A Survey of Algebraic Circuit Lower Bounds

Prashanth Amireddy (Harvard University)

July 12, 2023

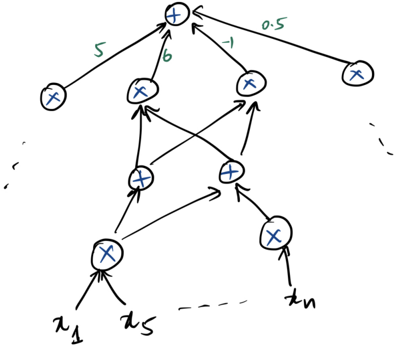
Outline

- Algebraic circuits: Definitions
- Depth-3 homogeneous lower bound (partial derivatives)
- Restricted circuit classes
- Constant-depth lower bound (partial derivatives $+$ varying set sizes)
- Follow-up works

Algebraic circuit

Computes $P(x) = P(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]$.

- Size = Number of gates
- Depth = Maximum length of a leaf-to-root path
- Product-depth
- $\Sigma\Pi\Sigma\Pi\cdots$ structure



VP **and** VNP

- VP: Polynomials $P(x)$ of degree $d = n^{O(1)}$ computable by $n^{O(1)}$ size circuits
  Examples: DET_n, $\mathit{IMM}_{n,d}$

- VNP: Polynomials
$$P(x) = \sum_{y \in \{0,1\}^m} Q(x, y)$$
  where $m = n^{O(1)}$ and $Q \in$ VP.
  Examples: PERM_n, *NW*

- VP $\subseteq$ VNP

VP **vs** VNP

Conjecture **[Valiant '79]:** VP $\subsetneq$ VNP
Stronger conjecture: VF $\subsetneq$ VBP $\subsetneq$ VP $\subsetneq$ VNP

- VF : Polynomial size algebraic *formulas*
- VBP : Polynomial size *algebraic branching programs* (ABPs)

- DET_n, $\mathit{IMM}_{n,d} \in$ VBP (complete)
- $\mathit{PERM}_n \in$ VNP (complete)

- Determinant vs Permanent

VP vs VNP: Connections

- VP = VNP and GRH $\implies$ P/poly = NP/poly
- Derandomizing Polynomial Identity Testing (PIT)
- Learning algebraic circuits

Is there an "explicit" polynomial that requires superpolynomial size circuits?

Lower bounds

- $x_1^d + x_2^d + \cdots + x_n^d$ requires circuit size $\Omega(n \log d)$. [Baur-Strassen '83, Strassen '73]
- *Esym*$_{n,.1n}$ requires formulas (or layered ABPs) of size $\Omega(n^2)$. [Chatterjee-Kumar-She-Volk '22]

Theorem. [Limaye-Srinivasan-Tavenas '21]

For $d = o(\log n)$ and $\mathrm{char}(\mathbb{F}) = 0$ or $> d$, *IMM*$_{n,d}$ requires product-depth Δ circuits of size $n^{\Omega(d^{c_\Delta})}$ where $0 < c_\Delta \leq 1$.

- Hardness escalation
- Non-FPT lower bounds for set-multilinear circuits
- Partial derivatives + varying set sizes

Restricted circuit models

- **Constant-depth circuits:** $\Delta =$ constant. Equivalent to constant-depth formulas.
- **Homogeneous circuits:** Each intermediate gate computes a *homogeneous polynomial*, e.g., $x_1^3 + 3x_2^2x_5 - x_9^3$.
- **Multilinear circuits:** Each intermediate gate computes a *multilinear polynomial*, e.g., $3x_1x_2x_5 - x_2x_9 + x_1 + 9$.
- **Set-multilinear circuits:** Each intermediate gate computes a *set-multilinear polynomial*, e.g., $x_1y_2z_3 - 5x_2y_5z_9 + 7x_1y_3z_5$.

  More generally, $P(\mathbf{x})$ is *set-multilinear* w.r.t. a partitioning $\mathbf{x} = \mathbf{x}_1 \cup \mathbf{x}_2 \cup \cdots \cup \mathbf{x}_d$.
- **Monotone circuits, non-commutative circuits etc.**

Homogeneous depth-3 lower bound

Theorem. [Nisan-Wigderson '97]

For $d \le \sqrt{n}$, there exists an explicit polynomial $P(x_1, \ldots, x_n)$ of degree d such that any homogeneous $\Sigma\Pi\Sigma$ circuit computing P has size $n^{\Omega(d)}$.

Proof sketch. Let $P(x) = \sum_{i=1}^{s} \underbrace{\ell_{i,1}(x)\ell_{i,2}(x)\ldots\ell_{i,d}(x)}_{T_i(x)}$.

Define $\mu : \mathbb{F}[x] \to \mathbb{Z}_{\ge 0}$ as $\mu(P) := \dim\left\{\partial^{=d/2}(P)\right\}$.

