Gröbner bases and critical values: The asymptotic combinatorics of determinantal systems

Jérémy Berthomieu[a], Alin Bostan[b], Andrew Ferguson[a], Mohab Safey El Din[a]

[a] *Sorbonne Université, CNRS, LIP6, F-75005, Paris, France*
[b] *Inria, Université Paris-Saclay, 1 rue Honoré d'Estienne d'Orves, 91120 Palaiseau, France*

Abstract

Determinantal polynomial systems are those involving maximal minors of some given matrix. An important situation where these arise is the computation of the critical values of a polynomial map restricted to an algebraic set. This leads directly to a strategy for, among other problems, polynomial optimisation.

Computing Gröbner bases is a classical method for solving polynomial systems in general. For practical computations, this consists of two main stages. First, a Gröbner basis is computed with respect to a DRL (degree reverse lexicographic) ordering. Then, a change of ordering algorithm, such as Sparse-FGLM, designed by Faugère and Mou, is used to find a Gröbner basis of the same system but with respect to a lexicographic ordering. The complexity of this latter step, in terms of the number of arithmetic operations in the ground field, is $O(mD^2)$, where D is the degree of the ideal generated by the input and m is the number of non-trivial columns of a certain $D \times D$ matrix.

While asymptotic estimates are known for m in the case of *generic* polynomial systems, thus far, the complexity of Sparse-FGLM was unknown for the class of determinantal systems.

By assuming Fröberg's conjecture, thus ensuring that the Hilbert series of generic determinantal ideals have the necessary structure, we expand the work of Moreno-Socías by detailing the structure of the DRL staircase in the determinantal setting. Then, we study the asymptotics of the quantity m by relating it to the coefficients of these Hilbert series. Consequently, we arrive at a new bound on the complexity of the Sparse-FGLM algorithm for generic determinantal systems and, in particular, for generic critical point systems.

We consider the ideal inside the polynomial ring $\mathbb{K}[x_1, \ldots, x_n]$, where $\mathbb{K}$ is some infinite field, generated by p generic polynomials of degree d and the maximal minors of a $p \times (n-1)$ polynomial matrix with generic entries of degree $d-1$. Then, in this setting, for the case $d = 2$ and for $n \gg p$ we establish an exact formula for m in terms of n and p. Moreover, for $d \geq 3$, we give a tight asymptotic formula, as $n \to \infty$, for m in terms of n, p and d.

Keywords: determinantal ideals, Gröbner bases, combinatorics, Hilbert series

1. Introduction and preliminaries

Motivation. By the Lagrange multiplier theorem, the local extrema of a polynomial mapping restricted to a real algebraic set are contained in the set of critical values of the map. Thus, computing these values, and the corresponding minimum/critical points where these extrema are reached, leads to a strategy for polynomial optimisation under some regularity assumptions.

Polynomial optimisation is of principal importance in many areas of engineering and social sciences (including control theory [17, 18], computer vision [1, 24] and optimal design [7], etc.).

Critical point computations are also a fundamental task in the algorithms of effective real algebraic geometry. For example, the problems of deciding the emptiness of the set of real solutions of a polynomial system, counting the number of connected components of such sets and one block quantifier elimination can all be accomplished, under some regularity assumptions, by the so-called critical point method [3, Ch. 7], see also [19, 25].

With $\mathbb{K}$ an infinite field, let $f = (f_1, \ldots, f_p) \in \mathbb{K}[x_1, \ldots, x_n]$ be a sequence of polynomials of degree d and let $\mathbf{V}(f) \subset \mathbb{K}^n$ be their simultaneous vanishing set. Define φ_1 to be the projection map onto the first coordinate. We denote by $\mathcal{J}$ the Jacobian of (φ_1, f),

$$\mathcal{J} := \begin{bmatrix} 1 & 0 & \cdots & 0 \\ \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial f_p}{\partial x_1} & \frac{\partial f_p}{\partial x_2} & \cdots & \frac{\partial f_p}{\partial x_n} \end{bmatrix}.$$

An example of the ideals we consider in this paper is the ideal I defined by f and the maximal minors of $\mathcal{J}$. By a corollary of the Jacobian criterion [8, Corollary 16.20], when f is a reduced regular sequence and $\mathbf{V}(f)$ is smooth, the algebraic set $\mathbf{V}(I)$ is exactly the set of critical points of the projection map φ_1 restricted to the algebraic set $\mathbf{V}(f)$.

Throughout this paper, we shall consider *generic* determinantal systems. Essentially, for the example of critical point systems, we choose the coefficients of the polynomials $f_1, \ldots, f_p$ so that they lie inside a non-empty Zariski open subset of $\mathbb{K}^{\binom{n+d}{d}}$ where the results of [12] hold. In particular, the generic systems we consider satisfy the conditions of the Jacobian criterion so that I encodes the critical points of φ_1 restricted to $\mathbf{V}(f)$ [26, Lemma A.2]. Moreover, by [12, Lemma 2] and [20, Proposition 4.2], I is a zero-dimensional, radical ideal. So, the quotient algebra $\mathbb{K}[x_1, \ldots, x_n]/I$ is a finite dimensional vector space over $\mathbb{K}$.

For the many applications of the critical point method previously discussed, one wishes to compute a rational parametrisation of this set of critical points. By our genericity conditions, we shall assume that the ideal I is in shape position, meaning that for a lexicographic (LEX) ordering with x_n as the least variable, the LEX Gröbner basis has the following structure:

$$\{x_1 - g_1(x_n), \ldots, x_{n-1} - g_{n-1}(x_n), g_n(x_n)\},$$

where the degree of g_n is the degree of the ideal I [4]. A fast method commonly used in practice, and the one which we shall use, to compute a LEX Gröbner basis is to first compute a Gröbner basis of I with respect to a degree reverse lexicographic ordering (DRL). Then, one uses a change of ordering algorithm to compute another Gröbner basis of I but with respect to a LEX ordering.

Previous works. In [12, Theorem 3], Faugère, Safey El Din and Spaenlehauer give an upper bound on the number of arithmetic operations necessary for computing a LEX Gröbner basis of a generic determinantal system within the DRL to LEX framework. They do so by deriving the Hilbert series of such a system, using results by Conca and Herzog [5, Corollary 1].

Then, based on a result of Bardet, Faugère and Salvy [2, Theorem 7], the authors of [12, Theorem 3] analyse the complexity of the DRL step using Faugère's F_5 algorithm [9]. Here, and in the whole text, complexity estimates are given in terms of arithmetic operations in the ground field $\mathbb{K}$. Next, to obtain a LEX Gröbner basis, since we are in the zero-dimensional case, they use the FGLM algorithm to perform the change of ordering [10]. The complexity of FGLM is $O(nD^3)$, where D is the degree of the determinantal ideal. In [22, Theorem 2.2], Nie and Ranestad use the Thom-Porteous-Giambelli formula to prove that this degree is

$$D = d^p(d-1)^{n-p}\binom{n-1}{p-1}.$$

In [11], Faugère and Mou proposed another algorithm that solves the change of ordering step, the Sparse-FGLM algorithm. Under some genericity assumptions, Sparse-FGLM relies primarily on the structure of the matrix M_n associated to the linear map of multiplication by x_n in the finite dimensional quotient algebra $\mathbb{K}[x_1, \ldots, x_n]/I$. Its complexity is $O(mD^2 + nD\log^2 D)$, where m is the number of non-trivial columns of the matrix M_n. This number is studied in the same paper for generic complete intersections using the results of Moreno-Socías [21]. By deriving the asymptotics of the number of non-trivial columns, as well as by proving that the structure of the matrix M_n is such that it can be computed free of arithmetic operations, Faugère and Mou demonstrate in [11] that the complexity of Sparse-FGLM is indeed an improvement of that of FGLM.

Main results. In this paper, under similar genericity assumptions and by assuming a variant of Fröberg's conjecture [14], we extend the results of [11, 21] to generic determinantal ideals. We emphasise here that our results hold not only for critical point systems but indeed for any sufficiently generic determinantal system. This is made precise in Definition 8.

Firstly, we prove a result on the structure of the DRL staircase, which implies that the only non-trivial columns of M_n correspond one-to-one with monomials which, once multiplied by x_n, give a leading monomial in the reduced DRL Gröbner basis. Furthermore, for each such monomial, one can read the entries of the corresponding non-trivial column from the polynomial in the Gröbner basis with that leading monomial. This implies the following theorem.

Theorem 1. *Let I be a generic determinantal ideal so that the conditions of Definition 8 hold. Assume that a reduced and minimal Gröbner basis of I with respect to a DRL ordering is known. Then, the multiplication matrix M_n can be constructed without performing any arithmetic operations.*

Continuing further, we prove an explicit formula for the number of non-trivial columns of M_n, which we denote m, in the case of quadratic polynomials with a large number of variables n compared to the number of polynomials p. Then, for any choice of degree $d \geq 3$ and for $n \to \infty$, we prove asymptotic formulae for m.

