Klim Efremenko
Ben Gurion
Ankit Garg
MSR New England
Rafael Oliveira
University of Toronto
Avi Wigderson
IAS

Barriers for Rank Methods in Arithmetic Complexity

1

Introduction & Background

The Big Picture

General Lower Bound Techniques

Rank Techniques

Example

Big Picture

Algebraic complexity studies computation of algebraic objects (**polynomials, matrices, tensors**). Two main features:

1. Extremely interesting:
- Euclid's GCD algorithm
- Gauss' FFT
- Abel's impossibility result for quintic
- Structural Theory similar to Boolean complexity. (Complete classes $\boldsymbol{VP}, \boldsymbol{VNP}$ developed shortly after $\boldsymbol{P}, \boldsymbol{NP}$.)

2. Generally easier (l.b.) than Boolean setting:
- Algebraic computation "syntactic" (computes *polynomials*),
- Boolean computation "semantic" (computes *functions*).
- Algebraic setting more constrained (only uses arithmetic)
- Indeed $\boldsymbol{P}_{/poly} \neq \boldsymbol{NP}_{/poly}$ is known* to imply $\boldsymbol{VP}_{\mathbb{C}} \neq \boldsymbol{VNP}_{\mathbb{C}}$.

Big Picture

Lower bounds easier to prove in algebraic setting... What do we know

(1) Bounded depth (remarkable advances):

- **[GKKS'14, KS'14, FLMS'15, ...]:** $n^{\sqrt{d}}$ for hom. depth-4 circuits
- **[GK'98, GR'00, CM'14]:** n^d for depth-3 circuits (*over small finite fields*)
- **[LO'17]:** $n^{d/2}$ for diagonal depth-3 circuits (*Waring Rank*)
- **[Raz'09, RY'09]:** $n^{n^{1/\Delta}}$ for multilinear depth-Δ formulas

(2) General setting (very little progress):

- **[BS'83]:** $n \cdot \log n$ for circuits
- **[Kal'85]:** $n^2 / \log^2 n$ for formulas
- **[K'17]:** n^2 for homogeneous ABPs
- **[AFT'11]:** $2n^{d/2}$ for d-dimensional tensors of side n

1. Bounds in (1 & 2) are far from the bounds for random polynomials.
2. Why is that the case?
3. Are the techniques from (1) limited in the general setting?

Boolean Barriers

Lower bounds harder to prove, easier to find barriers…

1. **[BGS'75] Relativization**
2. **[AW'09] Algebrization**
   - Extends relativization
3. **[Raz'92] Submodular Progress Measures**
   - Any μ s.t. $\mu(f \wedge g) + \mu(f \vee g) \leq \mu(f) + \mu(g)$
   - Can't prove super-linear l.b.s on non-monotone computation!
   - Unconditional!
4. **[RR'94] Natural Proofs**
   - Progress measures which are natural (i.e. useful, constructive & large) cannot prove $\boldsymbol{P \neq NP}$
   - Conditional (efficient construction of PRGs)

Attempts at Algebraic Barriers

Barriers for algebraic setting much harder to find.

1. **[AD'09, Gro'15] Encapsulating Lower Bounds**
   - polynomials ⇔ list of coefficients
   - Lower bounds are algebraic varieties in this coefficient space (Separating Modules)
   - Unifies but does not provide any barrier
2. **[FSV'17, GKSS'17] Succinct Lower Bounds**
   - No succinct hitting sets ⇔ barrier
   - No strong complexity assumption (to replace pseudo-random one from Boolean setting)

1 Introduction & Background

The Big Picture

General Lower Bound Techniques

Rank Techniques

Example

(Algebraic) Lower Bound Game Plan

General structure of lower bound proof:

1. **Decompose polynomial into sum of simpler polynomials**
2. **Come up with progress measure**
   - $\mu(f+g) \leq \mu(f) + \mu(g)$
   - $\mu(g)$ small on simple polynomials
3. **Find explicit polynomial with high measure**

Examples of Decompositions

1. **[Hya'79]:** if f computed by hom. circuit of size s
   - $f = g_1 + \cdots + g_s$, where $g_i = p_i q_i$ and $\deg(p_i), \deg(q_i) \leq \frac{2d}{3}$.
2. **Tensor Rank:** if f is a tensor of rank s then
   - $f = g_1 + \cdots + g_s$, where $g_i = \boldsymbol{u_{i1}} \otimes \cdots \otimes \boldsymbol{u_{id}}$
3. **Waring Rank:** of a hom. polynomial f is the minimum s s.t.
   - $f = g_1 + \cdots + g_s$, where $g_i = \ell(\boldsymbol{x})^{\boldsymbol{d}}$
4. **Bounded Depth Circuits:** f computed by depth h circuit of size s if
   - $f = g_1 + \cdots + g_s$, where g_i is computed by a circuit of depth $h - 1$ and with top gate being a product gate.

