ON THE ARITHMETIC COMPLEXITY OF COMPUTING GRÖBNER BASES OF COMAXIMAL DETERMINANTAL IDEALS

SRIRAM GOPALAKRISHNAN

Abstract. Let M be an $n \times n$ matrix of homogeneous linear forms over a field $\Bbbk$. If the ideal $\mathcal{I}_{n-2}(M)$ generated by minors of size $n-1$ is Cohen-Macaulay, then the Gulliksen-Negård complex is a free resolution of $\mathcal{I}_{n-2}(M)$. It has recently been shown that by taking into account the syzygy modules for $\mathcal{I}_{n-2}(M)$ which can be obtained from this complex, one can derive a refined signature-based Gröbner basis algorithm DetGB which avoids reductions to zero when computing a grevlex Gröbner basis for $\mathcal{I}_{n-2}(M)$. In this paper, we establish sharp complexity bounds on DetGB. To accomplish this, we prove several results on the sizes of reduced grevlex Gröbner bases of reverse lexicographic ideals, thanks to which we obtain two main complexity results which rely on conjectures similar to that of Fröberg. The first one states that, in the zero-dimensional case, the size of the reduced grevlex Gröbner basis of $\mathcal{I}_{n-2}(M)$ is bounded from below by n^6 asymptotically. The second, also in the zero-dimensional case, states that the complexity of DetGB is bounded from above by $n^{2\omega+3}$ asymptotically, where $2 \leq \omega \leq 3$ is any complexity exponent for matrix multiplication over $\Bbbk$.

1. Introduction

The MinRank problem. Let $\Bbbk$ be a field and let $\overline{\Bbbk}$ be an algebraic closure of $\Bbbk$. Let $\mathcal{R} = \Bbbk[x_1, \ldots, x_k]$ for some $k \in \mathbb{Z}_{>0}$. Let M be an $m \times n$ matrix whose entries are homogeneous polynomials in $\mathcal{R}$ of degree d. Without loss of generality, suppose $m \geq n$. Let $r \in \mathbb{Z}_{>0}$ with $r < n$. We denote by $\mathcal{I}_{r+1}(M) \subset \mathcal{R}$ the ideal generated by the collection of all minors of size $(r+1)$ of M, that is, by all determinants of submatrices of M of size $(r+1) \times (r+1)$. Note that for any point $x \in V_{\overline{\Bbbk}}(\mathcal{I}_{r+1}(M))$, the evaluation of each entry of M at x yields a matrix $M(x)$ with entries in $\overline{\Bbbk}$ whose rank is at most r. Ideals of the form $\mathcal{I}_{r+1}(M)$ are called *determinantal ideals* and have been well-studied (see e.g. [BV88]). For $d = 1$, meaning that the entries of M are linear forms, the problem of computing $V(\mathcal{I}_{r+1}(M))$ is known as the *MinRank* problem. For $d \geq 1$, the problem is known as the *generalized MinRank* problem. The MinRank problem is known to be $\mathcal{NP}$-hard (see [BFS99]).

The MinRank problem lies at the heart of many cryptographic schemes (e.g. [Cou01, Pat96, KS99]) and in many cases, it is possible to reduce the problem of breaking a cryptographic scheme to specific structured instances of the MinRank problem (see e.g. [FLP08, DS05, Beu22, BBC+22, BBB+20, BBC+20]).

Author's affiliations: Sorbonne Université, CNRS, LIP6, F-75005 Paris, France; University of Waterloo, Waterloo, ON, Canada

E-mail address: sriram.gopalakrishnan@lip6.fr.

Outside of the realm of cryptography, many problems in effective algebraic geometry can be modeled as (generalized) MinRank instances. Problems such as those of computing critical points (see e.g. [FSS12, Spa14]), polynomial optimization (see e.g. [GSED14, BGHS14]), quantifier elimination (see e.g. [HS09, HS12, LS21b]), and others in real algebraic geometry (see e.g. [SS03, BGHP05, BGH$^+$10, SS17, BS15, LS21a]) can all be viewed as instances of the (generalized) MinRank problem.

Gröbner basis algorithms. One possible technique to solve the MinRank problem is to solve the polynomial system of $(r+1)$-minors of M. Such systems, known as *determinantal systems*, are well-studied and highly structured. We refer the reader to [BV88, Las78, BCRV22] for a wealth of general theory about determinantal systems. This structure suggests that existing general polynomial systems solving techniques could be optimized in search of more efficient algorithms to solve the MinRank problem. For example in [HSEDSV21], specific properties of determinantal systems are taken into account to present adapted homotopy continuation techniques for solving determinantal systems.
In this paper, we investigate Gröbner basis techniques for solving determinantal polynomial systems. Many improvements have been made to the original general-purpose Gröbner basis algorithm given by Buchberger in his thesis [Buc65]. Perhaps one of the most important has been the introduction of linear algebra via Macaulay matrices to perform S-pair reduction in the F_4 algorithm given by Faugère in [Fau99]. The other critical improvement has been the identification and elimination of reductions to zero by way of a family of criteria, culminating in the F_5 algorithm given by Faugère in [Fau02]. The F_5 algorithm uses at its core a simple data structure called *signatures*, which keeps track of the way the Gröbner basis was computed. Since the introduction of the F_5 algorithm, many signature-based Gröbner basis algorithms have been developed. We refer to [EF16] for a survey of such algorithms.

Arithmetic complexity. We work with the arithmetic complexity model, counting basic arithmetic operations in $\Bbbk$ to estimate the complexity of Gröbner basis algorithms. Under this model of computation, the complexity of computing Gröbner bases using a linear-algebra based algorithm boils down to that of echelonizing Macaulay matrices over $\Bbbk$. One key requirement in order to obtain reasonable complexity estimates is sharp upper bounds on the degrees of the polynomials comprising the output Gröbner basis. For (non-determinantal) polynomial systems satisfying certain genericity properties, such bounds have been given in [Laz83, Giu84]. For determinantal ideals, such bounds have been given in [FSS10, FSS13], together with corresponding complexity analyses which simply compute the cost of echelonizing the appropriate Macaulay matrices. In these works, the impact of the specific structure of determinantal ideals on the shapes of the Macaulay matrices is not taken into account. In particular, reductions to zero arising from the structure of determinantal ideals are not studied or exploited. These reductions to zero are in direct correspondence with elements in the syzygy module of the considered determinantal ideal. In [GNSED23], these syzygy modules are described and used to introduce new criteria which avoid reductions to zero when computing Gröbner bases of determinantal ideals. In particular, when $r = n-2$, $m = n$, and under suitable genericity assumptions, all reductions to zero are avoided. This implies that all linearly redundant rows in the Macaulay matrices can be pruned a priori, leading to faster echelonization. A subsequent complexity analysis is given, which

takes into account these reductions to zero, but still does not exploit the specific structure of the Macaulay matrices encountered.

Main results. In this paper, we consider the *comaximal case* for square matrices of linear forms. That is, we take $d = 1$, $r = n - 2$, and $m = n$. The codimension of $\mathcal{I}_{r+1}(M)$ is $k - (n - r)^2$ (see e.g. [FSS13, Theorem 10]). We fix therefore $k = 4$, so that $\mathcal{I}_{n-2}(M)$ is of dimension zero. In this setting, under certain genericity assumptions which we make explicit, and assuming certain conjectures related to the generic grevlex staircase of $\mathcal{I}_{n-2}(M)$, we give two main results.

First, we provide an exact formula for the size of the reduced grevlex Gröbner basis of $\mathcal{I}_{n-2}(M)$ (see Theorem 8.3 for a precise statement and proof):

> Under certain genericity assumptions and assuming that the ideal $\mathcal{I}_{n-2}(M)$ is reverse lexicographic, the number of elements of $\Bbbk$ in the dense representation for the reduced grevlex Gröbner basis of $\mathcal{I}_{n-2}(M)$ is asymptotically bounded from below by n^6.

Second, we give a sharp complexity analysis of the algorithm [GNSED23, Algorithm 3]-which we call DetGB-taking into account the specific structure of the Macaulay matrices encountered to obtain our complexity bound (see Theorem 8.10 for the precise statement and proof):

> Under certain genericity assumptions and assuming that the ideal $\mathcal{I}_{n-2}(M)$ is reverse lexicographic, the number of arithmetic operations in $\Bbbk$ performed by [GNSED23, Algorithm 3] when computing the reduced grevlex Gröbner basis for $\mathcal{I}_{n-2}(M)$ is in $O(n^{2\omega+3})$.

To accomplish both of these analyses, we establish results on the structure of the grevlex staircase of a well-studied class of ideals known as reverse lexicographic ideals. In Section 6, we rely on the well-studied notion of *Lefschetz properties* (see [HMM+13b]) to relate Conjecture 5.5 which states that $\mathcal{I}_{n-2}(M)$ is generically reverse lexicographic to a long-standing conjecture of Goto (see [Got74]).

The statement and proof of Theorem 8.3 is obtained by simply determining the size of the output reduced grevlex Gröbner basis. In particular, we use a dense representation of the polynomials in the Gröbner basis and provide a formula for the number of nonzero coefficients appearing in this dense representation.

Inspired by the sharp complexity analysis of F_5 in the case of a regular sequence in simultaneous Noether position given in [BFS15], we again use our results on on the structure of the grevlex staircases of reverse lexicographic ideals to establish our complexity upper bound, stated in Theorem 8.10, assuming Conjecture 5.5. Our upper bound arises by first giving an explicit estimate for the number of arithmetic operations over $\Bbbk$ performed in [GNSED23, Algorithm 3], then analyzing the asymptotics of this formula. We conclude by showing that the asymptotic analysis we perform is sharp, by comparing it to the explicit estimate we give. The upper bound we obtain compares favorably to the bound $O(n^{4\omega+2})$ of [FSS13, Theorem 20].

2. Preliminaries

Throughout, we denote by $\mathcal{R}$ the ring $\Bbbk[x_1, \dots x_k]$, by $\mathrm{Mon}(\mathcal{R})$ the set of all monomials of $\mathcal{R}$, and by $\mathrm{Mon}_d(\mathcal{R})$ the set of monomials of degree d of $\mathcal{R}$. We use the standard multi-index notation, whereby for some k-tuple of integers $\alpha = (\alpha_1, \dots, \alpha_k) \in \mathbb{Z}^k_{\geq 0}$, we abbreviate $x^\alpha = x_1^{\alpha_1} \cdots x_k^{\alpha_k}$. We use $\mathbb{A}^s$, to denote the affine space of dimension s over $\overline{\Bbbk}$, viewed as an affine variety with the Zariski topology.

2.1. **Gröbner bases.** A wealth of general theory about Gröbner bases can be found, for example, in [CLO05] and the references therein. We recall here only what is necessary for our purposes.

We denote by $\succ$ an admissible monomial order on $\mathcal{R}$. That is, $\succ$ is a total order on $\mathrm{Mon}(\mathcal{R})$ such that if σ, τ are monomials with $\sigma \succ \tau$, then for any monomial $m \in \mathrm{Mon}(\mathcal{R})$, $m\sigma \succ m\tau$, and for which there is no infinitely decreasing sequence of monomials. Given a polynomial $f \in \mathcal{R}$, we use $\mathrm{LM}_\succ(f)$ to denote the leading monomial of f with respect to $\succ$, and $\mathrm{LT}_\succ(f)$ to denote the leading term of f with respect to $\succ$, that is, $\mathrm{LM}_\succ(f)$ multiplied by its coefficient in f. Given a set $F \subseteq \mathcal{R}$ of polynomials, we define the sets

$$\mathrm{LM}_\succ(F) := \{\mathrm{LM}_\succ(f) : f \in F\} \quad \text{and} \quad \mathrm{LT}_\succ(F) := \{\mathrm{LT}_\succ(f) : f \in F\}.$$

When $\succ$ is clear from the context, we remove it as a subscript.

We use e_i to denote the standard i-th basis element of the free $\mathcal{R}$-module $\mathcal{R}^m$. A monomial of $\mathcal{R}^m$ is an element of $\mathcal{R}^m$ of the form $x^\alpha e_i$, where $x^\alpha \in \mathrm{Mon}(\mathcal{R})$ and e_i is some standard basis element of $\mathcal{R}^m$. We use $\mathrm{Mon}(\mathcal{R}^m)$ to denote the set of all monomials of $\mathcal{R}^m$.

The free module $\mathcal{R}^m$ carries a standard grading induced by the grading by degree on $\mathcal{R}$. That is, we can write $\mathcal{R}^m = \bigoplus_{d=0}^\infty \mathcal{R}_d^m$, where

$$\mathcal{R}_d^m = \{f_1 e_1 + \cdots + f_m e_m : \deg(f_i) = d \text{ for all } 1 \leq i \leq m\}$$

is the additive group of *homogeneous elements of degree d*. Note that implicitly, we take $0 \in \mathcal{R}_d^m$ for all $d \geq 0$. With respect to this grading, a monomial $x^\alpha e_i \in \mathrm{Mon}(\mathcal{R}^m)$ has degree $\deg(x^\alpha)$. We use $\mathrm{Mon}_d(\mathcal{R}^m)$ to denote the set of all monomials of $\mathcal{R}^m$ of degree d.

