Polynomial Identity Testing via Low-Rank Matrices

Robert Andrews
UIUC

Michael A. Forbes
UIUC

Based on work from STOC '22

Polynomial Identity Testing

Given a polynomial $f(\bar{x})$, does $f(\bar{x}) = 0$?

Polynomial Identity Testing

Given a polynomial $f(\bar{x})$, does $f(\bar{x}) = 0$?

Algorithm: Test $f(\bar{a}) \stackrel{?}{=} 0$ for random $\bar{a} \in [2 \cdot \deg(f)]^n$

Polynomial Identity Testing

Given a polynomial $f(\bar{x})$, does $f(\bar{x}) = 0$?

Algorithm: Test $f(\bar{a}) \stackrel{?}{=} 0$ for random $\bar{a} \in [2 \cdot \deg(f)]^n$

Applications:

- Parallel algorithms for perfect matching

Polynomial Identity Testing

Given a polynomial $f(\bar{x})$, does $f(\bar{x}) = 0$?

Algorithm: Test $f(\bar{a}) \stackrel{?}{=} 0$ for random $\bar{a} \in [2 \cdot \deg(f)]^n$

Applications:

- Parallel algorithms for perfect matching
- Primality testing

Polynomial Identity Testing

Given a polynomial $f(\bar{x})$, does $f(\bar{x}) = 0$?

Algorithm: Test $f(\bar{a}) \stackrel{?}{=} 0$ for random $\bar{a} \in [2 \cdot \deg(f)]^n$

Applications:

- Parallel algorithms for perfect matching
- Primality testing
- Polynomial factorization

$\vdots$

POLYNOMIAL IDENTITY TESTING

Given a polynomial $f(\bar{x})$, does $f(\bar{x}) = 0$?

Algorithm: Test $f(\bar{a}) \stackrel{?}{=} 0$ for random $\bar{a} \in [2 \cdot \deg(f)]^n$

Applications:

- Parallel algorithms for perfect matching
- Primality testing
- Polynomial factorization

$\vdots$

Question: Is there an efficient deterministic algorithm for PIT?

HITTING SET GENERATORS

Let $\mathcal{C} \subseteq \mathbb{F}[\bar{x}]$ be a set of polynomials.

Hitting Set Generators

Let $\mathcal{C} \subseteq \mathbb{F}[\bar{x}]$ be a set of polynomials.
A map

$$G : \mathbb{F}^{\ell} \longrightarrow \mathbb{F}^{n}$$

$$(y_1, \ldots, y_\ell) \longmapsto (G_1(\bar{y}), \ldots, G_n(\bar{y}))$$

is a hitting set generator for $\mathcal{C}$ if $\forall f(\bar{x}) \in \mathcal{C}$,

Hitting Set Generators

Let $\mathcal{C} \subseteq \mathbb{F}[\bar{x}]$ be a set of polynomials.
A map

$$\mathcal{G} : \mathbb{F}^{\ell} \longrightarrow \mathbb{F}^{n}$$

$$(y_1, \ldots, y_\ell) \longmapsto (\mathcal{G}_1(\bar{y}), \ldots, \mathcal{G}_n(\bar{y}))$$

is a *hitting set generator* for $\mathcal{C}$ if $\forall f(\bar{x}) \in \mathcal{C}$,

$$f(\bar{x}) = 0 \iff f(\mathcal{G}(\bar{y})) = 0 .$$

Hitting Set Generators

Let $\mathcal{C} \subseteq \mathbb{F}[\bar{x}]$ be a set of polynomials.
A map

$$\mathcal{G} : \mathbb{F}^{\ell} \to \mathbb{F}^{n}$$

$$(y_1, \ldots, y_\ell) \mapsto (\mathcal{G}_1(\bar{y}), \ldots, \mathcal{G}_n(\bar{y}))$$

is a hitting set generator for $\mathcal{C}$ if $\forall f(\bar{x}) \in \mathcal{C}$,

$$f(\bar{x}) = 0 \iff f(\mathcal{G}(\bar{y})) = 0 .$$

Parameters:

- seed length ℓ
- degree $\deg(\mathcal{G}) := \max_i \deg(\mathcal{G}_i(\bar{y}))$

Hitting Set Generators

A generator leads to faster PIT for $\mathcal{C}$:

HITTING SET GENERATORS

A generator leads to faster PIT for $\mathcal{C}$:

Algorithm 1

Test $f(\bar{x}) = 0$ by brute force

HITTING SET GENERATORS

A generator leads to faster PIT for $\mathcal{C}$:

Algorithm 1

Test $f(\bar{x}) = 0$ by brute force

evaluations

$(\deg(f)+1)^n$

Hitting Set Generators

A generator leads to faster PIT for $\mathcal{C}$:

Algorithm 1

Test $f(\bar{x}) = 0$ by brute force

evaluations

$(\deg(f) + 1)^n$

Algorithm 2

Test $f(G(\bar{y})) = 0$ by brute force

Hitting Set Generators

A generator leads to faster PIT for $\mathcal{C}$:

Algorithm 1

Test $f(\bar{x}) = 0$ by brute force

\# evaluations

$(\deg(f)+1)^n$

Algorithm 2

Test $f(G(\bar{y})) = 0$ by brute force

$(\deg(f)\cdot\deg(G)+1)^\ell$

DESIGNING GENERATORS

Weak circuit classes $\left(\Sigma\Pi,\ \Sigma\wedge\Sigma,\ \Sigma^{[k]}\Pi\Sigma,\ \text{read-once formulas, ROABPs, } \ldots \right)$

Designing Generators

Weak circuit classes ($\Sigma\Pi$, $\Sigma\wedge\Sigma$, $\Sigma^{[k]}\Pi\Sigma$, read-once formulas, ROABPs, ...)

1) Work hard to understand why these circuits are weak

Designing Generators

Weak circuit classes $\left(\Sigma\Pi,\ \Sigma\wedge\Sigma,\ \Sigma^{[k]}\Pi\Sigma, \right.$ read-once formulas, ROABPs, ... $)$

1) Work hard to understand why these circuits are weak

2) Design a generator that exploits this weakness

Designing Generators

Weak circuit classes ($\Sigma\Pi$, $\Sigma\wedge\Sigma$, $\Sigma^{[k]}\Pi\Sigma$, read-once formulas, ROABPs, ...)