Theorem 2. *Let I be a generic determinantal ideal so that the conditions of Definition 8 hold, and let M_n be the multiplication matrix associated to multiplication by x_n. Denote by m the number of non-trivial columns of M_n. Then, for $d = 2$ and $n \gg p$, the number m is equal to:*

$$m = \sum_{k=0}^{p-1} \binom{n-p-1+k}{k} \binom{p}{\lfloor 3p/2 \rfloor - 1 - j}. \tag{1}$$

Moreover, for $d \geq 3$ and $n \to \infty$, the number m is asymptotically equal to

$$m \approx \frac{1}{\sqrt{(n-p)\pi}} \sqrt{\frac{6}{(d-1)^2-1}} d^p (d-1)^{n-p} \binom{n-2}{p-1}. \tag{2}$$

By [11, Theorem 3.2], and since the ideals we consider are in shape position, Theorem 2 leads directly to a complexity result for the Sparse-FGLM algorithm. Therefore, we arrive at an improved upper bound on the complexity of the change of ordering step for generic determinantal systems.

Theorem 3. *Let I be a generic determinantal ideal so that the conditions of Definition 8 hold. Assume that a reduced and minimal DRL Gröbner basis of I is known. Then, for $d \geq 3$, the arithmetic complexity of computing a LEX Gröbner basis of I is upper bounded by*

$$O\left(\frac{d^{3p}(d-1)^{3(n-p)}}{\sqrt{(n-p)d\pi}} \binom{n-2}{p-1} \binom{n-1}{p-1}^2 \right).$$

Hence, the complexity gain of Sparse-FGLM over FGLM for generic determinantal systems is approximately

$$O\left(\frac{m}{nD}\right) \approx O\left(\frac{\sqrt{n-p}}{n^2(d-1)}\right).$$

Organisation of the paper. The remainder of the paper consists of: Section 2, where we define the class of ideals for which our results hold; Section 3, where we prove our main results; and Section 4, where we test our formula for the number of non-trivial columns of the matrix M_n for various parameters.

2. Preliminaries

2.1. Shape position

Let $f_1, \ldots, f_p \in \mathbb{K}[x_1, \ldots, x_n]$ be polynomials of degree d. Similarly, let $h_{1,2}, \ldots, h_{p,n} \in \mathbb{K}[x_1, \ldots, x_n]$ be polynomials of degree $d-1$. Let I be the ideal generated by $\langle f_1, \ldots, f_p \rangle$ and the maximal minors of the following matrix:

$$\begin{bmatrix} h_{1,2} & \cdots & h_{1,n} \\ \vdots & \ddots & \\ h_{p,2} & \cdots & h_{p,n} \end{bmatrix}.$$

The authors of [20, Proposition 4.2] show that if the coefficients of $f_1, \ldots, f_p$ and $h_{1,2}, \ldots, h_{p,n}$ are chosen in some non-empty Zariski open subsets of $\mathbb{K}^{\binom{n+d}{d}}$ and $\mathbb{K}^{\binom{n+d-1}{d-1}}$ respectively, then the ideal I defined above is a zero-dimensional, radical ideal.

In order to apply the results of [11] to our determinantal ideals, we require they be in shape position. To ensure this, we add a new indeterminate. For any $\lambda \in \mathbb{K}^n$, define the ideal

$$J = I + \langle y - \sum_{j=1}^{n} \lambda_j x_j \rangle \quad \subset \quad \mathbb{K}[x_1, \ldots, x_n, y].$$

Lemma 4. *Let $\mathbb{K}$ be an infinite field. Then, there exists a non-empty Zariski open subset $\mathcal{O}$ of $\mathbb{K}^n$ such that for all $\lambda \in \mathcal{O}$ and with y as the least variable in the LEX ordering, the ideal J is in shape position.*

Proof. By [20, Proposition 4.2], the ideal I is radical and zero-dimensional. Thus, for all $\lambda \in \mathbb{K}^n$, the ideal J is also zero-dimensional and radical. By [16, Proposition 1.6], [4, Proposition 5] and the genericity of the polynomials defining I we have that J is in shape position if and only if each of the finitely many points in the algebraic set $\mathbf{V}(J)$, defined by J, has a unique y-coordinate. As $\mathbb{K}$ is infinite, the finitely many linear equations that give equality of the y coordinate of any two points in $\mathbf{V}(J)$ define a proper Zariski closed subset of $\mathbb{K}^n$. Therefore, there exists a non-empty Zariski open subset $\mathcal{O}$ of $\mathbb{K}^n$ such that for all $\lambda \in \mathcal{O}$ the y coordinate of each point in the algebraic set $\mathbf{V}(J)$ is unique. Hence, the ideal J is in shape position. □

2.2. Fröberg's conjecture

As a direct consequence of [5], the authors of [12] further show that under the same genericity assumptions, the following proposition holds:

Proposition 5 ([12, Proposition 1])**.** *The Hilbert series of $\mathbb{K}[x_1, \ldots, x_n]/I$ is*

$$H = \frac{\det(P(t^{d-1}))}{t^{(d-1)\binom{p-1}{2}}} \frac{(1-t^d)^p (1-t^{d-1})^{n-p}}{(1-t)^n}$$

where $P(t)$ is the $(p-1)\times(p-1)$ matrix whose (i,j)th entry is $\sum_k \binom{p-i}{k}\binom{n-1-j}{k} t^k$.

We shall consider the quotients of the algebra $\mathbb{K}[x_1, \ldots, x_n]/I$ by powers of generic linear forms. By the genericity introduced above, it suffices to consider the quotients of $A = \mathbb{K}[x_1, \ldots, x_n, y]/J$ by powers of y. Thus, denote by HQ_e the Hilbert series of $A/\langle y^e \rangle$, for $e \geq 1$. In order to control the shape of this Hilbert series, we rely on a variant of Fröberg's conjecture given in [13, Lemma 14]. First, however, a definition.

Definition 6. *For a series $S = \sum_k a_k t^k$, we define*

$$\left[\sum_k a_k t^k\right]_+$$

to be the series S truncated at the first non-positive coefficient.

Lemma 7 ([13, Lemma 14])**.** *If Fröberg's conjecture is true, then for all $e \geq 1$ we have that*

$$HQ_e = [(1 - t^e)H]_+ .$$

We remark that in [23], Pardue showed that Moreno-Socías' conjecture [21, Conjecture 4.2] implies Fröbergs conjecture, as well as a number of other interesting conjectures. Moreover, while these conjectures are usually given in a homogeneous setting, we shall assume that Lemma 7 holds also in the affine case.

2.3. Generic determinantal ideals

With the assumption of Fröberg's conjecture, we define precisely the class of ideals we consider in this paper.

Definition 8. *Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be an ideal with $\mathbb{K}$ an infinite field. We say that I is a generic determinantal ideal if the following three conditions hold:*

- *the ideal I is in shape position,*
- *the Hilbert series of $\mathbb{K}[x_1, \ldots, x_n]/I$ is given by Proposition 5,*
- *the conclusion of Lemma 7 holds for the Hilbert series of $\mathbb{K}[x_1, \ldots, x_n]/I$.*

By our genericity assumptions, $f_1, \ldots, f_p$ is a reduced, regular sequence defining a smooth algebraic set $\mathbf{V}(f_1, \ldots, f_p)$. By [12, Lemma 6] and [6, Ch. 9, Sec. 3, Prop. 9], the determinantal ideal defining the critical points of the projection map onto the first coordinate restricted to $\mathbf{V}(f_1, \ldots, f_p)$ satisfies Proposition 5. Moreover, using the same addition of a new indeterminate as in Lemma 4, one may assume that such an ideal is in shape position. Thus, by assuming Fröberg's conjecture, these generic critical value systems are an important example of the generic determinantal ideals we consider.

Remark 9. *We note that without the addition of a new indeterminate, generic critical point systems may not satisfy the conditions of Definition 8. In particular, if one considers a DRL ordering with x_n as the least variable for the determinantal system defining the critical values of the projection map onto the x_n-axis, then Lemma 7 no longer holds. The consequence of this is that the results of this paper cannot then be applied to this special case. However, introducing a new indeterminate to be the least variable in the DRL ordering, as in Lemma 4, rectifies this problem. Therefore, we may assume that all critical point systems satisfy the conditions of Definition 8.*

Furthermore, note that the Hilbert series of $\mathbb{K}[x_1, \ldots, x_n]/I$ is equal to the Hilbert series of $\mathbb{K}[x_1, \ldots, x_n, y]/J$. Therefore, for ease of notation, we shall assume that the determinantal ideals considered in this paper satisfy Definition 8 without introducing the new indeterminate y.

3. Proofs

Roadmap. Firstly, as in the papers [11, 12, 21], to prove our results we rely on manipulations of the Hilbert series H from Proposition 5. However, for our purposes, the form involving the determinant of the matrix P makes this difficult. Thus, our first step is to express H in a simpler form in Section 3.1. Then, we show that this Hilbert series is always unimodal in Section 3.2. This property, along with the assumption of Fröberg's conjecture, allows us to prove in Section 3.3 a structure theorem on the generic DRL staircase. This leads to our first main result, that the multiplication matrix M_n can be constructed for free. Combining this result with the unimodality property, we show that the number of non-trivial columns of this matrix, a key parameter of the Sparse-FGLM algorithm, is equal to the largest coefficient of the series H. In Section 3.4, we conclude the proof of our main results by studying the asymptotics of the largest coefficient of H.

3.1. Simplification of the Hilbert series

As in the works we wish to generalise [11, 12, 21], our results rely heavily on the Hilbert series of the generic determinantal ideals we consider. Thus, the first stage we take is to simplify the form given in Proposition 5. We do so by expressing the determinant of the binomial matrix in this Hilbert series as a binomial sum. We start with some general results involving binomial matrices that will lead to the simplification we want as a special case.

