Refined F5 Algorithms for Ideals of Minors of Square Matrices

Sriram Gopalakrishnan, Vincent Neiger, Mohab Safey El Din

REFINED F_5 ALGORITHMS FOR IDEALS OF MINORS OF SQUARE MATRICES

SRIRAM GOPALAKRISHNAN, VINCENT NEIGER, AND MOHAB SAFEY EL DIN

Abstract. We consider the problem of computing a grevlex Gröbner basis for the set $F_r(M)$ of minors of size r of an $n \times n$ matrix M of generic linear forms over a field of characteristic zero or large enough. Such sets are not regular sequences; in fact, the ideal $\langle F_r(M)\rangle$ cannot be generated by a regular sequence. As such, when using the general-purpose algorithm F_5 to find the sought Gröbner basis, some computing time is wasted on reductions to zero. We use known results about the first syzygy module of $F_r(M)$ to refine the F_5 algorithm in order to detect more reductions to zero. In practice, our approach avoids a significant number of reductions to zero. In particular, in the case $r = n - 2$, we prove that our new algorithm avoids all reductions to zero, and we provide a corresponding complexity analysis which improves upon the previously known estimates.

1. Introduction

Motivation and problem. Let M be an $n \times n$ matrix with entries in the polynomial ring $\mathcal{R} = \Bbbk[x_1, \ldots, x_k]$ where $\Bbbk$ is a field. For $r < n$, we let $\mathcal{I}_r(M)$ be the determinantal ideal generated by the sequence $F_r(M)$ of all minors of M of size $r + 1$. We consider the problem of computing the common roots in $\bar{\Bbbk}^k$ to $F_r(M)$, hence those points at which M has rank at most r. This $\mathcal{NP}$-hard problem *MinRank* [BFS99], and its variants where M may be rectangular, lies at the heart of multivariate cryptography. It is at the foundations of several schemes [Cou01, Pat96, KS99] and is still used to assess the security of encryption and signature schemes [FLP08, DS05, Beu22, BBC$^+$22, BBB$^+$20, BBC$^+$20].

Determinantal ideals also arise in fundamental areas such as effective real algebraic geometry as they encode critical points (see e.g. [FSS12, Spa14]), then used to solve a variety of problems. This includes polynomial optimization [GSED14, BGHS14], computing sample points and answering connectivity queries in smooth real algebraic sets [SS03, BGHP05, BGH$^+$10, SS17], determining the dimension of real algebraic sets [BS15, LS21a], and quantifier elimination over the reals [HS09, HS12, LS21b].

Determinantal ideals and polynomial system solving. Determinantal ideals enjoy plenty of combinatorial and algebraic properties [BV88, Las78, BCRV22] which can be leveraged to better understand the complexity of computing their roots, and to adapt and accelerate polynomial system solvers in this context. The most advanced results in this direction have been achieved in the context of symbolic homotopy techniques with the design of an adapted homotopy pattern [HSEDSV21] which

Authors' affiliation: Sorbonne Université, CNRS, LIP6, F-75005 Paris, France
E-mail addresses: firstname.lastname@lip6.fr.

has next been refined to take into account specific structures when the entries of the matrix M are sparse [LSSV21].

In this paper, we focus on the problem of computing *Gröbner bases* of the ideal $\mathcal{I}_r(M)$ w.r.t. some admissible monomial ordering, under the assumptions that $\mathcal{I}_r(M)$ has dimension 0 (or is $\mathcal{R}$) and that the entries of M have total degree at most 1.

Gröbner bases algorithms and determinantal ideals. Since Buchberger's algorithm [Buc65], the quest for fast algorithms for computing Gröbner bases has been driven by two main issues: *(i)* finding better strategies for handling critical pairs during the Gröbner basis construction and *(ii)* hunting reductions to 0 which are instrinsically related to algebraic objects named syzygies that are associated to the ideal under consideration. Issue *(i)* has been addressed by Faugère's celebrated F_4 algorithm [Fau99], which also made explicit the use of linear algebra subroutines in Gröbner bases algorithms. While a lot remains to be done in this direction (see e.g. [BESED22]), much attention has focused on issue *(ii)* and variants of Faugère's F_5 algorithm [Fau02] have been developed in several directions to give rise to signature-based Gröbner bases algorithms (see [EF16] and references therein). One byproduct of these works, which finds its roots in foundational works by Lazard and Giusti [Laz83, Giu84], is that they paved the way to complexity estimates *under some regularity assumptions*, thanks to the reduction to linear algebra and degree bounds on the maximum degree reached during the computation (related to the classical notion of index of regularity [CLO15, Chap. 9, §3]).

This has been developed, for determinantal ideals in [FSS10, FSS13] which yield complexity estimates for computing Gröbner bases *under regularity assumptions* (which are generic in the sense of algebraic geometry). These estimates are coarse: they do not leverage the shape of the matrices encountered during the computation.

Already in the simpler case of regular sequences, by exploiting the fact that the F_5 algorithm avoids all reductions to zero in this case, a sharper complexity analysis of F_5 [BFS15] shows significant improvements against such coarse estimates.

In the context of determinantal ideals, mimicking this to get better complexity estimates is premature. Indeed, $F_r(M)$ is *not* a regular sequence, and running the F_5 algorithm with input $F_r(M)$ does lead to a number of reductions to 0. Hence there is a need to refine and tune the F_5 algorithm for determinantal ideals. Such a refinement has already been achieved for boolean polynomial systems [BFSS13]. However, recall that these reductions to 0 are related to so-called syzygy modules of the ideal under study. Syzygy modules of determinantal ideals are notoriously more intricate than those of ideals generated by regular sequences or boolean systems.

In this paper, we tackle the following problems: *(i)* What is the suitable notion of regularity one can attach to determinantal ideals in order to hunt reductions to 0? *(ii)* What are the properties of modules of syzygies associated to determinantal ideals one can leverage under this notion of regularity? *(iii)* How to refine the F_5 algorithm for determinantal ideals to obtain fewer reductions to 0 and, ultimately, are there some instances of determinantal ideals for which one can prove that there are no reductions to 0?

Foundations. We begin by recalling first the connection between free resolutions and syzygy modules of ideals, and then the *syzygy criterion* from [EF16] which reveals the link between free resolutions and reductions to zero in F_5. In Algorithm 1, we give an altered version of the standard matrix-F_5 algorithm: it

computes Gröbner bases for modules over $\mathcal{R}$ and exploits the full syzygy criterion (see Proposition 4), allowing us to leverage reductions to zero in lower degrees to avoid reductions to zero in subsequent degrees.

Explicitly describing free resolutions of determinantal ideals is in general an extremely difficult problem. It is in fact not known if there even exists a minimal free resolution of the system of $(r+1)$-minors of a matrix of indeterminates over $\mathbb{Z}$ which remains minimal under arbitrary base change. While the Lascoux resolution [Las78] provides a free resolution of determinantal ideals, it is not minimal and requires that the coefficient ring have characteristic zero. Instead of computing a free resolution of these determinantal ideals directly, we instead adopt a strategy which relies on a theorem of Kurano [Kur89]. It describes the connection between syzygies of $(r+1)$-minors of a matrix M and syzygies between $(r+1)$-minors of the $(r+2)\times(r+2)$ submatrices of M. Using this theorem, we essentially reduce to the case $r = n-2$. In this case, an explicit free resolution exists, given by Gulliksen and Negård in [BV88].

Main results. Having made this reduction, we establish the genericity property which our ideals must satisfy in order for the Gulliksen-Negård complex to be exact: for any $1 \leq r < n$, the ideal of $(r+1)$-minors of an $n \times n$ matrix of indeterminates has the so-called *Cohen-Macaulay* property. Thus, for a suitably generic choice of coefficients of the linear forms in M, the ideal $\mathcal{I}_r(M)$ is Cohen-Macaulay as well. It is precisely under the genericity assumption derived from this notion that the complex of Gulliksen and Negård is a free resolution of $\mathcal{I}_{n-2}(M)$, and can therefore be exploited to avoid reductions to zero.

By tracing basis elements for the free modules which make up the complex of Gulliksen and Negård, we are able (Theorem 9) to explicitly compute a generating set for the first syzygy module of the system of $(n-1)$-minors of an $n \times n$ matrix of linear forms, provided the above stated genericity assumption holds. Kurano' s result [Kur89] states that for any $1 \leq r < n$, the first module of syzygies $\mathrm{Syz}(F_r(M))$ is generated by the syzygies between the $(r+1)$-minors of each $(r+2)\times(r+2)$ submatrix of M.

Therefore, combining the complex of Gulliksen and Negård with the result of [Kur89], we are able to explicitly compute a full generating set for $\mathrm{Syz}(F_r(M))$, and subsequently provide Algorithm 2, which computes a grevlex Gröbner basis for $\mathcal{I}_r(M)$ while avoiding all reductions to zero which arise from the syzygies in degree one.

Under our genericity assumption, when $r = n-2$, the Gulliksen-Negård complex allows us to compute generating sets for the higher syzygy modules of $F_{n-2}(M)$ as well. In Proposition 19, we give explicit generators for the second syzygy module of $\mathcal{I}_{n-2}(M)$. This study culminates in Algorithm 3 which is an altered version of matrix-F_5 which avoids all reductions to zero. Finally, in Proposition 23, we again exploit the Gulliksen-Negård complex to provide an explicit form for the Hilbert series of $\mathcal{I}_{n-2}(M)$ when the entries of M are sufficiently generic homogeneous linear forms, and when $\mathcal{I}_{n-2}(M)$ has dimension zero ($k = 4$). In Proposition 24, we use this series to give a complexity analysis of our new algorithm in the case $r = n-2$, demonstrating that asymptotically, the arithmetic complexity of our new algorithm is in $O(n^{4\omega-1})$, while the current best-known asymptotic arithmetic complexity of computing a grevlex Gröbner basis for $\mathcal{I}_{n-2}(M)$ is in $O(n^{5\omega+2})$. Here, $2 \leq \omega \leq 3$ is a complexity exponent for matrix multiplication.

We conclude by giving, in Table 1, some experimental data showing the amount of reductions to zero that is saved by our contributions and their practical interest.

Perspectives. In [Ma94], it is shown that in some cases, one can obtain generators for the second syzygy module of $\mathcal{I}_r(M)$ by lifting second syzygies of minors of submatrices, as is the case for first syzygies. Thus, the careful treatment of the Gulliksen-Negård complex which we give in this paper could be exploited in future works to avoid more reductions to zero when $r < n-2$.

Similarly, suppose M is no longer a square matrix, but is instead an $n \times m$, $n \neq m$ matrix of generic homogeneous linear forms over $\Bbbk$. Then when $r = \min(n,m)-1$ so that $\mathcal{I}_r(M)$ is the ideal of maximal minors of M, the Eagon-Northcott complex (see [BV88, 2.C] and [EN62]) provides a free resolution of $\mathcal{I}_r(M)$. Similarly, when $r = \min(n,m)-2$, the Akin-Buschbaum-Weyman complex (see [ABW81]) provides a free resolution of $\mathcal{I}_r(M)$. Again, the tools and methods brought in this paper could be adapted to accelerate Gröbner bases computations in this case and yield new complexity bounds.

