Lecture 5: Barriers to Lower Bound Techniques & Algebraic Natural Proofs

Rafael Oliveira

University of Waterloo
Cheriton School of Computer Science

rafael.oliveira.teaching@gmail.com

January 25, 2021

Overview

- Lower bound approaches - Rank Methods
- Barriers to Rank Methods
- Algebraic Natural Proofs & Succinct PIT
- Conclusion
- Acknowledgements

Lower Bound Approach

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 $\mathcal{S}$

$$\Phi \in \mathcal{C}(s) \implies \Phi = \underline{f_1 + \cdots + f_s}$$

$$f_i \in \mathcal{S}$$

Can think of class $\mathcal{C}$ as $\mathcal{S}$-complexity

Lower Bound Approach

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 $\mathcal{S}$

Lower Bound Approach

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 $\mathcal{S}$

Lower Bound Approach

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

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

Lower Bound Approach

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 $\mathcal{S}$
    - $\mu(f)$ 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 } constructible
4. *Hard polynomial:* find polynomial p such that $\mu(p)$ is large

Lower Bound Approach

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 $f \in \mathcal{S}$ $\mu(S) \leq U$

Lower Bound Approach

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

$$q = f_1 + f_2 + \cdots + f_s, \quad f_i \in \mathcal{S}$$

$$\mu(q) = \mu(f_1 + \cdots + f_s) \leq \mu(f_1) + \cdots + \mu(f_s)$$
$$\leq s \cdot U$$

Lower Bound Approach

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
$$q = f_1 + f_2 + \cdots + f_s, \quad f_i \in \mathcal{S}$$
- $\mu(p) \geq L$ and p can be computed by size s in $\mathcal{C} \Rightarrow s \cdot U \geq L$

Common aspects of complexity measures - rank methods

1. Most used complexity measures are *partial derivatives* based

Common aspects of complexity measures - rank methods

1. Most used complexity measures are *partial derivatives* based
2. Dimension of span of: partial derivatives, shifted partial derivatives

hom-$\Sigma\Pi\Sigma$ hom-$\Sigma\wedge^d\Sigma\Pi^2$

Common aspects of complexity measures - rank methods

1. Most used complexity measures are *partial derivatives* based
2. Dimension of span of: partial derivatives, shifted partial derivatives
3. Can be cast as *ranks of special matrices*:

$$f+g \longmapsto L(f+g) = L(f) + L(g)$$

$$L : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{F}^{m \times m} \qquad \text{linear map}$$

$$f \longmapsto L(f) = L(\mathrm{coeff}(f))$$

$$\mu : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{N} \qquad \mu(f) = \mathrm{rank}(L(f))$$

$$f(x_1, x_2, x_3, x_4) = E_{4,3} = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4$$

	x_1x_2	x_1x_3	x_1x_4	x_2x_3	x_2x_4	x_3x_4
x_1	0	0	0	1	1	1
x_2	0	1	1	0	0	1
x_3						
x_4						

Common aspects of complexity measures - rank methods

1. Most used complexity measures are *partial derivatives* based
2. Dimension of span of: partial derivatives, shifted partial derivatives
3. Can be cast as *ranks of special matrices*:

$$L : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{F}^{m \times m} \qquad \text{linear map}$$

$$\mu : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{N} \qquad \mu(f) = \mathrm{rank}(L(f))$$

4. Sub-additivity comes from sub-additivity of rank

$$\mathrm{rank}(A+B) \leq \mathrm{rank}(A) + \mathrm{rank}(B)$$

Common aspects of complexity measures - rank methods

1. Most used complexity measures are *partial derivatives* based
2. Dimension of span of: partial derivatives, shifted partial derivatives
3. Can be cast as *ranks of special matrices*:

$$L : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{F}^{m \times m} \qquad \text{linear map}$$

$$\mu : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{N} \qquad \mu(f) = \mathrm{rank}(L(f))$$

4. Sub-additivity comes from sub-additivity of rank
5. Examples:
   - dimension of partial derivatives $\to$ rank of partial derivative matrix
   - dimension of shifted paritals $\to$ same as above
   - Flattenings used in tensor rank lower bounds $\to$ flattening is such a matrix map!

