Critical Points and Gröbner Bases: the Unmixed Case

Jean-Charles Faugère, Mohab Safey El Din, Pierre-Jean Spaenlehauer
INRIA, Paris-Rocquencourt Center, PolSys Project
UPMC, Univ Paris 06, LIP6
CNRS, UMR 7606, LIP6
UFR Ingénierie 919, LIP6 Passy-Kennedy
Case 169, 4, Place Jussieu, F-75252 Paris
{Jean-Charles.Faugere,Mohab.Safey,Pierre-Jean.Spaenlehauer}@lip6.fr

ABSTRACT

We consider the problem of computing critical points of the restriction of a polynomial map to an algebraic variety. This is of first importance since the global minimum of such a map is reached at a critical point. Thus, these points appear naturally in non-convex polynomial optimization which occurs in a wide range of scientific applications (control theory, chemistry, economics,...).

Critical points also play a central role in recent algorithms of effective real algebraic geometry. Experimentally, it has been observed that Gröbner basis algorithms are efficient to compute such points. Therefore, recent software based on the so-called Critical Point Method are built on Gröbner bases engines.

Let $f_1, \ldots, f_p$ be polynomials in $\mathbb{Q}[x_1, \ldots, x_n]$ of degree D, $V \subset \mathbb{C}^n$ be their complex variety and π_1 be the projection map $(x_1, \ldots, x_n) \mapsto x_1$. The critical points of the restriction of π_1 to V are defined by the vanishing of $f_1, \ldots, f_p$ and some maximal minors of the Jacobian matrix associated to $f_1, \ldots, f_p$. Such a system is algebraically structured: the ideal it generates is the sum of a determinantal ideal and the ideal generated by $f_1, \ldots, f_p$.

We provide the first complexity estimates on the computation of Gröbner bases of such systems defining critical points. We prove that under genericity assumptions on $f_1, \ldots, f_p$, the complexity is polynomial in the generic number of critical points, i.e. $D^p(D-1)^{n-p}\binom{n-1}{p-1}$. More particularly, in the quadratic case $D = 2$, the complexity of such a Gröbner basis computation is polynomial in the number of variables n and exponential in p. We also give experimental evidence supporting these theoretical results.

Categories and Subject Descriptors

I.1.2 [**Computing Methodologies**]: Symbolic and Algebraic Manipulation; F.2.2 [**Theory of Computation**]: Analysis of Algorithms and Problem Complexity

Keywords

Critical points, Gröbner bases, Determinantal system, Polynomial minimization

1. INTRODUCTION

Motivations and problem statement. The local extrema of the restriction of a polynomial map to a real algebraic variety are reached at the critical points of the map under consideration. Hence, computing these critical points is of first importance for polynomial optimization which arises in a wide range of applications in engineering sciences (control theory, chemistry, economics, etc.).

Computing critical points is also the cornerstone of algorithms for asymptotically optimal algorithms for polynomial system solving over the reals (singly exponential in the number of variables). Indeed, for computing sample points in each connected component of a semi-algebraic set, the algorithms based on the so-called critical point method rely on a reduction of the initial problem to polynomial optimization problems. In [10, 11] (see also [27, 28, 29]), the best complexity bounds are obtained using infinitesimal deformation techniques of semi-algebraic geometry, nevertheless obtaining efficient implementations of these algorithms remains an issue.

Tremendous efforts have been made to obtain fast implementations relying on the critical point method (see [16, 17, 32, 33, 35, 36, 37]). This is achieved with techniques based on algebraic elimination and complex algebraic geometry. For instance, when the input polynomial system $(\mathbf{F}) : f_1 = \cdots = f_p = 0$ in $\mathbb{Q}[x_1, \ldots, x_n]$ satisfies genericity assumptions, one is led to compute the set of critical points of the restriction of the projection on the first coordinate $\pi_1 : (x_1, \ldots, x_n) \mapsto x_1$ to the algebraic variety $V(\mathbf{F}) \subset \mathbb{C}^n$ defined by $\mathbf{F}$; this set is denoted by $\mathsf{crit}(\pi_1, V(\mathbf{F}))$.

The set $\mathsf{crit}(\pi_1, V(\mathbf{F}))$ is defined by $\mathbf{F}$ and the vanishing of the maximal minors of the truncated Jacobian matrix of $\mathbf{F}$ obtained by removing the partial derivatives with respect to x_1. This system is highly-structured: algebraically, we are considering the sum of a determinantal ideal with the ideal $\langle f_1, \ldots, f_p \rangle$.

In practice, we compute a rational parametrization of this set through Gröbner bases computations which are fast in practice. We have observed that the behavior of Gröbner bases on these systems does not coincide with the generic one. In the particular case of quadratic equations, it seems to be polynomial in n and exponential in p which meets the best complexity known bound for the quadratic minimization problem [9, 26]. Understanding the complexity of these computations is a first step towards the design of dedicated Gröbner bases algorithms, so we focus on the following important open problems:

(A) Can we provide *complexity estimates* for the computation of Gröbner bases of ideals defined by such *structured algebraic systems*?

(B) Is this computation *polynomial in the generic number of critical points*?

(C) In the *quadratic case*, is this computation *polynomial in the number of variables* (and exponential in the codimension)?

Under genericity assumptions, we actually provide affirmative answers to all these questions.

Computational methodology and related complexity issues. Gröbner bases are computed using multi-modular arithmetics and we will focus only on arithmetic complexity results; so we may consider systems defining critical points with coefficients not only in $\mathbb{Q}$ but also in a prime field.

Let $\mathbb{K}$ be a field, $\overline{\mathbb{K}}$ be its algebraic closure and $\mathbf{F} = (f_1, \ldots, f_p)$ be a family of polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ of degree D and $V(\mathbf{F})$ be their set of common zeroes in $\overline{\mathbb{K}}^n$.

We denote the Jacobian matrix

$$\begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \ldots & \frac{\partial f_1}{\partial x_n} \\ \vdots & & \vdots \\ \frac{\partial f_p}{\partial x_1} & \ldots & \frac{\partial f_p}{\partial x_n} \end{bmatrix}$$

by $\mathsf{jac}(\mathbf{F})$ and the submatrix obtained by removing the first i columns by $\mathsf{jac}(\mathbf{F}, i)$. The set of maximal minors of a given rectangular matrix M will be denoted by $\mathsf{MaxMinors}(\mathsf{M})$.

Finally, let $\mathbf{I}(\mathbf{F}, 1)$ be the ideal $\langle \mathbf{F} \rangle + \langle \mathsf{MaxMinors}(\mathsf{jac}(\mathbf{F}, 1)) \rangle$. When $\mathbf{F}$ is a reduced regular sequence and $V(\mathbf{F})$ is smooth, the algebraic variety associated to $\mathbf{I}(\mathbf{F}, 1)$ is exactly $\mathsf{crit}(\pi_1, V(\mathbf{F}))$.

So, to compute a rational parametrization of $\mathsf{crit}(\pi_1, V(\mathbf{F}))$, we use the classical solving strategy which proceeds in two steps:

(i) compute a Gröbner basis for a *grevlex* ordering of $\mathbf{I}(\mathbf{F}, 1)$ using the F_5 algorithm (see [18]);

(ii) use the FGLM algorithm [19, 20] to obtain a Gröbner basis of $\mathbf{I}(\mathbf{F}, 1)$ for the lexicographical ordering or a rational parametrization of $\sqrt{\mathbf{I}(\mathbf{F}, 1)}$.

Algorithm F_5 (Step *(i)*) computes Gröbner bases by row-echelon form reductions of submatrices of the Macaulay matrix up to a given degree. This latter degree is called *degree of regularity*. When the input satisfies regularity properties, this complexity of this step can be analyzed by estimating the degree of regularity.

FGLM algorithm [19] (Step *(ii)*) and its recent efficient variant [20] are based on computations of characteristic polynomials of linear endomorphisms in $\mathbb{K}[x_1, \ldots, x_n]/\mathbf{I}(\mathbf{F}, 1)$. This is done by performing linear algebra operations of size the *degree of* $\mathbf{I}(\mathbf{F}, 1)$ (which is the number of solutions counted with multiplicities).

Thus, we are faced to the following problems:

(1) estimate the degree of regularity of the ideal generated by the homogeneous components of highest degree of the set of generators $\mathbf{F}$, $\mathsf{MaxMinors}(\mathsf{jac}(\mathbf{F}, 1))$;

(2) show that the above estimation allows to bound the complexity of computing a *grevlex* Gröbner basis of $\mathbf{I}(\mathbf{F}, 1)$;

(3) provide sharp bounds on the degree of the ideal $\mathbf{I}(\mathbf{F}, 1)$.

As far as we know, no results are known for problems *(1)* and *(2)*. Problem *(3)* has already been investigated in the literature: see [34] where some bounds are given on the cardinality of $\mathsf{crit}(\pi_1, V(\mathbf{F}))$. We give here a new algebraic proof of these bounds.

