

Debordering Closure Results in Determinantal and Pfaffian Ideals

Anakin Dey  

Department of Mathematics, The Ohio State University, Columbus, OH, USA

Zeyu Guo  

Department of Computer Science and Engineering, The Ohio State University, Columbus, OH, USA

Abstract

One important question in algebraic complexity is understanding the complexity of polynomial ideals (Grochow, Bulletin of EATCS 131, 2020). Andrews and Forbes (STOC 2022) studied the determinantal ideals $I_{n,m,r}^{\det}$ generated by the $r \times r$ minors of $n \times m$ matrices. Over fields of characteristic zero or of sufficiently large characteristic, they showed that for any nonzero $f \in I_{n,m,r}^{\det}$, the determinant of a $t \times t$ matrix of variables with $t = \Theta(r^{1/3})$ is approximately computed by a constant-depth, polynomial-size f -oracle algebraic circuit, in the sense that the determinant lies in the border of such circuits. An analogous result was also obtained for Pfaffians in the same paper.

In this work, we deborder the result of Andrews and Forbes by showing that when f has polynomial degree, the determinant is in fact exactly computed by a constant-depth, polynomial-size f -oracle algebraic circuit. We further establish an analogous result for Pfaffian ideals.

Our results are established using the isolation lemma, combined with a careful analysis of straightening-law expansions of polynomials in determinantal and Pfaffian ideals.

2012 ACM Subject Classification Theory of computation \rightarrow Algebraic complexity theory

Keywords and phrases Algebraic circuit complexity, Isolation lemma, Debordering

Digital Object Identifier 10.4230/LIPIcs.ITCS.2026.49

Related Version Full Version: <https://doi.org/10.48550/arXiv.2511.16492> [16]

Funding Zeyu Guo: Supported by NSF CAREER award CCF-2440926.

Acknowledgements We thank David Anderson, Robert Andrews, and Srikanth Srinivasan for helpful discussions. We also thank the anonymous reviewers of ITCS 2026 for their careful reading and insightful comments.

1 Introduction

Polynomial ideals naturally arise in many parts of algebraic complexity theory. Understanding their complexity is an important theme, with connections to polynomial identity testing, algebraic natural proofs, and proof complexity; see [24] for a survey on such connections.

Roughly speaking, the complexity of an ideal I under a given algebraic model (such as algebraic circuits or algebraic branching programs) is defined as the minimum complexity, in that model, of any nonzero polynomial $f \in I$ [24]. Proving lower bounds for ideals is harder than for individual polynomials, since one must establish a bound for every nonzero $f \in I$ rather than just a single polynomial. This motivates the search for a property of the following form: if an arbitrary nonzero $f \in I$ is efficiently computable in a given model, then some polynomial from a distinguished set $S = \{g_1, \dots, g_k\}$ (often a natural generating set of I or some related set with desirable properties) is also efficiently computable in the given model. In this way, proving lower bounds for arbitrary nonzero $f \in I$ reduces to proving them for g_1, \dots, g_k . We call such a property a *closure result*, by analogy with closure under factorization. In short, closure results reduce the task of showing hardness for all polynomials in I to proving hardness for a small set of distinguished polynomials.



© Anakin Dey and Zeyu Guo;
licensed under Creative Commons License CC-BY 4.0
17th Innovations in Theoretical Computer Science Conference (ITCS 2026).

Editor: Shubhangi Saraf; Article No. 49; pp. 49:1–49:24



Leibniz International Proceedings in Informatics

Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Connection with hitting set generators. Closure results for ideals are useful for constructing hitting set generators (HSGs), which are the algebraic-complexity analogs of pseudorandom generators and can be used to derandomize polynomial identity testing (PIT). The idea is as follows: for $s < n$, we seek a HSG $G: \mathbb{F}^s \rightarrow \mathbb{F}^n$ against a family \mathcal{C} of n -variate polynomials, meaning that for any nonzero polynomial $f \in \mathcal{C}$, we have $f \circ G \neq 0$. Here, one should think of \mathcal{C} as a family of “low-complexity” polynomials. Let I be the ideal of polynomials f satisfying $f \circ G = 0$, also known as the *vanishing ideal* of G [26]. To show that G has the desired HSG property, it suffices to show that every nonzero $f \in I$ has sufficiently high complexity so that no such f can belong to \mathcal{C} . With a closure result for I , this reduces to proving lower bounds for the distinguished set $\{g_1, \dots, g_k\}$. This can be viewed as a particular instance of the “hardness vs. randomness” paradigm of [37] in the setting of algebraic complexity.

Principal ideals. The simplest polynomial ideals are the *principal* ideals, i.e., the ideals generated by a single polynomial g . For such an ideal I , any nonzero $f \in I$ is a multiple of g and questions may be rephrased in the context of factorization. Thus, choosing $S = \{g\}$, the closure result described above follows from the classical closure result under factorization, which states that if f is efficiently computable in a given model, then so are its factors. For the class **VP**, this property follows from Kaltofen’s work on polynomial factorization, which in particular showed that if $f \in \mathbb{F}[x_1, \dots, x_n]$ is a polynomial of degree $\text{poly}(n)$ computed by an algebraic circuit of size $\text{poly}(n)$, then its factors also admit $\text{poly}(n)$ -size algebraic circuits [27, 28, 29]. Closure under factorization has also been studied, and in some cases established (or partially established), in more restricted models; see [38, 13, 7, 42, 20, 8].

Before moving to non-principal ideals, we recall some technical aspects of closure under factorization. Kaltofen’s result [27, 28, 29] more generally states that if $f \in \mathbb{F}[x_1, \dots, x_n]$ is computed by an algebraic circuit of size s , then each factor g of f can be computed by an algebraic circuit of size $\text{poly}(n, s, \deg(f))$. This polynomial dependence on $\deg(f)$ is not an obstacle when f has degree $\text{poly}(n)$. However, if $\deg(f)$ is much larger than $\deg(g)$, then the bound $\text{poly}(n, s, \deg(f))$ may be trivial and prevent one from deducing meaningful lower bounds on the complexity of f from those of g .

On the other hand, Bürgisser’s *Factor Conjecture* [11, Conjecture 8.3] states that over a field of characteristic zero, if f is computed by an algebraic circuit of size s , then any factor g of f can be computed by an algebraic circuit of size $\text{poly}(n, s, \deg(g))$ (rather than $\deg(f)$). Although the conjecture remains open, partial results are known [27, 11, 12, 20]. In particular, Bürgisser [12] proved that the Factor Conjecture holds when standard circuit complexity is replaced by *border complexity* (also known as *approximative complexity*). Specifically, Bürgisser showed that if f is computed by an algebraic circuit of size s , then any factor g of f is *approximately computed* by an algebraic circuit of size polynomial in n , s , and $\deg(g)$ over the function field $\mathbb{F}(\varepsilon)$. The notion of approximate computation is defined as follows:

► **Definition 1.** We say that $g \in \mathbb{F}[x_1, \dots, x_n]$ is approximately computed by a circuit C over $\mathbb{F}(\varepsilon)$ if C computes some polynomial $h \in \mathbb{F}(\varepsilon)[x_1, \dots, x_n]$, and $h - g \in \varepsilon \cdot \mathbb{F}[[\varepsilon]][x_1, \dots, x_n]$, where $\mathbb{F}[[\varepsilon]]$ denotes the ring of formal power series in ε .

In the settings where $\mathbb{F}[[\varepsilon]][x_1, \dots, x_n]$ can be equipped with the Euclidean topology in a natural way, such as $\mathbb{F} = \mathbb{C}$ or \mathbb{R} , this would imply that $h \rightarrow g$ as $\varepsilon \mapsto 0$. However, this does not mean that we could just substitute ε by zero in C and obtain a circuit exactly computing g , since C may use scalars in $\mathbb{F}(\varepsilon)$, such as $1/\varepsilon$, that are not well-defined at $\varepsilon = 0$.

Non-principal ideals. Closure results for non-principal ideals were not directly studied until recently. In [24], Grochow conjectured such a result for determinantal ideals. Specifically, for any nonzero f in the determinantal ideal I generated by the $\frac{n}{2} \times \frac{n}{2}$ minors of an $n \times n$ symbolic matrix $X = (x_{i,j})_{1 \leq i,j \leq n}$, the computation of minors reduces to the computation of f , although the determinant size may be polynomially smaller than $\frac{n}{2} \times \frac{n}{2}$. Formally:

► **Conjecture 2** ([24, Conjecture 6.3]). *Let X be an $n \times n$ matrix of indeterminates and let I_n be the ideal generated by the $\frac{n}{2} \times \frac{n}{2}$ minors of X . Then for every nonzero polynomial $f \in I_n$, there is a constant-depth¹ algebraic circuit of size $\text{poly}(n)$ with f -oracle gates that computes the $m \times m$ determinant for some $m = n^{\Theta(1)}$.*

► **Remark 3.** We note that Conjecture 2 asserts that the computation of $m \times m$ determinants reduces to that of f . The existence of such a reduction is formally stronger than a closure result, and we therefore refer to it as a *reducibility result*. In this paper we do not carefully distinguish between the two notions, since the main results we prove are also of the stronger reducibility type.

Analogous to Bürgisser’s theorem [12] that the Factor Conjecture holds with respect to border complexity, Andrews and Forbes [2] proved that Grochow’s conjecture holds with respect to border complexity. Formally, they proved the following theorem:

► **Theorem 4** ([2, Theorem 1.1]). *Let \mathbb{F} be a field of characteristic zero. Let $X = (x_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$ be an $n \times m$ matrix of variables over \mathbb{F} and let $I_{n,m,r}^{\text{det}} \subseteq \mathbb{F}[X] = \mathbb{F}[x_{i,j}]$ be the ideal generated by the $r \times r$ minors of X . Let $f \in I_{n,m,r}^{\text{det}}$ be a nonzero polynomial. Then there is a depth-three f -oracle circuit of size $O(n^2 m^2)$ that approximately computes the $t \times t$ determinant for $t = \Theta(r^{1/3})$.*

In the same paper, Andrews and Forbes also gave an analogous result for the Pfaffian of a $2n \times 2n$ skew-symmetric matrix and the ideal generated by Pfaffians of $2r \times 2r$ principal submatrices, and that these results still hold over fields of sufficiently large characteristic.

As mentioned above, closure results are useful for constructing HSGs and derandomizing PIT by reducing these tasks to proving lower bounds for distinguished polynomials. In particular, by combining Theorem 4 with the celebrated superpolynomial lower bounds for constant-depth algebraic circuits due to Limaye, Srinivasan, and Tavenas [33] (which also hold in the border complexity setting, as observed in [2]), Andrews and Forbes [2] obtained a simple construction of HSGs for constant-depth circuits. By further composing this construction with scaled copies of itself, they gave a final HSG construction that achieves a near-optimal trade-off between seed length and degree with subpolynomial seed length, improving upon the earlier construction of [13] and yielding improved subexponential-time deterministic PIT algorithms for constant-depth algebraic circuits.

Back to exact computation. Note that Theorem 4 proves Grochow’s conjecture (Conjecture 2), but only with respect to border complexity. This leaves open the natural question: Does the conjecture also hold in the standard (exact) setting?

We begin with a technical issue. In Grochow’s formulation of the conjecture, the algebraic circuit computing the determinant is required to have size $\text{poly}(n)$, independent of $\deg(f)$, even though $\deg(f)$ may be much larger than n . This degree-independent condition is the

¹ The original statement of the conjecture does not specify constant-depth algebraic circuits. However, it is already known that the $m \times m$ determinant can be computed by algebraic circuits of size $\text{poly}(m)$.

central technical challenge in proving the conjecture, because existing approaches naturally introduce a dependence on the degree. The situation is analogous to the difficulty encountered in Bürgisser’s Factor Conjecture, although neither conjecture implies the other, and they could well have different resolutions or require unrelated methods.

On the other hand, most applications in algebraic complexity involve only polynomials of polynomially bounded degree. For example, Kaltofen’s result showing that **VP** is closed under factorization suffices for many purposes, even though the full Factor Conjecture remains open. Motivated by this, we restrict our attention to polynomials f of degree $\text{poly}(n)$ and ask whether Grochow’s conjecture holds in this regime. More generally, we may allow circuit size to depend polynomially on both n and $\deg(f)$. This leads to the following question:

► **Question 5.** *Is Conjecture 2 true when $\deg(f) = \text{poly}(n)$? More generally, under the notation of Conjecture 2, is it true that there is a constant-depth algebraic circuit of size $\text{poly}(n, \deg(f))$ (rather than $\text{poly}(n)$ as in Conjecture 2) with f -oracle gates that computes the $t \times t$ determinant for some $t = n^{\Theta(1)}$?*

1.1 Main Results

In this paper, we answer Question 5 affirmatively by establishing the following theorem:

► **Theorem 6** (Informal version of Theorem 45 and Corollary 46). *Let $X = (x_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$ be an $n \times m$ matrix of variables over a field \mathbb{F} . Let $I_{n,m,r}^{\det} \subseteq \mathbb{F}[X] = \mathbb{F}[x_{i,j} \mid 1 \leq i \leq n, 1 \leq j \leq m]$ be the ideal generated by the $r \times r$ minors of X . Let $f \in I_{n,m,r}^{\det}$ be a nonzero polynomial. Assume that the characteristic of \mathbb{F} is either zero or greater than $\deg(f)$. Also assume that the size of \mathbb{F} is sufficiently large.² Then there exists a depth-three f -oracle circuit of size $\text{poly}(n, m, \deg(f))$ that computes the $t \times t$ determinant for $t = \Theta(r^{1/3})$.*

We also prove an analogous claim for the case where our matrix X is a $2n \times 2n$ skew-symmetric matrix of variables, so that $x_{j,i} = -x_{i,j}$. In this case, the determinant is actually a perfect square, and this polynomial is known as the *Pfaffian* of X .

