On the Complexity of the Generalized MinRank Problem

Jean-Charles Faugère [a] Mohab Safey El Din [a]
Pierre-Jean Spaenlehauer [b,a,*]

[a] *Université Paris 6, INRIA Paris-Rocquencourt, PolSys Project, CNRS, UMR 7606 UFR Ingénierie 919, LIP6. Case 169. 4, Place Jussieu, F-75252 Paris, France.*

[b] *Computer Science Department, University of Western Ontario, London, ON, Canada.*

Abstract

We study the complexity of solving the *generalized MinRank problem*, i.e. computing the set of points where the evaluation of a polynomial matrix has rank at most r. A natural algebraic representation of this problem gives rise to a *determinantal ideal*: the ideal generated by all minors of size $r+1$ of the matrix. We give new complexity bounds for solving this problem using Gröbner bases algorithms under genericity assumptions on the input matrix. In particular, these complexity bounds allow us to identify families of generalized MinRank problems for which the arithmetic complexity of the solving process is polynomial in the number of solutions. We also provide an algorithm to compute a rational parametrization of the variety of a 0-dimensional and radical system of bi-degree $(D,1)$. We show that its complexity can be bounded by using the complexity bounds for the generalized MinRank problem.

Key words: MinRank, Gröbner basis, determinantal, bi-homogeneous, structured algebraic systems.

1. Introduction

We focus in this paper on the following problem:

Generalized MinRank Problem: given a field $\mathbb{K}$, a $n\times m$ matrix $\mathscr{M}$ whose entries are polynomials of degree D in $\mathbb{K}[x_1,\dots,x_k]$, and $r<\min(n,m)$ an integer, compute the set of points at which the evaluation of $\mathscr{M}$ has rank at most r.

This problem arises in many applications and this is what motivates our study. In cryptology, the security of several multivariate cryptosystems relies on the difficulty of solving the classical MinRank problem (i.e. when the entries of the matrix are linear (Bettale et al., 2012; Faugère

* Corresponding author.
Email addresses: `Jean-Charles.Faugere@inria.fr` (Jean-Charles Faugère), `Mohab.Safey@lip6.fr` (Mohab Safey El Din), `Pierre-Jean.Spaenlehauer@lip6.fr` (Pierre-Jean Spaenlehauer).

et al., 2008; Kipnis and Shamir, 1999)). In coding theory, rank-metric codes can be decoded by computing the set of points where a polynomial matrix has rank less than a given value (Faugère et al., 2008; Ourivski and Johansson, 2002). In non-linear computational geometry, many incidence problems from enumerative geometry can be expressed by constraints on the rank of a matrix whose entries are polynomials of degree frequently larger than 1 (see e.g. (Macdonald et al., 2001; Sottile, 2002, 2003)). Also, in real geometry and optimization (Bank et al., 2010; Greuet et al., 2011; Safey El Din and Schost, 2003) the critical points of a map are defined by the rank defect of its Jacobian matrix (whose entries have degrees larger than 1 most of the time in applications). Moreover, this problem is also underlying other problems from symbolic computation (for instance solving multi-homogeneous systems, see e.g. Faugère et al. (2011)).

The ubiquity of this problem makes the development of algorithms solving it and complexity estimates of first importance. When $\mathbb{K}$ is finite, the generalized MinRank problem is known to be NP-complete (Buss et al., 1999); thus one can consider this problem as a hard problem.

To study the Generalized MinRank problem, we consider the algebraic system of all the $(r+1)$-minors of the input matrix. Indeed, these minors simultaneously vanish on the locus of rank defect and hence give rise to a section of a *determinantal ideal*.

Several solving tools can be used to solve this algebraic system by taking profit of the underlying structure. For instance, the *geometric resolution* in Giusti et al. (2001) can use the fact that these systems can be evaluated efficiently. Also, recent works on homotopy methods (Verschelde, 1999) show that numerical algorithms can solve determinantal problems.

In this paper, we focus on Gröbner bases algorithms. A representation of the locus of rank defect is obtained by computing a lexicographical Gröbner basis by using the algorithms F_5 (Faugère, 2002) and FGLM (Faugère et al., 1993). Indeed, experiments suggest that these algorithms take profit of the determinantal structure. The aim of this work is to give an explanation of this behavior from the viewpoint of asymptotic complexity analysis.

Related works

An important related theoretical issue is to understand the algebraic structure of the ideal $\mathscr{I}_r \subset \mathbb{K}[U]$ (where U is the set of variables $\{u_{1,1},\dots,u_{n,m}\}$) generated by the $(r+1)$-minors of the matrix:

$$\mathscr{U} = \begin{pmatrix} u_{1,1} & \dots & u_{1,m} \\ \vdots & \ddots & \vdots \\ u_{n,1} & \dots & u_{n,m} \end{pmatrix}.$$

The ideal $\mathscr{I}_r$ has been extensively studied during last decades. In particular, explicit formulas for its degree and for its Hilbert series are known (see e.g. Fulton (1997, Example 14.4.14) and Conca and Herzog (1994)), as well as structural properties such as Cohen-Macaulayness and primality (Hochster and Eagon, 1970, 1971).

In cryptology, Kipnis and Shamir (1999) have proposed a multi-homogeneous algebraic modeling which can be seen as a generalization of the Lagrange multipliers and is designed as follows: a polynomial $n\times m$ matrix $\mathscr{M} \in \mathbb{K}[X]^{n\times m}$ (where X denotes the set of variables $\{x_1,\dots,x_k\}$) has rank at most r if and only if the dimension of its right kernel is greater than $m-r-1$. Consequently, by introducing $r(m-r)$ fresh variables $y_{1,1},\dots,y_{r,m-r}$, we can consider the system of bi-degree $(D,1)$ in $\mathbb{K}[x_1,\dots,x_k,y_{1,1},\dots,y_{r,m-r}]$ defined by

$$\mathscr{M} \cdot \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \\ y_{1,1} & y_{1,2} & \cdots & y_{1,m-r} \\ \vdots & \vdots & \ddots & \vdots \\ y_{r,1} & y_{r,2} & \cdots & y_{r,m-r} \end{pmatrix} = 0.$$

If $(x_1, \dots, x_k, y_{1,1}, \dots, y_{r,m-r})$ is a solution of that system, then the evaluation of the matrix $\mathscr{M}$ at the point $(x_1, \dots, x_k)$ has rank at most r.

In (Faugère et al., 2010), the case of square linear matrices is studied by performing a complexity analysis of the Gröbner bases computations. In particular, this investigation showed that the overall complexity is polynomial in the size of the matrix when the rank defect $n-r$ is constant. This theoretical analysis is supported by experimental results. The proofs were complete when the system has positive dimension, but depended on a variant of a conjecture by Fröberg in the 0-dimensional case.

Main results

We generalize in several ways the results from (Faugère et al., 2010) where only the case of square linear matrices was investigated: our contributions are the following.

- We deal with non-square matrices whose entries are polynomials of degree D with generic coefficients; this is achieved by using more general tools than those considered in (Faugère et al., 2010) (weighted Hilbert series). This generalization is important for applications in geometry and optimization for instance.
- When $n = (p-r)(q-r)$, the solution set of the generalized MinRank problem has dimension 0. In that case, our proofs in this paper do not rely on Fröberg's conjecture; this has been achieved by modifying our proof techniques and using more sophisticated and structural properties of determinantal ideals. This is important for applications in cryptology (see e.g. the sets of parameters A, B and C in the MinRank authentication scheme (Courtois, 2001)).

Our results are complexity bounds for Gröbner bases algorithms when the input system is the set of $(r+1)$-minors of a $n \times m$ matrix $\mathscr{M}$, whose entries are polynomials of degree D with generic coefficients.

By generic, we mean that there exists a non-identically null multivariate polynomial h such that the complexity results hold when this polynomial does not vanish on the coefficients of the polynomials in the matrix. Therefore, from a practical viewpoint, the complexity bounds can be used for applications where the base field $\mathbb{K}$ is large enough: in that case, the probability that the coefficients of $\mathscr{M}$ do not belong to the zero set of h is close to 1.

We start by studying the homogeneous generalized MinRank problem (i.e. when the entries of $\mathscr{M}$ are homogeneous polynomials) and by proving an explicit formula for the Hilbert series of the ideal $\mathscr{I}_r$ generated by the $(r+1)$-minors of the matrix $\mathscr{M}$. The general framework of the proofs is the following: we consider the ideal $\mathscr{J}_r \subset \mathbb{K}[U]$ generated by the $(r+1)$-minors of a matrix $\mathscr{U} = (u_{i,j})$ whose entries are variables. Then we consider the ideal $\widetilde{\mathscr{I}}_r = \mathscr{J}_r + \langle g_1, \dots, g_{nm} \rangle \subset \mathbb{K}[U, X]$, where the polynomials g_i are quasi-homogeneous forms that are the sum of a linear form in $\mathbb{K}[U]$ and of a homogeneous polynomial of degree D in $\mathbb{K}[X]$. If some conditions on the g_i are verified, by performing a linear combination of the generators there exists $f_{1,1},\ldots,f_{n,m} \in \mathbb{K}[X]$ such that

$$\widetilde{\mathscr{J}_r} = \mathscr{J}_r + \langle u_{1,1} - f_{1,1}, \ldots, u_{n,m} - f_{n,m} \rangle.$$

Then we use the fact that $\left(\mathscr{J}_r + \langle u_{1,1} - f_{1,1}, \ldots, u_{n,m} - f_{n,m} \rangle\right) \cap \mathbb{K}[X] = \mathscr{I}_r$ to prove that properties of generic quasi-homogeneous sections of $\mathscr{J}_r$ transfer to $\mathscr{I}_r$ when the entries of the matrix $\mathscr{M}$ are generic. This allows us to use results known about the ideal $\mathscr{J}_r$ to study the algebraic structure of $\mathscr{I}_r$.

We study separately three different cases:

- $k > (n-r)(m-r)$. Under genericity assumptions on the input, the solutions of the generalized MinRank problem are an algebraic variety of positive dimension. Recall that the complexity results were only proven for $D = 1$ and $n = m$ in Faugère et al. (2010). We generalize here for any $D \in \mathbb{N}$.
- $k = (n-r)(m-r)$. This is the $0-$*dimensional* case, where the problem has finitely-many solutions under genericity assumptions. Recall that the results in Faugère et al. (2010) were only stated for $D = 1$ and $n = m$, and they depended on a variant of Fröberg's conjecture. In this paper, we give complete proofs for $D \in \mathbb{N}$ which do not rely on any conjecture.
- $k < (n-r)(m-r)$. In the over-determined case, we still need to assume a variant of Fröberg's conjecture to generalize the results in Faugère et al. (2010).

In particular, we prove that, for $k \geq (n-r)(m-r)$, the Hilbert series of $\mathscr{I}_r$ is the power series expansion of the rational function

$$\mathsf{HS}_{\mathscr{I}_r}(t) = \frac{\det A_r(t^D)(1-t^D)^{(n-r)(m-r)}}{t^{D\binom{r}{2}}(1-t)^k},$$

where $A_r(t)$ is the $r \times r$ matrix whose (i,j)-entry is $\sum_k \binom{m-i}{k}\binom{n-j}{k} t^k$. Assuming w.l.o.g. that $m \leq n$, we also prove that the degree of $\mathscr{I}_r$ is equal to

$$\mathsf{DEG}(\mathscr{I}_r) = D^{(n-r)(m-r)} \prod_{i=0}^{m-r-1} \frac{i!(n+i)!}{(m-1-i)!(n-r+i)!}.$$

These explicit formulas permit to derive complexity bounds on the complexity of the problem. Indeed, one way to get a representation of the solutions of the problem in the 0-dimensional case is to compute a *lexicographical* Gröbner basis of the ideal generated by the polynomials. This can be achieved by using first the F_5 algorithm (Faugère, 2002) to compute a Gröbner basis for the so-called *grevlex* ordering and then use the FGLM algorithm (Faugère et al., 1993) to convert it into a *lexicographical* Gröbner basis. The complexities of these algorithms are governed by the degree of regularity and by the degree of the ideal.

Therefore the theoretical results on the structure of $\mathscr{I}_r$ yield bounds on the complexity of solving the generalized MinRank problem with Gröbner bases algorithms. More specifically, when $k = (n-r)(m-r)$ and under genericity assumptions on the input polynomial matrix, we prove that the arithmetic complexity for computing a lexicographical Gröbner basis of $\mathscr{I}_r$ is upper bounded by

$$O\left(\binom{n}{r+1}\binom{m}{r+1}\binom{\mathbb{D}_{\mathrm{reg}}+k}{k}^{\omega} + k\left(\mathsf{DEG}\left(\mathscr{I}_r\right)\right)^3\right),$$

where $2 \leq \omega \leq 3$ is a feasible exponent for the matrix multiplication, and

$$\mathbb{D}_{\mathrm{reg}} = Dr(m-r) + (D-1)k + 1.$$

This complexity bound permits to identify families of Generalized MinRank problems for which the number of arithmetic operations during the Gröbner basis computations is polynomial in the number of solutions.

In the over-determined case (i.e. $k < (n-r)(m-r)$), we obtain similar complexity results, by assuming a variant of Fröberg's conjecture which is supported by experiments.

Finally, we show that complexity bounds for solving systems of bi-degree $(D,1)$ can be obtained from these results on the generalized MinRank problem. We give an algorithm whose arithmetic complexity is upper bounded by

$$O\left(\binom{n_x+n_y}{n_y+1}\binom{D(n_x+n_y)+1}{n_x}^{\omega}+n_x\left(D^{n_x}\binom{n_x+n_y}{n_x}\right)^3\right),$$

for solving systems of n_x+n_y equations of bi-degree $(D,1)$ in $\mathbb{K}[x_1,\ldots,x_{n_x},y_1,\ldots,y_{n_y}]$ which are radical and 0-dimensional.

Organization of the paper

Section 2 provides notations used throughout this paper and preliminary results. In Section 3, we show how properties of the ideal $\mathscr{J}_r$ generated by the $(r+1)$-minors of $\mathscr{U}$ transfer to the ideal $\mathscr{I}_r$. Then, the case when the homogeneous Generalized MinRank Problem has non-trivial solutions (under genericity assumptions) is studied in Section 4. Section 5 is devoted to the study of the over-determined MinRank Problem (i.e. when $k < (n-r)(m-r)$). Then, the complexity analysis is performed in Section 6. Some consequences of this complexity analysis are drawn in Section 7. Experimental results are given in Section 7.4 and applications to the complexity of solving bi-homogeneous systems of bi-degree $(D,1)$ are investigated in Section 8.

Acknowledgments

This work was supported in part by the HPAC grant and the GeoLMI grant (ANR 2011 BS03 011 06) of the French National Research Agency.

2. Notations and preliminaries

Let $\mathbb{K}$ be a field and $\overline{\mathbb{K}}$ be its algebraic closure. In the sequel, n, m, r and k and D are positive integers with $r < m \leq n$. For $d \in \mathbb{N}$, $\mathrm{Mon}(d,k)$ denotes the set of monomials of degree d in the polynomial ring $\mathbb{K}[x_1,\ldots,x_k]$. Its cardinality is $\#\mathrm{Mon}(d,k) = \binom{d-1+k}{d}$.

We denote by $\mathfrak{a}$ the set of parameters $\{\mathfrak{a}_t^{(i,j)} : 1 \leq i \leq n, 1 \leq j \leq m, t \in \mathrm{Mon}(D,k)\}$. The set of variables $\{u_{i,j} : 1 \leq i \leq n, 1 \leq j \leq m\}$ (resp. $\{x_1,\ldots,x_k\}$) is denoted by U (resp. X).

For $1 \leq i \leq n, 1 \leq j \leq m$, we denote by $f_{i,j} \in \mathbb{K}(\mathfrak{a})[X]$ a generic form of degree D

$$f_{i,j} = \sum_{t \in \mathrm{Mon}(D,k)} \mathfrak{a}_t^{(i,j)} t.$$

Let $\mathscr{I}_r \subset \mathbb{K}(\mathfrak{a})[X]$ be the ideal generated by the $(r+1)$-minors of the $n \times m$ matrix

$$\mathscr{M} = \begin{pmatrix} f_{1,1} & \cdots & f_{1,m} \\ \vdots & \ddots & \vdots \\ f_{n,1} & \cdots & f_{n,m} \end{pmatrix},$$

and $\mathscr{J}_r \subset \mathbb{K}(\mathfrak{a})[U,X]$ be the determinantal ideal generated by the $(r+1)$-minors of the matrix

$$\mathscr{U} = \begin{pmatrix} u_{1,1} & \dots & u_{1,m} \\ \vdots & \ddots & \vdots \\ u_{n,1} & \dots & u_{n,m} \end{pmatrix}.$$

We define $\widetilde{\mathscr{I}_r}$ as the ideal $\mathscr{J}_r + \langle u_{i,j} - f_{i,j} \rangle_{1\leq i\leq n, 1\leq j\leq m} \subset \mathbb{K}(\mathfrak{a})[U,X]$. Notice that $\widetilde{\mathscr{I}_r} = \mathscr{I}_r + \langle u_{i,j} - f_{i,j} \rangle_{1\leq i\leq n, 1\leq j\leq m} \subset \mathbb{K}(\mathfrak{a})[U,X]$. Therefore, $\mathscr{I}_r = \widetilde{\mathscr{I}_r} \cap \mathbb{K}(\mathfrak{a})[X]$.