Main results. Let $\mathbb{K}[x_1, \ldots, x_n]_D$ denote $\{f \in \mathbb{K}[x_1, \ldots, x_n] \mid \deg(f) = D\}$ and note that it is a finite-dimensional vector space. In the following, we solve the three aforementioned problems under a *genericity* assumption on $\mathbf{F}$: we actually prove that there exists a non-empty Zariski open set $\mathscr{O} \subset \overline{\mathbb{K}}[x_1, \ldots, x_n]_D^p$ such that for all $\mathbf{F} \in \mathscr{O}$:

(1) the degree of regularity of the ideal generated by the homogeneous components of largest degree of $\mathbf{F}$, $\mathsf{MaxMinors}$ $(\mathsf{jac}(\mathbf{F}, 1))$ is $\mathrm{d}_{\mathrm{reg}} = D(p-1) + (D-2)n + 2$ (see Theorem 1);

(2) with the F_5 algorithm, the highest degree reached during the computation is bounded by $\mathrm{d}_{\mathrm{reg}}$ (see Theorem 2);

(3) the degree of $\mathbf{I}(\mathbf{F}, 1)$ is $\leq \delta = D^p(D-1)^{n-p}\binom{n-1}{p-1}$.

The degree of regularity given in *(1)* is obtained thanks to an explicit formula for the Hilbert series of the homogeneous ideal under consideration (see Proposition 1). This is obtained by taking into account the determinantal structure of some of the generators of the ideal we consider. The above estimates are the key results which enable us to provide positive answers to questions **A**, **B** and **C** under genericity assumptions.

Before stating complexity results on the computation of critical points with Gröbner bases, we need to introduce a standard notation. Let ω be a real number such that a row echelon form of a $n \times n$-matrix with entries in $\mathbb{K}$ is computed within $O(n^\omega)$ arithmetic operations in $\mathbb{K}$.

We prove that there exists a non-empty Zariski open set $\mathscr{O} \subset \overline{\mathbb{K}}[x_1, \ldots, x_n]_D^p$ such that for all $\mathbf{F} \in \mathscr{O} \cap \mathbb{K}[x_1, \ldots, x_n]^p$:

(A) computing a *grevlex* Gröbner basis of $\mathbf{I}(\mathbf{F}, 1)$ can be done within $O\left(\binom{n+\mathrm{d}_{\mathrm{reg}}}{n}^\omega\right)$ arithmetic operations in $\mathbb{K}$ (see Theorem 3);

(B) computing a rational parametrization of $\mathsf{crit}(\pi_1, V(\mathbf{F}))$ using Gröbner bases can be done within $O\left(\delta^{4.03\omega}\right)$ arithmetic operations in $\mathbb{K}$ (see Corollary 5);

(C) when $D = 2$ (quadratic case), a rational parametrization of $\mathsf{crit}(\pi_1, V(\mathbf{F}))$ using Gröbner bases can be computed within $O\left(\binom{n+2p}{2p}^\omega + n2^{3p}\binom{n-1}{p-1}^3\right)$ arithmetic operations in $\mathbb{K}$, this is polynomial in n and exponential in p (see Corollary 3).

We also provide more accurate complexity results. The uniform complexity bound given for answering question **(B)** is rather pessimistic. The exponent 4.03ω being obtained after majorations which are not sharp; numerical experiments are given to support this (see Section 6). Moreover, under the above genericity assumption, we prove that, when p and D are fixed, computing a rational parametrization of $\mathsf{crit}(\pi_1, V(\mathbf{F}))$ using Gröbner bases is done within $O(D^{3.57n})$ arithmetic operations in $\mathbb{K}$ (see Corollary 4).

We also give timings for computing grevlex and lex Gröbner bases of $\mathbf{I}(\mathbf{F}, 1)$ with the MAGMA computational algebra system and with the FGb library when $\mathbb{K} = \mathsf{GF}(65521)$. These experiments show that the theoretical bounds on the degree of regularity and on the degree of $\mathbf{I}(\mathbf{F}, 1)$ (Theorem 2) are sharp. They also provide some indication on the size of problems that can be tackled in practice: e.g. when $D = 2$ and $p = 3$ (resp. $D = 3$ and $p = 1$), random dense systems with $n \leq 21$ (resp. $n \leq 14$) can be tackled (see Section 6).

Related works. As far as we know, dedicated complexity analysis of Gröbner bases on ideals defining critical points has not been investigated before. However, as we already mentioned, the determinantal structure of the system defining $\mathsf{crit}(\pi_1, V(\mathbf{F}))$ plays a central role in this paper.

In [21], we provided complexity estimates for the computation of Gröbner bases of ideals generated by minors of a linear matrix. This is generalized in [22] for matrices with entries of degree D. Nevertheless, the analysis which is done here differs significantly from these previous works. Indeed, in [21, 22] a genericity assumption is done on the entries of the considered matrix. We cannot follow the same reasonings since $\mathsf{MaxMinors}(\mathsf{jac}(\mathbf{F}, 1))$ depends on $\mathbf{F}$. Nevertheless, it is worthwhile to note that, as in [21, 22], we use properties of determinantal ideals given in [13].

Bounds on the number of critical points (under genericity assumptions) are given in [34] using the Giambelli-Thom-Porteous degree bounds on determinantal varieties (see [23, Ex. 14.4.14]).

In [9], the first polynomial time algorithms in n for deciding emptiness of a quadratic system of equations over the reals is given. Further complexity results in the quadratic case for effective real algebraic geometry have been given in [26]. In the general case, algorithms based on the so-called critical point method are given in [10, 11, 27, 28, 29]. Critical points defined by systems $\mathbf{F}$, $\mathsf{MaxMinors}(\mathrm{jac}(\mathbf{F}, 1))$ are computed in algorithms given in [1, 2, 3, 4, 5, 6, 17, 36]. The RAGlib maple package implements the algorithms given in [17, 36] using Gröbner bases.

The systems $\mathbf{F}$, $\mathsf{MaxMinors}(\mathrm{jac}(\mathbf{F}, 1))$ define polar varieties: indeed, this notion coincides with critical points in the regular case. In [2, 3, 4, 5, 6], rational parametrizations are obtained using the geometric resolution algorithm [24] and a local description of these polar varieties. This leads to algorithms computing critical points running in probabilistic time polynomial in $D^p(p(D-1))^{n-p}$. Note that this bound for $D = 2$ and $p = n/2$ is not satisfactory. In this paper, we also provide complexity estimations for computing critical points but using Gröbner bases, which is the engine we use in practice. Our results provide an explanation to the good practical behavior we have observed.

We would like to mention that other dedicated algebraic techniques exist for elimination in determinantal varieties. In particular, the *determinantal resultant* introduced and studied in [12] can be used for this task. It is implemented in the Macaulay2 package `Resultants`[1].

Organization of the paper. Section 2 recalls well-known properties of generic polynomial systems. Problems *(1)* and *(2)* mentioned above are respectively tackled in Sections 3 and 4. Problem *(3)* is solved at the end of Section 4. Complexity results are derived in Section 5. Experimental results supporting the theoretical results are given in Section 6.

Conclusions and Perspectives. We give new bounds on the degree of regularity and an explicit formula for the Hilbert series of the ideal vanishing on the critical points under genericity assumptions. This leads to new complexity bounds for computing Gröbner bases of these ideals.

However, we only considered the *unmixed case*: all polynomials $f_1, \dots, f_p$ share the same degree D. The *mixed case* (when the degrees of the polynomials $f_1, \dots, f_p$ are different) cannot be treated similarly since the difference of the degrees induce a combinatorial structure which has to be investigated. We intend to investigate this question in future works using the Eagon-Northcott complex, which yields a free resolution of the ideal generated by the maximal minors of a polynomial matrix under genericity assumptions. From this, we also expect to obtain a variant of the F_5 algorithm dedicated to these ideals.

Acknowledgments. This work was supported in part by the GeoLMI grant (ANR 2011 BS03 011 06) and by the EXACTA grant (ANR-09-BLAN-0371-01) of the French National Research Agency. We wish to thank anonymous referees for useful comments and suggestions.

2. PRELIMINARIES

NOTATIONS 1. *The set of variables $\{x_1, \dots, x_n\}$ is denoted by X. For $d \in \mathbb{N}$,* $\mathsf{Monomials}(d)$ *denotes the set of monomials of degree d in the polynomial ring $\mathbb{K}[X]$ (where $\mathbb{K}$ is a field, its algebraic closure being denoted by $\overline{\mathbb{K}}$). We let $\mathfrak{a}$ denote the finite set of parameters $\{\mathfrak{a}_{\mathfrak{m}}^{(i)} : 1 \le i \le p, \mathfrak{m} \in \bigcup_{0 \le d \le D} \mathsf{Monomials}(d)\}$.*

We also introduce the following generic systems:

- $\mathfrak{F} = (\mathfrak{f}_1, \dots, \mathfrak{f}_p) \in \mathbb{K}(\mathfrak{a})[X]^p$ *is the generic polynomial system of degree D:*
$$\mathfrak{f}_i = \sum_{\substack{\mathfrak{m} \text{ monomial} \\ \deg(\mathfrak{m}) \le D}} \mathfrak{a}_{\mathfrak{m}}^{(i)} \mathfrak{m};$$
- $\mathfrak{F}^{\mathrm{h}} = (\mathfrak{f}_1^h, \dots, \mathfrak{f}_p^h) \in \mathbb{K}(\mathfrak{a})[X]^p$ *is the generic* homogeneous *polynomial system of degree D:*
$$\mathfrak{f}_i = \sum_{\substack{\mathfrak{m} \text{ monomial} \\ \deg(\mathfrak{m}) = D}} \mathfrak{a}_{\mathfrak{m}}^{(i)} \mathfrak{m}.$$

We let $V(\mathbf{F}) \subset \overline{\mathbb{K}}^n$ denote the variety of $\mathbf{F} = (f_1, \dots, f_p)$. The projective variety of a homogeneous family of polynomials $\mathbf{F}^h$ is denoted by $W(\mathbf{F}^h)$. The projection on the first coordinate is denoted by π_1, and the critical points of the restriction of π_1 to $V(\mathbf{F})$ are denoted by $\mathsf{crit}(\pi_1, V(\mathbf{F})) \subset V(\mathbf{F})$. *Also, $\mathbf{I}(\mathbf{F}, 1)$ denotes the ideal generated by $\mathbf{F}$ and by the maximal minors of the truncated Jacobian matrix* $\mathrm{jac}(\mathbf{F}, 1)$.

