Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 189 (2025)

DEBORDERING CLOSURE RESULTS IN DETERMINANTAL AND PFAFFIAN IDEALS

ANAKIN DEY AND ZEYU GUO

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 $I^{\det}_{n,m,r}$ 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 $f \in I^{\det}_{n,m,r}$, 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.

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 [Gro20] for a survey that explains 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 $f \in I$ [Gro20]. 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 $S = \{g_1, \ldots, g_k\}$ (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 $g_1, \ldots, g_k$. We call such a property a *closure result*, by analogy with closure under factorization in the principal ideal case. In short, closure results reduce the task

Anakin Dey, Department of Mathematics, The Ohio State University, dey.92@osu.edu
Zeyu Guo, Department of Computer Science and Engineering, The Ohio State University, zguotcs@gmail.com.
Supported by NSF CAREER award CCF-2440926.

ISSN 1433-8092

of showing hardness for all polynomials in I to proving hardness for a small set of distinguished polynomials.

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 $G\colon \mathbb{F}^s \to \mathbb{F}^n$ against a family $\mathcal{C}$ of n-variate polynomials, meaning that G has the property 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 [HvMM24]. 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 of polynomials $\{g_1, \ldots, g_k\}$. This can be viewed as a particular way of implementing the "hardness vs. randomness" paradigm of [NW94] 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 $f \in \mathbb{F}[x_1, \ldots, x_n]$ is a polynomial of degree $\mathrm{poly}(n)$ computed by an algebraic circuit of size $\mathrm{poly}(n)$, then its factors also admit $\mathrm{poly}(n)$-size algebraic circuits [Kal86; Kal87; Kal89]. Closure under factorization has also been studied, and in some cases established (or partially established), in more restricted models; see [Oli16; CKS19; BSV20; ST21; DSS22; Bha+25].

Before moving to non-principal ideals, we recall some technical aspects of closure under factorization. Kaltofen's result [Kal86; Kal87; Kal89] more generally states that if $f \in \mathbb{F}[x_1, \ldots, x_n]$ is computed by an algebraic circuit of size s, then each factor g of f can be computed by an algebraic circuit of size $\mathrm{poly}(n, s, \deg(f))$. This polynomial dependence on $\deg(f)$ is not an obstacle when f has degree $\mathrm{poly}(n)$. However, if $\deg(f)$ is much larger than $\deg(g)$, then the bound $\mathrm{poly}(n, s, \deg(f))$ 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* [Bür00, 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 $\mathrm{poly}(n, s, \deg(g))$ (rather than $\deg(f)$). Although the conjecture remains open, partial results are known [Kal86; Bür00; Bür04; DSS22]. In particular, Bürgisser [Bür04] 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 1.1: We say that $g \in \mathbb{F}[x_1, \ldots, x_n]$ is *approximately computed by* a circuit C over $\mathbb{F}(\varepsilon)$ if C computes some polynomial $h \in \mathbb{F}(\varepsilon)[x_1, \ldots, x_n]$, and $h - g \in \varepsilon \cdot \mathbb{F}[[\varepsilon]][x_1, \ldots, x_n]$, where $\mathbb{F}[[\varepsilon]]$ denotes the ring of formal power series in ε.

In the settings where $\mathbb{F}[\varepsilon][x_1, \ldots, x_n]$ can be equipped with the Euclidean topology in a natural way, such as $\mathbb{F} = \mathbb{C}$ or $\mathbb{R}$, this would imply that $h \to g$ 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 [Gro20], Grochow conjectured such a result for determinantal ideals. Specifically, he conjectured that 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 $X = (x_{i,j})_{1 \le i,j \le n}$, the computation of determinants (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 1.2 ([Gro20, 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-depth* algebraic circuit of size $\mathrm{poly}(n)$ with f-oracle gates that computes the $m \times m$ determinant for some $m = n^{\Theta(1)}$.

Remark: We note that Conjecture 1.2 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 [Bür04] that the Factor Conjecture holds with respect to border complexity, Andrews and Forbes [AF22] proved that Grochow's conjecture holds with respect to border complexity. Formally, they proved the following theorem:

Theorem 1.3 ([AF22, Theorem 1.1]): Let $\mathbb{F}$ be a field of characteristic zero. Let $X = (x_{i,j})_{\substack{1 \le i \le n \\ 1 \le j \le m}}$ be an $n \times m$ matrix of variables over $\mathbb{F}$ and let $I^{\det}_{n,m,r} \subseteq \mathbb{F}[X] = \mathbb{F}[x_{i,j}]$ be the ideal generated by the $r \times r$ minors of X. Let $f \in I^{\det}_{n,m,r}$ be a nonzero polynomial. Then there is a depth-three f-oracle circuit of size $O\left(n^2 m^2\right)$ that approximately computes the $t \times t$ determinant for $t = \Theta\left(r^{1/3}\right)$.

*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 $\mathrm{poly}(m)$.

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 showed that these results continue to 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 1.3 with the celebrated superpolynomial lower bounds for constant-depth algebraic circuits due to Limaye, Srinivasan, and Tavenas [LST25] (which also hold in the border complexity setting, as observed in [AF22]), Andrews and Forbes [AF22] 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 [CKS19] and yielding improved subexponential-time deterministic PIT algorithms for constant-depth algebraic circuits.

Back to exact computation. Note that Theorem 1.3 proves Grochow's conjecture (Conjecture 1.2), 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 $\mathrm{poly}(n)$, independent of $\deg(f)$, even though $\deg(f)$ may be much larger than n. This degree-independent condition is the 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 $\mathrm{poly}(n)$ 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 1.4: Is Conjecture 1.2 true when $\deg(f) = \mathrm{poly}(n)$? More generally, under the notation of Conjecture 1.2, is it true that there is a constant-depth algebraic circuit of size $\mathrm{poly}(n, \deg(f))$ (rather than $\mathrm{poly}(n)$ as in Conjecture 1.2) 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 1.4 affirmatively by establishing the following theorem:

Theorem 1.5 (Informal version of Theorem 3.18 and Corollary 3.19): Let $X = (x_{i,j})_{\substack{1\le i\le n\\ 1\le j\le m}}$ be an $n \times m$ matrix of variables over a field $\mathbb{F}$. Let $I^{\det}_{n,m,r} \subseteq \mathbb{F}[X] = \mathbb{F}[x_{i,j} \mid 1 \le i \le n,\ 1 \le j \le m]$ be the ideal generated by the $r \times r$ minors of X. Let $f \in I^{\det}_{n,m,r}$ 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 $\mathrm{poly}(n, m, \deg(f))$ that computes the $t \times t$ determinant for $t = \Theta\left(r^{1/3}\right)$.

Theorem 1.6 (Informal version of Theorem 4.10 and Corollary 4.11): Let $X = (x_{i,j})_{1\le i<j\le 2n}$ be a $2n \times 2n$ skew-symmetric matrix of variables over a field $\mathbb{F}$ so that $x_{j,i} = -x_{i,j}$ for $1 \le j < i \le n$ and $x_{i,i} = 0$ for $1 \le i \le 2n$. Let $I^{\mathrm{pfaff}}_{2n,2r} \subseteq \mathbb{F}[X] = \mathbb{F}[x_{i,j} \mid 1 \le i < j \le 2n]$ be the ideal generated by the $2r \times 2r$ principal minors of X. Let $f \in I^{\mathrm{pfaff}}_{2n,2r}$ 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 $\mathrm{poly}(n, \deg(f))$ that computes the $t \times t$ Pfaffian of a skew-symmetric matrix for $t = \Theta\left(r^{1/3}\right)$.

It is worth noting that determinantal and Pfaffian ideals can be studied within unified frameworks, notably Hodge algebras [dCEP82] and Standard Monomial Theory [LR08; Ses16]. In this paper, however, we do not adopt these approaches as they are more abstract than necessary for our purposes.

While Theorem 1.5 does not by itself yield new PIT algorithms, because Theorem 1.3 already suffices given that the lower bounds of [LST25] hold in the border complexity setting, it resolves a natural theoretical question that was previously open.

Theorem 1.5 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 the exponentially large degree in ε of the scalars used in the approximation [LL89; Bür00]. Nevertheless, by exploiting the structure of determinantal and Pfaffian ideals, we show that this difficulty can be overcome, yielding debordering results. See [DDS22; BDS24; Dut+24; Shp25] for other nontrivial debordering results in various settings.

1.2 Proof Overview

The main tool in our proof is the *isolation lemma*, first introduced by Valiant and Vazirani [VV86]. This lemma, along with its derandomized variants, has found numerous applications in theoretical computer science, including parallel algorithms for perfect matching [MVV87;

[†]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.

FGT19; ST17], polynomial identity testing [KS01; AMS10; GT20], and search-to-decision reductions [VV86; Ben+92; GGR24], among others. To the best of our knowledge, however, this paper is the first to apply the isolation lemma to obtain debordering results.

The version of the isolation lemma we use [KS01] can be stated as follows. Consider a collection $\mathcal{C}$ of monomials of individual degree at most K in variables $x_1, \dots, x_\ell$. Suppose we substitute each variable by $x_i \mapsto w^{z_i}$, where the exponents $z_1, \dots, z_\ell$ 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 $\mathfrak{m} \in \mathcal{C}$ 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 1.5, let us first review the proof of Theorem 1.3 from [AF22]. Let $f \in I^{\det}_{n,m,r}$ be a nonzero polynomial. Our goal is to compute the $t \times t$ determinant using an f-oracle circuit. The proof in [AF22] relies on a technique from algebraic combinatorics, specifically *standard monomial theory*, 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 [AF22]; therefore, we focus on the first step.

At a high level, the way [AF22] 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, [AF22] 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

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

over $\mathbb{F}(\varepsilon)$, where g_0 is a distinguished standard bideterminant. This standard bideterminant can then be used to compute the $s \times s$ determinant that we aim to compute. The presence of the $O\left(\varepsilon^{k+1}\right)$ term poses no issue for proving Theorem 1.3, 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 [AF22] 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 [AF22] 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 $\{1, 2, \ldots, n-1, n\}$ 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 $\overline{x} = \{x_1, \ldots, x_n\}$, we write $\mathbb{F}[\overline{x}]$ for the ring of polynomials in the variables $x_1, \ldots, x_n$ with coefficients in $\mathbb{F}$. We note that in addition to $\mathbb{F}[\overline{x}]$ being a ring, it is also an $\mathbb{F}$-vector space and that ideals of $\mathbb{F}[\overline{x}]$ 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 $\mathbb{F}[\overline{x}]$ 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 $X = (x_{i,j})_{\substack{1 \le i \le n \\ 1 \le j \le m}}$, then we notate the respective

polynomial ring as $\mathbb{F}[X]$. In any case, when $f \in \mathbb{F}[\overline{x}]$, 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 [Sap21]. 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.

In addition to standard algebraic circuits, we will use algebraic oracle circuits and algebraic branching programs, defined below.

Definition 2.1 (Oracle circuit): Let $g(\overline{x}) \in \mathbb{F}[\overline{x}]$, where $\overline{x}$ denotes $x_1, \ldots, x_n$. 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 $f_1, \ldots, f_n$ outputs the polynomial $g(f_1, \ldots, f_n)$.

In our definition of algebraic branching programs, edges are assumed to be labeled by polynomials of degree at most one.

Definition 2.2 (Algebraic branching program): An *algebraic branching program* (*ABP*) over $\mathbb{F}[\overline{x}]$ is a directed acyclic graph A such that:

- The nodes V of A are partitioned into non-empty subsets $V = V_0 \sqcup \cdots \sqcup V_d$ for some integer $d \geq 0$ and we call V_i the *i-th layer*. Layer V_0 has exactly one node called the *source* s and layer V_d has exactly on node called the *sink* t.
- Each edge in A goes from layer V_{i-1} to V_i for some $i \in [d]$.
- Each edge e in A is labeled with a polynomial $\gamma_e \in \mathbb{F}[\overline{x}]$ of degree at most one.

For a path $\overline{e} = (e_1, \ldots, e_d)$ from s to t, where each edge e_i goes from layer $i-1$ to layer i, define the polynomial $\gamma_{\overline{e}} := \prod_{i=1}^{d} \gamma_{e_i}$. Then A computes the polynomial $\sum_{\text{path } \overline{e} \text{ from } s \text{ to } t} \gamma_{\overline{e}}$.

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 [Val79, Theorem 1].

2.1 Linear Algebra

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

Definition 2.3 (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 $\sigma : [n] \to [n]$. 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 $\sigma(i) > \sigma(j)$):

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

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

2.2 Bitableaux

Definition 2.4 (Partition, Young diagram): A *partition* is a non-increasing sequence of integers $\sigma = (\sigma_1 \ge \sigma_2 \ge \cdots \ge \sigma_k \ge 0)$ for some $k \ge 1$. 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* $\widehat{\sigma} = (\widehat{\sigma}_1 \ge \cdots \ge \widehat{\sigma}_\ell)$ for some $\ell \ge 1$ where $\widehat{\sigma}_i := \left|\{\, j \in \mathbb{N} \mid \sigma_j \ge i \,\}\right|$. A partition σ can be given pictorially as a *Young diagram* which formally is the set of points $\{(i, j) \mid j \le \sigma_i\} \subseteq \mathbb{N} \times \mathbb{N}$. 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 $\widehat{\sigma}$ is the reflection of the Young diagram for σ over the diagonal $y = x$. Note that $\widehat{\sigma}_1$ is the number of non-empty rows of the Young diagram for σ. For example, if $\sigma = (5, 4, 2, 1)$ then $\widehat{\sigma} = (4, 3, 2, 2, 1)$. Their Young diagrams can be seen in Figure 1.

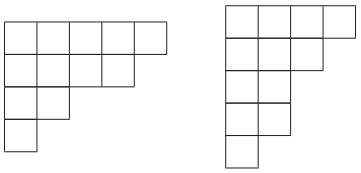

FIGURE 1. The Young diagrams for $\sigma = (5,4,2,1)$ and $\widehat{\sigma} = (4,3,2,2,1)$.

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

Definition 2.5: The ordering $1 < 2 < 3 < \cdots$ induces a lexicographic ordering on partitions, which we denote by $\leq_{\text{lex}}$. This ordering has a minor caveat in that extending a partition makes it smaller with respect to $\leq_{\text{lex}}$. Formally, for partitions $\lambda = (\lambda_1 \geq \cdots \geq \lambda_t)$ and $\mu = (\mu_1 \geq \cdots \geq \mu_s)$ 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 for all $1 \leq i \leq k-1$ we have that $\lambda_i = \mu_i$, 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.

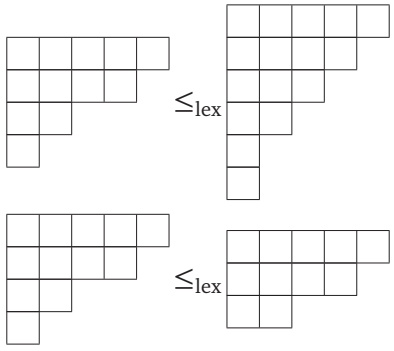

FIGURE 2. Two examples of the order $\leq_{\text{lex}}$ on partitions. First, we have that $(5,4,2,1) \leq_{\text{lex}} (5,4,3,2,1,1)$ as $2 < 3$. Next, we have that $(5,4,2,1) \leq_{\text{lex}} (5,4,2)$ as $(5,4,2)$ is a prefix of $(5,4,2,1)$.

Definition 2.6 (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. For example, if $\sigma = (5,4,2,1)$, then a semistandard tableau T for σ, as well as the conjugate semistandard tableau $\widehat{T}$, are given in Figure 3.

1	1	2	4	5
2	2	4	5	
3	4			
5				

1	2	3	5
1	2	4	
2	4		
4	5		
5			

FIGURE 3. A Young tableau T for $\sigma = (5,4,2,1)$ as well as its conjugate $\widehat{T}$. Note that T is semistandard and $\widehat{T}$ is conjugate semistandard.

We remark that much of the literature on straightening laws refers to what we call a conjugate semistandard Young tableau as just standard or semistandard. We stick to our convention as it is the one that is prevalent in more modern papers and texts.

