Purdue Theory CS/Math Seminar

Debordering Closure Results in Determinantal and Pfaffian Ideals

Anakin Dey & Zeyu Guo

The Ohio State University

Section 1

Background

What is Algebraic Complexity?

Question

How hard is it to compute polynomials?

Question

How hard is it to compute polynomials in restricted models?

Question

Can we find *explicit* polynomials which are hard to compute?

Algebraic Circuits

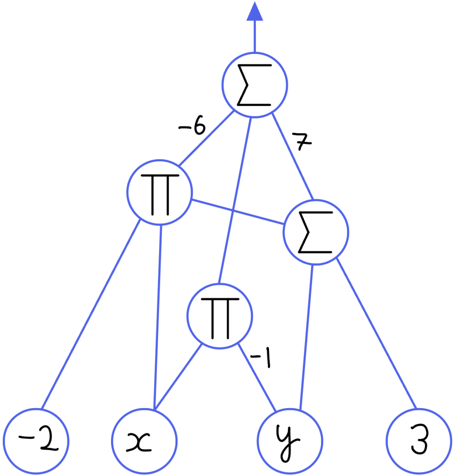


Figure: $-6(-2x \cdot (y+3)) - xy + 7(y+3)$

We have two measures of complexity:

- *Size:* The number of edges
- *Depth:* The length of the longest input-output path

Algebraic Circuits with Oracles

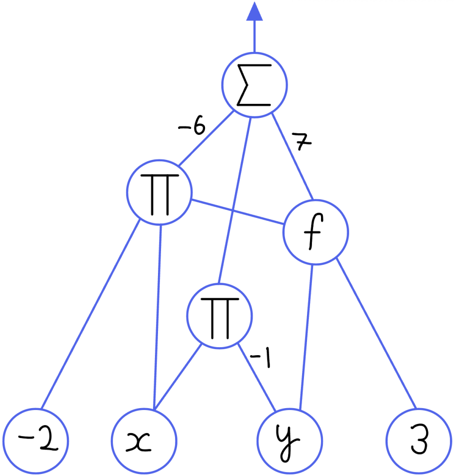


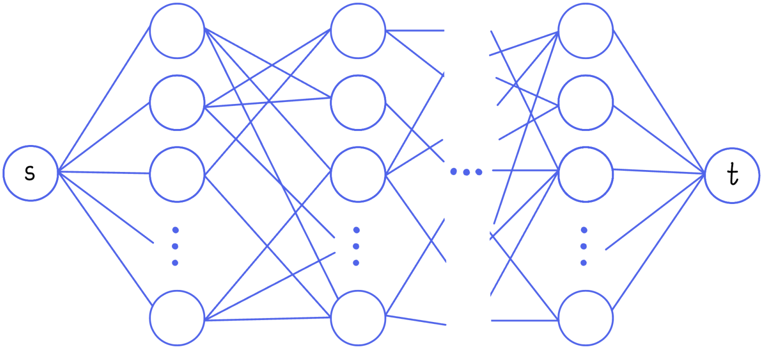
Figure: $-6(-2x \cdot f(y,3)) - xy + 7f(y,3)$

Question

How can we compare the *relative* complexity of two polynomials?

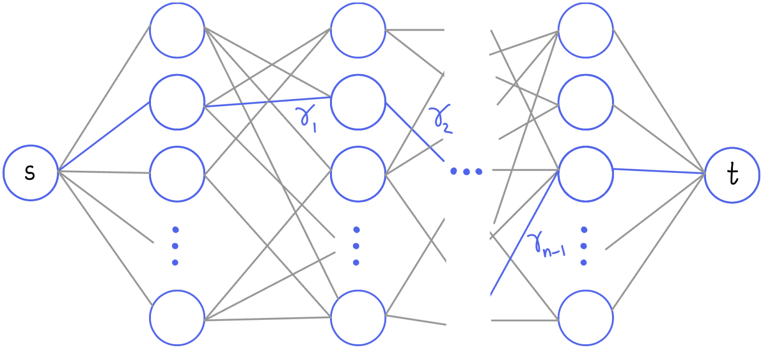
We can allow a fixed polynomial $f(\overline{x})$ to be computed with unit cost by allowing it to function as its own gate.

Algebraic Branching Programs



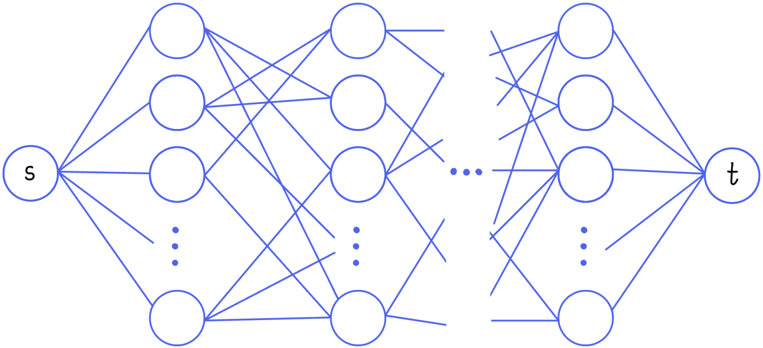
$$f(X) = \sum_{\text{path } \overline{e} \text{ from } s \text{ to } t} \gamma_{\overline{e}}$$

Algebraic Branching Programs



Contributes $\gamma_1\gamma_2\cdots\gamma_{n-1}$.

