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 $S$
2. *Normal form*: every circuit from circuit class $C$ can be expressed as small sum of simple polynomials in $S$

\[ \Phi \in \mathcal{C}(S) \Rightarrow \Phi = f_1 + \ldots + f_s \]

\[ f_i \in S \]

Can think of class $C$ as $S$-complexity
Lower Bound Approach

1. Define class of simple polynomials $S$

2. *Normal form:* every circuit from circuit class $C$ can be expressed as small sum of simple polynomials in $S$

3. *Complexity Measure:* find sub-additive complexity measure $\mu : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{N}$ which captures the simplicity of $S$
Lower Bound Approach

1. Define class of simple polynomials \( S \)

2. **Normal form**: every circuit from circuit class \( C \) can be expressed as small sum of simple polynomials in \( S \)

3. **Complexity Measure**: find sub-additive complexity measure \( \mu : \mathbb{F}[x_1, \ldots, x_n] \rightarrow \mathbb{N} \) which captures the simplicity of \( S \)
   - \( \mu(f) \) small for all polynomials in \( S \)
Lower Bound Approach

1. Define class of simple polynomials $S$

2. **Normal form**: every circuit from circuit class $C$ can be expressed as small sum of simple polynomials in $S$

3. **Complexity Measure**: find sub-additive complexity measure $\mu : \mathbb{F}[x_1, \ldots, x_n] \rightarrow \mathbb{N}$ which captures the simplicity of $S$
   - $\mu(f)$ small for all polynomials in $S$
   - $\mu$ is sub-additive
     \[
     \mu(f + g) \leq \mu(f) + \mu(g)
     \]
Lower Bound Approach

1. Define class of simple polynomials $S$

2. **Normal form:** every circuit from circuit class $C$ can be expressed as a small sum of simple polynomials in $S$

3. **Complexity Measure:** find sub-additive complexity measure $\mu : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{N}$ which captures the simplicity of $S$
   - $\mu(f)$ small for all polynomials in $S$
   - $\mu$ is sub-additive
     \[ \mu(f + g) \leq \mu(f) + \mu(g) \]
   - $\mu$ is “easy” to compute or estimate

4. **Hard polynomial:** find polynomial $p$ such that $\mu(p)$ is large
Lower Bound Approach

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

1. Define class of simple polynomials $S$

2. *Normal form:* every circuit from circuit class $C$ can be expressed as a small sum of simple polynomials in $S$

3. *Complexity Measure:* find sub-additive complexity measure $\mu : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{N}$ which captures the simplicity of $S$
   - $\mu(f)$ small for all polynomials in $S$
   - $\mu$ is sub-additive
     \[ \mu(f + g) \leq \mu(f) + \mu(g) \]
   - $\mu$ 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 $f \in S$
   - By sub-additivity $\mu(q) \leq s \cdot U$ for any $q \in C$ which can be written as
     \[ q = f_1 + f_2 + \cdots + f_s, \quad f_i \in S \]
     \[ \mu(q) = \mu(f_1 + \cdots + f_s) \leq \mu(f_1) + \cdots + \mu(f_s) \leq s \cdot U \]
Lower Bound Approach

1. Define class of simple polynomials $S$
2. **Normal form:** every circuit from circuit class $C$ can be expressed as small sum of simple polynomials in $S$
3. **Complexity Measure:** find sub-additive complexity measure $\mu : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{N}$ which captures the simplicity of $S$
   - $\mu(f)$ small for all polynomials in $S$
   - $\mu$ is sub-additive
     \[ \mu(f + g) \leq \mu(f) + \mu(g) \]
   - $\mu$ 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 $f \in S$
   - By sub-additivity $\mu(q) \leq s \cdot U$ for any $q \in C$ which can be written as
     \[ q = f_1 + f_2 + \cdots + f_s, \quad f_i \in S \]
   - $\mu(p) \geq L$ and $p$ can be computed by size $s$ in $C \Rightarrow s \cdot U \geq L$
Most used complexity measures are *partial derivatives* based.
Most used complexity measures are *partial derivatives* based.