Partial derivatives method as rank method

- Lower bound approaches - Rank Methods
- Barriers to Rank Methods
- Algebraic Natural Proofs & Succinct PIT
- Conclusion
- Acknowledgements

What is a barrier?

- Given a class of simple polynomials $\mathcal{S}$, let $c_{\mathcal{S}}(p)$ be the *$\mathcal{S}$-complexity* of polynomial p - that is, the min s such that

$$p = f_1 + \ldots , f_s, \quad f_i \in \mathcal{S}$$

What is a barrier?

- Given a class of simple polynomials $\mathcal{S}$, let $c_{\mathcal{S}}(p)$ be the *$\mathcal{S}$-complexity* of polynomial p - that is, the min s such that

$$p = f_1 + \ldots, f_s, \quad f_i \in \mathcal{S}$$

- Assume that $\mathcal{S}$ is *complete* – that is, any polynomial in $\mathbb{F}[x_1, \ldots, x_n]$ can be computed by the span of polynomials in $\mathcal{S}$

$S = \{ \prod_{i=1}^{d} \ell_i \mid$ linear forms of degree $d \}$

$x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ where $e_1 + \cdots + e_n = d$

$\in S$

know there are hard poly $\mathbb{F}[x_1, \ldots, x_n]_d$

Barrier: if $\mu(f)$ small $\forall f \in S$ then $\mu(p)$ is not too large for any polynomial in $\mathbb{F}[x_1, \ldots, x_n] = \mathrm{span}(S)$

What is a barrier?

- Given a class of simple polynomials $\mathcal{S}$, let $c_{\mathcal{S}}(p)$ be the *$\mathcal{S}$-complexity* of polynomial p - that is, the min s such that

$$p = f_1 + \ldots, f_s, \quad f_i \in \mathcal{S}$$

- Assume that $\mathcal{S}$ is *complete* – that is, any polynomial in $\mathbb{F}[x_1, \ldots, x_n]$ can be computed by the span of polynomials in $\mathcal{S}$
- Let $\underline{\Delta_{\mathcal{S}}}$ be set of all sub-additive measures over $\mathcal{S}$

all possible lower bound techniques (that we are considering)

What is a barrier?

- Given a class of simple polynomials $\mathcal{S}$, let $c_{\mathcal{S}}(p)$ be the *$\mathcal{S}$-complexity* of polynomial p - that is, the min s such that

$$p = f_1 + \dots, f_s, \quad f_i \in \mathcal{S}$$

- Assume that $\mathcal{S}$ is *complete* – that is, any polynomial in $\mathbb{F}[x_1, \dots, x_n]$ can be computed by the span of polynomials in $\mathcal{S}$
- Let $\Delta_{\mathcal{S}}$ be set of all sub-additive measures over $\mathcal{S}$
- $c_{\mathcal{S}} \in \Delta_{\mathcal{S}}$, but it is hard to understand

$$c_S(p+q) \le c_S(p) + c_S(q)$$

$$p = f_1 + \dots + f_r \qquad r = c_S(p)$$

$$q = g_1 + \dots + g_t \qquad t = c_S(q)$$

What is a barrier?

- Given a class of simple polynomials $\mathcal{S}$, let $c_{\mathcal{S}}(p)$ be the *$\mathcal{S}$-complexity* of polynomial p - that is, the min s such that

$$p = f_1 + \ldots, f_s, \quad f_i \in \mathcal{S}$$

- Assume that $\mathcal{S}$ is *complete* – that is, any polynomial in $\mathbb{F}[x_1, \ldots, x_n]$ can be computed by the span of polynomials in $\mathcal{S}$
- Let $\Delta_{\mathcal{S}}$ be set of all sub-additive measures over $\mathcal{S}$
- $c_{\mathcal{S}} \in \Delta_{\mathcal{S}}$, but it is hard to understand
- Let $\Delta \subset \Delta_{\mathcal{S}}$ subset of measures (simpler to understand, reason about) (set of techniques)

$\Delta \leftarrow$ rank methods
(very easy to analyze)

What is a barrier?

