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, Sorbonne Université, CNRS, LIP6, France
VINCENT NEIGER, Sorbonne Université, CNRS, LIP6, France
MOHAB SAFEY EL DIN, Sorbonne Université, CNRS, LIP6, France

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* [16], and its variants where M may be rectangular, lies at the heart of multivariate cryptography. It is at the foundations of several schemes [17, 37, 45] and is still used to assess the security of encryption and signature schemes [2, 7, 8, 12, 19, 26].

Determinantal ideals also arise in fundamental areas such as effective real algebraic geometry as they encode critical points (see e.g. [28, 48]), then used to solve a variety of problems. This includes polynomial optimization [4, 31], computing sample points and answering connectivity queries in smooth real algebraic sets [3, 5, 46] [47], determining the dimension of real algebraic sets [6, 40], and quantifier elimination over the reals [34, 35, 43].

Determinantal ideals and polynomial system solving. Determinantal ideals enjoy plenty of combinatorial and algebraic properties [13, 14, 41] 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 [33] which has next been refined to take into account specific structures when the entries of the matrix M are sparse [39].

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 [15], 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 the Faugère's celebrated F_4 algorithm [24], which also made explicit the use of linear algebra subroutines in Gröbner bases algorithms.

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.

While a lot remains to be done in this direction (see e.g. [11]), much attention has focused on issue *(ii)* and variants of Faugère's F_5 algorithm [25] have been developed in several directions to give rise to signature-based Gröbner bases algorithms (see [21] and references therein). One byproduct of these works, which finds its roots in foundational works by Lazard and Giusti [30, 42], 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 [18, Chap. 9, §3]).

This has been developed, in the context of determinantal ideals, by the series of works [27, 29], 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 [9] shows significant improvements against such coarse estimates.

In the context of determinantal ideals, mimicking this to get better complexity estimates is a premature gait. 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 [10]. 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 [21] 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 2.7), allowing us to leverage reductions to zero in lower degrees to avoid reductions to zero in subsequent degrees.

Next, we turn to genericity: 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 a complex of free modules, called 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.

Main results. We fix throughout $k = (n-r)^2$, which, by [29, Thm. 10], guarantees that $\mathcal{I}_r(M)$ has dimension zero.

By tracing basis elements for the free modules which make up the complex of Gulliksen and Negård, we are able, in Theorem 3.2, 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. A result from [38] 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, under some genericity assumptions. Thus, the problem of computing a generating set for $\mathrm{Syz}(\mathcal{I}_r(M))$ reduces to computing one for $\mathrm{Syz}(\mathcal{I}_{n-2}(M))$.

Therefore, combining the complex of Gulliksen and Negård with the result of [38], we are able to explicitly compute a full generating set for $\mathrm{Syz}(F_r(M))$, and subsequently provide Algorithm 4, 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 5.1, we give explicit generators for the second syzygy module of $\mathcal{I}_{n-2}(M)$. This study culminates in Algorithm 6 which is an altered version of matrix-F_5 which avoids all reductions to zero. Finally, in Proposition 6.1, 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. In Proposition 6.2, 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 in which we compare the ranks of the matrices computed by F_5 to the number of rows in the matrices computed by both F_5 and our new algorithm. When $r = n-2$, this experimental data confirms that we remove all reductions to zero. When $r < n-2$, it confirms that we avoid all reductions to zero arising from the minimal generating set for the first syzygy module of $F_r(M)$, of which there are many.

With knowledge of the higher syzygy modules of $\mathcal{I}_r(M)$, we could apply the same principle as we do in the case $r = n-2$ and compute elements of $\mathrm{Syz}(F_r(M))$ in higher degrees, thereby avoiding more of the reductions to zero present in Table 1.

Perspectives. In [44], 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 [14, 2.C] and [20]) provides a free resolution of $\mathcal{I}_r(M)$. Similarly, when $r = \min(n,m) - 2$, the Akin-Buschbaum-Weyman complex (see [1]) 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 [41]), 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 [22] 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. Having chosen a set of

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 2.1 ([23, Thm. A.2.49]). *If $(f_1, \ldots, f_\ell)$ is a regular sequence, then* $\mathrm{Syz}(F) = \left\langle f_i e_j - f_j e_i : 1 \leq i, j \leq \ell, i \neq j \right\rangle$ *where e_i is i-th standard basis vector. Furthermore,* $\mathrm{Syz}_2(F) = \{0\}$.

Thus, in that case, all syzygy modules of order ≥ 2 are trivial.

Example 2.2. Let $(f, g) \subseteq \mathcal{R}$ be a regular sequence. By definition, g is not a zero-divisor in $\mathcal{R}/\langle f\rangle$. In other words, for all $h \in \mathcal{R}$, if $hg \in \langle f\rangle$, then $h \in \langle f\rangle$. Suppose now that $s_1, s_2 \in \mathcal{R}$ are such that $s_1 f + s_2 g = 0$. Then $s_1 f = -s_2 g$, so $s_2 g \in \langle f\rangle$ and thus $s_2 \in \langle f\rangle$. We can therefore write $s_2 = pf$ for some $p \in \mathcal{R}$. Subsequently, we obtain $(s_1 + pg)f = 0$. Since $\mathcal{R}$ is a domain and $f \neq 0$, $s_1 = -pg$. This shows that $(s_1, s_2) = p(-g, f)$. Thus, any syzygy is generated by a Koszul syzygy. □

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

Example 2.3. Take $n = 3$ and $r = 1$, so that $M = (f_{i,j})_{1 \leq i,j \leq 3}$. Replacing the third row with the second row yields a matrix with determinant zero. Therefore, the Laplace expansion formula gives

$$f_{21}(f_{12}f_{23} - f_{13}f_{22}) - f_{22}(f_{11}f_{23} - f_{13}f_{21}) + f_{23}(f_{11}f_{22} - f_{12}f_{21}) = 0$$

This corresponds to a syzygy between the minors of M. To see that the corresponding syzygy is not Koszul, note that the degree of the syzygy is one, whereas since each minor has degree $r + 1 = 2$, the Koszul syzygies must all have degree at least two. □

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 m is called the *length* of $\mathcal{E}_\bullet$. In general, modules need not have finite free resolutions; however, it is the case for modules over $\mathcal{R} = \Bbbk[x_1, \ldots, x_k]$:

Theorem 2.4 (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.

