



HAL
open science

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

Andrew Ferguson, Huu Phuoc Le

► **To cite this version:**

Andrew Ferguson, Huu Phuoc Le. Finer Complexity Estimates for the Change of Ordering of Gröbner Bases for Generic Symmetric Determinantal Ideals. International Symposium on Symbolic and Algebraic Computation (ISSAC '22), Jul 2022, Villeneuve-d'Ascq, France. pp.9, 10.1145/3476446.3536182 . hal-03573833v2

HAL Id: hal-03573833

<https://hal.sorbonne-universite.fr/hal-03573833v2>

Submitted on 1 Jun 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

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

Andrew Ferguson*

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

Huu Phuoc Le*

Sorbonne Université, CNRS, LIP6
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 $O(1/n^3d)$.

CCS CONCEPTS

• **Computing methodologies** → **Symbolic and algebraic algorithms; Equation and inequality solving algorithms**; • **Theory of computation** → **Algebraic complexity theory**.

KEYWORDS

Symmetric matrices; Determinantal ideals; Gröbner bases; FGLM

ACM Reference Format:

Andrew Ferguson and Huu Phuoc Le. 2022. Finer Complexity Estimates for the Change of Ordering of Gröbner Bases for Generic Symmetric Determinantal Ideals. In *Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation (ISSAC ’22)*, July 4–7, 2022, Villeneuve-d’Ascq, France. ACM, New York, NY, USA, 9 pages. <https://doi.org/10.1145/3476446.3536182>

*Both authors contributed equally to the paper.

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 $\mathbf{x} = (x_1, \dots, x_k)$ and an $n \times n$ symmetric matrix $S = (f_{i,j})_{1 \leq i,j \leq n}$ where $f_{i,j} \in \mathbb{K}[x_1, \dots, x_k]$ 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. [34]). 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 [23–25, 31], lead to the study of rank defects of polynomial matrices, including symmetric and Hankel ones. In [27, 28], 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 [15, 16], 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. [7, 8, 10, 11, 36]).

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 [15, 16] 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 $I \subset \mathbb{K}[x_1, \dots, x_k]$ of degree D , the classical FGLM algorithm is based on linear algebra operations 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 [5]. Focusing on zero-dimensional ideals defining critical loci of polynomial maps restricted to algebraic sets, [5] introduces an explicit formula of the Hilbert series of those given ideals which significantly simplifies the formula given in [11]. 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 [20], 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.

Besides the Sparse-FGLM algorithm which exploits the sparsity of multiplication matrices, other algorithms are also developed using fast linear algebra techniques to improve the classical FGLM. In particular, under certain assumptions, [17] and [32] present two algorithms of complexity respectively $\tilde{O}(D^\omega)$ and $O(nD^\omega \log(D))$ where ω is the matrix multiplication exponent for changing ordering of Gröbner bases. The best known theoretical bound for ω is 2.37286 given in [1]. Comparing the Sparse-FGLM algorithm with these algorithms requires estimating the parameter m . Moreover, a bound on m serves independently as an indicator for the sparsity

of T_{x_k} and could be useful for any algorithm that relies on this sparsity (e.g., the algorithm of [6] that improves [17, 32]).

Main results. Our main result is a refined complexity of the Sparse-FGLM algorithm for zero-dimensional symmetric determinantal systems by bounding the aforementioned parameter m .

We consider a symmetric matrix $S = (s_{i,j})_{1 \leq i,j \leq n}$ where $s = (s_{1,1}, s_{2,1}, s_{2,2}, \dots, s_{n,1}, \dots, s_{n,n})$ are variables. Let $\mathbb{K}[s]_d$ denote the set of homogeneous polynomials of degree d in $\mathbb{K}[s]$ and 0.

Given $r \in \mathbb{N}$, \mathcal{S}_r denotes the ideal generated by all $(r+1)$ -minors of S and $A_r = \mathbb{K}[s]/\mathcal{S}_r$. The Hilbert series of A_r is defined as

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

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

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

where δ is the Krull dimension of A_r and $\mathcal{H}_r(t) \in \mathbb{Z}[t]$ such that $\mathcal{H}_r(1) \neq 0$ [13, Theorem 10.2.4] [14, Ch. 8]. We call this polynomial $\mathcal{H}_r(t)$ the reduced numerator of $\text{HS}_{A_r}(t)$.

