Gröbner Bases of Bihomogeneous Ideals Generated by Polynomials of Bidegree $(1,1)$: Algorithms and Complexity

Jean-Charles Faugère, Mohab Safey El Din, Pierre-Jean Spaenlehauer

INRIA, Paris-Rocquencourt, SALSA Project
UPMC, Univ Paris 06, LIP6
CNRS, UMR 7606, LIP6
UFR Ingénierie 919, LIP6 Passy-Kennedy
Case 169, 4, Place Jussieu, F-75252 Paris, France

Abstract

Solving multihomogeneous systems, as a wide range of *structured algebraic systems* occurring frequently in practical problems, is of first importance. Experimentally, solving these systems with Gröbner bases algorithms seems to be easier than solving homogeneous systems of the same degree. Nevertheless, the reasons of this behaviour are not clear. In this paper, we focus on bilinear systems (i.e. bihomogeneous systems where all equations have bidegree $(1,1)$). Our goal is to provide a theoretical explanation of the aforementioned experimental behaviour and to propose new techniques to speed up the Gröbner basis computations by using the multihomogeneous structure of those systems. The contributions are theoretical and practical. First, we adapt the classical F_5 criterion to avoid reductions to zero which occur when the input is a set of bilinear polynomials. We also prove an explicit form of the Hilbert series of bihomogeneous ideals generated by generic bilinear polynomials and give a new upper bound on the degree of regularity of generic affine bilinear systems. We propose also a variant of the F_5 Algorithm dedicated to multihomogeneous systems which exploits a structural property of the Macaulay matrix which occurs on such inputs. Experimental results show that this variant requires less time and memory than the classical homogeneous F_5 Algorithm. Lastly, we investigate the complexity of computing a Gröbner basis for the grevlex ordering of a generic 0-dimensional affine bilinear system over $k[x_1,\ldots,x_{n_x},y_1,\ldots,y_{n_y}]$. In particular, we show that this complexity is upper bounded by $O\left(\binom{n_x+n_y+\min(n_x+1,n_y+1)}{\min(n_x+1,n_y+1)}^{\omega}\right)$, which is polynomial in n_x+n_y (i.e. the number of unknowns) when $\min(n_x,n_y)$ is constant.

Keywords: Gröbner bases, bihomogeneous ideals, algorithms, complexity.

1. Introduction

The problem of multivariate polynomial system solving is an important topic in computer algebra since algebraic systems can arise from many practical applications (cryp-

Email addresses: Jean-Charles.Faugere@inria.fr (Jean-Charles Faugère), Mohab.Safey@lip6.fr (Mohab Safey El Din), Pierre-Jean.Spaenlehauer@lip6.fr (Pierre-Jean Spaenlehauer)

Preprint submitted to Elsevier *October 23, 2010*

tology, robotics, real algebraic geometry, coding theory, signal processing, etc...). One method to solve them is based on the Gröbner basis theory. Due to their practical importance, efficient algorithms to compute Gröbner bases of algebraic systems are required: for instance Buchberger's Algorithm (Buchberger (2006)), Faugère F_4 (Faugère (1999)) or F_5 (Faugère (2002)).

In this article, we focus on the F_5 Algorithm. In particular, the F_5 criterion is a tool which removes the so-called *reductions to zero* (which are useless) during the Gröbner basis computation when the input system is a regular sequence. For instance, consider a sequence of polynomials $(f_1, \ldots, f_m)$. The reductions to zero come from the leading monomials in the colon ideals $\langle f_1, \ldots, f_{i-1}\rangle : f_i$. Given a term order, let $\mathsf{LM}(I)$ denote the ideal generated by the leading monomials of the elements of an ideal I. Then the reductions to zero detected by the F_5 criterion are those related to $\mathsf{LM}(\langle f_1, \ldots, f_{i-1}\rangle)$. For *regular* systems, $\mathsf{LM}(\langle f_1, \ldots, f_{i-1}\rangle) = \mathsf{LM}(\langle f_1, \ldots, f_{i-1}\rangle : f_i)$. Therefore, the F_5 criterion removes all useless reductions. In practice, if a homogeneous polynomial system is chosen "at random", then it is regular.

In this paper, we consider multihomogeneous systems, which are not regular sequences in the polynomial ring. Such systems can appear in cryptography (Faugère et al. (2008)), in coding theory (Ourivski and Johansson (2002)) or in effective geometry (see Safey El Din and Schost (2003); Safey El Din and Trébuchet (2006)).

A multihomogeneous polynomial is defined with respect to a partition of the unknowns, and is homogeneous with respect to each subset of variables. The finite sequence of degrees is called the *multi-degree* of the polynomial. For instance, a bihomogeneous polynomial f of bidegree (d_1, d_2) over $k[x_0, \ldots, x_{n_x}, y_0, \ldots, y_{n_y}]$ is a polynomial such that

$$\forall \lambda, \mu, f(\lambda x_0, \ldots, \lambda x_{n_x}, \mu y_0, \ldots, \mu y_{n_y}) = \lambda^{d_1} \mu^{d_2} f(x_0, \ldots, x_{n_x}, y_0, \ldots, y_{n_y}).$$

In general, multihomogeneous systems are not regular. Consequently, the F_5 criterion does not remove all reductions to zero. Our goal is to understand the underlying structure of these multihomogeneous algebraic systems, and then use it to speed up the computation of a Gröbner basis in the context of F_5. In this paper, we focus on bihomogeneous ideals generated by polynomials of bidegree $(1, 1)$.

1.1. Main results

Let k be a field, $f_1, \ldots f_m \in k[x_0, \ldots, x_{n_x}, y_0, \ldots, y_{n_y}]$ be bilinear polynomials. We denote by F_i the polynomial family $(f_1, \ldots, f_i)$ and by I_i the ideal $\langle F_i \rangle$. We start by describing the algorithmic results of the paper, obtained by exploiting the algebraic structure of bilinear systems.

In order to understand this structure, we study properties of the jacobian matrices with respect to the two subsets of variables $x_0, \ldots, x_{n_x}$ and $y_0, \ldots, y_{n_y}$:

$$\mathsf{jac}_{\mathbf{x}}(F_i) = \begin{bmatrix} \frac{\partial f_1}{\partial x_0} & \cdots & \frac{\partial f_1}{\partial x_{n_x}} \\ \vdots & \vdots & \vdots \\ \frac{\partial f_i}{\partial x_0} & \cdots & \frac{\partial f_i}{\partial x_{n_x}} \end{bmatrix} \qquad \mathsf{jac}_{\mathbf{y}}(F_i) = \begin{bmatrix} \frac{\partial f_1}{\partial y_0} & \cdots & \frac{\partial f_1}{\partial y_{n_y}} \\ \vdots & \vdots & \vdots \\ \frac{\partial f_i}{\partial y_0} & \cdots & \frac{\partial f_i}{\partial y_{n_y}} \end{bmatrix}$$

We show that the kernels of those matrices (whose entries are linear forms) correspond to the reductions to zero not detected by the classical F_5 criterion. In general, all elements in these kernels are vectors of maximal minors of the jacobian matrices (Lemma 2). For instance, if $n_x = n_y = 2$ and $m = 4$, consider

$$\mathsf{v} = (\mathsf{minor}(\mathsf{jac}_{\mathbf{x}}(F_4), 1), -\mathsf{minor}(\mathsf{jac}_{\mathbf{x}}(F_4), 2), \mathsf{minor}(\mathsf{jac}_{\mathbf{x}}(F_4), 3), -\mathsf{minor}(\mathsf{jac}_{\mathbf{x}}(F_4), 4))$$

and

$$\mathsf{w} = (\mathsf{minor}(\mathsf{jac}_{\mathbf{y}}(F_4), 1), -\mathsf{minor}(\mathsf{jac}_{\mathbf{y}}(F_4), 2), \mathsf{minor}(\mathsf{jac}_{\mathbf{y}}(F_4), 3), -\mathsf{minor}(\mathsf{jac}_{\mathbf{y}}(F_4), 4)),$$

where $\mathsf{minor}(\mathsf{jac}_{\mathbf{x}}(F_4), k)$ (resp. $\mathsf{minor}(\mathsf{jac}_{\mathbf{y}}(F_4), k)$) denotes the determinant of the matrix obtained from $\mathsf{jac}_{\mathbf{x}}(F_4)$ (resp. $\mathsf{jac}_{\mathbf{y}}(F_4)$) by removing the k-th row. The generic *syzygies* corresponding to reductions to zero which are not detected by the classical F_5 criterion are

$$\mathsf{v} \in \mathsf{Ker}_L(\mathsf{jac}_{\mathbf{x}}(F_4)) \text{ and } \mathsf{w} \in \mathsf{Ker}_L(\mathsf{jac}_{\mathbf{y}}(F_4)).$$

We show (Corollary 2) that, in general, the ideal $I_{i-1} : f_i$ is spanned by I_{i-1} and by the maximal minors of $\mathsf{jac}_{\mathbf{x}}(F_{i-1})$ (if $i > n_y + 1$) and $\mathsf{jac}_{\mathbf{y}}(F_{i-1})$ (if $i > n_x + 1$). The leading monomial ideal of $I_{i-1} : f_i$ describes the reductions to zero associated to f_i. Thus we need results about ideals generated by maximal minors of matrices whose entries are linear forms in order to get a description of the syzygy module. In particular, we prove that, in general, *grevlex* Gröbner bases of those ideals are linear combinations of the generators (Theorem 3). Based on this result, one can compute efficiently a Gröbner basis of $I_{i-1} : f_i$ once a Gröbner basis of I_{i-1} is known.

This allows us to design an Algorithm (Algorithm 4) dedicated to bilinear systems, which yields an extension of the classical F_5 criterion. This subroutine, when merged within a matricial version of the F_5 Algorithm (Algorithm 2), eliminates all reductions to zero during the computation of a Gröbner basis of a generic bilinear system. For instance, during the computation of a grevlex Gröbner basis of a system of 12 generic bilinear equations over $k[x_0, \dots, x_6, y_0, \dots, y_6]$, the new criterion detects 990 reductions to zero which are not found by the usual F_5 criterion. Even if this new criterion seems to be more complicated than the usual F_5 criterion (some precomputations have to be performed), we prove that the cost induced by those precomputations is negligible compared to the cost of the whole computation.

Next, we introduce a notion of *bi-regularity* which describes the structure of generic bilinear systems. When the input of Algorithm 4 is a bi-regular system, then it returns all reductions to zero. We also give a complete description of the syzygy module of such systems, up to a conjecture (Conjecture 1) on a linear algebra problem over rings. This conjecture is supported by practical experiments. We also prove that there are no reductions to zero with the classical F_5 criterion for affine bilinear systems (Proposition 5) which is important for practical applications.

We describe now the main complexity results of the paper. We need some results on the so-called Hilbert bi-series of ideals generated by bilinear systems. For bi-regular bilinear system, we give an explicit form of these series (Theorem 5):

$$\mathsf{HS}_{I_m}(t_1, t_2) = \frac{N_m}{(1-t_1)^{n_x+1}(1-t_2)^{n_y+1}},$$

$$N_m(t_1, t_2) = (1 - t_1 t_2)^m + \sum_{\ell=1}^{m-(n_y+1)} (1 - t_1 t_2)^{m-(n_y+1)-\ell} t_1 t_2 (1 - t_2)^{n_y+1} \left[1 - (1 - t_1)^\ell \sum_{k=1}^{n_y+1} t_1^{n_y+1-k} \binom{\ell+n_y-k}{n_y+1-k}\right] + \sum_{\ell=1}^{m-(n_x+1)} (1 - t_1 t_2)^{m-(n_x+1)-\ell} t_1 t_2 (1 - t_1)^{n_x+1} \left[1 - (1 - t_2)^\ell \sum_{k=1}^{n_x+1} t_2^{n_x+1-k} \binom{\ell+n_x-k}{n_x+1-k}\right].$$

After this analysis, we propose a variant of the Matrix F_5 Algorithm dedicated to multihomogeneous systems. The key idea is to decompose the Macaulay matrices into a set of smaller matrices whose row echelon forms can be computed independently. We provide some experimental results of an implementation of this algorithm in `Magma2.15`. This multihomogeneous variant can be more than 20 times faster for bihomogeneous systems than our `Magma` implementation of the classical Matrix F_5 Algorithm. We perform a theoretical complexity analysis based on the Hilbert series in the case of bilinear systems, which provides an explanation of this gap.

Finally, we establish a sharp upper bound on the degree of regularity of 0-dimensional affine bilinear systems (Theorem 6). Let $f_1, \ldots, f_{n_x+n_y}$ be an affine bilinear system of $k[x_0, \ldots, x_{n_x-1}, y_0, \ldots, y_{n_y-1}]$, then the maximal degree reached during the computation of a Gröbner basis with respect to the grevlex ordering is upper bounded by:

$$\mathsf{d}_{\mathsf{reg}} \leq \min\left(n_x + 1, n_y + 1\right).$$

This bound is *exact* in practice for generic bilinear systems and permits to derive complexity estimates for solving bilinear systems (Corollary 3) which can be applied to practical problems (see for instance Faugère et al. (2010) for an application to the MinRank problem).

1.2. State of the art

The complexity analysis that we perform by proving properties on the Hilbert bi-series of bilinear ideals follows a path which is similar to the one used to analyze the complexity of the F_5 algorithm in the case of homogeneous regular sequences (see Bardet et al. (2005)). In Kreuzer et al. (2002), the properties of Buchberger's Algorithm are investigated in the context of multi-graded rings. Cox et al. (2007a) gives an analysis of the structure of the syzygy module in the case of three bihomogeneous equations with no common solution in the biprojective space.

The algorithmic use of multihomogeneous structures has been investigated mostly in the framework of multivariate resultants (see Dickenstein and Emiris (2003); Emiris and Mantzaflaris (2009) and references therein for the most recent results) following the line of work initiated by McCoy (1933). In the context of solving polynomial systems by using straight-line programs as data-structures, Jeronimo and Sabia (2007) provides an alternative way to compute resultant formula for multihomogeneous systems.

As we have seen in the description of the main results, the knowledge of Gröbner bases of ideals generated by maximal minors of linear matrices play a crucial role. Theorem 3 which states that such Gröbner bases are obtained by a single row echelon form computation is a variant of the main results in Sturmfels and Zelevinsky (1993) and Bernstein and Zelevinsky (1993) (see also the survey by Bruns and Conca (2003)).

More generally, the theory of multihomogeneous elimination is investigated in Rémond (2001) providing tools to generalize some well-known notions (e.g. Chow forms, resultant formula, heights) in the homogeneous case to multihomogeneous situations. Such works are initiated in Van der Waerden (1929) where the Hilbert bi-series of bihomogeneous ideals is introduced.

1.3. Structure of the paper

This paper is articulated as follows. Some tools from commutative algebra are introduced. Next, we investigate the case of bilinear systems and propose an algorithm to remove all reductions to zero during the Gröbner basis computation. Then we prove its correctness and explain why it is efficient for *generic* bilinear systems. To continue our study of the structure of bilinear ideals, we give the explicit form of the Hilbert bi-series of generic bilinear ideals. Finally, we prove a new bound on the degree of regularity of generic affine bilinear systems and we use it to derive new complexity bounds. Technical results and their proofs are postponed in Appendix.

Acknowledgments.

We are grateful to Ludovic Perret, Ioannis Z. Emiris and anonymous referees for their helpful comments and suggestions. This work is supported by the EXACTA grant of the French National Research Agency (ANR-09-BLAN-0371-01) and the National Science Foundation of China.

2. Gröbner bases: the Matrix F_5 Algorithm

2.1. Gröbner bases: notations

In this section, R denotes the polynomial ring $k[x_1, \ldots, x_n]$ (where k is a field) and for all $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$, x^β denotes $x_1^{\beta_1}, \cdots, x_n^{\beta_n}$. Gröbner bases are defined with respect to a monomial ordering (see Cox et al. (2007b), page 55, Definition 1). In this paper, we focus in particular on the so-called *grevlex* ordering (degree reverse lexicographical ordering).

Definition 1. *The* grevlex *ordering is defined by:*

$$x^\alpha \prec x^\beta \Leftrightarrow \begin{cases} \sum \alpha_i < \sum \beta_i \text{ or} \\ \sum \alpha_i = \sum \beta_i \text{ and the first coordinates} \\ \text{from the right which are different satisfy } \alpha_i > \beta_i. \end{cases}$$

If $\prec$ is a monomial ordering and $f \in R$ is a polynomial, then its greatest monomial with respect to $\prec$ is called *leading monomial* and denoted by $\mathsf{LM}_\prec(f)$ (or simply $\mathsf{LM}(f)$ when there is no ambiguity on the considered ordering).

If $I \subset R$ is a polynomial ideal, its *leading monomial ideal* (i.e. $\langle\{\mathsf{LM}_\prec(f) : f \in I\}\rangle$) is denoted by $\mathsf{LM}_\prec(I)$ (or simply $\mathsf{LM}(I)$ when there is no ambiguity on the ordering) .

Definition 2. *let $I \subset R$ be an ideal, and $\prec$ be a monomial ordering. A* Gröbner basis *of I (relatively to $\prec$) is a finite subset $G \subset I$ such that: $\langle \mathsf{LM}_\prec(G)\rangle = \mathsf{LM}_\prec(I)$.*

Definition 3. *Let $I \subset R$ be an ideal, $\prec$ be a monomial ordering and $f \in R$ be a polynomial. Then there exist unique polynomials $\tilde{f} \in R$ and $g \in I$ such that $f = \tilde{f} + g$ and none of the monomials appearing in $\tilde{f}$ are in $\mathsf{LM}_\prec(I)$. The polynomial $\tilde{f}$ is called the* normal form *of f (with respect to I and $\prec$), and is denoted $\mathsf{NF}_{I,\prec}(f)$.*

It is well known that $\mathsf{NF}_{I,\prec}(f) = 0$ if and only if $f \in I$ (see e.g. Cox et al. (2007b)).

Definition 4. *Let $I \subset R$ be a homogeneous ideal, $\prec$ be a monomial ordering and D be an integer. We call D-Gröbner basis a finite set of polynomials G such that $\langle G\rangle = I$ and*

$$\forall f \in I \text{ with } \deg(f) \le D, \text{ there exists } g \in G \text{ such that } \mathsf{LM}_\prec(g) \text{ divides } \mathsf{LM}_\prec(f).$$

The following Lemma is a straightforward consequence of Dickson's Lemma (Cox et al., 2007b, page 71, Theorem 5).

Lemma 1. *Let $I \subset R$ be an ideal and let $\prec$ be a monomial ordering. There exists $D \in \mathbb{N}$ such that every D-Gröbner basis with respect to $\prec$ is a Gröbner basis of I with respect to $\prec$.*

2.2. The Matrix F_5 Algorithm

We use a variant of the F_5 Algorithm, called Matrix F_5 Algorithm, which is suitable to perform complexity analyses (see Bardet (2004); Bardet et al. (2005); Faugère and Rahmany (2009)).

Given a set of generators $(f_1, \ldots, f_m)$ of a homogeneous polynomial ideal $I \subset R$, an integer D and a monomial ordering $\prec$, the Matrix F_5 Algorithm computes a D-Gröbner basis of I with respect to $\prec$. It performs incrementally by considering the ideals $I_i = \langle f_1, \ldots, f_i \rangle$ for $1 \leq i \leq m$.

Let $d \in \mathbb{N}$, denote by R_d the k-vector space of polynomials in R of degree d. As in Faugère (2002) and Bardet (2004), we use a definition of the row echelon form of a matrix which is slightly different from the usual definition: we call *row echelon form* the matrix obtained by applying the Gaussian elimination Algorithm *without permuting the rows*. The idea of the Matrix F_5 Algorithm (see Algorithm 2 below) is to calculate triangular bases of the vector spaces $I_i \cap R_d$ for $1 \leq d \leq D$ and $1 \leq i \leq m$ and to deduce from them a d-basis of I_{i+1}. These triangular bases are obtained by computing row echelon forms of the Macaulay matrices.

