On the complexity of the F5 Gröbner basis algorithm

Magali Bardet, Jean-Charles Faugère, Bruno Salvy

On the Complexity of the F_5 Gröbner basis Algorithm

Magali Bardet[a,*], Jean-Charles Faugère[b], Bruno Salvy[c]

[a] *Équipe C&A, LITIS, Université de Rouen*
[b] *UPMC, Univ Paris 06, LIP6*
CNRS, UMR 7606, LIP6
PolSys Project, Inria
[c] *AriC Project, Inria,*
LIP, ENS de Lyon,
CNRS, UCBL, Université de Lyon.

Abstract

We study the complexity of Gröbner bases computation, in particular in the generic situation where the variables are in simultaneous Noether position with respect to the system.

We give a bound on the number of polynomials of degree d in a Gröbner basis computed by Faugère's F_5 algorithm (2002) in this generic case for the grevlex ordering (which is also a bound on the number of polynomials for a reduced Gröbner basis, independently of the algorithm used). Next, we analyse more precisely the structure of the polynomials in the Gröbner bases with signatures that F_5 computes and use it to bound the complexity of the algorithm.

Our estimates show that the version of F_5 we analyse, which uses only standard Gaussian elimination techniques, outperforms row reduction of the Macaulay matrix with the best known algorithms for moderate degrees, and even for degrees up to the thousands if Strassen's multiplication is used. The degree being fixed, the factor of improvement grows exponentially with the number of variables.

Keywords: Gröbner bases, F_5 algorithm, Complexity, Regular Sequences, Noether Position

Introduction

The complexity of Gröbner bases has been the object of extensive studies. It is well-known that in the worst-case, the complexity is doubly exponential in the number of variables. This is the result of a series of works both on lower bounds by Mayr and Meyer (1982); Huỳnh (1986) and on upper bounds, first in characteristic 0 by Giusti (1984); Möller and Mora (1984) and then in positive characteristic by Dubé (1990).

These worst-case estimates have led to the unfortunately widespread belief that Gröbner bases are not a useful tool beyond toy examples. However, it has been observed for a long time that the actual behaviour of Gröbner bases implementations can be quite efficient. For instance, the matrix-F_5 algorithm that we analyse in this article, itself a downgraded version of

*Corresponding author
Email addresses: Magali.Bardet@univ-rouen.fr (Magali Bardet), Jean-Charles.Faugere@inria.fr (Jean-Charles Faugère), Bruno.Salvy@inria.fr (Bruno Salvy)

Faugère's F_5 algorithm (2002) and a particular case of Faugère and Rahmany (2009), has given surprisingly good results on a cryptographic challenge (see Faugère and Joux (2003) where a set of 80 dense polynomials in 80 variables was solved by this algorithm). This motivates an investigation of the complexity of Gröbner basis algorithms for useful special classes of polynomial systems.

In this article, we concentrate on the important case of homogeneous systems. Any system can be brought into this form by adding a variable and homogenizing. It is classical that the computation of Gröbner bases can be performed by linear algebra on a large matrix that has been described precisely by Macaulay (1902). The explicit relation with Gröbner bases can be found in the works of Lazard (1983) and Giusti (1984, 1985). From there, a simple statement of a complexity bound is the following.

Proposition 1. *Let $(f_1,\ldots,f_m)$ be a system of homogeneous polynomials in $k[x_1,\ldots,x_n]$ with k an arbitrary field. The number of operations in k required to compute a Gröbner basis of the ideal $\mathscr{I}$ generated by $(f_1,\ldots,f_m)$ for a graded monomial ordering* up to degree D *is bounded by*

$$O\left(mD\binom{n+D-1}{D}^{\omega}\right),\ \textit{as } D\to\infty$$

where ω is the exponent of matrix multiplication over k.

The terminology and notations relative to Gröbner bases are recalled in Section 1, and we generally follow Cox et al. (1997). The simple proof of this proposition is given in Section 1. For the notation ω and related notions, we refer to von zur Gathen and Gerhard (2003).

Getting a "small" bound on the highest degree of the elements of the Gröbner basis then leads to good complexity estimates. Such a bound is available for regular systems in the graded-reverse-lexicographical order (grevlex). In this situation, Lazard (1983) has shown that after a generic linear change of coordinates, a bound is given by the index of regularity of the ideal, which is itself bounded by

$$\text{Macaulay's bound:}\qquad i_{\text{reg}}\le\sum_{i=1}^{m}(d_i-1)+1, \tag{1}$$

where $d_i=\deg(f_i)$. This bound is named after Macaulay (1902), who obtained it as an upper bound on the degree of intermediate polynomials used in the computation of a resultant of generic multivariate polynomials.

Taking $m=n-\ell$ (with $\ell\ge 0$) and injecting Macaulay's bound (1) into the upper bound of Proposition 1 leads to a general asymptotic bound for the number of operations:

$$\left(\frac{\delta^{\delta}}{(\delta-1)^{\delta-1}}\right)^{\omega(n-\ell)} n^{2-\omega/2}\left((\delta-1)\left(\frac{\delta}{2\pi(\delta-1)^3}\right)^{\omega/2}+O(1/n)\right),\quad n\to\infty, \tag{2}$$

where δ, assumed to be larger than 1, is the arithmetic mean of the d_i's. (When $\delta=1$, the system is linear.)

