Algebraic circuit size lower bounds for restricted circuits, in a functional setting

Suryajith Chillara
Algebraic/Arithmetic circuits

(1 + x_1)^2

An Arithmetic Circuit is a directed acyclic graph where
- leaf nodes: labelled by constants or variables,
- internal nodes: labelled by either $\times$ or $+$,
- edges: labelled by constants.

(2x_1 + x_2) \times x_3

Circuit size: number of nodes present in it. [Measure of complexity]

Circuit depth: length of the longest leaf to root path. [Measure of parallelizability]

Formulas: circuits where computations are not reused, i.e., directed tree.
Best known general lower bounds

- **Existential circuit size lower bound:** $\Omega\left(\sqrt{\frac{N+d}{d}}\right)$ [Folklore].

- **Explicit circuit size lower bound:** $\Omega(N \log N)$ [Baur and Strassen, TCS 1983].

- **Explicit formula size lower bound:** $\Omega(N^2)$ [Kalorkoti, SICOMP 1985].

Circuit size lower bounds are known for restricted arithmetic circuits.
Simplifications considered

General arithmetic circuits/formulas

- Bounded fan-in
- Constant depth
- Small depth
- Multilinear
- Multi-r-
  ic
- Homogeneous
Functional lower bounds

Functionally equivalent (denoted by $\equiv^B_{\text{fn}}$)

$$P \equiv^B_{\text{fn}} Q \quad \text{if} \quad P(a) = Q(a) \quad \forall \ a \in B^{|X|}.$$ 

Functional Lower Bounds

The evaluation table (over $B^N$) of any circuit in $\mathcal{C}$ of size at most $s$, is not equal to that of $P$.

Further, if $P \equiv^B_{\text{fn}} Q$ then

$$P \not\equiv^B_{\text{fn}} \text{ASIZE}(s) \quad \implies \quad Q \not\equiv^B_{\text{fn}} \text{ASIZE}(s).$$
Previously known functional lower bounds

▶ All the lower bounds known in the (set-)multilinear setting.

▶ Exponential bounds against $\Sigma \Pi \Sigma$ circuits over $F_{O(1)}$,
  
  - [Grigoriev and Karpinski, STOC 1998]
  - [Grigoriev and Razborov, FOCS 1998]
  - [C. and Mukhopadhyay, Inf & Comp. 2017]

▶ Exponential bound against homogeneous $\Sigma \Pi \Sigma \Sigma$ circuits over $F_{O(1)}$,

  - [Kumar and Saptharishi, CCC 2016]

▶ Restricted depth four and depth three circuits
  
  - [Forbes, Kumar and Saptharishi, CCC 2016]
Previously known functional lower bounds

- All the lower bounds known in the (set-)multilinear setting.
- Over $\mathbb{F}_{O(1)}$, exponential bounds against $\Sigma \Pi \Sigma$ circuits
- Over $\mathbb{F}_{O(1)}$, exponential bounds against $\Sigma \Pi \Sigma$ circuits
- Restricted depth four and depth three circuits [Forbes, Kumar and Saptharishi, CCC2016]
Previously known functional lower bounds

- All the lower bounds known in the (set-)multilinear setting.

- Over $\mathbb{F}_{O(1)}$, exponential bounds against $\Sigma \Pi \Sigma$ circuits
  - [Grigoriev and Karpinski, STOC 1998],

- Exponential bound against homogeneous $\Sigma \Pi \Sigma \Pi \Sigma$ circuits over $\mathbb{F}_{O(1)}$ [Kumar and Saptharishi, CCC 2016].

- Restricted depth four and depth three circuits [Forbes, Kumar and Saptharishi, CCC 2016].
Previously known functional lower bounds

- All the lower bounds known in the (set-)multilinear setting.

- Over $\mathbb{F}_{O(1)}$, exponential bounds against $\Sigma \Pi \Sigma$ circuits
  - [Grigoriev and Karpinski, STOC 1998],
  - [Grigoriev and Razborov, FOCS 1998], and

- Restricted depth four and depth three circuits [Forbes, Kumar and Saptharishi, CCC 2016].
Previously known functional lower bounds

- All the lower bounds known in the (set-)multilinear setting.