Definition 5. *Let $F_i = (f_1, \ldots, f_i) \in R^i$ be a sequence of homogeneous polynomials of degrees $(d_1, \ldots, d_i)$ and $\prec$ be a monomial ordering. The Macaulay matrix in degree d $\mathsf{Macaulay}_{\prec}(F_i, d)$ is the matrix whose rows contain the coefficients of the polynomials $\{tf_j\}$ where $1 \leq j \leq i$ and $t \in R$ is a monomial of degree $d - d_j$. The columns correspond to the monomials in R of degree d and are sorted by $\prec$ in descending order. Each row has a signature (t, f_j) and they are sorted as follows: a row with signature (t_1, f_j) is preceding a row with signature (t_2, f_k) if $j < k$ or ($j = k$ and $t_1 \prec t_2$). The element at the intersection of the row (t, f_j) and the column corresponding to the monomial m is the coefficient of m in the polynomial tf_j.*

When the row echelon form of a Macaulay matrix is computed, the rows which are linear combinations of preceding rows are reduced to zero. Such computations are useless: removing these rows before computing the row echelon form will not modify the result but lead to significant practical improvements. The so-called F_5 criterion (see Faugère (2002)) is used to detect these *reductions to zero* and is given below. In Algorithm 2, the matrices $\mathcal{M}_{d,i}$ are similar to Macaulay matrices: their rows and their columns are sorted with the same orderings and their rows span the same vector spaces. Moreover, if $(f_1, \ldots, f_m)$ is a regular sequence, then the rows of their row echelon form $\widetilde{\mathcal{M}_{d,i}}$ are bases of $I_i \cap R_d$.

Algorithm 1. F_5 **criterion** - *returns a boolean*

Require: $\begin{cases} (t, f_i) \text{ the signature of a row} \\ A \text{ matrix } \mathcal{M} \text{ in row echelon form} \end{cases}$

If t is the leading monomial of a row of $\mathcal{M}$, then return `true`*,*
else return `false`*.*

Now, we give a description of the Matrix F_5 Algorithm.

Algorithm 2. Matrix F_5 *(see Faugère and Rahmany (2009); Bardet (2004); Faugère (2002))*

Require: $\begin{cases} (f_1, \ldots, f_m) \text{ homogeneous polynomials of degree } d_1 \leq d_2 \leq \ldots \leq d_m \\ D \text{ an integer} \\ \text{a monomial ordering } \prec \end{cases}$

Ensure: *G is a D-Gröbner basis of $\langle f_1, \ldots, f_m \rangle$ for $\prec$*

$G \leftarrow \{f_1, \ldots, f_m\}$
for *d from d_1 to D* ***do***
  $\widetilde{\mathcal{M}_{d,0}} \leftarrow$ *matrix with* 0 *rows*
  for *i from 1 to m* ***do***
    Construct $\mathcal{M}_{d,i}$ by adding to $\widetilde{\mathcal{M}_{d,i-1}}$ the following rows:
    if $d_i = d$ ***then***
      add the row f_i with signature $(1, f_i)$
    end if
    if $d > d_i$ ***then***
      for all f from $\widetilde{\mathcal{M}_{d-1,i}}$ with signature (e, f_i), such that x_λ is the
      greatest variable of e, add the $n - \lambda + 1$ rows $x_\lambda f, x_{\lambda+1} f, \ldots, x_n f$ with the
      signatures $(x_\lambda e, f_i), (x_{\lambda+1} e, f_i), \ldots, (x_n e, f_i)$ except those which satisfy:
      F_5**criterion** $((x_{\lambda+k} e, f_i), \widetilde{\mathcal{M}_{d-d_i,i-1}})$=*true*
    end if
    Compute $\widetilde{\mathcal{M}_{d,i}}$ the row echelon form of $\mathcal{M}_{d,i}$
    Add to G the polynomials corresponding to rows of $\widetilde{\mathcal{M}_{d,i}}$ such that their
    leading monomial is different from the leading monomial of
    the row with same signature in $\mathcal{M}_{d,i}$
  end for
end for
return G

We recall now some results mostly given by Faugère (2002) which justify the F_5 criterion by relating reductions to zero appearing in an incremental computation of a Gröbner basis of a homogeneous ideal with the syzygy module of the polynomial system under consideration.

Definition 6. *Let $(f_1, \ldots, f_m)$ be polynomials in R. A syzygy is an element $s = (s_1, \ldots, s_m) \in R^m$ such that $\sum_{j=1}^{m} f_j s_j = 0$. The degree of the syzygy is defined by*

$\max_j(\deg(f_j) + \deg(s_j))$. *The set of all syzygies is a submodule of* R^m *called the* syzygy module *of* $(f_1, \ldots, f_m)$.

The next theorem explains how reductions to zero and syzygies are related:

Theorem 1 (F_5 criterion, Faugère (2002))**.**

1. *If* $t \in \mathsf{LM}(I_{i-1})$ *then there exists a syzygy* $(s_1, \ldots, s_i)$ *of* $(f_1, \ldots, f_i)$ *such that* $\mathsf{LM}(s_i) = t$.
2. *Let* (t, f_i) *be the signature of a row of* $\mathcal{M}_{d,m}$. *Then the following assertions are equivalent:*
   (a) *the row* (t, f_i) *is zero in the row echelon form* $\widetilde{\mathcal{M}_{d,m}}$.
   (b) $t \notin \mathsf{LM}(I_{i-1})$ *and there exists a syzygy* $s = (s_1, \ldots, s_i)$ *of* $(f_1, \ldots, f_i)$ *such that* $t = \mathsf{LM}(s_i)$.

The rows eliminated by the F_5 criterion correspond to the trivial syzygies, i.e. the syzygies $(s_1, \ldots, s_m)$ such that $\forall 1 \leq i \leq m$, $s_i \in \langle f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_m \rangle$. These particular syzygies come from the commutativity of R (for all $1 \leq i, j \leq m$, $f_i f_j - f_j f_i = 0$). It is well known that in the generic case, the syzygy module of a polynomial system is generated by the trivial syzygies.

Definition 7. *(Eisenbud, 1995, page 419) Let* $(f_1, \ldots, f_m)$ *be a sequence of homogeneous polynomials and let* $I_i \subset R$ *be the ideal* $\langle f_1, \ldots, f_i \rangle$. *The following assertions are equivalent:*

1. *the syzygy module of* $(f_1, \ldots, f_m)$ *is generated by the trivial syzygies.*
2. *for* $2 \leq i \leq m$, f_i *is not a divisor of* 0 *in* R/I_{i-1}.

A sequence of polynomials which satisfies these conditions is called a regular sequence*.*

This notion of regularity is essential since the regular sequences correspond exactly to the systems such that there is no reduction to zero during the computation of a Gröbner basis with F_5 (see Faugère (2002)). Moreover, generic polynomial systems with less equations than unknowns are regular.

3. Gröbner bases computation for bilinear systems

3.1. Overview

Let $F = (f_1, \ldots, f_4)$ be four bilinear polynomials in $\mathbb{Q}[x_0, x_1, x_2, y_0, y_1, y_2]$, I be the ideal generated by F and $V \subset \mathbb{C}^6$ be its associated algebraic variety. As above, I_i denotes the ideal $\langle f_1, \ldots, f_i \rangle$, and we consider the grevlex ordering with $x_0 \succ \ldots \succ x_{n_x} \succ y_0 \succ \ldots \succ y_{n_y}$. Since $f_1, \ldots, f_4$ are bilinear, for all $(a_0, a_1, a_2) \in \mathbb{C}^3$ and $1 \leq i \leq 4$, $f_i(a_0, a_1, a_2, 0, 0, 0) = 0$. Hence, V contains the linear affine subspace defined by $y_0 = y_1 = y_2 = 0$ which has dimension 3. We conclude that V has dimension at least 3.

Consequently, the sequence (f_1, f_2, f_3, f_4) is not regular (since the codimension of an ideal generated by a regular sequence is equal to the length of the sequence). Hence, there are reductions to zero during the computation of a Gröbner basis with the F_5 Algorithm (see Faugère (2002)).

When the four polynomials are chosen randomly, one remarks experimentally that these reductions correspond to the rows with signatures (x_0^3, f_4) and (y_0^3, f_4). This experimental observation can be explained as follows.

Consider the jacobian matrices

$$\mathsf{jac}_{\mathbf{x}}(F) = \begin{bmatrix} \frac{\partial f_1}{\partial x_0} & \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} \\ \vdots & \vdots & \vdots \\ \frac{\partial f_4}{\partial x_0} & \frac{\partial f_4}{\partial x_1} & \frac{\partial f_4}{\partial x_2} \end{bmatrix} \quad \text{and} \quad \mathsf{jac}_{\mathbf{y}}(F) = \begin{bmatrix} \frac{\partial f_1}{\partial y_0} & \frac{\partial f_1}{\partial y_1} & \frac{\partial f_1}{\partial y_2} \\ \vdots & \vdots & \vdots \\ \frac{\partial f_4}{\partial y_0} & \frac{\partial f_4}{\partial y_1} & \frac{\partial f_4}{\partial y_2} \end{bmatrix}$$

and the vectors of variables $\mathbf{X}$ and $\mathbf{Y}$. By Euler's formula, it is immediate that for any sequence of polynomials (q_1, q_2, q_3, q_4),

$$(q_1, \ldots, q_4).\mathsf{jac}_{\mathbf{x}}(F).\mathbf{X} = \sum_{i=1}^{4} q_i f_i \quad \text{and} \quad (q_1, \ldots, q_4).\mathsf{jac}_{\mathbf{y}}(F).\mathbf{Y} = \sum_{i=1}^{4} q_i f_i \tag{1}$$

Denote by $\mathsf{Ker}_L(\mathsf{jac}_{\mathbf{x}}(F))$ (resp. $\mathsf{Ker}_L(\mathsf{jac}_{\mathbf{y}}(F))$) the left kernel of $\mathsf{jac}_{\mathbf{x}}(F)$ (resp. $\mathsf{jac}_{\mathbf{y}}(F)$).

Therefore, if $(q_1, \ldots, q_4)$ belongs to $\mathsf{Ker}_L(\mathsf{jac}_{\mathbf{x}}(F))$ (resp. $\mathsf{Ker}_L(\mathsf{jac}_{\mathbf{y}}(F))$), then the relation (1) implies that $(q_1, \ldots, q_4)$ belongs to the syzygy module of I.

Given a $(k+1, k)$-matrix M, denote by $\mathsf{minor}(\mathsf{M}, j)$ the minor obtained by removing the j-th row from M. Consider

$$\mathsf{v} = (\mathsf{minor}(\mathsf{jac}_{\mathbf{x}}(F), 1), -\mathsf{minor}(\mathsf{jac}_{\mathbf{x}}(F), 2), \mathsf{minor}(\mathsf{jac}_{\mathbf{x}}(F), 3), -\mathsf{minor}(\mathsf{jac}_{\mathbf{x}}(F), 4)).$$

By Cramer's rule, $\mathsf{v} \in \mathsf{Ker}_L(\mathsf{jac}_{\mathbf{x}}(F))$. A symmetric statement can be made for $\mathsf{jac}_{\mathbf{y}}(F)$. From this observation, one deduces that $\mathsf{minor}(\mathsf{jac}_{\mathbf{x}}(F), 4) f_4$ (resp. $\mathsf{minor}(\mathsf{jac}_{\mathbf{y}}(F), 4) f_4$) belongs to $I_3 = \langle f_1, f_2, f_3 \rangle$.

We conclude that the rows with signature

$$(\mathsf{LM}(\mathsf{minor}(\mathsf{jac}_{\mathbf{x}}(F), 4)), f_4) \text{ and } (\mathsf{LM}(\mathsf{minor}(\mathsf{jac}_{\mathbf{y}}(F), 4)), f_4)$$

are reduced to zero when performing the Matrix F_5 Algorithm described in the previous section. A straightforward computation shows that if F contains polynomials which are chosen randomly, $\mathsf{LM}(\mathsf{minor}(\mathsf{jac}_{\mathbf{x}}(F), 4)) = y_0^3$ and $\mathsf{LM}(\mathsf{minor}(\mathsf{jac}_{\mathbf{y}}(F), 4)) = x_0^3$.

In this section, we generalize this approach to sequences of bilinear polynomials of arbitrary length. Hence, the jacobian matrices have a number of rows which is is not the number of columns incremented by 1. But, even in this more general setting, we exhibit a relationship between the left kernels of the jacobian matrices and the syzygy module of the ideal spanned by the sequence under consideration. This allows us to prove a new F_5-criterion dedicated to bilinear systems. On the one hand, when plugged into the Matrix F_5 Algorithm, this criterion detects reductions to zero which are not detected by the classical criterion. On the other hand, we prove that a D-Gröbner basis is still computed by the Matrix F_5 Algorithm when it uses the new criterion.

3.2. Jacobian matrices of bilinear systems and syzygies

From now on, we use the following notations:

- $R = k[x_0, \ldots, x_{n_x}, y_0, \ldots, y_{n_y}]$;

- $F = (f_1, \ldots, f_m) \subset R^m$ is a sequence of bilinear polynomials and $F_i = (f_1, \ldots, f_i)$ for $1 \le i \le m$;
- I is the ideal generated by F and I_i is the ideal generated by F_i;
- Let M be a $\ell \times c$ matrix, with $\ell > c$. We call *maximal minors* of M the determinants of the $c \times c$ sub-matrices of M;
- $\mathsf{jac}_{\mathbf{x}}(F_i)$ and $\mathsf{jac}_{\mathbf{y}}(F_i)$ are respectively the jacobian matrices

$$\begin{bmatrix} \frac{\partial f_1}{\partial x_0} & \cdots & \frac{\partial f_1}{\partial x_{n_x}} \\ \vdots & \vdots & \vdots \\ \frac{\partial f_i}{\partial x_0} & \cdots & \frac{\partial f_i}{\partial x_{n_x}} \end{bmatrix} \text{ and } \begin{bmatrix} \frac{\partial f_1}{\partial y_0} & \cdots & \frac{\partial f_1}{\partial y_{n_y}} \\ \vdots & \vdots & \vdots \\ \frac{\partial f_i}{\partial y_0} & \cdots & \frac{\partial f_i}{\partial y_{n_y}} \end{bmatrix};$$

- Given a matrix M, $\mathsf{Ker}_L(\mathsf{M})$ denotes the left kernel of M;
- $\mathbf{X}$ is the vector $[x_0, \ldots, x_{n_x}]^t$ and $\mathbf{Y}$ is the vector $[y_0, \ldots, y_{n_y}]^t$;
- $(f_1, \ldots, f_m) \in k[x_0, \ldots, x_{n_x-1}, y_0, \ldots, y_{n_y-1}]^m$ is an *affine bilinear system* if there exists a homogeneous bilinear system $(f_1^h, \ldots, f_m^h) \in k[x_0, \ldots, x_{n_x}, y_0, \ldots, y_{n_y}]^m$ such that

$$f_i(x_0, \ldots, x_{n_x-1}, y_0, \ldots, y_{n_y-1}) = f_i^h(x_0, \ldots, x_{n_x-1}, 1, y_0, \ldots, y_{n_y-1}, 1).$$

Lemma 2. *Let $i > n_x + 1$ (resp. $i > n_y + 1$), and let $\mathfrak{s}$ be a maximal minor of* $\mathsf{jac}_{\mathbf{x}}(F_{i-1})$ *(resp.* $\mathsf{jac}_{\mathbf{y}}(F_{i-1})$*). Then there exists a vector $(s_1, \ldots, s_{i-1}, \mathfrak{s})$ in* $\mathsf{Ker}_L(\mathsf{jac}_{\mathbf{x}}(F_i))$ *(resp.* $\mathsf{Ker}_L(\mathsf{jac}_{\mathbf{y}}(F_i))$*).*

Proof. The proof is done when considering $\mathfrak{s}$ as a maximal minor of $\mathsf{jac}_{\mathbf{x}}(F_{i-1})$ with $i > n_x + 1$. The case where $\mathfrak{s}$ is a maximal minor of $\mathsf{jac}_{\mathbf{y}}(F_{i-1})$ with $i > n_y + 1$ is proved similarly.

Notice that $\mathsf{jac}_{\mathbf{x}}(F_{i-1})$ is a matrix with $i-1$ rows and n_x+1 columns and $i-1 \ge n_x+1$. Denote by $(j_1, \ldots, j_{i-n_x-2})$ the rows deleted from $\mathsf{jac}_{\mathbf{x}}(F_{i-1})$ to construct its submatrix J whose determinant is $\mathfrak{s}$.

Consider now the $i \times (i - n_x - 2)$-matrix T such that its (ℓ, k) entry is 1 if and only if $\ell = j_k$, else it is 0. N denotes the following $i \times (i-1)$ matrix:

$$\mathsf{N} = \left[\begin{array}{c|c} \mathsf{jac}_{\mathbf{x}}(F_i) & \mathsf{T} \end{array} \right].$$

A straightforward use of Cramer's rule shows that

$$(\mathsf{minor}(\mathsf{N}, 1), -\mathsf{minor}(\mathsf{N}, 2), \ldots, (-1)^{i+1}\mathsf{minor}(\mathsf{N}, i)) \in \mathsf{Ker}_L(\mathsf{N}).$$

Remark that this implies

$$(\mathsf{minor}(\mathsf{N}, 1), -\mathsf{minor}(\mathsf{N}, 2), \ldots, (-1)^{i+1}\mathsf{minor}(\mathsf{N}, i)) \in \mathsf{Ker}_L(\mathsf{jac}_{\mathbf{x}}(F_i)).$$

Computing $\mathsf{minor}(\mathsf{N}, i)$ by going across the last columns of N shows that $\mathsf{minor}(\mathsf{N}, i) = \pm\mathfrak{s}$. □

Theorem 2. *Let $i > n_x + 1$ (resp. $i > n_y + 1$) and let s be a linear combination of maximal minors of $\mathsf{jac}_{\mathbf{x}}(F_{i-1})$ (resp. $\mathsf{jac}_{\mathbf{y}}(F_{i-1})$). Then $s \in I_{i-1} : f_i$.*

Proof. By assumption, $s = \sum_\ell a_\ell \, \mathfrak{s}_\ell$ where each $\mathfrak{s}_\ell$ is a maximal minor of $\mathsf{jac}_{\mathbf{x}}(F_{i-1})$. According to Lemma 2, for each minor $\mathfrak{s}_\ell$ there exists $(s_1^{(\ell)}, \ldots, s_{i-1}^{(\ell)})$ such that

$$(s_1^{(\ell)}, \ldots, s_{i-1}^{(\ell)}, \mathfrak{s}_\ell) \in \mathsf{Ker}_L(\mathsf{jac}_{\mathbf{x}}(F_i))$$

Thus, by summation over ℓ, one obtains

$$(\sum_\ell a_\ell s_1^{(\ell)}, \ldots, \sum_\ell a_\ell s_{i-1}^{(\ell)}, s) \in \mathsf{Ker}_L(\mathsf{jac}_{\mathbf{x}}(F_i)). \tag{2}$$

Moreover, by Euler's formula

$$(\sum_\ell a_\ell s_1^{(\ell)}, \ldots, \sum_\ell a_\ell s_{i-1}^{(\ell)}, s)\mathsf{jac}_{\mathbf{x}}(F_i)\mathbf{X} = s\, f_i + \sum_{j=1}^{i-1} \left(\sum_\ell a_\ell s_j^{(\ell)} \right) f_j.$$

By the relation (2), $s\, f_i + \sum_{j=1}^{i-1} \left(\sum_\ell a_\ell s_j^{(\ell)} \right) f_j = 0$, which implies that $s \in I_{i-1} : f_i$. □

Corollary 1. *Let $i > n_x + 1$ (resp. $i > n_y + 1$), $M_{\mathbf{x}}^{(i)}$ (resp. $M_{\mathbf{y}}^{(i)}$) be the ideal generated by the maximal minors of $\mathsf{jac}_{\mathbf{x}}(F_i)$ (resp. $\mathsf{jac}_{\mathbf{y}}(F_i)$). Then $M_{\mathbf{x}}^{(i-1)} \subset I_{i-1} : f_i$ (resp. $M_{\mathbf{y}}^{(i-1)} \subset I_{i-1} : f_i$).*

