ON THE COMPLEXITY OF COMPUTING CRITICAL POINTS WITH GRÖBNER BASES[*]

PIERRE-JEAN SPAENLEHAUER[†]

Abstract. Computing the critical points of a polynomial function $q \in \mathbb{Q}[X_1, \ldots, X_n]$ restricted to the vanishing locus $V \subset \mathbb{R}^n$ of polynomials $f_1, \ldots, f_p \in \mathbb{Q}[X_1, \ldots, X_n]$ is of first importance in several applications in optimization and in real algebraic geometry. These points are solutions of a highly structured system of multivariate polynomial equations involving maximal minors of a Jacobian matrix. We investigate the complexity of solving this problem by using Gröbner basis algorithms under genericity assumptions on the coefficients of the input polynomials. The main results refine known complexity bounds (which depend on the maximum $D = \max(\deg(f_1), \ldots, \deg(f_p), \deg(q))$) to bounds which depend on the list $(\deg(f_1), \ldots, \deg(f_p), \deg(q))$: we prove that the Gröbner basis computation can be performed in $\delta^{O(\log(A)/\log(G))}$ arithmetic operations in $\mathbb{Q}$, where δ is the algebraic degree of the ideal vanishing on the critical points, and A and G are the arithmetic and geometric average of a multiset constructed from the sequence of degrees. As a by-product, we prove that solving such generic optimization problems with Gröbner bases requires at most $D^{O(n)}$ arithmetic operations in $\mathbb{Q}$, which meets the best-known complexity bound for this problem. Finally, we illustrate these complexity results with experiments, giving evidence that these bounds are relevant for applications.

Key words. critical points, polynomial minimization, complexity, Gröbner bases, structured polynomial system

AMS subject classifications. 90C26, 13P10, 13P15, 13P25

DOI. 10.1137/130936294

1. Introduction.

1.1. Problem statement and motivations. Let $p < n$ be two positive integers, $q, f_1, \ldots, f_p \in \mathbb{Q}[X_1, \ldots, X_n]$ be polynomials with rational coefficients, and $\mathbf{I}(q, \mathbf{F}) \subset \mathbb{Q}[X_1, \ldots, X_n]$ be the ideal generated by the maximal minors of the Jacobian matrix $\mathsf{jac}(q, f_1, \ldots, f_p)$ and by the polynomials $\mathbf{F} = (f_1, \ldots, f_p)$:

$$\mathbf{I}(q, \mathbf{F}) = \langle \mathsf{MaxMinors}(\mathsf{jac}(q, \mathbf{F})) \rangle + \langle \mathbf{F} \rangle.$$

Also, let $V \subset \mathbb{C}^n$ denote the variety associated with the polynomial system $f_1, \ldots, f_p$. If V is smooth, then the ideal $\mathbf{I}(q, \mathbf{F})$ is the set of polynomials vanishing on the critical points of the function q restricted to V. Computing these critical points is of first importance in a wide range of applications in optimization and in geometry, since the real local extrema of q under the constraints $f_1 = \cdots = f_p = 0$ are reached at such points.

Our strategy is to compute these critical points by a classical solving strategy with Gröbner bases algorithms (Buchberger [14], F_4 [22], F_5 [23], and FGLM [24]): we compute a parametrization of the critical points by the roots of a univariate polynomial via a lexicographical Gröbner basis of $\mathbf{I}(q, \mathbf{F})$ [41]. Once such a representation

is obtained, numerical algorithms can provide certified approximations of the critical points from the roots of the univariate polynomial.

It has been noticed that Gröbner bases algorithms perform well in practice on these families of polynomial systems and critical point computations are intensively used in the two software packages `Hexagon`[1] (for global optimization) and `RAGlib`[2] (for computational real algebraic geometry). Both of these software packages rely on the implementation of the F_5 algorithm [23] in the `FGb` library.[3] It is not the aim of this paper to propose new algorithms: the goal is to explain the efficiency of this approach by providing complexity bounds that reflect the experimental behavior of these Gröbner bases computations.

1.2. Main results. Let $\delta = \mathsf{DEG}(\mathbf{I}(q, \mathbf{F}))$ denote the degree of the ideal $\mathbf{I}(q, \mathbf{F})$ vanishing on the complex critical points. Classical results on the algebraic degree of polynomial optimization show that δ is, in general, exponential in n and in p. An important exception is the case of quadratic programming: in that case, δ is polynomial in the number of variables n (but still exponential in the codimension p) and this phenomenon is related to the existence of algorithms running in time polynomial in n in this special case [11, 30, 27].

The value δ is an important indicator of the algebraic complexity of the problem: under genericity assumptions on the input polynomials, the ideal $\mathbf{I}(q, \mathbf{F})$ is radical (all the critical points have multiplicity 1) and hence δ equals the number of complex critical points. Even though the number of real critical points is usually much lower than δ, in general, their coordinates lie in a field extension of $\mathbb{Q}$ of degree δ. Consequently, the complexity of Gröbner bases algorithms is lower bounded by this value and we wish to express all upper complexity bounds in terms of this lower bound. In this setting, the main result of this paper is the following theorem.

THEOREM 1.1. *Let $q, f_1, \ldots, f_p \in \mathbb{Q}[X_1, \ldots, X_n]$ be polynomials of respective degrees $d_0, d_1, \ldots, d_p \in \mathbb{N}$. Let A (resp., G) be the arithmetic (resp., geometric) average of the multiset*

$$\{d_1, \ldots, d_p, \underbrace{\max_{0 \leq i \leq p}\{d_i - 1\}, \ldots, \max_{0 \leq i \leq p}\{d_i - 1\}}_{n-p}\}.$$

Then, under genericity assumptions on the coefficients of $q, f_1, \ldots, f_p$, a lexicographical Gröbner basis of $\mathbf{I}(q, \mathbf{F})$ can be computed within

$$\delta^{O(\log(A)/\log(G))} \text{ arithmetic operations in } \mathbb{Q}.$$

In particular, by rephrasing this theorem and by bounding above $\log(A)/\log(G)$, we obtain the following complexity estimates in terms of the input size.

COROLLARY 1.2. *Let $D = \max\{\deg(f_1), \ldots, \deg(f_p), \deg(q)\}$ denote the maximum of the degrees of the input polynomials. Under genericity assumptions on the coefficients of the input system, the complexity of computing a lexicographical Gröbner basis of $\mathbf{I}(q, \mathbf{F})$ by classical Gröbner bases algorithms requires at most*

$$D^{O(n)} \text{ arithmetic operations in } \mathbb{Q}.$$

The bound $D^{O(n)}$ meets the best-known bound for the exact computation of such critical points [44, Thm. 8], [43, section 10.3].

---

[1]Written by Aurélien Greuet, http://www.lifl.fr/~greuet/indexFR.html.
[2]Written by Mohab Safey El Din, http://www-polsys.lip6.fr/~safey/RAGLib/.
[3]Written by Jean-Charles Faugère, http://www-polsys.lip6.fr/~jcf/Software/FGb/.

1.3. Roadmap of the proof. In order to compute a lexicographical Gröbner basis of $\mathbf{I}(q, \mathbf{F})$, we use a classical approach: first, we compute a *graded reverse lexicographical* (*grevlex* for short) Gröbner basis of $\mathbf{I}(q, \mathbf{F})$, then we use the FGLM algorithm to convert this Gröbner basis into a *lexicographical* (*lex*) Gröbner basis. The complexity of FGLM is well known [24, Prop. 4.1] and bounded above by $\delta^{O(1)}$. Consequently, we focus on the complexity of the first step of the solving process, namely, the computation of the grevlex Gröbner basis.

Let $f_1, \ldots, f_p, m_1, \ldots, m_{\binom{n}{p+1}}$ be the generators of $\mathbf{I}(q, \mathbf{F})$, i.e., the input polynomials and the maximal minors of the Jacobian matrix. It is known that a grevlex Gröbner basis can be obtained by computing the row echelon form of a matrix (the *Macaulay matrix*), which is parametrized by a degree $d \in \mathbb{N}$. Its row span is the $\mathbb{Q}$-vector space

$$T_d = \left\{ \sum_{i=1}^{p} f_i \alpha_i + \sum_{j=1}^{\binom{n}{p+1}} m_j \beta_j \mid \alpha_i, \beta_j \in \mathbb{Q}[X_1, \ldots, X_n], \deg(f_i \alpha_i) \leq d, \deg(m_j \beta_j) \leq d \right\}.$$

The minimal value of d such that a grevlex Gröbner basis of $\mathbf{I}(q, \mathbf{F})$ is included in T_d is called the *witness degree* $\mathrm{d}_{\mathrm{wit}}$ of the system (see, e.g., [10, section 2.2]). A crucial step in the proof of the main complexity result is to estimate $\mathrm{d}_{\mathrm{wit}}$: under genericity assumptions on the coefficients of $q, f_1, \ldots, f_p$ (Corollary 3.2), we show the inequality

$$\mathrm{d}_{\mathrm{wit}} \leq (n - p - 1) \max_{0 \leq i \leq p} \{d_i - 1\} - n - p + d_0 + 2 \sum_{1 \leq i \leq p} d_i.$$

To obtain this inequality, we first consider the case where all polynomials $q, f_1, \ldots, f_p$ are homogeneous with generic coefficients. In that case, the witness degree equals the *degree of regularity*, i.e., the smallest degree $d \in \mathbb{N}$ where the Hilbert function of the graded ring $\mathbb{Q}[X_1, \ldots, X_n] / \mathbf{I}(q, \mathbf{F})$ becomes zero.

Next, we use techniques from commutative algebra to derive an explicit formula for this Hilbert function. This formula is obtained by isolating the determinantal part of the ideal (Corollary 2.3) and by using the Eagon–Northcott complex [19][21, Appendix A2H] to analyze this determinantal component (Proposition 3.1). In fact, under genericity assumptions on the coefficients of $(q, \mathbf{F})$, the Eagon–Northcott complex associated with the Jacobian matrix $\mathsf{jac}(q, \mathbf{F})$ provides a *graded free resolution* of the ideal generated by its maximal minors, from which the Hilbert series can be extracted.

The inequality on the witness degree allows us to bound the dimension of the $\mathbb{Q}$-vector space $T_{\mathrm{d}_{\mathrm{wit}}}$: its dimension is at most $\binom{(n-p-1)\max_{0 \leq i \leq p}\{d_i-1\}-p+d_0+2\sum_{1 \leq i \leq p} d_i}{n}$. A grevlex Gröbner basis can be obtained by performing linear algebra in $S_{\mathrm{d}_{\mathrm{wit}}}$: this can be done within

$$O\left(\left(p + \binom{n}{p+1} \right) \binom{n + \mathrm{d}_{\mathrm{wit}}}{n}^{\omega} \right)$$

operations in $\mathbb{Q}$, where ω is a feasible exponent for the matrix multiplication ($\omega \leq 2.373$ with Williams' algorithm [47]). Rewriting this complexity bound in terms of the input degrees yields the claimed complexity bounds.