The monomial order $\succ$ on $\mathcal{R}$ induces the *term over position* order on $\mathcal{R}^m$ defined as follows: for $x^\alpha e_i, x^\beta e_j$ in $\mathrm{Mon}(\mathcal{R}^m)$, $x^\alpha e_i \succ_{\mathrm{TOP}} x^\beta e_j$ if and only if either $x^\alpha \succ x^\beta$ or $x^\alpha = x^\beta$ and $i > j$. We likewise extend the leading term and leading monomial notation from $\mathcal{R}$ to $\mathcal{R}^m$, so that for $\mathbf{f} \in \mathcal{R}^m$, $\mathrm{LM}_{\succ_{\mathrm{TOP}}}(\mathbf{f})$ is the leading monomial of $\mathbf{f}$ and $\mathrm{LT}_{\succ_{\mathrm{TOP}}}(\mathbf{f})$ is its leading term. Analogously, for a subset $\mathbf{F} \subseteq \mathcal{R}^m$, we denote $\mathrm{LM}_{\succ_{\mathrm{TOP}}}(\mathbf{F}) = \{\mathrm{LM}_{\succ_{\mathrm{TOP}}}(\mathbf{f}) : \mathbf{f} \in \mathbf{F}\}$ and $\mathrm{LT}_{\succ_{\mathrm{TOP}}}(\mathbf{F}) = \{\mathrm{LT}_{\succ_{\mathrm{TOP}}}(\mathbf{f}) : \mathbf{f} \in \mathbf{F}\}$.

Given $\mathbf{f}_1, \ldots, \mathbf{f}_s \in \mathcal{R}^m$, we denote by $\langle \mathbf{f}_1, \ldots, \mathbf{f}_s \rangle$ the submodule of $\mathcal{R}^m$ generated by $\mathbf{f}_1, \ldots, \mathbf{f}_s$.

If $\mathbf{f}_1, \ldots, \mathbf{f}_s \in \mathcal{R}^m$ are all homogeneous elements, then the module $\mathbf{F} = \langle \mathbf{f}_1, \ldots, \mathbf{f}_s \rangle$ is itself graded. In this setting, we denote by $\mathbf{F}_d$ the additive group of homogeneous elements of degree d of $\mathbf{F}$.

Definition 2.1 (Gröbner basis, [CLO05, Chapter 5, Definition 2.6])**.** Let $\mathbf{f}_1, \ldots, \mathbf{f}_s$ in $\mathcal{R}^m$ and let $\mathbf{F}$ be the submodule of $\mathcal{R}^m$ generated by $\mathbf{f}_1, \ldots, \mathbf{f}_s$. A finite set $G \subseteq \mathbf{F}$ is called a $\succ_{\mathrm{TOP}}$*-Gröbner basis* of $\mathbf{F}$ if $\langle \mathrm{LM}_{\succ_{\mathrm{TOP}}}(G) \rangle = \mathrm{LM}_{\succ_{\mathrm{TOP}}}(\mathbf{F})$.

Suppose $\mathbf{f}_1, \ldots, \mathbf{f}_s$ are homogeneous elements of $\mathcal{R}^m$. Then $\mathbf{F}$ is itself a graded module. In this case, for a given integer D, a finite set $G \subseteq \mathbf{F}$ is called a *$(D, \succ_{\mathrm{TOP}})$-Gröbner basis* of $\mathbf{F}$ if G forms the elements of degree at most D of a $\succ_{\mathrm{TOP}}$-Gröbner basis of $\mathbf{F}$.

Remark 2.2. If G is a $\succ_{\mathrm{TOP}}$-Gröbner basis of a submodule $\mathbf{F} \subseteq \mathcal{R}^m$, then $\langle G \rangle = \mathbf{F}$ (see [CLO05, Chapter 5, Proposition 2.7(b)]).

2.2. **Macaulay matrices.** We recall here the basic construction of Macaulay matrices for a system of homogeneous elements of $\mathcal{R}^m$.

Definition 2.3. Let $\mathbf{f} = (\mathbf{f}_1, \ldots, \mathbf{f}_s) \subseteq \mathcal{R}^m$ be homogeneous elements and for each $1 \leq i \leq s$, let $d_i = \deg \mathbf{f}_i$. For a given integer $d \geq \min_{1 \leq i \leq s} d_i$, the *Macaulay matrix in degree d with respect to $\succ_{\mathrm{TOP}}$*, $\mathcal{M}_{d,\succ}(\mathbf{f})$ is constructed as follows:

- its columns are indexed by $\mathrm{Mon}_d(\mathcal{R}^m)$, ordered in decreasing order with respect to $\succ_{\mathrm{TOP}}$,
- and for each monomial $\tau \in \mathrm{Mon}_{d-d_i}(\mathcal{R})$, one inserts into the matrix a single row whose entry in the column indexed by the monomial σ is the coefficient of σ in $\tau \mathbf{f}_i$.

The rows of $\mathcal{M}_{d,\succ}(\mathbf{f})$ are naturally interpreted as module elements, and we will freely refer to them as such. Note that these rows form a basis for $\mathcal{R}^m_d$ as a finite-dimensional $\Bbbk$-vector space.
We denote by $\widetilde{\mathcal{M}}_{d,\succ}(\mathbf{f})$ the reduced row-echelon form of $\mathcal{M}_{d,\succ}(\mathbf{f})$.

Theorem 2.4. Let $\mathbf{f} = (\mathbf{f}_1, \ldots, \mathbf{f}_s) \subseteq \mathcal{R}^m$ be homogeneous elements. Then the rows of $\widetilde{\mathcal{M}}_{d,\succ}(\mathbf{f})$, form the elements of degree d of a $\succ_{\mathrm{TOP}}$-Gröbner basis for the module generated by $\mathbf{f}$.

Proof. Let $\mathbf{F}$ be the module generated by $\mathbf{f}$. Let $\mathbf{g} \in \mathbf{F}$. Since $\mathbf{f}_1, \ldots, \mathbf{f}_s$ are homogeneous, the module $\mathbf{F}$ is graded. Thus, there exist some $\mathbf{g}_1, \ldots, \mathbf{g}_t \in \mathbf{F}$ such that for each $1 \leq i \leq t$, $\mathbf{g}_i$ is homogeneous of degree i and $\mathbf{g} = \mathbf{g}_1 + \cdots + \mathbf{g}_t$. For each $1 \leq i \leq t$, the rows of $\widetilde{\mathcal{M}}_{i,\succ}(\mathbf{f})$ form a basis for $\mathbf{F}_i$. Therefore, for each $1 \leq i \leq t$, there exist some $c_j \in \Bbbk$ such that

$$\mathbf{g}_i = \sum_{j=1}^{\dim_{\Bbbk}(\mathbf{F}_i)} c_j \mathbf{h}_j$$

where the module elements $\mathbf{h}_j$ are the (nonzero) rows of $\widetilde{\mathcal{M}}_{i,\succ}(\mathbf{f})$. Since $\widetilde{\mathcal{M}}_{d,\succ}(\mathbf{f})$ is in row echelon form, the leading monomials of the $\mathbf{h}_j$ are pairwise distinct. Using a natural generalization of [CLO15, Chapter 2, Lemma 8(ii)] to the setting of modules, there exists, for each $1 \leq i \leq t$, some $1 \leq j \leq \dim_{\Bbbk}(\mathbf{F}_i)$ such that $\mathrm{LM}_{\succ_{\mathrm{TOP}}}(\mathbf{g}_i) = \mathrm{LM}_{\succ_{\mathrm{TOP}}}(\mathbf{h}_j)$. Now since the degrees of the $\mathbf{g}_i$ are pairwise distinct, using once again a natural generalization of [CLO15, Chapter 2, Lemma 8(ii)], there exists some $1 \leq i \leq t$ such that $\mathrm{LM}_{\succ_{\mathrm{TOP}}}(\mathbf{g}) = \mathrm{LM}_{\succ_{\mathrm{TOP}}}(\mathbf{g}_i)$. □

Henceforth, we fix $\succ$ to be the *graded reverse lexicographic* (grevlex) order. When $\mathbf{f}$ is clear from context, $\mathcal{M}_{d,\succ}(\mathbf{f})$ and $\widetilde{\mathcal{M}}_{d,\succ}(\mathbf{f})$ will be denoted by $\mathcal{M}_d$ and $\widetilde{\mathcal{M}}_d$ respectively.

2.3. **Hilbert series.** Since the complexity of computing Gröbner bases is governed by that of echelonizing Macaulay matrices, understanding the sizes of these matrices is key in our complexity analysis. Hilbert series of graded modules encode precisely this information. Much general theory of Hilbert functions, polynomials, and series can be found, for example, in [CLO05, Chapter 6, Section 4].

Definition 2.5. Given homogeneous elements $\mathbf{f}_1, \ldots, \mathbf{f}_s \in \mathcal{R}^m$, the *Hilbert function* of the module $\mathbf{F}$ generated by $(\mathbf{f}_1, \ldots, \mathbf{f}_s)$ is defined by

$$\mathrm{HF}_{\mathbf{F}}(d) = \dim_{\Bbbk}(\mathbf{F}_d).$$

The *Hilbert series* of $\mathbf{F}$ is the generating series of the Hilbert function of $\mathbf{F}$. That is,

$$H_{\mathbf{F}}(t) = \sum_{d\geq 0} \mathrm{HF}_{\mathbf{F}}(d)t^d.$$

Proposition 2.6 ([BH98, Corollary 4.1.8])**.** Let $\mathbf{F} \subseteq \mathcal{R}^m$ be a graded module of Krull dimension zero. Then $H_{\mathcal{R}^m/\mathbf{F}}(t)$ is a polynomial.

2.4. **Free resolutions.** Free resolutions are a fundamental construction in commutative algebra. Many general facts about free resolutions can be found in [Eis95, III] and [CLO15, Chapter 6]. Again, we recall below only what we need for our purposes, and follow closely the exposition given in [GND24, Section 2]
Let $\mathbf{F}$ be a finitely generated $\mathcal{R}$-module. An exact sequence

$$\cdots \xrightarrow{\partial_{j+1}} \mathcal{E}_j \xrightarrow{\partial_j} \cdots \xrightarrow{\partial_2} \mathcal{E}_1 \xrightarrow{\partial_1} \mathcal{E}_0 \xrightarrow{\epsilon} \mathbf{F} \to 0$$

is a *left resolution* of $\mathbf{F}$. The maps ∂_i are *boundary homomorphisms*, and the map ϵ is an *augmentation homomorphism*. If for each i, the module $\mathcal{E}_i$ is free, then the resolution is a *free resolution*. For the sake of brevity, we will often refer to a resolution as above simply by $(\mathcal{E}_\bullet \xrightarrow{\epsilon} \mathbf{F}, \partial_\bullet)$. We call $\sup\{i \in \mathbb{Z} : \mathcal{E}_i \neq 0\}$ the *length* of the resolution $(\mathcal{E}_\bullet \xrightarrow{\epsilon} \mathbf{F}, \partial_\bullet)$. Note that the length of $(\mathcal{E}_\bullet \xrightarrow{\epsilon} \mathbf{F}, \partial_\bullet)$ could be infinity. Free resolutions of finite length are *finite free resolutions*.

Theorem 2.7 (Hilbert's syzygy theorem, [Eis95, Corollary 19.7])**.** Let $\mathbf{F}$ be a finitely generated $\mathcal{R}$-module. There exists a free resolution $(\mathcal{E}_\bullet \xrightarrow{\epsilon} \mathbf{F}, \partial_\bullet)$ of length at most k.

When $\mathbf{F}$ is a graded module over $\mathcal{R}$, it possesses a free resolution $(\mathcal{E}_\bullet \xrightarrow{\epsilon} \mathbf{F}, \partial_\bullet)$ where each free module $\mathcal{E}_i$ is graded in such a way that the boundary maps ∂_i and the augmentation map ϵ are graded $\mathcal{R}$-module homomorphisms. In this setting, those free resolutions $(\mathcal{E}_\bullet \xrightarrow{\epsilon} \mathbf{F}, \partial_\bullet)$ such that the ranks of each of the $\mathcal{E}_i$ are minimal are *minimal free resolutions*.
Let $(\mathcal{E}_\bullet \xrightarrow{\epsilon} \mathbf{F}, \partial_\bullet)$ be a free resolution of $\mathbf{F}$. Upon fixing a set of generators $(\mathbf{f}_1^{(0)}, \ldots, \mathbf{f}_{s_0}^{(0)})$ for $\mathbf{F}$ and sets of generators $(\mathbf{f}_1^{(i)}, \ldots, \mathbf{f}_{s_i}^{(i)})$ for each $\operatorname{im}\partial_i$, we can define, for each i, the *i-th syzygy module* of $(\mathbf{f}_1, \ldots, \mathbf{f}_s)$, as follows:

$$\mathrm{Syz}_i(\mathbf{F}) = \{(g_1, \ldots, g_{s_i}) \in \mathcal{R}^{s_i} : g_1\mathbf{f}_1^{(i)} + \cdots + g_{s_i}\mathbf{f}_{s_i}^{(i)} = 0\}.$$

Remark 2.8. The way we define syzygy modules here is quite ad-hoc. In particular, as defined here, the syzygy modules of a given module $\mathbf{F}$ depend on the choices of a free resolution of $\mathbf{F}$ and generating sets for the images of each of the boundary homomorphisms in the chosen free resolution. In our setting this suffices, since we consider only a single free resolution — the Gulliksen-Negård complex — and take explicit generating sets for the images of the boundary homomorphisms from [GNSED23, Theorem 9] and [GNSED23, Proposition 19].