Algebraic Branching Programs



$$f(X) = \sum_{\text{path } \overline{e} \text{ from } s \text{ to } t} \gamma_{\overline{e}}$$

Branching Programs as Determinants

Lemma ([AF22, Lemma 3.6], [Val79, Theorem 1])

Suppose $g(\overline{y})$ can be computed by an r-vertex branching program. Then there exists an $r \times r$ matrix A of degree-≤ 1 polynomials such that

- $\det_r(A) = 1 + g(\overline{y})$, and
- for all $1 \leq k < r$, $\det_k(A_{[k],[k]}) = 1$.

Border Complexity

One relaxation in algebraic complexity is to *approximate* a polynomial.

Instead of working over a field $\mathbb{F}$, we take a parameter ε, allow our coefficients to be rational functions in ε, and let ε tend to 0.

Definition

We say a circuit *border computes* $g(\overline{x})$ over $\mathbb{F}$ if it computes

$$g(\overline{x}) + \varepsilon^q \tilde{g}(\overline{x}, \varepsilon) \in \mathbb{F}(\varepsilon)[\overline{x}], \qquad q \geq 1.$$

We cannot set $\varepsilon = 0$ since we may divide by ε.

What does Border Computation Get Us?

Question

What is the power of border computation?

Is it strictly necessary? Can we prove something in the border setting and *deborder* the result to get an exact computation?

Circuit Complexity for Ideals

In algebraic complexity, we are interested in characterizing the *circuit complexity* of some family of polynomials.

Definition

Fix some polynomials $g_1(\overline{x}), \ldots, g_k(\overline{x}) \in \mathbb{F}[\overline{x}]$.
The *ideal* generated by $g_1(\overline{x}), \ldots, g_k(\overline{x})$ is the set of combinations

$$\langle\, g_1, \ldots, g_k \,\rangle = \left\{ \sum_{i=1}^{k} h_i(\overline{x}) \cdot g_i(\overline{x}) \;\middle|\; h_i(\overline{x}) \in \mathbb{F}[\overline{x}] \right\}.$$

Question

Suppose $f \in \langle\, g_1, \ldots, g_k \,\rangle$. How does the complexity of f compare to the complexity of the generators $g_1, \ldots, g_k$?

Principal Ideals

Example

The *principal ideals* are generated by a single polynomial g.

If $f \in \langle g \rangle$, then g is a *factor* of f.

Question

Suppose $f \in \langle g \rangle$. Does g have a small f-oracle circuit?

Principal Ideals

Conjecture ([Bür00, Conjecture 8.3])

If g is a factor of f, $\text{size}(g) \leq \text{poly}(\text{size}(f), \deg(f))$.

Theorem ([Bür04, Theorem 1.3])

Over fields of characteristic 0, g can be *border computed* by a circuit of size $\text{poly}(\text{size}(f), \deg(f))$.

Question

Can we *deborder* this result, that is can we remove this ε approximation?

What about Two Generators?

Consider an ideal with two generators $\langle\, g_1(\overline{x}), g_2(\overline{x})\,\rangle$.

Say $0 \neq f(\overline{x}) \in \langle\, g_1(\overline{x}), g_2(\overline{x})\,\rangle$:

$$f(\overline{x}) = h_1(\overline{x})g_1(\overline{x}) + h_2(\overline{x})g_2(\overline{x}).$$

Question

If $f(\overline{x})$ has a small circuit, do $g_1(\overline{x})$ or $g_2(\overline{x})$ have a small f-oracle circuit?

This is open for *general* polynomials $g_1(\overline{x}), g_2(\overline{x})$ [Gro20].

Determinantal Ideals

Questions about oracle circuit complexity are open for general ideals with more than one generator. We can instead ask about ideals whose generators have *additional structure*.

Example

Consider an $n \times m$ matrix $X = (x_{i,j})$ of variables. Let $I^{\mathrm{det}}_{n,m,r}$ be the *determinantal ideal* generated by the $r \times r$ minors of X.

Prior Closure Results in Determinantal Ideals

Example

Consider an $n \times m$ matrix $X = (x_{i,j})$ of variables. Let $I^{\det}_{n,m,r}$ be the *determinantal ideal* generated by the $r \times r$ minors of X.