Definition 2.7: Let $\sigma = (\sigma_1 \geq \cdots \geq \sigma_k \geq 0)$ 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:

$$|T| := \sum_{i=1}^{k} \sum_{j=1}^{\sigma_i} T(i,j).$$

In particular, much of our analysis will center around a special set of tableau which for a given shape σ are the maximal and minimal conjugate semistandard Young tableau of shape σ with respect to the size.

Definition 2.8 (Canonical/anti-canonical tableau): Fix a natural number n. Let $\sigma = (\sigma_1 \geq \cdots \geq \sigma_k > 0)$ 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 $1, 2, \ldots, \sigma_i$. Similarly, define $\overline{K}_{\sigma,n}$ to be the tableau of shape σ where row i has entries $(n-\sigma_i+1, n-\sigma_i+2, \ldots, n)$. We call $K_{\sigma,n}$ and $\overline{K}_{\sigma,n}$ the *canonical* and *anti-canonical* tableau respectively.[‡] 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 $\overline{K}_\sigma$. For example, if $\sigma = (5,4,2,1)$ and $n = 7$, then K_σ and $\overline{K}_\sigma$ are given in Figure 4.

[‡]In some sources, such as [BV88], these are referred to as the *initial* and *final* tableau.

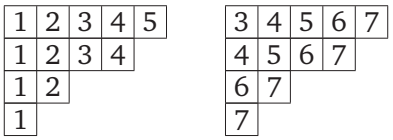

FIGURE 4. The canonical and anti-canonical tableau for $\sigma = (5,4,2,1)$ and $n = 7$.

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

Definition 2.9 (Bitableau, bideterminant): Let $\sigma = (\sigma_1 \ge \cdots \ge \sigma_k)$ 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 $S_i = (S(i,1),\ldots,S(i,\sigma_i))$ and $T_i = (T(i,1),\ldots,T(i,\sigma_i))$ respectively. The $\sigma_i \times \sigma_i$ minor of X defined by S_i and T_i is the matrix

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

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

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

An $n \times n$ determinant is homogeneous of degree n so that $(S \mid T)(X)$ is a homogeneous polynomial of degree $|\sigma|$. For example, if $\sigma = (4,2,1)$ and $(S \mid T)$ is the bitableau

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

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

$$\begin{pmatrix} x_{1,1} & x_{1,3} & x_{1,5} & x_{1,6} \\ x_{2,1} & x_{2,3} & x_{2,5} & x_{2,6} \\ x_{4,1} & x_{4,3} & x_{4,5} & x_{4,6} \\ x_{5,1} & x_{5,3} & x_{5,5} & x_{5,6} \end{pmatrix} \begin{pmatrix} x_{3,2} & x_{3,7} \\ x_{6,2} & x_{6,7} \end{pmatrix} \begin{pmatrix} x_{4,3} \end{pmatrix}.$$

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

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

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 2.11 (Standard bitableau, standard bideterminant): We call a bitableau $(S \mid T)$ and its associated bideterminant $(S \mid T)(X)$ *standard* if S and T are both conjugate semistandard Young tableaux.

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

Theorem 2.12 ([DRS74, §8, Theorem 3], [dCEP80, Corollary 2.3]): Let $(S \mid T)(X)$ be a bideterminant of shape σ. Then $(S \mid T)(X)$ can be uniquely expressed as a linear combination

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

where $(A \mid B)(X)$ 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 2.10 and Theorem 2.12, imply the following corollary.

Corollary 2.13: 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 $I^{\det}_{n,m,r}$ 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 2.14 ([BC03, Corollary 1.7]): Polynomials $f \in I^{\det}_{n,m,r}$ 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 $f \in I^{\det}_{n,m,r}$ 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 2.15: The polynomial ring $\mathbb{F}[X]$ has a natural $(\mathbb{N}^n \oplus \mathbb{N}^m)$-grading. Let $\overline{e}_i \in \mathbb{N}^n$ be the standard basis vector with a 1 in position i and 0's in the other positions. Define $\overline{e}_i \in \mathbb{N}^m$ the same way. Then we assign $x_{i,j}$ to have degree $\overline{e}_i \oplus \overline{e}_j$. We call this assignment the *multidegree*. We say a polynomial $f \in \mathbb{F}[X]$ is *multihomogeneous* of multidegree $(s_1\overline{e}_1 + \cdots + s_n\overline{e_n}) \oplus (t_1\overline{e}_1 + \cdots + t_m\overline{e}_m)$ if every monomial in f has multidegree $(s_1\overline{e}_1 + \cdots + s_n\overline{e_n}) \oplus (t_1\overline{e}_1 + \cdots + t_m\overline{e}_m)$.

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 2.16: Fix a natural number $n \in \mathbb{Z}_{\geq 0}$. Let $\sigma = (\sigma_1 \geq \cdots \geq \sigma_d)$ 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 $(s_1\overline{e}_1 + \cdots + s_n\overline{e_n}) \oplus (t_1\overline{e}_1 + \cdots + t_n\overline{e}_n)$, 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 $(\widehat{\sigma}_1\overline{e}_1 + \cdots + \widehat{\sigma}_n\overline{e}_1) \oplus (\widehat{\sigma}_1\overline{e}_1 + \cdots + \widehat{\sigma}_n\overline{e}_1)$. 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 $(\overline{K}_\tau \mid \overline{K}_\tau)(X)$.

Proof: The multidegree of a standard bideterminant $(S \mid T)(X)$ is immediate from Definition 2.9. To see that for distinct partitions $\sigma \neq \tau$ the multidegrees of $(K_\sigma \mid K_\sigma)(X)$ and $(K_\tau \mid K_\tau)(X)$ are distinct, we make the following observation. The number of 1's in K_σ is the coefficient of $\overline{e}_1$ in the multidegree, the number of 2's in K_σ is the coefficient of $\overline{e}_2$, and so on. This allows us to get the values $\widehat{\sigma}_1, \ldots, \widehat{\sigma}_n$ which in turn completely determines σ. □

2.4 Pfaffian Ideals We now introduce notation for Pfaffian ideals. Readers interested only in the classical determinantal case may skip this part. Let $x_{i,j}$ be indeterminates for $1 \leq i < j \leq 2n$ and let $x_{j,i} := -x_{i,j}$ for $1 \leq j < i \leq 2n$ and $x_{i,i} = 0$ for $1 \leq i \leq 2n$. Thus, $X = (x_{i,j})_{1 \leq i,j \leq 2n}$ is a skew-symmetric $2n \times 2n$ matrix of variables. For notational consistency with the prior subsections, we denote the polynomial ring $\mathbb{F}[x_{i,j} \mid 1 \leq i < j \leq 2n]$ by $\mathbb{F}[X]$.

Recall that for a skew-symmetric matrix X, the determinant when viewed as a polynomial in the entries of the skew-symmetric matrix is a perfect square of some other polynomial. The square root of $\det_{2n}(X)$ is called the *Pfaffian* of X. For the Pfaffian of a $2n \times 2n$ matrix $M \in \mathbb{F}^{2n \times 2n}$, we use the notation $\operatorname{pfaff}_{2n}$. The Pfaffian has a more intrinsic definition given as follows:

$$\operatorname{pfaff}_{2n}(X) = \frac{1}{2^n n!} \sum_{\sigma \in \mathfrak{S}_{2n}} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} x_{\sigma(2i-1),\sigma(2i)}. \tag{1}$$

Just like the determinant, this is a polynomial with coefficients ±1 so that it is well defined over any field. To see this, note that every monomial in Equation (1) appears exactly $2^n n!$ times. We also have that if m is odd, then $\det_m(X) = 0$ when X is a $m \times m$ skew-symmetric matrix so that $\operatorname{pfaff}_m(X) = 0$. Thus, we only consider Pfaffians on matrices of even order.

Pfaffians are deeply connected to determinants, as indicated by the following lemma:

Lemma 2.17 ([AF22, Lemma 2.27]): Let X be a $2n \times 2n$ skew-symmetric matrix and let E be an arbitrary $2n \times 2n$ matrix. Then $EXE^\top$ is also skew-symmetric and $\operatorname{pfaff}_{2n}(EXE^\top) = \det_{2n}(E)\operatorname{pfaff}_{2n}(X)$.

Since the Pfaffian is only well-defined for skew-symmetric matrices, we cannot consider all possible row and column combinations when looking at Pfaffians defined on minors of a matrix.

Definition 2.18 (Principal bitableau, bipfaffian): A bitableau $(S \mid T)$ is *principal* if $S = T$, i.e., if the submatrix of X with rows given by S and columns given by T is principal. In this case, we denote $[T] := (T \mid T)$. Since $m \times m$ determinants of skew-symmetric matrices are zero for odd m, we will assume all partitions have only even row lengths in this case. In particular, $|\sigma|$ will always be divisible by 2.

Let σ be a partition such that the length of each row of σ is even, and let T be a Young tableau of shape σ. Writing the rows as $T_i = (T(i,1), \ldots, T(i,\sigma_i))$, the submatrix of X with rows and columns given by T_i is skew-symmetric as well and thus has a well-defined *principal pfaffian*. The associated *bipfaffian*[§] $[T](X)$ is the product of all such Pfaffians defined by the rows of T:

$$[T](X) := \prod_{i=1}^{\widehat{\sigma}_1} \operatorname{pfaff}\left(x_{T(i,a),T(i,b)}\right)_{1 \le a,b \le \sigma_i}.$$

Note that the total degree $\deg([T](X))$ is equal to $|\sigma|/2$.

The following lemma shows that every monomial in $\mathbb{F}[X]$ can be expressed as a bipfaffian and hence the bipfaffians span $\mathbb{F}[X]$. The proof is immediate from the definition.

Lemma 2.19: A degree d monomial $\prod_{i=1}^{d} x_{r_i,c_i}$ where for each $1 \le i \le d$, $r_i < c_i$ is given by a bipfaffian:

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

Analogous to the classical determinantal case, a specific subset of bipfaffians form an $\mathbb{F}$-basis of $\mathbb{F}[X]$.

[§][AF22] call this a *standard monomial*. We deviate from this as standard monomial is a more general term which also refers to standard bideterminants and other analogues in standard monomial theory.

Definition 2.20 (Standard bipfaffian): A bipfaffian $[S](X)$ is *standard* if S is a conjugate semistandard Young tableau.

As in the determinantal case, the Pfaffian case also admits a straightening law.

Theorem 2.21 ([dCP76, Theorem 6.5], [HT92, §5]): Let S be a Young tableau of shape σ. Then $[S](X)$ can be uniquely expressed as a linear combination

$$[S](X) = \sum_A c_A [A](X),$$

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

Lemma 2.19 and Theorem 2.21 together imply the following corollary.

Corollary 2.22: The standard bipfaffians form an $\mathbb{F}$-basis of $\mathbb{F}[X]$. In particular, since bipfaffians are homogeneous with respect to total degree, the degree-d component of $\mathbb{F}[X]$ has as basis the standard bipfaffians of shape σ such that $|\sigma| = 2d$. Note that if $|\sigma| = 2d$, then the number of rows $\widehat{\sigma}_1$ of σ is at most d as each non-empty row of σ has length at least 2.

Let $I^{\text{pfaff}}_{2n,2r}$ be the ideal of $\mathbb{F}[X]$ generated by the $2r \times 2r$ principal bipfaffians of X. We have the following crucial statement.

Proposition 2.23 ([HT92, §5]): Polynomials $f \in I^{\text{pfaff}}_{2n,2r}$ are supported by standard bipfaffians of shape σ such that $\sigma_1 \geq 2r$.

Next, we describe a grading of the polynomial ring $\mathbb{F}[X]$ that is useful for the proof.

Definition 2.24: The polynomial ring $\mathbb{F}[X]$ has a natural $\mathbb{N}^{2n}$-grading. Let $\overline{e}_i \in \mathbb{N}^{2n}$ be the standard basis vector with a 1 in position i and 0's in the other positions. Then we assign $x_{i,j}$ to have degree $\overline{e}_i + \overline{e}_j$. We call this assignment the *multidegree*. We say a polynomial $f \in \mathbb{F}[X]$ is *multihomogeneous* of multidegree $s_1\overline{e}_1 + \cdots + s_{2n}\overline{e_{2n}}$ if every monomial in f has multidegree $s_1\overline{e}_1 + \cdots + s_{2n}\overline{e_{2n}}$.

The following lemma gives the multidegree of bipfaffians. It follows immediately from the definition and is proven similarly to Lemma 2.16 and thus we omit the proof.

Lemma 2.25: Fix a natural number $n \in \mathbb{Z}_{\geq 0}$. Let $\sigma = (\sigma_1 \geq \cdots \geq \sigma_k)$ be a partition such that the length of each row is at most $2n$. Let S be a conjugate semistandard Young tableau. Then a bipfaffian $[S](X)$ is multihomogeneous of multidegree $s_1\overline{e}_1 + \cdots + s_{2n}\overline{e}_{2n}$, where s_i is equal to the number of i's that appear in S. In particular, $[K_\sigma](X)$ is multihomogeneous of multidegree $\widehat{\sigma}_1\overline{e}_1 + \cdots + \widehat{\sigma}_{2n}\overline{e}_{2n}$. Moreover, for distinct partitions $\sigma \neq \tau$, the multidegrees of $[K_\sigma](X)$ and $[K_\tau](X)$ are distinct, and the same holds for the multidegrees of $[\overline{K}_\sigma](X)$ and $[\overline{K}_\tau](X)$.

2.5 Isolation Lemma One crucial tool used in this work is the *isolation lemma*. We use the following version due to Klivans and Spielman [KS01].

Lemma 2.26 ([KS01, Lemma 4]): Let C be any collection of distinct linear forms in variables $z_1, \ldots, z_\ell$ with coefficients in the range $\{0, \ldots, K\}$ for some integer $K \in \mathbb{Z}_{\geq 0}$. Let $\varepsilon > 0$. Let $z_1, \ldots, z_\ell$ be independently and uniformly chosen from $\{0, \ldots, M\}$ at random, where $M \geq K\ell/\varepsilon$. Then, with probability at least $1 - \varepsilon$, there is a unique form in C of minimum value at $z_1, \ldots, z_\ell$.

A simple rephrasing of Lemma 2.26 allows us to isolate a term of a multivariate polynomial $f(y_1, \ldots, y_\ell)$ under a random monomial substitution $y_i \mapsto w^{z_i}$:

Corollary 2.27: Let $K \in \mathbb{Z}_{\geq 0}$. Let A be any ring, and let $f(y_1, \ldots, y_\ell) \in A[\overline{y}]$ 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 $z_1, \ldots, z_\ell$ independently and uniformly at random from $\{0, \ldots, M\}$, where $M \geq K\ell/\varepsilon$. Let w be a new indeterminate, and define $\phi : A[y_1, \ldots, y_\ell] \to A[w]$ 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 $\mathfrak{m} = y_1^{e_1} \cdots y_\ell^{e_\ell}$ among all monomials of f such that $\phi(\mathfrak{m}) = w^{e_1 z_1 + \cdots + e_\ell z_\ell}$ attains the minimum degree in w.

2.6 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 2.28: For $f \in \mathbb{F}[\overline{x}, t]$ and an integer $i \in \mathbb{Z}_{\geq 0}$, denote by $\mathrm{coeff}_{t^i}(f)$ the coefficient of t^i in f when f is viewed as a univariate polynomial in t over the ring $\mathbb{F}[\overline{x}]$. Note that $\mathrm{coeff}_{t^i}(f) \in \mathbb{F}[\overline{x}]$.

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 $f \in \mathbb{F}[x_1, \ldots, x_n]$ is exactly $\mathrm{coeff}_{t^i}(f(tx_1, \ldots, tx_n))$.

Lemma 2.29: Let $g \in \mathbb{F}[\overline{x}, t]$, and let $f \in \mathbb{F}[\overline{x}, t]$ be a degree-d polynomial such that for each $\alpha \in \mathbb{F}$, the polynomial $f(\overline{x}, \alpha)$ 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 $\mathrm{coeff}_{t^i}(f)$, 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.