The connection between free resolutions and Hilbert series is elucidated in the following corollary.

Corollary 2.9. [CLO05, Theorem 4.4] Let $\mathbf{F}$ be a finitely generated graded $\mathcal{R}$-module, and let $(\mathcal{E}_\bullet \xrightarrow{\epsilon} \mathbf{F}, \partial_\bullet)$ be a finite graded free resolution of $\mathbf{F}$ of length ℓ. For

any $1 \leq i \leq \ell$, let $s_i = \mathrm{rk}(\mathcal{E}_i)$ and write $\mathcal{E}_i = \bigoplus_{j=1}^{s_i} \mathcal{R}\left(-d_i^{(j)}\right)$. Then

$$\mathrm{HF}_{\mathbf{F}}(d) = \sum_{i=0}^{\ell} (-1)^i \left(\sum_{j=1}^{s_i} \binom{k+d-d_i^{(j)}-1}{k-1} \right).$$

3. Genericity

We begin by fixing a notion of genericity for determinantal ideals on which we will rely to give subsequent results regarding the structure of Gröbner bases of determinantal ideals and the complexity of computing them.

If M is an $n \times n$ matrix over any ring A and $1 \leq r < n$, we will denote by $\mathcal{I}_{r+1}(M)$ the ideal generated by the $(r+1)$-minors of M. We use the notation of [FSS13, Section 2] to formalize various notions of genericity.

For some integer $d \in \mathbb{Z}_{>0}$, we call a polynomial of the form

$$f = \sum_{\tau \in \mathrm{Mon}_d(\mathcal{R})} \mathfrak{a}^{(\tau)} \tau \in \mathcal{R}\left[\left\{\mathfrak{a}^{(\tau)} : \tau \in \mathrm{Mon}_d(\mathcal{R})\right\}\right]$$

a *generic homogeneous polynomial of degree d*.

In what follows, we use $\mathscr{A}_n^d$ to denote the $n \times n$ matrix of generic homogeneous polynomials of degree d, whose i,j entry is

$$f_{ij} = \sum_{\tau \in \mathrm{Mon}_d(\mathcal{R})} \mathfrak{a}_{ij}^{(\tau)} \tau \in \mathcal{R}\left[\left\{{\mathfrak{a}_{ij}}^{(\tau)} : \tau \in \mathrm{Mon}_d(\mathcal{R})\right\}\right].$$

For a point $a = \left(a_{ij}^{(\tau)}\right) \in \mathbb{A}^{\binom{k+d-1}{k-1} \cdot n^2}$ we will denote by ϕ_a the specialization map

$$\begin{aligned} \phi_a : \mathcal{R}\left[\left\{{\mathfrak{a}_{ij}}^{(\tau)} : \tau \in \mathrm{Mon}_d(\mathcal{R})\right\}\right] &\to \mathcal{R} \\ \mathfrak{a}_{ij}^{(\tau)} &\mapsto a_{ij}^{(\tau)}. \end{aligned}$$

By abuse of notation, we will also use $\phi_a\left(\mathscr{A}_n^d\right)$ to denote the matrix (over $\mathcal{R}$) whose entries are simply the images of the entries of $\mathscr{A}_n^d$ under ϕ_a.

A map

$$\mathscr{P} : \{\text{Ideals of } \mathcal{R}\} \to \{\texttt{true}, \texttt{false}\}$$

is called a *property*.

Definition 3.1. A property $\mathscr{P}$ is (k,r,n,d)-*generic* if there exists a nonempty Zariski open subset $U \subseteq \mathbb{A}^{\binom{k+d-1}{k-1} \cdot n^2}$ such that for all $a \in U$,

$$\mathscr{P}\left(\mathcal{I}_{r+1}\left(\phi_a\left(\mathscr{A}_n^d\right)\right)\right) = \texttt{true}.$$

The following proposition is a fundamental result on determinantal ideals.

Proposition 3.2. Let CM be the property given by

$$\mathrm{CM}(I) = \begin{cases} \texttt{true} & \text{if } I \text{ is Cohen-Macaulay} \\ \texttt{false} & \text{otherwise} \end{cases}$$

Then for any $n, d \in \mathbb{Z}_{>0}$, $r < n$, CM is $((n-r)^2, r, n, d)$-generic.

Proof. By [BV88, Theorem 2.5], the depth of $\mathcal{I}_{r+1}\left(\phi_a(\mathscr{A}_n^d)\right)$ is at most $(n-r)^2$. By [FSS13, Theorem 10], there exists a Zariski open subset $U \subseteq \mathbb{A}^{\binom{k+d-1}{k-1} \cdot n^2}$ such that for all $a \in U$, $\mathcal{I}_{r+1}\left(\phi_a\left(\mathscr{A}_n^d\right)\right)$ has codimension $(n-r)^2$, and is therefore Cohen-Macaulay. □

4. The Hilbert series of determinantal ideals

One of the key inputs into our complexity analysis is the Hilbert series of determinantal ideals. Here, we give explicit formulæ for the Hilbert functions of determinantal ideals in the case $r = n - 2$, under certain genericity assumptions. We accomplish this by analyzing a complex associated to these ideals called the Gulliksen-Negård complex, which under suitable genericity assumptions turns out to be a free resolution. This allows us to obtain the Hilbert series' we require by computing the ranks of the component modules.

4.1. **The complex of Gulliksen and Negård.** We begin by recalling the construction of the complex of Gulliksen and Negård. This complex was originally given in [GN72]. A detailed exposition of this complex can be found in [BV88, Chapter 2, Section D]. We reproduce here only what is necessary to obtain the Hilbert series' we require.

In this section, we fix $n \in \mathbb{Z}$, $n \geq 3$. Let $M_n(\mathcal{R})$ be the set of $n \times n$ matrices over $\mathcal{R}$. The set $M_n(\mathcal{R})$ carries a natural $\mathcal{R}$-module structure, under which it is free of rank n^2. We will denote by I_n the identity matrix in $M_n(\mathcal{R})$.

Consider the zero sequence

$$\mathcal{R} \xrightarrow{\iota} M_n(\mathcal{R}) \oplus M_n(\mathcal{R}) \xrightarrow{\pi} \mathcal{R}$$

where $\iota(x) = (xI_n, xI_n)$ and $\pi(U, V) = \operatorname{trace}(U - V)$. It is immediate that $\operatorname{im}\iota \subset \ker\pi$.

Proposition 4.1. The quotient module $\mathcal{E}_1 = \ker\iota/\operatorname{im}\pi$ is free of rank $2n^2 - 2$.

Proof. We take as an $\mathcal{R}$-module basis for $M_n(\mathcal{R})$ the elementary matrices: for each $1 \leq i, j \leq n$, $E_{i,j}$ is the $n \times n$ matrix over $\mathcal{R}$ with entry 1 at (i, j) and 0 elsewhere. Following [BV88, Chapter 2, Section D], $\ker\pi$ is generated by the following $2n^2 - 1$ elements of $M_n(\mathcal{R}) \oplus M_n(\mathcal{R})$

- $(E_{i,j}, 0)$ for $1 \leq i, j, \leq n$ and $i \neq j$
- $(0, E_{u,v})$ for $1 \leq u, v \leq n$ and $u \neq v$
- $(E_{i,i}, E_{1,1})$ for $1 \leq i \leq n$
- $(0, E_{i,i} - E_{1,1})$ for $1 \leq i \leq n$

It is clear that $\operatorname{im}\iota$ is generated by

$$(I_n, I_n) = \sum_{i=1}^{n} (E_{i,i}, E_{1,1}) + (0, E_{i,i} - E_{1,1}).$$

Thus, $\ker\iota/\operatorname{im}\pi$ is free of rank $2n^2 - 2$. □

Equipped with $\mathcal{E}_1$, we can now give the full Gulliksen-Negård complex.

Let $M \in M_n(\mathcal{R})$ and let M^C be the matrix of cofactors of M. Let $\mathcal{E}_3 = \mathcal{R}$, $\mathcal{E}_2 = \mathcal{E}_0 = M_n(\mathcal{R})$, and $\mathcal{E}_1 = \ker\psi/\operatorname{im}\phi$.

We define the boundary maps as follows: $\partial_3 : x \mapsto xM^C$, $\partial_2 : N \mapsto \overline{(MN, NM)}$, $\partial_1 : \overline{(N_1, N_2)} \mapsto N_1M - MN_2$. Finally, we define the augmentation map by $\epsilon : N \mapsto \operatorname{trace}(M^C N)$.

Proposition 4.2 ([BV88, Theorem 2.26])**.** Let $M \in M_n(\mathcal{R})$. If $\mathcal{I}_{n-2}(M)$ is Cohen-Macaulay, then the sequence

$$0 \to \mathcal{E}_3 \xrightarrow{\partial_3} \mathcal{E}_2 \xrightarrow{\partial_2} \mathcal{E}_1 \xrightarrow{\partial_1} \mathcal{E}_0 \xrightarrow{\epsilon} \mathcal{I}_{n-2}(M) \to 0$$

with modules, boundary maps, and augmentation map defined as above is a free resolution of $\mathcal{I}_{n-2}(M)$.

4.2. **An explicit Hilbert series.** Applying Corollary 2.9, we extract from the Gulliksen-Negård complex the Hilbert series of $\mathcal{I}_{n-2}(M)$.

Proposition 4.3. For any $n \geq 3$, $D \geq 1$, let

$$H_{n,D}(t) = \sum_{d=D(n-1)}^{2Dn-3} \left(n^2 \binom{3+d-D(n-1)}{3} - (2n^2-2)\binom{3+d-Dn}{3} + n^2 \binom{3+d-D(n+1)}{3} \right) t^d.$$

Then the property

$$\mathrm{HS}(I) = \begin{cases} \texttt{true} & \text{if } H_I(t) = H_{n,D}(t) \\ \texttt{false} & \text{otherwise} \end{cases}$$

is $(4, n-2, n, D)$-generic.

Proof. By Proposition 3.2, there exists a Zariski open subset $U_{\mathrm{CM}} \subseteq \mathbb{A}^{4n^2}$ such that for all $a \in U_{\mathrm{CM}}$, $\mathcal{I}_{n-2}(\phi_a(\mathscr{A}_n^D))$ is Cohen-Macaulay. Subsequently, by Proposition 4.2, for any $a \in U_{\mathrm{CM}}$, the Gulliksen-Negård complex is a free resolution of $\mathcal{I}_{n-2}(\phi_a(\mathscr{A}_n^D))$. In order to apply Corollary 2.9 on the Gulliksen-Negård complex, we must write, for each $0 \leq i \leq 3$, $\mathcal{E}_i = \bigoplus_{j=1}^{\mathrm{rk}(\mathcal{E}_i)} \mathcal{R}(-d_i^{(j)})$.
First, $\mathrm{rk}(\mathcal{E}_0) = n^2$ and for each $1 \leq j \leq n^2$, the image of e_j under ϵ is an $(n-1)$-minor of $\phi_a(\mathscr{A}_n^D)$. Such a minor is a polynomial of degree $D(n-1)$, so in order for ϵ to be graded, e_i must be a member of the $D(n-1)$ graded piece of $\mathcal{E}_0$. This gives $d_0^{(j)} = D(n-1)$ for all $1 \leq j \leq n^2$.
Next, by Proposition 4.1, $\mathrm{rk}(\mathcal{E}_1) = 2n^2 - 2$. Consider the basis elements of $\mathcal{E}_1$ from Proposition 4.1 of the form $\overline{(E_{i,j}, 0)}$ for $1 \leq i, j \leq n$, $i \neq j$. These map, under ∂_1, to $E_{i,j}\phi_a(\mathscr{A}_n^D)$. Each nonzero coefficient of $E_{i,j}\phi_a(\mathscr{A}_n^D)$, written in terms of the standard basis elements of $\mathcal{E}_0 = M_n(\mathcal{R})$, is an entry of $\phi_a(\mathscr{A}_n^D)$, and is thus a polynomial of degree D. Thus, in order for the map $\partial_1 : \mathcal{E}_1 \to \mathcal{E}_0(-D(n-1))$ to be graded, $\overline{(E_{i,j}, 0)}$ must be a member of the Dn graded piece of $\mathcal{E}_1$. This gives $d_1^{(1)} = Dn$. A similar computation for the other basis elements of $\mathcal{E}_1$, described in Proposition 4.1 shows that, in fact, for all $1 \leq j \leq 2n^2 - 2$, $d_1^{(j)} = Dn$.
By construction, $\mathrm{rk}(\mathcal{E}_2) = n^2$. For any basis element $E_{i,j}$ of $\mathcal{E}_2$, each nonzero coefficient of $\partial_2(E_{i,j}) = \overline{(\phi_a(\mathscr{A}_n^D)E_{i,j}, E_{i,j}\phi_a(\mathscr{A}_n^D))}$, written in terms of the basis elements for $\mathcal{E}_1$ given in Proposition 4.1 is again an entry of $\phi_a(\mathscr{A}_n^D)$, and therefore a polynomial of degree D. In order for $\partial_2 : \mathcal{E}_2 \to \mathcal{E}_1(-Dn)$ to be graded, $E_{i,j}$ must then be a member of the $D(n+1)$ graded piece of $\mathcal{E}_2$. This gives, for each $1 \leq j \leq n^2$, $d_2^{(j)} = D(n+1)$.
Finally, $\mathrm{rk}(\mathcal{E}_3) = 1$, and $\partial_3(1) = \phi_a(\mathscr{A}_n^D)^C$. When written in terms of the standard basis of $\mathcal{E}_2 = M_n(\mathcal{R})$, the nonzero coefficients of $\phi_a(\mathscr{A}_n^D)^C$ are precisely the cofactors of $\phi_a(\mathscr{A}_n^D)$, which have degree $D(n-1)$, giving $d_3^{(1)} = 2Dn$.
Putting these quantities together and applying Corollary 2.9 gives precisely $H_{n,D}(t)$. □

We conclude this section with an auxiliary lemma regarding the structure of the Hilbert series given in Proposition 4.3 which will be necessary in order to perform the complexity analyses we give in later sections.

