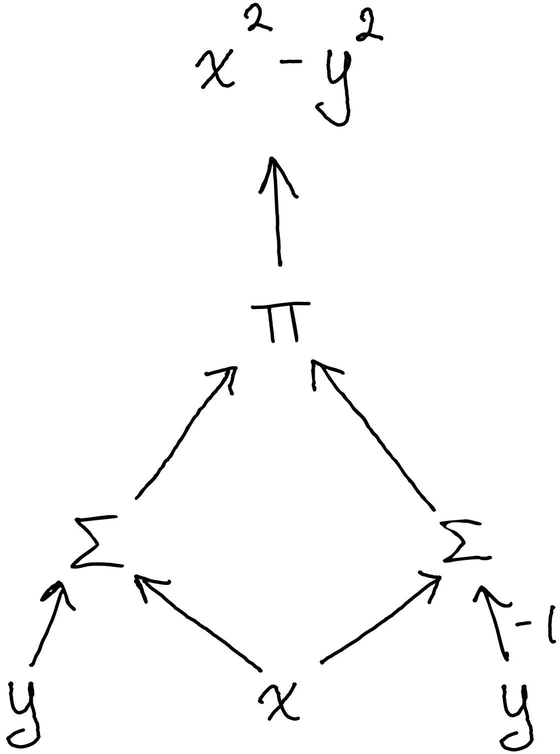
Ideals, Determinants, and Straightening

ICMS Edinburgh 2022

Robert Andrews
UIUC

Michael A. Forbes
UIUC

ALGEBRAIC CIRCUITS



Typical Question

Given a family of polynomials

$$\{ f_n(x_1,\dots,x_n) \in \mathbb{F}[x_1,\dots,x_n] : n \in \mathbb{N} \},$$

what is the complexity of computing $f_n(\bar{x})$ as a formal polynomial?

Examples: $\det_n(X)$, $\mathrm{perm}_n(X)$

Ideals

Definition

The ideal generated by $\{g_1, \dots, g_N\} \subseteq \mathbb{F}[\bar{x}]$ is

$$\langle g_1, \dots, g_N \rangle := \left\{ \sum_{i=1}^{N} h_i \cdot g_i \ : \ h_1, \dots, h_N \in \mathbb{F}[x_1, \dots, x_n] \right\}$$

Modified Question

Given a family of ideals $\{ I_n \subseteq \mathbb{F}[x_1, \dots, x_n] : n \in \mathbb{N} \}$, what is the minimum complexity of computing some nonzero polynomial $f_n \in I_n$?

Complexity Of Ideals

Theorem [Kaltofen '87, Bürgisser '04]

g requires large circuits $\Rightarrow$ $\forall f(x) \in \langle g(x) \rangle$, f requires large circuits

g has small circuit $\Leftarrow$ $\exists f(x) \in \langle g(x) \rangle$ with small circuit

Question What about ideals with ≥ 2 generators?

Answer Very little is known!

Applications:

- Derandomizing polynomial identity testing
- Lower bounds in proof complexity

DETERMINANTAL IDEALS

Conjecture [Grochow '18]

$$I_n := \left\langle \tfrac{n}{2} \times \tfrac{n}{2} \text{ minors of matrix } X \right\rangle$$

Computing a nonzero element of I_n is as hard as computing the determinant

Theorem [AF '22]

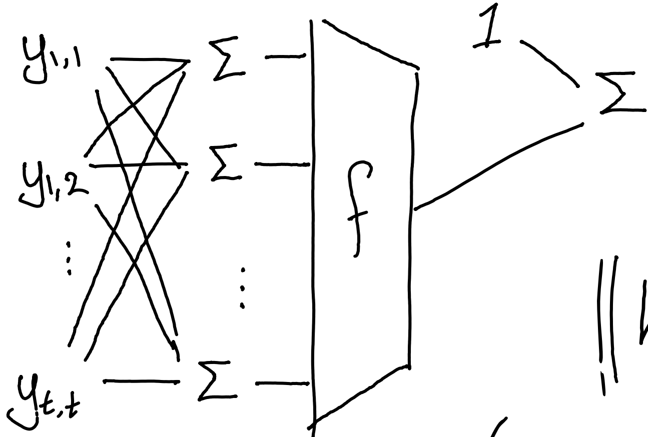
Grochow's conjecture is true under depth-3 approximate circuit reductions

Main 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



$\to h_\varepsilon(Y)$

such that

$$\| h_\varepsilon(Y) - \det_t(Y) \| \le \varepsilon$$

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

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

Proof uses alternate basis of $\mathbb{F}[X]$ given by products of minors of X (the "straightening law" of Doubilet–Rota–Stein)

APPLICATIONS

Assume $\mathrm{char}(\mathbb{F}) = 0$ or $\mathrm{char}(\mathbb{F})$ is large

Theorem [Limaye-Srinivasan-Tavenas '21]

Any constant-depth circuit that computes $\det_n(X) + O(\varepsilon)$ has size $n^{(\log n)^{\Omega(1)}}$

Corollary [AF '22]

$\forall f(X) \in \langle r \times r$ minors of $n \times n$ matrix $X \rangle$,
any constant-depth circuit that computes f has size $\geq r^{(\log r)^{\Omega(1)}}$

Useful for polynomial identity testing & proof complexity

REFUTING POLYNOMIAL EQUATIONS

Let $f_1(\bar{x}), \ldots, f_m(\bar{x})$ be polynomials such that

$$f_1(\bar{x}) = f_2(\bar{x}) = \cdots = f_m(\bar{x}) = 0$$

has no solution.