1) Work hard to understand why these circuits are weak

2) Design a generator that exploits this weakness

Strong circuit classes ($\Sigma\Pi\Sigma$, $\Sigma\Pi\Sigma\Pi$, ..., formulas, ABPs, circuits)

Designing Generators

Weak circuit classes ($\Sigma\Pi$, $\Sigma\wedge\Sigma$, $\Sigma^{[k]}\Pi\Sigma$, read-once formulas, ROABPs, ...)

1) Work hard to understand why these circuits are weak

2) Design a generator that exploits this weakness

Strong circuit classes ($\Sigma\Pi\Sigma$, $\Sigma\Pi\Sigma\Pi$, ..., formulas, ABPs, circuits)

1) Work hard to develop hardness versus randomness

Designing Generators

Weak circuit classes ($\Sigma\Pi$, $\Sigma\wedge\Sigma$, $\Sigma^{[k]}\Pi\Sigma$, read-once formulas, ROABPs, ...)

1) Work hard to understand why these circuits are weak
2) Design a generator that exploits this weakness

Strong circuit classes ($\Sigma\Pi\Sigma$, $\Sigma\Pi\Sigma\Pi$, ..., formulas, ABPs, circuits)

1) Work hard to develop hardness versus randomness
2) Prove lower bounds for $\mathrm{perm}(X)$

Extending Hardness vs Randomness

Can we implement hardness versus randomness for weak circuit classes?

EXTENDING HARDNESS VS RANDOMNESS

Can we implement hardness versus randomness for weak circuit classes? Yes!

EXTENDING HARDNESS VS RANDOMNESS

Can we implement hardness versus randomness for weak circuit classes? Yes!

Theorem [A-Forbes]: $\exists$ explicit generator

$$\mathcal{G} : \mathbb{F}^{\ell} \to \mathbb{F}^{n} \text{ with } \ell = n^{\frac{1}{2} + o(1)}$$

that hits any circuit class $\mathcal{C}$ that

Extending Hardness vs Randomness

Can we implement hardness versus randomness for weak circuit classes? Yes!

Theorem [A-Forbes]: $\exists$ explicit generator

$$\mathcal{G} : \mathbb{F}^{\ell} \to \mathbb{F}^{n} \text{ with } \ell = n^{\frac{1}{2} + o(1)}$$

that hits any circuit class $\mathcal{C}$ that

1) is closed under projections

EXTENDING HARDNESS VS RANDOMNESS

Can we implement hardness versus randomness for weak circuit classes? Yes!

Theorem [A-Forbes]: $\exists$ explicit generator

$$\mathcal{G} : \mathbb{F}^{\ell} \to \mathbb{F}^{n} \text{ with } \ell = n^{\frac{1}{2}+o(1)}$$

that hits any circuit class $\mathcal{C}$ that

1) is closed under projections
2) ——————//—————— linear change of variables

EXTENDING HARDNESS VS RANDOMNESS

Can we implement hardness versus randomness for weak circuit classes? Yes!

Theorem [A-Forbes]: $\exists$ explicit generator

$$\mathcal{G} : \mathbb{F}^{\ell} \to \mathbb{F}^{n} \text{ with } \ell = n^{\frac{1}{2}+o(1)}$$

that hits any circuit class $\mathcal{C}$ that

1) is closed under projections
2) ——//—— linear change of variables
3) ——//—— limits

Extending Hardness vs Randomness

Can we implement hardness versus randomness for weak circuit classes? Yes!

Theorem [A-Forbes]: $\exists$ explicit generator

$$\mathcal{G} : \mathbb{F}^{\ell} \to \mathbb{F}^{n} \quad \text{with} \quad \ell = n^{\frac{1}{2} + o(1)}$$

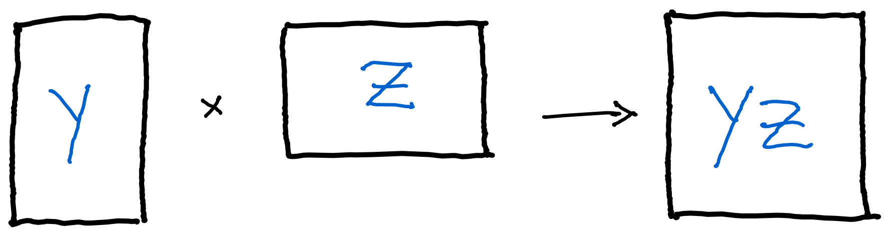
that hits any circuit class $\mathcal{C}$ that

1) is closed under projections
2) ——//—— linear change of variables
3) ——//—— limits
4) requires $n^{\omega(1)}$ size to compute $\det(X)$

THE GENERATOR

Definition: let $r \in \mathbb{N}$ and define

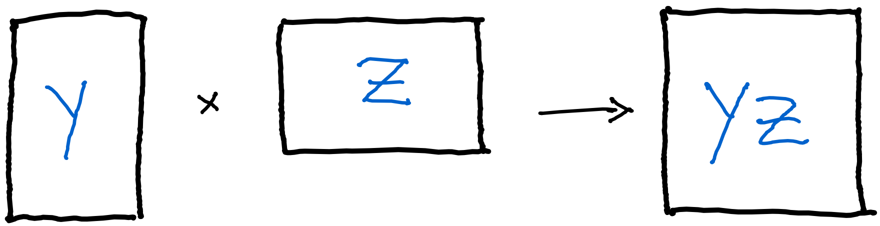
$$G_r : \mathbb{F}^{\sqrt{n} \times r} \times \mathbb{F}^{r \times \sqrt{n}} \longrightarrow \mathbb{F}^{\sqrt{n} \times \sqrt{n}}$$



The Generator

Definition: let $r \in \mathbb{N}$ and define

$$G_r : \mathbb{F}^{\sqrt{n} \times r} \times \mathbb{F}^{r \times \sqrt{n}} \longrightarrow \mathbb{F}^{\sqrt{n} \times \sqrt{n}}$$