- Over $\mathbb{F}_{O(1)}$, exponential bounds against $\Sigma \Pi \Sigma$ circuits
  - [Grigoriev and Karpinski, STOC 1998],
  - [Grigoriev and Razborov, FOCS 1998], and
  - [C. and Mukhopadhyay, Inf&Comp. 2017].
Previously known functional lower bounds

- All the lower bounds known in the (set-)multilinear setting.
- Over $\mathbb{F}_{O(1)}$, exponential bounds against $\Sigma \Pi \Sigma$ circuits
  - [Grigoriev and Karpinski, STOC 1998],
  - [Grigoriev and Razborov, FOCS 1998], and
  - [C. and Mukhopadhyay, Inf&Comp. 2017].
- Exponential bound against homogeneous $\Sigma \Pi \Sigma \Pi \Sigma$ circuits over $\mathbb{F}_{O(1)}$ [Kumar and Saptharishi, CCC 2016].
Previously known functional lower bounds

- All the lower bounds known in the (set-)multilinear setting.

- Over $\mathbb{F}_{O(1)}$, exponential bounds against $\Sigma \Pi \Sigma$ circuits
  - [Grigoriev and Karpinski, STOC 1998],
  - [Grigoriev and Razborov, FOCS 1998], and
  - [C. and Mukhopadhyay, Inf&Comp. 2017].

- Exponential bound against homogeneous $\Sigma \Pi \Sigma \Pi \Sigma$ circuits over $\mathbb{F}_{O(1)}$ [Kumar and Saptharishi, CCC 2016].

- Restricted depth four and depth three circuits [Forbes, Kumar and Saptharishi, CCC 2016].
Boolean parts of polynomials

Boolean part of a polynomial

For a polynomial $P$, let $BP(P)$ be the Boolean function that simulates the evaluations of $P$ over $\{0, 1\}^N$. 
Boolean parts of polynomials

Boolean part of a polynomial

For a polynomial $P$, let $BP(P)$ be the Boolean function that simulates the evaluations of $P$ over $\{0, 1\}^N$.

Boolean part of a class $C$

For a circuit $C \in C$, let $BP(C)$ be the boolean circuit that simulates the evaluation of $C$ over $\{0, 1\}^N$.

$$BP(C) = \{BP(C) \mid C \in C\}.$$
Path to boolean lower bounds

Theorem [Bürgisser, TCS 2000]

1. (GRH) Over large fields,
   - $\text{FNC}^1/\text{poly} \subseteq \text{BP}(\text{VP}) \subseteq \text{FNC}^3/\text{poly}$ and
   - $\#P/\text{poly} \subseteq \text{BP}(\text{VNP}) \subseteq \text{FP}^{\#P}/\text{poly}$

2. For fixed size finite fields,
   - $\text{FNC}^1/\text{poly} \subseteq \text{BP}(\text{VP}) \subseteq \text{FNC}^2/\text{poly}$ and
   - $\#P/\text{poly} = \text{BP}(\text{VNP})$
Constant depth Boolean circuits

$\text{ACC}^0$

Constant depth circuits with AND, OR, NOT and MOD gates.

Theorem [Allender and Gore, SICOMP 1994]

$\text{Perm}/2^{\text{Uniform-ACC}^0}$.

Theorem [Williams, J. ACM 2014]

$\text{NEXP} \not\subseteq \text{Non-uniform-ACC}^0$.

Theorem [Murray and Williams, SICOMP 2020]

$\text{NQP} \not\subseteq \text{Non-uniform-ACC}^0$. 
Constant depth Boolean circuits

$\text{ACC}^0$

Constant depth circuits with AND, OR, NOT and MOD gates.

Theorem [Allender and Gore, SICOMP 1994]

Perm $\notin$ Uniform-$\text{ACC}^0$.
Constant depth Boolean circuits

$\text{ACC}^0$

Constant depth circuits with AND, OR, NOT and MOD gates.

Theorem [Allender and Gore, SICOMP 1994]

$\text{Perm} \not\in \text{Uniform-ACC}^0$.