By slight abuse of notation, if I is a proper homogeneous ideal of a polynomial ring $\mathbb{K}[X]$, we call *Hilbert series* of I and we note $\mathsf{HS}_I \in \mathbb{Z}[[t]]$ the Hilbert series of its quotient algebra $\mathbb{K}[X]/I$ with the grading defined by $\deg(x_i) = 1$ for all i:

$$\mathsf{HS}_I(t) = \sum_{d\geq 0} \dim_{\mathbb{K}} (\mathbb{K}[X]_d / I_d)\, t^d,$$

where $\mathbb{K}[X]_d$ denotes the vector space of homogeneous polynomials of degree d and $I_d = I \cap \mathbb{K}[X]_d$.

We call *dimension* of I the Krull dimension of the quotient ring $\mathbb{K}[X]/I$.

Quasi-homogeneous polynomials.

We need to balance the degrees of the entries of the matrix $\mathscr{U}$ with the degrees of the entries of $\mathscr{M}$. This can be achieved by putting a *weight* on the variables $u_{i,j}$, giving rise to *quasi-homogeneous* polynomials. A polynomial $f \in \mathbb{K}[U,X]$ is called *quasi-homogeneous* (of type $(D,1)$) if the following condition holds (see e.g. Greuel et al. (2007, Definition 2.11, page 120)):

$$f(\lambda^D u_{1,1}, \dots, \lambda^D u_{n,m}, \lambda x_1, \dots, \lambda x_k) = \lambda^d f(u_{1,1}, \dots, u_{n,m}, x_1, \dots, x_k).$$

The integer d is called the weight degree of f and denoted by $\mathrm{wdeg}(f)$.

An ideal $I \subset \mathbb{K}[U,X]$ is called quasi-homogeneous (of type $(D,1)$) if there exists a set of quasi-homogeneous generators. In this case, we denote by $\mathbb{K}[U,X]_d$ the $\mathbb{K}$-vector space of quasi-homogeneous polynomials of weight degree d, and I_d denote the set $\mathbb{K}[U,X]_d \cap I$.

Proposition 1. *Let $I \subset \mathbb{K}[U,X]$ be an ideal. Then the following statements are equivalent:*
(1) there exists a set of quasi-homogeneous generators of I;
(2) the sets I_d are subspaces of $\mathbb{K}[U,X]_d$, and $I = \bigoplus_{d\in\mathbb{N}} I_d$.

Proof. See e.g. Miller and Sturmfels (2005, Chapter 8).
□

If I is a quasi-homogeneous ideal, then its *weighted Hilbert series* $\mathsf{wHS}_I(t) \in \mathbb{Z}[[t]]$ is defined as follows:

$$\mathsf{wHS}_I(t) = \sum_{d\in\mathbb{N}} \dim(\mathbb{K}[U,X]_d / I_d) t^d.$$

3. Transferring properties from $\mathscr{J}_r$ to $\mathscr{I}_r$

In this section, we prove that generic structural properties (such as the dimension, the structure of the leading monomial ideal,...) of the ideal $\widetilde{\mathscr{I}_r}$ are the same as properties of the ideal $\mathscr{J}_r$

where several generic forms have been added. Hence several classical properties of the determinantal ideal $\mathscr{J}_r$ transfer to the ideal $\widetilde{\mathscr{I}_r}$. For instance, this technique permits to obtain explicit forms of the Hilbert series of the ideal $\widetilde{\mathscr{I}_r}$.

In the following, we denote by $\mathfrak{b}$ and $\mathfrak{c}$ the following sets of parameters:

$$\begin{aligned} \mathfrak{b} &= \{\mathfrak{b}_t^{(\ell)} \mid t \in \mathrm{Mon}(D,k), 1 \leq \ell \leq nm\}; \\ \mathfrak{c} &= \{\mathfrak{c}_{i,j}^{(\ell)} \mid 1 \leq i \leq n, 1 \leq j \leq m, 1 \leq \ell \leq nm\}. \end{aligned}$$

Also, $g_1, \ldots, g_{nm} \in \mathbb{K}(\mathfrak{b},\mathfrak{c})[U,X]$ are generic quasi-homogeneous forms of type $(D,1)$ and of weight degree D:

$$g_\ell = \sum_{t \in \mathrm{Mon}(D,k)} \mathfrak{b}_t^{(\ell)} t + \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \mathfrak{c}_{i,j}^{(\ell)} u_{i,j}.$$

We let $\widetilde{\mathscr{J}_r}$ denote the ideal $\mathscr{J}_r + \langle g_1, \ldots, g_{nm}\rangle \subset \mathbb{K}(\mathfrak{b},\mathfrak{c})[U,X]$. Here and subsequently, for $\mathbf{a} = (a_{i,j}) \in \overline{\mathbb{K}}^{nm\binom{D-1+k}{D}}$, we denote by $\varphi_{\mathbf{a}}$ the following evaluation morphism:

$$\begin{aligned} \varphi_{\mathbf{a}}: \quad \mathbb{K}[\mathfrak{a}] &\longrightarrow \overline{\mathbb{K}} \\ f(\mathfrak{a}_{1,1}, \ldots, \mathfrak{a}_{n,m}) &\longmapsto f(a_{1,1}, \ldots, a_{n,m}) \end{aligned}$$

Also, for $(\mathbf{b},\mathbf{c}) \in \overline{\mathbb{K}}^{nm\left(\binom{D-1+k}{D}+nm\right)}$, we denote by $\psi_{\mathbf{b},\mathbf{c}}$ the evaluation morphism:

$$\begin{aligned} \psi_{\mathbf{b},\mathbf{c}}: \mathbb{K}[\mathfrak{b},\mathfrak{c}] &\longrightarrow \overline{\mathbb{K}} \\ f(\mathfrak{b},\mathfrak{c}) &\longmapsto f(\mathbf{b},\mathbf{c}) \end{aligned}$$

By abuse of notation, we let $\varphi_{\mathbf{a}}(\widetilde{\mathscr{I}_r})$ (resp. $\psi_{\mathbf{b},\mathbf{c}}(\widetilde{\mathscr{J}_r})$) denote the ideal $\mathscr{J}_r + \langle u_{i,j} - \varphi_{\mathbf{a}}(f_{i,j})\rangle \subset \overline{\mathbb{K}}[U,X]$ (resp. $\mathscr{J}_r + \langle \psi_{\mathbf{b},\mathbf{c}}(g_1), \ldots, \psi_{\mathbf{b},\mathbf{c}}(g_{nm})\rangle \subset \overline{\mathbb{K}}[U,X]$).

We call *property* a map from the set of ideals of $\overline{\mathbb{K}}[U,X]$ to $\{\mathtt{true}, \mathtt{false}\}$:

$$\mathscr{P}: \mathsf{Ideals}(\overline{\mathbb{K}}[U,X]) \to \{\mathtt{true}, \mathtt{false}\}.$$

Definition 2. Let $\mathscr{P}$ be a property. We say that $\mathscr{P}$ is

- $\widetilde{\mathscr{I}_r}$-generic if there exists a non-empty Zariski open subset $O \subset \overline{\mathbb{K}}^{nm\binom{D-1+k}{D}}$ such that

$$\mathbf{a} \in O \Rightarrow \mathscr{P}\left(\varphi_{\mathbf{a}}\left(\widetilde{\mathscr{I}_r}\right)\right) = \mathtt{true};$$

- $\widetilde{\mathscr{J}_r}$-generic if there exists a non-empty Zariski open subset $O \subset \overline{\mathbb{K}}^{nm\left(\binom{D-1+k}{D}+nm\right)}$ such that

$$(\mathbf{b},\mathbf{c}) \in O \Rightarrow \mathscr{P}\left(\psi_{\mathbf{b},\mathbf{c}}\left(\widetilde{\mathscr{J}_r}\right)\right) = \mathtt{true}.$$

The following lemma is the main result of this section:

Lemma 3. *A property $\mathscr{P}$ is $\widetilde{\mathscr{I}_r}$-generic if and only if it is $\widetilde{\mathscr{J}_r}$-generic.*

Proof. To obtain a representation of $\varphi_{\mathbf{a}}\left(\widetilde{\mathscr{J}_r}\right)$ for a generic $\mathbf{a}$ as a specialization of $\widetilde{\mathscr{I}_r}$ (and conversely), it is sufficient to perform a linear combination of the generators. The point of this proof is to show that genericity is preserved during this linear transform.

In the sequel we denote by $\mathfrak{A},\mathfrak{B}$ and $\mathfrak{C}$ the following matrices (of respective sizes $nm\times\binom{D-1+k}{D}$, $nm\times\binom{D-1+k}{D}$ and $nm\times nm$):

$$\mathfrak{A}=\begin{pmatrix}\mathfrak{a}^{(1)}_{x_1^D} & \mathfrak{a}^{(1)}_{x_1^{D-1}x_2} & \cdots & \mathfrak{a}^{(1)}_{x_k^D}\\ \vdots & \vdots & \vdots & \vdots\\ \mathfrak{a}^{(nm)}_{x_1^D} & \mathfrak{a}^{(nm)}_{x_1^{D-1}x_2} & \cdots & \mathfrak{a}^{(nm)}_{x_k^D}\end{pmatrix}$$
$$\mathfrak{B}=\begin{pmatrix}\mathfrak{b}^{(1)}_{x_1^D} & \mathfrak{b}^{(1)}_{x_1^{D-1}x_2} & \cdots & \mathfrak{b}^{(1)}_{x_k^D}\\ \vdots & \vdots & \vdots & \vdots\\ \mathfrak{b}^{(nm)}_{x_1^D} & \mathfrak{b}^{(nm)}_{x_1^{D-1}x_2} & \cdots & \mathfrak{b}^{(nm)}_{x_k^D}\end{pmatrix}$$
$$\mathfrak{C}=\begin{pmatrix}\mathfrak{c}^{(1)}_{1,1} & \cdots & \mathfrak{c}^{(1)}_{n,m}\\ \vdots & \vdots & \vdots\\ \mathfrak{c}^{(nm)}_{1,1} & \cdots & \mathfrak{c}^{(nm)}_{n,m}\end{pmatrix}.$$

Therefore, we have

$$\begin{pmatrix}u_{1,1}-f_{1,1}\\ \vdots\\ u_{n,m}-f_{n,m}\end{pmatrix}=\mathsf{Id}_{nm}\cdot\begin{pmatrix}u_{1,1}\\ \vdots\\ u_{n,m}\end{pmatrix}-\mathfrak{A}\cdot\begin{pmatrix}x_1^D\\ x_1^{D-1}x_2\\ \vdots\\ x_k^D\end{pmatrix}$$
$$\begin{pmatrix}g_1\\ \vdots\\ g_{nm}\end{pmatrix}=\mathfrak{C}\cdot\begin{pmatrix}u_{1,1}\\ \vdots\\ u_{n,m}\end{pmatrix}+\mathfrak{B}\cdot\begin{pmatrix}x_1^D\\ x_1^{D-1}x_2\\ \vdots\\ x_k^D\end{pmatrix}$$

In this proof, for $\mathbf{a}\in\mathbb{K}^{nm\binom{D-1+k}{D}}$ (resp. $\mathbf{b}\in\mathbb{K}^{nm\binom{D-1+k}{D}},\mathbf{c}\in\mathbb{K}^{n^2m^2}$), the notation $\mathbf{A}$ (resp. $\mathbf{B},\mathbf{C}$) stands for the evaluation of the matrix $\mathfrak{A}$ (resp. $\mathfrak{B},\mathfrak{C}$) at $\mathbf{a}$ (resp. $\mathbf{b},\mathbf{c}$). Also, we implicitly identify $\mathbf{A}$ with $\mathbf{a}$ (resp. $\mathbf{B}$ with b, $\mathbf{C}$ with $\mathbf{c}$, $\mathfrak{A}$ with $\mathfrak{a}$, $\mathfrak{B}$ with $\mathfrak{b}$, $\mathfrak{C}$ with $\mathfrak{c}$).

- Let $\mathscr{P}$ be a $\widetilde{\mathscr{I}_r}$-generic property. Thus there exists a non-zero polynomial $h_1(\mathfrak{A})\in\overline{\mathbb{K}}[\mathfrak{a}]$ such that if $h_1(\mathbf{A})\neq 0$ then $\mathscr{P}\left(\varphi_{\mathbf{a}}(\widetilde{\mathscr{I}_r})\right)=\texttt{true}$.

  Let $\mathsf{adj}(\mathfrak{C})$ denote the adjugate of $\mathfrak{C}$ (i.e. $\mathsf{adj}(\mathfrak{C})=\det(\mathfrak{C})\cdot\mathfrak{C}^{-1}$ in $\mathbb{K}(\mathfrak{c})$). Consider the polynomial $\widetilde{h_1}$ defined by $\widetilde{h_1}(\mathfrak{B},\mathfrak{C})=h_1(-\mathsf{adj}(\mathfrak{C})\cdot\mathfrak{B})\in\overline{\mathbb{K}}[\mathfrak{b},\mathfrak{c}]$. The polynomial inequality $\det(\mathfrak{C})\widetilde{h_1}(\mathfrak{B},\mathfrak{C})\neq 0$ defines a non-empty Zariski open subset $O\subset\overline{\mathbb{K}}^{nm\left(\binom{D-1+k}{D}+nm\right)}$. Let $(\mathbf{B},\mathbf{C})\in O$ be an element in this set, then $\mathbf{C}$ is invertible since $\det(\mathbf{C})\neq 0$. Let $\widetilde{\mathbf{A}}$ be the matrix $\widetilde{\mathbf{A}}=-\mathsf{adj}(\mathbf{C})\cdot\mathbf{B}$. Therefore the generators of the ideal $\varphi_{\widetilde{\mathbf{a}}}\left(\widetilde{\mathscr{I}_r}\right)$ are an invertible linear combination of the generators of $\psi_{\mathbf{b},\mathbf{c}}\left(\widetilde{\mathscr{J}_r}\right)$. Consequently, $\varphi_{\widetilde{\mathbf{a}}}\left(\widetilde{\mathscr{I}_r}\right)=\psi_{\mathbf{b},\mathbf{c}}\left(\widetilde{\mathscr{J}_r}\right)$. Moreover,

$h_1(\widetilde{\mathbf{A}}) = \widetilde{h_1}(\mathbf{B},\mathbf{C}) \neq 0$ implies that the polynomial $\widetilde{h_1}$ is not identically 0. Therefore,

$$\forall(\mathbf{b},\mathbf{c}) \in O, \mathscr{P}\left(\psi_{\mathbf{b},\mathbf{c}}\left(\widetilde{\mathscr{J}_r}\right)\right) = \mathscr{P}\left(\varphi_{\widetilde{\mathbf{a}}}\left(\widetilde{\mathscr{I}_r}\right)\right) = \texttt{true},$$

and hence $\mathscr{P}$ is a $\widetilde{\mathscr{J}_r}$-generic property.

- Conversely, consider a $\widetilde{\mathscr{J}_r}$-generic property $\mathscr{P}$. Thus, there exists a non-zero polynomial $h_2(\mathfrak{B},\mathfrak{C}) \in \overline{\mathbb{K}}[\mathfrak{b},\mathfrak{c}]$ such that if $h_2(\mathbf{b},\mathbf{c}) \neq 0$ then $\mathscr{P}\left(\psi_{\mathbf{b},\mathbf{c}}(\widetilde{\mathscr{J}_r})\right) = \texttt{true}$. Since $\mathscr{P}$ is $\widetilde{\mathscr{J}_r}$-generic, there exists $(\mathbf{b},\mathbf{c})$ such that $h_2(\mathbf{b},\mathbf{c})\det(\mathbf{c}) \neq 0$. Let $\widetilde{h_2}$ be the polynomial $\widetilde{h_2}(\mathfrak{b}) = h_2(-\mathbf{C}\cdot\mathfrak{B},\mathbf{C})$.
  Since $\det(\mathbf{C}) \neq 0$, the matrix $\mathbf{C}$ is invertible and $\widetilde{h_2}(-\mathbf{C}^{-1}\cdot\mathbf{B}) = h_2(\mathbf{B},\mathbf{C}) \neq 0$ and hence the polynomial $\widetilde{h_2}$ is not identically 0. Moreover, if $\mathbf{a} \in \mathbb{K}^{nm\binom{D-1+k}{D}}$ is such that $\widetilde{h_2}(\mathbf{A}) \neq 0$, then $h_2(-\mathbf{C}\cdot\mathbf{A},\mathbf{C}) \neq 0$ and thus $\mathscr{P}\left(\psi_{-\mathbf{C}\cdot\mathbf{A},\mathbf{C}}(\widetilde{\mathscr{J}_r})\right) = \texttt{true}$. Finally, $\psi_{-\mathbf{C}\cdot\mathbf{A},\mathbf{C}}(\widetilde{\mathscr{J}_r}) = \varphi_{\mathbf{A}}(\widetilde{\mathscr{I}_r})$ since the generators of $\psi_{-\mathbf{C}\cdot\mathbf{A},\mathbf{C}}(\widetilde{\mathscr{J}_r})$ are an invertible linear combination of that of $\varphi_{\mathbf{a}}(\widetilde{\mathscr{I}_r})$ (the linear transformation being given by the invertible matrix $\mathbf{C}$) and hence they generate the same ideal. Therefore, the property $\mathscr{P}$ is $\widetilde{\mathscr{I}_r}$-generic.

$\square$

In the sequel, $\prec$ is an admissible monomial ordering (see e.g Cox et al. (1997, Chapter 2, §2, Definition 1)) on $\mathbb{K}[U,X]$, and for any polynomial $f \in \mathbb{K}[U,X]$, $\mathsf{LM}(f)$ denotes its leading monomial with respect to $\prec$. If I is an ideal of $\mathbb{K}[U,X]$, $\mathbb{K}(\mathfrak{a})[U,X]$, or $\mathbb{K}(\mathfrak{b},\mathfrak{c})[U,X]$, we let $\mathsf{LM}(I)$ denote the ideal generated by the leading monomials of the polynomials.