Thus in this case, we have a complexity which is *simply* exponential in the number of variables. Since in this case, if the field is algebraically closed, by Bézout's bound, the degree of the variety is also exponential, the result can be interpreted as a polynomial complexity in some size of the result. No change of variable is necessary when the dimension is 0. Otherwise, without a

generic linear change of coordinates, the bound does not hold in general, as observed by Möller and Mora (1984).

These results can be made effective by a careful study of the required genericity condition. Indeed, Lejeune-Jalabert (1984) shows that a sufficient condition for the bound to hold is that the variables be in *simultaneous Noether position* with respect to the polynomial system. (The definition is recalled in Section 1). If the system is regular but the variables are not in simultaneous Noether position, and the field is sufficiently large, then a linear change of variables can be exhibited that puts the variables in this position. The complexity of actually finding such a linear change of variables in the worst case has been studied by Giusti (1988, §5.6) and later by Giusti and Heintz (1993). It is used as an ingredient to compute the dimension in small complexity (Giusti et al. (2000)). The name "simultaneous Noether position" for this situation has been used at least since the work of Krick and Pardo (1996).

This simply exponential behaviour being established, we are interested in sharpening the complexity estimates. This is important in order to compare various algorithms precisely, including approaches to polynomial system solving that do not use Gröbner bases, such as developed by Giusti et al. (2001). We concentrate on systems with variables in simultaneous Noether position. This forms the basis for many other applications, either by changes of coordinates as we have just indicated, or by changes of order following Faugère et al. (1993), or by other techniques as developed for instance by Lakshman and Lazard (1991); Lakshman (1991); Hashemi and Lazard (2011).

Most algorithmic variants of Buchberger's (1965) algorithm spend part of their time computing reductions to 0, which is why many criteria and strategies have been developed over the years. An assessment of the efficiency of these strategies is obtained for instance by a comparison of their complexity for $m = n - \ell$ polynomials in n variables with the bound (2), for an arbitrary fixed $\ell \geq 0$. We obtain such a complexity estimate for a specific algorithm, namely Faugère's F_5 algorithm (2002). This algorithm has been the first one to introduce signatures in order to detect efficiently useless reductions to zero. Since then, many researchers have worked on understanding the new criteria behind F_5, which has led to new variants of the signature-based approach. Eder and Faugère (2014) give a detailed introduction to this topic. In Section 2, we present and analyse the matrix-F_5 version of the algorithm. A consequence of our results is the following estimate.

Theorem 2. *Let $(f_1, \ldots, f_m)$ be a system of homogeneous polynomials of identical degree $\delta \geq 2$ in $k[x_1, \ldots, x_n]$ with $m = n - \ell$ and $\ell \geq 0$, with respect to which $(x_1, \ldots, x_n)$ are in simultaneous Noether position. Then the number of arithmetic operations in k required* by Algorithm matrix-F_5 *to compute a Gröbner basis for the grevlex order is bounded by a function of δ, ℓ, n that behaves asymptotically as*

$$B(\delta)^n n \left(A(\delta, \ell) + O(1/n)\right), \quad n \to \infty, \tag{3}$$

when ℓ and δ are $O(1)$. There, the coefficients $B(\delta)$ and $A(\delta, \ell)$ are given by

$$B(\delta) = \frac{\left(\frac{\lambda_0+1}{\lambda_0}\right)^{2\delta} - 1}{\frac{1}{\lambda_0^2} - \frac{1}{(\lambda_0+1)^2}} \quad \text{and} \quad A(\delta, \ell) = \frac{1 - \delta^{-1}}{2\pi} \cdot \frac{\left(1 + \lambda_0^{-1}\right)^3 - 1}{(1 + \lambda_0)^{1+\ell}},$$

λ_0 *being the unique positive root between* $\frac{\delta-1}{2}$ *and* $\delta-1$ *of*

$$\left(\frac{\lambda+1}{\lambda}\right)^{2\delta} = \frac{1}{1-\delta\frac{(\lambda+1)^2-\lambda^2}{(\lambda+1)^3-\lambda^3}}.$$

Moreover, the dominant term $B(\delta)$ *is bounded between* δ^3 *and* $3\delta^3$.

Explicit values of this bound (3), called the F_5-bound, are given in Table 1.

δ	2	3	4	5	6	7	8
$B(\delta)^n$	$2^{4.29n}$	$2^{6.16n}$	$2^{7.44n}$	$2^{8.43n}$	$2^{9.23n}$	$2^{9.90n}$	$2^{10.5n}$
=	$(2^n)^{4.3}$	$(3^n)^{3.9}$	$(4^n)^{3.7}$	$(5^n)^{3.6}$	$(6^n)^{3.6}$	$(7^n)^{3.5}$	$(8^n)^{3.5}$
=	$(2.5)^n 2^{3n}$	$(2.7)^n 3^{3n}$	$(2.7)^n 4^{3n}$	$(2.8)^n 5^{3n}$	$(2.8)^n 6^{3n}$	$(2.8)^n 7^{3n}$	$(2.8)^n 8^{3n}$

Table 1: Asymptotic Behaviour of the F_5-bound (Equation (3)), in terms of the Bézout bound δ^n.