- $\mu(T_i) \le 2^d$, as $\partial_m(T_i) \in \operatorname{span}\left\{\prod_{j\in S} \ell_{i,j}(x) : S \subseteq [d]\right\}$.
- $\mu(P) \gtrsim \binom{n}{d/2}$, for appropriate explicit P.
- Hence, $s \ge \mu(P)/\mu(T_i) \ge n^{\Omega(d)}$.

Homogeneous depth-4 lower bound

- A $n^{\Omega(\sqrt{d})}$ lower bound for homogeneous $\Sigma\Pi\Sigma\Pi$ circuits computing $\mathit{IMM}_{n,d}$ and *NW*.

  [Gupta-Kamath-Kayal-Saptharishi '14, Kayal-Limaye-Saha-Srinivasan '17, Kumar-Saraf '17,...]
- Proof technique: random restrictions + shifted partials
- Can be improved to $n^{\omega(\sqrt{d})} \implies \mathrm{VP} \neq \mathrm{VNP}$:

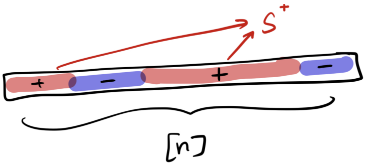
Depth reduction. [Valiant-Skyum-Berkowitz-Rackoff '83, Tavenas '15, ...]

Any circuit C of size s can be converted to a homogeneous $\Sigma\Pi\Sigma\Pi$ circuit of size $s^{O(\sqrt{d})}$.

Hence, a $n^{\omega(\sqrt{d})}$ lower bound for the latter model implies a $n^{\omega(1)}$ lower bound for general circuits.

Multilinear circuits

- $\mathsf{VF}_{\mathsf{mult}} \neq \mathsf{VBP}_{\mathsf{mult}}$ [Raz '06, Raz-Yehudayoff '08, Dvir-Malod-Perifel-Yehudayoff '12]
- A $2^{n^{\Omega(1/\Delta)}}$ lower bound for multilinear circuits computing DET_n, PERM_n and $\mathit{IMM}_{2,n}$ [Raz-Yehudayoff '09, Chillara-Limaye-Srinivasan '19]
- Depth hiearchy theorem [Raz-Yehudayoff '09, Chillara-Engels-Limaye-Srinivasan '18]
- Proof technique: Only use a subset of variables (called $S^+ \subseteq [n]$) for taking derivatives:

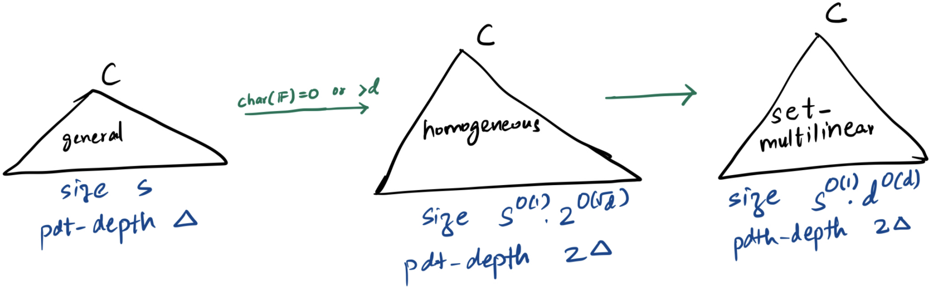


- How does it help? For a random partitioning $[n] = S^+ \cup S^-$ and any "multilinear" product $Q(x)R(y)$, either $|\mathrm{vars}(x) \cap S^+|$ or $|\mathrm{vars}(y) \cap S^+|$ is "small".

Set-multilinear circuits

Isn't this model already subsumed by the above results for homogeneous and multilinear circuits?!

Yes.. but the above previous lower bounds were FPT in the degree i.e., $f(d) \cdot n^{\Omega(1)}$.
In contrast, suppose we are able to get a *non-FPT* set-multilinear lower bound — $n^{\omega_d(1)}$.
Then, we can "escalate" such a lower bound to *general* circuits (of around the same depth) [Limaye-Srinivasan-Tavenas '21]:



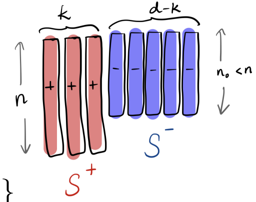
Non-FPT set-multilinear lower bound

Let $\mathbb{F}[\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_d]$ denote the space of all sml polynomials over variables $\mathbf{x} = \mathbf{x}_1 \cup \mathbf{x}_2 \cup \cdots \cup \mathbf{x}_d$ with $|\mathbf{x}_i| \leq n$.

Theorem. [Limaye-Srinivasan-Tavenas '21]

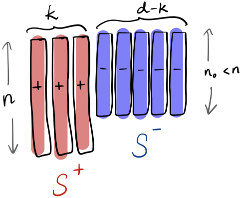
For $d = o(\log n)$, there exists an explicit sml $P(\mathbf{x}) \in \mathbb{F}[\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_d]$ that requires depth-5 (i.e., $\Delta = 2$) sml circuits of size $n^{\Omega(\sqrt{d})}$.