By slight abuse of notation, if I_1 and I_2 are ideals of $\mathbb{K}[U,X]$, $\mathbb{K}(\mathfrak{a})[U,X]$, or $\mathbb{K}(\mathfrak{b},\mathfrak{c})[U,X]$ (I_1 and I_2 are not necessarily ideals of the same ring), we write $\mathsf{LM}(I_1) = \mathsf{LM}(I_2)$ if the sets $\{\mathsf{LM}(f) \mid f \in I_1\}$ and $\{\mathsf{LM}(f) \mid f \in I_2\}$ are equal.

Lemma 4. *Let $\mathscr{P}_{\widetilde{\mathscr{I}_r}}$ and $\mathscr{P}_{\widetilde{\mathscr{J}_r}}$ be the properties defined by*

$$\mathscr{P}_{\widetilde{\mathscr{I}_r}}(I) = \begin{cases} \texttt{true} \textit{ if } \mathsf{LM}(I) = \mathsf{LM}\left(\widetilde{\mathscr{I}_r}\right); \\ \texttt{false} \textit{ otherwise.} \end{cases}$$
$$\mathscr{P}_{\widetilde{\mathscr{J}_r}}(I) = \begin{cases} \texttt{true} \textit{ if } \mathsf{LM}(I) = \mathsf{LM}\left(\widetilde{\mathscr{J}_r}\right); \\ \texttt{false} \textit{ otherwise.} \end{cases}$$

Then $\mathscr{P}_{\widetilde{\mathscr{I}_r}}$ (resp. $\mathscr{P}_{\widetilde{\mathscr{J}_r}}$) is a $\widetilde{\mathscr{I}_r}$-generic (resp. $\widetilde{\mathscr{J}_r}$-generic) property.

Proof. We prove here that $\mathscr{P}_{\widetilde{\mathscr{I}_r}}$ is $\widetilde{\mathscr{I}_r}$-generic (the proof for $\mathscr{P}_{\widetilde{\mathscr{J}_r}}$ is similar).

The outline of this proof is the following: during the computation of a Gröbner basis G of $\widetilde{\mathscr{I}_r}$ in $\mathbb{K}(\mathfrak{a})[U,X]$ (for instance with Buchberger's algorithm), a finite number of polynomials are constructed. Let $\varphi_{\mathbf{a}}$ be a specialization. If the images by $\varphi_{\mathbf{a}}$ of the leading coefficients of all non-zero polynomials arising during the computation do not vanish, then $\varphi_{\mathbf{a}}(G) \subset \varphi_{\mathbf{a}}(\widetilde{\mathscr{I}_r})$ is a Gröbner basis of the ideal it generates. It remains to prove that $\varphi_{\mathbf{a}}(G)$ is a Gröbner basis of $\varphi_{\mathbf{a}}(\widetilde{\mathscr{I}_r})$. This is achieved by showing that generically, the normal form (with respect to $\varphi_{\mathbf{a}}(G)$) of the generators of $\varphi_{\mathbf{a}}(\widetilde{\mathscr{I}_r})$ is equal to zero.

For polynomials f_1, f_2, we let $\mathsf{LC}(f_1)$ (resp. $\mathsf{LC}(f_2)$) denote the leading coefficient of f_1 (resp. f_2) and $\mathsf{Spol}(f_1, f_2) = \frac{\mathsf{LCM}(\mathsf{LM}(f_1),\mathsf{LM}(f_2))}{\mathsf{LC}(f_1)\mathsf{LM}(f_1)} f_1 - \frac{\mathsf{LCM}(\mathsf{LM}(f_1),\mathsf{LM}(f_2))}{\mathsf{LC}(f_2)\mathsf{LM}(f_2)} f_2$ denote the *S-polynomial* of f_1 and f_2.

We need to prove that there exists a non-empty Zariski open subset $O_1 \subset \overline{\mathbb{K}}^{nm\binom{D-1+k}{D}}$ such that

$$\mathbf{a} \in O_1 \Rightarrow \mathsf{LM}(\varphi_{\mathbf{a}}(\widetilde{\mathscr{I}_r})) = \mathsf{LM}(\widetilde{\mathscr{I}_r}).$$

To do so, consider a Gröbner basis $G \subset \mathbb{K}(\mathfrak{a})[U, X]$ of $\widetilde{\mathscr{I}_r}$ such that each polynomial g can be written as a combination $g = \sum h_\ell f_\ell$, where the f_ℓ's range over the set of minors of size $r+1$ of $\mathscr{U}$ and the polynomials $u_{i,j} - f_{i,j}$, and $h_\ell \in \mathbb{K}[\mathfrak{a}][U, X]$. Buchberger's criterion states that S-polynomials of polynomials in a Gröbner basis reduce to zero (Cox et al., 1997, Chapter 2, §6, Theorem 6). Thus each S-polynomial of $g_i, g_j \in G$ can be rewritten as an algebraic combination

$$\mathsf{Spol}(g_i, g_j) = \sum_\ell h'_\ell g_\ell,$$

where the polynomials h'_ℓ belongs to $\mathbb{K}(\mathfrak{a})[U, X]$ and such that $\{g_1, \ldots, g_{t_{i,j}}\} \subset G$ and for each $1 \le s \le t_{i,j}$, $\mathsf{LM}(g_s)$ divides $\mathsf{LM}(\mathsf{Spol}(g, g') - \sum_{\ell=1}^{s-1} h'_\ell g_\ell)$. Next, consider:

- the product $Q_1(\mathfrak{a}) = \prod_{g \in G} \mathsf{LC}(g)$ of the leading coefficients of the polynomials in the Gröbner basis;
- for all $(g_i, g_j) \in G^2$ such that $\mathsf{Spol}(g_i, g_j) \neq 0$, the product $Q_2(\mathfrak{a})$ of the numerators and denominators of the leading coefficients arising during the reduction of $\mathsf{Spol}(g_i, g_j)$.

These coefficients belongs to $\mathbb{K}[\mathfrak{a}]$. Denote by $Q(\mathfrak{a}) = Q_1(\mathfrak{a}) Q_2(\mathfrak{a}) \in \mathbb{K}[\mathfrak{a}]$ their product. The inequality $Q(\mathfrak{a}) \neq 0$ defines a non-empty Zariski open subset $O_1 \subset \overline{\mathbb{K}}^{nm\binom{D-1+k}{D}}$. If $\mathbf{a} \in O_1$, then

$$\varphi_{\mathbf{a}}(\mathsf{Spol}(g, g')) = \sum_{\ell=1}^{t} \varphi_{\mathbf{a}}(h'_\ell) \varphi_{\mathbf{a}}(g_\ell),$$

and for each $1 \le i \le t$, $\mathsf{LM}(\varphi_{\mathbf{a}}(g_i))$ divides $\mathsf{LM}(\varphi_{\mathbf{a}}(\mathsf{Spol}(g, g')) - \sum_{\ell=1}^{i-1} \varphi_{\mathbf{a}}(h'_\ell) \varphi_{\mathbf{a}}(g_\ell))$. Thus $\varphi_{\mathbf{a}}(G)$ is a Gröbner basis of the ideal it spans. Moreover, $\langle \varphi_{\mathbf{a}}(G) \rangle \subset \varphi_{\mathbf{a}}(\widetilde{\mathscr{I}_r})$.

We prove now that there exists a non-empty Zariski open set where the other inclusion $\varphi_{\mathbf{a}}(\widetilde{\mathscr{I}_r}) \subset \langle \varphi_{\mathbf{a}}(G) \rangle$ holds. Let $\mathsf{NF}_G(\cdot)$ be the normal form associated to this Gröbner basis (as defined as the *remainder of the division by G* in Cox et al. (1997, Chapter 2, §6, Proposition 1)). For each generator f of $\widetilde{\mathscr{I}_r}$ (i.e. either a maximal minor of the matrix $\mathscr{U}$, or a polynomial $u_{i,j} - f_{i,j}$), we have that $\mathsf{NF}_G(f) = 0$. During the computation of $\mathsf{NF}_G(f)$ by using the division Algorithm in Cox et al. (1997, Chapter 2, §3), a finite set of polynomials (in $\mathbb{K}(\mathfrak{a})[U, X]$) is constructed. Let $Q_3 \in \mathbb{K}[\mathfrak{a}]$ denote the product of the numerators and denominators of all their nonzero coefficients. Consequently, if $Q_3^{(f)}(\mathbf{a}) \neq 0$, then $\mathsf{NF}_{\varphi_{\mathbf{a}}(G)}(\varphi_{\mathbf{a}}(f)) = 0$ and hence $\varphi_{\mathbf{a}}(f) \in \langle \varphi_{\mathbf{a}}(G) \rangle$. Repeating this operation for all the generators of $\widetilde{\mathscr{I}_r}$ yields a finite set of non-identically null polynomials $Q_3^{(f)} \in \mathbb{K}[\mathfrak{a}]$. Let $Q_4 \in \mathbb{K}[\mathfrak{a}]$ denote their product. Therefore, if $Q_4(\mathbf{a}) \neq 0$, then $\varphi_{\mathbf{a}}(\widetilde{\mathscr{I}_r}) \subset \langle \varphi_{\mathbf{a}}(G) \rangle$.

Finally, consider the non-empty Zariski open subset $O \subset \mathbb{K}^{nm\binom{D+k-1}{D}}$ defined by the inequality $Q_1 \cdot Q_2 \cdot Q_4 \neq 0$. For all $\mathbf{a} \in O$, we have $\varphi_{\mathbf{a}}(\widetilde{\mathscr{I}_r}) = \langle \varphi_{\mathbf{a}}(G) \rangle$.

□

Corollary 5. *The leading monomials of $\widetilde{\mathscr{I}_r}$ are the same as that of $\widetilde{\mathscr{J}_r}$:*

$$\mathsf{LM}\left(\widetilde{\mathscr{I}_r}\right) = \mathsf{LM}\left(\widetilde{\mathscr{J}_r}\right).$$

Proof. By Lemmas 3 and 4, the property $\mathscr{P}_{\widetilde{\mathscr{I}_r}}$ (resp. $\mathscr{P}_{\widetilde{\mathscr{J}_r}}$) is $\widetilde{\mathscr{I}_r}$-generic and $\widetilde{\mathscr{J}_r}$-generic. Since $\mathscr{P}_{\widetilde{\mathscr{J}_r}}$ (resp. $\mathscr{P}_{\widetilde{\mathscr{I}_r}}$) is $\widetilde{\mathscr{J}_r}$-generic, there exists a non-empty Zariski open subset $O_1 \subset \overline{\mathbb{K}}^{nm\left(\binom{D-1+k}{D}+nm\right)}$ (resp. $O_2 \subset \overline{\mathbb{K}}^{nm\left(\binom{D-1+k}{D}+nm\right)}$) such that, for $(\mathbf{b},\mathbf{c}) \in O_1$ (resp. O_2), $\mathsf{LM}\left(\psi_{(\mathbf{b},\mathbf{c})}(\widetilde{\mathscr{J}_r})\right) = \mathsf{LM}\left(\widetilde{\mathscr{J}_r}\right)$ (resp. $\mathsf{LM}\left(\psi_{(\mathbf{b},\mathbf{c})}(\widetilde{\mathscr{J}_r})\right) = \mathsf{LM}\left(\widetilde{\mathscr{I}_r}\right)$).

Notice that $O_1 \cap O_2$ is not empty, since for the Zariski topology, the intersection of finitely-many non-empty open subsets is non-empty. Let $(\mathbf{b},\mathbf{c})$ be an element of $O_1 \cap O_2$. Then

$$\mathsf{LM}\left(\widetilde{\mathscr{I}_r}\right) = \mathsf{LM}\left(\psi_{(\mathbf{b},\mathbf{c})}(\widetilde{\mathscr{J}_r})\right) = \mathsf{LM}\left(\widetilde{\mathscr{J}_r}\right).$$

□

Corollary 6. *The weighted Hilbert series of $\widetilde{\mathscr{I}_r}$ is the same as that of $\widetilde{\mathscr{J}_r}$.*

Proof. It is well-known that, for any positively graded ideal I and for any monomial ordering, $\mathsf{wHS}_I(t) = \mathsf{wHS}_{\mathsf{LM}(I)}(t)$ (see e.g. the proof of Cox et al. (1997, Chapter 9, §3, Proposition 9) which is also valid for quasi-homogeneous ideals). By Corollary 5, $\mathsf{LM}\left(\widetilde{\mathscr{I}_r}\right) = \mathsf{LM}\left(\widetilde{\mathscr{J}_r}\right)$, which implies that

$$\mathsf{wHS}_{\mathsf{LM}\left(\widetilde{\mathscr{I}_r}\right)}(t) = \mathsf{wHS}_{\mathsf{LM}\left(\widetilde{\mathscr{J}_r}\right)}(t),$$

and hence $\mathsf{wHS}_{\widetilde{\mathscr{I}_r}}(t) = \mathsf{wHS}_{\widetilde{\mathscr{J}_r}}(t)$. □

4. The case $k \geq (n-r)(m-r)$

As we will see in the sequel, the Krull dimension of the ring $\mathbb{K}(\mathfrak{a})[X]/\mathscr{I}_r$ is equal to $\max(k-(n-r)(m-r),0)$. This section is devoted to the study of the case $k \geq (n-r)(m-r)$.

We show here that the algebraic structure of the ideal $\mathscr{I}_r$ is closely related to that of a generic section of a determinantal variety.

We recall that the polynomials g_ℓ are defined by

$$g_\ell = \sum_{t \in \mathrm{Mon}(D,k)} \mathfrak{b}_t^{(\ell)} t + \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \mathfrak{c}_{i,j}^{(\ell)} u_{i,j}.$$

Lemma 7. *Let $1 \leq \ell \leq nm$ be an integer. If g_ℓ divides zero in $\mathbb{K}(\mathfrak{b},\mathfrak{c})[U,X]/\left(\mathscr{J}_r + \langle g_1,\dots,g_{\ell-1}\rangle\right)$, then there exists a prime ideal P associated to $\mathscr{J}_r + \langle g_1,\dots,g_{\ell-1}\rangle$ such that* $\dim(P) = 0$.

Proof. If g_ℓ divides zero in $\mathbb{K}(\mathfrak{b},\mathfrak{c})[U,X]/\left(\mathscr{J}_r + \langle g_1,\dots,g_{\ell-1}\rangle\right)$, then there exists a prime ideal P associated to $\mathscr{J}_r + \langle g_1,\dots,g_{\ell-1}\rangle$ such that $g_\ell \in P$. For $\ell \leq nm$, let $\mathfrak{b}^{(\leq \ell)}$ and $\mathfrak{c}^{(\leq \ell)}$ denote the sets of parameters

$$\begin{aligned}
\mathfrak{b}^{(\leq \ell)} &= \{\mathfrak{b}_t^{(s)} \mid t \in \mathrm{Mon}(D,k), 1 \leq s \leq \ell\} \\
\mathfrak{c}^{(\leq \ell)} &= \{\mathfrak{c}_{i,j}^{(s)} \mid 1 \leq i \leq n, 1 \leq j \leq m, 1 \leq s \leq \ell\}.
\end{aligned}$$

Since $\left(\mathscr{J}_r + \langle g_1,\dots,g_{\ell-1}\rangle\right)$ is an ideal of $\mathbb{K}(\mathfrak{b}^{(\leq \ell-1)},\mathfrak{c}^{(\leq \ell-1)})[U,X]$, and P is an associated prime, there exists a Gröbner basis G_P of P (for any monomial ordering $\prec$) which is a finite subset of $\mathbb{K}(\mathfrak{b}^{(\leq \ell-1)},\mathfrak{c}^{(\leq \ell-1)})[U,X]$.

Let $\mathsf{NF}_P(\cdot)$ denote the normal form associated to this Gröbner basis (as defined as the *remainder of the division by G_P* in Cox et al. (1997, Chapter 2, §6, Proposition 1)).