Finally, in full generality, the Lascoux resolution (see [Las78]), is a free resolution for $\mathcal{I}_r(M)$ for any n, m, r provided $\mathbb{Q} \subseteq \Bbbk$. Again, one may expect refined F_5 algorithms by leveraging this resolution.

2. Preliminaries

2.1. **Syzygies.** We recall basic definitions and properties of syzygy modules, when working over the Noetherian ring $\mathcal{R} = \Bbbk[x_1, \ldots, x_k]$. We refer to [Eis95] for more details. For a finitely generated $\mathcal{R}$-module $\mathcal{M} = \langle p_1, \ldots, p_\ell \rangle$, the *first syzygy module* of $\mathcal{M}$ is defined as

$$\mathrm{Syz}(\mathcal{M}) := \{(s_1, \ldots, s_\ell) \in \mathcal{R}^\ell : s_1 p_1 + \cdots + s_\ell p_\ell = 0\}.$$

This definition depends on the generators; we sometimes write $\mathrm{Syz}(p_1, \ldots, p_\ell)$. From there one inductively defines the *j-th syzygy module of $\mathcal{M}$* as follows. Since $\mathcal{R}$ is Noetherian, $\mathrm{Syz}_{j-1}(\mathcal{M})$ is finitely generated. With generators $\{q_1, \ldots, q_t\}$ for $\mathrm{Syz}_{j-1}(\mathcal{M})$,

$$\mathrm{Syz}_j(\mathcal{M}) := \{(s_1, \ldots, s_t) \in \mathcal{R}^t : s_1 q_1 + \cdots + s_t q_t = 0\}.$$

It is frequent that $\mathcal{M}$ is the ideal generated by polynomials $F = (f_1, \ldots, f_\ell) \subseteq \mathcal{R}$. Then, the first syzygy module of F contains the Koszul syzygies, which are those following from the commutativity of polynomial multiplication: $f_i f_j - f_j f_i = 0$. In fact, they generate $\mathrm{Syz}(F)$ in the case of *regular sequences* (that is, when f_i is not a zero-divisor in $\mathcal{R}/\langle f_1, \ldots, f_{i-1} \rangle$ for any $2 \leq i \leq \ell$):

Theorem 1 ([Eis05, Thm. A.2.49])**.** If $(f_1, \ldots, f_\ell)$ is a regular sequence, then $\mathrm{Syz}(F) = \langle f_i e_j - f_j e_i : 1 \leq i, j \leq \ell, i \neq j \rangle$ where e_i is i-th standard basis vector.

In the context of $F_r(M)$, while the Koszul syzygies are among the syzygies of the minors of M, they do not generate $\mathrm{Syz}(F_r(M))$.

2.2. **Free resolutions.** As highlighted in Section 1, in relation to the k-th syzygy module of $F_r(M)$, our approach involves the description of a *free resolution* of $\mathcal{I}_r(M)$ (when $r = n-2$). For a finitely generated $\mathcal{R}$-module $\mathcal{M}$, a free resolution of $\mathcal{M}$ is an exact complex

$$\cdots \xrightarrow{d_{t+1}} \mathcal{E}_t \xrightarrow{d_t} \mathcal{E}_{t-1} \xrightarrow{d_{t-1}} \cdots \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \mathcal{M} \to 0$$

where for each $j > 0$, $\mathcal{E}_j$ is a finitely generated free $\mathcal{R}$-module, and the d_j are $\mathcal{R}$-module homomorphisms. The exactness condition precisely means that $\ker(d_j) = \mathrm{im}(d_{j+1})$. The free resolution $\mathcal{E}_\bullet$ is said to be *finite* if there exists some $m \geq 0$ such that for all $j > m$, $\mathcal{E}_j = \{0\}$; then the smallest such m is called the *length* of $\mathcal{E}_\bullet$. In general, modules need not have finite free resolutions; however, it is the case for finitely generated modules over $\mathcal{R} = \Bbbk[x_1, \ldots, x_k]$:

Theorem 2 (Hilbert's syzygy theorem)**.** Let $\mathcal{M}$ be a finitely generated $\mathcal{R}$-module. There exists a free resolution

$$0 \to \mathcal{E}_m \xrightarrow{d_m} \mathcal{E}_{m-1} \xrightarrow{d_{m-1}} \cdots \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \mathcal{M} \to 0$$

whose length m is at most the number of variables k.

Proposition 3. Let $\mathcal{M}$ be a finitely generated $\mathcal{R}$-module, $\mathcal{E}_\bullet$ be a free resolution of $\mathcal{M}$ of length $m \leq k$, and ℓ be the rank of $\mathcal{E}_0$. Let $\{e_1, \ldots, e_\ell\}$ be the standard basis for $\mathcal{E}_0$, and $p_i = \epsilon(e_i)$ for $1 \leq i \leq \ell$. Then $\ker(\epsilon) = \mathrm{Syz}(p_1, \ldots, p_\ell)$.

Following Proposition 3, if we fix a generating set $\{q_1, \ldots, q_t\}$ of $\mathrm{Syz}(\mathcal{M}) = \ker(\epsilon)$, then we can take $\mathcal{E}_1 = \mathcal{R}^t$ and, as a matrix, $d_1 = (q_{ij})_{1 \leq i \leq t, 1 \leq j \leq \ell}$. Continuing in this fashion, we construct $d_2, \ldots, d_m$ such that $\mathrm{Syz}_{j+1}(\mathcal{M}) = \ker(d_j)$ for $1 \leq j \leq m$.

2.3. **The matrix-F$_5$ algorithm.** The matrix-F_5 algorithm [BFS15] is based on F_5 [Fau02]. For the needs of this paper, we describe here a version of the former which exploits a more general *syzygy criterion* of the latter, as explained below.

Throughout, we will take $\prec$ to be the grevlex monomial order on $\mathcal{R}$, and $\prec_{\mathrm{pot}}$ to be the *position over term* order on the free module $\mathcal{R}^t$, for any $t \geq 1$. That is, for monomials $x = (0, \ldots, 0, x_i, 0, \ldots, 0)$ and $y = (0, \ldots, 0, y_j, 0, \ldots, 0)$ in $\mathcal{R}^t$ with respective supports i and j, $x \prec_{\mathrm{pot}} y$ if and only if $i < j$ or ($i = j$ and $x_i \prec y_j$).

2.3.1. *Macaulay matrices; signatures.* We take the standard grading by degree on $\mathcal{R}$, which induces a grading on the free module $\mathcal{R}^t$ for any $t \in \mathbb{Z}_{>0}$. Let $F = (f_1, \ldots, f_\ell) \subseteq \mathcal{R}^t$ be a sequence of homogeneous elements of $\mathcal{R}^t$. That is, for each $1 \leq i \leq \ell$, all coordinates of f_i (with respect to the standard basis of $\mathcal{R}^t$) are homogeneous of the same degree. We assume $d_1 \leq d_2 \leq \cdots \leq d_\ell$, where $d_i = \deg(f_i)$, without loss of generality. For $d \geq d_1$ and $1 \leq i \leq \ell$, let $\mathscr{M}_{d,i}$ be the Macaulay matrix of $(f_1, \ldots, f_i)$ in degree d. Each row of $\mathscr{M}_{d,i}$ corresponds to a polynomial τf_j where $1 \leq j \leq i$, $d_j \leq d$, and τ is a monomial of degree $d - d_j$; the pair (j, τ) is called the *signature* of this row. The columns of $\mathscr{M}_{d,i}$ are indexed by the monomials of $\mathcal{R}^t$ of degree d, and are ordered in decreasing order with respect to $\prec_{\mathrm{pot}}$. We take a position over term order $\prec_{\mathrm{sig}}$ on the set of pairs (j, τ) with $1 \leq j \leq \ell$ and τ a monomial of $\mathcal{R}$:

$$(j', \tau') \prec_{\mathrm{sig}} (j, \tau) \quad \text{if} \quad j' < j \text{ or } (j' = j \text{ and } \tau' \prec \tau).$$

A *valid row operation* on $\mathscr{M}_{d,i}$ consists in adding to a row with signature (j, τ) some $\Bbbk$-multiple of a row with signature which is $\prec_{\mathrm{sig}}$-less than (j, τ). We denote by $\bar{\mathscr{M}}_{d,i}$ any row echelon form of $\mathscr{M}_{d,i}$ obtained via a sequence of valid row operations. We will denote by $\mathrm{lt}(\bar{\mathscr{M}}_{d,i})$ the monomials corresponding to the pivot columns of $\bar{\mathscr{M}}_{d,i}$. Recall that the $f_1, \ldots, f_\ell$ are homogeneous. The nonzero rows of $\bar{\mathscr{M}}_{d,i}$ therefore form the elements of degree d of a Gröbner basis for $\langle f_1, \ldots, f_i \rangle$. For an integer $D \geq 0$, a set G is called a *D-Gröbner basis* for $\langle F \rangle$ if for all elements $f \in \langle F \rangle$ of

degree at most D, $\mathrm{lt}_{\mathrm{pot}}(f) \in \mathrm{lt}_{\mathrm{pot}}(\langle G \rangle)$. Thus, a D-Gröbner basis for $\mathcal{M} = \langle F \rangle$ is obtained by computing $\bar{\mathscr{M}}_{d,\ell}$ for all $d_1 \leq d \leq D$. Note that when $t = 1$, $f_1, \ldots, f_\ell$ are polynomials, and $\mathcal{M} = \langle F \rangle$ is simply a homogeneous ideal of $\mathcal{R}$, whence the rows of $\bar{\mathscr{M}}_{d,i}$ form the elements of degree d of a traditional Gröbner basis for $\langle f_1, \ldots, f_i \rangle$.

2.3.2. *The syzygy criterion.* When there are syzygies amongst $\boldsymbol{f} = (f_1, \ldots, f_\ell)$, the Macaulay matrices $\mathscr{M}_{d,i}$ do not have full rank. With prior knowledge of these syzygies, the matrix-F_5 algorithm can avoid rows which reduce to zero when computing $\bar{\mathscr{M}}_{d,i}$ from $\mathscr{M}_{d,i}$.

Proposition 4 (Syzygy Criterion, [EF16, Lem. 6.4])**.** Let $s = (s_1, \ldots, s_\ell)$ be a homogeneous syzygy of $\boldsymbol{f}$ and $\mathrm{lt}_{\mathrm{pot}}(s) = \tau e_i$. Then

(1) The row of $\mathscr{M}_{\deg \tau + d_i, i}$ with signature (i, τ) is a linear combination of rows of $\mathscr{M}_{\deg \tau + d_i, i}$ of smaller signature.
(2) For any monomial $\sigma \in \mathcal{R}$, the row of $\mathscr{M}_{\deg \tau + \deg \sigma + d_i, i}$ with signature $(i, \sigma\tau)$ is a linear combination of rows of $\mathscr{M}_{\deg \tau + \deg \sigma + d_i, i}$ of smaller signature.