Proof. By Theorem 2, all minors of $\mathsf{jac}_{\mathbf{x}}(F_{i-1})$ (resp. $\mathsf{jac}_{\mathbf{y}}(F_{i-1})$) are elements of $I_{i-1} : f_i$. Thus, $I_{i-1} : f_i$ contains a set of generators of $M_{\mathbf{x}}^{(i-1)}$ (resp. $M_{\mathbf{y}}^{(i-1)}$). Since $I_{i-1} : f_i$ is an ideal, our assertion follows. □

Example 1. *Consider the following bilinear system in $\mathsf{GF}(7)[x_0, x_1, x_2, y_0, y_1, y_2, y_3]$:*

$$\begin{aligned}
f_1 &= x_0y_0 + 5x_1y_0 + 4x_2y_0 + 5x_0y_1 + 3x_1y_1 + x_0y_2 + 4x_1y_2 + 5x_2y_2 + 5x_0y_3 + x_1y_3 + 2x_2y_3,\\
f_2 &= 2x_0y_0 + 4x_1y_0 + 6x_2y_0 + 2x_0y_1 + 5x_1y_1 + 6x_0y_2 + 4x_2y_2 + 3x_0y_3 + 2x_1y_3 + 4x_2y_3,\\
f_3 &= 5x_0y_0 + 5x_1y_0 + 2x_2y_0 + 4x_0y_1 + 6x_1y_1 + 4x_2y_1 + 6x_1y_2 + 4x_2y_2 + x_0y_3 + x_1y_3 + 5x_2y_3,\\
f_4 &= 6x_0y_0 + 5x_2y_0 + 4x_0y_1 + 5x_1y_1 + x_2y_1 + x_0y_2 + x_1y_2 + 6x_2y_2 + 2x_0y_3 + 4x_1y_3 + 5x_2y_3,\\
f_5 &= 6x_0y_0 + 3x_1y_0 + 6x_2y_0 + 3x_0y_1 + 5x_2y_1 + 2x_0y_2 + 4x_1y_2 + 5x_2y_2 + 2x_0y_3 + 4x_1y_3 + 5x_2y_3.
\end{aligned}$$

Its jacobian matrices $\mathsf{jac}_{\mathbf{x}}(F_4)$ and $\mathsf{jac}_{\mathbf{y}}(F_4)$ are:

$$\mathsf{jac}_{\mathbf{x}}(F_4) = \begin{pmatrix} y_0 + 5y_1 + y_2 + 5y_3 & 5y_0 + 3y_1 + 4y_2 + y_3 & 4y_0 + 5y_2 + 2y_3 \\ 2y_0 + 2y_1 + 6y_2 + 3y_3 & 4y_0 + 5y_1 + 2y_3 & 6y_0 + 4y_2 + 4y_3 \\ 5y_0 + 4y_1 + y_3 & 5y_0 + 6y_1 + 6y_2 + y_3 & 2y_0 + 4y_1 + 4y_2 + 5y_3 \\ 6y_0 + 4y_1 + y_2 + 2y_3 & 5y_1 + y_2 + 4y_3 & 5y_0 + y_1 + 6y_2 + 5y_3 \end{pmatrix}.$$

$$\mathsf{jac}_{\mathbf{y}}(F_4) = \begin{pmatrix} x_0 + 5x_1 + 4x_2 & 5x_0 + 3x_1 & x_0 + 4x_1 + 5x_2 & 5x_0 + x_1 + 2x_2 \\ 2x_0 + 4x_1 + 6x_2 & 2x_0 + 5x_1 & 6x_0 + 4x_2 & 3x_0 + 2x_1 + 4x_2 \\ 5x_0 + 5x_1 + 2x_2 & 4x_0 + 6x_1 + 4x_2 & 6x_1 + 4x_2 & x_0 + x_1 + 5x_2 \\ 6x_0 + 5x_2 & 4x_0 + 5x_1 + x_2 & x_0 + x_1 + 6x_2 & 2x_0 + 4x_1 + 5x_2 \end{pmatrix}.$$

An straightforward computation shows that the maximal minors of the matrix $\mathsf{jac}_{\mathbf{x}}(F_4)$ and $\mathsf{jac}_{\mathbf{y}}(F_4)$ are in $\langle f_1, f_2, f_3, f_4 \rangle : f_5$, in accordance with Corollary 1. An example of a corresponding syzygy is obtained by the vanishing of the determinant

$$\begin{aligned}
\det\,[\mathsf{jac}_{\mathbf{x}}(F_5)|T|F_5] = \det &\begin{pmatrix} y_0 + 5y_1 + y_2 + 5y_3 & 5y_0 + 3y_1 + 4y_2 + y_3 & 4y_0 + 5y_2 + 2y_3 & 1 & f_1 \\ 2y_0 + 2y_1 + 6y_2 + 3y_3 & 4y_0 + 5y_1 + 2y_3 & 6y_0 + 4y_2 + 4y_3 & 0 & f_2 \\ 5y_0 + 4y_1 + y_3 & 5y_0 + 6y_1 + 6y_2 + y_3 & 2y_0 + 4y_1 + 4y_2 + 5y_3 & 0 & f_3 \\ 6y_0 + 4y_1 + y_2 + 2y_3 & 5y_1 + y_2 + 4y_3 & 5y_0 + y_1 + 6y_2 + 5y_3 & 0 & f_4 \\ 6y_0 + 3y_1 + 2y_2 + 2y_3 & 3y_0 + 4y_2 + 4y_3 & 6y_0 + 5y_1 + 5y_2 + 5y_3 & 0 & f_5 \end{pmatrix}\\
= \ &0.
\end{aligned}$$

The above results imply that for all $g \in M_{\mathbf{x}}^{(i-1)}$ (resp. $g \in M_{\mathbf{y}}^{(i-1)}$), the rows of signature $(\mathsf{LM}(g), f_i)$ are reduced to zero during the Matrix F_5 Algorithm. In order to remove these rows, it is crucial to compute a Gröbner basis of the ideals $M_{\mathbf{x}}^{(i-1)}$ and $M_{\mathbf{y}}^{(i-1)}$. These ideals are generated by the maximal minors of matrices whose entries are linear forms. The goal of the following section is to understand the structure of such ideals and how Gröbner bases can be efficiently computed in that case.

3.3. Gröbner bases and maximal minors of matrices with linear entries

Let $\mathscr{L}$ be the set of homogeneous linear forms in the ring $R_{\mathbf{X}} = k[x_0, \ldots, x_{n_x}]$, $\prec$ be the *grevlex* ordering on $R_{\mathbf{X}}$ (with $x_0 \succ \cdots \succ x_{n_x}$) and $\mathsf{Mat}_{\mathscr{L}}(p, q)$ be the set of $p \times q$ matrices with entries in $\mathscr{L}$ with $p \geq q$ and $n_x \geq p - q$. Note that $\mathsf{Mat}_{\mathscr{L}}(p, q)$ is a k-vector space of finite dimension.

Given $\mathsf{M} \in \mathsf{Mat}_{\mathscr{L}}(p, q)$, we denote by $\mathsf{MaxMinors}(\mathsf{M})$ the set of maximal minors of M. We denote by $\mathsf{Macaulay}_{\prec}(\mathsf{MaxMinors}(\mathsf{M}), q)$ the Macaulay matrix in degree q associated to $\mathsf{MaxMinors}(\mathsf{M})$ and to the ordering $\prec$ (each row represents a polynomial of $\mathsf{MaxMinors}(\mathsf{M})$ and the columns represent the monomials of degree q in $k[x_0, \ldots, x_{n_x}]$ sorted by $\prec$, see Definition 5).

The main result of this paragraph lies in the following theorem: it states that, in general, a Gröbner basis of $\langle \mathsf{MaxMinors}(\mathsf{M}) \rangle$ is a *linear* combination of the generators.

Theorem 3. *There exists a nonempty Zariski-open set O in $\mathsf{Mat}_{\mathscr{L}}(p, q)$ such that for all $\mathsf{M} \in O$, a grevlex Gröbner basis of $\langle \mathsf{MaxMinors}(\mathsf{M}) \rangle$ with respect to $\prec$ is obtained by computing the row echelon form of $\mathsf{Macaulay}_{\prec}(\mathsf{MaxMinors}(\mathsf{M}), q)$.*

This theorem is related with a result from Sturmfels, Bernstein and Zelevinsky (1993), which states that the ideal generated by the maximal minors of a matrix whose entries are variables is a universal Gröbner Basis. We tried without success to use this result in order to prove Theorem 3. Therefore, we propose an ad-hoc proof, which is based on the following Lemmas whose proofs are postponed to the end of the paragraph.

Lemma 3. *Let $\mathsf{Monomials}_{p-q}(q)$ be the set of monomials of degree q in $k[x_0, \ldots, x_{p-q}]$. There exists a Zariski-open subset O' of $\mathsf{Mat}_{\mathscr{L}}(p, q)$ such that for all $\mathsf{M} \in O'$*

$$\langle \mathsf{Monomials}_{p-q}(q) \rangle \subset \mathsf{LM}(\langle \mathsf{MaxMinors}(\mathsf{M}) \rangle)$$

Lemma 4. *Let $\mathsf{Monomials}_{p-q}(q)$ be the set of monomials of degree q in $k[x_0, \ldots, x_{p-q}]$. There exists a Zariski-open subset O'' of $\mathsf{Mat}_{\mathscr{L}}(p, q)$ such that for all $\mathsf{M} \in O''$*

$$\mathsf{LM}(\langle \mathsf{MaxMinors}(\mathsf{M}) \rangle) \subset \langle \mathsf{Monomials}_{p-q}(q) \rangle$$

Lemma 5. *The Zariski-open set $O' \cap O'' \subset \mathsf{Mat}_{\mathscr{L}}(p, q)$ is nonempty.*

Proof of Theorem 3. From Lemmas 3, 4 and 5, $O = O' \cap O''$ is a nonempty Zariski open set. Now let M be a matrix in $O \subset \mathsf{Mat}_{\mathscr{L}}(p, q)$.

$$\langle \mathsf{Monomials}_{p-q}(q) \rangle = \mathsf{LM}(\langle \mathsf{MaxMinors}(\mathsf{M}) \rangle).$$

Thus all polynomials in a minimal Gröbner basis of $\langle \mathsf{MaxMinors}(\mathsf{M}) \rangle$ have degree q and then can be obtained by computing the row echelon form of $\mathsf{Macaulay}_{\prec}(\mathsf{MaxMinors}(\mathsf{M}), q)$. □

We prove now Lemmas 3, 4 and 5.

Proof of Lemma 3. Let $\mathfrak{M}$ be the (p,q)-matrix whose (i,j)-entry is a generic homogeneous linear form $\sum_{k=0}^{n_x} \mathfrak{a}_k^{(i,j)} x_k \in k(\mathfrak{a}_0^{(i,j)}, \dots, \mathfrak{a}_k^{(i,j)})[x_0, \dots, x_{n_x}]$. Denote by $\mathfrak{a}$ the set

$$\mathfrak{a} = \{\mathfrak{a}_k^{(i,j)}, 0 \le k \le n_x,\ 1 \le i \le p,\ 1 \le j \le q\}.$$

Given a set

$$\mathbf{a} = \{\mathbf{a}_k^{(i,j)} \in k, 0 \le k \le n_x,\ 1 \le i \le p,\ 1 \le j \le q\}$$

consider the specialization map $\varphi_{\mathbf{a}} : \mathfrak{M} \mapsto \mathfrak{M}_{\mathbf{a}} \in \mathsf{Mat}_{\mathscr{L}}(p,q)$ such that the (i,j)-entry of $\mathfrak{M}_{\mathbf{a}}$ is $\sum_{k=0}^{n_x} \mathbf{a}_k^{(i,j)} x_k \in k[x_0, \dots, x_{n_x}]$. We prove below that there exists a polynomial $g \in k[\mathfrak{a}]$ such that, if $g(\mathbf{a}) \neq 0$ then

$$\langle \mathsf{Monomials}_{p-q}(q) \rangle \subset \mathsf{LM}(\langle \mathsf{MaxMinors}(\varphi_{\mathbf{a}}(\mathfrak{M})) \rangle).$$

Consider the Macaulay matrix $\mathsf{Macaulay}_{\prec}(\mathsf{MaxMinors}(\mathfrak{M}), q)$.

Remark that the number of monomials in $\mathsf{Monomials}_{p-q}(q)$ equals the number of maximal minors of $\mathfrak{M}$. Moreover, by construction of $\mathsf{Macaulay}_{\prec}(\mathsf{MaxMinors}(\mathfrak{M}), q)$ and by definition of $\prec$ (see Definition 1), the first $\binom{p}{q}$ columns of $\mathsf{Macaulay}_{\prec}(\mathsf{MaxMinors}(\mathfrak{M}), q)$ contain the coefficients of the monomials in $\mathsf{Monomials}_{p-q}(q)$ of the polynomials in $\mathsf{MaxMinors}(\mathfrak{M})$.

Saying that $\langle \mathsf{Monomials}_{p-q}(q) \rangle \subset \mathsf{LM}(\langle \mathsf{MaxMinors}(\mathfrak{M}) \rangle)$ is equivalent to saying that the determinant of the square submatrix of $\mathsf{Macaulay}_{\prec}(\mathsf{MaxMinors}(\mathfrak{M}), q)$ containing its first $\binom{p}{q}$ columns is non-zero. Let $g \in k[\mathfrak{a}]$ be this determinant.

The inequality $g \neq 0$ defines a Zariski-open set O' such that for all $\mathbf{a} \in O'$

$$\langle \mathsf{Monomials}_{p-q}(q) \rangle \subset \mathsf{LM}(\langle \mathsf{MaxMinors}(\varphi_{\mathbf{a}}(\mathfrak{M})) \rangle).$$

□

In the following ψ denotes the canonical inclusion morphism from $k[x_0, \dots, x_{n_x}]$ to $k'[x_0, \dots, x_{p-q}]$, where k' is the field of fractions $k(x_{p-q+1}, \dots, x_{n_x})$.

For $(v_1, \dots, v_{n_x-p+q})$, $\psi_{\mathbf{v}}$ denotes the specialization morphism:

$$\begin{array}{rccc} \psi_{\mathbf{v}} : & k[x_0, \dots, x_{n_x}] & \longrightarrow & k[x_0, \dots, x_{p-q}] \\ & f(x_0, \dots, x_{n_x}) & \longmapsto & f(x_0, \dots, x_{p-q}, v_1, \dots, v_{n_x-p+q}) \end{array}$$

Lemma 6. *There exists a Zariski open set O''', such that if $\mathbf{a} \in O'''$, then the ideal $\langle \mathsf{MaxMinors}(\psi \circ \varphi_{\mathbf{a}}(\mathfrak{M})) \rangle$ is radical and its degree is $\binom{p}{q-1}$.*

Proof. There exists an affine bilinear system $f_1, \dots, f_p \in k'(\mathfrak{a})[x_0, \dots, x_{p-q}, y_0, \dots, y_{q-2}]$, such that:

$$\psi(\mathfrak{M}) \cdot \begin{pmatrix} y_0 \\ \vdots \\ y_{q-2} \\ 1 \end{pmatrix} = \begin{pmatrix} f_1 \\ \vdots \\ f_p \end{pmatrix}.$$

Let I denote the ideal $\langle f_1, \dots, f_p\rangle$. According to Lemma 17 (in Appendix), there exists a polynomial $h_1 \in k[\mathfrak{a}]$, such that if $h_1(\mathbf{a}) \neq 0$, then $\sqrt{\langle \mathsf{MaxMinors}(\psi \circ \varphi_{\mathbf{a}}(\mathfrak{M}))\rangle} = \langle \varphi_{\mathbf{a}}(f_1), \dots, \varphi_{\mathbf{a}}(f_p)\rangle \cap k'[x_0, \dots, x_{p-q}]$.

One remarks that there also exists a polynomial $h_2 \in k[\mathfrak{a}]$ such that if $h_2(\mathbf{a}) \neq 0$, then $\varphi_{\mathbf{a}}(I)$ is 0-dimensional (since $f_1, \dots, f_p$ is a generic affine bilinear system with p equations and p variables, see Proposition 8). From Lemma 16 (in Appendix), there exists a polynomial h_3 such that if $h_3(\mathbf{a}) \neq 0$, then $\varphi_{\mathbf{a}}(I)$ is radical. From now on, we suppose that $h_1(\mathbf{a})h_2(\mathbf{a})h_3(\mathbf{a}) \neq 0$. If $(w_0, \dots, w_{p-q}) \in Var(\langle \mathsf{MaxMinors}(\psi \circ \varphi_{\mathbf{a}}(\mathfrak{M}))\rangle)$ (where Var denotes the variety), then the set of points in $Var(\varphi_{\mathbf{a}}(I))$ whose projection is $(w_0, \dots, w_{p-q})$ can be obtained by solving an affine linear system. The set of solutions of this system is nonempty and finite (since $\varphi_{\mathbf{a}}(I)$ is 0-dimensional), thus it contains a unique element. So there is a bijection between $Var(\varphi_{\mathbf{a}}(I))$ and $Var(\langle \mathsf{MaxMinors}(\psi \circ \varphi_{\mathbf{a}}(\mathfrak{M}))\rangle)$. As $\varphi_{\mathbf{a}}(I)$ is radical,

$$\deg(\varphi_{\mathbf{a}}(I)) = \deg(\sqrt{\langle \mathsf{MaxMinors}(\psi \circ \varphi_{\mathbf{a}}(\mathfrak{M}))\rangle}).$$

By Corollary 4, this degree is $\binom{p}{q-1}$. According to Lemma 3,

$$\begin{aligned}\deg(\sqrt{\langle \mathsf{MaxMinors}(\psi \circ \varphi_{\mathbf{a}}(\mathfrak{M}))\rangle}) &\leq \deg(\langle \mathsf{MaxMinors}(\psi \circ \varphi_{\mathbf{a}}(\mathfrak{M}))\rangle) \\ &\leq \deg(\langle \mathsf{Monomials}_{p-q}(q)\rangle) = \binom{p}{q-1}.\end{aligned}$$

Therefore,

$$\deg(\sqrt{\langle \mathsf{MaxMinors}(\psi \circ \varphi_{\mathbf{a}}(\mathfrak{M}))\rangle}) = \deg(\langle \mathsf{MaxMinors}(\psi \circ \varphi_{\mathbf{a}}(\mathfrak{M}))\rangle)$$

and thus

$$\sqrt{\langle \mathsf{MaxMinors}(\psi \circ \varphi_{\mathbf{a}}(\mathfrak{M}))\rangle} = \langle \mathsf{MaxMinors}(\psi \circ \varphi_{\mathbf{a}}(\mathfrak{M}))\rangle.$$

Furthermore, the inequality $h_1(\mathbf{a})h_2(\mathbf{a})h_3(\mathbf{a}) \neq 0$ defines the wanted Zariski open set. □

Proof of Lemma 4. Consider the Zariski open set $O'' = O' \cap O'''$ (where O' is defined in Lemma 3 and O''' is defined in Lemma 6) and let $\mathbf{a}$ be taken in O''. According to Lemma 3,

$$\mathsf{Monomials}_{p-q}(q) \subset \mathsf{LM}(\langle \mathsf{MaxMinors}(\psi \circ \varphi_{\mathbf{a}}(\mathfrak{M}))\rangle).$$

A basis of $k'[x_0, \dots, x_{p-q}]/\langle \mathsf{Monomials}_{p-q}(q)\rangle$ is given by the set of all monomials of degree less than q. Therefore, the dimension of $k'[x_0, \dots, x_{p-q}]/\langle \mathsf{Monomials}_{p-q}(q)\rangle$ (as a k'-vector space) is $\binom{p}{q-1}$. Thus, from Lemma 6,

$$\deg(\langle \mathsf{MaxMinors}(\psi \circ \varphi_{\mathbf{a}}(\mathfrak{M}))\rangle) = \binom{p}{q-1} = \deg(\langle \mathsf{Monomials}_{p-q}(q)\rangle).$$

Therefore, all polynomials in $\langle \mathsf{MaxMinors}(\psi \circ \varphi_{\mathbf{a}}(\mathfrak{M}))\rangle$ have degree at least q.