1.4. Related work. The results in this paper generalize the main results in [27] which were restricted to the special case $q(X_1, \ldots, X_n) = X_1$ (i.e., $d_0 = 1$) and $d_1 = \cdots = d_p = D \in \mathbb{N}$. The complexity analysis was simpler in that case: assuming that the degrees of the input polynomials are equal simplifies the combinatorial and

algebraic structure of the ideal vanishing on the critical points. In this paper, we propose other algebraic tools in order to take into account the combinatorial structure induced by the mixed grading due to the different degrees of general input polynomials. In particular, ideals generated by maximal minors play an important role. When the grading is not uniform, general formulas for the Hilbert series and for the Castelnuovo regularity of such ideals are derived in [15].

A classical problem in optimization is to compute a minimizer of a polynomial program of the form

$$(1.1) \quad \begin{cases} \text{compute } \min_{(X_1,\dots,X_n)\in\mathbb{R}} q(X_1,\dots,X_n) \text{ under the constraints} \\ f_1(X_1,\dots,X_n) = \cdots = f_p(X_1,\dots,X_n) = 0. \end{cases}$$

Inequalities can also be added to the set of constraints but this does not change the algebraic degree of the problem if the minimizer lies in the interior of the feasible set. Such a minimizer is a critical point of q restricted to the variety associated with $f_1,\dots,f_p$. The explicit formula for the algebraic degree of this problem is given in [38, Theorem 2.2] under genericity assumptions on the input polynomials:

$$\delta = \left(\prod_{1\leq i\leq p} d_i\right) \sum_{i_0+\cdots+i_p=n-p} (d_0-1)^{i_0}\dots(d_p-1)^{i_p}.$$

Another area where such optimization problems appear frequently is computational real algebraic geometry. For instance, the *critical point method* is a general algorithmic framework for the study of topological properties of real algebraic varieties. The cornerstone of these methods is the computation of critical points of projections of varieties on linear subspaces and have led to efficient algorithms with optimal or near-optimal complexity for solving problems in real algebraic geometry [31, 16, 12, 30, 11]. *Polar varieties* describe the geometry of these critical loci and have also given rise to large families of algorithms [46, 2, 1, 6, 5, 42, 3, 8]. In particular, [7] gives complexity bounds that are polynomial in a geometrically defined quantity for solving these polynomial optimization problems with geometric resolution techniques [29], leading to a complexity bound $(nD)^{O(n)}$ in the worst case.

The critical points of a function under polynomial constraints can also be described as the set of solutions of a *bihomogeneous system* using *Lagrange multipliers*. This connection between determinantal systems and bihomogeneous systems appears quite frequently; for instance, in the Room–Kempf desingularization of determinantal varieties [40] (see also [4]), or in the Kipnis–Shamir modeling of the MinRank problem [33, 25, 26]. This modeling was used to obtain complexity bounds $D^{O(n)}$ by using the geometric resolution algorithm [44, Thm. 8]. In the context of generalized Lagrange systems, similar complexity bounds are proved in [43, section 10.3].

Other applications of critical point computations with algebraic methods appear in statistics and in biology [32, 17, 39]. In particular, computing *maximum likelihood estimates* is an important routine in algebraic statistics which involves computing the critical points of a monomial function restricted to an algebraic variety. Another related setting is the study of the critical points of the Euclidean distance function on an algebraic variety; algebraic properties of these critical points are investigated in [18].

1.5. Organization of the paper. The main notation used throughout the paper is introduced in section 2. Known results on the algebraic structure of the ideal $\mathbf{I}(q,\mathbf{F})$ are also recalled. The Eagon–Northcott complex is described in section 3.1, and formulas for the Hilbert series and for the degree of regularity are obtained in sec-

tion 3.2; finally, the main complexity results are given in section 3.4 and are illustrated by experimental results in section 4.

2. Notation and preliminaries.

2.1. Notation. Throughout this paper, $p, n \in \mathbb{N}$ are two integers s.t. $p < n$, and $(d_0, \ldots, d_p) \in \mathbb{N}^{p+1}$ is a sequence of degrees such that $d_0 \geq 1$, $d_1, \ldots, d_p \geq 2$. Assuming that all the constraints in the optimization problem are at least quadratic does not lose any generality: linear constraints can be removed by substituting one variable by a linear polynomial in the other equations. We let X (resp., U) denote a set of variables $\{X_1, \ldots, X_n\}$ (resp., $\{U_{0,1}, \ldots, U_{p,n}\}$) of cardinality n (resp., $(p+1)n$). We consider the following grading of the polynomial ring $\mathbb{Q}[U, X]$:

$$\begin{cases} \deg(X_i) = 1 \text{ for all } i \in \{1, \ldots, n\}, \\ \deg(U_{i,j}) = d_i - 1 \text{ for all } i \in \{0, \ldots, p\}, j \in \{1, \ldots, n\}. \end{cases}$$

For $d \in \mathbb{N}$, we let $\mathbb{Q}[X]_d$ denote the $\mathbb{Q}$ vector space of homogeneous polynomials of degree d in $\mathbb{Q}[X]$. For any polynomial f in $\mathbb{Q}[X]$, its homogeneous part of highest degree is denoted by $f^\infty \in \mathbb{Q}[X]_{\deg(f)}$. Also, for $i \in \{0, \ldots, p\}, j \in \{1, \ldots, n\}$, we define the polynomial $g_{in+j}^\infty \in \mathbb{Q}[U, X]$ as

$$g_{in+j}^\infty = \begin{cases} U_{i,j} - \frac{\partial f_i^\infty}{\partial X_j} \text{ if } i \in \{1, \ldots, p\}, \\ U_{i,j} - \frac{\partial q^\infty}{\partial X_j} \text{ if } i = 0. \end{cases}$$

For $i \in \{1, \ldots, p\}$, we define $g_{(p+1)n+i}^\infty \in \mathbb{Q}[U, X]$ to be equal to $f_i^\infty \in \mathbb{Q}[X]$. The determinantal ideal generated by all the maximal minors of the matrix

$$U = \begin{bmatrix} U_{0,1} & \ldots & U_{0,n} \\ \vdots & \vdots & \vdots \\ U_{p,1} & \ldots & U_{p,n} \end{bmatrix}$$

is denoted by $\mathscr{D}$. For $\mathbf{F} \in \mathbb{Q}[X]^p$ and an objective function $q \in \mathbb{Q}[X]$ we consider the ideal $\mathbf{I}(q, \mathbf{F})$ generated by $\langle f_1, \ldots, f_p \rangle$ and by the maximal minors of the Jacobian matrix $\mathsf{jac}(q, \mathbf{F})$,

$$\mathsf{jac}(q, \mathbf{F}) = \begin{bmatrix} \frac{\partial q}{\partial X_1} & \cdots & \frac{\partial q}{\partial X_n} \\ \frac{\partial f_1}{\partial X_1} & \cdots & \frac{\partial f_1}{\partial X_n} \\ \vdots & \vdots & \vdots \\ \frac{\partial f_p}{\partial X_1} & \cdots & \frac{\partial f_p}{\partial X_n} \end{bmatrix},$$

i.e., $\mathbf{I}(q, \mathbf{F}) = \langle f_1, \ldots, f_p \rangle + \langle \mathsf{MaxMinors}(\mathsf{jac}(q, \mathbf{F})) \rangle$. Therefore,

$$\mathbf{I}(q, \mathbf{F}) = \left(\mathscr{D} + \langle g_1, \ldots, g_{(p+1)n+p} \rangle \right) \cap \mathbb{Q}[X].$$

For a graded ideal I of an $\mathbb{N}$-graded $\mathbb{Q}$-algebra R, we call the *dimension* of I the Krull dimension of the quotient ring R/I, and we let $\mathsf{wHS}_{R/I} \in \mathbb{Z}[[t]]$ denote the *weighted Hilbert series* of I, defined by

$$\mathsf{wHS}_{R/I}(t) = \sum_{d \in \mathbb{N}} \dim_{\mathbb{Q}} (R_d/I_d) t^d,$$

where R_d (resp., I_d) denotes the $\mathbb{Q}$-vector space of homogeneous elements of degree d in R (resp., I). We shall use the notation $\mathsf{HS}_{R/I}(t)$ when R is the polynomial algebra $\mathbb{Q}[X]$ (or $\mathbb{Q}[X]$) with the canonical grading $\deg(X_i) = 1$ for all i.

If I is an homogeneous ideal of dimension 0 of a polynomial ring $\mathbb{Q}[X]$, its *degree of regularity* $\mathrm{d}_{\mathrm{reg}}(I)$ is the smallest integer d such that $\dim_{\mathbb{Q}}(\mathbb{Q}[X]_d/I_d) = 0$. Equivalently, it equals 1 plus the degree of the Hilbert series (which is a polynomial in the case of 0-dimensional ideals).

2.2. Genericity. Throughout this paper, $q, f_1, \ldots, f_p \in \mathbb{Q}[X]$ are polynomials of respective degrees at most $d_0, \ldots, d_p$. As in [38], we say that a property holds for a *generic system* $(q, f_1, \ldots, f_p)$ (resp., $(q^\infty, f_1^\infty, \ldots, f_p^\infty) \in \mathbb{Q}[X]_{d_0} \times \cdots \times \mathbb{Q}[X]_{d_p})$ if this property holds for all $(q, f_1, \ldots, f_p)$ (resp., $(q^\infty, f_1^\infty, \ldots, f_p^\infty)$) in a dense Zariski open subset of the space of all polynomials of degrees at most $d_0, \ldots, d_p$ (resp., of the space of all homogeneous polynomials of degrees $d_0, \ldots, d_p$). Note that the variety associated with a generic system $f_1, \ldots, f_p$ (resp., $f_1^\infty, \ldots, f_p^\infty$) is a reduced smooth complete intersection.