Let $\mathcal{A} = (a_{ij})_{i,j\geq 0}$ be the infinite Pascal matrix defined by $a_{ij} = \binom{i}{j}$ for $j \leq i$ and $a_{ij} = 0$ for $j > i$. The minor of this matrix corresponding to rows $0 \leq a_1 < \cdots < a_n$ and columns $0 \leq b_1 < \cdots < b_n$ will be denoted by

$$\binom{a_1, \ldots, a_n}{b_1, \ldots, b_n} = \begin{vmatrix} \binom{a_1}{b_1} & \cdots & \binom{a_1}{b_n} \\ \vdots & \ddots & \vdots \\ \binom{a_n}{b_1} & \cdots & \binom{a_n}{b_n} \end{vmatrix}.$$

We recall the following two lemmas from [15].

Lemma 10 ([15, Lemma 8]). *If $b_1 \neq 0$, then*

$$\binom{a_1,\ldots,a_k}{b_1,\ldots,b_k} = \frac{a_1\cdots a_k}{b_1\cdots b_k}\binom{a_1-1,\ldots,a_k-1}{b_1-1,\ldots,b_k-1}.$$

Lemma 11 ([15, Lemma 9]). *The following holds*

$$\binom{a,a+1,\ldots,a+k-1}{0,b_2,\ldots,b_k} = \binom{a,a+1,\ldots,a+k-2}{b_2-1,b_3-1,\ldots,b_k-1}.$$

We can now prove the following identity.

Lemma 12. *Let S be the $k\times(k+1)$ submatrix corresponding to rows $a+1,a+2,\ldots,a+k$ and columns $0,1,\ldots,k$. Then, for $0\leq l\leq k$, the minors of this submatrix are equal to*

$$\binom{a+1,a+2,\ldots,a+k}{0,1,\ldots\ell-1,\ell+1,\ldots,k} = \binom{a+k-\ell}{k-\ell}.$$

Proof. Apply ℓ times Lemma 11 to the minor

$$\binom{a+1,a+2,\ldots,a+k}{0,1,\ldots\ell-1,\ell+1,\ldots,k}.$$

The result is the minor

$$\binom{a+1,a+2,\ldots,a+k-\ell}{1,\ldots,k-\ell}.$$

Next, apply Lemma 10 to obtain the minor

$$\frac{(a+1)\cdots(a+k-\ell)}{1\cdots(k-\ell)}\binom{a,\ldots,a-1+k-\ell}{0,1,\ldots,k-\ell-1} = \binom{a+k-\ell}{k-\ell}\binom{a,\ldots,a-1+k-\ell}{0,1,\ldots,k-\ell-1}.$$

Finally, apply Lemma 11 another $k-\ell-2$ times until the minor is reduced to a single entry

$$\binom{a+k-\ell}{k-\ell}\binom{a}{0} = \binom{a+k-\ell}{k-\ell}.$$ □

Lemma 13. *Let M be the $m\times m$ matrix with entries in $\mathbb{K}[x,y,t]$ defined by $M_{i,j}=\sum_{k=0}^{m}\binom{x-i}{k}\binom{y-j}{k}t^k$. Then,*

$$\frac{\det(M)}{t^{\binom{m}{2}}} = \sum_{k=0}^{m}\binom{x-m-1+k}{k}\binom{y-m-1+k}{k}t^k.$$

Proof. Let A be the $m\times(m+1)$ matrix with entries $a_{ik}=\binom{x-i}{k-1}$. Let B be the $(m+1)\times m$ matrix with entries $B_{kj}=\binom{y-j}{k-1}t^{k-1}$. Observe that $M=AB$.

We shall write $A^{[\ell]}$ to denote the matrix A with the ℓth row removed. Similarly, $B^{[\ell]}$ denotes the matrix B with the ℓth row removed. By the Cauchy-Binet formula

$$\det(M) = \sum_{\ell=1}^{m+1} \det(A^{[\ell]}) \det(B^{[\ell]}).$$

We begin with the matrix A. Notice that by making $\frac{1}{2}m(m+1)$ column transpositions, one can rearrange A so that it is a submatrix of the Pascal matrix $\mathcal{A}$. Specifically, one can rearrange the columns of A so that it has rows $x-m, \ldots, x-1$ and columns $0, \ldots, m$ of $\mathcal{A}$. Then, by Lemma 12, the determinant of the minors of A equals, up to the sign difference from the transpositions,

$$\det(A^{[\ell]}) = \pm \binom{x-\ell}{m-\ell+1}.$$

Now, let C be the matrix B with $t = 1$. Then, note that

$$\det(B^{[\ell]}) = \det(C^{[\ell]}) t^{\binom{m}{2}+m-\ell+1}.$$

In the same way as for the matrix A, by taking the transpose of C and making $\frac{1}{2}m(m+1)$ column transpositions, one can rearrange C so that is has the form of a submatrix of $\mathcal{A}$. We find that

$$\det(C^{[\ell]}) = \pm \binom{y-\ell}{m-\ell+1}, \quad \text{and thus } \det(B^{[\ell]}) = \pm \binom{y-\ell}{m-\ell+1} t^{\binom{m}{2}+m-\ell+1}.$$

Returning to the Cauchy-Binet formula,

$$\det(M) = \sum_{\ell=1}^{m+1} \binom{x-\ell}{m-\ell+1} \binom{y-\ell}{m-\ell+1} t^{\binom{m}{2}+m-\ell+1}.$$

By a change of coordinates, substituting $k = m - \ell + 1$, we arrive at

$$\det(M) = \sum_{k=0}^{m} \binom{x-m-1+k}{k} \binom{y-m-1+k}{k} t^{\binom{m}{2}+k}. \qquad \square$$

Corollary 14. *The Hilbert series H from Proposition 5 can be expressed as*

$$H = \left(\sum_{k=0}^{p-1} \binom{n-p-1+k}{k} t^{k(d-1)} \right) \frac{(1-t^d)^p (1-t^{d-1})^{n-p}}{(1-t)^n}.$$

Proof. By Proposition 5, we have that

$$H = \frac{\det(P(t^{d-1}))}{t^{(d-1)\binom{p-1}{2}}} \frac{(1-t^d)^p (1-t^{d-1})^{n-p}}{(1-t)^n}$$

where $P(t)$ is the $(p-1)\times(p-1)$ matrix whose (i,j)th entry is $\sum_k \binom{p-i}{k}\binom{n-1-j}{k} t^k$. Thus, as the special case of Lemma 13 with $m = p-1, x = p$ and $y = n-1$,

$$\frac{\det(P(t))}{t^{\binom{p-1}{2}}} = \sum_{k=0}^{p-1} \binom{n-p-1+k}{k} t^k. \qquad \square$$

3.2. Unimodality

The Hilbert series of the systems we study are highly structured. In particular, it was shown in [21, Proposition 2.2] that the Hilbert series of generic complete intersections are symmetric and so-called unimodal polynomials. As we transition to more general determinantal ideals, we may lose some of this structure for certain choices of parameters. However, we show in this section that our series are always unimodal. This property will then be exploited in the remaining two parts of Section 3. We begin with the definition of unimodality.

Definition 15. *A polynomial $\sum_{k=0}^{n} a_k t^k$ with non-negative coefficients is unimodal if there exists an integer N such that*

$$a_{k+1} \geq a_k \quad \text{for } k \leq N, \quad \text{and} \quad a_{k+1} \leq a_k \quad \text{for } k \geq N.$$

Unimodality is not necessarily preserved by multiplication. For example, the polynomial $f = 3+t+t^2$ is unimodal, while its square $f^2 = 9+6t+7t^2+2t^3+t^4$ is not.

Definition 16. *A polynomial f with non-negative coefficients is strongly unimodal if, for all unimodal polynomials g, the product fg is unimodal.*

Note that a strongly unimodal polynomial is also unimodal. A classical example of a strongly unimodal polynomial is as follows.

Lemma 17. *For any $d \in \mathbb{N}$, the polynomial $f = 1 + t + \cdots + t^d$ is strongly unimodal.*

Proof. Let $g = \sum_{k=0}^{n} a_k t^k$ be a unimodal polynomial with integer N such that

$$a_{k+1} \geq a_k \text{ for all } k \leq N,$$
$$a_{k+1} \leq a_k \text{ for all } k \geq N.$$

For ease of notation, let $a_k = 0$ if $k < 0$ or $k > n$. Let $fg = \sum_{k=0}^{n+d} b_k t^k$ so that $b_k = a_{k-d} + \cdots + a_k$. Suppose that there does not exist an integer σ such that $b_{\sigma+1} < b_\sigma$, then fg is trivially unimodal. On the other hand, suppose such an index exists and let M be the least integer such that $b_{M+1} < b_M$. Clearly, $M \geq N$, since the coefficients of g are non-decreasing up to index N. Assume that for some k, for all ℓ such that $M \leq \ell < k$ we have that $b_{\ell+1} \leq b_\ell$. Then, $a_k - a_{k-d-1} < 0$. Since $k+1 \geq M+1 > N$, by the unimodality of g, $a_{k+1} \leq a_k$. Similarly, if $k - d \leq N$ we have $a_{k-d-1} \leq a_{k-d}$. Hence, by the inductive assumption, $b_{k+1} - b_k = a_{k+1} - a_{k-d} < a_k - a_{k-d-1} < 0$. Alternatively, if $k - d > N$, then by unimodality of g we have $a_{k+1} - a_{k-d} < 0$. Hence, by induction, we have that $b_{k+1} < b_k$ for all $k \leq N + d$. Thus, fg is a unimodal polynomial and we conclude that f is a strongly unimodal polynomial. □

Unlike unimodality, strong unimodality is preserved by multiplication.