Theorem [Williams, J.ACM 2014]

$\text{NEXP} \not\in \text{Non-uniform-ACC}^0$. 
Constant depth Boolean circuits

$\text{ACC}^0$

Constant depth circuits with AND, OR, NOT and MOD gates.

Theorem [Allender and Gore, SICOMP 1994]

\[ \text{Perm} \not\subseteq \text{Uniform-ACC}^0 . \]

Theorem [Williams, J.ACM 2014]

\[ \text{NEXP} \not\subseteq \text{Non-uniform-ACC}^0 . \]

Theorem [Murray and Williams, SICOMP 2020]

\[ \text{NQP} \not\subseteq \text{Non-uniform-ACC}^0 . \]
Theorem [Yao, FOCS 1985; Beigel-Tarui, CC 1994]

Every language $L$ in the class $\text{ACC}^0$ can be recognized by a family of depth two deterministic circuits with a symmetric function gate at the root and $2^{\log^{O(1)} n}$ many AND gates of fan-in $\log^{O(1)} n$. 
Observation

Observation [Forbes, Kumar and Saptharishi, CCC 2016]

Over \(\{0, 1\}^N\), any function \(F\) in \(\text{ACC}^0\) can also be computed algebraically as follows.

\[
F(X) = \sum_{i=1}^{s} (Q_i(X))^{d_i}.
\]

where \(s\) and each \(d_i\) are at most \(2^{\log^{O(1)} n}\). Further, monomials of \(Q_i\)'s are supported on at most \(\log^{O(1)} n\) variables.
Observation [Forbes, Kumar and Saptharishi, CCC 2016]

Over \( \{0, 1\}^N \), any function \( F \) in \( \text{ACC}^0 \) can also be computed algebraically as follows.

\[
F(X) = \sum_{i=1}^{s} (Q_i(X))^{d_i}.
\]

where \( s \) and each \( d_i \) are at most \( 2^{\log^{O(1)} n} \). Further, monomials of \( Q_i \)'s are supported on at most \( \log^{O(1)} n \) variables.

We denote such expressions by \( \Sigma \land \Sigma \Pi \).
An approach towards ACC\(^0\) lower bounds

A strategy

Show that there exists a function \(F\) such that

- the evaluation table of \(F\) \(\neq\) evaluation table of any “small” \(\Sigma \land \Sigma \Pi\) expressions, and

- \(F\) is computable in a class that is not “much larger” than ACC\(^0\).
An approach towards $\text{ACC}^0$ lower bounds

A strategy

Show that there exists a function $F$ such that

- the evaluation table of $F \neq$ evaluation table of any “small” $\Sigma \wedge \Sigma \Pi$ expressions, and
- $F$ is computable in a class that is not “much larger” than $\text{ACC}^0$.

Our result

There is a function $F$ such that

- $F$ is computable in $\text{GapL}$, and
- the evaluation table of $F$ is not equal to the evaluation table of any “small” and “bounded individual degree” $\Sigma \wedge \Sigma \Pi$ expressions.
Our results

Main result

There is a function $F$ such that

- $F$ is computable in $\text{GapL}$, and
- the evaluation table of $F \neq$ evaluation table of any “small” and “bounded individual degree” $\Sigma \land \Sigma \Pi$ expressions.
Our results

Main result

There is a function $F$ such that

- $F$ is computable in $\text{GapL}$, and

- the evaluation table of $F \neq$ evaluation table of any “small” and “bounded individual degree” $\Sigma \land \Sigma \Pi$ expressions.

This result is obtained by proving “functional” size lower bounds against restricted arithmetic circuits of depth four.
Bird’s eye view of proof

Step 1

There is an explicit polynomial $P$ such that it is not functionally equivalent to polynomials of bounded individual degree that are computed by "small" $\Sigma \land \Sigma \Pi$ circuits.

Step 2

Show that there is a function $F_{2 \text{GapL}}$ that simulates the evaluation of $P$ over $\{0, 1\}^N$. 
Bird’s eye view of proof

Step 1

There is an explicit polynomial $P$ such that it is not functionally equivalent to polynomials of bounded individual degree that are computed by “small” $\Sigma \land \Sigma \Pi$ circuits.
Bird’s eye view of proof

Step 1

There is an explicit polynomial $P$ such that it is not functionally equivalent to polynomials of bounded individual degree that are computed by “small” $\Sigma \land \Sigma \Pi$ circuits.