Proof. We have $\tau f_i = -\sum_{j \neq i} s_j f_j - f_i(s_i - \mathrm{lt}_{\mathrm{pot}}(s))$. The module element τf_i corresponds to the row of $\mathscr{M}_{\deg \tau + d_i, i}$ with signature (i, τ), while $\sum_{j \neq i} s_j f_j - f_i(s_i - \mathrm{lt}_{\mathrm{pot}}(s))$ is a $\Bbbk$-linear combination of other rows of $\mathscr{M}_{\deg \tau + d_i, i}$. This proves Item 1.

Suppose now that the row with signature (i, τ) of $\bar{\mathscr{M}}_{\deg \tau + d_i, i}$ is a zero row. Then the polynomial τf_i is a $\Bbbk$-linear combination of rows of $\mathscr{M}_{\deg \tau + d_i, i}$ with smaller signature, i.e.,

$$\tau f_i = \sum_{(i', \tau') \prec_{\mathrm{sig}} (i, \tau)} c_{(i', \tau')} \tau' f_{i'} \text{ for some } c_{(i', \tau')} \in \Bbbk.$$

We can write $\sigma\tau f_i = \sum_{(i', \tau') \prec_{\mathrm{sig}} (i, \tau)} c_{(i', \tau')} \sigma\tau' f_{i'}$, for any monomial σ in $\mathcal{R}$. Hence, the row with signature $(i, \sigma\tau)$ of $\mathscr{M}_{\deg \tau + \deg \sigma + d_i, i}$ is a $\Bbbk$-linear combination of rows with smaller signature. □

If $t = 1$, the Koszul syzygies $f_j f_i - f_i f_j = 0$ for all $1 \leq i, j \leq \ell$ always exist, and produce linear dependencies between the rows of the Macaulay matrices. The matrix-F_5 algorithm works by interpreting these syzygies in this way to predict the signatures of rows which will reduce to zero when computing $\bar{\mathscr{M}}_{d,i}$ from $\mathscr{M}_{d,i}$, and avoiding such rows altogether. Succinctly, this algorithm utilizes the following criterion, which is a specialization of Proposition 4.

Proposition 5 (F_5 Criterion, [Fau02, Thm. 1])**.** The rows with signature (i, τ) of $\mathscr{M}_{d,i}$ reduce to zero in $\bar{\mathscr{M}}_{d,i}$, for all $\tau \in \mathrm{lt}(\bar{\mathscr{M}}_{d - d_i, i-1})$.

2.3.3. *The matrix-F_5 algorithm.* When $t = 1$, combining the syzygy criterion with Proposition 5 leads to the matrix-F_5 algorithm. It works incrementally by degree and index. That is, for a fixed degree d, it first computes the elements of degree d of a Gröbner basis for (f_1) by reducing the matrix $\mathscr{M}_{d,1}$ to $\bar{\mathscr{M}}_{d,1}$, and then builds the matrix $\mathscr{M}_{d,2}$ using $\bar{\mathscr{M}}_{d,1}$. Continuing in this fashion, it eventually builds and reduces $\mathscr{M}_{d,\ell}$, yielding the elements of degree d of a Gröbner basis for the full system F.

In Algorithm 1, we complement the description of this algorithm from [BFS15] by integrating Item 2 of Proposition 4. This is important since it allows us to avoid a significant number of reductions to zero that would occur without it. We allow for the input of precomputed syzygies of F in order to exploit Proposition 4 and

we allow $t \geq 1$. The termination and correction of Algorithm 1 is from [BFS15, Thm. 9] when $t = 1$, and the same induction argument works when $t > 1$.

Algorithm 1 Matrix-$F_5(F, D, S)$

Input: A sequence $F = (f_1, \ldots, f_\ell)$ of homogeneous elements of degrees $d_1 \leq \cdots \leq d_\ell$ in $\Bbbk[x_1, \ldots, x_k]^t$; a degree bound D; a set S of syzygies of F.
Output: The reduced POT D-Gröbner basis for $\langle F \rangle$.

for $i \in \{1, \ldots, \ell\}$ **do** $G_i \leftarrow \emptyset$
for d from d_1 to D **do**
  $\mathscr{M}_{d,0} \leftarrow \emptyset$; Crit $\leftarrow \mathrm{lt}_{\mathrm{pot}}(S)$
  for i from 1 to ℓ **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 $\bar{\mathscr{M}}_{d,i-1}$ with signature $(i, 1)$
    else
      $\mathscr{M}_{d,i} \leftarrow \bar{\mathscr{M}}_{d,i-1}$
      if $t = 1$ **then**
        for $\tau \in \mathrm{lt}(\mathscr{M}_{d-d_i,i-1})$ **do**
          Crit $\leftarrow$ Crit $\cup \{(i, \tau)\}$
      for $f \in \mathrm{rows}(\bar{\mathscr{M}}_{d-1,i}) \setminus \mathrm{rows}(\bar{\mathscr{M}}_{d-1,i-1})$ **do**
        $(i, \tau) \leftarrow$ signature of f
        if $f = 0$ **then**
          for $j \in \{1, \ldots, k\}$ **do**
            Crit $\leftarrow$ Crit $\cup \{(i, \tau \cdot x_j)\}$
      for $f \in \mathrm{rows}(\mathscr{M}_{d-1,i}) \setminus \mathrm{rows}(\mathscr{M}_{d-1,i-1})$ **do**
        $(i, \tau) \leftarrow$ signature of f
        for $j \in \{\max\{j' : x_{j'} \mid \tau\}, \ldots, k\}$ **do**
          if $(i, \tau \cdot x_j) \notin$ Crit **then**
  $\mathscr{M}_{d,i} \leftarrow$ concatenate the row $x_j f$ to $\mathscr{M}_{d,i}$ with signature $(i, \tau \cdot x_j)$
    $\bar{\mathscr{M}}_{d,i} \leftarrow$ reduced row echelon form of $\mathscr{M}_{d,i}$ obtained via a sequence of valid elementary row operations
    $G_i \leftarrow G_i \cup \{f \in \mathrm{rows}(\bar{\mathscr{M}}_{d,i}) : f \notin \langle \mathrm{lt}(G_i) \rangle\}$
return G_ℓ

2.4. **Genericity.** We take notation from [FSS13, Sec. 2 and 3]. Fix $n, k \in \mathbb{Z}_{>0}$. Define $\mathfrak{a} = \{\mathfrak{a}_t^{(i,j)} : 1 \leq t \leq k, 1 \leq i, j \leq n\}$. For each $1 \leq i, j \leq n$, let $f_{i,j} = \sum_{t=1}^{k} a_t^{(i,j)} x_t \in \Bbbk[\mathfrak{a}, x_1, \ldots, x_k]$. We call $f_{i,j}$ a *generic homogeneous linear form*. We denote by $\mathscr{A}$ the matrix over $\Bbbk[\mathfrak{a}, x_1, \ldots, x_k]$ whose (i, j) entry is $f_{i,j}$. Next, for a fixed $\boldsymbol{a} = \left(a_t^{(i,j)}\right) \in \bar{\Bbbk}^{k \cdot n^2}$, we denote by $\varphi_{\boldsymbol{a}}$ the specialization map $\varphi_{\boldsymbol{a}} : \Bbbk[\mathfrak{a}, x_1, \ldots, x_k] \to \bar{\Bbbk}[x_1, \ldots, x_k]$ which specializes $\mathfrak{a}_t^{(i,j)}$ to $a_t^{(i,j)}$. We call a map

$$\mathscr{P} : \mathrm{Ideals}(\Bbbk[\mathfrak{a}, x_1, \ldots, x_k]) \to \{\mathtt{true}, \mathtt{false}\}.$$

a *property*. For an integer $1 \leq r < n$, we will denote by $\mathcal{I}_r(\mathscr{A})$ the ideal of $(r+1)$-minors of $\mathscr{A}$. Subsequently, a property $\mathscr{P}$ is called $\mathcal{I}_r(\mathscr{A})$-*generic* if there exists a nonempty Zariski open subset U of $\mathbb{A}_{\Bbbk}^{kn^2}$ such that for all $\boldsymbol{a} \in U$, $\mathscr{P}\left(\varphi_{\boldsymbol{a}}(\mathcal{I}_r(\mathscr{A}))\right) = \mathtt{true}$.

An important property is the notion of Cohen-Macaulayness. Let $\mathcal{I}$ be an ideal of $\mathcal{R}$. A sequence $(f_1, \ldots, f_\ell) \subseteq \mathcal{R}$ is called an *$\mathcal{I}$-regular sequence* if for all $1 \leq i \leq \ell$, f_i is not a zero-divisor in the module $\mathcal{I}/\langle f_1, \ldots, f_{i-1}\rangle$. The ideal $\mathcal{I}$ is called *Cohen-Macaulay* if there exists an $\mathcal{I}$-regular sequence $(f_1, \ldots, f_\ell)$ such that $\ell = \dim(\mathcal{I})$ (here $\dim(\mathcal{I})$ is the Krull dimension of $\mathcal{I}$ in $\mathcal{R}$).

Remark 6. If $(f_1, \ldots, f_\ell)$ is an $\mathcal{I}$-regular sequence, then $\ell \leq \dim(\mathcal{I})$. Hence, Cohen-Macaulayness requires that there exists an $\mathcal{I}$-regular sequence of maximal possible length in $\mathcal{R}$.

Proposition 7. Let CM be the property $\mathrm{CM}(\mathcal{I}) = \texttt{true}$ if $\mathcal{I}$ is Cohen-Macaulay and $\mathrm{CM}(\mathcal{I}) = \texttt{false}$ otherwise. Then for any $1 \leq r \leq n-2$, CM is $\mathcal{I}_r(\mathscr{A})$-generic.

Proof. Let U be an $n \times n$ matrix of indeterminates; $\mathcal{I}_r(U)$ is Cohen-Macaulay [BV88, Thm. 2.5]; [FSS13, Lem. 3] ends the proof. □

3. Syzygies of determinantal ideals

Here, we focus on the syzygies between the minors $F_r(M)$ of order $r+1$ of M. The module $\mathrm{Syz}(F_r(M))$ is known to be generated by syzygies between minors of order $r+1$ of submatrices of M of size $(r+2) \times (r+2)$ [Kur89, Thm. 5.1]. This allows us to reduce the problem of computing generators for $\mathrm{Syz}(F_r(M))$ from the general case to the case $r = n-2$. The Gulliksen-Negård complex [GN72, BV88] is a free resolution of $\mathcal{I}_{n-2}(M)$. We will exploit this complex to obtain $\mathrm{Syz}(F_r(M))$ first when $r = n-2$, then in full generality.