Conjecture ([Gro20, Conjecture 6.3])

Let $f \in I^{\det}_{n,n,n/2}$ be a nonzero polynomial. There is a constant depth f-oracle circuit of size $\mathrm{poly}(n)$ that computes the $t \times t$ determinant, $t = n^{\Theta(1)}$.

What does the Oracle Give Us?

Conjecture ([Gro20, Conjecture 6.3])

Let $f \in I^{\det}_{n,n,n/2}$ be a nonzero polynomial. There is a constant depth f-oracle circuit of size $\mathrm{poly}(n)$ that computes the $t \times t$ determinant, $t = n^{\Theta(1)}$.

- There exist polynomial size circuits for computing $\det(X)$.
- However, these circuits are *not* constant-depth.
- The oracle allows *constant depth* computation of the determinant.

Closure Results in Determinantal Ideals

Theorem ([AF22, Theorem 1.1])

Let $f \in I^{\det}_{n,m,r}$ be a nonzero polynomial. Then there is a depth-three f-oracle circuit of size $O\left(n^2 m^2\right)$ that *border computes* the $t \times t$ determinant for some $t = \Theta\left(r^{1/3}\right)$.

Question

Can we *deborder* this result, that is can we remove this ε approximation?

Closure Results in Determinantal Ideals

Theorem ([DG25, Theorem 1.5])

Let $f \in I^{\det}_{n,m,r}$ be a nonzero polynomial. Then there is a depth-three f-oracle circuit of size $\mathrm{poly}(n, m, \deg(f))$ that *exactly computes* the $t \times t$ determinant for some $t = \Theta\left(r^{1/3}\right)$.

Main Tools:

- We use *Straightening Laws* from Invariant Theory to express $f(X)$ in a standard basis indexed by combinatorial objects, and leverage the combinatorics to talk about specific terms.
- To get a circuit for a specific basis term, we use *Homogenization* as well as a new application of the *Isolation Lemma*.

Section 2

Preliminaries

Young Tableau

We will first discuss which combinatorial generators we use for $I^{\det}_{n,m,r}$.

Definition (Young Tableau)

A *partition* is a sequence of integers $\sigma = (\sigma_1 \geq \cdots \geq \sigma_k \geq 0)$.
A *Young Tableau* of shape σ is a filling of the squares in the diagram for σ using positive integers.
Such a filling is *conjugate semistandard* if it is strictly increasing along rows and weakly increasing down columns.

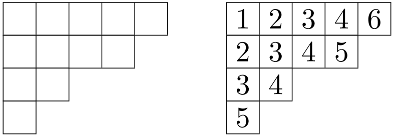


Figure: Diagram for $\sigma = (5, 4, 2, 1)$ and a Young Tableau of shape σ

Young Tableau

We have *canonical* and *anticanonical* tableau:

$$K_\sigma = \begin{array}{|c|c|c|c|c|}\hline 1 & 2 & 3 & 4 & 5 \\ \hline 1 & 2 & 3 & 4 & \\ \cline{1-4} 1 & 2 & & & \\ \cline{1-2} 1 & & & & \\ \cline{1-1} \end{array}, \qquad \overline{K}_\sigma = \begin{array}{|c|c|c|c|c|}\hline 1 & 2 & 3 & 4 & 5 \\ \hline 2 & 3 & 4 & 5 & \\ \cline{1-4} 4 & 5 & & & \\ \cline{1-2} 5 & & & & \\ \cline{1-1} \end{array}$$

Figure: Canonical and Anticanonical tableau of shape $\sigma = (5, 4, 2, 1)$

Bideterminants

Definition (Bideterminants)

Let $\sigma = (4, 2, 1)$. Consider the *bitableau* $(S \mid T)$

$$(S \mid T) = \left(\begin{array}{cccc} 1 & 2 & 4 & 5 \\ 3 & 6 & & \\ 4 & & & \end{array} \middle| \begin{array}{cccc} 1 & 3 & 5 & 6 \\ 2 & 7 & & \\ 3 & & & \end{array} \right).$$

Then the *bideterminant* $(S \mid T)(X)$ is given by

$$(S \mid T)(X) = \begin{pmatrix} x_{1,1} & x_{1,3} & x_{1,5} & x_{1,6} \\ x_{2,1} & x_{2,3} & x_{2,5} & x_{2,6} \\ x_{4,1} & x_{4,3} & x_{4,5} & x_{4,6} \\ x_{5,1} & x_{5,3} & x_{5,5} & x_{5,6} \end{pmatrix} \begin{pmatrix} x_{3,2} & x_{3,7} \\ x_{6,2} & x_{6,7} \end{pmatrix} \begin{pmatrix} x_{4,3} \end{pmatrix}.$$

Bideterminants

Definition (Bideterminants)