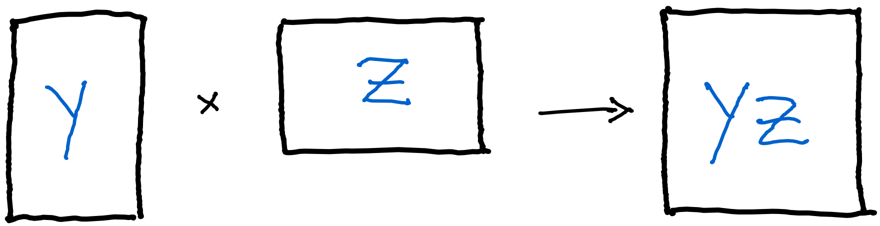


Clear that $\det_{r+1}\left(G_r(Y, Z)\right) = 0$

THE GENERATOR

Definition: let $r \in \mathbb{N}$ and define

$$G_r : \mathbb{F}^{\sqrt{n} \times r} \times \mathbb{F}^{r \times \sqrt{n}} \to \mathbb{F}^{\sqrt{n} \times \sqrt{n}}$$



Clear that $\det_{r+1}\big(G_r(Y, Z)\big) = 0$

Lemma [AF]: if a size-s $\mathcal{C}$-circuit vanishes on G_r, then the $r^{1/3} \times r^{1/3}$ determinant has a size-$s^{O(1)}$ $\mathcal{C}$-circuit

Low-Depth Circuits

Theorem [LST '21]: Any constant-depth circuit that computes $\det(X)$ must have size $\geq n^{(\log n)^{\Omega(1)}}$

Low-Depth Circuits

Theorem [LST '21]: Any constant-depth circuit that computes $\det(X)$ must have size $\geq n^{(\log n)^{\Omega(1)}}$

Corollary: constant-depth circuits of size s are hit by $\mathcal{G}_r$ for

$$r = 2^{(\log s)^{1-\Omega(1)}} = s^{o(1)}$$

Low-Depth Circuits

Theorem [LST '21]: Any constant-depth circuit that computes $\det(X)$ must have size $\geq n^{(\log n)^{\Omega(1)}}$

Corollary: constant-depth circuits of size s are hit by $\mathcal{G}_r$ for

$$r = 2^{(\log s)^{1-\Omega(1)}} = s^{o(1)}$$

Seed length: $2\sqrt{n} \cdot r = n^{1/2} s^{o(1)}$

Low-Depth Circuits

Theorem [LST '21]: Any constant-depth circuit that computes $\det(X)$ must have size $\geq n^{(\log n)^{\Omega(1)}}$

Corollary: constant-depth circuits of size s are hit by $\mathcal{G}_r$ for

$$r = 2^{(\log s)^{1-\Omega(1)}} = s^{o(1)}$$

Seed length: $2\sqrt{n} \cdot r = n^{1/2} s^{o(1)}$ Degree: 2

Low-Depth Circuits

Theorem [LST '21]: Any constant-depth circuit that computes $\det(X)$ must have size $\geq n^{(\log n)^{\Omega(1)}}$

Corollary: constant-depth circuits of size s are hit by $\mathcal{G}_r$ for

$$r = 2^{(\log s)^{1-\Omega(1)}} = s^{o(1)}$$

Seed length: $2\sqrt{n} \cdot r = n^{1/2} s^{o(1)}$ Degree: 2

Cost: $\Sigma\Pi$ circuit of size $2nr = n s^{o(1)}$ ($n \times r \times n$ matrix multiplication)

Low-Depth Circuits

Let $C(\tilde{x}) \neq 0$ be computed by a size-$n^{O(1)}$ constant-depth circuit.

LOW-DEPTH CIRCUITS

Let $C(\bar{x}) \neq 0$ be computed by a size-$n^{O(1)}$ constant-depth circuit.

For $r = n^{o(1)}$, the polynomial $C(G_r(Y,Z))$

Low-Depth Circuits

Let $C(\tilde{x}) \neq 0$ be computed by a size-$n^{O(1)}$ constant-depth circuit.

For $r = n^{o(1)}$, the polynomial $C(g_r(y,z))$

- is nonzero

Low-Depth Circuits

Let $C(\bar{x}) \neq 0$ be computed by a size-$n^{O(1)}$ constant-depth circuit.

For $r = n^{o(1)}$, the polynomial $C(G_r(Y,Z))$

- is nonzero
- can be computed by an $n^{O(1)}$ size constant-depth circuit

Low-Depth Circuits

Let $C(\bar{x}) \neq 0$ be computed by a size-$n^{O(1)}$ constant-depth circuit.

For $r = n^{o(1)}$, the polynomial $C(G_r(Y, Z))$

- is nonzero
- can be computed by an $n^{O(1)}$ size constant-depth circuit

Let $t = n^{o(1)}$. Then $G_t(V, W)$ hits $C \circ G_r$.

Low-Depth Circuits

Let $C(\bar{x}) \neq 0$ be computed by a size-$n^{O(1)}$ constant-depth circuit.

For $r = n^{o(1)}$, the polynomial $C(G_r(Y, Z))$

- is nonzero
- can be computed by an $n^{O(1)}$ size constant-depth circuit

Let $t = n^{o(1)}$. Then $G_t(V, W)$ hits $C \circ G_r$.

Equivalently, $G_r \circ G_t$ hits $C(\bar{x})$.

Low-Depth Circuits

Let $C(\bar{x}) \neq 0$ be computed by a size-$n^{O(1)}$ constant-depth circuit.

For $r = n^{o(1)}$ and $t = n^{o(1)}$, $\mathcal{G}_r \circ \mathcal{G}_t$ hits $C(\bar{x})$

Low-Depth Circuits

Let $C(\bar{x}) \neq 0$ be computed by a size-$n^{O(1)}$ constant-depth circuit.

For $r = n^{o(1)}$ and $t = n^{o(1)}$, $\mathcal{G}_r \circ \mathcal{G}_t$ hits $C(\bar{x})$

	$\mathcal{G}_r$	$\mathcal{G}_t$	$\mathcal{G}_r \circ \mathcal{G}_t$

Low-Depth Circuits

Let $C(\bar{x}) \neq 0$ be computed by a size-$n^{O(1)}$ constant-depth circuit.

For $r = n^{o(1)}$ and $t = n^{o(1)}$, $\mathcal{G}_r \circ \mathcal{G}_t$ hits $C(\bar{x})$

	$\mathcal{G}_r$	$\mathcal{G}_t$	$\mathcal{G}_r \circ \mathcal{G}_t$
Seed length			
Degree			
Cost			

Low-Depth Circuits

Let $C(\bar{x}) \neq 0$ be computed by a size-$n^{O(1)}$ constant-depth circuit.

