Finer Complexity Estimates for the Change of Ordering of Gröbner Bases for Generic Symmetric Determinantal Ideals

Andrew Ferguson, Huu Phuoc Le

Finer complexity estimates for the change of ordering of Gröbner bases for generic symmetric determinantal ideals

Andrew Ferguson
Sorbonne Université, CNRS, LIP6, Équipe PolSys
F-75252, Paris Cedex 05, France
andrew.ferguson@lip6.fr

Huu Phuoc Le
Sorbonne Université, CNRS, LIP6, Équipe PolSys
F-75252, Paris Cedex 05, France
huu-phuoc.le@lip6.fr

ABSTRACT

Polynomial matrices and ideals generated by their minors appear in various domains such as cryptography, polynomial optimization and effective algebraic geometry. When the given matrix is symmetric, this additional structure on top of the determinantal structure, affects computations on the derived ideals. Thus, understanding the complexity of these computations is important. Moreover, this study serves as a stepping stone towards further understanding the effects of structure in determinantal systems, such as those coming from moment matrices. In this paper, we focus on the Sparse-FGLM algorithm, the state-of-the-art for changing ordering of Gröbner bases of zero-dimensional ideals. Under a variant of Fröberg's conjecture, we study its complexity for symmetric determinantal ideals and identify the gain of exploiting sparsity in the Sparse-FGLM algorithm compared with the classical FGLM algorithm. For an $n \times n$ symmetric matrix with polynomial entries of degree d, we show that the complexity of Sparse-FGLM for zero-dimensional determinantal ideals obtained from this matrix over that of the FGLM algorithm is at least $O(1/d)$. Moreover, for some specific sizes of minors, we prove finer results of at least $O(1/nd)$ and $O(1/n^3d)$.

KEYWORDS

symmetric matrices, determinantal ideals, Gröbner bases, FGLM

1 INTRODUCTION

Let $\mathbb{K}$ be a field of characteristic 0 and $\overline{\mathbb{K}}$ denote its algebraic closure. We consider a set of variables $\boldsymbol{x} = (x_1, \ldots, x_k)$ and an $n \times n$ symmetric matrix $S = (f_{i,j})_{1 \le i,j \le n}$ where $f_{i,j} \in \mathbb{K}[x_1, \ldots, x_k]$ and $f_{i,j} = f_{j,i}$. Given $r \in \mathbb{N}$, the ideal generated by all $(r+1)$-minors of S defines an algebraic subset of $\overline{\mathbb{K}}^k$ at which S has rank at most r. We call such an ideal a *symmetric determinantal ideal*.

Polynomial matrices with special structures such as those above appear frequently in computer algebra. For example, determinantal ideals arise in cryptography especially through the Min-Rank problem (see e.g. [30]). Additionally, critical point methods in effective algebraic geometry often lead to polynomial systems defined by minors of Jacobian matrices. Symbolic computation based methods for semi-definite programming, such as in [20–22, 28], lead to the study of rank defects of polynomial matrices, including symmetric and Hankel ones. In [25, 26], an algorithm for solving parametric polynomial systems is developed based on parametric Hermite matrices which are symmetric matrices that encode the numbers of real/complex solutions to zero-dimensional parametric systems. Determinantal ideals obtained from those Hermite matrices define algebraic sets such that the parametric system under study has at most a given number of distinct complex solutions.

Thus, a task of great importance in the aforementioned works is to handle computations involving determinantal ideals efficiently and to understand the complexity of those computations. The Gröbner basis method for computing with ideals is commonly used. The most efficient Gröbner basis algorithms include the F4/F5 [14, 15], FGLM [18] and Sparse-FGLM [19] algorithms. In this paper, we study the complexity of the Sparse-FGLM algorithm [19] on zero-dimensional ideals generated by minors of symmetric polynomial matrices. Our main objective is to provide finer complexity estimates for these algorithms on special determinantal ideals compared to already known general complexity results.

Related works. Ideals generated by minors of a matrix whose entries are variables are studied intensively in commutative algebra. A popular technique in this subject is to use the theory of Gröbner bases to associate initial ideals of determinantal ideals (w.r.t. a suitable ordering) to simplicial complexes. This allows one to make a connection between determinantal ideals with combinatorial objects and establish many results using the Stanley-Reisner rings of those simplicial complexes (see e.g [6, 7, 9, 10, 32]).

In this paper, we are more interested in the computational aspects that arise when one considers matrices whose entries are multivariate polynomials. Computing with determinantal ideals generated by minors of these matrices gives rise to the question of estimating the complexity of Gröbner basis algorithms, e.g., F4/F5 [14, 15] and FGLM-like [18, 19] algorithms, to this class of ideals.

Previous works on the complexity of these algorithms depend on some regularity properties as well as some quantities of the given ideal that can be read from its Hilbert series. It is well-known that the practical behavior of Gröbner basis computation depends on the choice of monomial ordering. While Gröbner bases of lexicographical orderings provides many information on the solutions to a given system, algorithms like F4/F5 operate more efficiently for computing Gröbner bases w.r.t. graded reversed lexicographic (grevlex) orderings. Hence, a popular strategy for computing lexicographic Gröbner bases is to start with an easy ordering such as grevlex and then to apply a change of ordering algorithm. For this second step, the FGLM algorithm [18] can be used in the zero-dimensional case. Given a zero-dimensional ideal $I \subset \mathbb{K}[x_1, \ldots, x_k]$ of degree D, the classical FGLM algorithm is based on linear algebra operations

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

in $\mathbb{K}[x_1,\dots,x_k]/I$ which has the structure of a $\mathbb{K}$-vector space of dimension D. This leads to a complexity of $O(kD^3)$. However, the matrices representing linear maps of multiplication in the quotient ring used by the FGLM algorithm are sparse. In particular, the majority of the columns of the multiplication matrix T_{x_k} associated to the least variable x_k contain only one entry while the rest are dense. An improved variant of the FGLM algorithm that exploits this sparsity pattern was designed in [19] to obtain a more efficient change of ordering algorithm with better complexity results. With N the number of non-zero entries of T_{x_k}, the authors of [19] prove, under some genericity assumptions, the complexity $O(ND + kD\log(D)^2)$. Due to the structure of this multiplication matrix, one can bound N by mD, where m is its number of dense columns. When the input zero-dimensional system is generic, an asymptotic bound for m is given using the knowledge of the Hilbert series of the given system.

Inspired by [19], there have been attempts to study the complexity of the Sparse-FGLM algorithm for systems with special structures, the main task being to estimate the sparsity of the multiplication matrices involved. Research in this direction was undertaken in [4]. Focusing on zero-dimensional ideals defining critical loci of polynomial maps restricted to algebraic sets, [4] introduces an explicit formula of the Hilbert series of those given ideals which significantly simplifies the formula given in [10]. This allows one to derive a sharp asymptotic bound for the number of non-zero entries of the multiplication matrix T_{x_k}, when the number of variables k tends to infinity. Applying this to the complexity result of the Sparse-FGLM algorithm allows one to improve the change-of-ordering complexity estimate for critical loci computation compared to [16], which relies on the classical FGLM algorithm. Computational experiments are also provided to support that theoretical bound. We continue in this direction by considering determinantal ideals obtained from symmetric matrices.

Main results. Our main result is a complexity analysis of the Sparse-FGLM algorithm for zero-dimensional symmetric determinantal systems by giving dedicated bounds on the fundamental parameter m. Consider a symmetric matrix $S = (s_{i,j})_{1\le i,j\le n}$ where $s_{i,j}$ are variables and $s_{i,j} = s_{j,i}$. For any $r \in \mathbb{N}$, the ideal generated by all $(r+1)$-minors of S is denoted by $\mathcal{S}_r$. Let $\mathcal{H}_r$ be the numerator of the Hilbert series of $\mathcal{S}_r$. Then, given $d \in \mathbb{N}$, let $\mathbb{K}[x_1,\dots,x_k]_{\le d}$ be the set of polynomials of degree at most d in $\mathbb{K}[x_1,\dots,x_k]$ and $S^{k,d}$ be the symmetric matrix where we substitute the variables $s_{i,j}$ for polynomials $f_{i,j} \in \mathbb{K}[x_1,\dots,x_k]_{\le d}$ with $k = \binom{n-r+1}{2}$.