Proof: By definition,

$$f = \sum_{i=0}^{d} \mathrm{coeff}_{t^i}(f) t^i.$$

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

$$\begin{pmatrix} \alpha_1^d & \alpha_1^{d-1} & \cdots & \alpha_1 & 1 \\ \alpha_2^d & \alpha_2^{d-1} & \cdots & \alpha_2 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_d^d & \alpha_d^{d-1} & \cdots & \alpha_d & 1 \\ \alpha_{d+1}^d & \alpha_{d+1}^{d-1} & \cdots & \alpha_{d+1} & 1 \end{pmatrix} \begin{pmatrix} \operatorname{coeff}_{t^d}(f) \\ \operatorname{coeff}_{t^{d-1}}(f) \\ \vdots \\ \operatorname{coeff}_t(f) \\ \operatorname{coeff}_1(f) \end{pmatrix} = \begin{pmatrix} f(\overline{x}, \alpha_1) \\ f(\overline{x}, \alpha_2) \\ \vdots \\ f(\overline{x}, \alpha_d) \\ f(\overline{x}, \alpha_{d+1}) \end{pmatrix}$$

The $(d+1)\times(d+1)$ matrix $(\alpha_i^{d+1-j}) \in \mathbb{F}^{(d+1)\times(d+1)}$ is a Vandermonde matrix. As all the α_i are distinct, this matrix is invertible and so there exists a $(d+1)\times(d+1)$ matrix $(z_{i,j}) \in \mathbb{F}^{(d+1)\times(d+1)}$ such that

$$\begin{pmatrix} \operatorname{coeff}_{t^d}(f) \\ \operatorname{coeff}_{t^{d-1}}(f) \\ \vdots \\ \operatorname{coeff}_t(f) \\ \operatorname{coeff}_1(f) \end{pmatrix} = \begin{pmatrix} z_{1,1} & z_{1,2} & \cdots & z_{1,d} & z_{1,d+1} \\ z_{2,1} & z_{2,2} & \cdots & z_{2,d} & z_{2,d+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ z_{d,1} & z_{d,2} & \cdots & z_{d,d} & z_{d,d+1} \\ z_{d+1,1} & z_{d+1,2} & \cdots & z_{d+1,d} & z_{d+1,d+1} \end{pmatrix} \begin{pmatrix} f(\overline{x}, \alpha_1) \\ f(\overline{x}, \alpha_2) \\ \vdots \\ f(\overline{x}, \alpha_d) \\ f(\overline{x}, \alpha_{d+1}) \end{pmatrix}$$

Fix $0 \le i \le d$. We now have an explicit expression for $\operatorname{coeff}_{t^i}(f)$:

$$\operatorname{coeff}_{t^i}(f) = \sum_{j=1}^{d+1} z_{d+1-i,j} f(\overline{x}, \alpha_j). \tag{2}$$

With Equation (2), we can now describe the circuit for $\operatorname{coeff}_{t^i}(f)$. The scalars $\alpha_1, \ldots, \alpha_{d+1}$ are fixed a priori, and hence so are the $z_{i,j}$ for $i, j \in [d+1]$. Recall that scalar multiplications along wires are free. For each $j \in [d+1]$, computing $f(\overline{x}, \alpha_j)$ requires a single g-oracle circuit C_{α_j} of size at most s and depth Δ. Hence, evaluating all $d+1$ such terms requires total size $O(ds)$. The top-level summation uses one addition gate and $d+1$ scalar multiplications by the $z_{d+1-i,j}$ along $d+1$ wires. Therefore, Equation (2) yields a g-oracle circuit D_i of size $O(ds+d) = O(ds)$ and depth $\Delta+1$ computing $\operatorname{coeff}_{t^i}(f)$. Moreover, if the top gate of each C_{α_j} is an addition gate, then the top two layers of D_i consist entirely of additions and can be merged to reduce the depth bound to Δ. □

Remark: The condition $|\mathbb{F}| \ge d+1$ in Lemma 2.29, 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 [Str73], which requires no lower bound on $|\mathbb{F}|$.

3 Determinantal Ideals

Our application of the determinantal straightening law (Corollary 2.13), together with the isolation lemma (Corollary 2.27) and extraction of coefficients (Lemma 2.29), allows us to isolate a canonical

bitableau from the expansion of nonzero $f \in I^{\det}_{n,m,r}$ 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 2.27) as well as coefficient extraction (Lemma 2.29). This is in contrast to the proof of [AF22], 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 $f(X) \in I^{\det}_{n,m,r}$.

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 $I^{\det}_{n,m,r}$ to be the ideal in $\mathbb{F}[X]$ generated by the $r \times r$ minors of X.

Our first step will be to establish a series of linear transformations that send a conjugate semistandard bitableau to the anti-canonical conjugate semistandard bitableau of the same shape.

Definition 3.1 (Substitution operator): Let $i < j$. Define the operator $\mathrm{Sub}_{i\to j}$ 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 $h^j_i(S)$ to be the number of times i is replaced by j after applying $\mathrm{Sub}_{i\to j}$ to S.

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

Lemma 3.2 ([dCEP80, 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 $\{i, i+1, \ldots, j-1\}$. Then $\mathrm{Sub}_{i\to j}(S)$ is again conjugate semistandard. Furthermore, S is completely determined by $\mathrm{Sub}_{i\to j}(S)$ and $h^j_i(S)$.

We will primarily use Lemma 3.2 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 $\mathrm{Sub}_{i\to j}$ together with the values of h^j_i. We then apply these successive substitutions in the following lexicographic order:

Definition 3.3 (Lexicographic ordering): We order the elements of $\binom{[n]}{2} = \{(i, j) \mid 1 \leq i < j \leq n\}$ such that $(i, j) \preceq (i', j')$ if either $i < i'$, or $i = i'$ and $j \leq j'$.

In particular, note that the hypothesis in Lemma 3.2 holds trivially for the operator $\mathrm{Sub}_{1\to 2}$. Furthermore, as we apply the substitution operators successively in the lexicographic ordering, the resulting tableaux also satisfy the hypothesis.

Lemma 3.4 (implicit in the proof of [dCEP80, Corollary 1.7]; see [AF22, 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

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

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 3.2 for $\mathrm{Sub}_{i\to j}$, meaning that if a row of $S_{i',j'}$ contains an integer $k \le i$, then that same row in S contains all integers in $\{i, i+1, \ldots, j-1\}$.

Lemma 3.5: Fix a partition σ. For a natural number n and $1 \le i < j \le n$ and a conjugate semistandard tableau S of shape σ, define $h_{n,i,j}$ as $h_i^j(S_{i',j'})$ where

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

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 3.2 as S is completely determined by $\mathrm{Sub}_{1\to 2}(S)$ 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 3.2 and Lemma 3.4. 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 3.6 ([dCEP80, stated before Corollary 1.7]): Let S be a conjugate semistandard tableau of shape σ such that S has entries of value at most n. Then

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

We now study how these substitution operators act on bideterminants $(S \mid T)(X)$. From properties of the determinant, we see that multiplying the matrix of variables X by a elementary matrix $E_{i,j}$ (Definition 2.3) corresponds to applying substitution operators on S or T:

Lemma 3.7: Let λ be a new indeterminate. Let $(S \mid T)$ be a bitableau, not necessarily standard, of shape σ. For $0 \le h \le h_i^j(S) - 1$, let $C_{i\to j}^h(S)$ be the set of tableaux of shape σ obtained by changing

i to j at exactly h rows of S which contain i but not j and reordering those rows to be increasing. Then we have that

$$(S \mid T)(E_{i,j}(\lambda)X) = \pm\lambda^{h_i^j(S)}(\mathrm{Sub}_{i\to j}(S) \mid T)(X) + \sum_{h=0}^{h_i^j(S)-1} \lambda^h \sum_{S'\in\mathcal{C}_{i\to j}^h(S)} \pm(S' \mid T)(X). \tag{3}$$

Similarly, we also have that

$$(S \mid T)(XE_{i,j}(\lambda)^\top) = \pm\lambda^{h_i^j(T)}(S \mid \mathrm{Sub}_{i\to j}(T))(X) + \sum_{h=0}^{h_i^j(T)-1} \lambda^h \sum_{T'\in\mathcal{C}_{i\to j}^h(T)} \pm(S \mid T')(X). \tag{4}$$

Proof: We only prove Equation (3) as the proof of Equation (4) is completely analogous. First, suppose σ is exactly one row. Then $(S \mid T)(X)$ is just the determinant of some submatrix of X with rows specified by S and columns specified by T. Let $\widetilde{X}$ be matrix formed by replacing row i of X with λ times row j and let $X' = X + \widetilde{X}$. Thus, $E_{i,j}(\lambda)X = X'$. More explicitly, X' is formed by adding λ times row j to row i. We will consider cases based on if S contains i or j and make use of the multilinear and alternating properties of the determinant. If S does not contain i, then

$$(S \mid T)(X') = (S \mid T)(X)$$

because $(S \mid T)$ does not use row i and X and X' differ only in row i. If S contains both i and j, then as the determinant is alternating and the i-th row and j-th row of $\widetilde{X}$ only differ by a multiple, we must have that $(S \mid T)(\widetilde{X}) = 0$. Therefore, by the multilinearity of the determinant we can write

$$(S \mid T)(X') = (S \mid T)(X) + (S \mid T)(\widetilde{X}) = (S \mid T)(X).$$

Finally, if S contains i but not j, then by multilinearity of the determinant, we have that

$$(S \mid T)(X') = (S \mid T)(X) + \lambda(S \mid T)(X') = (S \mid T)(X) \pm \lambda(\mathrm{Sub}_{i\to j}(S) \mid T)(X).$$

The $\pm$ in front of the second term comes from the fact that $\mathrm{Sub}_{i\to j}$ not only changes i to j but also reorders the entries to be in increasing order again. Reordering rows induces a change in sign that we must account for. Thus, we overall have that

$$(S \mid T)(E_{i,j}(\lambda)X) = \begin{cases} (S \mid T)(X) \pm \lambda(\mathrm{Sub}_{i\to j}(S) \mid T)(X) & \text{if } S \text{ contains } i \text{ but not } j, \\ (S \mid T)(X) & \text{otherwise.} \end{cases} \tag{5}$$

This gives Equation (3) in the case of a single row.

The result for a general bitableau $(S \mid T)$ of shape σ then follows via repeated application of the one row case. As an application of the definition of a bideterminant (Definition 2.9), we can write

$(S \mid T)(X)$ as a product of one row bideterminants:

$$(S \mid T)(E_{i,j}(\lambda)X) = \prod_{k=1}^{\widehat{\sigma}_1} (S_k \mid T_k)(E_{i,j}(\lambda)X). \tag{6}$$

We then apply the one row case (Equation (5)) to each factor in the product in Equation (6), expand the product, and study the terms of various degree in λ after expansion. For each $0 \leq h \leq h_i^j(S)$, it is clear that terms of degree h in λ are of the form $\pm\lambda^h(S' \mid T)(X)$ where S' is obtained by changing i to j in exactly h rows of S which contain i but not j and reordering those rows to be increasing. Since $C_{i\to j}^{h_i^j(S)}(S) = \{\operatorname{Sub}_{i\to j}(S)\}$, there is exactly one term of degree $h_i^j(S)$ in λ, namely $\pm\lambda^{h_i^j(S)}(\operatorname{Sub}_{i\to j}(S) \mid T)(X)$ This proves Equation (3). The proof of Equation (4) is completely analogous. □

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 $|\Lambda| = \binom{n}{2} = O\left(n^2\right)$ and $|\Xi| = \binom{m}{2} = O\left(m^2\right)$. 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

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

and

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

Recall the lexicographic ordering $\preceq$ (Definition 3.3) 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 3.8: Let $f(X) \in I^{\det}_{n,m,r}$ be a nonzero polynomial of degree d. Then $f(MX)$ can be expressed as a sum

$$f(MX) = \sum_{k\in A} \widetilde{c}_k \Lambda^{\overline{e}_k} \cdot (\overline{K}_{\sigma_k} \mid T_k)(X) + \sum_{\ell \in A'} \widetilde{c}_\ell \Lambda^{\overline{e}_\ell} \cdot (S_\ell \mid T_\ell)(X), \tag{7}$$

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 (7) have the form $c\Lambda^{\overline{e}} \cdot (S \mid T)(X)$, where $c \in \mathbb{F}^\times$, $\overline{e} \in \{0,1,\ldots,d\}^{\binom{[n]}{2}}$, and $(S \mid T)(X)$ is a bideterminant in $I^{\det}_{n,m,r}$ 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 $\overline{e}_\ell$ is strictly smaller than $\overline{e}_k$ in the lexicographic order and the shape σ_ℓ of $(S_\ell \mid T_\ell)$ equals the shape σ_k.

(5) The triples $(\overline{e}_k, \sigma_k, T_k)$ are distinct as k ranges over A.

Proof: By Corollary 2.13 and Proposition 2.14, we can expand $f(X)$ as a linear combination of standard bideterminants over $\mathbb{F}$

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

where B is nonempty, each $c_k \in \mathbb{F}^\times$, and $(S_k \mid T_k)(X)$ is a standard bideterminant in $I^{\det}_{n,m,r}$ 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

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

For each $k \in B$, we expand the term $c_k \cdot (S_k \mid T_k)(MX)$ by repeatedly applying Lemma 3.7. This expansion shows that $c_k \cdot (S_k \mid T_k)(MX)$ equals $\pm c_k \Lambda^{\overline{e}_k} \cdot (\overline{K}_{\sigma_k} \mid T_k)(X)$ with $\overline{e}_k = (h_{n,i,j}(S_k))_{1\leq i<j\leq n} \in \{0,1,\ldots,d\}^{\binom{[n]}{2}}$ plus some terms of the form $\pm\widetilde{c}_\ell \Lambda^{\overline{e}_\ell} \cdot (S_\ell \mid T_\ell)(X)$, each with a new index ℓ, where $\widetilde{c}_\ell = \pm c_k$, $(S_\ell \mid T_\ell)(X)$ is a (not necessarily standard) bideterminant of shape $\sigma_\ell = \sigma_k$, and $\overline{e}_\ell$ is strictly smaller than $\overline{e}_k$ in the lexicographic order. Note that as $\sigma_\ell = \sigma_k$, their first rows both have length at least r, implying that $(S_\ell \mid T_\ell)(X) \in I^{\det}_{n,m,r}$ by Proposition 2.14. Also note that $\overline{e}_\ell \in \{0,1,\ldots,d\}^{\binom{[n]}{2}}$ since a substitution $i \mapsto j$ can be performed at most $(\widehat{\sigma_\ell})_1 \leq d$ 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

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

satisfying Items 1 to 4.

It remains to prove Item 5. Assume to the contrary that there exist distinct $k_1, k_2 \in A$ such that $(\overline{e}_{k_1}, \sigma_{k_1}, T_{k_1}) = (\overline{e}_{k_2}, \sigma_{k_2}, T_{k_2})$. As the bideterminants $(S_k \mid T_k)$ 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 $\overline{e}_{k_1} = (h_{n,i,j}(S_{k_1}))_{1\leq i<j\leq n}$ and $\overline{e}_{k_2} = (h_{n,i,j}(S_{k_2}))_{1\leq i<j\leq n}$. Note that S_{k_1} and S_{k_2} have the same shape $\sigma_{k_1} = \sigma_{k_2}$. By Lemma 3.5, S_{k_1} is completely determined by $\overline{K}_{\sigma_{k_1}}$ and $(h_{n,i,j}(S_{k_1}))_{1\leq i<j\leq n}$, and S_{k_2} is completely determined by $\overline{K}_{\sigma_{k_2}}$ and $(h_{n,i,j}(S_{k_2}))_{1\leq i<j\leq n}$. But then if $\overline{e}_{k_1} = \overline{e}_{k_2}$ and $\sigma_{k_1} = \sigma_{k_2}$, we must have that $S_{k_1} = S_{k_2}$, a contradiction. □

Lemma 3.9: Let $f(X) \in I^{\det}_{n,m,r}$ be a nonzero polynomial of degree d. Then $f(MXN)$ can be expressed as a sum

$$f(MXN) = \sum_{k\in A} \widehat{c}_k \Lambda^{\overline{e}_k} \Xi^{\overline{f}_k} \cdot (\overline{K}_{\sigma_k} \mid \overline{K}_{\sigma_k})(X) + \sum_{\ell\in B} \widehat{c}_\ell \Lambda^{\overline{e}_\ell} \Xi^{\overline{f}_\ell} \cdot (S_\ell \mid T_\ell)(X), \tag{8}$$

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 (8) have the form $c\Lambda^{\overline{e}}\Xi^{\overline{f}} \cdot (S \mid T)(X)$, where $c \in \mathbb{F}^\times$, $\overline{e} \in \{0, 1, \ldots, d\}^{\binom{[n]}{2}}$, $\overline{f} \in \{0, 1, \ldots, d\}^{\binom{[m]}{2}}$, and $(S \mid T)(X)$ is a bideterminant in $I^{\det}_{n,m,r}$ 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 $(\overline{e}_\ell, \overline{f}_\ell)$ is strictly smaller than $(\overline{e}_k, \overline{f}_k)$ in the lexicographic order and the shape σ_ℓ of $(S_\ell \mid T_\ell)$ equals the shape σ_k.