Let us now recall the classical relationship between free resolutions and syzygy modules.

Proposition 2.5. *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 2.5, 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 $1 \leq j \leq m$.

Example 2.6. Let $(f, g) \subseteq \mathcal{R}$ be a regular sequence and $\mathcal{I} = \langle f, g \rangle$. We can take $\mathcal{E}_0 = \mathcal{R}^2$ and $\epsilon : (q_1, q_2) \in \mathcal{E}_0 \mapsto q_1 f + q_2 g \in \mathcal{I}$, whose matrix is $\begin{pmatrix} f & g \end{pmatrix}$. As seen in Example 2.2, $\mathrm{Syz}(\mathcal{I}) = \langle (-g, f) \rangle$. Thus, we can take $\mathcal{E}_1 = \mathcal{R}$ and continue to construct a free resolution as

$$\mathcal{E}_1 \xrightarrow{\begin{pmatrix} g \\ -f \end{pmatrix}} \mathcal{E}_0 \xrightarrow{\begin{pmatrix} f & g \end{pmatrix}} \mathcal{I} \to 0.$$

If $h \in \mathcal{E}_1$, then $\begin{pmatrix} g \\ -f \end{pmatrix} h = \begin{pmatrix} gh \\ -fh \end{pmatrix}$ and if $gh = -fh = 0$, then $h = 0$ since g and f are both nonzero. This shows $\ker(d_1) = \{0\}$, and so our free resolution can be completed by taking $\mathcal{E}_3 = \{0\}$. That is,

$$0 \to \mathcal{E}_1 \xrightarrow{\begin{pmatrix} g \\ -f \end{pmatrix}} \mathcal{E}_0 \xrightarrow{\begin{pmatrix} f & g \end{pmatrix}} \mathcal{I} \to 0$$

is a free resolution of $\mathcal{I}$. □

2.3 The matrix-F$_5$ algorithm

The matrix-F_5 algorithm [9] is based on F_5 [25]. 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. Let $F = (f_1, \ldots, f_\ell) \subseteq \mathcal{R}^t$ be a set homogeneous elements of $\mathcal{R}^t$. 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 $\bar{\mathscr{M}}_{d,i}$ for $1 \leq i \leq \ell$

and $d_1 \leq d \leq D$. 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 the $m_1, \ldots, m_\ell$, 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 2.7 (Syzygy Criterion, [21, Lem. 6.4]). *Let $s = (s_1, \ldots, s_\ell)$ be a homogeneous syzygy of $m_1, \ldots, m_\ell$. Let $(i, \tau) = \mathrm{lt}_{\mathrm{pot}}(s)$. Then*

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

Proof. We have $\tau m_i = \sum_{j \neq i} s_j m_j - m_i(s_i - \mathrm{lt}_{\mathrm{pot}}(s))$. The module element τm_i corresponds to the row of $\mathscr{M}_{\deg \tau + d_i}$ with signature (i, τ), while $\sum_{j \neq i} s_j m_j - m_i(s_i - \mathrm{lt}_{\mathrm{pot}}(s))$ 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 $\bar{\mathscr{M}}_{d,i}$ is a zero row. Then the polynomial τf_i is a $\Bbbk$-linear combination of rows of $\mathscr{M}_{d,i}$ with smaller signature, i.e.,

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

As a consequence, for any monomial σ in $\mathcal{R}$, we can write $\sigma \tau f_i = \sum_{(i', \tau') \prec_{\mathrm{sig}} (i, \tau)} c_{i', \tau'} \sigma \tau' f_{i'}$, which shows that the row with signature $(i, \sigma\tau)$ of $\mathscr{M}_{\deg(\tau) + \deg(\sigma), i}$ is a $\Bbbk$-linear combination of rows with smaller signature. This proves Item 2 □

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 Koszul 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, the matrix-F_5 algorithm utilizes the following criterion, which is a specialization of Proposition 2.7.

Proposition 2.8 (F_5 Criterion, [25, Thm. 1]). *The rows with signature (i, t) of $\mathscr{M}_{d,i}$ reduce to zero in $\bar{\mathscr{M}}_{d,i}$, for all $t \in \mathrm{lt}(\bar{\mathscr{M}}_{d - d_i, i-1})$.*

2.3.3 The matrix-F_5 algorithm. When $t = 1$, combining the syzygy criterion with Proposition 2.8 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 given in [9] by integrating Item 2 of Proposition 2.7. This is important in our context since, as we will see further, this criterion allows us to avoid a significant number of reductions to zero that would occur without it. Further, we allow for the input of precomputed syzygies of F in order to exploit Proposition 2.7 and we allow $t \geq 1$.

Proposition 2.9. *Algorithm 1 terminates and is correct.*

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 $i \in \{1, \ldots, m\}$ **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 $\cup \{(i, \tau)\}$
      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

Proof. When $t = 1$, this is simply [9, Thm. 9]. When $t > 1$, the same induction argument works. □

2.4 Genericity

In this section, we take notation from [29, 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 $\boldsymbol{a} = (a_t^{(i,j)}) \in \bar{\Bbbk}^{k \cdot n^2}$, 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 *property*, a map

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

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 $\mathbb{A}_{\Bbbk}^{k \cdot \binom{n}{r+1}^2}$ such that for all $\boldsymbol{a} \in U$, $\varphi_{\boldsymbol{a}}(\mathcal{I}_r(\mathscr{A})) = \mathtt{true}$.