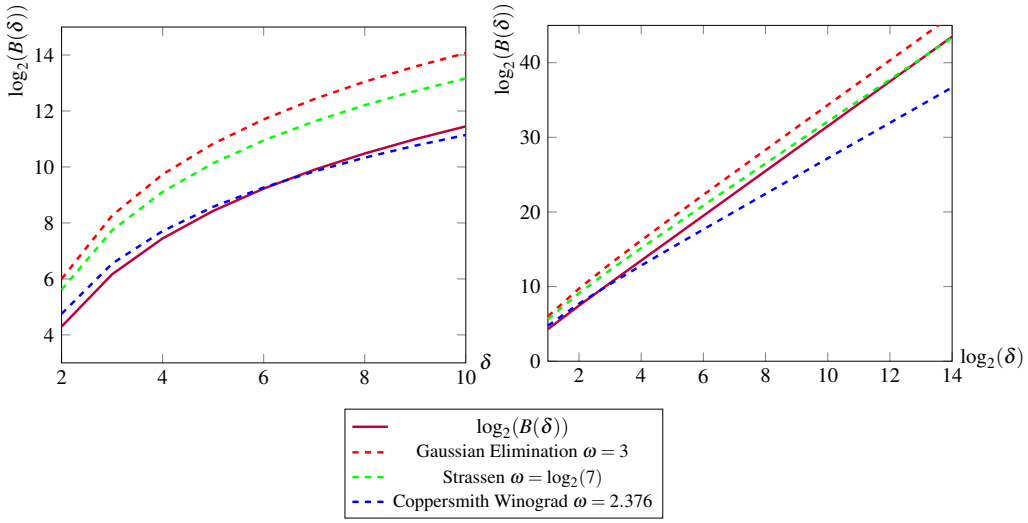

Figure 1: Asymptotic of the F_5-bound vs linear algebra on the Macaulay Matrix

We now draw a few consequences of this theorem.

Numerical estimates. In view of (2), $B(\delta)$ can be compared to $\left(\delta^\delta/(\delta-1)^{\delta-1}\right)^\omega$ where ω is the exponent of matrix multiplication over k, and therefore our result can be interpreted as a first measure of the extent to which the F_5 algorithm exploits the structure of the Macaulay matrix for the computation. In Figure 1, we display the values of $B(\delta)$ as well as the arithmetic complexity of the linear algebra performed on the Macaulay matrix for different values of the exponent ω. The first plot gives these values for δ from 2 to 10, and the second one gives the logarithm of these values in terms of $\log(\delta)$, for δ from 2^1 to $2^{14} = 16384$. For $2 \leq \delta < 7$, the F_5-bound gives a better complexity than the Coppersmith and Winograd (1990) bound $\omega < 2.376$ and the recently improved bounds down to $\omega < 2.373$ by Stothers (2010), Vassilevska Williams (2012)

and Le Gall (2014). It is better than Strassen's bound $\omega = \log_2 7$ for $2 \leq \delta < 9911$. Thus in practice, for this whole range of degrees, the complexity estimate of F_5 behaves asymptotically (wrt to n) exponentially better than linear algebra with fast matrix multiplication over the Macaulay matrix.

Nonhomogeneous systems. In the affine case, Theorem 2 can often be applied with $\ell = 1$: let $(f_1, \ldots, f_n)$ be a system of affine polynomials of identical degree $\delta \geq 2$ in $k[x_1, \ldots, x_n]$; we consider $(H_1, \ldots, H_n)$ the polynomials obtained by homogenizing the f_i in $k[x_1, \ldots, x_n, h]$. Provided $x_1, \ldots, x_n, h$ are in simultaneous Noether position with respect to the system $(H_1, \ldots, H_n)$ (or equivalently, $x_1, \ldots, x_n$ are in simultaneous Noether position with respect to the system formed by the homogeneous part of highest degree of the f_i), we can then apply the theorem to $(H_1, \ldots, H_n)$ and derive a bound on the number of operations.

Other term orders. Under the same hypotheses as in Theorem 2, the computation of a Gröbner basis for the lexicographical order can be achieved by first computing a Gröbner basis for the grevlex order using Algorithm matrix-F_5 in $O(nB^n)$ operations and then converting into a basis for the lexicographical order using the FGLM algorithm of Faugère et al. (1993) in $O(n\delta^{3n})$ operations. Since $B \geq \delta^3$, the overall complexity is still bounded by $O(nB^n)$ arithmetic operations over k.

System solving. If the field k is infinite and the system is regular, a generic linear change of variables puts the variables in simultaneous Noether position. The construction is given for instance by Giusti (1988, §5.6), see also Giusti and Heintz (1993). Thus in practice, for zero-dimensional polynomial system solving, the simultaneous Noether position hypothesis can be replaced by the regularity of the system.

This article is structured as follows. In Section 1, we recall the basic definitions and properties of regular sequences and Gröbner bases, the relation between Gröbner bases and linear algebra and the definition of simultaneous Noether position. In Section 2, we give a simple version of the F_5 algorithm and we give a structure theorem for Gröbner bases computed by this signature-based algorithm. In Section 3 we describe more precisely its behaviour for systems with variables in simultaneous Noether position for the grevlex ordering and deduce an upper bound for the complexity of F_5 in this case. Finally, in Section 4 we discuss the practical accuracy of the bounds we provide in this paper. In view of our numerical experiments, the practical behaviour of the algorithm F_5 seems to be asymptotically exponentially better than our bound. A characterisation of the exact exponent in the complexity is still open.

Preliminary versions of this work have appeared in Bardet's PhD thesis (2004).

1. Gröbner Bases and Regularity

This section gathers classical definitions and properties, so that this article is self-contained. We generally follow the terminology and notations of Cox et al. (1997).