For $d \in \mathbb{N}$ and $k = \binom{n-r+1}{2}$, $\mathbb{K}[x_1, \dots, x_k]_{\leq d}$ denotes the set of polynomials in $\mathbb{K}[x_1, \dots, x_k]$ of degree at most d and $S^{k,d}$ be the symmetric matrix where $s_{i,j}$ are replaced by $f_{i,j} \in \mathbb{K}[x_1, \dots, x_k]_{\leq d}$. For sufficiently generic $f_{i,j}$, we will prove that the ideal $\mathcal{S}_r^{k,d}$ generated by the $(r+1)$ -minors of $S^{k,d}$ is zero-dimensional.

For any ideal $I \subset \mathbb{K}[x_1, \dots, x_k]$ (not necessarily homogeneous), let I^h be the homogenized ideal of I with a new variable x_0 . The Hilbert series of $\mathbb{K}[x_1, \dots, x_k]/I$ is defined as the Hilbert series of $\mathbb{K}[x_0, \dots, x_n]/(I^h + \langle x_0 \rangle)$ in the homogeneous setting. Let $\mathcal{S}_r^{k,d,h}$ be the homogenization of $\mathcal{S}_r^{k,d}$ and $\mathcal{H}_r^{k,d}$ be the Hilbert series of $\mathbb{K}[x_1, \dots, x_k]/\mathcal{S}_r^{k,d}$. Our main results rely on some conditions on the Hilbert series associated to \mathcal{S}_r and $\mathcal{S}_r^{k,d}$ below.

Definition 1. A polynomial $\sum_{i=0}^n a_i t^i$ with non-negative coefficients and $a_n > 0$ is unimodal if there exists $N \in \mathbb{N}$, $N \leq n$ such that

$$\begin{aligned} a_{i-1} &\leq a_i \leq a_N & \text{for } 1 \leq i \leq N, \\ a_N &\geq a_i \geq a_{i+1} & \text{for } N \leq i \leq n-1. \end{aligned}$$

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 [22] on the shape of the Hilbert series of ideals generated by generic polynomial sequences.

CONJECTURE 2.

- (1) Given $r \in \mathbb{N}$, the reduced numerator $\mathcal{H}_r(t)$ of the Hilbert series of the symmetric determinantal ideal \mathcal{S}_r is unimodal.
- (2) For $e \geq 1$, let $\mathcal{Q}_r^{k,d,e}$ be the Hilbert series of the quotient algebra $\mathbb{K}[x_0, \dots, x_k]/(\mathcal{S}_r^{k,d,h} + \langle x_0, x_k^e \rangle)$. 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 non-positive coefficient.

Fröberg's conjecture and the second part of Conjecture 2 also relate to the strong Lefschetz property in homogeneous setting. A graded Artinian algebra A has the strong Lefschetz property if there exists a linear form ℓ such that the Hilbert series of the quotient

$A/\langle \ell^e \rangle$ is equal to $[(1 - t^e)HS_A(t)]_+$ for any $e \geq 1$. We refer the interested readers to [29] for a survey on this subject.

To support Conjecture 2, we refer in Section 5 to a computational database for testing the two conditions in our conjecture.

Throughout this paper, the notations \prec_{grevlex} and \prec_{lex} always denote the grevlex and lexicographic orderings in $\mathbb{K}[x_1, \dots, x_k]$ with $x_1 > \dots > x_k$. 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 \mathcal{F}_r of $\mathbb{K}[x_1, \dots, x_k]_{\leq d}^{n(n+1)/2}$ such that, when the entries of $S^{k,d}$ are taken in \mathcal{F}_r , the following holds:*

The ideal $S_r^{k,d}$ is zero-dimensional and radical. When Conjecture 2 holds and a reduced Gröbner basis of $S_r^{k,d}$ w.r.t. \prec_{grevlex} is known, 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} equals the largest coefficient of the Hilbert series $\mathcal{H}_r^{k,d}$.

Through the Sparse-FGLM algorithm [19], Theorem 3 leads directly to a complexity result for the change-of-ordering to a \prec_{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 \mathcal{F}_r defined in Theorem 3. Assume that Conjecture 2 holds and the reduced Gröbner basis of $S_r^{k,d}$ w.r.t. \prec_{grevlex} is known. Then as $d \rightarrow \infty$, the Sparse-FGLM algorithm computes a \prec_{lex} Gröbner basis of $S_r^{k,d}$ within*

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

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

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

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 [8, 10]. 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 6. Finally, in Section 5, experiments are provided to support our asymptotic bounds.

ACKNOWLEDGMENTS

We would like to thank Jérémy Berthomieu and Mohab Safey El Din for fruitful discussions. We also thank the anonymous reviewers for their helpful comments on our paper.