Throughout the paper, if R is a ring and $I \subset R$ is an ideal, we call dimension *of I the Krull dimension of the quotient ring R/I.*

The goal of this section is to prove that the ideal $\mathbf{I}(\mathfrak{F}^{\mathrm{h}}, 1)$ is 0-dimensional. This will be done in Lemma 2 below; to do that we will use geometric statements of Sard's Theorem which require $\mathbb{K}$ to have characteristic 0. This latter assumption can be weakened using algebraic equivalents of Sard's Theorem (see [15, Corollary 16.23]).

LEMMA 1. *Let $\mathbf{I}(\mathfrak{F}, 0)$ be the ideal generated by $\mathfrak{F}$ and by the maximal minors of its Jacobian matrix. Its variety $V(\mathbf{I}(\mathfrak{F}, 0)) \subset \overline{\mathbb{K}(\mathfrak{a})}^n$ is empty and hence $V(\mathfrak{F})$ is* smooth.

PROOF. To simplify notations hereafter, we denote by $h_1, \dots, h_p$ the polynomials obtained from $\mathfrak{f}_1, \dots, \mathfrak{f}_p$ by removing their respective constant terms $\mathfrak{a}_1^{(1)}, \dots, \mathfrak{a}_1^{(p)}$. We will also denote by $\mathscr{A}$ the remaining parameters in $h_1, \dots, h_p$. Let ψ denote the mapping
$$\begin{array}{rcl} \psi : \overline{\mathbb{K}(\mathscr{A})}^n & \longrightarrow & \overline{\mathbb{K}(\mathscr{A})}^p \\ \mathbf{c} & \longmapsto & (h_1(\mathbf{c}), \dots, h_p(\mathbf{c})) \end{array}$$

Suppose first that $\psi(\overline{\mathbb{K}(\mathscr{A})}^n)$ is not dense (for the Zariski topology) in $\overline{\mathbb{K}(\mathscr{A})}^p$. Since the image $\psi(\overline{\mathbb{K}(\mathscr{A})}^n)$ is a constructible set, it is contained in a proper Zariski closed subset $\mathscr{W} \subset \overline{\mathbb{K}(\mathscr{A})}^p$. Since there is no algebraic relation between $\mathfrak{a}_1^{(1)}, \dots, \mathfrak{a}_1^{(p)}$ and the parameters in $\mathscr{A}$, this implies that the variety defined by $h_1 + \mathfrak{a}_1^{(1)} = \dots = h_p + \mathfrak{a}_1^{(p)} = 0$ is empty and consequently smooth. Since $h_i + \mathfrak{a}_i^{(1)} = \mathfrak{f}_i$, our statement follows.

Suppose now that $\psi(\overline{\mathbb{K}(\mathscr{A})}^n)$ is dense in $\overline{\mathbb{K}(\mathscr{A})}^p$. Let $K_0 \subset \overline{\mathbb{K}(\mathscr{A})}^p$ be the set of critical values of ψ. By Sard's Theorem [38, Chap. 2, Sec. 6.2, Thm 2], K_0 is contained in a proper closed subset of $\overline{\mathbb{K}(\mathscr{A})}^p$. Again, there is no algebraic relation between $\mathfrak{a}_1^{(1)}, \dots, \mathfrak{a}_1^{(p)}$ and the parameters in $\mathscr{A}$. Consequently, the variety associated to the ideal generated by the system $\mathfrak{f}_1, \dots, \mathfrak{f}_p$ and by the maximal minors of $\mathrm{jac}(\mathfrak{F})$ is empty. □

COROLLARY 1. *Let $\mathbf{I}(\mathfrak{F}^{\mathrm{h}}, 0)$ be the ideal generated by $\mathfrak{F}^{\mathrm{h}}$ and by the maximal minors of its Jacobian matrix. Then the associated projective variety $W(\mathbf{I}(\mathfrak{F}^{\mathrm{h}}, 0)) \subset \mathbb{P}^{n-1}\overline{\mathbb{K}(\mathfrak{a})}$ is empty.*

PROOF. For $1 \le i \le n$, we denote by O_i the set
$$\{(c_1 : \ldots : c_n) \mid c_i \neq 0\} \subset \mathbb{P}^{n-1}\overline{\mathbb{K}(\mathfrak{a})}$$
and we consider the canonical open covering of $\mathbb{P}^{n-1}\overline{\mathbb{K}(\mathfrak{a})}$:
$$\mathbb{P}^{n-1}\overline{\mathbb{K}(\mathfrak{a})} = \bigcup_{1 \le i \le n} O_i.$$
Therefore $W(\mathbf{I}(\mathfrak{F}^{\mathrm{h}}, 0)) = \bigcup_{1 \le i \le n} (W(\mathbf{I}(\mathfrak{F}^{\mathrm{h}}, 0)) \cap O_i)$. Denote by $\mathfrak{F}_i$ the system obtained by substituting the variable x_i by 1 in $\mathfrak{F}^{\mathrm{h}}$. According to Lemma 1 applied to $\mathfrak{F}_i$, the variety $V(\mathbf{I}(\mathfrak{F}_i, 0))$ is empty. Therefore, the set $W(\mathbf{I}(\mathfrak{F}^{\mathrm{h}}, 0)) \cap O_i$ is also empty. Consequently, $W(\mathbf{I}(\mathfrak{F}^{\mathrm{h}}, 0)) = \emptyset$. □

We can now deduce the following result.

[1] written by L. Busé, N. Botbol and M. Dubinsky

LEMMA 2. *The projective variety $W(\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1)) \subset \mathbb{P}^{n-1}\overline{\mathbb{K}(\mathfrak{a})}$ is empty, and hence $\dim(\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1)) = 0$.*

PROOF. We let φ_0 and φ_1 denote the two following morphisms:

$$\begin{array}{rccc} \varphi_0: & \mathbb{K}(\mathfrak{a})[x_1,\dots,x_n] & \to & \mathbb{K}(\mathfrak{a})[x_2,\dots,x_n] \\ & g(x_1,\dots,x_n) & \mapsto & g(0,x_2,\dots,x_n) \end{array}$$

$$\begin{array}{rccc} \varphi_1: & \mathbb{K}(\mathfrak{a})[x_1,\dots,x_n] & \to & \mathbb{K}(\mathfrak{a})[x_2,\dots,x_n] \\ & g(x_1,\dots,x_n) & \mapsto & g(1,x_2,\dots,x_n) \end{array}$$

Then $W(\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1))$ can be identified with the disjoint union of the variety $V(\varphi_1(\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1))) \subset \overline{\mathbb{K}(\mathfrak{a})}^{n-1}$ and the projective variety $W(\varphi_0(\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1))) \subset \mathbb{P}^{n-2}\overline{\mathbb{K}(\mathfrak{a})}$.

- Notice that $\varphi_1(\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1)) = \mathbf{I}(\varphi_1(\mathfrak{F}^{\mathrm{h}}),0)$. Therefore, the ideal $\varphi_1(\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1)) \subset \overline{\mathbb{K}(\mathfrak{a})}[x_2,\dots,x_n]$ is spanned by $\varphi_1(\mathbf{F}^h)$ (which is a generic system of degree D in $n-1$ variables) and by the maximal minors of its Jacobian matrix. According to Lemma 1, the variety $V(\varphi_1(\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1)))$ is empty.
- Similarly, $\varphi_0(\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1)) = \mathbf{I}(\varphi_0(\mathfrak{F}^{\mathrm{h}}),0) \subset \mathbb{K}(\mathfrak{a})[x_2,\dots,x_n]$ is generated by the homogeneous polynomials $\varphi_0(\mathfrak{F}^{\mathrm{h}})$ and by the maximal minors of the Jacobian matrix $\operatorname{jac}(\varphi_0(\mathfrak{F}^{\mathrm{h}}))$. Thus, according to Corollary 1, the variety $W(\varphi_0(\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1)))$ is also empty.

□

3. THE HOMOGENEOUS CASE

In this section, our goal is to estimate the degree of regularity of the ideal $\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1) \subset \mathbb{K}(\mathfrak{a})[X]$ which is a homogeneous ideal generated by $\mathfrak{F}^{\mathrm{h}}$ and $\mathsf{MaxMinors}(\mathfrak{F}^{\mathrm{h}},1)$ (see Notations 1). Recall that the degree of regularity $\mathrm{d}_{\mathrm{reg}}(I)$ of a 0-dimensional homogeneous ideal I is the smallest positive integer such that all monomials of degree $\mathrm{d}_{\mathrm{reg}}(I)$ are in I. Notice that $\mathrm{d}_{\mathrm{reg}}(I)$ is an upper bound on the degrees of the polynomials in a minimal Gröbner basis of I with respect to the grevlex ordering.