1.1. Basic Notation and Definitions

The polynomial systems we consider are always denoted $(f_1, \ldots, f_m) \in k[x_1, \ldots, x_n]$ where k is a field. We denote by d_i the degree of f_i. Throughout this article, the polynomials are homogenous. The set of homogeneous polynomials of degree d is denoted $k[x_1, \ldots, x_n]_d$. We

use $\mathscr{T}^i$ to denote the set of nonzero *monomials* in $x_1,\ldots,x_i$ (i.e., products $x_1^{\alpha_1}\cdots x_i^{\alpha_i}$ with non-negative integer exponents α_j), and $\mathscr{T}_d^i$ the subset of monomials of degree d. When $i=n$, we use simply $\mathscr{T}=\mathscr{T}^n$ and $\mathscr{T}_d=\mathscr{T}_d^n$. The ideal generated by the polynomial system is denoted $\mathscr{I}=\langle f_1,\ldots,f_m\rangle$ and the vector space of homogeneous polynomials of degree d in $\mathscr{I}$ is denoted $\mathscr{I}_d$.

A *monomial ordering* is a total order on monomials that is compatible with the product and such that every nonempty set has a smallest element for the order. Such an ordering is *graded* if monomials of different degrees are ordered according to their degree. The *leading term* $\mathrm{LT}(f)$ of a polynomial f is the *term* (i.e., monomial multiplied by a nonzero constant in k) corresponding to its largest monomial for the given monomial ordering.

The *grevlex* ordering is a graded ordering. The order between two monomials of the same degree $x_\alpha=x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ and $x_\beta=x_1^{\beta_1}\cdots x_n^{\beta_n}$ is given by $x_\alpha\succ x_\beta$ when the last nonzero element of $(\alpha_1-\beta_1,\ldots,\alpha_n-\beta_n)$ is negative. Thus, among the monomials of degree d, the order is

$$x_1^d\succ x_1^{d-1}x_2\succ x_1^{d-2}x_2^2\succ\cdots\succ x_2^d\succ x_1^{d-1}x_3\succ x_1^{d-2}x_2x_3\succ x_1^{d-2}x_3^2\succ\cdots\succ x_n^d.$$

A *Gröbner basis* of an ideal $\mathscr{I}$ for a given monomial ordering is a set G of generators of $\mathscr{I}$ such that the leading terms of G generate the monomial ideal $\langle\mathrm{LT}(\mathscr{I})\rangle$, which is the ideal generated by the monomials $\mathrm{LT}(f), f\in\mathscr{I}$. A polynomial is *reduced* with respect to the Gröbner basis G when its leading term is not a multiple of those of G. The basis is *reduced* if each element $g\in G$ is reduced with respect to $G\setminus\{g\}$.

1.2. Macaulay's Matrix

We recall briefly the construction of this matrix and the explicit relation with Gröbner bases, which can be found in the works by Lazard (1983) and Giusti (1984, 1985). There are several advantages to this point of view: one is that, for a graded order, it gives an easy access to the Hilbert function of the ideal, another one is that upper bounds on the complexity are easily recovered from classical linear algebra.

For a given degree d and polynomial system $(f_1,\ldots,f_m)$, Macaulay's matrix $\mathscr{M}_{d,m}$ has its columns indexed by the monomials of $\mathscr{T}_d$. For each polynomial f_i of the system and each monomial $t\in\mathscr{T}_{d-d_i}$, it contains one row whose entry in the column indexed by a monomial t' is the coefficient of t' in tf_i. Thus, the rows of this matrix generate the vector space $\mathscr{I}_d$. The *Hilbert function* is defined by

$$\mathrm{HF}_{\mathscr{I}}(d)=\dim k[x_1,\ldots,x_n]_d/\mathscr{I}_d,$$

it is therefore equal to the dimension $\binom{n+d-1}{d}$ of $k[x_1,\ldots,x_n]_d$ minus the rank of $\mathscr{M}_{d,m}$. For d large enough, this function is a polynomial (the *Hilbert polynomial* $\mathrm{HP}_{\mathscr{I}}$). The generating function $\mathrm{H}_{\mathscr{I}}=\sum_{d\geq 0}\mathrm{HF}_{\mathscr{I}}(d)z^d$ is called the *Hilbert series* of the ideal.

1.3. Gröbner Bases

Performing a Gaussian elimination on the matrix $\mathscr{M}_{d,m}$ computes a basis of $\mathscr{I}_d$. If moreover, the columns are ordered by decreasing order with respect to the chosen graded monomial ordering, and column pivoting is not allowed, then the leading terms of this basis give $\mathrm{LT}(\mathscr{I}_d)$. From these bases for $\min(d_1,\ldots,d_m)\leq d\leq D$, where D is the maximal degree of the elements in the reduced Gröbner basis of $\mathscr{I}$, this Gröbner basis can be reconstructed. This way, the computation is reduced to linear algebra operations.

From there we now prove the general upper bound on the complexity that has been given in Proposition 1.

Macaulay's matrix $\mathscr{M}_{d,m}$ has $C_d = |\mathscr{T}_d| = \binom{n+d-1}{d}$ columns and $R_d = |\mathscr{T}_{d-d_1}| + \cdots + |\mathscr{T}_{d-d_m}|$ rows. A basis of its rows is obtained by the computation of a reduced row echelon form. Storjohann (2000) has shown that fast matrix multiplication can be used to compute this form with a complexity of $O(R_d C_d r^{\omega-2})$, where r is the rank of the matrix. Thus, this is bounded by $O(R_d C_d^{\omega-1})$.