The authors are supported by the ANR grants ANR-18-CE33-0011 SESAME, ANR-19-CE40-0018 DE RERUM NATURA, ANR-FWF ANR-19-CE48-0015 ECARP, the EU's Horizon 2020 network under the Marie Skłodowska-Curie grant agreement No. 813211 (POEMA) and the grant FA8665-20-1-7029 of the EOARD-AFOSR.

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.

We start with variable matrices before transitioning to the zero-dimensional setting. As in Section 1, consider a symmetric matrix $S = (s_{i,j})_{1 \leq i,j \leq n}$ with variables $s = (s_{1,1}, s_{2,1}, s_{2,2}, \dots, s_{n,1}, \dots, s_{n,n})$.

For $r \in \mathbb{N}$, \mathcal{S}_r is the homogeneous ideal generated by all the $(r+1)$ -minors of S and $A_r = \mathbb{K}[s]/\mathcal{S}_r$. The reduced numerator of the Hilbert series of A_r is denoted by $\mathcal{H}_r(t)$.

By [26], the quotient ring $\mathbb{K}[s]/\mathcal{S}_r$ 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

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

Now we discuss some particular cases when the numerator of the Hilbert series is unimodal (Definition 1). Note that unimodality 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.*

For an $n \times p$, with $n \leq p$, general variable matrix, the authors of [5] simplify a formula given in [11] for the Hilbert series of the ideal generated by its maximal minors. The reduced numerator in this simplified formula of the Hilbert series,

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

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 $1 + \dots + t^{d-1}$, it is also proved in [5] that the corresponding reduced numerator is also unimodal.

In the case of symmetric matrices, we focus on the following special cases for which the Hilbert series are known [8, 10]:

- 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

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

One can see that the reduced numerators of these Hilbert series are unimodal. However, except these cases, closed forms of the Hilbert series are unknown. Although whether all the reduced numerators are unimodal remains open, an affirmative answer can be observed experimentally for generic determinantal systems (see Section 5).

3 THE ZERO-DIMENSIONAL SETTING

As in [5, 20, 21], 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 $\mathbb{K}[x_1, \dots, x_k]_{\leq d}$ the subset of $\mathbb{K}[x_1, \dots, x_k]$ of polynomials of degree at most d . Let $S^{k,d} = (f_{i,j})_{1 \leq i,j \leq n}$ be an $n \times n$ symmetric matrix with entries in $\mathbb{K}[x_1, \dots, x_k]_{\leq d}$. 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.

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_{lex} ordering with x_k as the least variable, the \prec_{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 $1 \leq i \leq k-1$, $\deg g_i < \deg g_k = D$, the degree of I .

Proposition 6. *Let $r, d \in \mathbb{N}$, $\mathcal{H}_r(t)$ be the reduced numerator of the Hilbert series 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 \mathcal{F}_r of $\mathbb{K}[x_1, \dots, x_k]_{\leq d}^{n(n+1)/2}$ such that if the entries of the matrix $S^{k,d}$ are taken in \mathcal{F}_r , then the ideal $\mathcal{S}_r^{k,d}$ is radical and zero-dimensional and its Hilbert series $\mathcal{H}_r^{k,d}$ is equal to*

$$(1 + t + \dots + t^{d-1})^k \mathcal{H}_r(t^d).$$

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

Proof. We start in a homogeneous setting with $\mathbb{K}[x_0, x_1, \dots, x_k]_d$ denoting the subset of homogeneous polynomials of degree d in $\mathbb{K}[x_0, x_1, \dots, x_k]$ 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 $\mathbb{K}[s, x_0, \dots, x_k]$ generated by the $(r+1)$ -minors of S . By [26], $\mathbb{K}[s, x_0, \dots, x_k]/\mathcal{S}_r$ is a Cohen-Macaulay ring.

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

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

Assume that $f_{i,j} \in \mathbb{K}[x_1, \dots, x_n]_d$. Let $f_{i,j}^h$ be the homogenization of $f_{i,j}$ in $\mathbb{K}[x_0, \dots, x_k]$. We consider the quasi-homogeneous ideal

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

Through similar techniques as in [21, Sec. 3 and 4], there exists a non-empty Zariski-open subset \mathcal{Z} of $\mathbb{K}[x_0, \dots, x_k]_d^{n(n+1)/2}$ such that when the polynomials $f_{i,j}^h$ lie in \mathcal{Z} , the ideals J and $J + \langle x_0 \rangle$ have dimension one and zero respectively. Since $\mathcal{S}_r^{k,d}$ is the dehomogenized ideal of J , it has dimension zero. Moreover, by the unmixedness theorem [14, Cor. 18.14], the $n(n+1)/2+1$ polynomials

