sum of simple polynomials in $\mathcal{S}$
3. *Complexity Measure:* find sub-additive complexity measure $\mu : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{N}$ which captures the simplicity of $\mathcal{S}$
   - $\mu(f)$ small for all polynomials in $\mathcal{S}$
   - μ is sub-additive

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

How have we usually proved lower bounds?

1. Define class of simple polynomials $\mathcal{S}$
2. *Normal form:* every circuit from circuit class $\mathcal{C}$ can be expressed as small sum of simple polynomials in $\mathcal{S}$
3. *Complexity Measure:* find sub-additive complexity measure $\mu : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{N}$ which captures the simplicity of $\mathcal{S}$
   - $\mu(f)$ small for all polynomials in $\mathcal{S}$
   - μ is sub-additive

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

   - μ is "easy" to compute or estimate
4. *Hard polynomial:* find polynomial p such that $\mu(p)$ is large

How have we usually proved lower bounds?

1. Define class of simple polynomials $\mathcal{S}$
2. *Normal form:* every circuit from circuit class $\mathcal{C}$ can be expressed as small sum of simple polynomials in $\mathcal{S}$
3. *Complexity Measure:* find sub-additive complexity measure $\mu : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{N}$ which captures the simplicity of $\mathcal{S}$
   - $\mu(f)$ small for all polynomials in $\mathcal{S}$
   - μ is sub-additive
   $$\mu(f+g) \leq \mu(f) + \mu(g)$$
   - μ is "easy" to compute or estimate
4. *Hard polynomial:* find polynomial p such that $\mu(p)$ is large

- If $\mu(f) \leq U$ for all $f \in \mathcal{S}$

How have we usually proved lower bounds?

1. Define class of simple polynomials $\mathcal{S}$
2. *Normal form:* every circuit from circuit class $\mathcal{C}$ can be expressed as small sum of simple polynomials in $\mathcal{S}$
3. *Complexity Measure:* find sub-additive complexity measure $\mu : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{N}$ which captures the simplicity of $\mathcal{S}$
   - $\mu(f)$ small for all polynomials in $\mathcal{S}$
   - μ is sub-additive
     $$\mu(f+g) \leq \mu(f) + \mu(g)$$
   - μ is "easy" to compute or estimate
4. *Hard polynomial:* find polynomial p such that $\mu(p)$ is large

- If $\mu(f) \leq U$ for all $f \in \mathcal{S}$
- By sub-additivity $\mu(q) \leq s \cdot U$ for any $q \in \mathcal{C}$ which can be written as

$$\boxed{q = \sum_{i=1}^{s} f_i,} \quad f_i \in \mathcal{S}$$

$$\Rightarrow \mu(q) \leq \sum_{i=1}^{s} \mu(f_i) \leq s \cdot U$$

How have we usually proved lower bounds?

1. Define class of simple polynomials $\mathcal{S}$
2. *Normal form:* every circuit from circuit class $\mathcal{C}$ can be expressed as small sum of simple polynomials in $\mathcal{S}$
3. *Complexity Measure:* find sub-additive complexity measure $\mu : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{N}$ which captures the simplicity of $\mathcal{S}$
   - $\mu(f)$ small for all polynomials in $\mathcal{S}$
   - μ is sub-additive
   $$\mu(f+g) \leq \mu(f) + \mu(g)$$
   - μ is "easy" to compute or estimate
4. *Hard polynomial:* find polynomial p such that $\mu(p)$ is large

- If $\mu(f) \leq U$ for all $f \in \mathcal{S}$
- By sub-additivity $\mu(q) \leq s \cdot U$ for any $q \in \mathcal{C}$ which can be written as
$$\overset{p}{\cancel{q}} = \sum_{i=1}^{s} f_i, \quad f_i \in \mathcal{S}$$

$L \leq \mu(p) \leq s \cdot U$

$s \geq L/U$

- $\boxed{\mu(p) \geq L}$ and p can be computed by size s in $\mathcal{C} \Rightarrow s \cdot U \geq L$

Lower bounds

Why study constant depth circuits?

$\Sigma\Pi\Sigma$ homogeneous

$\Sigma\Lambda^d(\underbrace{\Sigma\Pi^2}_{\text{quadratic polynomials}})$

$\Sigma\Pi^{\sqrt{d}}\Sigma\Pi^{\sqrt{d}}$

- AV'08, GKKS'12,13, Koi'10s, Tav'13

depth reduction

P computed by circuits of size s

$\Rightarrow$ P computed by depth-4 homogeneous ckts (depth-3 non-homogeneous) of size $n^{\sqrt{s}}$

if we prove strong enough lower bds for depth-3/4 ckts $\Rightarrow$ general ckt lbs.