► **Theorem 7** (Informal Pfaffian Analogue [16]). *Let $X = (x_{i,j})_{1 \leq i < j \leq 2n}$ be a $2n \times 2n$ skew-symmetric matrix of variables over a field \mathbb{F} so that $x_{j,i} = -x_{i,j}$ for $1 \leq j < i \leq n$ and $x_{i,i} = 0$ for $1 \leq i \leq 2n$. Let $I_{2n,2r}^{\text{pfaff}} \subseteq \mathbb{F}[X] = \mathbb{F}[x_{i,j} \mid 1 \leq i < j \leq 2n]$ be the ideal generated by the $2r \times 2r$ principal minors of X . Let $f \in I_{2n,2r}^{\text{pfaff}}$ be a nonzero polynomial. Assume that the characteristic of \mathbb{F} is either zero or greater than $\deg(f)$. Also assume that the size of \mathbb{F} is sufficiently large. Then there exists a depth-three f -oracle circuit of size $\text{poly}(n, \deg(f))$ that computes the $t \times t$ Pfaffian of a skew-symmetric matrix for $t = \Theta(r^{1/3})$.*

It is worth noting that determinantal and Pfaffian ideals can be studied within unified frameworks, notably Hodge algebras [15] and Standard Monomial Theory [31, 40]. In this paper, however, we do not adopt these approaches as they are more abstract than necessary.

While Theorem 6 does not by itself yield new PIT algorithms, because Theorem 4 already suffices given that the lower bounds of [33] hold in the border complexity setting, it resolves a natural theoretical question that was previously open.

² Specifically, we require $|\mathbb{F}|$ to be bounded below by some polynomial in n , m , and $\deg(f)$. Such assumptions are standard in the literature (for instance, in work on polynomial factorization), since one can often achieve them by passing to a suitable field extension.

Theorem 6 may also be viewed as a “debordering” result: showing that a statement known to hold with respect to border complexity continues to hold in the exact setting, possibly with somewhat larger complexity bounds. In general, such results are highly nontrivial: naively converting a circuit that approximately computes a polynomial into one that computes it exactly can cause an exponential blow-up, due to exponentially large degree in ε of the scalars used in the approximation [32, 11]. Nevertheless, by exploiting the structure of determinantal and Pfaffian ideals, we show that this difficulty can be overcome, yielding debordering results. See [18, 6, 19, 41] for other nontrivial debordering results in various settings.

1.2 Proof Overview

The main tool in our proof is the *isolation lemma* of Valiant and Vazirani [46]. This lemma, along with derandomized variants, has found applications in theoretical computer science, including parallel algorithms for perfect matching [35, 21, 44], polynomial identity testing [30, 3, 25], and search-to-decision reductions [46, 5, 23], among others. To the best of our knowledge, this paper is the first to apply the isolation lemma to debordering results.

The version of the isolation lemma we use [30] can be stated as follows. Consider a collection \mathcal{C} of monomials of individual degree at most K in variables x_1, \dots, x_ℓ . Suppose we substitute each variable by $x_i \mapsto w^{z_i}$, where the exponents z_1, \dots, z_ℓ are chosen independently and uniformly from $\{0, \dots, M\}$ with $M \geq K\ell/\varepsilon$. Then, with probability at least $1 - \varepsilon$, there is a unique monomial $\mathbf{m} \in \mathcal{C}$ that attains the minimum degree in w under this substitution.

In this way, we reduce the number of variables to a single one while ensuring that the polynomial does not vanish after substitution: the unique monomial of minimum degree in w cannot be canceled by others. For comparison, a Kronecker substitution $x_i \mapsto w^{D^{i-1}}$ for sufficiently large D achieves the same effect. However, the advantage of the isolation lemma is that the exponents z_i need only be polynomial in ℓ and K , whereas the Kronecker map requires that D is exponentially large.

To see why this advantage helps us prove Theorem 6, let us first review the proof of Theorem 4 from [2]. Let $f \in I_{n,m,r}^{\det}$ be a nonzero polynomial. Our goal is to compute the $t \times t$ determinant using an f -oracle circuit. The proof in [2] relies on a technique from algebraic combinatorics called the straightening law, which expresses f as a linear combination of special polynomials known as standard bideterminants. Each standard bideterminant is a product of determinants of submatrices of $X = (x_{i,j})$, and in our setting, every such bideterminant includes at least one determinant of sufficiently large size.

The argument then proceeds in two steps. The first step transforms this linear combination of standard bideterminants into a single “canonical” standard bideterminant. The second step computes a determinant from a standard bideterminant. Our second step is identical to that in [2]; therefore, we focus on the first step.

At a high level, the way [2] transforms a linear combination of standard bideterminants into a single standard bideterminant is by applying a sequence of linear transformations of the variables, so that each standard bideterminant in the combination is eventually mapped to a term that equals (up to sign) the target standard bideterminant. However, applying this idea naively does not work, since terms arising from different standard bideterminants may cancel each other. To avoid this, [2] choose the linear transformations so that they effectively multiply the terms by distinct monomials in some new variables. As a result, terms originating from different standard bideterminants are “tagged” with different monomials. Finally, a Kronecker-type substitution is applied to merge these new variables into a single one while still maintaining the existence of nonzero terms, yielding a polynomial of the form

$$g = \varepsilon^k g_0 + O(\varepsilon^{k+1})$$

over $\mathbb{F}(\varepsilon)$, where g_0 is a distinguished standard bideterminant. This standard bideterminant can then be used to compute the $t \times t$ determinant. The presence of the $O(\varepsilon^{k+1})$ term poses no issue for proving Theorem 4, as the theorem concerns only approximate computation.

To turn approximate computation into exact computation, a natural idea is to extract the degree- k homogeneous component of g in ε and then set $\varepsilon = 1$. However, this approach does not work directly because the degree of g in ε can become exponentially large due to the use of the Kronecker-type substitution. Consequently, the circuit obtained by extracting the degree- k component directly would have exponential size.

This is precisely where the isolation lemma becomes useful. By replacing the Kronecker-type substitution with the randomized variable substitution from the isolation lemma, we can ensure that the degree in ε remains only polynomially large. Consequently, extracting the degree- k homogeneous component yields a polynomial-size circuit, as desired.

Although the high-level idea is simple, carrying it out requires substantial technical work. Unlike the Kronecker substitution, the isolation lemma offers only limited control over which monomial is isolated. In particular, the linear transformations from [2] produce additional “garbage” terms which, in their setting, were always dominated in the lexicographic order and could be safely ignored. With the isolation lemma, however, these extraneous terms may instead be isolated – something we must avoid. Thus, simply combining the isolation lemma with the analysis of [2] does not suffice. To address this, we integrate the isolation lemma with additional ideas in a subtle way, allowing us to recover the desired terms while discarding the extraneous ones. The technical details are deferred to Section 3.

2 Preliminaries

For a natural number n , we denote the set $\{1, 2, \dots, n-1, n\}$ by $[n]$. We will denote fields by \mathbb{F} . Throughout, we will work primarily with polynomial rings with coefficients in a field. For a field \mathbb{F} and a set of indeterminates $\bar{x} = \{x_1, \dots, x_n\}$, we write $\mathbb{F}[\bar{x}]$ for the ring of polynomials in the variables x_1, \dots, x_n with coefficients in \mathbb{F} . We note that in addition to $\mathbb{F}[\bar{x}]$ being a ring, it is also an \mathbb{F} -vector space and that ideals of $\mathbb{F}[\bar{x}]$ are subspaces. Thus, it will make sense to talk about an \mathbb{F} -basis of an ideal in addition to a generating set for that ideal. Occasionally, we will just mention $\mathbb{F}[\bar{x}]$ without specifying the number of variables when the exact number is not important or is implied by context. If the variables come from an $n \times m$ matrix $X = (x_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$, then we notate the respective polynomial ring as $\mathbb{F}[X]$.

In any case, when $f \in \mathbb{F}[\bar{x}]$, we write $\deg(f)$ to denote the total degree of f . We will also write $\deg_{x_i}(f)$ to denote the total degree of f with respect to x_i specifically.

We will assume basic notions in algebraic complexity theory; see, e.g., the survey of Saptharishi [39]. In particular, the size of an algebraic circuit is the number of gates plus the number of wires, and scalar multiplications along wires are free. As we will be working with constant-depth circuits, gates are assumed to have unbounded fan-in and fan-out. We will also work with algebraic branching programs and will assume their edges are labeled by polynomials of degree at most one. One motivation for the connection to algebraic branching programs is that algebraic branching programs on n nodes compute polynomials which are determinants of $O(n) \times O(n)$ matrices [45, Theorem 1].

In addition to standard algebraic circuits, we will use algebraic oracle circuits:

► **Definition 8 (Oracle circuit).** *Let $g(\bar{x}) \in \mathbb{F}[\bar{x}]$, where \bar{x} denotes x_1, \dots, x_n . A (algebraic) g -oracle circuit C over \mathbb{F} is an algebraic circuit augmented with an additional type of gate called a g -gate. A g -gate with inputs f_1, \dots, f_n outputs the polynomial $g(f_1, \dots, f_n)$.*

2.1 Linear Algebra

Throughout, all rings will be commutative with 1. For any ring A and natural numbers n, m , let $A^{n \times m}$ be the set of all $n \times m$ matrices over A . For such a matrix $M \in A^{n \times m}$, we will write $M = (m_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$ to denote that (i, j) -th entry of M by $m_{i,j}$. For a square matrix $M \in A^{n \times n}$, we will denote the $n \times n$ determinant by $\det_n(M)$.

► **Definition 9** (Elementary matrix). *Let i, j be distinct elements in $[n]$, and let $z \in A$. Then the elementary matrix $E_{i,j}(z) \in A^{n \times n}$ is an $n \times n$ matrix with 1's down the main diagonal, z in position (i, j) , and 0's elsewhere. Note that $\det_n(E_{i,j}(z)) = 1$. These elementary matrices correspond to row operations when multiplying on the left, and column operations when multiplying on the right. Indeed if $M \in A^{n \times m}$, consider $E_{i,j}(z) \in A^{n \times n}$. Then the product $E_{i,j}(z)M$ is the matrix given by adding z times row j of M to row i of M . Similarly, if we take $E_{i,j}(z) \in A^{m \times m}$, then the product $ME_{i,j}(z)^\top$ is the matrix given by adding z times column j of M to column i of M .*

Let A be any ring and $M \in A^{n \times m}$. For subsets $R \subseteq [n]$ and $C \subseteq [m]$, we will denote by $M_{R,C}$ the submatrix of M with rows given by R and columns given by C . If $R = C$ then such a submatrix is *principal*.

For a positive integer n , let S_n be the *permutation group* on $[n]$, i.e., the group of bijections $\sigma: [n] \rightarrow [n]$. For a permutation $\sigma \in S_n$, we may associate an $n \times n$ *permutation matrix* C_σ such that $(C_\sigma)_{i,j} = 1$ if $\sigma(i) = j$ and 0 otherwise. Note that $C_\sigma^{-1} = C_\sigma^\top$. The *sign* of a permutation $\sigma \in S_n$ is defined using the number of inversions ($i < j$ such that $\sigma(i) > \sigma(j)$):

$$\text{sgn}(\sigma) = (-1)^{|\{(i,j) \mid 1 \leq i < j \leq n, \sigma(i) > \sigma(j)\}|} = \pm 1.$$

Then we have that $\det_n(C_\sigma) = \text{sgn}(\sigma) = \pm 1$. For a $n \times n$ matrix $M \in A^{n \times n}$, we have that $(C_\sigma M C_\sigma^\top)_{i,j} = M_{\sigma(i), \sigma(j)}$, i.e. $C_\sigma M C_\sigma^\top$ is the matrix such that $(C_\sigma M C_\sigma^\top)_{i,j} = M_{\sigma(i), \sigma(j)}$.

2.2 Bitableaux

► **Definition 10** (Partition, Young diagram). *A partition is a non-increasing sequence of integers $\sigma = (\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_k \geq 0)$ for some $k \geq 1$. The size of a partition is the sum of the size of its parts and is denoted $|\sigma| = \sum_{i=0}^k \sigma_i$. To such a partition σ , we can associate the transpose $\hat{\sigma} = (\hat{\sigma}_1 \geq \dots \geq \hat{\sigma}_\ell)$ for some $\ell \geq 1$ where $\hat{\sigma}_i := |\{j \in \mathbb{N} \mid \sigma_j \geq i\}|$. A partition σ can be given pictorially as a Young diagram which formally is the set of points $\{(i, j) \mid j \leq \sigma_i\} \subseteq \mathbb{N} \times \mathbb{N}$. This indexing follows the same indexing as entries of a matrix, so that the first coordinate increases as one traverses downwards and the second coordinate increases as one traverses to the right. We refer to each point of a Young diagram as a cell. The Young diagram of $\hat{\sigma}$ is the reflection of the Young diagram for σ over the diagonal $y = x$. Note that $\hat{\sigma}_1$ is the number of non-empty rows of the Young diagram for σ .*

These partitions have a natural lexicographic ordering which is useful for describing ideals indexed by partitions of a given shape or size.

► **Definition 11.** *The ordering $1 < 2 < 3 < \dots$ induces a lexicographic ordering on partitions, which we denote by \leq_{lex} . This ordering has a minor caveat in that extending a partition makes it smaller with respect to \leq_{lex} . Formally, for partitions $\lambda = (\lambda_1 \geq \dots \geq \lambda_t)$ and $\mu = (\mu_1 \geq \dots \geq \mu_s)$ we have that $\lambda \leq_{\text{lex}} \mu$ if and only if exactly one of the following holds:*

1. *For some $1 \leq k \leq \min\{s, t\}$, we have that $\lambda_k < \mu_k$ and $\lambda_i = \mu_i$ for all $1 \leq i \leq k-1$, or*
2. *We have that $s \geq t$ and for all $1 \leq i \leq t$ we have that $\lambda_i = \mu_i$, i.e., μ is a prefix of λ .*

► **Definition 12** (Young tableau). A Young tableau, or tableau for short, of shape σ is an assignment of positive integers to each cell of the Young diagram of σ . A Young tableau is semistandard if its entries are nondecreasing along the rows of the diagram and strictly increasing along the columns. A Young tableau is standard if its entries are both strictly increasing along the rows of the diagram and strictly increasing along the columns. If T is a Young tableau of shape σ , then its conjugate \widehat{T} is a Young tableau of shape $\widehat{\sigma}$ whose entry $T(i, j)$ in cell (i, j) is the entry $T(j, i)$ of cell (j, i) of T . We will also denote the i -th row of T by T_i . Throughout this paper, we will mostly work with conjugate semistandard Young tableaux whose entries are strictly increasing along the rows of the diagram and nondecreasing along the columns, i.e., they are the conjugates of semistandard Young tableaux.