Step 2

Show that there is a function $F \in \text{GapL}$ that simulates the evaluation of $P$ over $\{0, 1\}^N$. 
Iterated Matrix Multiplication polynomial

\[ \text{IMM}_{n,d} = \sum_{(s \rightsquigarrow t) \text{ paths } \pi} \text{wt}(\pi) = \sum_{\pi_1, \pi_2, \ldots, \pi_d \in [n]} X^{(1)}_{\pi_1, \pi_1} \cdot X^{(2)}_{\pi_1, \pi_2} \cdot \ldots \cdot X^{(d)}_{\pi_d, 1} \]

\text{IMM}_{n,d} \text{ is the (1, 1) entry in the product of adjacency matrices } X_1, X_2, \ldots, X_d.

\{\text{IMM}_{n,d}\}_{n,d \geq 0} \in \text{VP} \text{ and has a depth four circuit of size } n^{O(\sqrt{d})}.\]
Step 1: Broad theme of the proof

Define a suitable complexity measure $\Gamma : \mathbb{F}[X] \mapsto \mathbb{R}$ such that the following holds:

- For any polynomial $f$ that is computed by a “small” circuit, $\Gamma(f)$ is “small”.

- For the target polynomial $P$, $\Gamma(P)$ is “large”.
Step 1: Broad theme of the proof

Define a suitable complexity measure $\Gamma : \mathbb{F}[X] \mapsto \mathbb{R}$ such that the following holds:

- For any polynomial $f$ that is computed by a “small” circuit, $\Gamma(f)$ is “small”.

- For the target polynomial $P$, $\Gamma(P)$ is “large”.

Multilinear Shifted Evaluation Dimension (denoted by $\text{mSED}_{k,\ell}^{[Y,Z]}(P(Y,Z))$)

$$\dim \left( \text{Eval}_{\{0,1\}^{\lfloor z \rfloor}} \left\{ \text{mult} \left( Z^{=\ell} \cdot \mathbb{F}\text{-span} \left\{ P(a, Z) \mid a \in \{0,1\}^{\lfloor Y \rfloor}_{\leq k} \right\} \right) \right\} \right)$$

Based on the measure of Shifted Evaluation Dimension, of [Forbes, Kumar, and Saptharishi, CCC 2016]
Evaluation Dimension

Let $\rho : X \mapsto Y \sqcup Z$ be a partitioning function.

$M_\rho(P) : \{0, 1\}^{|Y|} \rightarrow \{0, 1\}^{|Z|}$

Evaluation Dimension of $P$ wrt $\rho$ is $\text{rank}(M_\rho(P))$. 
Let $\rho : X \mapsto Y \sqcup Z$ be a partitioning function.

$$M_\rho(P) : \{0, 1\}^{|Y|} \to \{0, 1\}^{|Z|}$$

Evaluation Dimension of $P$ wrt $\rho$ is $\text{rank}(M_\rho(P))$.

Further,

$$\text{rank}(M_\rho(P)) = \dim \left( \text{Eval}_{\{0, 1\}^{|Z|}} \left( \mathbb{F}\text{-span} \left\{ P(a, Z) \mid a \in \{0, 1\}^{|Y|} \right\} \right) \right).$$
Evaluation Dimension

Let $\rho : X \mapsto Y \sqcup Z$ be a partitioning function.

$M_\rho(P)$:

Evaluation Dimension of $P$ wrt $\rho$ is $\text{rank}(M_\rho(P))$.