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

forms a regular sequence over $\mathbb{K}[s, x_0, \dots, x_k]/\mathcal{S}_r$. Therefore, the Hilbert series of $J + \langle x_0 \rangle$ is equal to

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

Next, we prove that there exists a non-empty Zariski-open subset $\mathcal{J} \subset \mathbb{K}[x_0, \dots, x_k]_d^{n(n+1)/2}$ such that, for $f_{i,j}^h \in \mathcal{J}$, J is radical. By [7, Theorem 2.9], there exists a monomial ordering \prec such that the corresponding initial ideal $\text{in}_{\prec}(\mathcal{S}_r)$ is generated by square-free 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 [2, 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 $f_{i,j}^h$ as new variables c in the space $\mathcal{C} = \overline{\mathbb{K}}[x_0, \dots, x_k]_d^{n(n+1)/2}$. Define the map φ by

$$\begin{aligned} \varphi : \overline{\mathbb{K}}^{\binom{n+1}{2}+k} \times \mathcal{C} &\rightarrow \overline{\mathbb{K}}^{\binom{n-r+1}{2}} \times \overline{\mathbb{K}}^{\binom{n+1}{2}} \\ (s, \mathbf{x}, \mathbf{c}) &\mapsto (\mathfrak{M}, s_{1,1} - f_{1,1}^h, \dots, s_{n,n} - f_{n,n}^h) \end{aligned}$$

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

$$\text{jac}(\varphi) := \begin{bmatrix} \text{jac}_s(\mathfrak{M}) & \mathbf{0} & \dots & \mathbf{0} & \mathbf{0} \\ * & \mathbf{x}_0^d \text{Id} & \dots & \mathbf{x}_k^d \text{Id} & \dots \end{bmatrix},$$

where the blocks $\mathbf{x}_i^d \text{Id}$ come from the derivatives of $s_{i,j} - f_{i,j}^h$ w.r.t. the coefficients of x_i^d of $f_{i,j}^h$.

For any s such that $\mathfrak{m}(s) \neq 0$, $\text{jac}_s(\mathfrak{M})$, and therefore $\text{jac}(\varphi)$, has maximal rank over the projective space of (x_0, \dots, x_k) . Thus, the Jacobian criterion [14, Theorem 16.19] implies that $\mathbf{0}$ is a regular value of φ . By Thom's weak transversality theorem [33, Proposition B.3], there exists a Zariski-open dense subset $\mathcal{C}_{\mathfrak{m}}$ of \mathcal{C} such that for any $c \in \mathcal{C}_{\mathfrak{m}}$, $\mathbf{0}$ is a regular value of φ_c and the Jacobian matrix of

φ_c has maximal rank when $\mathfrak{m}(s) \neq 0$ and $(x_0, \dots, x_k) \neq \mathbf{0}$, which means J is radical. By dehomogenizing J , the ideal $S_r^{k,d}$ is radical.

Now, let $S_r^{k,d,h}$ be the homogenized ideal of $S_r^{k,d}$. The radicality of $S_r^{k,d}$ implies that $S_r^{k,d,h}$ is also radical. As $J + \langle x_0 \rangle$ has dimension zero, the projective varieties $V(J)$ and $V(S_r^{k,d,h})$ in $\mathbb{P}(\overline{\mathbb{K}})^k$ coincide. Since J is radical, the homogeneous Hilbert's Nullstellensatz [3, Corollary 4.80] gives $J = I(V(J)) = I(V(S_r^{k,d,h})) = S_r^{k,d,h}$. Thus, the Hilbert series of $S_r^{k,d}$ equals the Hilbert series of $J + \langle x_0 \rangle$ whose explicit form is already proven above.

Finally, let \mathcal{F}_r be the intersection of \mathcal{L} and \mathcal{J} , identified as a Zariski-open dense subset of $\mathbb{K}[x_1, \dots, x_k]_{\leq d}^{n(n+1)/2}$ by specializing x_0 to one, with the sets \mathcal{C}_m for all r -minors \mathfrak{m} of S . For any $c \in \mathcal{F}_r$, the ideal $S_r^{k,d}$ 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 [4, Proposition 5]. There exists a Zariski-open dense subset \mathcal{O} of $\text{GL}(k, \mathbb{K})$ such that for all $A \in \mathcal{O}$, after applying A , the points of the variety $V(S_r^{k,d})$ have distinct x_k coordinates. Thus, the ideal $S_r^{k,d}$ is in shape position. \square