- "Natural" lower bound strategies
- Lower Bounds for Homogeneous Depth-3 Circuits
- Shifted Partial Derivatives and Depth-4 Circuits
- Conclusion
- Acknowledgements

Homogeneous depth-3 circuits

- Simple polynomials: products of linear forms

$$\boxed{\prod_{i=1}^{d}(a_{i1}x_1 + \cdots + a_{in}x_n)}$$

$$\Sigma\,\Pi^{[d]}\,\Sigma$$

$$P = \sum_{i=1}^{s} \underbrace{\prod_{j=1}^{d} l_{ij}(\bar{x})}$$

Homogeneous depth-3 circuits

- Simple polynomials: products of linear forms

$$\prod_{i=1}^{d}(a_{i1}x_1 + \cdots + a_{in}x_n)$$

- Circuit class $\mathcal{C}$

$$\mathcal{C}(s, n, d) := \left\{ f \in \mathbb{F}[x_1, \ldots, x_n]_d \mid f = \sum_{i=1}^{s}\prod_{j=1}^{d}\ell_{ij}(x_1, \ldots, x_n) \right\}$$

homogeneous
poly of degree d

Homogeneous depth-3 circuits

- Simple polynomials: products of linear forms

$$\prod_{i=1}^{d}(a_{i1}x_1 + \cdots + a_{in}x_n)$$

- Circuit class $\mathcal{C}$

$$\mathcal{C}(s,n,d) := \left\{ f \in \mathbb{F}[x_1,\ldots,x_n]_d \mid f = \sum_{i=1}^{s}\prod_{j=1}^{d}\ell_{ij}(x_1,\ldots,x_n) \right\}$$

- Complexity measure: dimension of space of all partial derivatives

$$\mu(f) = \dim(\partial^* f)$$

Homogeneous depth-3 circuits

$\partial_j x_i = \delta_{ij}$

x_i

- Simple polynomials: products of linear forms

$$\prod_{i=1}^{d}(a_{i1}x_1 + \cdots + a_{in}x_n)$$

- Circuit class $\mathcal{C}$

$$\mathcal{C}(s,n,d) := \left\{ f \in \mathbb{F}[x_1,\ldots,x_n]_d \mid f = \sum_{i=1}^{s}\prod_{j=1}^{d}\ell_{ij}(x_1,\ldots,x_n) \right\}$$

- Complexity measure: dimension of space of all partial derivatives

$$\mu(f) = \dim(\partial^* f)$$

- Examples:

$$\mu(x_i) = 2 \qquad\qquad \mu(x_1 \cdot x_2 \cdots x_n) = 2^n$$

$\dim(\mathbb{F}\text{-span}\{1, x_i\}) = 2$ $\quad\dim\langle x_S\rangle_{S\subseteq[n]} = 2^n$

Property of partial derivatives

$\partial f \qquad \partial(\alpha f) = \alpha \cdot \partial f$

Given polynomials $f, f_1, \ldots, f_k \in \mathbb{F}[x_1, \ldots, x_n]$, $\alpha \in \mathbb{F}^*$ we have:

- $\dim(\partial^*(\alpha f)) = \dim(\partial^* f)$ ✓
- $$\dim\left(\partial^*\left(\sum_{i=1}^{k} f_i\right)\right) \leq \sum_{i=1}^{k} \dim\left(\partial^* f_i\right)$$ subadditive
- $$\dim\left(\partial^*\left(\prod_{i=1}^{k} f_i\right)\right) \leq \prod_{i=1}^{k} \dim\left(\partial^* f_i\right)$$

$\underbrace{x_i^2}_{1,\ x_i,\ x_i^2}$

have dependencies

$\dim(U+V) \leq \dim(U) + \dim(V)$

3

$\mu(x_i) \cdot \mu(x_i) = 2 \cdot 2$

Lower Bound

Theorem ([Nisan & Wigderson 1997])

Any depth-3 homogeneous circuit computing the elementary symmetric polynomial $E_{n,2d}$ must be of size