General Lower Bound Techniques

- $S \leftarrow$ set of "simple" polynomials
- $\hat{S} \leftarrow span(S)$
- **S-complexity:** $c_S(f) \leftarrow \min\ s$ s.t.

$$f = g_1 + g_2 + \cdots + g_s$$

and each $g_i \in S$.

A **sub-additive** measure $\mu : \hat{S} \to \mathbb{R}^+$ s.t.

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

Let $\mu(T) = \max\{\mu(g) : g \in T\}$.

Lower Bound: $c_S(f) \geq \mu(f)/\mu(S)$

Barriers to Lower Bound Techniques

- $\Delta_S \leftarrow$ set of sub-additive measures
- $c_S \in \Delta_s$ but hard to understand
- Approximate c_S by "simpler" measures $\Delta \subset \Delta_S$

A **barrier** for set of measures Δ is a bound on

$$c(\Delta) = \max_{\mu \in \Delta} \frac{\mu(\hat{S})}{\mu(S)}$$

$c(\Delta)$ bounds the best lower bound attainable by Δ

Rank Methods

Any measure which can be cast as the rank of a matrix.

- $L : \hat{S} \to Mat_m(\mathbb{F})$ any **linear** map
- $\mu_L(f) = rank_{\mathbb{F}}\,(L(f))$
- Let $\Delta_S^0 \subset \Delta_S$ be the set of all such μ_L

Includes: *(shifted) partial derivatives, evaluation dimension, coefficient dimension, flattenings*

Used in **[Nis'91, Smo'93, NW'96, Raz'09, RY'09 Kay'12, GKKS'14, KLSS'14, FSS'14, FLMS'15, KS'14, LO'17]** and many others…

Example of Lower Bound [NW'96]

Homogeneous depth-3 circuits:

$$\sum_{i=1}^{s} \prod_{j=1}^{d} \ell_{ij}(\mathbf{x})$$

Simple polynomials $\boldsymbol{S}$:

$$\mathrm{g_i}(\mathbf{x}) = \prod_{j=1}^{d} \ell_{ij}(\mathbf{x})$$

Matrix of partial derivatives:

$$\bar{x}^{\bar{e}_2}$$

$$L(f) = \begin{array}{c} \text{monomial degree } d/2 \\ \bar{x}^{\bar{e}_1} \end{array} \begin{pmatrix} & \vdots & \\ \cdots & \boxed{} & \cdots \\ & \vdots & \end{pmatrix}$$

coefficient of $\bar{x}^{\bar{e}_2}$ in $\frac{\partial^{d_1} f}{(\partial \bar{x})^{\bar{e}_1}}$

Monomial of degree $d/2$

Coefficient of x^{e_2} in $\frac{\partial^{d/2} f}{(\partial x)^{e_1}}$

Example of Lower Bound [NW'96]

Matrix of partial derivatives, example:

$$\boldsymbol{L}(x^2 - y^2) = \begin{array}{cc} \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix} & \begin{array}{c} \boldsymbol{x} \\ \boldsymbol{y} \end{array} \\ \begin{array}{cc} \boldsymbol{x} & \boldsymbol{y} \end{array} & \end{array}$$

Lower bound:

1. $\mu(f) \leftarrow \boldsymbol{rank}(\boldsymbol{L}(f)) = \boldsymbol{dim}(\boldsymbol{span}(\partial^{=d/2} f))$
2. $g = \prod_{i=1}^{d} \ell_i \Rightarrow \mu(g) \leq 2^{d/2}$
3. $\boldsymbol{\mu}(sym_n^d) \geq \binom{n}{d/2}$

$$\mathbf{c_S}(sym_n^d) \geq \binom{\boldsymbol{n}}{\lfloor \boldsymbol{d}/\mathbf{2} \rfloor} \cdot \mathbf{2}^{-\frac{d}{2}} = \boldsymbol{\Omega_d}(\boldsymbol{n}^{\lfloor d/2 \rfloor})$$