Let $\sigma = (4, 2, 1)$. Consider the *bitableau* $(S \mid T)$

$$(S \mid T) = \left(\begin{array}{|c|c|c|c|} \hline 1 & 2 & 4 & 5 \\ \hline 3 & 6 \\ \cline{1-2} 4 \\ \cline{1-1} \end{array} \;\middle|\; \begin{array}{|c|c|c|c|} \hline 1 & 3 & 5 & 6 \\ \hline 2 & 7 \\ \cline{1-2} 3 \\ \cline{1-1} \end{array} \right).$$

Then the *bideterminant* $(S \mid T)(X)$ is given by

$$(S \mid T)(X) = \begin{pmatrix} x_{1,1} & x_{1,3} & x_{1,5} & x_{1,6} \\ x_{2,1} & x_{2,3} & x_{2,5} & x_{2,6} \\ x_{4,1} & x_{4,3} & x_{4,5} & x_{4,6} \\ x_{5,1} & x_{5,3} & x_{5,5} & x_{5,6} \end{pmatrix} \begin{pmatrix} x_{3,2} & x_{3,7} \\ x_{6,2} & x_{6,7} \end{pmatrix} \begin{pmatrix} x_{4,3} \end{pmatrix}.$$

Bideterminants

Definition (Bideterminants)

Let $\sigma = (4, 2, 1)$. Consider the *bitableau* $(S \mid T)$

$$(S \mid T) = \left(\begin{array}{|c|c|c|c|} \hline 1 & 2 & 4 & 5 \\ \hline 3 & 6 \\ \cline{1-2} 4 \\ \cline{1-1} \end{array} \;\middle|\; \begin{array}{|c|c|c|c|} \hline 1 & 3 & 5 & 6 \\ \hline 2 & 7 \\ \cline{1-2} 3 \\ \cline{1-1} \end{array} \right).$$

Then the *bideterminant* $(S \mid T)(X)$ is given by

$$(S \mid T)(X) = \begin{vmatrix} x_{1,1} & x_{1,3} & x_{1,5} & x_{1,6} \\ x_{2,1} & x_{2,3} & x_{2,5} & x_{2,6} \\ x_{4,1} & x_{4,3} & x_{4,5} & x_{4,6} \\ x_{5,1} & x_{5,3} & x_{5,5} & x_{5,6} \end{vmatrix} \begin{vmatrix} x_{3,2} & x_{3,7} \\ x_{6,2} & x_{6,7} \end{vmatrix} \begin{vmatrix} x_{4,3} \end{vmatrix}.$$

A Natural Generating Set for Determinantal Ideals

Lemma

A degree d monomial $\prod_{i=1}^{d} x_{r_i,c_i}$ is given by a bideterminant:

$$\prod_{i=1}^{d} x_{r_i,c_i} = \left(\begin{array}{c|c} \boxed{r_1} & \boxed{c_1} \\ \boxed{r_2} & \boxed{c_2} \\ \vdots & \vdots \\ \boxed{r_d} & \boxed{c_d} \end{array} \right)(X).$$

Thus, the bideterminants span $\mathbb{F}[X]$.

A Natural Generating Set for Determinantal Ideals

Theorem ([DRS74, §8, Theorem 3], [dCEP80, Corollary 2.3])

Let $(S \mid T)(X)$ be a bideterminant of shape σ. Then $(S \mid T)(X)$ can be uniquely expressed as a linear combination

$$(S \mid T)(X) = \sum_{(A|B)} c_{A,B}(A \mid B)(X),$$

where A and B are *conjugate semistandard*.

Since $I^{\text{det}}_{n,m,r}$ is generated by the $r \times r$ minors, the bideterminants in our basis should have at least one determinant of length at least r.

Proposition ([BC03, Corollary 1.7])

The ideal $I^{\text{det}}_{n,m,r}$ has as basis the conjugate semistandard bideterminants of shape σ whose first row has length at least r.

Example Straightening

$$X = \begin{pmatrix} x_{1,1} & x_{1,2} & x_{1,3} & x_{1,4} \\ x_{2,1} & x_{2,2} & x_{2,3} & x_{2,4} \end{pmatrix}$$

$$\left(\begin{array}{|c|c|}\hline 1 & 2 \\ \hline 1 & 2 \\ \hline \end{array} \,\middle|\, \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 4 & 3 \\ \hline \end{array} \right)(X) = \left(\begin{array}{|c|c|}\hline 1 & 2 \\ \hline 1 & 2 \\ \hline \end{array} \,\middle|\, \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 & 4 \\ \hline \end{array} \right)(X) - \left(\begin{array}{|c|c|}\hline 1 & 2 \\ \hline 1 & 2 \\ \hline \end{array} \,\middle|\, \begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 & 4 \\ \hline \end{array} \right)(X)$$

Proof of Grochow's Conjecture Given Theorem

Conjecture ([Gro20, Conjecture 6.3])

Let $f \in I^{\det}_{n,n,n/2}$ be a nonzero polynomial. Then there is a constant depth f-oracle circuit of size $\mathrm{poly}(n)$ that computes the $t \times t$ determinant for some $t = n^{\Theta(1)}$.