(4) The triples $(\overline{e}_k, \overline{f}_k, \sigma_k)$ are distinct, where k ranges over A.

Proof: We use Lemma 3.8 to write $f(MX)$ as

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

which satisfies Lemma 3.8. Then

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

For each $k \in A$, we expand the term $\widetilde{c}_k \Lambda^{\overline{e}_k} \cdot (\overline{K}_{\sigma_k} \mid T_k)(XN)$ by repeatedly applying Lemma 3.7. This expansion shows that $\widetilde{c}_k \Lambda^{\overline{e}_k} \cdot (\overline{K}_{\sigma_k} \mid T_k)(XN)$ equals $\pm\widetilde{c}_k \Lambda^{\overline{e}_k} \Xi^{\overline{f}_k} \cdot (\overline{K}_{\sigma_k} \mid \overline{K}_{\sigma_k})(X)$ with $\overline{f}_k = (h_{m,i,j}(T_k))_{1\leq i<j\leq m} \in \{0, 1, \ldots, d\}^{\binom{[m]}{2}}$, plus some terms of the form $\widehat{c}_\ell \Lambda^{\overline{e}_\ell} \Xi^{\overline{f}_\ell} \cdot (S_\ell \mid T_\ell)(X)$, each with a new index ℓ, where $\widehat{c}_\ell = \pm\widetilde{c}_k$, $(S_\ell \mid T_\ell)(X)$ is a (not necessarily standard) bideterminant of shape $\sigma_\ell = \sigma_k$, $\overline{e}_\ell = \overline{e}_k$, and $\overline{f}_\ell$ is strictly smaller than $\overline{f}_k$ in the lexicographic order. In particular, $(\overline{e}_\ell, \overline{f}_\ell)$ is strictly smaller than $(\overline{e}_k, \overline{f}_k)$ in the lexicographic order. Note that as $\sigma_\ell = \sigma_k$, their first rows both have length at least r, implying that $(S_\ell \mid T_\ell)(X) \in I^{\det}_{n,m,r}$ by Proposition 2.14. Also note that

$\overline{f}_\ell \in \{0,1,\dots,d\}^{\binom{[m]}{2}}$ since a substitution $i \mapsto j$ can be performed at most $(\widehat{\sigma_\ell})_1 \le d$ 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 $\widetilde{c}_\ell \Lambda^{\overline{e}_\ell} \cdot (S_\ell \mid T_\ell)(XN)$ by repeatedly applying Lemma 3.7. Note that $(S_\ell \mid T_\ell)$ is not necessarily standard, but Lemma 3.7 still applies. Consider any term $\widehat{c}_{\ell'} \Lambda^{\overline{e}_{\ell'}} \Xi^{\overline{f}_{\ell'}} \cdot (S_{\ell'} \mid T_{\ell'})(X)$ generated this way, where ℓ' is a new index. Let $k = k(\ell)$ as in Lemma 3.8 (4). We have $\widehat{c}_{\ell'} = \pm\widetilde{c}_\ell$, $(S_{\ell'} \mid T_{\ell'})(X)$ is a (not necessarily standard) bideterminant of shape $\sigma_{\ell'} = \sigma_\ell = \sigma_k$, and $\overline{e}_{\ell'} = \overline{e}_\ell$, which is strictly smaller than $\overline{e}_k$ in the lexicographic order. In particular, $(\overline{e}_{\ell'}, \overline{f}_{\ell'})$ is strictly smaller than $(\overline{e}_k, \overline{f}_k)$ in the lexicographic order. Note that as $\sigma_{\ell'} = \sigma_k$, their first rows both have length at least r, implying that $(S_{\ell'} \mid T_{\ell'})(X) \in I^{\det}_{n,m,r}$ by Proposition 2.14. Also note that $\overline{f}_{\ell'} \in \{0,1,\dots,d\}^{\binom{[m]}{2}}$ 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

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

satisfying Items 1 to 3.

It remains to prove Item 4. Assume to the contrary that there exist distinct $k_1, k_2 \in A$ such that $(\overline{e}_{k_1}, \overline{f}_{k_1}, \sigma_{k_1}) = (\overline{e}_{k_2}, \overline{f}_{k_2}, \sigma_{k_2})$. By Lemma 3.8 (5), we have $T_{k_1} \ne T_{k_2}$, both of which are conjugate semistandard. From the proof above, we have $\overline{f}_{k_1} = (h_{m,i,j}(T_{k_1}))_{1 \le i < j \le m}$ and $\overline{f}_{k_2} = (h_{m,i,j}(T_{k_2}))_{1 \le i < j \le m}$. Note that T_{k_1} and T_{k_2} have the same shape $\sigma_{k_1} = \sigma_{k_2}$. By Lemma 3.5, T_{k_1} is completely determined by $\overline{K}_{\sigma_{k_1}}$ and $(h_{m,i,j}(T_{k_1}))_{1 \le i < j \le m}$, and T_{k_2} is completely determined by $\overline{K}_{\sigma_{k_2}}$ and $(h_{m,i,j}(T_{k_2}))_{1 \le i < j \le m}$. But then if $\overline{f}_{k_1} = \overline{f}_{k_2}$ and $\sigma_{k_1} = \sigma_{k_2}$, we must have that $T_{k_1} = T_{k_2}$, a contradiction. □

Next, we reformulate Lemma 3.9 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 $m - j + 1$. This turns an anti-canonical bitableau $(\overline{K}_\sigma \mid \overline{K}_\sigma)$ into a canonical one $(K_\sigma \mid K_\sigma)$.

Corollary 3.10: Let $f(X) \in I^{\det}_{n,m,r}$ be a nonzero polynomial of degree d. Then $f(MJ_nXJ_mN)$ can be expressed as a sum

$$f(MJ_nXJ_mN) = \sum_{k \in A} \widehat{c}_k \Lambda^{\overline{e}_k} \Xi^{\overline{f}_k} \cdot (K_{\sigma_k} \mid K_{\sigma_k})(X) + \sum_{\ell \in B} \widehat{c}_\ell \Lambda^{\overline{e}_\ell} \Xi^{\overline{f}_\ell} \cdot (S_\ell \mid T_\ell)(X), \tag{9}$$

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 (9) have the form $c\Lambda^{\overline{e}}\Xi^{\overline{f}} \cdot (S \mid T)(X)$, where $c \in \mathbb{F}^\times$, $\overline{e} \in \{0,1,\ldots,d\}^{\binom{[n]}{2}}$, $\overline{f} \in \{0,1,\ldots,d\}^{\binom{[m]}{2}}$, and $(S \mid T)(X)$ is a bideterminant in $I^{\det}_{n,m,r}$ of degree 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 $(\overline{e}_\ell, \overline{f}_\ell)$ is strictly smaller than $(\overline{e}_k, \overline{f}_k)$ in the lexicographic order and the shape σ_ℓ of $(S_\ell \mid T_\ell)$ equals the shape σ_k.

(4) The triples $(\overline{e}_k, \overline{f}_k, \sigma_k)$ are distinct, where k ranges over A.

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

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

Lemma 3.11: Let $(S \mid T)(X)$ be a bideterminant of degree at most d. Then

$$(S \mid T)(DXD') = Y^{\overline{s}}Z^{\overline{t}} \cdot (S \mid T)(X),$$

where $\overline{s} = (s_1,\ldots,s_n) \in \{0,1,\ldots,d\}^n$, $\overline{t} = (t_1,\ldots,t_m) \in \{0,1,\ldots,d\}^m$, s_i is the number of times i appears in S, t_j is the number of times j appears in T, i.e., $(s_1e_1 + \cdots + s_ne_n) \oplus (t_1e_1 + \cdots + t_me_m)$ is the multidegree of $(S \mid T)(X)$ with respect to the grading defined in Definition 2.15.

Proof: Reduce to the case in which S and T each have one row, and then use the multilinearity of the determinant. □

We will often simply say that $(S \mid T)(X)$ in Lemma 3.11 has multidegree $(\overline{s}, \overline{t})$ rather than writing it as $(s_1e_1 + \cdots + s_ne_n) \oplus (t_1e_1 + \cdots + t_me_m)$.

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

$$\widetilde{D} = \operatorname{diag}(y_1v, y_2v^2\ldots, y_nv^n) \in \mathbb{F}[Y,v]^{n\times n} \quad \text{and} \quad \widetilde{D}' = \operatorname{diag}(z_1v, z_2v^2,\ldots,z_mv^m) \in \mathbb{F}[Z,v]^{m\times m}.$$

Lemma 3.12: Let $(S \mid T)(X)$ be a bideterminant. Then

$$(S \mid T)(\widetilde{D}X\widetilde{D}') = Y^{\overline{s}}Z^{\overline{t}}v^{|S|+|T|} \cdot (S \mid T)(X),$$

where $(\overline{s}, \overline{t})$ is the multidegree of $(S \mid T)(X)$.

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 $|S| + |T|$, i.e., the sum of the entries of S and of T. □

Before proceeding, we clarify the relationship between our arguments and those in [AF22]. Much of our proof follows the overall structure of [AF22]: the expansions in (7), (8), and (9) already appear there. However, our statements refine those in [AF22] by providing more detailed information about the "garbage" terms (those indexed by the sets A' or B in (7), (8), and (9)). In particular, we establish additional properties of these terms that will be essential in the proof of the key technical 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 [AF22] 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 3.10, that isolating a term of lowest degree in v indeed yields a canonical standard bideterminant.

Lemma 3.13: Let $f(X) \in I^{\det}_{n,m,r}$ be a nonzero polynomial of degree d. Let $g = f(MJ_n\widetilde{D}X\widetilde{D}'J_mN) \in \mathbb{F}[X, \Lambda, \Xi, Y, Z, v]$. View g as a univariate polynomial in v with coefficients in $\mathbb{F}[X, \Lambda, \Xi, Y, Z]$, and write $g = \sum_i \operatorname{coeff}_{v^i}(g)v^i$, where $\operatorname{coeff}_{v^i}(g) \in \mathbb{F}[X, \Lambda, \Xi, Y, Z]$ denotes the coefficient of v^i in g. Choose the smallest integer $d_{\min}$ such that $\operatorname{coeff}_{v^{d_{\min}}}(g) \neq 0$. Then $d_{\min} = 2|K_\sigma|$ for some shape σ with $|\sigma| \leq d$ and we may write $\operatorname{coeff}_{v^{d_{\min}}}(g)$ as a finite sum

$$\operatorname{coeff}_{v^{d_{\min}}}(g) = \sum_{k \in I} c_k \Lambda^{\overline{e}_k} \Xi^{\overline{f}_k} Y^{\overline{s}_k} Z^{\overline{t}_k} \cdot (K_{\sigma_k} \mid K_{\sigma_k})(X), \tag{10}$$

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 $(\overline{e}_k, \overline{f}_k, \overline{s}_k, \overline{t}_k)$ are distinct, where k ranges over I.

Proof: Consider the expansion

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

given by Corollary 3.10. Then we have

$$
\begin{aligned}
g &= \sum_{k\in A} \widehat{c}_k \Lambda^{\overline{e}_k} \Xi^{\overline{f}_k} \cdot (K_{\sigma_k} \mid K_{\sigma_k})(\widetilde{D} X \widetilde{D}') + \sum_{\ell \in B} \widehat{c}_\ell \Lambda^{\overline{e}_\ell} \Xi^{\overline{f}_\ell} \cdot (S_\ell \mid T_\ell)(\widetilde{D} X \widetilde{D}') \\
&= \sum_{k\in A} \widehat{c}_k \Lambda^{\overline{e}_k} \Xi^{\overline{f}_k} Y^{\overline{s}_k} Z^{\overline{t}_k} \nu^{2\left|K_{\sigma_k}\right|} \cdot (K_{\sigma_k} \mid K_{\sigma_k})(X) + \sum_{\ell \in B} \widehat{c}_\ell \Lambda^{\overline{e}_\ell} \Xi^{\overline{f}_\ell} Y^{\overline{s}_\ell} Z^{\overline{t}_\ell} \nu^{|S_\ell|+|T_\ell|} \cdot (S_\ell \mid T_\ell)(X),
\end{aligned} \tag{11}
$$

where for $k \in A$, $(\overline{s}_k, \overline{t}_k)$ is the multidegree of $(K_{\sigma_k} \mid K_{\sigma_k})(X)$, and for $\ell \in B$, $(\overline{s}_\ell, \overline{t}_\ell)$ is the multidegree of $(S_\ell \mid T_\ell)(X)$. Here, the second equality holds by Lemma 3.12.

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

For any $k \in A$, consider the term $\widehat{c}_k \Lambda^{\overline{e}_k} \Xi^{\overline{f}_k} Y^{\overline{s}_k} Z^{\overline{t}_k} \nu^{2\left|K_{\sigma_k}\right|} \cdot (K_{\sigma_k} \mid K_{\sigma_k})(X)$ in Equation (11). It is homogeneous of degree $2\left|K_{\sigma_k}\right| \geq 2\left|K_{\sigma_{k_0}}\right| = d_0$ with respect to ν by the minimality of $\left|K_{\sigma_{k_0}}\right|$, and contributes to $\operatorname{coeff}_{\nu^{d_0}}(g)$ if and only if $\left|K_{\sigma_k}\right| = \left|K_{\sigma_{k_0}}\right|$. Even if it can potentially contribute to $\operatorname{coeff}_{\nu^{d_0}}(g)$, its (multi)degree $(\overline{e}_k, \overline{f}_k, \overline{s}_k, \overline{t}_k)$ 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 $(\overline{e}_k, \overline{f}_k, \sigma_k) \neq (\overline{e}_{k_0}, \overline{f}_{k_0}, \sigma_{k_0})$. If $\sigma_k = \sigma_{k_0}$, then $(\overline{e}_k, \overline{f}_k) \neq (\overline{e}_{k_0}, \overline{f}_{k_0})$. On the other hand, if $\sigma_k \neq \sigma_{k_0}$, then $(\overline{s}_k, \overline{t}_k) \neq (\overline{s}_{k_0}, \overline{t}_{k_0})$ by Lemma 2.16. Overall, we always have that

$$(\overline{e}_k, \overline{f}_k, \overline{s}_k, \overline{t}_k) \neq (\overline{e}_{k_0}, \overline{f}_{k_0}, \overline{s}_{k_0}, \overline{t}_{k_0}).$$

Now consider $\ell \in B$ and the term $\mathfrak{m}_\ell := \widehat{c}_\ell \Lambda^{\overline{e}_\ell} \Xi^{\overline{f}_\ell} Y^{\overline{s}_\ell} Z^{\overline{t}_\ell} \nu^{|S_\ell|+|T_\ell|} \cdot (S_\ell \mid T_\ell)(X)$ in Equation (11). The degree of $\mathfrak{m}_\ell$ in ν is $|S_\ell| + |T_\ell|$. Let $k = k(\ell)$ as in Corollary 3.10. Then by Corollary 3.10 (3), S_ℓ and T_ℓ have shape $\sigma_\ell = \sigma_k$. Note that among all bideterminants $(S \mid T)$ of shape σ, the quantity $|S| + |T|$ is minimized when, and only when, $(S \mid T) = (K_\sigma \mid K_\sigma)$. Thus, we have

$$|S_\ell| + |T_\ell| \geq 2\left|K_{\sigma_k}\right| \geq 2\left|K_{\sigma_{k_0}}\right| = d_0$$

and $\deg_\nu(\mathfrak{m}_\ell) = |S_\ell| + |T_\ell| = d_0$ if and only if $(S_\ell \mid T_\ell) = (K_{\sigma_k} \mid K_{\sigma_k})$ and $\left|K_{\sigma_k}\right| = \left|K_{\sigma_{k_0}}\right|$. Even though this can happen, when it happens we have that $(\overline{e}_k, \overline{f}_k)$ is smaller than or equal to $(\overline{e}_{k_0}, \overline{f}_{k_0})$ in the lexicographic order by the choice of k_0, noting that $\left|K_{\sigma_k}\right| = \left|K_{\sigma_{k_0}}\right|$. And by Corollary 3.10 (3), $(\overline{e}_\ell, \overline{f}_\ell)$ is strictly smaller than $(\overline{e}_k, \overline{f}_k)$ in the lexicographic order. Overall, either $\deg_\nu(\mathfrak{m}_\ell) > d_0$, or $(\overline{e}_\ell, \overline{f}_\ell, \overline{s}_\ell, \overline{t}_\ell) \neq (\overline{e}_{k_0}, \overline{f}_{k_0}, \overline{s}_{k_0}, \overline{t}_{k_0})$.