3.1. The Gulliksen-Negård complex.

The Gulliksen-Negård complex is a free resolution of $\mathcal{I}_{n-2}(M)$,

$$0 \to \mathcal{E}_3 \xrightarrow{d_3} \mathcal{E}_2 \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \mathcal{I}_{n-2}(M) \to 0.$$

As such, we can use Proposition 3 to compute the first syzygy module of the set of generators $F_{n-2}(M)$ as the kernel of the augmentation map ϵ of this complex. We recall the construction of the complex here; details and proofs can be found in [BV88, 2.D].

We denote by $\mathcal{M}_n(\mathcal{R})$ the set of $n \times n$ matrices over $\mathcal{R}$, with the structure of a free $\mathcal{R}$-module of rank n^2. We will denote by $\boldsymbol{E}_{i,j}$ the standard (i,j)-th basis matrix of $\mathcal{M}_n(\mathcal{R})$. In this section we will take as generators for $\mathcal{I}_{n-2}(M)$ the cofactors of M. To that end, let $M^* = (M^*_{i,j})_{i,j} \in \mathcal{M}_n(\mathcal{R})$ be the matrix of these cofactors.

3.1.1. *The modules.* We begin by defining the component modules $\mathcal{E}_3$, $\mathcal{E}_2$, $\mathcal{E}_1$, $\mathcal{E}_0$. Let $\mathcal{E}_0 = \mathcal{M}_n(\mathcal{R})$. Consider the sequence

$$\mathcal{R} \xrightarrow{\iota} \mathcal{M}_n(\mathcal{R}) \oplus \mathcal{M}_n(\mathcal{R}) \xrightarrow{\pi} \mathcal{R}$$

with $\iota(a) = (aI_n, aI_n)$, where I_n is the identity matrix in $\mathcal{M}_n(\mathcal{R})$ and $\pi(X, Y) = \mathrm{tr}(X - Y)$ is the trace of $X - Y$. The module $\ker(\pi)$ is generated by the union of the following sets:

- $\{(0, \boldsymbol{E}_{i,j}) \in \mathcal{M}_n(\mathcal{R}) \oplus \mathcal{M}_n(\mathcal{R}) : 1 \leq i, j \leq n, i \neq j\}$,
- $\{(\boldsymbol{E}_{i,j}, 0) \in \mathcal{M}_n(\mathcal{R}) \oplus \mathcal{M}_n(\mathcal{R}) : 1 \leq i, j \leq n, i \neq j\}$,
- $\{(\boldsymbol{E}_{i,i}, \boldsymbol{E}_{1,1}) \in \mathcal{M}_n(\mathcal{R}) \oplus \mathcal{M}_n(\mathcal{R}) : 1 \leq i \leq n\}$, and
- $\{(0, \boldsymbol{E}_{i,i} - \boldsymbol{E}_{1,1}) \in \mathcal{M}_n(\mathcal{R}) \oplus \mathcal{M}_n(\mathcal{R}) : 2 \leq i \leq n\}$.

On the other hand, $\operatorname{im}(\iota)$ is generated by

$$(I_n, I_n) = (\boldsymbol{E}_{1,1}, \boldsymbol{E}_{1,1}) + \textstyle\sum_{i=2}^{n} (\boldsymbol{E}_{i,i}, \boldsymbol{E}_{1,1}) + \sum_{i=2}^{n} (0, \boldsymbol{E}_{i,i} - \boldsymbol{E}_{1,1}).$$

This shows that $\mathcal{E}_1 = \ker(\pi)/\operatorname{im}(\iota)$ is a free module. Finally, let $\mathcal{E}_2 = \mathcal{M}_n(\mathcal{R})$ and $\mathcal{E}_3 = \mathcal{R}$.

3.1.2. *The maps.* We next define the maps d_1, d_2, d_3, ϵ, as follows:

- $\epsilon : \mathcal{E}_0 \to \mathcal{I}_{n-2}(M), \quad N \mapsto \operatorname{tr}(M^*N)$,
- $d_1 : \mathcal{E}_1 \to \mathcal{E}_0, \quad \overline{(N_1, N_2)} \mapsto N_1 M - M N_2$,
- $d_2 : \mathcal{E}_2 \to \mathcal{E}_1, \quad N \mapsto \overline{(MN, NM)}$, and
- $d_3 : \mathcal{E}_3 \to \mathcal{E}_2, \quad x \mapsto xM^*$,

where for $(N_1, N_2) \in \mathcal{M}_n(\mathcal{R}) \oplus \mathcal{M}_n(\mathcal{R})$, we denote by $\overline{(N_1, N_2)}$ its image under the canonical surjection $\mathcal{M}_n(\mathcal{R}) \oplus \mathcal{M}_n(\mathcal{R}) \twoheadrightarrow \mathcal{E}_1$.

Proposition 8. Let M be a matrix of homogeneous linear forms in $\mathcal{R}$. Assume $\mathcal{I}_{n-2}(M)$ is Cohen-Macaulay. With

$$\mathcal{E}_0, \mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3, \epsilon, d_1, d_2, d_3.$$

as defined above, the sequence

$$0 \to \mathcal{E}_3 \xrightarrow{d_3} \mathcal{E}_2 \xrightarrow{d_2} \mathcal{E}_1 \xrightarrow{d_1} \mathcal{E}_0 \xrightarrow{\epsilon} \mathcal{I}_{n-2}(M) \to 0$$

is a free resolution of $\mathcal{I}_{n-2}(M)$.

Proof. Since $\mathcal{I} = \mathcal{I}_{n-2}(M)$ is Cohen-Macaulay, there exists an $\mathcal{I}$-regular sequence of length equal to the Krull dimension of $\mathcal{I}$ in $\mathcal{R}$. By [FSS13, Thm. 10] and Proposition 7, the Krull dimension of $\mathcal{I}$ is exactly 4. Then, the result follows from [BV88, Thm. 2.26]. □

3.2. **The case $r = n - 2$.** We give generators for the first syzygy module in the case $r = n - 2$, assuming $\mathcal{I}_{n-2}(M)$ is Cohen-Macaulay.

Theorem 9. Let $M = (m_{i,j})$ be a matrix of homogeneous linear forms in $\mathcal{R}$. Suppose that $\mathcal{I}_{n-2}(M)$ is Cohen-Macaulay. Then the first syzygy module of $F_{n-2}(M)$ is generated by:

(i) $\sum_{k=1}^{n} (-1)^{k+j} m_{k,i} \boldsymbol{E}_{k,j}$ for $i \neq j$;
(ii) $\sum_{k=1}^{n} (-1)^{i+k} m_{j,k} \boldsymbol{E}_{i,k}$ for $i \neq j$;
(iii) $\sum_{k=1}^{n} ((-1)^{i+k} m_{k,i} \boldsymbol{E}_{k,i} - (-1)^{k+1} m_{1,k} \boldsymbol{E}_{1,k})$ for $1 \leq i \leq n-1$;
(iv) $\sum_{k=1}^{n} ((-1)^{j+k} m_{j,k} \boldsymbol{E}_{j,k} - (-1)^{k+1} m_{1,k} \boldsymbol{E}_{1,k})$ for $2 \leq j \leq n$.

Furthermore, the syzygies described by Items *(i), (ii), (iii)* and *(iv)* form a minimal generating set for the $\operatorname{Syz}(F_{n-2}(M))$ of size $2n^2 - 2$.

Proof. By Proposition 3, $\ker(\epsilon)$ is the first syzygy module of the cofactors of M. By Proposition 8, since $\mathcal{I}_{n-2}(M)$ is Cohen-Macaulay, the Gulliksen-Negård complex is exact and $\ker(\epsilon) = \operatorname{im}(d_1)$. The image $\operatorname{im}(d_1)$ is generated by the images of generators for $\mathcal{E}_1$ under d_1. Thus, by Section 3.1, the first syzygy module of $F_{n-2}(M)$ is generated by the following syzygies. For $i \neq j$,

$$d_1\Big(\overline{(\boldsymbol{E}_{i,j}, 0)}\Big) = \boldsymbol{E}_{i,j} M = \sum_{k=1}^{n} m_{k,i} \boldsymbol{E}_{k,j}. \tag{1}$$

Similarly, for $i \neq j$,

$$d_1\Big(\overline{(0, \boldsymbol{E}_{i,j})}\Big) = M \boldsymbol{E}_{i,j} = \sum_{k=1}^{n} m_{j,k} \boldsymbol{E}_{i,k}. \tag{2}$$

For any $1 \leq i \leq n-1$,

$$d_1\Big(\overline{(\boldsymbol{E}_{i,i}, \boldsymbol{E}_{1,1})}\Big) = E_{i,i}M - M\boldsymbol{E}_{1,1} = \sum_{k=1}^{n} m_{k,i}\boldsymbol{E}_{k,i} - m_{1,k}\boldsymbol{E}_{1,k}. \tag{3}$$

Finally, for any $2 \leq j \leq n$,

$$d_1\Big(\overline{(0, \boldsymbol{E}_{j,j} - \boldsymbol{E}_{1,1})}\Big) = M\boldsymbol{E}_{j,j} - M\boldsymbol{E}_{1,1} = \sum_{k=1}^{n} m_{j,k}\boldsymbol{E}_{j,k} - m_{1,k}\boldsymbol{E}_{1,k}. \tag{4}$$

Since the generators for $\mathcal{I}_{n-2}(M)$ taken in the Gulliksen-Negård complex are the cofactors of M rather than the $(n-1)$-minors of M, we obtain Items (i) to (iv) by pulling back each of Eqs. (1) to (4), respectively under the isomorphism $M^*_{i,j} \in \mathcal{I}_{n-2}(M) \mapsto (-1)^{(i+j)}M^*_{i,j} \in \mathcal{I}_{n-2}(M)$. There are $n^2 - n$ syzygies described by each of Item (i) and Item (ii), and $n-1$ syzygies described by each of Item (iii) and Item (iv). This gives a total of $2n^2 - 2$ syzygies.