2

Results & Open Questions

Tensor & Waring Rank

Proof for Waring Rank

Open Questions

Barrier for Tensor Rank

Theorem: Rank methods cannot prove a lower bound better than

$$\Omega_d\left(\boldsymbol{n}^{\lfloor d/2 \rfloor}\right)$$

on the tensor rank of *any* **d**-dimensional tensor of side **n.**

In particular, they cannot prove **super-linear** lower bounds – even $> \boldsymbol{8n}$, when $\boldsymbol{d} = \boldsymbol{3}$.

Constant factor away from trivial:

$$n^{\lfloor d/2 \rfloor}$$

Far from random tensors:

$$n^{d-1}$$

Bound needed for circuit lower bounds **[Raz'10]**:

$$n^{d(1-o(1))}$$

Barrier for Waring Rank

Theorem: Rank methods cannot prove a lower bound better than

$$(\mathrm{d}+1)\cdot\binom{n+\lfloor d/2\rfloor}{\lfloor d/2\rfloor} = \Omega_d\left(n^{\lfloor d/2\rfloor}\right)$$

on the Waring rank of *any* **n**-variate polynomial of degree **d.**

Almost matches the best lower bounds achieved by rank methods **[LO'17]**:

$$\binom{n+\lfloor d/2\rfloor-1}{\lfloor d/2\rfloor} + \lfloor n/2\rfloor - 1$$

Far from random polynomials:

$$\frac{1}{n}\cdot\binom{n+d-1}{d}$$

Proof of Waring Rank Case

- $S = \{(\sum_{i=1}^{n} a_i x_i)^d \ : \ a_i \in \mathbb{F}\}$
- $\widehat{S} = \langle S \rangle = \mathbb{F}[x_1, \ldots, x_n]_d$
- Let $\mathbf{L} : \widehat{S} \to \boldsymbol{Mat}_m(\mathbb{F})$ be any linear map
- Let $\boldsymbol{\mu}(f) = \boldsymbol{rank}_{\mathbb{F}}(\boldsymbol{L}(f))$

L is a linear map and $f(x) = \sum_e a_e x^e$ then:

$$\boldsymbol{L}(f) = \sum_{e} a_e \boldsymbol{L}(\boldsymbol{x}^{e}) = \sum_{e} a_e \boldsymbol{M}_e$$

Thus

$$\boldsymbol{\mu}(\widehat{\boldsymbol{S}}) = \boldsymbol{rank}(\langle \boldsymbol{M}_e \rangle)$$

Proof of Waring Rank Case

If, $g = (\sum_{i=1}^{n} a_i x_i)^d$ we have:

$$\boldsymbol{L}(g) = \sum_{\boldsymbol{e}} \binom{d}{e_1, \dots, e_n} \boldsymbol{a}^{\boldsymbol{e}} \boldsymbol{M}_{\boldsymbol{e}}$$

- $\boldsymbol{L}(g)$ is a matrix whose entries are polynomials of degree d in parameters $\boldsymbol{a}$
- Let $r = \boldsymbol{\mu}(\boldsymbol{S}) = \max_{g \in \boldsymbol{S}}(\boldsymbol{rank}_{\mathbb{F}}(\boldsymbol{L}(g)))$
- Then, $r = \boldsymbol{rank}_{\mathbb{F}(\boldsymbol{a})}(\boldsymbol{L}(g))$ for a generic choice of g.

Proof of Waring Rank Case

Thus, to prove a barrier, we need to upper bound

$$\frac{\mu(\widehat{S})}{\mu(S)} = \frac{\boldsymbol{rank}(\langle \boldsymbol{M_e} \rangle)}{\boldsymbol{rank}_{\mathbb{F}(\boldsymbol{a})}(\boldsymbol{L}(g))} = \frac{\boldsymbol{rank}(\langle \boldsymbol{M_e} \rangle)}{r}$$

- Plan is to find especial decomposition of each $\boldsymbol{M_e}$
- We will show that there exists a "small" set $\boldsymbol{W} \subset \mathbb{F}^m$ s.t. each

$$\boldsymbol{M_e} = \sum_{\boldsymbol{w} \in \boldsymbol{W}} \boldsymbol{w} \otimes \boldsymbol{y_w} + \boldsymbol{z_w} \otimes \boldsymbol{w}$$

- Then, $\boldsymbol{rank}(\langle \boldsymbol{M_e} \rangle) \leq \mathbf{2}|\boldsymbol{W}|$.

