9th Workshop on Algebraic Complexity Theory

Debordering Closure Results in Determinantal and Pfaffian Ideals

Anakin Dey & Zeyu Guo

The Ohio State University

What is Algebraic Complexity?

Question

How hard is it to compute some explicit polynomial?

Question

How hard it is to compute this polynomial *relative* to another polynomial?

Algebraic Circuits with Oracles

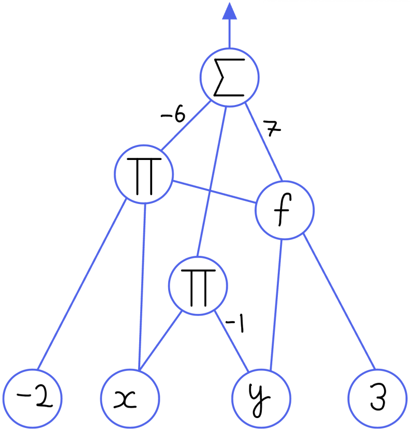


Figure:
$-6(-2x \cdot f(y,3)) - xy + 7f(y,3)$

Question

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

We have two measures of complexity:

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

Idea: We are allowing a fixed $f(\overline{x})$ to be computed with unit cost.

Broadly Speaking

Theorem ([DG25])

Let $X = (x_{i,j})$ be a matrix of indeterminates and let $0 \neq f(X) \in \mathbb{F}[X]$ be a *"polynomial in the $r \times r$ minors"* of X:

$$f(X) = \sum_{i \in I} h_i(X) g_i(X)$$

where each $g_i(X)$ is an $r \times r$ minor of X and $h_i(X) \in \mathbb{F}[X]$.

Then, we can use $f(X)$ as an *oracle* to compute the $t \times t$ determinant, $t = \Theta\left(r^{1/3}\right)$, with a *polynomial size, constant depth* circuit.

Circuit Complexity for Ideals

We want to characterize the circuit complexity of *families* 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

Consider $0 \neq f \in \langle\, g_1, \ldots, g_k \,\rangle$. 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

Consider $0 \neq f \in \langle\, g \,\rangle$. Does g have a small f-oracle circuit?

Principal Ideals

Conjecture ([Bür00, Conjecture 8.3])

If g is a factor of $f \neq 0$, $\text{size}(g) \leq \text{poly}(\text{size}(f), \deg(g))$.

The conjecture as stated is still open.

However, it is known in a relaxed setting known as *border computation*.

Border Complexity

Instead of exact computation, we can ask to *approximate* a polynomial.

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

Definition

A circuit C *border computes* $g(\overline{x})$ if it is defined over $\mathbb{F}(\varepsilon)$ and computes

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

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

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?

Principal Ideals

Conjecture ([Bür00, Conjecture 8.3])

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

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?

Debordering in Other Settings

Let $\overline{\mathcal{C}}$ be the set of polynomials border-computed by the elements of $\mathcal{C}$.

- $\overline{\Sigma\Pi} = \Sigma\Pi$ and $\overline{\Pi\Sigma} = \Pi\Sigma$ [DL25].
- Debordering results for depth-3 and depth-4 circuits already would have strong implications [AV08, GKKS16].
- Debordering *Waring Rank* dates back to early work in classical algebraic geometry [Pal06, Ter11].

$$\mathrm{Waring}(f) = \min_{r} \left\{ f(\overline{x}) = \sum_{i=1}^{r} \ell_i(\overline{x})^d \;\middle|\; \deg(\ell_i) = 1 \right\}$$

- Forbes conjectured that if $f \in \overline{\Sigma^s \wedge^d \Sigma}$ then $f \in \Sigma^{s'} \wedge^d \Sigma$ for $s' \in \mathrm{poly}(s, n, d)$ [Shp16].

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

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 $I^{\det}_{n,m,r}$ be the *determinantal ideal* generated by the $r \times r$ minors of X.

A Conjecture on Determinantal Ideals

Example

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

Conjecture ([Gro20, Conjecture 6.3])

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

Upshot: This means that the complexity of the determinant is a *lower bound* on the complexity of $I^{\text{det}}_{n,m,r}$.

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.

Prior 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 $O\left(n^2m^2\right)$ 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:

- Both [AF22, DG25] use *Straightening Laws* from Invariant Theory to express $f(X)$ in a standard basis indexed by combinatorial objects.
- To get a circuit for a specific basis term, we use *Homogenization* as well as a new application of the *Isolation Lemma*.