► **Definition 13.** Let $\sigma = (\sigma_1 \geq \dots \geq \sigma_k \geq 0)$ be any partition and T a Young tableau of shape σ . Then we define the size of T , denoted $|T|$, to be the sum of all entries of T .

Much of our analysis will center around special tableau which are the maximal and minimal conjugate semistandard Young tableau of shape σ with respect to the size.

► **Definition 14** (Canonical/anti-canonical tableau). Fix a natural number n . Let $\sigma = (\sigma_1 \geq \dots \geq \sigma_k > 0)$ be a partition such that the length σ_i of each row is at most n . Define $K_{\sigma,n}$ to be the tableau of shape σ where row i has entries $1, 2, \dots, \sigma_i$. Similarly, define $\overline{K}_{\sigma,n}$ to be the tableau of shape σ where row i has entries $(n - \sigma_i + 1, n - \sigma_i + 2, \dots, n)$. We call $K_{\sigma,n}$ and $\overline{K}_{\sigma,n}$ the canonical and anti-canonical tableau respectively.³ Note that $K_{\sigma,n}$ and $\overline{K}_{\sigma,n}$ are both conjugate semistandard. When n is clear from context, we will just write K_σ and \overline{K}_σ .

2.3 Determinantal Ideals

Let \mathbb{F} be a field. Let $X = (x_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$ be a $n \times m$ matrix of variables. We will denote by $\mathbb{F}[X]$ the polynomial ring $\mathbb{F}[x_{i,j} \mid 1 \leq i \leq n, 1 \leq j \leq m]$. We can naturally associate a product of minors of X to a pair of Young tableau where the minors are described by their entries.

► **Definition 15** (Bitableau, bideterminant). Let $\sigma = (\sigma_1 \geq \dots \geq \sigma_k)$ be a partition. An (n, m) -bitableau $(S \mid T)$ of shape σ is a pair of two Young tableau of shape σ with where the entries of S come from $[n]$ and the entries of T come from $[m]$. When n and m are clear from context, we just call $(S \mid T)$ a bitableau. For each $i \in [\widehat{\sigma}_1]$, write the i -th row of S and the i -th row of T as $S_i = (S(i, 1), \dots, S(i, \sigma_i))$ and $T_i = (T(i, 1), \dots, T(i, \sigma_i))$ respectively. The $\sigma_i \times \sigma_i$ minor of X defined by S_i and T_i is the matrix

$$\left(x_{S(i,a), T(i,b)} \right)_{1 \leq a, b \leq \sigma_i} = \begin{pmatrix} x_{S(i,1), T(i,1)} & x_{S(i,1), T(i,2)} & \cdots & x_{S(i,1), T(i, \sigma_i)} \\ x_{S(i,2), T(i,1)} & x_{S(i,2), T(i,2)} & \cdots & x_{S(i,2), T(i, \sigma_i)} \\ \vdots & \vdots & \ddots & \vdots \\ x_{S(i, \sigma_i), T(i,1)} & x_{S(i, \sigma_i), T(i,2)} & \cdots & x_{S(i, \sigma_i), T(i, \sigma_i)} \end{pmatrix}.$$

Then the associated bideterminant $(S \mid T)(X)$ is the product of all such minors over $i \in [\widehat{\sigma}_1]$:

$$(S \mid T)(X) := \prod_{i=1}^{\widehat{\sigma}_1} \det_{\sigma_i} \left(x_{S(i,a), T(i,b)} \right)_{1 \leq a, b \leq \sigma_i}.$$

An $n \times n$ determinant is homogeneous of degree n so that $(S \mid T)(X)$ is a homogeneous polynomial of degree $|\sigma|$.

³ In some sources, such as [10], these are referred to as the *initial* and *final* tableau.

The following lemma shows that every monomial in $\mathbb{F}[X]$ can be expressed as a bideterminant, and hence the bideterminants span $\mathbb{F}[X]$ as an \mathbb{F} -vector space. The proof is immediate from the definition.

► **Lemma 16.** *A degree d monomial $\prod_{i=1}^d x_{r_i, c_i}$ is given by a bideterminant:*

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

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

While the bideterminants span $\mathbb{F}[X]$, there is a specific subset of bideterminants, the *standard* bideterminants, which form an \mathbb{F} -basis of $\mathbb{F}[X]$.

► **Definition 17** (Standard bitableau, standard bideterminant). *We call a bitableau $(S | T)$ and its associated bideterminant $(S | T)(X)$ standard if S and T are both conjugate semistandard Young tableaux.*

The next theorem is known in the literature as the *straightening law*.

► **Theorem 18** ([17, §8, Theorem 3], [14, Corollary 2.3]). *Let $(S | T)(X)$ be a bideterminant of shape σ . Then $(S | T)(X)$ can be uniquely expressed as a linear combination*

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

where $(A | B)(X)$ is a standard bideterminant of shape $\tau \geq_{\text{lex}} \sigma$, and $c_{A,B} \in \mathbb{Z}$ when $\text{char}(\mathbb{F}) = 0$, while $c_{A,B} \in \mathbb{Z}/p\mathbb{Z}$ when $\text{char}(\mathbb{F}) = p > 0$.

The fact that bideterminants are homogeneous polynomials, together with Lemma 16 and Theorem 18, imply the following corollary.

► **Corollary 19.** *The standard bideterminants form an \mathbb{F} -basis of $\mathbb{F}[X]$. In particular, since bideterminants are homogeneous with respect to total degree, the degree- d component of $\mathbb{F}[X]$ has as basis the standard bideterminants of shape σ such that $|\sigma| = d$.*

Let $I_{n,m,r}^{\det}$ be the ideal of $\mathbb{F}[X]$ generated by the $r \times r$ minors of X . Note that this ideal is a \mathbb{F} -subspace of $\mathbb{F}[X]$. We have the following crucial statement on the \mathbb{F} -basis of this ideal.

► **Proposition 20** ([9, Corollary 1.7]). *Polynomials $f \in I_{n,m,r}^{\det}$ are supported by standard bideterminants of shape σ such that $\sigma_1 \geq r$; that is, by those whose first row has length at least r .*

The notion of the total degree of a polynomial is too coarse for differentiating terms in the expansion of a polynomial $f \in I_{n,m,r}^{\det}$ with respect to the standard basis. Thus, we describe a grading of the polynomial ring $\mathbb{F}[X]$ that is better suited for this purpose.

► **Definition 21.** *The polynomial ring $\mathbb{F}[X]$ has a natural $(\mathbb{N}^n \oplus \mathbb{N}^m)$ -grading. Let $\bar{e}_i \in \mathbb{N}^n$ be the standard basis vector with a 1 in position i and 0's in the other positions. Define $\bar{e}_i \in \mathbb{N}^m$ the same way. Then we assign $x_{i,j}$ to have degree $\bar{e}_i \oplus \bar{e}_j$. We call this assignment the multidegree. We say a polynomial $f \in \mathbb{F}[X]$ is multihomogeneous of multidegree $(s_1 \bar{e}_1 + \cdots + s_n \bar{e}_n) \oplus (t_1 \bar{e}_1 + \cdots + t_m \bar{e}_m)$ if every monomial in f has multidegree $(s_1 \bar{e}_1 + \cdots + s_n \bar{e}_n) \oplus (t_1 \bar{e}_1 + \cdots + t_m \bar{e}_m)$.*

The following lemma gives the multidegree of bideterminants. In particular, the multidegree of canonical and anti-canonical bideterminants will allow us to extract terms of a particular shape.

► **Lemma 22.** *Fix a natural number $n \in \mathbb{Z}_{\geq 0}$. Let $\sigma = (\sigma_1 \geq \dots \geq \sigma_d)$ be a partition such that the length σ_i of each row is at most n . Let S, T be two conjugate semistandard Young tableaux. Then a bideterminant $(S \mid T)(X)$ is multihomogeneous of multidegree $(s_1 \bar{e}_1 + \dots + s_n \bar{e}_n) \oplus (t_1 \bar{e}_1 + \dots + t_n \bar{e}_n)$, where s_i is equal to the number of i 's that appear in S and t_j is equal to the number of j 's that appear in T . In particular, $(K_\sigma \mid K_\sigma)(X)$ is multihomogeneous of multidegree $(\hat{\sigma}_1 \bar{e}_1 + \dots + \hat{\sigma}_n \bar{e}_n) \oplus (\hat{\sigma}_1 \bar{e}_1 + \dots + \hat{\sigma}_n \bar{e}_1)$. Moreover, for distinct partitions $\sigma \neq \tau$, the multidegrees of $(K_\sigma \mid K_\sigma)(X)$ and $(K_\tau \mid K_\tau)(X)$ are distinct, and the same holds for the multidegrees of $(\overline{K}_\sigma \mid \overline{K}_\sigma)(X)$ and $(\overline{K}_\tau \mid \overline{K}_\tau)(X)$.*

2.4 Isolation Lemma

One crucial tool used in this work is the *isolation lemma*. We use the following version due to Klivans and Spielman [30].

► **Lemma 23** ([30, Lemma 4]). *Let C be any collection of distinct linear forms in variables z_1, \dots, z_ℓ with coefficients in the range $\{0, \dots, K\}$ for some integer $K \in \mathbb{Z}_{\geq 0}$. Let $\varepsilon > 0$. Let z_1, \dots, z_ℓ be independently and uniformly chosen from $\{0, \dots, M\}$ at random, where $M \geq K\ell/\varepsilon$. Then, with probability at least $1 - \varepsilon$, there is a unique form in C of minimum value at z_1, \dots, z_ℓ .*

A simple rephrasing of Lemma 23 allows us to isolate a term of a multivariate polynomial $f(y_1, \dots, y_\ell)$ under a random monomial substitution $y_i \mapsto w^{z_i}$:

► **Corollary 24.** *Let $K \in \mathbb{Z}_{\geq 0}$. Let A be any ring, and let $f(y_1, \dots, y_\ell) \in A[\bar{y}]$ be a polynomial whose individual degree in each variable is at most K , i.e., $\deg_{y_i}(f) \leq K$ for all $i \in [\ell]$. Fix $\varepsilon > 0$. Choose z_1, \dots, z_ℓ independently and uniformly at random from $\{0, \dots, M\}$, where $M \geq K\ell/\varepsilon$. Let w be a new indeterminate, and define $\phi: A[y_1, \dots, y_\ell] \rightarrow A[w]$ to be the ring homomorphism sending $y_i \mapsto w^{z_i}$ for each $i \in [\ell]$. Then, with probability at least $1 - \varepsilon$, there exists a unique monomial $\mathbf{m} = y_1^{e_1} \dots y_\ell^{e_\ell}$ among all monomials of f such that $\phi(\mathbf{m}) = w^{e_1 z_1 + \dots + e_\ell z_\ell}$ attains the minimum degree in w .*

2.5 Computing the Homogeneous Components

There are multiple methods in the literature for computing the homogeneous components of a given polynomial. In this paper, we use an interpolation-based method and observe that it also applies in the oracle-circuit setting.

► **Definition 25.** *For $f \in \mathbb{F}[\bar{x}, t]$ and an integer $i \in \mathbb{Z}_{\geq 0}$, denote by $\text{coeff}_{t^i}(f)$ the coefficient of t^i in f when f is viewed as a univariate polynomial in t over the ring $\mathbb{F}[\bar{x}]$. Note that $\text{coeff}_{t^i}(f) \in \mathbb{F}[\bar{x}]$.*

The following lemma shows that the coefficients of a polynomial computed by a g -oracle circuit C can be extracted by another g -oracle circuit of comparable depth. While this differs from computing homogeneous components, the two notions are closely related: the degree- i homogeneous component of $f \in \mathbb{F}[x_1, \dots, x_n]$ is exactly $\text{coeff}_{t^i}(f(tx_1, \dots, tx_n))$. While the result on homogenization is standard, we use a careful analysis of the structure of the resulting oracle circuit. With this, we are able to get a tighter control on the depth of circuits in our proofs. See [16, Lemma 2.29] for a proof.

► **Lemma 26.** *Let $g \in \mathbb{F}[\bar{x}, t]$, and let $f \in \mathbb{F}[\bar{x}, t]$ be a degree- d polynomial such that for each $\alpha \in \mathbb{F}$, the polynomial $f(\bar{x}, \alpha)$ is computed by a g -oracle circuit C_α of size at most s and depth at most Δ . Assume that $|\mathbb{F}| \geq d + 1$. Then, for every $0 \leq i \leq d$, there exists a g -oracle circuit D_i of size $O(ds)$ and depth $\Delta + 1$ that computes $\text{coeff}_{t^i}(f)$, with its top gate being an addition gate and bottom Δ layers consisting of $d + 1$ copies of g -oracle circuits of the form C_α . Moreover, if the top gate of each C_α is an addition gate, then the depth bound can be improved to Δ .*

► **Remark 27.** The condition $|\mathbb{F}| \geq d + 1$ in Lemma 26, required for interpolation, is the sole reason our main theorems assume the base field \mathbb{F} to be sufficiently large. We also note that if g is given not as a black box but as a white-box circuit, then its homogeneous components can be extracted in a gate-by-gate fashion [43], which requires no lower bound on $|\mathbb{F}|$.

3 Determinantal Ideals

Our application of the determinantal straightening law (Corollary 19), together with the isolation lemma (Corollary 24) and extraction of coefficients (Lemma 26), allows us to isolate a canonical bitableau from the expansion of nonzero $f \in I_{n,m,r}^{\det}$ in the basis of standard bideterminants. In particular, we will show that this can be done via a polynomial-sized depth-three f -oracle circuit using the isolation lemma (Corollary 24) as well as coefficient extraction (Lemma 26). This is in contrast to the proof of [2], where they use a Kronecker-type substitution in order to isolate terms. To do this, we will give a more careful analysis of the terms that arise when applying the substitution operators to the expression of a polynomial $f(X) \in I_{n,m,r}^{\det}$.