We conclude by proving that these $2n^2 - 2$ syzygies form a minimal generating set for $\mathrm{Syz}(F_{n-2}(M))$. Let $m_1, \ldots, m_{2n^2-2} \in \mathrm{Syz}(F_{n-2}(M))$ denote the generating set given by Item (i), Item (ii), Item (iii), Item (iv). Suppose that for some $1 \leq i \leq 2n^2 - 2$, m_i is generated by $\{m_1, \ldots, m_{2n^2-2}\} \smallsetminus \{m_i\}$. Then we can write $\sum_{j \neq i} a_j m_j = m_i$ for some $a_j \in \mathcal{R}$. Since the m_j are all homogeneous, this forces $a_j \in \Bbbk$ for all $j \neq i$. Subsequently, $a_j \in \mathrm{im}(d_2) \cap \Bbbk^{2n^2-2}$ for all $j \neq i$.
Letting $a_i = 1$, and taking $N \in d_2^{-1}((a_1, \ldots, a_{2n^2-2}))$, we find that $MN, NM \in \mathcal{M}_n(\mathcal{R})$ are matrices with entries in $\Bbbk$. For $1 \leq j \leq n$, the entries of the j-th row of MN are members of the ideal generated by the j-th row of M. The entries of M are homogeneous linear forms, so the only constant element contained in this ideal 0. Similarly, for $1 \leq j \leq n$, the entries of the j-th row of NM are members of the ideal generated by the j-th column of M, and an analogous argument applies. Thus, $a_j = 0$ for each $1 \leq j \leq 2n^2 - 2$. □

One can easily construct an algorithm, named SyzCorankOne, which, given a matrix M, computes the syzygies described in Theorem 9.

Remark 10. In both Theorem 9 and SyzCorankOne(M) we require that $F_{n-2}(M)$ is Cohen-Macaulay. This is necessary, as without it the Gulliksen-Negård complex need not be exact and subsequently we cannot compute $\mathrm{Syz}(F_{n-2}(M))$ using its differential maps. However, since ϵ is defined by $\epsilon(N) = \mathrm{tr}(M^*N)$, where $M^* = (M^*_{i,j})$ is the matrix of cofactors of M, a matrix $N = (N_{i,j}) \in \mathcal{M}_n(\mathcal{R})$ is in the kernel of ϵ if and only if $\sum_{1 \leq i,j \leq n} N_{j,i}M^*_{i,j} = 0$. That is, $\ker(\epsilon)$ corresponds to $\mathrm{Syz}(F_{n-2}(M))$ even if $\mathcal{I}_{n-2}(M)$ is not Cohen-Macaulay. Moreover, even if $\mathcal{I}_{n-2}(M)$ is not Cohen-Macaulay, the Gulliksen-Negård complex is still a complex. Thus, in all cases, $\mathrm{im}(d_1) \subseteq \ker \epsilon$, so if $\mathcal{I}_{n-2}(M)$ is not Cohen-Macaulay, Theorem 9 describes (and subsequently SyzCorankOne(M) computes) a generating set for a submodule of $\mathrm{Syz}(F_{n-2}(M))$.

Remark 11. If the entries of M are not homogeneous, then assuming $\mathcal{I}_{n-2}(M)$ is Cohen-Macaulay, the syzygies computed by Theorem 9 still generate $\mathrm{Syz}(F_{n-2}(M))$, but they need no longer be a *minimal* generating set.

3.3. **The general case.**

Theorem 12. Let $n \geq 3$ and let $1 \leq r \leq n-2$. Then there exists a nonempty Zariski open set $U \subseteq \mathbb{A}_{\Bbbk}^{kn^2}$ such that for all $\boldsymbol{a} \in U$, taking $M = \varphi_{\boldsymbol{a}}(\mathscr{A})$, the

following holds: Let M' be the set of submatrices of size $(r+2)\times(r+2)$ of M. For each matrix $N \in M'$, let $S(N)$ be the set of syzygies of $F_r(N)$ computed using Theorem 9. Then $\mathrm{Syz}(F_r(M)) = \bigcup_{N\in M'} S(N)$.

Proof. Let $\mathscr{U}$ be an $n \times n$ matrix of indeterminates over $\Bbbk$. Let $\mathscr{U}'$ be the set of $(r+2)\times(r+2)$ submatrices of $\mathscr{U}$. For each $\mathscr{N} \in \mathscr{U}'$, let $S(\mathscr{N})$ be the set of syzygies of $F_r(\mathscr{N})$ computed using Theorem 9. By [Kur89, Thm. 5.1], $\mathrm{Syz}(F_r(\mathscr{A})) = \bigcup_{\mathscr{N}\in\mathscr{U}'} S(\mathscr{N})$. Thus, by [FSS13, Lem. 3], there is a nonempty Zariski open subset $U_1 \subseteq \mathbb{A}_{\Bbbk}^{kn^2}$ such that for all $\boldsymbol{a} \in U_1$, the syzygies between the $(r+1)$-minors of $\varphi_{\boldsymbol{a}}(\mathscr{A})$ are those between the $(r+1)$-minors of each $(r+2)\times(r+2)$ submatrix of $\varphi_{\boldsymbol{a}}(\mathscr{A})$. We denote by $\mathscr{A}'$ the set of $(r+2)\times(r+2)$ submatrices of $\mathscr{A}$. By Proposition 7, for each submatrix N of $\mathscr{A}'$, there exists a nonempty Zariski open subset $U_N \subseteq \mathbb{A}_{\Bbbk}^{k\cdot n^2}$ such that for all $\boldsymbol{a} \in U_N$, the ideal generated by the $(r+1)$-minors of N is Cohen-Macaulay, so that Theorem 9 applies. Thus, taking $U = \bigcap_{N\in\mathscr{A}'} U_N \cap U_1$, the result follows. □

Consequently, using $\mathrm{SyzCorankOne}(M)$ we obtain an algorithm $\mathrm{SyzGen}(M, r)$ which constructs a set of generators for $\mathrm{Syz}(F_r(M))$.

Remark 13. From Theorems 9 and 12, neither $\mathrm{SyzGen}(M, r)$ nor $\mathrm{SyzCorankOne}(M)$ require any arithmetic $\Bbbk$-operations.

Again in the statement of Theorem 12 we require that $\mathcal{I}_r(M)$ is Cohen-Macaulay. This is necessary in order for $\mathrm{Syz}(\mathcal{I}_r(M))$ to be computed via the syzygies of $(r+1)$-minors of $(r+2)\times(r+2)$ submatrices. If $\mathcal{I}_r(M)$ is not Cohen-Macaulay, Theorem 12 gives a (possibly proper) subset of a generating set for $\mathrm{Syz}(\mathcal{I}_r(M))$.

Finally, we require that the entries of M be homogeneous linear forms. Once again, the theorem holds if the entries are affine, as long as $\mathcal{I}_r(M)$ satisfies the stated genericity assumption.

Note that no claim is made as to the minimality of the generating set computed in Theorem 12. However, one can show that when the entries of M are homogeneous, a minimal generating set can be extracted from the set computed in Theorem 12 by throwing away any element which differs by multiplication by -1 from another element. This need no longer hold if the entries are affine.

4. Determinantal matrix-F_5 algorithm

In this section, we use the syzygies returned by $\mathrm{SyzGen}(M, r)$ to avoid reductions to zero when running Algorithm 1. As explained below, the following result will be instrumental.

Proposition 14 ([EF16, Lem. 6.4])**.** Let $(f_1, \ldots, f_\ell) = F \subseteq \mathcal{R}^t$ be a system of homogeneous module elements. Let $D \in \mathbb{Z}_{\geq 0}$, and let $G = G_{D-\min_i\{\deg(f_i)\}}$ be the elements up to degree $D - \min_i\{\deg(f_i)\}$ of a POT-Gröbner basis for $\mathrm{Syz}(F)$. Then,

(1) If $\tau e_i \in \mathrm{lt}_{\mathrm{pot}}(G)$, the row of $\mathscr{M}_{\deg(\tau)+\deg(f_i),i}$ with signature (i,τ) is a linear combination of rows with smaller signature.
(2) If a row with signature (i,τ) of $\mathscr{M}_{\deg(\tau)+\deg(f_i),i}$ reduces to zero, then τe_i is in the module generated by $\mathrm{lt}_{\mathrm{pot}}(G)$.

Proof. Item 1 is simply Proposition 4. We turn to Item 2. Fix $\min_i\{\deg(f_i)\} \leq d \leq D$ and $1 \leq i \leq \ell$. Suppose that the row with signature (i,τ) reduces to zero

in $\bar{\mathscr{M}}_{\deg(\tau)+\deg(f_i),i}$. Then there is a linear dependency $s_1 f_1 + \cdots + s_\ell f_\ell = 0$. This corresponds to a syzygy $s = s_1 e_1 + \cdots + s_\ell e_\ell \in \mathrm{Syz}(F)$ with $\mathrm{lt}_{\mathrm{pot}}(s) = \tau e_i$. Finally,

$$\deg(s_i) = d - \deg(f_i) \leq D - \deg(f_i) \leq D - \min_i\{\deg(f_i)\}.$$

for each $1 \leq i \leq \ell$. Thus $\mathrm{lt}_{\mathrm{pot}}(s) = \tau e_i$ is in $\langle \mathrm{lt}_{\mathrm{pot}}(G)\rangle$. □

Using Proposition 14, in order to remove all reductions to zero when running Algorithm 1 to compute a D-Gröbner basis for a graded module $F \subseteq \mathcal{R}^t$, we compute the leading terms of the elements up to degree $D - \min_{f\in F}\{\deg f\}$ of a Gröbner basis for $\mathrm{Syz}(F)$. We can compute them by running Algorithm 1 on a set of chosen generators for $\mathrm{Syz}(F)$ itself, with the appropriate degree bound given by Proposition 14. However, if $\mathrm{Syz}_2(F) \neq \{0\}$, then Proposition 14 once again shows that reductions to zero will be encountered when computing the elements up to degree $D - \min_{f\in F}\{\deg f\}$ of a Gröbner basis for $\mathrm{Syz}(F)$.

When $r = n - 2$, the Gulliksen-Negård complex allows us to explicitly compute generating sets for all higher syzygy modules. Thus, we can avoid all reductions to zero when computing a D-Gröbner basis for $F_r(M)$. When $r < n - 2$, we can only compute a generating set for the first syzygy module $\mathrm{Syz}(F_r(M))$, and thus cannot efficiently remove all reductions to zero.

Now we are ready to describe an algorithm which exploits the syzygies computed by $\mathrm{SyzGen}(M, r)$ to compute a grevlex Gröbner basis for $F_r(M)$ without reductions to zero in degree $r + 2$.

Algorithm 2 Determinantal-Matrix-$F_5(M, r, D)$

Input: An integer $1 \leq r \leq n-2$, an $n \times n$ matrix M of homogeneous linear forms over $\Bbbk$ in $(n-r)^2$ variables such that $\mathcal{I}_r(M)$ is Cohen-Macaulay, and a degree bound D.

Output: A grevlex D-Gröbner basis for $\mathcal{I}_r(M)$.

1: $S \leftarrow \mathrm{SyzGen}(M, r)$
2: $S' \leftarrow$ Matrix-F$_5(S, 1, \emptyset)$
3: $G \leftarrow$ Matrix-F$_5(F_r(M), D, S')$
4: **return** G

Proposition 15. Algorithm 2 terminates and is correct.