2.3. Complexity model and notation. All complexity estimates count the number of operations $\{+, -, \times, \div\}$ in $\mathbb{Q}$. It is not the goal of this paper to estimate the bit complexity induced by the growth of the coefficients due to the arithmetic operations in $\mathbb{Q}$. All complexity counts are parametrized by n and by the sequence of degrees $(d_0, \ldots, d_p)$ of length $p + 1$. More precisely, complexities in this model are partial functions $\mathbb{N} \times \mathbf{c}_0(\mathbb{N}) \to \mathbb{N}$, where $\mathbf{c}_0(\mathbb{N})$ is the set of sequences $(d_i)_{i \in \mathbb{N}}$ with finite support. For two nonnegative functions $C_1, C_2 : \mathbb{N} \times \mathbf{c}_0(\mathbb{N}) \to \mathbb{R}_+$, we write $C_1 = O(C_2)$ if there exists a constant $A \in \mathbb{N}$ such that $C_1(n, d_0, \ldots, d_p) \leq A \cdot C_2(n, d_0, \ldots, d_p)$. For three functions $C_1, C_2, C_3 : \mathbb{N} \times \mathbf{c}_0(\mathbb{N}) \to \mathbb{R}_+$ taking values greater than 1, the notation $C_1 = C_2^{O(C_3)}$ means that

$$\frac{\log(C_1)}{\log(C_2)} = O(C_3).$$

2.4. Algebraic structure of $\mathbf{I}(q^\infty, \mathbf{F}^\infty)$. We recall in this section results from a previous paper [27], where we investigated the special case where all the constraints shared the same degree: $d_1 = \cdots = d_p = D$ and $q = X_1$ is the projection on the first coordinate. Some of their properties also hold in the general case. We state them and recall their proofs in this section. The next lemma shows that the set of complex critical points of a generic polynomial optimization problem is finite. It is stated for the homogeneous system $(q^\infty, \mathbf{F}^\infty)$ but the same statement for an inhomogeneous generic system $(q, \mathbf{F})$ can be proved similarly (see [38, Prop. 2.1]).

LEMMA 2.1. *If $(q^\infty, \mathbf{F}^\infty)$ is a generic system, then the ideal $\mathbf{I}(q^\infty, \mathbf{F}^\infty)$ has dimension 0.*

Proof. This proof is similar to that of [18, Lemma 2.1]. Let $V \subset \mathbb{C}^n$ be the affine variety associated with $\mathbf{F}^\infty$. Since $\mathbf{F}^\infty$ is generic, V is smooth at any nonzero point. We consider the correspondence variety

$$\mathcal{E}_{V,d_0} = \mathbb{C}[x_1, \ldots, x_n]_{d_0} \times V \subset \mathbb{C}^{\binom{n+d_0-1}{n}+n}.$$

The set $W = \{(q^\infty, \mathbf{x}) \in \mathcal{E}_{V,d_0} \mid \mathrm{Rank}(\mathsf{jac}(q^\infty(\mathbf{x}), \mathbf{F}^\infty(\mathbf{x}))) \leq p\}$ is a proper subvariety of $\mathcal{E}_{V,d_0}$ and $\mathbf{I}(q^\infty, \mathbf{F}^\infty)$ is the generic fiber of its projection on $\mathbb{C}[x_1, \ldots, x_n]_{d_0}$. Since V is smooth at any nonzero point, for all $\mathbf{x} \in V \setminus \{0\}$, the fiber

$$\{q^\infty \in \mathbb{C}[x_1, \ldots, x_n]_{d_0} \mid (q^\infty, \mathbf{x}) \in W\}$$

is a linear subspace of codimension $n-p$ in $\mathbb{C}[x_1, \ldots, x_n]_{d_0}$. Since V has dimension $n-p$ and the fibers of the projection on V have codimension $n-p$, W must have dimension $\dim_{\mathbb{C}}(\mathbb{C}[x_1, \ldots, x_n]_{d_0})$ and hence the generic fiber of its projection on $\mathbb{C}[x_1, \ldots, x_n]_{d_0}$ is finite. $\square$

Since the ideal $\mathbf{I}(q^\infty, \mathbf{F}^\infty)$ is homogeneous and has dimension 0, its variety is the unique point $\{0\} \in \mathbb{C}^n$. However, the ideal $\mathbf{I}(q^\infty, \mathbf{F}^\infty)$ is not radical and an important indicator of the complexity of the Gröbner basis computation is its Hilbert series. The two next statements describe the relationship between the Hilbert series of $\mathbb{Q}[X]/\mathbf{I}(q^\infty, \mathbf{F}^\infty)$ and that of $\mathbb{Q}[U]/\mathscr{D}$.

LEMMA 2.2. *For $\ell \in \{1, \ldots, p + n(p+1)\}$, the polynomial g_ℓ^∞ does not divide* 0 *in the quotient ring $\mathbb{Q}[U, X]/\left(\mathscr{D} + \langle g_1^\infty, \ldots, g_{\ell-1}^\infty \rangle\right)$.*

Proof. The quotient ring $\mathbb{Q}[U, X]/\mathscr{D}$ is Cohen–Macaulay of dimension $p + n(p+1)$ [13, Prop. 1.1], [13, Coro. 2.8] and $\mathscr{D} + \langle g_1^\infty, \ldots, g_{p+n(p+1)}^\infty \rangle$ has dimension 0 in $\mathbb{Q}[U, X]$ by Lemma 2.1. Consequently, $\langle g_1^\infty, \ldots, g_{p+n(p+1)}^\infty \rangle$ is a regular sequence in $\mathbb{Q}[U, X]/\mathscr{D}$ by Macaulay's unmixedness theorem [20, Corollary 18.14]. $\square$

Homogeneous regular sequences provide relations between the Hilbert series of the associated ideals, leading to the following corollary.

COROLLARY 2.3. *The Hilbert series of $\mathbb{Q}[X]/\mathbf{I}(q^\infty, \mathbf{F}^\infty)$ is related to that of $\mathbb{Q}[U]/\mathscr{D}$ by*

$$\mathsf{HS}_{\mathbb{Q}[X]/\mathbf{I}(q^\infty, \mathbf{F}^\infty)}(t) = \mathsf{wHS}_{\mathbb{Q}[U]/\mathscr{D}}(t) \cdot \frac{(1 - t^{d_0-1})^n \prod_{1 \le i \le p}(1 - t^{d_i})(1 - t^{d_i-1})^n}{(1-t)^n}.$$

Proof. First, we use the fact that $\mathbb{Q}[U, X]/\mathscr{D} \cong \mathbb{Q}[U]/\mathscr{D} \otimes_{\mathbb{Q}} \mathbb{Q}[X]$ which yields

$$\mathsf{wHS}_{\mathbb{Q}[U, X]/\mathscr{D}}(t) = \mathsf{wHS}_{\mathbb{Q}[U]/\mathscr{D}}(t) \cdot \mathsf{HS}_{\mathbb{Q}[X]}(t) = \frac{\mathsf{wHS}_{\mathbb{Q}[U]/\mathscr{D}}(t)}{(1-t)^n}.$$

We recall that, with the notation of Lemma 2.2,

$$\mathbf{I}(q^\infty, \mathbf{F}^\infty) = \left(\mathscr{D} + \left\langle g_1^\infty, \ldots, g_{p+n(p+1)}^\infty \right\rangle\right) \cap \mathbb{Q}[X].$$

According to Lemma 2.2, for each $2 \le \ell \le p + n(p+1)$, g_ℓ^∞ does not divide 0 in $\mathbb{Q}[X]/\langle g_1^\infty, \ldots, g_{\ell-1}^\infty \rangle$. Adding to an ideal a polynomial of degree d that does not divide zero in the quotient ring multiplies its Hilbert series by $(1 - t^d)$. To conclude the proof, we notice that

$$\mathbb{Q}[U, X]/\left(\mathscr{D} + \langle g_1^\infty, \ldots, g_{p+n(p+1)}^\infty \rangle\right) \cong \mathbb{Q}[X]/\mathbf{I}(q^\infty, \mathbf{F}^\infty)$$

via the map

$$\begin{cases} X_i \mapsto X_i, \\ U_{i,j} \mapsto \dfrac{\partial f_i}{\partial X_j}. \end{cases}$$

Consequently,

$$\begin{aligned}
&\mathsf{HS}_{\mathbb{Q}[X]/\mathbf{I}(q^\infty, \mathbf{F}^\infty)}(t) \\
&= \mathsf{HS}_{\mathbb{Q}[U, X]/\left(\mathscr{D} + \langle g_1^\infty, \ldots, g_{p+n(p+1)}^\infty \rangle\right)}(t) \\
&= \mathsf{wHS}_{\mathbb{Q}[U, X]/\mathscr{D}}(t)(1 - t^{d_0-1})^n \prod_{1 \le i \le p}(1 - t^{d_i})(1 - t^{d_i-1})^n \\
&= \mathsf{wHS}_{\mathbb{Q}[U]/\mathscr{D}}(t) \cdot \frac{(1 - t^{d_0-1})^n \prod_{1 \le i \le p}(1 - t^{d_i})(1 - t^{d_i-1})^n}{(1-t)^n}. \quad \square
\end{aligned}$$

3. The Eagon–Northcott complex and the Hilbert series of weighted determinantal ideals. The goal of this section is to obtain an explicit formula for the degree of regularity of $\mathbf{I}(q^\infty, \mathbf{F}^\infty)$, namely, the smallest positive integer ℓ such that the coefficient of t^ℓ in the series expansion of $\mathsf{HS}_{\mathbb{Q}[X]/\mathbf{I}(q^\infty, \mathbf{F}^\infty)}(t)$ is zero. This

value bounds the witness degree of any system of generators of $\mathbf{I}(q, \mathbf{F})(t)$ and hence is an indicator of the complexity of the Gröbner basis computation.

The bound on $\mathrm{d_{wit}}$ shall be obtained via an explicit formula for the Hilbert series of $\mathbf{I}(q^\infty, \mathbf{F}^\infty)$. The main principle is to isolate first the determinantal component (generated by the maximal minors of the Jacobian matrix) and to analyze it separately. We obtain in that case a determinantal ideal $\mathscr{D}$, with a grading induced by the degrees of the input polynomials. A free resolution of this ideal $\mathscr{D}$ is given by the so-called *Eagon–Northcott complex* [19]. From this free resolution, we shall read off an explicit formula for the Hilbert series and for the degree of regularity of $\mathbf{I}(q^\infty, \mathbf{F}^\infty)$.

3.1. Preliminaries on the Eagon–Northcott complex. Free resolutions are classical tools in commutative algebra to describe the relations existing between a given set of polynomials. The main principles of these techniques go back to Hilbert and his *syzygy theorem* (see, e.g., [20, Corollary 19.7] for a statement in the modern formalism).

An explicit description of a minimal free resolution of the ideal generated by the maximal minors of a generic matrix is given by the Eagon–Northcott complex [19]. We refer to [21, Appendix A2H] for a complete presentation. After describing the general construction of the complex, we shall detail an example of Hilbert series computations.