By the above analysis, the term $\widehat{c}_{k_0} \Lambda^{\overline{e}_{k_0}} \Xi^{\overline{f}_{k_0}} Y^{\overline{s}_{k_0}} Z^{\overline{t}_{k_0}} \nu^{2\left|K_{\sigma_{k_0}}\right|} \cdot (K_{\sigma_{k_0}} \mid K_{\sigma_{k_0}})(X)$ is not canceled by other terms contributing to $\operatorname{coeff}_{\nu^{d_0}}(g)$ due to the uniqueness of its (multi)degree $(\overline{e}_{k_0}, \overline{f}_{k_0}, \overline{s}_{k_0}, \overline{t}_{k_0})$ in Λ, Ξ, Y, and Z. Thus $\operatorname{coeff}_{\nu^{d_0}}(g) \neq 0$. The above analysis also shows that $\operatorname{coeff}_{\nu^i}(g) = 0$ for $i < d_0$. Thus, $d_0 = d_{\min}$.

Moreover, the above analysis shows that any term that contributes to $\operatorname{coeff}_{v^{d_0}}(g)$ contains a bideterminant of the form $(K_\sigma \mid K_\sigma)(X)$.

We then merge the terms contributing to $\operatorname{coeff}_{v^{d_0}}(g)$ with the same (multi)degree in Λ, Ξ, Y, and Z. When we merge two terms $\widehat{c}_k \Lambda^{\bar{e}_k} \Xi^{\bar{f}_k} Y^{\bar{s}_k} Z^{\bar{t}_k} v^{d_0} \cdot (K_{\sigma_k} \mid K_{\sigma_k})(X)$ and $\widehat{c}_{k'} \Lambda^{\bar{e}_{k'}} \Xi^{\bar{f}_{k'}} Y^{\bar{s}_{k'}} Z^{\bar{t}_{k'}} v^{d_0} \cdot (K_{\sigma_{k'}} \mid K_{\sigma_{k'}})(X)$ 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 $(K_{\sigma_k} \mid K_{\sigma_k}) = (K_{\sigma_{k'}} \mid K_{\sigma_{k'}})$. This follows from Lemma 2.16 and the fact that $(\bar{s}_k, \bar{t}_k)$ is the multidegree of $(K_{\sigma_k} \mid K_{\sigma_k})(X)$ and $(\bar{s}_{k'}, \bar{t}_{k'})$ is the multidegree of $(K_{\sigma_{k'}} \mid K_{\sigma_{k'}})(X)$. Thus, merging the two terms yields a scalar multiple of both.

After merging/canceling terms, we can write $\operatorname{coeff}_{v^{d_{\min}}}(g) = \operatorname{coeff}_{v^{d_0}}(g)$ in the form of Equation (10) such that Item 2 holds. Furthermore, Item 1 holds as well by Corollary 3.10 (2) and Proposition 2.14. □

Lemma 3.13 helps us separate a collection of terms solely containing canonical bideterminants. The next lemma further applies the isolation lemma to single out one term from this collection.

Lemma 3.14: Let $f(X) \in I^{\det}_{n,m,r}$ be a nonzero polynomial of degree d. Let $g = f(MJ_n\widetilde{D}X\widetilde{D}'J_mN) \in \mathbb{F}[X, \Lambda, \Xi, Y, Z, v]$. Then there exist integers $z_t = O\left(d(n^2+m^2)\right)$ for each variable $t \in \Lambda \sqcup \Xi \sqcup Y \sqcup Z$, and an integer $z_v = O\left(d^2(n^2+m^2)\right)$ such that for the two variable substitution maps

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

and

$$\psi : v \mapsto w^{z_v},$$

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

Proof: Consider the finite sum from Lemma 3.13:

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

The coordinates of $\bar{e}_k$, $\bar{f}_k$, $\bar{s}_k$, and $\bar{t}_k$ are in $\{0, 1, \ldots, d\}$ for each $k \in I$ by Corollary 3.10 (2) and Lemma 3.12. Choose a sufficiently large $L = \Theta\left(d(n^2+m^2)\right)$, and pick integers z_t independently and uniformly at random from $\{0, 1, \ldots, L\}$, where $t \in \Lambda \sqcup \Xi \sqcup Y \sqcup Z$. Then by Corollary 2.27, 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 $c \cdot (K_\sigma \mid K_\sigma)(X) \in \mathbb{F}[X]$, where $c \in \mathbb{F}^\times$, $\sigma_1 \ge r$, and $|\sigma| \le d$. Fix the integers z_t such that this occurs.

By Lemma 3.12, 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 $|\sigma| \le d$ 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 $O(dL) = O\left(d^2(n^2+m^2)\right)$. Choose $z_v = \deg_w(\phi(g))+1 = O\left(d^2(n^2+m^2)\right)$. 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 $\mathrm{coeff}_{w^i}(h) = c\cdot(K_\sigma \mid K_\sigma)$. Finally, we have that

$$\deg_w(h) \le z_v \cdot O(d(n+m)) + d' \le O\left(d^2(n^2+m^2)\right)\cdot O(d(n+m)) + O\left(d^2(n^2+m^2)\right) = O\left(d^3(n^3+m^3)\right).$$

□

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

Theorem 3.15: Let $f(X) \in I^{\det}_{n,m,r}$ be a nonzero polynomial of degree d. Assume $|\mathbb{F}| \ge c_0 d^3(n^3+m^3)$, where $c_0 > 0$ is a large enough constant. Then, there exists a depth-three f-oracle circuit of size $O\left(n^2m^2d^3(n^3+m^3)\right) = \mathrm{poly}(n,m,d)$ computing $(K_\sigma \mid K_\sigma)(X)$, where $\sigma_1 \ge r$ and $|\sigma| \le d$. Furthermore, the top gate of this circuit is an addition gate, and the bottom layer consists of $O\left(nmd^3(n^3+m^3)\right)$ addition gates. The total number of gates and wires, excluding those between the bottom addition gates and the input gates, is $O\left(nmd^3(n^3+m^3)\right)$.[¶]

Proof: Let h be as in Lemma 3.14. 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 $MJ_n\widetilde{D}$ (resp. $\widetilde{D}'J_mN$) 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 $s \ge 0$, 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 $O\left(n^2m^2\right)$ 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 $O\left(n^2m^2\right)$.

Let $d_w = \deg_w(h)$. By Lemma 3.14, we have that $d_w = O\left(d^3(n^3+m^3)\right)$ and that $\mathrm{coeff}_{w^i}(h) = c\cdot(K_\sigma \mid K_\sigma)(X)$ for some integer $i \le d_w$, where $c \in \mathbb{F}^\times$, $\sigma_1 \ge r$ and $|\sigma| \le d$. As $|\mathbb{F}| \ge c_0 d^3(n^3+m^3)$, where $c_0 > 0$ is a large enough constant, we may assume $|\mathbb{F}| \ge d_w + 1$. Then by Lemma 2.29, we have a depth-three f-oracle circuit C of size $O\left(d_w(n^2m^2)\right) = O\left(n^2m^2d^3(n^3+m^3)\right)$ computing $\mathrm{coeff}_{w^i}(h) = c\cdot(K_\sigma \mid K_\sigma)$. The top gate of C is an addition gate, which connects to $d_w+1 = O\left(d^3(n^3+m^3)\right)$ f-gates on the middle layer. And these f-gates connect to $(d_w+1)nm = O\left(nmd^3(n^3+m^3)\right)$ addition gates on the bottom layer.

The above circuit C computes $c\cdot(K_\sigma \mid K_\sigma)(X)$. 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 $(K_\sigma \mid K_\sigma)(X)$. This proves the theorem. □

[¶]In the final circuit construction, these wires will be removed and replaced by wires connecting to fewer input gates (see Theorem 3.18). Hence we state the circuit size bound excluding these wires, which leads to a sharper bound for the final circuit.

3.2 Expressing Algebraic Branching Programs as Determinants The remainder of the proof follows [AF22], 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 lemma:

Lemma 3.16 ([AF22, Lemma 3.6], [Val79, Theorem 1]): Let $g(\overline{y}) \in \mathbb{F}[\overline{y}]$ and suppose g can be computed by an algebraic branching program on r vertices. Then there is an $r \times r$ matrix A over $\mathbb{F}[\overline{y}]$ whose entries are polynomials in $\overline{y}$ of degree at most 1 such that

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

Algebraic branching programs are closed under homogenization, as stated in the following lemma.

Lemma 3.17 ([AF22, Lemma 3.7]): Let $g(\overline{y}) \in \mathbb{F}[\overline{y}]$ 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 $\widehat{g}(\overline{y}, z)$ such that $g = \widehat{g}(\overline{y}, 1)$ and $\widehat{g}$ can be computed by an algebraic branching program on m vertices.

3.3 Computing the Determinant of a Matrix We will use Theorem 3.15 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 1.4. We start by proving the following more general theorem.

Theorem 3.18: Let $f(X) \in I^{\det}_{n,m,r}$ be a nonzero polynomial of degree d. Let $g(y_1, \ldots, y_\ell) \in \mathbb{F}[\overline{y}]$ 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 $O\left(nmd^4\ell r(n^3 + m^3)\right)$ defined over $\mathbb{F}$ such that

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

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

Proof: By Lemma 3.17, there is a homogeneous polynomial $\widehat{g}(\overline{y}, z) \in \mathbb{F}[\overline{y}, z]$ such that $\widehat{g}(\overline{y}, 1) = g(\overline{y})$ and $\widehat{g}(\overline{y}, z)$ 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 3.16, there is a matrix $A(\overline{y}, z) \in \mathbb{F}[\overline{y}, z]^{r \times r}$ such that

- $\det_r(A(\overline{y}, z)) = 1 + \widehat{g}(\overline{y}, z)$,
- $\det_i(A(\overline{y}, z)_{[i],[i]}) = 1$ for all $1 \leq i \leq r - 1$,

and all entries of $A(\overline{y},z)$ have degree at most 1 in $\overline{y}$ and z. Extend $A(\overline{y},z)$ to an $n\times m$ matrix by adding 1's to the main diagonal and 0's elsewhere.

By Theorem 3.15, there exists a depth-three f-oracle circuit C over $\mathbb{F}$ of size $O\left(n^2m^2d^3(n^3+m^3)\right)$ computing $(K_\sigma \mid K_\sigma)(X)$ such that $\sigma_1 \geq r$ and $|\sigma| \leq d$. Furthermore, the top gate of C is an addition gate, the bottom layer of C consists of $O\left(nmd^3(n^3+m^3)\right)$ addition gates, and the total number of gates and wires excluding the wires between the bottom addition gates and the input gates is $O\left(nmd^3(n^3+m^3)\right)$. Replacing the nm input gates of C by the $O(\ell)$ new input gates $\overline{y}$, z, and 1, and further connecting these gates to the $O\left(nmd^3(n^3+m^3)\right)$ bottom addition gates, we obtain a depth-three f-oracle circuit over $\mathbb{F}$ of size $O\left(nmd^3\ell(n^3+m^3)\right)$ computing

$$h(\overline{y},z) := (K_\sigma \mid K_\sigma)(A(\overline{y},z)) = (1+\widehat{g}(\overline{y},z))^t$$

where $t := |\{\, i \mid \sigma_i \geq r \,\}| \geq 1$. Note that $t \leq \widehat{\sigma}_1 \leq d$.

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

$$\begin{aligned} h(\delta\cdot\overline{y},\delta) &= (1+\widehat{g}(\delta\cdot\overline{y},\delta))^t \\ &= (1+\delta^{\deg(\widehat{g})}\widehat{g}(\overline{y},1))^t \\ &= (1+\delta^{\deg(\widehat{g})}g(\overline{y}))^t \\ &= \sum_{i=0}^{t}\binom{t}{i}\delta^{i\cdot\deg(\widehat{g})}g(\overline{y})^i = 1+\delta^{\deg(\widehat{g})}g(\overline{y})+\cdots. \end{aligned} \tag{12}$$

Then $\deg_\delta(h(\delta\cdot\overline{y},\delta)) \leq t\cdot\deg(\widehat{g}) \leq dr$. For each $\alpha\in\mathbb{F}$, we can construct from the depth-three f-oracle circuit computing $h(\overline{y},z)$ another f-oracle circuit C_α computing $h(\alpha\overline{y},\alpha)$, whose size is $O\left(nmd^3\ell(n^3+m^3)\right)$ and top gate is an addition gate. Also, as $|\mathbb{F}| \geq c_0d^3(n^3+m^3)$, where $c_0>0$ is a large enough constant, we may assume $|\mathbb{F}| \geq dr+1$. Therefore, by Lemma 2.29, we can compute $\mathrm{coeff}_{\delta^{\deg(\widehat{g})}}(h(\delta\cdot\overline{y},\delta)) = g(\overline{y})$ using a depth-three f-oracle circuit of size

$$O\left(\deg_\delta(h(\delta\cdot\overline{y},\delta))\cdot nmd^3\ell(n^3+m^3)\right) = O\left(nmd^4\ell r(n^3+m^3)\right).$$

Now suppose that $\mathrm{char}(\mathbb{F}) = p > 0$. 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 $t = p^kb$ 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 (12), we get that

$$h(\delta\cdot\overline{y},\delta) = \sum_{i=0}^{t}\binom{t}{i}\delta^{i\cdot\deg(\widehat{g})}g(\overline{y})^i = 1+b\cdot\delta^{\deg(\widehat{g})p^k}g(\overline{y})^{p^k}+\cdots. \tag{13}$$

Again, $\deg_\delta(h(\delta \cdot \overline{y}, \delta)) \leq t \cdot \deg(\widehat{g}) \leq dr$. For each $\alpha \in \mathbb{F}$, we can construct from the depth-three f-oracle circuit computing $h(\overline{y}, z)$ another f-oracle circuit C_α computing $h(\alpha\overline{y}, \alpha)$, whose size is $O\left(nmd^3\ell(n^3+m^3)\right)$ 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 $|\mathbb{F}| \geq dr+1$. Therefore, by Lemma 2.29, we have a depth-three f-oracle circuit of size $O\left(nmd^4\ell r(n^3+m^3)\right)$ computing $\operatorname{coeff}_{\delta^{\deg(\widehat{g})p^k}}(h(\delta \cdot \overline{y}, \delta)) = b \cdot g(\overline{y})^{p^k}$. By dividing the multipliers on the wires connecting to the top gate by b, this circuit computing $b \cdot g(\overline{y})^{p^k}$ can be turned into a depth-three f-oracle circuit with the same underlying graph that computes $g(\overline{y})^{p^k}$. □

The following corollaries are a debordering of the results [AF22, Corollary 3.9, Corollary 3.10] of Andrews and Forbes. In particular, we can use Theorem 3.18 to construct a small constant-depth f-oracle circuit for the determinant, which partially resolves Conjecture 1.2 posed by Grochow as stated before.

Corollary 3.19: Let $f(X) \in I^{\det}_{n,m,r}$ be a nonzero polynomial of degree d. Let $t = O\left(r^{1/3}\right)$ 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 $O\left(nmd^4rt^2(n^3+m^3)\right) \leq O\left(nmd^4r^{5/3}(n^3+m^3)\right)$ over $\mathbb{F}$ such that

- if $\operatorname{char}(\mathbb{F}) = 0$ then Φ computes $\det_t(Y)$, and
- if $\operatorname{char}(\mathbb{F}) = p > 0$ 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 [MV97, Theorem 2] construct an algebraic branching program on $O\left(t^3\right) \leq r$ vertices which computes $\det_t(Y)$. Then, the total number of variables in Y is $t^2 = O\left(r^{2/3}\right)$. The result then follows by applying Theorem 3.18. □

We can also apply Theorem 3.18 to other polynomials which are important in the setting of algebraic complexity.