Theorem ([DG25, Theorem 1.5])

Let $f \in I^{\det}_{n,m,r}$ be a nonzero polynomial. Then there is a depth-three f-oracle circuit of size $\mathrm{poly}(n, m, \deg(f))$ that *exactly computes* the $t \times t$ determinant for some $t = \Theta\left(r^{1/3}\right)$.

Main Theorem

Theorem

Let $f(X) \in I^{\det}_{n,m,r}$ be a nonzero polynomial of degree d. Then, there exists a depth-three f-oracle circuit of size $O\left(n^2 m^2 d^3 (n^3 + m^3)\right)$ computing $(K_\sigma \mid K_\sigma)(X)$, where $\sigma_1 \geq r$ and $|\sigma| \leq d$.

Let $\sigma = (4, 2, 1)$:

$$(K_\sigma \mid K_\sigma)(X) = \left(\begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline 1 & 2 \\ \cline{1-2} 1 \\ \cline{1-1} \end{array} \;\middle|\; \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline 1 & 2 \\ \cline{1-2} 1 \\ \cline{1-1} \end{array} \right)(X)$$

$$= \text{product of upper-left minors.}$$

Computing Determinants with Branching Programs

- Mahajan and Vinay [MV97] construct an algebraic branching program on $O\left(t^3\right) \leq r$ vertices which computes the $t \times t$ determinant
- There is an $r \times r$ matrix A such that $\det_r(A) = 1 + \det_t(\overline{y})$, and for all $1 \leq k < r$, $\det_k(A_{[k],[k]}) = 1$
- Our main theorem gives us an f-oracle circuit computing $(K_\sigma \mid K_\sigma)(X)$ and we know at least one row of σ has length $\geq r$
- So we compute $(1 + \det_t(\overline{y}))^k$ for some k
- Over characteristic zero fields, we can isolate $\det_t(\overline{y})$ via homogenization (coming soon)

Computing Iterated Matrix Multiplication with Branching Programs

Definition

Let W, D be positive integers. Let $X^{(1)}, \ldots, X^{(W)}$ be W disjoint $D \times D$ matrices of variables. The *iterated matrix multiplication* polynomial, $\mathrm{IMM}_{W,D}$ is the $(1,1)$ entry of the product $X^{(1)} \cdots X^{(W)}$.

- There is an algebraic branching program on $W(D-1)+2 \leq r$ vertices which computes $\mathrm{IMM}_{W,D}$
- There is an $r \times r$ matrix A such that $\det_r(A) = 1 + \mathrm{IMM}_{W,D}$, and for all $1 \leq k < r$, $\det_k(A_{[k],[k]}) = 1$
- Our main theorem gives us an f-oracle circuit computing $(K_\sigma \mid K_\sigma)(X)$ and we know at least one row of σ has length $\geq r$
- So we compute $(1 + \mathrm{IMM}_{W,D})^k$ for some k
- Again, we can isolate $\mathrm{IMM}_{W,D}$ via homogenization

Section 3

Proof Techniques

Proof Outline

Since we are starting with $f(X) \in I^{\det}_{n,m,r} \subseteq \mathbb{F}[X]$, we can express in terms of our standard basis:

$$f(X) = \sum_{k \in I} c_k (S_k \mid T_k)(X).$$

Our goal will be to use $f(X)$ as an oracle to compute a canonical bideterminant.

To do this, we will isolate one of the terms $(S_k \mid T_k)(X)$.

Linear Operators

Definition (Substitution operator)

For $i < j$, the operator $\mathrm{Sub}_{i\to j}$ takes a tableau S and returns the tableau S' formed by taking each row of S which has an i but not a j, replacing that i with j, and sorting the row in increasing order.

$$\underset{2\to 4}{\mathrm{Sub}} \begin{array}{|c|c|c|c|}\hline 1 & 2 & 3 & 4 \\ \hline 1 & 2 \\ \cline{1-2} 1 \\ \cline{1-1}\end{array} = \begin{array}{|c|c|c|c|}\hline 1 & 2 & 3 & 4 \\ \hline 1 & 4 \\ \cline{1-2} 1 \\ \cline{1-1}\end{array}$$

Let $h_i^j(S)$ be the number of times i is replaced by j in S.

Linear Operators

These operators send conjugate semistandard tableau to conjugate semistandard tableau.