Lemma 18. *Let f, g be strongly unimodal polynomials. Then, fg is a strongly unimodal polynomial.*

Proof. Let h be a unimodal polynomial. Then, since g is strongly unimodal, gh is a unimodal polynomial. Hence, since f is strongly unimodal, fgh is unimodal polynomial and so fg is strongly unimodal. □

We shall prove that the Hilbert series of a generic determinantal ideal is unimodal by showing that it is the product of a strongly unimodal polynomial and a unimodal polynomial.

Lemma 19. *Let H be the Hilbert series from Proposition 5, with parameters $n, p, d \in \mathbb{N}$ where $n > p$. Then, H is a unimodal polynomial.*

Proof. Firstly, by Corollary 14,

$$H = \left(\sum_{k=0}^{p-1} \binom{n-p-1+k}{k} t^{k(d-1)} \right) \frac{(1-t^d)^p (1-t^{d-1})^{n-p}}{(1-t)^n}.$$

Our strategy is to show that we can write this polynomial as the product of a unimodal polynomial and a strongly unimodal polynomial. By the definition of strongly unimodal, the polynomial H would then be unimodal.

For $d > 2$, the binomial sum factor

$$\sum_{k=0}^{p-1} \binom{n-p-1+k}{k} t^{k(d-1)}$$

is not unimodal. However, since we have $n \geq p-1$, the remaining factor of H always has the following polynomial as a factor:

$$\frac{1-t^{d-1}}{1-t} = 1 + t + \cdots + t^{d-2}.$$

Therefore, we can always multiply this factor into the first binomial sum factor to get:

$$\sum_{k=0}^{p-1} \binom{n-p-1+k}{k} t^{k(d-1)} (1+t+\cdots+t^{d-2}) = \sum_{k=0}^{p-1} \sum_{i=0}^{d-2} \binom{n-p-1+k}{k} t^{k(d-1)+i},$$

which is now a unimodal polynomial as its coefficients are non-decreasing with no internal zeroes.

Consider the remaining quotient

$$\frac{(1-t^d)^p (1-t^{d-1})^{n-p-1}}{(1-t)^{n-1}}.$$

This polynomial is the product of $n-1$ polynomials of the form $1+t+\cdots+t^m$ for some $m \in \mathbb{N}$. By Lemma 17, each of these polynomials is strongly unimodal. Thus, by Lemma 18, the remaining quotient,

$$\frac{(1-t^d)^p (1-t^{d-1})^{n-p-1}}{(1-t)^{n-1}},$$

is strongly unimodal. Therefore, since H is the product of a strongly unimodal polynomial and a unimodal polynomial, H is unimodal. □

Remark 20. *In the context of this paper, by the unimodality of the Hilbert series H, Definition 6 is equivalent to the definition given in [21, Section 1].*

3.3. Staircase structure

In this section, we prove a structure theorem on the DRL staircase for generic determinantal ideals. Let $(g_1, \ldots, g_k)$ be a reduced and minimal Gröbner basis of I with respect to a DRL ordering with x_n as the least variable. For $1 \leq i \leq k$, let $r_i \in \mathscr{M}$ be the leading monomial of g_i, where $\mathscr{M}$ is set of monomials of $\mathbb{K}[x_1, \ldots, x_n]$. Then, we shall denote the DRL staircase by

$$E = \bigcap_{i=1}^{k} \left\{ r \in \mathscr{M} \mid r_i \nmid r \right\}.$$

The elements of the staircase give a natural basis for the quotient algebra $\mathbb{K}[x_1, \ldots, x_n]/I$. Then, for each $b \in E$, the columns of the matrix M_n are the normal forms of $x_n b$ with respect to the DRL Gröbner basis expressed in terms of the basis E. Then, for each $b \in E$, the construction of the columns of M_n corresponding to $x_n b$ falls into exactly one of following three cases:

1. $x_n b \in E$: Then, the corresponding column is sparse, consisting of all zeroes except one entry with a value of 1 in the row corresponding to $x_n b$.

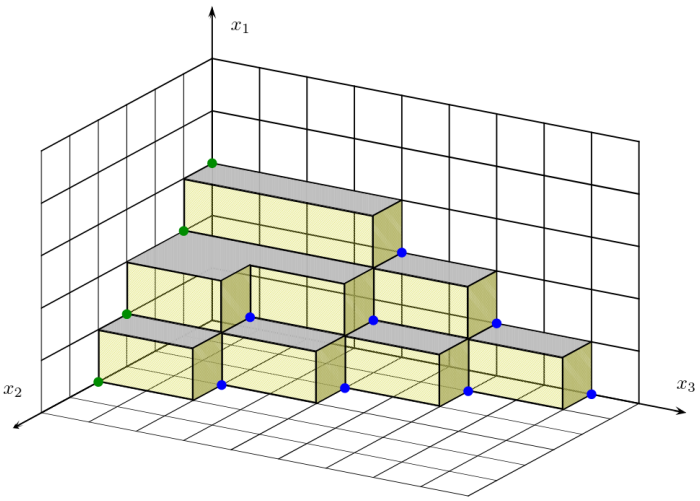
2. $x_n b$ is a leading term of the reduced DRL Gröbner basis: Then, the normal form is obtained from the polynomial g in the Gröbner basis whose leading term is $x_n b$.

3. Otherwise, the normal form must be computed.

In the first case, the corresponding column is trivial. In the latter two cases, the corresponding columns are non-trivial. Usually, and in the case we consider with generic polynomials, these non-trivial columns are dense. Moreover, constructing columns that fall into the first two cases do not require any arithmetic operations.

We establish in this subsection that, for generic determinantal ideals, only the first two cases occur. This implies that the number of non-trivial columns of the matrix M_n is equal to the number of leading monomials of elements of the reduced DRL Gröbner basis that have positive degree in x_n.

To prove this result, we consider the Hilbert series H and used its simplified form from Corollary 14 as well as the unimodal property of Lemma 19. Another object we shall use repeatedly is the DRL staircase of I. This is the set of monomials that are not elements of the initial ideal of I with respect to the DRL ordering. We illustrate an example here in the case $n = d = 3$, $p = 2$.



Here, the cubes represent elements of the staircase and the dots are the leading monomials of the reduced DRL Gröbner basis. We can see that in this instance, the number of non-trivial columns will be equal to the number of blue dots, the number of leading monomials of elements of the reduced Gröbner basis that have positive degree in x_n.

We recall the definition of HQ_e, the Hilbert series of $(\mathbb{K}[x_1, \ldots, x_n]/I)/\langle x_n^e \rangle$, for $e \geq 1$. For the remainder of the paper, we will assume that Fröberg's conjecture is true and so the conclusion of Lemma 7 holds. In particular, this implies that the degree of the polynomial HQ_1 is equal to the degree of the term of largest coefficient of H, or the first time this happens if there are multiple terms with the largest coefficient. We shall refer to this degree by Σ. Moreover, for ease of notation, we shall denote

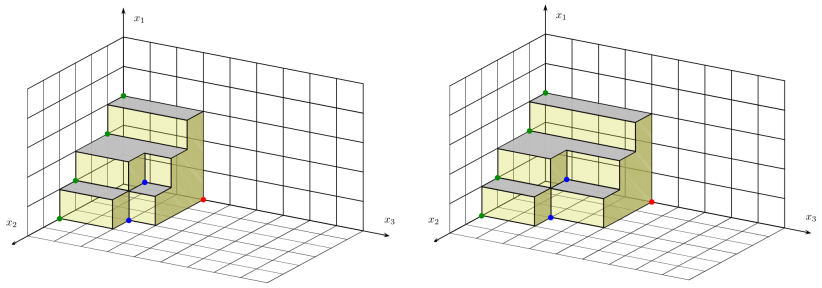
$$\Delta = (p-1)(d-1) + p(d-1) + (n-p)(d-2),$$

so that Δ equals the degree of H.

Note that the DRL ordering with x_n as the least variable is compatible with these quotients. We recall the following property that can be easily verified:

Lemma 21 ([21, Lemma 1.9])**.** *Let $I \in \mathbb{K}[x_1, \ldots, x_n]$ be a polynomial ideal and let $\{g_1, \ldots, g_k\}$ be a Gröbner basis of I with respect to a DRL ordering with x_n as the least variable. Then, $\{g_1, \ldots, g_k, x_n^e\}$ is a Gröbner basis of $I + \langle x_n^e \rangle$. Moreover, if $\{f_1, \ldots, f_k\}$ is additionally a reduced Gröbner basis, then removing from $\{g_1, \ldots, g_k, x_n^e\}$ all g_i such that x_n^e divides the leading term of g_i gives a reduced Gröbner basis of $I + \langle x_n^e \rangle$.*

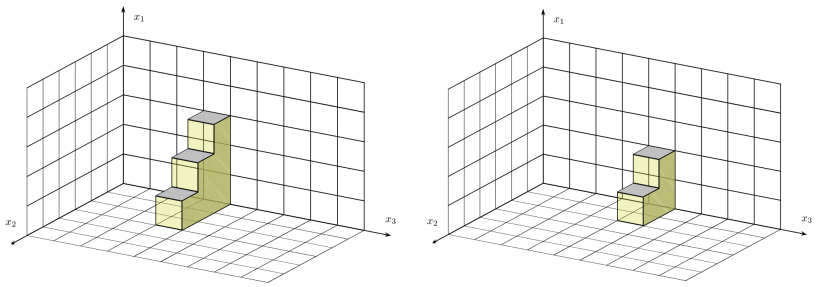
This compatibility can be easily seen from the corresponding staircases:



Here we see the quotients by x_3^3 and x_3^4. Adding these monomials to the Gröbner basis is indicated by the red dots. As in [21], for $e \geq 1$ we consider the eth section

$$H_e = \frac{HQ_{e+1} - HQ_e}{t^e}.$$

Effectively, we consider the Hilbert series of a cross section of the DRL staircase.