Now let $g \neq 0$ be a polynomial in $\langle \mathsf{MaxMinors}(\varphi_{\mathbf{a}}(\mathfrak{M}))\rangle$. Then there exists $\mathbf{v} = (v_1, \dots, v_{n_x-p+q})$ such that the specialized polynomial verifies $\psi_{\mathbf{v}}(g) \neq 0$ and such that $\deg(\langle \mathsf{MaxMinors}(\psi_{\mathbf{v}} \circ \varphi_{\mathbf{a}}(\mathfrak{M}))\rangle) = \binom{p}{q-1}$. Thus $\psi_{\mathbf{v}}(g)$ is a polynomial of degree at least q in $k[x_0, \dots, x_{p-q}]$. Now suppose by contradiction that $\mathsf{LM}(g) \notin \langle \mathsf{Monomials}_{p-q}(q)\rangle$. Since $\deg(\psi_{\mathbf{v}}(g)) \geq q$, there exists a monomial $\mathfrak{m}$ in g such that $\mathfrak{m} \in \langle \mathsf{Monomials}_{p-q}(q)\rangle$. Thus consider $g_1 = g - \lambda\mathfrak{m} + \lambda\mathsf{NF}(\mathfrak{m})$ (where λ is the coefficient of $\mathfrak{m}$ in g). One remarks that

$\mathsf{LM}(g) = \mathsf{LM}(g_1) \notin \langle \mathsf{Monomials}_{p-q}(q) \rangle$. Since $g_1 \in \langle \mathsf{MaxMinors}(\varphi_{\mathbf{a}}(\mathfrak{M})) \rangle$, by a similar argument there also exists a monomial $\mathfrak{m}_1 \in \langle \mathsf{Monomials}_{p-q}(q) \rangle$ in g_1. By induction construct the sequence $g_i = g_{i-1} - \lambda_{i-1}\mathfrak{m}_{i-1} + \lambda_{i-1}\mathsf{NF}(\mathfrak{m}_{i-1})$. This sequence is infinite and strictly decreasing (for the induced partial ordering on polynomials: $h_1 \prec h_2$ if $\mathsf{LM}(h_1) \prec \mathsf{LM}(h_2)$ or if $\mathsf{LM}(h_1) = \mathsf{LM}(h_2)$ and $h_1 - \mathsf{LM}(h_1) \prec h_2 - \mathsf{LM}(h_2)$). But, when $\prec$ is the grevlex ordering, there does not exist such an infinite and strictly decreasing sequence.

Therefore $\mathsf{LM}(g) \in \langle \mathsf{Monomials}_{p-q}(q) \rangle$, which concludes the proof. □

Proof of Lemma 5. In order to prove that the Zariski open set $O' \cap O''$ is nonempty, we exhibit an explicit element. Consider the matrix M of $\mathsf{Mat}_{\mathscr{L}}(p, q)$ whose (i, j)-entry is x_{i+j-2} if $0 \leq i + j - 2 \leq p - q$ and $i \geq j$, else it is 0.

$$\mathsf{M} = \begin{pmatrix} x_0 & 0 & \dots & 0 \\ x_1 & x_0 & \ddots & 0 \\ \vdots & x_1 & \ddots & \vdots \\ x_{p-q} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & x_{p-q-1} \\ 0 & 0 & \dots & x_{p-q} \end{pmatrix}.$$

Remark that $\mathsf{MaxMinors}(\mathsf{M}) \subset k[x_0, \dots, x_{p-q}]$. Since $\langle \mathsf{Monomials}_{p-q}(q) \rangle$ is a zero-dimensional ideal in $k[x_0, \dots, x_{p-q}]$, the fact that $\mathsf{LM}(\mathsf{MaxMinors}(\mathsf{M})) = \mathsf{Monomials}_{p-q}(q)$ implies that $\mathsf{LM}(\langle \mathsf{MaxMinors}(\mathsf{M}) \rangle) = \langle \mathsf{Monomials}_{p-q}(q) \rangle$. Thus, we prove in the sequel that $\mathsf{LM}(\mathsf{MaxMinors}(\mathsf{M})) = \mathsf{Monomials}_{p-q}(q)$.

A first observation is that the cardinality of $\mathsf{MaxMinors}(\mathsf{M})$ equals the cardinality of $\mathsf{Monomials}_{p-q}(q)$. Let m be a maximal minor of M. Thus m is the determinant of a $q \times q$ submatrix M' obtained by removing $p - q$ rows from M. Let $i_1, \dots, i_{p-q}$ be the indices of these rows (with $i_1 < \dots < i_{p-q}$). Denote by $\star$ the product coefficient by coefficient of two matrices (i.e. the *Hadamard product*) and let $\mathfrak{S}_q$ be the set of $q \times q$ permutation matrices. Thus $m = \sum_{\sigma \in \mathfrak{S}_q} (-1)^{\mathsf{sgn}(\sigma)} \det(\sigma \star \mathsf{M}')$.

Since for all $\sigma \in \mathfrak{S}_q$, $\det(\sigma \star \mathsf{M}')$ is a monomial, there exists $\sigma^0 \in \mathfrak{S}_q$ such that $\mathsf{LM}(m) = \pm \det(\sigma^0 \star \mathsf{M}')$

We prove now that $\sigma^0 = \mathsf{id}$. Suppose by contradiction that $\sigma^0 \neq \mathsf{id}$. In the sequel, we denote by

- $\mathsf{M}'[i, j]$ the (i, j)-entry of M'.
- $\mathbf{e}_i$ the $q \times 1$ unit vector whose i-th coordinate is 1 and all its other coordinates are 0;
- σ^0_j is the integer i such that $\sigma^0 \mathbf{e}_j = \mathbf{e}_i$.

Since, by assumption, $\sigma^0 \neq \mathsf{id}$, there exists $1 \leq i < j \leq q$ such that $\sigma^0_j > \sigma^0_i$. Because of the structure of M, we know that for the *grevlex* ordering $x_0 \succ \dots \succ x_{n_x}$,

$$\mathsf{M}'[i, \sigma^0_j]\mathsf{M}'[j, \sigma^0_i] \succ \mathsf{M}'[i, \sigma^0_i]\mathsf{M}'[j, \sigma^0_j].$$

Let σ' be defined by

$$\sigma'_k = \begin{cases} \sigma^0_k \text{ if } k \neq i \text{ and } k \neq j \\ \sigma^0_j \text{ if } k = i \\ \sigma^0_i \text{ if } k = j \end{cases}$$

Then $\det(\sigma' \star \mathsf{M}') \succ \det(\sigma^0 \star \mathsf{M}')$ and by induction $\det(\mathsf{id} \star \mathsf{M}') \succ \det(\sigma^0 \star \mathsf{M}')$. This also proves that the coefficient of $\det(\mathsf{id} \star \mathsf{M}')$ in $\mathsf{MaxMinors}(\mathsf{M})$ is 1 and contradicts the fact that $\mathsf{LM}(m) = \pm\det(\sigma^0 \star \mathsf{M}')$.

This proved that $\mathsf{LM}(m) = |\det(\mathsf{id} \star \mathsf{M}')|$. Now one can remark that

$$\det(\mathsf{id} \star \mathsf{M}') = x_0^{i_1-1} x_1^{i_2-i_1-1} x_2^{i_3-i_2-1} \ldots x_{p-q}^{p-i_{p-q}-1}.$$

Thus if m_1, m_2 are distinct elements in $\mathsf{MaxMinors}(\mathsf{M})$, then $\mathsf{LM}(m_1) \neq \mathsf{LM}(m_2)$. Since for all m in $\mathsf{MaxMinors}(\mathsf{M})$, $\mathsf{LM}(m) \in \mathsf{Monomials}_{p-q}(q)$, and $\mathsf{MaxMinors}(\mathsf{M})$ has the same cardinality as $\mathsf{Monomials}_{p-q}(q)$, we can deduce that $\mathsf{LM}(\mathsf{MaxMinors}(\mathsf{M})) = \mathsf{Monomials}_{p-q}(q)$. □

3.4. An extension of the F_5 criterion for bilinear systems

We can now present the main algorithm of this section. Given a sequence of homogeneous bilinear forms $F = (f_1, \ldots, f_m) \subset R$ generating an ideal $I \subset R$ and $\prec$ a monomial ordering, it returns a set of pairs (g, f_i) such that $g \in I_{i-1} : f_i$ and $g \notin I_{i-1}$ (for $i > \min(n_x+1, n_y+1)$). Following Theorem 2 and 3, this is done by considering the matrices $\mathsf{jac}_{\mathbf{x}}(F_i)$ (resp. $\mathsf{jac}_{\mathbf{y}}(F_i)$) for $i > n_x + 1$ (resp. $i > n_y + 1$) and performing a row echelon form on $\mathsf{Macaulay}_{\prec}(\mathsf{MaxMinors}(\mathsf{jac}_{\mathbf{x}}(F_i)), n_x + 1)$ (resp. $\mathsf{Macaulay}_{\prec}(\mathsf{MaxMinors}(\mathsf{jac}_{\mathbf{y}}(F_i)), n_y + 1)$).

First we describe the subroutine **Reduce** (Algorithm 3) which reduces a set of homogeneous polynomials of the same degree:

Algorithm 3. Reduce

Require: *$\prec$ a monomial ordering and (S, q) where S is a set of homogeneous polynomials of degree q.*

Ensure: *T is a reduced set of homogeneous polynomials of degree q.*

1: $\mathsf{M} \leftarrow \mathsf{Macaulay}_{\prec}(S, q)$.

2: $\mathsf{M} \leftarrow \mathsf{RowEchelonForm}(\mathsf{M})$.

3: Return T the set of polynomials corresponding to the rows of M.

The main algorithm uses this subroutine in order to compute a row echelon form of $\mathsf{Macaulay}_{\prec}(\mathsf{MaxMinors}(\mathsf{jac}_{\mathbf{x}}(F_i)), n_x+1)$ (resp. $\mathsf{Macaulay}_{\prec}(\mathsf{MaxMinors}(\mathsf{jac}_{\mathbf{y}}(F_i)), n_y+1)$):

Algorithm 4. BLcriterion

Require: $\begin{cases} m \text{ bilinear polynomials } f_1, \ldots, f_m \text{ such that } m \leq n_x + n_y. \\ \prec \text{ a monomial ordering over } k[x_0, \ldots, x_{n_x}, y_0, \ldots, y_{n_y}] \end{cases}$

Ensure: *V a set of pairs (h, f_i) such that $h \in I_{i-1} : f_i$ and $h \notin I_{i-1}$.*

1: $V \leftarrow \emptyset$

2: ***for*** *i from 2 to m* ***do***

3: ***if*** $i > n_y + 1$ ***then***

4: $T \leftarrow$ **Reduce**$(\mathsf{MaxMinors}(\mathsf{jac}_{\mathbf{y}}(F_{i-1})), n_y + 1)$.

  for h *in* T ***do***
   $V \leftarrow V \cup \{(h, f_i)\}$
  end for
 end if
 if $i > n_x + 1$ ***then***
  $T' \leftarrow \mathbf{Reduce}(\mathsf{MaxMinors}(\mathsf{jac}_{\mathbf{x}}(F_{i-1})), n_x + 1)$.
  for h *in* T' ***do***
   $V \leftarrow V \cup \{(h, f_i)\}$
  end for
 end if
end for
Return V

The following proposition explains how the output of Algorithm 4 is related to reductions to zero occurring during the Matrix F_5 Algorithm.

Proposition 1 (Extended F_5 criterion for bilinear systems)**.** *Let $f_1, \dots, f_m$ be bilinear polynomials and $\prec$ be a monomial ordering. Let (t, f_i) be the signature of a row during the Matrix F_5 Algorithm and let V be the output of Algorithm* BLcriterion*. Then if there exists (h, f_i) in V such that $\mathsf{LM}(h) = t$, then the row with signature (t, f_i) will be reduced to zero.*

Proof. According to Theorem 2, $hf_i \in I_{i-1}$. Therefore

$$tf_i = (h - t)f_i + \sum_{j=1}^{i-1} g_j f_j.$$

This implies that the row with signature (t, f_i) is a linear combination of preceding rows in $\mathsf{Macaulay}(F_i, \deg(tf_i))$. Hence this row will be reduced to zero. □

Now we can merge this extended criterion with the Matrix F_5 Algorithm. To do so, we denote by V the output of BLcriterion (V has to be computed at the beginning of Matrix F_5 Algorithm), and we replace in Algorithm 2 the F_5criterion by the following BilinF_5criterion:

Algorithm 5. BilinF_5criterion - *returns a boolean*

Require: $\begin{cases} (t, f_i) \text{ the signature of a row} \\ \text{A matrix } \mathcal{M} \text{ in row echelon form} \end{cases}$

Return `true` *if* $\begin{cases} t \text{ is the leading monomial of a row of } \mathcal{M} \textbf{ or} \\ \exists (h, f_i) \in V \text{ such that } \mathsf{LM}(h) = t \end{cases}$

4. F_5 without reduction to zero for generic bilinear systems

4.1. Main results

The goal of this part of the paper is to show that Algorithm 4 finds all reductions to zero for generic bilinear systems. In order to describe the structure of ideals generated by generic bilinear systems, we define a notion of *bi-regularity* (Definition 8). For bi-regular systems, we give a complete description of the syzygy module (Proposition 3 and Corollary 2). Finally, we show that, for such systems, Algorithm 4 finds all reductions to zero and that generic bilinear systems are bi-regular (Theorem 4), assuming a conjecture about the kernel of generic matrices whose entries are linear forms (Conjecture 1).

4.2. Kernel of matrices whose entries are linear forms

Consider a monomial ordering $\prec$ such that its restriction to $k[x_0,\ldots,x_{n_x}]$ (resp. $k[y_0,\ldots,y_{n_y}]$) is the *grevlex* ordering (for instance the usual *grevlex* ordering with $x_0 \succ x_1 \succ \ldots \succ y_0 \succ \ldots \succ y_{n_y}$).

Let ℓ, c, n_x be integers such that $c < \ell \leq n_x + c - 1$. Let $\mathcal{M}$ be the set of matrices $\ell \times c$ whose coefficients are linear forms in $k[x_0,\ldots,x_{n_x}]$. Let $\mathcal{T}$ be the set of $\ell \times (\ell - c - 1)$ matrices T such that:

- each column of T has exactly one 1 and the rest of the coefficients are 0.
- each row of T has at most one 1 and all the other coefficients are 0.
- $(\mathsf{T}[i_1,j_1] = \mathsf{T}[i_2,j_2] = 1$ and $i_1 < i_2) \Rightarrow j_1 < j_2$

If $\mathsf{T} \in \mathcal{T}$ and $\mathsf{M} \in \mathcal{M}$, we denote by M_T the $\ell \times (\ell - 1)$ matrix obtained by adding to M the columns of T. According to the proof of Lemma 2, some elements of the left kernel of a matrix M can be expressed as vectors of maximal minors:

$$\forall \mathsf{T} \in \mathcal{T}, \begin{pmatrix} \mathsf{minor}(\mathsf{M}_\mathsf{T}, 1) \\ -\mathsf{minor}(\mathsf{M}_\mathsf{T}, 2) \\ \vdots \\ (-1)^{m+1}\mathsf{minor}(\mathsf{M}_\mathsf{T}, m) \end{pmatrix} \in \mathsf{Ker}_L(\mathsf{M}).$$

Actually, we observed experimentally that kernels of random matrices $\mathsf{M} \in \mathcal{M}$ are generated by those vectors of minors. This leads to the formulation of the following conjecture:

Conjecture 1. *The set of matrices* $\mathsf{M} \in \mathcal{M}$ *such that*

$$\mathsf{Ker}_L(\mathsf{M}) = \left\langle \left\{ \begin{pmatrix} \mathsf{minor}(\mathsf{M}_\mathsf{T}, 1) \\ -\mathsf{minor}(\mathsf{M}_\mathsf{T}, 2) \\ \vdots \\ (-1)^{m+1}\mathsf{minor}(\mathsf{M}_\mathsf{T}, m) \end{pmatrix} \right\}_{\mathsf{T} \in \mathcal{T}} \right\rangle$$

contains a nonempty Zariski open subset of $\mathcal{M}$.

4.3. Structure of generic bilinear systems

With the following definition, we try to give an analog of regular sequences for bilinear systems. This definition is closely related to the generic behaviour of Algorithm 4.

Remark 1. *In the following,* $\mathsf{Monomials}^{\mathbf{x}}_n(d)$ *(resp.* $\mathsf{Monomials}^{\mathbf{y}}_n(d)$*) denotes the set of monomials of degree d in $k[x_0,\ldots,x_n]$ (resp. $k[y_0,\ldots,y_n]$). If $n < 0$, we use the convention* $\mathsf{Monomials}^{\mathbf{x}}_n(d) = \mathsf{Monomials}^{\mathbf{y}}_n(d) = \emptyset$.

Definition 8. *Let $\prec$ be a monomial ordering such that its restriction to $k[x_0, \ldots, x_{n_x}]$ (resp. $k[y_0, \ldots, y_{n_y}]$) is the grevlex ordering. Let $m \leq n_x + n_y$ and $f_1, \ldots, f_m$ be bilinear polynomials of R. We say that the polynomial sequence $(f_1, \ldots, f_m)$ is a* bi-regular sequence *if $m = 1$ or if $(f_1, \ldots, f_{m-1})$ is a bi-regular sequence and*

$$\begin{aligned}\mathsf{LM}(I_{m-1} : f_m) \quad &= \langle \mathsf{Monomials}^{\mathbf{x}}_{m-n_y-2}(n_y+1)\rangle \\ &+\langle \mathsf{Monomials}^{\mathbf{y}}_{m-n_x-2}(n_x+1)\rangle \\ &+\mathsf{LM}(I_{m-1})\end{aligned}$$

In the following, we use the notations:

- $\mathcal{BL}(n_x, n_y)$ the k-vector space of bilinear polynomials in $K[x_0, \ldots, x_{n_x}, y_0, \ldots, y_{n_y}]$;
- X (resp. Y) is the ideal $\langle x_0, \ldots, x_{n_x}\rangle$ (resp. $\langle y_0, \ldots, y_{n_y}\rangle$);
- An ideal is called *bihomogeneous* if it admits a set of bihomogeneous generators.
- J_i denotes the saturated ideal $I_i : (X \cap Y)^\infty$;
- Given a polynomial sequence $(f_1, \ldots, f_m)$, we denote by Syz_{triv} the module of trivial syzygies, i.e. the set of all syzygies $(s_1, \ldots, s_m)$ such that

$$\forall i, s_i \in \langle f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_m\rangle;$$

- A primary ideal $P \subset R$ is called *admissible* if $X \not\subset \sqrt{P}$ and $Y \not\subset \sqrt{P}$;
- Let E be a k-vector space such that $\dim(E) < \infty$. We say that a property $\mathcal{P}$ is *generic* if it is satisfied on a nonempty open subset of E (for the Zariski topology), i.e. $\exists h \in k[\mathfrak{a}_1, \ldots, \mathfrak{a}_{\dim(E)}], h \neq 0$, such that

$$\mathcal{P} \text{ does not hold on } (a_1, \ldots, a_{\dim(E)}) \Rightarrow h(a_1, \ldots, a_{\dim(E)}) = 0.$$

Without loss of generality, we suppose in the sequel that $n_x \leq n_y$.

Lemma 7. *Let I_m be an ideal spanned by m generic bilinear equations $f_1, \ldots, f_m$ and $I_m = \cap_{P \in \mathcal{P}} P$ be a minimal primary decomposition.*

- *If $m < n_x + 1$, then all components of I_m are admissible.*
- *If $n_x + 1 \leq m < n_y + 1$ and $P_0 \in \mathcal{P}$ is a primary non-admissible component, then $Y \not\subset \sqrt{P_0}$.*

Proof. We prove that if $m < n_x+1$ (resp. $m < n_y+1$) and P_0 is a primary non-admissible component, then $X \not\subset \sqrt{P_0}$ (resp. $Y \not\subset \sqrt{P_0}$). Lemma 7 is a consequence of this fact.