Since $g_\ell \in P$, we have $\mathsf{NF}_P(g_\ell) = 0$. By linearity of $\mathsf{NF}_P(\cdot)$, we obtain

$$\sum_{t\in \mathrm{Mon}(D,k)} \mathfrak{b}_t^{(\ell)} \,\mathsf{NF}_P(t) + \sum_{\substack{1\le i\le n\\ 1\le j\le m}} \mathfrak{c}_{i,j}^{(\ell)} \,\mathsf{NF}_P(u_{i,j}) = 0.$$

Since $G_p \subset \mathbb{K}(\mathfrak{b}^{(\le \ell-1)}, \mathfrak{c}^{(\le \ell-1)})[U,X]$, we can deduce that for any monomial t, $\mathsf{NF}_P(t) \in \mathbb{K}(\mathfrak{b}^{(\le \ell-1)}, \mathfrak{c}^{(\le \ell-1)})[U,X]$. Therefore, by algebraic independence of the parameters, the following properties hold: for all $t \in \mathrm{Mon}(D,k)$, $\mathsf{NF}_P(t) = 0$, and for all i, j, $\mathsf{NF}_P(u_{i,j}) = 0$. Consequently, all monomials of weight degree D in $\mathbb{K}(\mathfrak{b},\mathfrak{c})[U,X]$ are in P, and hence P has dimension 0. □

Lemma 8. *For all $\ell \in \{2,\dots,nm\}$, the polynomial g_ℓ does not divide zero in $\mathbb{K}(\mathfrak{b},\mathfrak{c})[U,X]/(\mathscr{J}_r + \langle g_1,\dots,g_{\ell-1}\rangle)$ and $\dim(\mathscr{J}_r + \langle g_1,\dots,g_\ell\rangle) = k+(n+m-r)r-\ell$.*

Proof. We prove the Lemma by induction on ℓ. According to Hochster and Eagon (1970, Corollary 2 of Theorem 1), the ring $\mathbb{K}(\mathfrak{b},\mathfrak{c})[U,X]/\mathscr{J}_r$ is Cohen-Macaulay and purely equidimensional. First, notice that the dimension is equal to $k+(n+m-r)r$ for $\ell = 0$ since the dimension of the ideal $\mathscr{J}_r \subset \mathbb{K}[U]$ is $(n+m-r)r$ (see e.g. Conca and Herzog (1994) and references therein). Now, suppose that the dimension of the ideal $\mathscr{J}_r + \langle g_1,\dots,g_{\ell-1}\rangle \subset \mathbb{K}(\mathfrak{b},\mathfrak{c})[U,X]$ is $k+(n+m-r)r-\ell+1$. Since the ring $\mathbb{K}(\mathfrak{b},\mathfrak{c})[U,X]/\mathscr{J}_r$ is Cohen-Macaulay and $\langle g_1,\dots,g_{\ell-1}\rangle$ has co-dimension $\ell-1$ in $\mathbb{K}(\mathfrak{b},\mathfrak{c})[U,X]$, the Macaulay unmixedness Theorem (Eisenbud, 1995, Corollary 18.14) implies that $\langle g_1,\dots,g_{\ell-1}\rangle$ has no embedded component and is equidimensional in $\mathbb{K}(\mathfrak{b},\mathfrak{c})[U,X]/\mathscr{J}_r$. Hence $\mathscr{J}_r + \langle g_1,\dots,g_{\ell-1}\rangle$ as an ideal in $\mathbb{K}(\mathfrak{b},\mathfrak{c})[U,X]$ has no embedded component and is equidimensional. By contradiction, suppose that g_ℓ divides zero in $\mathbb{K}(\mathfrak{b},\mathfrak{c})[U,X]/(\mathscr{J}_r + \langle g_1,\dots,g_{\ell-1}\rangle)$. By Lemma 7, there exists a prime P associated to $\mathscr{J}_r + \langle g_1,\dots,g_{\ell-1}\rangle$ such that $\dim(P) = 0$, which contradicts the fact that $\mathscr{J}_r + \langle g_1,\dots,g_{\ell-1}\rangle$ is purely equidimensional of dimension $k+(n+m-r)r-\ell+1 > 0$. □

Lemma 9. *The Hilbert series of the $\mathscr{I}_r \subset \mathbb{K}(\mathfrak{a})[X]$ equals the weighted Hilbert series of $\widetilde{\mathscr{I}_r} \subset \mathbb{K}(\mathfrak{a})[X,U]$.*

Proof. Let $\prec_{lex}$ denote a lexicographical ordering on $\mathbb{K}(\mathfrak{a})[X,U]$ such that $x_k \prec_{lex} u_{i,j}$ for all k,i,j. By Cox et al. (1997, Section 9.3, Proposition 9), $\mathsf{HS}_{\mathscr{I}_r}(t) = \mathsf{HS}_{\mathsf{LM}_{\prec_{lex}}(\mathscr{I}_r)}(t)$ and $\mathsf{wHS}_{\widetilde{\mathscr{I}_r}}(t) = \mathsf{wHS}_{\mathsf{LM}_{\prec_{lex}}(\widetilde{\mathscr{I}_r})}(t)$. Since $\mathsf{LM}_{\prec_{lex}}(u_{i,j} - f_{i,j}) = u_{i,j}$, we deduce that all monomials which are multiples of a variable $u_{i,j}$ are in $\mathsf{LM}_{\prec_{lex}}(\widetilde{\mathscr{I}_r})$. Therefore, the remaining monomials in $\mathsf{LM}_{\prec_{lex}}(\widetilde{\mathscr{I}_r})$ are in $\mathbb{K}(\mathfrak{a})[X]$:

$$\begin{aligned}\mathsf{LM}_{\prec_{lex}}(\widetilde{\mathscr{I}_r}) &= \left\langle \{u_{i,j}\} \cup \mathsf{LM}_{\prec_{lex}}(\widetilde{\mathscr{I}_r} \cap \mathbb{K}(\mathfrak{a})[X]) \right\rangle \\ &= \left\langle \{u_{i,j}\} \cup \mathsf{LM}_{\prec_{lex}}(\mathscr{I}_r) \right\rangle.\end{aligned}$$

Therefore, $\frac{\mathbb{K}(\mathfrak{a})[U,X]}{\mathsf{LM}_{\prec_{lex}}(\widetilde{\mathscr{I}_r})}$ is isomorphic (as a graded $\mathbb{K}(\mathfrak{a})$-algebra) to $\frac{\mathbb{K}(\mathfrak{a})[X]}{\mathsf{LM}_{\prec_{lex}}(\mathscr{I}_r)}$. Thus

$$\mathsf{HS}_{\mathsf{LM}_{\prec_{lex}}(\mathscr{I}_r)}(t) = \mathsf{wHS}_{\mathsf{LM}_{\prec_{lex}}(\widetilde{\mathscr{I}_r})}(t),$$

and hence

$$\mathsf{HS}_{\mathscr{I}_r}(t) = \mathsf{wHS}_{\widetilde{\mathscr{I}_r}}(t).$$

□

In the sequel, $A_r(t)$ denotes the $r\times r$ matrix whose (i,j)-entry is $\sum_k \binom{m-i}{k}\binom{n-j}{k}t^k$. The following theorem is the main result of this section:

Theorem 10. *The dimension of the ideal $\mathscr{I}_r$ is $k-(n-r)(m-r)$ and its Hilbert series is*

$$\mathsf{HS}_{\mathscr{I}_r}(t)=\frac{\det\left(A_r(t^D)\right)(1-t^D)^{(n-r)(m-r)}}{t^{D\binom{r}{2}}(1-t)^k}.$$

Proof. According to Conca and Herzog (1994, Corollary 1) (and references therein), the ideal $\mathscr{J}_r$ seen as an ideal of $\mathbb{K}[U]$ has dimension $(m+n-r)r$ and its Hilbert series (for the standard gradation: $\deg(u_{i,j})=1$) is the power series expansion of

$$\mathsf{HS}_{\mathscr{J}_r\subset\mathbb{K}[U]}(t)=\frac{\det A_r(t)}{t^{\binom{r}{2}}(1-t)^{(n+m-r)r}}.$$

By putting a weight D on each variable $u_{i,j}$ (i.e. $\deg(u_{i,j})=D$), the weighted Hilbert series of $\mathscr{J}_r\subset\mathbb{K}[U]$ is

$$\mathsf{wHS}_{\mathscr{J}_r\subset\mathbb{K}[U]}(t)=\frac{\det A_r(t^D)}{t^{D\binom{r}{2}}(1-t^D)^{(n+m-r)r}}.$$

By considering $\mathscr{J}_r$ as an ideal of $\mathbb{K}(\mathfrak{b},\mathfrak{c})[U,X]$, the dimension becomes $k+(m+n-r)r$ and its weighted Hilbert series is

$$\mathsf{wHS}_{\mathscr{J}_r\subset\mathbb{K}(\mathfrak{b},\mathfrak{c})[U,X]}(t)=\frac{\det A_r(t^D)}{t^{D\binom{r}{2}}(1-t)^k(1-t^D)^{(n+m-r)r}}.$$

According to Lemma 8, for each $\ell\le nm$, the polynomial g_ℓ does not divide zero in the ring $\mathbb{K}(\mathfrak{b},\mathfrak{c})[U,X]/(\mathscr{J}_r+\langle g_1,\dots,g_{\ell-1}\rangle)$. This implies the following relations:

$$\begin{aligned}\dim\left(\mathscr{J}_r+\langle g_1,\dots,g_\ell\rangle\right) &= \dim\left(\mathscr{J}_r+\langle g_1,\dots,g_{\ell-1}\rangle\right)-1\\ \mathsf{wHS}_{\mathscr{J}_r+\langle g_1,\dots,g_\ell\rangle}(t) &= (1-t^D)\,\mathsf{wHS}_{\mathscr{J}_r+\langle g_1,\dots,g_{\ell-1}\rangle}(t).\end{aligned}$$

Therefore the dimension of $\widetilde{\mathscr{J}}_r$ is $k-nm+(n+m-r)r$ and its quasi-homogeneous Hilbert series is

$$\mathsf{wHS}_{\widetilde{\mathscr{J}}_r}(t)=\frac{\det\left(A_r(t^D)\right)}{t^{D\binom{r}{2}}(1-t)^k(1-t^D)^{(n+m-r)r-nm}}=\frac{\det\left(A_r(t^D)\right)(1-t^D)^{(n-r)(m-r)}}{t^{D\binom{r}{2}}(1-t)^k}.$$

By Corollary 6, the ideal $\widetilde{\mathscr{I}_r}$ has the same weighted Hilbert series. Finally, by Lemma 9, the Hilbert series of $\mathscr{I}_r=\widetilde{\mathscr{I}_r}\cap\mathbb{K}(\mathfrak{a})[X]$ is the same as that of $\widetilde{\mathscr{I}_r}$. $\square$

Corollary 11. *The degree of the ideal $\mathscr{I}_r$ is:*

$$\begin{aligned}\mathsf{DEG}(\mathscr{I}_r) &= D^{(n-r)(m-r)}\prod_{i=0}^{m-r-1}\frac{i!(n+i)!}{(m-1-i)!(n-r+i)!}\\ &= D^{(n-r)(m-r)}\prod_{i=0}^{m-r-1}\frac{\binom{n+m-r-1}{r+i}}{\binom{n+m-r-1}{i}}.\end{aligned}$$

Proof. From Fulton (1997, Example 14.4.14), the degree of the ideal $\mathscr{J}_r$ is

$$\prod_{i=0}^{m-r-1} \frac{i!(n+i)!}{(m-1-i)!(n-r+i)!}.$$

Since the degree is equal to the numerator of the Hilbert series of $\mathscr{J}_r$ evaluated at $t=1$,

$$\det A_r(1) = \prod_{i=0}^{m-r-1} \frac{i!(n+i)!}{(m-1-i)!(n-r+i)!}.$$

By Theorem 10, the Hilbert series of $\mathscr{I}_r$ is

$$\begin{aligned}\mathsf{HS}_{\mathscr{I}_r}(t) &= \frac{\det\left(A_r(t^D)\right)(1-t^D)^{(n-r)(m-r)}}{t^{D\binom{r}{2}}(1-t)^k} \\ &= \frac{\det\left(A_r(t^D)\right)(1+t+\cdots+t^{D-1})^{(n-r)(m-r)}}{t^{D\binom{r}{2}}(1-t)^{k-(n-r)(m-r)}}.\end{aligned}$$

Thus, the evaluation of the numerator in $t=1$ yields

$$\mathsf{DEG}(\mathscr{I}_r) = D^{(n-r)(m-r)} \prod_{i=0}^{m-r-1} \frac{i!(n+i)!}{(m-1-i)!(n-r+i)!}.$$

To prove the second equality, notice that

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

By substituting i by $m-r-1-i$, we obtain that

$$\begin{aligned}\prod_{i=0}^{m-r-1}(n+m-r-i-1)! &= \prod_{i=0}^{m-r-1}(n+i)! \\ \prod_{i=0}^{m-r-1}(r+i)! &= \prod_{i=0}^{m-r-1}(m-i-1)! \\ \prod_{i=0}^{m-r-1}(n+m-2r-i-1)! &= \prod_{i=0}^{m-r-1}(n-r+i)!.\end{aligned}$$

Consequently,

$$\prod_{i=0}^{m-r-1} \frac{i!(n+i)!}{(m-1-i)!(n-r+i)!} = \prod_{i=0}^{m-r-1} \frac{\binom{n+m-r-1}{r+i}}{\binom{n+m-r-1}{i}}.$$

□

5. The over-determined case

To study the over-determined case ($k < (n-r)(m-r)$), we need to assume a variant of Fröberg's conjecture (Fröberg, 1985):

Conjecture 12. *Let $\mathscr{J}_{\ell,i}$ denote the vector space of quasi-homogeneous polynomials of weight degree i in $\mathscr{J}_r + \langle g_1,\dots,g_\ell\rangle$. Then the linear map*

$$\begin{array}{ccc}\mathbb{K}(\mathfrak{b},\mathfrak{c})[U,X]_i/\mathscr{J}_{\ell,i} & \longrightarrow & \mathbb{K}(\mathfrak{b},\mathfrak{c})[U,X]_{i+D}/\mathscr{J}_{\ell,i+D} \\ f & \longmapsto & fg_{\ell+1}\end{array}$$

has maximal rank, i.e. it is either injective or onto.

Remark 13. If $k+(n+m-r)r-\ell>0$, then Conjecture is proved by Lemma 8: $g_{\ell+1}$ does not divide zero in $\mathbb{K}(\mathfrak{b},\mathfrak{c})[U,X]/\left(\mathscr{J}_r+\langle g_1,\dots,g_\ell\rangle\right)$ and hence the linear map is injective for all $i\in\mathbb{N}$.

Notation. Given a power series $S(t)\in\mathbb{Z}[[t]]$, we let $[S(t)]_+$ denote the power series obtained by truncated $S(t)$ at its first non positive coefficient.

Lemma 14. *If Conjecture 13 is true, then the Hilbert series of $\mathscr{J}_r+\langle g_1,\dots,g_{\ell+1}\rangle$ is*

$$\mathsf{wHS}_{\mathscr{J}_r+\langle g_1,\dots,g_{\ell+1}\rangle}(t)=\left[(1-t^D)\,\mathsf{wHS}_{\mathscr{J}_r+\langle g_1,\dots,g_\ell\rangle}(t)\right]_+.$$

Proof. In this proof, for simplicity of notation, we let R denote the ring $\mathbb{K}(\mathfrak{b},\mathfrak{c})[U,X]$. If $S(t)=\sum_{i\in\mathbb{N}}s_it^i\in\mathbb{Z}[[t]]$ is a power series, $[S(t)]_{\geq 0}$ denotes the series

$$[S(t)]_{\geq 0}=\sum_{i\in\mathbb{N}}\max(s_i,0)t^i.$$

Let $\mathsf{ann}(g_{\ell+1})$ be the ideal $\{f\in R: fg_{\ell+1}\in\mathscr{J}_r+\langle g_1,\dots,g_\ell\rangle\}$. For $i\in\mathbb{N}$, consider the following exact sequence:

$$\begin{aligned}0\to\mathsf{ann}(g_{\ell+1})_i\to R_i/\mathscr{J}_{\ell,i}\xrightarrow{\times g_{\ell+1}}R_{i+D}/\mathscr{J}_{\ell,i+D}\to&\\ \to R_{i+D}/\mathscr{J}_{\ell+1,i+D}\to 0.&\end{aligned}$$

By Conjecture 13, we obtain

$$\dim(\mathsf{ann}(g_{\ell+1})_i)=\max(0,\dim(R_i/\mathscr{J}_{\ell,i})-\dim(R_{i+D}/\mathscr{J}_{\ell,i+D})).$$

The alternate sum of the dimensions of the vector spaces occurring in an exact sequence is zero; it follows that

$$\begin{aligned}\dim(R_{i+D}/\mathscr{J}_{\ell+1,i+D}) &= \dim(R_{i+D}/\mathscr{J}_{\ell,i+D})-\dim(R_i/\mathscr{J}_{\ell,i})+\\ &\quad\max(0,\dim(R_i/\mathscr{J}_{\ell,i})-\dim(R_{i+D}/\mathscr{J}_{\ell,i+D}))\\ &= \max(0,\dim(R_{i+D}/\mathscr{J}_{\ell,i+D})-\dim(R_i/\mathscr{J}_{\ell,i})).\end{aligned}$$

Multiplying this identity by t^{i+D} yields

$$\begin{aligned}\left[t^{i+D}\right]\mathsf{wHS}_{\mathscr{J}_r+\langle g_1,\dots,g_{\ell+1}\rangle}(t) &= \dim\left(R_{i+D}/\mathscr{J}_{\ell+1,i+D)}\right)\\ &= \max\left(0,\dim(R_{i+D}/\mathscr{J}_{\ell,i+D})-\dim(R_i/\mathscr{J}_{\ell,i})\right)\\ &= \max\left(0,[t^{i+D}](1-t^D)\,\mathsf{wHS}_{\mathscr{J}_r+\langle g_1,\dots,g_\ell\rangle}(t)\right)\\ &= [t^{i+D}]\left[(1-t^D)\,\mathsf{wHS}_{\mathscr{J}_r+\langle g_1,\dots,g_\ell\rangle}(t)\right]_{\geq 0}.\end{aligned}$$

Since any monomial in $\mathbb{K}(\mathfrak{a})[X,U]$ of weight degree greater that D is a multiple of a monomial of weight degree D, we deduce that if there exists $i_0\geq D$ such that

$$\left[t^{i_0}\right]\mathsf{wHS}_{\mathscr{J}_r+\langle g_1,\dots,g_{\ell+1}\rangle}(t)=0,$$

then for all $i>i_0$, $\left[t^i\right]\mathsf{wHS}_{\mathscr{J}_r+\langle g_1,\dots,g_{\ell+1}\rangle}(t)=0$. Therefore

$$\left[t^{i+D}\right]\mathsf{wHS}_{\mathscr{J}_r+\langle g_1,\dots,g_{\ell+1}\rangle}(t)=[t^{i+D}]\left[(1-t^D)\,\mathsf{wHS}_{\mathscr{J}_r+\langle g_1,\dots,g_\ell\rangle}(t)\right]_+,$$

Finally, by summing over i, we get

$$\mathsf{wHS}_{\mathscr{I}_r+\langle g_1,\ldots,g_{\ell+1}\rangle}(t) = \left[(1-t^D)\mathsf{HS}_{\mathscr{I}_r+\langle g_1,\ldots,g_\ell\rangle}(t)\right]_+.$$

□

Theorem 15. *If Conjecture 13 is true, then the Hilbert series of $\mathscr{I}_r$ is*

$$\mathsf{HS}_{\mathscr{I}_r}(t) = \left[(1-t^D)^{(n-r)(m-r)}\frac{\det\left(A_r(t^D)\right)}{t^{D\binom{r}{2}}(1-t)^k}\right]_+,$$

where $A_r(t)$ is the $r\times r$ matrix whose (i,j)-entry is $\displaystyle\sum_{k=0}^{\min(m-i,n-j)}\binom{m-i}{k}\binom{n-j}{k}t^k$.