Dimension of span of: partial derivatives, shifted partial derivatives

\[
\text{hom} - \sum_{\lambda} \sum_{\Gamma} \\
\text{hom} - \sum_{\lambda} \sum_{\Gamma} \sum_{\lambda} \\
\text{hom} - \sum_{\lambda} \sum_{\Gamma} \sum_{\lambda} ^{2}
\]
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*:

   \[ L(f + g) = L(f) + L(g) \]

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

   \[ f \mapsto L(f) = L(\text{coeff}(f)) \]

   \[ \mu : \mathbb{F}[x_1, \ldots, x_n] \rightarrow \mathbb{N} \quad \mu(f) = \text{rank}(L(f)) \]

\[ f(x_1, x_2, x_3, x_4) = E_{4,3} = x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_3 x_4 + x_2 x_3 x_4 \]

<table>
<thead>
<tr>
<th></th>
<th>x_1</th>
<th>x_2</th>
<th>x_3</th>
<th>x_4</th>
</tr>
</thead>
<tbody>
<tr>
<td>x_1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>x_2</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>x_3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>x_4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Common aspects of complexity measures - rank methods

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

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

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

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

   \[
   \text{rank}(A+B) \leq \text{rank}(A) + \text{rank}(B)
   \]
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*:

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

\[ \mu : \mathbb{F}[x_1, \ldots, x_n] \rightarrow \mathbb{N} \quad \mu(f) = \text{rank}(L(f)) \]

4. Sub-additivity comes from sub-additivity of rank
5. Examples:
   - dimension of partial derivatives $\rightarrow$ rank of partial derivative matrix
   - dimension of shifted paritals $\rightarrow$ same as above
   - Flattenings used in tensor rank lower bounds $\rightarrow$ 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 $S$, let $c_S(p)$ be the $S$-complexity of polynomial $p$ - that is, the min $s$ such that

\[ p = f_1 + \ldots + f_s, \quad f_i \in S \]
What is a barrier?

Given a class of simple polynomials $S$, let $c_S(p)$ be the $S$-complexity of polynomial $p$ - that is, the min $s$ such that

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

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

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

where $e_1 + \ldots + e_n = d$.

Know there are hard poly $\mathbb{F}[x_1, \ldots, x_n]^d$

**Barrier:** if $\varepsilon(f)$ small $\forall f \in S$ then $g(p)$ is not too large for any polynomial in $\mathbb{F}[x_1, \ldots, x_n] = \text{span}(S)$.
What is a barrier?

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

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

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

- Let $\Delta_S$ be set of all sub-additive measures over $S$
What is a barrier?

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

\[
p = f_1 + \ldots + f_s, \quad f_i \in S
\]

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

- Let \( \Delta_S \) be set of all sub-additive measures over \( S \)

- \( c_S \in \Delta_S \), but it is hard to understand

\[
c_S(p+q) \leq c_S(p) + c_S(q)
\]

\[
p = f_1 + \ldots + f_s, \quad \pi = c_S(p)
\]

\[
q = g_1 + \ldots + g_t, \quad \tau = c_S(q)
\]
What is a barrier?

- Given a class of simple polynomials $S$, let $c_S(p)$ be the $S$-complexity of polynomial $p$ - that is, the min $s$ such that
  \[ p = f_1 + \ldots + f_s, \quad f_i \in S \]

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

- Let $\Delta_S$ be the set of all sub-additive measures over $S$

- $c_S \in \Delta_S$, but it is hard to understand

- Let $\Delta \subset \Delta_S$ subset of measures (simpler to understand, reason about) (set of techniques)

  \[ \Delta \leftarrow \text{Rank methods} \]

  \text{(very easy to analyze)}
What is a barrier?

- Given a class of simple polynomials $S$, let $c_S(p)$ be the $S$-complexity of polynomial $p$ - that is, the min $s$ such that

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

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

- Let $\Delta_S$ be set of all sub-additive measures over $S$

- $c_S \in \Delta_S$, but it is hard to understand

- Let $\Delta \subset \Delta_S$ subset of measures (simpler to understand, reason about) (set of techniques)

- A barrier for the subset $\Delta$ is a statement of the following kind:

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

- Given a class of simple polynomials $S$, let $c_S(p)$ be the $S$-complexity of polynomial $p$ - that is, the min $s$ such that

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

- Assume that $S$ is complete – that is, any polynomial in $\mathbb{F}[x_1, \ldots, x_n]$ can be computed by the span of polynomials in $S$
- Let $\Delta_S$ be set of all sub-additive measures over $S$
- $c_S \in \Delta_S$, but it is hard to understand
- Let $\Delta \subset \Delta_S$ subset of measures (simpler to understand, reason about) (set of techniques)
- A barrier for the subset $\Delta$ is a statement of the following kind:
  
  If $\mu \in \Delta$ and $\mu(f)$ is small for every $f \in S$, 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 $S$ be the class of powers of linear forms (Waring Rank)

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

$S$ is complete: write any monomial in $\text{span}(S)$
Barriers to rank methods

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

\[
\binom{n+d-1}{n-1} = \dim \text{ polys of deg } d \text{ in } n \text{ vars}
\]

\[
\sum_{t=1}^{n} (a_{t1}x_1 + \cdots + a_{tn}x_n)^d
\]

$n$ degrees of freedom

\[
t \approx n^{d-1}
\]

$n.t \approx n^d$

match degrees of freedom
Barriers to rank methods

- Let $S$ 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 $S$ 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 bd
Barriers to rank methods

- Let $S$ 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.*

- Note that this implies a barrier for depth-3 circuits as well!
  
