Optimized Gröbner basis algorithms for maximal determinantal ideals and critical point computations

Sriram Gopalakrishnan*
Sorbonne Université, CNRS, LIP6
F-75005 Paris, France

Vincent Neiger
Sorbonne Université, CNRS, LIP6
F-75005 Paris, France

Mohab Safey El Din
Sorbonne Université, CNRS, LIP6
F-75005 Paris, France

ABSTRACT

Given polynomials g and $f_1, \ldots, f_p$, all in $\mathbb{k}[x_1, \ldots, x_n]$ for some field $\mathbb{k}$, we consider the problem of computing the critical points of the restriction of g to the variety defined by $f_1 = \cdots = f_p = 0$. These are defined by the simultaneous vanishing of the f_i's and all maximal minors of the Jacobian matrix associated to $(g, f_1, \ldots, f_p)$. We use the Eagon-Northcott complex associated to the ideal generated by these maximal minors to gain insight into the syzygy module of the system defining these critical points. We devise new F_5-type criteria to predict and avoid more reductions to zero when computing a Gröbner basis for the defining system of this critical locus. We give a bound for the arithmetic complexity of this enhanced F_5 algorithm and compare it to the best previously known bound for computing critical points using Gröbner bases.

KEYWORDS

Gröbner bases, critical points, optimization, real algebraic geometry

1 INTRODUCTION

Motivation and problem. Let $n \in \mathbb{Z}_{>0}$, $\mathbb{k}$ be a field with algebraic closure $\bar{\mathbb{k}}$, and $\mathcal{R}_n = \mathbb{k}[x_1, \ldots, x_n]$ be the ring of polynomials in $x_1, \ldots, x_n$ with coefficients in $\mathbb{k}$. Consider a sequence $F = (f_1, \ldots, f_p)$ of polynomials and another polynomial g, all of them in $\mathcal{R}_n$, and the Jacobian matrix $\mathrm{jac}(g, F)$ associated to g and F. We denote by $\langle F \rangle$ the ideal of $\mathcal{R}_n$ generated by F, and by $I_{p+1}(\mathrm{jac}(g, F))$ the ideal generated by the maximal minors of $\mathrm{jac}(g, F)$. We consider the problem of computing a *Gröbner basis* of the ideal

$$\mathcal{I}(g, F) = \langle F \rangle + I_{p+1}(\mathrm{jac}(g, F)) .$$

When $\langle F \rangle$ is radical, is equidimensional of codimension p, and defines a smooth algebraic set $V(F)$ in $\bar{\mathbb{k}}^n$, the algebraic set $V(\mathcal{I}(g, F))$ in $\bar{\mathbb{k}}^n$ defined by $\mathcal{I}(g, F)$ is the set of critical points of the restriction of the polynomial map defined by g to $V(F)$. Such sets arise in many areas such as polynomial optimization [21, 22], real algebraic geometry [28, 29, 31, 32] and their applications in sciences such as robotics [5–7, 35] and biology [24, 36].

Gröbner bases. Throughout the paper, we assume that the set of critical points under consideration is finite. To compute these critical points, we solve the system consisting of $(f_1, \ldots, f_p)$ and the maximal minors of $\mathrm{jac}(g, F)$. While several recently developed algorithms for solving such systems use symbolic homotopies (see e.g. [23, 25]), we focus here on algebraic algorithms, based on Gröbner bases. These are central in the area of polynomial system solving through computer algebra. We refer to [9] for a reference textbook on Gröbner bases. The classical two-step solving strategy consists in first computing a Gröbner basis for $\mathcal{I}(g, F)$ with respect to the graded reverse lexicographic (grevlex) order, and then using a change of order algorithm to obtain a lexicographic Gröbner basis for $\mathcal{I}(g, F)$, from which the solutions can be read off.

Our focus in this paper is on the first of these two steps, which is nowadays frequently the most expensive of the two [2, 16].

Evolutions of Buchberger's original Gröbner basis algorithm [4] have led to linear algebra-based algorithms, which go back to Lazard's algorithm [27] and include the now standard F_4 and F_5 algorithms [14, 15] which have shown their practical efficiency.

These algorithms work by row echelonization of *Macaulay matrices*, whose columns are indexed by the monomials of $\mathcal{R}_n$ up to some degree d and sorted by grevlex, and whose rows store the coefficients of the input polynomials multiplied by the monomials required to reach the degree d. If d is large enough, the obtained echelon form yields a Gröbner basis [27]. This large enough degree is often called *degree of regularity*. Successive enhancements of this approach have culminated with the F_5 algorithm [15] (see also [11]), which manages to a priori discard rows that would otherwise reduce to 0 upon echelonization. It has been shown that for sequences of polynomials that are *generic* (in the sense of the Zariski topology), the so-called F_5-criterion detects all reductions to 0 a priori, and F_5 thus saves all computations related to them. A key observation behind this criterion is that these reductions to 0 come from the Koszul syzygies, induced by the commutativity of the multiplication in $\mathcal{R}_n$. This yields faster Gröbner basis computations for ideals generated by such generic sequences [1].

However, it is not the case that the F_5-criterion eliminates all reductions to 0 on classes of structured systems, including the ones defining critical points. For these systems, it has been established [33, Thm. 3.4] [17] that under genericity assumptions on (g, F), a *grevlex* Gröbner basis of $\mathcal{I}(g, F)$ can be computed using

$$O\left(\left(p + \binom{n}{p+1}\right)\binom{n + (n+p)d_0 + 1}{n}^{\omega}\right)$$

operations in $\mathbb{k}$; this is done by determining the degree of regularity of the ideal. (Here, $\omega > 2$ is a feasible exponent for square matrix multiplication over $\mathbb{k}$.) The goal of this paper is to introduce a criterion, for critical point systems, that complements the F_5-criterion so as to avoid more reductions to 0 and thus gain in efficiency.

Contributions. It is known that the F_5 algorithm can be enhanced with some insight into the syzygy modules associated to the generators of the ideal under study [11]. This is exploited in [20, Algo. 3], where a free resolution is used to obtain generators for each syzygy module, allowing then to call the F_5 algorithm to compute Gröbner bases without reductions to 0 for the syzygy modules and finally for the ideal itself. The latter reference studies the case of square matrices with rank deficiency, which leads to considering free resolutions of a fixed length, whose boundary homomorphisms admit transparent enough descriptions that computing syzygy modules

*Also with University of Waterloo.

from them is a straightforward process. In contrast, here we have to deal with a more involved complex, namely the Eagon-Northcott one [10], whose length depends on the size of the matrix under consideration. It is thus not clear that computing Gröbner bases for the syzygy modules could lead to an efficient algorithm. Still, the specific nature of syzygies between maximal minors allows us to take a more sophisticated approach for the detection of reductions to 0.

We actually analyze the first syzygy module of the Eagon-Northcott complex and exhibit a submodule of its leading terms (w.r.t. some module ordering induced by grevlex). This has a simple algorithmic consequence: by incrementally computing Gröbner bases of ideals generated by the leftmost entries of the considered matrix (which fits perfectly with the incremental nature of F_5), one obtains enough information to easily identify a submodule of the one generated by the leading terms of the first syzygy module. When combined with the syzygy criterion of F_5 (see [11, Lemma 6.4]), this allows us to discard a significant number of rows in the Macaulay matrices that arise when computing critical points. This technique can also be used for pure determinantal ideals, i.e. ideals generated maximal minors of a given matrix with entries in $\mathcal{R}_n$. Hence, all in all, we obtain a new F_5-type algorithm dedicated to systems involving the maximal minors of a matrix with entries in $\mathcal{R}_n$ that avoids some reductions to 0 that the F_5-criterion alone does not avoid.

Quantifying the resulting complexity gain is challenging. As usual for analyzing Gröbner basis algorithms, one needs genericity assumptions. Here, genericity regards the coefficients of F and g, and we assume a variant of Fröberg's conjecture. We show that the extra computations performed to identify some of the leading terms of the first syzygy module is negligible compared to the cost of the whole computation. To obtain a complexity estimate, we count those leading terms, which provides a lower bound on the number of rows of the Macaulay matrices which our approach discards. The obtained formula is rather involved, but much more precise than an analysis based on the degree of regularity alone.

Our complexity analysis does not take into account all rows removed by the full syzygy criterion. Hence, it is plausible that our complexity bound may be improved in the future. Since the complexity bound that we give is rather involved, we evaluate the number of rows in the Macaulay matrices that we build for certain parameters. Comparing this count to the upper bound on the number of rows built by Lazard's algorithm obtained in [33, Theorem 3.4], we see that the complexity bound improvement that we obtain is at least polynomial in n and that, if we were able to take into account the full syzygy criterion, it may be exponential in n.

Outline. Basic notions from algebra and signature Gröbner bases are recalled in Sections 2 and 3, respectively. In Section 4, we present constructions on which the Eagon-Northcott complex relies and show how to use them to obtain a new F5-type criterion. In Section 5, we apply this criterion to design a Gröbner basis algorithm dedicated to critical points. Finally, Section 6 carries out a complexity analysis of that algorithm under genericity assumptions.

2 PRELIMINARIES

In this section, we recall the basic constructions and establish the notation upon which we rely throughout the paper.

Polynomials and matrices. We denote by $\mathcal{R}_n = \Bbbk[x_1, \ldots, x_n]$ the ring of polynomials in n indeterminates over $\Bbbk$. For a module $\mathcal{M}$ over a ring $\mathcal{R}$ and a subset $F \subseteq \mathcal{M}$, we denote by $\langle\langle F \rangle\rangle$ the $\mathcal{R}$-submodule of $\mathcal{M}$ generated by F. In particular, if $\mathcal{M} = \mathcal{R}$, so that $F \subseteq \mathcal{R}$ is a collection of elements of $\mathcal{R}$, the $\mathcal{R}$-submodule $\langle\langle F \rangle\rangle$ of $\mathcal{R}$ is the ideal $\langle F \rangle$ of $\mathcal{R}$ generated by F.

For $\alpha \in \mathbb{Z}^n_{\geq 0}$, we take $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in \mathcal{R}_n$. For $d \in \mathbb{Z}_{\geq 0}$, we denote by $\mathrm{Mon}_d(\mathcal{R}_n)$ the set of monomials of $\mathcal{R}_n$ of degree d.

For a ring $\mathcal{R}$, we will denote by $\mathcal{R}^{p\times q}$ the set of matrices with p rows and q columns with entries in $\mathcal{R}$; this is a free $\mathcal{R}$-module of rank $p \cdot q$. Let $A \in \mathcal{R}^{p\times q}$, and let $r \in \{1, \ldots, \min(p, q)\}$. Let $1 \leq i_1 < \cdots < i_r \leq p$ and $1 \leq j_1 < \cdots < j_r \leq q$ be two strictly increasing sequences of integers. We denote by $[i_1 \cdots i_r \mid j_1 \cdots j_r]_A$ the $r \times r$ submatrix of A with rows indexed by $(i_1, \ldots, i_r)$ and columns indexed by $(j_1, \ldots, j_r)$. We denote by $F_r(A)$ the subset of $\mathcal{R}$ consisting of the minors of A of size $r \times r$, and by $I_r(A) = \langle F_r(A) \rangle$ the ideal of $\mathcal{R}$ generated by $F_r(A)$.