4 ASYMPTOTIC COMPLEXITY

4.1 The general case

Given a Gröbner basis of a zero-dimensional ideal in $\mathbb{K}[x_1, \dots, x_k]$ w.r.t. an ordering $<_1$, the Sparse-FGLM algorithm [19] computes a Gröbner basis of the same ideal but w.r.t. a target ordering $<_2$. A common change of ordering for practical uses is from a grevlex ordering to a lexicographic one [12, 20, 21]. 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 $\mathcal{F}_r \subset \mathbb{K}[x_1, \dots, x_k]_{\leq d}^{n(n+1)/2}$ defined by Proposition 6. Then, the ideal $S_r^{k,d}$ is zero-dimensional and in shape position.

Given a zero-dimensional ideal $I \subset \mathbb{K}[x_1, \dots, x_k]$ of degree D , let \mathcal{G} be its reduced Gröbner basis w.r.t. the ordering $<_{\text{grevlex}}$. It is well known that $\mathbb{K}[x_1, \dots, x_k]/I$ 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, \dots, x_k are linear maps of $\mathbb{K}[x_1, \dots, x_k]/I$, whose matrix representations T_{x_1}, \dots, 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-Socias conjecture [30, 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 $(0, \dots, 0, 1, 0, \dots, 0)$ where the row of 1 corresponds to $x_k \cdot b$.

- $x_k \cdot b$ is the leading monomial of some $g \in \mathcal{G}$: in this case, the column is easily obtained from the coefficients of $x_k \cdot b - g$.
- 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-Socias' 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 [5], 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. The existence of the set \mathcal{F}_r such that $S_r^{k,d}$ is zero-dimensional and radical is given by Proposition 6. By the first item of Conjecture 2, \mathcal{H}_r is unimodal, which then implies that $(1 + \dots + t^{d-1})\mathcal{H}_r(t^d)$ is unimodal. By [5, Lemma 17], $1 + \dots + t^{d-1}$ is a strongly unimodal polynomial. Hence, the Hilbert series $\mathcal{H}_r^{k,d}$ given in Proposition 6 is also unimodal.

Let $A_r^{k,d} = \mathbb{K}[x_1, \dots, x_k]/S_r^{k,d}$ and $S_r^{k,d,h}$ be the homogenization of $S_r^{k,d}$. We shall construct the matrix T_{x_k} column by column. As in [19], the columns are indexed by elements in the basis \mathcal{B} of $A_r^{k,d}$, given by the ordering $<_{\text{grevlex}}$. For any $b \in \mathcal{B}$, the entries in its corresponding column are the coefficients of the normal form of $x_k \cdot b$ expressed in terms of the basis \mathcal{B} . By [5, 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, there are bijections between the dense columns of T_k , the polynomials in \mathcal{G} whose leading terms are divisible by x_k and then the elements in \mathcal{B} which are not divisible by x_k . The cardinal of the last set equals the dimension of $\mathbb{K}[x_0, \dots, x_k]/(S_r^{k,d,h} + \langle x_0, x_k \rangle)$ which can be read by evaluating $Q_r^{k,d,1}(1)$. When Conjecture 2 holds, similar to [5, Lemma 25], we deduce that the largest coefficient of $\mathcal{H}_r^{k,d}$ equals $Q_r^{k,d,1}(1)$. \square

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

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

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

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

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

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

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

Note that the coefficient of t^i in g is the sum of the coefficients of t^{i-d+1}, \dots, 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 . \square

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

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

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

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

Proof. By Lemma 11, $(1 + \dots + t^{d-1})^6$ is unimodal and symmetric. And so is \mathcal{H}_{n-3} from its explicit formula. Thus, by Lemma 11, the largest coefficient m of the Hilbert series $\mathcal{H}_{n-3}^{6,d}$, which is actually a polynomial, depends only on the central $5(d-1) + 1$ coefficients of $(1 + \dots + t^{d-1})\mathcal{H}_{n-3}(t^d)$. This number then depends on at most the central 5 coefficients of the polynomial $\mathcal{H}_{n-3}(t)$.

By [19, Corollary 5.10], all coefficients of $(1 + \dots + t^{d-1})^6$ 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 $d \rightarrow \infty$,

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

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

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

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

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

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

Proposition 14. *The largest coefficient of*

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

as $n \rightarrow \infty$ 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 $(1 + \dots + t^{d-1})^{\binom{n}{2}}$ is symmetric and unimodal, its largest coefficient is central. By an abridged version of [35, Theorem 2], this largest coefficient is asymptotically equal to

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

as $n \rightarrow \infty$. 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 $n \rightarrow \infty$ is at least

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

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

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

5 EXPERIMENTS

5.1 Supporting Conjecture 2

This subsection reports on our testing of Conjecture 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 [21], it is not proven to be unimodal.