Here we illustrate t^3H_3 and t^4H_4. From this example, it is clear that by scaling these polynomials, by dividing by t^3 and t^4 respectively, the difference of these polynomials tells us about how the stairs change as we increase the degree of x_n. To study these sections, we first prove a result restricting the degree they can have.

Lemma 22. *For all $e \geq 1$, $\deg HQ_{e+1} - \deg HQ_e \in \{0, 1\}$.*

Proof. Let $H = \sum_{k=0}^{\Delta} a_k$. For a given e, let σ be the degree of HQ_e. By Lemma 19, H is unimodal. Therefore, by Lemma 7, we have that:

$$HQ_e = a_0 + \cdots + a_{e-1}t^{e-1} + (a_e - a_0)t^e + \cdots + (a_\sigma - a_{\sigma-e})t^\sigma$$

Moreover, since H is unimodal, the degree of HQ_{e+1} is at least the degree of HQ_e and $\sigma \geq \Sigma$, where Σ is the degree of HQ_1. For the purpose of contradiction, suppose that the degree of HQ_{e+1} is at least $\sigma + 2$. Then, since σ is the degree of HQ_e, we have

$$HQ_e = \left[a_0 + \cdots + (a_\sigma - a_{\sigma-e})t^\sigma + (a_{\sigma+1} - a_{\sigma+1-e})t^{\sigma+1}\right]_+$$

and

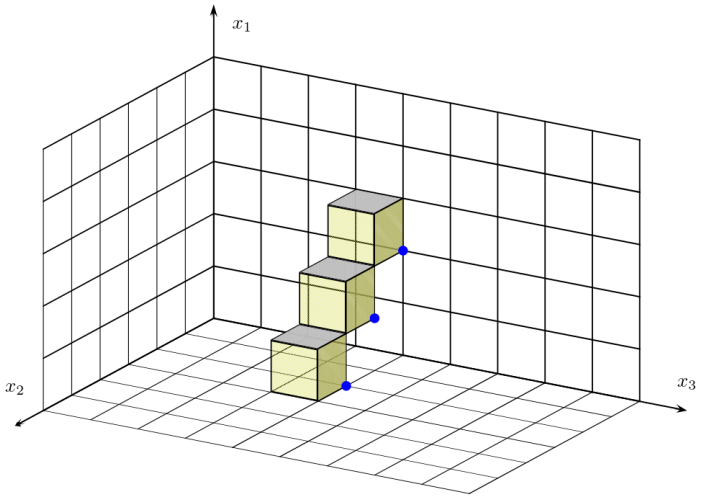
$$HQ_{e+1} = a_0 + \cdots + (a_{\sigma+2} - a_{\sigma+1-e})t^{\sigma+2}.$$

This implies that

$$a_{\sigma+1} \leq a_{\sigma+1-e},$$
$$a_{\sigma+2} > a_{\sigma+1-e}.$$

Therefore, $a_{\sigma+1} < a_{\sigma+2}$. This is a contradiction, as a_Σ is the largest coefficient of H and so $a_{\sigma+1} \geq a_{\sigma+2}$ by unimodality. Therefore, the degree of HQ_{e+1} is either σ or $\sigma + 1$. □

With Lemma 22, we greatly restrict the possible degrees these sections can have. This allows us to prove a result on the differences of these sections.



We see here that the difference of sections tells us when there are drops in the staircase as we increase the degree of x_n. Note that the three monomials in the illustration of the difference $t^3(H_4 - H_3)$ correspond to the three leading monomials in the reduced Gröbner basis that have degree 4 in x_3. With the following lemmas, we show that this correspondence always occurs.

Lemma 23. *For all $e \geq 1$, the difference of sections $H_{e+1} - H_e$ is either 0 or a monomial.*

Proof. For a fixed e we need to consider the three quotients HQ_e, HQ_{e+1} and HQ_{e+2}. Let $\sigma \geq \Sigma$ be the degree of HQ_e. Then, by Lemma 22, the degree of HQ_{e+1} is either σ or $\sigma + 1$ and the degree of HQ_{e+2} is between σ and $\sigma + 2$. We consider the following four cases and show that the result holds in each:

- $\deg HQ_{e+1} - \deg HQ_e = 0$ and $\deg HQ_{e+2} - \deg HQ_{e+1} = 0$. Then, we have the quotients:

$$\begin{aligned}
HQ_e &= a_0 + \cdots + a_{e-1}t^{e-1} + (a_e - a_0)t^e + \cdots + (a_\sigma - a_{\sigma-e})t^\sigma, \\
HQ_{e+1} &= a_0 + \cdots + a_e t^e + (a_{e+1} - a_0)t^{e+1} + \cdots + (a_\sigma - a_{\sigma-e-1})t^\sigma, \\
HQ_{e+2} &= a_0 + \cdots + a_{e+1}t^{e+1} + (a_{e+2} - a_0)t^{e+2} + \cdots + (a_\sigma - a_{\sigma-e-2})t^\sigma.
\end{aligned}$$

This gives the sections:

$$\begin{aligned}
H_e &= a_0 + (a_1 - a_0)t + \cdots + (a_{\sigma-e-1} - a_{\sigma-e-2})t^{\sigma-e-1} \\
&\quad + (a_{\sigma-e} - a_{\sigma-e-1})t^{\sigma-e}, \\
H_{e+1} &= a_0 + (a_1 - a_0)t + \cdots + (a_{\sigma-e-1} - a_{\sigma-e-2})t^{\sigma-e-1}.
\end{aligned}$$

Therefore, the difference is:

$$H_{e+1} - H_e = (a_{\sigma-e-1} - a_{\sigma-e})t^{\sigma-e}.$$

- $\deg HQ_{e+1} - \deg HQ_e = 1$ and $\deg HQ_{e+2} - \deg HQ_{e+1} = 0$. Then, we have the quotients:

$$\begin{aligned}
HQ_e &= a_0 + \cdots + a_{e-1}t^{e-1} + (a_e - a_0)t^e + \cdots + (a_\sigma - a_{\sigma-e})t^\sigma, \\
HQ_{e+1} &= a_0 + \cdots + a_e t^e + (a_{e+1} - a_0)t^{e+1} + \cdots + (a_\sigma - a_{\sigma-e-1})t^\sigma \\
&\quad + (a_{\sigma+1} - a_{\sigma-e})t^{\sigma+1}, \\
HQ_{e+2} &= a_0 + \cdots + a_{e+1}t^{e+1} + (a_{e+2} - a_0)t^{e+2} + \cdots + (a_\sigma - a_{\sigma-e-2})t^\sigma \\
&\quad + (a_{\sigma+1} - a_{\sigma-e-1})t^{\sigma+1}.
\end{aligned}$$

This gives the sections:

$$\begin{aligned}
H_e &= a_0 + (a_1 - a_0)t + \cdots + (a_{\sigma-e} - a_{\sigma-e-1})t^{\sigma-e} \\
&\quad + (a_{\sigma+1} - a_{\sigma-e})t^{\sigma-e+1}, \\
H_{e+1} &= a_0 + (a_1 - a_0)t + \cdots + (a_{\sigma-e} - a_{\sigma-e-1})t^{\sigma-e}.
\end{aligned}$$

Therefore, the difference is:

$$H_{e+1} - H_e = (a_{\sigma-e} - a_{\sigma+1})t^{\sigma-e+1}.$$

- $\deg HQ_{e+1} - \deg HQ_e = 0$ and $\deg HQ_{e+2} - \deg HQ_{e+1} = 1$. Then, we have the quotients:

$$\begin{aligned}
HQ_e &= a_0 + \cdots + a_{e-1}t^{e-1} + (a_e - a_0)t^e + \cdots + (a_\sigma - a_{\sigma-e})t^\sigma, \\
HQ_{e+1} &= a_0 + \cdots + a_e t^e + (a_{e+1} - a_0)t^{e+1} + \cdots + (a_\sigma - a_{\sigma-e-1})t^\sigma, \\
HQ_{e+2} &= a_0 + \cdots + a_{e+1}t^{e+1} + (a_{e+2} - a_0)t^{e+2} + \cdots + (a_\sigma - a_{\sigma-e-2})t^\sigma \\
&\quad + (a_{\sigma+1} - a_{\sigma-e-1})t^{\sigma+1}.
\end{aligned}$$

This gives the sections:

$$\begin{aligned} H_e &= a_0 + (a_1 - a_0)t + \cdots + (a_{\sigma-e-1} - a_{\sigma-e-2})t^{\sigma-e-1} \\ &\quad + (a_{\sigma-e} - a_{\sigma-e-1})t^{\sigma-e}, \\ H_{e+1} &= a_0 + (a_1 - a_0)t + \cdots + (a_{\sigma-e-1} - a_{\sigma-e-2})t^{\sigma-e-1} \\ &\quad + (a_{\sigma+1} - a_{\sigma-e-1})t^{\sigma-e}. \end{aligned}$$