The computation is performed for $d = \min(d_1,\ldots,d_m),\ldots,D$. The number of rows is bounded by mC_d and C_d is an increasing sequence, so that the conclusion of Proposition 1 follows.

The remaining problems are to bound D and to perform this Gaussian elimination efficiently by taking the structure of the matrix into account. An important class where this can be done is the class of regular systems.

1.4. Regular Systems

Definition 1. $(f_1,\ldots,f_m)$ is regular if for all $i = 1,\ldots,m$, f_i is not a zero-divisor in the quotient ring $k[x_1,\ldots,x_n]/\langle f_1,\ldots,f_{i-1}\rangle$. In other words if there exists g such that $gf_i \in \langle f_1,\ldots,f_{i-1}\rangle$ then g belongs to $\langle f_1,\ldots,f_{i-1}\rangle$.

The following Lemma gives a characterisation of zero-divisors for homogeneous polynomials:

Lemma 3. *Let $\mathscr{I} \subset k[x_1,\ldots,x_n]$ be an homogeneous ideal, $\mathscr{I} \neq \langle 1\rangle$, and $f \in k[x_1,\ldots,x_n]$ homogeneous of degree $\delta \geq 1$. Then f is not a zero-divisor in $k[x_1,\ldots,x_n]/\mathscr{I}$ if and only if $\mathrm{H}_{\mathscr{I}+\langle f\rangle}(z) = (1-z^\delta)\,\mathrm{H}_{\mathscr{I}}(z)$.*

Proof. The proof boils down to using the relation between the dimensions of the kernel K_d and image of the application of multiplication by f from $k[x_1,\ldots,x_n]_{d-\delta}/\mathscr{I}_{d-\delta}$ to $k[x_1,\ldots,x_n]_d/\mathscr{I}_d$. This gives

$$\mathrm{HF}_{\mathscr{I}+\langle f\rangle}(d) = \mathrm{HF}_{\mathscr{I}}(d) - \mathrm{HF}_{\mathscr{I}}(d-\delta) + \dim(K_d), \qquad d \in \mathbb{N}. \tag{4}$$

(with the convention $\mathrm{HF}(-d) = 0$ for $d \geq 1$). Multiplying (4) by z^d and summing over d leads to

$$H_{\mathscr{I}+\langle f\rangle}(z) = (1-z^\delta)H_{\mathscr{I}}(z) + \sum_{d\geq 0} \dim(K_d) z^d.$$

The equivalence results from the definition: f is not a zero-divisor in $k[x_1,\ldots,x_n]/\mathscr{I}$ if and only if $\dim(K_d) = 0$ for all $d \geq 0$. □

This leads to a classical property of regular systems, essentially due to Macaulay (1916, §58):

Proposition 4. *The system of homogeneous polynomials $(f_1,\ldots,f_m) \subset k[x_1,\ldots,x_n]$ is regular if and only if its Hilbert series is*

$$\mathrm{H}_{\mathscr{I}}(z) = \frac{\prod_{j=1}^m (1-z^{d_j})}{(1-z)^n}. \tag{5}$$

If $m = n$, then the sequence $(f_1,\ldots,f_n)$ is regular if and only if its Hilbert series is a polynomial.

Proof. The first part follows from the previous lemma and $H_{\langle\rangle}(z) = (1-z)^{-n}$ that counts the number of homogeneous monomials.

For $m = n$, if $\mathrm{H}_{\mathscr{I}}(z)$ is a polynomial, then Bézout's bound (Cox et al., 2005, ch. 3§5) states that $\mathrm{H}_{\mathscr{I}}(1)$, which is the number of solutions of $\mathscr{I}$ in the algebraic closure of k, is bounded by $\Pi_{j=1}^{n} d_j$. But Equation (4) leads to $\mathrm{H}_{\mathscr{I}}(z) \geq \prod_{j=1}^{n}(1-z^{d_j})/(1-z)^n$ with inequality coefficient by coefficient. By taking the value at $z = 1$, we get $\prod_{j=1}^{n} d_j \geq \mathrm{H}_{\mathscr{I}}(1) \geq \prod_{j=1}^{n} d_j$, which proves the equality. As each coefficient of the Hilbert series is nonnegative, we deduce that $\mathrm{H}_{\mathscr{I}}(z) = \prod_{j=1}^{n}(1-z^{d_j})/(1-z)^n$ and the sequence is regular by the first part of the lemma. □

Corollary 5. *Let $(f_1,\ldots,f_n)$ be a regular system of homogeneous polynomials in $k[x_1,\ldots,x_n]$, then the highest degree in the elements of a Gröbner basis for a graded ordering is bounded by Macaulay's bound* (1)*.*

Proof. When $m = n$, the Hilbert series (5) is a polynomial, whose degree D is one less than the bound (1). This implies that the Hilbert function is 0 for degree D. In other words all the monomials of $\mathscr{T}_D$ belong to $\mathscr{I}_D$, whence the result. □

Example 1. *The system*

$$\left\{\begin{array}{lcl} f_1 &=& x^2+y^2-2xz-2yz+z^2+h^2 \\ f_2 &=& x^2+xy+yz-z^2-2h^2 \\ f_3 &=& x^2-y^2+2yz-2z^2 \end{array}\right. \tag{6}$$

in $k[x,y,z,h]$, represents, for $h = 0$, the intersection of a projective circle and two hyperbolas over $k = \mathbb{R}$. The coefficient of h^2 is chosen so that the point $(1,1,1,1)$ is a solution of the system. The Hilbert series of the systems (f_1,f_2) and (f_1,f_2,f_3) (computed from a Gröbner Basis for a grevlex ordering) are respectively $H_{(f_1,f_2)}(t) = (1+t)^2/(1-t)^2 = (1-t^2)^2/(1-t)^4$ and $H_{(f_1,f_2,f_3)}(t) = (1+t)^3/(1-t) = (1-t^2)^3/(1-t)^4$, showing that these systems are regular.