Secondly, the second item of Conjecture 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 . Homogenizing this Gröbner basis, we obtain a Gröbner basis of the homogenized ideal I^h w.r.t. the \langle_{grevlex} ordering where $x_1 > \dots > x_k > x_0$. Finally, adding $\langle x_0, x_k \rangle$ gives a Gröbner basis of $I^h + \langle x_0, x_k \rangle$ w.r.t. the \langle_{grevlex} ordering with $x_1 > \dots > x_k > x_0$ [30, Lemma 1.9]. Then, we can compute the Hilbert series and compare this to the formula $[(1 - t^e)P]_+$ to test the second item. The current status of testing this conjecture can be found at the following website: https://www-polsys.lip6.fr/~ferguson/conjecture_testing.html.

5.2 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 exact numbers of dense columns in the matrices T_{x_3} using Proposition 9.

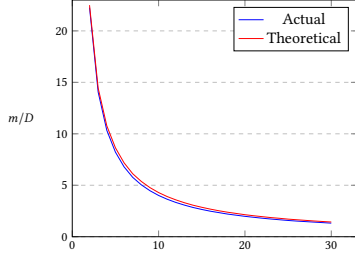


Figure 1: Density of T_{x_3} for $S_{n-2}^{3,d}$ for $d \in \{2, \dots, 50\}$

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 (d, n)	Degree D	Matrix Density		
		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 $S_3^{6,d}$

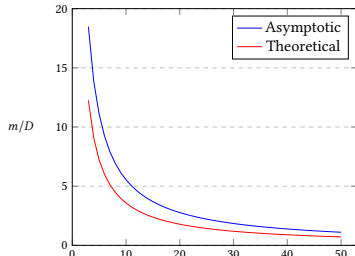


Figure 2: Density of T_{x_6} for $S_{n-3}^{6,d}$ for $d \in \{3, \dots, 50\}$

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.

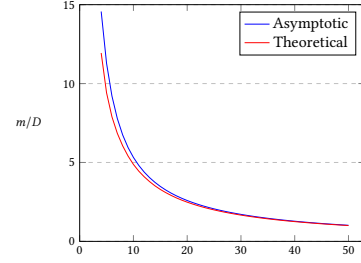


Figure 3: Density of $T_{x_{(2)}}$ for $S_1^{(n),4}$ for $n \in \{4, \dots, 50\}$

6 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 [6]. There, 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. Our bound on m enables more precise comparison of this new algorithm in [6] with the existing algorithms based on fast linear algebra [17, 32] whose complexities lie in $\tilde{O}(D^\omega)$.

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. For instance, we discuss the case of Hankel variable matrices and derive an alternative derivation of the Hilbert series of S_{n-2} .

Let $n \in \mathbb{N}$, c_0, \dots, c_{2n-2} be new variables and C be the Hankel matrix

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

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

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

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

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

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

Since $\mathbb{K}[m_{0,0}, \dots, m_{r,2n-r-2}]/I$ is a Cohen-Macaulay ring of the same codimension $2n-2r-1$ as $\mathbb{K}[c_0, \dots, c_{2n-2}]/C_r$, the unmixedness theorem [14, Cor. 18.14] and [5] 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 S_{n-2} have codimension three, one can obtain a different derivation of the Hilbert series of 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 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.