Modules and bases. In order to introduce the portions of the Eagon-Northcott complex which are relevant to us, we will need to briefly use the language of tensor, symmetric, and exterior algebras (we refer to [26, Chap. 16,19] as a reference book on these topics). As such, we introduce their notation and canonical bases.

A ring $\mathcal{R}$ is called *graded* if, for each integer $d \geq 0$, there exist additive abelian groups $\mathcal{R}_{[d]}$ such that $\mathcal{R} = \bigoplus_{d=0}^{\infty} \mathcal{R}_{[d]}$ and $\mathcal{R}_{[d]}\mathcal{R}_{[e]} \subseteq \mathcal{R}_{[d+e]}$. The elements of $\mathcal{R}_{[d]}$ are called the *homogeneous elements of degree d*. Our prototypical example of a graded ring will be the ring $\mathcal{R}_n$. Here, $\Bbbk[x_1, \ldots, x_n]_{[d]}$ consists of the homogeneous polynomials of degree d (together with 0, which is, by definition, homogeneous of every degree).

A module $\mathcal{M}$ over a graded ring $\mathcal{R}$ is called *graded* if, for each $d \geq 0$, there exist abelian groups $\mathcal{M}_{[d]}$ such that $\mathcal{M} = \bigoplus_{d=0}^{\infty} \mathcal{M}_{[d]}$ and $\mathcal{R}_{[d]}\mathcal{M}_{[e]} \subseteq \mathcal{M}_{[d+e]}$. For an integer $s \geq 1$, $\mathcal{R}^s$ naturally carries the structure of a free $\mathcal{R}$-module of rank s. We take as a basis for $\mathcal{R}^s$ the standard basis vectors $\{e_i : 1 \leq i \leq s\}$. If $\mathcal{R}$ is graded, it induces a natural grading on all free modules $\mathcal{R}^s$. For a graded module $\mathcal{M}$ and $e \in \mathbb{Z}$, we denote by $\mathcal{M}(e)$ the module $\mathcal{M}$ with the grading such that $\mathcal{M}(e)_{[d]} = \mathcal{M}_{[d+e]}$.

For $s \in \mathbb{Z}_{>0}$, we call an element of $\mathcal{R}_n^s$ a *monomial* if it takes the form $x^\alpha e_i$ for some $\alpha \in \mathbb{Z}^n_{\geq 0}$ and $1 \leq i \leq s$. Note that $\mathcal{R}_n$ is naturally graded by degree and thus so is $\mathcal{R}_n^s$. We denote by $\mathrm{Mon}_d(\mathcal{R}_n^s)$ the set of all monomials of $\mathcal{R}_n^s$ of degree d.

The *tensor algebra* of a module $\mathcal{M}$ over a ring $\mathcal{R}$ is denoted $T(\mathcal{M})$ and is defined by $T(\mathcal{M}) = \bigoplus_{d=0}^{\infty} \mathcal{M}^{\otimes d}$. Explicitly, for pure tensors $f_1 \otimes \cdots \otimes f_d \in \mathcal{M}^{\otimes d}$ and $g_1 \otimes \cdots \otimes g_e \in \mathcal{M}^{\otimes e}$ of ranks d and e respectively, we have

$$(f_1 \otimes \cdots \otimes f_d) \cdot (g_1 \otimes \cdots \otimes g_e) = f_1 \otimes \cdots \otimes f_d \otimes g_1 \otimes \cdots \otimes g_e \in \mathcal{M}^{\otimes (d+e)}.$$

The algebra $T(\mathcal{M})$ carries a natural grading as a ring, wherein its homogeneous part of degree d is precisely the $\mathcal{R}$-module $\mathcal{M}^{\otimes d}$.

Proposition 2.1. *[12, Cor. A2.3] Let $\mathcal{R}$ be a ring and let $\mathcal{M}$ be a finite free $\mathcal{R}$-module with basis $e_1, \ldots, e_s$. Then for any integer $d \geq 1$,*

$\mathcal{M}^{\otimes d}$ is a free module of rank s^d and the set $\{e_{i_1} \otimes \cdots \otimes e_{i_d} : 1 \leq i_1, \ldots, i_d \leq s\}$ is an $\mathcal{R}$-basis for $\mathcal{M}^{\otimes d}$.

The *symmetric algebra* $\mathrm{Sym}(\mathcal{M})$ of a module $\mathcal{M}$ over a ring $\mathcal{R}$ is simply the quotient $T(\mathcal{M})/\langle u \otimes v - v \otimes u : u, v \in \mathcal{M}\rangle$. The grading on $T(\mathcal{M})$ naturally induces a grading on $\mathrm{Sym}(\mathcal{M})$, wherein the homogeneous part of degree d of $\mathrm{Sym}(\mathcal{M})$ is called the *d-th symmetric power of $\mathcal{M}$* and is denoted $\mathrm{Sym}_d(\mathcal{M})$.

The *exterior algebra* of a module $\mathcal{M}$ over a ring $\mathcal{R}$ is denoted $\bigwedge(\mathcal{M})$ and is defined by $\bigwedge(\mathcal{M}) = T(\mathcal{M})/\langle x \otimes x : x \in \mathcal{M}\rangle$. We denote by $f_1 \wedge \cdots \wedge f_d$ the image of the pure tensor $f_1 \otimes \cdots \otimes f_d$ in $\bigwedge(\mathcal{M})$. The grading on $T(\mathcal{M})$ described above naturally induces a grading on $\bigwedge(\mathcal{M})$. In this case, the homogeneous part of degree d of $\bigwedge(\mathcal{M})$ is called the *d-th exterior power of $\mathcal{M}$* and is denoted $\bigwedge^d(\mathcal{M})$. As in the case of $\mathcal{M}^{\otimes d}$, the abelian group $\bigwedge^d(\mathcal{M})$ naturally carries the structure of an $\mathcal{R}$-module.

Proposition 2.2. *[12, Cor. A2.3] Let $\mathcal{R}$ be a ring and let $\mathcal{M}$ be a finite free $\mathcal{R}$-module with basis $e_1, \ldots, e_s$. Then for any integer $d \geq 1$, $\bigwedge^d(\mathcal{M})$ is a free module of rank $\binom{s}{d}$ and the set $\{e_{i_1} \otimes \cdots \otimes e_{i_d} : 1 \leq i_1 < \cdots < i_d \leq s\}$ is an $\mathcal{R}$-basis for $\bigwedge^d(\mathcal{M})$.*

For a module $\mathcal{M}$ over a ring $\mathcal{R}$, we denote by $(\mathcal{M})^* = \mathrm{Hom}(\mathcal{M}, \mathcal{R})$ the *dual module* of $\mathcal{M}$. A sequence $(f_1, \ldots, f_s) \subseteq \mathcal{R}$ is said to be *$\mathcal{M}$-regular* if f_1 is not a zero-divisor in $\mathcal{M}$ and, for all $2 \leq i \leq s$, f_i is not a zero-divisor in $\mathcal{M}/\langle f_1, \ldots, f_{i-1}\rangle$. If $\mathcal{I}$ is an ideal of $\mathcal{R}$, the *grade of $\mathcal{I}$ with respect to $\mathcal{M}$*, denoted $\mathrm{grade}(\mathcal{I}, \mathcal{M})$ is the length of a maximal $\mathcal{M}$-regular sequence of elements of $\mathcal{I}$. We take $\mathrm{grade}(\mathcal{I}) = \mathrm{grade}(\mathcal{I}, \mathcal{R})$.

Hilbert functions. For a graded module $\mathcal{M}$ over $\mathcal{R}_n$ equipped with its natural grading by degree, the *Hilbert function* of $\mathcal{M}$ is defined by $\mathrm{HF}_{\mathcal{M}}(d) = \dim_{\Bbbk}(\mathcal{M}_d)$. The *Hilbert series* $H_{\mathcal{M}}(t) = \sum_{d \geq 0} \mathrm{HF}_{\mathcal{M}}(d) t^d \in \mathbb{Z}[\![t]\!]$ of $\mathcal{M}$ is the generating function of $\mathrm{HF}_{\mathcal{M}}(d)$.

Theorem 2.3. *[12, Thm. 1.1] If $\mathcal{M}$ is a finitely generated graded module over $\mathcal{R}_n$, then $\mathrm{HF}_{\mathcal{M}}(d)$ is, for sufficiently large d, a polynomial $P_{\mathcal{M}}(d)$ of degree at most $n-1$.*

Pursuant to Theorem 2.3, the polynomial $P_{\mathcal{M}}(d)$ is called the *Hilbert polynomial* of d. The *Hilbert regularity* of $\mathcal{M}$, is the smallest integer d such that for all $d' \geq d$, $\mathrm{HF}_{\mathcal{M}}(d') = P_{\mathcal{M}}(d')$.

Syzygies and free resolutions. Free resolutions are a fundamental construction, with many general properties [12, Part III] [9, Ch. 6]. Again, we recall below only what we need for our purposes.

Let $\mathcal{R}$ be a ring and $\mathcal{M}$ a finite $\mathcal{R}$-module. An exact sequence

$$\cdots \xrightarrow{\partial_{j+1}} \mathcal{E}_j \xrightarrow{\partial_j} \cdots \xrightarrow{\partial_2} \mathcal{E}_1 \xrightarrow{\partial_1} \mathcal{E}_0 \xrightarrow{\epsilon} \mathcal{M} \to 0$$

is a *left resolution* of $\mathcal{M}$. The maps ∂_i are *boundary homomorphisms*, and the map ϵ is an *augmentation homomorphism*. If for each i, the module $\mathcal{E}_i$ is free, then the resolution is a *free resolution*. For the sake of brevity, we will often refer to a resolution as above simply by $(\mathcal{E}_\bullet \xrightarrow{\epsilon} \mathcal{M}, \partial_\bullet)$. We call $\sup\{i \in \mathbb{Z} : \mathcal{E}_i \neq 0\}$ the *length* of the resolution $(\mathcal{E}_\bullet \xrightarrow{\epsilon} \mathcal{M}, \partial_\bullet)$. The length of $(\mathcal{E}_\bullet \xrightarrow{\epsilon} \mathcal{M}, \partial_\bullet)$ could be infinite and free resolutions of finite length are *finite free resolutions*.

Theorem 2.4 (Hilbert's syzygy theorem, [12, Cor. 19.7]). *Let $\mathcal{M}$ be a finitely generated $\Bbbk[x_1, \ldots, x_n]$-module. There exists a free resolution $(\mathcal{E}_\bullet \xrightarrow{\epsilon} \mathcal{M}, \partial_\bullet)$ of length at most n.*

When $\mathcal{R}$ is graded and $\mathcal{M}$ is a graded $\mathcal{R}$-module, $\mathcal{M}$ possesses a free resolution $(\mathcal{E}_\bullet \xrightarrow{\epsilon} \mathcal{M}, \partial_\bullet)$ where each $\mathcal{E}_i$ is graded so that the boundary maps ∂_i and the augmentation map ϵ are graded $\mathcal{R}$-module homomorphisms. Such free resolutions are called *graded free resolutions*. Graded free resolutions $(\mathcal{E}_\bullet \xrightarrow{\epsilon} \mathcal{M}, \partial_\bullet)$ such that the ranks of each of the $\mathcal{E}_i$ are minimal are *minimal free resolutions*.