THEOREM 1. *The degree of regularity of the ideal $\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1)$ is*

$$\mathrm{d}_{\mathrm{reg}}(\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1)) = D(p-1) + (D-2)n + 2.$$

NOTATIONS 2. *To prove Theorem 1, we need to introduce a few more objects and notations.*

- *A set of new variables $\{u_{i,j} : 1 \le i \le p, 2 \le j \le n\}$ which is denoted by U;*
- *the determinantal ideal $\mathcal{D} \subset \mathbb{K}[U]$ generated by the maximal minors of the matrix*

$$\begin{bmatrix} u_{1,2} & \dots & u_{1,n} \\ \vdots & \vdots & \vdots \\ u_{p,2} & \dots & u_{p,n} \end{bmatrix}.$$

- *$\mathfrak{g}_1,\dots,\mathfrak{g}_{p(n-1)}$ which denote the polynomials $u_{i,j} - \frac{\partial \mathfrak{f}_i^h}{\partial x_j}$, for $1 \le i \le p, 2 \le j \le n$ and $\mathfrak{g}_{p(n-1)+1},\dots,\mathfrak{g}_{pn}$ which denote the polynomials $\mathfrak{f}_1^h,\dots,\mathfrak{f}_p^h$;*
- *the ideals $\mathfrak{I}_{(\ell)} = \mathcal{D} + \langle \mathfrak{g}_1,\dots,\mathfrak{g}_\ell\rangle \subset \mathbb{K}(\mathfrak{a})[U,X]$;*
- *if $g \in \mathbb{K}[X]$ (resp. $I \subset \mathbb{K}[X]$) is a polynomial and $\prec$ is a monomial ordering (see e.g. [14, Ch. 2, §2, Def. 1]), $\mathsf{LM}_\prec(g)$ (resp. $\mathsf{LM}_\prec(I)$) denotes its leading monomial (resp. the ideal generated by the leading monomials of the polynomials in I);*
- *a* degree ordering *is a monomial ordering $\prec$ such that for all pair of monomials $m_1, m_2 \in \mathbb{K}[X]$, $\deg(m_1) < \deg(m_2)$ implies $m_1 \prec m_2$.*

Obviously the polynomials $\mathfrak{g}_k$ for $1 \le k \le p(n-1)$ will be used to mimic the process of substituting the new variables $u_{i,j}$ by $\frac{\partial \mathfrak{f}_i^h}{\partial x_j}$; indeed we have $\mathfrak{I}_{(pn)} \cap \mathbb{K}[X] = \mathbf{I}(\mathfrak{F}^{\mathrm{h}},1)$.

Our strategy to prove Theorem 1 will be to deduce the degree of regularity of $\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1)$ from an explicit form of its *Hilbert series*.

Recall that, if I is a homogeneous ideal of a polynomial ring R with ground field $\mathbb{K}$, its *Hilbert series* is the series

$$\mathsf{HS}_I(t) = \sum_{d\in\mathbb{N}} \dim_{\mathbb{K}}(R_d/I_d)t^d,$$

where R_d denotes the $\mathbb{K}$-vector space of homogeneous polynomials of degree d and I_d denotes the $\mathbb{K}$-vector space $R_d \cap I$.

PROPOSITION 1. *The Hilbert series of the homogeneous ideal $\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1) \subset \mathbb{K}(\mathfrak{a})[X]$ is*

$$\mathsf{HS}_{\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1)}(t) = \frac{\det(A(t^{D-1}))}{t^{(D-1)\binom{p-1}{2}}}\frac{(1-t^D)^p(1-t^{D-1})^{n-p}}{(1-t)^n},$$

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

The proof of Proposition 1 is postponed to Section 3.3.

PROOF OF THEOREM 1. By definition, the Hilbert series of a zero-dimensional homogeneous ideal is a polynomial of degree $\mathrm{d}_{\mathrm{reg}} - 1$. By Lemma 2, $\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1)$ has dimension 0. Thus, using Proposition 1, we deduce that:

$$\mathrm{d}_{\mathrm{reg}}(\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1)) = 1 + \deg\left(\frac{\det(A(t^{D-1}))}{t^{(D-1)\binom{p-1}{2}}}\frac{(1-t^D)^p(1-t^{D-1})^{n-p}}{(1-t)^n}\right).$$

The highest degree on each row of $A(t)$ is reached on the diagonal. Thus $\deg(\det A(t)) = \frac{p(p-1)}{2}$ and a direct degree computation yields $\mathrm{d}_{\mathrm{reg}}(\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1)) = D(p-1) + (D-2)n + 2$. □

From Proposition 1, one can also deduce the degree of $\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1)$; this provides an alternate proof of [34, Theorem 2.2].

COROLLARY 2. *The degree of the ideal $\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1)$ is*

$$\mathsf{DEG}(\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1)) = \binom{n-1}{p-1}D^p(D-1)^{n-p}.$$

PROOF. By definition of the Hilbert series, the degree of the 0-dimensional homogeneous ideal $\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1)$ is equal to $\mathsf{HS}_{\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1)}(1)$. By Proposition 1, direct computations show that $\mathsf{HS}_{\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1)}(1) = \det(A(1))D^p(D-1)^{n-p}$. The determinant of the matrix $A(1)$ can be evaluated by using Vandermonde's identity and a formula by Harris-Tu (see e.g. [23, Example 14.4.14, Example A.9.4]). We deduce that $\det(A(1)) = \binom{n-1}{p-1}$ and hence $\mathsf{HS}_{\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1)}(1) = \binom{n-1}{p-1}D^p(D-1)^{n-p}$. □

It remains to prove Proposition 1. This is done in the next subsections following several steps:

- provide an explicit form of the Hilbert series of the ideal $\mathcal{D}$; this is actually already done in [13]; we recall the statement of this result in Lemma 3;
- deduce from it an explicit form of Hilbert series of the ideal $\mathfrak{I}_{(pn)}$ using genericity properties satisfied by the polynomials $\mathfrak{g}_k$ and properties of quasi-homogeneous ideals; this is done respectively in Lemma 4 and Section 3.2;
- deduce from it the Hilbert series associated to $\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1)$.

3.1 Auxiliary results

We start by restating a special case of [13, Cor. 1].

LEMMA 3 ([13, COROLLARY 1]). *The Hilbert series of the ideal $\mathcal{D} \subset \mathbb{K}[U]$ is $\mathsf{HS}_{\mathcal{D}}(t) = \frac{\det A(t)}{t^{\binom{p-1}{2}}(1-t)^{n(p-1)}}$.*

LEMMA 4. *For each $2 \leq \ell \leq np$, $\mathfrak{g}_\ell$ does not divide 0 in $\mathbb{K}(\mathfrak{a})[U, X]/\,\mathfrak{I}_{(\ell-1)}$.*

PROOF. According to [30, Thm. 2][31], the ring $\mathbb{K}(\mathfrak{a})[U]/\mathcal{D}$ is a Cohen-Macaulay domain of Krull dimension $(n - 1 + p - (p - 1))(p - 1) = n(p - 1)$. Therefore, the ring $\mathbb{K}(\mathfrak{a})[U, X]/\mathcal{D}$ is also a Cohen-Macaulay domain, and has dimension np.

Consider now the ideal $\langle \mathfrak{g}_1, \ldots, \mathfrak{g}_{np}\rangle \subset (\mathbb{K}(\mathfrak{a})[U]/\mathcal{D})[X]$. According to Lemma 2, the ideal $\mathbf{I}(\mathfrak{F}^{\mathrm{h}}, 1) = (\mathcal{D}+\langle \mathfrak{g}_1, \ldots, \mathfrak{g}_{n(p-1)}\rangle)\cap \mathbb{K}(\mathfrak{a})[X]$ is zero-dimensional. Let $\prec$ denote a lexicographical monomial ordering such that for all i, j, k, $u_{i,j} \succ x_k$. Since the variables U can be expressed as functions of X ($u_{i,j} - \frac{\partial f_i}{\partial x_j} \in \mathfrak{I}_{(pn)}$), we have $\mathsf{LM}_\prec(\mathcal{D} + \langle \mathfrak{g}_1, \ldots, \mathfrak{g}_{np}\rangle) = \langle u_{i,j}\rangle + \mathsf{LM}_\prec(\mathbf{I}(\mathfrak{F}^{\mathrm{h}}, 1))$ which is zero-dimensional. Therefore, the ideal $\mathcal{D} + \langle \mathfrak{g}_1, \ldots, \mathfrak{g}_{np}\rangle \subset \mathbb{K}(\mathfrak{a})[U, X]$ is zero-dimensional and hence so is $\langle \mathfrak{g}_1, \ldots, \mathfrak{g}_{np}\rangle \subset \mathbb{K}(\mathfrak{a})[U, X]/\mathcal{D}$. Now suppose by contradiction that there exists ℓ such that $\mathfrak{g}_\ell$ divides 0 in $\mathbb{K}(\mathfrak{a})[U, X]/\,\mathfrak{I}_{(\ell-1)}$. Let ℓ_0 be the smallest integer satisfying this property. Since $\mathcal{D}$ is equidimensional and for all $\ell < \ell_0, \mathfrak{g}_\ell$ does not divide 0 in $\mathbb{K}(\mathfrak{a})[U, X]/\,\mathfrak{I}_{(\ell-1)}$, the ideal $\langle \mathfrak{g}_1, \ldots, \mathfrak{g}_{\ell_0-1}\rangle \subset \mathbb{K}(\mathfrak{a})[U, X]/\mathcal{D}$ is equidimensional, has codimension $\ell_0 - 1$, and thus has no embedded components by the unmixedness Theorem [15, Corollary 18.14]. Since $\mathfrak{g}_{\ell_0}$ divides 0 in the ring $\mathbb{K}(\mathfrak{a})[U, X]/(\mathcal{D} + \langle \mathfrak{g}_1, \ldots, \mathfrak{g}_{\ell_0-1}\rangle)$, the ideal $\langle \mathfrak{g}_1, \ldots, \mathfrak{g}_{\ell_0}\rangle \subset \mathbb{K}(\mathfrak{a})[U, X]/\mathcal{D}$ has also codimension ℓ_0-1. Therefore the codimension of $\langle \mathfrak{g}_1, \ldots, \mathfrak{g}_{np}\rangle \subset \mathbb{K}(\mathfrak{a})[U, X]/\mathcal{D}$ is strictly less than np, which leads to a contradiction since we have proved that the dimension of this ideal is 0. □