Let $R = Q[U]$ be the polynomial ring. Following the notation in [21, Appendix A2H], we write $F = R^f$ and $G = R^g$, where f and g are two integers such that $g < f$. For a $g \times f$ matrix whose entries are in R, we let $\alpha : F \to G$ denote the corresponding morphism of modules. Let $\otimes^i G$ be the R-module of tensors of order i:

$$\otimes^i G = \mathrm{Span}_R \{g_1 \otimes \cdots \otimes g_i \mid g_1, \ldots, g_i \in G\}$$

and let M_i (resp., N_i) be the submodule of $\otimes^i G$ generated by the elements

$$\{g_1 \otimes \cdots \otimes g_i - g_{\sigma(1)} \otimes \cdots \otimes g_{\sigma(i)} \mid g_1, \ldots, g_i \in G, \sigma \text{ a permutation of } \{1, \ldots, i\}\}$$

(resp.,

$$\{g_1 \otimes \cdots \otimes g_i - (-1)^{\mathsf{sgn}(\sigma)} g_{\sigma(1)} \otimes \cdots \otimes g_{\sigma(i)} \mid g_1, \ldots, g_i \in G, \sigma \text{ a permutation of} \{1, \ldots, i\}\}).$$

Then we let $\mathsf{Sym}_i G = (\otimes^i G)/M_i$ (resp., $\bigwedge^i G = (\otimes^i G)/N_i$) be the R-module of elements of order i in the *symmetric algebra* (resp., in the *exterior algebra*). The Eagon–Northcott complex is then defined by

$$\mathsf{EN}(\alpha): \quad 0 \to (\mathsf{Sym}_{f-g} G)^* \otimes \bigwedge^f F \xrightarrow{\sigma_{f-g-1}} (\mathsf{Sym}_{f-g-1} G)^* \otimes \bigwedge^{f-1} F \xrightarrow{\sigma_{f-g}}$$

$$\cdots \to (\mathsf{Sym}_2 G)^* \otimes \bigwedge^{g+2} F \xrightarrow{\sigma_3} G^* \otimes \bigwedge^{g+1} F \xrightarrow{\sigma_2} \bigwedge^g F \xrightarrow{\wedge^g \alpha} \bigwedge^g G.$$

First, notice that as an R-module, $\mathsf{Sym}_i G$ (and hence also its dual $(\mathsf{Sym}_i G)^*$) is a free module isomorphic to $R^{\binom{i+g-1}{i}}$. Similarly, $\bigwedge^i F$ is isomorphic to $R^{\binom{f}{i}}$ as an R-module. For a detailed description of the maps σ_i, we refer to [21, Appendix A2H] and [20, Appendix A2.6]. In the context of this paper, $f = n$, $g = p + 1$, $R = \mathbb{Q}[U]$ with the grading given by $\deg(U_{i,j}) = d_i - 1$, and the map α corresponds to the matrix

$$\mathscr{U} = \begin{pmatrix} U_{0,1} & \ldots & U_{0,n} \\ \vdots & \vdots & \vdots \\ U_{p,1} & \ldots & U_{p,n} \end{pmatrix}.$$

The next step is to take into account the grading $\deg(U_{i,j}) = d_i - 1$. We use here the classical notation $R(-s)$ to denote the ring R where the grading has been shifted

by s, i.e., $R(-s)_d = R_{d-s}$. For instance, if $\eta : R \to R$ is a morphism of degree s, the induced morphism

$$R(-s) \xrightarrow{\eta} R(0)$$

maps elements of degree d in $R(-s)$ to elements of degree d in R. Using the notation $s = \sum_{0 \le i \le p}(d_i - 1)$, and taking into account the grading of $\mathbb{Q}[U]$ and the description of the maps in [21, Appendix A2H], the complex can be rewritten as

$$\mathsf{EN}(\alpha) : 0 \to \bigoplus_{\substack{i_0+\cdots+i_p \\ = \\ n-p-1}} R\left(-s - \sum_{0 \le j \le p} i_j(d_j - 1)\right)$$

$$\xrightarrow{\sigma_{f-g-1}} \bigoplus_{\substack{i_0+\cdots+i_p \\ = \\ n-p-2}} R\left(-s - \sum_{0 \le j \le p} i_j(d_j - 1)\right)^{\binom{n}{n-1}}$$

$$\xrightarrow{\sigma_{f-g}} \bigoplus_{\substack{i_0+\cdots+i_p \\ = 2}} R\left(-s - \sum_{0 \le j \le p} i_j(d_j - 1)\right)^{\binom{n}{p+3}}$$

$$\xrightarrow{\sigma_3} \bigoplus_{1 \le i \le p} R\left(-s - (d_i - 1)\right)^{\binom{n}{p+2}} \xrightarrow{\sigma_2}$$

$$\to R(-s)^{\binom{n}{p+1}} \xrightarrow{\wedge^g \alpha} R(0).$$

The last map $\wedge^g \alpha$ sends each generator of $R(-s)^{\binom{n}{p+1}}$ on a maximal minor of α (note that the number of such maximal minors is precisely $\binom{n}{p+1}$), hence the image of $\wedge^g \alpha$ is indeed the ideal generated by the maximal minors.

Example. Set $n = 4$ and $p = 1$. The ideal $\mathscr{D}$ is generated by the maximal minors of the following 2×4 matrix:

$$\begin{pmatrix} U_{0,1} & U_{0,2} & U_{0,3} & U_{0,4} \\ U_{1,1} & U_{1,2} & U_{1,3} & U_{1,4} \end{pmatrix}.$$

In this case, the Eagon–Northcott complex is

$$\mathsf{EN} : \quad 0 \to R^3 \xrightarrow{\sigma_3} R^8 \xrightarrow{\sigma_2} R^6 \xrightarrow{\sigma_1} R \ ,$$

where the letter R stands for the ring $\mathbb{Q}[U]$, and the morphisms σ_i are given by the following matrices:

$$\wedge \alpha = (U_{0,2}U_{1,4} - U_{1,2}U_{0,4}, U_{0,3}U_{1,2} - U_{0,2}U_{1,3}, U_{0,1}U_{1,3}$$
$$- U_{0,3}U_{1,1}, U_{0,4}U_{1,1} - U_{1,4}U_{0,1}, U_{0,4}U_{1,3} - U_{1,4}U_{0,3}, U_{0,2}U_{1,1} - U_{1,2}U_{0,1}),$$

$$\sigma_2 = \begin{pmatrix} -U_{0,3} & -U_{1,3} & 0 & 0 & U_{0,1} & U_{1,1} & 0 & 0 \\ -U_{0,4} & -U_{1,4} & 0 & 0 & 0 & 0 & U_{0,1} & U_{1,1} \\ 0 & 0 & -U_{0,4} & -U_{1,4} & 0 & 0 & U_{0,2} & U_{1,2} \\ 0 & 0 & -U_{0,3} & -U_{1,3} & U_{0,2} & U_{1,2} & 0 & 0 \\ -U_{0,2} & -U_{1,2} & U_{0,1} & U_{1,1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -U_{0,4} & -U_{1,4} & U_{0,3} & U_{1,3} \end{pmatrix},$$

$$\sigma_3 = \begin{pmatrix} U_{0,1} & U_{1,1} & 0 \\ 0 & U_{0,1} & U_{1,1} \\ U_{0,2} & U_{1,2} & 0 \\ 0 & U_{0,2} & U_{1,2} \\ U_{0,3} & U_{1,3} & 0 \\ 0 & U_{0,3} & U_{1,3} \\ U_{0,4} & U_{1,4} & 0 \\ 0 & U_{0,4} & U_{1,4} \end{pmatrix}.$$

Direct computations show that this is a complex (i.e., for all i, $\sigma_{i-1} \circ \sigma_i = 0$) and $\mathsf{Im}(\sigma_1) = \mathscr{D}$. Taking the grading into account, the Eagon–Northcott complex is rewritten as

$$
\begin{aligned}
\mathsf{EN}: \quad & 0 \to R(-3d_0 - d_1 - 4) \oplus R(-2d_0 - 2d_1 - 4) \oplus R(-d_0 - 3d_1 - 4) \\
& \xrightarrow{\sigma_3} R(-2d_0 - d_1 - 3)^4 \oplus R(-d_0 - 2d_1 - 3)^4 \xrightarrow{\sigma_2} R(-d_0 - d_1 - 2)^6 \\
& \xrightarrow{\wedge \alpha} R(0) \to R/\mathscr{D} \to 0.
\end{aligned}
$$

3.2. Hilbert series and degree of regularity. The next goal is to derive an explicit formula for the Hilbert series of $\mathbf{I}(q^\infty, \mathbf{F}^\infty)$. We use the fact that the Hilbert series can be computed once a free resolution is known, since the Hilbert series of I is equal to the alternate sum of the Hilbert series of the free modules occurring in the resolution. This is a classical strategy for obtaining an explicit formula for the Hilbert series (see, e.g., [21, Theorem 1.11] for more details). The next proposition is a special case of [15, Prop. 2.4], which gives an explicit formula for the Hilbert series for more general gradings.

PROPOSITION 3.1. *The weighted Hilbert series of the ideal $\mathscr{D} \subset \mathbb{Q}[U]$ generated by the maximal minors of the matrix $\mathscr{U}$ with $\deg(U_{i,j}) = d_i - 1$ is the power series expansion of the rational function*

$$
\mathsf{wHS}_{\mathbb{Q}[U]/\mathscr{D}}(t) = \frac{1 - \left[\sum_{0 \le k \le n-p-1} \left[(-1)^k \sum_{i_0 + \cdots + i_p = k} \binom{n}{p+k+1} \cdot t^{\sum_{0 \le j \le p}(i_j+1)(d_j-1)} \right] \right]}{\prod_{0 \le i \le p}(1 - t^{d_i-1})^n}.
$$

Proof. According to [21, Theorem 1.11], the Hilbert series of a graded ideal can be computed from a minimal free resolution: it equals the alternate sum of the Hilbert series of the free modules occurring in the resolution. For $\ell, j \in \mathbb{N}$, the Hilbert series of $R(-\ell)^j$ equals

$$
\mathsf{wHS}_{R(-\ell)^j}(t) = \frac{jt^\ell}{\prod_{0 \le i \le p}(1 - t^{d_i-1})^n}.
$$

Moreover, the Hilbert series of a direct sum of modules is equal to the sum of their Hilbert series. Therefore, by considering the alternate sum of the Hilbert series of the free modules in the Eagon–Northcott complex (which is a free resolution of $\mathscr{D}$), direct computations yield the formula for the weighted Hilbert series of $\mathscr{D}$. ☐

The degree of regularity can be extracted from the Hilbert series, yielding the following formula.