An important property which we will make frequent reference to in the following sections is the notion of Cohen-Macaulayness. Let $\mathcal{I}$ be an ideal of $\mathcal{R}$. A sequence of polynomials $(f_1, \ldots, f_\ell) \subseteq \mathcal{R}$ 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 $\ell = \dim(\mathcal{I})$ ($\dim(\mathcal{I})$ is the Krull dimension of $\mathcal{I}$ in $\mathcal{R}$).

Remark 2.10. If $(f_1, \ldots, f_\ell)$ is an $\mathcal{I}$-regular sequence, then necessarily $\ell \leq \dim(\mathcal{I})$. The notion of Cohen-Macaulayness can therefore be understood as requiring that there exists an $\mathcal{I}$-regular sequence of maximal possible length in $\mathcal{R}$.

Proposition 2.11. *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 $I_r(\mathscr{A})$-generic.*

Proof. Let $U = (u_{i,j})$ be an $n \times n$ matrix of indeterminates over $\Bbbk$. By [14, Thm. 2.5], $I_r(U)$ is Cohen-Macaulay. Subsequently, we may use [29, Lem. 3] to conclude. □

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 $(r+2) \times (r+2)$ [38, 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 [14, 32] is a free resolution of $I_{n-2}(M)$. We will exploit this complex to obtain $\mathrm{Syz}(F_r(M))$ first when $r = n-2$, then in full generality. We conclude this section with an algorithm which returns a generating set for $\mathrm{Syz}(F_r(M))$ for any r and n.

3.1 The Gulliksen-Negård complex

The Gulliksen-Negård complex is a free resolution of $I_{n-2}(M)$,

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

As such, we can use Proposition 2.5 to compute the first syzygy module of the set of generators $F_{n-2}(M)$ as the kernel of the augmentation map of this complex. We recall the construction of the complex here; details and proofs can be found in [14, 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 $I_{n-2}(M)$ 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, $\mathrm{im}(\iota)$ is generated by

$$(I_n, I_n) = (E_{1,1}, E_{1,1}) + \sum_{i=2}^{n}(E_{i,i}, E_{1,1}) + \sum_{i=2}^{n}(0, E_{i,i} - E_{1,1}).$$

This shows that $\mathcal{E}_1 = \ker(\pi)/\mathrm{im}(\iota)$ 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:

- $\epsilon : \mathcal{E}_0 \to \mathcal{I}_{n-2}(M), \quad N \mapsto \mathrm{tr}(M^*N)$,
- $d_1 : \mathcal{E}_1 \to \mathcal{E}_0, \quad \overline{(N_1, N_2)} \mapsto N_1M - MN_2$,
- $d_2 : \mathcal{E}_2 \to \mathcal{E}_1, \quad N \mapsto \overline{(MN, NM)}$, 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 3.1. *Let M be a matrix of homogeneous linear forms in four variables. 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. The condition that $\mathcal{I}_{n-2}(M)$ is Cohen-Macaulay means that there exists an $\mathcal{I}_{n-2}(M)$-regular sequence of length equal to the Krull dimension of $\mathcal{I}_{n-2}(M)$ in $\mathcal{R}$. By [29, Thm. 10] and Proposition 2.11, the Krull dimension of $\mathcal{I}_{n-2}(M)$ is exactly 4. Therefore, the result follows immediately from [14, Thm. 2.26]. □

3.2 The case $r = n - 2$

We begin by giving generators for the first syzygy module in the case $r = n - 2$, assuming $\mathcal{I}_{n-2}(M)$ is Cohen-Macaulay. In particular, we prove the following theorem.

Theorem 3.2. *Let $M = (m_{i,j})$ be a matrix of homogeneous linear forms in four variables. Suppose that $\mathcal{I}_{n-2}(M)$ is Cohen-Macaulay. Then the first syzygy module of $F_{n-2}(M)$ is generated by:*

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

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

Proof. This is a straightforward computation. Using Proposition 2.5, $\ker(\epsilon)$ is the first syzygy module of the cofactors of M. By Proposition 3.1, since we assume that $\mathcal{I}_{n-2}(M)$ is Cohen-Macaulay, the Gulliksen-Negård complex is exact. In particular, $\ker(\epsilon) = \mathrm{im}(d_1)$. The image $\mathrm{im}(d_1)$ is generated by the images of generators for $\mathcal{E}_1$ under d_1. Thus, following Section 3.1, the first syzygy module of $F_{n-2}(M)$ is generated by the following syzygies. For $i \neq j$,

$$d_1\left(\overline{(E_{i,j}, 0)}\right) = E_{i,j}M = \sum_{k=1}^{n} m_{k,i}E_{k,j}. \tag{1}$$

Similarly, for $i \neq j$,

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

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

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

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

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

Finally, 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 Item (i), Item (ii), Item (iii), Item (iv) by pulling back each of Eq. (1), Eq. (2), Eq. (3), Eq. (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 sequence of polynomials $a_1, \ldots, a_{2n^2-2} \in \mathcal{R}$,

$$a_1m_1 + \cdots + \cdots + a_{2n^2-2}m_{2n^2-2} = 0. \tag{5}$$

For each $1 \leq j \leq 2n^2 - 2$, the coefficients a_j lie in $\Bbbk$ since the m_i's are all homogeneous. By Proposition 3.1, the Gulliksen-Negård complex is exact. Eq. (5) corresponds therefore to an element

$$(a_1, \ldots, a_{2n^2-2}) \in \mathrm{im}(d_2) \cap \Bbbk^{2n^2-2}.$$

Letting $N \in d_2^{-1}((a_1, \ldots, a_{2n^2-2}))$, we find that $MN, NM \in \mathcal{M}_n(\mathcal{R})$ are both matrices with entries purely in $\Bbbk$. For each $1 \leq i \leq n$, the entries of the i-th row of MN are members of the ideal generated by the i-th row of M. The entries of M are homogeneous linear forms, so the only constant element that they contain is 0. Similarly, for each $1 \leq i \leq n$, the entries of the i-th row of NM are members of the ideal generated by the i-th column of M, and an analogous argument applies. Thus, $a_j = 0$ for each $1 \leq j \leq 2n^2 - 2$. □

Theorem 3.2 directly leads to Algorithm 2.