In fact, after enough applications we arrive at *anticanonical* tableau:

Lemma ([dCEP80, stated before Corollary 1.7])

Let S be a conjugate semistandard tableau of shape σ such that S has entries of value at most n. Then

$$\Big(\underset{n-1\to n}{\mathrm{Sub}} \circ \underset{n-2\to n}{\mathrm{Sub}} \circ \underset{n-2\to n-1}{\mathrm{Sub}} \circ \cdots \circ \underset{2\to n}{\mathrm{Sub}} \circ \cdots \circ \underset{2\to 3}{\mathrm{Sub}} \circ \underset{1\to n}{\mathrm{Sub}} \circ \cdots \circ \underset{1\to 2}{\mathrm{Sub}}\Big)(S) = \overline{K}_\sigma.$$

Linear Operators

Lemma ([dCEP80, stated before Corollary 1.7])

Let S be a conjugate semistandard tableau of shape σ such that S has entries of value at most n. Then

$$\Big(\underset{n-1\to n}{\mathrm{Sub}} \circ \underset{n-2\to n}{\mathrm{Sub}} \circ \underset{n-2\to n-1}{\mathrm{Sub}} \circ \cdots \circ \underset{2\to n}{\mathrm{Sub}} \circ \cdots \circ \underset{2\to 3}{\mathrm{Sub}} \circ \underset{1\to n}{\mathrm{Sub}} \circ \cdots \circ \underset{1\to 2}{\mathrm{Sub}}\Big)(S) = \overline{K}_\sigma.$$

Example

Say $n = 5$

1	2	3	4
1	2		
1			

$\rightsquigarrow$

2	3	4	5
4	5		
5			

Applying the Linear Operators

Substituting i for j corresponds to multiplication of X by an *elementary matrix* $E_{i,j}$, adding a multiple of row j to row i.

Lemma

Let λ be a new indeterminate and let $(S \mid T)$ be a bitableau. Then we have that

$$(S \mid T)(E_{i,j}(\lambda)X) = \pm\lambda^{h_i^j(S)}(\underset{i\to j}{\mathrm{Sub}}(S) \mid T)(X) + \sum_{h=0}^{h_i^j(S)-1} \lambda^h \sum_{S' \in \mathcal{C}_{i\to j}^h(S)} \pm(S' \mid T)(X).$$

For $0 \leq h \leq h_i^j(S) - 1$, let $\mathcal{C}_{i\to j}^h(S)$ be the set of tableaux of shape σ obtained by changing i to j at exactly h rows of S which contain i but not j and reordering those rows to be increasing.

Applying the Linear Operators

We have seen now that after applying a sequence of linear transformations $E_{i,j}$ to our matrix of variables X, we can send a bitableau $(S \mid T)$ of shape σ to $(\overline{K}_\sigma \mid \overline{K}_\sigma)$.

Let J_n be the $n \times n$ matrix with 1's along the anti-diagonal.

Lemma

$$(\overline{K}_\sigma \mid \overline{K}_\sigma)(J_n X J_m) = \pm (K_\sigma \mid K_\sigma)(X).$$

We now have linear transformations sending bitableau to canonical semistandard Young tableau.

Where Does Isolation Arise?

$$f(X) = \sum_{k \in I} c_k (S_k \mid T_k)(X) \in I^{\det}_{n,m,r}.$$

Corollary

We have matrices M, N such that

$$f(MXN) = \sum_{k \in A} \widehat{c}_k \Lambda^{\overline{e}_k} \Xi^{\overline{f}_k} \cdot (K_{\sigma_k} \mid K_{\sigma_k})(X) + \sum_{\ell \in B} \widehat{c}_\ell \Lambda^{\overline{e}_\ell} \Xi^{\overline{f}_\ell} \cdot (S_\ell \mid T_\ell)(X),$$

Upshot: linear transformations correspond to plugging in linear equations into the input for $f(X)$, so this is the start of our f-oracle circuit.

Where Does Isolation Arise?

$$f(X) = \sum_{k \in I} c_k (S_k \mid T_k)(X) \in I^{\det}_{n,m,r}, \qquad \deg(f) = d.$$

Corollary

We have matrices M, N such that

$$f(MXN) = \sum_{k \in A} \widehat{c}_k \Lambda^{\overline{e}_k} \Xi^{\overline{f}_k} \cdot (K_{\sigma_k} \mid K_{\sigma_k})(X) + \sum_{\ell \in B} \widehat{c}_\ell \Lambda^{\overline{e}_\ell} \Xi^{\overline{f}_\ell} \cdot (S_\ell \mid T_\ell)(X),$$

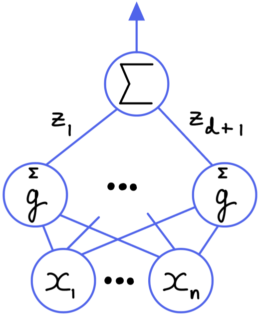
Homogenization

Definition

Consider a degree d polynomial $g(\overline{x}, t) = \sum_{i=0}^{d} \mathrm{coeff}_{t^i}(g) t^i$.