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

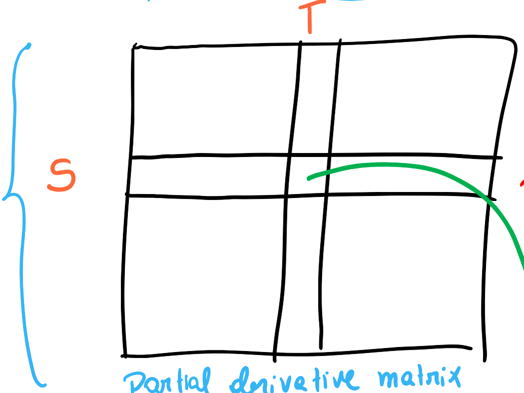
$$\mu\left(\prod_{i=1}^{2d} \ell_i\right) \leq \prod_{i=1}^{2d} \mu(\ell_i) = \prod_{i=1}^{2d} 2 = 2^{2d} = 4^d$$

- upper bound on measure for simple polynomials.

Lower Bounding $\mu(E_{n,2d})$

$$\dim\Big(\underbrace{\partial^{*}(E_{n,2d})}\Big) \geq \dim\Big(\partial^{=d}(E_{n,2d})\Big)$$

coeff of the polynomial



Partial derivative matrix

partial derivative

$S, T \subset \binom{[n]}{d}$

$\partial_S\, \alpha_{S,T} \cdot x_S x_T$

$= \alpha_{S,T} \cdot x_T$

coeff of $x_S \cdot x_T$ in $E_{n,2d}$

$x_S = \prod_{i \in S} x_i$

Lower Bounding $\mu(E_{n,2d})$

$2d = 2$

$$E_{3,2} = x_1x_2 + x_1x_3 + x_2x_3$$

$$\begin{array}{c|ccccccc}
 & \begin{matrix}x_1x_2\\1,2\end{matrix} & \begin{matrix}x_1x_3\\13\end{matrix} & \begin{matrix}x_2x_3\\23\end{matrix} & \begin{matrix}x_1\\1\end{matrix} & \begin{matrix}x_2\\2\end{matrix} & \begin{matrix}x_3\\3\end{matrix} & \begin{matrix}1\\\emptyset\end{matrix} \\
\hline
\emptyset & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
\{1\} & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
\{2\} & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
\{3\} & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
\{1,2\} & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
\{1,3\} & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
\{2,3\} & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}$$

$1\cdot x_1x_2 + 1x_1x_3 + 1\cdot x_2x_3$

$x_2 + x_3 = \partial_1 E_{3,2}$

$x_1 + x_3$

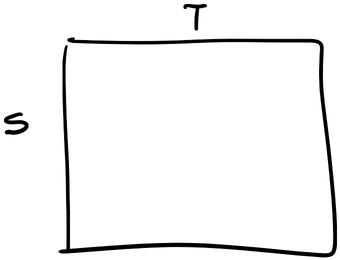
$\partial_3 E_{3,2} = x_1 + x_2$

M

$\mathrm{rank}(M) = \dim(\partial^* f) \geq \mathrm{rank}(\text{submatrix})$

Lower Bounding $\mu(E_{n,2d})$

Problem: rank submatrix



$|S| = |T| = d$

$S, T \in \binom{[n]}{d}$

Comm. complexity [Kushilevitz-Nisan]
Pages 23, 24

rank of this submatrix is full
(induction)

if $p \in \Sigma^{[s]} \Pi^{[2d]} \Sigma$ then

$$\mu(p) \le 4^d \cdot s$$

upper bd on measure

$$\mu(E_{n,2d}) \geq \binom{n}{d} \geq \left(\frac{n}{d}\right)^d$$

if $E_{n,2d} \in \Sigma^{[s]} \Pi^{[2d]} \Sigma$

then

$$\left(\frac{n}{d}\right)^d \le s \cdot 4^d \Rightarrow s \geq \left(\frac{n}{4d}\right)^d \quad \square$$

- “Natural” lower bound strategies
- Lower Bounds for Homogeneous Depth-3 Circuits
- Shifted Partial Derivatives and Depth-4 Circuits
- Conclusion
- Acknowledgements

Our Circuit Class

- Simple polynomials: powers of quadratics Q^d, where $Q \in \mathbb{F}[x_1, \dots, x_n]_2$