Therefore, the difference is:

$$H_{e+1} - H_e = (a_{\sigma+1} - a_{\sigma-e})t^{\sigma-e}.$$

- $\deg HQ_{e+1} - \deg HQ_e = 1$ and $\deg HQ_{e+2} - \deg HQ_{e+1} = 1$. Then, we have the quotients:

$$\begin{aligned} HQ_e &= a_0 + \cdots + a_{e-1}t^{e-1} + (a_e - a_0)t^e + \cdots + (a_\sigma - a_{\sigma-e})t^\sigma, \\ HQ_{e+1} &= a_0 + \cdots + a_e t^e + (a_{e+1} - a_0)t^{e+1} + \cdots + (a_\sigma - a_{\sigma-e-1})t^\sigma \\ &\quad + (a_{\sigma+1} - a_{\sigma-e})t^{\sigma+1}, \\ HQ_{e+2} &= a_0 + \cdots + a_{e+1}t^{e+1} + (a_{e+2} - a_0)t^{e+2} + \ldots \\ &\quad + (a_{\sigma+1} - a_{\sigma-e-1})t^{\sigma+1} + (a_{\sigma+2} - a_{\sigma-e})t^{\sigma+2}. \end{aligned}$$

This gives the sections:

$$\begin{aligned} H_e &= a_0 + (a_1 - a_0)t + \cdots + (a_{\sigma-e} - a_{\sigma-e-1})t^{\sigma-e} \\ &\quad + (a_{\sigma+1} - a_{\sigma-e})t^{\sigma-e+1}, \\ H_{e+1} &= a_0 + (a_1 - a_0)t + \cdots + (a_{\sigma-e} - a_{\sigma-e-1})t^{\sigma-e}, \\ &\quad + (a_{\sigma+2} - a_{\sigma-e})t^{\sigma-e+1}. \end{aligned}$$

Therefore, the difference is:

$$H_{e+1} - H_e = (a_{\sigma+2} - a_{\sigma+1})t^{\sigma-e+1}.$$ □

We now can translate these results to describe the DRL staircase. For all $e \geq 0$, the sections of the staircase will be denoted by

$$E^e = \{x_1^{i_1} \cdots x_{n-1}^{i_{n-1}} \mid x_1^{i_1} \cdots x_{n-1}^{i_{n-1}} x_n^e \in E\}.$$

We can now state and prove our structure result.

Proposition 24. *For all $b \in E$, either $x_n b \in E$ or $x_n b$ is a leading monomial in the reduced DRL Gröbner basis of I.*

Proof. Let $b \in E$ be a monomial of degree δ. Assume that $x_n b \notin E$. Let $b' \in E^e$ so that $b = b' x_n^e$. The coefficient of the δth term of a Hilbert series is the number of monomials of degree δ under the staircase. Thus, b is accounted for in the δth term of HQ_{e+1}. Furthermore, since $x_n^e \mid b$, b is not accounted for in HQ_e

and so in the section H_e, b' is accounted for $(\delta - e)$th coefficient. However, since $x_n^{e+1} \nmid b$, b is still accounted for in the δth term of HQ_{e+2}. Therefore, these parts cancel in the section H_{e+1} and so in the difference $H_{e+1} - H_e$, b' is accounted for in the $(\delta - e)$th term. The absolute value of the sum of the coefficients of this difference gives the number of monomials that are in E^e that are not in E^{e+1}. By Lemma 23, $H_{e+1} - H_e$ is a monomial. Therefore, all monomials that are in E^e and are not in E^{e+1} are of the same degree and so are independent. The monomial b' is accounted for in the coefficient of $H_{e+1} - H_e$ and so $x_n b$ is a leading monomial in the reduced DRL Gröbner basis of I. □

Theorem 1. *Let I be a generic determinantal ideal so that the conditions of Definition 8 hold. Assume that a reduced and minimal Gröbner basis of I with respect to a DRL ordering is known. Then, the multiplication matrix M_n can be constructed without performing any arithmetic operations.*

Proof. Each column of the matrix M_n is the normal form of a monomial $x_n b$ such that $b \in E$. By Lemma 24, either $x_n b \in E$, in which case the column is all zeroes except one entry with a value of 1 in the row corresponding to $x_n b$, or $x_n b$ is a leading term in the reduced DRL Gröbner basis of I. In the latter case, the normal form is obtained from the DRL Gröbner basis without cost. Therefore, the multiplication matrix M_n can be constructed for free. □

With this structure theorem in tow, we aim to count this number of non-trivial columns. The following lemma gives a useful classification of this number.

Lemma 25. *If Fröberg's conjecture is true, then the number of non-trivial columns of M_n is equal to the largest coefficient of H.*

Proof. By Theorem 1, we can count the number of non-trivial columns of M_n by counting the number of leading terms of the DRL Gröbner basis. Lemma 24 implies that this number is equal to the number of monomials $b \in E$ such that $x_n b \notin E$. Note that this number is also equal to the number of monomials in the section E^0, which forms a monomial basis of the quotient algebra $(\mathbb{K}[x_1, \ldots, x_n]/I)/\langle x_n \rangle$. The Hilbert series of this algebra is HQ_1. Thus, the number of non-trivial columns of M_n is equal to the sum of the coefficients of HQ_1. Using Fröberg's conjecture, we can express HQ_1 in terms of the coefficients of H:

$$HQ_1 = a_0 + (a_1 - a_0)t + \cdots + (a_\Sigma - a_{\Sigma-1})t^\Sigma.$$

Therefore, the sum of the coefficients of HQ_1, and so the number of non-trivial columns of M_n, equals a_Σ, the largest coefficient of H. □

3.4. Asymptotics

By [11], the complexity of the Sparse-FGLM algorithm depends linearly on the number of non-trivial columns of the multiplication matrix M_n, denoted m. In the previous section, we proved Lemma 25, meaning that we can find this

number by finding the largest coefficient of the Hilbert series H from Proposition 5. We consider two cases. Firstly, we suppose that $d = 2$. This assumption leads to a simplification of the Hilbert series so that, by Corollary 14 and a trivial identity, it can be written as

$$H = \left(\sum_{k=0}^{p-1} \binom{n-p-1+k}{k} t^k \right) (1+t)^p.$$

On the other hand, for any $d \geq 2$, to find an asymptotic formula for the largest coefficient of H we will consider the central coefficients of polynomials of the form $(1 + t + \cdots + t^r)^s$ for some r, s. Therefore, we recall an abridged version of the following result from [27].

Proposition 26 ([27, Theorem 2])**.** *Let $r, s \geq 1$ and choose $0 \leq k \leq s^{1/2}$. Then, the $(sr + k)$th coefficient of the polynomial $(1 + t + \cdots + t^r)^s$ is asymptotically equal to*

$$\frac{1}{\sqrt{s\pi}} \sqrt{\frac{6}{r^2-1}} r^s \left(1 + O\left(\frac{k}{s} \right) \right).$$

We can now restate and prove our main result.

Theorem 2. *Let I be a generic determinantal ideal so that the conditions of Definition 8 hold, and let M_n be the multiplication matrix associated to multiplication by x_n. Denote by m the number of non-trivial columns of M_n. Then, for $d = 2$ and $n \gg p$, the number m is equal to:*

$$m = \sum_{k=0}^{p-1} \binom{n-p-1+k}{k} \binom{p}{\lfloor 3p/2 \rfloor - 1 - j}. \tag{1}$$

Moreover, for $d \geq 3$ and $n \to \infty$, the number m is asymptotically equal to

$$m \approx \frac{1}{\sqrt{(n-p)\pi}} \sqrt{\frac{6}{(d-1)^2-1}} d^p (d-1)^{n-p} \binom{n-2}{p-1}. \tag{2}$$

Proof. By Lemma 25, m is equal to the largest coefficient of the Hilbert series H. First, assume that $d = 2$. Then, the Hilbert series can be written as

$$H = \left(\sum_{k=0}^{p-1} \binom{n-p-1+k}{k} t^k \right) (1+t)^p = \sum_{k=0}^{p(p-1)} h_k t^k.$$

In this setting, we consider the binomial coefficients:

$$(1+t)^p = \sum_{k=0}^{p} \binom{p}{k} t^k = \sum_{k=0}^{p} a_k t^k.$$

We shall prove our first result by finding the degree of the term of H with the largest coefficient. The number m can then be found by a convolution formula.