For $r = n^{o(1)}$ and $t = n^{o(1)}$, $\mathcal{G}_r \circ \mathcal{G}_t$ hits $C(\bar{x})$

	$\mathcal{G}_r$	$\mathcal{G}_t$	$\mathcal{G}_r \circ \mathcal{G}_t$
Seed length	$n^{\frac{1}{2}+o(1)}$		
Degree	2		
Cost	$\Sigma\Pi$ ckt $n^{1+o(1)}$ size		

Low-Depth Circuits

Let $C(\bar{x}) \neq 0$ be computed by a size-$n^{O(1)}$ constant-depth circuit.

For $r = n^{o(1)}$ and $t = n^{o(1)}$, $\mathcal{G}_r \circ \mathcal{G}_t$ hits $C(\bar{x})$

	$\mathcal{G}_r$	$\mathcal{G}_t$	$\mathcal{G}_r \circ \mathcal{G}_t$
Seed length	$n^{1/2 + o(1)}$	$n^{1/4 + o(1)}$	
Degree	2	2	
Cost	$\Sigma\Pi$ ckt $n^{1+o(1)}$ size	$\Sigma\Pi$ ckt $n^{1/2+o(1)}$ size	

Low-Depth Circuits

Let $C(\bar{x}) \neq 0$ be computed by a size-$n^{O(1)}$ constant-depth circuit.

For $r = n^{o(1)}$ and $t = n^{o(1)}$, $\mathcal{G}_r \circ \mathcal{G}_t$ hits $C(\bar{x})$

	$\mathcal{G}_r$	$\mathcal{G}_t$	$\mathcal{G}_r \circ \mathcal{G}_t$
Seed length	$n^{1/2 + o(1)}$	$n^{1/4 + o(1)}$	$n^{1/4 + o(1)}$
Degree	2	2	4
Cost	$\Sigma\Pi$ ckt $n^{1+o(1)}$ size	$\Sigma\Pi$ ckt $n^{1/2+o(1)}$ size	$\Sigma\Pi\Sigma\Pi$ ckt $n^{1+o(1)}$ size

Low-Depth Circuits

Theorem [A-Forbes]: New generators for size-s constant-depth circuits

For every fixed $k \in \mathbb{N}$:

	This work
Seed length	
Degree	
Cost	

Low-Depth Circuits

Theorem [A-Forbes]: New generators for size-s constant-depth circuits

For every fixed $k \in \mathbb{N}$:

	This work
Seed length	$n^{1/2^k} s^{o(1)}$
Degree	
Cost	

Low-Depth Circuits

Theorem [A-Forbes]: New generators for size-s constant-depth circuits

For every fixed $k \in \mathbb{N}$:

	This work
Seed length	$n^{1/2^k} s^{o(1)}$
Degree	2^k
Cost	

Low-Depth Circuits

Theorem [A-Forbes]: New generators for size-s constant-depth circuits

For every fixed $k \in \mathbb{N}$:

	This work
Seed length	$n^{1/2^k} s^{o(1)}$
Degree	2^k
Cost	Depth-$2k$ ckt $n s^{o(1)}$ size

Low-Depth Circuits

Theorem [A-Forbes]: New generators for size-s constant-depth circuits

For every fixed $k \in \mathbb{N}$:

	This work
Seed length	$n^{1/2^k} s^{o(1)}$
Degree	2^k
Cost	Depth-$2k$ ckt $n s^{o(1)}$ size

Fact

Every generator with seed length ℓ and degree d satisfies

$$\binom{\ell + d}{d} \geq n$$

$$\rightsquigarrow \quad \ell \geq \Omega(n^{1/d})$$

Low-Depth Circuits

Theorem [A-Forbes]: New generators for size-s constant-depth circuits

For every fixed $k \in \mathbb{N}$:

	This work	[Limaye–Srinivasan–Tavenas '21] + [Chou–Kumar–Solomon '19]
Seed length	$n^{1/2^k} s^{o(1)}$	
Degree	2^k	
Cost	Depth-$2k$ ckt $n s^{o(1)}$ size	

Low-Depth Circuits

Theorem [A-Forbes]: New generators for size-s constant-depth circuits

For every fixed $k \in \mathbb{N}$:

	This work	[Limaye–Srinivasan–Tavenas '21] + [Chou–Kumar–Solomon '19]
Seed length	$n^{1/2^k} s^{o(1)}$	$n^{1/2^k} s^{o(1)}$
Degree	2^k	
Cost	Depth-$2k$ ckt $n s^{o(1)}$ size	

Low-Depth Circuits

Theorem [A-Forbes]: New generators for size-s constant-depth circuits

For every fixed $k \in \mathbb{N}$:

	This work	[Limaye–Srinivasan–Tavenas '21] + [Chou–Kumar–Solomon '19]
Seed length	$n^{1/2^k} s^{o(1)}$	$n^{1/2^k} s^{o(1)}$
Degree	2^k	$O\left(\frac{\log n}{\log \log n}\right)$
Cost	Depth-$2k$ ckt $ns^{o(1)}$ size	

LOW-DEPTH CIRCUITS

Theorem [A-Forbes]: New generators for size-s constant-depth circuits

For every fixed $k \in \mathbb{N}$:

	This work	[Limaye–Srinivasan–Tavenas '21] + [Chou–Kumar–Solomon '19]
Seed length	$n^{1/2^k} s^{o(1)}$	$n^{1/2^k} s^{o(1)}$
Degree	2^k	$O\left(\frac{\log n}{\log \log n}\right)$
Cost	Depth-$2k$ ckt $n s^{o(1)}$ size	Constant-depth ckt $s^{\Omega(1)}$ size *

LOW-DEPTH CIRCUITS

Theorem [A-Forbes]: New generators for size-$\cancel{s}$ $n^{O(1)}$ constant-depth circuits

For every fixed $k \in \mathbb{N}$:

	This work	[Limaye–Srinivasan–Tavenas '21] + [Chou–Kumar–Solomon '19]
Seed length	$n^{1/2^k} s^{o(1)}$	$n^{1/2^k} s^{o(1)}$
Degree	2^k	$O\left(\frac{\log n}{\log \log n}\right)$
Cost	General ckt $\tilde{O}(n)$ size	Constant-depth ckt $s^{\Omega(1)}$ size *

VANISHING IDEAL

Given a polynomial map $G : \mathbb{F}^{\ell} \to \mathbb{F}^{n}$,
its vanishing ideal is

$$\mathrm{Van}[G] := \left\{ f(\bar{x}) \in \mathbb{F}[\bar{x}] : f(G(\bar{y})) = 0 \right\}$$

VANISHING IDEAL

Given a polynomial map $\mathcal{G} : \mathbb{F}^{\ell} \to \mathbb{F}^{n}$,
its vanishing ideal is

$$\mathrm{Van}[\mathcal{G}] := \left\{ f(\bar{x}) \in \mathbb{F}[\bar{x}] : \quad f(\mathcal{G}(\bar{y})) = 0 \right\}$$

Lemma: A map $\mathcal{G}$ hits $\mathcal{C}$

$$\Updownarrow$$

$$\mathrm{Van}[\mathcal{G}] \cap \mathcal{C} \subseteq \{0\}$$

VANISHING IDEAL

Given a polynomial map $\mathcal{G} : \mathbb{F}^{\ell} \to \mathbb{F}^{n}$,
its vanishing ideal is

$$\mathrm{Van}[\mathcal{G}] := \left\{ f(\bar{x}) \in \mathbb{F}[\bar{x}] : f(\mathcal{G}(\bar{y})) = 0 \right\}$$

Lemma: A map $\mathcal{G}$ hits $\mathcal{C}$

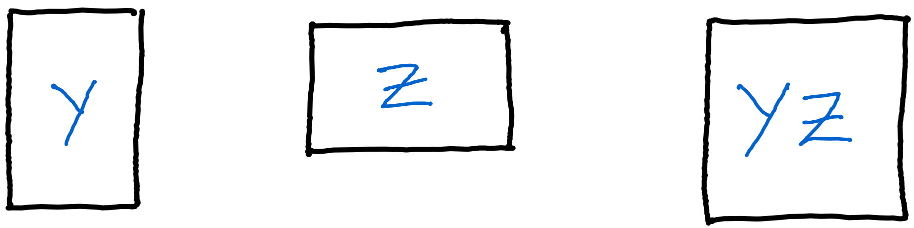
$$\Updownarrow$$

$$\mathrm{Van}[\mathcal{G}] \cap \mathcal{C} \subseteq \{0\}$$

Corollary: Correctness of $\mathcal{G}$ $\equiv$ Circuit lower bounds for $\mathrm{Van}[\mathcal{G}]$

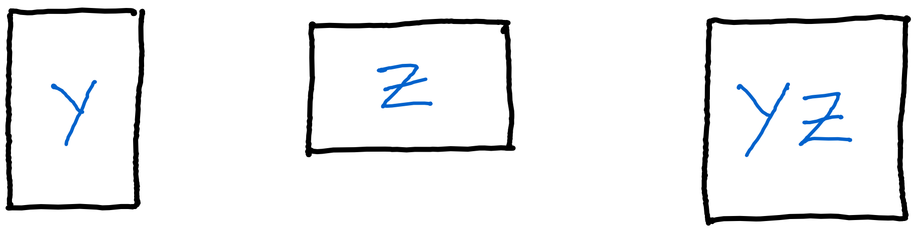
The Generator

$$\mathcal{G}_r : \mathbb{F}^{n \times r} \times \mathbb{F}^{r \times n} \to \mathbb{F}^{n \times n}$$



The Generator

$$\mathcal{G}_r : \mathbb{F}^{n\times r} \times \mathbb{F}^{r\times n} \to \mathbb{F}^{n\times n}$$



Fact: $\mathrm{Van}[\mathcal{G}_r] = \left\langle \det(X_{A,B}) : \begin{array}{l} A, B \subseteq [n] \\ |A| = |B| = r+1 \end{array} \right\rangle$

The Generator

$$G_r : \mathbb{F}^{n \times r} \times \mathbb{F}^{r \times n} \to \mathbb{F}^{n \times n}$$

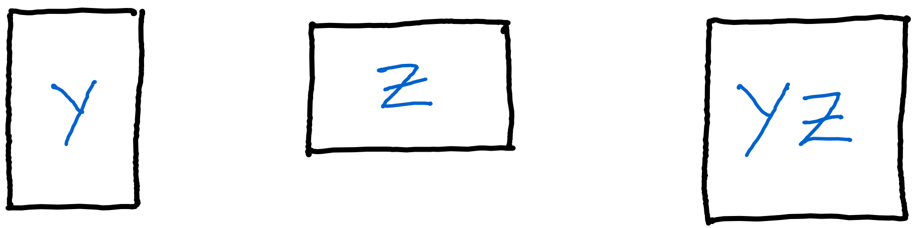
$$\boxed{Y} \qquad \boxed{Z} \qquad \boxed{YZ}$$

Fact: $\mathrm{Van}[G_r] = \left\langle \det(X_{A,B}) : \begin{array}{l} A, B \subseteq [n] \\ |A| = |B| = r+1 \end{array} \right\rangle$

$$\langle g_1(X), \dots, g_m(X) \rangle := \left\{ \sum_{i=1}^{m} f_i(X)\, g_i(X) : f_i \in \mathbb{F}[X] \right\}$$

The Generator

$$G_r : \mathbb{F}^{n\times r} \times \mathbb{F}^{r\times n} \to \mathbb{F}^{n\times n}$$



Fact: $$\mathrm{Van}[G_r] = \left\langle \det(X_{A,B}) : \begin{array}{c} A, B \subseteq [n] \\ |A| = |B| = r+1 \end{array} \right\rangle$$

We want to prove circuit lower bounds for all nonzero polynomials here

$$\langle g_1(X), \dots, g_m(X) \rangle := \left\{ \sum_{i=1}^{m} f_i(X)\, g_i(X) : f_i \in \mathbb{F}[X] \right\}$$

Complexity in Ideals

Goal: small ckt for some $f \in \langle r \times r \text{ minors of } X \rangle$

$\Longrightarrow$ small ckt for $r^{\Theta(1)} \times r^{\Theta(1)}$ determinant

Complexity in Ideals

Goal: small ckt for some $f \in \langle r \times r \text{ minors of } X \rangle$

$\Longrightarrow$ small ckt for $r^{\Theta(1)} \times r^{\Theta(1)}$ determinant

How to prove this?