1.5. Noether position

Definition 2. The variables $(x_1,\ldots,x_m)$ are in *Noether position* with respect to the system $(f_1,\ldots,f_m)$ if their canonical images in $k[x_1,\ldots,x_n]/\langle f_1,\ldots,f_m\rangle$ are algebraic integers over $k[x_{m+1},\ldots,x_n]$ and moreover $k[x_{m+1},\ldots,x_n] \cap \langle f_1,\ldots,f_m\rangle = \langle 0\rangle$.

The variable $x_i \in k[x_1,\ldots,x_n]/\langle f_1,\ldots,f_m\rangle$ is an algebraic integer over $k[x_{m+1},\ldots,x_n]$ when there exists a polynomial $g \in k[x_i,x_{m+1},\ldots,x_n] \cap \langle f_1,\ldots,f_m\rangle$ that is monic with respect to x_i. A Gröbner basis of $\langle f_1,\ldots,f_m\rangle$ for an elimination monomial ordering such that $\{x_j, 1 \leq j \neq i \leq m\} > \{x_i,x_{m+1},\ldots,x_n\}$ contains such a g (up to a constant) if and only if x_i has the desired property.

Example 2. *The variables (x,y) are in Noether position with respect to the system (f_1,f_2) from Example 1. Indeed, a Gröbner basis of the system for the lexicographical ordering $x > y > z > h$ (resp. $y > x > z > h$) contains the polynomial $2y^4-6y^3z+12y^2z^2+7y^2h^2-8yz^3-20yzh^2+4z^2h^2+9h^4$ (resp. $2x^4+2x^3z-2x^2z^2-3x^2h^2-2xz^3-2xzh^2+z^2h^2+4h^4$).*

On the other hand, the variables (y,z) are not in Noether position with respect to the system (f_1,f_2). Again, a Gröbner basis computation for the lexicographical ordering shows that $\mathscr{I} \cap k[y,x,h] = \langle 2y^3x+4y^2x^2-y^2h^2+8yx^3-8yxh^2-4x^2h^2-h^4\rangle$.

Geometrically, the Noether position implies that the algebraic set defined by the system has dimension $n-m$ and, in an algebraic closure of k, for any value of $(x_{m+1},\dots,x_n)$, the system has exactly the same number of solutions (counting multiplicity). In a sufficiently large field, for regular systems, the variables can be put in Noether position by a generic linear change of variables, as explained by Giusti (1988).

The following proposition characterises algebraically the Noether position property for homogeneous ideals. It shows that in this case, this position is also equivalent to the condition that the system $(f_1,\dots,f_m,x_{m+1},\dots,x_n)$ has only the solution $\{0\}$.

Proposition 6 (Lejeune-Jalabert, 1984)**.** *Let $(f_1,\dots,f_m)$ be a system of homogeneous polynomials of $k[x_1,\dots,x_n]$, such that $\langle f_1,\dots,f_m\rangle \neq \langle 1\rangle$. If the variables $(x_1,\dots,x_m)$ are in Noether position with respect to the system $(f_1,\dots,f_m)$, then the sequence $(f_1,\dots,f_m,x_{m+1},\dots,x_n)$ is regular.*

Proof. The variables $(x_1,\dots,x_m)$ being in Noether position with respect to the system $(f_1,\dots,f_m)$, for each $1\leq i\leq m$, there exists a polynomial $g\in k[x_i,x_{m+1},\dots,x_n]\cap\langle f_1,\dots,f_m\rangle$ of degree $n_i\geq 1$ in x_i such that the coefficient of $x_i^{n_i}$ in g is 1. This implies that the Hilbert series $H_{(f_1,\dots,f_m,x_{m+1},\dots,x_n)}(z)$ is a polynomial. Then by Proposition 4, $(f_1,\dots,f_m,x_{m+1},\dots,x_n)$ is a regular sequence. □

From the computational point of view, the following proposition gives very precise information on the structure of a grevlex Gröbner basis, it plays an important role in obtaining good complexity estimates in the next section.

Proposition 7 (Lejeune-Jalabert, 1984, Ch. 3, Prop. 3.4)**.** *Let $(x_1,\dots,x_m)$ be in Noether position with respect to the homogeneous system $(f_1,\dots,f_m)$. Let θ_m be a ring endomorphism of $k[x_1,\dots,x_n]$ such that $\theta_m(x_i)=x_i$ for $i\in\{1,\dots,m\}$, while $\theta_m(x_i)=0$ for $i>m$. Then, for the grevlex monomial ordering*

$$\mathrm{LT}(\langle f_1,\dots,f_m\rangle)=\mathrm{LT}(\theta_m(\langle f_1,\dots,f_m\rangle))\cdot\langle x_{m+1},\dots,x_n\rangle.$$

In other words, the leading terms of the elements of the reduced Gröbner basis do not depend on the variables $(x_{m+1},\dots,x_n)$.

