Improved Lower Bound and Proof Barrier for Constant Depth Algebraic Circuits

C S Bhargav
IIT Kanpur

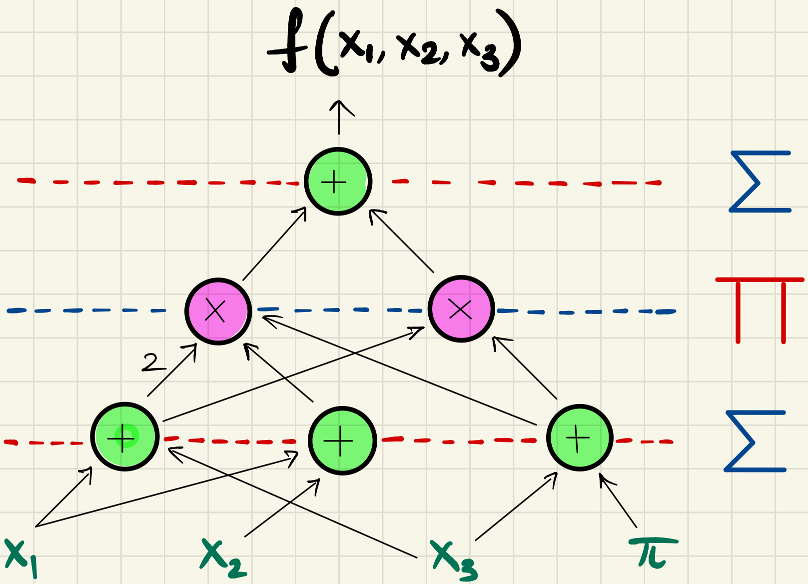
Sagnik Dutta
Chennai Mathematical Institute

Nitin Saxena
IIT Kanpur

WACT, March 2023

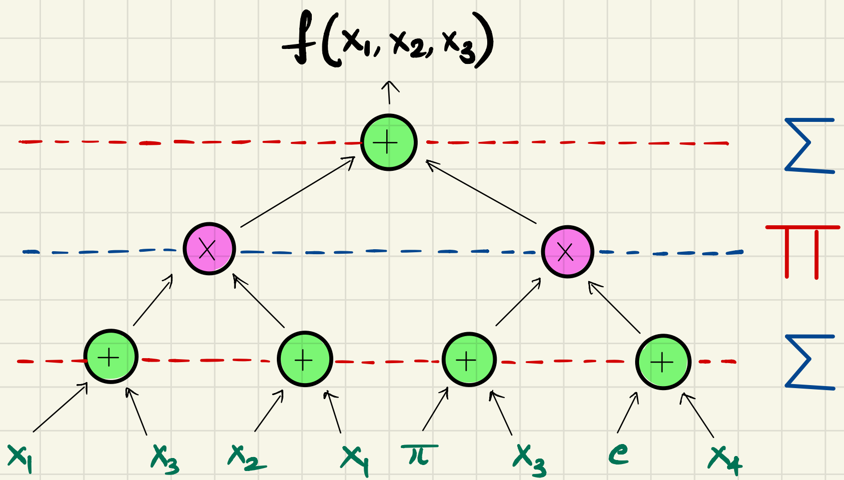
The Problem

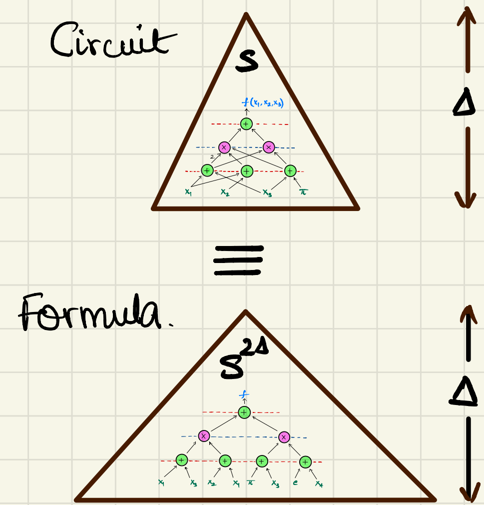
- Prove lower bounds against constant depth algebraic ckts.