Corollary 3.20: Let $f(X) \in I^{\det}_{n,m,r}$ be a nonzero polynomial of degree d. Let W, D be positive integers such that $W(D-1)+2 \leq r$ and let $Y = Y_1 \sqcup \cdots \sqcup Y_W$ be a set of indeterminates such that each Y_i is a $D \times D$ matrix of indeterminates. Let $\mathrm{IMM}_{W,D}$ be the iterated matrix multiplication polynomial, which is the entry in position $(1,1)$ of the matrix product $Y_1 \cdots Y_W$. 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 $O\left(nmd^4r(n^3+m^3)WD^2\right)$ defined over $\mathbb{F}$ such that

- if $\operatorname{char}(\mathbb{F}) = 0$ then Φ computes $\mathrm{IMM}_{W,D}(Y)$, and

- if $\mathrm{char}(\mathbb{F}) = p > 0$ then Φ computes $\mathrm{IMM}_{W,D}(Y)^{p^k}$ for some $k \leq \lfloor \log_p(d) \rfloor$.

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

Proof: We have that $\mathrm{IMM}_{W,D}(Y)$ has an algebraic branching program with $W(D-1)+2 \leq r$ vertices computing it. Then, the total number of variables in Y is WD^2. The result then follows by applying Theorem 3.18. □

4 Pfaffian Ideals

We will now mimic the determinantal results in Section 3 for the case of the ideal $I^{\mathrm{pfaff}}_{2n,2r}$ of $2r \times 2r$ principal Pfaffians of a $2n \times 2n$ skew-symmetric matrix. Our application of the straightening law in the skew-symmetric case (Corollary 2.22) will be to isolate a canonical bitableau from the expansion of nonzero $f \in I^{\mathrm{pfaff}}_{2n,2r}$. In particular, we will show that this can be done via a polynomial-sized depth-three f-oracle circuit using the isolation lemma (Corollary 2.27) as well as coefficient extraction (Lemma 2.29). This is in contrast to the proof of [AF22], where they use a Kronecker-type substitution in order to isolate terms.

Throughout, fix a field $\mathbb{F}$. Let n be a natural number, and for $1 \leq i < j \leq 2n$, let $x_{i,j}$ be indeterminates. Throughout this section, let $X = (x_{i,j})$ be a $2n \times 2n$ skew-symmetric matrix of variables so that for all $1 \leq i < j \leq 2n$ we have that $x_{j,i} := -x_{j,i}$ and for all $1 \leq i \leq 2n$ we have that $x_{i,i} := 0$. To maintain notation with the prior section, we will write $\mathbb{F}[X] = \mathbb{F}[x_{i,j} \mid 1 \leq i < j \leq 2n]$. Let $1 \leq r \leq n$ and define $I^{\mathrm{pfaff}}_{2n,2r}$ to be the ideal in $\mathbb{F}[X]$ generated by principal Pfaffians of size $2r$. As stated in Definition 2.18, we will assume that all partitions, tableaux, and bipfaffians of shape σ are such that every row of σ has even length. We will omit this assumption throughout this section. The proofs below are similar to the ones in Section 3 and as such some details may be omitted.

The following is proved in the same manner as Lemma 3.7 by studying the case of a single row, making use of Lemma 2.17, and then iterating that argument down each row.

Lemma 4.1 (c.f. [AF22, proof of Lemma 4.1]): Recall the definition of the elementary matrices $E_{i,j}$ from Definition 2.3. Let λ be a new indeterminate. Let S be a tableau, not necessarily standard, of shape σ. For $0 \leq h \leq h^j_i(S) - 1$, let $\mathcal{C}^h_{i \to j}(S)$ 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

$$[S](E_{i,j}(\lambda) X E_{i,j}(\lambda)^\top) = \pm\lambda^{h^j_i(S)}[\mathrm{Sub}_{i \to j}(S)](X) + \sum_{h=0}^{h^j_i(S)-1} \lambda^h \sum_{S' \in \mathcal{C}^h_{i \to j}(S)} \pm[S'](X). \tag{14}$$

4.1 Isolating One Term In this subsection, in addition to the variables $x_{i,j}$, where $i,j \in [2n]$, we introduce a new set of indeterminates $\Lambda = \{\lambda_{i,j} \mid 1 \le i < j \le 2n\}$. We have that $|\Lambda| = \binom{n}{2} = O\left(n^2\right)$.

Define $M \in \mathbb{F}[\Lambda]^{2n\times 2n}$ by

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

We order the elements of $\binom{[2n]}{2} = \{(i,j) \mid 1 \le i < j \le 2n\}$ such that $(i,j) \preceq (i',j')$ if either $i < i'$, or $i = i'$ and $j \le j'$. This induces a lexicographic order on $(\mathbb{Z}_{\ge 0})^{\binom{[2n]}{2}}$ which in turn induces a lexicographic term order on the monomials in the variables Λ via their degree vectors. We use M to obtain a polynomial in $\mathbb{F}[X,\Lambda]$ with some terms consisting of anti-canonical bipfaffians.

Lemma 4.2: Let $f(X) \in I^{\det}_{2n,2r}$ be a nonzero polynomial of degree d. Then $f(MXM^\top)$ can be expressed as a sum

$$f(MXM^\top) = \sum_{k\in A} \widetilde{c}_k \Lambda^{\overline{e}_k} \cdot [\overline{K}_{\sigma_k}](X) + \sum_{\ell \in A'} \widetilde{c}_\ell \Lambda^{\overline{e}_\ell} \cdot [S_\ell](X), \tag{15}$$

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 (15) have the form $c\Lambda^{\overline{e}} \cdot [S](X)$, where $c \in \mathbb{F}^\times$, $\overline{e} \in \{0,1,\ldots,d\}^{\binom{[2n]}{2}}$, and S has shape σ such that $\sigma_1 \ge 2r$ and $|\sigma| \le 2d$.

(3) For every $\ell \in A'$, there exists $k = k(\ell) \in A$ such that $\overline{e}_\ell$ is strictly smaller than $\overline{e}_k$ in the lexicographic order and the shape σ_ℓ of $[S_\ell]$ equals the shape σ_k.

(4) The triples $(\overline{e}_k, \sigma_k)$ are distinct, where k ranges over A.

Proof: By Corollary 2.22 and Proposition 2.23, we can expand $f(X)$ as a linear combination of standard bipfaffians over $\mathbb{F}$

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

where B is nonempty, each $c_k \in \mathbb{F}^\times$, and $[S_k](X)$ is a standard bipfaffian in $I^{\text{pfaff}}_{2n,2r}$ of shape σ_k such that $(\sigma_k)_1 \ge 2r$ and $|\sigma_k| \le 2d$, with these standard bipfaffians being distinct as k ranges over B. It follows that

$$f(MXM^\top) = \sum_{k\in B} c_k \cdot [S_k](MXM^\top).$$

For each $k \in B$, we expand the term $c_k \cdot [S_k](MXM^\top)$ by repeatedly applying Lemma 4.1. This expansion shows that $c_k \cdot [S_k](MXM^\top)$ equals $\pm c_k \Lambda^{\overline{e}_k} \cdot [\overline{K}_{\sigma_k}](X)$ with $\overline{e}_k = (h_{2n,i,j}(S_k))_{1\le i<j\le 2n} \in \{0,1,\ldots,d\}^{\binom{[2n]}{2}}$, plus some terms of the form $\pm\widetilde{c}_\ell \Lambda^{\overline{e}_\ell} \cdot [S_\ell](X)$, each with a new index ℓ, where

$\widetilde{c}_\ell = \pm c_k$, $[S_\ell](X)$ is a (not necessarily standard) bipfaffian of shape $\sigma_\ell = \sigma_k$, and $\overline{e}_\ell$ is strictly smaller than $\overline{e}_k$ in the lexicographic order. Note that as $\sigma_\ell = \sigma_k$, their first rows both have length at least $2r$, implying that $[S_\ell](X) \in I^{\text{pfaff}}_{2n,2r}$ by Proposition 2.23. Also note that $\overline{e}_\ell \in \{0,1,\ldots,d\}^{\binom{[2n]}{2}}$ since a substitution $i \mapsto j$ can be performed at most once per row, i.e., at most $(\widehat{\sigma_\ell})_1 \leq d$ times to any tableau of shape σ_ℓ. The fact that $(\widehat{\sigma_\ell})_1 \leq d$ follows from the fact that all non-empty rows of σ_ℓ have length ≥ 2 by Corollary 2.22. 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

$$f(MXM^\top) = \sum_{k\in A} \pm c_k \Lambda^{\overline{e}_k} \cdot [\overline{K}_{\sigma_k}](X) + \sum_{\ell \in A'} \widetilde{c}_\ell \Lambda^{\overline{e}_\ell} \cdot [S_\ell](X)$$

satisfying Items 1 to 3.

It remains to prove Item 4. Recall that as k ranges over A that the S_k are distinct. Assume to the contrary that there exist distinct $k_1, k_2 \in A$ such that $(\overline{e}_{k_1}, \sigma_{k_1}) = (\overline{e}_{k_2}, \sigma_{k_2})$. Then if $\sigma_{k_1} = \sigma_{k_2}$ we have that $\overline{K}_{\sigma_1} = \overline{K}_{\sigma_2}$. But then as $\overline{K}_{\sigma_1} = \overline{K}_{\sigma_2}$ and $\overline{e}_{k_1} = \overline{e}_{k_2}$, by Lemma 3.5 we have that $S_{k_1} = S_{k_2}$, a contradiction. □

Let $J_{2n} \in \mathbb{F}^{2n\times 2n}$ be the $2n \times 2n$ matrix with 1's along the anti-diagonal and 0's elsewhere. In particular, $J_{2n} = J_{2n}^\top$ and so $J_{2n}XJ_{2n}$ is still skew-symmetric.. Note that the map $X \mapsto J_{2n}XJ_{2n}$ maps the bipfaffian $[\overline{K}_\sigma](X) \mapsto [K_\sigma](X)$ for any partition σ.

Corollary 4.3: Let $f(X) \in I^{\text{det}}_{2n,2r}$ be a nonzero polynomial of degree d. Then $f(MJ_{2n}XJ_{2n}M^\top)$ can be expressed as a sum

$$f(MJ_{2n}XJ_{2n}M^\top) = \sum_{k\in A} \widetilde{c}_k \Lambda^{\overline{e}_k} \cdot [K_{\sigma_k}](X) + \sum_{\ell \in A'} \widetilde{c}_\ell \Lambda^{\overline{e}_\ell} \cdot [S_\ell](X), \tag{16}$$

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 (16) have the form $c\Lambda^{\overline{e}} \cdot [S](X)$, where $c \in \mathbb{F}^\times$, $\overline{e} \in \{0,1,\ldots,d\}^{\binom{[2n]}{2}}$, and S has shape σ such that $\sigma_1 \geq 2r$ and $|\sigma| \leq 2d$.

(3) For every $\ell \in A'$, there exists $k = k(\ell) \in A$ such that $\overline{e}_\ell$ is strictly smaller than $\overline{e}_k$ in the lexicographic order and the shape σ_ℓ of $[S_\ell]$ equals the shape σ_k.

(4) The triples $(\overline{e}_k, \sigma_k)$ are distinct, where k ranges over A.

Next, we introduce new variables $Y = \{y_1,\ldots,y_{2n}\}$. Define the diagonal matrix

$$D = \text{diag}(y_1,\ldots,y_{2n}) \in \mathbb{F}[Y]^{2n\times 2n}.$$

Note that $D = D^\top$ and that DXD is still skew-symmetric and so taking bipfaffians is still well defined.

Lemma 4.4: Let $[S](X)$ be a bideterminant of degree d. Then

$$[S](DXD) = Y^{\bar{s}}[S](X),$$

where $\bar{s} = (s_1, \ldots, s_{2n}) \in \{0, 1, \ldots, 2d\}^{2n}$, s_i is the number of times i appears in S, i.e., $s_1e_1 + \cdots + s_{2n}e_{2n}$ is the multidegree of $[S](X)$ with respect to the grading defined in Definition 2.24.

Proof: Reduce to the case in which S has only one row, and then use the multilinearity of the determinant and the fact that the Pfaffian is the square-root of the determinant. □

We will often simply say that $[S](X)$ in Lemma 4.4 has multidegree $\bar{s}$ (rather than writing it as $s_1e_1 + \cdots + s_ne_n$).

Next, we introduce another variable v and modify D:

$$\widetilde{D} = \operatorname{diag}(y_1v, y_2v^2 \ldots, y_{2n}v^{2n}) \in \mathbb{F}[Y, v]^{2n\times 2n}.$$

Note that $\widetilde{D} = \widetilde{D}^\top$ and that $\widetilde{D}X\widetilde{D}$ is still skew-symmetric and so taking bipfaffians is still well defined. The proof of the following lemma is similar to the one of Lemma 3.12 and is thus omitted.

Lemma 4.5: Let $[S](X)$ be a bipfaffian of degree d. Then

$$[S](\widetilde{D}X\widetilde{D}) = Y^{\bar{s}}v^{|S|} \cdot [S](X),$$

where $\bar{s}$ is the multidegree of $[S](X)$.

Lemma 4.6: Let $f(X) \in I_{2n,2r}^{\text{pfaff}}$ be a nonzero polynomial of degree d. Let $g = f(MJ_{2n}\widetilde{D}X\widetilde{D}J_{2n}M^\top) \in \mathbb{F}[X, \Lambda, Y, v]$. View g as a univariate polynomial in v with coefficients in $\mathbb{F}[X, \Lambda, Y]$, and write $g = \sum_i \operatorname{coeff}_{v^i}(g)v^i$, where $\operatorname{coeff}_{v^i}(g) \in \mathbb{F}[X, \Lambda, Y]$ denotes the coefficient of v^i in g. Choose the smallest integer $d_{\min} = O(dn)$ such that $\operatorname{coeff}_{v^{d_{\min}}}(g) \neq 0$. Then $d_{\min} = |K_\sigma|$ for some shape σ with $|\sigma| \leq 2d$ and we may write $\operatorname{coeff}_{v^{d_{\min}}}(g)$ as a finite sum

$$\operatorname{coeff}_{v^{d_{\min}}}(g) = \sum_{k\in I} c_k\Lambda^{\bar{e}_k}Y^{\bar{s}_k} \cdot [K_{\sigma_k}](X),$$

such that the following hold:

(1) For each $k \in I$, $c_k \in \mathbb{F}^\times$, $(\sigma_k)_1 \geq 2r$, and $|\sigma_k| \leq 2d$.

(2) The tuples $(\bar{e}_k, \bar{s}_k)$ are distinct, where k ranges over I.

Proof: Consider the expansion

$$f(MJ_{2n}XJ_{2n}M^\top) = \sum_{k\in A} \widetilde{c}_k\Lambda^{\bar{e}_k} \cdot [K_{\sigma_k}](X) + \sum_{\ell\in A'} \widetilde{c}_\ell\Lambda^{\bar{e}_\ell} \cdot [S_\ell](X),$$

given by Corollary 4.3. Then we have that

$$\begin{aligned} g &= \sum_{k\in A} \widetilde{c}_k \Lambda^{\bar{e}_k} \cdot [K_{\sigma_k}](\widetilde{D}X\widetilde{D}) + \sum_{\ell\in A'} \widetilde{c}_\ell \Lambda^{\bar{e}_\ell} \cdot [S_\ell](\widetilde{D}X\widetilde{D}) \\ &= \sum_{k\in A} \widetilde{c}_k \Lambda^{\bar{e}_k} Y^{\bar{s}_k} \nu^{\left|K_{\sigma_k}\right|} \cdot [K_{\sigma_k}](X) + \sum_{\ell\in A'} \widetilde{c}_\ell \Lambda^{\bar{e}_\ell} Y^{\bar{s}_\ell} \nu^{|S_\ell|} \cdot [S_\ell](X), \end{aligned} \tag{17}$$

where for $k \in A$, $\bar{s}_k$ is the multidegree of $[K_{\sigma_k}](X)$, and for $\ell \in B$, $\bar{s}_\ell$ is the multidegree of $[S_\ell](X)$. Here, the second equality holds by Lemma 4.5.