Firstly, note that $(1+t)^p$ is a symmetric unimodal polynomial. Therefore, its largest coefficient is at the term of degree $\lfloor \frac{p}{2} \rfloor$. Since this polynomial is unimodal, we have that

$$h_{\lfloor \frac{3p}{2} \rfloor} = \sum_{k=0}^{p-1} \binom{n-2-k}{p-1-k} a_{\lfloor \frac{p}{2} \rfloor + 1 + k} \leq \sum_{k=0}^{p-1} \binom{n-2-k}{p-1-k} a_{\lfloor \frac{p}{2} \rfloor + k} = h_{\lfloor \frac{3p}{2} \rfloor - 1}.$$

By Lemma 19, H is unimodal and so the largest coefficient of H is at least $h_{\lfloor \frac{3p}{2} \rfloor - 1}$. We now show that the previous coefficient of H is also no more than $h_{\lfloor \frac{3p}{2} \rfloor - 1}$. By unimodality, this shows that $h_{\lfloor \frac{3p}{2} \rfloor - 1}$ is the largest coefficient. We have that:

$$h_{\lfloor \frac{3p}{2} \rfloor - 1} = \sum_{k=0}^{p-1} \binom{n-p-1+k}{k} \binom{p}{\lfloor \frac{3p}{2} \rfloor - 1 - k}$$

and

$$h_{\lfloor \frac{3p}{2} \rfloor - 2} = \sum_{k=0}^{p-1} \binom{n-p-1+k}{k} \binom{p}{\lfloor \frac{3p}{2} \rfloor - 2 - k}.$$

As $n \to \infty$ we can write this as:

$$h_{\lfloor \frac{3p}{2} \rfloor - 1} = \binom{n-2}{p-1} \binom{p}{\lfloor \frac{p}{2} \rfloor} + O(n^{p-2})$$

and

$$h_{\lfloor \frac{3p}{2} \rfloor - 2} = \binom{n-2}{p-1} \binom{p}{\lfloor \frac{p}{2} \rfloor - 1} + O(n^{p-2}).$$

Therefore,

$$h_{\lfloor \frac{3p}{2} \rfloor - 1} - h_{\lfloor \frac{3p}{2} \rfloor - 2} = \binom{n-2}{p-1} \left(\binom{p}{\lfloor \frac{p}{2} \rfloor} - \binom{p}{\lfloor \frac{p}{2} \rfloor - 1} \right) + O(n^{p-2})$$

If $p = 1$, then $H = 1 + t$, and so the largest coefficient is indeed $h_0 = 1$. Otherwise, $\binom{p}{\lfloor \frac{p}{2} \rfloor} > \binom{p}{\lfloor \frac{p}{2} \rfloor - 1}$ and so we have that this difference tends to positive infinity as $n \to \infty$.

Therefore, for sufficiently large n, the largest coefficient is $h_{\lfloor \frac{3p}{2} \rfloor - 1}$.

Suppose now that $d > 2$. We return to the Hilbert series form given in Corollary 14 along with a trivial identity:

$$H = \left(\sum_{k=0}^{p-1} \binom{n-p-1+k}{k} t^{k(d-1)} \right) (1 + t + \cdots + t^{d-1})^p (1 + t + \cdots + t^{d-2})^{n-p}.$$

Firstly, consider the binomial sum factor. Note that as $n \to \infty$, the dominant term is the term of highest degree. Specifically, we may write

$$\sum_{k=0}^{p-1} \binom{n-p-1+k}{k} t^{k(d-1)} = \binom{n-2}{p-1} t^{(p-1)(d-1)} + O(n^{p-2} t^{(p-2)(d-1)}).$$

Therefore, since we only consider the largest coefficient of H as $n \to \infty$, we see that this is equal to the largest coefficient of the polynomial

$$h = \binom{n-2}{p-1}(1+t+\cdots+t^{d-1})^p(1+t+\cdots+t^{d-2})^{n-p}.$$

Thus, we can replace the binomial sum in the expression we consider with just a binomial coefficient.

For ease of notation, denote the other factors of h by $f_1 = (1+t+\cdots+t^{d-1})^p$ and $f_2 = (1+t+\cdots+t^{d-2})^{n-p}$. By [21, Proposition 2.2], these polynomials are symmetric. In particular, this means that we have $a_i = a_{(d-2)(n-p)-i}$, where

$$f_2 = \sum_{i=0}^{(d-2)(n-p)} a_i t^i.$$

Then, by Lemma 17 the polynomial f_2 is unimodal and so its largest coefficient is the central one. Therefore, by Proposition 26, the largest coefficient of f_2 is asymptotically equal to

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

Also by Proposition 26, since $p(d-1)+1$ is fixed as $n \to \infty$, the central $p(d-1)+1$ coefficients of f_2 tend to its largest coefficient. Note that for sufficiently large n, the largest coefficient of the product $f_1 f_2$ depends only on the central $p(d-1)+1$ coefficients of f_2, since f_1 does not depend on n. Therefore, since the sum of the coefficients of f_1 equals d^p, as $n \to \infty$, the largest coefficient of H is asymptotically equal to

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

We conclude that, for $d \geq 3$ and $n \to \infty$, the number of non-trivial columns of M_n is asymptotically equal to

$$m \approx \frac{1}{\sqrt{(n-p)\pi}}\sqrt{\frac{6}{(d-1)^2-1}}d^p(d-1)^{n-p}\binom{n-2}{p-1}. \qquad \square$$

Theorem 3. *Let I be a generic determinantal ideal so that the conditions of Definition 8 hold. Assume that a reduced and minimal DRL Gröbner basis of I is known. Then, for $d \geq 3$, the arithmetic complexity of computing a LEX Gröbner basis of I is upper bounded by*

$$O\left(\frac{d^{3p}(d-1)^{3(n-p)}}{\sqrt{(n-p)d\pi}}\binom{n-2}{p-1}\binom{n-1}{p-1}^2\right).$$

Hence, the complexity gain of Sparse-FGLM *over* FGLM *for generic determinantal systems is approximately*

$$O\left(\frac{m}{nD}\right) \approx O\left(\frac{\sqrt{n-p}}{n^2(d-1)}\right).$$

Proof. Firstly, by Definition 8, we may apply the shape position variant of the Sparse-FGLM algorithm. Assuming the multiplication matrix M_n is constructed, its complexity is $O(mD^2 + nD\log^2(D))$, where m is the number of non-trivial columns of the multiplication matrix M_n and D is the degree of the ideal I [11, Theorem 3.2]. By Theorem 1, the construction of the matrix M_n requires no arithmetic operations. Recall that the degree of the ideal I is equal to

$$D = d^p(d-1)^{n-p}\binom{n-1}{p-1}.$$

Then, for $d \geq 3$, by Theorem 2 we have that, as $n \to \infty$,

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

Since the dominant term of the complexity is $O(mD^2)$, substituting the formula for D and the asymptotics of m gives the complexity result.

The complexity gain is then:

$$O\left(\frac{mD^2}{nD^3}\right) = O\left(\frac{m}{nD}\right) \approx O\left(\frac{\sqrt{n-p}}{n^2(d-1)}\right). \qquad \square$$

4. Experiments

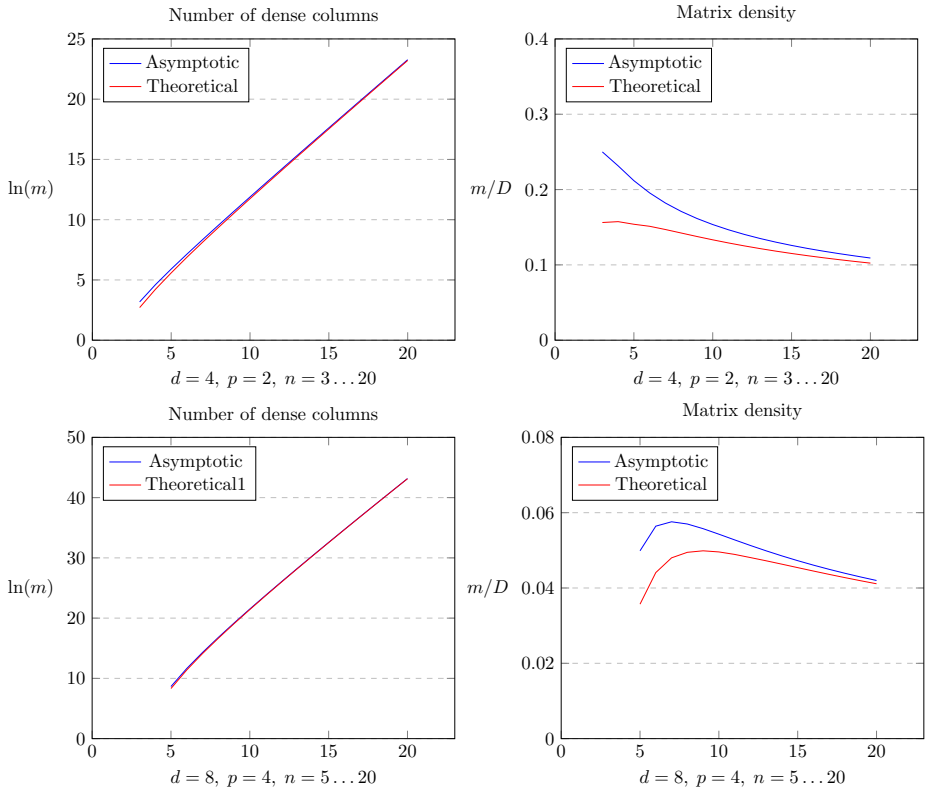
In this section, we test the practical accuracy of our formulae in Theorem 2, for the number of dense columns of the multiplication matrix M_n. For $d = 2$ we use our exact formula (1), while for $d \geq 3$ we use the asymptotic formula (2). The matrix density refers to the number of non-zero entries of M_n divided by its total number of entries. As seen in Theorem 3, the matrix density gives an idea of the complexity gain of using Sparse-FGLM over FGLM for the change of ordering.