Let $\mathcal{R}$ be a ring and $F = (f_1, \ldots, f_s) \subseteq \mathcal{R}$ a sequence of elements of $\mathcal{R}$. We define the *syzygy module* of F to be the $\mathcal{R}$-module

$$\mathrm{Syz}(F) = \{(g_1, \ldots, g_s) \in \mathcal{R}^s : g_1 f_1 + \cdots + g_s f_s = 0\}.$$

If $(\mathcal{E}_\bullet \xrightarrow{\epsilon} \mathcal{M}, \partial_\bullet)$ is a free resolution of length ℓ, with $\mathrm{rank}(\mathcal{E}_i) = r_i$ then $\mathrm{Syz}(\epsilon(e_1), \ldots, \epsilon(e_{r_0})) = \ker(\epsilon) = \mathrm{im}(\partial_1)$ and for each $1 \leq i \leq \ell$, $\mathrm{Syz}(\partial_i(e_1), \ldots, \partial_i(e_{r_i})) = \ker(\partial_i) = \mathrm{im}(\partial_{i+1})$.

The following consequence of Hilbert's syzygy theorem elucidates the connection between free resolutions and Hilbert series.

Corollary 2.5. *[8, Thm. 4.4] Let $\mathcal{R}$ be a graded ring, let $\mathcal{M}$ be a finitely generated graded $\mathcal{R}$-module, and let $(\mathcal{E}_\bullet \xrightarrow{\epsilon} \mathcal{M}, \partial_\bullet)$ be a finite graded free resolution of $\mathcal{M}$ of length ℓ. For any $1 \leq i \leq \ell$, let $s_i = \mathrm{rank}(\mathcal{E}_i)$ and write $\mathcal{E}_i = \bigoplus_{j=1}^{s_i} \mathcal{R}(-d_i^{(j)})$. Then*

$$\mathrm{HF}_{\mathcal{M}}(d) = \textstyle\sum_{i=0}^{\ell} (-1)^i \sum_{j=1}^{s_i} \binom{k+d-d_i^{(j)}-1}{k-1}.$$

Genericity. Several of our results rely on genericity assumptions. Let $\mathrm{Mon}_d(\mathcal{R}_n)$ be the set of monomials in $\mathcal{R}_n$ of degree d. For $n, d \in \mathbb{Z}_{>0}$, and a set $\mathfrak{c} = \{\mathfrak{c}_\tau : \tau \in \mathrm{Mon}_d(\mathcal{R}_n)\}$ of indeterminates, we call the polynomial

$$\mathfrak{f}^{\mathfrak{c}}_{(n,d)} = \textstyle\sum_{\tau \in \mathrm{Mon}_d(\mathcal{R}_n)} \mathfrak{c}_\tau \tau \quad \in \mathcal{R}_n[\mathfrak{c}]$$

the *generic homogeneous polynomial in n variables of degree d*. A point $c = (c_\tau : \tau \in \mathrm{Mon}_d(\mathcal{R}_n)) \in \mathbb{A}^{\binom{n+d-1}{n-1}}$ defines a map

$$\phi_{\mathfrak{c}} : \mathcal{R}_n[\mathfrak{c}] \to \mathcal{R}_n; \quad \mathfrak{c}_\tau \mapsto c_\tau$$

which maps $\mathfrak{f}^{\mathfrak{c}}_{(n,d)}$ to a homogeneous polynomial of degree d.

Let $(d_1, \ldots, d_s) \in \mathbb{Z}^s_{>0}$ and let $\mathfrak{c}^{(1)}, \ldots, \mathfrak{c}^{(s)}$ be sets of indeterminates, with $\mathfrak{c}^{(i)} = \{\mathfrak{c}_\tau^{(i)} : \tau \in \mathrm{Mon}_{d_i}(\mathcal{R}_n)\}$ for each $1 \leq i \leq s$. For a point $c = (c^{(1)}, \ldots, c^{(s)}) \in \prod_{i=1}^s \mathbb{A}^{\binom{n+d_i-1}{n-1}}$, the map

$$\phi_c : \mathcal{R}_n[\mathfrak{c}^{(1)}, \ldots, \mathfrak{c}^{(s)}] \to \mathcal{R}_n; \quad \mathfrak{c}_\tau^{(i)} \mapsto c_\tau^{(i)}$$

defines a sequence of polynomials $(\phi_c(\mathfrak{f}^{\mathfrak{c}^{(1)}}_{(n,d_1)}), \ldots, \phi_c(\mathfrak{f}^{\mathfrak{c}^{(s)}}_{(n,d_s)}))$, with $\phi_c(\mathfrak{f}^{\mathfrak{c}^{(1)}}_{(n,d_i)})$ homogeneous of degree d_i, for each $1 \leq i \leq s$. Given such a point c, we will simply denote by $\phi_c(\mathfrak{f}_{(n,d_1,\ldots,d_s)})$ the sequence of polynomials defined by c in this way.

Similarly, let $p, q \in \mathbb{Z}_{>0}$ with $q \geq p$ and for $1 \leq i \leq p$, $1 \leq j \leq q$, let $d_{i,j} \in \mathbb{Z}_{>0}$ and let $\mathfrak{c}^{(i,j)} = \{\mathfrak{c}_\tau^{(i,j)} : \tau \in \mathrm{Mon}_{d_{(i,j)}}(\mathcal{R}_n)\}$ be a set of indeterminates. For a sequence of points $c = (c^{(1,1)}, \ldots, c^{(p,q)})$ with $c^{(i,j)} \in \mathbb{A}^{\binom{n+d_{i,j}-1}{n-1}}$, the map

$$\phi_c : \mathcal{R}_n[\mathfrak{c}^{(1,1)}, \ldots, \mathfrak{c}^{(p,q)}] \to \mathcal{R}_n; \quad \mathfrak{c}_\tau^{(i,j)} \mapsto c_\tau^{(i,j)}$$

defines a matrix $(\phi_c(\mathfrak{f}^{\mathfrak{c}^{(i,j)}}_{(n,d_{i,j})}))_{i,j} \in \mathcal{R}_n^{p \times q}$. Again, given such a sequence of points $c = (c^{(1,1)}, \ldots, c^{(p,q)})$, we will simply denote by $\phi_c(\mathfrak{f}_{(n,d_{i,j})}) \in \mathcal{R}_n^{p \times q}$ the $p \times q$ matrix defined by c in this way.

The following important fact is what will allow us to use the Eagon-Northcott complex to compute syzygies amongst maximal minors of polynomial matrices.

Proposition 2.6 ([3, Thm. 2.5]). *Let $n, p, q, d_0 \in \mathbb{Z}_{>0}$ with $q \geq p$. Then there exists a Zariski open subset $U \subseteq \mathbb{A}^{pq\binom{n+d_0-1}{n-1}}$ such that for all $c \in U$, $\operatorname{grade}(I_p(\phi_c(\mathfrak{f}_{(n,d_0)}))) = q - p + 1$.*

3 SIGNATURE GRÖBNER BASES

From here on, we take $\succ$ to be the *graded reverse lexicographic* (or grevlex) order on $\mathcal{R}_n$, and $\succ^{\mathrm{POT}}$ to be the corresponding *position over term* (or POT) order on $\mathcal{R}_n^s$ (see e.g. [8, Def. 2.4, p211]).

Gröbner bases and modules. By Proposition 2.2, if $\mathcal{M}$ is a free $\mathcal{R}_n$-module of rank s, then $\bigwedge^d(\mathcal{M})$ is also a free $\mathcal{R}_n$-module of rank $\binom{s}{d}$. Since the basis we fix on $\bigwedge^d(\mathcal{M})$ is not indexed by the integers $1, \ldots, \binom{s}{d}$ we slightly generalize the definition of the POT order: for $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$ and two strictly increasing sequences $1 \leq i_1 < \cdots < i_d \leq s$, $1 \leq i'_1 < \cdots < i'_d \leq s$, we take $x^\alpha(e_{i_1} \otimes \cdots \otimes e_{i_d}) \succ^{\mathrm{POT}} x^\beta(e_{i'_1} \otimes \cdots \otimes e_{i'_d})$ if and only if $(i_1, \ldots, i_d) \succ_{\mathrm{lex}} (i'_1, \ldots, i'_d)$ or $(i_1, \ldots, i_d) = (i'_1, \ldots, i'_d)$ and $x^\alpha \succ x^\beta$.

The set of all monomials of $\mathcal{R}_n$ (resp. $\mathcal{R}_n^s$) forms a basis for $\mathcal{R}_n$ (resp. $\mathcal{R}_n^s$) as an infinite-dimensional $\Bbbk$-vector space. The *leading monomial* of an element $f \in \mathcal{R}_n$ (resp. $f \in \mathcal{R}_n^s$), denoted $\mathrm{LM}_\succ(f)$ (resp. $\mathrm{LM}_\succ^{\mathrm{POT}}(f)$) is the largest monomial, with respect to $\succ$ (resp. $\succ^{\mathrm{POT}}$), which appears in the unique representation of f in this $\Bbbk$-basis. We naturally extend the leading monomial notation to sets: for a set $F \subseteq \mathcal{R}_n^s$, $\mathrm{LM}_\succ^{\mathrm{POT}}(F) = \{\mathrm{LM}_\succ^{\mathrm{POT}}(f) : f \in F\}$.

For some $s \in \mathbb{Z}_{>0}$, a *$\succ^{POT}$-Gröbner basis* of a submodule $\mathcal{M} \subseteq \mathcal{R}_n^s$ is a set $G \subseteq \mathcal{M}$ such that $\langle\!\langle \mathrm{LM}_\succ^{\mathrm{POT}}(G) \rangle\!\rangle = \langle\!\langle \mathrm{LM}_\succ^{\mathrm{POT}}(\mathcal{M}) \rangle\!\rangle$. When $s = 1$ so that $\succ^{\mathrm{POT}}$ coincides with $\succ$ and $\mathcal{M}$ is an ideal of $\mathcal{R}_n$, we call a $\succ^{\mathrm{POT}}$-Gröbner basis of $\mathcal{M}$ a $\succ$-Gröbner basis.

Macaulay matrices. For integers $s, n \in \mathbb{Z}_{>0}$ and a set $F = \{f_1, \ldots, f_t\} \subseteq \mathcal{R}_n^s$ of homogeneous elements, the *Macaulay matrix of F in degree d with respect to $\succ^{POT}$*, denoted $\mathscr{M}_d(F)$, is constructed as follows: its rows are indexed by the set $\bigcup_{i=1}^s \{\tau e_i : \tau \in \mathrm{Mon}_{d-\deg f_i}(\mathcal{R}_n)\}$, its columns are indexed by $\mathrm{Mon}_d\left(\mathcal{R}_n^s\right)$, ordered decreasingly by $\succ^{\mathrm{POT}}$, and for some $1 \leq i, j \leq s$ and $\tau \in \mathrm{Mon}_{d-\deg f_i}(\mathcal{R}_n)$, $\sigma \in \mathrm{Mon}_d\left(\mathcal{R}_n^s\right)$, the entry of the row indexed by τe_i in the column indexed by σe_j is the coefficient of σe_j in τf_i. The monomial τe_i is the *signature* of the row of $\mathscr{M}_d(F)$ which it indexes.

For $1 \leq i \leq t$, we abbreviate $\mathscr{M}_{d,i}(F) = \mathscr{M}_d(\{f_1, \ldots, f_i\})$.