COROLLARY 3.2. *For generic homogeneous polynomials $(q^\infty, f_1^\infty, \ldots, f_p^\infty)$, the degree of regularity of $\mathbf{I}(q^\infty, \mathbf{F}^\infty)$ is*

$$
\mathrm{d}_{\mathrm{reg}}(\mathbf{I}(q^\infty, \mathbf{F}^\infty)) = (n - p - 1)\max_{0 \le i \le p}\{d_i - 1\} - n - p + d_0 + 2 \sum_{1 \le i \le p} d_i.
$$

Proof. Since the ideal $\mathbf{I}(q^\infty, \mathbf{F}^\infty)$ is 0-dimensional (Lemma 2.1), $\mathsf{HS}_{\mathbb{Q}[X]/\mathbf{I}(q^\infty, \mathbf{F}^\infty)}(t)$ is a polynomial and $\mathrm{d}_{\mathrm{reg}} = \deg(\mathsf{HS}_{\mathbb{Q}[X]/\mathbf{I}(q^\infty, \mathbf{F}^\infty)}(t)) + 1$. Let j_0 be the index of one of the maximal degrees: $d_{j_0} = \max_{0 \le j \le p}\{d_j\}$. In the sums in the numerator of the formula given in Proposition 3.1, the maximal degree is reached when $k = n - p - 1$, $i_{j_0} = k$, and $i_j = 0$ for $j \ne j_0$. Therefore the degree of the numerator of $\mathsf{wHS}_{\mathbb{Q}[U]/\mathscr{D}}(t)$

equals

$$\deg \left(1 - \left[\sum_{0 \leq k \leq n-p-1} \left[(-1)^k \sum_{i_0 + \cdots + i_p = k} \binom{n}{p+k+1} t^{\sum_{0 \leq j \leq p} (i_j+1)(d_j-1)} \right] \right] \right)$$

$$= (n-p-1)(\max\{d_j\}-1) + \sum_{0 \leq j \leq p} (d_j - 1).$$

On the other hand, we have

$$\begin{cases} \deg \left(\prod_{1 \leq i \leq p} (1 - t^{d_i}) \right) = \sum_{1 \leq i \leq p} d_i, \\ \deg \left((1-t)^n \right) = n. \end{cases}$$

Therefore, using the formula in Corollary 2.3, we obtain

$$\deg(\mathsf{HS}_{\mathbb{Q}[X]/\, \mathbf{I}(q^\infty, \mathbf{F}^\infty)}) = (n-p-1)(\max\{d_i\}-1) + \sum_{0 \leq i \leq p} (d_i - 1) + \sum_{1 \leq i \leq p} d_i - n$$

$$= (n-p-1)\max\{d_i - 1\} - n - p + d_0 - 1 + 2 \sum_{1 \leq i \leq p} d_i,$$

and hence $d_{\mathrm{reg}} = (n-p-1)\max\{d_i - 1\} - n - p + d_0 + 2\sum_{1 \leq i \leq p} d_i$. □

3.3. Grothendieck polynomials. In this section, we discuss briefly another approach to compute the Hilbert series of weighted determinantal via Grothendieck polynomials introduced in [35].

The numerator of the rational function in Proposition 3.1—also called K-polynomial—is equal to the evaluation of Grothendieck polynomials at powers of t; see [34, Theorem A]. On the other hand, the *(multi)degree* of the ideal may be expressed in the evaluation of Schubert polynomials [37, Theorem 15.40]. In the sequel, S_{n+1} denotes the group of permutations of the set $\{1, \ldots, n+1\}$ and for all i, σ_i is the transposition $i \leftrightarrow i+1$.

DEFINITION 3.3. *The divided difference operators ∂_i are defined by*

$$\forall H \in \mathbb{Z}[t_1, \ldots, t_{n+1}], \partial_i H = \frac{H(t_1, \ldots, t_{n+1}) - H(t_1, \ldots, t_{i-1}, t_{i+1}, t_i, t_{i+2}, \ldots t_{n+1})}{t_i - t_{i+1}}.$$

Let $w_0 \in S_{n+1}$ be the permutation $w(i) = n + 2 - i$. For $w \in S_{n+1}$, the Grothendieck polynomial $\mathcal{G}_w \in \mathbb{Z}[t_1, \ldots, t_{n+1}]$ is defined by

$$\mathcal{G}_{w_0}(t_1, \ldots, t_{p+1}) = \prod_{i=1}^{n+1} (1 - t_i)^{n+1-i},$$

$$\mathcal{G}_{w \cdot \sigma_i}(t_1, \ldots, t_{p+1}) = -\partial_i \left(t_{i+1} \mathcal{G}_w(t_1, \ldots, t_{p+1}) \right) \text{ when } \mathrm{length}(w \cdot \sigma_i) < \mathrm{length}(w).$$

Let S_{n+1} be the group of permutations on the set $\{1, \ldots, n+1\}$. To the determinantal ideal $\mathscr{D}$ is associated the following permutation $w \in S_{n+1}$ (see [37, Chapter 15] for details):

- $w(i) = i$ for $i \in \{1, \ldots, p\}$;
- $w(i) = i + 1$ for $i \in \{p+1, \ldots, n\}$;
- $w(n+1) = p + 1$.

In that case, the Grothendieck polynomial $\mathcal{G}_w$ associated with w is a polynomial in $\mathbb{Z}[t_1, \ldots, t_{p+1}]$. Its evaluation at $t_1 = t^{d_0-1}, \ldots, t_{p+1} = t^{d_p-1}$ yields the desired numerator of the weighted Hilbert series of $\mathscr{D}$. This representation provides more combinatorial insights, and it would be interesting to investigate if the formula for the degree of regularity can also be obtained from the evaluation of the Grothendieck polynomials. Moreover, this approach extends to matrices of corank greater than 1 while the Eagon–Northcott complex is restricted to the case of maximal minors. We refer the reader to [34] for more details.

Example. Set $n = 3$, $p = 1$, $d_0 = 3$, $d_1 = 2$. This corresponds to the problem of minimizing a cubic function in three variables on a quadric surface. The ideal $\mathscr{D} \in \mathbb{Q}[U_{0,1}, U_{0,2}, U_{0,3}, U_{1,1}, U_{1,2}, U_{1,3}]$ is generated by the 2-minors of the matrix $(U_{i,j})$. The grading is given by $\deg(U_{0,i}) = d_0 - 1 = 2$ and $\deg(U_{1,i}) = d_1 - 1 = 1$ for $i \in \{1, 2, 3\}$. In that case, Proposition 3.1 yields

$$\mathsf{wHS}_{\mathbb{Q}[U]/\mathscr{D}}(t) = \frac{1 - \left[\sum_{0 \le k \le 1} \left[(-1)^k \sum_{i_0 + i_1 = k} \binom{3}{2+k} t^{2i_0 + i_1 + 3} \right] \right]}{(1-t^2)^3(1-t)^3}$$

$$= \frac{t^5 + t^4 - 3t^3 + 1}{(1-t^2)^3(1-t)^3}.$$

The permutation $w \in S_4$ associated with the ideal $\mathscr{D}$ is given by $w(1) = 1, w(2) = 3, w(3) = 4, w(4) = 2$. The corresponding Grothendieck polynomial is

$$\mathcal{G}_w(t_1, t_2) = t_1^2 t_2 + t_1 t_2^2 - 3t_1 t_2 + 1.$$

Evaluating $\mathcal{G}_w$ at (t^2, t) recovers the K-polynomial of the determinantal ideal:

$$\mathcal{G}_w(t^2, t) = t^5 + t^4 - 3t^3 + 1.$$

3.4. Complexity analysis. We bound in this section the complexity of the following general solving strategy: first, one computes a Gröbner basis of $\mathbf{I}(q, \mathbf{F})$ with respect to the *grevlex* with the F_4/F_5 algorithm. Then, the FGLM algorithm is used to convert it into a lex Gröbner basis. Once a lex Gröbner basis is known, a rational parametrization of the critical points can be computed, for instance, with the RUR algorithm [41]. Since the most costly steps of the solving process are the Gröbner bases computations, we focus in this paper on their complexities.

First, we need to estimate the complexity in terms of the degree and of the witness degree. Since Gröbner bases computations can be reduced to the computation of row echelon forms of Macaulay matrices, we have the following estimate.

THEOREM 3.4. *A grevlex Gröbner basis of* $\mathbf{I}(q, \mathbf{F})$ *can be computed within*

$$O\left(\left(p + \binom{n}{p+1} \right) \binom{n + \mathrm{d}_{\mathrm{wit}}}{n}^\omega \right)$$

arithmetic operations in $\mathbb{Q}$, *where* $\mathrm{d}_{\mathrm{wit}} \le \mathrm{d}_{\mathrm{reg}}(\mathbf{I}(q^\infty, \mathbf{F}^\infty))$ *and* ω *is a feasible exponent for the matrix multiplication* ($\omega < 2.373$ *with Williams' algorithm* [47]).

Proof. Proof is postponed to section 5. ☐

Finally we can obtain a general formula for the complexity of computing a lex Gröbner basis of $\mathbf{I}(\mathbf{F}, q)$ in terms of the generic values of the degree and of the witness degree.

COROLLARY 3.5. *Let* $p, n \in \mathbb{N}$ *with* $p < n$, $(d_0, \ldots, d_p) \in \mathbb{N}^p$, *and* $(q, \mathbf{F}) \in \mathbb{Q}[X]^{p+1}$ *be a generic system of respective degrees at most* $(d_0, \ldots, d_p)$. *Then the*

complexity of computing a lex Gröbner basis of $\mathbf{I}(q, \mathbf{F})$ *is bounded above by*

$$O\left(\left(p + \binom{n}{p+1}\right)\binom{n + \mathrm{d_{wit}}}{n}^{\omega} + n \cdot \delta^3\right),$$

where

$$\mathrm{d_{wit}} \leq (n - p - 1)\max\{d_i - 1\} - n - p + d_0 + 2\sum_{1 \leq i \leq p} d_i,$$

$$\delta = \left(\prod_{1 \leq i \leq p} d_i\right)\sum_{i_0 + \cdots + i_p = n - p}(d_0 - 1)^{i_0}\ldots(d_p - 1)^{i_p}.$$

Proof. This is a direct consequence of Theorem 3.4 and Corollaries 5.3 and 3.2, of the complexity of the FGLM algorithm $O\left(n \cdot \delta^3\right)$ [24, Proposition 4.1] and from the explicit formula for the algebraic degree of polynomial optimization [38, Theorem 2.2]. □

In what follows, A (resp., G) is the arithmetic (resp., geometric) average of the multiset

$$\{d_1, \ldots, d_p, \underbrace{\max_{0 \leq i \leq p}\{d_i - 1\}, \ldots, \max_{0 \leq i \leq p}\{d_i - 1\}}_{n - p}\},$$

$$A = \frac{1}{n}\left((n - p)\max_{0 \leq i \leq p}\{d_i - 1\} + \sum_{1 \leq i \leq p} d_i\right),$$

$$G = \left(\max_{0 \leq i \leq p}\{d_i - 1\}^{n - p}\prod_{1 \leq i \leq p} d_i\right)^{1/n}.$$

Also, we let δ denote the generic algebraic degree of polynomial optimization [38]:

$$\delta = \mathsf{DEG}(\mathbf{I}(q, \mathbf{F})) = \left(\prod_{1 \leq i \leq p} d_i\right)\sum_{i_0 + \cdots + i_p = n - p}(d_0 - 1)^{i_0}\ldots(d_p - 1)^{i_p}.$$

The next statement is the main result of this paper and bounds the complexity in terms of δ.