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

For any $k \in A$, consider the term $\widetilde{c}_k \Lambda^{\bar{e}_k} Y^{\bar{s}_k} \nu^{\left|K_{\sigma_k}\right|} \cdot [K_{\sigma_k}](X)$ in Equation (17). It is homogeneous of degree $\left|K_{\sigma_k}\right| \geq \left|K_{\sigma_{k_0}}\right| = d_0$ with respect to ν by the minimality of $\left|K_{\sigma_{k_0}}\right|$, and contributes to $\operatorname{coeff}_{\nu^{d_0}}(g)$ if and only if $\left|K_{\sigma_k}\right| = \left|K_{\sigma_{k_0}}\right|$. Even if it can potentially contribute to $\operatorname{coeff}_{\nu^{d_0}}(g)$, its (multi)degree $(\bar{e}_k, \bar{s}_k)$ in the variables Λ and Y is different from that of the term indexed by k_0 unless $k = k_0$. To see this, suppose $k \neq k_0$. Then $(\bar{e}_k, \sigma_k) \neq (\bar{e}_{k_0}, \sigma_{k_0})$. If $\sigma_k = \sigma_{k_0}$, then $\bar{e}_k \neq \bar{e}_{k_0}$. On the other hand, if $\sigma_k \neq \sigma_{k_0}$, then $\bar{s}_k \neq \bar{s}_{k_0}$ by Lemma 2.25. Thus, we always have that

$$(\bar{e}_k, \bar{s}_k) \neq (\bar{e}_{k_0}, \bar{s}_{k_0}).$$

Now consider $\ell \in B$ and the term $\mathfrak{m}_\ell := \widehat{c}_\ell \Lambda^{\bar{e}_\ell} Y^{\bar{s}_\ell} \nu^{|S_\ell|} \cdot [S_\ell](X)$ in Equation (17). The degree of $\mathfrak{m}_\ell$ in ν is $|S_\ell|$. Let $k = k(\ell)$ as in Corollary 4.3. Then by Corollary 4.3 (3), S_ℓ has shape $\sigma_\ell = \sigma_k$. Note that among all bipfaffians $[S]$ of shape σ, the quantity $|S|$ is minimized when, and only when, $[S] = [K_\sigma]$. Thus, we have

$$|S_\ell| \geq \left|K_{\sigma_k}\right| \geq \left|K_{\sigma_{k_0}}\right| = d_0.$$

and $\deg_\nu(\mathfrak{m}_\ell) = |S_\ell| = d_0$ if and only if $[S_\ell] = [K_{\sigma_k}]$ and $\left|K_{\sigma_k}\right| = \left|K_{\sigma_{k_0}}\right|$. Even though this can happen, when it happens we have that $\bar{e}_k$ is smaller than or equal to $\bar{e}_{k_0}$ in the lexicographic order by the choice of k_0, noting that $\left|K_{\sigma_k}\right| = \left|K_{\sigma_{k_0}}\right|$. And by Corollary 4.3 (3), $\bar{e}_\ell$ is strictly smaller than $\bar{e}_k$ in the lexicographic order. Overall, either $\deg_\nu(\mathfrak{m}_\ell) > d_0$, or $(\bar{e}_\ell, \bar{s}_\ell) \neq (\bar{e}_{k_0}, \bar{s}_{k_0})$.

By the above analysis, the term $\widehat{c}_{k_0} \Lambda^{\bar{e}_{k_0}} Y^{\bar{s}_{k_0}} \nu^{\left|K_{\sigma_{k_0}}\right|} \cdot [K_{\sigma_{k_0}}](X)$ is not canceled by other terms contributing to $\operatorname{coeff}_{\nu^{d_0}}(g)$ due to the uniqueness of its (multi)degree $(\bar{e}_{k_0}, \bar{s}_{k_0})$ in Λ and Y. Thus $\operatorname{coeff}_{\nu^{d_0}}(g) \neq 0$. The above analysis also shows that $\operatorname{coeff}_{\nu^i}(g) = 0$ for $i < d_0$. Thus, $d_0 = d_{\min}$. Note that $d_{\min} = \left|K_{\sigma_{k_0}}\right| \leq O(dn)$ as each of the at most $2d$ boxes in $K_{\sigma_{k_0}}$ have entry at most $2n$.

Moreover, the above analysis shows that any term that contributes to $\operatorname{coeff}_{\nu^{d_0}}(g)$ contains a bipfaffian of the form $[K_\sigma](X)$. We then merge the terms contributing to $\operatorname{coeff}_{\nu^{d_0}}(g)$ with the same (multi)degree in Λ and Y. When we merge two terms $\widehat{c}_k \Lambda^{\bar{e}_k} Y^{\bar{s}_k} \nu^{d_0} \cdot [K_{\sigma_k}](X)$ and $\widehat{c}_{k'} \Lambda^{\bar{e}_{k'}} Y^{\bar{s}_{k'}} \nu^{d_0} \cdot [K_{\sigma_{k'}}](X)$ with

$(\bar{e}_k, \bar{s}_k) = (\bar{e}_{k'}, \bar{s}_{k'})$, we always have $[K_{\sigma_k}] = [K_{\sigma_{k'}}]$. This follows from Lemma 2.25 and the fact that $\bar{s}_k$ is the multidegree of $[K_{\sigma_k}](X)$ and $\bar{s}_{k'}$ is the multidegree of $[K_{\sigma_{k'}}]$. Thus, merging the two terms yields a scalar multiple of both.

After merging/canceling terms, we can write $\operatorname{coeff}_{v^{d_{\min}}}(g) = \operatorname{coeff}_{v^{d_0}}(g)$ in the form of Equation (10) such that Item 2 holds. Furthermore, Item 1 holds as well by Corollary 4.3 (2) and Proposition 2.23.

□

Lemma 4.6 helps us separate a collection of terms solely containing canonical bipfaffians. The next lemma further applies the isolation lemma to single out one term from this collection.

Lemma 4.7: Let $f(X) \in I^{\text{pfaff}}_{2n,2r}$ be a nonzero polynomial of degree d. Let $g = f(MJ_{2n}\widetilde{D}X\widetilde{D}J_{2n}M^\top) \in \mathbb{F}[X, \Lambda, Y, v]$. Then there exist integers $z_t = O(dn^2)$ for each variable $t \in \Lambda \sqcup Y$, and an integer $z_v = O(d^2n^2)$ such that for the two variable substitution maps

$$\phi : t \mapsto w^{z_t} \quad \text{for } t \in \Lambda \sqcup Y$$

and

$$\psi : v \mapsto w^{z_v},$$

we have that $h := (\psi \circ \phi)(g) \in \mathbb{F}[X, w]$ has $\deg_w(h) = O(d^3n^3)$ such that $\operatorname{coeff}_{w^i}(h) = c \cdot [K_\sigma]$ for some integer $i \le \deg_w(h)$, where $c \in \mathbb{F}^\times$, $\sigma_1 \ge 2r$ and $|\sigma| \le 2d$.

Proof: Consider the finite sum from Lemma 4.6:

$$\operatorname{coeff}_{v^{d_{\min}}}(g) = \sum_{k \in I} c_k \Lambda^{\bar{e}_k} Y^{\bar{s}_k} \cdot [K_{\sigma_k}](X)$$

The coordinates of $\bar{e}_k$ and $\bar{s}_k$ are in $\{0, 1, \ldots, d\}$ and $\{0, 1, \ldots, 2d\}$ respectively for each $k \in I$ by Corollary 4.3 (2) and Lemma 4.5. Choose a sufficiently large $L = \Theta(()dn^2)$, and pick integers z_t independently and uniformly at random from $\{0, 1, \ldots, L\}$, where $t \in \Lambda \sqcup Y$. Then by Corollary 2.27, 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 $c \cdot [K_\sigma](X) \in \mathbb{F}[X]$, where $c \in \mathbb{F}^\times$, $\sigma_1 \ge 2r$, and $|\sigma| \le 2d$. Fix the integers z_t such that this occurs.

By Lemma 4.5, the degree of $\phi(g)$ in v is at most $O(dn)$ as each of the at most $2d$ boxes has entry at most $2n$. The degree of $\phi(g)$ in w is bounded by $O(dL) = O(d^2n^2)$. Choose $z_v = \deg_w(\phi(g)) + 1 = O(d^2n^2)$. 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 $\operatorname{coeff}_{w^i}(h) = c \cdot [K_\sigma](X)$. Finally, we have that

$$\deg_w(h) \le z_v \cdot O(dn) + d' \le O(d^2n^2) \cdot O(dn) + O(d^2n^2) = O(d^3n^3).$$

□

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

Theorem 4.8: Let $f(X) \in I^{\text{pfaff}}_{2n,2r}$ be a nonzero polynomial of degree d. Assume $|\mathbb{F}| \geq c_0 d^3 n^3$, where $c_0 > 0$ is a large enough constant. Then there exists a depth-three f-oracle circuit of size $O\left(d^3n^7\right) = \text{poly}(n,d)$ computing $[K_\sigma](X)$, where $\sigma_1 \geq 2r$ and $|\sigma| \leq 2d$. Furthermore, the top gate of this circuit is an addition gate, and the bottom layer consists of $O\left(d^3n^5\right)$ addition gates. The total number of gates and wires excluding the wires between the bottom addition gates and the input gates is $O\left(d^3n^5\right)$.

Proof: Let h be as in Lemma 4.7. Let $\alpha \in \mathbb{F}$ be arbitrary. By construction, $h(X,\alpha)$ equals $f(M_\alpha X M_\alpha^\top)$, where M_α is obtained from $MJ_{2n}\widetilde{D}$ by substituting powers of α for the variables Λ, Y, and ν. 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 $X \mapsto M_\alpha X M_\alpha^\top$ 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 $O\left(n^2\right)$ addition gates and $O\left(n^4\right)$ wires at the bottom layer computing the $4n^2$ entries of $M_\alpha X M_\alpha^\top$. The top gate is an f-gate connecting to the n^2 addition gates via n^2 wires. Thus, the size of C_α is $O\left(n^4\right)$.

Let $d_w = \deg_w(h)$. By Lemma 4.7, we have that $d_w = O\left(d^3n^3\right)$ and that $\text{coeff}_{w^i}(h) = c \cdot [K_\sigma]$ for some integer $i \leq \deg_w(h)$, where $c \in \mathbb{F}^\times$, $\sigma_1 \geq 2r$ and $|\sigma| \leq 2d$. As $|\mathbb{F}| \geq c_0 d^3 n^3$, where $c_0 > 0$ is a large enough constant, we may assume $|\mathbb{F}| \geq d_w + 1$. Then by Lemma 2.29, we have a depth-three f-oracle circuit C of size $O\left(d_w n^4\right) = O\left(d^3n^7\right)$ computing $\text{coeff}_{w^i}(h) = c \cdot (K_\sigma \mid K_\sigma)$. The top gate of C is an addition gate, which connects to $d_w + 1 = O\left(d^3n^3\right)$ f-gates on the middle layer. Then, these f-gates connect to $(d_w+1)n^2 = O\left(d^3n^5\right)$ addition gates on the bottom layer.

The above circuit C computes $c \cdot [K_\sigma]$. But by dividing the constants 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 $[K_\sigma](X)$. This proves the theorem. □

4.2 Expressing Algebraic Branching Programs as Pfaffians of a Skew-Symmetric Matrix

The remainder of the proof follows [AF22], 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 lemma:

Lemma 4.9 ([AF22, Lemma 4.3]): Let A be an $n \times n$ matrix. Then there is a $2n \times 2n$ skew-symmetric matrix M such that for all $k \in [n]$, we have that $\text{pfaff}_{2k}(M_{[2k],[2k]}) = \pm \det_k(A_{[k],[k]})$.

4.3 Computing the Pfaffian of a Skew-Symmetric Matrix We will use Theorem 4.8 to obtain a constant-depth algebraic circuit of size $\text{poly}(n, \deg(f))$ with f-oracle gates that computes

the Pfaffian of a skew-symmetric symbolic matrix, thereby resolving the analogue of Question 1.4 for the Pfaffian case. We start by proving the following more general theorem.

Theorem 4.10: Let $f(X) \in I_{2n,2r}^{\text{pfaff}}$ be a nonzero polynomial of degree d. Let $g(y_1,\dots,y_\ell) \in \mathbb{F}[\overline{y}]$ be a polynomial computable by an algebraic branching program with at most r vertices. Assume $|\mathbb{F}| \geq c_0 d^3 n^3$, where $c_0 > 0$ is a large enough constant. Then there is a depth-three f-oracle circuit Φ of size $O\left(d^4 \ell n^5 r\right)$ defined over $\mathbb{F}$ such that

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

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

Proof: By Lemma 3.17, there is a homogeneous polynomial $\widehat{g}(\overline{y},z) \in \mathbb{F}[\overline{y},z]$ such that $\widehat{g}(\overline{y},1) = g(\overline{y})$ and $\widehat{g}(\overline{y},z)$ 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 3.16, there is a matrix $A(\overline{y},z) \in \mathbb{F}[\overline{y},z]^{r\times r}$ such that

- $\det_r(A(\overline{y},z)) = 1 + \widehat{g}(\overline{y},z)$,
- $\det_i(A(\overline{y},z)_{[i],[i]}) = 1$ for all $1 \leq i \leq r-1$,

and all entries of $A(\overline{y},z)$ have degree at most 1 in $\overline{y}$ and z. Extend $A(\overline{y},z)$ to an $n \times n$ matrix by adding 1's to the main diagonal and 0's elsewhere. Then, by Lemma 4.9, there exists a $2n \times 2n$ skew-symmetric matrix M such that $\text{pfaff}_{2k}(M_{[2k],[2k]}) = \pm \det_k(A_{[k],[k]})$ for all $1 \leq k \leq n$.

By Theorem 4.8, there exists a depth-three f-oracle circuit C over $\mathbb{F}$ of size $O\left(d^3 n^7\right)$ computing $[K_\sigma](X)$ such that $\sigma_1 \geq 2r$ and $|\sigma| \leq 2d$. Furthermore, the top gate of C is an addition gate, the bottom layer of C consists of $O\left(d^3 n^5\right)$ addition gates, and the total number of gates and wires excluding the wires between the bottom addition gates and the input gates is $O\left(d^3 n^5\right)$. Replacing the n^2 input gates of C by the $O(\ell)$ new input gates $\overline{y}$, z, and 1, and further connecting these gates to the $O\left(d^3 n^5\right)$ bottom addition gates, we obtain a depth-three f-oracle circuit over $\mathbb{F}$ of size $O\left(d^3 \ell n^5\right)$

computing

$$\begin{aligned} h(\overline{y},z) &:= [K_\sigma](A(\overline{y},z)) \\ &= \prod_{i=1}^{\widehat{\sigma}_1} \mathrm{pfaff}_{\sigma_i}(A(\overline{y},z)_{[\sigma_i],[\sigma_i]}) \\ &= \pm \prod_{i=1}^{\widehat{\sigma}_1} \det_{\sigma_i/2}(A(\overline{y},z)_{[\sigma_i/2],[\sigma_i/2]}) \\ &= \pm \prod_{i;\ \sigma_i \geq 2r} \det_{\sigma_i/2}(A(\overline{y},z)_{[\sigma_i/2],[\sigma_i/2]}) \cdot \prod_{i;\ \sigma_i < 2r} \det_{\sigma_i/2}(A(\overline{y},z)_{[\sigma_i/2],[\sigma_i/2]}) \\ &= \pm(1+\widehat{g}(\overline{y},z))^t \end{aligned}$$

where $t := |\{\, i \mid \sigma_i \geq 2r \,\}| \geq 1$. Note that $t \leq \widehat{\sigma}_1 \leq d$.