Lemma 4.4. For all $n-1 \leq d < 2n-3$, $h_{d+1} > h_d$.

Proof. Taking $D = 1$ in Proposition 4.3 and simplifying the summand, we find that

$$h_d = \frac{(2+d-n)(d^2+(-2n+4)d+4n^2-4n+3)}{3}.$$

Let $f(d) = h_d$ and view f as a continuous function in one real variable. Then $f''(d) = 2d-2n+4$ has its unique root at $d = n-2$. Thus, $f'(d)$ attains its minimum at $d = n-2$, and f is therefore strictly increasing on the interval $[n-1, \infty)$. □

5. Reverse lexicographic ideals

Reverse lexicographic ideals have been studied for the special place they hold amongst all ideals with a given Hilbert function (see e.g. [Dee96]). After recalling their definition in Section 5.1, we prove a general result about the structure of the grevlex leading monomials in the case of a homogeneous reverse lexicographic ideal (Proposition 5.3). In Section 5.2, we show that as long as a certain Zariski open subset that we make explicit is nonempty, this result can be applied to the determinantal ideals considered in this paper. In the following section, Section 6, we further investigate when the determinantal ideals that we consider are generically reverse lexicographic, and relate this property to a conjecture of Goto (see [Got74]).
Recall that we have fixed our monomial order $\succ$ to be the graded reverse lexicographic order and suppressed the symbol $\succ$ from all relevant notation.

5.1. The grevlex staircase of a homogeneous reverse lexicographic ideal.

Definition 5.1. Let $I \subseteq \mathcal{R}$ be a nonzero ideal. We call I *reverse lexicographic* if for all $\tau \in \mathrm{LM}(I)$,

$$\{\sigma \in \mathrm{Mon}_{\deg \tau}(\mathcal{R}) : \sigma \succ \tau\} \subseteq \mathrm{LM}(I).$$

We begin with a simple and helpful observation about the grevlex staircase of a reverse lexicographic ideal.

Lemma 5.2. Let $I \subseteq \mathcal{R}$ be a reverse lexicographic ideal. Let $\tau \in \mathrm{LM}(I)$ and x_j be the smallest variable in τ. For any variable $y \in \{x_1, \ldots, x_k\}$ with $y \succ x_j$, the monomial $\sigma = \frac{\tau}{x_j} y \in \mathrm{Mon}_{\deg \tau}(\mathcal{R})$ is such that $\sigma \succ \tau$ and $\sigma \in \mathrm{LM}(I)$.

We come now to the main result of this section, which provides a formula to calculate the number of polynomials of degree $d+1$ in a grevlex Gröbner basis of a homogeneous reverse lexicographic ideal whose leading monomials are not divisible by any leading monomial of degree d.

Proposition 5.3. Let $F \subseteq \Bbbk[x_1, \ldots, x_k]$ be a sequence of homogeneous polynomials, all of degree d_0. Suppose $I = \langle F \rangle$ is a reverse lexicographic ideal. Let $\mathrm{HF}_I(d) = h_d$ be the Hilbert function of I and let D be the largest degree of a polynomial appearing in the reduced grevlex Gröbner basis of F. For any $d_0 \leq d \leq D$,

let G_d be the set of elements of degree at most d in the reduced grevlex Gröbner basis for F and let ℓ_d be the largest integer such that

$$\binom{\ell_d + d - 1}{\ell_d - 1} < h_d.$$

Then for any $d_0 \leq d \leq D$,

$$\begin{aligned}\#(\mathrm{LM}(G_{d+1}) \setminus \mathrm{LM}(G_d)) = h_{d+1} + (\ell_d - k)h_d \\ + \sum_{j=1}^{\ell_d} \binom{j+d-2}{j-1}(j-1) \\ - \ell_d \binom{\ell_d + d - 1}{\ell_d - 1}\end{aligned}$$

Proof. We begin by noting that G_{d+1} can be obtained from G_d by multiplying each of the h_d nonzero rows of $\widetilde{\mathcal{M}}_d$ by each of the k variables to build $\mathcal{M}_{d+1}$, echelonizing to obtain $\widetilde{\mathcal{M}}_{d+1}$, then discarding zero rows and rows that are redundant because their leading terms are already divisible by those in $\mathrm{LM}(G_d)$. Letting z_{d+1} (resp. r_d) be the number of these zero (resp. redundant) rows, we can write

$$\#(\mathrm{LM}(G_{d+1}) \setminus \mathrm{LM}(G_d)) = kh_d - z_{d+1} - r_{d+1}. \tag{1}$$

Note also that if the echelonization process alters the leading term of some row of $\mathcal{M}_{d+1}$ built in this way, then either that row reduces to zero, or its new leading term is no longer divisible by any monomial in $\mathrm{LM}(G_d)$. Thus, denoting by c_{d+1} the number of rows of $\mathcal{M}_{d+1}$ which are to be reduced during the echelonization process, one has

$$c_{d+1} = z_{d+1} + \#(\mathrm{LM}(G_{d+1}) \setminus \mathrm{LM}(G_d)) \tag{2}$$

$$\text{and} \quad r_{d+1} = kh_d - c_{d+1}. \tag{3}$$

Combining Eqs. (1) to (3) gives

$$\#(\mathrm{LM}(G_{d+1}) \setminus \mathrm{LM}(G_d)) = h_{d+1} - kh_d + c_{d+1}.$$

The rest of the proof consists in computing c_{d+1}. Fix $\tau \in \mathrm{LM}(G_d)$, and let x_j be the grevlex smallest variable in τ. Then by Lemma 5.2, for each of the $j-1$ variables larger than x_j, there exists some $\sigma \in \mathrm{LM}(G_d)$ such that σx_j appears as the leading term of some row of $\mathcal{M}_{d+1}$ which can be reduced by a multiple of τ. Thus, the row of $\widetilde{\mathcal{M}}_d$ with leading term τ generates exactly $j-1$ rows of $\mathcal{M}_{d+1}$ which are to be reduced. The number of monomials of degree d whose grevlex smallest variable is some x_j is simply

$$\underbrace{\binom{j+d-1}{j-1}}_{\substack{\text{number of monomials of degree } d \\ \text{in } j \text{ variables}}} - \underbrace{\binom{j+d-2}{j-2}}_{\substack{\text{number of monomials of degree } d \\ \text{in } j-1 \text{ variables}}} = \underbrace{\binom{j+d-2}{j-1}}_{\substack{\text{number of monomials of degree } d \\ \text{with grevlex smallest variable } x_j}}$$

Finally, since the leading monomials of $\widetilde{\mathcal{M}}_d$ are simply the h_d grevlex largest monomials of degree d, we obtain the final result

$$\begin{aligned}\#(\mathrm{LM}(G_{d+1}) \setminus \mathrm{LM}(G_d)) &= h_{d+1} - kh_d + c_{d+1} \\ &= h_{d+1} - kh_d + \sum_{j=1}^{\ell_d} \binom{j+d-2}{j-1}(j-1) \\ &\quad + \ell_d \left(h_d - \binom{\ell_d + d - 1}{\ell_d - 1} \right) \\ &= h_{d+1} + (\ell_d - k)h_d + \sum_{j=1}^{\ell_d} \binom{j+d-2}{j-1}(j-1) \\ &\quad - \ell_d \binom{\ell_d + d - 1}{\ell_d - 1}. \end{aligned}$$

□

5.2. **Reverse lexicographic determinantal ideals.** With the hope of applying Proposition 5.3, we investigate here the conditions under which the determinantal ideals we consider are indeed reverse lexicographic. We begin by showing that the Macaulay matrices of reverse lexicographic ideals possess a certain structure. Next, we construct an explicit Zariski open subset whose points correspond to reverse lexicographic ideals of the form $\mathcal{I}_{n-2}(M)$. That this Zariski open subset is nonempty is left as a conjecture, which we give insight into in Section 6.

Lemma 5.4. Let $F \subseteq \mathcal{R}$ be a sequence of homogeneous polynomials. Then $I = \langle F \rangle$ is a reverse lexicographic ideal if and only if for any $d \in \mathbb{Z}_{>0}$, the first h_d columns of the Macaulay matrix in degree d, $\mathcal{M}_d$, have rank $h_d = \mathrm{rk}(\mathcal{M}_d)$, or equivalently, the echelonized Macaulay matrix in degree d, $\widetilde{\mathcal{M}}_d$ takes the form

$$\widetilde{\mathcal{M}}_d = \left(\begin{array}{c|c} I & X \end{array} \right)$$

after having removed reductions to zero and up to a permutation of rows, where I is the identity matrix of size $h_d \times h_d$.

Proof. Fix $d \in \mathbb{Z}_{>0}$. Suppose I is reverse lexicographic, and let

$$\tau_0 = \min\{\tau \in \mathrm{LM}(I) : \deg(\tau) = d\}.$$

Then τ_0 appears as the rightmost pivot of $\widetilde{\mathcal{M}}_d$. Since

$$\{\sigma \in \mathrm{Mon}_d(\mathcal{R}) : \sigma \succ \tau\} \subseteq \mathrm{LM}(I),$$

all columns to the left of that indexed by τ_0 contain a pivot.
Conversely, suppose $\widetilde{\mathcal{M}}_d$ takes the desired form. For any $\tau \in \mathrm{LM}(I)$ of degree d, the column indexed by τ contains a pivot, and thus belongs to the left identity block. Thus, any column to the left of that indexed by τ must also contain a pivot. □

We conclude by showing that comaximal determinantal ideals of matrices of linear forms are reverse lexicographic.

Conjecture 5.5. Let RL be the property defined by

$$\mathrm{RL}(I) = \begin{cases} \texttt{true} & \text{if } I \text{ is reverse lexicographic} \\ \texttt{false} & \text{otherwise} \end{cases}.$$

Then for any $n \geq 3$, RL is $(4, n-2, n, 1)$-generic.

By Lemma 5.4, it is sufficient to prove that there exists some Zariski open subset $U \subseteq \mathbb{A}^{4n^2}$ such that for all $a \in U$, for any $d \in \mathbb{Z}_{>0}$, the reduced Macaulay matrix $\widetilde{\mathcal{M}}_d(F_{n-2}(\phi_a(\mathscr{A}_n^1)))$ takes the form

$$\widetilde{\mathcal{M}}_d(F_{n-2}(\phi_a(\mathscr{A}_n^1))) = \left(\begin{array}{c|c} I & X \end{array} \right)$$

after a suitable row permutation and removal of reductions to zero. Recall that the notation used here was introduced in Section 3.

By Proposition 4.3, there exists a Zariski open subset $U_{\mathrm{HS}} \subseteq \mathbb{A}^{4n^2}$ such that for all $a \in U_{\mathrm{HS}}$, the Hilbert series of $\mathcal{I}_{n-2}(\phi_a(\mathscr{A}_n^1))$ is the one given in Proposition 4.3. For any $d \in \mathbb{Z}_{>0}$, let $h_d = \mathrm{HF}_{\mathcal{I}_{n-2}(\phi_a(\mathscr{A}_n^1))}(d)$.

Now fix some $d \in \mathbb{Z}_{>0}$, $n-1 \leq d \leq 2n-3$. The determinant of the square submatrix of the Macaulay matrix $\widetilde{\mathcal{M}}_d(F_{n-2}(\mathscr{A}_n^1))$ given by the first h_d columns after removing zero rows is a polynomial in $\mathfrak{a}$, $g_d(\mathfrak{a}) \in \Bbbk[\mathfrak{a}]$.