Throughout, fix a field \mathbb{F} . Let n, m be natural numbers, and for $1 \leq i \leq n$ and $1 \leq j \leq m$, let $x_{i,j}$ be indeterminates. Throughout this section, let $X = (x_{i,j})$ be an $n \times m$ matrix of variables. Let $1 \leq r \leq \min(n, m)$ and define $I_{n,m,r}^{\det}$ to be the ideal in $\mathbb{F}[X]$ generated by the $r \times r$ minors of X .

Our first step is to define a series of linear transformations sending a conjugate semistandard bitableau to the anti-canonical conjugate semistandard bitableau of the same shape.

► **Definition 28** (Substitution operator). *Let $i < j$. Define the operator $\text{Sub}_{i \rightarrow j}$ which takes as input a tableau S and returns the tableau S' which is formed by taking each row of S which has an i but not a j , replacing that i with j , and then sorting the row in increasing order. We also define $h_i^j(S)$ to be the number of times i is replaced by j after applying $\text{Sub}_{i \rightarrow j}$ to S .*

While these substitution operators $\text{Sub}_{i \rightarrow j}$ on their own are not injective, they are injective when restricted to the set of conjugate semistandard tableau if we make use of the value h_i^j .

► **Lemma 29** ([14, Proposition 1.6]). *Let $i, j \in [n]$. Consider a conjugate semistandard tableau S such that if a row in S contains an integer $k \leq i$, then that same row in S contains all integers in $\{i, i + 1, \dots, j - 1\}$. Then $\text{Sub}_{i \rightarrow j}(S)$ is again conjugate semistandard. Furthermore, S is completely determined by $\text{Sub}_{i \rightarrow j}(S)$ and $h_i^j(S)$.*

We will primarily use Lemma 29 in the context of successive applications. In particular, we will be able to completely determine the original tableau from the tableau obtained after successive applications of $\text{Sub}_{i \rightarrow j}$ together with the values of h_i^j . We then apply these successive substitutions in the following lexicographic order:

► **Definition 30** (Lexicographic ordering). *We order the elements of $\{(i, j) \mid 1 \leq i < j \leq n\}$ such that $(i, j) \preceq (i', j')$ if either $i < i'$, or $i = i'$ and $j \leq j'$.*

49:12 Debordering Closure Results in Determinantal and Pfaffian Ideals

In particular, note that the hypothesis in Lemma 29 holds trivially for the operator $\text{Sub}_{1 \rightarrow 2}$. Furthermore, as we apply the substitution operators successively in the lexicographic ordering, the resulting tableaux also satisfy the hypothesis.

► **Lemma 31** (implicit in the proof of [14, Corollary 1.7]; see [2, Claim 3.2] for a proof). *Fix a partition σ . For a natural number n and $1 \leq i < j \leq n$ and a conjugate semistandard tableau S of shape σ , define $S_{i',j'}$ where*

$$S_{i',j'} = (\text{Sub}_{i' \rightarrow j'} \circ \cdots \circ \text{Sub}_{2 \rightarrow n} \circ \cdots \circ \text{Sub}_{2 \rightarrow 3} \circ \text{Sub}_{1 \rightarrow n} \circ \cdots \circ \text{Sub}_{1 \rightarrow 2})(S),$$

and (i', j') is the immediate predecessor of (i, j) in the lexicographic ordering on $\binom{[n]}{2}$. By convention, if $(i, j) = (1, 2)$, then we define $S_{i',j'} = S$. Then $S_{i',j'}$ satisfies the hypothesis of Lemma 29 for $\text{Sub}_{i \rightarrow j}$, meaning that if a row of $S_{i',j'}$ contains an integer $k \leq i$, then that same row in S contains all integers in $\{i, i+1, \dots, j-1\}$.

► **Lemma 32.** *Fix a partition σ . For a natural number n and $1 \leq i < j \leq n$ and a conjugate semistandard tableau S of shape σ , define $h_{n,i,j}$ as $h_i^j(S_{i',j'})$ where*

$$S_{i',j'} = (\text{Sub}_{i' \rightarrow j'} \circ \cdots \circ \text{Sub}_{2 \rightarrow n} \circ \cdots \circ \text{Sub}_{2 \rightarrow 3} \circ \text{Sub}_{1 \rightarrow n} \circ \cdots \circ \text{Sub}_{1 \rightarrow 2})(S),$$

and (i', j') is the immediate predecessor of (i, j) in the ordering on $\binom{[n]}{2}$. By convention, if $(i, j) = (1, 2)$, then we define $S_{i',j'} = S$. Then S is completely determined by $S_{i,j}(S)$ and the ordered sequence $\{h_{n,a,b}(S)\}_{(a,b) \preceq (i,j)}$.

Proof. We prove via induction on (i, j) in the lexicographic order. If $(i, j) = (1, 2)$, this follows from Lemma 29 as S is completely determined by $\text{Sub}_{1 \rightarrow 2}(S)$ and $h_1^2(S)$.

Now, suppose (i, j) is strictly larger than $(1, 2)$ in the lexicographic ordering, and let (i', j') be the immediate predecessor of (i, j) . Assume the claim holds for (i', j') in place of (i, j) . As $h_{n,i,j}(S) = h_i^j(S_{i',j'})$, we have that $S_{i',j'}(S)$ is completely determined by S and $h_{n,i,j}(S)$ via Lemma 29 and Lemma 31. By the induction hypothesis, S is completely determined by $S_{i',j'}(S)$ and the sequence $\{h_{n,a,b}(S)\}_{(a,b) \preceq (i',j')}$. Thus S is completely determined by $S_{i,j}(S)$ and the sequence $\{h_{n,a,b}(S)\}_{(a,b) \preceq (i,j)}$, completing the proof. ◀

Applying the substitution operators along the full lexicographic ordering transforms a conjugate semistandard tableau into the anti-canonical tableau of the same shape:

► **Lemma 33** ([14, 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*

$$(\text{Sub}_{n-1 \rightarrow n} \circ \text{Sub}_{n-2 \rightarrow n} \circ \cdots \circ \text{Sub}_{2 \rightarrow n} \circ \cdots \circ \text{Sub}_{2 \rightarrow 3} \circ \text{Sub}_{1 \rightarrow n} \circ \cdots \circ \text{Sub}_{1 \rightarrow 2})(S) = \overline{K}_\sigma.$$

We now study how these substitution operators act on bideterminants $(S | T)(X)$. From properties of the determinant, we see that multiplying the matrix of variables X by an elementary matrix $E_{i,j}$ corresponds to applying substitution operators on S or T . With this, we use the multilinearity of the determinant and careful analysis to show that the values $h_i^j(S)$ “mark” terns containing bitableau where $(S | T)$ has turned into $(\text{Sub}_{i \rightarrow j}(S) | T)$.

► **Lemma 34.** *Let λ be a new indeterminate. Let $(S | T)$ be a bitableau, not necessarily standard, of shape σ . For $0 \leq h \leq h_i^j(S) - 1$, let $\mathcal{C}_{i \rightarrow j}^h(S)$ 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. Then we have that*

$$(S | T)(E_{i,j}(\lambda)X) = \pm \lambda^{h_i^j(S)} (\text{Sub}_{i \rightarrow j}(S) | T)(X) + \sum_{h=0}^{h_i^j(S)-1} \lambda^h \sum_{S' \in \mathcal{C}_{i \rightarrow j}^h(S)} \pm (S' | T)(X). \quad (1)$$

Similarly, we also have that

$$(S | T)(X E_{i,j}(\lambda)^\top) = \pm \lambda^{h_i^j(T)} (S | \text{Sub}_{i \rightarrow j}(T))(X) + \sum_{h=0}^{h_i^j(T)-1} \lambda^h \sum_{T' \in \mathcal{C}_{i \rightarrow j}^h(T)} \pm (S | T')(X). \quad (2)$$

3.1 Isolating One Term

In this subsection, in addition to the variables $x_{i,j}$, where $i \in [n]$ and $j \in [m]$, we introduce new sets of indeterminates $\Lambda = \{\lambda_{i,j} \mid 1 \leq i < j \leq n\}$ and $\Xi = \{\xi_{i,j} \mid 1 \leq i < j \leq m\}$. We have that $|\Lambda| = \binom{n}{2} = O(n^2)$ and $|\Xi| = \binom{m}{2} = O(m^2)$. The purpose of these new indeterminates is that they will allow us to keep track of the effects of substitution operators as we isolate a canonical bitableau.

Define $M \in \mathbb{F}[\Lambda]^{n \times n}$ and $N \in \mathbb{F}[\Xi]^{m \times m}$ by

$$M = E_{1,2}(\lambda_{1,2}) \cdots E_{1,n}(\lambda_{1,n}) E_{2,3}(\lambda_{2,3}) \cdots E_{2,n}(\lambda_{2,n}) \\ \cdots E_{n-2,n-1}(\lambda_{n-2,n-1}) E_{n-2,n}(\lambda_{n-2,n}) E_{n-1,n}(\lambda_{n-1,n})$$

and

$$N = E_{m-1,m}(\xi_{m-1,m})^\top E_{m-2,m}(\xi_{m-2,m})^\top E_{m-2,m-1}(\xi_{m-2,m-1})^\top \\ \cdots E_{2,m}(\xi_{2,m})^\top \cdots E_{2,3}(\xi_{2,3})^\top E_{1,m}(\xi_{1,m})^\top \cdots E_{1,2}(\xi_{1,2})^\top.$$

Recall the lexicographic ordering \preceq (Definition 30) on the elements of $\binom{[n]}{2}$. This induces a lexicographic order on $(\mathbb{Z}_{\geq 0})^{\binom{[n]}{2}}$. In the same way, we order the elements of $\binom{[m]}{2} = \{(i,j) \mid 1 \leq i < j \leq m\}$, which induces a lexicographic order on $(\mathbb{Z}_{\geq 0})^{\binom{[m]}{2}}$. This also induces a lexicographic term order on the monomials in the variables Λ and Ξ via their degree vectors. Finally, we define the lexicographic order on $(\mathbb{Z}_{\geq 0})^{\binom{[n]}{2}} \times (\mathbb{Z}_{\geq 0})^{\binom{[m]}{2}}$ by comparing the first component before the second component. We use M and N to obtain polynomials in $\mathbb{F}[X, \Lambda, \Xi]$ with some terms consisting of anti-canonical bideterminants.

► **Lemma 35.** *Let $f(X) \in I_{n,m,r}^{\det}$ be a nonzero polynomial of degree d . Then $f(MX)$ can be expressed as a sum*

$$f(MX) = \sum_{k \in A} \tilde{c}_k \Lambda^{\bar{e}_k} \cdot (\bar{K}_{\sigma_k} | T_k)(X) + \sum_{\ell \in A'} \tilde{c}_\ell \Lambda^{\bar{e}_\ell} \cdot (S_\ell | T_\ell)(X), \quad (3)$$

such that the following hold:

1. A is a nonempty finite set and A' is finite set disjoint from A .
2. All terms in Equation (3) have the form $c \Lambda^{\bar{e}} \cdot (S | T)(X)$, $c \in \mathbb{F}^\times$, $\bar{e} \in \{0, 1, \dots, d\}^{\binom{[n]}{2}}$, and $(S | T)(X)$ is a bideterminant in $I_{n,m,r}^{\det}$ of degree d . In particular, if S and T have shape σ , then $|\sigma| \leq d$.
3. T_k is a conjugate semistandard tableau of shape σ_k for $k \in A$.
4. For every $\ell \in A'$, there exists $k = k(\ell) \in A$ such that \bar{e}_ℓ is strictly smaller than \bar{e}_k in the lexicographic order and the shape σ_ℓ of $(S_\ell | T_\ell)$ equals the shape σ_k .
5. The triples $(\bar{e}_k, \sigma_k, T_k)$ are distinct as k ranges over A .

Proof. By Corollary 19 and Proposition 20, we can expand $f(X)$ as a linear combination of standard bideterminants over \mathbb{F}

$$f(X) = \sum_{k \in B} c_k \cdot (S_k | T_k)(X)$$

49:14 Debordering Closure Results in Determinantal and Pfaffian Ideals

where B is nonempty, each $c_k \in \mathbb{F}^\times$, and $(S_k | T_k)(X)$ is a standard bideterminant in $I_{n,m,r}^{\det}$ of shape σ_k where $|\sigma_k| \leq d$ for $k \in A$, with these bideterminants being distinct as k ranges over B . It follows that

$$f(MX) = \sum_{k \in B} c_k \cdot (S_k | T_k)(MX).$$

For each $k \in B$, we expand the term $c_k \cdot (S_k | T_k)(MX)$ by repeatedly applying Lemma 34. This expansion shows that $c_k \cdot (S_k | T_k)(MX)$ equals $\pm c_k \Lambda^{\bar{e}_k} \cdot (\bar{K}_{\sigma_k} | T_k)(X)$ with $\bar{e}_k = (h_{n,i,j}(S_k))_{1 \leq i < j \leq n} \in \{0, 1, \dots, d\}^{\binom{[n]}{2}}$ plus some terms of the form $\pm \tilde{c}_\ell \Lambda^{\bar{e}_\ell} \cdot (S_\ell | T_\ell)(X)$, each with a new index ℓ , where $\tilde{c}_\ell = \pm c_k$, $(S_\ell | T_\ell)(X)$ is a (not necessarily standard) bideterminant of shape $\sigma_\ell = \sigma_k$, and \bar{e}_ℓ is strictly smaller than \bar{e}_k in the lexicographic order. Note that as $\sigma_\ell = \sigma_k$, their first rows both have length at least r , implying that $(S_\ell | T_\ell)(X) \in I_{n,m,r}^{\det}$ by Proposition 20. Also note that $\bar{e}_\ell \in \{0, 1, \dots, d\}^{\binom{[n]}{2}}$ since a substitution $i \mapsto j$ can be performed at most $(\hat{\sigma}_\ell)_1 \leq d$ times to any tableau of shape σ_ℓ . We add ℓ to A' for each such term and let $k(\ell) = k$ and add this k to A .