Proof. Termination follows from that of $\mathrm{SyzGen}(M, r)$ and Algorithm 1. To prove correctness, we need to show that the set S' of Line 2 is indeed a set of syzygies between the elements of $\mathcal{I}_r(M)$. By Theorem 12, the set S computed on Line 1 is a minimal generating set for $\mathrm{Syz}(F_r(M))$. By the construction of this generating set, given in Theorem 12, each element of S is homogeneous of degree one. Hence, according to Section 2.3.3, the set S' consists of the elements of degree one of a POT-Gröbner basis for $\mathrm{Syz}(F_r(M))$. □

Remark 16. Both the number of rows and the number of columns of the Macaulay matrix in degree one for the set S on Line 2 of Algorithm 2 is bounded by the number of rows of the Macaulay matrix for $F_r(M)$ in degree $r + 1$. Therefore, asymptotically, the arithmetic cost of Algorithm 2 is bounded by the arithmetic cost of its final step, computing the Gröbner basis of $F_r(M)$.

Proposition 17. Let $n \geq 3$, let $1 \leq r \leq n-2$, let $D = r \cdot (n-r) + 1$, and let $k = (n-r)^2$. There exists a nonempty Zariski open set $U \subseteq \mathbb{A}_{\Bbbk}^{kn^2}$ such that for all $\boldsymbol{a} \in U$, taking $M = \varphi_{\boldsymbol{a}}(\mathscr{A})$, upon running Algorithm 2 with arguments M, r, D:

(1) a full grevlex Gröbner basis is returned; and
(2) for each $1 \leq i \leq \binom{n}{r+1}^2$, the matrix $\mathscr{M}_{r+2,i}$ has full rank.

Proof. By [FSS13,], there exists a Zariski open subset $U_1 \subseteq \mathbb{A}_{\Bbbk}^{kn^2}$ such that the maximal degree of a polynomial in the reduced grevlex Gröbner basis for $\mathcal{I}_r(M)$ is precisely D. Let U_2 be a nonempty Zariski open subset of $\mathbb{A}_{\Bbbk}^{kn^2}$ such that the results of Theorem 12 hold. Let $U = U_1 \cap U_2$. Item 1 follows immediately from the degree bound given in [FSS13]. We turn to Item 2. By Proposition 14, Item 2, it suffices to show that the leading terms of the set S' of Line 2 consists of the elements of degree at most $r+2$ of $\mathrm{lt}_{\mathrm{pot}}(\mathrm{Syz}(\mathcal{I}_r(M)))$. This is immediate from Theorem 12 and Section 2.3.3. □

Remark 18. If we do not impose the genericity assumption on $\mathcal{I}_r(M)$ Algorithm 2 will still return a D-Gröbner basis for $\mathcal{I}_r(M)$, though $\mathscr{M}_{r+2,i}$ need no longer be full rank for all $1 \leq i \leq \binom{n}{r+1}^2$.

If the entries of M are affine, by Remark 13, there are two possibilities. First, $\mathrm{SyzGen}(M, r)$ still returns a generating set for the first syzygy module of $F_r(M)$, and these may be used in the original F_5 algorithm which works on affine input to avoid reductions to zero. Alternatively, following [CLO15, Ch. 8, § 2, Prop. 7], one can simply homogenize $F_r(M)$ with respect to a variable h which is taken to be grevlex smaller than all other variables of $\mathcal{R}$, and specialize $h = 1$ upon termination of Algorithm 2.

5. The case $r = n - 2$

Now, we describe an altered version of the F_5 algorithm which computes a Gröbner basis for $\mathcal{I}_r(M)$ when $r = n-2$ without any reductions to zero. Note that Algorithm 2 does not require $r < n-2$. Thus, we could simply compute a Gröbner basis for $\mathcal{I}_r(M)$ using Algorithm 2 when $r = n-2$. However, only those reductions to zero arising from syzygies of degree $r+2$ will be avoided. By Proposition 14, any syzygies of degree $d > r+2$ which cannot be generated by the syzygies of degree $r+2$ will manifest as reductions to zero in the Macaulay matrices in degree d.

5.1. **Higher syzygy modules.** By Proposition 8, the Gulliksen-Negård complex is a free resolution of $\mathcal{I}_r(M)$ as soon as $\mathcal{I}_r(M)$ is Cohen-Macaulay. Thus, the kernels of its differential maps are precisely the syzygy modules of $\mathcal{I}_r(M)$. The map d_3 is defined by $d_3(x) = xM^*$, where M^* is the matrix of cofactors of M. The third syzygy module $\mathrm{Syz}_3(\mathcal{I}_r(M))$ is the image of d_3, and is thus free of rank n^2 and principally generated by the entries of M^*.

Proposition 19. Let M be an $n \times n$ matrix of homogenoeus linear forms in $\mathcal{R}$. Suppose $\mathcal{I}_{n-2}(M)$ is Cohen-Macaulay. In the $\mathcal{R}$-basis for $\ker(\pi)/\operatorname{im}(\iota)$ given in Section 3.1, the second syzygy module $\mathrm{Syz}_2(F_r(M))$ is generated by the following syzygies:

(i) For $2 \leq i \leq n$ and $1 \leq j \leq n-1$,

$$\sum_{k \neq j} m_{k,i} \overline{(E_{k,j}, 0)} + \sum_{k \neq i} m_{j,k} \overline{(0, E_{i,k})} + m_{j,i} \left(\overline{(E_{j,j}, E_{1,1})} + \overline{(0, E_{i,i} - E_{1,1})} \right).$$

(ii) For $2 \leq i \leq n$,

$$\sum_{k \neq n} m_{k,i} \overline{(E_{k,n}, 0)} + \sum_{k \neq i} m_{n,k} \overline{(0, E_{i,k})} - m_{n,i} \left(\sum_{j=1}^{n-1} \overline{(E_{j,j}, E_{1,1})} + \sum_{j=2}^{n-1} \overline{(0, E_{j,j} - E_{1,1})} \right)$$

(iii) For $1 \leq j \leq n-1$,

$$\sum_{k \neq j} m_{k,1} \overline{(E_{k,j}, 0)} + \sum_{k \neq 1} m_{j,k} \overline{(0, E_{1,k})} + m_{j,1} \overline{(E_{j,j}, E_{1,1})}$$

(iv) Finally,

$$\sum_{k \neq n} m_{k,1} \overline{(E_{k,n}, 0)} + \sum_{k \neq 1} m_{n,k} \overline{(0, E_{1,k})} - m_{n,1} \left(\sum_{j=1}^{n-1} \overline{(E_{j,j}, E_{1,1})} + \sum_{j=2}^{n} \overline{(0, E_{j,j} - E_{1,1})} \right)$$

Proof. The second syzygy module $\mathrm{Syz}_2(\mathcal{I}_r(M))$ is the image of d_2, by Proposition 8. The map d_2 is defined by

$$d_2(N) = \overline{(MN, NM)}.$$

Taking $\boldsymbol{E}_{i,j}$, $1 \leq i, j \leq n$ to be the canonical $\mathcal{R}$-basis for $\mathcal{M}_n(\mathcal{R})$, a basis for $\mathrm{im}(d_2)$ is given by $\{\overline{(M\boldsymbol{E}_{i,j}, \boldsymbol{E}_{i,j}M)} \mid 1 \leq i, j \leq n\}$. We can express $M\boldsymbol{E}_{i,j}$ and $\boldsymbol{E}_{i,j}M$ in the canonical $\mathcal{R}$-basis for $\mathcal{M}_n(\mathcal{R})$,

$$M\boldsymbol{E}_{i,j} = m_{j,i}\boldsymbol{E}_{j,j} + \sum_{k \neq j} m_{k,i}\boldsymbol{E}_{k,j}; \ \boldsymbol{E}_{i,j}M = m_{j,i}\boldsymbol{E}_{i,i} + \sum_{k \neq i} m_{j,k}\boldsymbol{E}_{i,k}.$$

From this, we express generators for $\mathrm{Syz}_2(\mathcal{I}_r(M))$ in the $\mathcal{R}$-basis for $\ker(\pi)/\mathrm{im}(\iota)$. Doing so gives precisely Items (i) to (iv). □

Using Proposition 19, one can easily construct an algorithm, which we will call Syz2GenCorankOne(M) which constructs the set $\mathrm{Syz}_2(F_{n-2}(M))$. We use this algorithm in the next section to design a dedicated F_5-type algorithm which performs no reduction to zero when computing a Gröbner basis of $\mathcal{I}_{n-2}(M)$ when $\mathcal{I}_{n-2}(M)$ is Cohen-Macaulay and $k = 4$.

Remark 20. Analogous to Remark 18, if $\mathcal{I}_{n-2}(M)$ is not Cohen-Macaulay, the Gulliksen-Negård complex need not be a free resolution of $\mathcal{I}_{n-2}(M)$, though it is still a complex. Thus, even if $\mathcal{I}_{n-2}(M)$ is not Cohen-Macaulay, $\mathrm{im}(d_2) \subseteq \ker(d_1)$, so the syzygies described by Proposition 19 are a subset of a generating set for the syzygies between the generators for $\ker \epsilon$ given by Theorem 9.

5.2. **A refined $\mathbf{F_5}$ algorithm.** We combine Proposition 19, Theorem 9, and Proposition 14 to give an algorithm which computes a grevlex Gröbner basis for $F_{n-2}(M)$ without any reductions to zero, provided $\mathcal{I}_{n-2}(M)$ is Cohen-Macaulay. In order to obtain the leading terms of the first syzygy module, of $F_{n-2}(M)$, we must know which rows will reduce to zero when echelonizing the Macaulay matrices associated to the first syzygy module in various degrees. By Proposition 14, the signatures of these rows are precisely the leading terms of a Gröbner basis for the second syzygy module in the appropriate degree.

Subsequently, applying Proposition 14 once again, the leading terms of the first syzygy module in various degrees are precisely the signatures of the rows which reduce to zero when echelonizing the Macaulay matrices associated to $F_{n-2}(M)$.

Algorithm 3 Determinantal-Corank-One-Matrix-F_5

Input: An integer $n \geq 3$, an $n \times n$ matrix of generic homogeneous linear forms over $\Bbbk$ in 4 variables, and an integer $D \geq n-1$

Output: The elements up to degree D of a grevlex Gröbner basis for $\mathcal{I}_{n-2}(M)$.

1: $S_1 \leftarrow \text{SyzCorankOne}(M)$
2: $S_2 \leftarrow \text{Syz2GenCorankOne}(M)$
3: $S_2' \leftarrow \text{Matrix-F}_5(S_2, D-n, \emptyset)$
4: $S_1' \leftarrow \text{Matrix-F}_5(S_1, D-n+1, S_2')$
5: $G \leftarrow \text{Matrix-F}_5(F_{n-2}(M), D, S_1')$
6: **return** G

Proposition 21. Algorithm 3 terminates and is correct.