For sufficiently generic $f_{i,j}$, we consider the zero-dimensional ideal $\mathcal{S}_r^{k,d}$ generated by the $(r+1)$-minors of $S^{k,d}$. Let $\mathcal{H}_r^{k,d}$ be the Hilbert series of $\mathcal{S}_r^{k,d}$. Our main results rely on some combinatorial and algebraic conditions on the Hilbert series of $\mathcal{S}_r$ and $\mathcal{S}_r^{k,d}$.

Definition 1. *A polynomial $\sum_{i=0}^{n} a_i t^i$ with non-negative coefficients is* unimodal *if there exists an integer N such that*

$$a_i \le a_{i+1} \le a_N \quad \text{for } i \le N \quad \text{and} \quad a_N \ge a_i \ge a_{i+1} \quad \text{for } i \ge N.$$

Additionally, we require a condition on the cross-sections of the Hilbert series of $\mathcal{S}_r^{k,d}$. This conjecture is a determinantal variant of Fröberg's well-known conjecture on the shape of the Hilbert series of ideals generated by generic polynomial sequences.

Conjecture 2.

(1) *Given $r \in \mathbb{N}$, the Hilbert polynomial $\mathcal{H}_r(t)$ of the symmetric determinantal ideal $\mathcal{S}_r$ is unimodal.*
(2) *For $e \ge 1$, let $\mathcal{Q}_r^{k,d,e}$ be the Hilbert series of the quotient algebra $\left(\mathbb{K}[x_1,\dots,x_k]/\mathcal{S}_r^{k,d}\right)/\left\langle x_k^e\right\rangle$. We conjecture that $\mathcal{Q}_r^{k,d,e} = \left[(1-t^e)\mathcal{H}_r^{k,d}(t)\right]_+$, where $\left[(1-t^e)\mathcal{H}_r^{k,d}(t)\right]_+$ is the series truncated at its first negative coefficient.*

Section 6 refers to our computational database for supporting this conjecture.

Throughout this paper, the notations $\prec_{\text{grevlex}}$ and $\prec_{\text{lex}}$ always denote the grevlex and lexicographic orderings in $\mathbb{K}[x_1,\dots,x_k]$ with $x_1 \succ \cdots \succ x_k$. We can now state our main results.

Theorem 3. *Given $r,n,d \in \mathbb{N}$ and $k = \binom{n-r+1}{2}$, there exists a non-empty Zariski-open subset $\mathscr{F}_r$ of $\mathbb{K}[x_1,\dots,x_k]_{\le d}^{n(n+1)/2}$ such that, when the entries of $S^{k,d}$ are taken in $\mathscr{F}_r$, the following holds:*

The ideal $\mathcal{S}_r^{k,d}$ is a zero-dimensional ideal. Assume that Conjecture 2 holds and that a reduced Gröbner basis of $\mathcal{S}_r^{k,d}$ w.r.t. $\prec_{\text{grevlex}}$ is known. Then, the matrix T_{x_k} of multiplication by x_k can be constructed without any arithmetic operations. Moreover, the number of dense columns of T_{x_k} is equal to the largest coefficient of the Hilbert series of $\mathcal{S}_r^{k,d}$.

Through the Sparse-FGLM algorithm [19], Theorem 3 leads directly to a complexity result for the change-of-ordering to a $\prec_{\text{lex}}$ Gröbner basis for symmetric determinantal ideals.

Theorem 4. *Given $r,n,d \in \mathbb{N}$ and $k = \binom{n-r+1}{2}$, we consider the matrix $S^{k,d}$ with entries taken in the Zariski-open set $\mathscr{F}_r$ defined in Theorem 3. Assume that Conjecture 2 holds and the reduced Gröbner basis of $\mathcal{S}_r^{k,d}$ w.r.t. $\prec_{\text{grevlex}}$ is known. Then as $d \to \infty$, the Sparse-FGLM algorithm computes a $\prec_{\text{lex}}$ Gröbner basis of $\mathcal{S}_r^{k,d}$ within*

$$O\left(m\mathcal{H}_r^{k,d}(1)^2\right) = O\left(md^{2k}\mathcal{H}_r(1)^2\right) = O\left(md^{2k}\left(\prod_{i=0}^{n-r-1}\frac{\binom{n+i}{2i+r}}{\binom{2i+1}{i}}\right)^2\right)$$

arithmetic operations in $\mathbb{K}$ where m is the number of dense columns of the multiplication matrix T_{x_k}. Moreover, as $d \to \infty$, m is bounded above by

$$d^{k-1}\mathcal{H}_r(1) = \sqrt{\frac{6}{k\pi}}d^{k-1}\prod_{i=0}^{n-r-1}\frac{\binom{n+i}{2i+r}}{\binom{2i+1}{i}}.$$

Our results provide dedicated estimates of the complexity of the Sparse-FGLM algorithm for symmetric determinantal ideals. This new complexity result is finer than previous results that do not take the specific structure into account. Moreover, we focus on three special cases in particular, $r = n-2$, $r = n-3$ and $r = 1$. In these cases, the Hilbert series is known [7, 9]. This allows us to provide sharper complexity results by analyzing the largest coefficients of these Hilbert series. To illustrate this result, we provide some numerical results to compare this theoretical bound with the actual number of dense columns that is observed in practice.

Organization of the paper. In Section 2, we recall some basic notions and known results for determinantal ideals that will be used further. The transition from variable matrices to polynomial matrices is described in Section 3. There, we prove some properties that

relate the largest coefficient of the Hilbert series to the complexity of the Sparse-FGLM algorithm applied to symmetric determinantal ideals. Using these properties, in Section 4 we asymptotically bound said complexity, with sharper estimates in some special cases. Based on our findings, we touch on topics for further study, including triangular and moment matrices, in Section 5. Finally, in Section 6, experiments are provided to support our asymptotic bounds.

2 PRELIMINARIES

In this section, we recall some properties of determinantal systems associated to symmetric matrices. In Section 3, we show that these properties can be transferred to determinantal ideals generated by polynomial matrices. Under certain hypotheses, these properties serve as main ingredients for our complexity estimate of the Sparse-FGLM algorithm for symmetric determinantal ideals in Section 4.

Firstly, we investigate matrices whose entries are variables before transitioning to the zero-dimensional setting. Hence, consider a symmetric matrix $S = (s_{i,j})_{1\le i,j\le n}$ where $s_{i,j}$ are variables and $s_{i,j} = s_{j,i}$. Let $\boldsymbol{s} = (s_{1,1}, s_{2,1}, s_{2,2}, \dots, s_{n,1}, \dots, s_{n,n})$ be the $n(n+1)/2$ variables appearing in S. In what follows, we work over the polynomial ring $\mathbb{K}[\boldsymbol{s}]$ and denote by $\mathbb{K}[\boldsymbol{s}]_d$ the set of polynomials of degree d in $\mathbb{K}[\boldsymbol{s}]$ and 0.

Given $r \in \mathbb{N}$, we denote by $\mathcal{S}_r$ the ideal generated by all the $(r+1)$-minors of S. It defines the algebraic set

$$\left\{ \boldsymbol{s} \in \overline{\mathbb{K}}^{n(n+1)/2} \,\middle|\, S \text{ has rank at most } r \text{ at } \boldsymbol{s} \right\}.$$

Let $A_r = \mathbb{K}[\boldsymbol{s}]/\mathcal{S}_r$. The Hilbert series of A_r is defined to be

$$\mathrm{HS}_{A_r}(t) = \sum_{i=0}^{\infty} \dim_{\mathbb{K}} \mathbb{K}[\boldsymbol{s}]_d/(\mathcal{S}_r \cap \mathbb{K}[\boldsymbol{s}]_d) \cdot t^i$$

where $\dim_{\mathbb{K}}$ means the dimension as a $\mathbb{K}$-vector space. It is well-known that $\mathrm{HS}_{A_r}(t)$ can be written in the form

$$\mathrm{HS}_{A_r}(t) = \frac{\mathcal{H}_r(t)}{(1-t)^{\ell}}$$

where ℓ is the Krull dimension of A_r and $\mathcal{H}_r(t) \in \mathbb{K}[t]$ is the Hilbert polynomial of A_r [12, Theorem 10.2.4] [13, Ch. 8].