$Q = x_1x_2 + x_1x_3 + x_2x_3$

Q^d simple polynomials

Our Circuit Class

- Simple polynomials: powers of quadratics Q^d, where $Q \in \mathbb{F}[x_1, \ldots, x_n]_2$
- Sums of powers of quadratic polynomials:

$$\mathcal{C}(n, d, s) = \left\{ f \in \mathbb{F}[x_1, \ldots, x_n]_{2d} \mid f = \sum_{i=1}^{s} Q_i(x_1, \ldots, x_n)^d \right\}$$

where $Q_i \in \mathbb{F}[x_1, \ldots, x_n]_2$

Our Circuit Class

- Simple polynomials: powers of quadratics Q^d, where $Q \in \mathbb{F}[x_1, \ldots, x_n]_2$
- Sums of powers of quadratic polynomials:

$$\mathcal{C}(n, d, s) = \left\{ f \in \mathbb{F}[x_1, \ldots, x_n]_{2d} \mid f = \sum_{i=1}^{s} Q_i(x_1, \ldots, x_n)^d \right\}$$

  where $Q_i \in \mathbb{F}[x_1, \ldots, x_n]_2$
- Complexity measure?
  - dimension of partial derivatives won't work, as space of partial derivatives of Q^d could be as large as can be expected

Our Circuit Class

- Simple polynomials: powers of quadratics Q^d, where $Q \in \mathbb{F}[x_1, \ldots, x_n]_2$
- Sums of powers of quadratic polynomials:

$$\mathcal{C}(n,d,s) = \left\{ f \in \mathbb{F}[x_1, \ldots, x_n]_{2d} \mid f = \sum_{i=1}^{s} Q_i(x_1, \ldots, x_n)^d \right\}$$

  where $Q_i \in \mathbb{F}[x_1, \ldots, x_n]_2$
- Complexity measure?
  - dimension of partial derivatives won't work, as space of partial derivatives of Q^d could be as large as can be expected
  - *Observation:* k^{th} order partial derivative of Q^d is of the form $Q^{d-k}p$, where $p \in \mathbb{F}[x_1, \ldots, x_n]_k$.
  - small order partial derivatives share *large common factors*

Complexity Measure [Kayal 2012]

- Let $\partial^k f$ be the set of all k^{th} order partial derivatives of f
- $\mathbf{x}^{\leq \ell}$ be the set of all monomials of degree $\leq \ell$

$x_1 \quad x_1^2 \quad x_1^3 \ldots \quad x_1^{\ell}$

$x_1 x_2 \quad , \quad x_1^{\ell-1} x_2$

Complexity Measure [Kayal 2012]

- Let $\partial^k f$ be the set of all k^{th} order partial derivatives of f
- $\mathbf{x}^{\leq \ell}$ be the set of all monomials of degree $\leq \ell$
- The *shifted partials* measure of f, denoted

$$\mu_{k,\ell}(f) = \dim(\mathrm{span}(\underbrace{\mathbf{x}^{\leq \ell}} \cdot \underbrace{\partial^k f}))$$

$$Q = (x_1x_2 + x_2x_3 + x_1x_3)^{d}$$

$$\mathrm{span}\left\{ \begin{array}{l} x^m \cdot (x_2+x_3)Q^{d-1} \cdot d \\ x^m \cdot (x_1+x_3)Q^{d-1} \cdot d \\ x^m \quad (x_1+x_2)Q^{d-1} \cdot d \end{array} \right\}$$

$$m = (m_1, \ldots, m_n)$$

$$\sum m_i \leq \ell$$

Complexity Measure [Kayal 2012]

- Let $\partial^k f$ be the set of all k^{th} order partial derivatives of f
- $\mathbf{x}^{\leq \ell}$ be the set of all monomials of degree $\leq \ell$
- The *shifted partials* measure of f, denoted

$$\mu_{k,\ell}(f) = \dim(\mathrm{span}(\mathbf{x}^{\leq \ell} \cdot \partial^k f))$$

Lemma (Simple polynomials have small measure)

If $f = Q^d$ where Q is a quadratic, then

$$\mu(f) \leq \binom{n+k+\ell}{n}$$

which is the number of monomials of degree $\leq k + \ell$ in n variables.

Complexity Measure [Kayal 2012]

- Let $\partial^k f$ be the set of all k^{th} order partial derivatives of f
- $\mathbf{x}^{\leq \ell}$ be the set of all monomials of degree $\leq \ell$
- The *shifted partials* measure of f, denoted

$$\mu_{k,\ell}(f) = \dim(\text{span}(\mathbf{x}^{\leq \ell} \cdot \partial^k f))$$

Lemma (Simple polynomials have small measure)

If $f = Q^d$ where Q is a quadratic, then

$$\mu(f) \leq \binom{n+k+\ell}{n}$$

which is the number of monomials of degree $\leq k + \ell$ in n variables.