Consider the field $k' = k(y_0, \ldots, y_{n_y})$ and the canonical inclusion

$$\psi : R \to k'[x_0, \ldots, x_{n_x}].$$

$\psi(I_m)$ is an ideal of $k'[x_0, \ldots, x_{n_x}]$ spanned by m polynomials in $k'[x_0, \ldots, x_{n_x}]$. Generically, $(\psi(f_1), \ldots, \psi(f_m))$ is a regular sequence of $k'[x_0, \ldots, x_{n_x}]$. Thus there exists an polynomial $f \in X$ (homogeneous in the x_is) such that $\psi(f)$ is not a divisor of 0 in

$k'[x_0, \ldots, x_{n_x}]/\psi(I_m)$. This means that $\psi(I_m) : \psi(f) = \psi(I_m)$. Suppose the assertion of Lemma 7 is false. Then $X \subset \sqrt{P_0}$ and hence, $f \in \sqrt{P_0}$. Therefore there exists $g \in k[y_0, \ldots, y_{n_y}]$ such that, in R, $gf \in \sqrt{I_m}$ (take g in $(\cap_{P \in \mathcal{P} \setminus \{P_0\}} \sqrt{P}) \setminus \{\sqrt{P_0}\}$ which is nonempty). Thus $\psi(f) \in \sqrt{\psi(I_m)}$ (since $\psi(g)$ is invertible in k'), which is impossible since $\psi(I_m) : \psi(f) = \psi(I_m)$. □

Lemma 8.

- *If $m \leq n_x$ there exists a nonempty Zariski-open set $\mathcal{O} \subset \mathcal{BL}_K(n_x, n_y)^m$ such that $(f_1, \ldots, f_m) \subset \mathcal{O}$ implies that I_m has codimension m and all the components of a minimal primary decomposition of I_m are admissible;*
- *if $n_x + 1 \leq m$, then there exists a nonempty Zariski-open set $\mathcal{O} \subset \mathcal{BL}_K(n_x, n_y)^m$ such that $(f_1, \ldots, f_m) \subset \mathcal{O}$ implies that X is a prime associated to $\sqrt{I_m}$;*
- *if $n_y + 1 \leq m$, then there exists a nonempty Zariski-open set $\mathcal{O} \subset \mathcal{BL}_K(n_x, n_y)^m$ such that $(f_1, \ldots, f_m) \subset \mathcal{O}$ implies that Y is a prime associated to $\sqrt{I_m}$.*

Proof.

- If $m \leq n_x$, then by Lemma 7, $J_m = I_m$. Then according to Theorem 7, there exists a nonempty Zariski-open set $\mathcal{O} \subset \mathcal{BL}_K(n_x, n_y)^m$ such that $(f_1, \ldots, f_m) \subset \mathcal{O}$ implies that $(f_1, \ldots, f_m)$ is a regular sequence. Therefore, I_m has codimension m and all the components of a minimal primary decomposition of I_m are admissible.
- If $n_x+1 \leq m$, then according to Proposition 8, $J_m = (I_m : Y^\infty) : X^\infty$ is equidimensional of codimension m. Let V_x be the set $\{(0, \ldots, 0, a_0, \ldots, a_{n_y}) | a_i \in k\}$. Since $V_x \subset Var(I_m : Y^\infty)$ and $\mathsf{codim}(V_x) = n_x+1$, it can be deduced that $V_x \not\subset Var(J_m)$ and $Var(I_m : Y^\infty) = Var(J_m) \cup V_x$. This means that $\sqrt{I_m : Y^\infty} = \sqrt{J_m} \cap X$ and $\sqrt{J_m} \not\subset X$. Thus X is a prime associated to $\sqrt{I_m : Y^\infty}$. Since Y is not a subset of X, X is also a prime ideal associated to $\sqrt{I_m}$.
- Similar proof in the case $n_y + 1 \leq m$.

□

Lemma 9. *Suppose that the local ring R_X/I_X (resp. R_Y/I_Y) is regular and that X (resp. Y) is a prime ideal associated to $\sqrt{I}$ and let Q be an isolated primary component of a minimal primary decomposition of I containing X (resp. Y). Then $Q = X$ (resp. $Q = Y$).*

Proof. By assumption, X is a prime ideal associated to $\sqrt{I}$. Then, there exists an isolated primary component of a minimal primary decomposition of I which contains a power of X and does not meet $R \setminus X$. This proves that I_X does not contain a unit in R_X.

By assumption R_X/I_X is regular and local, then R_X/I_X is an integral ring (see e.g. (Eisenbud, 1995, Corollary 10.14)) which implies that I_X is prime and does not contain a unit in R_X.

Let $I = Q_1 \cap \cdots \cap Q_s$ be a minimal primary decomposition of I. In the sequel, Q_{i_X} denotes the localization of Q_i by X. Suppose first that there exists $1 \leq i \leq s$ such that $I_X = Q_{i_X}$ with Q_i non-admissible which does not meet the multiplicatively closed part $R \setminus X$. Then Q_{i_X} is obviously prime which implies that Q_i itself is prime (Atiyah and MacDonald, 1969, Proposition 3.11 (iv)). Our claim follows.

It remains to prove that $I_X = Q_{i_X}$ for some $1 \leq i \leq s$. Suppose that the Q_i's are numbered such that Q_j meets the multiplicatively closed set $R \setminus X$ for $r + 1 \leq j \leq s$

but not $Q_1, \ldots, Q_r$. $I_X = Q_{1_X} \cap \cdots \cap Q_{r_X}$ and it is a minimal primary decomposition (Atiyah and MacDonald, 1969, Proposition 4.9). Hence, since I_X is prime, $r = 1$ and Q_1 is the isolated minimal primary component containing X. □

Proposition 2. *Let k be a field of characteristic 0. There exists a nonempty Zariski-open set $\mathcal{O} \subset \mathcal{BL}(n_x, n_y)^m$ such that for all $(f_1, \ldots, f_m) \subset \mathcal{O}$ the non-admissible components of a minimal primary decomposition of $\langle f_1, \ldots, f_m\rangle$ are either X or Y.*

Proof. Suppose that $n_x + 1 \leq m$. Then, by Lemma 8, there exists a nonempty Zariski-open set O_1 such that X is an associated prime to $\sqrt{I}$. Note also that this implies that I_X has codimension $n_x + 1$. Thus, by Lemma 9, it is sufficient to prove that there exists a nonempty Zariski-open set O_2 such that for all $(f_1, \ldots, f_m) \in O_1 \cap O_2$, R_X/I_X is a regular local ring.

From the Jacobian Criterion (see e.g. Eisenbud (1995), Theorem 16.19), the local ring R_X/I_X is regular if and only if $\text{jac}(f_1, \ldots, f_m)$ taken modulo X has codimension $n_x + 1$. Since the generators of I are bilinear, the latter condition is equivalent to saying that the matrix

$$J_X = \begin{bmatrix} \frac{\partial f_1}{\partial x_0} & \cdots & \frac{\partial f_1}{\partial x_{n_x}} \\ \vdots & \cdots & \vdots \\ \frac{\partial f_m}{\partial x_0} & \cdots & \frac{\partial f_m}{\partial x_{n_x}} \end{bmatrix}$$

has rank $n_x + 1$. We prove below that there exists a nonempty Zariski-open set O_3 such that for all $(f_1, \ldots, f_m) \in O_3$, J_X has rank $n_x + 1$.

Let $\mathfrak{c}_1, \ldots, \mathfrak{c}_m$ be vectors of coordinates of $\mathcal{BL}(n_x, n_y)^m$, $\mathfrak{M}$ be the vector of all bilinear monomials in R and $\mathfrak{K}$ be the field of rational fractions $k(\mathfrak{c}_1, \ldots, \mathfrak{c}_m)$. Consider the polynomials $\mathfrak{g}_i = \mathfrak{M}.\mathfrak{c}_i^T$ for $1 \leq i \leq m$ and the Zariski-open set O_3 in $\mathcal{BL}(n_x, n_y)^m$ defined by the non-vanishing of all the coefficients of the maximal minors of the generic matrix

$$\mathfrak{J}_X = \begin{bmatrix} \frac{\partial \mathfrak{g}_1}{\partial x_0} & \cdots & \frac{\partial \mathfrak{g}_1}{\partial x_{n_x}} \\ \vdots & \cdots & \vdots \\ \frac{\partial \mathfrak{g}_m}{\partial x_0} & \cdots & \frac{\partial \mathfrak{g}_m}{\partial x_{n_x}} \end{bmatrix}.$$

It is obvious that $(f_1, \ldots, f_m) \in O_3$ implies that J_X has rank $n_x + 1$; our claim follows.

In the case where $n_y \leq m$, the proof follows the same pattern using Lemmas 8 and 9 and the Jacobian criterion. The only difference is that one has to prove that there exists a nonempty Zariski-open set O_4 such that for all $(f_1, \ldots, f_m) \in O_4$ the matrix

$$J_Y = \begin{bmatrix} \frac{\partial f_1}{\partial y_0} & \cdots & \frac{\partial f_1}{\partial y_{n_x}} \\ \vdots & \cdots & \vdots \\ \frac{\partial f_m}{\partial y_0} & \cdots & \frac{\partial f_m}{\partial y_{n_y}} \end{bmatrix}$$

has rank $n_y + 1$, which is done as above. □

Remark 2. *The proof of Proposition 2 relies on the use of the Jacobian Criterion. From (Eisenbud, 1995, Theorem 16.19), it remains valid if the characteristic of k is large enough so that the residue class field of X (resp. Y) is separable.*

The two following propositions explain why the rows reduced to zero in the generic case during the F_5 Algorithm have a signature (t, f_i) such that $t \in k[x_0, \ldots, x_{n_x}]$ or $t \in k[y_0, \ldots, y_{n_y}]$.

Proposition 3. *Let m be an integer such that $m \le n_x + n_y$. Let L be the set of bilinear systems with m polynomials ($L \subset R^m$). Then the set of bilinear systems $f_1, \ldots, f_m$ such that $Syz = \langle (Syz \cap k[x_0, \ldots, x_{n_x}]^m) \cup (Syz \cap k[y_0, \ldots, y_{n_y}]^m) \cup Syz_{triv} \rangle$ contains a nonempty Zariski-open subset of L.*

Proof. Let $s = (s_1, \ldots, s_m)$ be a syzygy. Thus, s_m is in $I_{m-1} : f_m$. We can suppose without loss of generality that the s_i are bihomogeneous of same bidegree (Proposition 6). According to Theorem 7, there exists a nonempty Zariski open set $O_1 \subset \mathcal{BL}(n_x, n_y)^m$, such that if $(f_1, \ldots, f_m) \in O_1$, then f_m is not a divisor of 0 in R/J_{m-1}. We can deduce from this observation that $s_m \in J_{m-1}$. So $s_m \in I_{m-1}$ or there exists P a non-admissible primary component of I_{m-1} such that $s_m \notin P$. Assume that $s_m \notin I_{m-1}$. From Proposition 2, there exists a nonempty Zariski open set $O_2 \subset \mathcal{BL}(n_x, n_y)^m$, such that if $(f_1, \ldots, f_m) \in O_2$, then $\langle x_0, \ldots, x_{n_x} \rangle = P$ (or $\langle y_0, \ldots, y_{n_y} \rangle = P$), which implies that $s_m \in k[y_0, \ldots, y_{n_y}]$ (or $s_m \in k[x_0, \ldots, x_{n_x}]$).

Finally, we see that, if $(f_1, \ldots, f_m) \in O_1 \cap O_2$, then $s_m \in I_{m-1} \cup k[y_0, \ldots, y_{n_y}] \cup k[x_0, \ldots, x_{n_x}]$. Since the syzygy module of a bihomogeneous system is generated by bihomogeneous syzygies, it can be deduced that $Syz = \langle (Syz \cap k[x_0, \ldots, x_{n_x}]^m) \cup (Syz \cap k[y_0, \ldots, y_{n_y}]^m) \cup Syz_{triv} \rangle$. □

Proposition 4. *Let V be the output of Algorithm* BLcriterion *and let (h, f_i) be an element of V. Then*

- *if $h \in k[x_0, \ldots, x_{n_x}]$, then $\forall j, y_j h \in I_{i-1}$.*
- *if $h \in k[y_0, \ldots, y_{n_y}]$, then $\forall j, x_j h \in I_{i-1}$.*

Proof. Suppose that $h \in k[x_0, \ldots, x_{n_x}]$ is a maximal minor of $\mathsf{jac}_{\mathbf{y}}(F_{i-1})$ (the proof is similar if $h \in k[y_0, \ldots, y_{n_y}]$). Consider the matrix $\mathsf{jac}_{\mathbf{y}}(F_{i-1})$ as defined in Algorithm 4. Then there exists an $(i-1) \times (i-1)$ extension M_T of $\mathsf{jac}_{\mathbf{y}}(F_{i-1})$ such that $\det(\mathsf{M}_T) = h$ (similarly to the proof of Lemma 2). Let $0 \le j \le n_y$ be an integer. Consider the polynomials $h_1, \ldots, h_{i-1}$, where h_k is the determinant of the $(i-2) \times (i-2)$ matrix obtained by removing the $(j+1)$th column and the kth row from M_T.

Then we can remark that

$$\begin{pmatrix} h_1 & -h_2 & \ldots & (-1)^i h_{i-1} \end{pmatrix} \cdot \mathsf{M}_T = \begin{pmatrix} 0 & \ldots & 0 & (-1)^j \det(\mathsf{M}_T) & 0 & \ldots & 0 \end{pmatrix}$$

where the only non-zero component is in the $(j+1)$th column. Keeping only the $n_y + 1$ first columns of M_T, we obtain

$$\begin{pmatrix} h_1 & -h_2 & \ldots & (-1)^i h_{i-1} \end{pmatrix} \cdot \mathsf{jac}_{\mathbf{y}}(F_{i-1}) = \begin{pmatrix} 0 & \ldots & 0 & (-1)^j \det(\mathsf{M}_T) & 0 & \ldots & 0 \end{pmatrix}$$

Since $\mathsf{jac}_{\mathbf{y}}(F_{i-1}) \cdot \begin{pmatrix} y_0 \\ \vdots \\ y_{n_y} \end{pmatrix} = \begin{pmatrix} f_1 \\ \vdots \\ f_{i-1} \end{pmatrix}$, the following equality holds

$$\begin{pmatrix} h_1 & -h_2 & \ldots & (-1)^{i-1} h_{i-2} & (-1)^i h_{i-1} \end{pmatrix} \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_{i-1} \end{pmatrix} = y_j \det(\mathsf{M}_T) = y_j h.$$

This implies that $y_j h \in I_{i-1}$. □

Corollary 2. *Let m be an integer such that $m \leq n_x + n_y$ and let $f_1, \ldots, f_m$ be bilinear polynomials. Let V be the output of Algorithm* BLcriterion. *Assume that*

$$(I_{m-1} : f_m) \cap k[x_0, \ldots, x_{n_x}] = \langle \{h \in k[x_0, \ldots, x_{n_x}] \quad : \quad (h, f_m) \in V\} \rangle.$$

$$(I_{m-1} : f_m) \cap k[y_0, \ldots, y_{n_y}] = \langle \{h \in k[y_0, \ldots, y_{n_y}] \quad : \quad (h, f_m) \in V\} \rangle.$$

Let G_x (resp G_y) be a Gröbner basis of $(I_{m-1} : f_m) \cap k[x_0, \ldots, x_{n_x}]$ (resp. $(I_{m-1} : f_m) \cap k[y_0, \ldots, y_{n_y}]$) and let G_{m-1} be a Gröbner basis of I_{m-1}. If $Syz = \langle (Syz \cap k[x_0, \ldots, x_{n_x}]^m) \cup (Syz \cap k[y_0, \ldots, y_{n_y}]^m) \cup Syz_{triv} \rangle$, then $G_x \cup G_y \cup G_{m-1}$ is a Gröbner basis of $I_{m-1} : f_m$.

Proof. Let $f \in I_{m-1} : f_m$ be a polynomial. Thus there exist $s_1, \ldots, s_{m-1}$ such that $(s_1, \ldots, s_{m-1}, f) \in Syz$. Since I_{m-1} and f_m are bihomogeneous, we can suppose without loss of generality that f is bihomogeneous (Proposition 6). Let (d_1, d_2) denote its bidegree.

- If $d_2 = 0$ (resp. $d_1 = 0$), then $f \in \langle G_x \rangle$ (resp. $f \in \langle G_y \rangle$).
- Let $G_x = \{g_i^{(x)}\}_{1 \leq i \leq \mathsf{card}(G_x)}$ and $G_y = \{g_i^{(y)}\}_{1 \leq i \leq \mathsf{card}(G_y)}$. If $d_1 \neq 0$ and $d_2 \neq 0$ then, since $Syz = \langle (Syz \cap k[x_0, \ldots, x_{n_x}]^m) \cup (Syz \cap k[y_0, \ldots, y_{n_y}]^m) \cup Syz_{triv} \rangle$,

$$f = \sum_{1 \leq i \leq \mathsf{card}(G_x)} q_i g_i^{(x)} + \sum_{1 \leq i \leq \mathsf{card}(G_y)} q_i' g_i^{(y)} + t$$

  where $t \in I_{m-1}$ is a bihomogeneous polynomial and the q_i and q_i' are also bihomogeneous. Since $d_2 \neq 0$ and $g_i^{(x)} \in k[x_0, \ldots, x_{n_x}]$, q_i must be in $\langle y_0, \ldots, y_{n_y} \rangle$. According to Proposition 4, $\forall i, q_i g_i^{(x)} \in I_{m-1}$. By a similar argument, $\forall i, q_i' g_i^{(y)} \in I_{m-1}$. Finally, $f \in I_{m-1}$.

We just proved that $I_{m-1} : f_m \subset I_{m-1} \cup \langle G_x \rangle \cup \langle G_y \rangle$. By construction, we also have the other inclusion $I_{m-1} \cup \langle G_x \rangle \cup \langle G_y \rangle \subset I_{m-1} : f_m$. Thus, $G_x \cup G_y \cup G_{m-1}$ is a Gröbner basis of $I_{m-1} : f_m$. □

Corollary 2 shows that, when a bilinear system is bi-regular, it is possible to find a Gröbner basis of $I_{m-1} : f_m$ (which yields the monomials t such that the row (t, f_m) reduces to zero) as soon as we know the three Gröbner bases G_x, G_y, and G_{m-1}. In fact, we only need G_x and G_y since the reductions to zero corresponding to G_{m-1} are eliminated by the usual F_5 criterion. Fortunately, we can obtain G_x and G_y just by performing linear algebra over the maximal minors of a matrix (Theorem 3).

We now present the main result of this section. If we suppose that Conjecture 1 is true, then the following Theorem shows that generic bilinear systems are bi-regular.