3.2 Quasi-homogeneous polynomials

The degrees in the matrix whose entries are the variables $u_{i,j}$ have to be balanced with $D-1$, the degree of the partial derivatives. This is done by changing the gradation by putting a *weight* on the variables $u_{i,j}$, giving rise to *quasi-homogeneous* polynomials. This approach has been used in [22] in the context of the Generalized MinRank Problem. A polynomial $f \in \mathbb{K}[U, X]$ is said to be *quasi-homogeneous* if the following condition is satisfied (see e.g. [25, Definition 2.11, page 120]):

$$f(\lambda^{D-1}u_{1,2}, \ldots, \lambda^{D-1}u_{p,n}, \lambda x_1, \ldots, \lambda x_k) = \lambda^d f(u_{1,2}, \ldots, u_{p,n}, x_1, \ldots, x_k).$$

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* if there exists a set of quasi-homogeneous generators of I. We let $\mathbb{K}[U, X]_d^{(w)}$ denote the $\mathbb{K}$-vector space of quasi-homogeneous polynomials of weight degree d, and $I_d^{(w)}$ denote the set $\mathbb{K}[U, X]_d^{(w)} \cap I$. Ideals generated by quasi-homogeneous polynomials are positively graded, as shown in [22, Proposition 1] that we restate below.

PROPOSITION 2 ([22, PROPOSITION 1]). *Let $I \subset \mathbb{K}[U, X]$ be an ideal. Then the following statements are equivalent:*

- *there exists a set of quasi-homogeneous generators of I;*
- *the sets $I_d^{(w)}$ are vector subspaces of $\mathbb{K}[U, X]_d^{(w)}$, and $I = \bigoplus_{d\in\mathbb{N}} I_d^{(w)}$.*

If I is a quasi-homogeneous ideal, then $\mathbb{K}[U, X]/I$ is a graded algebra and hence its weighted Hilbert series $\mathsf{wHS}_I(t) \in \mathbb{Z}[[t]]$ is well defined: $\mathsf{wHS}_I(t) = \sum_{d\in\mathbb{N}} \dim_{\mathbb{K}}(\mathbb{K}[U, X]_d^{(w)}/I_d^{(w)})t^d$.

The following lemma and its proof are similar to [22, Lemma 5].

LEMMA 5. *The Hilbert series of $\mathbf{I}(\mathfrak{F}^{\mathrm{h}}, 1) \subset \mathbb{K}(\mathfrak{a})[X]$ and the weighted Hilbert series of $\mathfrak{I}_{(pn)} \subset \mathbb{K}(\mathfrak{a})[X, U]$ are equal.*

PROOF. Let $\prec_{\mathsf{lex}}$ be a lex ordering on the variables of the polynomial ring $\mathbb{K}(\mathfrak{a})[X, U]$ such that $x_k \prec_{\mathsf{lex}} u_{i,j}$ for all k, i, j. By [14, Sec. 6.3, Prop. 9], $\mathsf{HS}_{\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1)}(t) = \mathsf{HS}_{\mathsf{LM}_{\prec_{\mathsf{lex}}}(\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1))}(t)$ and $\mathsf{wHS}_{\mathfrak{I}_{(p(n-1))}}(t) = \mathsf{wHS}_{\mathsf{LM}_{\prec_{\mathsf{lex}}}(\mathfrak{I}_{(p(n-1))})}(t)$. Since $\mathsf{LM}_{\prec_{\mathsf{lex}}}(u_{i,j} - f_{i,j}) = u_{i,j}$ and $\mathfrak{I}_{(pn)} \cap \mathbb{K}[X] = \mathbf{I}(\mathfrak{F}^{\mathrm{h}}, 1)$, we deduce that

$$\begin{array}{rcl} \mathsf{LM}_{\prec_{\mathsf{lex}}}(\mathfrak{I}_{(pn)}) & = & \left\langle \{u_{i,j}\} \cup \mathsf{LM}_{\prec_{\mathsf{lex}}}(\mathfrak{I}_{(pn)} \cap \mathbb{K}(\mathfrak{a})[X])\right\rangle \\ & = & \left\langle \{u_{i,j}\} \cup \mathsf{LM}_{\prec_{\mathsf{lex}}}(\mathbf{I}(\mathfrak{F}^{\mathrm{h}}, 1))\right\rangle. \end{array}$$

Therefore, $\frac{\mathbb{K}(\mathfrak{a})[U,X]}{\mathsf{LM}_{\prec_{\mathsf{lex}}}(\mathfrak{I}_{(pn)})}$ is isomorphic (as a graded $\mathbb{K}(\mathfrak{a})$-algebra) to $\frac{\mathbb{K}(\mathfrak{a})[X]}{\mathsf{LM}_{\prec_{\mathsf{lex}}}(\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1))}$.

Thus, $\mathsf{HS}_{\mathsf{LM}_{\prec_{\mathsf{lex}}}(\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1))}(t) = \mathsf{wHS}_{\mathsf{LM}_{\prec_{\mathsf{lex}}}(\mathfrak{I}_{(pn)})}(t)$, and hence $\mathsf{HS}_{\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1)}(t) = \mathsf{wHS}_{\mathfrak{I}_{(pn)}}(t)$. □

3.3 Proof of Proposition 1

We reuse Notations 2: $\mathbf{I}(\mathfrak{F}^{\mathrm{h}}, 1) = (\mathcal{D}+\langle \mathfrak{g}_1, \ldots, \mathfrak{g}_{pn}\rangle)\cap\mathbb{K}(\mathfrak{a})[X]$. According to Lemma 3 and by putting a weight $D - 1$ on the variables U, the weighted Hilbert series of $\mathcal{D} \subset \mathbb{K}(\mathfrak{a})[U]$ is

$$\mathsf{wHS}_{\mathcal{D}\subset\mathbb{K}(\mathfrak{a})[U]}(t) = \frac{\det A(t^{D-1})}{t^{(D-1)\binom{p-1}{2}}(1 - t^{D-1})^{n(p-1)}}.$$

Considering $\mathcal{D}$ as an ideal of $\mathbb{K}(\mathfrak{a})[X, U]$, we obtain

$$\mathsf{wHS}_{\mathcal{D}\subset\mathbb{K}(\mathfrak{a})[U,X]}(t) = \frac{1}{(1 - t)^n}\,\mathsf{wHS}_{\mathcal{D}\subset\mathbb{K}(\mathfrak{a})[U]}(t).$$

If $I \subset \mathbb{K}(\mathfrak{a})[U, X]$ is a quasi-homogeneous ideal and if g is a quasi-homogeneous polynomial of weight degree d which does not divide 0 in the quotient ring $\mathbb{K}(\mathfrak{a})[U, X]/I$, then the Hilbert series of the ideal $I + \langle g\rangle$ is equal to $(1 - t^d)$ multiplied by the Hilbert series of I (see e.g. the proof of [22, Thm 1] for more details).

Notice that the polynomials $\mathfrak{g}_1, \ldots, \mathfrak{g}_{p(n-1)}$ are quasi-homogeneous of weight degree $D - 1$ (these polynomials have the form $u_{i,j} - \frac{\partial \mathfrak{f}_i}{\partial x_j}$) and the polynomials $\mathfrak{g}_{p(n-1)+1}, \ldots, \mathfrak{g}_{pn}$ are quasi-homogeneous of weight degree D (these polynomials are $\mathfrak{f}_1, \ldots, \mathfrak{f}_p$). Since $\mathfrak{g}_\ell$ does not divide 0 in $\mathbb{K}(\mathfrak{a})[U, X]/\,\mathfrak{I}_{(\ell-1)}$ (Lemma 4), the Hilbert series of the ideal $\mathfrak{I}_{(pn)} \subset \mathbb{K}(\mathfrak{a})[X, U]$ is

$$\mathsf{wHS}_{\mathfrak{I}_{(pn)}}(t) = \frac{\det A(t^{D-1})}{t^{(D-1)\binom{p-1}{2}}}\,\frac{(1 - t^D)^p(1 - t^{D-1})^{n-p}}{(1 - t)^n}.$$

Finally, by Lemma 5, $\mathsf{wHS}_{\mathfrak{I}_{(pn)}}(t) = \mathsf{HS}_{\mathbf{I}(\mathfrak{F}^{\mathrm{h}},1)}(t)$.

4. THE AFFINE CASE

The degree of regularity of a polynomial system is the highest degree reached during the computation of a Gröbner basis with respect to the grevlex ordering with the F_5 algorithm. Therefore, it is a crucial indicator of the complexity of the Gröbner basis computation. On the other hand, the complexity of the FGLM algorithm depends on the degree of the ideal $\mathbf{I}(\mathbf{F}, 1)$ since this value is equal to $\dim_{\mathbb{K}}(\mathbb{K}[X]/\,\mathbf{I}(\mathbf{F}, 1))$.

In this section, we show that the bounds on the degree and the degree of regularity of the ideal $\mathbf{I}(\mathfrak{F}^{\mathrm{h}}, 1)$ are also valid for (not necessarily homogeneous) polynomial families in $\mathbb{K}[X]$ under genericity assumptions.