By [23], the quotient ring $\mathbb{K}[\boldsymbol{s}]/\mathcal{S}_r$ is a Cohen-Macaulay normal domain. Moreover, we have the following properties:

- The Krull dimension ℓ of A_r is
$$\dim A_r = \binom{n+1}{2} - \binom{n-r+1}{2} = \frac{(2n+1-r)r}{2}.$$
- The degree of A_r, i.e. $\mathcal{H}_r(1)$, equals
$$\mathcal{H}_r(1) = \prod_{i=0}^{n-r-1} \frac{\binom{n+i}{2i+r}}{\binom{2i+1}{i}} \le \frac{n^{\binom{n-r+1}{2}}}{2^{\binom{n-r}{2}} \prod_{i=1}^{n-r-1} i!}.$$

In what follows, we require the Hilbert series to have some combinatorial properties. Note that unimodality (Definition 1) is not necessarily preserved by multiplication, for example $f = 3+t+t^2$ is unimodal (for $N = 0$) while $f^2 = 9+6t+7t^2+2t^3+t^4$ is not. This motivates the following definition.

Definition 5. *A polynomial f with non-negative coefficients is* strongly unimodal *if, for any unimodal polynomial g, the product fg is unimodal.*

In the case of maximal minors, the authors of [4] simplify a formula given in [10] for the Hilbert series of the ideal generated by the minors of an $n \times p$, with $n \le p$, general variable matrix. The Hilbert polynomial in this simplified formula,

$$\sum_{i=0}^{n-1} \binom{p-n+i}{i} t^i,$$

is easily seen to be unimodal. This allows one to derive the Hilbert series of ideals generated by the maximal minors of matrices whose entries are generic homogeneous polynomials of *the same degree d*. Using the strong unimodality of $1 + \cdots + t^{d-1}$, it is also proved in [4] that this Hilbert polynomial is also unimodal.

In the case of symmetric matrices, we focus on the following special cases for which the Hilbert series are known [7, 9]:

- When $r = n-2$, the Hilbert series of $\mathcal{S}_{n-2}$ is
$$\frac{1}{(1-t)^{n(n+1)/2-3}} \sum_{i=0}^{n-2} \binom{i+2}{2} t^i.$$
- When $r = n-3$, the Hilbert series of $\mathcal{S}_{n-3}$ is symmetric
$$\frac{1}{(1-t)^{n(n+1)/2-6}} \left(\sum_{i=0}^{n-3} \binom{i+5}{5} t^i + \sum_{i=0}^{n-4} \binom{i+5}{5} t^{2n-6-i} \right).$$
- When $r = 1$, the Hilbert series of $\mathcal{S}_1$ is
$$\frac{1}{(1-t)^n} \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} t^i.$$

It is easy to see that these Hilbert polynomials are unimodal. However, outside of these cases, closed forms of the Hilbert series are unknown. Although whether the corresponding Hilbert polynomials are unimodal is still an open question, an affirmative answer can be observed experimentally for generic determinantal systems. For more detail on supporting this conjecture, see Section 6.

3 THE ZERO-DIMENSIONAL SETTING

As in [4, 16, 17], we are interested in studying the behavior of Gröbner basis computations for zero-dimensional systems. In this section, some properties of zero-dimensional ideals generated by minors of a symmetric polynomial matrix are established.

We denote by $\mathbb{K}[x_1, \dots, x_k]_{\le d}$ the subset of $\mathbb{K}[x_1, \dots, x_k]$ of polynomials of degree *at most* d. Let $S^{k,d} = (f_{i,j})_{1\le i,j\le n}$ be an $n \times n$ symmetric matrix with entries in $\mathbb{K}[x_1, \dots, x_k]_{\le d}$. Then, for $r \in \mathbb{N}$, $\mathcal{S}_r^{k,d}$ denotes the ideal generated by the $(r+1)$-minors of $S^{k,d}$. It is expected that when the entries of $S^{k,d}$ are sufficiently generic, the ideal $\mathcal{S}_r^{k,d}$ retains some of the structure of $\mathcal{S}_r$ defined in Section 2.

Given an ideal $I \subset \mathbb{K}[x_1, \dots, x_k]$ (not necessarily homogeneous), let I^{h} be the homogenized ideal with a new variable x_0. The Hilbert series of I is defined to be the Hilbert series of $I^{\mathrm{h}} + \langle x_0 \rangle$, that is the Hilbert series of the associated graded algebra.

In order to apply the reasoning of [19] to generic symmetric determinantal ideals we require them to be in shape position. This means that for a $\prec_{\mathrm{lex}}$ ordering with x_k as the least variable, the $\prec_{\mathrm{lex}}$ Gröbner basis has the structure

$$\{x_1 - g_1(x_k), \dots, x_{k-1} - g_{k-1}(x_k), g_k(x_k)\},$$

where for $1 \le i \le k-1$, $\deg g_i < \deg g_k = D$, the degree of I.

Proposition 6. *Let $r, d \in \mathbb{N}$, $\mathcal{H}_r(t)$ be the Hilbert polynomial of the ideal $\mathcal{S}_r$ and $k = \binom{n-r+1}{2}$, the codimension of $\mathcal{S}_r$. There exists a non-empty Zariski-open subset $\mathscr{F}_r$ of $\mathbb{K}[x_1, \ldots, x_k]_{\leq d}^{n(n+1)/2}$ such that if the entries of the matrix $S^{k,d}$ are taken in $\mathscr{F}_r$, then the ideal $\mathcal{S}_r^{k,d}$ is radical and zero-dimensional and its Hilbert series is bounded above, coefficient-wise, by*

$$\mathcal{H}_r^{k,d}(t) \coloneqq \left(1 + t + \cdots + t^{d-1}\right)^k \mathcal{H}_r\left(t^d\right).$$

Moreover, there exists a non-empty Zariski-open subset $\mathscr{O}$ of the set $\mathrm{GL}(k, \mathbb{K})$ of invertible $k \times k$ matrices such that, after applying any linear change of coordinates $A \in \mathscr{O}$, the ideal $\mathcal{S}_r^{k,d}$ is in shape position.

Proof. We start in a homogeneous setting with $\mathbb{K}[x_0, x_1, \ldots, x_k]_d$ denoting the subset of homogeneous polynomials of degree d in $\mathbb{K}[x_0, x_1, \ldots, x_k]$ together with 0. Let $S = (s_{i,j})_{1 \leq i,j \leq n}$ be an $n \times n$ symmetric matrix. Throughout this proof, $\mathcal{S}_r$ denotes the ideal of $\mathbb{K}[\boldsymbol{s}, x_0, \ldots, x_k]$ generated by the $(r+1)$-minors of S. By [23], $\mathbb{K}[\boldsymbol{s}, x_0, \ldots, x_k]/\mathcal{S}_r$ is a Cohen-Macaulay ring.