A *valid elementary row operation* on a Macaulay matrix $\mathscr{M}_d(F)$ consists in adding to a row of $\mathscr{M}_d(F)$ with signature τe_i a $\Bbbk$-multiple of a row with some signature σe_j, where $\tau e_i \succ^{\mathrm{POT}} \sigma e_j$. Finally, we denote by $\widetilde{\mathscr{M}_d}(F)$ a row-echelon form of $\mathscr{M}_d$ computed via a sequence of valid elementary row operations.

Each row of $\mathscr{M}_d(F)$ can be interpreted as an element of $\mathcal{R}_n^s$ by multiplying the entry in a given column by the monomial which indexes that column and taking the sum over all columns. We refer to rows of $\mathscr{M}_d(F)$ (resp. $\widetilde{\mathscr{M}_d}(F)$) as elements of $\mathcal{R}_n^s$, denoting them by $\mathrm{rows}(\mathscr{M}_d(F))$ (resp. $\mathrm{rows}(\widetilde{\mathscr{M}_d}(F))$).

For some $D \in \mathbb{Z}_{>0}$, we call $(D, \succ^{POT})$*-Gröbner basis* of $\langle F \rangle$ the union of the sets $\mathrm{rows}(\widetilde{\mathscr{M}_d}(F))$ for $d = \{\min_{1 \leq i \leq t}\{\deg f_i\}, \ldots, D\}$. This is justified by the following.

Proposition 3.1. *[27, Sec. 3] Let $s, n \in \mathbb{Z}_{>0}$ and let $F = \{f_1, \ldots, f_t\} \subseteq \mathcal{R}_n^s$ be homogeneous elements with respect to the standard grading on $\mathcal{R}_n^s$. Then there exists $D \in \mathbb{Z}_{>0}$ such that a $(D, \succ^{POT})$-Gröbner basis of $\langle F \rangle$ is a $\succ^{POT}$-Gröbner basis of $\langle F \rangle$.*

Moreover, it is shown in [27, Sec. 3] that generically (in the sense of Section 2), the integer D in Proposition 3.1 satisfies the bound $D \leq 1 + \sum_{i=1}^t (\deg(f_i) - 1)$.

The matrix-F_5 algorithm. Proposition 3.1 leads to an algorithm to compute Gröbner bases using linear algebra. This algorithm, known as Lazard's algorithm, is described in [27]. Informally, given a polynomial system $F \subseteq \mathcal{R}_n$ and a degree bound $D \in \mathbb{Z}_{>0}$, it works by building the matrices $\mathscr{M}_d(F)$ and computing from them $\widetilde{\mathscr{M}_d}(F)$, for each degree $\min_{1 \leq i \leq t}\{\deg(f_i)\} \leq d \leq D$.

The following proposition, known as the syzygy criterion, lies at the core of the MatrixF$_5$ algorithm, which improves upon Lazard's algorithm by building Macaulay matrices with fewer rows.

Proposition 3.2 (Syzygy Criterion, [11, Lem. 6.4]). *Let $s \in \mathbb{Z}_{>0}$, $F = (f_1, \ldots, f_t) \subseteq \mathcal{R}_n^s$ be homogeneous elements and let $h = (h_1, \ldots, h_\ell)$ be a homogeneous syzygy of F with $\mathrm{LM}_\succ^{\mathrm{POT}}(h) = \tau e_i$.*

1. *The row of $\mathscr{M}_{\deg \tau + d_i}$ with signature τe_i is a linear combination of rows of $\mathscr{M}_{\deg \tau + \deg f_i}$ of smaller signature.*
2. *For any monomial $\sigma \in \mathcal{R}_n$, the row of $\mathscr{M}_{\deg \tau + \deg \sigma + \deg f_i}$ with signature $\sigma\tau e_i$ is a linear combination of rows of $\mathscr{M}_{\deg \tau + \deg \sigma + \deg f_i}$ of smaller signature.*

Suppose now that $F = (f_1, \ldots, f_t) \subseteq \mathcal{R}_n$ is a polynomial system. Then for each $1 \leq i, j \leq t$, $f_i e_j - f_j e_i \in \mathrm{Syz}(F)$. Syzygies of this form are called *Koszul syzygies* and the MatrixF$_5$ algorithm exploits precisely these syzygies to improve upon Lazard's algorithm.

Theorem 3.3 (F_5 Criterion, [15, Thm. 1]). *Let $F = (f_1, \ldots, f_\ell)$ be a polynomial system in $\mathcal{R}_n$. Then for any $d \in \mathbb{Z}_{>0}$, any $1 \leq i \leq \ell$, any $\tau \in \mathrm{LM}_\succ(\mathrm{rows}(\widetilde{\mathscr{M}_{d,i}}(F)))$, and any $i < j \leq \ell$, the row of $\mathscr{M}_{d+\deg(f_j)}(F)$ with signature τe_j is a linear combination of rows of $\mathscr{M}_{d+\deg(f_j)}(F)$ with smaller signature.*

We recall here [20, Algorithm 1], which is a slightly modified version of the standard MatrixF$_5$ algorithm [1] (see also [11, Sec. 3]) permitting the input of precomputed syzygies.

4 THE FIRST SYZYGIES OF MAXIMAL MINORS

First defined in [10], the Eagon-Northcott complex is a complex of free modules associated to a matrix with entries in any commutative ring with unity. We are specifically concerned with the first syzygies of maximal minors of some polynomial matrix. The Eagon-Northcott complex provides access to them.

4.1 The Eagon-Northcott complex

Theorem 4.1 ([10, Thm. 1], [13, Thm. A2.60]). *Let $\mathcal{R}$ be a commutative ring with unity and let A be a $p \times q$ matrix with entries in $\mathcal{R}$, with $p \leq q$. For each $0 \leq i \leq q - p$, let*

$$\mathcal{E}_i = \left(\mathrm{Sym}_i \mathcal{R}^p\right)^* \otimes \bigwedge^{p+i}(\mathcal{R}^q).$$

Then there are graded morphisms $\partial_i : \mathcal{E}_i \to \mathcal{E}_{i-1}$, $1 \leq i \leq q-p$, such that the complex $\mathbf{EN}(A) = (\mathcal{E}_\bullet \xrightarrow{\epsilon} \mathcal{R}/I_p(A), \partial_\bullet)$ is a free resolution if and only if $\operatorname{grade}(I_p(A)) = q - p + 1$.

Algorithm 1 MatrixF$_5(F, D, S)$

Input: A sequence $F = (f_1, \dots, f_t)$ of homogeneous elements of degrees $d_1 \leq \cdots \leq d_t$ in $\Bbbk[x_1, \dots, x_n]^s$; a degree bound D; a set S of syzygies of F.
Output: A $(D, >^{\text{POT}})$-Gröbner basis for $\langle F \rangle$.

for i from 1 to t **do** $G_i \leftarrow \emptyset$
for d from d_1 to D **do**
  $\mathscr{M}_{d,0} \leftarrow \emptyset$; Crit $\leftarrow \text{LM}_>^{\text{POT}}(S)$
  for i from 1 to t **do**
    if $d < d_i$ **then** $\mathscr{M}_{d,i} \leftarrow \mathscr{M}_{d,i-1}$
    else if $d = d_i$ **then** $\mathscr{M}_{d,i} \leftarrow$ concatenate the row f_i to $\widetilde{\mathscr{M}}_{d,i-1}$ with signature e_i
    else
      $\mathscr{M}_{d,i} \leftarrow \widetilde{\mathscr{M}}_{d,i-1}$
      if $s = 1$ **then**
        for $\tau \in \text{LM}_>(\text{rows}(\mathscr{M}_{d-d_i,i-1}))$ **do**
          Crit $\leftarrow$ Crit $\cup \{\tau e_i\}$
      for $f \in \text{rows}(\widetilde{\mathscr{M}}_{d-1,i}) \setminus \text{rows}(\widetilde{\mathscr{M}}_{d-1,i-1})$ **do**
        $\tau e_i \leftarrow$ signature of f
        if $f = 0$ **then**
          for j from 1 to k **do**
            Crit $\leftarrow$ Crit $\cup \{\tau x_j e_i\}$
      for $f \in \text{rows}(\mathscr{M}_{d-1,i}) \setminus \text{rows}(\mathscr{M}_{d-1,i-1})$ **do**
        $\tau e_i \leftarrow$ signature of f
        for $j \in \{\max\{j' : x_{j'} \mid \tau\}, \dots, k\}$ **do**
          if $\tau x_j e_i \notin$ Crit **then** $\mathscr{M}_{d,i} \leftarrow$ concatenate the row $x_j f$ to $\mathscr{M}_{d,i}$ with signature $\tau x_j e_i$
    $\widetilde{\mathscr{M}}_{d,i} \leftarrow$ reduced row echelon form of $\mathscr{M}_{d,i}$ obtained via a sequence of valid elementary row operations
    $G_i \leftarrow G_i \cup \{f \in \text{rows}(\widetilde{\mathscr{M}}_{d,i}) : f \notin \langle \text{LM}_>^{\text{POT}}(G_i) \rangle\}$
return $G_1, \dots, G_t$

We make explicit the first boundary morphism ∂_1, whose image is precisely the first syzygy module of $I_p(A)$. First, by the definition of the free modules $\mathcal{E}_i$, the map ∂_1 is a map

$$\partial_1 : (\mathcal{R}^p)^* \otimes \bigwedge^{p+1}(\mathcal{R}^q) \to \bigwedge^{p}(\mathcal{R}^q).$$

We take as a basis for $(\mathcal{R}^p)^*$ the standard basis functionals e_i for $1 \leq i \leq q$. It follows immediately from Propositions 2.1 and 2.2 that a basis for the $\mathcal{R}$-module $(\mathcal{R}^p)^* \otimes \bigwedge^{p+1}(\mathcal{R}^q)$ is given by

$$\{e_i \otimes (e_{i_1} \wedge \cdots \wedge e_{i_p}) : 1 \leq i \leq p, 1 \leq i_1 < \cdots < i_p \leq q\}.$$

Subsequently, $\partial_1(e_i \otimes (e_{i_1} \wedge \cdots \wedge e_{i_{p+1}}))$ equals

$$\sum_{t=1}^{p+1} (-1)^{t-1} \left(e_{i_t} A^T e_i\right) (e_{i_1} \wedge \cdots \wedge \widehat{e_{i_t}} \wedge \cdots \wedge e_{i_{p+1}}).$$

The map $\epsilon : \bigwedge^p(\mathcal{R}^q) \to \mathcal{R}/I_p(A)$ is given by

$$\epsilon(e_{i_1} \wedge \cdots \wedge e_{i_p}) = \det([1 \cdots p \mid i_1 \cdots i_p]_A).$$

The image of ∂_1 (and thus $\text{Syz}(F_p(A))$ then admits an explicit description. For each $p \times (p+1)$ submatrix A' of A, the determinant of the square matrix formed by duplicating any row of A', computed via Laplace expansion around the duplicated row, is zero.