Upper bounding $rank(\langle M_e \rangle)$

For a generic $g = (\sum_{i=1}^{n} a_i x_i)^d$, we have:

$$\boldsymbol{L}(g) = \sum_{\boldsymbol{e}} \binom{d}{e_1, \dots, e_n} \boldsymbol{a}^{\boldsymbol{e}} \boldsymbol{M}_{\boldsymbol{e}}$$

- $\boldsymbol{L}(g)$ is a matrix whose entries are polynomials of degree d in parameters $\boldsymbol{a}$
- Then, $r = \boldsymbol{rank}_{\mathbb{F}(\boldsymbol{a})}(\boldsymbol{L}(g))$ for a generic choice of g.
- Can we find succinct decomposition of $\boldsymbol{L}(g)$?

Upper bounding $rank(\langle M_e \rangle)$

Since $r = \boldsymbol{rank}_{\mathbb{F}(\boldsymbol{a})}(\boldsymbol{L}(g))$, can decompose $\boldsymbol{L}(g)$ as:

$$\boldsymbol{L}(g) = \sum_{k=1}^{r} \frac{1}{1 - p_k(\boldsymbol{a})} \boldsymbol{u}_k(\boldsymbol{a}) \otimes \boldsymbol{v}_k(\boldsymbol{a})$$

Where $\boldsymbol{u}_k(\boldsymbol{a}), \boldsymbol{v}_k(\boldsymbol{a}) \in \mathbb{F}[\boldsymbol{a}]^m$ are vectors of polynomials and $p_k(\boldsymbol{a})$ are polynomials such that $p_k(\boldsymbol{0}) = 0$.

- Write $\frac{1}{1 - p_k(\boldsymbol{a})} = 1 + \mathrm{q}_1(\boldsymbol{a}) + \cdots + \mathrm{q}_\mathrm{d}(\boldsymbol{a}) + \cdots$
- Each $\mathrm{q}_\mathrm{i}(\boldsymbol{a})$ is homogeneous of degree i
- Equality above is then equality of power series.
- But LHS is homogeneous of degree d

Upper bounding $rank(\langle M_e \rangle)$

Letting $\widehat{\boldsymbol{u}}_k(\boldsymbol{a}) = \big(1 + \mathrm{q}_1(\boldsymbol{a}) + \cdots + \mathrm{q}_\mathrm{d}(\boldsymbol{a})\big) \cdot \boldsymbol{u}_k(\boldsymbol{a})$

$$\boldsymbol{L}(g) = H_d\left(\sum_{k=1}^{r} \widehat{\boldsymbol{u}}_k(\boldsymbol{a}) \otimes \boldsymbol{v}_k(\boldsymbol{a})\right)$$

Where $\widehat{\boldsymbol{u}}_k(\boldsymbol{a}), \boldsymbol{v}_k(\boldsymbol{a}) \in \mathbb{F}[\boldsymbol{a}]^m$ are vectors of polynomials.

Note that:

$$H_d(\widehat{\boldsymbol{u}}_k(\boldsymbol{a}) \otimes \boldsymbol{v}_k(\boldsymbol{a})) = \sum_{j=0}^{d} H_j(\widehat{\boldsymbol{u}}_k(\boldsymbol{a})) \otimes H_{d-j}(\boldsymbol{v}_k(\boldsymbol{a}))$$

Upper bounding $rank(\langle M_e \rangle)$

Putting things together:

$$L(g) = \sum_{k=1}^{r} \sum_{j=0}^{d} H_j(\hat{\boldsymbol{u}}_k(\boldsymbol{a})) \otimes H_{d-j}(\boldsymbol{v}_k(\boldsymbol{a}))$$

Where $H_j(\hat{\boldsymbol{u}}_k(\boldsymbol{a})), H_{d-j}(\boldsymbol{v}_k(\boldsymbol{a})) \in \mathbb{F}[\boldsymbol{a}]^m$ are vectors of homogeneous polynomials.