- Size (s): # gates/wires
- Depth (δ): # layers
- Product depth (Δ): # Π layers

Equivalence and Motivation





Theorem [Gupta-Kamath-Kayal-Saptharishi-16]

An n-var, deg-d poly computed by a ckt of size s can also be computed by a product-depth Δ ckt of size $s^{O(d^{1/2\Delta})}$.

PREVIOUS LOWER BOUNDS

Before 2021.

- Depth 3 circuits : $\Omega(n^3/(\log n)^3)$

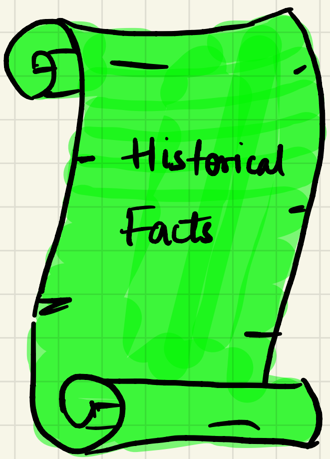
  [Kayal-Saha-Tavenas-16]

- Depth 4 circuits : $\Omega(n^{2.5})$

  [Gupta-Saha-Thankey-20]

- Constant depth ckts : $\Omega(\Delta n^{1+1/\Delta})$

  [Shoup-Smolensky-97, Raz 10]



Previous Lower Bounds

After 2021

Let $d = o(\log N / \log\log N)$

Needs large fields

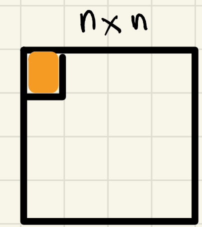
Theorem [Limaye - Srinivasan - Tavenas - 21]

There is an explicit N-var, deg-d poly P that has no algebraic ckts of product-depth Δ and size at most

$$N^{O(d^{1/(2^{2\Delta}-1)}/\Delta)}$$

Iterated Matrix Multiplication

$$\mathrm{IMM}(X_1, \ldots, X_d) = \underset{n \times n}{X_1} \; \underset{n \times n}{X_2} \; \cdots \; \underset{n \times n}{X_d}$$



$N \approx dn^2$

Set-multilinear w.r.t. $X = X_1 \sqcup \ldots \sqcup X_d$

- For every $\Delta \leq \log d$, $\mathrm{IMM}_{n,d}$ has product-depth Δ set-multilinear circuits of size $n^{O(d^{1/\Delta})}$

- No significantly better upper bound is known even for general bounded-depth circuits!

Improved Constant Depth Circuit Lower Bound

Needs large fields

Let $d = o(\log N / \log\log N)$

Theorem [B.-Dutta-Saxena-22]

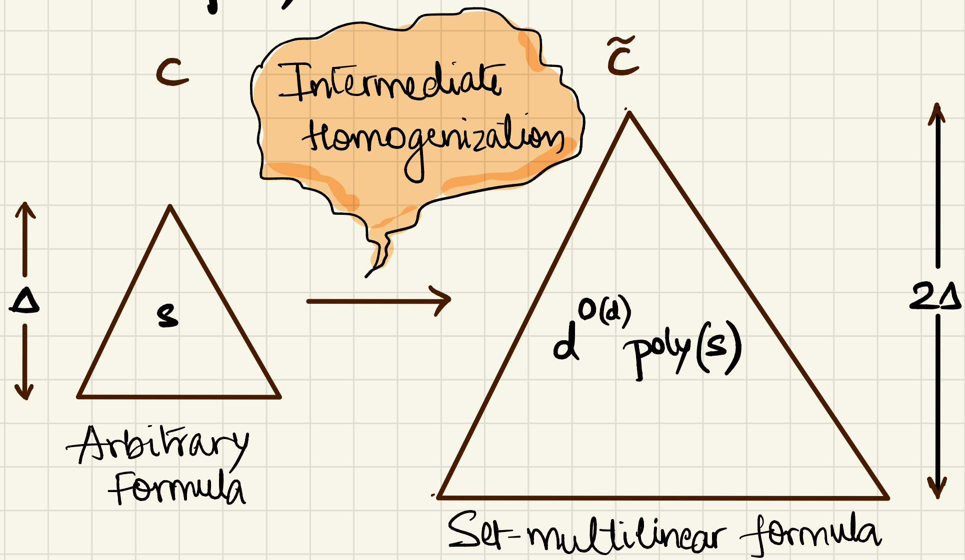
$IMM_{n,d}$ on $N = dn^2$ variables has no product-depth Δ algebraic circuits of size at most $N^{O(d^{1/F_{2\Delta}-1}/\Delta)}$