Proof. Let $\mathscr{I}=\langle f_1,\dots,f_m\rangle$. The inclusion $\mathrm{LT}(\mathscr{I})\supset\mathrm{LT}(\theta_m(\mathscr{I}))\cdot\langle x_{m+1},\dots,x_n\rangle$ follows from the fact that for the grevlex monomial ordering, when $\theta_m(f)\neq 0$, $\mathrm{LT}(f)=\mathrm{LT}(\theta_m(f))$.

Conversely let $f\in\mathscr{I}$ and let $M=x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ be its leading monomial for the grevlex ordering. We have to prove that there exists $g\in\mathscr{I}$ with leading monomial $x_1^{\alpha_1}\cdots x_m^{\alpha_m}$. Since the ideal is homogeneous, we can assume f to be homogeneous as well. Let l be the largest index such that $x_l|M$. By definition of the grevlex ordering and the fact that M is the leading monomial of f, there exist homogeneous polynomials $g_l,\dots,g_n\in k[x_1,\dots,x_n]$ such that

$$f=x_l^{\alpha_l}g_l+x_{l+1}g_{l+1}+\cdots+x_ng_n,\qquad g_l\in k[x_1,\dots,x_l]\backslash\{0\}\text{ and }\mathrm{LT}(g_l)=x_1^{\alpha_1}\cdots x_{l-1}^{\alpha_{l-1}}. \quad (7)$$

By Proposition 6, the sequence $(f_1,\dots,f_m,x_{m+1},\dots,x_n)$ is regular. If $l>m$, then $f\equiv x_l^{\alpha_l}g_l\equiv 0 \mod \mathscr{I}+\langle x_{l+1},\dots,x_n\rangle$ and since from Proposition 4 x_l is not a zero-divisor in $k[x_1,\dots,x_n]/(\mathscr{I}+\langle x_{l+1},\dots,x_n\rangle)$ we deduce successively that $g_l\equiv 0 \mod \mathscr{I}+\langle x_{l+1},\dots,x_n\rangle$ and $g_l\equiv 0 \mod \mathscr{I}$. Hence, starting from $f\in\mathscr{I}$ such that $\mathrm{LT}(f)\in k[x_1,\dots,x_l]$ with $l>m$, we obtain $g_l\in\mathscr{I}$ such that $\mathrm{LT}(f)=x_l^{\alpha_l}\mathrm{LT}(g_l)$ and $\mathrm{LT}(g_l)\in k[x_1,\dots,x_{l-1}]$. By induction on l we can find a polynomial $g\in\mathscr{I}$ such that $\mathrm{LT}(f)=x_{m+1}^{\alpha_{m+1}}\cdots x_l^{\alpha_l}\mathrm{LT}(g)$ and $\mathrm{LT}(g)\in k[x_1,\dots,x_m]$. This proves the converse inclusion. □

In view of the incremental nature of the F_5 algorithm, an even stronger property will be useful in our considerations.

Definition 3. The variables $(x_1,\ldots,x_n)$ are in *simultaneous Noether position* with respect to the system $(f_1,\ldots,f_m)$ when the variables $(x_1,\ldots,x_i)$ are in Noether position with respect to $(f_1,\ldots,f_i)$ for all $i \in \{1,\ldots,m\}$.

Example 3. *The variables (x,y,z,h) in Example 1 are in simultaneous Noether position with respect to the system (f_1,f_2,f_3) from Equation* (6)*.*

Again, this situation is generic for regular systems and can be reached by a linear change of coordinates if the field is sufficiently large.

2. Signature-based Gröbner basis computations: the F_5 Algorithm

2.1. Description of the Matrix-F_5 algorithm

Faugère's (2002) F_5 algorithm is designed so that it ensures that no "useless" reduction to 0 is performed when the input system is regular. We now describe a matrix version of F_5 that is well-suited to a complexity analysis. The main difference with the original algorithm is that the maximal degree occurring in the computation is given as an input of the algorithm. As in Faugère's F_4 algorithm (1999), linear algebra is used to reduce the polynomials. The resulting algorithm is very easy to implement. It is probably somewhat less efficient than the original F_5 on most practical examples, but it lets us compute an upper bound on the complexity of F_5. It is this matrix variant that was used with success by Faugère and Joux (2003).

In order to keep track of the polynomials that lead to the different rows of the matrices encountered during the algorithm, it is convenient to view a matrix (M) as a map $(s,t) \in S \times T \mapsto M_{s,t} \in k$ where S is a finite subset of $\mathbb{N} \times \mathscr{T}$ and T a finite subset of $\mathscr{T}$ ordered using a graded ordering. A row indexed by $s = (i,\tau)$ will be used to represent a polynomial obtained as the sum of τf_i and some other "smaller" polynomials in $\mathscr{I}$; this index s is the *signature* of the corresponding polynomial. A row in the matrix M is specified by its signature s, and we identify the vector $\mathrm{Row}(M,s) = [M_{s,t} \,|\, t \in T]$ and the polynomial $\sum_{t\in T} M_{s,t}t$; the leading term of a row is the leading term of the corresponding polynomial. We fix the following notation: $\mathrm{Rows}(M) = S$ and $\mathrm{LT}(M)$ is the set of leading terms of all the rows of M. A *valid* elementary row operation on M consists in replacing the row $s \in S$ by the linear combination $\mathrm{Row}(M,s) \leftarrow \mathrm{Row}(M,s) + \lambda\,\mathrm{Row}(M,s')$ where $\lambda \in k$, $s' \in S$ and the *additional condition* that $s' = (j',u') < s = (j,u)$ (i.e., $j' < j$ or $(j = j'$ and $u' \prec u)$). The index of the line is unchanged. We denote by $\tilde{\mathscr{M}}_{d,i}$ the result of Gaussian elimination applied to the matrix $\mathscr{M}_{d,i}$ using a sequence of *valid* elementary row operations.