- Given a class of simple polynomials $\mathcal{S}$, let $c_{\mathcal{S}}(p)$ be the *$\mathcal{S}$-complexity* of polynomial p - that is, the min s such that

$$p = f_1 + \ldots, f_s, \quad f_i \in \mathcal{S}$$

- Assume that $\mathcal{S}$ is *complete* – that is, any polynomial in $\mathbb{F}[x_1, \ldots, x_n]$ can be computed by the span of polynomials in $\mathcal{S}$
- Let $\Delta_{\mathcal{S}}$ be set of all sub-additive measures over $\mathcal{S}$
- $c_{\mathcal{S}} \in \Delta_{\mathcal{S}}$, but it is hard to understand
- Let $\Delta \subset \Delta_{\mathcal{S}}$ subset of measures (simpler to understand, reason about) (set of techniques)
- A *barrier* for the subset $\boxed{\Delta}$ is a statement of the following kind:

  If $\underline{\mu \in \Delta}$ and $\underline{\mu(f)}$ is small for every $f \in \mathcal{S}$, then it is small for every $\underline{p \in \mathbb{F}[x_1, \ldots, x_n]}$

$\mu(p) / \mu(s)$ small (this ratio is our lower bound)

What is a barrier?

- Given a class of simple polynomials $\mathcal{S}$, let $c_{\mathcal{S}}(p)$ be the *$\mathcal{S}$-complexity* of polynomial p - that is, the min s such that

$$p = f_1 + \ldots, f_s, \quad f_i \in \mathcal{S}$$

- Assume that $\mathcal{S}$ is *complete* – that is, any polynomial in $\mathbb{F}[x_1, \ldots, x_n]$ can be computed by the span of polynomials in $\mathcal{S}$
- Let $\Delta_{\mathcal{S}}$ be set of all sub-additive measures over $\mathcal{S}$
- $c_{\mathcal{S}} \in \Delta_{\mathcal{S}}$, but it is hard to understand
- Let $\Delta \subset \Delta_{\mathcal{S}}$ subset of measures (simpler to understand, reason about) (set of techniques)
- A *barrier* for the subset Δ is a statement of the following kind:

  If $\mu \in \Delta$ and $\mu(f)$ is small for every $f \in \mathcal{S}$, then it is small for every $p \in \mathbb{F}[x_1, \ldots, x_n]$
- The above would rule out even *non-explicit* lower bounds!

Barriers to rank methods

- Let $\mathcal{S}$ be the class of powers of linear forms (Waring Rank)

$$S = \{ (a_1 x_1 + \cdots + a_n x_n)^d \mid (a_1, \ldots, a_n) \in \mathbb{F}^n \}$$

S is complete

write any monomial in span(S)

Barriers to rank methods

- Let $\mathcal{S}$ be the class of powers of linear forms ✓ (Waring Rank)
- A simple dimension count over $\boxed{\mathbb{F}[x_1, \ldots, x_n]_d}$ shows us that we must have polynomials requiring n^{d-1}

simple polynomials

$$n^d \approx \binom{n+d-1}{n-1} = \text{dim polys of deg } d$$

n vars

$$\sum_{\ell=1}^{t} \underbrace{(a_{\ell 1} x_1 + \cdots + a_{\ell n} x_n)}_{n \text{ degrees of freedom}}^{d}$$

$$\boxed{t \approx n^{d-1}}$$

$n \cdot t \approx n^d$

match degrees of freedom

Barriers to rank methods

- Let $\mathcal{S}$ be the class of powers of linear forms (Waring Rank)
- A simple dimension count over $\mathbb{F}[x_1, \ldots, x_n]_d$ shows us that we must have polynomials requiring n^{d-1}
- Easy to find explicit polynomial with $n^{d/2}$ Waring Rank