Example 4.2. Let $p = 2$, $q = 4$, and suppose

$$A = \begin{pmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \end{pmatrix} \in \mathcal{R}^{2\times 4}.$$

We have

$$\partial_1(e_1 \otimes (e_2 \wedge e_3 \wedge e_4)) = f_{12}(e_3 \wedge e_4) - f_{13}(e_2 \wedge e_4) + f_{14}(e_2 \wedge e_3).$$

Note that the fact that $\partial_1(e_1 \otimes (e_2 \wedge e_3 \wedge e_4)) \in \ker \epsilon$ is precisely the statement that the determinant

$$\det \begin{pmatrix} f_{12} & f_{13} & f_{14} \\ f_{12} & f_{13} & f_{14} \\ f_{22} & f_{23} & f_{24} \end{pmatrix}$$

is zero. More explicitly, $\epsilon(\partial_1(e_1 \otimes (e_2 \wedge e_3 \wedge e_4)))$ is simply the determinant of this matrix, computed via Laplace expansion along its first row. Analogously, $\epsilon(\partial_1(e_2 \otimes (e_1 \wedge e_3 \wedge e_4)))$ is simply the determinant of the singular matrix

$$\begin{pmatrix} f_{21} & f_{23} & f_{24} \\ f_{11} & f_{13} & f_{14} \\ f_{21} & f_{23} & f_{24} \end{pmatrix}$$

computed via Laplace expansion along its first row.

4.2 Leading terms of syzygies

We start with a consequence of the description of the first syzygy module provided by the Eagon-Northcott complex.

Proposition 4.3. *Let $A = (a_{i,j})$ be an $p \times q$ matrix with entries in $\Bbbk[x_1, \dots, x_n]$, with $p \leq q$. For each $1 \leq k \leq q - p$, let $\mathcal{J}_k(A)$ be the ideal $\langle a_{i,j} : 1 \leq i \leq p, j \leq k \rangle$ of $\Bbbk[x_1, \dots, x_n]$. Let $\mathscr{H}$ be the set*

$$\bigcup_{k=1}^{q-p} \bigcup_{k+1<i_2<\cdots<i_p\leq q} \left\{\text{LM}_>(g)(e_{k+1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_p}) : g \in \mathcal{J}_k(A)\right\}.$$

Then the module $\langle\langle \mathscr{H} \rangle\rangle$ is a submodule of $\text{LM}_>^{\text{POT}}(\text{Syz}(F_p(A)))$.

Proof. Fix $1 \leq k \leq q - p$. Let $i_2, \dots, i_p \in \mathbb{Z}_{>0}$ be integers such that $k + 1 < i_2 < \cdots < i_p < q$, and let $g \in \mathcal{J}_k(A)$. Then there exist polynomials $h_{i,j} \in \mathcal{R}_n$ such that $g = \sum_{i,j} h_{i,j} a_{i,j}$. Let

$$G = \sum_{i,j} h_{i,j} \partial_1(e_i \otimes (e_j \wedge e_{k+1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_p})).$$

We claim that

$$\text{LM}_>^{\text{POT}}(G) = \text{LM}_>(g)(e_{k+1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_p}).$$

Now taking $\phi = \left((e_{k+1} \wedge \cdots \wedge e_{i_p})\right)^*$, we have

$$\begin{aligned} \phi(G) &= \sum_{i,j} \phi(h_{i,j} \partial_1(e_i \otimes (e_j \wedge e_{k+1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_p}))) \\ &= \sum_{i,j} h_{i,j} \phi(\partial_1(e_i \otimes (e_j \wedge e_{k+1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_p}))) \\ &= \sum_{i,j} h_{i,j} a_{i,j} = g \end{aligned}$$

By the definition of ∂_1, only those basis vectors of $\bigwedge^p(\mathcal{R}_n^q)$ of the form $e_j \wedge \cdots \wedge \widehat{e_{i_t}} \wedge \cdots \wedge e_{i_p}$ appear with nonzero coefficient in G. The largest of these basis vectors with respect to the lexicographic

order is clearly $e_{k+1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_p}$, so our claim is proven. Having constructed an element of $\mathrm{LM}_{\succ}^{\mathrm{POT}}(\mathrm{Syz}(F_p\,(A)))$ whose leading term is precisely $\mathrm{LM}_{\succ}(g)(e_{k+1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_p})$, we are done. □

Remark 4.4. We have seen, in Section 4.1, that the syzygies described by the Eagon-Northcott complex between the maximal minors of a $p \times q$ matrix A over $\mathcal{R}_n$ are given by choosing a $p \times (p+1)$ submatrix A' of A, duplicating any row of A', and computing the determinant of this matrix by Laplace expansion over the duplicated row (see Example 4.2 for an example). The $\succ^{\mathrm{POT}}$-leading term of such a syzygy is simply the leading term of the leftmost entry of the duplicated row.

Upon fixing a maximal minor of A, the leading monomials of a $\succ$-Gröbner basis of the polynomial system formed by the set of columns to the left of the leftmost column of this minor are leading monomials of syzygies amongst the maximal minors of A.

Proposition 4.3 leads directly to the following algorithm.

Algorithm 2 MaxDetMatrixF$_5(A, D)$

Input: A matrix $A = (a_{i,j}) \in \Bbbk[x_1, \ldots, x_n]^{p \times q}$ of homogeneous polynomials, with $p \leq q$ and an integer D.
Output: A $(D, \succ)$-Gröbner basis of $I_p\,(A)$.

1: $C \leftarrow \{a_{1,1}, \ldots, a_{p,1}, \ldots, a_{1,q-p}, \ldots, a_{p,q-p}\}$
2: $G_1, \ldots, G_{p(q-p)} \leftarrow \mathrm{MatrixF}_5(C, \emptyset, D - \min_{f \in F_p(A)}\{\deg(f)\})$
3: $H \leftarrow \emptyset$
4: **for** $i \in \{1, \ldots, p(q-p)\}$ **do**
5: **for** $f \in F_p\left(\left[1 \cdots p+1 \mid \left(\left\lfloor \frac{i}{p} \right\rfloor + 1\right) \cdots q\right]_A\right)$ **do**
6: $j \leftarrow$ index of f in $F_p\,(A)$
7: $H \leftarrow H \cup \{\mathrm{LM}_{\succ}(g)e_j : g \in G_i\}$
8: **return** $\mathrm{MatrixF}_5(F_p\,(A), H, D)$

Theorem 4.5. *Algorithm* MaxDetMatrixF$_5$ *is correct.*

Proof. This follows from the correctness of MatrixF$_5$ [1, Thm. 9], and from Proposition 4.3 which establishes that the set H input to MatrixF$_5$ on Line 8 is a subset of $\mathrm{LM}_{\succ}^{\mathrm{POT}}(\mathrm{Syz}(F_p\,(A)))$. □

5 CRITICAL POINTS

Recall that for a set of homogeneous polynomials $F = (f_1, \ldots, f_p) \subseteq \mathcal{R}_n$, and a homogeneous polynomial $g \in \mathcal{R}_n$, our goal is to compute a Gröbner basis for $\mathcal{I}(g, F) = I_p\,(\mathrm{jac}(g, F)) + \langle F \rangle$. Note that if g and the f_i's are affine, by [9, Ch. 8, Sec. 4, Thm. 4], one can simply homogenize them with respect to a variable h which is smaller than all of the x_i, apply the algorithms in this paper, then set $h = 1$.

Via a minor modification of Algorithm 2, we obtain an algorithm which computes a Gröbner basis for the ideal $\mathcal{I}(g, F)$.

Proposition 5.1. *Algorithm* CritGB *is correct.*

Proof. The only modification made to Algorithm 2 to obtain Algorithm 3 is to add the set F to the polynomial system upon which we run MatrixF$_5$. Thus, the correctness follows immediately from that of Algorithm 2, proven in Theorem 4.5. □

For a system of homogeneous polynomials $F = (f_1, \ldots, f_p) \subseteq \mathcal{R}_n$ and a polynomial $g \in \mathcal{R}_n$, there may exist, a priori, nontrivial

Algorithm 3 CritGB(F, g, D)

Input: A system of homogeneous polynomials $F = (f_1, \ldots, f_p) \subseteq \mathcal{R}_n$, a homogeneous polynomial $g \in \mathcal{R}_n$, and an integer D.
Output: A $(D, \succ)$-Gröbner basis of $\mathcal{I}(g, F)$.

1: $J \leftarrow \mathrm{jac}(g, F)$
2: $C \leftarrow \{J_{1,1}, \ldots, J_{p+1,1}, \ldots, J_{1,n-p-1}, \ldots, J_{p,n-p-1}\}$
3: $G_1, \ldots, G_{(p+1)(n-p-1)} \leftarrow \mathrm{MatrixF}_5\left(C, D - \min\left\{\deg\left(\frac{\partial f_i}{\partial x_j}\right)\right\}\right)$
4: $H \leftarrow \emptyset$
5: **for** $i \in \{1, \ldots, (p+1)(n-p-1)\}$ **do**
6: **for** $f \in F_{p+1}\left(\left[1 \cdots p+1 \mid \left(\left\lfloor \frac{i}{p+1} \right\rfloor + 1\right) \cdots n\right]_J\right)$ **do**
7: $j \leftarrow$ index of f in $F_{p+1}\,(J)$
8: $H \leftarrow H \cup \{\mathrm{LM}_{\succ}(g)e_j : g \in G_i\}$
9: **return** $\mathrm{MatrixF}_5(F \cup F_{p+1}\,(J), H, D)$

syzygies between the polynomials in F and the maximal minors of $\mathrm{jac}(g, F)$. Generically, this does not occur.

Proposition 5.2. *Let $n, p, d_0 \in \mathbb{Z}_{>0}$. There exists a nonempty Zariski open subset $U \subseteq \mathbb{A}^{(p+1)\binom{n+d_0-1}{n-1}}$ such that for all $c \in U$, taking $(g, f_1, \ldots, f_p) = \phi_c(\mathfrak{f}_{(n,(d_0,\ldots,d_0))})$,*

$$\mathrm{Syz}(F \cup F_{p+1}\,(\mathrm{jac}(g, F))) = \mathrm{Syz}(F) \oplus \mathrm{Syz}(F_p\,(\mathrm{jac}(g, F)))$$

where $F = (f_1, \ldots, f_p)$.

Proof. By [33, Lem. 2.2], there exists a nonempty Zariski open subset $U \subseteq \mathbb{A}^{(p+1)\binom{n+d_0-1}{n-1}}$ such that for all $c \in U$, taking

$$(g, f_1, \ldots, f_p) = \phi_c(\mathfrak{f}_{(n,(d_0,\ldots,d_0))}).$$

and $F = (f_1, \ldots, f_p)$, the sequence $(f_1, \ldots, f_p)$ is a $\mathcal{R}_n/I_p\,(\mathrm{jac}(g, F))$-regular sequence. Since for such c, F is also a regular sequence in $\mathcal{R}_n$, the two $\mathcal{R}_n$-modules $\mathcal{R}_n/I_p\,(\mathrm{jac}(g, F))$ and $\mathcal{R}_n/\langle F \rangle$ are Tor-independent. That is, for all $i \geq 1$,

$$\mathrm{Tor}_i^{\mathcal{R}_n}(\mathcal{R}_n/I_p\,(\mathrm{jac}(F)), \mathcal{R}_n/\langle F \rangle) = 0.$$

It follows that $\mathbf{EN}(\mathrm{jac}(F)) \otimes_{\mathcal{R}_n} \mathcal{K}(F)$ is a free resolution of the tensor product $\mathcal{R}_n/\langle F \rangle \otimes_{\mathcal{R}_n} \mathcal{R}_n/I_p\,(\mathrm{jac}(F)) \cong \mathcal{R}_n/\big(\langle F \rangle + I_p\,(\mathrm{jac}(F))\big)$. □

6 COMPLEXITY ANALYSIS

The complexity of linear-algebra based Gröbner basis algorithms is governed by the cost of echelonizing Macaulay matrices. The work that we have done thus far allows us to estimate these costs, since the sizes and ranks of the Macaulay matrices computed can be deduced from the Eagon-Northcott complex.