By giving the weighted degrees d and 1 for the variables $\boldsymbol{s}$ and $x_0, \ldots, x_k$ respectively, the Hilbert series of $\mathbb{K}[\boldsymbol{s}, x_0, \ldots, x_k]/\mathcal{S}_r$ is

$$\tilde{\mathcal{H}}_r(t) = \frac{\mathcal{H}_r(t^d)}{(1-t)^{k+1}\left(1-t^d\right)^{\binom{n+1}{2}-k}}.$$

Let $f_{i,j}^{\mathrm{h}}$ be the homogenization of $f_{i,j}$ in $\mathbb{K}[x_0, \ldots, x_k]$. We consider the quasi-homogeneous ideal

$$J = \mathcal{S}_r + \left\langle s_{i,j} - f_{i,j}^{\mathrm{h}} | 1 \leq i \leq j \leq n \right\rangle.$$

Through similar techniques as in [17, Sec. 3 and 4], there exists a non-empty Zariski-open subset $\mathscr{Z}$ of $\mathbb{K}[x_0, \ldots, x_k]_d^{n(n+1)/2}$ such that when the polynomials $f_{i,j}^{\mathrm{h}}$ lie in $\mathscr{Z}$, the ideals J and $J + \langle x_0 \rangle$ have dimension one and zero respectively. Hence, by the unmixedness theorem [13, Cor. 18.14], the $\binom{n+1}{2} + 1$ polynomials

$$s_{i,j} - f_{i,j}^{\mathrm{h}} \text{ for } 1 \leq i \leq j \leq n \text{ and } x_0$$

forms a regular sequence over $\mathbb{K}[\boldsymbol{s}, x_0, \ldots, x_k]/\mathcal{S}_r$. Therefore, the Hilbert series of the homogenized ideal $\mathcal{S}_r^{k,d,\mathrm{h}}$ of $\mathcal{S}_r^{k,d}$ is equal to

$$\mathcal{H}_r^{k,d}(t) = (1-t^d)^{\binom{n+1}{2}} \tilde{\mathcal{H}}_r(t) = \left(1 + \cdots + t^{d-1}\right)^k \mathcal{H}_r\left(t^d\right).$$

As $\mathcal{S}_r^{k,d,\mathrm{h}} \subset J$, the Hilbert series of $\mathcal{S}_r^{k,d,\mathrm{h}} + \langle x_0 \rangle$, which is a polynomial, is bounded coefficient-wise by the Hilbert series of $J + \langle x_0 \rangle$, that is $\mathcal{H}_r^{k,d}(t)$. Since the Hilbert series of $\mathcal{S}_r^{k,d,\mathrm{h}}$ is also the Hilbert series of the affine ideal $\mathcal{S}_r^{k,d}$, we obtain the zero-dimensionality of $\mathcal{S}_r^{k,d}$ and the bound on the coefficients of its Hilbert series.

Next, we prove that the ideal $\mathcal{S}_r^{k,d}$ is radical. For this, we work completely with the affine polynomials $f_{i,j}$. By [6, Theorem 2.9], there exists a monomial ordering such that the corresponding initial ideal is generated by squarefree monomials and so, is radical. Thus, $\mathcal{S}_r$ is a radical ideal of codimension $\binom{n-r+1}{2}$. Fixing an r-minor $\mathfrak{m}$ of S, we consider the set $\mathfrak{M}$ of the $\binom{n-r+1}{2}$ $(r+1)$-minors that contain $\mathfrak{m}$ as a submatrix. As the ideal $\mathcal{S}_r$ is radical, so is the ideal generated by the minors $\mathfrak{M}$. By the exchange lemma [1, Lemma 4], these minors, together with $\mathfrak{m} \neq 0$, define the locally closed algebraic set $V(\mathcal{S}_r) \setminus V(\mathfrak{m})$, which has codimension $\binom{n-r+1}{2}$.

We now consider the coefficients of $f_{i,j}$ as new variables $\boldsymbol{c}$ in the space $\mathscr{C} = \overline{\mathbb{K}}[x_1, \ldots, x_k]_{\leq d}^{n(n+1)/2}$. Define the map φ by

$$\begin{array}{rccc} \varphi : & \overline{\mathbb{K}}^{\binom{n+1}{2}+k} \times \mathscr{C} & \to & \overline{\mathbb{K}}^{\binom{n-r+1}{2}} \times \overline{\mathbb{K}}^{\binom{n+1}{2}} \\ & (\boldsymbol{s}, \boldsymbol{x}, \boldsymbol{c}) & \mapsto & (\mathfrak{M}, s_{1,1} - f_{1,1}, \ldots, s_{n,n} - f_{n,n}) \end{array}$$

and $\varphi_{\boldsymbol{c}}$ denotes the restriction of the map φ to a given $\boldsymbol{c} \in \mathscr{C}$. Let $\mathrm{jac}_{\boldsymbol{s}}(\mathfrak{M})$ be the Jacobian matrix of $\mathfrak{M}$ w.r.t. $\boldsymbol{s}$. Note that the Jacobian matrix of φ has the following structure

$$\mathrm{jac}(\varphi) \coloneqq \begin{bmatrix} \mathrm{jac}_{\boldsymbol{s}}(\mathfrak{M}) & 0 & 0 \\ * & \mathrm{Id} & * \end{bmatrix},$$

where the identity block comes from the derivatives of $s_{i,j} - f_{i,j}$ with respect to the constant coefficients of $f_{i,j}$.

For any $\boldsymbol{s}$ such that $\mathfrak{m}(\boldsymbol{s}) \neq 0$, $\mathrm{jac}_{\boldsymbol{s}}(\mathfrak{M})$, and therefore $\mathrm{jac}(\varphi)$, has maximal rank. Thus, the Jacobian criterion [13, Theorem 16.19] implies that $\mathbf{0}$ is a regular value of φ. By Thom's weak transversality theorem [29, Proposition B.3], there exists a Zariski-open dense subset $\mathscr{C}_{\mathfrak{m}}$ of $\mathscr{C}$ such that for any $\boldsymbol{c} \in \mathscr{C}_{\mathfrak{m}}$, $\mathbf{0}$ is a regular value of $\varphi_{\boldsymbol{c}}$ and the Jacobian matrix of $\varphi_{\boldsymbol{c}}$ has maximal rank when $\mathfrak{m}(\boldsymbol{s}) \neq 0$.

Finally, let $\mathscr{F}_r$ be the intersection of $\mathscr{Z}$, identified as a Zariski-open dense subset of $\mathbb{K}[x_1, \ldots, x_k]_{\leq d}^{n(n+1)/2}$, specializing x_0 to one, with the sets $\mathscr{C}_{\mathfrak{m}}$ for all r-minors $\mathfrak{m}$ of S. For any $\boldsymbol{c} \in \mathscr{F}_r$, the ideal $\mathcal{S}_r^{k,d}$ is zero-dimensional and radical as the Jacobian matrix associated to its defining equations has rank $\binom{n+1}{2} + \binom{n-r+1}{2}$. Therefore, we may apply the shape lemma [2, Proposition 5]. There exists a Zariski-open dense subset $\mathscr{O}$ of $\mathrm{GL}(k, \mathbb{K})$ such that for all $A \in \mathscr{O}$, after applying A, the points of the variety $V(\mathcal{S}_r^{k,d})$ have distinct x_k coordinates. Thus, the ideal $\mathcal{S}_r^{k,d}$ is in shape position. □

4 ASYMPTOTIC COMPLEXITY

4.1 The general case

Given a Gröbner basis of a zero-dimensional ideal in $\mathbb{K}[x_1, \ldots, x_k]$ w.r.t. an ordering $\prec_1$, the Sparse-FGLM algorithm [19] computes a Gröbner basis of the same ideal but w.r.t. a target ordering $\prec_2$. A common change of ordering for practical uses is from a grevlex ordering to a lexicographic one [11, 16, 17]. In this section, we prove an asymptotic upper bound on the complexity of this computation for zero-dimensional symmetric determinantal ideals.

We keep the same setting as in Section 3. Given $n, r \in \mathbb{N}$ and $k = \binom{n-r+1}{2}$, we consider an $n \times n$ symmetric matrix $S^{k,d}$ whose entries are taken in $\mathscr{F}_r \subset \mathbb{K}[x_1, \ldots, x_k]_{\leq d}^{n(n+1)/2}$ defined by Proposition 6. Then, the ideal $\mathcal{S}_r^{k,d}$ is zero-dimensional and in shape position.