Theorem 4. *Let $m, n_x, n_y \in \mathbb{N}$ such that $m < n_x + n_y$. If Conjecture 1 is true, then the set of bi-regular sequences $(f_1, \ldots, f_m)$ contains a nonempty Zariski-open set. Moreover, if $(f_1, \ldots, f_m)$ is a bi-regular sequence, then there are no reductions to zero with the extended F_5 criterion.*

Proof. Let G_m be a minimal Gröbner basis of $I_{m-1} : f_m$. The reductions to zero (t, f_m) which are not detected by the usual F_5 criterion are exactly those such that $t \in \mathsf{LM}(G_m)$ and $t \notin \mathsf{LM}(I_{m-1})$. We showed that there exists a nonempty Zariski-open subset O_1 of $\mathcal{BL}(n_x, n_y)$ such that if $f_m \in O_1$, then $t \in \mathsf{LM}(I_{m-1} : f_m \cap k[x_0, \ldots, x_{n_x}])$ or $t \in \mathsf{LM}(I_{m-1} : f_m \cap k[y_0, \ldots, y_{n_y}])$ (Proposition 3). If we suppose that Conjecture 1 is true, then there exists a nonempty Zariski-open subset O_2 of $\mathcal{BL}(n_x, n_y)$ such that if $f_m \in O_2$, $I_{m-1} : f_m \cap k[x_0, \ldots, x_{n_x}]$ (resp. $I_{m-1} : f_m \cap k[y_0, \ldots, y_{n_y}]$) is spanned by the maximal minors of $\mathsf{jac}_{\mathbf{x}}(F_{m-1})$ (resp. $\mathsf{jac}_{\mathbf{y}}(F_{m-1})$). Thus, by Theorem 3, there exists a nonempty Zariski-open subset O_3 of $\mathcal{BL}(n_x, n_y)$ such that if $f_m \in O_3$, $\mathsf{LM}(I_{m-1} : f_m \cap k[x_0, \ldots, x_{n_x}]) = \mathsf{Monomials}^{\mathbf{x}}_{m-n_y-2}(n_y+1)\rangle$ (resp. $\mathsf{LM}(I_{m-1} : f_m \cap k[y_0, \ldots, y_{n_y}]) = \mathsf{Monomials}^{\mathbf{y}}_{m-n_x-2}(n_x+1)\rangle$). Suppose that $f_m \in O_1 \cap O_2 \cap O_3$ (which is a nonempty Zariski-open subset) and that (t, f_m) is a reduction to zero such that $t \notin \mathsf{LM}(I_{m-1})$. Then

$$t \in \langle \mathsf{Monomials}^{\mathbf{x}}_{m-n_y-2}(n_y+1)\rangle$$

or

$$t \in \langle \mathsf{Monomials}^{\mathbf{y}}_{m-n_x-2}(n_x+1)\rangle.$$

By Lemma 3, t is a leading monomial of a linear combination of the maximal minors of $\mathsf{jac}_{\mathbf{x}}(F_{m-1})$ (or $\mathsf{jac}_{\mathbf{y}}(F_{m-1})$). Consequently, the reduction to zero (t, f_m) is detected by the extended F_5 criterion. □

Remark 3. *Thanks to the analysis of Algorithm 4, we know exactly which reductions to zero can be avoided during the computation of a Gröbner basis of a bilinear system. If a bilinear system is bi-regular, then Algorithm 4 finds all reductions to zero. Indeed, this algorithm detects reductions to zero coming from linear combinations of maximal minors of the matrices* $\mathsf{jac}_{\mathbf{x}}(F_i)$ *and* $\mathsf{jac}_{\mathbf{y}}(F_i)$*. According to Theorem 4, there are no other reductions to zero for bi-regular systems.*

Example 1 (continued). *The system* $f_1, \ldots, f_5$ *given in Example 1 is bi-regular and there are no reduction to zero during the computation of a Gröbner basis with the extended* F_5 *criterion.*

5. Hilbert bi-series of bilinear systems

An important tool to describe ideals spanned by bilinear equations is the so-called *Hilbert series*. In the homogeneous case, complexity results for F_5 were obtained with this tool (see e.g. Bardet et al. (2005)). In this section, we provide an explicit form of the Hilbert bi-series – a bihomogeneous analog of the Hilbert series – for ideals spanned by generic bilinear systems. To find this bi-series, we use the combinatorics of the syzygy module of bi-regular systems. With this tool, we will be able to do a complexity analysis of a special version of the F_5 which will be presented in the next section.

The following notation will be used throughout this paper: the vector space of bihomogeneous polynomials of bidegree (α, β) will be denoted by $R_{\alpha,\beta}$. If I is a bihomogeneous ideal, then $I_{\alpha,\beta}$ will denote the vector space $I \cap R_{\alpha,\beta}$.

Definition 9 (Van der Waerden (1929); Safey El Din and Trébuchet (2006))**.** *Let I be a bihomogeneous ideal of R. The Hilbert bi-series is defined by*

$$\mathrm{HS}_I(t_1, t_2) = \sum_{(\alpha,\beta)\in\mathbb{N}^2} \dim(R_{\alpha,\beta}/I_{\alpha,\beta}) t_1^{\alpha} t_2^{\beta}.$$

Remark 4. *The usual univariate Hilbert series for homogeneous ideals can easily be deduced from the Hilbert bi-series by putting $t_1 = t_2$ (see Safey El Din and Trébuchet (2006)).*

We can now present the main result of this section: an explicit form of the bi-series for bi-regular bilinear systems.

Theorem 5. *Let $f_1, \ldots, f_m \in R$ be a bi-regular bilinear sequence, with $m \leq n_x + n_y$. Then*

$$\mathrm{HS}_{I_m}(t_1, t_2) = \frac{N_m(t_1, t_2)}{(1-t_1)^{n_x+1}(1-t_2)^{n_y+1}},$$

where

$$N_m(t_1,t_2) = (1-t_1t_2)^m + \sum_{\ell=1}^{m-(n_y+1)} (1-t_1t_2)^{m-(n_y+1)-\ell} t_1t_2(1-t_2)^{n_y+1}\left[1-(1-t_1)^{\ell}\sum_{k=1}^{n_y+1} t_1^{n_y+1-k}\binom{\ell+n_y-k}{n_y+1-k}\right] + \sum_{\ell=1}^{m-(n_x+1)} (1-t_1t_2)^{m-(n_x+1)-\ell} t_1t_2(1-t_1)^{n_x+1}\left[1-(1-t_2)^{\ell}\sum_{k=1}^{n_x+1} t_2^{n_x+1-k}\binom{\ell+n_x-k}{n_x+1-k}\right].$$

We decompose the proof of this theorem into a sequence of lemmas.

If I is an ideal of R and f is a polynomial, we denote by $\bar{f}$ the equivalence class of f in R/I and

$$\mathrm{ann}_{R/I}(f) = \{v \in R/I : v\bar{f} = 0\},$$
$$\mathrm{ann}_{R/I}(f)_{\alpha,\beta} = \{v \in R/I \text{ of bidegree } (\alpha,\beta) : v\bar{f} = 0\}.$$

If I is a bihomogeneous ideal and f is a bihomogeneous polynomial, we use the following notation:

$$G_{I,f}(t_1,t_2) = \sum_{(\alpha,\beta)\in\mathbb{N}^2} \dim(\mathrm{ann}_{R/I}(f)_{\alpha,\beta}) t_1^{\alpha} t_2^{\beta}.$$

Lemma 10. *Let $f_1, \ldots, f_m \in R$ be bihomogeneous polynomials, with $1 < m \leq n_x + n_y$. Let (d_1, d_2) be the bidegree of f_m. Then*

$$\mathrm{HS}_{I_m}(t_1,t_2) = (1 - t_1^{d_1} t_2^{d_2})\mathrm{HS}_{I_{m-1}} + t_1^{d_1} t_2^{d_2} G_{I_{m-1},f}(t_1,t_2).$$

Proof. We have the following exact sequence:

$$0 \to \mathrm{ann}_{R/I_{m-1}}(f) \xrightarrow{\varphi_1} R/I_{m-1} \xrightarrow{\varphi_2} R/I_{m-1} \xrightarrow{\varphi_3} R/I_m \to 0.$$

where φ_1 and φ_3 are the canonical inclusion and projection, and φ_2 is the multiplication by f_m.

From this exact sequence of ideals, we can deduce an exact sequence of vector spaces:

$$0 \to (\mathrm{ann}_{R/I_{m-1}}(f))_{\alpha,\beta} \xrightarrow{\varphi_1} \left(\frac{R}{I_{m-1}}\right)_{\alpha,\beta} \xrightarrow{\varphi_2} \left(\frac{R}{I_{m-1}}\right)_{\alpha+d_1,\beta+d_2} \xrightarrow{\varphi_3} \left(\frac{R}{I_m}\right)_{\alpha+d_1,\beta+d_2} \to 0.$$

Thus the alternate sum of the dimensions of vector spaces of an exact sequence is 0:

$$\dim((\mathrm{ann}_{R/I_{m-1}}(f))_{\alpha,\beta}) - \dim\left(\left(\frac{R}{I_{m-1}}\right)_{\alpha,\beta}\right) + \\ \dim\left(\left(\frac{R}{I_{m-1}}\right)_{\alpha+d_1,\beta+d_2}\right) - \dim\left(\left(\frac{R}{I_m}\right)_{\alpha+d_1,\beta+d_2}\right) = 0.$$

By multiplying this relation by $t_1^\alpha t_2^\beta$ and by summing over (α, β), we obtain the claimed recurrence:

$$\mathrm{HS}_{I_m}(t_1,t_2) = (1 - t_1^{d_1}t_2^{d_2})\mathrm{HS}_{I_{m-1}} + t_1^{d_1}t_2^{d_2}G_{I_{m-1},f}(t_1,t_2).$$

□

Lemma 11. *Let $f_1, \dots, f_m \in R$ be a bi-regular bilinear sequence, with $m \le n_x + n_y$. Then, for all $2 \le i \le m$,*

$$G_{I_{i-1},f_i}(t_1,t_2) = g_x^{(i-1)}(t_1) + g_y^{(i-1)}(t_2),$$

where

$$g_x^{(i-1)}(t) = \begin{cases} 0 \text{ if } i \le n_y+1 \\ \frac{1}{(1-t)^{n_x+1}} - \sum_{1\le j \le n_y+1} \frac{\binom{i-1-j}{n_y+1-j} t^{n_y+1-j}}{(1-t)^{n_x+n_y-i+2}} \end{cases}.$$

$$g_y^{(i-1)}(t) = \begin{cases} 0 \text{ if } i \le n_x+1 \\ \frac{1}{(1-t)^{n_y+1}} - \sum_{1\le j \le n_x+1} \frac{\binom{i-1-j}{n_x+1-j} t^{n_x+1-j}}{(1-t)^{n_x+n_y-i+2}} \end{cases}.$$

Proof. Saying that $v \in \mathrm{ann}_{R/I_{i-1}}(f_i)$ is equivalent to saying that the row with signature $(\mathsf{LM}(v), f_i)$ is not detected by the classical F_5 criterion. According to Theorem 4, if the system is bi-regular, the reductions to zero corresponding to non-trivial syzygies are exactly:

$$\bigcup_{i=n_x+2}^{m} \{(t, f_i) : t \in \mathsf{Monomials}^{\mathbf{y}}_{i-n_x-2}(n_x+1)\} \bigcup_{i=n_y+2}^{m} \{(t, f_i) : t \in \mathsf{Monomials}^{\mathbf{x}}_{i-n_y-2}(n_y+1)\}.$$

By Proposition 4, we know that if $P \in k[x_0, \dots, x_{n_x}] \cap (I_{i-1} : f_i)$ (resp. $k[y_0, \dots, y_{n_y}] \cap (I_{i-1} : f_i)$), then $\forall j, y_j P \in I_{i-1}$ (resp. $x_j P \in I_{i-1}$). Thus $G_{I_{i-1},f_i}(t_1,t_2)$ is the generating bi-series of the monomials in $k[x_0, \dots, x_{n_x}]$ which are a multiple of a monomial of degree $n_y + 1$ in $x_0, \dots, x_{i-n_y-2}$ and of the monomials in $k[y_0, \dots, y_{n_y}]$ which are a multiple of a monomial of degree $n_x + 1$ in $y_0, \dots, y_{i-n_x-2}$. Denote by $g_x^{(i-1)}(t)$ (resp. $g_y^{(i-1)}(t)$) the generating series of the monomials in $k[x_0, \dots, x_{n_x}]$ (resp. $k[y_0, \dots, y_{n_y}]$) which are a multiple of a monomial of degree $n_y + 1$ (resp. $n_x + 1$) in $x_0, \dots, x_{i-n_y-2}$ (resp. $y_0, \dots, y_{i-n_x-2}$). Then we have

$$G_{I_{i-1},f_i}(t_1,t_2) = g_x^{(i-1)}(t_1) + g_y^{(i-1)}(t_2).$$

Next we use combinatorial techniques to give an explicit form of $g_x^{(i-1)}(t)$ and $g_y^{(i-1)}(t)$. Let $c(t)$ denote the generating series of the monomials in $k[x_{i-n_y-1}, \dots, x_{n_x}]$:

$$c(t) = \sum_{j=0}^{\infty} \binom{n_x+n_y-i+j+1}{j} t^j = \frac{1}{(1-t)^{n_x+n_y-i+2}}.$$

Let B_j denote the number of monomials in $k[x_0, \ldots, x_{i-n_y-2}]$ of degree j. Then

$$\frac{1}{(1-t)^{n_x+n_y+2}} = c(t) + B_1 c(t) t + \cdots + B_{n_y} c(t) t^{n_y} + g_x^{(i-1)}(t).$$

Since $B_j = \binom{i-n_y-1+j}{j}$, we can conclude:

$$g_x^{(i-1)}(t) = \begin{cases} 0 \text{ if } i \leq n_y + 1 \\ \frac{1}{(1-t)^{n_x+1}} - \sum_{1 \leq j \leq n_y+1} \frac{\binom{i-1-j}{n_y+1-j} t^{n_y+1-j}}{(1-t)^{n_x+n_y-i+2}} \end{cases}.$$

□

Proof of Theorem 5. Since the polynomials are bilinear, by Lemma 10, we have

$$\mathrm{HS}_{I_i}(t_1, t_2) = (1 - t_1 t_2)\mathrm{HS}_{I_{i-1}} + t_1 t_2 G_{I_{i-1}, f_i}(t_1, t_2).$$

Lemma 11 gives the value of $G_{I_{i-1}, f_i}(t_1, t_2)$. To initiate the recurrence, we need

$$\mathrm{HS}_{I_0}(t_1, t_2) = \mathrm{HS}_{\langle 0 \rangle}(t_1, t_2) = \frac{1}{(1-t_1)^{n_x+1}(1-t_2)^{n_y+1}}.$$

Then we can obtain the claimed form of the bi-series by solving the recurrence:

$$\mathrm{HS}_{I_i}(t_1, t_2) = \frac{N_i(t_1, t_2)}{(1-t_1)^{n_x+1}(1-t_2)^{n_y+1}}$$

$$N_i(t_1, t_2) = (1 - t_1 t_2)^i + \sum_{j=0}^{m-1} t_1 t_2 (1 - t_1 t_2)^j G_{I_j, f_{j+1}}(t_1, t_2).$$

□

Example 1 (continued). *The Hilbert bi-series of the ideal generated by the five polynomials of Example 1 is*

$$\begin{aligned}\mathrm{HS}(t_1, t_2) \quad = \quad & \frac{1}{(1-t_1)^3(1-t_2)^4}({t_1}^5{t_2}^5 - 4{t_1}^5{t_2}^4 + 6{t_1}^5{t_2}^3 - 4{t_1}^5{t_2}^2 + {t_1}^5 t_2 - 6{t_1}^3{t_2}^5 + \\ & 15{t_1}^3{t_2}^4 - 10{t_1}^3{t_2}^3 + 8{t_1}^2{t_2}^5 - 15{t_1}^2{t_2}^4 + 10{t_1}^2{t_2}^2 - 3t_1{t_2}^5 + 5t_1{t_2}^4 - 5t_1 t_2 + 1),\end{aligned}$$

and is in accordance with the formula given in Theorem 5. Also, notice that the intermediate series $g_x(t)$ and $g_y(t)$ match the theoretical values. For instance:

$$g_y^{(3)} = \frac{t^3}{(1-t)^4}.$$

6. Towards complexity results

6.1. A multihomogeneous F_5 Algorithm

We now describe how it is possible to use the multihomogeneous structure of the matrices arising in the Matrix F_5 Algorithm to speed-up the computation of a Gröbner basis. In order to have simple notations, the description is made in the context of bihomogeneous systems, but it can be easily transposed in the context of multihomogeneous systems.

					Multihomogeneous		Homogeneous		
n_x	n_y	m	bidegree	D	time	memory	time	memory	speed-up
3	4	7	$(1,1)$	6	**16.9s**	**30MB**	265.7s	280MB	**16**
3	4	7	$(1,1)$	7	**105s**	**92MB**	2018s	1317MB	**19**
4	4	8	$(1,1)$	7	**582s**	**275MB**	13670s	4210MB	**23**
5	4	9	$(1,1)$	7	**3343s**	**957MB**	66371s	12008MB	**20**
5	5	10	$(1,1)$	6	**645s**	**435MB**	10735s	4330MB	**17**
2	2	4	$(1,2)$	10	**11.4s**	**19MB**	397s	299MB	**35**
2	2	4	$(1,2)$	8	**1.7s**	**10MB**	16s	52MB	**9**
3	3	6	$(1,2)$	8	**67s**	**80MB**	1146s	983MB	**17**
4	4	8	$(1,2)$	8	**2222s**	**1031MB**	40830s	12319MB	**63**
2	2	4	$(2,2)$	11	**29s**	**27MB**	899s	553MB	**31**
3	3	6	$(2,2)$	8	**27s**	**47MB**	277s	452MB	**10**
3	3	6	$(2,2)$	9	**152s**	**154MB**	2380s	1939MB	**16**
3	4	7	$(2,2)$	9	**1034s**	**505MB**	18540s	7658MB	**18**
4	4	8	$(2,2)$	8	**690s**	**385MB**	7260s	4811MB	**11**
4	4	8	$(2,2)$	9	**6355s**	**2216MB**	—	>20000MB	—

Table 1: Execution time and memory usage of the multihomogeneous variant of F_5

Let $f_1, \dots, f_m$ be a sequence of bihomogeneous polynomials. Consider the matrices M_d in degree d appearing during the Matrix F_5 Algorithm. One can remark that each row represents a bihomogeneous polynomial. Let (d_1, d_2) be the bidegree of one row of this matrix. Then the only non-zero coefficients on this row are in columns which represent a monomial of bidegree (d_1, d_2). Therefore a possible strategy to use the bihomogeneous structure is the following:

- For each couple (d_1, d_2) such that $d_1 + d_2 = d$, construct the matrix M_{d_1,d_2}. The rows of this matrix represent the polynomials of M_d of bidegree (d_1, d_2) and the columns represent the monomials of R_{d_1,d_2}.
- Compute the row echelon form of the matrices M_{d_1,d_2}. This gives bases of I_{d_1,d_2}.
- The union of the bases gives a basis of I_d since $I_d = \bigoplus_{d_1+d_2=d} I_{d_1,d_2}$.

This way, instead of computing the row echelon form of a big matrix, we can decompose the problem and compute independently the row echelon form of smaller matrices. This strategy can be extended to multihomogeneous systems.

In Table 1, the execution time and the memory usage of this multihomogeneous variant of F_5 are compared to the classical homogeneous Matrix F_5 Algorithm for computing a D-Gröbner basis for random bihomogeneous systems (for the grevlex ordering). Both implementations are made in `Magma2.15-7`. The experimental results have been obtained with a Xeon processor 2.50GHz cores and 20 GB of RAM. We are aware that we should compare efficient implementations of these two algorithms to have a more precise evaluation of the speed-up we can expect for practical applications. However, these experiments give a first estimation of that speed-up. Furthermore, we can also expect to save a lot of memory by decomposing the Macaulay matrix into smaller matrices. This is crucial for practical applications, since untractability is often due to the lack of memory.