Proposition 3.3. *Algorithm 2 terminates and is correct.*

Proof. The loop on Line 3 constructs the syzygies corresponding to (1) and (2) in Theorem 3.2. Indeed, upon the conclusion of the loop on Line 11, the tuple s (resp. t) instantiated on Line 4 exactly becomes the syzygy (1) (resp. (2)).

Similarly, the loop on Line 9 corresponds to (3) in Theorem 3.2 and the loop on Line 16 corresponds to (4) in Theorem 3.2. Termination is clear. □

Remark 3.4. In both Theorem 3.2 and Algorithm 2 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

Algorithm 2 SyzGenCorankOne

Input: An integer $n \geq 3$ and an $n \times n$ matrix $M = (m_{i,j})$ of homogeneous linear forms in $\mathcal{R}$ such that $\mathcal{I}_{n-2}(M)$ is Cohen-Macaulay.

Output: A minimal generating set for $\mathrm{Syz}(F_{n-2}(M))$.

$S \leftarrow \emptyset$ ▷ *to be filled with the output generating set*
▷ *handle syzygies from Items (i) and (ii) of Theorem 3.2*
for $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, n\}$ such that $i \neq j$ **do**
  $s \leftarrow \mathbf{0} \in \mathcal{R}^{n^2}$; $t \leftarrow \mathbf{0} \in \mathcal{R}^{n^2}$
  for $k \in \{1, \ldots, n\}$ **do**
    $s_{n\cdot(k-1)+j} \leftarrow (-1)^{k+j} m_{k,i}$; $t_{n\cdot(i-1)+k} \leftarrow (-1)^{k+i} m_{j,k}$
  $S \leftarrow S \cup \{s, t\}$
▷ *handle syzygies from Item (iii) of Theorem 3.2*
for $i \in \{1, \ldots, n-1\}$ **do**
  $s \leftarrow \mathbf{0} \in \mathcal{R}^{n^2}$
  for $k \in \{1, \ldots, n\}$ **do**
    $s_{n\cdot(k-1)+i} \leftarrow s_{n\cdot(k-1)+i} + (-1)^{k+i} m_{k,i}$
    $s_k \leftarrow s_k - (-1)^{k+1} m_{1,k}$
  $S \leftarrow S \cup \{s\}$
▷ *handle syzygies from Item (iv) of Theorem 3.2*
for $i \in \{2, \ldots, n\}$ **do**
  $s \leftarrow \mathbf{0} \in \mathcal{R}^{n^2}$
  for $k \in \{1, \ldots, n\}$ **do**
    $s_{n\cdot(i-1)+k} \leftarrow s_{n\cdot(i-1)+k} + (-1)^{i+k} m_{i,k}$
    $s_k \leftarrow s_k - (-1)^{k+1} m_{1,k}$
  $S \leftarrow S \cup \{s\}$
return S

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 3.2 describes (and subsequently Algorithm 2 computes) a generating set for a submodule of $\mathrm{Syz}(F_{n-2}(M))$.

Remark 3.5. In Theorem 3.2, we require that the entries of M are homogeneous. However, as long as the ideal $\mathcal{I}_{n-2}(M)$ is Cohen-Macaulay, the entries of M may be taken to be affine without issue.

Example 3.6. Let $n = 3$ and $r = 1$ and M as in Example 2.3. We construct the syzygy described by (1) of Theorem 3.2 for $i = 1$, $j = 2$. This syzygy takes the form

$$-f_{1,1}E_{1,2} + f_{2,1}E_{2,2} - f_{3,1}E_{3,2}. \tag{6}$$

The basis element $E_{u,v}$ maps under ϵ to the minor of M obtained by computing the determinant of the submatrix of M given by deleting the u-th row and v-th column. Thus, Eq. (6) is simply the syzygy obtained by replacing the second column of M by the first one, then computing the determinant of this (now singular) matrix via the Laplace expansion around the second column.

Similarly, for some choice of $i \neq j$, (2) of Theorem 3.2 corresponds to computing via Laplace expansion the determinant of the singular matrix obtained by replacing row j by row i.

For $i = 1$, we next construct the syzygy described by (3) of Theorem 3.2. This takes the form

$$-f_{2,1}E_{2,1} + f_{1,2}E_{1,2} + f_{3,1}E_{3,1} - f_{1,3}E_{1,3} \tag{7}$$

Once again we can map each basis element of this syzygy to its corresponding minor under ϵ. In this way, Eq. (7) is obtained by computing the determinant of M via the Laplace expansion with respect to the first row and again with respect to the first column, and setting these equal to one another. □

3.3 The general case

THEOREM 3.7. *Let $n \geq 3$ and let $1 \leq r \leq n-2$. Let $k = (n-r)^2$. Then there exists a nonempty Zariski open set $U \subseteq \mathbb{A}_{\Bbbk}^{k\cdot\binom{n}{r+1}^2}$ 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 3.2. Then* $\operatorname{Syz}(F_r(M)) = \bigcup_{N\in M'} S(N)$.