Therefore, we have the expansion

$$f(MX) = \sum_{k \in A} \pm c_k \Lambda^{\bar{e}_k} \cdot (\bar{K}_{\sigma_k} | T_k)(X) + \sum_{\ell \in A'} \tilde{c}_\ell \Lambda^{\bar{e}_\ell} \cdot (S_\ell | T_\ell)(X)$$

satisfying Items 1–4.

It remains to prove Item 5. Assume to the contrary that there exist distinct $k_1, k_2 \in A$ such that $(\bar{e}_{k_1}, \sigma_{k_1}, T_{k_1}) = (\bar{e}_{k_2}, \sigma_{k_2}, T_{k_2})$. As the bideterminants $(S_k | T_k)$ are distinct as k ranges over A , we have $S_{k_1} \neq S_{k_2}$, both of which are conjugate semistandard. From the proof above, we have $\bar{e}_{k_1} = (h_{n,i,j}(S_{k_1}))_{1 \leq i < j \leq n}$ and $\bar{e}_{k_2} = (h_{n,i,j}(S_{k_2}))_{1 \leq i < j \leq n}$. Note that S_{k_1} and S_{k_2} have the same shape $\sigma_{k_1} = \sigma_{k_2}$. By Lemma 32, S_{k_1} is completely determined by $\bar{K}_{\sigma_{k_1}}$ and $(h_{n,i,j}(S_{k_1}))_{1 \leq i < j \leq n}$, and S_{k_2} is completely determined by $\bar{K}_{\sigma_{k_2}}$ and $(h_{n,i,j}(S_{k_2}))_{1 \leq i < j \leq n}$. But then if $\bar{e}_{k_1} = \bar{e}_{k_2}$ and $\sigma_{k_1} = \sigma_{k_2}$, we must have that $S_{k_1} = S_{k_2}$, a contradiction. \blacktriangleleft

► **Lemma 36.** *Let $f(X) \in I_{n,m,r}^{\det}$ be a nonzero polynomial of degree d . Then $f(MXN)$ can be expressed as a sum*

$$f(MXN) = \sum_{k \in A} \hat{c}_k \Lambda^{\bar{e}_k} \Xi^{\bar{f}_k} \cdot (\bar{K}_{\sigma_k} | \bar{K}_{\sigma_k})(X) + \sum_{\ell \in B} \hat{c}_\ell \Lambda^{\bar{e}_\ell} \Xi^{\bar{f}_\ell} \cdot (S_\ell | T_\ell)(X), \quad (4)$$

such that the following hold:

1. A is a nonempty finite set and B is finite set disjoint from A .
2. All terms in Equation (4) have the form $c \Lambda^{\bar{e}} \Xi^{\bar{f}} \cdot (S | T)(X)$, where $c \in \mathbb{F}^\times$, $\bar{e} \in \{0, 1, \dots, d\}^{\binom{[n]}{2}}$, $\bar{f} \in \{0, 1, \dots, d\}^{\binom{[m]}{2}}$, and $(S | T)(X)$ is a bideterminant in $I_{n,m,r}^{\det}$ of degree at most d . In particular, if S and T have shape σ , then $|\sigma| \leq d$.
3. For every $\ell \in B$, there exists $k = k(\ell) \in A$ such that $(\bar{e}_\ell, \bar{f}_\ell)$ is strictly smaller than (\bar{e}_k, \bar{f}_k) in the lexicographic order and the shape σ_ℓ of $(S_\ell | T_\ell)$ equals the shape σ_k .
4. The triples $(\bar{e}_k, \bar{f}_k, \sigma_k)$ are distinct, where k ranges over A .

Proof. We use Lemma 35 to write $f(MX)$ as

$$f(MX) = \sum_{k \in A} \tilde{c}_k \Lambda^{\bar{e}_k} \cdot (\bar{K}_{\sigma_k} | T_k)(X) + \sum_{\ell \in A'} \tilde{c}_\ell \Lambda^{\bar{e}_\ell} \cdot (S_\ell | T_\ell)(X).$$

Then

$$f(MXN) = \sum_{k \in A} \tilde{c}_k \Lambda^{\bar{e}_k} \cdot (\bar{K}_{\sigma_k} | T_k)(XN) + \sum_{\ell \in A'} \tilde{c}_\ell \Lambda^{\bar{e}_\ell} \cdot (S_\ell | T_\ell)(XN).$$

For each $k \in A$, we expand the term $\tilde{c}_k \Lambda^{\bar{e}_k} \cdot (\overline{K}_{\sigma_k} \mid T_k)(XN)$ by repeatedly applying Lemma 34. This expansion shows that $\tilde{c}_k \Lambda^{\bar{e}_k} \cdot (\overline{K}_{\sigma_k} \mid T_k)(XN)$ equals $\pm \tilde{c}_k \Lambda^{\bar{e}_k} \Xi^{\bar{f}_k} \cdot (\overline{K}_{\sigma_k} \mid \overline{K}_{\sigma_k})(X)$ with $\bar{f}_k = (h_{m,i,j}(T_k))_{1 \leq i < j \leq m} \in \{0, 1, \dots, d\}^{\binom{m}{2}}$, plus some terms of the form $\hat{c}_\ell \Lambda^{\bar{e}_\ell} \Xi^{\bar{f}_\ell} \cdot (S_\ell \mid T_\ell)(X)$, each with a new index ℓ , where $\hat{c}_\ell = \pm \tilde{c}_k$, $(S_\ell \mid T_\ell)(X)$ is a (not necessarily standard) bideterminant of shape $\sigma_\ell = \sigma_k$, $\bar{e}_\ell = \bar{e}_k$, and \bar{f}_ℓ is strictly smaller than \bar{f}_k in the lexicographic order. In particular, $(\bar{e}_\ell, \bar{f}_\ell)$ is strictly smaller than (\bar{e}_k, \bar{f}_k) in the lexicographic order. Note that as $\sigma_\ell = \sigma_k$, their first rows both have length at least r , implying that $(S_\ell \mid T_\ell)(X) \in I_{n,m,r}^{\det}$ by Proposition 20. Also note that $\bar{f}_\ell \in \{0, 1, \dots, d\}^{\binom{m}{2}}$ since a substitution $i \mapsto j$ can be performed at most $(\hat{\sigma}_\ell)_1 \leq d$ times to any tableau of shape σ_ℓ . We add ℓ to B for each such term and let $k(\ell) = k$.

For each $\ell \in A'$, we expand the term $\tilde{c}_\ell \Lambda^{\bar{e}_\ell} \cdot (S_\ell \mid T_\ell)(XN)$ by repeatedly applying Lemma 34. Note that $(S_\ell \mid T_\ell)$ is not necessarily standard, but Lemma 34 still applies. Consider any term $\hat{c}_{\ell'} \Lambda^{\bar{e}_{\ell'}} \Xi^{\bar{f}_{\ell'}} \cdot (S_{\ell'} \mid T_{\ell'})(X)$ generated this way, where ℓ' is a new index. Let $k = k(\ell)$ as in Lemma 35 (4). We have $\hat{c}_{\ell'} = \pm \tilde{c}_\ell$, $(S_{\ell'} \mid T_{\ell'})(X)$ is a (not necessarily standard) bideterminant of shape $\sigma_{\ell'} = \sigma_\ell = \sigma_k$, and $\bar{e}_{\ell'} = \bar{e}_\ell$, which is strictly smaller than \bar{e}_k in the lexicographic order. In particular, $(\bar{e}_{\ell'}, \bar{f}_{\ell'})$ is strictly smaller than (\bar{e}_k, \bar{f}_k) in the lexicographic order. Note that as $\sigma_{\ell'} = \sigma_k$, their first rows both have length at least r , implying that $(S_{\ell'} \mid T_{\ell'})(X) \in I_{n,m,r}^{\det}$ by Proposition 20. Also note that $\bar{f}_{\ell'} \in \{0, 1, \dots, d\}^{\binom{m}{2}}$ for the same reason as in the previous paragraph. We add ℓ' to B for each such term and let $k(\ell') = k$.

Therefore, we have the expansion satisfying Items 1–3:

$$f(MXN) = \sum_{k \in A} \pm \tilde{c}_k \Lambda^{\bar{e}_k} \Xi^{\bar{f}_k} \cdot (\overline{K}_{\sigma_k} \mid \overline{K}_{\sigma_k})(X) + \sum_{\ell \in B} \hat{c}_\ell \Lambda^{\bar{e}_\ell} \Xi^{\bar{f}_\ell} \cdot (S_\ell \mid T_\ell)(X).$$

It remains to prove Item 4. Assume to the contrary that there exist distinct $k_1, k_2 \in A$ such that $(\bar{e}_{k_1}, \bar{f}_{k_1}, \sigma_{k_1}) = (\bar{e}_{k_2}, \bar{f}_{k_2}, \sigma_{k_2})$. By Lemma 35 (5), we have $T_{k_1} \neq T_{k_2}$, both of which are conjugate semistandard. From the proof above, we have $\bar{f}_{k_1} = (h_{m,i,j}(T_{k_1}))_{1 \leq i < j \leq m}$ and $\bar{f}_{k_2} = (h_{m,i,j}(T_{k_2}))_{1 \leq i < j \leq m}$. Note that T_{k_1} and T_{k_2} have the same shape $\sigma_{k_1} = \sigma_{k_2}$. By Lemma 32, T_{k_1} is completely determined by $\overline{K}_{\sigma_{k_1}}$ and $(h_{m,i,j}(T_{k_1}))_{1 \leq i < j \leq m}$, and T_{k_2} is completely determined by $\overline{K}_{\sigma_{k_2}}$ and $(h_{m,i,j}(T_{k_2}))_{1 \leq i < j \leq m}$. But then if $\bar{f}_{k_1} = \bar{f}_{k_2}$ and $\sigma_{k_1} = \sigma_{k_2}$, we must have that $T_{k_1} = T_{k_2}$, a contradiction. ◀

Next, we reformulate Lemma 36 by permuting the rows and columns of X , thereby transforming the anti-canonical bitableaux into canonical tableaux. This transformation is not essential, but it simplifies the notation and analysis.

For an integer $k > 0$, let $J_k \in \mathbb{F}^{k \times k}$ be the $k \times k$ matrix with 1's along the anti-diagonal from the bottom left to the top right and 0's elsewhere. Note that $\det_k(J_k) = (-1)^{\binom{k}{2}} = \pm 1$. The substitution $X \mapsto J_n X J_m$ has the effect of replacing row i with row $n - i + 1$ and column j with column $m - j + 1$, mapping $(\overline{K}_\sigma \mid \overline{K}_\sigma)$ to a canonical tableau $(K_\sigma \mid K_\sigma)$.

► **Corollary 37.** *Let $f(X) \in I_{n,m,r}^{\det}$ be a nonzero polynomial of degree d . Then $f(MJ_n X J_m N)$ can be expressed as a sum*

$$f(MJ_n X J_m N) = \sum_{k \in A} \hat{c}_k \Lambda^{\bar{e}_k} \Xi^{\bar{f}_k} \cdot (K_{\sigma_k} \mid K_{\sigma_k})(X) + \sum_{\ell \in B} \hat{c}_\ell \Lambda^{\bar{e}_\ell} \Xi^{\bar{f}_\ell} \cdot (S_\ell \mid T_\ell)(X), \quad (5)$$

such that the following hold:

1. A is a nonempty finite set and B is finite set disjoint from A .
2. All terms in Equation (5) have the form $c \Lambda^{\bar{e}} \Xi^{\bar{f}} \cdot (S \mid T)(X)$, where $c \in \mathbb{F}^\times$, $\bar{e} \in \{0, 1, \dots, d\}^{\binom{m}{2}}$, $\bar{f} \in \{0, 1, \dots, d\}^{\binom{m}{2}}$, and $(S \mid T)(X)$ is a bideterminant in $I_{n,m,r}^{\det}$ of degree d . In particular, if S and T have shape σ , then $|\sigma| \leq d$.

49:16 Debordering Closure Results in Determinantal and Pfaffian Ideals

3. For every $\ell \in B$, there exists $k = k(\ell) \in A$ such that $(\bar{e}_\ell, \bar{f}_\ell)$ is strictly smaller than (\bar{e}_k, \bar{f}_k) in the lexicographic order and the shape σ_ℓ of $(S_\ell | T_\ell)$ equals the shape σ_k .
4. The triples $(\bar{e}_k, \bar{f}_k, \sigma_k)$ are distinct, where k ranges over A .

Next, we introduce new variables $Y = \{y_1, \dots, y_n\}$ and $Z = \{z_1, \dots, z_m\}$. Define the diagonal matrices

$$D = \text{diag}(y_1, \dots, y_n) \in \mathbb{F}[Y]^{n \times n} \quad \text{and} \quad D' = \text{diag}(z_1, \dots, z_m) \in \mathbb{F}[Z]^{m \times m}.$$

► **Lemma 38.** *Let $(S | T)(X)$ be a bideterminant of degree at most d . Then $(S | T)(DXD') = Y^{\bar{s}}Z^{\bar{t}} \cdot (S | T)(X)$, where $\bar{s} = (s_1, \dots, s_n) \in \{0, 1, \dots, d\}^n$, $\bar{t} = (t_1, \dots, t_m) \in \{0, 1, \dots, d\}^m$, s_i is the number of times i appears in S , t_j is the number of times j appears in T .*

Proof. Reduce to the case in which S and T have one row, then use the multilinearity. ◀

We will often simply say that $(S | T)(X)$ in Lemma 38 has multidegree (\bar{s}, \bar{t}) rather than writing it as $(s_1 e_1 + \dots + s_n e_n) \oplus (t_1 e_1 + \dots + t_m e_m)$.