6.2. A theoretical complexity analysis in the bilinear case

In this section, we provide a theoretical explanation of the speed-up observed when using the bihomogeneous structure of bilinear systems. To estimate the complexity of the Matrix F_5 Algorithm, we consider that the cost is dominated by the cost of the reductions of the matrices with the highest degree. By using the new criterion described in Section 3.4, all the matrices appearing during the computations have full rank for generic inputs (these ranks are the dimensions of the k-vector spaces I_{d_1,d_2}). We consider that the complexity of reducing a $r \times c$ matrix with Gauss elimination is $O(r^2c)$. Thus the complexity of computing a D-Gröbner basis with the usual Matrix F_5 Algorithm and the extended criterion for a bilinear system of m equations over $k[x_0, \ldots, x_{n_x}, y_0, \ldots, y_{n_y}]$ is

$$T_{hom} = C_1 \left(\left(\binom{D+n_x+n_y+1}{D} - [t^D]\mathrm{HS}(t,t) \right)^2 \binom{D+n_x+n_y+1}{D} \right).$$

When using the multihomogeneous structure, the complexity becomes:

$$T_{multihom} = C_2 \left(\sum_{\substack{d_1+d_2=D \\ 1 \le d_1,d_2 \le D-1}} \left(\dim(R_{d_1,d_2}) - [t_1^{d_1} t_2^{d_2}]\mathrm{HS}(t_1,t_2) \right)^2 \dim(R_{d_1,d_2}) \right),$$

where $\dim(R_{d_1,d_2}) = \binom{d_1+n_x}{d_1}\binom{d_2+n_y}{d_2}$. Thus the theoretical speed-up that we expect is:

$$speedup_{th} = C_3 F(n_x, n_y, m, D)$$

where $C_3 = \frac{C_1}{C_2}$ is a constant and

$$F(n_x,n_y,m,D) = \left(\frac{\left(\binom{D+n_x+n_y+1}{D} - [t^D]\mathrm{HS}(t,t) \right)^2 \binom{D+n_x+n_y+1}{D}}{\sum_{\substack{d_1+d_2=D \\ 1 \le d_1,d_2 \le D-1}} \left(\dim(R_{d_1,d_2}) - [t_1^{d_1} t_2^{d_2}]\mathrm{HS}(t_1,t_2) \right)^2 \dim(R_{d_1,d_2})} \right).$$

Now let us compare this theoretical speed-up with the one observed in practice. We can see in Table 2 that experimental results match the theoretical complexity:

$$speedup \approx 0.6 F(n_x, n_y, m, D).$$

6.3. Number of reductions to zero removed by the extended F_5 criterion

Table 3 shows the number of reductions to zero during the execution of the Buchberger, F_4 and F_5 algorithm. The input systems are random bilinear systems of $n_x + n_y$ equations over $\mathsf{GF}(65521)[x_0, \ldots, x_{n_x}, y_0, \ldots, y_{n_y}]$. Experimentally, there is no reduction to zero when using the extended criterion (Algorithm 4). Notice that the number of reductions to zero which are not detected by the classical F_5 criterion matches the theorical value for a bi-regular system (Definition 8):

$$\sum_{i=n_y+1}^{n_x+n_y-1} \binom{i}{n_y+1} + \sum_{i=n_x+1}^{n_x+n_y-1} \binom{i}{n_x+1}.$$

n_x	n_y	m	D	*experimental speed−up*	$F(n_x, n_y, m, D)$
3	4	7	6	**16**	**29**
3	4	7	7	**19**	**34**
4	4	8	7	**23**	**34**
5	4	9	7	**20**	**32**
5	5	10	6	**17**	**27**

Table 2: Decomposing the matrices: experimental speed-up

(n_x, n_y)	Nb. useful red. (Buch./F_4)	Nb red. to 0 (Buch./F_4)	Nb red. to 0 (F_5)
$(5,5)$	752	5772	240
$(5,6)$	1484	13063	495
$(6,6)$	3009	29298	990
$(6,7)$	5866	64093	2002
$(4,8)$	1912	19055	990
$(4,9)$	2869	31737	1794
$(3,10)$	1212	13156	1300
$(3,11)$	1665	19780	2016
$(3,12)$	2123	27295	3018

Table 3: Experimental number of reductions to zero

Although the number of reductions to zero removed by the extended criterion is not small compared to the number of useful reductions, they arise in low degree (n_x+1 and n_y+1). Hence, it is not clear what speed-up could be expected with an efficient implementation.

6.4. Structure of generic affine bilinear systems

In this section, we show that generic *affine* bilinear systems have a particular structure: they are regular (Definition 7). Consequently, the usual F_5 criterion removes all reductions to zero.

Proposition 5. *Let S be the set of affine bilinear systems over $k[x_1, \dots, x_{n_x}, y_1, \dots, y_{n_y}]$ with $m \leq n_x + n_y$ equations. Then the subset*

$$\{(f_1, \dots, f_m) \in S \quad : \quad (f_1, \dots, f_m) \text{ is a regular sequence}\}$$

contains a Zariski nonempty open subset of S.

Proof. Let $(f_1, \dots, f_m)$ be a generic affine bilinear system. Assume that it is not regular. Then for some i, there exists $g \in R$ such that $g \notin I_{i-1}$ and $gf_i \in I_{i-1}$. Denote by g^h the bi-homogenization of g. Then $g^h \in \langle f_1^h, \dots, f_{i-1}^h \rangle : f_i^h$. $(f_1^h, \dots, f_m^h)$ is a generic bilinear system, hence it is bi-regular (Theorem 4). Thus $g^h \in k[x_0, \dots, x_{n_x}]$ or $g^h \in k[y_0, \dots, y_{n_y}]$. Let us suppose that $g^h \in k[x_0, \dots, x_{n_x}]$ (the proof is similar if $g^h \in k[y_0, \dots, y_{n_y}]$). Therefore $y_{n_y} g^h \in \langle f_1^h, \dots, f_{i-1}^h \rangle$ when the system is bi-regular (Proposition 4). By putting $x_{n_x} = 1$ and $y_{n_y} = 1$, we see that in this case, $g \in I_{i-1}$, which yields a contradiction. This shows that generic affine bilinear systems are regular. □

6.5. Degree of regularity of affine bilinear systems

In this part, m, n_x and n_y are three integers such that $m = n_x + n_y$. We consider a system of bilinear polynomials $F = (f_1, \dots, f_m) \in k[x_0, \dots, x_{n_x}, y_0, \dots, y_{n_y}]^m$. ϑ denotes the dehomogenization morphism:

$$\begin{array}{ccc} k[x_0, \dots, x_{n_x}, y_0, \dots, y_{n_y}] & \longrightarrow & k[x_0, \dots, x_{n_x-1}, y_0, \dots, y_{n_y-1}] \\ f(x_0, \dots, x_{n_x}, y_0, \dots, y_{n_y}) & \longmapsto & f(x_0, \dots, x_{n_x-1}, 1, y_0, \dots, y_{n_y-1}, 1) \end{array}.$$

Also, I stands for the ideal $\langle f_1, \dots, f_m \rangle$ and $\vartheta(I)$ denotes the ideal $\langle \vartheta(f_1), \dots, \vartheta(f_m) \rangle$. In the following, we suppose without loss of generality that $n_x \leq n_y$. We also assume in this part of the paper that the characteristic of k is 0 (although the results remain true when the characteristic is large enough).

The goal of this section is to give an upper bound on the so-called *degree of regularity* of an ideal I generated by a generic affine bilinear system with m equations and m variables. The degree of regularity is a crucial indicator of the complexity of Gröbner basis algorithms: for 0-dimensional ideals, it is the lowest integer d_{reg} such that all monomials of degree d_{reg} are in $\mathsf{LM}(I)$ (see Bardet et al. (2005)). As a consequence, the degrees of all polynomials occurring in the F_5 algorithm are lower than $d_{reg} + 1$. In the following, $\prec$ still denotes the grevlex ordering.

Lemma 12. *If the system F is generic, then there exists polynomials $g_0, \dots, g_{n_x-1} \in k[y_0, \dots, y_{n_y-1}]$ such that*

$$\forall j \in \{0, \dots, n_x - 1\}, x_j - g_j(y_0, \dots, y_{n_y-1}) \in \vartheta(I).$$

Proof. We consider the $m \times n_x$ matrix $A = \mathsf{jac}_{\mathbf{x}}(\vartheta(F))$ and the vector

$$B = \begin{pmatrix} \vartheta(f_1)(0, \dots, 0, y_0, \dots, y_{n_y-1}) & \dots & \vartheta(f_m)(0, \dots, 0, y_0, \dots, y_{n_y-1}) \end{pmatrix}.$$

Thus $A \cdot \begin{pmatrix} x_0 \\ \vdots \\ x_{n_x-1} \end{pmatrix} + B = \begin{pmatrix} \vartheta(f_1) \\ \vdots \\ \vartheta(f_m) \end{pmatrix}$.

We denote by $\{A^{(i)}\}$ all the $n_x \times n_x$ sub-matrices of A.

Let $(\alpha_0, \dots, \alpha_{n_y-1}) \in Var(\langle \mathsf{MaxMinors}(\vartheta(\mathsf{jac}_{\mathbf{x}}(F))) \rangle)$ be an element of the variety. Let A_α (resp. B_α) denote the matrix A (resp. B) where y_i has been substituted by α_i for all i. Since $\vartheta(I)$ is 0-dimensional, the affine linear system

$$A_\alpha \cdot \begin{pmatrix} x_0 \\ \dots \\ x_{n_x-1} \end{pmatrix} + B_\alpha = 0$$

has a unique solution. Therefore, the matrix A_α is of full rank. Consequently, there exists an invertible $n_x \times n_x$ sub-matrix of A_α.

Since k is infinite, we can suppose without loss of generality that, if the system is generic, then for all α in the variety, the matrix $A_\alpha^{(1)}$ obtained by considering the n_x first rows of A_α is invertible (if $A_\alpha^{(1)}$ is not invertible, just replace the original bilinear system by an equivalent system where each new equation is a generic linear combination of the original equations). Thus $\det(A_\alpha^{(1)}) \neq 0$.

According to Lemma 6 and 17, $\langle \mathsf{MaxMinors}(\vartheta(\mathsf{jac}_{\mathbf{x}}(F)))\rangle = \langle \vartheta(f_1), \ldots, \vartheta(f_m)\rangle \cap k[y_0, \ldots, y_{n_y-1}]$. Thus $\det(A^{(1)})$ (i.e. the matrix of the n_x first rows of A) does not vanish on any element of the variety of $\vartheta(I)$. Therefore, the Nullstellensatz says that $\det(A^{(1)})$ is invertible in $k[y_0, \ldots, y_{n_y-1}]/(\vartheta(I) \cap k[y_0, \ldots, y_{n_y-1}])$. Let h denote its inverse. We know from Cramer's rule that there exists polynomials $g_j \in k[y_0, \ldots, y_{n_y-1}]$ such that

$$x_j \det(A^{(1)}) - g_j(y_0, \ldots, y_{n_y-1}) \in \vartheta(I).$$

Multiplying this relation by h, we obtain:

$$x_j - hg_j(y_0, \ldots, y_{n_y-1}) \in \vartheta(I).$$

□

Theorem 6. *If the system F is generic, then the degree of regularity of $\vartheta(I)$ is upper bounded by*

$$d_{reg} \le \min(n_x + 1, n_y + 1).$$

Proof. We supposed that $n_x \le n_y$, so we want to prove that $d_{reg} \le n_x + 1$. Let $t = \prod_{j=0}^{n_x-1} x_j^{\alpha_j} \prod_{k=0}^{n_y-1} y_k^{\beta_k}$ be a monomial of degree $n_x + 1$. According to Lemma 12,

$$t - \prod_{j=0}^{n_x-1} g_j(y_0, \ldots, y_{n_y-1})^{\alpha_j} \prod_{k=0}^{n_y-1} y_k^{\beta_k} \in \vartheta(I).$$

Now consider the normal form with respect to the ideal $J = \langle \mathsf{MaxMinors}(\vartheta(\mathsf{jac}_{\mathbf{x}}(F)))\rangle$. Then

$$t - \mathsf{NF}_{J,\prec}(\prod_{j=0}^{n_x-1} g_j(y_0, \ldots, y_{n_y-1})^{\alpha_j} \prod_{k=0}^{n_y-1} y_k^{\beta_k}) \in \vartheta(I).$$

Since all monomials of degree $n_x + 1$ are in $\mathsf{LM}(\langle \mathsf{MaxMinors}(\vartheta(\mathsf{jac}_{\mathbf{x}}(F)))\rangle)$ (Lemma 3),

$$\deg(\mathsf{NF}_{J,\prec}(\prod_{j=0}^{n_x-1} g_j(y_0, \ldots, y_{n_y-1})^{\alpha_j} \prod_{k=0}^{n_y-1} y_k^{\beta_k})) < n_x + 1.$$

This implies that

$$\mathsf{LM}(t - \mathsf{NF}_{J,\prec}(\prod_{j=0}^{n_x-1} g_j(y_0, \ldots, y_{n_y-1})^{\alpha_j} \prod_{k=0}^{n_y-1} y_k^{\beta_k})) = t.$$

Therefore, for each monomial t of degree $n_x + 1$, $t \in \mathsf{LM}(\vartheta(I))$. This means that $d_{reg} \le n_x + 1$. □

Example 1 (continued). *The degree of regularity of the affine system $(\vartheta(f_1), \ldots, \vartheta(f_5))$ is 3 in accordance with Theorem 6 and the classical F_5 criterion removes all reductions to zero during the computation of a Gröbner basis for the grevlex ordering.*

The following corollary is a consequence of Theorem 6.

n_x	n_y	nb. eq.	d_{reg}	nb. reductions to 0
2	3	5	3	0
2	4	6	3	0
3	10	13	4	0
5	8	13	6	0
6	6	12	7	0

Table 4: Experimental results: degree of regularity and reductions to zero for random affine bilinear systems

Corollary 3. *The arithmetic complexity of computing a Gröbner basis of a generic bilinear system* $f_1, \dots, f_{n_x+n_y} \in k[x_0, \dots, x_{n_x-1}, y_0, \dots, y_{n_y-1}]$ *with the* F_5 *Algorithm is upper bounded by*

$$O\left(\binom{n_x + n_y + \min(n_x+1, n_y+1)}{\min(n_x+1, n_y+1)}^{\omega}\right),$$

where $2 \le \omega \le 3$ *is the linear algebra constant.*

Proof. According to Bardet et al. (2005), the complexity of the computation of the Gröbner basis of a 0-dimensional ideal is upper bounded by

$$O\left(\binom{n + d_{reg}}{d_{reg}}^{\omega}\right),$$

where n is the number of variables and d_{reg} denotes the degree of regularity. In the case of a generic affine bilinear system in $k[x_0, \dots, x_{n_x-1}, y_0, \dots, y_{n_y-1}]$, $n = n_x + n_y$ and $d_{reg} \le \min(n_x+1, n_y+1)$ (Theorem 6). □

Remark 5. *This bound on the degree of regularity should be compared with the degree of regularity of a generic quadratic system with n equations and n variables. The Macaulay bound (see Lazard (1983)) says that the degree of regularity of such systems is* $m + 1$*. The complexity of computing a Gröbner basis of a generic quadratic system of* n *equations in* $k[x_1, \dots, x_n]$ *is upper bounded by* $O\left(\binom{2n}{n+1}^{\omega}\right)$*, which is larger than* $O\left(\binom{n_x+n_y+\min(n_x+1,n_y+1)}{\min(n_x+1,n_y+1)}^{\omega}\right)$ *when* $n = n_x + n_y$*. Notice also that if* $\min(n_x, n_y)$ *is constant, then the complexity of computing a Gröbner basis of a* 0*-dimensional generic affine bilinear system is polynomial in the number of unknowns* $n = n_x + n_y$*. Moreover, the inequality* $d_{reg} \le \min(n_x+1, n_y+1)$ *is experimentally sharp, it is an equality for random bilinear systems (see Table 4).*

7. Perspectives and conclusion

In this paper, we analyzed the structure of ideals generated by generic bilinear equations. We proposed an explicit description of their syzygy module. With this analysis, we were able to propose an extension of the F_5 criterion dedicated to bilinear systems.

Furthermore, an explicit formula for the Hilbert bi-series is deduced from the combinatorics of the syzygy module. With this tool, we made a complexity analysis of a multihomogeneous variant of the F_5 Algorithm.

We also analyzed the complexity of computing Gröbner bases of affine bilinear systems. We showed that generic affine bilinear systems are regular, and we proposed an upper bound for the degree of regularity of those systems.

Interestingly, properties of the ideals generated by the maximal minors of the jacobian matrices are especially important. In particular, a Gröbner basis (for the grevlex ordering) of such an ideal is a linear combination of the generators. In the affine case, this ideal permits to eliminate variables.

The next step of this work would be to generalize the results to more general multihomogeneous systems. For the time being, it is not clear how the results can be extended. In particular, it would be interesting to understand the structure of the syzygy module of general multihomogeneous systems, and to have an explicit formula of their Hilbert series. Also, having sharp upper bounds on the degree of regularity of multihomogeneous systems would be important for practical applications.

References

Adams, W., Loustaunau, P., 1994. An introduction to Gröbner bases. American Mathematical Society.

Ars, G., 2005. Applications des bases de Gröbner à la cryptographie. Ph.D. thesis, Université de Rennes I.

Atiyah, M., MacDonald, I., 1969. Introduction to Commutative Algebra. Series in Mathematics. Addison-Wesley.

Bardet, M., 2004. Étude des systèmes algébriques surdéterminés. applications aux codes correcteurs et à la cryptographie. Ph.D. thesis, Université Paris 6.

Bardet, M., Faugere, J., Salvy, B., 2004. On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations. In: Proceedings of the International Conference on Polynomial System Solving. pp. 71–74.

Bardet, M., Faugère, J.-C., Salvy, B., Yang, B., 2005. Asymptotic behaviour of the degree of regularity of semi-regular polynomial systems. In: Proceedings of Effective Methods in Algebraic Geometry (MEGA).

Bernstein, D., Zelevinsky, A., 1993. Combinatorics of maximal minors. Journal of Algebraic Combinatorics 2 (2), 111–121.

Bruns, W., Conca, A., 2003. Gröbner bases and determinantal ideals. In: Herzog, J., Vuletescu, V. (Eds.), Commutative algebra, singularities and computer algebra. pp. 9–66.

Buchberger, B., 2006. An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. Journal of Symbolic Computation 41 (3-4), 475–511.

Cox, D., Dickenstein, A., Schenck, H., 2007a. A case study in bigraded commutative algebra. In: Peeva, I. (Ed.), Syzygies and Hilbert functions. Lecture Notes in Pure and Applied Mathematics. CRC Press.

Cox, D., Little, J., O'Shea, D., 2007b. Ideals, Varieties, and Algorithms. Springer.

Dickenstein, A., Emiris, I., 2003. Multihomogeneous resultant formulae by means of complexes. Journal of Symbolic Computation 36 (3-4), 317–342.

Eisenbud, D., 1995. Commutative algebra with a view toward algebraic geometry. Vol. 150 of Graduate Texts in Mathematics. Springer-Verlag.

Emiris, I. Z., Mantzaflaris, A., 2009. Multihomogeneous resultant formulae for systems with scaled support. In: Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation. ACM, pp. 143–150.

Faugère, J.-C., 1994. Résolution des systemes d'équations algébriques. Ph.D. thesis, Université Paris 6.

Faugère, J.-C., 1999. A new efficient algorithm for computing Gröbner bases (F4). Journal of Pure and Applied Algebra 139, 61–88.

Faugère, J.-C., 2002. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In: Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation (ISSAC). ACM New York, NY, USA, pp. 75–83.

Faugère, J.-C., Levy-Dit-Vehel, F., Perret, L., 2008. Cryptanalysis of MinRank. In: Proceedings of the 28th Annual conference on Cryptology: Advances in Cryptology. Springer, pp. 280–296.

Faugère, J.-C., Rahmany, S., 2009. Solving systems of polynomial equations with symmetries using SAGBI-Gröbner bases. In: Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation. ACM, pp. 151–158.

Faugère, J.-C., Safey El Din, M., Spaenlehauer, P.-J., 2010. Computing loci of rank defects of linear matrices using Gröbner bases and applications to cryptology. In: Watt, S. M. (Ed.), Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation (ISSAC 2010). pp. 257–264.

Fröberg, R., 1997. An introduction to Gröbner bases. John Wiley & Sons.

Gabidulin, E., 1985. Theory of codes with maximum rank distance. Problemy Peredachi Informatsii 21 (1), 3–16.

Hartshorne, R., 1977. Algebraic geometry. Springer.

Jeronimo, G., Sabia, J., 2007. Computing multihomogeneous resultants using straight-line programs. Journal of Symbolic Computation 42 (1-2), 218–235.

Kreuzer, M., Robbiano, L., 2003. Basic tools for computing in multigraded rings. In: Herzog, J., Vuletescu, V. (Eds.), Commutative Algebra, Singularities and Computer Algebra. Kluwer Academic Publishers, pp. 197–216.

Kreuzer, M., Robbiano, L., Herzog, J., Vulutescu, V., 2002. Basic tools for computing in multigraded rings. In: Commutative Algebra, Singularities and Computer Algebra, Proc. Conf. Sinaia. pp. 197–216.

Lazard, D., 1983. Gröbner bases, gaussian elimination and resolution of systems of algebraic equations. In: EUROCAL. pp. 146–156.

Li, T., Lin, Z., Bai, F., 2003. Heuristic methods for computing the minimal multi-homogeneous Bézout number. Applied Mathematics and Computation 146 (1), 237–256.

Matsumura, H., 1989. Commutative ring theory. Cambridge Univ Pr.

Mayr, E., Meyer, A., 1982. The complexity of the word problems for commutative semigroups and polynomial ideals. Adv. Math 46 (3), 305–329.

McCoy, N., 1933. On the resultant of a system of forms homogeneous in each of several sets of variables. Transactions of the American Mathematical Society, 215–233.