PROOF. Let U be an $n \times n$ matrix of indeterminates over $\Bbbk$. Let U' be the set of $(r+2)\times(r+2)$ submatrices of U. For each $N \in U'$, let $S(N) = \operatorname{Syz}(F_r(N))$. By [38, Thm. 5.1], $\operatorname{Syz}(F_r(\mathscr{A})) = \bigcup_{N\in M'} S(N)$. Thus, by [29, Lem. 3], there is a nonempty Zariski open subset $U_1 \subseteq \mathbb{A}_{\Bbbk}^{k\cdot\binom{n}{r+1}^2}$ 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 $\varphi_{\boldsymbol{a}}(\mathscr{A})$. By Proposition 2.11, for each $(r+2)\times(r+2)$ 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. Thus, taking $U = \bigcap_N N \cap U_1$, the result follows. □

As a result of Theorem 3.7, and using Algorithm 2, we obtain Algorithm 3 which constructs a set of generators for $\operatorname{Syz}(F_r(M))$.

Algorithm 3 SyzGen

Input: An integer $n \geq 3$, an integer $1 \leq r \leq n-2$, and an $n \times n$ matrix of linear forms over $\Bbbk$.
Output: A minimal generating set for $\operatorname{Syz}(F_r(M))$.

1: $S \leftarrow \emptyset$
2: $P \leftarrow (r+2)$-element subsets of $[n]$
3: **for** $R \in P$ **do**
4: **for** $C \in P$ **do**
5: $M' \leftarrow$ submatrix of M with rows indexed by R and columns indexed by C
6: $L \leftarrow \mathbf{0} \in \mathcal{R}^{(r+2)^2}$
7: **for** $i \in [(r+2)^2]$ **do**
8: $L_i \leftarrow$ index of $(F_r(M'))_i$ in $F_r(M)$
9: **for** $s \in \text{SyzGenCorankOne}(M')$ **do**
10: $s' \leftarrow \mathbf{0} \in \mathcal{R}^{\binom{n}{r+1}^2}$
11: **for** $i \in [\binom{n}{r+1}^2]$ **do**
12: $s'_{L_i} \leftarrow s_i$
13: $S \leftarrow S \cup \{s'\}$
14: **return** S

PROPOSITION 3.8. *Algorithm 3 terminates and is correct.*

PROOF. Line 2 defines P to be the set of $(r+2)$ element subsets of the set $\{1,\dots,n\}$. Subsequently, Line 3 and Line 4 define R and C to be sets of indices which define the rows and columns respectively of the submatrix M' defined on Line 5. Following Theorem 3.7, and Proposition 3.3 the syzygy module of $F_r(M)$ is generated by the syzygies returned by Algorithm 2 run on M' as R and C each run over the subsets in P.

The syzygies returned by Algorithm 2 take the form of elements of $\Bbbk[x_1, \ldots, x_k]^{(r+2)^2}$. Note however that $F_r(M)$ contains $\binom{n}{r+1}^2$ polynomials. Thus, in order to interpret the syzygies returned by Algorithm 2 run on M' as syzygies between the polynomials in $F_r(M)$, we must determine the index of each minor of M' in $F_r(M)$. The loop on Line 7 accomplishes this by building a tuple $L \in \Bbbk[x_1, \ldots, x_k]^{(r+2)^2}$ whose i-th entry is the index of the i-th entry of $F_r(M')$ in $F_r(M)$.

Finally, the loop on Line 9 iterates over each syzygy returned by Algorithm 2 and uses the tuple L to correctly map these syzygies to syzygies between the polynomials in $F_r(M)$. □

Remark 3.9. From Theorems 3.2 and 3.7, neither Algorithm 3 nor Algorithm 2 require any arithmetic $\Bbbk$-operations.

Again in the statement of Theorem 3.7 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 3.7 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 $\mathcal{I}_r(M)$ is satisfies the stated genericity assumption.

4 DETERMINANTAL MATRIX-F_5 ALGORITHM

In this section, we use the syzygies returned by Algorithm 3 to avoid reductions to zero when running Algorithm 1 to compute a grevlex Gröbner basis for $F_r(M)$.

4.1 The degree bound

Proposition 4.1 ([21, 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) $\tau e_i \in \mathrm{lt}_{\mathrm{pot}}(G)$, 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 $\mathscr{M}_{\deg(\tau),i}$ reduces to zero in $\bar{\mathscr{M}}_{d,i}$, then τe_i is in the module generated by $\mathrm{lt}_{\mathrm{pot}}(G)$.

Proof. Item 1 is simply Proposition 2.7. 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 $\bar{\mathscr{M}}_{d,i}$. 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 4.1, 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 these elements by running Algorithm 1 on a set of chosen generators for $\mathrm{Syz}(F)$ itself, with the appropriate degree bound given by Proposition 4.1. However, if $\mathrm{Syz}_2(F) \neq \{0\}$, then Proposition 4.1 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 $\mathrm{Syz}(F)$.

In the determinantal setting, 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 $F_r(M)$. In the general case, 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.

4.2 Algorithm description

We describe an algorithm which exploits the syzygies computed by Algorithm 3 to compute a grevlex Gröbner basis for $F_r(M)$ without reductions to zero in degree $r+2$.

Algorithm 4 Determinantal-Matrix-$F_5(M, r, D)$

Input: An integer $n \geq 3$, an integer $1 \leq r \leq n-2$, and an $n \times n$ matrix M of homogeneous linear forms over $\mathbb{k}$ in $(n-r)^2$ variables such that $\mathcal{I}_r(M)$ is Cohen-Macaulay.
Output: A grevlex D-Gröbner basis for $\mathcal{I}_r(M)$.
1: $S \leftarrow \text{SyzGen}(M, r)$
2: $S' \leftarrow \text{Matrix-F}_5(S, 1, \emptyset)$
3: $G \leftarrow \text{Matrix-F}_5(F_r(M), D, S')$
4: **return** G

Proposition 4.2. *Algorithm 4 terminates and is correct.*

Proof. Termination follows from that of Algorithm 3 and Algorithm 1. To prove correctness, we need to show that the set S' computed on Line 2 is indeed a set of syzygies between the elements of $\mathcal{I}_r(M)$. By Theorem 3.7, the set S computed on Line 1 is a minimal generating set for $\text{Syz}(F_r(M))$. The construction of this generating set, given by Theorem 3.7, shows that each element of S is homogeneous of degree one. Hence, by Proposition 2.9, the set S' consists of the elements of degree one of a POT-Gröbner basis for $\text{Syz}(F_r(M))$. □

Remark 4.3. 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 4 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 4 is bounded by the arithmetic cost of its final step, computing the Gröbner basis of $F_r(M)$.