Practice problem

Barriers to rank methods

- Let $\mathcal{S}$ be the class of powers of linear forms (Waring Rank)
- A simple dimension count over $\mathbb{F}[x_1, \ldots, x_n]_d$ shows us that we must have polynomials requiring n^{d-1}
- Easy to find explicit polynomial with $n^{d/2}$ Waring Rank

Theorem ([Efremenko et al. 2018])

Rank methods cannot prove lower bounds better than $n^{d/2}$ for Waring Rank.

take easiest lower bd rank method
this is as good as any rank method
cannot give you non-trivial lower bds

Barriers to rank methods

- Let $\mathcal{S}$ be the class of powers of linear forms (Waring Rank)
- A simple dimension count over $\mathbb{F}[x_1, \ldots, x_n]_d$ shows us that we must have polynomials requiring n^{d-1}
- Easy to find explicit polynomial with $n^{d/2}$ Waring Rank

really weak

Theorem ([Efremenko et al. 2018])

Rank methods cannot prove lower bounds better than $n^{d/2}$ for Waring Rank.

- Note that this implies a barrier for depth-3 circuits as well!

S ← Waring rank

T ← hom. depth 3

S weaker than T

Barrier for Waring Rank - Symbolic Rank

- Going from generic rank to symbolic rank

$$L\left((a_1x_1+\cdots+a_nx_n)^d\right) \longrightarrow M(a_1,\ldots,a_n)$$

a_1^d

$\mathrm{rank}(M(a_1,\ldots,a_n)) \leq r$

$\forall (a_1,\ldots,a_n) \in \mathbb{F}^n$

measure is small for any element in S

symbolic matrix

$$M(y_1,\ldots,y_n) = \sum_{|\bar{e}|=d} M_{\bar{e}}\, \bar{y}^{\bar{e}}$$

polynomial matrix homogeneous of degree d

$M_{(d,0,\ldots,0)} \cdot y_1^d + \cdots$

$\mathrm{rank}_{\mathbb{F}(y)}(M(y)) \leq r$

$\det(M(y)) \neq 0$

$\Rightarrow M(\bar{a})$ invertible

Symbolic Rank to Small Decomposition

- Small symbolic rank $\Rightarrow$ small decomposition in field of fractions

$$M(\bar{y}) \qquad \mathrm{rank}_{\mathbb{F}(\bar{y})}\left(M(\bar{y})\right) \leq r$$

$$M(\bar{y}) = A(\bar{y}) \cdot B(\bar{y}) \qquad A \in \mathbb{F}(\bar{y})^{m \times r}, \quad B \in \mathbb{F}(\bar{y})^{r \times m}$$

$$M(\bar{y}) = \sum_{i=1}^{r} \frac{1}{g_i(\bar{y})} \cdot \underbrace{\vec{u}_i(\bar{y}) \cdot \vec{v}_i(\bar{y})^T}_{\text{rank-1 decompositions}}$$

$$g_i(\bar{y}) \in \mathbb{F}[\bar{y}] \qquad \vec{u}_i, \vec{v}_i \in \mathbb{F}[\bar{y}]^m$$

From field of fractions to polynomials

- From field of fractions decomposition, obtain small polynomial matrix decomposition

$$M(\bar{y}) = \sum_{i=1}^{r} \vec{u}_i(\bar{y}) \cdot \vec{v}_i(\bar{y})^T$$

polynomial vectors

Grouping elements based on degree

- Each rank-1 polynomial matrix can be broken down into pieces of degree $\leq d/2$

degree d

$$M(\bar{y}) = \sum_{i=1}^{r} \underbrace{\vec{u}_i(\bar{y})}\ \underbrace{\vec{v}_i(\bar{y})}^T$$