The complexity measure: parital derivative measure (with appropriate set sizes)



- Define $\mu(P) := \dim \{\partial_{S^+}(P)\}$
- If Q is sml w.r.t. $S \subseteq [d]$, $\mu(Q) := \dim \{\partial_{S^+ \cap S}(Q)\}$

Non-FPT sml lower bound: Proof sketch



An upper bound: $\mu(Q) = \dim\{\partial_{S^+ \cap S}(Q)\} \leq \min\left\{n^{|S^+ \cap S|},\ n_0^{|S^- \cap S|}\right\}$

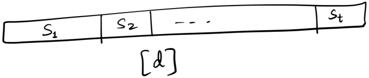
The hard polynomial P**:** $\mu(P) = n^k = n_0^{d-k}$, i.e., $n_0 = n^{k/(d-k)}$

To upper bound $\mu(C)$ **for a depth-5 sml** C **of size** s**:**

<u>Step 1: Decomposition</u>

$$C = \sum_{i=1}^{s} T_i$$

s.t. each $T = Q_1 Q_2 \ldots Q_t$ where Q_j is sml w.r.t. $S_j \subseteq [d]$, and $\sqrt{d}/2 \leq |S_j| \leq \sqrt{d}$ or $|S_j| = 1$, for at least $\Omega(\sqrt{d})$ many j's.



Non-FPT sml lower bound: Proof sketch

Step 2: Bounding each term

$$\mu(T) = \prod_j \mu(Q_j) \le \prod_j \min\left\{n^{|S^+\cap S_j|},\ n_0^{|S^-\cap S_j|}\right\}$$

$$= \prod_j \frac{\sqrt{n^{|S^+\cap S_j|}\cdot n_0^{|S^-\cap S_j|}}}{\sqrt{n^{|a_j^+ - ka_j^-/(d-k)|}}} \qquad \text{(where } a_j^+ + a_j^- = |S_j|\text{)}$$

$$= \frac{\sqrt{n^k\cdot n^k} \;\; = \mu(P)}{n^{\Omega(\sum_j |a_j^+ - ka_j^-/(d-k)|)}}$$

Suffices to show for each "good" j that $\left|a_j^+ - \frac{k}{d-k}a_j^-\right| \ge \Omega(1)$. Set $k = \frac{d-\sqrt{d}}{2}$.

Lower bound: $s \ge \mu(P)/\mu(T) \ge n^{\Omega(\#\text{good } j)} = n^{\Omega(\sqrt{d})}$.

Further improvements

..to the "lopsided" partial derivative framework:

- A $(\log n)^{\Omega(\log d)}$ lower bound for sml formulas of unbounded depth for $\mathit{IMM}_{n,d}$ [Tavenas-Limaye-Srinivasan '22]
- A depth hierarchy theorem for algebraic circuits [Limaye-Srnivasan-Tavenas '21]
- A $n^{\Omega(d^{1/\phi^{\Delta}})}$ lower bound [Bhargav-Dutta-Saxena '22]
- A more general framework for sml formulas lower bounds and barriers [Limaye-Srinivasan-Tavenas '22]

Revisiting homogeneous lower bounds

An alternative proof of the low-depth lower bound using *shifted partials* [A.-Garg-Kayal-Saha-Thankey '23]

- Skips set-multilinearization step, and analyzes homogeneous circuits directly
- Gives similar lower bounds for *NW* and non-sml polynomials, besides *IMM*
- Lower bounds against homogeneous unique-parse-tree formulas
- Uses known measures like shifted partials and affine projections of partials measures (with different parameter settings)

Technical ingredient

$\left\{x^{=\ell} \cdot \partial^{=k} (Q_1 Q_2 \ldots Q_t)\right\} \subseteq$ some low-dimensional space, depending on $\deg(Q_i)$'s

Revisiting set-multilinear lower bounds

Set-multilinear formula lower bounds for large degree [Kush-Saraf '22, Kush-Saraf '23]

- A $n^{\Omega(n^{1/\Delta}/\Delta)}$ lower bound for sml formulas computing a *set-multilinear* ABP
- An unbounded depth lower bound of $n^{\Omega(\log n)}$
- Self-reducibility of *IMM*: Can compute $\mathit{IMM}_{n,n}$ using $\mathit{IMM}_{n,d}$ for $d < n$.
- Implies VF $\neq$ VBP if the above ABP can be made "ordered" sml

Conclusion

Common lower bound themes:

- Hardness escalation (via homogenization/set-multilinearization)
- Decomposition/ depth-reduction to $\Sigma\Pi\Sigma\Pi$ and lower bound the top fain-in

Open problems:

- Improved (non-FPT) set-multilinear lower bounds?
- Large-degree homogeneous depth-5 lower bound? Or an exponential depth-3 lower bound?
- Depth-4 constant-size field lower bounds?

Thank you! Questions?