- Improvement over LST since $F_n = \Theta(\varphi^n) \ll 2^n$.

$\varphi = 1.618\ldots$

The LST Proof Idea

- Set-multilinearization : convert formulas computing set-multinear polynomials to set-multilinear formulas.

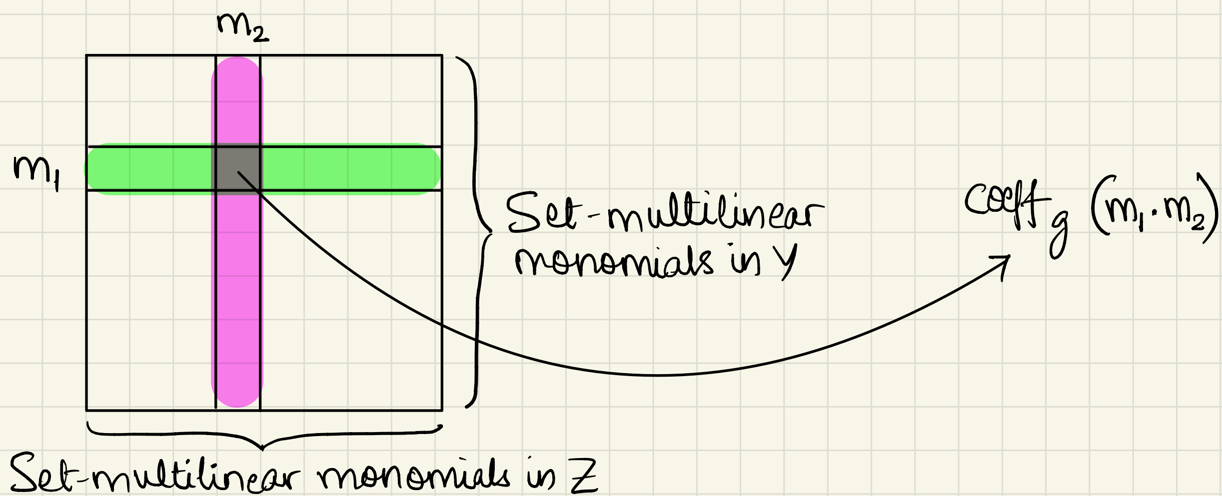


- Prove lower bounds for set-multilinear bounded-depth formulas.

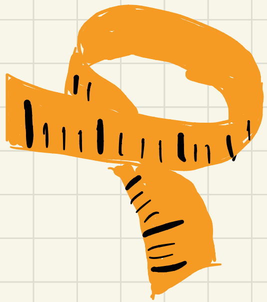
PROVING SET-MULTILINEAR LOWER BOUNDS

- Split $X = X_1 \sqcup \ldots \sqcup X_d$ into $Y \sqcup Z$ where
  $Y = Y_1 \sqcup \ldots \sqcup Y_r$ and $Z = Z_1 \sqcup \ldots \sqcup Z_{r'}$ $(r + r' = d)$

$M(g) =$



The Lower Bound Measure



Relative rank:

$$\text{rel-rank}(g) = \frac{\text{rank}(M(g))}{\sqrt{\#\text{rows} \cdot \#\text{columns}}}$$