Given a zero-dimensional ideal $I \subset \mathbb{K}[x_1, \ldots, x_k]$ of degree D, let $\mathcal{G}$ be its reduced Gröbner basis w.r.t. the ordering $\prec_{\mathrm{grevlex}}$. It is well known that $\mathbb{K}[x_1, \ldots, x_k]/I$ is a finite-dimensional vector space for which the set $\mathcal{B}$ of monomials irreducible by $\mathcal{G}$ forms a basis. The multiplications by $x_1, \ldots, x_k$ are linear maps of $\mathbb{K}[x_1, \ldots, x_k]/I$, whose matrix representations $T_{x_1}, \ldots, T_{x_k}$ in $\mathcal{B}$ appear with sparsity. The Sparse-FGLM algorithm [19] improves upon the classical FGLM algorithm [18], whose arithmetic complexity is $O(kD^3)$, by taking advantage of this sparsity. In [19], the authors also provide a careful complexity analysis of their algorithm. By assuming the widely accepted Moreno-Socías conjecture [27, Conjecture 4.1], they show that the matrix T_{x_k} can be obtained from $\mathcal{G}$ without additional cost.

With m as the number of dense columns of T_{x_k}, when I is in shape position they bound the complexity of this algorithm by

$$O\left(mD^2 + kD\log^2 D\right).$$

This complexity analysis relies on the observation that there are three possible cases when one multiplies a monomial $b \in \mathcal{B}$ by x_k:

- $x_k \cdot b \in \mathcal{B}$: in this case, the associated column in T_{x_k} is a column of the identity matrix $(0, \ldots, 0, 1, 0, \ldots, 0)$ where the 1 is in the row corresponding to $x_k \cdot b$.
- $x_k \cdot b$ is a leading monomial in $\mathcal{G}$: in this case, the column is easily obtained from the coefficients of $x_k \cdot b - g$ where $g \in \mathcal{G}$ has leading term $x_k \cdot b$.
- Otherwise, the column is non-trivial and requires a normal form reduction of $x_k \cdot b$ by $\mathcal{G}$ to compute its canonical representation in $\mathcal{B}$, i.e. the corresponding column in T_{x_k}.

The most dense columns of the matrix T_{x_k} correspond to the second and the third cases. Only the third case requires extra computation. If Moreno-Socías' conjecture holds, then the third case does not occur for generic polynomial systems [19]. Thus, the multiplication matrix T_{x_k} can be obtained without further computation. In [4], it is shown that under similar genericity assumptions, the third case does not occur for critical point systems either. We shall now prove that the same holds for generic symmetric determinantal ideals.

Proof of Theorem 3. Let $A_r^{k,d} = \mathbb{K}[x_1, \ldots, x_k]/\mathcal{S}_r^{k,d}$. We shall construct the matrix T_{x_k} column by column. As in [19], there is a column for each monomial in the basis $\mathcal{B}$ of $A_r^{k,d}$, given by the ordering $\prec_{\text{grevlex}}$. For a monomial $b \in \mathcal{B}$, the entries in its corresponding column are the coefficients of the normal form of $x_k \cdot b$ expressed in the basis $\mathcal{B}$. By [4, Theorem 1], under Conjecture 2, $x_k \cdot b$ is either an element of $\mathcal{B}$ or a leading monomial of the known grevlex Gröbner basis $\mathcal{G}$. In the first case, the column corresponding to b is a column of the identity matrix and requires no computation. In the second case, the column corresponding to b can be read from the coefficients of the polynomial in $\mathcal{G}$ for which $x_k \cdot b$ is the leading monomial. Thus, the number of dense columns equals the number of polynomials in $\mathcal{G}$ whose leading terms are divisible by x_k.

By [27, Lemma 1.9], the Gröbner basis of $\mathcal{S}_r^{k,d} + \langle x_k \rangle$ w.r.t. the ordering $\prec_{\text{grevlex}}$ equals the subset of $\mathcal{G}$ containing all polynomials whose leading term is divisible by x_k. Hence, the number of dense columns equals the number of monomials in the basis of $A_r^{k,d}/\langle x_k \rangle$, which is the sum of the coefficients of the corresponding Hilbert series. By Conjecture 2.2, the Hilbert series $HQ_{r,d}^1$ of $\mathcal{S}_r^{k,d} + \langle x_k \rangle$ is equal to $\left[(1-t)\mathcal{H}_r^{k,d}\right]_+$, where $\mathcal{H}_r^{k,d}$ is given in Proposition 6.

By Conjecture 2.1, h_r is unimodal, which implies easily that $(1 + \cdots + t^{d-1})h_r(t^d)$ is unimodal. By [4, Lemma 17], $1 + \cdots + t^{d-1}$ is a strongly unimodal polynomial. As $\mathcal{H}_r^{k,d}$ is the product of a unimodal polynomial and $(1 + \cdots + t^{d-1})^{k-1}$, it is also unimodal. Thus, the number of dense columns is equal to $Q_r^{k,d,1}(1)$ which is equal to largest coefficient of $\mathcal{H}_r^{k,d}$. □

Hence, assuming that $k = \binom{n-r+1}{2}$ and that the entries of $S^{k,d}$ are taken from the $\mathscr{F}_r$ described in Proposition 6, we study the asymptotic behavior of the largest coefficient of the Hilbert series of the zero-dimensional ideal $\mathcal{S}_r^{k,d}$ as d tends to infinity.

Lemma 7. *Let $k = \binom{n-r+1}{2}$. The largest coefficient of*

$$\mathcal{H}_r^{k,d}(t) = (1 + t + \cdots + t^{d-1})^k \mathcal{H}_r(t)$$

as $d \to \infty$ is bounded above by

$$\sqrt{\frac{6}{k\pi}} d^{k-1} \mathcal{H}_r(1) = \sqrt{\frac{6}{k\pi}} d^{k-1} \prod_{i=0}^{n-r-1} \frac{\binom{n+i}{2i+r}}{\binom{2i+1}{i}}.$$

Proof. By [19, Corollary 5.10], as $d \to \infty$, all the coefficients of $\left(1 + \cdots + t^{d-1}\right)^k$ are bounded by $\sqrt{\frac{6}{k\pi}} d^{k-1}$. Substituting this asymptotic formula into the convolution formula for the largest coefficient gives the first result. By [23], we conclude using the equation

$$\mathcal{H}_r(1) = \prod_{i=0}^{n-r-1} \frac{\binom{n+i}{2i+r}}{\binom{2i+1}{i}}.$$ □

We now apply Lemma 7 to prove an asymptotic complexity estimate for the Sparse-FGLM algorithm on generic determinantal systems (not necessarily those derived from symmetric matrices).

Proof of Theorem 4. By Proposition 6, we apply the shape position variant of the Sparse-FGLM algorithm. Then, by Theorem 3, the multiplication matrix T_{x_k} can be constructed without any additional arithmetic operations and the number of dense columns m equals the largest coefficient of the Hilbert series of $\mathcal{S}_r^{k,d}$. The dominant term in the complexity is $O(mD^2)$, where D is the degree of $\mathcal{S}_r^{k,d}$. This degree is given by the evaluation of the Hilbert series of $\mathcal{S}_r^{k,d}$ at one. By Proposition 6, this Hilbert series is equal to

$$\mathcal{H}_r^{k,d}(t) = \left(1 + t + \cdots + t^{d-1}\right)^k \mathcal{H}_r\left(t^d\right).$$

By [23], the degree of $S_r^{k,d}$ is equal to

$$D = \mathcal{H}_r^{k,d}(1) = d^k \mathcal{H}_r(1) = d^k \prod_{i=0}^{n-r-1} \frac{\binom{n+i}{2i+r}}{\binom{2i+1}{i}}.$$

Finally, Lemma 7 implies the bound on m as $d \to \infty$. □

Theorem 4 leads directly to the following corollary.

Corollary 8. *The complexity of the Sparse-FGLM algorithm over that of the FGLM algorithm for generic symmetric determinantal ideals as $d \to \infty$ is at least $O(1/d)$.*

4.2 Cases $r = n-2, r = n-3$ and $r = 1$

Additionally, we treat the cases of $r = n-2$, $r = n-3$ and $r = 1$ separately. With the knowledge on the Hilbert polynomials $\mathcal{H}_{n-2}$, $\mathcal{H}_{n-3}$ and $\mathcal{H}_1$, we know that Conjecture 2.1 holds in these cases. Furthermore, one can arrive at finer asymptotic estimates on the largest coefficient. Recall that the codimension of $\mathcal{S}_r$, and hence the number of variables we consider in the zero-dimensional setting, equals 3, 6 and $\binom{n}{2}$ for $r = n-2$, $r = n-3$ and $r = 1$ respectively.