6.1 New complexity bound

Recall that given a polynomial system $F \subseteq \mathcal{R}_n$, the columns of $\mathscr{M}_d(F)$, are indexed by the monomials of degree d in $\mathcal{R}_n$. We are left to compute the rank of $\mathscr{M}_d(F)$ and the number of rows of $\mathscr{M}_d(F)$ taken into account by our algorithm. We first count the number of syzygies from Proposition 4.3.

Proposition 6.1. *Let $A = (a_{i,j})$ be a $p \times q$ matrix with entries homogeneous polynomials of degree d_0 in $\mathcal{R}_n$, with $q \geq p$. For each $1 \leq k \leq q - p$, let $\mathcal{J}_k(A) := \langle a_{i,j} : 1 \leq i \leq p, 1 \leq j \leq k \rangle \subseteq \mathcal{R}_n$.*

Then for any $D \in \mathbb{Z}_{>0}$ and any $d \in \{d_0 p, \dots, D\}$, the number of elements of degree $d - pd_0$ of the set H computed in Algorithm 2 is

$$\sum_{k=1}^{q-p} \mathrm{HF}_{\mathcal{J}_k(A)}(d - pd_0)\binom{q-k-1}{p-1}$$

Proof. Let $H_{d-pd_0} \subseteq H$ be the subset of the set H in Line 8 of Algorithm 2 consisting of elements of degree $d - pd_0$. This set H is precisely the set $\mathscr{H}$ defined in the statement of Proposition 4.3. We can therefore write

$$\begin{aligned}\#H_{d-pd_0} &= \sum_{k=1}^{q-p} \sum_{k+1<i_2<\cdots<i_p\le q} \Big\{\mathrm{LM}_>(g)(e_{k+1}\wedge e_{i_2}\wedge\cdots\wedge e_{i_p}) : \\ &\qquad\qquad g \in \mathcal{J}_k(A), \deg(g) = d - pd_0\Big\} \\ &= \sum_{k=1}^{q-p} \sum_{k+1<i_2<\cdots<i_p\le q} \mathrm{HF}_{\mathcal{J}_k(A)}(d - pd_0).\end{aligned}$$

The last equality follows from the fact that the number of monomials of of $\mathrm{LM}_>(\mathcal{J}_k(A))$ of degree $d - pd_0$ is $\mathrm{HF}_{\mathcal{J}_k(A)}(d - pd_0)$. The result follows from the fact that for $1 \le k \le q - p$, there are $\binom{q-k-1}{p-1}$ sequences of the form $k + 1 < i_2 < \cdots < i_p \le q$. □

Using Proposition 6.1, we are left to compute the Hilbert functions of the ideals $\mathcal{J}_k(A)$ of flattened columns, of course under certain genericity assumptions. To do this, we rely on Fröberg's conjecture [19, Sec. 1], which we reformulate below.

In what follows, for polynomials $P(t), Q(t) \in \mathbb{Z}[t]$, we denote by $\left[\frac{P(t)}{Q(t)}\right]_+$ the power series expansion of $\frac{P(t)}{Q(t)}$, truncated at its first non-positive coefficient.

Conjecture 6.2 ([19, Sec. 1],[30, Conj. 1]). *Consider $(f_1, \dots, f_m)$ be a sequence of homogeneous polynomials in $\mathcal{R}_n$, whose coefficients are algebraically independent. For each $1 \le i \le m$, let $d_i = \deg(f_i)$. Then*

$$H_{\mathcal{R}_n/\langle f_1,\dots,f_m\rangle}(t) = \left[\frac{\prod_{i=1}^m (1 - t^{d_i})}{(1-t)^n}\right]_+.$$

Proposition 6.3. *Let $m, n \in \mathbb{Z}_{>0}$ and let $F = (f_1, \dots, f_m) \subseteq \Bbbk[x_1, \dots, x_n]$ be a sequence of homogeneous polynomials, all of degree d_0. Let D be the Hilbert regularity of $\langle F\rangle$. If F is a semi-regular sequence, and Conjecture 6.2 is true, then for any $d \ge 0$,*

$$\mathrm{HF}_{\mathcal{R}_n/\langle f_1,\dots,f_m\rangle}(d) = \begin{cases} \sum_{j=0}^{\left\lfloor \frac{n+d-1}{d_0}\right\rfloor} (-1)^j \binom{n+d-d_0 j-1}{n-1}\binom{m}{j} & \text{if } d < D \\ 0 & \text{if } d \ge D \end{cases}.$$

Proof. By Conjecture 6.2, the Hilbert series of $\mathcal{R}_n/\langle F\rangle$ is

$$H_{\mathcal{R}_n/\langle f_1,\dots,f_m\rangle}(t) = \left[\frac{(1-t^{d_0})^m}{(1-t)^n}\right]_+.$$

The numerator $(1 - t^{d_0})^m$ can be expanded as $\sum_{j=0}^m (-1)^j \binom{m}{j} t^{jd_0}$ while the reciprocal of the denominator has the classical expansion

$$\frac{1}{(1-t)^n} = \sum_{j\ge 0} \binom{n+j-1}{n-1} t^j.$$

The result follows by taking the product of these expansions. □

Proposition 6.4. *Let $n \in \mathbb{Z}_{>0}$. For any $p \le n$ and any $d_0 \in \mathbb{Z}_{>0}$, there exists a Zariski open set $U \subseteq \mathbb{A}^{(p+1)\binom{n+d_0-1}{n-1}}$ such that for all $c \in U$, taking $(g, f_1, \dots, f_p) = \phi_c(\mathfrak{f}_{(n,d_0,\dots,d_0)})$, the sequence*

$$\left(\frac{\partial g}{\partial x_1}, \frac{\partial f_1}{\partial x_1}, \dots, \frac{\partial f_p}{\partial x_1}, \dots, \frac{\partial g}{\partial x_{n-p-1}}, \frac{\partial f_1}{\partial x_{n-p-1}}, \dots, \frac{\partial f_p}{\partial x_{n-p-1}}\right)$$

formed by the leftmost $n - p - 1$ columns of $\mathrm{jac}(g, f_1, \dots, f_p)$ is semi-regular.

Proof. Let $\mathfrak{c}^{(1)}, \dots, \mathfrak{c}^{(p+1)}$ be sets of indeterminates, with $\mathfrak{c}^{(i)} = \{\mathfrak{c}_\tau^{(i)} : \tau \in \mathrm{Mon}_{d_0}(\mathcal{R}_n)$. For any $1 \le i \le p + 1$ and for $1 \le j \le n - p - 1$, the coefficients of the partial derivative $\frac{\partial \mathfrak{f}^{\mathfrak{c}^{(i)}}_{(n,d_0)}}{\partial x_j}$ are polynomials in the indeterminate coefficients $\mathfrak{c}^{(i)}$.

For any $d \ge d_0$, (upon fixing bases for the domain and codomain), the multiplication map by $\frac{\partial \mathfrak{f}^{\mathfrak{c}^{(i)}}_{(n,d_0)}}{\partial x_j}$

$$\left(\frac{\mathcal{R}_n}{\left\langle \frac{\partial \mathfrak{f}^{\mathfrak{c}^{(1)}}_{(n,d_0)}}{\partial x_1}, \dots, \frac{\partial \mathfrak{f}^{\mathfrak{c}^{(i-1)}}_{(n,d_0)}}{\partial x_{j-1}}\right\rangle}\right)_{d-d_0} \to \left(\frac{\mathcal{R}_n}{\left\langle \frac{\partial \mathfrak{f}^{\mathfrak{c}^{(1)}}_{(n,d_0)}}{\partial x_1}, \dots, \frac{\partial \mathfrak{f}^{\mathfrak{c}^{(i-1)}}_{(n,d_0)}}{\partial x_{j-1}}\right\rangle}\right)_d$$

is represented by a matrix whose entries are rational functions in the indeterminate coefficients $\mathfrak{c}^{(i)}$.

The points $c \in \mathbb{A}^{(p+1)\binom{n+d_0-1}{n-1}}$ such that this map is full-rank form a Zariski open subset. By intersecting all such subsets for all $1 \le i \le p+1$ and $1 \le j \le n-p-1$, we obtain the set U we seek. □

Corollary 6.5. *Let $n \in \mathbb{Z}_{>0}$ and assume Conjecture 6.2 is true. For any $p \le n$ and any $d_0 \in \mathbb{Z}_{>0}$, there exists a Zariski open set $U \subseteq \mathbb{A}^{(p+1)\binom{n+d_0-1}{n-1}}$ such that for all $c \in U$, taking $(g, f_1, \dots, f_p) = \phi_c(\mathfrak{f}_{(n,d_0,\dots,d_0)})$, for any $1 \le k \le n - p - 1$, $\mathrm{HF}_{\mathcal{J}_k(\mathrm{jac}(g,F))}(d)$ is*

$$\begin{cases} \binom{n+d-1}{n-1} - \sum_{j=0}^{\left\lfloor \frac{n+d-1}{d_0}\right\rfloor} (-1)^j \binom{n+d-d_0 j-1}{n-1}\binom{(p+1)k}{j} & \text{if } d < D \\ \binom{n+d-1}{n-1} & \text{if } d \ge D \end{cases}$$

where $\mathcal{J}_k(\mathrm{jac}(g, F))$ is the ideal generated by the first k columns of $\mathrm{jac}(g, F)$, and D is its Hilbert regularity.

Proof. Let U be the set defined in Proposition 6.4 and take any $c \in U$. Then for any $1 \le k \le n - p - 1$, the set of generators for $\mathcal{J}_k(\mathrm{jac}(g, F))$ given by the first k columns of $\mathrm{jac}(g, F)$ forms a semi-regular sequence. We can therefore apply Proposition 6.3 to obtain the Hilbert function of $\mathcal{R}_n/\mathcal{J}_k(\mathrm{jac}(g, F))$. Since the Hilbert function of $\mathcal{R}_n$ itself is $\mathrm{HF}_{\mathcal{R}_n}(d) = \binom{n+d-1}{n-1}$, the result follows. □

Conjecture 6.6. *The set U defined in Proposition 6.3 is nonempty.*

Remark 6.7. Such a conjecture is a variation of Fröberg's.

Finally, we compute the ranks of the Macaulay matrices associated to the maximal minors of a polynomial matrix from the Eagon-Northcott complex.