homogeneous polynomials

$$= \sum_{|\bar{e}|=d} M_{\bar{e}} \cdot \bar{y}^{\bar{e}}$$

$\mathbb{F}^{m \times m}$

$$\begin{pmatrix} u_{i1}(\bar{y}) \\ \vdots \\ u_{im}(\bar{y}) \end{pmatrix} \qquad \begin{pmatrix} v_{i1}(\bar{y}) \\ \vdots \\ v_{im}(\bar{y}) \end{pmatrix}$$

same degree k

same degree $d-k$

$k \leq d-k \quad (k \leq d/2)$

Upper bound on generic rank

- Note that we can break up any matrix in the form $L \times \mathbb{F}^m + \mathbb{F}^m \times L'$

$$\sum M_{\bar{e}} \bar{y}^{\bar{e}} = \boxed{M(y)} = \sum_{i=1}^{r} \underbrace{u_i(\bar{y})}_{\deg \leq \frac{d}{2}} \underbrace{v_i(\bar{y})^T}_{\deg \geq d/2}$$

$$= \sum_{i=1}^{r} \Big(\sum_{|\bar{a}|=k} \bar{y}^{\bar{a}} \cdot \underbrace{u_{i\bar{a}}}_{\uparrow\ \mathbb{F}^m} \Big) v_i(\bar{y})^T$$

$$\begin{pmatrix} xy \\ x^2 \end{pmatrix} = xy \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + x^2 \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$n^{d/2}$$

$$\downarrow$$

$$U = \{ u_{i\bar{a}} \} \qquad \dim(\mathrm{span}(U)) \leq \# U \leq r \cdot \begin{pmatrix} \#\text{mon.} \\ \deg \\ \leq d/2 \end{pmatrix}$$

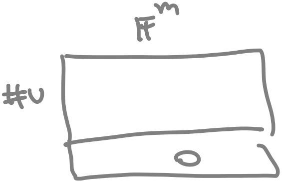
Barrier

- Linearity now bounds the rank of *any* matrix in image of map!

$$\underline{\sum M_{\bar e}\, \bar y^{\bar e}} = \sum_{i=1}^{r} \sum_{|\bar a| \le d/2} \bar y^{\bar a} \cdot u_{i\bar a}\, v_i(\bar y)^T$$

$U \subset \mathbb{F}^m$

$$\Rightarrow M_{\bar e} = \sum \underbrace{u_{i\bar a}}_{\in U} \cdot \underbrace{v_{i\bar a}^T}_{\text{anything}} \subset \mathrm{span}(U) \otimes \mathbb{F}^m$$



$\Rightarrow$ all $M_{\bar e}$ and linear combinations have low rank!

Barrier

$$f = \sum f_{\bar{e}} \bar{x}^{\bar{e}}$$

$$L(f) = \sum f_{\bar{e}} \cdot \mu_{\bar{e}}$$

$$\text{rank}\left(\sum \alpha_{\bar{e}} \mu_{\bar{e}} \right) \leq \dim(U) \leq r \cdot n^{d/2}$$

$$\Rightarrow \mu(f) \leq r \cdot n^{d/2} \quad \text{upper bd}$$

on measure for <u>any</u> polynomial f.

$$\frac{\mu(f)}{\mu(S)} \leq \frac{r \cdot n^{d/2}}{r} = n^{d/2}.$$

$$L : \mathbb{F}[\bar{x}]_d \longrightarrow \mathbb{F}^{m\times m}$$

$$\underline{\text{linear}}$$

$$L(\bar{x}^{\bar{e}}) = M_{\bar{e}}$$

$$M(\bar{y}) = L\left((y_1x_1 + \dots + y_nx_n)^d\right) =$$

$$= \underbrace{\sum_{|\bar{e}|=d} \bar{y}^{\bar{e}} \cdot \underset{\mathbb{F}}{\underset{\in}{(\quad)}} \cdot \underset{\mathbb{F}^{m\times m}}{\underset{\in}{M_{\bar{e}}}}}_{\text{degree } d}$$