THEOREM 2. *There exists a non-empty Zariski open subset $\mathscr{O} \subset \overline{\mathbb{K}}[X]_D^p$ such that, for any $\mathbf{F}$ in $\mathscr{O} \cap \mathbb{K}[X]^p$,*

$$\begin{array}{rcl} \mathrm{d}_{\mathrm{reg}}(\mathbf{I}(\mathbf{F}, 1)) & \leq & D(p - 1) + (D - 2)n + 2, \\ \mathsf{DEG}(\mathbf{I}(\mathbf{F}, 1)) & \leq & \binom{n-1}{p-1}D^p(D - 1)^{n-p}. \end{array}$$

In the sequel, $\overline{\mathbb{K}}[X]_D$ denotes $\{f \in \overline{\mathbb{K}}[X] \mid \deg(f) = D\}$, and $\overline{\mathbb{K}}[X]_{D,\mathsf{hom}}$ denotes the homogeneous polynomials in $\overline{\mathbb{K}}[X]_D$. In order to prove Theorem 2 (the proof is postponed to the end of this section), we first need two technical lemmas.

LEMMA 6. *There exists a non-empty Zariski open subset* $\mathscr{O} \subset \overline{\mathbb{K}}[X]^p_{D,\mathsf{hom}}$ *such that for all* $\mathbf{F}^h \in \mathscr{O} \cap \mathbb{K}[X]^p$, $\mathsf{LM}_\prec(\mathbf{I}(\mathbf{F}^h, 1)) = \mathsf{LM}_\prec(\mathbf{I}(\mathfrak{F}^{\mathrm{h}}, 1))$.

PROOF. See e.g. [22, Proof of Lemma 2] for a similar proof. □

LEMMA 7. *Let* $G = (g_1, \dots, g_m)$ *be a polynomial family and let* $G^h = (g_1^h, \dots, g_m^h)$ *denote the family of homogeneous components of highest degree of* G*. If the dimension of the ideal* $\langle G^h \rangle$ *is* 0*, then* $\mathsf{DEG}(\langle G \rangle) \le \mathsf{DEG}(\langle G^h \rangle)$.

PROOF. Let $\prec$ be an admissible degree monomial ordering. Let $\mathsf{LM}_\prec(h)$ denote the leading monomial of a polynomial h with respect to $\prec$. Let $m \in \mathsf{LM}_\prec(\langle G^h \rangle)$ be a monomial. Then there exist polynomials $s_1, \dots, s_m$ such that $\mathsf{LM}_\prec\left(\sum_{i=1}^m s_i g_i^h\right) = m$. Since $\prec$ is a degree ordering, $\mathsf{LM}_\prec\left(\sum_{i=1}^m s_i g_i\right) = m$. Therefore $\mathsf{LM}_\prec(\langle G^h \rangle) \subset \mathsf{LM}_\prec(\langle G \rangle)$. If the ideal $\langle G^h \rangle$ is 0-dimensional, then so is $\langle G \rangle$ and $\mathsf{DEG}(\mathsf{LM}_\prec(\langle G \rangle)) \le \mathsf{DEG}(\mathsf{LM}_\prec(\langle G \rangle))$. Since $\mathsf{DEG}(I) = \mathsf{DEG}(\mathsf{LM}_\prec(I))$, we obtain $\mathsf{DEG}(\langle G \rangle) \le \mathsf{DEG}(\langle G^h \rangle)$. □

PROOF OF THEOREM 2. Let $\prec$ be a degree monomial ordering, and $\mathbf{F}^h = (f_1^h, \dots, f_p^h) \in \overline{\mathbb{K}}[X]^p_{D,\mathsf{hom}}$ denote the homogeneous system where f_i^h is the homogeneous component of highest degree of f_i. By Lemma 6, there exists a non-empty Zariski subset $\mathscr{O} \subset \overline{\mathbb{K}}[X]^p_D$ such that, for any $\mathbf{F}$ in $\mathscr{O} \cap \mathbb{K}[X]^p$, $\mathsf{LM}_\prec(\mathbf{I}(\mathbf{F}^h, 1)) = \mathsf{LM}_\prec(\mathbf{I}(\mathfrak{F}^{\mathrm{h}}, 1))$. By [14, Ch.9, §3, Prop.9], the Hilbert series (and thus the dimension, the degree, and the degree of regularity) of a homogeneous ideal is the same as that of its leading monomial ideal. Hence, by Lemma 2,

$$\begin{aligned}\dim(\mathbf{I}(\mathbf{F}^h, 1)) = \dim(\mathsf{LM}_\prec(\mathbf{I}(\mathbf{F}^h, 1))) &= \dim(\mathsf{LM}_\prec(\mathbf{I}(\mathfrak{F}^{\mathrm{h}}, 1))) \\ &= \dim(\mathbf{I}(\mathfrak{F}^{\mathrm{h}}, 1)) = 0.\end{aligned}$$

Similarly, by Theorem 1,

$$\mathrm{d}_{\mathrm{reg}}(\mathbf{I}(\mathbf{F}^h, 1)) = \mathrm{d}_{\mathrm{reg}}(\mathbf{I}(\mathfrak{F}^{\mathrm{h}}, 1)) = D(p-1) + (D-2)n + 2.$$

The highest degree reached during the F_5 Algorithm is upper bounded by the degree of regularity of the ideal generated by the homogeneous components of highest degree of the generators when this homogeneous ideal has dimension 0 (see e.g. [8] and references therein). Therefore, the highest degree reached during the computation of a Gröbner basis of $\mathbf{I}(\mathbf{F}, 1)$ with the F_5 Algorithm with respect to a degree ordering is upper bounded by

$$\mathrm{d}_{\mathrm{reg}} \le D(p-1) + (D-2)n + 2.$$

The bound on the degree is obtained by Corollary 2 and Lemma 7,

$$\begin{aligned}\mathsf{DEG}(\mathbf{I}(\mathbf{F}, 1)) \le \mathsf{DEG}(\mathbf{I}(\mathbf{F}^h, 1)) &\le \mathsf{DEG}(\mathsf{LM}_\prec(\mathbf{I}(\mathfrak{F}^{\mathrm{h}}, 1))) \\ &\le \tbinom{n-1}{p-1} D^p (D-1)^{n-p}.\end{aligned}$$

□

5. COMPLEXITY

In the sequel, ω is a real number such that there exists an algorithm which computes the row echelon form of $n \times n$ matrix in $O(n^\omega)$ arithmetic operations (the best known value is $\omega \approx 2.376$ by using the Coppersmith-Winograd algorithm, see [39]).

THEOREM 3. *There exists a non-empty Zariski open subset* $\mathscr{O} \subset \overline{\mathbb{K}}[X]^p_D$*, such that, for all* $\mathbf{F} \in \mathscr{O} \cap \mathbb{K}[X]^p$*, the arithmetic complexity of computing a lexicographical Gröbner basis of* $\mathbf{I}(\mathbf{F}, 1)$ *is upper bounded by*

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

PROOF. According to [7, 8], the complexity of computing a Gröbner basis with the F_5 Algorithm with respect to the grevlex ordering of a zero-dimensional ideal is bounded by $O\left(\binom{n+\mathrm{d}_{\mathrm{reg}}}{\mathrm{d}_{\mathrm{reg}}}^\omega\right)$ where $\mathrm{d}_{\mathrm{reg}}$ is the highest degree reached during the computation. In order to obtain a lexicographical Gröbner basis, one can use the FGLM algorithm [19]. Its complexity is $O\left(n\,\mathsf{DEG}(\mathbf{I}(\mathbf{F}, 1))^3\right)$ (better complexity bounds are known in specific cases, see [20]).

According to Theorem 2, there exists a non-empty Zariski open subset $\mathscr{O} \subset \overline{\mathbb{K}}[X]^p_D$ such that, for all $\mathbf{F}$ in $\mathscr{O} \cap \mathbb{K}[X]^p$,

$$\begin{array}{rcl}\mathrm{d}_{\mathrm{reg}}(\mathbf{I}(\mathbf{F}, 1)) & \le & D(p-1) + (D-2)n + 2, \\ \mathsf{DEG}(\mathbf{I}(\mathbf{F}, 1)) & \le & \binom{n-1}{p-1} D^p (D-1)^{n-p}.\end{array}$$

Therefore, for all $\mathbf{F}$ in $\mathscr{O} \cap \mathbb{K}[X]^p$, the total complexity of computing a lexicographical Gröbner basis of $\mathbf{I}(\mathbf{F}, 1)$:

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

□

COROLLARY 3. *If* $D = 2$*, then there exists a non-empty Zariski open subset* $\mathscr{O} \subset \overline{\mathbb{K}}[X]^p_2$*, such that for all* $\mathbf{F} \in \mathscr{O} \cap \mathbb{K}[X]^p$*, the arithmetic complexity of computing a lexicographical Gröbner basis of* $\mathbf{I}(\mathbf{F}, 1)$ *is upper bounded by*

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

Moreover, if p *is constant and* $D = 2$*, the arithmetic complexity is upper bounded by* $O\left(n^{2p\omega}\right)$.