$L(g)$ spanned by the following "low degree" vectors:

$$H_j(\hat{\boldsymbol{u}}_k(\boldsymbol{a})), H_j(\boldsymbol{v}_k(\boldsymbol{a})) \quad 0 \le j \le \lfloor d/2 \rfloor, 1 \le k \le r$$

Upper bounding $rank(\langle M_e \rangle)$

Writing

$$H_j\left(\hat{\boldsymbol{u}}_k(\boldsymbol{a})\right) = \sum_{\boldsymbol{b} \in \boldsymbol{Mon}(j)} \boldsymbol{a}^{\boldsymbol{b}} \boldsymbol{u}_{k,\boldsymbol{b}}$$

and

$$H_j\left(\boldsymbol{v}_k(\boldsymbol{a})\right) = \sum_{\boldsymbol{b} \in \boldsymbol{Mon}(j)} \boldsymbol{a}^{\boldsymbol{b}} \boldsymbol{v}_{k,\boldsymbol{b}}$$

And setting

$$\boldsymbol{W} = \{\boldsymbol{u}_{k,\boldsymbol{b}}\} \cup \{\boldsymbol{v}_{k,\boldsymbol{b}}\}$$

Where $1 \leq k \leq r$ and $\boldsymbol{b} \in \boldsymbol{Mon}(j)$ for $0 \leq j \leq \lfloor d/2 \rfloor$.

Upper bounding $rank(\langle M_e \rangle)$

From:

$$L(g) = \sum_{k=1}^{r} \sum_{j=0}^{d} H_j(\hat{\boldsymbol{u}}_k(\boldsymbol{a})) \otimes H_{d-j}(\boldsymbol{v}_k(\boldsymbol{a}))$$

And from:

$$\boldsymbol{L}(\boldsymbol{g}) = \sum_{\boldsymbol{e} \in \boldsymbol{Mon}(d)} \boldsymbol{a}^{\boldsymbol{e}} \boldsymbol{M}_{\boldsymbol{e}}$$

By collecting monomials:

$$\boldsymbol{M}_{\boldsymbol{e}} = \sum_{k=1}^{r} \sum_{j=0}^{\lfloor d/2 \rfloor} \sum_{\substack{\boldsymbol{b}+\boldsymbol{c}=\boldsymbol{e} \\ \boldsymbol{b} \in \boldsymbol{Mon}(j)}} \boldsymbol{u}_{k,\boldsymbol{b}} \otimes \boldsymbol{v}_{k,\boldsymbol{c}} + \boldsymbol{u}_{k,\boldsymbol{c}} \otimes \boldsymbol{v}_{k,\boldsymbol{b}}$$

Each $\boldsymbol{M}_{\boldsymbol{e}}$ can be decomposed by $\boldsymbol{W}$ as we wanted.

Upper bounding $rank(\langle M_e \rangle)$

Can upper bound $|\boldsymbol{W}|$ by the number of "low degree" vectors:

$$|\boldsymbol{W}| \leq \left|\{\boldsymbol{u}_{k,\boldsymbol{b}}\}\right| + \left|\{\boldsymbol{v}_{k,\boldsymbol{b}}\}\right|$$

As $1 \leq k \leq r$ and $\boldsymbol{b} \in \boldsymbol{Mon}(j)$ for $0 \leq j \leq \lfloor d/2 \rfloor$, we have

$$\boldsymbol{W} \leq 2r \cdot \#(mon.\, of\ deg. \leq \lfloor d/2 \rfloor) \leq r(d+1) \cdot \binom{n + \lfloor d/2 \rfloor}{\lfloor d/2 \rfloor}$$

Thus:

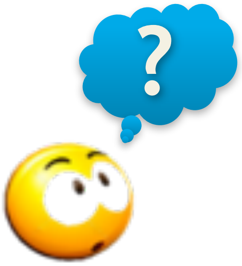
$$\frac{\boldsymbol{\mu}(\widehat{\boldsymbol{S}})}{\boldsymbol{\mu}(\boldsymbol{S})} = \frac{\boldsymbol{rank}(\langle \boldsymbol{M_e} \rangle)}{r} \leq \frac{2|\boldsymbol{W}|}{r} \leq (d+1) \cdot \binom{n + \lfloor d/2 \rfloor}{\lfloor d/2 \rfloor}$$

Open questions

- Can we extend this barrier to other circuit classes? What about other mappings (such as non-linear mappings L)?

- Can we use these barrier techniques to prove better lower bounds?

- Is the matrix decomposition that we obtained tight?



Thank you!