Proof. By applying nm times Lemma 14, we obtain that

$$\mathsf{wHS}_{\widetilde{\mathscr{I}_r}}(t) = \left[(1-t^D)\left[(1-t^D)\ldots\left[(1-t^D)\frac{\det A_r(t^D)}{t^{D\binom{r}{2}}(1-t)^k(1-t^D)^{(n+m-r)r}}\right]_+\ldots\right]_+\right]_+.$$

Let $S=\sum_{0\leq i}a_it^i\in\mathbb{Z}[[t]]$ be a power series such that $a_0>0$, and let $i_0\in\mathbb{N}\cup\{\infty\}$ be defined as

$$i_0=\begin{cases}\infty \text{ if for all } i\geq 0, a_i>0;\\ \min(\{i\mid a_i\leq 0\}) \text{ otherwise.}\end{cases}$$

Therefore, $[S(t)]_+=\sum_{0\leq i<i_0}a_it^i$. By convention, for $i<0$, we put $a_i=0$. Then

$$\begin{array}{rcl}(1-t^D)S(t) &=& \sum_{0\leq i}(a_i-a_{i-D})t^i\\ (1-t^D)\left[S(t)\right]_+ &=& \sum_{0\leq i<i_0}(a_i-a_{i-D})t^i\end{array}.$$

Consequently, the coefficients of $(1-t^D)S(t)$ and of $(1-t^D)\left[S(t)\right]_+$ are equal up to the index i_0.

- If $i_0=\infty$, then $(1-t^D)S(t)=(1-t^D)\left[S(t)\right]_+$ and hence

$$\left[(1-t^D)S(t)\right]_+=\left[(1-t^D)\left[S(t)\right]_+\right]_+;$$

- if $i_0<\infty$, then a_{i_0-D} is positive and thus $a_{i_0}-a_{i_0-D}$ is negative. Let i_1 be the index of the first non-positive coefficient of $(1-t^D)S(t)$. Then $i_1<i_0$, and hence $\left[(1-t^D)S(t)\right]_+=\left[(1-t^D)\left[S(t)\right]_+\right]_+$.

  Therefore, for all power series $S\in\mathbb{Z}[[t]]$ such that $S(0)>0$, we have

$$\left[(1-t^D)\left[S\right]_+\right]_+=\left[(1-t^D)S\right]_+.$$

Consequently, an induction shows that

$$\mathsf{wHS}_{\widetilde{\mathscr{I}_r}}(t) = \left[(1-t^D)^{(n-r)(m-r)}\frac{\det A(t^D)}{t^{D\binom{r}{2}}(1-t)^k}\right]_+.$$

Then, by Corollary 6, $\mathsf{wHS}_{\widetilde{\mathscr{I}_r}}(t)=\mathsf{wHS}_{\widetilde{\mathscr{I}_r}}(t)$. Finally, by Lemma 9, we conclude that $\mathsf{HS}_{\mathscr{I}_r}(t)=\mathsf{wHS}_{\widetilde{\mathscr{I}_r}}(t)$. □

6. Complexity analysis

Using the previous results on the Hilbert series of $\mathscr{I}_r$, we analyze now the arithmetic complexity of solving the generalized MinRank problem with Gröbner bases algorithms. In the first part of this section (until Section 6.2), we consider the homogeneous MinRank problem (i.e. the polynomials $f_{i,j}$ are homogeneous).

Computing a Gröbner basis of the ideal $\varphi_{\mathbf{a}}(\mathscr{I}_r)$ for the lexicographical ordering yields an explicit description of the set of points V such that the matrix

$$\varphi_{\mathbf{a}}(\mathscr{M}) = \begin{pmatrix} \varphi_{\mathbf{a}}(f_{1,1}) & \dots & \varphi_{\mathbf{a}}(f_{1,m}) \\ \vdots & \ddots & \vdots \\ \varphi_{\mathbf{a}}(f_{n,1}) & \dots & \varphi_{\mathbf{a}}(f_{n,m}) \end{pmatrix}$$

has rank less than $r+1$. In this section, we study the complexity of this computation when $\mathbf{a} \in \mathbb{K}^{nm\binom{k+D-1}{D}}$ is generic (i.e. $\mathbf{a}$ belongs to a given non-empty Zariski open subset of $\overline{\mathbb{K}}^{nm\binom{k+D-1}{D}}$) by using the theoretical results from Sections 4 and 5. We focus on the 0-dimensional cases $k = (n-r)(m-r)$ and $k < (n-r)(m-r)$ (over-determined case). Therefore, the set of points where the evaluation of the matrix $\varphi_{\mathbf{a}}(\mathscr{M})$ has rank less than $r+1$ is finite.

In order to compute this set of points, we use the following strategy:

- compute a Gröbner basis of $\varphi_{\mathbf{a}}(\mathscr{I}_r)$ for the *grevlex* (graded reverse lexicographical) ordering with the F_5 algorithm (Faugère, 2002);
- convert it into a lexicographical Gröbner basis of $\varphi_{\mathbf{a}}(\mathscr{I}_r)$ by using the FGLM algorithm (Faugère et al., 1993; Faugère and Mou, 2011).

First, we recall some results about the complexity of the algorithms F_5 and FGLM. The two quantities which allow us to estimate their complexity are respectively the *degree of regularity* and the *degree* of the ideal. The degree of regularity of a 0-dimensional homogeneous ideal I is the smallest integer d such that all monomials of degree d are in I; it is independent on the monomial ordering and it bounds the degrees of the polynomials in a minimal Gröbner basis of I. Moreover, in the 0-dimensional case, the Hilbert series is a polynomial from which the degree of regularity can be read off: $\mathbb{D}_{\text{reg}}(I) = \deg(\mathsf{HS}_I(t)) + 1$.

In the sequel, ω denotes a feasible exponent for the matrix multiplication (i.e. a number such that there exists an deterministic algorithm which computes the product of two $n \times n$ matrices in $O(n^\omega)$ arithmetic operations in $\mathbb{K}$). The best known bound on this exponent is $\omega < 2.3727$ (Williams, 2011).

The following proposition and its proof are a variant of a result known in the context of semi-regular sequences (see e.g. Lazard (1983) and Faugère (1999) for the relation between Gröbner basis computation and linear algebra, Bardet et al. (2004, Proposition 10) and Bardet (2004, Section 3.4) for the complexity analysis).

Proposition 16 (Bardet (2004); Bardet et al. (2004))**.** *Let $h_1, \dots, h_\ell \in \mathbb{K}[x_1, \dots, x_k]$ be homogeneous polynomials of degrees $d_1, \dots, d_\ell$, and $I = \langle h_1, \dots, h_\ell \rangle$. The complexity of computing a Gröbner basis of I for a monomial ordering $\prec$ is upper bounded by*

$$O\left(\left(\binom{k+\mathbb{D}_{\text{reg}}(I)}{\mathbb{D}_{\text{reg}}(I)} - \mathsf{DEG}(I)\right)^{\omega-2} \binom{k+\mathbb{D}_{\text{reg}}(I)}{\mathbb{D}_{\text{reg}}(I)} \sum_{i=1}^{\ell} \binom{k+\mathbb{D}_{\text{reg}}(I)-d_i}{\mathbb{D}_{\text{reg}}(I)-d_i}\right).$$

Proof. Since I is homogeneous, a Gröbner basis can be obtained by computing the row echelon form of the so-called *Macaulay matrix* of the system up to degree $\mathbb{D}_{\mathrm{reg}}(I)$. This matrix is constructed as follows:

- the rows are indexed by the products th_i, where $1 \le i \le \ell$ and $t \in \mathbb{K}[x_1,\dots,x_k]$ is a monomial of degree at most $\mathbb{D}_{\mathrm{reg}}(I) - d_i$;
- the columns are indexed by the monomials $m \in \mathbb{K}[x_1,\dots,x_k]$ of degree at most $\mathbb{D}_{\mathrm{reg}}(I)$ and are sorted in descending order with respect to $\prec$;
- the coefficient at the intersection of the row th_i and the column m is the coefficient of m in the polynomial th_i.

The number of columns of this matrix is the number of monomials in $\mathbb{K}[x_1,\dots,x_k]$ of degree at most $\mathbb{D}_{\mathrm{reg}}(I)$, namely $\binom{k+\mathbb{D}_{\mathrm{reg}}(I)}{\mathbb{D}_{\mathrm{reg}}(I)}$. The number of rows is $\sum_{i=1}^{\ell}\binom{k+\mathbb{D}_{\mathrm{reg}}(I)-d_i}{\mathbb{D}_{\mathrm{reg}}(I)-d_i}$, and its rank is equal to $\left(\binom{k+\mathbb{D}_{\mathrm{reg}}(I)}{\mathbb{D}_{\mathrm{reg}}(I)} - \mathsf{DEG}(I)\right)$.

According to Storjohann (2000, Theorem 2.10), the complexity of computing the row echelon form of a $p \times q$ matrix of rank r is upper bounded by $O(r^{\omega-2}pq)$.

Consequently, the complexity of computing a Gröbner basis of I is upper bounded by

$$O\left(\left(\binom{k+\mathbb{D}_{\mathrm{reg}}(I)}{\mathbb{D}_{\mathrm{reg}}(I)} - \mathsf{DEG}(I)\right)^{\omega-2}\binom{k+\mathbb{D}_{\mathrm{reg}}(I)}{\mathbb{D}_{\mathrm{reg}}(I)}\sum_{i=1}^{\ell}\binom{k+\mathbb{D}_{\mathrm{reg}}(I)-d_i}{\mathbb{D}_{\mathrm{reg}}(I)-d_i}\right).$$

□

Remark 17. Notice that

$$\begin{aligned}\binom{k+\mathbb{D}_{\mathrm{reg}}(I)}{\mathbb{D}_{\mathrm{reg}}(I)} - \mathsf{DEG}(I) &\le \binom{k+\mathbb{D}_{\mathrm{reg}}(I)}{\mathbb{D}_{\mathrm{reg}}(I)}\\ \sum_{i=1}^{\ell}\binom{k+\mathbb{D}_{\mathrm{reg}}(I)-d_i}{\mathbb{D}_{\mathrm{reg}}(I)-d_i} &\le \ell\binom{k+\mathbb{D}_{\mathrm{reg}}(I)}{\mathbb{D}_{\mathrm{reg}}(I)}.\end{aligned}$$

Therefore, the complexity of computing a Gröbner basis of I can also be upper bounded by the simpler expression $O\left(\ell\binom{k+\mathbb{D}_{\mathrm{reg}}(I)}{\mathbb{D}_{\mathrm{reg}}(I)}^{\omega}\right)$.

Lemma 18. *If $k = (n-r)(m-r)$, then the degree of regularity of $\mathscr{I}_r$ is*

$$\mathbb{D}_{\mathrm{reg}}(\mathscr{I}_r) = Dr(m-r) + (D-1)k + 1.$$

Proof. According to Theorem 10, the Hilbert series of $\mathscr{I}_r$ is

$$\mathsf{HS}_{\mathscr{I}_r}(t) = \frac{\det A_r(t^D)(1-t^D)^{(n-r)(m-r)}}{t^{D\binom{r}{2}}(1-t)^k}.$$

By definition of the matrix $A_r(t)$, the highest degree on each row is reached on the diagonal. Thus, the degree of $\det(A_r(t))$ is the degree of the product of its diagonal elements:

$$\deg(\det(A_r(t))) = \sum_{i=1}^{r}(\min(n,m)-i) = rm - \binom{r+1}{2}.$$

Therefore, we can compute the degree of the Hilbert series which is a polynomial since the ideal is 0-dimensional:

$$\begin{aligned}\mathbb{D}_{\mathrm{reg}}(\mathscr{I}_r) &= \deg(\mathsf{HS}_{\mathscr{I}_r}(t))+1\\ &= \deg(\det(A_r(t^D)))+D(n-r)(m-r)-D\tbinom{r}{2}-k+1\\ &= D(rm-\tbinom{r+1}{2}+nm-(n+m-r)r-\tbinom{r}{2})-k+1\\ &= Dr(m-r)+(D-1)k+1.\end{aligned}$$

□

Corollary 19. *If $k=(n-r)(m-r)$, then there exists a non-empty Zariski open subset $O\subset \overline{\mathbb{K}}^{nm\binom{D-1+k}{D}}$ such that for all $\mathbf{a}\in O$, the degree of regularity of $\varphi_{\mathbf{a}}(\mathscr{I}_r)$ is*

$$\mathbb{D}_{\mathrm{reg}}(\varphi_{\mathbf{a}}(\mathscr{I}_r)) = Dr(m-r)+(D-1)k+1.$$

Proof. According to Lemma 4, there exists a Zariski open subset O such that for all $\mathbf{a}\in O$, $\mathsf{LM}(\mathscr{I}_r)=\mathsf{LM}(\varphi_{\mathbf{a}}(\mathscr{I}_r))$. Consequently, the polynomials in minimal Gröbner bases of $\mathscr{I}_r$ and $\varphi_{\mathbf{a}}(\mathscr{I}_r)$ have the same leading monomials. Since the degree of regularity is the highest degree of the polynomials in a minimal Gröbner basis, we have $\mathbb{D}_{\mathrm{reg}}(\varphi_{\mathbf{a}}(\mathscr{I}_r))=\mathbb{D}_{\mathrm{reg}}(\mathscr{I}_r)$. Lemma 18 concludes the proof. □

The degree of regularity governs the complexity of the Gröbner basis computation with respect to the grevlex ordering. The complexity of the algorithm FGLM is upper bounded by $O(k\cdot \mathsf{DEG}(I)^3)$ which is polynomial in the degree of the ideal (Faugère et al., 1993; Faugère and Mou, 2011).

We can now state the main complexity result:

Theorem 20. *There exists a non-empty Zariski open subset $O\subset \overline{\mathbb{K}}^{nm\binom{D-1+k}{D}}$ such that for any $\mathbf{a}\in O$, the arithmetic complexity of computing a lexicographical Gröbner basis of the ideal generated by the $(r+1)\times(r+1)$-minors of the matrix $\varphi_{\mathbf{a}}(\mathscr{M})$ is upper bounded by*

$$O\left(\binom{n}{r+1}\binom{m}{r+1}\binom{\mathbb{D}_{\mathrm{reg}}(\varphi_{\mathbf{a}}(\mathscr{I}_r)+k}{k}^{\omega}+k\left(\mathsf{DEG}(\varphi_{\mathbf{a}}(\mathscr{I}_r))\right)^3\right),$$

where $2\leq\omega\leq 3$ is a feasible exponent for the matrix multiplication, and

- *if $k=(n-r)(m-r)$, then*

$$\mathbb{D}_{\mathrm{reg}}(\varphi_{\mathbf{a}}(\mathscr{I}_r) = \deg(\mathsf{HS}_{\varphi_{\mathbf{a}}(\mathscr{I}_r)}(t))+1 = Dr(m-r)+(D-1)k+1$$

  and $\mathsf{DEG}(\varphi_{\mathbf{a}}(\mathscr{I}_r))=\mathsf{HS}_{\varphi_{\mathbf{a}}(\mathscr{I}_r)}(1)=D^{nm-(n+m-r)r}\prod_{i=0}^{m-r-1}\frac{i!(n+i)!}{(m-1-i)!(n-r+i)!}$.
- *if $k<(n-r)(m-r)$, then assuming that Conjecture 13 is true,*

$$\mathbb{D}_{\mathrm{reg}}(\varphi_{\mathbf{a}}(\mathscr{I}_r) = \deg(\mathsf{HS}_{\varphi_{\mathbf{a}}(\mathscr{I}_r)}(t))+1$$

  and $\mathsf{DEG}(\varphi_{\mathbf{a}}(\mathscr{I}_r))=\mathsf{HS}_{\varphi_{\mathbf{a}}(\mathscr{I}_r)}(1)$ where

$$\mathsf{HS}_{\varphi_{\mathbf{a}}(\mathscr{I}_r)}(t)=\left[(1-t^D)^{nm-(n+m-r)r}\frac{\det A(t^D)}{t^{D\binom{r}{2}}(1-t)^k}\right]_+.$$

Proof. The number of $(r+1)$-minors of the matrix $\varphi_a(\mathscr{M})$ is $\binom{n}{r+1}\binom{m}{r+1}$. Consequently, the theorem is a straightforward consequence of the bounds on the complexity of the F_5 algorithm

(Proposition 16) and of the FGLM algorithm (Faugère et al., 1993; Faugère and Mou, 2011), together with the formulas for the degree of regularity (Corollary 19) and for the degree (Corollary 11). $\square$

Remark 21. There exists a polynomial $h(\mathfrak{a})$ in $\mathbb{Z}[\mathfrak{a}]$ when the characteristic of $\mathbb{K}$ is 0, such that

$$h(\mathbf{a}) \neq 0 \Rightarrow \mathbf{a} \in O.$$

Also note that this polynomial does not depend on the field $\mathbb{K}$: if $\mathbb{K} = \mathbb{F}_q$ is a finite field ($q = p^e$), then the polynomial $\bar{h}(\mathfrak{a})$ (where all coefficients are taken modulo p) verifies the requested property. Schwartz-Zippel's Lemma states that, if $\mathbf{a}$ is chosen uniformly at random in $\mathbb{F}_q^{nm\binom{D-1+k}{D}}$, the probability that $h(\mathbf{a}) = 0$ is upper bounded by $\deg(h)/q$ and therefore tends towards 0 when the cardinality q of the field tends to infinity. This explains why these complexity results can be used for practical applications when $\mathsf{char}(\mathbb{K}) = 0$ or $\mathbb{K}$ is a sufficiently large finite field.