PROOF. This complexity is obtained by putting $D = 2$ in the formula from Theorem 3. □

In the sequel, the binary entropy function is denoted by h_2:

$$\forall x \in [0, 1], h_2(x) = -x\log_2(x) - (1-x)\log_2(1-x).$$

COROLLARY 4. *Let* $D > 2$ *and* $p \in \mathbb{N}$ *be constant. There exists a non-empty Zariski open subset* $\mathscr{O} \subset \overline{\mathbb{K}}[X]^p_D$*, such that, for all* $\mathbf{F} \in \mathscr{O} \cap \mathbb{K}[X]^p$*, the arithmetic complexity of computing a lexicographical Gröbner basis of* $\mathbf{I}(\mathbf{F}, 1)$ *is upper bounded by*

$$O\left(\frac{1}{\sqrt{n}} 2^{(D-1)h_2\left(\frac{1}{D-1}\right)n\omega}\right) = O\left((D-1)^{3.57n}\right).$$

PROOF. Let x be a real number in $[0, 1]$. Then by applying Stirling's Formula, we obtain that $\binom{n}{xn} = O\left(\frac{1}{\sqrt{n}} 2^{h_2(x)n}\right)$. Therefore,

$$\begin{array}{rcl}\binom{(D-1)n}{n} & = & O\left(\frac{1}{\sqrt{n}} 2^{(D-1)h_2\left(\frac{1}{D-1}\right)n}\right) \\ & = & O\left(\frac{1}{\sqrt{n}}((D-1)e)^n\right).\end{array}$$

Let C denote the constant $D(p-1) + 2$. Then

$$\begin{array}{rcl}\binom{D(p-1)+(D-1)n+2}{D(p-1)+(D-2)n+2} & = & \binom{(D-1)n+C}{n} = O\left(\binom{(D-1)n}{n}\right) \\ & = & O\left(\frac{1}{\sqrt{n}} 2^{(D-1)h_2\left(\frac{1}{D-1}\right)n}\right).\end{array}$$

The right summand in the complexity formula given in Theorem 3 is $O\left(n^{3p}(D-1)^{3n}\right)$ when p and D are constants; this is upper bounded by $O\left(\frac{1}{\sqrt{n}} 2^{(D-1)h_2\left(\frac{1}{D-1}\right)n\omega}\right)$. Let $\mathscr{O}$ be the non-empty Zariski open subset defined in Theorem 3. For all $\mathbf{F} \in \mathscr{O} \cap \mathbb{K}[X]^p$, the arithmetic complexity of computing a grevlex Gröbner basis of $\mathbf{F}$ is upper bounded by

$$\begin{aligned}O\left(\frac{1}{\sqrt{n}} 2^{(D-1)h_2\left(\frac{1}{D-1}\right)n\omega}\right) &= O\left(\frac{1}{\sqrt{n}}((D-1)e)^{n\omega}\right) \\ &= O\left((D-1)^{(1+1/\log(D-1))n\omega}\right) \\ &= O\left((D-1)^{3.57n}\right),\end{aligned}$$

since $D \ge 3$ and $\omega \le 2.376$ with the Coppersmith-Winograd algorithm. On the other hand the asymptotic complexity of the FGLM part of the solving process is

$$O\left(n^{3(p-1)+1}(D-1)^{3n}\right) = \widetilde{O}\left((D-1)^{3n}\right),$$

which is upper bounded by the complexity of the grevlex Gröbner basis computation. □

The following corollary shows that the arithmetic complexity is polynomial in the number of critical points.

COROLLARY 5. *For $D \geq 3$, $p \geq 2$ and $n \geq 2$, There exists a non-empty Zariski open subset $\mathscr{O} \subset \overline{\mathbb{K}}[X]_D^p$, such that, for $\mathbf{F} \in \mathscr{O} \cap \mathbb{K}[X]^p$, the arithmetic complexity of computing a lexicographical Gröbner basis of* $\mathbf{I}(\mathbf{F}, 1)$ *is upper bounded by*

$$O\left(\mathsf{DEG}\left(\mathbf{I}(\mathbf{F},1)\right)^{\max\left(\frac{\log(2eD)}{\log(D-1)}\omega,4\right)}\right) \leq O\left(\mathsf{DEG}\left(\mathbf{I}(\mathbf{F},1)\right)^{4.03\omega}\right).$$

PROOF. Let $\mathscr{O} \subset \overline{\mathbb{K}}[X]_D^p$ be the non-empty Zariski open subset defined in Theorem 2, and $\mathbf{F} \in \mathscr{O} \cap \mathbb{K}[X]_D^p$ be a polynomial family. First, notice that, since $p \geq 2$ and $n \geq 2$,

$$\begin{array}{rcl} \mathsf{DEG}\left(\mathbf{I}(\mathbf{F},1)\right) & = & \binom{n-1}{p-1}(D-1)^{n-p}D^p \\ & \geq & n \end{array}$$

Therefore the complexity of the FGLM algorithm is upper bounded by $O\left(n\,\mathsf{DEG}\left(\mathbf{I}(\mathbf{F},1)\right)^3\right) \leq O\left(\mathsf{DEG}\left(\mathbf{I}(\mathbf{F},1)\right)^4\right)$. The complexity of computing a grevlex Gröbner basis of $\mathbf{I}(\mathbf{F}, 1)$ is upper bounded by

$$\begin{aligned} \mathsf{GREVLEX}(p,n,D) &= O\left(\binom{D(p-1)+(D-1)n+2}{n}^{\omega}\right) \\ &\leq O\left(\binom{2Dn}{n}^{\omega}\right). \end{aligned}$$

Notice that $\binom{2Dn}{n} \leq (2D)^n \frac{n^n}{n!}$. By Stirling's formula, there exists C_0 such that $\frac{n^n}{n!} \leq C_0 e^n$. Hence $\mathsf{GREVLEX}(p, n, D) = O\left((2De)^n\right)$.

Since $D \geq 3$ and $n \leq \log(\mathsf{DEG}(\mathbf{I}(\mathbf{F}, 1)))/\log(D - 1)$, we obtain

$$\begin{array}{rcl} O\left((2De)^{n\omega}\right) & \leq & O\left(D^{\frac{\log(2eD)}{\log D}n\omega}\right) \\ & \leq & O\left(\mathsf{DEG}\left(\mathbf{I}(\mathbf{F},1)\right)^{\frac{\log(2eD)}{\log(D-1)}\omega}\right). \end{array}$$

The function $D \mapsto \frac{\log(2eD)}{\log(D-1)}$ is decreasing, and hence its maximum is reached for $D = 3$, and $\frac{\log(6e)}{\log(2)} \leq 4.03$. □

Notice that in the complexity formula in Corollary 5, the exponent $\frac{\log(2eD)}{\log(D-1)}\omega$ tends towards ω when D grows. Therefore, when D is large, the complexity of the grevlex Gröbner basis computation is close to the cost of linear algebra $O\left(\mathsf{DEG}(\mathbf{I}(\mathbf{F},1))^{\omega}\right)$. Also, we would like to point out that the bound in Corollary 5 is not sharp since the formula $O\left(\binom{n+\mathrm{d}_{\mathrm{reg}}}{n}^{\omega}\right)$ for the complexity of the F_5 algorithm is pessimistic, and the majorations performed in the proof of Corollary 5 are not tight.

6. EXPERIMENTAL RESULTS

In this section, we report experimental results supporting the theoretical complexity results in the previous sections. Since our complexity results concern the arithmetic complexity, we run experiments where $\mathbb{K}$ is the finite field $\mathsf{GF}(65521)$ (Tables 1 and 2), so that the timings represent the arithmetic complexity. In that case, systems are chosen uniformly at random in $\mathsf{GF}(65521)[X]_D$.

We give experiments by using respectively the implementation of F_4 and FGLM algorithms in the MAGMA Computer Algebra Software, and by using the F_5 and FGLM implementations from the FGb package.

Experiments were conducted on a 2.93GHz Intel Xeon E7220 with 128 GB RAM.

Interpretation of the results. Notice that the degree of regularity and the degree match exactly the bounds given in Theorem 2. In Tables 1 and 2, we can see a different behavior when $D = 2$ or $D = 3$. In the case $D = 2$, since the complexity is polynomial in n (Corollary 3), the computations can be performed even when n is large (close to 20). Moreover, notice that for $D = 2$ or $D = 3$, there is a strong correlation between the degree of the ideal and the timings, showing that, in accordance with Corollary 5, this degree is a good indicator of the complexity.

n	p	D	$\mathrm{d}_{\mathrm{reg}}$	DEG	F_4 time	FGLM time
9	4	2	8	896	3.12s	18.5s
11	4	2	8	1920	61s	202s
13	4	2	8	3520	369s	1372s
15	4	2	8	5824	2280s	7027s
17	4	2	8	8960	10905s	>1d
30	2	2	4	116	3.00s	0.14s
35	2	2	4	136	7.5s	0.36s
40	2	2	4	156	13.3s	0.64s
6	4	3	17	3240	16s	400s
8	4	3	19	45360	35593s	>1d
7	2	3	12	1728	9.9s	91s
8	2	3	13	4032	121s	1169s
9	2	3	14	9216	736s	>1d

Table 1: Experiments in MAGMA measuring the arithmetic complexity ($\mathbb{K} = \mathsf{GF}(65521)$).

n	p	D	$\mathsf{DEG}(\mathbf{I}(\mathbf{F},1))$	F_5 time	FGLM time	matrix density
16	3	2	840	2.20s	0.03s	36.91%
18	3	2	1088	4.62s	0.12s	37.00%
20	3	2	1368	9.54s	0.10s	37.07%
15	4	2	5824	131.65	10.66s	33.53%
17	4	2	8960	480.9s	68.9s	34.00%
19	4	2	13056	1600.1s	215.1s	34.35%
21	4	2	18240	10371.7s	590.3s	34.62%
10	1	3	1536	1.5s	0.15s	20.84%
12	1	3	6144	19.6s	2.46s	19.32%
14	1	3	24576	1759s	587s	18.08%
7	2	3	1728	1.4s	0.14s	20.73%
9	2	3	9216	105s	37s	19.47%
10	2	3	20736	909s	504s	19.08%
7	3	3	6480	31.3s	3.81s	17.39%
8	4	3	45360	5126.9s	3833.9s	15.15%
8	2	4	81648	21362.6s	19349.4s	13.26%
7	3	4	77760	13856.8s	16003s	11.83%

Table 2: Timings using the FGb library and $\mathbb{K} = \mathsf{GF}(65521)$.