Further,

$$\text{rank}_{\leq k}(M_\rho(P)) = \dim \left( \text{Eval}_{0,1}^{\{0,1\}^{|Y|}} \left( \mathbb{F}-\text{span} \left\{ P(a,Z) \mid a \in \{0,1\}^{\leq k} \right\} \right) \right).$$
Partial derivatives as a proxy

For a set-multilinear polynomial $P$ and $a \in \{0, 1\}_{\leq k}$,\[
\frac{\partial^k P}{\partial Y^a} = P(a, Z).
\]

For a polynomial $Q$ of individual-degree at most $r$,\[
\mathbb{F}\text{-span} \left\{ Q(a, Z) \mid a \in \{0, 1\}_{\leq k} \right\} \subseteq \mathbb{F}\text{-span} \left\{ (\partial^{r \cdot k} Q)|_{Y=0} \right\}.
\]
Evolved measures

- **Shifted Evaluation Dimension** [Forbes, Kumar and Saptharishi, CCC 2016]:
  \[ \dim \left( \text{Eval}_{\{0,1\}^{|Z|}} \left\{ Z^\ell \cdot \mathbb{F}\text{-span} \left\{ P(a, Z) \mid a \in \{0, 1\}^{\leq k} \right\} \right\} \right) \]

- **Multilinear Shifted Evaluation Dimension** [Our work]:
  \[ \dim \left( \text{Eval}_{\{0,1\}^{|Z|}} \left\{ \text{mult} \left( Z^\ell \cdot \mathbb{F}\text{-span} \left\{ P(a, Z) \mid a \in \{0, 1\}^{\leq k} \right\} \right) \right\} \right) \]
Main Theorem

Let $n$ be a large integer and $d, k$ and $r$ be such that

- $\omega(\log^2 n) \leq d \leq n^{0.01}$ and
- $r \leq \frac{d}{1201k^2}$.

Any depth four $\Sigma \land \Sigma \Pi$ circuit of bounded individual degree $r$ computing a function equivalent to $\text{IMM}_{n,d}$ on $\{0, 1\}^{n^2d}$, must have size at least $n^{\Omega(k)}$. 
Step 2

Theorem [Vinay, CCC 1991]

Evaluation of $\text{IMM}_{n,d}$ over $\{0, 1\}^{n^2d}$ can be simulated in $\text{GapL}$. 
Our result

Main Theorem

Let $n$ be a large integer and $d$, $k$ and $r$ be such that

1. $\omega(\log^2 n) \leq d \leq n^{0.01}$ and
2. $r \leq \frac{d}{1201k^2}$.

Any depth four $\Sigma \land \Sigma \Pi$ circuit of bounded individual degree $r$ computing a function equivalent to $\text{IMM}_{n,d}$ on $\{0, 1\}^{n^2d}$, must have size at least $n^{\Omega(k)}$.

“Improving” this result could lead us to a separation of $\text{ACC}^0$ from $\text{GapL}$. 
## Other results and related work

<table>
<thead>
<tr>
<th>Circuit model</th>
<th>Work</th>
<th>Poly</th>
<th>Lower Bound</th>
<th>Range of parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>((\Sigma \land \Sigma \Pi) \leq r)</td>
<td>This work</td>
<td>IMM(_n,d)</td>
<td>(n^{\Omega(k)})</td>
<td>(\omega(\log^2 n) \leq d \leq n^{0.01}), and (r \leq \frac{d}{1201k^2}).</td>
</tr>
<tr>
<td>((\Sigma \Pi \Sigma \Pi) \leq r)</td>
<td>[FKS16]</td>
<td>NW(_m,d)</td>
<td>(2^{\Omega(\sqrt{d} \log (md))})</td>
<td>(m = \Theta(d^2)), and (r \leq O(1)).</td>
</tr>
<tr>
<td>((\Sigma \Pi \Sigma \Pi) \leq r)</td>
<td>This work</td>
<td>IMM(_n,d)</td>
<td>(n^{\Omega(\sqrt{\frac{d}{r}})})</td>
<td>(\omega(\log^2 n) \leq d \leq n^{0.01}), and (r \leq \frac{\log n}{12}).</td>
</tr>
</tbody>
</table>

[FKS16] = [Forbes, Kumar and Saptharishi, CCC 2016].
Further observations

At least one of the following is true.

▶ There exists a multilinear polynomial which is “hard” for $\Sigma \land \Sigma \Pi$ circuits but can be evaluated using a “small” $\Sigma \land \Sigma \Pi$ circuits.

▶ $\text{ACC}^0 \subsetneq \text{GapL}$. 
Thank you!