Proposition 4.4. *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 $U \subseteq \mathbb{A}_{\mathbb{k}}^{k \cdot \binom{n}{r+1}^2}$ such that for all $\boldsymbol{a} \in U$, taking $M = \varphi_{\boldsymbol{a}}(\mathscr{A})$, upon running Algorithm 4 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 [29], there exists a Zariski open subset $U_1 \subseteq \mathbb{A}_{\mathbb{k}}^{k \cdot \binom{n}{r+1}^2}$ 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 $\mathbb{A}_{\mathbb{k}}^{k \cdot \binom{n}{r+1}^2}$ such that the results of Theorem 3.7 hold. Let $U = U_1 \cap U_2$.

Item 1 follows immediately from the degree bound given in [29]. We turn to Item 2. By Proposition 4.1, Item 2, it suffices to show that the leading terms of the set S' computed on Line 2 consists of the elements of degree at most $r+2$ of $\text{lt}_{\text{pot}}(\text{Syz}(\mathcal{I}_r(M)))$. This is immediate from Theorem 3.7 and Proposition 2.9. □

Remark 4.5. If we do not impose the genericity assumption on $\mathcal{I}_r(M)$ Algorithm 4 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 3.9, there are two possibilities. First, Algorithm 3 will still return 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 [18, 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 4.

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 4 does not require $r < n - 2$. Thus, we could simply compute a Gröbner basis for $\mathcal{I}_r(M)$ using Algorithm 4 when $r = n - 2$. However, only those reductions to zero arising from syzygies of degree $r + 2$ will be avoided. By Proposition 4.1, 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. The algorithm we describe in this section avoids such reductions as well.

5.1 Higher syzygy modules

By Proposition 3.1, 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_4 is defined by $d_4(x) = xM^*$, 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_4, and is thus free of rank n^2 and principally generated by the entries of M^*.

Proposition 5.1. *Let M be an $n \times n$ matrix of homogeneous linear forms in $\mathcal{R}$. Suppose $\mathcal{I}_{n-2}(M)$ is Cohen-Macaulay. In the $\mathcal{R}$-basis for $\ker(\pi)/\mathrm{im}(\iota)$ given in Section 3.1, the second syzygy module $\mathrm{Syz}_2(F_r(M))$ is generated by the following syzygies:*

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

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

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

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

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

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

(iv) Finally,

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

Algorithm 5 Syz2GenCorankOne

Input: An integer $n \geq 3$ and an $n \times n$ matrix M of generic homogeneous linear forms in $\Bbbk[x_1, \ldots, x_k]$.
Output: A minimal generating set for $\mathrm{Syz}_2(F_{n-2}(M))$.

$S \leftarrow \emptyset$ ▷ *to be filled with the output generating set*
▷ *handle syzygies from Item (i) of Proposition 5.1*
for $i \in \{2, \ldots, n\}$ and $j \in \{1, \ldots, n-1\}$ **do**
  $s \leftarrow \mathbf{0} \in \Bbbk[x_1, \ldots, x_k]^{2n^2-2}$
  $s_{\overline{(E_{j,j}, E_{1,1})}} \leftarrow M_{j,i}$; $s_{\overline{(0, E_{i,i} - E_{1,1})}} \leftarrow M_{j,i}$
  for $k \in \{1, \ldots, n\}$ **do**
    if $k \neq j$ **then** $s_{\overline{(E_{k,j}, 0)}} \leftarrow M_{k,i}$
    if $k \neq i$ **then** $s_{\overline{(0, E_{i,k})}} \leftarrow M_{j,k}$
  $S \leftarrow S \cup \{s\}$
▷ *handle syzygies from Item (ii) of Proposition 5.1*
for $i \in \{2, \ldots, n\}$ **do**
  $s \leftarrow \mathbf{0} \in \Bbbk[x_1, \ldots, x_k]^{2n^2-2}$
  for $k \in \{1, \ldots, n\}$ **do**
    if $k \neq n$ **then** $s_{\overline{(E_{k,n}, 0)}} \leftarrow M_{k,i}$
    if $k \neq i$ **then** $s_{\overline{(0, E_{i,k})}} \leftarrow M_{n,k}$
  for $j \in \{1, \ldots, n-1\}$ **do**
    $s_{\overline{(E_{j,j}, E_{1,1})}} \leftarrow -M_{n,i}$
    if $j \neq 1$ **then** $s_{\overline{(0, E_{j,j} - E_{1,1})}} \leftarrow -M_{n,i}$
  $S \leftarrow S \cup \{s\}$
▷ *handle syzygies from Item (iii) of Proposition 5.1*
for $j \in \{1, \ldots, n-1\}$ **do**
  $s \leftarrow \mathbf{0} \in \Bbbk[x_1, \ldots, x_k]^{2n^2-2}$
  $s_{\overline{(E_{j,j}, E_{1,1})}} \leftarrow M_{j,1}$
  for $k \in \{1, \ldots, n\}$ **do**
    if $k \neq j$ **then** $s_{\overline{(E_{k,j}, 0)}} \leftarrow M_{k,1}$
    if $k \neq 1$ **then** $s_{\overline{(0, E_{1,k})}} \leftarrow M_{j,k}$
  $S \leftarrow S \cup \{s\}$
▷ *handle syzygies from Item (iv) of Proposition 5.1*
$s \leftarrow \mathbf{0} \in \Bbbk[x_1, \ldots, x_k]^{2n^2-2}$
for $k \in \{1, \ldots, n\}$ **do**
  if $k \neq n$ **then** $s_{\overline{(E_{k,n}, 0)}} \leftarrow M_{k,1}$
  if $k \neq 1$ **then** $s_{\overline{(0, E_{1,k})}} \leftarrow M_{n,k}$
  for $j \in \{1, \ldots, n\}$ **do**
    if $j \neq 1$ **then** $s_{\overline{(0, E_{j,j} - E_{1,1})}} \leftarrow -M_{n,i}$
    if $j \neq n$ **then** $s_{\overline{(E_{j,j}, E_{1,1})}} \leftarrow -M_{n,1}$
$S \leftarrow S \cup \{s\}$
return S