We start by identifying the largest coefficient of $\mathcal{H}_{n-2}^{3,d}$ exactly.

Proposition 9. *The largest coefficient of*

$$\mathcal{H}_{n-2}^{3,d}(t) = \left(1 + t + \cdots + t^{d-1}\right)^3 \sum_{i=0}^{n-2} \binom{i+2}{2} t^{id}$$

is the value of

$$\binom{n-1}{2}\binom{j+1}{2} + \binom{n}{2}\left(\binom{d+1}{2} + j(d-j-1)\right).$$

when j is any integer that minimizes $\left|\frac{2nd-n-2}{2(n+2)} - j\right|$.

Proof. Note that

$$\left(1+t+\cdots+t^{d-1}\right)\sum_{i=0}^{n-2}\binom{i+2}{2}t^{id} = \sum_{i=0}^{n-2}\sum_{j=0}^{d-1}\binom{i+2}{2}t^{id+j}.$$

We write these coefficients in the following $d \times ((n-2)d-1)$ grid:

t^0	$\cdots$	t^{d-1}	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$t^{(n-1)d-1}$	$\cdots$	$t^{(n-2)d-2}$
		1	$\cdots$	1	$\cdots$	$\cdots$	$\binom{n}{2}$	$\cdots$	$\binom{n}{2}$
	$\iddots$	$\vdots$	$\iddots$	$\iddots$	$\iddots$	$\iddots$	$\vdots$	$\iddots$	
1	$\cdots$	1	$\cdots$	$\cdots$	$\binom{n}{2}$	$\cdots$	$\binom{n}{2}$		

The coefficients of $\left(1+t+\cdots+t^{d-1}\right)^2\mathcal{H}_{n-2}(t)$ are the sums of columns of this grid, which are

$$\binom{i+2}{2}(j+1) + \binom{i+1}{2}(d-j-1).$$

Hence, the coefficients of $\left(1+t+\cdots+t^{d-1}\right)^3\mathcal{H}_{n-2}(t)$ can be computed by taking the sums of all d consecutive columns.

As $\binom{i+2}{2}$ is increasing as a sequence in i, the largest coefficient of $\mathcal{H}^{3,d}_{n-2}$ must be the coefficient of t^{nd-j-2} for some $0 \le j \le d-1$. By a simple calculation, this coefficient can be expressed as

$$\begin{aligned}&\binom{n-1}{2}\binom{j+1}{2} + \binom{n}{2}\left(\binom{d+1}{2} + j(d-j-1)\right)\\ &= C - \frac{(n-1)(n+2)}{16}\left(\frac{2nd-n-2}{n+2} - 2j\right)^2\end{aligned}$$

where $C = \binom{n}{2}\binom{d+1}{2} + \frac{(n-1)(2nd-n-2)^2}{16(n+2)}$ does not depend on j. Hence, to identify j, we minimize

$$\min_{j\in\mathbb{N}, 0\le j\le d-1}\left|\frac{2nd-n-2}{2(n+2)} - j\right|.$$

Let $\alpha = \frac{2nd-n-2}{2(n+2)}$, which lies in $[0, d-1/2)$ if $n \ge 2$. Then, to conclude the proof, we take j to be the nearest integer to α. □

Recall that D denotes the degree of the ideal under study. When $r = n-2$ we have that $D = \binom{d+1}{3}$. Since the complexity of the Sparse-FGLM algorithm over that of the FGLM algorithm is $O\left(\frac{mD^2}{kD^3}\right) = O\left(\frac{m}{kD}\right)$, Proposition 9 immediately implies the following corollary.

Corollary 10. *By the proof of Proposition 9, $m \le C = \binom{n}{2}\binom{d+1}{2} + \frac{(n-1)(2nd-n-2)^2}{16(n+2)}$, the complexity of the Sparse-FGLM algorithm over that of the FGLM algorithm when $r = n-2$ is at least $O\left(\frac{1}{nd}\right)$.*

Next, we consider $r = n-3$. Notice that the Hilbert polynomial $\mathcal{H}_{n-3}$ is symmetric, i.e. $\mathcal{H}_{n-3}(t) = t^{\deg(h)}\mathcal{H}_{n-3}(1/t)$. The lemma below will be useful for proving a finer complexity in this case.

Lemma 11. *Let $f(t)$ be a unimodal symmetric polynomial. Then*

$$g(t) = (1+t+\cdots+t^{d-1})f(t)$$

is also unimodal and symmetric. Moreover, the c largest coefficients of $g(t)$ are combinations of the $d+c-1$ largest coefficients of $f(t)$. As a point of notation, if $f(t)$ has fewer than $d+c-1$ coefficients then we consider all other coefficients to be zero.

Proof. The unimodality of g comes from the strong unimodality of $1+t+\cdots+t^{d-1}$. The symmetry can be deduced from the equality

$$t^{\deg(g)}g(1/t) = \left(1+\cdots+t^{d-1}\right)t^{\deg(g)}f(1/t) = g(t).$$

Note that the coefficient of t^i in g is the sum of the coefficients of $t^{i-d+1}, \ldots, t^i$ in f. As f is unimodal and symmetric, the largest coefficient of g is the sum of the d central coefficients of f. Since g is unimodal and symmetric, the c largest coefficients of g are consecutive and any of them is at most $\lceil\frac{c-1}{2}\rceil$ elements away from the central and thus largest coefficient. Hence, the c largest coefficients of g involve only the central $d+c-1$ coefficients of f. □

Proposition 12. *The largest coefficient of the Hilbert series*

$$\mathcal{H}^{6,d}_{n-3}(t) = \left(1+t+\cdots+t^{d-1}\right)^6\mathcal{H}_{n-3}\left(t^d\right)$$

as $d \to \infty$ is bounded above by

$$\left(\binom{n+2}{5} + 2\binom{n+1}{5} + 2\binom{n}{5}\right)\sqrt{\frac{1}{\pi}}d^5 \le 5\binom{n+2}{5}\sqrt{\frac{1}{\pi}}d^5 \in O\left(n^5d^5\right).$$

Proof. By Lemma 11, $(1+\cdots+t^{d-1})^6$ is unimodal and symmetric. From observation, $\mathcal{H}_{n-3}$ is also unimodal and symmetric. Thus, by Lemma 11, the largest coefficient m of $\mathcal{H}^{6,d}_{n-3}$ depends only on the central $5(d-1)+1$ coefficients of $(1+\cdots+t^{d-1})\mathcal{H}_{n-3}(t^d)$. This number then depends on at most the central 5 coefficients of $\mathcal{H}_{n-3}$.

By [19, Corollary 5.10], all coefficients of $(1+\cdots+t^{d-1})^6$ are at most $\sqrt{\frac{1}{\pi}}d^5$. Therefore, by the definition of $\mathcal{H}_{n-3}$ and its symmetry, we have that as $d \to \infty$,

$$m \le \left(\binom{n+2}{5} + 2\binom{n+1}{5} + 2\binom{n}{5}\right)\sqrt{\frac{1}{\pi}}d^5 \le 5\binom{n+2}{5}\sqrt{\frac{1}{\pi}}d^5.$$ □

When $r = n-3$, the ideal $\mathcal{S}^{k,d}_{n-3}$ has degree

$$D = \left(\binom{n+2}{6} + \binom{n+3}{6}\right)d^6 \in O(n^6d^6).$$

By Proposition 12, the number of dense columns m lies in $O(n^5d^5)$ as $d \to \infty$, which implies Corollary 13.