THEOREM 3.6. *Let* $(q, f_1, \ldots, f_p) \in \mathbb{Q}[X]$ *be a generic system of polynomials of respective degrees at most* $(d_0, \ldots, d_p)$ *with* $1 \leq p < n$, $d_0 \geq 1$, $d_1, \ldots, d_p \geq 2$. *The complexity of computing a lex Gröbner basis of* $\mathbf{I}(q, \mathbf{F})$ *is bounded above by* $\delta^{O(\log(A)/\log(G))}$.

Proof. First note that the number of sequences $(i_0, \ldots, i_p)$ such that $i_0 = 0$ and $\sum_{j=0}^{p} i_j = n - p$ is $\binom{n-1}{p-1}$. Consequently, the inequality $\delta \geq 2^p\binom{n-1}{p-1}$ holds, and hence the algorithm FGLM is polynomial in δ since its complexity is $O(n \cdot \delta^3)$ [24, Thm. 5.1] and $n \leq 2\binom{n-1}{p-1} \leq \delta$. It is thus sufficient to prove that a grevlex Gröbner basis of $\mathbf{I}(q, \mathbf{F})$ can be computed within $\delta^{O(\log(A)/\log(G))}$ arithmetic operations.

Next, the same inequality $\delta \geq 2^p\binom{n-1}{p-1}$ yields

$$p + \binom{n}{p+1} = \delta^{O(1)}.$$

Since $d_{\mathrm{wit}} + n < 2An$, we obtain

$$O\left(\left(p + \binom{n}{p+1}\right)\binom{n + d_{\mathrm{wit}}}{n}^{\omega}\right) \leq \delta^{O(1)} \cdot O\left(\binom{2An}{n}^{\omega}\right)$$
$$\leq \delta^{O(1)} \cdot O\left(\frac{(2An)^{\omega n}}{(n!)^{\omega}}\right)$$
$$\leq \delta^{O(1)} \cdot A^{O(n)}.$$

Finally, using the fact that $\delta \geq G^n$, we obtain

$$\frac{\log\left(\left(p + \binom{n}{p+1}\right)\binom{n + d_{\mathrm{wit}}}{n}^{\omega}\right)}{\log \delta} = O\left(\frac{n \log A}{\log \delta}\right) = O\left(\frac{n \log A}{n \log G}\right) = O\left(\frac{\log A}{\log G}\right). \qquad \square$$

The next statement shows that this complexity meets the best known complexity bound $D^{O(n)}$. Note that the codimension p does not appear in the following complexity bound: this comes from the fact that $p \leq n$ and hence the dependency in p is hidden in the $O(n)$.

COROLLARY 3.7. *Set* $D = \max_{0 \leq i \leq p}\{d_i\}$. *If* $D \geq 2$ *and with the same notation and the same genericity assumptions as in Theorem* 3.6, *the complexity of computing a lex Gröbner basis of* $\mathbf{I}(q, \mathbf{F})$ *is bounded above by* $D^{O(n)}$.

Proof. By Corollary 3.5, we have

$$d_{\mathrm{wit}} \leq (n - p - 1)\max\{d_i - 1\} - n - p + d_0 + 2\sum_{1 \leq i \leq p} d_i$$
$$\leq (n - p - 1)(D - 1) - n - p + D + 2pD.$$

Next, a proof exactly similar to that of Theorem 3.6 shows that the complexity is bounded above by

$$\delta^{O(1)} \cdot \left(\frac{n - p}{n}(D - 1) + \frac{p}{n}D\right)^{O(n)} = \delta^{O(1)} \cdot D^{O(n)}.$$

The proof is concluded by noticing that $\delta \leq D^p(D - 1)^{n-p}\binom{n}{p} \leq (2D)^n = D^{O(n)}$. $\quad\square$

In several applications, p is small compared to n. Recall that the size of the Gröbner basis is polynomial in δ [24, Cor. 2.1]. Although the following estimate is sometimes worse than the one derived in Corollary 3.7 (for instance, when $p = n - 1$), it shows that the complexity is polynomial in δ for subfamilies of problems where p grows sufficiently slowly with n:

COROLLARY 3.8. *If* $\max\{d_i\} \geq 3$, *then* $\frac{\log(A)}{\log(G)} = O(\frac{n}{n-p})$, *and hence the complexity bound in Theorem* 3.6 *can be specialized to*

$$\delta^{O(n/(n-p))}.$$

Consequently, if $p < \alpha n$ *for* $0 < \alpha < 1$, *the complexity of computing a lex Gröbner basis of* $\mathbf{I}(q, \mathbf{F})$ *(where* $q, \mathbf{F}$ *is a generic system) is bounded above by* $\delta^{O\left(\frac{1}{1-\alpha}\right)}$.

Proof. The first statement is a direct consequence of Theorem 3.6 and of the following inequalities:

$$\log(A) = \log\left(\frac{1}{n}\left[\sum_{i=1}^{p} d_i + (n-p)\max_{0\leq i\leq p}\{d_i - 1\}\right]\right)$$
$$\leq \log\left(\max_{0\leq i\leq p}\{d_i\}\right),$$
$$\log(G) = \frac{1}{n}\left(\sum_{i=1}^{p}\log(d_i) + (n-p)\log\left(\max_{0\leq i\leq p}\{d_i - 1\}\right)\right)$$
$$\geq \frac{n-p}{n}\log\left(\max_{0\leq i\leq p}\{d_i - 1\}\right).$$

Since $\max\{d_i\} \geq 3$, we obtain $\log(A)/\log(G) \leq \frac{\log_2(3)\,n}{n-p}$. The second statement is a direct consequence of the first statement: if $p < \alpha n$, then $n/(n-p) < 1/(1-\alpha)$. □

The next corollary shows that in the context of quadratic programming, the complexity is polynomial in n. Such a bound was already obtained by a different approach in [27].

COROLLARY 3.9 (quadratic programming). *If $d_0 = \cdots = d_p = 2$ and $(q, \mathbf{F})$ is a generic quadratic system, then the complexity of computing a lex Gröbner basis of $\mathbf{I}(q, \mathbf{F})$ is bounded by $n^{O(p)}$.*

Proof. If $d_0 = \cdots = d_p = 2$, then $d_{\mathrm{wit}} \leq 2p + 1$. The complexity bound in Corollary 3.5 for computing a lex Gröbner basis gives

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

Since we have

$$p + \binom{n}{p+1} = n^{O(p)},$$
$$\binom{n+2p+1}{n} = n^{O(p)},$$
$$\delta = 2^p\binom{n}{p} = n^{O(p)},$$

we obtain that the total complexity is bounded by $n^{O(p)}$. □

4. Experimental results. The goal of this section is to provide experimental evidence that the asymptotic complexity results proved in section 3.4 hold in practice for tractable sets of parameters. We use the software FGb 1.58[4] to compute the grevlex Gröbner basis.

Workstation and experimental setting. All computations have been performed on an Intel Core i5-3570 3.4 GHz processor. Since we wish to count the number of arithmetic operations, all computations are done over the finite field GF(65521) so that there is no effect of the growth of the coefficients on the timings. Instances are generated as follows: for $p, n \in \mathbb{N}$, $(d_0, \ldots, d_p) \in \mathbb{N}^{p+1}$ we pick inhomogeneous polynomials $q, f_1, \ldots, f_p \in \mathsf{GF}(65521)[X_1, \ldots, X_n]$ of respective degree $d_0, \ldots, d_p$ uniformly at random. Then, we compute a grevlex Gröbner basis of the ideal $\mathbf{I}(q, (f_1, \ldots, f_p))$ with FGb. For all tests, $\max_{0\leq i\leq p}\{d_i\} \geq 3$.

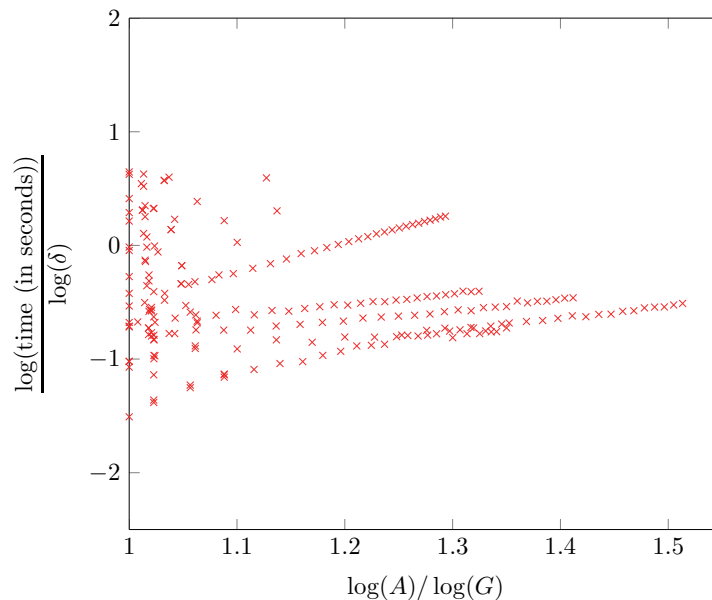[4]Maple package available at http://www-polsys.lip6.fr/~jcf/Software/FGb/.

FIG. 1. *Experimental verification of the complexity bound in Theorem* 3.6.

Experimental verification of Theorem 3.6. Figure 1 shows the behavior of the logarithm of the complexity of the grevlex Gröbner basis computation with `FGb` in terms of $\log(A)/\log(G)$. Theorem 3.6 states that $\log(timing)/\log(\delta)$ should be linear in $\log(A)/\log(G)$ which seems to be validated by experiments.