The distinguished Zariski open set $\mathbb{A}^{4n^2} \smallsetminus V(g_d(\mathfrak{a}))$ consists precisely of those $a \in \mathbb{A}^{4n^2}$ such that

$$\widetilde{\mathcal{M}}_d(F_{n-2}(\mathscr{A}_n^1)) = \left(\begin{array}{c|c} I & X \end{array} \right).$$

By [FSS13, Corollary 19], there exists a Zariski open subset $O \subseteq \mathbb{A}^{4n^2}$ such that the largest degree Macaulay matrix which needs to be reduced is $\mathcal{M}_{2n-3}$. Thus, letting

$$U_{\mathrm{RL}} = O \cap U_{\mathrm{HS}} \cap \bigcap_{d=n-1}^{2n-3} \left(\mathbb{A}^{4n^2} \smallsetminus V_{\overline{\Bbbk}}(g_d(\mathfrak{a})) \right),$$

for any $a \in U_{\mathrm{RL}}$, the ideal $\mathcal{I}_{n-2}(\phi_a(\mathscr{A}_n^1))$ is reverse lexicographic.

It is not clear, however, that the set U_{RL} is nonempty. Equivalently, it is not clear that the polynomials $g_d(\mathfrak{a}) \in \Bbbk[\mathfrak{a}]$ are nonzero.

In [Par10, Theorem 3] (see also the references therein), necessary and sufficient conditions are given in order for a given power series to be the Hilbert series of a reverse lexicographic ideal. By Lemma 4.4, these assumptions are satisfied by the Hilbert series given in Proposition 4.3.

In the following section, we relate Conjecture 5.5 to the Lefschetz properties (see [HMM$^+$13b]), and give a connection between Conjecture 5.5 and a conjecture of Goto (see [Got74]).

6. Determinantal ideals and the Lefschetz properties

We devote this section to exploring conditions under which determinantal ideals possess the so-called Lefschetz properties, in the hope of shedding some light on Conjecture 5.5. These properties have been widely studied in various contexts, notably that of Artinian Gorenstein algebras.

This section is entirely self-contained, and for ease of exposition we do not provide definitions of several classical properties from commutative algebra (e.g. Artinian, Gorenstein). Such definitions and a wealth of related facts can be found, e.g., in [Mat87].

Definition 6.1 ([HMM$^+$13b, Definitions 3.1 and 3.8])**.** Let $A = \bigoplus_{d=0}^{c} A_d$ be a graded Artinian $\Bbbk$-algebra with $A_c \neq 0$. The algebra A has the *weak Lefschetz property*, or simply WLP if there exists some $\ell \in A_1$ such that for all $0 \leq d \leq c-1$, the map of $\Bbbk$-vector spaces

$$\times \ell : A_d \to A_{d+1}$$

given by multiplication by ℓ has full rank. Such an ℓ is called a *weak Lefschetz element*. If, in addition, for all $0 \leq d \leq c-1$ and $1 \leq s \leq c-d$, the map

$$\times \ell^s : A_d \to A_{d+s}$$

has full rank, then A is said to have the *strong Lefschetz property*, or simply SLP, and ℓ is called a *strong Lefschetz element*.

A natural generalization is the t-Lefschetz property.

Definition 6.2 ([HMM+13a, Definition 6.1])**.** Let $A = \bigoplus_{d=0}^{c} A_d$ be a graded Artinian $\Bbbk$-algebra. For some $t \geq 1$, A has the t-WLP (resp. t-SLP) if there are some $\ell_1, \ldots, \ell_t \in A_1$ such that ℓ_1 is a weak (resp. strong) Lefschetz element for A and, for each $1 < i \leq t$, the linear form ℓ_i is a weak (resp. strong) Lefschetz element for $A/(\ell_1, \ldots, \ell_{i-1})$.

When A is an Artinian ideal of a polynomial ring over $\Bbbk$, the notion of the t-SLP has useful description in terms of the Hilbert series of A.

Proposition 6.3 ([HMM+13a, Remark 6.11])**.** Let $I \subseteq \mathcal{R}$ be a graded Artinian ideal. Then ℓ is a Lefschetz element for $\mathcal{R}/I$ if and only if for all $s \geq 1$,

$$\mathrm{HF}_{\mathcal{R}/(I+\langle \ell^s \rangle)}(d) = \max\{\mathrm{HF}_{\mathcal{R}/I}(d) - \mathrm{HF}_{\mathcal{R}/I}(d-s), 0\}.$$

If $I \subseteq \mathcal{R}$ is an Artinian ideal, then $\mathcal{R}/I$ has dimension zero. Thus, there is some D such that for all $d > D$, $\mathrm{HF}_{\mathcal{R}/I}(d) = 0$. Clearly, one can restrict to $s \leq D$ in the above proposition.

Theorem 6.4 ([HMM+13a, Corollary 6.30])**.** Let $I \subseteq \Bbbk[x_1, x_2, x_3, x_4]$ be a graded Artinian ideal such that $\mathcal{R}/I$ has the 2-SLP. Then the generic initial ideal $\mathrm{gin}(I)$ of I with respect to the grevlex order is the unique weakly reverse lexicographic ideal with Hilbert function $\mathrm{HF}_{\mathcal{R}/I}$.

To establish Conjecture 5.5, it is therefore sufficient to prove, in our setting, that the 2-SLP is $(4, n-2, n, 1)$-generic. On the other hand, while it would not establish Conjecture 5.5, it would still be useful to discern whether or not the WLP is $(4, n-2, n, 1)$-generic.

Theorem 6.5 ([MMR03, Remark 4.4])**.** Let $I \subseteq \Bbbk[x_1, \ldots, x_k]$ be a graded ideal. If I is Artinian and has no generator in degree 1, and if the quotient $\mathcal{R}/I$ is Gorenstein and compressed with even socle degree, then $\mathcal{R}/I$ has the weak Lefschetz property.

The socle degree of a zero-dimensional ideal $I \subseteq \Bbbk[x_1, \ldots, x_k]$ is simply the degree of its Hilbert series, which is a polynomial. In this context, to be compressed simply means that $\mathrm{HF}_{\mathcal{R}/I}(d) = \mathrm{HF}_{\mathcal{R}}(d)$ for all $0 \leq d \leq \frac{s}{2}$, where $s = \deg(H_{\mathcal{R}/I}(t))$ is the socle degree of $\mathcal{R}/I$.
By [FSS13, Theorem 10], the property of being zero-dimensional is $(4, n-2, n, 1)$-generic, thus so is the property of being Artinian.
As soon as $n \geq 3$, the 2-minors of M are of degree at least 2 and generate $\mathcal{I}_{n-2}(M)$. Again by [FSS13, Theorem 10], the property that $\mathcal{R}/I$ has socle degree exactly $2n-2$ is $(4, n-2, n, 1)$-generic.
If M is a matrix of linear forms the degree of the $(n-1)$-minors of M is $n-1$. Thus, the property that $\mathcal{R}/I$ is compressed is also $(4, n-2, n, 1)$-generic.
What remains is to establish that the property of being Gorenstein is $(4, n-2, n, 1)$-generic. This is not so clear, and is in fact directly related to a conjecture due to Goto:

Conjecture 6.6 ([Got74])**.** Let $\Bbbk[x_{11}, \ldots, x_{pq}]$ be a polynomial ring over a field in pq indeterminates, with $q \geq p$. Let X be the $p \times q$ matrix whose (i,j)-th entry is x_{ij}. Then $\Bbbk[x_{11}, \ldots, x_{pq}]/\mathcal{I}_{r+1}(X)$ is Gorenstein if and only if $(q-p)r = 0$.

Since we work with square matrices, the condition that $(q-p)r = 0$ in Goto's conjecture is satisfied. So, if true, Goto's conjecture would establish that the determinantal ring of $n-1$ minors of the generic $n \times n$ matrix is Gorenstein.

7. A signature-based Gröbner basis algorithm for $\mathcal{I}_{n-2}(M)$

We describe here the algorithm DetGB, an altered version of the F_5 algorithm from [GNSED23], which given a matrix M of linear forms over $\mathcal{R}$ computes the reduced grevlex Gröbner basis for $\mathcal{I}_{n-2}(M)$. It is precisely this algorithm which we analyze in the subsequent section. In contrast to the standard matrix-F_5 algorithm (see [Fau02] and [BFS15]), the algorithm which we analyze does not compute Gröbner bases for subsequences of the input sequence. However, as in the matrix-F_5 algorithm, the algorithm described below does compute the Gröbner basis degree by degree.

7.1. **A signature-based Gröbner basis algorithm for modules.** We begin by describing an algorithm (Algorithm 1) which, given a set $\mathbf{F}$ of homogeneous elements (all of the same degree) of the free module $\mathcal{R}^m$, a monomial order $\succ$ on $\mathcal{R}$, a subset $Z \subseteq \mathrm{LM}_{\succ_{\mathrm{TOP}}}(\mathrm{Syz}(\mathbf{F}))$, and a degree bound D, computes the reduced D-$\succ_{\mathrm{TOP}}$-Gröbner basis of $\langle \mathbf{F} \rangle$ while avoiding those reductions to zero which arise from the leading monomials given by Z.

Algorithm 1 ModGB$(F, \succ, Z, D)$

Input: A collection of homogeneous module elements $\mathbf{F} = \{\mathbf{f}_1, \ldots, \mathbf{f}_s\} \subseteq \mathcal{R}^m$ all of degree d_0, a monomial order $\succ$ on $\mathcal{R}$, a subset $Z \subseteq \mathrm{LM}_{\succ_{\mathrm{TOP}}}(\mathrm{Syz}(\mathbf{F}))$, and a degree bound D.

Output: The reduced D-Gröbner basis of the module $\langle \mathbf{F} \rangle$ with respect to the module order $\mathrm{TOP}_{\succ}$.

for $i \in [1, \ldots, s]$ **do**
  $\mathcal{M}_{d_0} \leftarrow$ concatenate $\mathbf{f}_i$ to $\mathcal{M}_{d_0}$ with signature $(i, 1)$
$\widetilde{\mathcal{M}}_{d_0} \leftarrow \mathrm{rref}(\mathcal{M}_{d_0})$
$G \leftarrow \mathrm{rows}(\widetilde{\mathcal{M}}_{d_0})$
for $d \in [d_0 + 1, \ldots, D]$ **do**
  for $g \in \mathrm{rows}(\widetilde{\mathcal{M}}_{d-1})$ **do**
    $(i, \tau) \leftarrow \mathrm{sgn}(g)$
    for $j \in \max_k\{x_k \mid \tau\}$ **do**
      if $x_k \tau e_i \notin Z$ **then**
        $\mathcal{M}_d \leftarrow$ concatenate $x_k g$ to $\mathcal{M}_d$ with signature $(i, x_k\tau)$
  $\widetilde{\mathcal{M}}_d \leftarrow \mathrm{rref}(\widetilde{\mathcal{M}}_d)$
  $G \leftarrow G \cup \mathrm{rows}(\mathcal{M}_d)$
return G

In Algorithm 1, $\mathrm{rref}(\mathcal{M}_d)$ is the reduced row echelon form of a Macaulay matrix $\mathcal{M}_d$, and $\mathrm{rows}(\widetilde{\mathcal{M}}_d)$ is the set of rows of $\widetilde{\mathcal{M}}_d$, interpreted as elements of $\mathcal{R}^m$.
The algorithm works by building Macaulay matrices in various degrees for the module $\langle \mathbf{f}_1, \ldots, \mathbf{f}_s \rangle$. It then echelonizes these Macaulay matrices using a general-purpose

echelon form algorithm. From these echelonized matrices, it extracts polynomials whose leading terms do not belong to the ideal generated by the leading terms of the intermediate Gröbner basis computed. Algorithm 1 uses the additional data of leading terms of syzygies (the input Z) to avoid adding to the Macaulay matrix rows which are known to reduce to zero upon echelonization. Furthermore, it builds the Macaulay matrix $\mathcal{M}_d$ from $\widetilde{\mathcal{M}}_{d-1}$ rather than from the original system $\mathbf{f}_1, \ldots, \mathbf{f}_s$ since in doing so, a portion of $\mathcal{M}_d$ will already be echelonized. It is precisely by exploiting this specific structure of $\mathcal{M}_d$ that we arrive at sharp complexity analyses in Section 8.
The termination and correctness of Algorithm 1 follow essentially from Theorem 2.4. A detailed proof can be found in [BFS15, Theorem 9].

Remark 7.1. When $m = 1$, Algorithm 1 is essentially just Lazard's algorithm (see [Laz83]), with the additional input of a set of precomputed syzygies. Given this, the standard matrix-F_5 algorithm is recovered as a very slight alteration to Algorithm 1 by updating the set Z with the leading monomials of the matrices $\widetilde{\mathcal{M}}_d$ along the way.

7.2. **The DetGB algorithm.** Using Algorithm 1 combined with syzygy information from the Gulliksen-Negård complex leads to Algorithm 2 (see also [GNSED23, Algorithm 3]) to compute Gröbner bases for the determinantal ideals considered in this paper.

Algorithm 2 DetGB(M)

Input: An $n \times n$ matrix M of homogeneous linear forms in four variables.
Output: The reduced grevlex Gröbner basis for $\mathcal{I}_{n-2}(M)$.