Proposition 6.8. *Let A be a $p \times q$ matrix with entries homogeneous polynomials of degree d_0 in $\Bbbk[x_1, \dots, x_n]$, with $q \ge p$. If $\mathrm{grade}(I_p(A)) = q - p + 1$, then*

$$\mathrm{HF}_{I_p(A)}(d) = \sum_{j=0}^{q-p} (-1)^j \binom{n + d - (p + j)d_0 - 1}{n-1}\binom{p+j-1}{p-1}\binom{q}{p+j}.$$

Proof. Since $\operatorname{grade}(I_p(A)) = q - p + 1$, by Theorem 4.1, the Eagon-Northcott complex is a free resolution of $I_p(A)$. In order to turn the Eagon-Northcott complex into a graded resolution, we need to shift the grading on the component free modules to ensure that the boundary homomorphisms are graded.

First, the degree of the maximal minors of A is pd_0. As such, in order to make the augmentation homomorphism ϵ of $\mathbf{EN}(A)$ graded, we need only replace $\mathcal{E}_0$ by $\mathcal{E}_0(-pd_0)$.

Now, by the description of the boundary homomorphisms in [13, A2H] (see also [13, Exa. A2.69]), each boundary homomorphism (except for the augmentation homomorphism) can be represented by a matrix with entries linear in the entries of A. Thus, in order to make these boundary homomorphisms graded, we need to replace $\mathcal{E}_j$ by $\mathcal{E}_j(-pd_0 - id_0)$ for each $1 \le j \le q - p$.

Finally, we have $\operatorname{rank}(\mathcal{E}_0(-pd_0)) = \binom{q}{p}$ and

$$\begin{aligned}\operatorname{rank}(\mathcal{E}_j(-d_0(p+j))) &= \operatorname{rank}\left(\left(\operatorname{Sym}_j(\mathcal{R}^p)\right)^* \otimes \bigwedge^{p+j}(\mathcal{R}^q)\right)\\ &= \binom{p+j-1}{p-1}\binom{q}{p+j}.\end{aligned}$$

The result then follows from Corollary 2.5. □

Proposition 6.9. *Let $F = (f_1, \ldots, f_p) \subseteq \Bbbk[x_1, \ldots, x_n]$ be a regular sequence of homogeneous polynomials, all of degree d_0, and let $g \in \Bbbk[x_1, \ldots, x_n]$ be a homogeneous polynomial of degree d_0. Then the Hilbert function of the ideal $\mathcal{I}(g, F) = \langle F\rangle + I_{p+1}(\operatorname{jac}(g, F))$ is given by $\operatorname{HF}_{\mathcal{R}_n/\mathcal{I}(g,F)}(d)$ which is*

$$\begin{aligned}&\sum_{i=0}^{p}(-1)^i\binom{p}{i}\left(\binom{n+d-id_0-1}{n-1}-\right.\\ &\left.\sum_{j=0}^{n-p-1}(-1)^j\binom{n+d-(p+j+i+1)d_0-1}{n-1}\binom{p+j}{p}\binom{n}{p+j+1}\right)\end{aligned}$$

Proof. By [33, Lem. 2.2], the sequence F is a $\mathcal{R}_n/I_{p+1}(\operatorname{jac}(g, F))$-regular sequence. It follows (see e.g. [12, Exe. 10.13(a)]) that

$$H_{\mathcal{R}_n/\mathcal{I}(g,F)}(t) = H_{\mathcal{R}_n/I_{p+1}(\operatorname{jac}(g,F))}(t)(1 - t^{d_0})^p. \tag{1}$$

By Proposition 6.8, $\operatorname{HF}_{I_{p+1}(\operatorname{jac}(g,F))}(d)$ equals

$$\sum_{j=0}^{n-p-1}(-1)^j\binom{n+d-(p+j+1)d_0-1}{n-1}\binom{p+j}{p}\binom{n}{p+j+1}. \tag{2}$$

Since the Hilbert series $H_{\mathcal{R}_n/I_{p+1}(\operatorname{jac}(g,F))}(t)$ is the generating series of the difference between the Hilbert function of $\mathcal{R}_n$ (which is simply $\operatorname{HF}_{\mathcal{R}_n}(d) = \binom{n+d-1}{n-1}$) and this Hilbert function, the result follows by combining Eq. (2) with Eq. (1) and expanding. □

We use the Hilbert functions to estimate the cost of echelonizing each of the Macaulay matrices encountered in Algorithm 3.

Theorem 6.10. *Let $F = (f_1, \ldots, f_p) \subseteq \Bbbk[x_1, \ldots, x_n]$ be a regular sequence of homogeneous polynomials, all of degree d_0, and let $g \in \Bbbk[x_1, \ldots, x_n]$ be a homogeneous polynomial of degree d_0. Finally, for each $1 \le k \le n - p - 1$, let $\mathcal{J}_k(\operatorname{jac}(g, F))$ be the ideal of $\mathcal{R}_n$ generated by the first k columns of $\operatorname{jac}(g, F)$. Then assuming that Conjecture 6.2 and Conjecture 6.6 are true, the number of arithmetic operations in $\Bbbk$ required to compute a grevlex Gröbner basis for the ideal $\mathcal{I}(g, F) = \langle F\rangle + I_{p+1}(\operatorname{jac}(g, F))$ is in*

$$O\left(\sum_{d=d_0}^{D}\left(\binom{n+d-1}{n-1} - \operatorname{HF}_{\mathcal{R}_n/\mathcal{I}(g,F)}(d)\right)^{\omega-2}\mathcal{R}(d)\binom{n+d-1}{n-1}\right)$$

with

$$\begin{aligned}\mathcal{R}(d) = p&\binom{n+d-d_0-1}{n-1} + \binom{n+d-(p+1)d_0-1}{n-1}\binom{n}{p+1}\\ &-\left(\sum_{k=1}^{n-p-1}\operatorname{HF}_{\mathcal{J}_k(\operatorname{jac}(g,F))}(d-(p+1)d_0)\binom{n-k-1}{p}\right)\end{aligned}$$

where the Hilbert function $\operatorname{HF}_{\Bbbk[x_1,\ldots,x_n]/\mathcal{I}(g,F)}(d)$ is given in Proposition 6.9, the Hilbert functions $\operatorname{HF}_{\mathcal{J}_k(\operatorname{jac}(g,F))}(d)$ are those given in Corollary 6.5, $D = (n+p)d_0 + 1$, and $2 \le \omega \le 3$ is a suitable exponent of matrix multiplication.

Proof. By [33, Cor. 2.3], the largest degree of an element of the reduced grevlex Gröbner basis of $\mathcal{I}(g, F)$ is $D = (n + p)d_0 + 1$. Therefore, the output of $\operatorname{CritGB}(F, g, D)$ (see Algorithm 3) is a grevlex Gröbner basis of $\mathcal{I}(g, F)$.

The arithmetic complexity of Algorithm 3 is clearly bounded by that of its final step. $\operatorname{MatrixF}_5$ only performs arithmetic operations when computing row-echelon forms for the Macaulay matrices it builds. We can therefore bound the number of arithmetic operations performed by $\operatorname{MatrixF}_5$ on any given input by the cost of echelonizing the Macaulay matrices it encounters. For a given $d_0 \le d \le D$, the Macaulay matrix $\mathscr{M}_d(\mathcal{I}(g, F))$ is of rank $\operatorname{HF}_{\mathcal{I}(g,F)}(d)$and has $\#\operatorname{Mon}_d(\mathcal{R}_n) = \binom{n+d-1}{n-1}$. The rows of $\mathscr{M}_d(\mathcal{I}(g, F))$ are indexed by a subset of

$$\left(\operatorname{Mon}_{d-d_0}\left(\mathcal{R}_n^{\#F}\right) \cup \operatorname{Mon}_{d-(p+1)d_0}\left(\mathcal{R}_n^{\#F_{p+1}(\operatorname{jac}(g,F))}\right)\right) \setminus H_{d-pd_0},$$

which has cardinality precisely $\mathcal{R}(d)$ by Proposition 6.1. By [34, Sec. 2.2], an $s \times t$ matrix of rank r over $\Bbbk$ can be echelonized using $O(r^{\omega-2}st)$ operations, so the result follows. □

6.2 Comparison with Lazard's algorithm

We conclude with a comparison of the upper bound

$$\sum_{d=pd_0}^{d_0(p-1)+(d_0-1)n+1}\mathcal{R}(d)$$

from Theorem 6.10 on the total number of rows in all of the Macaulay matrices built by Algorithm 2 to the upper bound

$$\binom{q}{p}\binom{d_0(p-1)+(d_0-1)n+1+n}{n}.$$

on the number of rows in the Macaulay matrices built by Lazard's algorithm obtained in [18, Theorem 20].

This comparison does not take into account the fact that in Algorithm 1, Macaulay matrices are computed degree-by-degree, so that reductions to zero in lower degrees can be used to eliminate reductions to zero in subsequent degrees.

This comparison also does not take into account the F_5 criterion [15, Thm. 1], which allows for several more reductions to zero to be avoided. However, the complexity of F_5 has only been analyzed in the case of a regular sequence, in [1].

Remark 6.11. By computing a $>^{\mathrm{POT}}$-Gröbner basis for $\mathrm{Syz}(F_p(A))$, we can estimate the number of extra reductions to zero avoided by Algorithm 2 thanks to Proposition 3.2 (ii). For $p = 3, q = 6, n = 4, d_0 = 3$, the ratio of the number of rows estimated by taking into account this criterion to the number of rows computed by Lazard's algorithm is 29.397, while not taking into account this criterion yields a ratio of 26.786. Similarly, for $p = 3, q = 7, n = 5, d_0 = 3$, taking into account this criterion gives a ratio of 41.006, while not taking into account this criterion gives a ratio of 34.946. This suggests that a careful complexity analysis of Algorithm 3 might provide a theoretical complexity improvement that is better than the one suggested by the graphs we give here.

6.2.1 p, n fixed, d_0 grows. First, we fix the number of polynomials p and the number of variables n, and allow the degree d_0 to grow. We take $q = n+p-1$, so that the ideal of maximal minors has dimension zero. Figure 1 shows that for a fixed p and n, the theoretical gain

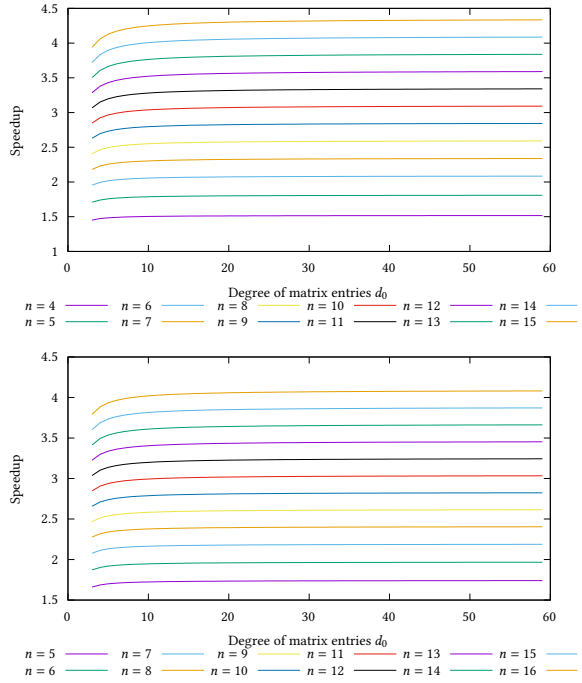

Figure 1: Speedup of Algorithm 2. Top: $p = 3$; bottom: $p = 4$

which we obtain appears to grow logarithmically in d_0.