REFERENCES

- [1] Josh Alman and Virginia Vassilevska Williams. 2021. A Refined Laser Method and Faster Matrix Multiplication. In *Proceedings of the Thirty-Second Annual ACM-SIAM Symposium on Discrete Algorithms* (Virtual Event, Virginia) (SODA '21). Society for Industrial and Applied Mathematics, USA, 522–539. <https://doi.org/10.1137/1.9781611976465.32>
- [2] Bernd Bank, Marc Giusti, Joos Heintz, and Guy Merlin Mbakop. 2001. Polar varieties and efficient real elimination. *Mathematische Zeitschrift* 238, 1 (2001), 115–144. <https://doi.org/10.1007/PL00004896>
- [3] Saugata Basu, Richard Pollack, and Marie-Françoise Roy. 2006. *Algorithms in Real Algebraic Geometry*. Springer-Verlag, Berlin, Heidelberg. <https://doi.org/10.1007/3-540-33099-2>
- [4] Becker, Eberhard and Mora, Teo and Marinari, Maria Grazia and Traverso, Carlo. 1994. The Shape of the Shape Lemma. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation* (Oxford, United Kingdom) (ISSAC '94). Association for Computing Machinery, New York, NY, USA, 129–133. <https://doi.org/10.1145/190347.190382>
- [5] Jérémy Berthomieu, Alin Bostan, Andrew Ferguson, and Mohab Safey El Din. 2022. Gröbner bases and critical values: The asymptotic combinatorics of determinantal systems. *Journal of Algebra* 602 (2022), 154–180. <https://doi.org/10.1016/j.jalgebra.2022.03.002>
- [6] Jérémy Berthomieu, Vincent Neiger, and Mohab Safey El Din. 2022. Faster Change of Order Algorithm for Gröbner Bases Under Shape and Stability Assumptions. In *Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation* (Villeneuve-d'Ascq, France) (ISSAC '22). Association for Computing Machinery, New York, NY, USA, 9 pages. <https://doi.org/10.1145/3476446.3535484>
- [7] Aldo Conca. 1994. Gröbner Bases of Ideals of Minors of a Symmetric Matrix. *Journal of Algebra* 166 (1994), 406–421. <https://doi.org/10.1006/jabr.1994.1160>
- [8] Aldo Conca. 1994. Symmetric ladders. *Nagoya Mathematical Journal* 136 (1994), 35–56. <https://doi.org/10.1017/S0027763000024958>
- [9] Aldo Conca. 1998. Straightening Law and Powers of Determinantal Ideals of Hankel Matrices. *Advances in Mathematics* 138, 2 (1998), 263–292. <https://doi.org/10.1006/aima.1998.1740>
- [10] Aldo Conca, Emanuela De Negri, and Volkmar Welker. 2016. A Gorenstein simplicial complex for symmetric minors. *Israel Journal of Mathematics* 212 (2016), 237–257. <https://doi.org/10.1007/s11856-016-1285-x>
- [11] Aldo Conca and Jürgen Herzog. 1994. On the Hilbert Function of Determinantal Rings and Their Canonical Module. *Proc. Amer. Math. Soc.* 122, 3 (1994), 677–681. <https://doi.org/10.2307/2160740>
- [12] David A. Cox, John Little, and Donal O'Shea. 2005. *Using Algebraic Geometry*. Springer-Verlag New York, New York, NY. <https://doi.org/10.1007/b138611>
- [13] David A. Cox, John Little, and Donal O'Shea. 2015. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer-Verlag, Berlin, Heidelberg. <https://doi.org/10.1007/978-3-319-16721-3>
- [14] David Eisenbud. 1995. *Commutative Algebra: With a View Toward Algebraic Geometry*. Springer New York, New York, NY. <https://doi.org/10.1007/978-1-4612-5350-1>
- [15] Jean-Charles Faugère. 1999. A new efficient algorithm for computing Gröbner bases (F4). *Journal of pure and applied algebra* 139, 1-3 (1999), 61–88. [https://doi.org/10.1016/S0022-4049\(99\)00005-5](https://doi.org/10.1016/S0022-4049(99)00005-5)
- [16] Jean-Charles Faugère. 2002. 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* (Lille, France) (ISSAC '02). Association for Computing Machinery, New York, NY, USA, 75–83. <https://doi.org/10.1145/780506.780516>
- [17] Jean-Charles Faugère, Pierrick Gaudry, Louise Huot, and Guénaél Renault. 2014. Sub-Cubic Change of Ordering for Gröbner Basis: A Probabilistic Approach. In *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation* (Kobe, Japan) (ISSAC '14). Association for Computing Machinery, New York, NY, USA, 170–177. <https://doi.org/10.1145/2608628.2608669>
- [18] Jean-Charles Faugère, Patrizia Gianni, Daniel Lazard, and Teo Mora. 1993. Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering. *Journal of Symbolic Computation* 16, 4 (1993), 329–344. <https://doi.org/10.1006/jsc.1993.1051>