1: $S_2 \leftarrow$ a set of generators for $\mathrm{Syz}_2(F_{n-2}(M))$ computed using the Gulliksen-Negård complex.
2: $S_1 \leftarrow$ a set of generators for $\mathrm{Syz}(F_{n-2}(M))$ computed using the Gulliksen-Negård complex.
3: $L_2 \leftarrow \mathrm{ModGB}(S_2, \mathrm{grevlex}, \emptyset, n-3)$
4: $L_1 \leftarrow \mathrm{ModGB}(S_1, \mathrm{grevlex}, \mathrm{LM}_{\succ_{\mathrm{TOP}}}(L_2), n-2)$
5: **return** $\mathrm{ModGB}(F_{n-2}(M), \mathrm{grevlex}, \mathrm{LM}_{\succ_{\mathrm{TOP}}}(L_1), 2n-3)$

The termination and correctness of Algorithm 2 is proven in [GNSED23, Proposition 21].

Remark 7.2. If $\mathcal{I}_{n-2}(M)$ is not Cohen-Macaulay, the Gulliksen-Negård complex need not be a free resolution for $\mathcal{I}_{n-2}(M)$. However, it is still a complex. Thus, the syzygy modules of $\mathcal{I}_{n-2}(M)$ contain, possibly properly, the modules computed from the Gulliksen-Negård complex. It is for this reason that we do not need to assume any genericity properties in order for Algorithm 2 to be correct.
See [GNSED23, Remarks 10 and 20] for a more detailed discussion.

Remark 7.3. The image of the standard basis elements of $\mathcal{E}_0$ under the augmentation map ϵ in the Gulliksen-Negård complex are actually the cofactors of order $n-1$ of M, not the minors of order $n-1$. Computing the images of the boundary maps in the Gulliksen-Negård complex therefore gives syzygy modules for the cofactors of order $n-1$, rather than the minors, as we would like. This can be corrected by simply replacing $F_{n-2}(M)$ with the cofactors of order $n-1$ of M in Algorithm 2. Alternatively, we can easily turn the syzygies of the cofactors obtained from the

Gulliksen-Negård complex into syzygies of the minors, as explained in the proof of [GNSED23, Theorem 9].

8. Complexity analysis

We consider a matrix of the form $M = \phi_a(\mathscr{A}_n^1)$, where a is taken to be a point in some suitable Zariski open subset of $\mathbb{A}^{4n^2}$. We make precise which Zariski open subsets we must take a to lie in below, appealing to the various genericity statements we have established above (e.g. Propositions 3.2 and 4.3 and Conjecture 5.5). Our complexity analysis begins by computing the number of polynomials of each degree in the reduced grevlex Gröbner basis of $\mathcal{I}_{n-2}(M)$.

The coefficient of t^d in the Hilbert series of $\mathcal{I}_{n-2}(M)$ is, by definition, the dimension of the $\Bbbk$-vector space of homogeneous polynomials in $\mathcal{I}_{n-2}(M)$ of degree d. This dimension is also precisely the rank of the Macaulay matrix of $F_{n-2}(M)$ in degree d. Combining these ranks with the aforementioned count of polynomials of degree d in the reduced grevlex Gröbner basis of $\mathcal{I}_{n-2}(M)$ allows us to compute tight bounds on the complexity of the overall Gröbner basis computation using fast linear algebra techniques.

Following the standard for complexity bounds, we use the Bachmann-Landau notation $O(\cdot)$ (see e.g. [CLRS22, Section 3.1]).

8.1. **Bounding $\#(\mathrm{LM}(G_{d+1}) \smallsetminus \mathrm{LM}(G_d))$.** The work of computing the number of polynomials of degree d in the reduced grevlex Gröbner basis for $\mathcal{I}_{n-2}(M)$ is already accomplished by our analysis of staircases of reverse lexicographic ideals in Section 5. The following proposition arises from plugging in the relevant quantities into the formula given in Proposition 5.3.

Proposition 8.1. Suppose Conjecture 5.5 is true. Fix $a \in U_{\mathrm{RL}} \cap U_{\mathrm{HS}} \subseteq \mathbb{A}^{4n^2}$. Let $M = \phi_a(\mathscr{A}_n^1)$. For any integer $n-1 \leq d < 2n-3$,

$$\#(\mathrm{LM}(G_{d+1}) \smallsetminus \mathrm{LM}(G_d)) = \frac{(d-2n+3)(d-2n+2)}{2},$$

where G_d is the reduced d-Gröbner basis for $\mathcal{I}_{n-2}(M)$ with respect to the grevlex order.

Proof. If Conjecture 5.5 is true, then the ideal $\mathcal{I}_{n-2}(M)$ is reverse lexicographic. Therefore, we can apply Proposition 5.3. We begin by showing that for all $d \geq n-1$, the integer ℓ_d is 3. Recall, from the statement of Proposition 5.3, that ℓ_d is defined to be the largest integer such that

$$\binom{\ell_d + d - 1}{\ell_d - 1} < h_d,$$

where $h_d = \mathrm{HF}_{\mathcal{I}_{n-2}(M)}(d)$. For any $a \in U_{\mathrm{HS}}$, the Hilbert series $H_{\mathcal{I}_{n-2}(M)}(t)$ is given by Proposition 4.3.

First, note that $h_{n-1} = n^2$ and

$$\binom{(n-1)+2}{2} = \frac{n^2+n}{2}.$$

Since $n > 1$, this shows that $\ell_{n-1} \geq 3$. As $k = 4$, $\ell_{n-1} \leq 3$.

We proceed by induction. Suppose $\ell_d = 3$ for some $d \geq n-1$. Then there must be at least one monomial τ in which the variable x_4 appears in $\mathrm{LM}(G_d)$. Subsequently

for any variable x, $x\tau \in \mathrm{LM}(G_{d+1})$ and $x\tau$ contains the variable x_4 as well, showing that $\ell_{d+1} = 3$.
Finally, applying Proposition 5.3, we obtain

$$\begin{aligned}\#\,\mathrm{LM}(G_{d+1}) \smallsetminus \mathrm{LM}(G_d) &= h_{d+1} - h_d + \binom{d}{1} + 2\binom{d+1}{2} - 3\binom{d+2}{2} \\ &= h_{d+1} - h_d + d + 2\binom{d+1}{2} - 3\binom{d+2}{2} \\ &= \frac{(d-2n+3)(d-2n+2)}{2}.\end{aligned}$$

□

8.2. **Lower bounds.** As a first application of Proposition 8.1, we establish an exact expression for the size of the reduced grevlex Gröbner basis of ideals of the form $\mathcal{I}_{n-2}(M)$ under certain genericity assumptions.

Proposition 8.2. Fix $a \in U_{\mathrm{RL}} \subseteq \mathbb{A}^{4n^2}$. Let $M = \phi_a(\mathscr{A}_n^1)$. The total number of polynomials in the reduced grevlex Gröbner basis for $\mathcal{I}_{n-2}(M)$ is

$$\#G = \frac{n(n+1)(n+2)}{6}.$$

Proof. Enumerating the polynomials in the reduced grevlex Gröbner basis for $\mathcal{I}_{n-2}(M)$ is equivalent to enumerating the leading monomials of these polynomials. That is,

$$\#G = \#\,\mathrm{LM}(G_{n-1}) + \sum_{d=n-1}^{2n-4} \#(\mathrm{LM}(G_{d+1}) \smallsetminus \mathrm{LM}(G_d)).$$

Using Proposition 8.1,

$$\#G = n^2 + \sum_{d=n-1}^{2n-4} \frac{(d-2n+3)(d-2n+2)}{2} = \frac{n(n^2+3n+2)}{6}.$$

□

Recall that here, we consider the computation of a dense representation of the sought Gröbner basis, meaning that all coefficients in $\Bbbk$ of all elements in this basis are explicitly computed.
The expression obtained in Proposition 8.2 counts only the leading monomials of the polynomials in the reduced grevlex Gröbner basis of $\mathcal{I}_{n-2}(M)$, and not the smaller monomials in these polynomials. In the following theorem, we compute — under our genericity assumptions — the number of nonzero coefficients in each of these polynomials.

Theorem 8.3. Suppose Conjecture 5.5 is true. Fix $a \in U_{\mathrm{RL}} \cap U_{\mathrm{HS}} \subseteq \mathbb{A}^{4n^2}$. Let $M = \phi_a(\mathscr{A}_n^1)$. The number of elements of $\Bbbk$ in the dense representation of the reduced grevlex Gröbner basis of $\mathcal{I}_{n-2}(M)$ is asymptotically bounded from below by n^6.

Proof. Since $a \in U_{\mathrm{HS}}$, the Hilbert series of $\mathcal{I}_{n-2}(M)$ is the one given in Proposition 4.3. Let $h_d = \mathrm{HF}_{\mathcal{R}/\mathcal{I}_{n-2}(M)}(d)$. The number of monomials appearing in a degree d polynomial in the reduced grevlex Gröbner basis for $\mathcal{I}_{n-2}(M)$ is

$$\binom{3+d}{3} - h_d + 1.$$

Therefore, using Proposition 8.1, we find that the number of nonzero monomials appearing in the grevlex Gröbner basis for $\mathcal{I}_{n-2}(M)$ is

$$N = n^2\left(\binom{2+n}{3} - n^2 + 1\right) + \sum_{d=n-1}^{2n-4} \frac{(d-2n+3)(d-2n+2)}{2}\left(\binom{3+d}{3} - h_d + 1\right).$$

Expanding this gives

$$N = \frac{1}{72}n^6 + \frac{13}{120}n^5 - \frac{4}{9}n^4 + \frac{13}{24}n^3 + \frac{31}{72}n^2 + \frac{7}{20}n \qquad \square$$

8.3. **Upper bounds.** For a given degree $d > n-1$, Algorithm 2 builds the Macaulay matrix in degree d by multiplying each row of the Macaulay matrix in degree $d-1$ by each variable, utilizing the signatures attached to each row to avoid redundancies in rows. The reverse lexicographic property of determinantal ideals provides the unreduced Macaulay matrix in degree d with a precise structure, which we analyze to obtain complexity upper bounds.

Proposition 8.4. Suppose Conjecture 5.5 is true. Fix $a \in U_{\mathrm{RL}} \subseteq \mathbb{A}^{4n^2}$. Let $M = \phi_a(\mathscr{A}_n^1)$ and let $d \in \mathbb{Z}_{>0}$, $n-1 \leq d < 2n-3$. Then after a suitable row permutation, the unreduced Macaulay matrix $\mathcal{M}_{d+1}$ of $\mathcal{I}_{n-2}(M)$ built by Algorithm 2 is of the form

$$\left(\begin{array}{c|c} T_{d+1} & X_{d+1} \\ \hline A_{d+1} & Y_{d+1} \end{array}\right)$$

where T_{d+1} is a square upper triangular block of size $h_{d+1} - \frac{(d-2n+3)(d-2n+2)}{2}$ and $h_{d+1} = \mathrm{HF}_{\mathcal{I}_{n-2}(M)}(d+1)$ is the Hilbert function of $\mathcal{I}_{n-2}(M)$ evaluated at $d+1$.

Proof. Let G be the reduced grevlex Gröbner basis of $\mathcal{I}_{n-2}(M)$. We partition the rows of $\widetilde{\mathcal{M}}_{d+1}$ into the following two sets

$$R_1 = \{f \in \mathrm{rows}(\widetilde{\mathcal{M}}_{d+1}) : f \in G\} \quad R_2 = \{f \in \mathrm{rows}(\widetilde{\mathcal{M}}_{d+1}) : f \notin G\}.$$

Let $\tau = \min_{f \in R_2}\{\mathrm{LM}(f)\}$. Then there must exist some variable x_j such that $\frac{\tau}{x_j} \in \mathrm{LM}(G)$. Fix $\sigma \in R_1$. In Proposition 8.1 it was shown that all monomials involving x_1, x_2, x_3 appear in $\mathrm{LM}(G_{n-1})$. Thus, since $d+1 > n-1$, $x_4 \mid \sigma$. As G is a reduced Gröbner basis and $\sigma \in \mathrm{LM}(G)$, the monomial $\frac{\sigma}{x_4}$ is not in $\mathrm{LM}(G)$. Since we assume Conjecture 5.5, this forces $\frac{\tau}{x_j} \succ \frac{\sigma}{x_4}$. Subsequently, since $x_j \succ x_4$, we have that $\tau \succ \sigma$.

This shows that any monomial of $\mathrm{LM}(R_1)$ is smaller than τ. On the other hand, assuming Conjecture 5.5, for any $\tau' \succ \tau$, there exists some $g \in R_2$ such that $\mathrm{LM}(g) = \tau'$.