Finally, we compare Lazard's algorithm to a (nonexistent) algorithm which would compute full-rank Macaulay matrices. **??** shows that such an algorithm appears to also only provide a theoretical gain which grows logarithmically in d_0.

6.2.2 p, d_0 fixed, n grows. Next, we fix the number of polynomials p and the degree d_0 and allow the number of variables n to grow. Again, we take $q = n + p - 1$ so that the ideal of maximal minors has dimension zero. Figure 3 shows that for a fixed p and d_0, the theoretical gain which we obtain appears to grow linearly in n.

We conclude by again comparing Lazard's algorithm to a (nonexistent) algorithm which would compute full-rank Macaulay matrices. Figure 4 shows that such an algorithm appears to provide a

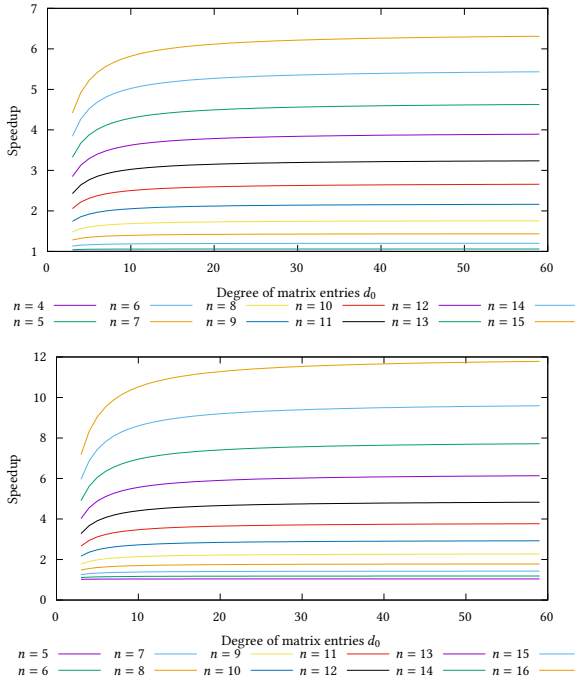

Figure 2: Speedup of an algorithm which computes full-rank Macaulay matrices. Top: $p = 3$; bottom: $p = 4$.

theoretical gain which grows exponentially in n, demonstrating that there is still potentially much to be gained by devising new criteria which predict more reductions to zero.

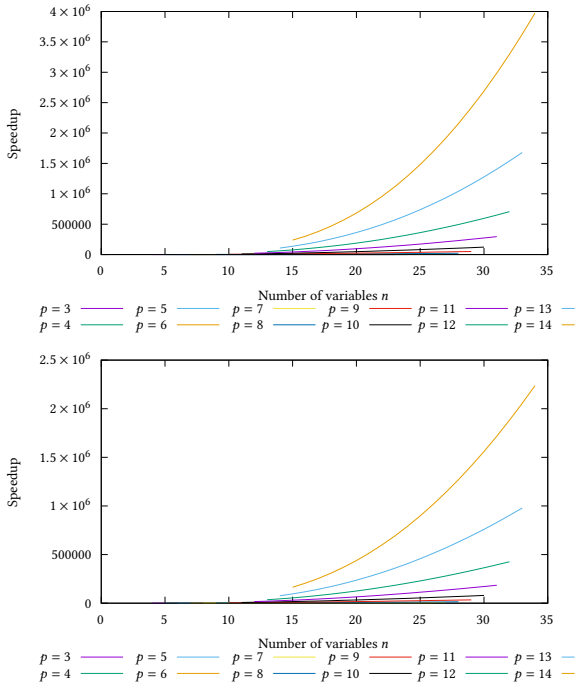

Figure 3: Speedup of Algorithm 2. Top: $d_0 = 3$; bottom: $d_0 = 4$.

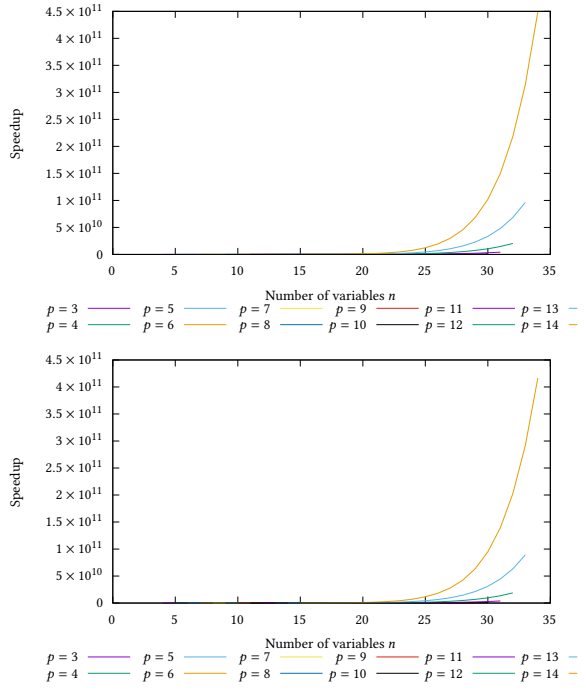

Figure 4: Speedup of an algorithm which computes full-rank Macaulay matrices. Top: $d_0 = 3$; bottom: $d_0 = 4$.

REFERENCES

[1] M. Bardet, J.-C. Faugère, and B. Salvy. 2015. On the complexity of the F5 Gröbner basis algorithm. *J. Symb. Comput.* 70 (2015), 49–70.

[2] J. Berthomieu, V. Neiger, and M. Safey El Din. 2022. Faster change of order algorithm for Gröbner bases under shape and stability assumptions. In *Proceedings of ISSAC'2022.*

[3] W. Bruns and U. Vetter. 1988. *Determinantal Rings.* Springer.

[4] B. Buchberger. 1965. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* Ph. D. Dissertation. University of Innsbruck.

[5] J. Capco, M. Safey El Din, and J. Schicho. 2020. Robots, computer algebra and eight connected components. In *Proceedings of ISSAC'20.* pp. 62–69.

[6] J. Capco, M. Safey El Din, and J. Schicho. 2023. Positive dimensional parametric polynomial systems, connectivity queries and applications in robotics. *J. Symb. Comput.* 115 (2023), 320–345.

[7] D. Chablat, R. Prébet, M. Safey El Din, D. Salunkhe, and P. Wenger. 2022. Deciding Cuspidality of Manipulators through Computer Algebra and Algorithms in Real Algebraic Geometry. In *Proceedings of ISSAC 2022.*

[8] D. A. Cox, J. Little, and D. O'Shea. 2005. *Using Algebraic Geometry.* Springer.

[9] D. A. Cox, J. Little, and D. O'Shea. 2015. *Ideals, Varieties, and Algorithms.* Springer.

[10] J. A. Eagon and D. G. Northcott. 1962. Ideals Defined by Matrices and a Certain Complex Associated with Them. *Proc. of the Royal Society of London* 269, 1337 (1962), 188–204.

[11] C. Eder and J.-C. Faugère. 2016. A survey on signature-based algorithms for computing Gröbner basis computations. *J. Symb. Comput.* (2016), 1–75.

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

[13] D. Eisenbud. 2005. *The geometry of syzygies: A second course in commutative algebra and algebraic geometry.* Vol. 229. Springer.

[14] J.-C. Faugère. 1999. A New Efficient Algorithm for Computing Gröbner bases (F4). *J. Pure Appl. Algebra* 139, 1 (1999), 61–88.

[15] J.-C. Faugère. 2002. A New Efficient Algorithm for Computing Gröbner Bases without Reduction to Zero (F5). In *Proceedings ISSAC 2002.* ACM, 75–83.

[16] J.-C. Faugère and C. Mou. 2017. Sparse FGLM algorithms. *J. Symb. Comput.* 80, 3 (2017), 538–569. https://doi.org/10/gfz47c

[17] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. 2012. Critical points and Gröbner bases: the unmixed case. In *Proceedings of ISSAC'12.* 162–169.

[18] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. 2013. On the complexity of the generalized MinRank problem. *J. Symb. Comput.* 55 (2013), 30–58.

[19] R. Fröberg. 1985. An inequality for Hilbert series of graded algebras. *Mathematica Sandinavica* 56 (Dec. 1985), 117–144.

[20] S. Gopalakrishnan, V. Neiger, and M. Safey El Din. 2023. Refined F5 Algorithms for Ideals of Minors of Square Matrices. In *Proceedings of ISSAC' 2023.* 270–279.

[21] A. Greuet and M. Safey El Din. 2011. Deciding reachability of the infimum of a multivariate polynomial. In *Proceedings of ISSAC'11.* 131–138.

[22] A. Greuet and M. Safey El Din. 2014. Probabilistic Algorithm for Polynomial Optimization over a Real Algebraic Set. *SIAM J. on Optimization* 24, 3 (2014), 1313–1343.

[23] J. D. Hauenstein, M. Safey El Din, É. Schost, and T. X. Vu. 2021. Solving determinantal systems using homotopy techniques. *J. Symb. Comput.* 104 (2021), 754–804.

[24] N. Kaihnsa, Y. Ren, M. Safey El Din, and J. Martini. 2020. Cooperativity, absolute interaction, and algebraic optimization. *Journal of Mathematical Biology* (2020).

[25] G. Labahn, M. Safey El Din, É. Schost, and T. X. Vu. 2021. Homotopy techniques for solving sparse column support determinantal polynomial systems. *J. Complexity* 66 (2021), 101557.

[26] S. Lang. 2002. *Algebra.* Springer, New York, NY.

[27] D. Lazard. 1983. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In *Proceedings EUROSAM 83.* Springer, 146–156.

[28] H. P. Le and M. Safey El Din. 2021. Faster one block quantifier elimination for regular polynomial systems of equations. In *Proceedings ISSAC 2021.* 265–272.

[29] H. P. Le and M. Safey El Din. 2022. Solving parametric systems of polynomial equations over the reals through Hermite matrices. *J. Symb. Comput.* 112 (2022), 25–61.

[30] L. Nicklasson. 2017. On the Hilbert series of ideals generated by generic forms. *Communications in Algebra* 45, 8 (2017), 3390–3395.

[31] M. Safey El Din and É. Schost. 2003. Polar varieties and computation of one point in each connected component of a smooth real algebraic set. In *Proceedings ISSAC 2003.* ACM, 224–231.

[32] M. Safey El Din and É. Schost. 2017. A Nearly Optimal Algorithm for Deciding Connectivity Queries in Smooth and Bounded Real Algebraic Sets. *J. ACM* 63, 6 (2017).

[33] P.-J. Spaenlehauer. 2014. On the Complexity of Computing Critical Points with Gröbner Bases. *SIAM J. Optim.* 24, 3 (2014), 1382–1401.

[34] A. Storjohann. 2000. *Algorithms for Matrix Canonical Forms.* Ph. D. Dissertation. Swiss Federal Institute of Technology – ETH.

[35] P. Trutman, M. Safey El Din, D. Henrion, and T. Pajdla. 2022. Globally Optimal Solution to Inverse Kinematics of 7DOF Serial Manipulator. *IEEE Robotics and Automation Letters* 7, 3 (July 2022), 6012 – 6019.

[36] A. Yabo, M. Safey El Din, J.-B. Caillau, and J.-L. Gouzé. 2023. Stability analysis of a bacterial growth model through computer algebra. *MathematicS In Action* 12, 1 (2023), 175–189.