Morgan, A., Sommese, A., 1987. A homotopy for solving general polynomial systems that respects m-homogeneous structures. Appl. Math. Comput. 24 (2), 101–113.

Ourivski, A., Johansson, T., 2002. New technique for decoding codes in the rank metric and its cryptography applications. Problems of Information Transmission 38 (3), 237–246.

Rémond, G., 2001. Elimination multihomogène. Introduction to Algebraic Independence Theory. Lect. Notes Math 1752, 53–81.

Rémond, G., 2001. Géométrie diophantienne multiprojective, chapitre 7 de Introduction to algebraic independence theory. Lecture Notes in Math, 95–131.

Safey El Din, M., Schost, E., 2003. Polar varieties and computation of one point in each connected component of a smooth real algebraic set. In: Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation. ACM New York, NY, USA, pp. 224–231.

Safey El Din, M., Trébuchet, P., 2006. Strong bi-homogeneous Bézout theorem and its use in effective real algebraic geometry. Arxiv preprint cs/0610051.

Shafarevich, I., 1977. Basic Algebraic Geometry 1. Springer Verlag.

Sturmfels, B., Zelevinsky, A., 1993. Maximal minors and their leading terms. Adv. Math 98 (1), 65–112.

Traverso, C., 1996. Hilbert functions and the Buchberger algorithm. Journal of Symbolic Computation 22 (4), 355–376.

Van der Waerden, B. L., 1929. On Hilbert's Function, Series of Composition of Ideals and a generalization of the Theorem of Bezout. In: Proceedings Roy. Acad. Amsterdam. Vol. 31. pp. 749–770.

Appendix A. Bihomogeneous ideals

In this part, we use notations similar to those used in Section 4:

- $\mathcal{BH}(n_x, n_y)$ the k-vector space of bilinear polynomials in $k[x_0, \ldots, x_{n_x}, y_0, \ldots, y_{n_y}]$;
- X (resp. Y) is the ideal $\langle x_0, \ldots, x_{n_x} \rangle$ (resp. $\langle y_0, \ldots, y_{n_y} \rangle$);

- An ideal is called *bihomogeneous* if it admits a set of bihomogeneous generators.
- J_i denotes the saturated ideal $I_i : (X \cap Y)^\infty$;
- Given a polynomial sequence $(f_1, \ldots, f_m)$, we denote by Syz_{triv} the module of trivial syzygies, i.e. the set of all syzygies $(s_1, \ldots, s_m)$ such that $\forall 1 \leq i \leq m$, $s_i \in \langle f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_m \rangle$;
- A primary ideal $P \subset R$ is called *admissible* if $X \not\subset \sqrt{P}$ and $Y \not\subset \sqrt{P}$;
- Let E be a k-vector space such that $\dim(E) < \infty$. We say that a property $\mathcal{P}$ is *generic* if it is satisfied on a nonempty open subset of E (for the Zariski topology), i.e. $\exists h \in k[\mathfrak{a}_1, \ldots, \mathfrak{a}_{\dim(E)}], h \neq 0$, such that

$$\mathcal{P} \text{ does not hold on } (a_1, \ldots, a_{\dim(E)}) \Rightarrow h(a_1, \ldots, a_{\dim(E)}) = 0.$$

Proposition 6 (Safey El Din and Trébuchet (2006))**.** *Let I be an ideal of R. The two following assertions are equivalent:*

- *I is* bihomogeneous.
- *For all $h \in I$, every bihomogeneous component of h is in I.*

Lemma 13 (Safey El Din and Trébuchet (2006))**.** *Let $f_1, \ldots, f_m \in R$ be polynomials, and $I_m = \cap P_l$ be a minimal primary decomposition of I_m and let Adm be the set of the admissible ideals of the decomposition. Then $J_m = \cap_{P \in Adm} P$.*

Proposition 7. *let $f_1, \ldots, f_m \in R$ be polynomials with $m \leq n_x + n_y$, and $Ass(I_{i-1})$ be the set of prime ideals associated to I_{i-1}. The following assertions are equivalent:*

1. *for all i such that $2 \leq i \leq m$, f_i is not a divisor of 0 in R/J_{i-1}.*
2. *for all i such that $2 \leq i \leq m$, $(f_i \in P, P \in Ass(I_{i-1})) \Rightarrow P$ is non-admissible.*

Proof. It is a straightforward consequence of Lemma 13. □

Remark 6. *All results in this section can be generalized to multihomogeneous systems. Since we focus on bilinear systems in this paper, we describe them in this more restrictive context.*

Lemma 14. *Let P be an admissible prime ideal of R. The set of bilinear polynomials $f \in R$ such that $f \notin P$ contains a Zariski nonempty open set.*

Proof. Let $\mathfrak{f}$ be the generic bilinear polynomial

$$\mathfrak{f} = \sum_{j,k} \mathfrak{a}_{j,k} x_j y_k$$

in $k(\{\mathfrak{a}_{j,k}\}_{0 \leq j \leq n_x, 0 \leq k \leq n_y})[x_0, \ldots, x_{n_x}, y_0, \ldots, y_{n_y}]$. Since P is admissible, there exists $x_{j_0} y_{k_0}$ such that $x_{j_0} y_{k_0} \notin P$ (this shows the non-emptiness). Let $\prec$ be an admissible order. Then consider the normal form for this order

$$\mathsf{NF}_P(\mathfrak{f}) = \sum_{t \text{ monomial}} h_t(\mathfrak{a}_{0,0} \ldots, \mathfrak{a}_{n_x,n_y}) t.$$

By multiplying by the least common multiple of the denominators, we can assume without loss of generality that for each t, h_t is a polynomial. Thus, if a bilinear polynomial is in P, then its coefficients are in the variety of the polynomial system $\forall t, h_t(\mathfrak{a}_{0,0}, \dots, \mathfrak{a}_{n_x,n_y}) = 0$. $\square$

Theorem 7. *Let $m, n_x, n_y \in \mathbb{N}$ such that $m \leq n_x + n_y$. Then the set of bilinear systems $f_1, \dots, f_m$ such that for all i, f_i does not divide 0 in R/J_{i-1} contains a Zariski nonempty open subset.*

Proof. We prove the Theorem by recurrence on m. Suppose that for all i such that $2 \leq i \leq m-1$, f_i is not a divisor of 0 in R/J_{i-1}. We prove that the set of bilinear polynomials f such that f is not a divisor of 0 in R/J_{m-1} contains a nonempty Zariski open subset. According to Lemma 14, for each admissible prime ideal $P \in Ass(I_{m-1})$, the set $\mathcal{O}_P = \{f \notin P\}$ contains a nonempty Zariski open subset. Thus $\bigcap_P \mathcal{O}_P$ contains a nonempty Zariski subset. Therefore, the set of bilinear polynomials f which are not divisor of 0 in R/J_{m-1} (this set is exactly $\bigcap_P \mathcal{O}_P$) contains a Zariski nonempty open subset. $\square$

Proposition 8. *Let $m \leq n_x + n_y$ and $f_1, \dots, f_m$ be bilinear polynomials such that for all i such that $2 \leq i \leq m$, f_i is not a divisor of 0 in R/J_{i-1}. Then for all i such that $1 \leq i \leq m$, the ideal J_i is equidimensional and its codimension is i.*

Proof. We prove the Proposition by recurrence on m.

- $J_1 = I_1$ is equidimensional and $\mathsf{codim}(I_1) = 1$;
- Suppose that J_{i-1} is equidimensional of codimension $i-1$. Then $J_i = (J_{i-1} + f_i) : (X \cap Y)^\infty$. f_i does not divide 0 in R/J_{i-1} (Theorem 7), thus $J_{i-1} + f_i$ is equidimensional of codimension i. The saturation does not decrease the dimension of any primary component of $J_{i-1} + f_i$. Therefore, J_i is equidimensional and its codimension is i.

$\square$

Appendix B. Ideals generated by generic affine bilinear systems

Let k be a field of characteristic 0, $m = n_x + n_y$, and $\mathfrak{a}$ be the set

$$\mathfrak{a} = \{\mathfrak{a}_{j,k}^{(i)} : 1 \leq i \leq m, 0 \leq j \leq n_x, 0 \leq k \leq n_y\}.$$

We consider generic polynomials $f_1, \dots, f_m$ in $k(\mathfrak{a})[x_0, \dots, x_{n_x}, y_0, \dots, y_{n_y}]$:

$$f_i = \sum \mathfrak{a}_{j,k}^{(i)} x_j y_k$$

and we denote by $I \subset k(\mathfrak{a})[x_0, \dots, x_{n_x}, y_0, \dots, y_{n_y}]$ the ideal they generate. In the sequel, ϑ denotes the dehomogenization morphism:

$$\begin{array}{ccc} k[x_0, \dots, x_{n_x}, y_0, \dots, y_{n_y}] & \longrightarrow & k[x_0, \dots, x_{n_x-1}, y_0, \dots, y_{n_y-1}] \\ f(x_0, \dots, x_{n_x}, y_0, \dots, y_{n_y}) & \longmapsto & f(x_0, \dots, x_{n_x-1}, 1, y_0, \dots, y_{n_y-1}, 1) \end{array}.$$

For $\mathbf{a} \in k^{m(n_x+n_y+2)}$, $\varphi_{\mathbf{a}}$ stands for the specialization:

$$\begin{array}{rccc} \varphi_{\mathbf{a}}: & k(\mathfrak{a})[x_0,\dots,x_{n_x},y_0,\dots,y_{n_y}] & \rightarrow & k[x_0,\dots,x_{n_x},y_0,\dots,y_{n_y}] \\ & f(\mathfrak{a})(x_0,\dots,x_{n_x},y_0,\dots,y_{n_y}) & \mapsto & f(\mathbf{a})(x_0,\dots,x_{n_x},y_0,\dots,y_{n_y}) \end{array}$$

Also $Var(\varphi_{\mathbf{a}}(I)) \subset \mathbb{P}^{n_x} \times \mathbb{P}^{n_y}$ (resp. $Var(\vartheta \circ \varphi_{\mathbf{a}}(I)) \subset \bar{k}^{n_x+n_y}$) denotes the variety of $\varphi_{\mathbf{a}}(I)$ (resp. $\vartheta \circ \varphi_{\mathbf{a}}(I)$).

Lemma 15. *There exists a nonempty Zariski open set O_1 such that if $\mathbf{a} \in O_1$, then for all $(\alpha_0,\dots,\alpha_{n_x},\beta_0,\dots,\beta_{n_y}) \in Var(\varphi_{\mathbf{a}}(I))$, $\alpha_{n_x} \neq 0$ and $\beta_{n_y} \neq 0$. This implies that the application*

$$\begin{array}{ccc} Var(\vartheta \circ \varphi_{\mathbf{a}}(I)) & \longrightarrow & Var(\varphi_{\mathbf{a}}(I)) \\ (\alpha_0,\dots,\alpha_{n_x-1},\beta_0,\dots,\beta_{n_y-1}) & \longmapsto & (\alpha_0,\dots,\alpha_{n_x-1},1,\beta_0,\dots,\beta_{n_y-1},1) \end{array}$$

is a bijection.

Proof. See (Van der Waerden, 1929, page 751). □

Lemma 16. *There exists a nonempty Zariski open set O_2, such that if $\mathbf{a} \in O_2$, then the ideal $\vartheta \circ \varphi_{\mathbf{a}}(I)$ is radical.*

Proof. Denote by F the polynomial family $(f_1,\dots,f_m) \in k[\mathfrak{a},X,Y]^m$. Let $J \subset k[\mathfrak{a}]$ be the ideal $\big(I + \langle \det(\mathsf{jac}_{X,Y}(F)) \rangle\big) \cap k[\mathfrak{a}]$ and $\mathscr{J}$ be its associated algebraic variety. By the Jacobian Criterion (see e.g. (Eisenbud, 1995, Theorem 16.19)), if $\mathbf{a}$ does not belong to $\mathscr{J}$, then $\vartheta \circ \varphi_{\mathbf{a}}(I)$ is radical. Thus, it is sufficient to prove that $k^{m(n_x+n_y+2)} \setminus \mathscr{J}$ is non-empty.

To do that, we prove that for all $\mathbf{a} \in k^{m(n_x+n_y+2)}$, there exists $(\varepsilon_1,\dots,\varepsilon_m)$ such that the ideal $\langle \vartheta \circ \varphi_{\mathbf{a}}(f_1) + \varepsilon_1, \dots, \vartheta \circ \varphi_{\mathbf{a}}(f_m) + \varepsilon_m \rangle$ is radical. Denote by $g_i = \vartheta \circ \varphi_{\mathbf{a}}(f_i)$ for $1 \leq i \leq m$ and consider the mapping Ψ

$$x \in k^m \rightarrow (g_1(x),\dots,g_m(x)) \in k^m.$$

Suppose first that $\Psi(k^m)$ is not dense in k^m. Since $\Psi(k^m)$ is a constructible set, it is contained in a Zariski-closed subset of k^m and there exists $(\varepsilon_1,\dots,\varepsilon_m)$ such that the algebraic variety defined by $g_1 - \varepsilon_1 = \cdots = g_m - \varepsilon_m = 0$ is empty. Since there exists $\mathbf{a}'$ such that $g_i - \varepsilon_i = \vartheta \circ \varphi_{\mathbf{a}'}(f_i)$, we conclude that $\vartheta \circ \varphi_{\mathbf{a}'}(I) = \langle 1 \rangle$. This implies that $\mathbf{a}' \notin \mathscr{J}$.

Suppose now that $\Psi(k^m)$ is dense in k^m. By Sard's theorem (Shafarevich, 1977, Chap. 2, Section 6.2, Theorem 2), there exists $(\varepsilon_1,\dots,\varepsilon_m) \in k^m$ which does not lie in the set of critical values of Ψ. This implies that at any point of the algebraic variety defined by $g_1 - \varepsilon_1 = \cdots = g_m - \varepsilon_m = 0$, $\vartheta \circ \varphi_{\mathbf{a}}(\det(\mathsf{jac}_{X,Y}(F)))$ does not vanish. Remark now that there exists $\mathbf{a}'$ such that $g_i - \varepsilon_i = \vartheta \circ \varphi_{\mathbf{a}'}(f_i)$. We conclude that $\mathbf{a}' \in k^{m(n_x+n_y+2)} \setminus \mathscr{J}$, which ends the proof. □

Lemma 17. *There exists a nonempty Zariski open set O_3, such that if $\mathbf{a} \in O_3$,*

$$\sqrt{\langle \mathsf{MaxMinors}(\vartheta \circ \varphi_{\mathbf{a}}(\mathsf{jac}_{\mathbf{y}}(F))) \rangle} = \langle \vartheta \circ \varphi_{\mathbf{a}}(f_1),\dots,\vartheta \circ \varphi_{\mathbf{a}}(f_m) \rangle \cap k[x_0,\dots,x_{n_x-1}].$$

Proof. Let $\mathbf{a}$ be an element in O_2 (as defined in Lemma 16). Thus $\vartheta \circ \varphi_{\mathbf{a}}(I)$ is radical. Now let $(v_0, \ldots, v_{n_x-1}, w_0, \ldots, w_{n_y-1}) \in Var(\vartheta \circ \varphi_{\mathbf{a}}(I))$ be an element of the variety. Then

$$\left(\vartheta \circ \varphi_{\mathbf{a}}(\mathsf{jac}_{\mathbf{y}}(F))_{x_i=v_i}\right) \cdot \begin{pmatrix} w_0 \\ \vdots \\ w_{n_y-1} \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

This implies that $\mathsf{rank}(\vartheta \circ \varphi_{\mathbf{a}}(\mathsf{jac}_{\mathbf{y}}(F))_{x_i=v_i}) < n_y + 1$, and therefore

$$(v_0, \ldots, v_{n_x-1}) \in Var(\langle \mathsf{MaxMinors}(\vartheta \circ \varphi_{\mathbf{a}}(\mathsf{jac}_{\mathbf{y}}(F))) \rangle).$$

Conversely, let $(v_0, \ldots, v_{n_x-1}) \in Var(\langle \mathsf{MaxMinors}(\vartheta \circ \varphi_{\mathbf{a}}(\mathsf{jac}_{\mathbf{y}}(F))) \rangle)$. Thus there exists a non trivial vector $(w_0, \ldots, w_{n_y})$ in the right kernel $\mathsf{Ker}(\vartheta \circ \varphi_{\mathbf{a}}(\mathsf{jac}_{\mathbf{y}}(F))_{x_i=v_i})$. This means that $(v_0, \ldots, v_{n_x-1}, 1, w_0, \ldots, w_{n_y})$ is in the variety of $\varphi_{\mathbf{a}}(I)$:

$$(v_0, \ldots, v_{n_x-1}, 1, w_0, \ldots, w_{n_y}) \in Var(\varphi_{\mathbf{a}}\left(\mathsf{jac}_{\mathbf{y}}(F)\right) \cdot \begin{pmatrix} y_0 \\ \vdots \\ y_{n_y} \end{pmatrix})$$

From Lemma 15, $w_{n_y} \neq 0$ if the system is generic. Hence

$$(v_0, \ldots, v_{n_x-1}, \frac{w_0}{w_{n_y}}, \ldots, \frac{w_{n_y-1}}{w_{n_y}}) \in Var(\vartheta \circ \varphi_{\mathbf{a}}(I)).$$

Finally, we have

$$Var(\langle \mathsf{MaxMinors}(\vartheta \circ \varphi_{\mathbf{a}}(\mathsf{jac}_{\mathbf{y}}(F))) \rangle) = Var(\langle \vartheta \circ \varphi_{\mathbf{a}}(f_1), \ldots, \vartheta \circ \varphi_{\mathbf{a}}(f_m) \rangle \cap k[x_0, \ldots, x_{n_x-1}])$$

and $\vartheta \circ \varphi_{\mathbf{a}}(I)$ is radical (Lemma 16). The Nullstellensatz concludes the proof. □

Corollary 4. *There exists a nonempty Zariski open set* O_4*, such that if* $\mathbf{a} \in O_4$*,*

$$\mathsf{card}(Var(\vartheta \circ \varphi_{\mathbf{a}}(I))) = \deg(\vartheta \circ \varphi_{\mathbf{a}}(I)) = \binom{n_x + n_y}{n_x}$$

Proof. According to Lemma 16 and Lemma 15, if $\mathbf{a} \in O_1 \cap O_2$, then $\deg(\vartheta \circ \varphi_{\mathbf{a}}(I)) = \mathsf{card}(Var(\vartheta \circ \varphi_{\mathbf{a}}(I)) = \mathsf{card}(Var(\varphi_{\mathbf{a}}(I)))$. This value is the so-called multihomogeneous Bézout number of $\varphi_{\mathbf{a}}(I)$, i.e. the coefficient of $z_1^{n_x} z_2^{n_y}$ in $(z_1 + z_2)^{n_x+n_y}$ (see e.g. Morgan and Sommese (1987)), namely $\binom{n_x+n_y}{n_x}$. □

Remark 7. *Actually, by studying ideals spanned by maximal minors of matrices whose entries are linear forms, it can be shown that, for a generic affine bilinear system,* $\langle \mathsf{MaxMinors}(\vartheta \circ \varphi_{\mathbf{a}}(\mathsf{jac}_{\mathbf{y}}(F))) \rangle$ *is radical (see Lemma 6). Hence Lemma 17 shows that, for generic affine bilinear systems,*

$$\langle \mathsf{MaxMinors}(\vartheta \circ \varphi_{\mathbf{a}}(\mathsf{jac}_{\mathbf{y}}(F))) \rangle = \langle \vartheta \circ \varphi_{\mathbf{a}}(f_1), \ldots, \vartheta \circ \varphi_{\mathbf{a}}(f_m) \rangle \cap k[x_0, \ldots, x_{n_x-1}],$$

$$\langle \mathsf{MaxMinors}(\vartheta \circ \varphi_{\mathbf{a}}(\mathsf{jac}_{\mathbf{x}}(F))) \rangle = \langle \vartheta \circ \varphi_{\mathbf{a}}(f_1), \ldots, \vartheta \circ \varphi_{\mathbf{a}}(f_m) \rangle \cap k[y_0, \ldots, y_{n_y-1}].$$