- This measure has an algebro-geometric meaning (see Affine Hilbert function of an ideal)

Proof of Lemma

$|\bar{u}| \le \ell$

$Q \quad , \quad |S| = k$

$$\boxed{\partial_S Q^d} = \alpha_k \cdot Q^{d-k} \cdot \underbrace{\bar{X}^{\bar{m}}} \cdot \bar{x}^{\bar{u}} = Q^{d-k} \cdot \bar{x}^{\bar{m}+\bar{u}}$$

$|\bar{m}| = k = \sum_{i=1}^{n} m_i$

$\underbrace{|\bar{m}+\bar{u}|} \le k+\ell$

$= |\bar{m}| + |\bar{u}|$

$$\text{span}\left\{ \boxed{Q^{d-k} \cdot \bar{X}^{\bar{e}}} \right\} \supset \underline{\bar{X}^{\le \ell} \partial^k (Q^d)}$$

$|\bar{e}| = k+\ell$

$$\Rightarrow \dim\left(\bar{X}^{\le \ell} \partial^k (Q^d)\right) \le \#\,\text{monomials of } x_1, \ldots, x_n \text{ of degree} \le k+\ell = \binom{n+k+\ell}{n}$$

Lower Bound

Theorem ([Kayal 2012])

The monomial $x_1 x_2 \cdots x_n$ has complexity $2^{\Omega(n)}$ in the model of sums of powers of quadratics.

hard polynomial : $x_1 x_2 \cdots x_n$

Lower Bound

Theorem ([Kayal 2012])

The monomial $x_1 x_2 \cdots x_n$ has complexity $2^{\Omega(n)}$ in the model of sums of powers of quadratics.

- Lower bound $\mu_{k\ell}(x_1 \cdots x_n) \geq \underbrace{\binom{n}{k}}_{\text{\# sets of size } k} \cdot \underbrace{\binom{n-k+\ell}{\ell}}_{\text{\# monomials in } [n]\setminus S \text{ of deg.} \leq \ell}$

$S \subset [n]$ $\quad |S| = k$ $\quad$ (to take derivative)

$$\partial_S (x_1 \cdots x_n) = \underbrace{x_{[n]\setminus S} \cdot \left(\begin{array}{c}\text{monomials over}\\ \text{variables in } [n]\setminus S\\ \text{of degree} \leq \ell\end{array}\right)}_{\text{don't change support}}$$

for each $\underline{S}$ we get $\geq \binom{n-k+\ell}{\ell}$

Lower Bound

Theorem ([Kayal 2012])

The monomial $x_1 x_2 \cdots x_n$ has complexity $2^{\Omega(n)}$ in the model of sums of powers of quadratics.

- Lower bound $\mu_{k\ell}(x_1 \cdots x_n) \geq \binom{n}{k} \cdot \binom{n-k+\ell}{\ell}$
- Parameters: $\ell = 2n$, $k = \epsilon \cdot n/2$

$$x_1 \cdots x_n = \sum_{i=1}^{s} Q_i^d \qquad d = n/2$$

$$\underbrace{s \cdot \binom{n+k+\ell}{n}}_{\text{upper bd on simples}} \geq \underbrace{\binom{n}{k}\binom{n-k+\ell}{\ell}}_{\text{lower bd on hard polynomial}}$$

Conclusion

- Today we learned that constant depth circuits are essentially as general as general algebraic circuits
- Natural approaches to prove lower bounds on circuit classes
- Use of partial derivatives as a complexity measure
- Shifted partial derivatives

Acknowledgement

- Lecture based largely on:
  - Survey [Saptharishi, Chapters 7 & 13]
  - Survey [Chen, Kayal & Wigderson 2010]
  - Paper [Kayal 2012]

References I

Nisan, Noam and Wigderson, Avi 1997.
Lower Bounds on Arithmetic Circuits via Partial Derivatives
Computational Complexity

Kayal, Neeraj 2012.
An exponential lower bound for the sum of powers of bounded degree polynomials
Electronic Colloquium of Computational Complexity

Chen, Xi and Kayal, Neeraj and Wigderson, Avi 2010.
Partial Derivatives in Arithmetic Complexity and Beyond
Foundations and Trends in Theoretical Computer Science

Saptharishi, Ramprasad.
Lower Bounds in Algebraic Complexity
Github