Corollary 13. *Let $r = n-3$. As $d \to \infty$, the complexity improvement of the Sparse-FGLM algorithm over that of the FGLM algorithm for the generic symmetric determinantal ideal $S^{6,d}_{n-3}$ is at least $O\left(\frac{1}{nd}\right)$.*

Finally, in the case $r = 1$, the number of variables k is equal to $\binom{n}{2}$. Since this depends on n, we consider the complexity as $n \to \infty$.

Proposition 14. *The largest coefficient of*

$$\mathcal{H}^{\binom{n}{2},d}_1(t) = \left(1+t+\cdots+t^{d-1}\right)^{\binom{n}{2}}\sum_{i=0}^{\lfloor\frac{n}{2}\rfloor}\binom{n}{2i}t^{id}$$

as $n \to \infty$ is at most

$$\sqrt{\frac{6}{\binom{n}{2}\pi(d^2-1)}}d^{\binom{n}{2}}2^{n-1} \in O\left(\frac{2^{n-1}}{n}d^{\binom{n}{2}-1}\right).$$

Proof. As $(1+\cdots+t^{d-1})^{\binom{n}{2}}$ is symmetric and unimodal, its largest coefficient is central. By an abridged version of [31, Theorem 2], this largest coefficient is asymptotically equal to

$$\sqrt{\frac{6}{\binom{n}{2}\pi(d^2-1)}}d^{\binom{n}{2}}$$

as $n \to \infty$. Then, the largest coefficient of $\mathcal{H}_1^{\binom{n}{2},d}$ is at most

$$\sqrt{\frac{6}{\binom{n}{2}\pi(d^2-1)}}d^{\binom{n}{2}}\sum_{i=0}^{\lfloor \frac{n}{2} \rfloor}\binom{n}{2i}.$$

The following equality gives the result

$$\sum_{i=0}^{\lfloor \frac{n}{2} \rfloor}\binom{n}{2i} = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor}\left(\binom{n-1}{2i-1}+\binom{n-1}{2i}\right) = \sum_{i=0}^{n-1}\binom{n-1}{i} = 2^{n-1}. \quad \square$$

As the degree of $\mathcal{S}_1^{\binom{n}{2},d}$ is $d^{\binom{n}{2}}2^{n-1}$, by applying Proposition 14 to Theorem 4 we arrive at the following corollary.

Corollary 15. *When $r = 1$ the degree of $\mathcal{S}_1^{\binom{n}{2},d}$ is $d^{\binom{n}{2}}2^{n-1}$. Therefore, the complexity of the Sparse-FGLM algorithm over that of the FGLM algorithm as $n \to \infty$ is at least*

$$O\left(\frac{1}{knd}\right) = O\left(\frac{1}{\binom{n}{2}nd}\right) = O\left(\frac{1}{n^3d}\right).$$

Moreover, the bound on m in Theorem 4 implies that the complexity gain as $d \to \infty$ is also at least

$$O\left(\frac{1}{k^{3/2}d}\right) = O\left(\frac{1}{\binom{n}{2}^{3/2}d}\right) = O\left(\frac{1}{n^3d}\right).$$

5 PERSPECTIVES

Our results describe the fundamental parameter m, the number of dense columns of T_{x_k}. Therefore, while the complexity results in this article focus on the application to the Sparse-FGLM algorithm, we can also apply the propositions of Section 4 to the new change-of-ordering algorithm of [5]. Here, the authors prove a complexity result, excluding logarithmic factors, of $\tilde{O}(m^{\omega-1}D)$, where ω is the exponent of the complexity of matrix multiplication. Applying our estimates for m leads to even finer complexity results for symmetric determinantal systems.

The finer complexity results of Section 4 rely primarily on the knowledge of the Hilbert series of the special cases $r = 1, n-2$ and $n-3$. Should further cases be explored, we could expect to obtain stronger results for those cases as well. We would also like to study more types of matrix structure, such as moment matrices that arise in tensor decomposition [3] and sums of squares computations for polynomial optimization [24]. For instance, we discuss the case of Hankel variable matrices and derive an alternative derivation of the Hilbert series of $\mathcal{S}_{n-2}$.

Given an $n \times n$ Hankel matrix

$$C = \begin{bmatrix} c_0 & \cdots & c_{n-1} \\ \vdots & \iddots & \vdots \\ c_{n-1} & \cdots & c_{2n-2} \end{bmatrix},$$

we denote by C_r the ideal generated by all the $(r+1)$-minors of C.

Lemma 16. *Given $r \in \mathbb{N}$, the Hilbert series of C_r is equal to*

$$\frac{1}{(1-t)^{2r}}\sum_{i=0}^{r}\binom{2n-2r-2+i}{i}t^i.$$

Proof. By [8, Corollary 2.2], C_r coincides with the ideal generated by $(r+1)$-minors of the $(r+1) \times (2n-r-1)$ Hankel matrix

$$\overline{C} = (c_{i+j})_{0 \le i \le r, 0 \le j \le 2n-r-2}$$

and the codimension of C_r is $2n-2r-1$.

Let $M = (m_{i,j})_{0 \le i \le r, 0 \le j \le 2n-r-2}$ be a general variable matrix of the same size of $\overline{C}$ and I be the ideal generated by all the $(r+1)$-minors of M. Hence, the ideal C_r can be identified with

$$I + \left\langle c_i - m_{j,i-j}, \mid 0 \le i \le 2n-2, 0 \le j \le i \right\rangle.$$

Since $\mathbb{K}[m_{0,0}, \ldots, m_{r,2n-r-2}]/I$ is a Cohen-Macaulay ring of the same codimension $2n-2r-1$ as $\mathbb{K}[c_0, \ldots, c_{2n-2}]/C_r$, the unmixedness theorem [13, Cor. 18.14] and [4] give the result. $\square$

The above lemma allows one to study similar problems on Hankel matrices. Furthermore, using the same technique as in Lemma 16 and noting that both C_{n-2} and $\mathcal{S}_{n-2}$ have codimension three, one can obtain a different derivation of the Hilbert series of $\mathcal{S}_{n-2}$.

Additionally, we make the following conjecture for triangular matrices that, as far as we are aware, is new.

Conjecture 17. *Let T be an $n \times n$ triangular variable matrix and $\mathcal{T}_r$ be the ideal generated by its $(r+1)$-minors. Then the Hilbert series associated to $\mathcal{T}_r$ equals the Hilbert series associated to the ideal $\mathcal{S}_r$.*

As the proofs in this paper rely solely on the Hilbert series of the ideal we consider, if Conjecture 17 holds then our results also hold for ideals generated by minors of triangular matrices.

6 EXPERIMENTS

6.1 Supporting Conjecture 2

This subsection reports on our testing of Conditions 1 and 2 upon which our main results rely. Firstly, except for the cases $r \in \{1, n-2, n-3\}$ considered in Subsection 4.2, the unimodality of the Hilbert polynomials of generic symmetric determinantal ideals remains open in general. Moreover, for non-symmetric determinantal ideals, while a formula for the Hilbert series is known in the generic case [17], it is not proven to be unimodal.

Secondly, Condition 2 is not proven in any of the cases we consider. We test this conjecture by computing the leading monomials of the reduced Gröbner basis of a generic symmetric determinantal system I with Hilbert series P. Adding x_k gives a Gröbner basis of $I + \langle x_k \rangle$ w.r.t. the ordering $\prec_{\text{grevlex}}$ [27, Lemma 1.9]. Then, we can compute the Hilbert series and compare this to the formula $[(1-t^e)P]_+$ to test Condition 2. The current status of testing this conjecture can be found at the following website: https://www-polsys.lip6.fr/~ferguson/conjecture_testing.html.

6.2 Asymptotics in practice

In this subsection, we compare the true density of the multiplication matrix T_{x_k} (Actual) against the percentage of dense columns (Theoretical) and the asymptotic bounds established in Section 4 (Asymptotic), following the notation of [19, Table 2].

We begin with $n \times n$ symmetric matrices with rank at most $r = n-2$. We consider 3 variables and vary the size of the matrix

and the degree of its entries. When the entries are sufficiently generic, this construction yields symmetric determinantal ideals of dimension zero. Figure 1 reports on the density of T_{x_3} obtained from this setting. Using Proposition 9, we obtain exactly the numbers of dense columns in the matrices T_{x_3} of these systems.