- [19] Jean-Charles Faugère and Chenqi Mou. 2017. Sparse FGLM algorithms. *Journal of Symbolic Computation* 80 (2017), 538–569. <https://doi.org/10.1016/j.jsc.2016.07.025>
- [20] Jean-Charles Faugère, Mohab Safey El Din, and Pierre-Jean Spaenlehauer. 2012. Critical Points and Gröbner Bases: The Unmixed Case. In *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation* (Grenoble, France) (ISSAC '12). Association for Computing Machinery, New York, NY, USA, 162–169. <https://doi.org/10.1145/2442829.2442855>
- [21] Jean-Charles Faugère, Mohab Safey El Din, and Pierre-Jean Spaenlehauer. 2013. On the complexity of the generalized MinRank problem. *J. Symbolic Comput.* 55 (2013), 30–58. <https://doi.org/10.1016/j.jsc.2013.03.004>
- [22] Ralf Fröberg. 1985. An inequality for Hilbert series of graded algebras. *Math. Scand.* 56, 2 (1985), 117–144. <http://www.jstor.org/stable/24491560>
- [23] Didier Henrion, Simone Naldi, and Mohab Safey El Din. 2015. Real Root Finding for Rank Defects in Linear Hankel Matrices. In *Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation* (Bath, United Kingdom) (ISSAC '15). Association for Computing Machinery, New York, NY, USA, 221–228. <https://doi.org/10.1145/2755996.2756667>
- [24] Didier Henrion, Simone Naldi, and Mohab Safey El Din. 2016. Exact Algorithms for Linear Matrix Inequalities. *SIAM Journal on Optimization* 26, 4 (2016), 2512–2539. <https://doi.org/10.1137/15M1036543>
- [25] Didier Henrion, Simone Naldi, and Mohab Safey El Din. 2016. Real root finding for determinants of linear matrices. *Journal of Symbolic Computation* 74 (2016), 205–238. <https://doi.org/10.1016/j.jsc.2015.06.010>
- [26] Ronald E. Kutz. 1974. Cohen-Macaulay Rings and Ideal Theory in Rings of Invariants of Algebraic Groups. *Trans. Am. Math. Soc.* 194 (1974), 115–129. <https://doi.org/10.2307/1996796>
- [27] Huu Phuoc Le and Mohab Safey El Din. 2021. Faster One Block Quantifier Elimination for Regular Polynomial Systems of Equations. In *Proceedings of the 2021 on International Symposium on Symbolic and Algebraic Computation* (Virtual Event, Russian Federation) (ISSAC '21). Association for Computing Machinery, New York, NY, USA, 265–272. <https://doi.org/10.1145/3452143.3465546>
- [28] Huu Phuoc Le and Mohab Safey El Din. 2022. Solving parametric systems of polynomial equations over the reals through Hermite matrices. *Journal of Symbolic Computation* 112 (2022), 25–61. <https://doi.org/10.1016/j.jsc.2021.12.002>
- [29] Juan Migliore and Uwe Nagel. 2013. Survey Article: A tour of the weak and strong Lefschetz properties. *Journal of Commutative Algebra* 5, 3 (2013), 329–358. <https://doi.org/10.1216/JCA-2013-5-3-329>
- [30] Guillermo Moreno-Socías. 2003. Degrevlex Gröbner bases of generic complete intersections. *J. Pure Appl. Algebra* 180, 3 (2003), 263–283. [https://doi.org/10.1016/S0022-4049\(02\)00297-9](https://doi.org/10.1016/S0022-4049(02)00297-9)
- [31] Simone Naldi. 2018. Solving rank-constrained semidefinite programs in exact arithmetic. *Journal of Symbolic Computation* 85 (2018), 206–223. <https://doi.org/10.1016/j.jsc.2017.07.009>
- [32] Vincent Neiger and Éric Schost. 2020. Computing syzygies in finite dimension using fast linear algebra. *Journal of Complexity* 60 (2020), 101502. <https://doi.org/10.1016/j.jco.2020.101502>
- [33] Mohab Safey El Din and Éric Schost. 2017. A Nearly Optimal Algorithm for Deciding Connectivity Queries in Smooth and Bounded Real Algebraic Sets. *J. ACM* 63, 6, Article 48 (Jan. 2017), 37 pages. <https://doi.org/10.1145/2996450>
- [34] Pierre-Jean Spaenlehauer. 2014. On the Complexity of Computing Critical Points with Gröbner Bases. *SIAM Journal on Optimization* 24 (07 2014), 1382–1401. <https://doi.org/10.1137/130936294>
- [35] Z. Star. 1975. An asymptotic formula in the theory of compositions. *Aequationes Mathematicae* 13 (1975), 279–284. <https://doi.org/10.1007/BF01836532>
- [36] Bernd Sturmfels. 1990. Gröbner bases and Stanley decompositions of determinantal rings. *Mathematische Zeitschrift* 205 (1990), 137–144. <https://doi.org/10.1007/BF02571229>