Now for any polynomial $g \in R_2$, there exists some $h \in \mathrm{rows}(\widetilde{\mathcal{M}}_d)$ such that $\mathrm{LM}(h) \mid \mathrm{LM}(g)$. Since Algorithm 1 constructs the rows of $\mathcal{M}_{d+1}$ by multiplying the rows of $\widetilde{\mathcal{M}}_d$ by suitable variables, we see that there must be a row of $\mathcal{M}_{d+1}$ with leading monomial precisely $\mathrm{LM}(g)$. Thus, the set of rows of $\mathcal{M}_{d+1}$ which, upon echelonization, are in R_2 form a submatrix of $\mathcal{M}_{d+1}$ of the form

$$\left(\begin{array}{c|c} T_{d+1} & X_{d+1} \end{array}\right)$$

with T_{d+1} upper triangular. The rows of T_{d+1} are in bijection with R_2, and by Proposition 8.1, the set R_1 has cardinality $\frac{(d-2n+3)(d-2n+2)}{2}$. As $\mathcal{M}_{d+1}$ has exactly h_{d+1} rows, we see that T_{d+1} has $h_{d+1} - \frac{(d-2n+3)(d-2n+2)}{2}$ rows. □

By Proposition 8.4, A_{d+1} is a matrix with $\alpha_{d+1} = \frac{(d-2n+3)(d-2n+2)}{2}$ rows, T_{d+1} is a matrix with $\beta_{d+1} = h_{d+1} - \alpha_{d+1}$ rows, and and X_{d+1} is a matrix with $\gamma_{d+1} = \binom{4+d}{3} - \beta_{d+1}$ columns. We begin by establishing various useful facts about the behavior of $h_{d+1}, \alpha_{d+1}, \beta_{d+1}, \gamma_{d+1}$.

Lemma 8.5. For all $n-1 < d < 2n-3$, $\alpha_{d+1} < \alpha_d$.

Proof. Let $f(d) = \alpha_d$ and view f as a continuous function in one real variable. Then $f'(d) = d - 2n + \frac{5}{2}$ has its unique root at $d = 2n - \frac{5}{2}$. Thus, f is strictly decreasing on the interval $\left(-\infty, 2n - \frac{5}{2}\right]$. □

Lemma 8.6. For all $n-1 \leq d < 2n-3$, $\alpha_{d+1} < \beta_{d+1}$.

Proof. In view of Lemmas 4.4 and 8.5, it suffices to show that $\alpha_n < \frac{h_n}{2}$. We have $\alpha_n = \frac{n^2-3n+2}{2}$ and $h_n = 2n^2 + 2$. Thus, $\frac{h_n}{2} - \alpha_n = \frac{n^2+3n}{2}$, which is certainly positive for $n \geq 3$. □

Lemma 8.7. For all $n-1 \leq d < 2n-3$, $\alpha_{d+1} \leq \gamma_{d+1}$.

Proof. Recall that $h_{d+1} = \dim_{\Bbbk}(\mathcal{I}_{n-2}(M)_{d+1})$. The $\Bbbk$-vector space $\mathcal{I}_{n-2}(M)_{d+1}$ is a sub-$\Bbbk$ vector space of $\mathcal{R}_{d+1}$. Since $\dim_{\Bbbk}(\mathcal{R}_{d+1}) = \binom{4+d}{3}$, we have that $h_{d+1} \leq \binom{4+d}{3}$. Finally,

$$\begin{aligned}\gamma_{d+1} &= \binom{4+d}{3} - \beta_{d+1} \\ &= \binom{4+d}{3} - h_{d+1} + \alpha_{d+1} \\ &\geq \alpha_{d+1}\end{aligned}$$

□

Before turning to the complexity of echelonizing a Macaulay matrix in a fixed degree, we need one final auxiliary lemma regarding the cost of solving several triangular systems.

Lemma 8.8 (see [DGP04, Lemma 3.1])**.** Let $U \in \Bbbk^{p \times p}$ be an invertible $p \times p$ upper triangular matrix and $V \in \Bbbk^{p \times q}$ a $p \times q$ matrix. Let $C(p,q)$ be the arithmetic complexity of computing $U^{-1}V$ using [DGP04, `ULeft-TRSM`(U,V)]. Then

$$C(p,q) \in \begin{cases} O(qp^{\omega-1}) & \text{if } p \leq q \\ O(p^2q^{\omega-2}) & \text{if } p > q \end{cases}.$$

Proof. For $p \leq q$, this is precisely the statement of [DGP04, Lemma 3.1]. Assume then that $p > q$. In the following, we denote by C_ω the constant associated to rectangular matrix multiplication with exponent ω. That is, the cost of multiplying a $p \times q$ matrix by a $q \times s$ matrix (all with entries in $\Bbbk$) is bounded by $C_\omega \min\{p,q,s\}^{\omega-2} \max\{pq, ps, qs\}$. We use the case $p \leq q$ as a base case for the

recursion. The complexity in this case is given directly by [DGP04, Lemma 3.1]. That is,

$$C(p,q) = \begin{cases} \frac{C_\omega}{2(2^{\omega-2}-1)} qp^{\omega-1} & \text{if } p \leq q \\ C(\lceil \frac{p}{2} \rceil, q) + C(\lfloor \frac{p}{2} \rfloor, q) + C_\omega p^2 q^{\omega-2} & \text{otherwise} \end{cases}.$$

By padding U with an identity block and V with zeroes, we may assume that $\frac{p}{q}$ is a power of two. Subsequently, we have

$$\begin{aligned} C(p,q) &= \frac{p}{q} C(q,q) + C_\omega p^2 q^{\omega-2} \sum_{j=0}^{\log_2\left(\frac{p}{q}\right)-1} \frac{1}{2^j} \\ &= \frac{C_\omega}{2(2^{\omega-2}-1)} pq^{\omega-1} + 2C_\omega p^2 q^{\omega-2} \left(1 - \frac{q}{p}\right) \\ &= 2C_\omega p^2 q^{\omega-2} + \left(\frac{C_\omega}{2(2^{\omega-2}-1)} - 2C_\omega\right) pq^{\omega-1} \end{aligned}$$

as desired. □

Putting together Lemmas 4.4 and 8.5 to 8.7, we can compute an upper bound on the cost of echelonizing a Macaulay matrix in a fixed degree.

Proposition 8.9. For any $n-1 \leq d \leq 2n-3$, the number of arithmetic operations in $\Bbbk$ required to compute the matrix $\widetilde{\mathcal{M}}_{d+1}$ from $\mathcal{M}_{d+1}$ is in

$$O\left(\beta_{d+1}^2 \alpha_{d+1}^{\omega-2} + \alpha_{d+1}^{\omega-2} \beta_{d+1} \gamma_{d+1}\right).$$

Proof. The computation of $\widetilde{\mathcal{M}}_{d+1}$ from $\mathcal{M}_{d+1}$ can be broken up into four steps.
Step 1. First, we echelonize the upper block, which is of the form $\left(\begin{array}{c|c} T_{d+1} & X_{d+1} \end{array}\right)$, with T_{d+1} upper triangular. Applying Lemma 8.8, the cost of this step is $O(\beta_{d+1}^2 \alpha_{d+1}^{\omega-2})$
Step 2. Next, we use the I_{d+1} block to eliminate A_{d+1}. The resulting matrix takes the form

$$\left(\begin{array}{c|c} I_{d+1} & X_{d+1} \\ \hline 0 & Y_{d+1} - A_{d+1} X_{d+1} \end{array}\right).$$

The arithmetic complexity of this step is bounded by the cost of computing $A_{d+1}X_{d+1}$. The matrix A_{d+1} has α_{d+1} rows and β_{d+1} columns, while X_{d+1} has β_{d+1} rows and γ_{d+1} columns. By Lemmas 8.6 and 8.7,

$$\min\{\alpha_{d+1}, \beta_{d+1}, \gamma_{d+1}\} = \alpha_{d+1}.$$

Hence, by [Kni95, Section 2.1], the matrix $A_{d+1}X_{d+1}$ can be computed using $O(\alpha_{d+1}^{\omega-2} \beta_{d+1} \gamma_{d+1})$ arithmetic operations in $\Bbbk$.
Step 3. Next, we compute the reduced row echelon form of $Y_{d+1} - A_{d+1}X_{d+1}$ which has α_{d+1} rows and β_{d+1} columns. By Lemma 8.6, and using the general results of [Sto00, Section 2.2] (see also [JPS13, Appendix A]), this can be done using $O(\alpha_{d+1}^{\omega-1} \gamma_{d+1})$ operations in $\Bbbk$.
Step 4. The matrix after the previous step takes the form

$$\left(\begin{array}{c|c|c} I_{d+1} & X_{d+1}^{(1)} & X_{d+1}^{(2)} \\ \hline 0 & I^{(\alpha_{d+1})} & Y_{d+1} \end{array}\right),$$

where $X_{d+1} = \left(\begin{array}{c|c} X_{d+1}^{(1)} & X_{d+1}^{(2)} \end{array}\right)$ and $I^{(\alpha_{d+1})}$ is an identity matrix of size α_{d+1}. The final step of the echelonization process is then to reduce X_{d+1} using the identity

block $I^{(\alpha_{d+1})}$. The resulting matrix takes the form

$$\left(\begin{array}{c|c|c} I_{d+1} & 0 & X_{d+1}^{(2)} - X_{d+1}^{(1)} Y_{d+1} \\ \hline 0 & I^{(\alpha_{d+1})} & Y_{d+1} \end{array}\right).$$

Similarly to above, the arithmetic complexity of this step is bounded by that of computing $X_{d+1}^{(1)} Y_{d+1}$. The matrix $X_{d+1}^{(1)}$ has β_{d+1} rows and α_{d+1} columns, while the matrix Y_{d+1} has α_{d+1} rows and $\binom{4+d}{3} - h_{d+1}$ columns. Therefore, by the general bound given in [Kni95, Section 2.1], the number of arithmetic $\Bbbk$ operations required to compute the matrix $X_{d+1}^{(1)} Y_{d+1}$ is in

$$\begin{cases} O\left(\left(\binom{4+d}{3} - h_{d+1}\right)^{\omega-2} \alpha_{d+1}\beta_{d+1}\right) & \text{if } \alpha_{d+1} > \binom{4+d}{3} - h_{d+1} \\ O\left(\left(\binom{4+d}{3} - h_{d+1}\right) \alpha_{d+1}^{\omega-2}\beta_{d+1}\right) & \text{otherwise} \end{cases}$$

In the first case,

$$O\left(\left(\binom{4+d}{3} - h_{d+1}\right)^{\omega-2} \alpha_{d+1}\beta_{d+1}\right) \subseteq O(\alpha_{d+1}^{\omega-1}\beta_{d+1}) \subseteq O(\alpha_{d+1}^{\omega-2}\beta_{d+1}\gamma_{d+1})$$

and in the second case, since $\binom{4+d}{3} - h_{d+1} \geq \gamma_{d+1}$,

$$O\left(\left(\binom{4+d}{3} - h_{d+1}\right) \alpha_{d+1}^{\omega-2}\beta_{d+1}\right) \subseteq O(\alpha_{d+1}^{\omega-2}\beta_{d+1}\gamma_{d+1})$$

so the complexity of the second step dominates. □

Our main complexity upper bound, given in the following theorem, is now an easy consequence of Proposition 8.9.

Theorem 8.10. Fix $a \in U_{\mathrm{RL}} \subseteq \mathbb{A}^{4n^2}$. Let $M = \phi_a(\mathscr{A}_n^1)$. The number of arithmetic operations in $\Bbbk$ performed by Algorithm 2 when computing the reduced grevlex Gröbner basis for $\mathcal{I}_{n-2}(M)$ is in $O\left(n^{2\omega+3}\right)$.

Proof. Note first that all arithmetic operations occur when computing the $\widetilde{\mathcal{M}}_d$ from the $\mathcal{M}_d$. Secondly, note that the complexity of the final step of Algorithm 2 bounds the complexity of the algorithm as a whole, since the number of rows to be reduced in the Macaulay matrix in degree d for the first (resp. second) syzygy module is precisely the number of (a priori) reductions to zero encountered in $\mathcal{M}_{d+1}$ (resp. the Macaulay matrix in degree $d+1$ of the first syzygy module). Note also that $\mathcal{M}_{n-1}$ has n^2 rows, and $\binom{n+2}{3}$ columns, and is of rank n^2. Thus, by [Sto00, Section 2.2] (see also [JPS13, Appendix A]) the arithmetic complexity of computing $\widetilde{\mathcal{M}}_{n-1}$ from $\mathcal{M}_{n-1}$ is in

$$O\left(n^{2\omega-2}\binom{n+2}{3}\right) \subseteq O\left(n^{2\omega+1}\right).$$

It follows, by Proposition 8.9, that the total complexity of computing the reduced grevlex Gröbner basis for $\mathcal{I}_{n-2}(M)$ is in $O(n^{2\omega+1} + f_\omega(n))$, where

$$f_\omega(n) = \sum_{d=n-1}^{2n-4} \beta_{d+1}^2 \alpha_{d+1}^{\omega-2} + \alpha_{d+1}^{\omega-2}\beta_{d+1}\gamma_{d+1}.$$

By Lemma 8.5, for all $n-1 \leq d \leq 2n-4$, $\alpha_{d+1} \leq \alpha_n < n^2$, hence

$$f_\omega(n) \in O\left(n^{2\omega-4} \sum_{d=n-1}^{2n-4} \beta_{d+1}\gamma_{d+1} + \beta_{d+1}^2\right). \tag{4}$$

One can verify (e.g. using the Maple computer algebra system [MGH+05]) that

$$\sum_{d=n-1}^{2n-4} \beta_{d+1}\gamma_{d+1}+\beta_{d+1}^2 = \frac{619}{1260}n^7 - \frac{341}{360}n^6 - \frac{7}{360}n^5 + \frac{7}{36}n^4 - \frac{169}{360}n^3 - \frac{89}{360}n^2 - \frac{1}{420}n.$$

It follows that $f_\omega(n) \in O(n^{2\omega+3})$, which concludes the proof. □

Remark 8.11. The upper bound on Algorithm 2 obtained in Theorem 8.10 is subquadratic in the size of the dense representation of the output Gröbner basis obtained in Theorem 8.3.