- Lower bound approaches - Rank Methods
- Barriers to Rank Methods
- Algebraic Natural Proofs & Succinct PIT
- Conclusion
- Acknowledgements

Natural Proofs [Razborov & Rudich 1997]

- To prove (boolean) lower bounds, want to find property P such that

Natural Proofs [Razborov & Rudich 1997]

- To prove (boolean) lower bounds, want to find property P such that
  1. P is *useful*: any "easy" boolean function has such property

Natural Proofs [Razborov & Rudich 1997]

- To prove (boolean) lower bounds, want to find property P such that
  1. P is *useful*: any "easy" boolean function has such property
  2. *Largeness*: random functions do not have property P, with high probability

Natural Proofs [Razborov & Rudich 1997]

- To prove (boolean) lower bounds, want to find property P such that
  1. P is *useful*: any "easy" boolean function has such property
  2. *Largeness*: random functions do not have property P, with high probability
  3. *Constructive*: given truth table of boolean function f of size $N = 2^n$, decide in poly(N)-time if f has property P

Natural Proofs [Razborov & Rudich 1997]

- To prove (boolean) lower bounds, want to find property P such that
  1. P is *useful*: any "easy" boolean function has such property
  2. *Largeness*: random functions do not have property P, with high probability
  3. *Constructive*: given truth table of boolean function f of size $N = 2^n$, decide in poly(N)-time if f has property P
- Most boolean function lower bounds (that we can prove) have these three properties

Natural Proofs [Razborov & Rudich 1997]

- To prove (boolean) lower bounds, want to find property P such that

natural proofs

  1. P is *useful*: any "easy" boolean function has such property
  2. *Largeness*: random functions do not have property P, with high probability
  3. *Constructive*: given truth table of boolean function f of size $N = 2^n$, decide in poly(N)-time if f has property P
- Most boolean function lower bounds (that we can prove) have these three properties
- In [Razborov & Rudich 1997] they show that (under cryptographic assumptions) natural proofs *cannot* yield super-polynomial boolean circuit lower bounds!
  - would contradict existence of cryptographic pseudorandom functions.

Algebraic Natural Proofs [Forbes & Shpilka & Volk 2018, Grochow et al. 2017]

- What would be an algebraic "natural" proof?

  Property P given by an *algebraic variety* that is $\underbrace{\textit{easy to compute}}_{\text{constructive}}$: that is matrix $M : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{F}^{m\times m}$ such that

$$p \text{ has property P} \Leftrightarrow \underbrace{\det(M(\mathit{coeff}(p))) = 0}$$

$$f = \sum f_{\bar{e}} \bar{x}^{\bar{e}} \longmapsto \underbrace{\sum f_{\bar{e}} M_{\bar{e}}}_{M(\mathrm{coeff}(f))}$$

easy poly $\in V(\det(M(\bar{y})))$

find hard poly outside

Algebraic Natural Proofs [Forbes & Shpilka & Volk 2018, Grochow et al. 2017]

- What would be an algebraic "natural" proof?

  Property P given by an *algebraic variety* that is *easy to compute*: that is matrix $M : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{F}^{m \times m}$ such that

  $$p \text{ has property P} \Leftrightarrow \det(M(\mathit{coeff}(p))) = 0$$

- Properties of an algebraic natural proof:
  1. *Useful*: for easy polynomials, $M(\mathit{coeff}(p))$ is singular

Algebraic Natural Proofs [Forbes & Shpilka & Volk 2018, Grochow et al. 2017]

- What would be an algebraic "natural" proof?

  Property P given by an *algebraic variety* that is *easy to compute*: that is matrix $M : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{F}^{m \times m}$ such that

  $m = \mathrm{poly}(N)$

  $$p \text{ has property P} \Leftrightarrow \det(M(\mathit{coeff}(p))) = 0$$

- Properties of an algebraic natural proof:
  1. *Useful*: for easy polynomials, $M(\mathit{coeff}(p))$ is singular
  2. *Constructive*: one can decide in time poly(N)-time whether p has property P.