Complexity in Ideals

Goal: small ckt for some $f \in \langle r \times r \text{ minors of } X \rangle$

$\Rightarrow$ small ckt for $r^{\Theta(1)} \times r^{\Theta(1)}$ determinant

How to prove this?

- For $r = n$, we have $f(X) = g(X) \cdot \det(X)$, and need to factor f [Kaltofen '87, Bürgisser '04, ...]

Complexity in Ideals

Goal: small ckt for some $f \in \langle r \times r \text{ minors of } X \rangle$

$\Rightarrow$ small ckt for $r^{\Theta(1)} \times r^{\Theta(1)}$ determinant

How to prove this?

- For $r = n$, we have $f(X) = g(X) \cdot \det(X)$ and need to factor f [Kaltofen '87, Bürgisser '04, ...]
- For $r < n$, we also have to handle cancellations

MAIN TECHNICAL RESULT

Theorem [AF '22]

MAIN TECHNICAL RESULT

Theorem [AF '22]

$\forall \varepsilon > 0$,

MAIN TECHNICAL RESULT

Theorem [AF '22]

$\forall \varepsilon > 0$, $\forall f(X) \in \langle r \times r$ minors of $n \times n$ matrix $X \rangle$,

Main Technical Result

Theorem [AF '22]

$\forall \varepsilon > 0$, $\forall f(X) \in \langle r \times r$ minors of $n \times n$ matrix $X \rangle$,

$\exists$ circuit

Main Technical Result

Theorem [AF '22]

$\forall \varepsilon > 0$, $\forall f(X) \in \langle r \times r$ minors of $n \times n$ matrix $X \rangle$,

$\exists$ circuit

$y_{1,1}$

$y_{1,2}$

$\vdots$

$y_{t,t}$

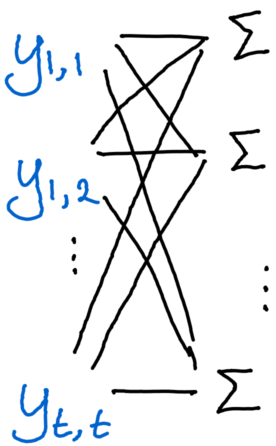
$t = \Theta(r^{1/3})$

MAIN TECHNICAL RESULT

Theorem [AF '22]

$\forall \varepsilon > 0$, $\forall f(X) \in \langle r \times r$ minors of $n \times n$ matrix $X \rangle$,

$\exists$ circuit



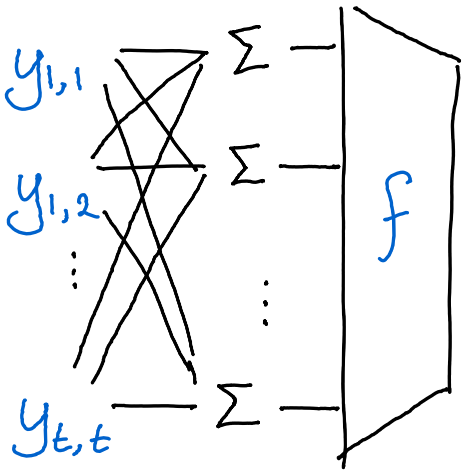
$t = \Theta(r^{1/3})$

MAIN TECHNICAL RESULT

Theorem [AF '22]

$\forall \varepsilon > 0$, $\forall f(X) \in \langle r \times r$ minors of $n \times n$ matrix $X \rangle$,

$\exists$ circuit



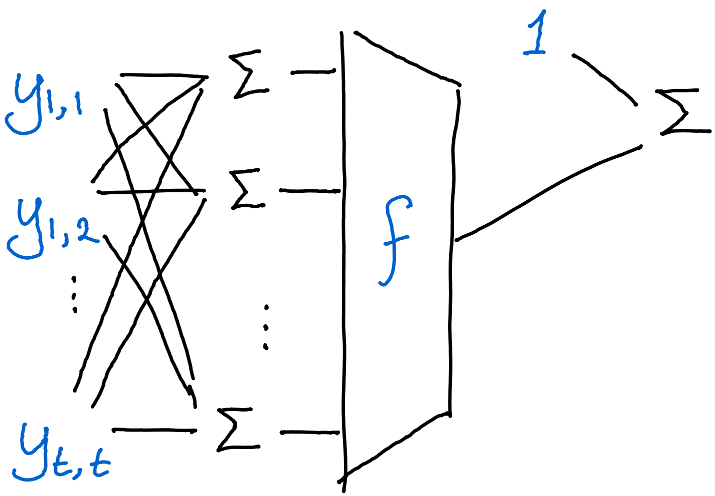
$t = \Theta(r^{1/3})$

Main Technical Result

Theorem [AF '22]

$\forall \varepsilon > 0, \ \forall f(X) \in \langle r \times r$ minors of $n \times n$ matrix $X \rangle$,

$\exists$ circuit



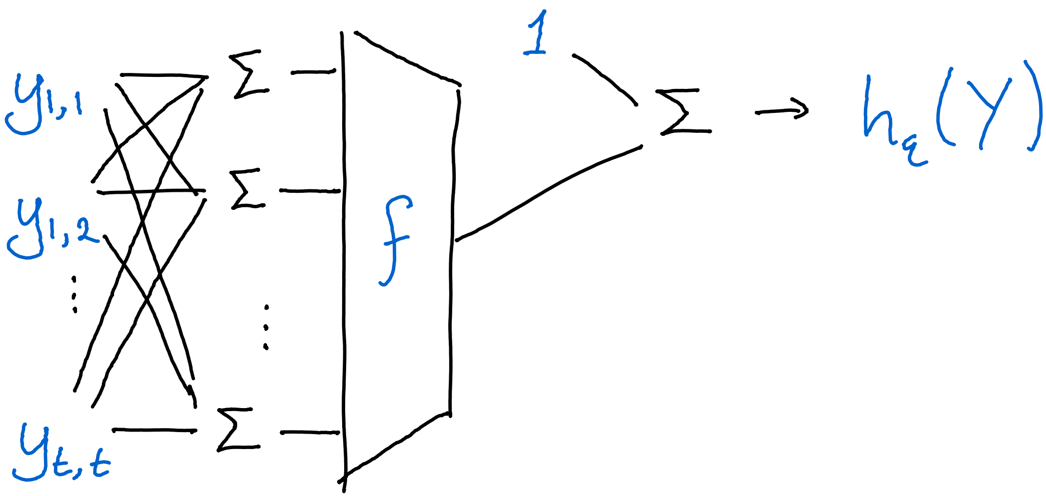
$t = \Theta(r^{1/3})$

MAIN TECHNICAL RESULT

Theorem [AF '22]