6.1. *Positive dimension*

When $k > (n-r)(m-r)$, the ideal $\mathscr{I}_r$ has positive dimension. To achieve complexity bounds in that case, we need upper bounds on the maximal degree in a minimal Gröbner basis of $\mathscr{I}_r$.

Lemma 22. *If $k > (n-r)(m-r)$, then the maximal degree in a minimal Gröbner basis of $\mathscr{I}_r$ is bounded by*

$$Dr(m-r) + (D-1)(n-r)(m-r) + 1.$$

Proof. Consider the ideal J obtained by specializing the last $k-(n-r)(m-r)$ variables to zero in $\mathscr{I}_r$. We prove now that $\mathsf{LM}(\mathscr{I}_r) = \mathsf{LM}(J)$. First, notice that for the grevlex ordering, $\mathsf{LM}(J) \subset \mathsf{LM}(\mathscr{I}_r)$. According to Theorem 10, the Hilbert series of the ideal $J \cap \mathbb{K}(\mathfrak{a})[x_1,\dots,x_{(n-r)(m-r)}]$ is equal to

$$\frac{\det A_r(t^D)(1-t^D)^{(n-r)(m-r)}}{t^{D\binom{r}{2}}(1-t)^{(n-r)(m-r)}}.$$

By construction, $J \subset \mathbb{K}(\mathfrak{a})[x_1,\dots,x_{(n-r)(m-r)}]$, thus the Hilbert series of J as an ideal of the ring $\mathbb{K}(\mathfrak{a})[x_1,\dots,x_k]$ is equal to

$$\frac{\det A_r(t^D)(1-t^D)^{(n-r)(m-r)}}{t^{D\binom{r}{2}}(1-t)^{k}},$$

which is equal to the Hilbert series of $\mathscr{I}_r$.

Since $\mathsf{HS}_J(t) = \mathsf{HS}_{\mathscr{I}_r}(t)$ and $\mathsf{LM}(J) \subset \mathsf{LM}(\mathscr{I}_r)$, we can deduce that $\mathsf{LM}(J) = \mathsf{LM}(\mathscr{I}_r)$.

Consequently, the leading monomials in minimal Gröbner bases of J and $\mathscr{I}_r$ are the same. Hence, the polynomials in both Gröbner bases have the same degrees since they are homogeneous.

Finally, notice that the Gröbner basis of the ideal J is the same as that of the ideal $J \cap \mathbb{K}(\mathfrak{a})[x_1,\dots,x_{(n-r)(m-r)}]$ which, by Lemma 18, is a zero-dimensional ideal whose degree of regularity is $Dr(m-r)+(D-1)(n-r)(m-r)+1$. Therefore the maximal degree of the polynomials in the minimal reduced Gröbner basis of $\mathscr{I}_r$ is bounded by $Dr(m-r)+(D-1)(n-r)(m-r)+1$. $\square$

Using exactly the same argumentation as in the proof of Corollary 19, we deduce that

Corollary 23. *If $k > (n-r)(m-r)$, then there exists a non-empty Zariski open subset $O \subset \overline{\mathbb{K}}^{nm\binom{D-1+k}{D}}$ such that, for $\mathbf{a} \in O$, the maximal degree of the polynomials in a minimal grevlex Gröbner basis of $\varphi_{\mathbf{a}}(\mathscr{I}_r)$ is*

$$Dr(m-r) + (D-1)(n-r)(m-r) + 1.$$

Theorem 24. *If $k > (n-r)(m-r)$, then there exists a non-empty Zariski open subset $O \subset \overline{\mathbb{K}}^{nm\binom{D-1+k}{D}}$ such that for any $\mathbf{a} \in O$, the arithmetic complexity of computing a grevlex Gröbner basis of $\varphi_{\mathbf{a}}(\mathscr{I}_r)$ is upper bounded by*

$$O\left(\binom{n}{r+1}\binom{m}{r+1}\binom{Dr(m-r)+(D-1)(n-r)(m-r)+1+k}{k}^{\omega}\right).$$

Proof. This is a consequence of Proposition 16 and Corollary 23. □

6.2. The 0-dimensional affine case

For practical applications, the affine case (i.e. when the entries of the input matrix $\mathscr{M}$ are affine polynomials of degree D) is more often encountered than the homogeneous one. In this case, the matrix $\mathscr{M}$ is defined as follows

$$\mathscr{M} = \begin{pmatrix} f_{1,1} & \cdots & f_{1,m} \\ \vdots & \ddots & \vdots \\ f_{n,1} & \cdots & f_{n,m} \end{pmatrix} \qquad f_{i,j} = \sum_{\ell=0}^{D} \sum_{t \in \mathrm{Mon}(\ell,k)} \mathfrak{a}_t^{(i,j)} t.$$

We show in this section that the complexity results (Theorems 20 and 24) still hold in the affine case. This is achieved by considering the homogenized system:

Definition 25. (Cox et al., 1997, Chapter 8, §2, Proposition 7) Let $(q_1, \ldots, q_\ell) \in \mathbb{K}[x_1, \ldots, x_k]^\ell$ be an affine polynomial system. We let $(\widetilde{q_1}, \ldots, \widetilde{q_\ell}) \in \mathbb{K}[x_1, \ldots, x_k, x_{k+1}]^\ell$ denote its *homogenized system* defined by

$$\forall i, \text{ s.t. } 1 \le i \le \ell, \widetilde{q_i}(x_1, \ldots, x_k, x_{k+1}) = x_{k+1}^{\deg(q_i)} q_i\left(\frac{x_1}{x_{k+1}}, \ldots, \frac{x_k}{x_{k+1}}\right).$$

Notice that if an affine polynomial system has solutions, then the dimension of the ideal generated by its homogenized system is positive.

The study of the homogenized system is motivated by the fact that, for the grevlex ordering, the dehomogenization of a Gröbner basis of $\langle \widetilde{q_1}, \ldots, \widetilde{q_\ell} \rangle$ is a Gröbner basis of $\langle q_1, \ldots, q_\ell \rangle$. Therefore, in order to compute a Gröbner basis of the affine system, it is sufficient to compute a Gröbner basis of the homogenized system (for which we have complexity estimates by Theorems 20 and 24).

To estimate the complexity of the change of ordering, we need bounds on the degree of the ideal in the affine case:

Lemma 26. *The degree of the ideal $\langle q_1, \ldots, q_\ell \rangle$ is upper bounded by that of $\langle \widetilde{q_1}, \ldots, \widetilde{q_\ell} \rangle$.*

Proof. The rings $\mathbb{K}[x_1, \ldots, x_k]/\langle q_1, \ldots, q_\ell \rangle$ and $\mathbb{K}[x_1, \ldots, x_k, x_{k+1}]/\langle \widetilde{q_1}, \ldots, \widetilde{q_\ell}, x_{k+1} - 1 \rangle$ are isomorphic. Therefore the degrees of the ideals $\langle q_1, \ldots, q_\ell \rangle$ and $\langle \widetilde{q_1}, \ldots, \widetilde{q_\ell}, x_{k+1} - 1 \rangle$ are equal. Since

$\deg(x_{k+1}-1)=1$, we obtain:

$$\begin{aligned}\mathsf{DEG}(\langle q_1,\dots,q_\ell\rangle) &= \mathsf{DEG}(\langle \widetilde{q}_1,\dots,\widetilde{q}_\ell, x_{k+1}-1\rangle)\\ &\le \mathsf{DEG}(\langle \widetilde{q}_1,\dots,\widetilde{q}_\ell\rangle).\end{aligned}$$

□

Lemma 27. *The degree of regularity with respect to the grevlex ordering of the ideal $\langle q_1,\dots,q_\ell\rangle$ is upper bounded by that of $\langle \widetilde{q}_1,\dots,\widetilde{q}_\ell\rangle$.*

Proof. Let χ denote the dehomogenization morphism:

$$\begin{aligned}\chi:\quad \mathbb{K}[x_1,\dots,x_{k+1}] &\longrightarrow \mathbb{K}[x_1,\dots,x_k]\\ f(x_1,\dots,x_k,x_{k+1}) &\longmapsto f(x_1,\dots,x_k,1)\end{aligned}$$

If G is a grevlex Gröbner basis of $\langle \widetilde{q}_1,\dots,\widetilde{q}_\ell\rangle$, then $\chi(G)$ is a grevlex Gröbner basis of $\langle q_1,\dots,q_\ell\rangle$ (this is a consequence of the following property of the grevlex ordering: $\forall f\in\mathbb{K}[x_1,\dots,x_{k+1}]$ homogeneous, $\mathsf{LM}(\chi(f))=\chi(\mathsf{LM}(f))$). Also, notice that for each $g\in G$, any relation $g=\sum_{i=1}^{\ell} q_i h_i$ gives a relation $\chi(g)=\sum_{i=1}^{\ell}\chi(q_i)\chi(h_i)$ of lower degree since

$$\deg(\chi(q_i)\chi(h_i))\le\deg(q_ih_i).$$

Consequently, a Gröbner basis of $\langle q_1,\dots,q_\ell\rangle$ can be obtained by computing the row echelon form of the Macaulay matrix of $(q_1,\dots,q_\ell)$ in degree $\mathbb{D}_{\mathrm{reg}}(\langle \widetilde{q}_1,\dots,\widetilde{q}_\ell\rangle)$. Therefore, the degree of regularity with respect to the grevlex ordering of the ideal $\langle q_1,\dots,q_\ell\rangle$ is upper bounded by that of $\langle \widetilde{q}_1,\dots,\widetilde{q}_\ell\rangle$. □

We can now state the main complexity result for the affine generalized MinRank problem:

Theorem 28. *Suppose that the matrix $\mathscr{M}$ contains generic affine polynomials of degree D:*

$$\mathscr{M}=\begin{pmatrix} f_{1,1} & \cdots & f_{1,m}\\ \vdots & \ddots & \vdots\\ f_{n,1} & \cdots & f_{n,m}\end{pmatrix}\qquad\qquad f_{i,j}=\sum_{\ell=0}^{D}\sum_{t\in\mathrm{Mon}(\ell,k)}\mathfrak{a}_t^{(i,j)}t.$$

There exists a non identically null polynomial $h\in\mathbb{K}[\mathfrak{a}]$ such that for any $\mathbf{a}\in\overline{\mathbb{K}}^{nm\binom{D+k}{D}}$ such that $h(\mathbf{a})\neq 0$, the overall arithmetic complexity of computing the set of points such that the matrix $\varphi_{\mathbf{a}}(\mathscr{M})$ has rank less than $r+1$ with Gröbner basis algorithms is upper bounded by

$$O\left(\binom{n}{r+1}\binom{m}{r+1}\binom{\mathbb{D}_{\mathrm{reg}}(\varphi_{\mathbf{a}}(\mathscr{I}_r))+k}{k}^{\omega}+k\left(\mathsf{DEG}(\varphi_{\mathbf{a}}(\mathscr{I}_r))\right)^3\right),$$

where $2\le\omega\le 3$ is a feasible exponent for the matrix multiplication and

- *if $k=(n-r)(m-r)$, then*

$$\mathbb{D}_{\mathrm{reg}}(\varphi_{\mathbf{a}}(\mathscr{I}_r))\le Dr(m-r)+(D-1)k+1,$$

$$\mathsf{DEG}(\varphi_{\mathbf{a}}(\mathscr{I}_r))\le D^{(n-r)(m-r)}\prod_{i=0}^{m-r-1}\frac{i!(n+i)!}{(m-1-i)!(n-r+i)!}.$$

- *if $k < (n-r)(m-r)$, then assuming that Conjecture 13 is true,*
$$\mathbb{D}_{\text{reg}}(\varphi_{\mathbf{a}}(\mathscr{I}_r)) \leq \deg(P(t)) + 1,$$
and $\mathsf{DEG}(\varphi_{\mathbf{a}}(\mathscr{I}_r)) \leq P(1)$ *where*
$$P(t) = \left[(1-t^D)^{(n-r)(m-r)} \frac{\det A(t^D)}{t^{D\binom{r}{2}}(1-t)^k} \right]_+ .$$

Proof. This is a direct consequence of Proposition 16, Lemma 26, Lemma 27 and the complexity of the FGLM algorithm (Faugère et al., 1993; Faugère and Mou, 2011) ($O(k\,\mathsf{DEG}(\varphi_{\mathbf{a}}(\mathscr{I}_r)^3))$). □

7. Case studies

The aim of this section is to compare the complexity of the grevlex Gröbner basis computation with the degree of the ideal in the 0-dimensional case (i.e. the number of solutions of the MinRank problem counted with multiplicities). Since the "arithmetic" size (i.e. the number of coefficients) of the lexicographical Gröbner basis is close to the degree of the ideal in the 0-dimensional case, it is interesting to identify families of parameters for which the arithmetic complexity of the computation is polynomial in this degree under genericity assumptions.

Throughout this section, we focus on the 0-dimensional case: $k = (n-r)(m-r)$. Under genericity assumptions, we recall that, by Corollary 11 and Lemma 18,

$$\begin{aligned} \mathbb{D}_{\text{reg}} &= Dr(m-r) + (D-1)k + 1 \\ \mathsf{DEG} &= D^{(n-r)(m-r)} \prod_{i=0}^{m-r-1} \frac{i!(n+i)!}{(m-1-i)!(n-r+i)!}. \end{aligned}$$

According to Theorem 28, the complexity of the computation of the grevlex Gröbner basis is then upper bounded by

$$O\left(\binom{n}{r+1} \binom{m}{r+1} \binom{Dr(m-r) + (D-1)k + 1}{k}^{\omega} + k\left(\mathsf{DEG}\left(\varphi_{\mathbf{a}}\left(\mathscr{I}_r\right)\right)\right)^3 \right).$$

In this section, Ω and O are the Landau notations: for any positive functions f and g, we write $f = \Omega(g)$ (resp. $f = O(g)$) if there exists a positive constant C such that $f \geq C \cdot g$ (resp. $f \leq C \cdot g$).

7.1. *D grows, n, m, r are fixed*

We first study the case where n, m and r are fixed (and thus $k = (n-r)(m-r)$ is constant too), and D grows. In that case, the arithmetic complexity of the grevlex Gröbner basis computation is $O(D^{k\omega})$, and the degree is $\Omega(D^k)$. Therefore the arithmetic complexity has a polynomial dependence in the degree for these parameters.

7.2. *n grows, m, r, D are fixed*

This paragraph is devoted to the study of the subfamilies of Generalized MinRank problems when the parameters m, r and D are constant values and n grows. Let ℓ denote the constant value $\ell = m - r$. First, we assume that $D = 1$. When n grows, by Corollary 11 we have

$$\begin{aligned} \log(\mathsf{DEG}) &= \log\left(\prod_{i=0}^{\ell-1} \frac{\binom{n+\ell-1}{r+i}}{\binom{n+\ell-1}{i}} \right) \\ &\underset{n\to\infty}{\sim} r\ell \log(n) \end{aligned}$$

On the other hand,

$$\begin{aligned}
\log(\mathsf{Compl}) &= \omega\log\binom{(n-r)\ell+r\ell+1}{(n-r)\ell}+\log\binom{n}{r+1}+\log\binom{m}{r+1}\\
&= \omega\log\binom{n\ell+1}{r\ell+1}+\log\binom{n}{r+1}+\log\binom{m}{r+1}\\
&\underset{n\to\infty}{\sim} (\omega(r\ell+1)+r+1)\log(n).
\end{aligned}$$

Therefore, $\log(\mathsf{Compl})/\log(\mathsf{DEG}) \underset{n\to\infty}{\sim} \dfrac{\omega(r\ell+1)+r+1}{r\ell}$ and hence the number of arithmetic operations is polynomial in the degree of the ideal.

Also, if $D \geq 2$ is constant, a similar analysis yields

$$\begin{aligned}
\log(\mathsf{DEG}) &= (n-r)\ell\log(D)+\log\left(\prod_{i=0}^{\ell-1}\frac{\binom{n+\ell-1}{r+i}}{\binom{n+\ell-1}{i}}\right)\\
&\underset{n\to\infty}{\sim} \log(D)\ell n.\\
\log(\mathsf{Compl}) &= \omega\log\binom{k+Dr\ell+(D-1)k+1}{k}+\log\binom{n}{r+1}+\log\binom{m}{r+1}\\
&= \omega\log\binom{Dn\ell+1}{(n-r)\ell}+\log\binom{n}{r+1}+\log\binom{m}{r+1}\\
&\underset{n\to\infty}{\sim} \omega\log\binom{Dn\ell}{n\ell}.
\end{aligned}$$

Then, using the fact that $\binom{\alpha n}{\beta n} \underset{n\to\infty}{\sim} n\left(\alpha\log(\alpha)-\beta\log(\beta)-(\alpha-\beta)\log(\alpha-\beta)\right)$, we obtain that

$$\log(\mathsf{Compl}) \underset{n\to\infty}{\sim} n\omega\ell(D\log(D)-(D-1)\log(D-1)).$$

Therefore, $\log(\mathsf{Compl})/\log(\mathsf{DEG})$ is upper bounded by a constant value and hence the arithmetic complexity of the Gröbner basis computation is also polynomial in the degree of the ideal for this subclass of Generalized MinRank problems under genericity assumptions.