     $\binom{n+d}{d}$

     This amounts to being able to compute $\det(M((\mathit{coeff}(p)))$, which is poly($N$)-size if $\dim(M) = \mathrm{poly}(N)$.

Algebraic Natural Proofs [Forbes & Shpilka & Volk 2018, Grochow et al. 2017]

- What would be an algebraic "natural" proof?

  Property P given by an *algebraic variety* that is *easy to compute*: that is matrix $M : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{F}^{m \times m}$ such that

  $$p \text{ has property P} \Leftrightarrow \det(M(\mathit{coeff}(p))) = 0$$

- Properties of an algebraic natural proof:
  1. *Useful*: for easy polynomials, $M(\mathit{coeff}(p))$ is singular
  2. *Constructive*: one can decide in time poly(N)-time whether p has property P.

     This amounts to being able to compute $\det(M((\mathit{coeff}(p)))$, which is poly($N$)-size if $\dim(M) = \text{poly}(N)$.
  3. *Largeness*: Most polynomials are hard.
     This is *intrinsic* in the case of polynomials, since we know that the zero set of an algebraic variety has *measure zero*.

Algebraic Natural Proofs - Definition

- Let $\mathcal{C} \subset \mathbb{F}[x_1, \ldots, x_n]$ be a circuit class

Algebraic Natural Proofs - Definition

- Let $\mathcal{C} \subset \mathbb{F}[x_1, \ldots, x_n]$ be a circuit class
- Let $\mathcal{D} \subset \mathbb{F}[\underline{coeff(\mathcal{C})}]$ be another circuit class

$$f(\bar{x}) = \sum y_{\bar{e}} \bar{x}^{\bar{e}}$$

variables of coeff $(\mathcal{C})$

Algebraic Natural Proofs - Definition

- Let $\mathcal{C} \subset \mathbb{F}[x_1, \ldots, x_n]$ be a circuit class
- Let $\mathcal{D} \subset \mathbb{F}[coeff(\mathcal{C})]$ be another circuit class
- A polynomial $D \in \mathcal{D}$ (distinguisher) is a *algebraic natural proof* against $\mathcal{C}$ if
  1. $D \not\equiv 0$
  2. $D(coeff(f)) = 0$ for all $f \in \mathcal{C}$

$ax^2 + bxy + c$

$\mathcal{C} \subset V(D)$

$\mathcal{C} \subset \mathbb{F}[x, y]_2$ squares $(\alpha x + \beta y)^2$

$\mathcal{D} = \{ b^2 - 4ac \}$ $\qquad$ $\mathcal{C} \subset V(b^2 - 4ac)$

Algebraic Natural Proofs - Definition

- Let $\mathcal{C} \subset \mathbb{F}[x_1, \ldots, x_n]$ be a circuit class
- Let $\mathcal{D} \subset \mathbb{F}[coeff(\mathcal{C})]$ be another circuit class
- A polynomial $D \in \mathcal{D}$ (distinguisher) is a *algebraic natural proof* against $\mathcal{C}$ if
    1. $D \not\equiv 0$
    2. $D(coeff(f)) = 0$ for all $f \in \mathcal{C}$

Open Question (Existence of natural proofs)

Is VP a natural proof for VP?

$\mathcal{C} = VP$

$\mathcal{D} = VP$
$T(\bar{y})$

$VP(\bar{x}) \subset V(T)$
?

Algebraic Natural Proofs - Definition

- Let $\mathcal{C} \subset \mathbb{F}[x_1, \ldots, x_n]$ be a circuit class
- Let $\mathcal{D} \subset \mathbb{F}[coeff(\mathcal{C})]$ be another circuit class
- A polynomial $D \in \mathcal{D}$ (distinguisher) is a *algebraic natural proof* against $\mathcal{C}$ if
  1. $D \not\equiv 0$
  2. $D(coeff(f)) = 0$ for all $f \in \mathcal{C}$

Open Question (Existence of natural proofs)

Is VP a natural proof for VP?