Next, we introduce another variable v , and modify D and D' as follows:

$$\tilde{D} = \text{diag}(y_1 v, y_2 v^2, \dots, y_n v^n) \in \mathbb{F}[Y, v]^{n \times n}, \quad \tilde{D}' = \text{diag}(z_1 v, z_2 v^2, \dots, z_m v^m) \in \mathbb{F}[Z, v]^{m \times m}.$$

► **Lemma 39.** *Let $(S | T)(X)$ be a bideterminant. Then $(S | T)(\tilde{D}X\tilde{D}') = Y^{\bar{s}}Z^{\bar{t}}v^{|\bar{s}|+|\bar{t}|} \cdot (S | T)(X)$, where (\bar{s}, \bar{t}) is the multidegree of $(S | T)(X)$.*

Proof. Replacing y_i by $y_i v^i$ in D multiplies the expression by v^i exactly s_i times. Similarly, replacing z_j by $z_j v^j$ in D' multiplies the expression by v^j exactly t_j times. Taking all $i \in [n]$ and $j \in [m]$ into account, the total exponent of v is $|\bar{s}| + |\bar{t}|$. ◀

Before proceeding, we clarify the relationship between our arguments and those in [2]. Much of our proof follows the overall structure of [2]: the expansions in (3), (4), and (5) already appear there. However, our statements refine those in [2] by providing more detailed information about the “garbage” terms (those indexed by the sets A' or B in (3), (4), and (5)). In particular, we establish additional properties of these terms that will be used in the proof of the key lemma below, which serves as preparation for our use of the isolation lemma.

The main difference between the two approaches lies in how a term associated with a canonical standard bideterminant is singled out. The proof in [2] uses a Kronecker-type substitution and therefore only needs to ensure that the lexicographically leading term is unique. In contrast, our argument applies the isolation lemma, which isolates a term but does not, a priori, guarantee that the isolated term corresponds to a canonical standard bideterminant. The following lemma shows, through a careful analysis that relies on the properties established in Corollary 37, that isolating a term of lowest degree in v indeed yields a canonical standard bideterminant.

► **Lemma 40.** *Let $f(X) \in I_{n,m,r}^{\det}$ be a nonzero polynomial of degree d and let $g = f(MJ_n \tilde{D}X\tilde{D}'J_m N) \in \mathbb{F}[X, \Lambda, \Xi, Y, Z, v]$.*

View g as a univariate polynomial in v with coefficients in $\mathbb{F}[X, \Lambda, \Xi, Y, Z]$, and write $g = \sum_i \text{coeff}_{v^i}(g)v^i$, where $\text{coeff}_{v^i}(g) \in \mathbb{F}[X, \Lambda, \Xi, Y, Z]$ denotes the coefficient of v^i in g . Choose the smallest integer d_{\min} such that $\text{coeff}_{v^{d_{\min}}}(g) \neq 0$. Then $d_{\min} = 2|K_\sigma|$ for some shape σ with $|\sigma| \leq d$ and we may write $\text{coeff}_{v^{d_{\min}}}(g)$ as a finite sum

$$\text{coeff}_{v^{d_{\min}}}(g) = \sum_{k \in I} c_k \Lambda^{\bar{e}_k} \Xi^{\bar{f}_k} Y^{\bar{s}_k} Z^{\bar{t}_k} \cdot (K_{\sigma_k} | K_{\sigma_k})(X), \quad (6)$$

such that the following hold:

1. For each $k \in I$, $c_k \in \mathbb{F}^\times$, $(\sigma_k)_1 \geq r$, and $|\sigma_k| \leq d$.
2. The tuples $(\bar{e}_k, \bar{f}_k, \bar{s}_k, \bar{t}_k)$ are distinct, where k ranges over I .

Proof. Consider the expansion

$$f(MJ_n X J_m N) = \sum_{k \in A} \hat{c}_k \Lambda^{\bar{e}_k} \Xi^{\bar{f}_k} \cdot (K_{\sigma_k} | K_{\sigma_k})(X) + \sum_{\ell \in B} \hat{c}_\ell \Lambda^{\bar{e}_\ell} \Xi^{\bar{f}_\ell} \cdot (S_\ell | T_\ell)(X)$$

given by Corollary 37. Then we have

$$\begin{aligned} g &= \sum_{k \in A} \hat{c}_k \Lambda^{\bar{e}_k} \Xi^{\bar{f}_k} \cdot (K_{\sigma_k} | K_{\sigma_k})(\tilde{D}X\tilde{D}') + \sum_{\ell \in B} \hat{c}_\ell \Lambda^{\bar{e}_\ell} \Xi^{\bar{f}_\ell} \cdot (S_\ell | T_\ell)(\tilde{D}X\tilde{D}') \\ &= \sum_{k \in A} \hat{c}_k \Lambda^{\bar{e}_k} \Xi^{\bar{f}_k} Y^{\bar{s}_k} Z^{\bar{t}_k} v^{2|K_{\sigma_k}|} \cdot (K_{\sigma_k} | K_{\sigma_k})(X) \\ &\quad + \sum_{\ell \in B} \hat{c}_\ell \Lambda^{\bar{e}_\ell} \Xi^{\bar{f}_\ell} Y^{\bar{s}_\ell} Z^{\bar{t}_\ell} v^{|\bar{S}_\ell|+|\bar{T}_\ell|} \cdot (S_\ell | T_\ell)(X), \end{aligned} \tag{7}$$

where for $k \in A$, (\bar{s}_k, \bar{t}_k) is the multidegree of $(K_{\sigma_k} | K_{\sigma_k})(X)$, and for $\ell \in B$, $(\bar{s}_\ell, \bar{t}_\ell)$ is the multidegree of $(S_\ell | T_\ell)(X)$. Here, the second equality holds by Lemma 39.

Choose $k_0 \in A$ so that $|K_{\sigma_{k_0}}|$ is minimized, and subject to this, $(\bar{e}_{k_0}, \bar{f}_{k_0})$ is maximized in the lexicographic order. Let $d_0 = 2|K_{\sigma_{k_0}}|$. We will show that $\text{coeff}_{v^{d_0}}(g) \neq 0$.

For any $k \in A$, consider the term $\hat{c}_k \Lambda^{\bar{e}_k} \Xi^{\bar{f}_k} Y^{\bar{s}_k} Z^{\bar{t}_k} v^{2|K_{\sigma_k}|} \cdot (K_{\sigma_k} | K_{\sigma_k})(X)$ in Equation (7). It is homogeneous of degree $2|K_{\sigma_k}| \geq 2|K_{\sigma_{k_0}}| = d_0$ with respect to v by the minimality of $|K_{\sigma_{k_0}}|$, and contributes to $\text{coeff}_{v^{d_0}}(g)$ if and only if $|K_{\sigma_k}| = |K_{\sigma_{k_0}}|$. Even if it can potentially contribute to $\text{coeff}_{v^{d_0}}(g)$, its (multi)degree $(\bar{e}_k, \bar{f}_k, \bar{s}_k, \bar{t}_k)$ in the variables Λ, Ξ, Y , and Z is different from that of the term indexed by k_0 unless $k = k_0$. To see this, suppose $k \neq k_0$. Then $(\bar{e}_k, \bar{f}_k, \sigma_k) \neq (\bar{e}_{k_0}, \bar{f}_{k_0}, \sigma_{k_0})$. If $\sigma_k = \sigma_{k_0}$, then $(\bar{e}_k, \bar{f}_k) \neq (\bar{e}_{k_0}, \bar{f}_{k_0})$. On the other hand, if $\sigma_k \neq \sigma_{k_0}$, then $(\bar{s}_k, \bar{t}_k) \neq (\bar{s}_{k_0}, \bar{t}_{k_0})$ by Lemma 22. Overall, we always have that $(\bar{e}_k, \bar{f}_k, \bar{s}_k, \bar{t}_k) \neq (\bar{e}_{k_0}, \bar{f}_{k_0}, \bar{s}_{k_0}, \bar{t}_{k_0})$.

Now consider $\ell \in B$ and the term $\mathbf{m}_\ell := \hat{c}_\ell \Lambda^{\bar{e}_\ell} \Xi^{\bar{f}_\ell} Y^{\bar{s}_\ell} Z^{\bar{t}_\ell} v^{|\bar{S}_\ell|+|\bar{T}_\ell|} \cdot (S_\ell | T_\ell)(X)$ in Equation (7). The degree of \mathbf{m}_ℓ in v is $|\bar{S}_\ell| + |\bar{T}_\ell|$. Let $k = k(\ell)$ as in Corollary 37. Then by Corollary 37 (3), S_ℓ and T_ℓ have shape $\sigma_\ell = \sigma_k$. Note that among all bideterminants $(S | T)$ of shape σ , the quantity $|S| + |T|$ is minimized when, and only when, $(S | T) = (K_\sigma | K_\sigma)$. Thus, we have $|\bar{S}_\ell| + |\bar{T}_\ell| \geq 2|K_{\sigma_k}| \geq 2|K_{\sigma_{k_0}}| = d_0$ and $\deg_v(\mathbf{m}_\ell) = |\bar{S}_\ell| + |\bar{T}_\ell| = d_0$ if and only if $(S_\ell | T_\ell) = (K_{\sigma_k} | K_{\sigma_k})$ and $|K_{\sigma_k}| = |K_{\sigma_{k_0}}|$. Even though this can happen, when it happens we have that (\bar{e}_k, \bar{f}_k) is smaller than or equal to $(\bar{e}_{k_0}, \bar{f}_{k_0})$ in the lexicographic order by the choice of k_0 , noting that $|K_{\sigma_k}| = |K_{\sigma_{k_0}}|$. And by Corollary 37 (3), $(\bar{e}_\ell, \bar{f}_\ell)$ is strictly smaller than (\bar{e}_k, \bar{f}_k) in the lexicographic order. Overall, either $\deg_v(\mathbf{m}_\ell) > d_0$, or $(\bar{e}_\ell, \bar{f}_\ell, \bar{s}_\ell, \bar{t}_\ell) \neq (\bar{e}_{k_0}, \bar{f}_{k_0}, \bar{s}_{k_0}, \bar{t}_{k_0})$.

By the above analysis, the term $\hat{c}_{k_0} \Lambda^{\bar{e}_{k_0}} \Xi^{\bar{f}_{k_0}} Y^{\bar{s}_{k_0}} Z^{\bar{t}_{k_0}} v^{2|K_{\sigma_{k_0}}|} \cdot (K_{\sigma_{k_0}} | K_{\sigma_{k_0}})(X)$ is not canceled by other terms contributing to $\text{coeff}_{v^{d_0}}(g)$ due to the uniqueness of its (multi)degree $(\bar{e}_{k_0}, \bar{f}_{k_0}, \bar{s}_{k_0}, \bar{t}_{k_0})$ in Λ, Ξ, Y , and Z . Thus $\text{coeff}_{v^{d_0}}(g) \neq 0$. The above analysis also shows that $\text{coeff}_{v^i}(g) = 0$ for $i < d_0$. Thus, $d_0 = d_{\min}$. Moreover, the above analysis shows that any term that contributes to $\text{coeff}_{v^{d_0}}(g)$ contains a bideterminant of the form $(K_\sigma | K_\sigma)(X)$.

We then merge the terms contributing to $\text{coeff}_{v^{d_0}}(g)$ with the same (multi)degree in Λ, Ξ, Y , and Z . When we merge two terms $\hat{c}_k \Lambda^{\bar{e}_k} \Xi^{\bar{f}_k} Y^{\bar{s}_k} Z^{\bar{t}_k} v^{d_0} \cdot (K_{\sigma_k} | K_{\sigma_k})(X)$ and $\hat{c}_{k'} \Lambda^{\bar{e}_{k'}} \Xi^{\bar{f}_{k'}} Y^{\bar{s}_{k'}} Z^{\bar{t}_{k'}} v^{d_0} \cdot (K_{\sigma_{k'}} | K_{\sigma_{k'}})(X)$ with $(\bar{e}_k, \bar{f}_k, \bar{s}_k, \bar{t}_k) = (\bar{e}_{k'}, \bar{f}_{k'}, \bar{s}_{k'}, \bar{t}_{k'})$, we always have $(K_{\sigma_k} | K_{\sigma_k}) = (K_{\sigma_{k'}} | K_{\sigma_{k'}})$. This follows from Lemma 22 and the fact that (\bar{s}_k, \bar{t}_k) is the multidegree of $(K_{\sigma_k} | K_{\sigma_k})(X)$ and $(\bar{s}_{k'}, \bar{t}_{k'})$ is the multidegree of $(K_{\sigma_{k'}} | K_{\sigma_{k'}})(X)$. Thus, merging the two terms yields a scalar multiple of both.

49:18 Debordering Closure Results in Determinantal and Pfaffian Ideals

After merging, we can write $\text{coeff}_{v^{d_{\min}}}(g) = \text{coeff}_{v^{d_0}}(g)$ in the form of Equation (6) such that Item 2 holds. Furthermore, Item 1 holds as well by Corollary 37 (2) and Proposition 20. \blacktriangleleft

Lemma 40 helps us separate a collection of terms solely containing canonical bideterminants. The next lemma applies the isolation lemma to single out one term from this collection.

► **Lemma 41.** *Let $f(X) \in I_{n,m,r}^{\det}$ be a nonzero polynomial of degree d and let $g = f(MJ_n \tilde{D}X \tilde{D}'J_m N) \in \mathbb{F}[X, \Lambda, \Xi, Y, Z, v]$. Then there exist integers $z_t = O(d(n^2 + m^2))$ for each variable $t \in \Lambda \sqcup \Xi \sqcup Y \sqcup Z$, and an integer $z_v = O(d^2(n^2 + m^2))$ such that for the two variable substitution maps*

$$\phi: t \mapsto w^{z_t} \quad \text{for } t \in \Lambda \sqcup \Xi \sqcup Y \sqcup Z, \quad \psi: v \mapsto w^{z_v},$$

we have that $h := (\psi \circ \phi)(g) \in \mathbb{F}[X, w]$ has $\deg_w(h) = O(d^3(n^3 + m^3))$, and that $\text{coeff}_{w^i}(h) = c \cdot (K_\sigma | K_\sigma)(X)$ for some integer $i \leq \deg_w(h)$, where $c \in \mathbb{F}^\times$, $\sigma_1 \geq r$ and $|\sigma| \leq d$.