Lemma (Folklore)

Say g is computed by a size s, depth Δ f-oracle circuit with top Σ-gate.



Then, we can compute $\mathrm{coeff}_{t^i}(g)$ by a size $O(ds)$, depth Δ f-oracle circuit.

Proof of Homogenization: Interpolation

Let $\alpha_1, \ldots, \alpha_{d+1}$ be $d+1$ distinct elements in $\mathbb{F}$.

$$\begin{pmatrix} \alpha_1^d & \alpha_1^{d-1} & \cdots & \alpha_1 & 1 \\ \alpha_2^d & \alpha_2^{d-1} & \cdots & \alpha_2 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_d^d & \alpha_d^{d-1} & \cdots & \alpha_d & 1 \\ \alpha_{d+1}^d & \alpha_{d+1}^{d-1} & \cdots & \alpha_{d+1} & 1 \end{pmatrix} \begin{pmatrix} \mathrm{coeff}_{t^d}(f) \\ \mathrm{coeff}_{t^{d-1}}(f) \\ \vdots \\ \mathrm{coeff}_{t}(f) \\ \mathrm{coeff}_{1}(f) \end{pmatrix} = \begin{pmatrix} f(\overline{x}, \alpha_1) \\ f(\overline{x}, \alpha_2) \\ \vdots \\ f(\overline{x}, \alpha_d) \\ f(\overline{x}, \alpha_{d+1}) \end{pmatrix}$$

This left matrix is a *Vandermonde* matrix and is invertible since the α_i are all distinct.

Proof of Homogenization: Interpolation

$$\begin{pmatrix} \mathrm{coeff}_{t^d}(f) \\ \mathrm{coeff}_{t^{d-1}}(f) \\ \vdots \\ \mathrm{coeff}_{t}(f) \\ \mathrm{coeff}_{1}(f) \end{pmatrix} = \begin{pmatrix} z_{1,1} & z_{1,2} & \cdots & z_{1,d} & z_{1,d+1} \\ z_{2,1} & z_{2,2} & \cdots & z_{2,d} & z_{2,d+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ z_{d,1} & z_{d,2} & \cdots & z_{d,d} & z_{d,d+1} \\ z_{d+1,1} & z_{d+1,2} & \cdots & z_{d+1,d} & z_{d+1,d+1} \end{pmatrix} \begin{pmatrix} f(\overline{x}, \alpha_1) \\ f(\overline{x}, \alpha_2) \\ \vdots \\ f(\overline{x}, \alpha_d) \\ f(\overline{x}, \alpha_{d+1}) \end{pmatrix}$$

$$\mathrm{coeff}_{t^i}(f) = \sum_{j=1}^{d+1} z_{d+1-i,j} f(\overline{x}, \alpha_j).$$

Issues with Homogenization

If a circuit border computes $g(\overline{x})$, then it computes

$$g(\overline{x}) + \varepsilon^q \tilde{g}(\overline{x}, \varepsilon), \qquad q \geq 1.$$

Idea: Homogenize with respect to ε.

Problem: q can be *arbitrarily large*

$\implies$ Homogenization gives *large circuit*.

Idea: Kronecker Substitution

Say there is a specific coefficient $c_{\overline{e}}$ in $g(\overline{x}) = \sum_{\overline{e} \in \mathcal{L}} c_{\overline{e}} \overline{x}^{\overline{e}}$ we want to *isolate*.

Lemma

Suppose that $\deg(g) \leq d$, then the *Kronecker substitution*

$$x_i \mapsto w^{d^i}$$

maps distinct monomials to distinct monomials.

Problem: The resulting polynomial has *large degree*.

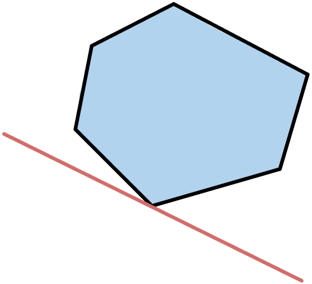
$\implies$ Homogenization gives *large circuit*.

Isolation Lemma

Say there is a specific coefficient $c_{\overline{e}}$ in $g(\overline{x}) = \sum_{\overline{e}} c_{\overline{e}} \overline{x}^{\overline{e}}$ we want to *isolate*.

Lemma ([KS01, Lemma 4])

Linear programs with *random* cost functions will have a unique minimum.



Moreover, if the linear equations have bounded integer coefficients, then evaluation at *small, random* values has a unique minimum.

Isolation Lemma

Lemma ([KS01, Lemma 4])

Let $\mathcal{L}$ be any collection of distinct linear forms in variables $z_1, \ldots, z_\ell$ with coefficients in the range $\{0, \ldots, K\}$ for some integer $K \in \mathbb{Z}_{\geq 0}$. Let $\varepsilon > 0$.