Experimental verification of Corollary 3.7. Figure 2 shows the behavior of the logarithm of the complexity in terms of the maximum of the degrees of the input system. The figure seems to indicate that $\log(timing)/\log(D)$ is linear in n, where $D = \max\{d_0, \ldots, d_p\}$. This provides experimental evidence of Corollary 3.7, namely, that the complexity is bounded above by $D^{O(n)}$.

5. Proof of Theorem 3.4. One method to bound the witness degree and the complexity of computing Gröbner bases when the input polynomials are inhomogeneous is to bound the degree of the polynomials in a grevlex Gröbner basis of the homogenized system (by introducing a homogenization variable). In the sequel, we use the following notation.

NOTATION 5.1.
- *The ring* $\mathbb{Q}[U_{0,1}, \ldots, U_{p,n}, X_1, \ldots, X_n, H]$ *with grading* $\deg(U_{i,j}) = d_i - 1$, $\deg(X_i) = \deg(H) = 1$ *is denoted by* S^h.
- *For any polynomial* $f \in \mathbb{Q}[X]$, *we let* $f^h \in S^h$ *denote its homogenization*:

$$f^h = H^{\deg(f)} \cdot f\left(\frac{X_1}{H}, \ldots, \frac{X_n}{H}\right) \in S^h.$$

- *For* $i \in \{0, \ldots, p\}, j \in \{1, \ldots, n\}$, *let* $g_{in+j}^h \in S^h$ *denote the polynomial*

$$g_{in+j}^h = \begin{cases} U_{i,j} - \frac{\partial f_i^h}{\partial X_j} & \textit{if } i \in \{1, \ldots, p\}, \\ U_{i,j} - \frac{\partial q^h}{\partial X_j} & \textit{if } i = 0. \end{cases}$$

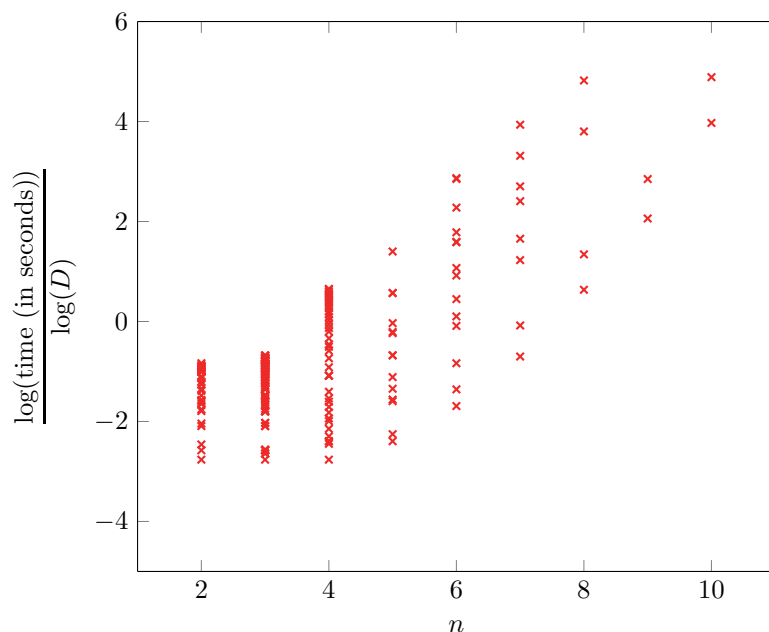- *For* $i \in \{1, \ldots, p\}$, *we set* $g_{(p+1)n+i}^h = f_i^h$.

FIG. 2. *Experimental verification of the complexity bound in Corollary* 3.7.

The two following statements show that the algebraic structure of the ideal generated by the homogenized critical system is the same as the structure of the ideal generated by the homogeneous components of highest degree.

COROLLARY 5.2. *The following equality holds for a generic system* $(q, f_1, \ldots, f_p)$ *of degrees at most* $(d_0, \ldots, d_p)$:

$$\mathsf{HS}_{\mathbb{Q}[X,H]/\mathbf{I}(q^h, \mathbf{F}^h)}(t) = \mathsf{HS}_{\mathbb{Q}[X,H]/\mathbf{I}(q^\infty, \mathbf{F}^\infty)}(t).$$

Proof. First, note that the rings $\mathbb{Q}[X]/\mathbf{I}(q^\infty, \mathbf{F}^\infty)$ and $\mathbb{Q}[X,H]/(\mathbf{I}(q^h, \mathbf{F}^h) + \langle H \rangle)$ are isomorphic. Consequently, they also share the same Krull dimension, which is 0 by Lemma 2.1. Therefore, $\mathbb{Q}[X,H]/\mathbf{I}(q^h, \mathbf{F}^h)$ has dimension at most 1 since dividing by H can only decrease the dimension by one. Since $\mathbb{Q}[X,H]/\mathbf{I}(q^h, \mathbf{F}^h)$ is isomorphic to $\mathbb{Q}[U, X, H]/(\mathscr{D} + \langle g_1^h, \ldots, g_{p+n(p+1)}^h \rangle)$, this latter ring also has Krull dimension at most 1. Next, note that $\mathbb{Q}[U, X, H]$ is a polynomial ring in $n + n(p+1) + 1$ variables. Consequently, by Macaulay's unmixedness theorem and similarly to the proof of Lemma 2.2, $g_1^h, \ldots, g_{p+n(p+1)}^h$ is a regular sequence in $\mathbb{Q}[U, X, H]/\mathscr{D}$. Therefore, the Hilbert series of $\mathbb{Q}[X,H]/(\mathbf{I}(q^h, \mathbf{F}^h)$ is

$$\mathsf{wHS}_{\mathbb{Q}[X,H]/(\mathbf{I}(q^h, \mathbf{F}^h)}(t) = \mathsf{wHS}_{\mathbb{Q}[U,H]/\mathscr{D}}(t) \cdot \frac{(1 - t^{d_0-1})^n \prod_{1 \leq i \leq p}(1 - t^{d_i})(1 - t^{d_i-1})^n}{(1-t)^n}.$$

Finally, by the same proof as in Lemma 2.3, we obtain for $\mathbb{Q}[X,H]/\mathbf{I}(q^\infty, \mathbf{F}^\infty)$

$$\mathsf{wHS}_{\mathbb{Q}[X,H]/\mathbf{I}(q^\infty, \mathbf{F}^\infty)}(t) = \mathsf{wHS}_{\mathbb{Q}[U,H]/\mathscr{D}}(t) \cdot \frac{(1 - t^{d_0-1})^n \prod_{1 \leq i \leq p}(1 - t^{d_i})(1 - t^{d_i-1})^n}{(1-t)^n},$$

which concludes the proof. □

The next statement relates the degree of regularity of $\mathbf{I}(q^\infty, \mathbf{F}^\infty)$ with the maximal degree in the reduced grevlex Gröbner basis of the homogenized system $\mathbf{I}(q^h, \mathbf{F}^h)$.

COROLLARY 5.3.   *For any homogeneous ideal* $I \subset S$, *let* $\mathrm{dmax}_S(I)$ *denote the maximal degree of a polynomial in the reduced grevlex Gröbner basis of* I. *If* $q, f_1, \ldots, f_p$ *are generic polynomials, then*

$$\mathrm{dmax}_{S^h}(\mathbf{I}(q^h, \mathbf{F}^h)) = \mathrm{dmax}_S(\mathbf{I}(q^\infty, \mathbf{F}^\infty)) = \mathrm{d}_{\mathrm{reg}}(\mathbf{I}(q^\infty, \mathbf{F}^\infty)).$$

Proof. For f in S or S^h, let $\mathsf{LM}(f)$ denote its leading monomial with respect to the grevlex ordering with $h \prec X_n \prec \cdots \prec X_1$. For any polynomial $f^h \in S^h$ not divisible by h, $\mathsf{LM}(f^h(X_1, \ldots, X_n, 0)) = \mathsf{LM}(f^h(X_1, \ldots, X_n, H))$. Consequently $\mathsf{LM}(\mathbf{I}(q^\infty, \mathbf{F}^\infty)) \subset \mathsf{LM}(\mathbf{I}(q^h, \mathbf{F}^h))$. By Corollary 5.2 and since for any homogeneous ideal I, $\mathsf{wHS}_{S/I} = \mathsf{wHS}_{S/\mathsf{LM}(I)}$, we obtain $\mathsf{LM}(\mathbf{I}(q^h, \mathbf{F}^h)) = \mathsf{LM}(\mathbf{I}(q^\infty, \mathbf{F}^\infty))$. The degrees of the polynomials in the reduced Gröbner basis of a homogeneous ideal I equal the degrees of a minimal set of generators of $\mathsf{LM}(I)$. Consequently, $\mathrm{dmax}_{S^h}(\mathbf{I}(q^h, \mathbf{F}^h)) = \mathrm{dmax}_S(\mathbf{I}(q^\infty, \mathbf{F}^\infty))$. The second equality $\mathrm{dmax}_S(\mathbf{I}(q^\infty, \mathbf{F}^\infty)) = \mathrm{d}_{\mathrm{reg}}(\mathbf{I}(q^\infty, \mathbf{F}^\infty))$ is a consequence of the definition of the degree of regularity (see section 2.1).   □

We can now conclude the proof of the complexity of the grevlex Gröbner basis computation.

Proof of Theorem 3.4. Recall that the witness degree $\mathrm{d}_{\mathrm{wit}}$ is defined as the smallest integer d such that the $\mathbb{Q}$-vector space

$$T_d = \left\{ \sum f_i \alpha_i + \sum m_j \beta_j \mid \alpha_i, \beta_j \in \mathbb{Q}[X_1, \ldots, X_n], \deg(f_i \alpha_i) \leq d, \deg(m_j \beta_j) \leq d \right\}$$

contains the reduced grevlex Gröbner basis of $\mathbf{I}(q, \mathbf{F})$. It is known that dehomogenizing a grevlex Gröbner basis of $\mathbf{I}(q^h, \mathbf{F}^h)$ yields a Gröbner basis of $\mathbf{I}(q, \mathbf{F})$. A consequence of this fact is that $\mathrm{d}_{\mathrm{wit}} \leq \mathrm{dmax}_{S^h}(\mathbf{I}(q^h, \mathbf{F}^h))$ (see, e.g., [36, 9][28, Proposition 16]). By Corollary 5.3, $\mathrm{dmax}_{S^h}(\mathbf{I}(q^h, \mathbf{F}^h)) = \mathrm{d}_{\mathrm{reg}}(\mathbf{I}(q^\infty, \mathbf{F}^\infty))$.