7.3. The case $r = m-1$

The case $r = m-1$ is a special case of the setting studied in Section 7.2 which arises in several applications, since it is the problem of finding at which points the evaluation of a polynomial matrix is rank defective. In this setting, the formulas in Theorem 28 are much simpler:

- the 0-dimensional condition yields $k = n-m+1$;
- $\mathbb{D}_{\mathrm{reg}} \leq Dn-(n-m)$;
- $\mathsf{DEG} \leq D^{n-m+1}\binom{n}{m-1}$.

Therefore, the arithmetic complexity of the Gröbner basis computation is

$$\mathsf{Compl} = O(\binom{n}{m}\binom{Dn+1}{n-m+1}^{\omega}).$$

If $D>1$ and m are fixed, $\log\left(\binom{n}{m}\binom{Dn+1}{n-m+1}^{\omega}\right) \underset{n\to\infty}{\sim} m\log(n)+\omega\log\binom{Dn}{n}$ and a direct application of Stirling's formula shows that

$$\omega\log\binom{Dn}{n} \underset{n\to\infty}{\sim} \omega(D\log D-(D-1)\log(D-1))n.$$

(n,m,D,r,k)	DEG	$\mathbb{D}_{\text{reg}}$	F_4 time(Magma)	FGLM time(Magma)	F_5 time/nb.ops(FGb)	FGLM time(FGb)
(6,5,2,4,2)	60	11	0.001s	0.001s	0.00s/$2^{13.32}$	0.00s
(6,5,3,4,2)	135	17	0.002s	0.019s	0.00s/$2^{15.29}$	0.00s
(6,5,4,4,2)	240	23	0.004s	0.09s	0.01s/$2^{16.79}$	0.01s
(5,5,2,3,4)	800	17	0.25s	6.3s	0.24s/$2^{25.56}$	0.19s
(8,5,2,4,4)	1120	13	0.7s	20s	0.43s/$2^{26.71}$	0.58s
(5,5,3,3,4)	4050	27	6.7s	567s	5.43s/$2^{30.68}$	3s
(6,5,2,3,6)	11200	19	479s	17703s	94.85s/$2^{35.7}$	203s

Table 1. Experimental results

On the other hand, $\log(\mathsf{DEG}) \underset{n\to\infty}{\sim} n \log D$. Therefore, $\log(\mathsf{Compl})/\log(\mathsf{DEG})$ has a finite limit when n grows and m is fixed, showing that, in this setting, the arithmetic complexity is polynomial in the degree of the ideal.

7.4. *Experimental results*

In this section, we present some experimental results obtained by using the Gröbner bases package FGb (using the F_5 algorithm) and the implementation of the F_4 algorithm in the MAGMA computer algebra system (Bosma et al., 1997). All instances were constructed as random (with uniform distribution) 0-dimensional MinRank problems (i.e. $nm-(n+m-r)r=k$) over the finite field $\mathbb{F}_{65521}$. All experiments were conducted on a 2.93 GHz Intel Xeon with 132 GB RAM.

Useful information can be read from Table 1. First, the experimental values of the degree of regularity and of the degree match exactly the theoretical values given in Lemma 18 and in Corollary 11. Also, it can be noted that the most relevant indicator of the complexity of the Gröbner basis computation seems to be the degree of the ideal.

The comparison between the complexity bound and the degree of the ideal is illustrated in Figures 1 and 2. First, Figure 1 shows that the bound on the complexity of the Gröbner computation is polynomial in the degree of the ideal when D grows ($n=m=20$, $r=10$ fixed), since $\log(\mathsf{Compl}_{\mathsf{F}_5})/\log(\mathsf{DEG})$ is upper bounded by 5. This is in accordance with the analysis performed in Section 7.1.

Then Figure 2 shows empirically that if $m=\lfloor \beta n\rfloor$ and $r=\lfloor \alpha n\rfloor-1$ (with $\alpha\leq\beta\leq 1$) and n grows, then the complexity bound is also polynomial in the degree of the ideal.

However, there also exist families of generalized MinRank problem where the complexity bound for the Gröbner basis computation is *not* polynomial in the degree of ideal. For instance, taking $n=m$ and fixing the values of r and D yields such a family.

The experimental behavior of $\log(\mathsf{Compl}_{\mathsf{F}_5})/\log(\mathsf{DEG})$ is plotted in Figure 3. We would like to point out that this does not necessarily mean that the complexity of the Gröbner basis computation is not polynomial in the degree of the ideal. Indeed, the complexity bound $O\left(\binom{n}{r+1}\binom{m}{r+1}\binom{k+\mathbb{D}_{\text{reg}}}{k}^{\omega}\right)$ is not sharp and the figure only shows that the bound is not polynomial.

The problem of showing whether the actual arithmetic complexity of the F_5 algorithm is polynomial or not in the degree of the ideal for any families of parameters of the generalized MinRank problem remains an open problem.

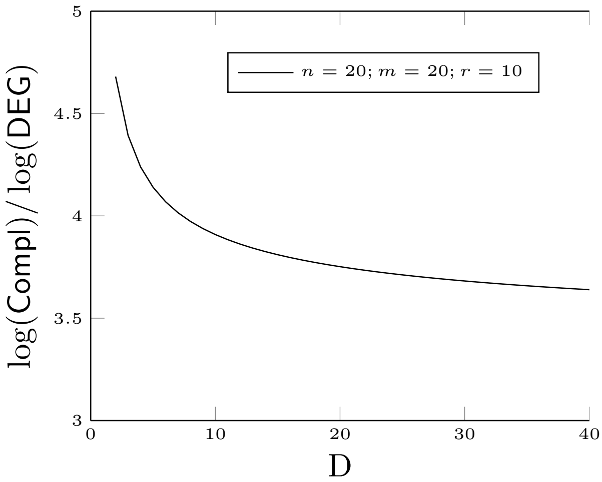

Fig. 1. Numerical values of $\log(\mathsf{Compl}_{\mathsf{F_5}})/\log(\mathsf{DEG})$, for $n = m = 20, r = 10, k = (n-r)(m-r)$.

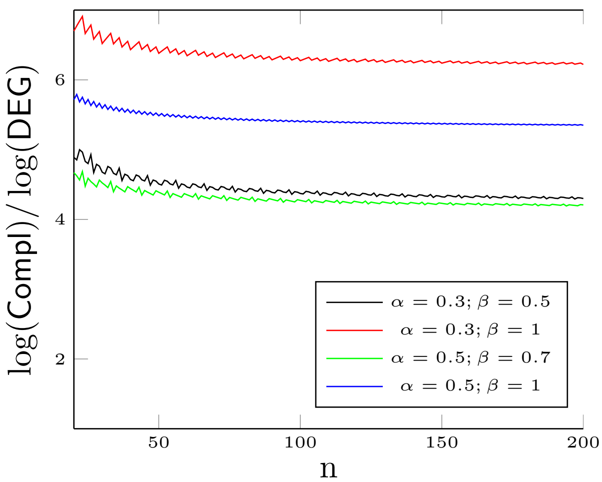

Fig. 2. Numerical values of $\log(\mathsf{Compl}_{\mathsf{F_5}})/\log(\mathsf{DEG})$, for $m = \lfloor \beta n \rfloor, r = \lfloor \alpha n \rfloor - 1, D = 1, k = (n-r)(m-r)$.

8. Application to bi-homogeneous systems of bi-degree $(D,1)$

In this section, we show that the previous complexity analysis can be used to obtain bounds on the complexity of solving bi-homogeneous systems of bi-degree $(D,1)$ by using Gröbner bases algorithms. These structured systems can appear naturally in some applications, for instance in geometry and in optimization. Indeed the classical technique of *Lagrange multipliers* – when used to optimize a polynomial function under polynomial constraints – gives rise to a bi-homogeneous system of bi-degree $(D,1)$.

Bi-homogeneous polynomials are defined as follows: given two finite sets of variables $X = \{x_0,\dots,x_{n_x}\}$ and $Y = \{y_0,\dots,y_{n_y}\}$, a polynomial $f \in \mathbb{K}[X,Y]$ is called *bi-homogeneous* if for any $\lambda, \mu \in \mathbb{K}$, there exist $d_x, d_y \in \mathbb{N}$ such that

$$f(\lambda X, \mu Y) = \lambda^{d_x}\mu^{d_y} f(X,Y).$$

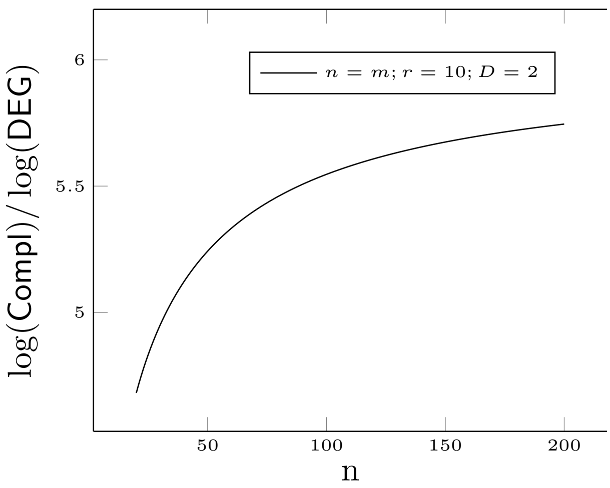

Fig. 3. Numerical values of $\log(\mathsf{Compl}_{\mathsf{F}_5})/\log(\mathsf{DEG})$, for $m = \lfloor \beta n \rfloor, r = \lfloor \alpha n \rfloor - 1, D = 1, k = (n-r)(m-r)$.

The couple (d_x, d_y) is called the *bi-degree* of f.

In this section, we focus on generic systems of $n_x + n_y$ bi-homogeneous equations of bi-degree $(D, 1)$. Such systems have a finite number of solutions on the biprojective space $\mathbb{P}^{n_x} \times \mathbb{P}^{n_y}$. One way to compute them is to start by computing their projection on $\mathbb{P}^{n_x}$, and then lift them to $\mathbb{P}^{n_x} \times \mathbb{P}^{n_y}$ by solving linear systems (this can be done since the equations are linear with respect the variables $y_0, \ldots, y_{n_y}$).

The following proposition shows that computing the projection on $\mathbb{P}^{n_y}$ can be computed by solving a homogeneous MinRank problem.

Proposition 29. *Let $f_1, \ldots, f_m \in \mathbb{K}[X, Y]$ be a bi-homogeneous system of bi-degree $(D, 1)$. If $m > n_y$, then $(x_0 : \ldots : x_{n_x}, y_0 : \ldots : y_{n_y}) \in \mathbb{P}^{n_x} \times \mathbb{P}^{n_y}$ is a zero of this system if and only if the matrix*

$$\mathrm{jac}_Y(x_0, \ldots, x_{n_x}) = \begin{pmatrix} \frac{\partial f_1}{\partial y_0} & \cdots & \frac{\partial f_1}{\partial y_{n_y}} \\ \vdots & \vdots & \vdots \\ \frac{\partial f_m}{\partial y_0} & \cdots & \frac{\partial f_m}{\partial y_{n_y}} \end{pmatrix}$$

is rank defective.

Proof. First, notice that

$$\begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix} = \mathrm{jac}_Y(x_0, \ldots, x_{n_x}) \cdot \begin{pmatrix} y_0 \\ \vdots \\ y_{n_y} \end{pmatrix}.$$

Therefore, $(x_0 : \ldots : x_{n_x}, y_0 : \ldots : y_{n_y}) \in \mathbb{P}^{n_x} \times \mathbb{P}^{n_y}$ is a zero of the system if and only if $(y_0, \ldots, y_{n_y})$ belongs to the kernel of jac_Y. Since $m > n_y$, the number of rows is greater than or equal to the number of columns of jac_Y, and hence jac_Y is rank defective. $\square$

In applications, most of bi-homogeneous systems occurring are *affine*: A polynomial $f \in \mathbb{K}[x_1, \ldots, x_{n_x}, y_1, \ldots, y_{n_y}]$ is called affine of bi-degree $(D, 1)$ if there exists a bi-homogeneous polynomial $f^h \in \mathbb{K}[x_0,\ldots,x_{n_x},y_0,\ldots,y_{n_y}]$ of bi-degree $(D,1)$ such that

$$f(x_1,\ldots,x_{n_x},y_1,\ldots,y_{n_y}) = f^h(1,x_1,\ldots,x_{n_x},1,y_1,\ldots,y_{n_y}).$$

This means that each monomial occurring in f has bi-degree (i,j) with $i \leq D$ and $j \leq 1$. Notice that the polynomial f^h is uniquely defined and that Proposition 29 also holds in the affine context:

Proposition 30. *Let $f_1,\ldots,f_m \in \mathbb{K}[x_1,\ldots,x_{n_x},y_1,\ldots,y_{n_y}]$ be an affine system of bi-degree $(D,1)$. If $m > n_y$ and $(x_1,\ldots,x_{n_x},y_1,\ldots,y_{n_y}) \in \mathbb{K}^{n_x} \times \mathbb{K}^{n_y}$ is a zero of the system, then the $m \times (n_y+1)$ matrix*

$$\mathrm{jac}_Y^a(x_1,\ldots,x_{n_x}) = \begin{pmatrix} f_1(x_1,\ldots,x_{n_x},0,\ldots,0) & \frac{\partial f_1}{\partial y_1} & \cdots & \frac{\partial f_1}{\partial y_{n_y}} \\ \vdots & \vdots & \vdots & \\ f_m(x_1,\ldots,x_{n_x},0,\ldots,0) & \frac{\partial f_m}{\partial y_0} & \cdots & \frac{\partial f_m}{\partial y_{n_y}} \end{pmatrix}$$

is rank defective.

Proof. The proof is similar to that of 29 since

$$\begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix} = \mathrm{jac}_Y^a(x_1,\ldots,x_{n_x}) \cdot \begin{pmatrix} 1 \\ y_1 \\ \vdots \\ y_{n_y} \end{pmatrix}.$$

Therefore, if $(x_1,\ldots,x_{n_x},y_1,\ldots,y_{n_y})$ is a zero of the system then there is a non-zero vector in the kernel of jac_Y^a (however in the affine case, the converse is not true). □

An algebraic description of the variety V of a 0-dimensional polynomial system can be obtained by computing a rational parametrization, i.e. a polynomial $g(u) \in \mathbb{K}[u]$ and a set of rational functions $g_1,\ldots,g_{n_x},h_1,\ldots,h_{n_y} \in \mathbb{K}(u)$ such that

$$(x_1,\ldots,x_{n_x},y_1,\ldots,y_{n_y}) \in V$$
$$\Updownarrow$$
$$\exists u \in \mathbb{K}, s.t. g(u) = 0, \forall i \in \{1,\ldots,n_x\}, x_i = g_i(u), \forall j \in \{1,\ldots,n_y\}, y_j = h_j(u).$$

To obtain a rational parametrization, we need a separating element: a linear form which takes different values on all points of V. Therefore, a rational parametrization exists only if the cardinality of the field $\mathbb{K}$ is infinite or large enough.

Under the assumption that the field $\mathbb{K}$ is sufficiently large, Algorithm 1 uses the property described in Proposition 30 to find a rational parametrization of the zeroes of a radical and 0-dimensional system of $n_x + n_y$ affine polynomials of bi-degree $(D,1)$. The algorithm proceeds by computing first a rational parametrization of the projection of the zero set on $\mathbb{K}^{n_x}$. This is done by computing a lexicographical Gröbner basis of a Generalized MinRank Problem. Then this parametrization is lifted to the whole space by solving a linear system (this can be done since the equations are linear with respect to the variables $y_1,\ldots,y_{n_y}$).

The success of Algorithm 1 depends on the choice of the parameters α (a linear change of coordinates such that x_n is a separating element) and M. However, as we will see in Theorem 31,

Algorithm 1 Rational parametrization of systems of bi-degree $(D,1)$

Input: $f_1,\dots,f_{n_x+n_y} \in \mathbb{K}[X,Y]$ a system of affine polynomials of bi-degree $(D,1)$ such that the ideal they generate is radical and 0-dimensional;
$(\alpha_1,\dots,\alpha_{n_x-1}) \in \mathbb{K}^{n_x-1}$;
a full rank matrix $M = (m_{i,j}) \in \mathbb{K}^{ny\times(n_x+n_y)}$.

Output: Returns a rational parametrization of the variety of the system or "fail".

1: Compute for each $i \in \{1,\dots,n_x+n_y\}$,

$$\widetilde{f_i}(x_1,\dots,x_{n_x-1},u,y_1,\dots,y_{n_y}) = f_i(x_1,\dots,x_{n_x-1},u-\sum_{\ell=1}^{n_x-1}\alpha_\ell x_\ell,y_1,\dots,y_{n_y}).$$

2: Compute the matrix $\mathrm{jac}_Y^a(\widetilde{f_1},\dots,\widetilde{f_{n_x+n_y}})$.