$\forall \varepsilon > 0$, $\forall f(X) \in \langle r \times r$ minors of $n \times n$ matrix $X \rangle$,

$\exists$ circuit



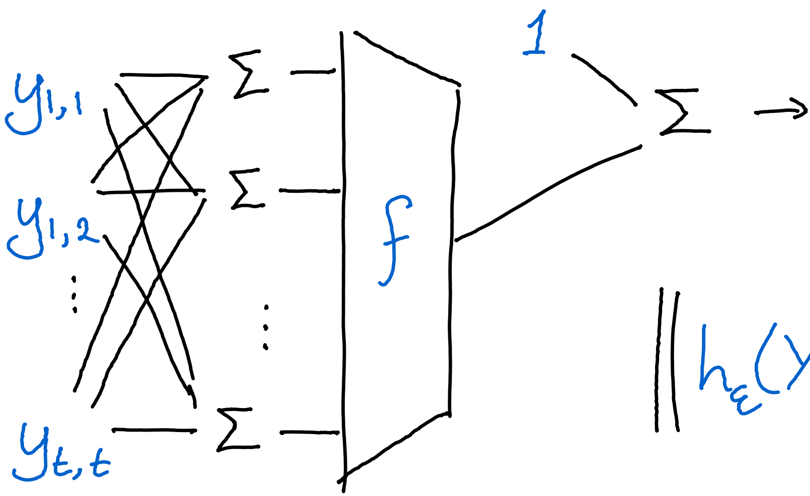
$t = \Theta(r^{1/3})$

Main Technical Result

Theorem [AF '22]

$\forall \varepsilon > 0$, $\forall f(X) \in \langle r \times r \text{ minors of } n \times n \text{ matrix } X \rangle$,

$\exists$ circuit



$\to h_\varepsilon(Y)$

such that

$$\| h_\varepsilon(Y) - \det(Y) \| \leq \varepsilon$$

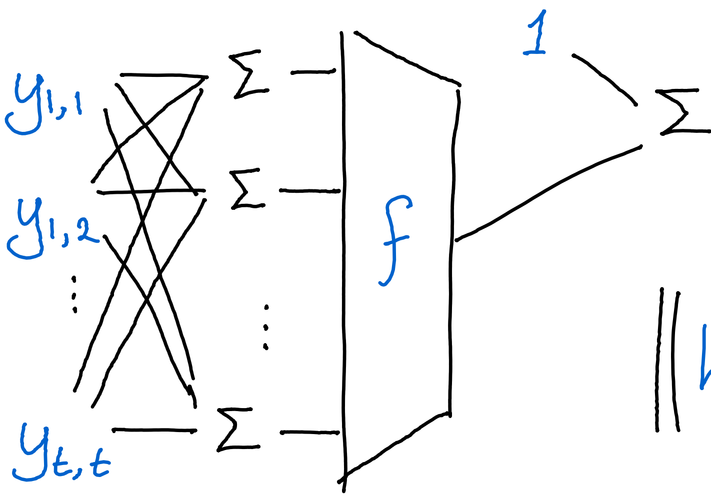
$t = \Theta(r^{1/3})$

Main Technical Result

Theorem [AF '22]

$\forall \varepsilon > 0, \ \forall f(X) \in \langle r \times r$ minors of $n \times n$ matrix $X \rangle$,

$\exists$ circuit



$\rightarrow h_\varepsilon(Y)$

$t = \Theta(r^{1/3})$

such that

$$\| h_\varepsilon(Y) - \det(Y) \| \leq \varepsilon$$

(if $\mathrm{char}(\mathbb{F}) = p > 0$, $h_\varepsilon \approx \det(Y)^{p^k}$)

PROOF OUTLINE

Given $f(X) \in I := \langle r \times r \text{ minors of } X \rangle$

Proof Outline

Given $f(X) \in I := \langle r \times r \text{ minors of } X \rangle$

Roadblock: expression $f = \sum_{A, B \subseteq [n]} \det(X_{A,B}) \cdot g_{A,B}(X)$ is hard to control

PROOF OUTLINE

Given $f(X) \in I := \langle r \times r \text{ minors of } X \rangle$

Roadblock: expression $f = \sum_{A, B \subseteq [n]} \det(X_{A,B}) \cdot g_{A,B}(X)$ is hard to control

- In general, this expression is not unique

Proof Outline

Given $f(X) \in I := \langle r \times r \text{ minors of } X \rangle$

Roadblock: expression $f = \sum_{A, B \subseteq [n]} \det(X_{A,B}) \cdot g_{A,B}(X)$ is hard to control

- In general, this expression is not unique
- The $g_{A,B}(X)$ are arbitrary polynomials

Proof Outline

Given $f(X) \in I := \langle r \times r \text{ minors of } X \rangle$

Roadblock: expression $f = \sum_{A, B \subseteq [n]} \det(X_{A,B}) \cdot g_{A,B}(X)$ is hard to control

- In general, this expression is not unique
- The $g_{A,B}(X)$ are arbitrary polynomials

$\boxed{\text{Find } \underline{\text{alternate basis}} \ \mathcal{B} \subseteq \mathbb{F}[X]}$

Proof Outline

Given $f(X) \in I := \langle r \times r \text{ minors of } X \rangle$

$$\boxed{\textcircled{\scriptsize 0}\quad \text{Find } \underline{\text{alternate basis}} \quad B \subseteq \mathbb{F}[X]}$$

Proof Outline

Given $f(X) \in I := \langle r \times r \text{ minors of } X \rangle$

$\boxed{0 \quad \text{Find } \underline{\text{alternate basis}} \quad \mathcal{B} \subseteq \mathbb{F}[X]}$