Remark 8.12. When $\omega = 2$, the bound $O(n^{2\omega+3})$ becomes $O(n^7)$, which still differs from the lower bound on the output size obtained in Theorem 8.3 by a factor of n. This suggests that there might still be room for improvement upon the bound obtained in Theorem 8.10. In experiments, when working on input of matrices of homogeneous linear forms in four variables with coefficients chosen uniformly at random from some large prime field, one can observe that the submatrices A_d defined in Proposition 8.4 are sparse. Perhaps by taking into account this sparsity, a tighter upper bound could be achieved.

8.4. **The asymptotic behavior of $f_\omega(n)$.** In the proof of Theorem 8.10, only one upper bound is actually used — the bound $\alpha_{d+1} < n^2$. We conclude our complexity analysis by presenting precise asymptotics for $f_\omega(n)$ for various ω. Using the SageMath computer algebra system (see [The22]), we obtain the asymptotic data in Table 1. It suggests that the asymptotic result $f_\omega(n) = O\left(n^{2\omega+3}\right)$ obtained in Theorem 8.10 is sharp.

TABLE 1. The asymptotics of $f_\omega(n)$ compared to $n^{2\omega+3}$ for various $2 \leq \omega \leq 3$.

ω	$f_\omega(n) \sim_{n\to\infty}$	$n^{2\omega+3}$
3	$\frac{401}{18144}n^9$	n^9
2.7	$\frac{2^{\frac{7}{10}}\cdot 765332825537474763353 23}{27611718750000000000000000}n^{8.4}$	$n^{8.4}$
2.5	$\frac{29\sqrt{2}}{10080}n^8$	n^8
2.38	$\frac{2^{\frac{19}{50}}\cdot 380871054542460964056498187634372038 7}{41658431291580200195312500000000000000}n^{7.76}$	$n^{7.76}$
2	$\frac{619}{1260}n^7$	n^7

ACKNOWLEDGMENTS

Funding: The author is supported by *Quantum Information Center Sorbonne* (QICS); by the Agence nationale de la recherche (ANR) [ANR-19-CE40-0018 DE RERUM NATURA, ANR-18-CE33-0011 SESAME, and ANR-23-CE48-0003 CREAM]; the joint ANR-Austrian Science Fund FWF [ANR-22-CE91-0007 EAGLES and ANR-FWF ANR-19-CE48-0015 ECARP]; and the EOARD-AFOSR [FA8665-20-1-7029].

Some computations required for the proof of Theorem 8.10 were performed using Maple^{TM}.
The author would like to thank his Ph.D. advisors Mohab Safey El Din and Vincent Neiger for numerous helpful discussions and suggestions.

References

[BBB+20] M. Bardet, P. Briaud, M. Bros, P. Gaborit, V. Neiger, O. Ruatta, and J.-P. Tillich. An algebraic attack on rank metric code-based cryptosystems. In *Proceedings EUROCRYPT 2020*, volume 12105 of *LNCS*. Springer, 2020.

[BBC+20] M. Bardet, M. Bros, D. Cabarcas, P. Gaborit, R. Perlner, D. Smith-Tone, J.-P. Tillich, and J. Verbel. Improvements of algebraic attacks for solving the rank decoding and minrank problems. In *Proceedings ASIACRYPT 2020*, pages 507–536, 2020.

[BBC+22] J. Baena, P. Briaud, D. Cabarcas, R. Perlner, D. Smith-Tone, and J. Verbel. Improving Support-Minors Rank Attacks: Applications to GeMSS and Rainbow. In *Proceedings CRYPTO 2022*, pages 376–405, Cham, 2022. Springer.

[BCRV22] W. Bruns, A. Conca, C. Raicu, and M. Varbaro. *Determinants, Gröbner bases and cohomology*. Springer, 2022.

[Beu22] W. Beullens. Breaking rainbow takes a weekend on a laptop. In *Proceedings CRYPTO 2022*, pages 464–479. Springer, 2022.

[BFS99] J. F. Buss, G. S. Frandsen, and J. O. Shallit. The computational complexity of some problems of linear algebra. *J. Comput. Syst. Sci.*, 58(3):572–596, 1999.

[BFS15] M. Bardet, J.-C. Faugère, and B. Salvy. On the complexity of the F5 Gröbner basis algorithm. *J. Symbolic Comput.*, 70:49–70, 2015.

[BGH+10] B. Bank, M. Giusti, J. Heintz, M. Safey El Din, and É. Schost. On the geometry of polar varieties. *Appl. Algebra Engrg. Comm. Comput.*, 21(1):33–83, 2010.

[BGHP05] B. Bank, M. Giusti, J. Heintz, and L. M. Pardo. Generalized polar varieties: Geometry and algorithms. *J. Complexity*, 21(4):377–412, 2005.

[BGHS14] B. Bank, M. Giusti, J. Heintz, and M. Safey El Din. Intrinsic complexity estimates in polynomial optimization. *J. Complexity*, 30(4):430–443, 2014.

[BH98] Winfried Bruns and H. Jürgen Herzog. *Cohen-Macaulay Rings*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2 edition, 1998.

[BS15] I. Bannwarth and M. Safey El Din. Probabilistic algorithm for computing the dimension of real algebraic sets. In *Proceedings ISSAC 2015*, pages 37–44. ACM, 2015.

[Buc65] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. PhD thesis, University of Innsbruck, 1965.

[BV88] W. Bruns and U. Vetter. *Determinantal Rings*. Springer Berlin Heidelberg, 1988.

[CLO05] D. A. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*. Springer New York, New York, NY, 2005.

[CLO15] D. A. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms (fourth edition)*. Springer, 2015.

[CLRS22] Thomas H Cormen, Charles E Leiserson, Ronald L Rivest, and Clifford Stein. *Introduction to algorithms*. MIT press, 2022.

[Cou01] N. T. Courtois. Efficient zero-knowledge authentication based on a linear algebra problem MinRank. In *Proceedings ASIACRYPT 2001*, pages 402–421. Springer, 2001.

[Dee96] Todd Deery. Rev-lex segment ideals and minimal betti numbers. In *The Curves Seminar at Queen's*, volume 10, pages 193–219, 1996.

[DGP04] Jean-Guillaume Dumas, Pascal Giorgi, and Clément Pernet. Ffpack: Finite field linear algebra package. In *Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation*, ISSAC '04, page 119–126, New York, NY, USA, 2004. Association for Computing Machinery.

[DS05] J. Ding and D. Schmidt. Rainbow, a new multivariable polynomial signature scheme. In *Proceedings ACNS 2005*, pages 164–175. Springer, 2005.

[EF16] C. Eder and J.-C. Faugère. A survey on signature-based algorithms for computing Gröbner basis computations. *J. Symbolic Comput.*, pages 1–75, 2016.

[Eis95] D. Eisenbud. *Commutative Algebra: with a View Toward Algebraic Geometry*. Graduate Texts in Mathematics. Springer, 1995.

[Fau99] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases (f4). *J. Pure Appl. Algebra*, 139(1):61–88, 1999.

[Fau02] J.-C. Faugère. A new efficient algorithm for computing gröbner bases without reduction to zero (f5). In *Proceedings ISSAC 2002*, pages 75–83. ACM, 2002.

[FLP08] J.-C. Faugère, F. Levy-dit-Vehel, and L. Perret. Cryptanalysis of MinRank. In *Proceedings CRYPTO 2008*, pages 280–296. Springer, 2008.

[FSS10] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. Computing loci of rank defects of linear matrices using gröbner bases and applications to cryptology. In *Proceedings ISSAC 2010*, pages 257–264, 2010.

[FSS12] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. Critical points and Gröbner bases: the unmixed case. In *Proceedings ISSAC 2012*, pages 162–169. ACM, 2012.

[FSS13] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. On the complexity of the generalized MinRank problem. *J. Symbolic Comput.*, 55:30–58, 2013.

[Giu84] M. Giusti. Some effectivity problems in polynomial ideal theory. In *Proceedings EUROSAM 84*, pages 159–171. Springer, 1984.

[GN72] T. H. Gulliksen and O. G. Negård. Un complexe résolvant pour certains idéaux déterminantiels. *C. R. Acad. Sci. Paris*, 274:16–18, 1972.

[GND24] Sriram Gopalakrishnan, Vincent Neiger, and Mohab Safey El Din. Optimized gröbner basis algorithms for maximal determinantal ideals and critical point computations, 2024.

[GNSED23] Sriram Gopalakrishnan, Vincent Neiger, and Mohab Safey El Din. Refined f5 algorithms for ideals of minors of square matrices. In *Proceedings of the 2023 International Symposium on Symbolic and Algebraic Computation*, ISSAC '23, page 270–279, New York, NY, USA, 2023. Association for Computing Machinery.

[Got74] Shiro Goto. When do the determinantal ideals define gorenstein rings? *Science Reports of the Tokyo Kyoiku Daigaku, Section A*, 12(329/346):129–145, 1974.

[GSED14] A. Greuet and M. Safey El Din. Probabilistic algorithm for polynomial optimization over a real algebraic set. *SIAM J. Optim.*, 24(3):1313–1343, 2014.

[HMM+13a] Tadahito Harima, Toshiaki Maeno, Hideaki Morita, Yasuhide Numata, Akihito Wachi, and Junzo Watanabe. *k-Lefschetz Properties*, pages 171–188. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[HMM+13b] Tadahito Harima, Toshiaki Maeno, Hideaki Morita, Yasuhide Numata, Akihito Wachi, and Junzo Watanabe. *Lefschetz Properties*, pages 97–140. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[HS09] H. Hong and M. Safey El Din. Variant real quantifier elimination: algorithm and application. In *Proceedings ISSAC 2009*, pages 183–190, 2009.

[HS12] H. Hong and M. Safey El Din. Variant quantifier elimination. *J. Symbolic Comput.*, 47(7):883–901, 2012.

[HSEDSV21] J. D. Hauenstein, M. Safey El Din, É. Schost, and T. X. Vu. Solving determinantal systems using homotopy techniques. *J. Symbolic Comput.*, 104:754–804, 2021.

[JPS13] C.-P. Jeannerod, C. Pernet, and A. Storjohann. Rank-profile revealing Gaussian elimination and the CUP matrix decomposition. *J. Symbolic Comput.*, 56:46–68, 2013.

[Kni95] Philip A. Knight. Fast rectangular matrix multiplication and qr decomposition. *Linear Algebra and its Applications*, 221:69–81, 1995.

[KS99] A. Kipnis and A. Shamir. Cryptanalysis of the HFE public key cryptosystem by relinearization. In *Proceedings CRYPTO 1999*, pages 19–30. Springer, 1999.

[Las78] A. Lascoux. Syzygies des variétés déterminantales. *Adv. Math*, 30(3):202–237, 1978.

[Laz83] D. Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In *Proceedings EUROSAM 83*, pages 146–156. Springer, 1983.

[LS21a] P. Lairez and M. Safey El Din. Computing the dimension of real algebraic sets. In *Proceedings ISSAC 2021*, pages 257–264. ACM, 2021.

[LS21b] H. P. Le and M. Safey El Din. Faster one block quantifier elimination for regular polynomial systems of equations. In *Proceedings ISSAC 2021*, pages 265–272, 2021.

[Mat87] H. Matsumura. *Commutative Ring Theory*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1987.

[MGH+05] Michael B. Monagan, Keith O. Geddes, K. Michael Heal, George Labahn, Stefan M. Vorkoetter, James McCarron, and Paul DeMarco. *Maple 10 Programming Guide*. Maplesoft, Waterloo ON, Canada, 2005.

[MMR03] J. Migliore and R.M. Miró-Roig. Ideals of general forms and the ubiquity of the weak lefschetz property. *Journal of Pure and Applied Algebra*, 182(1):79–107, 2003.

[Par10] Keith Pardue. Generic sequences of polynomials. *Journal of Algebra*, 324(4):579–590, 2010.

[Pat96] J. Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. In *Proceedings EUROCRYPT 1996*, pages 33–48. Springer, 1996.

[Spa14] P.-J. Spaenlehauer. On the complexity of computing critical points with Gröbner bases. *SIAM J. Optim.*, 24(3):1382–1401, 2014.

[SS03] M. Safey El Din and É. Schost. Polar varieties and computation of one point in each connected component of a smooth real algebraic set. In *Proceedings ISSAC 2003*, pages 224–231. ACM, 2003.

[SS17] M. Safey El Din and É. Schost. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. *J. ACM*, 63(6), jan 2017.

[Sto00] A. Storjohann. *Algorithms for Matrix Canonical Forms*. PhD thesis, Swiss Federal Institute of Technology – ETH, 2000.

[The22] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.8.beta6)*, 2022. `https://www.sagemath.org`.