Proof. Consider the finite sum from Lemma 40:

$$\text{coeff}_{v^{d_{\min}}}(g) = \sum_{k \in I} c_k \Lambda^{\bar{e}_k} \Xi^{\bar{f}_k} Y^{\bar{s}_k} Z^{\bar{t}_k} \cdot (K_{\sigma_k} | K_{\sigma_k})(X).$$

The coordinates of \bar{e}_k , \bar{f}_k , \bar{s}_k , and \bar{t}_k are in $\{0, 1, \dots, d\}$ for each $k \in I$ by Corollary 37 (2) and Lemma 39. Choose a sufficiently large $L = \Theta(d(n^2 + m^2))$, and pick integers z_t independently and uniformly at random from $\{0, 1, \dots, L\}$, where $t \in \Lambda \sqcup \Xi \sqcup Y \sqcup Z$. Then by Corollary 24, with high probability, there exists an integer d' such that the coefficient of the monomial $v^{d_{\min}} w^{d'}$ in $\phi(g) \in \mathbb{F}[X, v, w] = \mathbb{F}[X][v, w]$, has the form $c \cdot (K_\sigma | K_\sigma)(X) \in \mathbb{F}[X]$, where $c \in \mathbb{F}^\times$, $\sigma_1 \geq r$, and $|\sigma| \leq d$. Fix the integers z_t such that this occurs.

By Lemma 39, the degree of $\phi(g)$ in v is at most $O(d(n + m))$. To see this, note that if a tableau of shape σ has $|\sigma| \leq d$ and all entries are at most n , then the sum of its entries is at most dn ; similarly, with entries at most m the sum is at most dm . The degree of $\phi(g)$ in w is bounded by $O(dL) = O(d^2(n^2 + m^2))$. Choose $z_v = \deg_w(\phi(g)) + 1 = O(d^2(n^2 + m^2))$. Then the map $\psi: v \mapsto w^{z_v}$ sends the monomials of $\phi(g)$ bijectively to that of $(\psi \circ \phi)(g) = h$, preserving coefficients. Thus, there exists an integer i such that $\text{coeff}_{w^i}(h) = c \cdot (K_\sigma | K_\sigma)$. Finally, we have that

$$\begin{aligned} \deg_w(h) &\leq z_v \cdot O(d(n + m)) + d' \\ &\leq O(d^2(n^2 + m^2)) \cdot O(d(n + m)) + O(d^3(n^3 + m^3)). \quad \blacktriangleleft \end{aligned}$$

We are now ready to prove the main theorem in this subsection.

► **Theorem 42.** *Let $f(X) \in I_{n,m,r}^{\det}$ be a nonzero polynomial of degree d . Assume $|\mathbb{F}| \geq c_0 d^3(n^3 + m^3)$, where $c_0 > 0$ is a large enough constant. Then, there exists a depth-three f -oracle circuit of size $O(n^2 m^2 d^3(n^3 + m^3)) = \text{poly}(n, m, d)$ computing $(K_\sigma | K_\sigma)(X)$, where $\sigma_1 \geq r$ and $|\sigma| \leq d$. Furthermore, the top gate of this circuit is an addition gate, and the bottom layer consists of $O(nmd^3(n^3 + m^3))$ addition gates. The total number of gates and wires, excluding those between the bottom addition gates and the input gates, is $O(nmd^3(n^3 + m^3))$.⁴*

⁴ In the final circuit construction, these wires will be removed and replaced by wires connecting to fewer input gates (see Theorem 45). Hence we state the circuit size bound excluding these wires, which leads to a sharper bound for the final circuit.

Proof. Let h be as in Lemma 41. Let $\alpha \in \mathbb{F}$ be arbitrary. By construction, $h(X, \alpha)$ equals $f(M_\alpha X N_\alpha)$, where M_α (resp. N_α) is obtained from $M J_n \tilde{D}$ (resp. $\tilde{D}' J_m N$) by substituting powers of α for the variables Λ, Ξ, Y, Z , and v . Specifically, if under $\psi \circ \phi$ a variable is mapped to w^s for some integer $s \geq 0$, then we substitute α^s for that variable here. As the map $X \mapsto M_\alpha X N_\alpha$ is a linear map, we can construct a depth-two f -oracle circuit C_α computing $h(X, \alpha) = f(M_\alpha X N_\alpha)$ as follows: Use nm addition gates and $O(n^2 m^2)$ wires at the bottom layer computing the nm entries of $M_\alpha X N_\alpha$. The top gate is an f -gate connecting to the nm addition gates via nm wires. Thus, the size of C_α is $O(n^2 m^2)$.

Let $d_w = \deg_w(h)$. By Lemma 41, we have that $d_w = O(d^3(n^3 + m^3))$ and that $\text{coeff}_{w^i}(h) = c \cdot (K_\sigma | K_\sigma)(X)$ for some integer $i \leq d_w$, where $c \in \mathbb{F}^\times$, $\sigma_1 \geq r$ and $|\sigma| \leq d$. As $|\mathbb{F}| \geq c_0 d^3(n^3 + m^3)$, where $c_0 > 0$ is a large enough constant, we may assume $|\mathbb{F}| \geq d_w + 1$. By Lemma 26, we have a depth-three f -oracle circuit C of size $O(d_w(n^2 m^2)) = O(n^2 m^2 d^3(n^3 + m^3))$ computing $\text{coeff}_{w^i}(h) = c \cdot (K_\sigma | K_\sigma)$. The top gate of C is an addition gate, which connects to $d_w + 1 = O(d^3(n^3 + m^3))$ f -gates on the middle layer. These f -gates connect to $(d_w + 1)nm = O(nmd^3(n^3 + m^3))$ addition gates on the bottom layer.

The above circuit C computes $c \cdot (K_\sigma | K_\sigma)(X)$. By dividing the multipliers on the wires connecting the top addition gate by c , we can transform C into an f -oracle circuit with the same underlying graph that computes $(K_\sigma | K_\sigma)(X)$. This proves the theorem. \blacktriangleleft

3.2 Expressing Algebraic Branching Programs as Determinants

The remainder of the proof follows [2], which we include here for completeness. One key idea is exploiting the close connection between two models: algebraic branching programs and determinants. In particular, we will need the following lemmas:

► **Lemma 43** ([2, Lemma 3.6], [45, Theorem 1]). *Let $g(\bar{y}) \in \mathbb{F}[\bar{y}]$ and suppose g can be computed by an algebraic branching program on r vertices. Then there is an $r \times r$ matrix A over $\mathbb{F}[\bar{y}]$ whose entries are polynomials in \bar{y} of degree at most 1 such that $\det_r(A) = 1 + g(\bar{y})$, and for all $1 \leq k < r$, $\det_k(A_{[k],[k]}) = 1$.*

► **Lemma 44** ([2, Lemma 3.7]). *Let $g(\bar{y}) \in \mathbb{F}[\bar{y}]$ and suppose g can be computed by an algebraic branching program on m vertices. Let z be a new indeterminate. Then there is a homogeneous polynomial $\hat{g}(\bar{y}, z)$ such that $g = \hat{g}(\bar{y}, 1)$ and \hat{g} can be computed by an algebraic branching program on m vertices.*

3.3 Computing the Determinant of a Matrix

We will use Theorem 42 to construct a constant-depth algebraic circuit of size $\text{poly}(n, \deg(f))$ with f -oracle gates that computes the determinant, thereby resolving Question 5. We start by proving the following more general theorem.

► **Theorem 45.** *Let $f(X) \in I_{n,m,r}^{\det}$ be a nonzero polynomial of degree d . Let $g(y_1, \dots, y_\ell) \in \mathbb{F}[\bar{y}]$ be a polynomial computable by an algebraic branching program with at most r vertices. Assume $|\mathbb{F}| \geq c_0 d^3(n^3 + m^3)$, where $c_0 > 0$ is a large enough constant. Then there is a depth-three f -oracle circuit Φ of size $O(nmd^4 \ell r(n^3 + m^3))$ defined over \mathbb{F} such that*

- if $\text{char}(\mathbb{F}) = 0$ then Φ computes $g(\bar{y})$, and
- if $\text{char}(\mathbb{F}) = p > 0$ then Φ computes $g(\bar{y})^{p^k}$ for some $k \leq \lfloor \log_p(d) \rfloor$.

Furthermore, the top layer of this circuit consists of an addition gate.

Proof. By Lemma 44, there is a homogeneous polynomial $\hat{g}(\bar{y}, z) \in \mathbb{F}[\bar{y}, z]$ such that $\hat{g}(\bar{y}, 1) = g(\bar{y})$ and $\hat{g}(\bar{y}, z)$ can be computed by an algebraic branching program over \mathbb{F} with at most r vertices. We may add isolated vertices such that the algebraic branching program has

exactly r vertices. Then by Lemma 43, there is a matrix $A(\bar{y}, z) \in \mathbb{F}[\bar{y}, z]^{r \times r}$ such that $\det_r(A(\bar{y}, z)) = 1 + \widehat{g}(\bar{y}, z)$, $\det_i(A(\bar{y}, z)_{[i],[i]}) = 1$ for all $1 \leq i \leq r - 1$, and all entries of $A(\bar{y}, z)$ have degree at most 1 in \bar{y} and z . Extend $A(\bar{y}, z)$ to an $n \times m$ matrix by adding 1's to the main diagonal and 0's elsewhere.

By Theorem 42, there exists a depth-three f -oracle circuit C over \mathbb{F} of size $O(n^2 m^2 d^3 (n^3 + m^3))$ computing $(K_\sigma | K_\sigma)(X)$ such that $\sigma_1 \geq r$ and $|\sigma| \leq d$. The top gate of C is an addition gate, the bottom layer of C consists of $O(n m d^3 (n^3 + m^3))$ addition gates, and the total number of gates and wires excluding the wires between the bottom addition gates and the input gates is $O(n m d^3 (n^3 + m^3))$. Replacing the $n m$ input gates of C by the $O(\ell)$ new input gates \bar{y} , z , and 1, and further connecting these gates to the $O(n m d^3 (n^3 + m^3))$ bottom addition gates, we obtain a depth-three f -oracle circuit over \mathbb{F} of size $O(n m d^3 \ell (n^3 + m^3))$ computing $h(\bar{y}, z) := (K_\sigma | K_\sigma)(A(\bar{y}, z)) = (1 + \widehat{g}(\bar{y}, z))^t$ where $d \geq \widehat{\sigma}_1 \geq t := |\{i \mid \sigma_i \geq r\}| \geq 1$.

First, suppose that $\text{char}(\mathbb{F}) = 0$. Let δ be a new indeterminate. Then under the map $y_i \mapsto \delta \cdot y_i$ and $z \mapsto \delta$, we have that

$$\begin{aligned} h(\delta \cdot \bar{y}, \delta) &= (1 + \widehat{g}(\delta \cdot \bar{y}, \delta))^t \\ &= (1 + \delta^{\deg(\widehat{g})} \widehat{g}(\bar{y}, 1))^t \\ &= (1 + \delta^{\deg(\widehat{g})} g(\bar{y}))^t = \sum_{i=0}^t \binom{t}{i} \delta^{i \cdot \deg(\widehat{g})} g(\bar{y})^i = 1 + \delta^{\deg(\widehat{g})} g(\bar{y}) + \dots \end{aligned} \quad (8)$$

Then $\deg_\delta(h(\delta \cdot \bar{y}, \delta)) \leq t \cdot \deg(\widehat{g}) \leq d r$. For each $\alpha \in \mathbb{F}$, we can construct from the depth-three f -oracle circuit computing $h(\bar{y}, z)$ another f -oracle circuit C_α computing $h(\alpha \bar{y}, \alpha)$, whose size is $O(n m d^3 \ell (n^3 + m^3))$ and top gate is an addition gate. Also, as $|\mathbb{F}| \geq c_0 d^3 (n^3 + m^3)$, where $c_0 > 0$ is a large enough constant, we may assume $|\mathbb{F}| \geq d r + 1$. Therefore, by Lemma 26, we can compute $\text{coeff}_{\delta^{\deg(\widehat{g})}} \widehat{h}(\delta \cdot \bar{y}, \delta) = g(\bar{y})$ using a depth-three f -oracle circuit of size

$$O(\deg_\delta(h(\delta \cdot \bar{y}, \delta)) \cdot n m d^3 \ell (n^3 + m^3)) = O(n m d^4 \ell r (n^3 + m^3)).$$

Now suppose that $\text{char}(\mathbb{F}) = p > 0$. The above computation only needs to be modified in the case that $p \mid t$. Let $k \in \mathbb{N}$ be the largest natural number such that $t = p^k b$ for some natural number b . Since $p^k \leq t \leq d$, we have that $k \leq \lfloor \log_p(d) \rfloor$ as claimed. Then by a similar computation to Equation (8), we get that

$$h(\delta \cdot \bar{y}, \delta) = \sum_{i=0}^t \binom{t}{i} \delta^{i \cdot \deg(\widehat{g})} g(\bar{y})^i = 1 + b \cdot \delta^{\deg(\widehat{g}) p^k} g(\bar{y})^{p^k} + \dots \quad (9)$$

Again, $\deg_\delta(h(\delta \cdot \bar{y}, \delta)) \leq t \cdot \deg(\widehat{g}) \leq d r$. For each $\alpha \in \mathbb{F}$, we can construct from the depth-three f -oracle circuit computing $h(\bar{y}, z)$ another f -oracle circuit C_α computing $h(\alpha \bar{y}, \alpha)$, whose size is $O(n m d^3 \ell (n^3 + m^3))$ and top gate is an addition gate. Also, as $|\mathbb{F}| \geq c_0 d^3 (n^3 + m^3)$, where $c_0 > 0$ is a large enough constant, we may assume $|\mathbb{F}| \geq d r + 1$. Therefore, by Lemma 26, we have a depth-three f -oracle circuit of size $O(n m d^4 \ell r (n^3 + m^3))$ computing $\text{coeff}_{\delta^{\deg(\widehat{g}) p^k}} \widehat{h}(\delta \cdot \bar{y}, \delta) = b \cdot g(\bar{y})^{p^k}$. By dividing the multipliers on the wires connecting to the top gate by b , this circuit computing $b \cdot g(\bar{y})^{p^k}$ can be turned into a depth-three f -oracle circuit with the same underlying graph that computes $g(\bar{y})^{p^k}$. \blacktriangleleft

The following corollary are a debordering of the results [2, Corollary 3.9, Corollary 3.10] of Andrews and Forbes. In particular, we use Theorem 45 to construct a small constant-depth f -oracle circuit for the determinant, which partially resolves Conjecture 2 posed by Grochow.