Q: How to prove this?

A: Find polynomials $g_1(\bar{x}), \ldots, g_m(\bar{x})$ such that

$$\sum_{i=1}^{m} g_i(\bar{x})\, f_i(\bar{x}) = 1$$

(Sound + complete over alg. closed fields (e.g. $\mathbb{C}$))

IDEAL PROOF SYSTEM I

Definition [Grochow–Pitassi '14]

Let $f_1(\bar{x}) = \cdots = f_m(\bar{x}) = 0$ be unsatisfiable system of polynomials. An **Ideal Proof System** refutation is a polynomial $\mathrm{Ref}(\bar{x}, \bar{y})$ s.t.

(1) $\mathrm{Ref}(\bar{x}, \bar{y}) \in \langle y_1, \cdots, y_m \rangle$

(2) $\mathrm{Ref}(\bar{x}, f_1(\bar{x}), \ldots, f_m(\bar{x})) = 1$

($\mathrm{Ref}(\bar{x}, \bar{y})$ proves $1 \in \langle f_1, \ldots, f_m \rangle$)

IDEAL PROOF SYSTEM II [GP14]

- Number of lines in PC is p-equivalent to IPS restricted to alg. branching programs
- If $\mathrm{char}(\mathbb{F}) = p > 0$,
  - constant-depth IPS p-simulates $AC^0[p]$-Frege
  - formula-IPS p-simulates Frege
- Every unsatisfiable CNF formula φ has a VNP-IPS refutation

  (so non-explicit lower bounds $\Rightarrow$ $VP \neq VNP$)

IDEAL PROOF SYSTEM III

Let $R(\bar{x}, \bar{y})$ refute $f_1(\bar{x}) = \cdots = f_m(\bar{x}) = 0$.

- $R(\bar{x}, \bar{y}) \in \langle y_1, \ldots, y_m \rangle \subseteq \mathbb{F}[\bar{x}, \bar{y}]$
- $R(\bar{x}, f_1(\bar{x}), \ldots, f_m(\bar{x})) = 1$

$$\iff R(\bar{x}, \bar{y}) \in 1 + \langle y_1 - f_1(\bar{x}), \ldots, y_m - f_m(\bar{x}) \rangle \subseteq \mathbb{F}[\bar{x}, \bar{y}]$$

So $\{\text{IPS refutations of } f_1 = \cdots = f_m = 0\}$

$$= \langle y_1, \ldots, y_m \rangle \cap \left(1 + \langle y_1 - f_1, \ldots, y_m - f_m \rangle \right)$$

IPS lower bounds $\equiv$ lower bounds for ideal cosets

New IPS Lower Bounds

Theorem [AF '22]

The constant-depth Ideal Proof System requires $n^{\log^{\Omega(1)} n}$ size to refute

$$\det_n(X) = 0$$

$$XY = \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}$$

$$X, Y \in \{0,1\}^{n \times n}$$

(requires $\mathrm{char}(\mathbb{F}) = 0$ or large)

New IPS Lower Bounds

Theorem [AF '22]

The constant-depth Ideal Proof System requires $n^{\log^{\Omega(1)} n}$ size to refute

$$\det_n(X) = 0$$

$$X = \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}$$

(requires $\mathrm{char}(\mathbb{F}) = 0$ or large)

PROOF SKETCH

- Let $\mathrm{Ref}(X, z, W)$ refute $\left\{ \begin{aligned} \det(X) &= 0 \\ X - \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} &= 0 \end{aligned} \right\} \begin{matrix} (z) \\ (W) \end{matrix}$

- Define $f(X) := 1 - \mathrm{Ref}\left(X,\ 0,\ X - \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}\right)$

[Forbes–Shpilka–Tzameret–Wigderson '16]:

- Ref is a refutation $\Rightarrow f(X) \in \langle \det(X) \rangle$
- IPS is sound $\Rightarrow f(X) \neq 0$

- Ref computable in size s & depth d

  $\Rightarrow f$ — $s+n+1$ — $d+1$

- Use lower bound for $\langle \det(X) \rangle$ $\square$

Open Questions

(1) Can we prove lower bounds for other ideals?

(2) Is the use of approximate computation necessary?

(3) Can we prove IPS lower bounds for simpler equations? (See Tuomas's talk!)

(4) Can low-depth IPS efficiently refute

$$\left\{ XY = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix},\ YX = \begin{pmatrix} 2 & & & \\ & 2 & & \\ & & \ddots & \\ & & & 2 \end{pmatrix} \right\}?$$

Thank You!