3: Compute a lex Gröbner basis G of the ideal $I \subset \mathbb{K}[x_1,\dots,x_{n_x-1},u]$ generated by the maximal minors of the matrix $\mathrm{jac}_Y^a(\widetilde{f_1},\dots,\widetilde{f_{n_x+n_y}})$. If the Gröbner basis has the following shape (the *shape position*):

$$\begin{aligned} x_1 &- g_1(u) \\ x_2 &- g_2(u) \\ &\vdots \\ x_{n_x-1} &- g_{n_x-1}(u) \\ &g(u), \end{aligned}$$

then continue to Step 4, else return "fail".

4: Using M, compute a linear combination of the polynomials of the system evaluated at $(g_1(u),\dots,g_{n_x-1}(u))$:

$$\begin{pmatrix} \widehat{f_1}(y_1,\dots,y_{n_y},u) \\ \vdots \\ \widehat{f_{n_y}}(y_1,\dots,y_{n_y},u) \end{pmatrix} = M\cdot \begin{pmatrix} \widetilde{f_1}(g_1(u),\dots,g_{n_x-1}(u),u,y_1,\dots,y_{n_y}) \mod g(u) \\ \vdots \\ \widetilde{f_{n_x+n_y}}(g_1(u),\dots,g_{n_x-1}(u),u,y_1,\dots,y_{n_y}) \mod g(u) \end{pmatrix}$$

5: If the linear system $\widehat{f_1} = \ldots = \widehat{f_{n_y}} = 0$ has rank n_y (as a linear system in $\mathbb{K}(u)[Y]$ where the variables are $y_1,\dots,y_{n_y}$), continue to Step 6, else return "fail".

6: Using Cramer's rule, solve the system $\widehat{f_1} = \ldots = \widehat{f_{n_y}} = 0$ as a linear system in $\mathbb{K}(u)[Y]$. This yields rational functions $h_i(u) \in \mathbb{K}(u)$ such that, for $i \in \{1,\dots,n_y\}$, $y_i - h_i(u) = 0$.

7: Return the rational parametrization

$$\begin{array}{ll} g(u) = 0 & \\ x_1 = g_1(u) & y_1 = h_1(u) \\ \vdots & \vdots \\ x_{n_x-1} = g_{n_x-1}(u) & y_{n_y-1} = h_{n_y-1}(u) \\ x_{n_x} = u - \sum_{\ell=1}^{n_x-1}\alpha_\ell g_\ell(u) & y_{n_y} = h_{n_y}(u) \end{array}$$

if the cardinality of $\mathbb{K}$ is infinite or large enough, then almost all choices of α and M are good. Therefore, these parameters can be chosen at random. If Algorithm 1 unluckily fails, then it can be restarted with the same algebraic system and different values of α and M.

We now prove that the complexity of Algorithm 1 is bounded by the complexity of the underlying generalized MinRank problem and that most choices of $(\alpha_1, \ldots, \alpha_{n_x-1})$ and M do not fail.

Theorem 31. *Let $f_1, \ldots, f_{n_x+n_y} \in \mathbb{K}[X,Y]$ be an affine system of bi-degree $(D,1)$ such that the ideal $\langle f_1, \ldots, f_{n_x+n_y} \rangle$ is radical and 0-dimensional. Then there exists non-identically null polynomials $h_1 \in \mathbb{K}[z_1, \ldots, z_{n_x-1}]$ and $h_2 \in \mathbb{K}[z_{1,1}, \ldots, z_{n_y,n_x+n_y}]$ such that, for any choice of $(\alpha_1, \ldots, \alpha_{n_x-1})$ and $M = (m_{i,j}) \in \mathbb{K}^{n_y \times (n_x+n_y)}$ verifying:*

- *the matrix $\mathrm{jac}_Y^{\alpha}(\widetilde{f_1}, \ldots, \widetilde{f_{n_x+n_y}})$ verifies the conditions of Theorem 28;*
- *$h_1(\alpha_1, \ldots, \alpha_{n_x-1}) h_2(m_{1,1}, \ldots, m_{n_y,n_x+n_y}) \neq 0$,*

Algorithm 1 returns a rational parametrization of the variety of the system and its complexity is upper bounded by

$$O\left(\binom{n_x+n_y}{n_x-1}\binom{D(n_x+n_y)+1}{n_x}^{\omega} + n_x\left(D^{n_x}\binom{n_x+n_y}{n_x}\right)^3\right).$$

Proof. In this proof, $\widetilde{O}()$ stands for the *soft-Oh* notation: if f and g are positive functions, $f = \widetilde{O}(g)$ means that there exists $k \in \mathbb{N}$ such that $f = O(g \cdot \log^k(g))$. Let I denote the ideal generated by $f_1, \ldots, f_{n_x+n_y}$. According to Becker et al. (1994); Lakshman (1990), for any radical 0-dimensional ideal, there exists a polynomial h_1 such that if $h_1(\alpha_1, \ldots, \alpha_{n_x-1}) \neq 0$, then the system is in shape position after the change of coordinates

$$x_{n_x} \mapsto x_{n_x} - \sum_{\ell=1}^{n_x-1} \alpha_\ell x_\ell.$$

The polynomial h_2 is chosen such that if $h_2(m_{i,j}) \neq 0$, then the linear system $\widehat{f_1} = \cdots = \widehat{f_{n_y}} = 0$ in $\mathbb{K}(u)[Y]$ has rank exactly n_y. Consider now the following linear system (where the variables are $y_1, \ldots, y_{n_y}$):

$$\begin{pmatrix} z_{1,1} & \ldots & z_{1,n_x+n_y} \\ \vdots & \vdots & \vdots \\ z_{n_y,1} & \ldots & z_{n_y,n_x+n_y} \end{pmatrix} \cdot \begin{pmatrix} \widetilde{f_1}(g_1(u), \ldots, g_{n_x-1}(u), u, y_1, \ldots, y_{n_y}) \mod g(u) \\ \vdots \\ \widetilde{f_{n_x+n_y}}(g_1(u), \ldots, g_{n_x-1}(u), u, y_1, \ldots, y_{n_y}) \mod g(u) \end{pmatrix} = 0.$$

Its determinant (which lies in $\mathbb{K}[z_{1,1}, \ldots, z_{n_y,n_x+n_y}, u]$) is not zero since the ideal generated by the input system $(f_1, \ldots, f_{n_x+n_y})$ is 0-dimensional and proper. By considering this determinant as a polynomial in $\mathbb{K}[z_{1,1}, \ldots, z_{n_y,n_x+n_y}][u]$, the polynomial $h_2 \in \mathbb{K}[z_{1,1}, \ldots, z_{n_y,n_x+n_y}]$ is chosen as a non-zero coefficient of a term u^β. Consequently, the algorithm does not fail if $h_1(\alpha_1, \ldots, \alpha_{n_x-1}) \neq 0$ and $h_2(m_{i,j}) \neq 0$.

Now we proceed with the complexity analysis:

- the complexity of the substitution step to compute the polynomials $\widetilde{f_i}$ is upper bounded by $\widetilde{O}((n_x+n_y)Dn_xn_y)$.
- By Theorem 28, the complexity of the Gröbner basis computation is upper bounded by

$$O\left(\binom{n_x+n_y}{n_x-1}\binom{D(n_x+n_y)+1}{n_x}^{\omega} + n_x(\mathsf{DEG}(I))^3\right).$$

- Since $\deg(g_{n_x}) \leq \mathsf{DEG}(I)$, a monomial $u^{n_x}\prod_{i=1}^{n_x-1} x_i^{\alpha_i}$ of degree D can be evaluated in the univariate polynomials $(g_1(u),\ldots,g_{n_x-1}(u))$ modulo $g(u)$ in complexity $\widetilde{O}(D\,\mathsf{DEG}(I))$ by using a subproduct tree (Bostan and Schost, 2005), quasi-linear multiplication of univariate polynomials and quasi-linear modular reduction. Since there are at most $(n_x+n_y)(n_y+1)\binom{n_x+D}{n_x}$ such monomials in the system $f_1,\ldots,f_{n_x+n_y}$, the Step 4 of the Algorithm needs at most
$$\widetilde{O}\left((n_x+n_y)n_y\binom{n_x+D}{n_x}D\,\mathsf{DEG}(I)\right)$$
arithmetic operations in $\mathbb{K}$.
Notice that $n_x+n_y \leq \binom{n_x+n_y}{n_x-1}$ and $\mathsf{DEG}(I) \leq \binom{D(n_x+n_y)+1}{n_x}$.
· If $D \geq 2$: for any $a,b,c \in \mathbb{N}$ such that $b<a$, $\binom{a}{b}c \leq \binom{a+c}{b}$. Therefore, $Dn_y\binom{n_x+D}{n_x} \leq \binom{n_x+n_y+2D}{n_x}$. Also, notice that, for $D \geq 2$ and for any n_x, n_y such that $n_xn_y > 1$, $n_x+n_y+2D \leq D(n_x+n_y)+1$. Therefore,
$$\widetilde{O}\left((n_x+n_y)n_y\binom{n_x+D}{n_x}D\,\mathsf{DEG}(I)\right) \leq \widetilde{O}\left(\binom{n_x+n_y}{n_x-1}\binom{D(n_x+n_y)+1}{n_x}^2\right).$$
· If $D=1$: $(n_x+n_y)n_y\binom{n_x+1}{n_x} = (n_x+n_y)n_yn_x$ is bounded by $\binom{n_x+n_y}{n_x-1}\binom{(n_x+n_y)+1}{n_x}$.
Therefore, the complexity of the Step 4 of Algorithm 1 is upper bounded by the complexity of the Gröbner basis computation: $O\left(\binom{n_x+n_y}{n_x-1}\binom{D(n_x+n_y)+1}{n_x}^{\omega}\right)$.
- To solve the linear system by using Cramer's rule, we need to compute n_x+1 determinants of $(n_x\times n_x)$-matrices whose entries are univariate polynomials of degree D. This can be achieved by using a fast evaluation-interpolation strategy with complexity $\widetilde{O}\left(Dn_x^{\omega+1}\right)$ (since multi-set evaluation and interpolation of univariate polynomials can be done in quasi-linear time, see e.g. Bostan and Schost (2005)).

Since $\mathsf{DEG}(I)$ is bounded by $D^{n_x}\binom{n_x+n_y}{n_x}$, the sum of all these complexities is upper bounded by
$$O\left(\binom{n_x+n_y}{n_x-1}\binom{D(n_x+n_y)+1}{n_x}^{\omega}+n_x\left(D^{n_x}\binom{n_x+n_y}{n_x}\right)^3\right).$$
□

Remark 32. According to Faugère et al. (2011, Lemma 15) and Faugère et al. (2011, Lemma 16), if $D=1$, there exists a non-empty Zariski open subset O_1 of the set of systems of bi-degree $(1,1)$, such that any system $(f_1,\ldots,f_{n_x+n_y}) \in O_1$ is 0-dimensional and radical. This statement also holds for systems of bi-degree $(D,1)$ with $D \in \mathbb{N}$, and the proof is similar.

Acknowledgments

This work was supported in part by the HPAC grant and the GeoLMI grant (ANR 2011 BS03 011 06) of the French National Research Agency. The second author is member of the Institut Universitaire de France. We wish to thank anonymous referees for their comments and suggestions.

References

Bank, B., Giusti, M., Heintz, J., Safey El Din, M., Schost, E., 2010. On the geometry of polar varieties. Applicable Algebra in Engineering, Communication and Computing 21 (1), 33–83.

Bardet, M., 2004. étude des systèmes algébriques surdéterminés. applications aux codes correcteurs et à la cryptographie. Ph.D. thesis, Université Paris 6.

Bardet, M., Faugère, J.-C., Salvy, B., 2004. Asymptotic expansion of the degree of regularity for semi-regular systems of equations. In: Effective Methods in Algebraic Geometry (MEGA). pp. 71–74.

Becker, E., Mora, T., Marinari, M., Traverso, C., 1994. The shape of the shape lemma. In: Proceedings of the International Symposium on Symbolic and Algebraic Computation. ISSAC '94. ACM, New York, NY, USA, pp. 129–133.
URL http://doi.acm.org/10.1145/190347.190382

Bettale, L., FaugÃ¨re, J.-C., Perret, L., 2012. Cryptanalysis of HFE, Multi-HFE and Variants for Odd and Even Characteristic. Designs, Codes and Cryptography, 1–52Accepted.
URL http://www-polsys.lip6.fr/ jcf/Papers/DCC2012.pdf

Bosma, W., Cannon, J., Playoust, C., 1997. The Magma algebra system. I. The user language. Journal of Symbolic Computation 24 (3–4), 235–265.

Bostan, A., Schost, É., 2005. Polynomial evaluation and interpolation on special sets of points. Journal of Complexity 21 (4), 420–446.

Buss, J. F., Frandsen, G. S., Shallit, J., 1999. The computational complexity of some problems of linear algebra. Journal of Computer and System Sciences 58 (3), 572–596.

Conca, A., Herzog, J., 1994. On the Hilbert function of determinantal rings and their canonical module. Proceedings of the American Mathematical Society 122 (3), 677–681.

Courtois, N., 2001. Efficient zero-knowledge authentication based on a linear algebra problem MinRank. In: Advances in Cryptology - ASIACRYPT 2001. Vol. 2248 of LNCS. Springer, pp. 402–421.

Cox, D., Little, J., O'Shea, D., 1997. Ideals, Varieties and Algorithms, 3rd Edition. Springer.

Eisenbud, D., 1995. Commutative Algebra with a View Toward Algebraic Geometry. Springer.

Faugère, J.-C., 1999. A new efficient algorithm for computing Gröbner bases (F4). Journal of Pure and Applied Algebra 139 (1–3), 61–88.

Faugère, J.-C., 2002. A new efficient algorithm for computing Gröbner bases without reductions to zero (F5). In: Mora, T. (Ed.), Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation (ISSAC). ACM Press, pp. 75–83.

Faugère, J.-C., Gianni, P., Lazard, D., Mora, T., 1993. Efficient computation of zero-dimensional Gröbner bases by change of ordering. Journal of Symbolic Computation 16 (4), 329–344.

Faugère, J.-C., Lévy-dit-Vehel, F., Perret, L., 2008. Cryptanalysis of MinRank. In: Advances in Cryptology - CRYPTO 2008. Vol. 5157 of LNCS. Springer, pp. 280–296.

Faugère, J.-C., Mou, C., 2011. Fast algorithm for change of ordering of zero-dimensional Gröbner bases with sparse multiplication matrices. In: ISSAC '11: Proceedings of the 2011 International Symposium on Symbolic and Algebraic Computation. ISSAC '11. ACM, pp. 1–8.

Faugère, J.-C., Safey El Din, M., Spaenlehauer, P.-J., 2010. Computing loci of rank defects of linear matrices using Gröbner bases and applications to cryptology. In: Watt, S. M. (Ed.), Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation (ISSAC 2010). pp. 257–264.

Faugère, J.-C., Safey El Din, M., Spaenlehauer, P.-J., 2011. Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree (1,1): Algorithms and complexity. Journal Of Symbolic Computation 46 (4), 406–437.

Fröberg, R., 1985. An inequality for Hilbert series of graded algebras. Mathematica Scandinavica 56, 117–144.

Fulton, W., 1997. Intersection Theory, 2nd Edition. Springer.
Giusti, M., Lecerf, G., Salvy, B., 2001. A Gröbner free alternative for polynomial system solving. Journal of Complexity 17 (1), 154–211.
Greuel, G., Lossen, C., Shustin, E., 2007. Introduction to singularities and deformations. Springer.
Greuet, A., Guo, F., Safey El Din, M., Zhi, L., 2011. Global optimization of polynomials restricted to a smooth variety using sums of squares. Journal of Symbolic Computation.
Hochster, M., Eagon, J. A., 1970. A class of perfect determinantal ideals. Bulletin of the American Mathematical Society 76 (5), 1026–1029.
Hochster, M., Eagon, J. A., 1971. Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci. American Journal of Mathematics 93 (4), 1020–1058.
Kipnis, A., Shamir, A., 1999. Cryptanalysis of the HFE public key cryptosystem by relinearization. In: Advances in Cryptology - CRYPTO' 99. Vol. 1666 of LNCS. Springer, pp. 19–30.
Lakshman, Y. N., 1990. On the complexity of computing a Gröbner basis for the radical of a zero dimensional ideal. In: Proceedings of the twenty-second annual ACM Symposium on Theory Of computing. STOC '90. ACM, New York, NY, USA, pp. 555–563.
URL `http://doi.acm.org/10.1145/100216.100294`
Lazard, D., 1983. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In: Computer Algebra, EUROCAL'83. Vol. 162 of LNCS. Springer, pp. 146–156.
Macdonald, I. G., Pach, J., Theobald, T., 2001. Common tangents to four unit balls in r 3. Discrete & Computational Geometry 26 (1), 1–17.
Miller, E., Sturmfels, B., 2005. Combinatorial commutative algebra. Vol. 227. Springer Verlag.
Ourivski, A., Johansson, T., 2002. New technique for decoding codes in the rank metric and its cryptography applications. Problems of Information Transmission 38 (3), 237–246.
Safey El Din, M., Schost, E., 2003. Polar varieties and computation of one point in each connected component of a smooth real algebraic set. In: Proceedings of the 2003 international symposium on Symbolic and algebraic computation. ACM, pp. 224–231.
Sottile, F., 2002. From enumerative geometry to solving systems of polynomial equations. Computations in algebraic geometry with Macaulay 2, 101–129.
Sottile, F., 2003. Enumerative real algebraic geometry. Algorithmic and Quantitative Real Algebraic Geometry, 139–179.
Storjohann, A., 2000. Algorithms for matrix canonical forms. Ph.D. thesis, University of Waterloo.
Verschelde, J., 1999. Polynomial homotopies for dense, sparse and determinantal systems.
Williams, V., 2011. Breaking the coppersmith-winograd barrier.