Now the goal is to compute a triangular basis of the $\mathbb{Q}$-vector space $T_{\mathrm{d}_{\mathrm{reg}}(\mathbf{I}(q^\infty, \mathbf{F}^\infty))}$. This vector space is equal to the row span of the *Macaulay matrix* in degree $\mathrm{d}_{\mathrm{reg}}(\mathbf{I}(q^\infty, \mathbf{F}^\infty))$, which is constructed as follows. The rows of the Macaulay matrix are indexed by all products $\mu \cdot k_\ell$, where k_ℓ is a polynomial of the system generating $\mathbf{I}(q, \mathbf{F})$ (i.e., either an input polynomial f_i or a maximal minor of $\mathsf{jac}(q, \mathbf{F})$) and μ ranges through all monomials of degree at most $\mathrm{d}_{\mathrm{reg}}(\mathbf{I}(q^\infty, \mathbf{F}^\infty)) - \deg(k_\ell)$. The columns of this matrix are indexed by all the monomials of degree at most $\mathrm{d}_{\mathrm{reg}}(\mathbf{I}(q^\infty, \mathbf{F}^\infty))$. The entries of a row of the matrix are the coefficients of the corresponding polynomial $\mu \cdot k_\ell$. The number of rows (resp., columns) of the Macaulay matrix is bounded above by $(n + \binom{n}{p+1})\binom{n + \mathrm{d}_{\mathrm{reg}}(\mathbf{I}(q^\infty, \mathbf{F}^\infty))}{n}$ (resp., $\binom{n + \mathrm{d}_{\mathrm{reg}}(\mathbf{I}(q^\infty, \mathbf{F}^\infty))}{n}$). Since the row echelon form of a $A \times B$ matrix can be computed within $O(AB \min(A, B)^{\omega-2})$ operations [45, Prop. 2.11] (where ω is a feasible exponent for matrix multiplication), this computation can be performed within

$$O\left(\left(n + \binom{n}{p+1} \right) \left(\frac{n + \mathrm{d}_{\mathrm{reg}}(\mathbf{I}(q^\infty, \mathbf{F}^\infty))}{n} \right)^\omega \right)$$

arithmetic operations in $\mathbb{Q}$. The polynomials corresponding to the rows of the reduced Macaulay matrix yield a grevlex Gröbner basis of $\mathbf{I}(q, \mathbf{F})$.   □

helpful discussions and suggestions. The author is grateful to Elisa Gorla for pointing out important references and to an anonymous referee for useful suggestions.

REFERENCES

[1] B. BANK, M. GIUSTI, J. HEINTZ, AND G.-M. MBAKOP, *Polar varieties and efficient real equation solving: the hypersurface case*, J. Complexity, 13 (1997), pp. 5–27.

[2] B. BANK, M. GIUSTI, J. HEINTZ, AND G.-M. MBAKOP, *Polar varieties and efficient real elimination*, Math. Z., 238 (2001), pp. 115–144.

[3] B. BANK, M. GIUSTI, J. HEINTZ, AND L.M. PARDO, *Generalized polar varieties: Geometry and algorithms*, J. Complexity, 21 (2005), pp. 377–412.

[4] B. BANK, M. GIUSTI, J. HEINTZ, AND L.M. PARDO, *Bipolar varieties and real solving of a singular polynomial equation*, Jaen J. Approx., 2 (2010), pp. 65–77.2

[5] B. BANK, M. GIUSTI, J. HEINTZ, AND L.-M. PARDO, *Generalized polar varieties and efficient real elimination procedure*, Kybernetika, 40 (2004), pp. 519–550.

[6] B. BANK, M. GIUSTI, J. HEINTZ, AND L.-M. PARDO, *Generalized polar varieties: Geometry and algorithms*, J. Complexity, 21 (2005), pp. 377–412.

[7] B. BANK, M. GIUSTI, J. HEINTZ, AND M. SAFEY EL DIN, *Intrinsic Complexity Estimates in Polynomial Optimization*, J. Complexity, 30 (2014), pp. 430–443.

[8] B. BANK, M. GIUSTI, J. HEINTZ, M. SAFEY EL DIN, AND É. SCHOST, *On the geometry of polar varieties*, Applicable Algebra Engrg., Comm. Comput., 21 (2010), pp. 33–83.

[9] 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), Paris, France, 2004, pp. 71–74.

[10] M. BARDET, J.-C. FAUGÈRE, B. SALVY, AND P.-J. SPAENLEHAUER, *On the complexity of solving quadratic Boolean systems*, J. Complexity, 29 (2012), pp. 53–75.

[11] A.I. BARVINOK, *Feasibility testing for systems of real quadratic equations*, Discrete Comput. Geom., 10 (1993), pp. 1–13.

[12] 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, Vienna, 1998.

[13] W. BRUNS AND U. VETTER, *Determinantal Rings*, Springer, Berlin, 1988.

[14] B. BUCHBERGER, *An Algorithm for Finding the Basis Elements of the Residue Class Ring of a Zero Dimensional Polynomial Ideal*, Ph.D. thesis, University of Innsbruck, Innsbruck, Austria, 1965.

[15] N. BUDUR, M. CASANELLAS, AND E. GORLA, *Hilbert functions of irreducible arithmetically Gorenstein schemes*, J. Algebra, 272 (2004), pp. 292–310.

[16] J.F. CANNY, *Complexity of Robot Motion Planning*, Ph.D. thesis, Massachusetts Institute of Technology, Cambridge, MA, 1988.

[17] F. CATANESE, S. HOŞTEN, A. KHETAN, AND B. STURMFELS, *The maximum likelihood degree*, Amer. J. Math., 128 (2006), pp. 671–697.

[18] J. DRAISMA, E. HOROBET, G. OTTAVIANI, B. STURMFELS, AND R. R. THOMAS, *The Euclidean Distance Degree of an Algebraic Variety*, preprint, ArXiv:1309.0049, 2013.

[19] J.A. EAGON AND D.G. NORTHCOTT, *Ideals defined by matrices and a certain complex associated with them*, R. Soc. Lond. Proc. Ser. A. Math. Phys. Eng. Sci., 269 (1962), pp. 188–204.

[20] D. EISENBUD, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer, New York, 1995.

[21] D. EISENBUD, *The Geometry of Syzygies*, Springer Verlag, New York, 2005.

[22] J.-C. FAUGÈRE, *A new efficient algorithm for computing Gröbner bases* (F4), J. Pure Appl. Algebra, 139 (1999), pp. 61–88.

[23] J.-C. FAUGÈRE, *A new efficient algorithm for computing Gröbner bases without reductions to zero* (F5), in Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation (ISSAC), ACM, New York, 2002, pp. 75–83.

[24] J.-C. FAUGÈRE, P. GIANNI, D. LAZARD, AND T. MORA, *Efficient computation of zero-dimensional Gröbner bases by change of ordering*, J. Symbolic Comput., 16 (1993), pp. 329–344.

[25] J.-C. FAUGÈRE, F. LÉVY-DIT-VEHEL, AND L. PERRET, *Cryptanalysis of MinRank*, in Advances in Cryptology—CRYPTO 2008, Lecture Notes in Comput. Sci. 5157, Springer, Berlin, 2008, pp. 280–296.

[26] 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 Proceedings of

the 2010 International Symposium on Symbolic and Algebraic Computation (ISSAC 2010), Stephen M. Watt, ed., ACM, New York, 2010, pp. 257–264.

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

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

[29] M. Giusti, G. Lecerf, and B. Salvy, *A Gröbner free alternative for polynomial system solving*, J. Complexity, 17 (2001), pp. 154–211.

[30] D. Grigoriev and D.V. Pasechnik, *Polynomial-time computing over quadratic maps i: Sampling in real algebraic sets*, Comput. Complexity, 14 (2005), pp. 20–52.

[31] D. Grigoriev and N. Vorobjov, *Solving systems of polynomial inequalities in subexponential time*, J. Symbolic Comput., 5 (1988), pp. 37–64.

[32] S. Hosten, A. Khetan, and B. Sturmfels, *Solving the likelihood equations*, Found. Comput. Math., 5 (2005), pp. 389–407.

[33] A. Kipnis and A. Shamir, *Cryptanalysis of the HFE public key cryptosystem by relinearization*, in Advances in Cryptology—CRYPTO' 99, Lecture Notes in Comput. Sci. 1666, Springer, Berlin, 1999, pp. 19–30.

[34] A. Knutson and E. Miller, *Gröbner geometry of Schubert polynomials*, Ann. of Math. (2), (2005), pp. 1245–1318.

[35] A Lascoux and M.-P. Schützenberger, *Structure de Hopf de l'anneau de cohomologie et de l'anneau de Grothendieck d'une variété de drapeaux*, C.R. Acad. Sci. Paris Sér. I Math., 295 (1982), pp. 629–633.

[36] D. Lazard, *Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations*, in Computer Algebra: EUROCAL'83, Lecture Notes in Comput. Sci. 162, Springer, Berlin, 1983, pp. 146–156.

[37] E. Miller and B. Sturmfels, *Combinatorial Commutative Algebra*, Grad. Texts Math. 227, Springer Verlag, New York, 2005.

[38] J. Nie and K. Ranestad, *Algebraic degree of polynomial optimization*, SIAM J. Optim., 20 (2009), pp. 485–502.

[39] L. Pachter and B. Sturmfels, *Algebraic Statistics for Computational Biology*, Cambridge University Press, Cambridge, 2005.

[40] T.G. Room, *The Geometry of Determinantal Loci*, Cambridge University Press, Cambridge, 1938.

[41] F. Rouillier, *Solving zero-dimensional systems through the rational univariate representation*, Applicable Algebra Engrg., Comm. Comput., 9 (1999), pp. 433–461.

[42] M. Safey El Din and É. Schost, *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, New York, 2003, pp. 224–231.

[43] Mohab Safey El Din and Éric Schost, *A Nearly Optimal Algorithm for Deciding Connectivity Queries in Smooth and Bounded Real Algebraic Sets*, preprint, arXiv:1307.7836, 2013.

[44] M. Safey El Din and P. Trébuchet, *Strong Bi-homogeneous Bézout Theorem and its Use in Effective Real Algebraic Geometry*, preprint, Arxiv cs/0610051, 2006.

[45] A. Storjohann, *Algorithms for Matrix Canonical Forms*, Ph.D. thesis, University of Waterloo, Waterloo, Canada, 2000.

[46] L.D. Tráng and B. Teissier, *Variétés polaires locales et classes de Chern des variétés singulieres*, Ann. of Math. (2), 114 (1981), pp. 457–491.

[47] V. Vassilevska Williams, *Multiplying matrices faster than Coppersmith-Winograd*, in Proceedings of the 44th Symposium on Theory of Computing, ACM, New York, 2012, pp. 887–898.