Also, in Table 2, we give the proportion of non-zero entries in the multiplication matrices. This proportion plays an important role in the complexity of FGLM, since recent versions of FGLM take advantage of this sparsity [20]. We can notice that the sparsity of the multiplication matrices increases as D grows.

Numerical estimates of the complexity. Corollary 5 states that the complexity of the grevlex Gröbner basis computation is upper bounded by $O\left(\mathsf{DEG}(\mathbf{I}(\mathbf{F},1))^{4.03\omega}\right)$ when $D \geq 3$, $p \geq 2$, $n \geq 2$. However, the value 4.03 is not sharp. In Table 3, we report numerical values of the ratio $\log\binom{n+\mathrm{d}_{\mathrm{reg}}}{n} / \log\left(\mathsf{DEG}(\mathbf{I}(\mathbf{F},1))\right)$ which show the difference between 4.03 and experimental values.

Notice that all ratios are smaller than 4.03, as predicted by Corollary 5. Experimentally, the ratio decreases and tends towards 1

n	p	D	$\log\binom{n+\mathrm{d}_{\mathrm{reg}}}{n} / \log(\mathsf{DEG})$
5	4	3	1.53
10	4	3	1.36
100	4	3	1.73
10000	4	3	1.99
10000	9999	3	2.28
30000	29999	3	2.28
1000	500	3	1.32
20000	2	3	2.00
500	250	1000	1.09
500	2	10000	1.11

Table 3: Numerical values: $\log\binom{n+\mathrm{d}_{\mathrm{reg}}}{n} / \log\left(\mathsf{DEG}(\mathbf{I}(\mathbf{F},1))\right)$.

when D grows, in accordance with the complexity formula

$$O\left(\mathsf{DEG}\left(\mathbf{I}(\mathbf{F},1)\right)^{\frac{\log(2eD)}{\log(D-1)}\omega}\right)$$

for the grevlex Gröbner basis computation. Also, when $D \geq 3$, the worst ratio seems to be reached when $p = n-1$, $D = 3$ and n grows, and experiments in Table 3 tend to show that it is bounded from above by 2.28.

Systems with rational coefficients. In applications, the critical points appearing are most often with rational coefficients. However, by using a multi-modular approach, the bit complexity of the lexicographical Gröbner basis computation will be quasi-linear in the heights of these coefficients. Therefore, the whole bit complexity will still be polynomial in the bit size of the output (the lex Gröbner basis). For instance, with the FGb library, the lex Gröbner basis of a critical point system with $p = 1$, $D = 4$ and $n = 7$ and integer coefficients between -99 and 99 was computed in 45 minutes.

Nevertheless, it is still an interesting question to obtain good theoretical bounds on the heights of the polynomials in the lex Gröbner basis of critical point system – in particular in order to know if the bit complexity is still polynomial in the number variables in the case $D = 2$. We plan to investigate these issues in future works.

References

[1] P. Aubry, F. Rouillier, and M. Safey El Din. Real solving for positive dimensional systems. *Journal of Symbolic Computation*, 34(6):543–560, 2002.

[2] B. Bank, M. Giusti, J. Heintz, and G.-M. Mbakop. Polar varieties and efficient real equation solving: the hypersurface case. *Journal of Complexity*, 13(1):5–27, 1997.

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

[4] B. Bank, M. Giusti, J. Heintz, and L.-M. Pardo. Generalized polar varieties and efficient real elimination procedure. *Kybernetika*, 40(5):519–550, 2004.

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

[6] B. Bank, M. Giusti, J. Heintz, M. Safey El Din, and E. Schost. On the Geometry of Polar Varieties. *Applicable Algebra in Engineering, Communication and Computing*, 21(1):33–83, 2010.

[7] M. Bardet, J.-C. Faugère, and B. Salvy. On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations. In *Proceedings of the International Conference on Polynomial System Solving (ISCPP)*, pages 71–74, 2004.

[8] M. Bardet, J.-C. Faugère, B. Salvy, and B.-Y. Yang. Asymptotic expansion of the degree of regularity for semi-regular systems of equations. In *Effective Methods in Algebraic Geometry (MEGA)*, pages 71–74, 2004.

[9] A. Barvinok. Feasibility testing for systems of real quadratic equations. *Discrete & Computational Geometry*, 10(1):1–13, 1993.

[10] S. Basu, R. Pollack, and M.-F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. *Journal of ACM*, 43(6):1002–1045, 1996.

[11] S. Basu, R. Pollack, and M.-F. Roy. A new algorithm to find a point in every cell defined by a family of polynomials. In *Quantifier elimination and cylindrical algebraic decomposition*. Springer-Verlag, 1998.

[12] L. Busé. Resultants of determinantal varieties. *Journal of Pure and Applied Algebra*, 193(1-3):71–97, 2004.

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

[14] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties and Algorithms*. Springer, 3rd edition, 1997.

[15] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Springer, 1995.

[16] H. Everett, D. Lazard, S. Lazard, and M. Safey El Din. The voronoi diagram of three lines. *Discrete & Computational Geometry*, 42(1):94–130, 2009.

[17] J. Faugère, G. Moroz, F. Rouillier, and M. Safey El Din. Classification of the perspective-three-point problem, discriminant variety and real solving polynomial systems of inequalities. In *Proceedings of the twenty-first international symposium on Symbolic and algebraic computation*, pages 79–86. ACM, 2008.

[18] J.-C. Faugère. A New Efficient Algorithm for Computing Gröbner bases without reductions to zero (F5). In T. Mora, editor, *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation (ISSAC)*, pages 75–83. ACM Press, 2002.

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

[20] J.-C. Faugère and C. Mou. Fast Algorithm for Change of Ordering of Zero-dimensional Gröbner Bases with Sparse Multiplication Matrices. In *Proceedings of the 36th international symposium on Symbolic and algebraic computation*, ISSAC '11, pages 115–122, New York, NY, USA, 2011. ACM.

[21] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. Computing Loci of Rank Defects of Linear Matrices using Gröbner Bases and Applications to Cryptology. In S. M. Watt, editor, *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation (ISSAC 2010)*, pages 257–264, 2010.

[22] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. On the complexity of the Generalized Minrank Problem. arXiv:1112.4411, 2011.

[23] W. Fulton. *Intersection Theory*. Springer, 2nd edition, 1997.

[24] M. Giusti, G. Lecerf, and B. Salvy. A Gröbner free alternative for polynomial system solving. *Journal of Complexity*, 17(1):154–211, 2001.

[25] G. Greuel, C. Lossen, and E. Shustin. *Introduction to singularities and deformations*. Springer, 2007.

[26] D. Grigoriev and D. V. Pasechnik. Polynomial-time computing over quadratic maps i: sampling in real algebraic sets. *Computational Complexity*, 14(1):20–52, Apr. 2005.

[27] D. Grigoriev and N. Vorobjov. Solving systems of polynomials inequalities in subexponential time. *Journal of Symbolic Computation*, 5:37–64, 1988.

[28] J. Heintz, M.-F. Roy, and P. Solernò. On the complexity of semi-algebraic sets. In *Proceedings IFIP'89 San Francisco, North-Holland*, 1989.

[29] J. Heintz, M.-F. Roy, and P. Solernò. On the theoretical and practical complexity of the existential theory of the reals. *The Computer Journal*, 36(5):427–431, 1993.

[30] M. Hochster and J. A. Eagon. A class of perfect determinantal ideals. *Bulletin of the American Mathematical Society*, 76(5):1026–1029, 1970.

[31] M. Hochster and J. A. Eagon. Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci. *American Journal of Mathematics*, 93(4):1020–1058, 1971.

[32] H. Hong and M. Safey El Din. Variant real quantifier elimination: algorithm and application. In *Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation*, pages 183–190. ACM, 2009.

[33] H. Hong and M. Safey El Din. Variant quantifier elimination. *Journal of Symbolic Computation*, 2011.

[34] J. Nie and K. Ranestad. Algebraic Degree of Polynomial Optimization. *SIAM Journal on Optimization*, 20(1):485–502, 2009.

[35] M. Safey El Din. Testing sign conditions on a multivariate polynomial and applications. *Mathematics in Computer Science*, 1(1):177–207, 2007.

[36] M. Safey El Din and E. Schost. Polar varieties and computation of one point in each connected component of a smooth real algebraic set. In J. Sendra, editor, *Proceedings of ISSAC 2003*, pages 224–231. ACM Press, aug 2003.

[37] M. Safey El Din and É. Schost. Properness defects of projections and computation of one point in each connected component of a real algebraic set. *Discrete and Computational Geometry*, 32(3):417–430, 2004.

[38] I. Shafarevich. *Basic Algebraic Geometry I*. Springer, second, re edition, 1988.

[39] A. Storjohann. *Algorithms for Matrix Canonical Forms*. PhD thesis, University of Waterloo, 2000.