Proof. Termination is an easy consequence from the one of SyzCorankOne(M), Syz2GenCorankOne(M), and Algorithm 1. For correctness, it suffices to show that the set S_1' computed on Line 4 is indeed a set of syzygies of the polynomials in $F_{n-2}(M)$. This follows from Theorem 9. □

Proposition 22. Let $D = 2n-3$. Then there is a nonempty Zariski open subset U of $\mathbb{A}_{\Bbbk}^{4\cdot n^2}$ such that for all $\boldsymbol{a} \in U$, upon running Algorithm 3 with arguments $\varphi_{\boldsymbol{a}}(\mathcal{I}_{n-2}(\mathscr{A})), D$,

(1) a full grevlex Gröbner basis is returned; and
(2) for each $1 \leq i \leq n^2$ and for each $n-1 \leq d \leq 2n-3$, the matrix $\mathscr{M}_{d,i}$ is full rank.

Proof. By [FSS13, Lem. 18], there is a Zariski dense subset U_1 of $\mathbb{A}_{\Bbbk}^{4\cdot n^2}$ such that for all $\boldsymbol{a} \in U_1$, the maximal degree of a polynoimal in the reduced grevlex Gröbner basis of $\mathcal{I}_{n-2}(M)$ is $2n-3$. By Proposition 7, there is a nonempty Zariski open subset U_2 of $\mathbb{A}_{\Bbbk}^{4\cdot n^2}$ such that for all $\boldsymbol{a} \in U_2$, the ideal $\varphi_{\boldsymbol{a}}(\mathcal{I}_{n-2}(\mathscr{A}))$ is Cohen Macaulay. Thus, taking $U = U_1 \cap U_2$, we obtain Item 1.

We turn to Item 2. By Proposition 14, Item 2, it suffices to show that the leading terms of the set S_1' computed on Line 4 consists of the elements of degree at most $2n-3$ of $\text{lt}_{\text{pot}}(\text{Syz}(\mathcal{I}_{n-2}(M)))$. This is immediate from Theorem 9 and Section 2.3.3. □

6. Complexity in the case $r = n-2$

Throughout this section we focus on the dimension zero case. Thus, $k = (n-r)^2 = 4$. For a homogeneous ideal $\mathcal{I} \subseteq \mathcal{R}$, we take $\text{HF}_{\mathcal{I}}(d)$ to be the *Hilbert*

function of $\mathcal{I}$. That is, for an integer $d \geq 0$, $\mathrm{HF}_{\mathcal{I}}(d) = \dim_{\Bbbk} \mathcal{I}_d$. Further, we take $H_{\mathcal{I}}(t) = \sum_d \mathrm{HF}_{\mathcal{I}}(d)t^d$ to be the *Hilbert series* of $\mathcal{I}$. We refer to [Eis95, 1.9] for further details.

When $r = n-2$, we can use the results of the previous section to give explicit formulae for the coefficients of the Hilbert series $H_{\mathcal{I}_r(M)}(t)$. Subsequently, we can exactly compute the ranks of the Macaulay matrices in each degree computed by the F_5 algorithm, and bound the complexity of computing the reduced grevlex Gröbner basis of a matrix of generic homogeneous linear forms by that of computing the row reduction of each of these matrices.

First, note that for any $1 \leq d \leq r$, both the number of rows and the number of columns of the Macaulay matrix in degree d for the set S_2 (resp. S_1) computed by Algorithm 3 is bounded by the number of rows of the Macaulay matrix in degree $d+1$ (resp. $d+r+1$) for the set S_1 (resp. $F_{n-2}(M)$). Thus, the arithmetic cost of Algorithm 3 is bounded by the arithmetic cost of the final step, computing the grevlex Gröbner basis for $F_{n-2}(M)$.

Proposition 23. There exists a Zariski open set $U \subseteq \mathbb{A}_{\Bbbk}^{4\cdot n^2}$ such that for all $\boldsymbol{a} \in U$, the Hilbert series $H_{\varphi_{\boldsymbol{a}}(\mathcal{I}_r(\mathscr{A}))}(t)$ for $\varphi_{\boldsymbol{a}}(\mathcal{I}_r(\mathscr{A}))$ is given by:

$$\sum_{d=r+1}^{2r+1} \left(n^2 \binom{d-r+2}{3} - (2n^2-2)\binom{d-r+1}{3} + n^2 \binom{d-r}{3} \right) t^d. \tag{5}$$

Proof. Let U be as in Proposition 22. If $\mathcal{M}$ is a free $\mathcal{R}$-module of rank t, then the monomials of $\mathcal{M}$ of degree d form a basis for the finite-dimensional $\Bbbk$-vector space of homogeneous elements of degree d of $\mathcal{M}$. Thus, $\mathrm{HF}_{\mathcal{M}}(d) = t \cdot \binom{k+d-1}{d-1}$. The description of each free module in the Gulliksen-Negård complex given in Section 3.1 gives rise to

$$\operatorname{rk} \mathcal{E}_0 = \#F_{n-2}(M) = \tbinom{n}{n-1}^2 = n^2, \quad \operatorname{rk} \mathcal{E}_1 = 2n^2 - 2$$
$$\operatorname{rk} \mathcal{E}_2 = n^2, \quad \operatorname{rk} \mathcal{E}_3 = 1$$

Thus, by [Eis95, Thm. 1.13], $\mathrm{HF}_{\mathcal{I}_{n-2}(M)}(d) = \sum_{i=0}^{3} (-1)^i \mathrm{HF}_{\mathcal{E}_i}(d)$, which equals $n^2\binom{d-r+2}{3} - (2n^2-2)\binom{d-r+1}{3} + n^2\binom{d-r}{3} - \binom{d-r-1}{3}$. □

In the following proposition, we take

$$\mathscr{B} = \sum_{d=r+1}^{2r+1} n^2 \binom{d-r+2}{3} - (2n^2-2)\binom{d-r+1}{3} + n^2 \binom{d-r}{3}.$$

Proposition 24. There is a Zariski dense subset U of $\mathbb{A}_{\Bbbk}^{4\cdot n^2}$ such that for all $\boldsymbol{a} \in U$, the arithmetic cost of computing the reduced grevlex Gröbner basis for $\varphi_{\boldsymbol{a}}(\mathcal{I}_{n-2}(\mathscr{A}))$ using Algorithm 3 is in

$$O\left(\mathscr{B}^{\omega-1}\tbinom{2r+5}{5}\right) = O\left(n^{4(\omega-1)}\tbinom{2n}{3}\right).$$

Proof. Take U as in Proposition 23. Fix $\boldsymbol{a} \in U$ and let $M = \varphi_{\boldsymbol{a}}(\mathcal{I}_{n-2}(\mathscr{A}))$. The ideal $\mathcal{I}_{n-2}(M)$ is homogeneous, so the complexity of computing a grevlex Gröbner basis for $\mathcal{I}_{n-2}(M)$ is bounded by the complexity of reducing the intermediate Macaulay matrices encountered in the matrix-F_5 algorithm. The coefficient on t^d in the Hilbert series Eq. (5) gives the rank of the Macaulay matrix of $F_r(M)$ in degree d. The Macaulay matrices computed in Algorithm 3 have full row rank, allowing for the use of any echelonization algorithm when computing $\bar{\mathscr{M}}_{d,i}$. Hence,

the result follows from the complexity of computing the reduced row echelon form [Sto00, Sec. 2.2] (see also [JPS13, App. A]) and the fact that the number of columns in the Macaulay matrix in degree $2n-3$, the maximal degree of a polynomial in the grevlex Gröbner basis of $\mathcal{I}_r(M)$, is the number of monomials of degree $2n-3$ in $\Bbbk[x_1,\ldots,x_4]$. □

Asymptotically, the bound given in [FSS13, Thm. 20] is in $O\left(n^{5\omega+2}\right)$ whereas that given by Proposition 24 is in $O\left(n^{4\omega-1}\right)$.

7. Experimental results

Here we present some experimental results on numbers of reductions to zero in our refinements of the F_5 algorithm compared to the standard F_5 algorithm. The systems used for these results were obtained by building square matrices of homogeneous linear forms with random coefficients over $\Bbbk = \mathbb{F}_{65521}$. This field is large enough that the genericity assumptions necessary for our results to hold do so with high probability when taking random coefficients.

All Gröbner basis computations were performed using an implementation of both standard F_5 and our refinements to F_5 written in SageMath (see [The22]) using the FFLAS-FFPACK library (see [gro19]) for the linear algebra subroutines. When $r = n-2$, we compute a full Gröbner basis for $F_{n-2}(M)$, whereas when $r < n-2$, we only compute a Gröbner basis of $F_r(M)$ up to degree $r+2$, as past this degree our algorithm performs no differently to standard F_5.

When $r = n-2$, all reductions to zero are avoided and thus all Macaulay matrices are full rank. By virtue of Proposition 4, if a row of $\mathscr{M}_{d,i}$ reduces to zero, then all multiples of this row in $\mathscr{M}_{d',i}$ for $d' > d$ reduce to zero as well, and the standard F_5 algorithm avoids these rows. Note however, that there are a significant number of reductions to zero which do not arise from reductions to zero in lower degree, as evidenced by the discrepancy between the size of the generating set for $\mathrm{Syz}(F_{n-2}(M))$, which is $2n^2-2$ (when $r = n-2$) and the number of reductions to zero encountered by the standard F_5 algorithm.

Note also that by [FSS13, Cor. 19], the largest degree of a polynomial in the reduced grevlex Gröbner basis for $\mathcal{I}_{n-2}(M)$ is $2n-3$, which is strictly smaller than $2(r+1) = 2n-2$. Thus, Proposition 5 is never used when running either the standard F_5 algorithm, or our refined algorithm on $\mathcal{I}_{n-2}(M)$.

When $r < n-2$, we avoid all reductions to zero in the Macaulay matrices $\mathscr{M}_{r+2,i}$ for all $1 \leq i \leq \binom{n}{r+1}^2$. As the data in Table 1 shows, this already allows us to avoid a significant number of reductions to zero. In fact, in all higher corank cases, over half of the reductions to zero overall appear in degree $r+2$. The number of reductions to zero in degree $r+2$ (and thus the size of a minimal generating set for $\mathrm{Syz}(\mathcal{I}_r(M))$) appears to be

$$\binom{n}{r+2}^2 \left(\frac{2(r+2)(r+1)}{n-r-1} + 2r + 2\right).$$

From this quantity one could derive a refined estimate of the complexity of Algorithm 2.

Note that generically, in the case $r < n-2$, the largest degree of a polynomial appearing in the reduced grevlex Gröbner basis for $\mathcal{I}_r(M)$ is $r \cdot (n-r) + 1$ again by [FSS13, Cor. 19]. Thus, in this case, Proposition 5 is used as soon as the degree exceeds $2(r+1)$.

Finally, we observe that the speedups which can already be achieved using the results of this paper, within our software framework, increase when n grows and $n-r$ remains fixed. In the case where $n-r=2$ we obtain speedup which are close to 10. This clearly indicates the potential of these results with respect to practical computation times.

