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

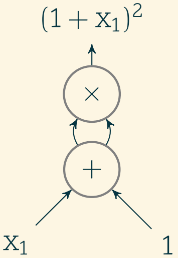
Suryajith Chillara

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY

HYDERABAD

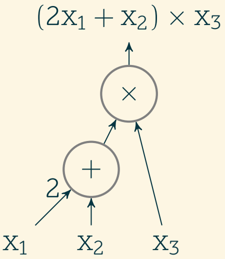
WACT 2023
28.03.2023

Algebraic/Arithmetic circuits



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.



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

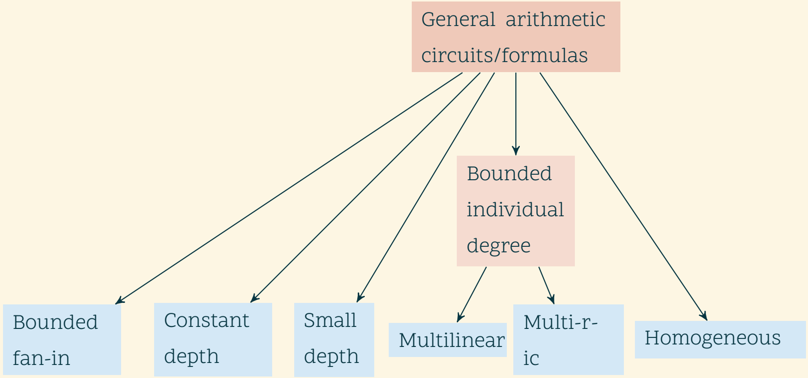
- Existential circuit size lower bound: $\Omega\left(\sqrt{\binom{N+d}{d}}\right)$ [Folklore].

- 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



Functional lower bounds

Functionally equivalent (denoted by $\equiv^{\mathbb{B}}_{\mathrm{fn}}$)

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

Functional Lower Bounds

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

Further, if $P \equiv^{\mathbb{B}}_{\mathrm{fn}} Q$ then

$$P \notin_{\mathrm{fn}} \mathsf{ASIZE}(s) \quad \implies \quad Q \notin_{\mathrm{fn}} \mathsf{ASIZE}(s)\,.$$

Previously known functional lower bounds

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

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

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],

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

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

Boolean part of a class $\mathcal{C}$

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

$$\mathsf{BP}(\mathcal{C}) = \{\mathsf{BP}(C) \mid C \in \mathcal{C}\}.$$

Path to boolean lower bounds

Theorem [Bürgisser, TCS 2000]

1. (GRH) Over large fields,
   - $\mathsf{FNC}^1/\mathrm{poly} \subseteq \mathsf{BP}(\mathsf{VP}) \subseteq \mathsf{FNC}^3/\mathrm{poly}$ and
   - $\#\mathsf{P}/\mathrm{poly} \subseteq \mathsf{BP}(\mathsf{VNP}) \subseteq \mathsf{FP}^{\#\mathsf{P}}/\mathrm{poly}$
2. For fixed size finite fields,
   - $\mathsf{FNC}^1/\mathrm{poly} \subseteq \mathsf{BP}(\mathsf{VP}) \subseteq \mathsf{FNC}^2/\mathrm{poly}$ and
   - $\#\mathsf{P}/\mathrm{poly} = \mathsf{BP}(\mathsf{VNP})$

Constant depth Boolean circuits

ACC^0

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

Constant depth Boolean circuits

ACC^0

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

Theorem [Allender and Gore, SICOMP 1994]

$$\mathsf{Perm} \notin \text{Uniform-}\mathsf{ACC}^0 .$$

Constant depth Boolean circuits

ACC^0

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

Theorem [Allender and Gore, SICOMP 1994]

$$\mathsf{Perm} \notin \text{Uniform-}\mathsf{ACC}^0 .$$

Theorem [Williams, J.ACM 2014]