Let $z_1, \ldots, z_\ell$ be independently and uniformly chosen from $\{0, \ldots, M\}$ at random, where $M \geq K\ell/\varepsilon$.

Then, with probability at least $1 - \varepsilon$, there is a unique form in $\mathcal{L}$ of minimum value at $z_1, \ldots, z_\ell$.

Isolating Monomials

Lemma ([DG25, Corollary 2.27])

Consider a polynomial $g(x_1, \ldots, x_\ell)$ such that the individual degree of each x_i in g is at most K:

$$g(x_1, \ldots, x_\ell) = \sum_{\overline{e} \in \mathcal{L}} c_{\overline{e}} x_1^{e_1} \cdots x_\ell^{e_\ell}.$$

Randomly choose $z_1, \ldots, z_\ell$ and define a morphism

$$x_i \mapsto w^{z_i}, \qquad g \mapsto \sum_{\overline{e} \in \mathcal{L}} c_{\overline{e}} \cdot w^{\sum_{i=1}^{\ell} e_i z_i}.$$

The Isolation Lemma shows that the $z_1, \ldots, z_\ell$ can be choose to be small $\implies$ unique lowest $\deg_w$-term and homogenization w.r.t w is small.

Section 4

Related and Future Work

Pfaffian Analogues

Definition

If X is a $2n \times 2n$ skew-symmetric matrix,then $\det(X)$ is the perfect square of another polynomial called the *Pfaffian* of X.

Theorem ([DG25, Theorem 1.6])

Let $f \in I_{2n,2r}^{\text{pfaff}}$ be a nonzero polynomial. Then there is a depth-three f-oracle circuit of size $\text{poly}(n, \deg(f))$ that *exactly computes* the $t \times t$ pfaffian for some $t = \Theta\left(r^{1/3}\right)$.

Symmetric Analogue?

The focus on determinantal ideals and pfaffian ideals stem from *invariant theory*. Are there other natural settings to study from there?

Question

Is there an analogue to our results for the ideal of determinants of a symmetric matrix?

Roadblocks for the Permanent

The other big star in algebraic complexity is the *permanent* of a matrix.

Question

Is there an analogue to our results for the ideal of permanents of a matrix?

The main roadblock is that we have no analogue of the following result:

$$(S \mid T)(E_{i,j}(\lambda)X) = \pm\lambda^{h_i^j(S)}(\operatorname*{Sub}_{i\to j}(S) \mid T)(X) + \sum_{h=0}^{h_i^j(S)-1} \lambda^h \sum_{S' \in \mathcal{C}^h_{i\to j}(S)} \pm(S' \mid T)(X).$$

Thank You!

Algebra is generous; she often gives more than is asked of her.

— Jean Le Rond d'Alembert

Slides can be found on my site anakin.phd

Bibliography I

Robert Andrews and Michael A. Forbes.

Ideals, determinants, and straightening: Proving and using lower bounds for polynomial ideals.

In *STOC '22: 54th Annual ACM SIGACT Symposium on Theory of Computing, Rome, Italy, June 20 - 24, 2022*, pages 389–402. ACM, 2022.

Winfried Bruns and Aldo Conca.

Gröbner bases and determinantal ideals.

In *Commutative Algebra, Singularities and Computer Algebra*, pages 9–66. Springer Netherlands, 2003.

Bibliography II

Peter Bürgisser.

Completeness and Reduction in Algebraic Complexity Theory.

Springer Berlin Heidelberg, 2000.

Peter Bürgisser.

The complexity of factors of multivariate polynomials.

Foundations of Computational Mathematics, 4(4):369–396, September 2004.

Corrado de Concini, David Eisenbud, and Claudio Procesi.

Young diagrams and determinantal varieties.

Inventiones mathematicae, 56(2):129–165, 1980.

Bibliography III

Anakin Dey and Zeyu Guo.

Debordering closure results in determinantal and pfaffian ideals.

ITCS, 2025.

Peter Doubilet, Gian-Carlo Rota, and Joel Stein.

On the foundations of combinatorial theory: Ix combinatorial methods in invariant theory.

Studies in Applied Mathematics, 53(3):185–216, 1974.

Bibliography IV

Joshua A. Grochow.

Complexity in ideals of polynomials: Questions on algebraic complexity of circuits and proofs.

Bulleting of the EATCS, 131, 2020.

Adam R. Klivans and Daniel Spielman.

Randomness efficient identity testing of multivariate polynomials.

In *Proceedings of the 33rd Annual ACM Symposium on Theory of Computing*, pages 216–223, 2001.

Bibliography V

Meena Mahajan and V. Vinay.

Determinant: Combinatorics, algorithms, and complexity.

Technical Report 5, Institute of Mathematical Sciences India, 1997.

Leslie G. Valiant.

Completeness classes in algebra.

In *Proceedings of the 11th Annual ACM Symposium on Theory of Computing*, pages 249–261, 1979.