Proof. The second syzygy module $\mathrm{Syz}_2(\mathcal{I}_r(M))$ is the image of d_2, by Proposition 3.1. The map d_2 is defined by

$$d_3(N) = \overline{(MN, NM)}.$$

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 $\mathrm{im}(d_3)$ 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 can 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 5.1, one deduces Algorithm Syz2GenCorankOne(M) (Algorithm 5), 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 5.2. Analogous to Remark 4.5, 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 5.1 are a subset of a generating set for the syzygies between the generators for $\ker \epsilon$ given by Theorem 3.2.

5.2 A new $\mathbf{F_5}$ algorithm

In this section, we combine Proposition 5.1, Theorem 3.2, and Proposition 4.1 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 4.1, 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 4.1 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 6 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: $S_1 \leftarrow$ SyzGenCorankOne(M)
2: $S_2 \leftarrow$ Syz2GenCorankOne(M)
3: $S_2' \leftarrow$ Matrix-F$_5(S_2, D - n, \emptyset)$
4: $S_1' \leftarrow$ Matrix-F$_5(S_1, D - n + 1, S_2')$
5: $G \leftarrow$ Matrix-F$_5(F_{n-2}(M), D, S_1')$
6: **return** G

Proposition 5.3. *Algorithm 6 terminates and is correct.*

Proof. Termination follows from that of Algorithm 2, **??**, and Algorithm 1. To show 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 3.2. □

Proposition 5.4. *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 6 with arguments $\varphi_{\boldsymbol{a}}(\mathcal{I}_{n-2}(\mathscr{A})), D$,*

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

Proof. By [29, 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 2.11, 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 4.1, 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 $\mathrm{lt}_{\mathrm{pot}}(\mathrm{Syz}(\mathcal{I}_{n-2}(M)))$. This is immediate from Theorem 3.2 and Proposition 2.9. □

6 COMPLEXITY IN THE CASE $r = n-2$

In this section, for a homogeneous ideal $\mathcal{I} \subseteq \mathcal{R}$, we take $\mathrm{HF}_{\mathcal{I}}(d)$ to be the *Hilbert function* of $\mathcal{I}$. That is, for an integer $d \ge 0$, $\mathrm{HF}_{\mathcal{I}}(d) = \dim_{\Bbbk} \mathcal{I}_d$. 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 [22, 1.9] for details about these constructions.

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 the complexity of computing the row reduction of each of these matrices.

First, note that for any $1 \le d \le r$ (resp. $1 \le d \le r+1$), 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 6 is bounded by the number of rows of the Macaulay matrix in degree d for the set S_1 (resp. $F_{n-2}(M)$). Thus, the arithmetic cost of Algorithm 6 is bounded by the arithmetic cost of the final step, computing the grevlex Gröbner basis for $F_{n-2}(M)$.

Proposition 6.1. *There exists a Zariski open subset U of $\mathbb{A}_{\Bbbk}^{4\cdot n^2}$ 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:*

$$\sum_{d=r+1}^{2r+1} \left(n^2 \binom{d-r+2}{3} - (2n^2-2)\binom{d-r+1}{3} + n^2 \binom{d-r}{3} \right) t^d. \tag{8}$$

Proof. Let U be as in Proposition 5.4. 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, $\mathrm{HF}_{\mathcal{M}}(d) = t \cdot \binom{k+d-1}{d-1}$. We have $\mathrm{rk}\,\mathcal{E}_0 = \#F_{n-2}(M) = \binom{n}{n-1}^2 = n^2$. The description of each free module in the Gulliksen-Negård complex given in Section 3.1 gives rise to

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

Thus, by [22, 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 6.2. *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 6 is in*

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

Proof. Take U as in Proposition 6.1. 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. (8) gives the rank of the Macaulay matrix of $F_r(M)$ in degree d. The Macaulay matrices computed in Algorithm 6 are full-rank. Hence, the result follows from the complexity of computing the reduced row echelon form [49, Sec. 2.2] (see also [36, 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 [29, Thm. 20] is in $O\left(n^{5\omega+2}\right)$ whereas that given by Proposition 6.2 is in $O\left(n^{4\omega-1}\right)$.

7 EXPERIMENTAL RESULTS

When $r = n-2$, as Table 1 shows, all reductions to zero are avoided and thus all Macaulay matrices are full rank. By virtue of Proposition 2.7, 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 ranks of the Macaulay matrices in each degree and the number of rows of the matrices computed by F_5 in each degree. Note also that by [29, 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 2.8 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 $1 \le i \le \binom{n}{r+1}^2$. As the data in Table 1 shows, there are more reductions to zero in higher degrees. However, 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 4.

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 [29, Cor. 19]. Thus, in this case, Proposition 2.8 is used as soon as the degree exceeds $2(r+1)$.