► **Corollary 46.** *Let $f(X) \in I_{n,m,r}^{\det}$ be a nonzero polynomial of degree d . Let $t = O(r^{1/3})$ and let Y be a $t \times t$ matrix of indeterminates. Assume $|\mathbb{F}| \geq c_0 d^3 (n^3 + m^3)$, where $c_0 > 0$ is a large enough constant. Then there is a depth-three f -oracle circuit Φ of size $O(nmd^4 r t^2 (n^3 + m^3)) \leq O(nmd^4 r^{5/3} (n^3 + m^3))$ over \mathbb{F} such that*

- if $\text{char}(\mathbb{F}) = 0$ then Φ computes $\det_t(Y)$, and
- if $\text{char}(\mathbb{F}) = p > 0$ then Φ computes $\det_t(Y)^{p^k}$ for some $k \leq \lfloor \log_p(d) \rfloor$.

Furthermore, the top gate of this circuit is an addition gate.

Proof. Mahajan and Vinay [34, Theorem 2] construct an algebraic branching program on $O(t^3) \leq r$ vertices which computes $\det_t(Y)$. Then, the total number of variables in Y is $t^2 = O(r^{2/3})$. The result then follows by applying Theorem 45. ◀

4 Conclusions and Open Questions

In this work, we showed that for any nonzero $f \in I_{n,m,r}^{\det}$ of polynomial degree, the $t \times t$ determinant with $t = \Theta(r^{1/3})$ can be exactly computed by a depth-three, polynomial-size f -oracle circuit. We also established an analogous result for Pfaffian ideals. These results extend and deborder the work of Andrews and Forbes [2]. Our results can be viewed as providing non-principal-ideal analogs of the classical closure results for principal ideals, as factoring results for $g \mid f$ can be viewed as closure results for the principal ideal generated by g . However, our results currently only hold for certain non-principal examples.

We conclude with several open questions and directions:

1. In our main theorem Theorem 6, the circuit size depends polynomially on the degree $\deg(f)$ of f . Grochow conjectured that this dependence on $\deg(f)$ can be completely removed (see Conjecture 2). It would be interesting to see whether the dependence can at least be improved to subpolynomial. Conversely, if one doubts the conjecture, it would be valuable to identify candidate families of polynomials in determinantal ideals that might serve as counterexamples.
2. Our results, like those of [2], are proved only over fields of characteristic zero or sufficiently large positive characteristic. The difficulty in small characteristic is that in Theorem 45, the f -oracle circuit Φ does not compute $g(\bar{y})$ directly, but only a power of $g(\bar{y})$. Obtaining a polynomial-sized circuit that computes the p -th root of a given circuit over a field of characteristic p is currently feasible only when the number of variables is small [1]. This obstacle is closely related to the fact that the celebrated superpolynomial lower bound for constant-depth algebraic circuits in [33] is not known to imply subexponential-time deterministic PIT algorithms in small positive characteristic, even though the lower bound itself and some of its proof-complexity applications do extend to that setting [22, 4]. Determining whether our results, and those of [2], can be extended to small positive characteristic therefore remains an important open problem.
3. It is natural to ask whether similar results on the complexity of ideals can be obtained in other settings. For instance, we expect analogous results for symmetric determinantal ideals (where the matrix variables satisfy $x_{i,j} = x_{j,i}$). As mentioned in the introduction, determinantal and Pfaffian ideals can all be studied within a unified framework known as Standard Monomial Theory [31, 40]. The key observation is that the corresponding determinantal varieties can be realized as affine open subsets of certain Schubert varieties. As noted in [36], this approach also applies to other affine varieties such as ladder determinantal ideals, varieties of complexes, and quiver varieties, potentially yielding further cases in which one can establish complexity results for ideals.

References

- 1 Robert Andrews. Algebraic hardness versus randomness in low characteristic. In *35th Computational Complexity Conference (CCC 2020)*, Leibniz International Proceedings in Informatics (LIPIcs), pages 37:1–37:32. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2020. doi:10.4230/LIPIcs.CCC.2020.37.
- 2 Robert Andrews and Michael A. Forbes. Ideals, determinants, and straightening: proving and using lower bounds for polynomial ideals. In *Proceedings of the 54th Annual ACM Symposium on Theory of Computing*, pages 389–402, 2022. doi:10.1145/3519935.3520025.
- 3 Vikraman Arvind, Partha Mukhopadhyay, and Srikanth Srinivasan. New results on noncommutative and commutative polynomial identity testing. *computational complexity*, 19(4):521–558, 2010. doi:10.1007/s00037-010-0299-8.
- 4 Amik Raj Behera, Nutan Limaye, Varun Ramanathan, and Srikanth Srinivasan. New bounds for the ideal proof system in positive characteristic, 2025. doi:10.48550/arXiv.2506.16397.
- 5 Shai Ben-David, Benny Chor, Oded Goldreich, and Michael Luby. On the theory of average case complexity. *Journal of Computer and System Sciences*, 44(2):193–219, 1992. doi:10.1016/0022-0000(92)90019-F.
- 6 C. S. Bhargav, Prateek Dwivedi, and Nitin Saxena. Learning the coefficients: A presentable version of border complexity and applications to circuit factoring. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, pages 130–140, 2024. doi:10.1145/3618260.3649743.
- 7 Vishwas Bhargava, Shubhangi Saraf, and Ilya Volkovich. Deterministic factorization of sparse polynomials with bounded individual degree. *Journal of the ACM*, 67(2):8:1–8:28, 2020. doi:10.1145/3365667.
- 8 Somnath Bhattacharjee, Mrinal Kumar, Shanthanu S. Rai, Varun Ramanathan, Ramprasad Satharishi, and Shubhangi Saraf. Closure under factorization from a result of Furstenberg, 2025. doi:10.48550/arXiv.2506.23214.
- 9 Winfried Bruns and Aldo Conca. Gröbner bases and determinantal ideals. In *Commutative Algebra, Singularities and Computer Algebra*, pages 9–66. Springer Netherlands, 2003. doi:10.1007/978-94-007-1092-4_2.
- 10 Winfried Bruns and Udo Vetter. *Determinantal Rings*. Springer, 1988. doi:10.1007/BFb0080378.
- 11 Peter Bürgisser. *Completeness and Reduction in Algebraic Complexity Theory*. Springer, 2000. doi:10.1007/978-3-662-04179-6.
- 12 Peter Bürgisser. The complexity of factors of multivariate polynomials. *Foundations of Computational Mathematics*, 4(4):369–396, 2004. doi:10.1007/s10208-002-0059-5.
- 13 Chi-Ning Chou, Mrinal Kumar, and Noam Solomon. Closure results for polynomial factorization. *Theory of Computing*, 15(1):1–34, 2019. doi:10.4086/toc.2019.v015a013.
- 14 Corrado de Concini, David Eisenbud, and Claudio Procesi. Young diagrams and determinantal varieties. *Inventiones mathematicae*, 56(2):129–165, 1980. doi:10.1007/BF01392548.
- 15 Corrado de Concini, David Eisenbud, and Claudio Procesi. *Hodge Algebras*. Number 91 in Astérisque. Société mathématique de France, 1982. URL: https://www.numdam.org/item/AST_1982__91__1_0/.
- 16 Anakin Dey and Zeyu Guo. Debordering closure results in determinantal and Pfaffian ideals, 2025. arXiv:2511.16492.
- 17 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. doi:10.1002/sapm1974533185.
- 18 Pranjal Dutta, Prateek Dwivedi, and Nitin Saxena. Demystifying the border of depth-3 algebraic circuits. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 92–103. IEEE, 2022. doi:10.1109/FOCS52979.2021.00018.

- 19 Pranjali Dutta, Fulvio Gesmundo, Christian Ikenmeyer, Gorav Jindal, and Vladimir Lysikov. Fixed-parameter debordering of Waring rank. In *41st International Symposium on Theoretical Aspects of Computer Science (STACS 2024)*, Leibniz International Proceedings in Informatics (LIPIcs), pages 30:1–30:15. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2024. doi:10.4230/LIPIcs.STACS.2024.30.
- 20 Pranjali Dutta, Nitin Saxena, and Amit Sinhababu. Discovering the roots: Uniform closure results for algebraic classes under factoring. *Journal of the ACM*, 69(3):1–39, 2022. doi:10.1145/3510359.
- 21 Stephen Fenner, Rohit Gurjar, and Thomas Thierauf. Bipartite perfect matching is in quasi-NC. *SIAM Journal on Computing*, 50(3):STOC16–218–STOC16–235, 2019. doi:10.1137/16M1097870.
- 22 Michael A. Forbes. Low-depth algebraic circuit lower bounds over any field. In *39th Computational Complexity Conference (CCC 2024)*, Leibniz International Proceedings in Informatics (LIPIcs), pages 31–1. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2024. doi:10.4230/LIPIcs.CCC.2024.31.
- 23 Sumanta Ghosh, Rohit Gurjar, and Roshan Raj. A deterministic parallel reduction from weighted matroid intersection search to decision. *Algorithmica*, 86(4):1057–1079, 2024. doi:10.1137/1.9781611977073.44.
- 24 Joshua A. Grochow. Complexity in ideals of polynomials: questions on algebraic complexity of circuits and proofs. *Bulletin of the European Association for Theoretical Computer Science*, 131, 2020. URL: <http://smtp.eatcs.org/index.php/beatcs/article/view/620>.
- 25 Rohit Gurjar and Thomas Thierauf. Linear matroid intersection is in quasi-NC. *computational complexity*, 29(2):9, 2020. doi:10.1007/s00037-020-00200-z.
- 26 Ivan Hu, Dieter van Melkebeek, and Andrew Morgan. Polynomial identity testing via evaluation of rational functions. *Theory of Computing*, 20(1), 2024. doi:10.4086/toc.2024.v020a001.
- 27 Erich Kaltofen. Uniform closure properties of P-computable functions. In *Proceedings of the 18th Annual ACM Symposium on Theory of Computing*, pages 330–337, 1986. doi:10.1145/12130.12163.
- 28 Erich Kaltofen. Single-factor Hensel lifting and its application to the straight-line complexity of certain polynomials. In *Proceedings of the 19th Annual ACM Symposium on Theory of Computing*, pages 443–452, 1987. doi:10.1145/28395.28443.
- 29 Erich Kaltofen. Factorization of polynomials given by straight-line programs. In *Randomness and Computation, Volume 5 of Advances in Computing Research*, pages 375–412, 1989.
- 30 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. doi:10.1145/380752.380801.
- 31 Venkatramani Lakshmibai and Komaranapuram N. Raghavan. *Standard Monomial Theory: Invariant Theoretic Approach*. Springer, 2008. doi:10.1007/978-3-540-76757-2.
- 32 Thomas Lehmkuhl and Thomas Lickteig. On the order of approximation in approximative triadic decompositions of tensors. *Theoretical computer science*, 66(1):1–14, 1989. doi:10.1016/0304-3975(89)90141-2.
- 33 Nutan Limaye, Srikanth Srinivasan, and Sébastien Tavenas. Superpolynomial lower bounds against low-depth algebraic circuits. *Journal of the ACM*, 72(4):1–35, 2025. doi:10.1145/3734215.
- 34 Meena Mahajan and V. Vinay. Determinant: Combinatorics, algorithms, and complexity. Technical Report 5, Institute of Mathematical Sciences India, 1997.
- 35 Ketan Mulmuley, Umesh V. Vazirani, and Vijay V. Vazirani. Matching is as easy as matrix inversion. *Combinatorica*, 7(1):105–113, 1987. doi:10.1007/BF02579206.
- 36 Chitikila Musili. The development of standard monomial theory-I. In *A Tribute to C. S. Seshadri: Perspectives in Geometry and Representation Theory*, pages 385–420. Springer, 2003. doi:10.1007/978-93-86279-11-8_24.

- 37 Noam Nisan and Avi Wigderson. Hardness vs randomness. *Journal of computer and System Sciences*, 49(2):149–167, 1994. doi:10.1016/S0022-0000(05)80043-1.
- 38 Rafael Oliveira. Factors of low individual degree polynomials. *computational complexity*, 25(2):507–561, 2016. doi:10.1007/s00037-016-0130-2.
- 39 Ramprasad Saptharishi. A survey of lower bounds in arithmetic circuit complexity, July 2021. Version 9.0.3. URL: <https://github.com/dasarpmar/lowerbounds-survey/releases>.
- 40 C. S. Seshadri. *Introduction to the Theory of Standard Monomials*. Springer, second edition edition, 2016. doi:10.1007/978-981-10-1813-8.
- 41 Amir Shpilka. Improved debordering of Waring rank, 2025. doi:10.48550/arXiv.2502.03150.
- 42 Amit Sinhababu and Thomas Thierauf. Factorization of polynomials given by arithmetic branching programs. *computational complexity*, 30(2):15, 2021. doi:10.1007/s00037-021-00215-0.
- 43 Volker Strassen. Vermeidung von divisionen. *Journal für die reine und angewandte Mathematik*, 264:184–202, 1973. URL: <http://eudml.org/doc/151394>.
- 44 Ola Svensson and Jakub Tarnawski. The matching problem in general graphs is in quasi-NC. In *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 696–707. IEEE, 2017. doi:10.1109/FOCS.2017.70.
- 45 Leslie G. Valiant. Completeness classes in algebra. In *Proceedings of the 11th Annual ACM Symposium on Theory of Computing*, pages 249–261, 1979. doi:10.1145/800135.804419.
- 46 Leslie G. Valiant and Vijay V. Vazirani. Np is as easy as detecting unique solutions. *Theoretical Computer Science*, 47(1):85–93, 1986. doi:10.1016/0304-3975(86)90135-0.