TABLE 1. Reductions to zero in standard F_5 (there is none in determinantal-F_5) as well as ratio of timings for standard F_5 compared to determinantal-F_5, when computing a D-Gröbner basis for the system of $(r+1)$-minors of a generic $n \times n$ matrix of homogeneous linear forms in k variables over $\Bbbk = \mathbb{F}_{65521}$.

n	r	k	D	Red. to 0 (Std. F_5)	$\frac{\text{(Std. } F_5\text{)}}{\text{(Det. } F_5\text{)}}$
4	2	4	5	56	0.11
5	3	4	7	129	0.08
6	4	4	9	239	0.43
7	5	4	11	414	0.69
8	6	4	13	663	1.46
9	7	4	15	959	1.65
10	8	4	17	1387	2.26
11	9	4	19	1871	3.07
12	10	4	21	2525	3.99
13	11	4	23	3181	4.94
14	12	4	25	4032	6.00
15	13	4	27	4977	6.03
16	14	4	29	6213	7.93
17	15	4	31	7515	7.22
18	16	4	33	8845	7.99
19	17	4	35	10544	8.65
20	18	4	37	12969	10.59
4	1	9	3	160	1.27
5	2	9	4	450	1.77
6	3	9	5	1008	2.04
7	4	9	6	1960	2.16
8	5	9	7	3456	2.40
9	6	9	8	5670	2.50
5	1	16	3	800	1.34
6	2	16	4	3150	1.59
7	3	16	5	9408	1.72
6	1	25	3	2800	1.28
7	2	25	4	14700	1.39
7	1	36	3	7840	1.22

ACKNOWLEDGEMENTS

The authors are supported by *Quantum Information Center Sorbonne* (QICS); by the Agence nationale de la recherche (ANR), grant agreements ANR-19-CE40-0018 DE RERUM NATURA and ANR-18-CE33-0011 SESAME projects; by the

joint ANR-Austrian Science Fund FWF projects ANR-22-CE91-0007 EAGLES and ANR-FWF ANR-19-CE48-0015 ECARP; and by the EOARD-AFOSR, grant agreement FA8665-20-1-7029.

References

[ABW81] K. Akin, D. A. Buchsbaum, and J. Weyman. Resolutions of determinantal ideals: The submaximal minors. *Advances in Mathematics*, 39(1):1–30, 1981.

[BBB+20] M. Bardet, P. Briaud, M. Bros, P. Gaborit, V. Neiger, O. Ruatta, and J.-P. Tillich. An algebraic attack on rank metric code-based cryptosystems. In *Proceedings EUROCRYPT 2020*, volume 12105 of *LNCS*. Springer, 2020.

[BBC+20] M. Bardet, M. Bros, D. Cabarcas, P. Gaborit, R. Perlner, D. Smith-Tone, J.-P. Tillich, and J. Verbel. Improvements of algebraic attacks for solving the rank decoding and minrank problems. In *Proceedings ASIACRYPT 2020*, pages 507–536, 2020.

[BBC+22] J. Baena, P. Briaud, D. Cabarcas, R. Perlner, D. Smith-Tone, and J. Verbel. Improving Support-Minors Rank Attacks: Applications to GeMSS and Rainbow. In *Proceedings CRYPTO 2022*, pages 376–405, Cham, 2022. Springer.

[BCRV22] W. Bruns, A. Conca, C. Raicu, and M. Varbaro. *Determinants, Gröbner bases and cohomology*. Springer, 2022.

[BESED22] J. Berthomieu, C. Eder, and M. Safey El Din. New efficient algorithms for computing Gröbner bases of saturation ideals (F4SAT) and colon ideals (Sparse-FGLM-colon). Working paper, 2022.

[Beu22] W. Beullens. Breaking rainbow takes a weekend on a laptop. In *Proceedings CRYPTO 2022*, pages 464–479. Springer, 2022.

[BFS99] J. F. Buss, G. S. Frandsen, and J. O. Shallit. The computational complexity of some problems of linear algebra. *J. Comput. Syst. Sci.*, 58(3):572–596, 1999.

[BFS15] M. Bardet, J.-C. Faugère, and B. Salvy. On the complexity of the F5 Gröbner basis algorithm. *J. Symbolic Comput.*, 70:49–70, 2015.

[BFSS13] M. Bardet, J.-C. Faugère, B. Salvy, and P.-J. Spaenlehauer. On the complexity of solving quadratic boolean systems. *J. Complexity*, 29(1):53–75, 2013.

[BGH+10] B. Bank, M. Giusti, J. Heintz, M. Safey El Din, and É. Schost. On the geometry of polar varieties. *Appl. Algebra Engrg. Comm. Comput.*, 21(1):33–83, 2010.

[BGHP05] B. Bank, M. Giusti, J. Heintz, and L. M. Pardo. Generalized polar varieties: Geometry and algorithms. *J. Complexity*, 21(4):377–412, 2005.

[BGHS14] B. Bank, M. Giusti, J. Heintz, and M. Safey El Din. Intrinsic complexity estimates in polynomial optimization. *J. Complexity*, 30(4):430–443, 2014.

[BS15] I. Bannwarth and M. Safey El Din. Probabilistic algorithm for computing the dimension of real algebraic sets. In *Proceedings ISSAC 2015*, pages 37–44. ACM, 2015.

[Buc65] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. PhD thesis, University of Innsbruck, 1965.

[BV88] W. Bruns and U. Vetter. *Determinantal Rings*. Springer Berlin Heidelberg, 1988.

[CLO15] D. A. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms (fourth edition)*. Springer, 2015.

[Cou01] N. T. Courtois. Efficient zero-knowledge authentication based on a linear algebra problem MinRank. In *Proceedings ASIACRYPT 2001*, pages 402–421. Springer, 2001.

[DS05] J. Ding and D. Schmidt. Rainbow, a new multivariable polynomial signature scheme. In *Proceedings ACNS 2005*, pages 164–175. Springer, 2005.

[EF16] C. Eder and J.-C. Faugère. A survey on signature-based algorithms for computing Gröbner basis computations. *J. Symbolic Comput.*, pages 1–75, 2016.

[Eis95] D. Eisenbud. *Commutative Algebra: with a View Toward Algebraic Geometry*. Graduate Texts in Mathematics. Springer, 1995.

[Eis05] D. Eisenbud. *The geometry of syzygies: A second course in commutative algebra and algebraic geometry*, volume 229. Springer, 2005.

[EN62] J. A. Eagon and D. G. Northcott. Ideals defined by matrices and a certain complex associated with them. *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences*, 269(1337):188–204, 1962.

[Fau99] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases (f4). *J. Pure Appl. Algebra*, 139(1):61–88, 1999.

[Fau02] J.-C. Faugère. A new efficient algorithm for computing gröbner bases without reduction to zero (f5). In *Proceedings ISSAC 2002*, pages 75–83. ACM, 2002.

[FLP08] J.-C. Faugère, F. Levy-dit-Vehel, and L. Perret. Cryptanalysis of MinRank. In *Proceedings CRYPTO 2008*, pages 280–296. Springer, 2008.

[FSS10] 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 ISSAC 2010*, pages 257–264, 2010.

[FSS12] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. Critical points and Gröbner bases: the unmixed case. In *Proceedings ISSAC 2012*, pages 162–169. ACM, 2012.

[FSS13] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. On the complexity of the generalized MinRank problem. *J. Symbolic Comput.*, 55:30–58, 2013.

[Giu84] M. Giusti. Some effectivity problems in polynomial ideal theory. In *Proceedings EUROSAM 84*, pages 159–171. Springer, 1984.

[GN72] T. H. Gulliksen and O. G. Negård. Un complexe résolvant pour certains idéaux déterminantiels. *C. R. Acad. Sci. Paris*, 274:16–18, 1972.

[gro19] The FFLAS-FFPACK group. *FFLAS-FFPACK: Finite Field Linear Algebra Subroutines / Package*, v2.4.1 edition, 2019. `http://github.com/linbox-team/fflas-ffpack`.

[GSED14] A. Greuet and M. Safey El Din. Probabilistic algorithm for polynomial optimization over a real algebraic set. *SIAM J. Optim.*, 24(3):1313–1343, 2014.

[HS09] H. Hong and M. Safey El Din. Variant real quantifier elimination: algorithm and application. In *Proceedings ISSAC 2009*, pages 183–190, 2009.

[HS12] H. Hong and M. Safey El Din. Variant quantifier elimination. *J. Symbolic Comput.*, 47(7):883–901, 2012.

[HSEDSV21] J. D. Hauenstein, M. Safey El Din, É. Schost, and T. X. Vu. Solving determinantal systems using homotopy techniques. *J. Symbolic Comput.*, 104:754–804, 2021.

[JPS13] C.-P. Jeannerod, C. Pernet, and A. Storjohann. Rank-profile revealing Gaussian elimination and the CUP matrix decomposition. *J. Symbolic Comput.*, 56:46–68, 2013.

[KS99] A. Kipnis and A. Shamir. Cryptanalysis of the HFE public key cryptosystem by relinearization. In *Proceedings CRYPTO 1999*, pages 19–30. Springer, 1999.

[Kur89] K. Kurano. The first syzygies of determinantal ideals. *J. Algebra*, 124(2):414–436, 1989.

[Las78] A. Lascoux. Syzygies des variétés déterminantales. *Adv. Math*, 30(3):202–237, 1978.

[Laz83] D. Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In *Proceedings EUROSAM 83*, pages 146–156. Springer, 1983.

[LS21a] P. Lairez and M. Safey El Din. Computing the dimension of real algebraic sets. In *Proceedings ISSAC 2021*, pages 257–264. ACM, 2021.

[LS21b] H. P. Le and M. Safey El Din. Faster one block quantifier elimination for regular polynomial systems of equations. In *Proceedings ISSAC 2021*, pages 265–272, 2021.

[LSSV21] G. Labahn, M. Safey El Din, É. Schost, and T. X. Vu. Homotopy techniques for solving sparse column support determinantal polynomial systems. *J. Complexity*, 66:101557, 2021.

[Ma94] Y. Ma. On the minors defined by a generic matrix. *J. Symbolic Comput.*, 18(6):503–518, 1994.

[Pat96] J. Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. In *Proceedings EUROCRYPT 1996*, pages 33–48. Springer, 1996.

[Spa14] P.-J. Spaenlehauer. On the complexity of computing critical points with Gröbner bases. *SIAM J. Optim.*, 24(3):1382–1401, 2014.

[SS03] 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 ISSAC 2003*, pages 224–231. ACM, 2003.

[SS17] M. Safey El Din and É. Schost. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. *J. ACM*, 63(6), jan 2017.

[Sto00] A. Storjohann. *Algorithms for Matrix Canonical Forms*. PhD thesis, Swiss Federal Institute of Technology – ETH, 2000.

[The22] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.8.beta6)*, 2022. `https://www.sagemath.org`.