  $S \leq$ Waring rank
  
  $T \leq$ hom. depth 3

  $S$ weaker than $T$
Barrier for Waring Rank - Symbolic Rank

- Going from generic rank to symbolic rank

\[ L \left( (a_1 x_1 + \ldots + a_n x_n)^d \right) \rightarrow M(a_1, \ldots, a_n) \]

\[ a_i \]

Measure is small for any element in \( S \)

Symbolic matrix

\[ M(y_1, \ldots, y_n) = \sum_{1 \leq i \leq d} M_{\vec{e}} \vec{y}^\vec{e} \]

Polynomial matrix homogeneous of degree \( d \)

\[ M(d, \ldots, d) \cdot y_1^d + \ldots \]

\[ \text{rank} \mathbb{F}(\mathbb{G}) (M(y_1)) \leq n \]

\[ \det(M(y)) \neq 0 \]

\[ M(a) \] invertible
Symbolic Rank to Small Decomposition

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

$$M(\bar{y}) \quad \text{rank} \ F(\bar{y})(M(\bar{y})) \leq \pi$$

$$M(\bar{y}) = A(\bar{y}) \cdot B(\bar{y}) \quad A \in F(\bar{y})^{m \times n}$$
$$B \in F(\bar{y})^{n \times m}$$

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

**rank-1 decomposition**

$q_i(\bar{y}) \in F[\bar{y}] \quad \vec{u}_i, \vec{v}_i \in F[\bar{y}]^m$
From field of fractions to polynomials

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

\[
M(y) = \sum_{i=1}^{k} \mathbf{u}_i(y) \cdot \mathbf{u}_i(y)^T
\]

\[\text{polynomial vectors}\]
Grouping elements based on degree

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

\[
M(\bar{y}) = \sum_{i=1}^{n} \left( \bar{u}_i(\bar{y}) \bar{v}_i(\bar{y})^T \right)
\]

where $\bar{X} = \frac{1}{d} \sum_{i=1}^{d} \bar{E}_i \cdot \bar{y}^2$

$H = \text{m} \times \text{m}$

$U_{i_1}(\bar{y})$

$U_{i_2}(\bar{y})$

$U_{i_m}(\bar{y})$

$V_{i_1}(\bar{y})$

$V_{i_2}(\bar{y})$

$V_{i_m}(\bar{y})$

Same degree

$k \leq d-k \quad (k \leq d/2)$
Upper bound on generic rank

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

\[
\sum_{v \in Y} M(v) = \sum_{i=1}^{\ell} u_i(y) v_i(y)^T
\]

\[
= \sum_{i=1}^{\ell} \left( \sum_{\deg \leq \frac{d}{2}} y^a \cdot u_{ia} \right) v_i(y)^T
\]

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

\[
U = \{ u_i \} \quad \dim(\text{span}(U)) \leq \#U \leq n \cdot \binom{\#m_n \cdot \deg}{\frac{d}{2}}
\]
Linearity now bounds the rank of any matrix in image of map!

\[ \sum \bar{M} \bar{g} = \sum \sum g^a \cdot u_{ia} v_i(y)^T \]

\[ \Rightarrow \bar{M} = \sum u_{ia} \cdot v_i^T \subseteq \text{span}(v) \otimes F^m \]

\[ \Rightarrow \text{all } \bar{M} \text{ and linear combinations } \text{ have low rank!} \]
Barrier

\[ f = \sum f_\mathbf{e} \mathbf{x}^e \]

\[ L(f) = \sum f_\mathbf{e} \cdot M_\mathbf{e} \]

\[ \text{rank} \left( \sum \alpha_\mathbf{e} M_\mathbf{e} \right) \leq \text{dim} \left( U \right) \leq \pi \cdot n^{d/2} \]

\[ \Rightarrow \mathcal{M}(f) \leq \pi \cdot n^{d/2} \quad \text{upper bd} \]