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

$$\begin{aligned} h(\delta\cdot\overline{y},\delta) &= \pm(1+\widehat{g}(\delta\cdot\overline{y},\delta))^t \\ &= \pm(1+\delta^{\deg(\widehat{g})}\widehat{g}(\overline{y},1))^t \\ &= \pm(1+\delta^{\deg(\widehat{g})}g(\overline{y}))^t \\ &= \pm\sum_{i=0}^{t}\binom{t}{i}\delta^{i\cdot\deg(\widehat{g})}g(\overline{y})^i = \pm\left(1+\delta^{\deg(\widehat{g})}t\cdot g(\overline{y})+\cdots\right). \end{aligned} \tag{18}$$

Then $\deg_\delta(h(\delta\cdot\overline{y},\delta)) \leq t\cdot\deg(\widehat{g}) \leq dr$. For each $\alpha \in \mathbb{F}$, we can construct from the depth-three f-oracle circuit computing $h(\overline{y},z)$ another f-oracle circuit C_α computing $h(\alpha\overline{y},\alpha)$, whose size is $O\left(d^3\ell n^5\right)$ and top gate is an addition gate. Also, as $|\mathbb{F}| \geq c_0 d^3 n^3$, where $c_0 > 0$ is a large enough constant, we may assume $|\mathbb{F}| \geq dr+1$. Therefore, by Lemma 2.29, we can compute $\mathrm{coeff}_{\delta^{\deg(\widehat{g})}}(h(\delta\cdot\overline{y},\delta)) = \pm t\cdot g(\overline{y})$ using a depth-three f-oracle circuit of size

$$O\left(\deg_\delta(h(\delta\cdot\overline{y},\delta))\cdot d^3\ell n^5\right) = O\left(d^4\ell n^5 r\right).$$

Dividing the constants on the incoming wires to the top addition gate from Lemma 2.29 by $\pm t$, we get a circuit using the same underlying graph computing $g(\overline{y})$.

Now suppose that $\mathrm{char}(\mathbb{F}) = p > 0$. 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 (18), we get that

$$h(\delta\cdot\overline{y},\delta) = \sum_{i=0}^{t}\binom{t}{i}\delta^{i\cdot\deg(\widehat{g})}g(\overline{y})^i = \pm(1+b\cdot\delta^{\deg(\widehat{g})p^k}g(\overline{y})^{p^k}+\cdots). \tag{19}$$

Again, $\deg_\delta(h(\delta \cdot \overline{y}, \delta)) \leq t \cdot \deg(\widehat{g}) \leq dr$. For each $\alpha \in \mathbb{F}$, we can construct from the depth-three f-oracle circuit computing $h(\overline{y}, z)$ another f-oracle circuit C_α computing $h(\alpha\overline{y}, \alpha)$, whose size is $O\left(d^3\ell n^5\right)$ and top gate is an addition gate. Also, as $|\mathbb{F}| \geq c_0 d^3 n^3$, where $c_0 > 0$ is a large enough constant, we may assume $|\mathbb{F}| \geq dr + 1$. By Lemma 2.29, we have a depth-three f-oracle circuit of size $O\left(d^4\ell n^5 r\right)$ computing $\operatorname{coeff}_{\delta^{\deg(\widehat{g})p^k}}(h(\delta \cdot \overline{y}, \delta)) = \pm \cdot b \cdot g(\overline{y})^{p^k}$. By dividing the constants on the wires connecting to the top gate by $\pm b$, this circuit computing $b \cdot g(\overline{y})^{p^k}$ can be turned into a depth-three f-oracle circuit with the same underlying graph that computes $g(\overline{y})^{p^k}$. □

The following corollary is a debordering of the result [AF22, Corollary 4.5] of Andrews and Forbes.

Corollary 4.11: Let $f(X) \in I^{\text{pfaff}}_{2n,2r}$ be a nonzero polynomial of degree d. Let $t \leq O\left(\sqrt[3]{r}\right)$ and let Y be a $t \times t$ matrix of indeterminates. Assume $|\mathbb{F}| \geq c_0 d^3 n^3$, where $c_0 > 0$ is a large enough constant. Then there is a depth-three f-oracle circuit Φ of size $O\left(d^4 t^2 n^5 r\right) \leq O\left(d^4 n^5 r^{5/3}\right)$ defined over $\mathbb{F}$ such that

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

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

Proof: Mahajan, Subramany, and Vinay [MSV04, Theorem 12] construct an algebraic branching program on $O\left(t^3\right) \leq r$ vertices which computes $\operatorname{pfaff}_t(Y)$. Then, the total number of variables is $t^2 \leq O\left(r^{2/3}\right)$. The result then follows by applying Theorem 4.10. □

5 Conclusions and Open Questions

In this work, we showed that for any nonzero $f \in I^{\det}_{n,m,r}$ of polynomial degree, the $t \times t$ determinant with $t = \Theta\left(r^{1/3}\right)$ 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 [AF22]. 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 1.5, 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 1.2). 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 [AF22], are proved only over fields of characteristic zero or sufficiently large positive characteristic The difficulty in small characteristic is that in Theorem 3.18, the f-oracle circuit Φ does not compute $g(\overline{y})$ directly, but only a power of $g(\overline{y})$. 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 [And20]. This obstacle is closely related to the fact that the celebrated superpolynomial lower bound for constant-depth algebraic circuits in [LST25] 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 [For24; Beh+25]. Determining whether our results, and those of [AF22], 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 $x_{i,j} = x_{j,i}$), though we leave this for future work. As mentioned in the introduction, determinantal and Pfaffian ideals can all be studied within a unified framework known as Standard Monomial Theory [LR08; Ses16]. The key observation is that the corresponding determinantal varieties can be realized as affine open subsets of certain Schubert varieties. With this connection in place, one can develop the theory—including standard monomial bases and straightening laws—on these Schubert varieties and then restrict to the affine open subsets to obtain the desired statements about the determinantal ideals. As noted in [Mus03], 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.

Acknowledgments

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.

References

[AF22] 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. 2022, pp. 389–402. DOI: 10.1145/3519935.3520025.

[AMS10] Vikraman Arvind, Partha Mukhopadhyay, and Srikanth Srinivasan. "New Results on Noncommutative and Commutative Polynomial Identity Testing". In: *computational complexity* 19.4 (2010), pp. 521–558. DOI: 10.1007/s00037-010-0299-8.

[And20] Robert Andrews. "Algebraic Hardness versus Randomness in Low Characteristic". In: *35th Computational Complexity Conference (CCC 2020)*. Leibniz International Proceedings in Informatics (LIPIcs). Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2020, 37:1–37:32. DOI: 10.4230/LIPIcs.CCC.2020.37.

[BC03] Winfried Bruns and Aldo Conca. "Gröbner Bases and Determinantal Ideals". In: *Commutative Algebra, Singularities and Computer Algebra*. Springer Netherlands, 2003, pp. 9–66. DOI: 10.1007/978-94-007-1092-4_2.

[BDS24] 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*. 2024, pp. 130–140. DOI: 10.1145/3618260.3649743.

[Beh+25] Amik Raj Behera, Nutan Limaye, Varun Ramanathan, and Srikanth Srinivasan. *New Bounds for the Ideal Proof System in Positive Characteristic*. 2025. arXiv: 2506.16397.

[Ben+92] Shai Ben-David, Benny Chor, Oded Goldreich, and Michael Luby. "On the Theory of Average Case Complexity". In: *Journal of Computer and System Sciences* 44.2 (1992), pp. 193–219. DOI: 10.1016/0022-0000(92)90019-F.

[Bha+25] Somnath Bhattacharjee, Mrinal Kumar, Shanthanu S. Rai, Varun Ramanathan, Ramprasad Saptharishi, and Shubhangi Saraf. *Closure Under Factorization From a Result of Furstenberg*. 2025. arXiv: 2506.23214.

[BSV20] Vishwas Bhargava, Shubhangi Saraf, and Ilya Volkovich. "Deterministic Factorization of Sparse Polynomials with Bounded Individual Degree". In: *Journal of the ACM* 67.2 (2020), 8:1–8:28. DOI: 10.1145/3365667.

[Bür00] Peter Bürgisser. *Completeness and Reduction in Algebraic Complexity Theory*. Springer, 2000. DOI: 10.1007/978-3-662-04179-6.

[Bür04] Peter Bürgisser. "The Complexity of Factors of Multivariate Polynomials". In: *Foundations of Computational Mathematics* 4.4 (2004), pp. 369–396. DOI: 10.1007/s10208-002-0059-5.

[BV88] Winfried Bruns and Udo Vetter. *Determinantal Rings*. Springer, 1988. DOI: 10.1007/BFb0080378.

[CKS19] Chi-Ning Chou, Mrinal Kumar, and Noam Solomon. "Closure Results for Polynomial Factorization". In: *Theory of Computing* 15.1 (2019), pp. 1–34. DOI: DOI:10.4086/toc.2019.v015a013.

[dCEP80] Corrado de Concini, David Eisenbud, and Claudio Procesi. "Young Diagrams and Determinantal Varieties". In: *Inventiones mathematicae* 56.2 (1980), pp. 129–165. DOI: 10.1007/BF01392548.

[dCEP82] Corrado de Concini, David Eisenbud, and Claudio Procesi. *Hodge Algebras*. Astérisque 91. Société mathématique de France, 1982. URL: https://www.numdam.org/item/AST_1982__91__1_0/.

[dCP76] Corrado de Concini and Claudio Procesi. "A Characteristic Free Approach to Invariant Theory". In: *Advances in Mathematics* 21.3 (1976), pp. 330–354. ISSN: 0001-8708. DOI: 10.1016/S0001-8708(76)80003-5.

[DDS22] 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)*. IEEE. 2022, pp. 92–103. DOI: 10.1109/FOCS52979.2021.00018.

[DRS74] Peter Doubilet, Gian-Carlo Rota, and Joel Stein. "On the Foundations of Combinatorial Theory: IX Combinatorial Methods in Invariant Theory". In: *Studies in Applied Mathematics* 53.3 (1974), pp. 185–216. DOI: 10.1002/sapm1974533185.

[DSS22] Pranjal Dutta, Nitin Saxena, and Amit Sinhababu. "Discovering the Roots: Uniform Closure Results for Algebraic Classes Under Factoring". In: *Journal of the ACM* 69.3 (2022), pp. 1–39. DOI: 10.1145/3510359.

[Dut+24] Pranjal 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). Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2024, 30:1–30:15. DOI: 10.4230/LIPIcs.STACS.2024.30.

[FGT19] Stephen Fenner, Rohit Gurjar, and Thomas Thierauf. "Bipartite Perfect Matching Is in Quasi-NC". In: *SIAM Journal on Computing* 50.3 (2019), STOC16-218–STOC16-235. DOI: 10.1137/16M1097870.

[For24] 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). Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2024, pp. 31–1. DOI: 10.4230/LIPIcs.CCC.2024.31.

[GGR24] Sumanta Ghosh, Rohit Gurjar, and Roshan Raj. "A Deterministic Parallel Reduction from Weighted Matroid Intersection Search to Decision". In: *Algorithmica* 86.4 (2024), pp. 1057–1079. DOI: 10.1137/1.9781611977073.44.

[Gro20] Joshua A. Grochow. “Complexity in Ideals of Polynomials: Questions on Algebraic Complexity of Circuits and Proofs”. In: *Bulletin of the European Association for Theoretical Computer Science* 131 (2020). URL: http://smtp.eatcs.org/index.php/beatcs/article/view/620.

[GT20] Rohit Gurjar and Thomas Thierauf. “Linear Matroid Intersection Is in Quasi-NC”. In: *computational complexity* 29.2 (2020), p. 9. DOI: 10.1007/s00037-020-00200-z.

[HT92] Jürgen Herzog and Ngô Viêt Trung. “Gröbner Bases and Multiplicity of Determinantal and Pfaffian Ideals”. In: *Advances in Mathematics* 96.1 (1992), pp. 1–37. DOI: 10.1016/0001-8708(92)90050-U.

[HvMM24] Ivan Hu, Dieter van Melkebeek, and Andrew Morgan. “Polynomial Identity Testing via Evaluation of Rational Functions”. In: *Theory of Computing* 20.1 (2024). DOI: http://dx.doi.org/10.4086/toc.2024.v020a001.

[Kal86] Erich Kaltofen. “Uniform Closure Properties of P-Computable Functions”. In: *Proceedings of the 18th Annual ACM Symposium on Theory of Computing*. 1986, pp. 330–337. DOI: 10.1145/12130.12163.

[Kal87] 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*. 1987, pp. 443–452. DOI: 10.1145/28395.28443.

[Kal89] Erich Kaltofen. “Factorization of Polynomials Given by Straight-Line Programs”. In: *Randomness and Computation, Volume 5 of Advances in Computing Research*. 1989, pp. 375–412.

[KS01] 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*. 2001, pp. 216–223. DOI: 10.1145/380752.380801.

[LL89] Thomas Lehmkuhl and Thomas Lickteig. “On the Order of Approximation in Approximative Triadic Decompositions of Tensors”. In: *Theoretical computer science* 66.1 (1989), pp. 1–14. DOI: 10.1016/0304-3975(89)90141-2.

[LR08] Venkatramani Lakshmibai and Komaranapuram N. Raghavan. *Standard Monomial Theory: Invariant Theoretic Approach*. Springer, 2008. DOI: 10.1007/978-3-540-76757-2.

[LST25] Nutan Limaye, Srikanth Srinivasan, and Sébastien Tavenas. “Superpolynomial Lower Bounds Against Low-Depth Algebraic Circuits”. In: *Journal of the ACM* 72.4 (2025), pp. 1–35. DOI: 10.1145/3734215.

[MSV04] Meena Mahajan, P.R. Subramanya, and V. Vinay. “The Combinatorial Approach Yields an NC Algorithm for Computing Pfaffians”. In: *Discrete Applied Mathematics* 143.1-3 (2004), pp. 1–16. DOI: 10.1016/j.dam.2003.12.001.

[Mus03] Chitikila Musili. “The Development of Standard Monomial Theory-I”. In: *A Tribute to C. S. Seshadri: Perspectives in Geometry and Representation Theory*. Springer, 2003, pp. 385–420. DOI: 10.1007/978-93-86279-11-8_24.

[MV97] Meena Mahajan and V. Vinay. *Determinant: Combinatorics, Algorithms, and Complexity*. Tech. rep. 5. Institute of Mathematical Sciences India, 1997.

[MVV87] Ketan Mulmuley, Umesh V. Vazirani, and Vijay V. Vazirani. “Matching is as Easy as Matrix Inversion”. In: *Combinatorica* 7.1 (1987), pp. 105–113. DOI: 10.1007/BF02579206.

[NW94] Noam Nisan and Avi Wigderson. “Hardness vs Randomness”. In: *Journal of computer and System Sciences* 49.2 (1994), pp. 149–167. DOI: 10.1016/S0022-0000(05)80043-1.

[Oli16] Rafael Oliveira. “Factors of Low Individual Degree Polynomials”. In: *computational complexity* 25.2 (2016), pp. 507–561. DOI: 10.1007/s00037-016-0130-2.

[Sap21] Ramprasad Saptharishi. *A Survey of Lower Bounds in Arithmetic Circuit Complexity*. Version 9.0.3. July 2021. URL: https://github.com/dasarpmar/lowerbounds-survey/releases.

[Ses16] C. S. Seshadri. *Introduction to the Theory of Standard Monomials*. Second Edition. Springer, 2016. DOI: 10.1007/978-981-10-1813-8.

[Shp25] Amir Shpilka. *Improved Debordering of Waring Rank*. 2025. arXiv: 2502.03150.

[ST17] 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)*. IEEE. 2017, pp. 696–707. DOI: 10.1109/FOCS.2017.70.

[ST21] Amit Sinhababu and Thomas Thierauf. “Factorization of Polynomials Given by Arithmetic Branching Programs”. In: *computational complexity* 30.2 (2021), p. 15. DOI: 10.1007/s00037-021-00215-0.

[Str73] Volker Strassen. “Vermeidung von Divisionen”. In: *Journal für die reine und angewandte Mathematik* 264 (1973), pp. 184–202. URL: http://eudml.org/doc/151394.

[Val79] Leslie G. Valiant. “Completeness Classes in Algebra”. In: *Proceedings of the 11th Annual ACM Symposium on Theory of Computing*. 1979, pp. 249–261. DOI: 10.1145/800135.804419.

[VV86] Leslie G. Valiant and Vijay V. Vazirani. “NP is as Easy as Detecting Unique Solutions”. In: *Theoretical Computer Science* 47.1 (1986), pp. 85–93. DOI: 10.1016/0304-3975(86)90135-0.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il