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

Constant depth Boolean circuits

ACC^0

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

Theorem [Allender and Gore, SICOMP 1994]

$$\mathsf{Perm} \notin \text{Uniform-}\mathsf{ACC}^0 .$$

Theorem [Williams, J.ACM 2014]

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

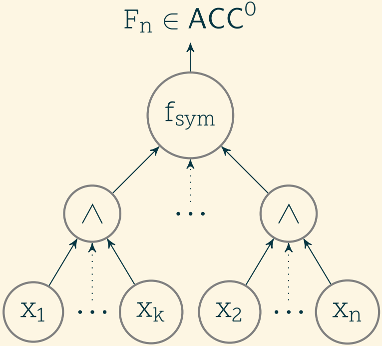
Theorem [Murray and Williams, SICOMP 2020]

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

Characterization for ACC^0

Theorem [Yao, FOCS 1985; Beigel-Tarui, CC 1994]

Every language L in the class 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 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

Observation [Forbes, Kumar and Saptharishi, CCC 2016]

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

$$F(X) = \sum_{i=1}^{s} \left(Q_i(X)\right)^{d_i} \, .$$

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 $\Sigma\wedge\Sigma\Pi$.

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" $\Sigma\wedge\Sigma\Pi$ expressions, and
- F is computable in a class that is not "much larger" than ACC^0.

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" $\Sigma\wedge\Sigma\Pi$ expressions, and
- F is computable in a class that is not "much larger" than ACC^0.

Our result

There is a function F such that

- F is computable in 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 GapL, and
- the evaluation table of $F \neq$ 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 GapL, and
- the evaluation table of F $\neq$ evaluation table of any "small" and "bounded individual degree" $\Sigma\wedge\Sigma\Pi$ expressions.

This result is obtained by proving "functional" size lower bounds against restricted arithmetic circuits of depth four.

Bird's eye view of proof

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” $\Sigma\wedge\Sigma\Pi$ circuits.

Bird's eye view of proof

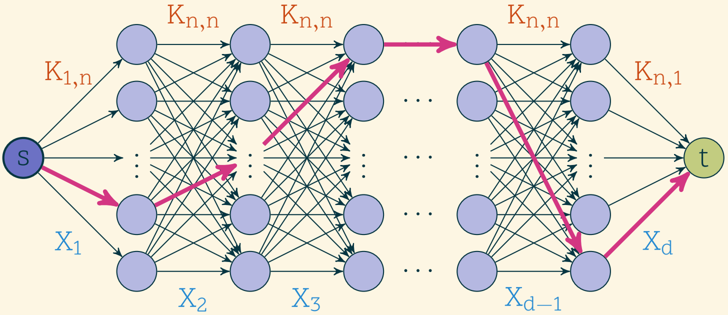
Step 1

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

Step 2

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

Iterated Matrix Multiplication polynomial



$$\mathrm{IMM}_{n,d} = \sum_{(s \rightsquigarrow t) \text{ paths } \pi} \mathrm{wt}(\pi)$$

$$= \sum_{\pi_1,\ldots,\pi_d \in [n]} x^{(1)}_{1,\pi_1} \cdot x^{(2)}_{\pi_1,\pi_2} \cdot \ldots \cdot x^{(d)}_{\pi_{d-1},1}$$

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

$\{\mathrm{IMM}_{n,d}\}_{n,d\geqslant 0} \in \mathrm{VP}$ 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 $\mathrm{mSED}_{k,\ell}^{[Y,Z]}(P(Y,Z))$)

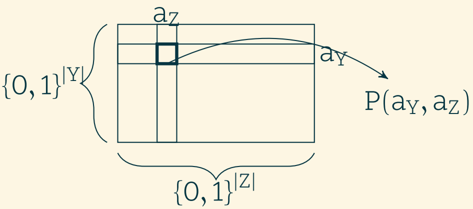
$$\dim\left(\mathrm{Eval}_{\{0,1\}^{|Z|}}\left\{\mathrm{mult}\left(Z^{=\ell}\cdot \mathbb{F}\text{-span}\left\{P(a,Z) \mid a\in\{0,1\}^{|Y|}_{\leqslant k}\right\}\right)\right\}\right)$$

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.