\[ \frac{\mathcal{M}(f)}{\mathcal{M}(s)} \leq \frac{\pi \cdot n^{d/2}}{\pi} = n^{d/2}. \]
\[ L : \mathbb{F}[x]_d \rightarrow \mathbb{F}^{m \times m} \]

linear

\[ L(x) = M \bar{e} \]

\[ M(y) = L \left( \left( y_1, x, \ldots, y_{nm} \right)^d \right) = \sum_{|\bar{e}| = d} \bar{y} \bar{e} \cdot ( ) \cdot M \bar{e} \]

\[ \mathbb{F}^{m \times m} \]

degree \( d \)
Lower bound approaches - Rank Methods

Barriers to Rank Methods

Algebraic Natural Proofs & Succinct PIT

Conclusion

Acknowledgements
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
  - $P$ is *useful*: any “easy” boolean function has such property
To prove (boolean) lower bounds, want to find property P such that

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

1. **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 $\text{poly}(N)$-time if $f$ has property $P$

Most boolean function lower bounds (that we can prove) have these three properties
To prove (boolean) lower bounds, want to find property $P$ such that

1. **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 $\text{poly}(N)$-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.
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

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

$$f = \sum f_i x^e_i \mapsto \sum f_i M(\text{coeff}(f))$$

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

*find hard poly outside*
What would be an algebraic “natural” proof?

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

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

Properties of an algebraic natural proof:

1. **Useful**: for easy polynomials, $M(\text{coeff}(p))$ 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 $M : \mathbb{F}[x_1, \ldots, x_n] \rightarrow \mathbb{F}^{m \times m}$ such that

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

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

  This amounts to being able to compute $\det(M((\text{coeff}(p))))$, which is poly($N$)-size if $\dim(M) = \text{poly}(N)$.
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 $M : \mathbb{F}[x_1, \ldots, x_n] \rightarrow \mathbb{F}^{m \times m}$ such that

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

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

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

  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 $C \subseteq \mathbb{F}[x_1, \ldots, x_n]$ be a circuit class
Algebraic Natural Proofs - Definition

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

\[ f(\overline{x}) = \bigoplus_{y \in \text{variables of coeff}(\mathcal{C})} x^y \]
Algebraic Natural Proofs - Definition

- Let $C \subset \mathbb{F}[x_1, \ldots, x_n]$ be a circuit class.
- Let $D \subset \mathbb{F}[^{\text{coeff}}(C)]$ be another circuit class.
- A polynomial $D \in D$ (distinguisher) is an \textit{algebraic natural proof} against $C$ if:
  1. $D \neq 0$
  2. $D(^{\text{coeff}}(f)) = 0$ for all $f \in C$

\[ \mathbb{C} = \mathbb{V}(D) \]

\[ \mathbb{C} = \mathbb{F}[x, y] \frac{\mathbb{Z}}{ \{ \frac{b^2 - 4ac}{4} \} } \]

\[ a \cdot x^2 + b \cdot xy + c \]
Algebraic Natural Proofs - Definition

- Let $C \subset F[x_1, \ldots, x_n]$ be a circuit class
- Let $D \subset F[\text{coeff}(C)]$ be another circuit class
- A polynomial $D \in D$ (distinguisher) is a *algebraic natural proof* against $C$ if
  1. $D \neq 0$
  2. $D(\text{coeff}(f)) = 0$ for all $f \in C$

Open Question (Existence of natural proofs)

Is VP a natural proof for VP?
Algebraic Natural Proofs - Definition

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

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 $\mathcal{D} \subset \mathbb{F}[\text{coeff}(\mathcal{C})]$ be another circuit class.
- A polynomial $D \in \mathcal{D}$ (distinguisher) is a \textit{algebraic natural proof} against $\mathcal{C}$ if:
  1. $D \neq 0$
  2. $D(\text{coeff}(f)) = 0$ for all $f \in \mathcal{C}$

Open Question (Existence of natural proofs)

\textit{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 \textit{not} an algebraic natural proof against VNP.
When will a natural proof fail? Succinct Hitting sets

\[ C \leftarrow \text{easy polynomials} \]

\[ D \subset \{ x \} \in \text{distinct} \]

\[ D \text{ is NOT algebraic natural proof against } C \]

\[ \Rightarrow \forall D \subseteq D \exists f \in C \text{ s.t.} \]

\[ D(\text{coeff}(f)) \neq 0 \]

\[ \Rightarrow C \text{ is hitting set for } D \]

\[ x = \{ \text{coeff}(f) : f \in C \} \]
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]
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