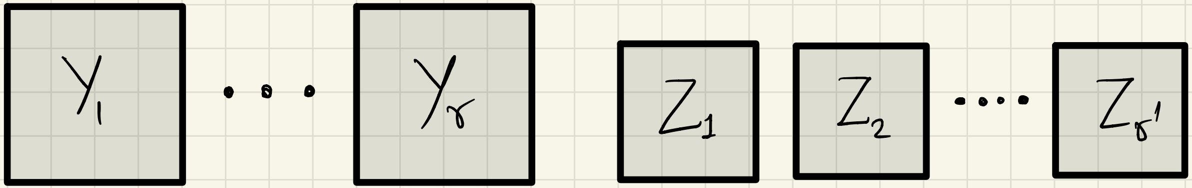
Properties

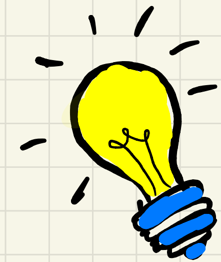
- $\text{rel-rank}(g) \leq \min\left\{\sqrt{\frac{\#\text{rows}}{\#\text{cols}}}, \sqrt{\frac{\#\text{cols}}{\#\text{rows}}}\right\} \leq 1$

- $\text{rel-rank}(f+g) \leq \text{rel-rank}(f) + \text{rel-rank}(g)$

- $\text{rel-rank}(f \cdot g) = \text{rel-rank}(f) \cdot \text{rel-rank}(g)$

Different Set Sizes





Maintain

columns

$$\prod_{i=1}^{r} \overset{= s_+}{|Y_i|} \approx \prod_{j=1}^{r'} \underset{= s_+^{\alpha}}{|Z_j|}$$

rows

- Different set sizes lead to a "cumulative" loss in rank.

- LST-21 choose two "fixed" set-sizes.

IMPROVED SET-MULTILINEAR LOWER BOUND

- Let degree $d = O(\log n)$.

Works over all fields.

Theorem [B.-Dutta-Saxena-22]

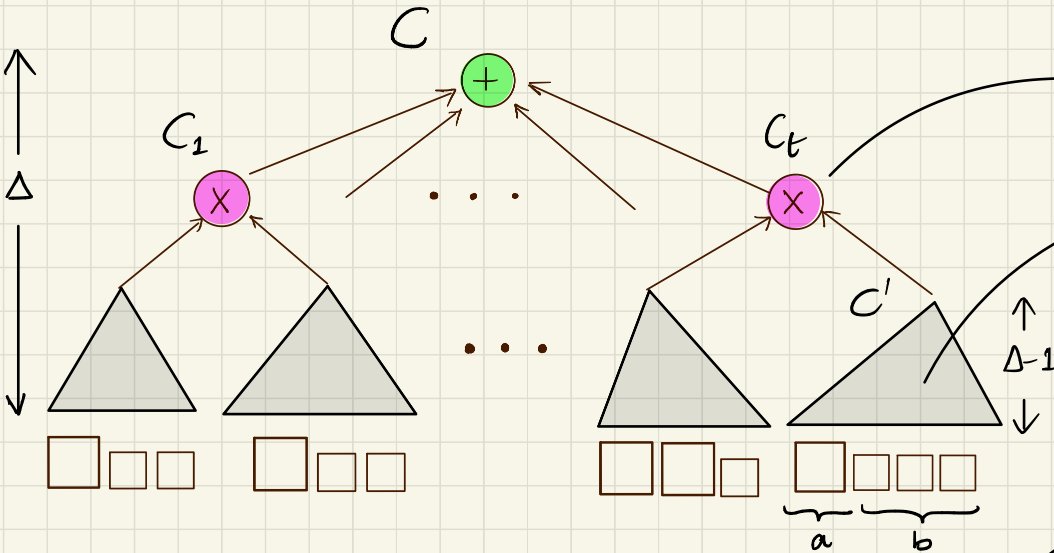
$IMM_{n,d}$ has no product-depth Δ set-multilinear circuits of size at most

$$n^{O(d^{1/F_\Delta - 1}/\Delta)}$$

$F_\Delta = \Theta(\varphi^\Delta) \ll 2^n$

- The set sizes we choose depend on the depth Δ and are chosen to satisfy a system of inequalities.