- Question above is open even under any assumptions.

Algebraic Natural Proofs - Definition

- Let $\mathcal{C} \subset \mathbb{F}[x_1, \ldots, x_n]$ be a circuit class
- Let $\mathcal{D} \subset \mathbb{F}[coeff(\mathcal{C})]$ be another circuit class
- A polynomial $D \in \mathcal{D}$ (distinguisher) is a *algebraic natural proof* against $\mathcal{C}$ if
  1. $D \not\equiv 0$
  2. $D(coeff(f)) = 0$ for all $f \in \mathcal{C}$

Open Question (Existence of natural proofs)

Is VP a natural proof for VP?

- Question above is open even under any assumptions.
- In [KRST'20] the authors proved that if Per requires circuits of exponential size, then VP is *not* an algebraic natural proof against VNP.

When will a natural proof fail? Succinct Hitting sets

$\mathcal{C} \leftarrow$ easy polynomials

$\mathcal{D} \subset \mathbb{F}[\mathrm{coeff}(\mathcal{C})] \leftarrow$ distinguisher

$\mathcal{D}$ is NOT algebraic natural proof against $\mathcal{C}$

$\iff \forall D \in \mathcal{D} \quad \exists f \in \mathcal{C}$ s.t.

$D(\mathrm{coeff}(f)) \not\equiv 0$

$\iff \mathcal{C}$ is hitting set for $\mathcal{D}$

$\mathcal{H} = \{\mathrm{coeff}(f) : f \in \mathcal{C}\}$

Succinct Hitting Sets

- Lower bound approaches - Rank Methods
- Barriers to Rank Methods
- Algebraic Natural Proofs & Succinct PIT
- **Conclusion**
- Acknowledgements

Conclusion

- Today we learned about barriers to lower bound techniques
- Saw barriers to proving non-trivial Waring Rank

Conclusion

- Today we learned about barriers to lower bound techniques
- Saw barriers to proving non-trivial Waring Rank
- Lots of open questions left
  1. Can we improve our barriers to better bounds and rule out method of shifted partial derivatives?
  2. What are the connections between this line of work and *cactus rank* of varieties?
  3. More generally, can other notions of rank help us in proving lower bounds?

Conclusion

- Today we learned about barriers to lower bound techniques
- Saw barriers to proving non-trivial Waring Rank
- Lots of open questions left
  1. Can we improve our barriers to better bounds and rule out method of shifted partial derivatives?
  2. What are the connections between this line of work and *cactus rank* of varieties?
  3. More generally, can other notions of rank help us in proving lower bounds?
- Algebraic Natural Proofs
- Existence of algebraic natural proofs implies it may be harder to find succinct hitting sets (so PIT may have to be solved using more complex methods)
- Relationship between algebraic natural proofs and problems in algebraic geometry?

Acknowledgement

- Lecture based largely on:
  - [Efremenko et al. 2018]
  - [Forbes & Shpilka & Volk 2018]

References I

Efremenko, Klim and Garg, Ankit and Oliveira, Rafael and Wigderson, Avi 2018.
Barriers for Rank Methods in Arithmetic Complexity
ITCS

Forbes, Michael and Shpilka, Amir and Volk, Ben Lee 2018.
Succinct Hitting Sets and Barriers to Proving Lower Bounds for Algebraic Circuits
Theory of Computing

Grochow, Joshua and Kumar, Mrinal and Saks, Michael and Saraf, Shubhangi 2017.
Towards an algebraic natural proofs barrier via polynomial identity testing
Manuscript

Razborov, Alexander and Rudich, Steven 1997.
Natural Proofs
Journal of Computer and System Sciences

References II

Garg, Ankit and Makam, Visu and Oliveira, Rafael and Wigderson, Avi 2019.
More barriers to rank methods, via a "numeric to symbolic" transfer
2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)

Gałazka, Maciej 2017
Vector bundles give equations of cactus varieties
Linear Algebra and its Applications