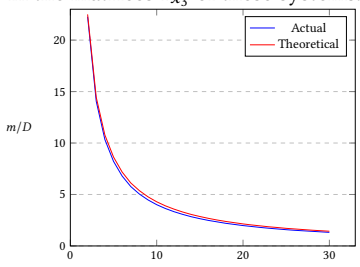

Figure 1: Density of T_{x_3} for $\mathcal{S}_{n-2}^{3,d}$ for $d \in \{2, \ldots, 50\}$

In Table 1, we analyze the ideal $S_{n-3}^{6,d}$, where we also compare the matrix density and number of dense columns against the asymptotic bound obtained in Proposition 12 (Asymptotic). Additionally, Figure 2 illustrates how the asymptotic result approaches the true number of dense columns as the degree d increases.

Parameters	Degree	Matrix Density		
(d, n)	D	Actual	Theoretical	Asymptotic
$(2, 5)$	2240	20.23%	21.96%	28.21%
$(3, 5)$	25515	12.58%	13.96%	18.81%
$(2, 6)$	7168	17.40%	19.14%	27.71%
$(3, 6)$	81648	10.89%	12.26%	18.47%
$(2, 7)$	18816	15.20%	16.96%	26.87%

Table 1: Density of T_{x_6} for $\mathcal{S}_3^{6,d}$

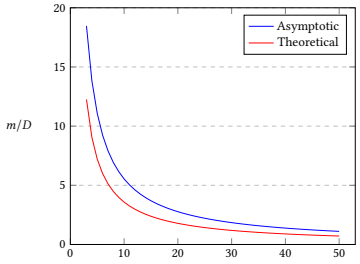

Figure 2: Density of T_{x_6} for $\mathcal{S}_{n-3}^{6,d}$ for $d \in \{3, \ldots, 50\}$

Finally, Figure 3 reports on the case $r = 1$ in where we fix $d = 4$ and increase the size of the matrix n. Here, the Asymptotic curve comes from Proposition 14.

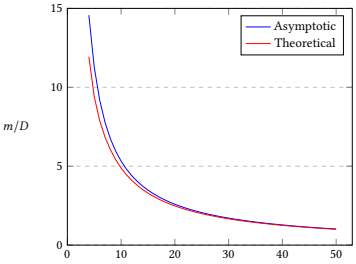

Figure 3: Density of $T_{x_{\binom{n}{2}}}$ for $\mathcal{S}_1^{\binom{n}{2},4}$ for $n \in \{4, \ldots, 50\}$

REFERENCES

[1] Bank, B., Giusti, M., Heintz, J., and Mbakop, G. M. Polar varieties and efficient real elimination. *Mathematische Zeitschrift 238*, 1 (2001), 115–144.

[2] Becker, E. and Mora, T. and Marinari, M. G. and Traverso, C. The Shape of the Shape Lemma. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation* (New York, NY, USA, 1994), ISSAC '94, Association for Computing Machinery, p. 129–133.

[3] Bernardi, A., Brachat, J., Comon, P., and Mourrain, B. General tensor decomposition, moment matrices and applications. *Journal of Symbolic Computation 52* (May 2013), 51–71.

[4] Berthomieu, J., Bostan, A., Ferguson, A., and Safey El Din, M. Gröbner bases and critical values: The asymptotic combinatorics of determinantal systems. Preprint, Apr. 2021.

[5] Berthomieu, J., Neiger, V., and Safey El Din, M. Faster change of order algorithm for Gröbner bases under shape and stability assumptions. Preprint.

[6] Conca, A. Gröbner Bases of Ideals of Minors of a Symmetric Matrix. *Journal of Algebra 166* (1994), 406–421.

[7] Conca, A. Symmetric ladders. *Nagoya Mathematical Journal 136* (1994), 35–56.

[8] Conca, A. Straightening Law and Powers of Determinantal Ideals of Hankel Matrices. *Advances in Mathematics 138*, 2 (1998), 263–292.

[9] Conca, A., De Negri, E., and Welker, V. A Gorenstein simplicial complex for symmetric minors. *Israel Journal of Mathematics 212* (2014), 237–257.

[10] Conca, A., and Herzog, J. On the Hilbert Function of Determinantal Rings and Their Canonical Module. *Proceedings of the American Mathematical Society 122*, 3 (1994), 677–681.

[11] Cox, D., Little, J., and O'Shea, D. *Using Algebraic Geometry.* Graduate Texts in Mathematics. Springer New York, 2006.

[12] Cox, D. A., Little, J., and O'Shea, D. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, 4/e (Undergraduate Texts in Mathematics).* Springer-Verlag, Berlin, Heidelberg, 2015.

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

[14] Faugère, J.-C. A new efficient algorithm for computing Gröbner bases (F4). *Journal of pure and applied algebra 139*, 1-3 (1999), 61–88.

[15] Faugère, J.-C. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In *Proceedings of the 2002 international symposium on Symbolic and algebraic computation* (2002), pp. 75–83.

[16] Faugère, J.-C., Safey El Din, M., and Spaenlehauer, P.-J. Critical points and Gröbner bases: the unmixed case. In *ISSAC 2012—Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation* (2012), ACM, New York, pp. 162–169.

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

[18] Faugère, J.-C., Gianni, P., Lazard, D., and Mora, T. Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering. *Journal of Symbolic Computation 16*, 4 (1993), 329–344.

[19] Faugère, J.-C., and Mou, C. Sparse FGLM algorithms. *Journal of Symbolic Computation 80* (2017), 538–569.

[20] Henrion, D., Naldi, S., and Safey El Din, M. Real Root Finding for Rank Defects in Linear Hankel Matrices. In *Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation* (New York, NY, USA, 2015), ISSAC '15, Association for Computing Machinery, p. 221–228.

[21] Henrion, D., Naldi, S., and Safey El Din, M. Exact Algorithms for Linear Matrix Inequalities. *SIAM Journal on Optimization 26*, 4 (2016), 2512–2539.

[22] Henrion, D., Naldi, S., and Safey El Din, M. Real root finding for determinants of linear matrices. *Journal of Symbolic Computation 74* (2016), 205–238.

[23] Kutz, R. E. Cohen-Macaulay Rings and Ideal Theory in Rings of Invariants of Algebraic Groups. *Trans. Am. Math. Soc. 194* (1974), 115–129.

[24] Lasserre, J.-B. *Moments, Positive Polynomials and Their Applications.* Imperial College Press, 10 2009.

[25] Le, H. P., and Safey El Din, M. Faster One Block Quantifier Elimination for Regular Polynomial Systems of Equations. In *Proceedings of the 2021 on International Symposium on Symbolic and Algebraic Computation* (New York, NY, USA, 2021), ISSAC '21, Association for Computing Machinery, p. 265–272.

[26] Le, H. P., and Safey El Din, M. Solving parametric systems of polynomial equations over the reals through Hermite matrices. *Journal of Symbolic Computation 112* (2022), 25–61.

[27] Moreno-Socías, G. Degrevlex Gröbner bases of generic complete intersections. *J. Pure Appl. Algebra 180*, 3 (2003), 263–283.

[28] Naldi, S. Solving rank-constrained semidefinite programs in exact arithmetic. *Journal of Symbolic Computation 85* (2018), 206–223. 41th International Symposium on Symbolic and Algebraic Computation (ISSAC'16).

[29] Safey El Din, M., and Schost, É. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. *J. ACM 63*, 6 (Jan. 2017), 48:1–48:37.

[30] Spaenlehauer, P.-J. On the Complexity of Computing Critical Points with Gröbner Bases. *SIAM Journal on Optimization 24* (07 2014), 1382–1401.

[31] Star, Z. An asymptotic formula in the theory of compositions. *Aequationes Mathematicae 13* (1975), 279–284.

[32] Sturmfels, B. Gröbner bases and Stanley decompositions of determinantal rings. *Mathematische Zeitschrift 205* (1990), 137–144.