Choosing Set Sizes.



Suffices to bound the measure for one term

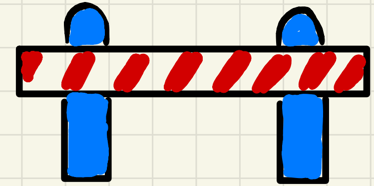
If deg is "high", the loss in the measure we get from induction is enough.

- All children of C_t have "low" degree.

Together, these give a set of constraints

$$\text{rel-rank}(C') \le \min\left\{\sqrt{\frac{\#\text{rows}}{\#\text{cols}}}, \sqrt{\frac{\#\text{cols}}{\#\text{rows}}}\right\} = 1/\sqrt{s_t^{a-\alpha b}}$$

Proof Barrier



* Fix $X_1,\dots,X_d$ s.t. $|X_i| \in \{s_1,\dots,s_r\}\ \forall i$

set sizes

Theorem [B.-Dutta-Saxena-22]

high relative rank

There exist poly P_Δ and Q_Δ set-multilinear wrt $X_1,\dots,X_d$ s.t

- P_Δ can be computed by product depth Δ set-ml ckts of size

$$n^{O(r\Delta d^{1/F_\Delta - 1})}$$

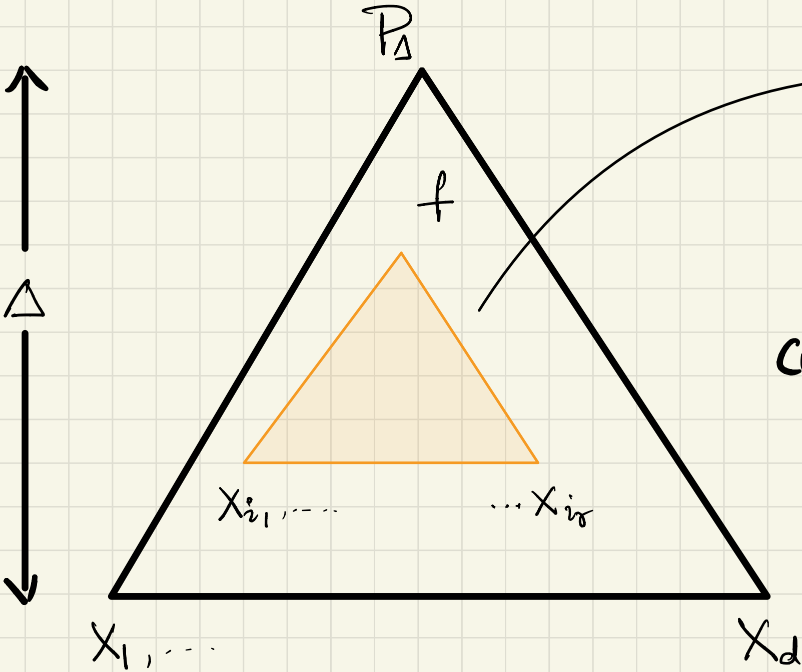
$r = O(1)$

- Q_Δ can be computed by product depth Δ set-ml ckts of size

$$n^{O(\Delta d^{1/F_{\Delta-1}^{-1}} + r)}$$

$r = d^{o(1)}$

Why Fibonacci?

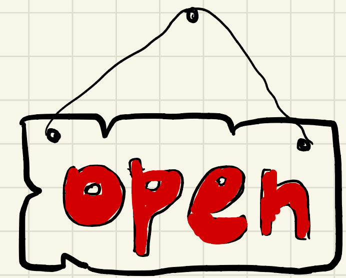


subformula of high relative rank.

cost $\approx$ loss in relative rank due to building f

The cost decreases like Fibonacci with depth.

Related Work And Open Questions



- Using d set sizes, can the bound be improved? Mostly not [Limaye-Srinivasan-Tavenas-22]

- Can other measures be used to improve the bound? Possibly! [Kush-Saraf-22], [Amireddy-Garg-Kayal-Saha-Thankey-22]

- Can we prove the "optimal" lower bound for IMM?


Thank you