$M_\rho(P)$:

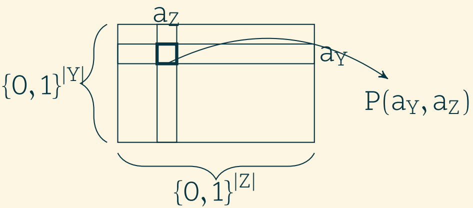


Evaluation Dimension of P wrt ρ is $\mathrm{rank}(M_\rho(P))$.

Evaluation Dimension

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

$M_\rho(P)$:



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

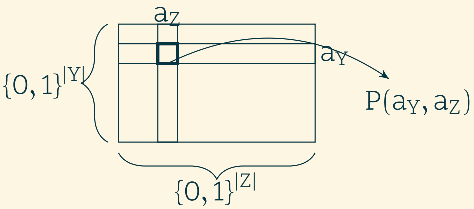
Further,

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

Evaluation Dimension

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

$M_\rho(P)$:



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

Further,

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

Partial derivatives as a proxy

- For a set-multilinear polynomial P and $a \in \{0,1\}^{||Y||}_{\leqslant k}$,

$$\frac{\partial^k P}{\partial Y^a} = P(a, Z).$$

- For a polynomial Q of individual-degree at most r,

$$\mathbb{F}\text{-span}\left\{Q(a, Z) \mid a \in \{0,1\}^{|Y|}_{\leqslant k}\right\} \subseteq \mathbb{F}\text{-span}\left\{(\partial^{\leqslant r \cdot k} Q)|_{Y=0}\right\}.$$

Evolved measures

- Shifted Evaluation Dimension [Forbes, Kumar and Saptharishi, CCC 2016]:

$$\dim\left(\mathrm{Eval}_{\{0,1\}^{|Z|}}\left\{Z^{=\ell}\cdot\mathbb{F}\text{-span}\left\{P(a,Z)\mid a\in\{0,1\}^{|Y|}_{\leqslant k}\right\}\right\}\right)$$

- Multilinear Shifted Evaluation Dimension [Our work]:

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

Formal statement

Main Theorem

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

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

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

Step 2

Theorem [Vinay, CCC 1991]

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

Our result

Main Theorem

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

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

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

“Improving” this result could lead us to a separation of ACC^0 from GapL.

Other results and related work

Circuit model	Work	Poly	Lower Bound	Range of parameters
$(\Sigma\wedge\Sigma\Pi)^{\leqslant r}$	This work	$\mathrm{IMM}_{n,d}$	$n^{\Omega(k)}$	$\omega(\log^2 n) \leqslant d \leqslant n^{0.01}$, and $r \leqslant \frac{d}{1201k^2}$.
$(\Sigma\Pi\Sigma\Pi)^{\leqslant r}_{[\leqslant d]}$	[FKS16]	$\mathrm{NW}_{m,d}$	$2^{\Omega\left(\sqrt{d}\log(md)\right)}$	$m = \Theta(d^2)$, and $r \leqslant O(1)$.
$(\Sigma\Pi\Sigma\Pi)^{\leqslant r}_{[\leqslant d]}$	This work	$\mathrm{IMM}_{n,d}$	$n^{\Omega\left(\sqrt{\frac{d}{r}}\right)}$	$\omega(\log^2 n) \leqslant d \leqslant n^{0.01}$, and $r \leqslant \frac{\log n}{12}$.

[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 $\Sigma\wedge\Sigma\Pi$ circuits but can be evaluated using a "small" $\Sigma\wedge\Sigma\Pi$ circuits.

- $\mathsf{ACC}^0 \subsetneq \mathsf{GapL}$.

Thank you!