Proof Outline

1. Express $f(X) \in I^{\det}_{n,m,r}$ in a combinatorial basis $\mathcal{B}$.
2. Give a linear change of variables $x_{i,j} \mapsto \ell_{i,j}(X)$ so that

$$f(X) \mapsto \sum_{i \in I} K_i(X) + \text{lower degree “junk” terms},$$

   where $K_i(X) \in \mathcal{B} \cap I^{\det}_{n,m,r}$.
3. Use *homogenization* and *isolation* to get a circuit for a single $K_i(X)$.
4. Apply a projection $K_i(X) \mapsto \det_t(Y)$.

Why Isolation and Homogenization?

1. Express $f(X) \in I^{\det}_{n,m,r}$ in a combinatorial basis $\mathcal{B}$.
2. Give a linear change of variables $x_{i,j} \mapsto \ell_{i,j}(X)$ so that

$$f(X) \mapsto \sum_{i \in I} K_i(X) + \text{lower degree “junk” terms},$$

   where $K_i(X) \in \mathcal{B} \cap I^{\det}_{n,m,r}$.
3. Use *homogenization* and *isolation* to get a circuit for a single $K_i(X)$.
4. Apply a projection $K_i(X) \mapsto \det_t(Y)$.

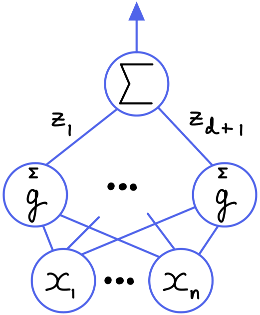
Homogenization

Definition

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

Lemma (Folklore)

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



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

Issues with Homogenization

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

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

Idea: Homogenize with respect to ε.

Problem: $\deg_\varepsilon(\tilde{g})$ can be *arbitrarily large*

$\implies$ Homogenization gives *large circuit*.

Idea: Kronecker Substitution

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

Lemma

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

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

maps distinct monomials to distinct monomials.

Problem: The resulting polynomial has *large degree*

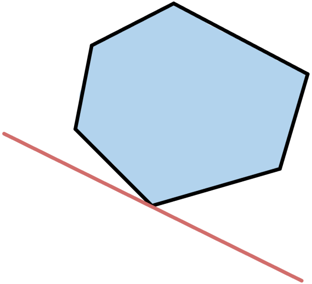
$\implies$ Homogenization gives *large circuit*.

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], [MVV87])

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 $z_1, \ldots, z_\ell$.

Idea: The probabalistic method says there is a good choice of $z_1, \ldots, z_\ell$.

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 chosen to be small $\implies$ unique lowest $\deg_w$-term and homogenization w.r.t w is small.

Pfaffian Analogue

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 $f \in I^{\text{pfaff}}_{2n,2r}$ 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 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 while the determinant and Pfaffian are alternating in the rows, but the permanent is not.

Thank You!

Like the Arabian phoenix rising out of its ashes, the theory of invariants, pronounced dead at the turn of the century, is once again at the forefront of mathematics.

— Joseph P.S. Kung, Gian-Carlo Rota [KR84]

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.

Manindra Agrawal and V. Vinay.

Arithmetic Circuits: A Chasm at Depth Four.

In *2008 49th Annual IEEE Symposium on Foundations of Computer Science*, pages 67–75, 2008.

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.

Anakin Dey and Zeyu Guo.

Debordering closure results in determinantal and pfaffian ideals.

ITCS, 2025.

Bibliography III

Pranjal Dutta and Vladimir Lysikov.

Recent Advances in Debordering Methods, 2025.

Ankit Gupta, Pritish Kamath, Neeraj Kayal, and Ramprasad Saptharishi.

Arithmetic Circuits: A Chasm at Depth 3.

45(3):1064–1079, 2016.

Joshua A. Grochow.

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

Bulleting of the EATCS, 131, 2020.

Bibliography IV

Joseph P. S. Kung and Gian-Carlo Rota.

The invariant theory of binary forms.

Bulletin of the American Mathematical Society, 10(1):27–85, 1984.

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.

Ketan Mulmuley, Umesh V. Vazirani, and Vijay V. Vazirani.

Matching is as easy as matrix inversion.

Combinatorica, 7(1):105–113, March 1987.

Bibliography V

Francesco Palatini.

Sulle superficie algebriche i cui S_h $(h+1)$-seganti non riempiono lo spazio ambiente.

Atti della R. Acc. delle Scienze di Torino, 41:634–640, 1906.

Amir Shpilka.

Some accessible open problems, 2016.

Alessandro Terracini.

Sulle V_k per cui la varietà degli S_h $(h+1)$-seganti ha dimensione minore dell'ordinario.

Rend. Circ. Mat., 31:392–396, 1911.