1 Linear change of variables $x_{i,j} \longmapsto \ell_{i,j}(X, \varepsilon)$

sending $f(X) \to h(X) + O(\varepsilon^2)$

for some $h(X) \in \mathcal{B} \cap I$

Proof Outline

Given $f(X) \in I := \langle r \times r \text{ minors of } X \rangle$

0 Find alternate basis $\mathcal{B} \subseteq \mathbb{F}[X]$

1 Linear change of variables $x_{i,j} \longmapsto \ell_{i,j}(X, \varepsilon)$

sending $f(X) \to h(X) + O(\varepsilon^2)$

for some $h(X) \in \mathcal{B} \cap I$

2 Well-behaved projection $X \to \mathbb{F}(\varepsilon)[Y]$

sending $h(X) \longrightarrow 1 + \varepsilon \cdot \det_{r^{1/3}}(Y) + O(\varepsilon^2)$

SPARSIFICATION LEMMA

Lemma [AF '22]

Let $f(X) \in \langle r \times r \text{ minors of } X \rangle$.

SPARSIFICATION LEMMA

Lemma [AF '22]

Let $f(X) \in \langle r \times r \text{ minors of } X \rangle$.

$\exists$ invertible linear change of variables $X \to L(X, \varepsilon)$ such that

$$f(L(X,\varepsilon)) =$$

SPARSIFICATION LEMMA

Lemma [AF '22]

Let $f(X) \in \langle r \times r \text{ minors of } X \rangle$.

$\exists$ invertible linear change of variables $X \to L(X, \varepsilon)$ such that

$$f(L(X,\varepsilon)) = \prod_{i=1}^{n} \det(X_{\leq i, \leq i})^{a_i}$$

SPARSIFICATION LEMMA

Lemma [AF '22]

Let $f(X) \in \langle r \times r \text{ minors of } X \rangle$.

$\exists$ invertible linear change of variables $X \to L(X, \varepsilon)$ such that

$$f(L(X,\varepsilon)) = \prod_{i=1}^{n} \det(X_{\leq i, \leq i})^{a_i} + O(\varepsilon)$$

Sparsification Lemma

Lemma [AF '22]

Let $f(X) \in \langle r \times r \text{ minors of } X \rangle$.

$\exists$ invertible linear change of variables $X \to L(X, \varepsilon)$ such that

$$f(L(X,\varepsilon)) = \prod_{i=1}^{n} \det(X_{\leq i, \leq i})^{a_i} + O(\varepsilon)$$

where $\max(a_r, \dots, a_n) \geq 1$

SPARSIFICATION LEMMA

Lemma [AF '22]

Let $f(X) \in \langle r \times r \text{ minors of } X \rangle$.

$\exists$ invertible linear change of variables $X \to L(X, y)$ ~~$L(X, \varepsilon)$~~

such that the leading coefficient of $f(L(X,y))$

$$= \prod_{i=1}^{n} \det\left(X_{\leq i, \leq i}\right)^{a_i}$$

where $\max(a_r, \dots, a_n) \geq 1$

PROJECTION LEMMA

Lemma [AF '22]

Let Y be an $m \times m$ matrix of variables.

Projection Lemma

Lemma [AF '22]

Let Y be an $m \times m$ matrix of variables.

$\exists$ matrix $M(Y)$ of size $t = O(m^3)$

PROJECTION LEMMA

Lemma [AF '22]

Let Y be an $m \times m$ matrix of variables.

$\exists$ matrix $M(Y)$ of size $t = O(m^3)$ such that

$$\det_k\left(M(Y)_{\leq k, \leq k} \right) =$$

PROJECTION LEMMA

Lemma [AF '22]

Let Y be an $m \times m$ matrix of variables.

$\exists$ matrix $M(Y)$ of size $t = O(m^3)$ such that

$$\det_k \left(M(Y)_{\leq k, \leq k} \right) = \begin{cases} & \text{if } k = t \\ & \text{if } k < t \end{cases}$$

Projection Lemma

Lemma [AF '22]

Let Y be an $m \times m$ matrix of variables.

$\exists$ matrix $M(Y)$ of size $t = O(m^3)$ such that

$$\det_k\left(M(Y)_{\le k, \le k}\right) = \begin{cases} 1 + \varepsilon \cdot \det_m(Y) & \text{if } k = t \\ & \text{if } k < t \end{cases}$$

Projection Lemma

Lemma [AF '22]

Let Y be an $m \times m$ matrix of variables.

$\exists$ matrix $M(Y)$ of size $t = O(m^3)$ such that

$$\det_k\left(M(Y)_{\le k, \le k}\right) = \begin{cases} 1 + \varepsilon \cdot \det_m(Y) & \text{if } k = t \\ 1 & \text{if } k < t \end{cases}$$

PROJECTION LEMMA

Lemma [AF '22]

Let Y be an $m \times m$ matrix of variables.

$\exists$ matrix $M(Y)$ of size $t = O(m^3)$ such that

$$\det_k\left(M(Y)_{\leq k, \leq k}\right) = \begin{cases} 1 + \varepsilon \cdot \det_m(Y) & \text{if } k = t \\ 1 & \text{if } k < t \end{cases}$$

Proof uses simulation of ABPs by det [Valiant '79]
+ small ABPs for det [Mahajan-Vinay '97]

Open Questions

(1) Can these techniques be adapted to other circuit classes?

Open Questions

(1) Can these techniques be adapted to other circuit classes?

(2) Is border complexity necessary?

Open Questions

(1) Can these techniques be adapted to other circuit classes?

(2) Is border complexity necessary?

(3) What can be said about the complexity of other ideals, like

$$\left\langle \operatorname{perm}(X_{S,T}) : \begin{array}{c} S, T \subseteq [n] \\ |S| = |T| = r \end{array} \right\rangle ?$$

Open Questions

(1) Can these techniques be adapted to other circuit classes?

(2) Is border complexity necessary?

(3) What can be said about the complexity of other ideals, like

$$\left\langle \mathrm{perm}(X_{S,T}) : \begin{array}{c} S, T \subseteq [n] \\ |S| = |T| = r \end{array} \right\rangle ?$$

Thank You!