Table 1. Rank and number of rows in Macaulay matrix $\mathscr{M}_{d,\binom{n}{r+1}^2}$ for $\mathcal{I}_r(M)$ computed by both the standard F_5 algorithm and the determinantal F_5 algorithm, where M is an $n \times n$ matrix of homogeneous linear forms in $k = (n-r)^2$ variables over $\Bbbk = \mathbb{F}_{65521}$.

n	r	k	D	d	rank	Std. F_5	Det. F_5
4	2	4	5	3	16	16	16
				4	34	64	34
				5	56	82	56
5	3	4	7	4	25	25	25
				5	52	100	52
				6	83	124	83
				7	120	160	120
6	4	4	9	5	36	36	36
				6	74	144	74
				7	116	176	116
				8	164	220	164
				9	220	273	220
7	5	4	11	6	49	49	49
				7	100	196	100
				8	155	242	155
				9	216	298	216
				10	285	366	285
				11	364	432	364
8	6	4	13	7	64	64	64
				8	130	256	130
				9	200	322	200
				10	276	385	276
				11	360	471	360
				12	454	559	454
				13	560	650	560
9	7	4	15	8	81	81	81
				9	164	324	164
				10	251	401	251
				11	344	486	344
				12	445	584	445
				13	556	675	556
				14	679	813	679
				15	816	931	816
4	1	9	4	2	36	36	36
				3	164	324	164
				4	495	582	582
5	2	9	7	3	100	100	100
				4	450	900	450
				5	1278	1956	1956
				6	3002	3546	3546
				7	6435	6685	6685
6	3	9	6	4	225	225	225
				5	1017	2025	1017
				6	2838	4715	4715
7	4	9	6	5	441	441	441
				6	2009	3969	2009
5	1	16	4	2	100	100	100
				3	800	1600	800
				4	3875	4662	4662
6	2	16	4	3	400	400	400
				4	3250	6400	3250

REFERENCES

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

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

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

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

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

[6] I. Bannwarth and M. Safey El Din. 2015. Probabilistic Algorithm for Computing the Dimension of Real Algebraic Sets. In *Proceedings ISSAC 2015*. ACM, 37–44.

[7] M. Bardet, P. Briaud, M. Bros, P. Gaborit, V. Neiger, O. Ruatta, and J. P. Tillich. 2020. An Algebraic Attack on Rank Metric Code-Based Cryptosystems. In *Proceedings EUROCRYPT 2020 (LNCS, Vol. 12105)*. Springer.

[8] M. Bardet, M. Bros, D. Cabarcas, P. Gaborit, R. Perlner, D. Smith-Tone, J. P. Tillich, and J. Verbel. 2020. Improvements of Algebraic Attacks for Solving the Rank Decoding and MinRank Problems. In *Proceedings ASIACRYPT 2020*. 507–536.

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

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

[11] J. Berthomieu, C. Eder, and M. Safey El Din. 2022. New efficient algorithms for computing Gröbner bases of saturation ideals (F4SAT) and colon ideals (Sparse-FGLM-colon). (2022). https://hal.science/hal-03590430 Working paper.

[12] W. Beullens. 2022. Breaking Rainbow Takes a Weekend on a Laptop. In *Proceedings CRYPTO 2022*. Springer, 464–479.

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

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

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

[16] J. F. Buss, G. S. Frandsen, and J. O. Shallit. 1999. The Computational Complexity of Some Problems of Linear Algebra. *J. Comput. Syst. Sci.* 58, 3 (1999), 572–596.

[17] N. T. Courtois. 2001. Efficient Zero-Knowledge Authentication Based on a Linear Algebra Problem MinRank. In *Proceedings ASIACRYPT 2001*. Springer, 402–421.

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

[19] J. Ding and D. Schmidt. 2005. Rainbow, a New Multivariable Polynomial Signature Scheme. In *Proceedings ACNS 2005*. Springer, 164–175.

[20] J. A. Eagon and D. G. Northcott. 1962. 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 (1962), 188–204.

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

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

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

[24] J.-C. Faugère. 1999. A New Efficient Algorithm for Computing Gröbner bases (F4). *J. Pure Appl. Algebra* 139, 1 (1999), 61–88. https://doi.org/10/bpq5dx

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

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

[27] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. 2010. Computing loci of rank defects of linear matrices using Gröbner bases and applications to cryptology. In *Proceedings ISSAC 2010*. 257–264.

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

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

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

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

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

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

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

[35] H. Hong and M. Safey El Din. 2012. Variant quantifier elimination. *J. Symbolic Comput.* 47, 7 (2012), 883–901.
[36] C. P. Jeannerod, C. Pernet, and A. Storjohann. 2013. Rank-profile revealing Gaussian elimination and the CUP matrix decomposition. *J. Symbolic Comput.* 56 (2013), 46–68.
[37] A. Kipnis and A. Shamir. 1999. Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization. In *Proceedings CRYPTO 1999*. Springer, 19–30.
[38] K. Kurano. 1989. The first syzygies of determinantal ideals. *J. Algebra* 124, 2 (1989), 414–436.
[39] 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.
[40] P. Lairez and M. Safey El Din. 2021. Computing the Dimension of Real Algebraic Sets. In *Proceedings ISSAC 2021*. ACM, 257–264.
[41] A. Lascoux. 1978. Syzygies des variétés déterminantales. *Adv. Math* 30, 3 (1978), 202–237.
[42] D. Lazard. 1983. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In *Proceedings EUROSAM 83*. Springer, 146–156.
[43] 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.
[44] Y. Ma. 1994. On The Minors Defined By A Generic Matrix. *J. Symbolic Comput.* 18, 6 (1994), 503–518.
[45] J. Patarin. 1996. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In *Proceedings EUROCRYPT 1996*. Springer, 33–48.
[46] 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.
[47] 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, Article 48 (jan 2017), 37 pages. https://doi.org/10.1145/2996450
[48] P. J. Spaenlehauer. 2014. On the Complexity of Computing Critical Points with Gröbner Bases. *SIAM J. Optim.* 24, 3 (2014), 1382–1401.
[49] A. Storjohann. 2000. *Algorithms for Matrix Canonical Forms.* Ph. D. Dissertation. Swiss Federal Institute of Technology – ETH.