Table 1 originates as a cropped version of a table given in [11, Table 2]. In this paper, the authors give the values in the actual column, obtained by computing the multiplication matrix and calculating exactly the number of non-zero entries, but the entries in the theoretical and asymptotic columns were blank. Now, with Theorem 2 we can complete this table, and we put the new entries in blue. The entries of the theoretical and asymptotic columns are the values of m/D, approximately the density of non-zero entries, for the varying parameters. In the theoretical column, the value of m is taken to be the largest coefficient of the Hilbert series. Then, for the asymptotic column we take m as in Theorem 2.

Parameters D	Degree Actual	Theoretical	Asymptotic	
$(2, 4, 9)$	896	30.17%	30.80%	30.80%
$(2, 4, 10)$	1344	31.13%	31.77%	31.77%
$(2, 4, 11)$	1920	31.86%	32.50%	32.50%
$(3, 3, 6)$	2160	17.52%	18.52%	27.73%
$(3, 3, 7)$	6480	17.39%	18.31%	26.62%
$(3, 3, 8)$	18144	17.63%	18.72%	25.50%
$(4, 2, 5)$	1728	14.46%	15.45%	21.24%
$(4, 2, 6)$	6480	14.11%	15.13%	19.56%
$(5, 2, 5)$	6400	11.00%	11.94%	15.47%
$(6, 2, 5)$	18000	8.80%	9.63%	12.22%

Table 1: Density of multiplication matrix M_n for generic critical point systems

Exceptionally, we consider the generic determinantal ideals defined by two quartics, and also the generic determinantal ideals defined by four polynomials of degree 8, with an increasing number of variables n.



Note that the number of dense columns increases exponentially with n in

about the same exponent for either the theoretical or the asymptotic in both examples. On the other hand, the matrix density can have different behaviours as the number of variables n increases for different degrees d and number of polynomials p. However, in both examples we see that the asymptotic approximation of the matrix density is rather inaccurate for small n. But, for moderate n, the approximation becomes good.

Acknowledgements. The authors are supported by the ANR grants ANR-18-CE33-0011 Sesame, ANR-19-CE40-0018 De Rerum Natura and ANR-19-CE48-0015 ECARP, the PGMO grant CAMiSAdo and the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement N. 813211 (POEMA).

References

[1] Aholt, C., Sturmfels, B., Thomas, R., 2013. A Hilbert Scheme in Computer Vision. Canadian Journal of Mathematics 65, 961–988. URL: http://dx.doi.org/10.4153/CJM-2012-023-2, doi:10.4153/cjm-2012-023-2.

[2] Bardet, M., Faugère, J.Ch., Salvy, B., 2004. On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations, in: Proceedings of the International Conference on Polynomial System Solving, pp. 71–74. URL: http://magali.bardet.free.fr/Publis/ltx43BF.pdf.

[3] Basu, S., Pollack, R., Roy, M.F., 2006. Algorithms in real algebraic geometry. volume 10 of *Algorithms and Computation in Mathematics*. Second ed., Springer-Verlag, Berlin. URL: https://link.springer.com/book/10.1007/3-540-33099-2.

[4] Becker, E. and Mora, T. and Marinari, M. G. and Traverso, C., 1994. The Shape of the Shape Lemma, in: Proceedings of the International Symposium on Symbolic and Algebraic Computation, Association for Computing Machinery, New York, NY, USA. p. 129–133. URL: https://doi.org/10.1145/190347.190382, doi:10.1145/190347.190382.

[5] Conca, A., Herzog, J., 1994. On the Hilbert function of determinantal rings and their canonical module. Proc. Amer. Math. Soc. 122, 677–681. URL: https://doi.org/10.2307/2160740, doi:10.2307/2160740.

[6] Cox, D.A., Little, J., O'Shea, D., 2007. Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, 3/e (Undergraduate Texts in Mathematics). Springer-Verlag, Berlin, Heidelberg.

[7] De Castro, Y., Gamboa, F., Henrion, D., Hess, R., Lasserre, J.B., 2019. Approximate optimal designs for multivariate polynomial regression. Ann. Statist. 47, 127–155. URL: https://doi.org/10.1214/18-AOS1683, doi:10.1214/18-AOS1683.

[8] Eisenbud, D., 2013. Commutative Algebra: with a view toward algebraic geometry. volume 150. Springer Science & Business Media. URL: https://www.springer.com/gp/book/9780387942681.

[9] Faugère, J.C., 2002. A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5), in: Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, ACM, New York. pp. 75–83. URL: https://doi.org/10.1145/780506.780516, doi:10.1145/780506.780516.

[10] Faugère, J.C., Gianni, P., Lazard, D., Mora, T., 1993. Efficient computation of zero-dimensional Gröbner bases by change of ordering. J. Symbolic Comput. 16, 329–344. URL: https://doi.org/10.1006/jsco.1993.1051, doi:10.1006/jsco.1993.1051.

[11] Faugère, J.C., Mou, C., 2017. Sparse FGLM algorithms. J. Symbolic Comput. 80, 538–569. URL: https://doi.org/10.1016/j.jsc.2016.07.025, doi:10.1016/j.jsc.2016.07.025.

[12] Faugère, J.C., Safey El Din, M., Spaenlehauer, P.J., 2012. Critical points and Gröbner bases: the unmixed case, in: ISSAC 2012—Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation, ACM, New York. pp. 162–169. URL: https://doi.org/10.1145/2442829.2442855, doi:10.1145/2442829.2442855.

[13] Faugère, J.C., Safey El Din, M., Spaenlehauer, P.J., 2013. On the complexity of the generalized MinRank problem. J. Symbolic Comput. 55, 30–58. URL: https://doi.org/10.1016/j.jsc.2013.03.004, doi:10.1016/j.jsc.2013.03.004.

[14] Fröberg, R., 1985. An inequality for Hilbert series of graded algebras. Math. Scand. 56, 117–144. URL: https://doi.org/10.7146/math.scand.a-12092, doi:10.7146/math.scand.a-12092.

[15] Gessel, I., Viennot, G., 1985. Binomial determinants, paths, and hook length formulae. Adv. in Math. 58, 300–321. URL: https://doi.org/10.1016/0001-8708(85)90121-5, doi:10.1016/0001-8708(85)90121-5.

[16] Gianni, P., Mora, T., 1989. Algebraic solution of systems of polynomial equations using Groebner bases, in: Applied algebra, algebraic algorithms and error-correcting codes (Menorca, 1987). Springer, Berlin. volume 356 of *Lecture Notes in Comput. Sci.*, pp. 247–257. URL: https://doi.org/10.1007/3-540-51082-6_83, doi:10.1007/3-540-51082-6_83.

[17] Henrion, D., Garulli, A. (Eds.), 2005. Positive polynomials in control. volume 312 of *Lecture Notes in Control and Information Sciences*. Springer-Verlag, Berlin. URL: https://doi.org/10.1007/b96977, doi:10.1007/b96977.

[18] Henrion, D., Šebek, M., Kučera, V., 2003. Positive polynomials and robust stabilization with fixed-order controllers. IEEE Trans. Automat. Control 48, 1178–1186. URL: https://doi.org/10.1109/TAC.2003.814103, doi:10.1109/TAC.2003.814103.

[19] Hong, H., Safey El Din, M., 2012. Variant quantifier elimination. J. Symbolic Comput. 47, 883–901. URL: https://doi.org/10.1016/j.jsc.2011.05.014, doi:10.1016/j.jsc.2011.05.014.

[20] Labahn, G., Safey El Din, M., Schost, É., Vu, T.X., 2021. Homotopy techniques for solving sparse column support determinantal polynomial systems. URL: https://doi.org/10.1016/j.jco.2021.101557, doi:10.1016/j.jco.2021.101557.

[21] Moreno-Socías, G., 2003. Degrevlex Gröbner bases of generic complete intersections. J. Pure Appl. Algebra 180, 263–283. URL: https://doi.org/10.1016/S0022-4049(02)00297-9, doi:10.1016/S0022-4049(02)00297-9.

[22] Nie, J., Ranestad, K., 2009. Algebraic degree of polynomial optimization. SIAM J. Optim. 20, 485–502. URL: https://doi.org/10.1137/080716670, doi:10.1137/080716670.

[23] Pardue, K., 2010. Generic sequences of polynomials. J. Algebra 324, 579–590. URL: https://doi.org/10.1016/j.jalgebra.2010.04.018, doi:10.1016/j.jalgebra.2010.04.018.

[24] Probst, T., Paudel, D.P., Chhatkuli, A., Van Gool, L., 2019. Convex Relaxations for Consensus and Non-Minimal Problems in 3D Vision, in: Proceedings of the IEEE International Conference on Computer Vision, pp. 10233–10242. URL: http://dx.doi.org/0.1109/ICCV.2019.01033, doi:0.1109/ICCV.2019.01033.

[25] Safey El Din, M., Schost, E., 2003. Polar varieties and computation of one point in each connected component of a smooth algebraic set, in: Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, ACM, New York. pp. 224–231. URL: https://doi.org/10.1145/860854.860901, doi:10.1145/860854.860901.

[26] Safey El Din, M. and Schost, É., 2017. A Nearly Optimal Algorithm for Deciding Connectivity Queries in Smooth and Bounded Real Algebraic Sets. J. ACM 63. URL: https://doi.org/10.1145/2996450, doi:10.1145/2996450.

[27] Star, Z., 1975. An asymptotic formula in the theory of compositions. Aequationes Math. 13, 279–284. URL: https://doi.org/10.1007/BF01836532, doi:10.1007/BF01836532.