There are two distinct ways of performing a valid Gaussian elimination: either we perform reductions only for the leading term of each row, in which case we call the reduction a *top-reduction*, or we perform more valid reductions so that each column containing a leading coefficient has zeros elsewhere below, in which case we call the reduction a *full-reduction*. The complexity analysis of this paper is done in the top-reduction case, and in Section 4 an experimental comparison with the full-reduction case is given.

The algorithm matrix-F_5 constructs matrices incrementally in the degree and the number of polynomials. Let d be the current degree and i the current number of polynomials (in other words we are computing a Gröbner basis of $\langle f_1,\ldots,f_i\rangle$ truncated in degree d). The algorithm

constructs a matrix $\mathscr{M}_{d,i}$ obtained from the Macaulay matrix $\mathscr{M}_{d,i}$ by removing selected rows. With the previous notation, $\mathscr{M}_{d,i}$ is a map $S \times \mathscr{T}_d \mapsto k$ such that S is a subset of $\{1,\ldots,i\} \times \mathscr{T}$.

Faugère (2002) defines the signature of a polynomial and uses it to give a new criterion to remove useless computations. In the matrix-F_5 algorithm the signatures become the indices of the rows and the original criterion translates as:

Proposition 8 (F_5 criterion)**.** *If t is the leading term of* $\mathrm{Row}(\tilde{\mathscr{M}}_{d-d_i,i-1}, s)$ *where $s < (i,1)$ then the row indexed by (i,t) belongs to the vector space generated by the rows of $\mathscr{M}_{d,i}$ having smaller index.*

Proof. The hypothesis is that $t \in \mathrm{LT}(\langle f_1,\ldots,f_{i-1}\rangle_{d-d_i})$, say $t = \mathrm{LT}(h)$ with $h = \sum_{k=1}^{i-1} h_k f_k$. This implies that $t f_i = \sum_{k=1}^{i-1} f_i h_k f_k + (t-h) f_i$, where the first term belongs to $\langle \mathrm{Row}\, \mathscr{M}_{d,i-1}\rangle$ and the last one is a linear combination of rows of $\mathscr{M}_{d,i}$ having smaller index, as $\mathrm{LT}(t-h) \prec \mathrm{LT}(h)$. □

We now describe the matrix-F_5 algorithm. Here the order is any monomial ordering. It enters the algorithm through the function LT.

Algorithm matrix-F_5

Input: homogeneous polynomials $(f_1,\ldots,f_m)$ with degrees $d_1 \le \cdots \le d_m$;
a maximal degree D.
Output: The elements of degree at most D of the reduced
Gröbner bases of $(f_1,\ldots,f_i)$, for $i = 1,\ldots,m$.

1. **for** i **from** 1 **to** n **do** $G_i := \emptyset$; **end for** // *initialise the Gröbner Bases G_i of $(f_1,\ldots,f_i)$.*
2. **for** d **from** d_1 **to** D **do**
3. $\quad \mathscr{M}_{d,0} := \emptyset$, $\tilde{\mathscr{M}}_{d,0} := \emptyset$
4. $\quad$ **for** i **from** 1 **to** m **do**
5. $\quad\quad$ **if** $d < d_i$ **then** $\mathscr{M}_{d,i} := \mathscr{M}_{d,i-1}$
6. $\quad\quad$ **else if** $d = d_i$ **then**
7. $\quad\quad\quad$ $\mathscr{M}_{d_i,i}$:= add the new row f_i to $\tilde{\mathscr{M}}_{d_i,i-1}$ with index $(i,1)$
8. $\quad\quad$ **else**
9. $\quad\quad\quad$ $\mathscr{M}_{d,i} := \tilde{\mathscr{M}}_{d,i-1}$
10. $\quad\quad\quad$ Crit $:= \mathrm{LT}(\tilde{\mathscr{M}}_{d-d_i,i-1})$
11. $\quad\quad\quad$ **for** f **in** $\mathrm{Rows}(\mathscr{M}_{d-1,i}) \setminus \mathrm{Rows}(\mathscr{M}_{d-1,i-1})$ **do**
12. $\quad\quad\quad\quad$ $(i,u) := \mathrm{index}(f)$, with $u = x_{j_1}\cdots x_{j_{d-d_i-1}}$,
13. $\quad\quad\quad\quad\quad\quad$ and $1 \le j_1 \le \cdots \le j_{d-d_i-1} \le n$
14. $\quad\quad\quad\quad$ **for** j **from** j_{d-d_i-1} **to** n **do**
15. $\quad\quad\quad\quad\quad$ **if** $ux_j \notin$ Crit **then**
16. $\quad\quad\quad\quad\quad\quad$ add the new row $x_j f$ with index (i,ux_j) in $\mathscr{M}_{d,i}$
17. $\quad\quad\quad\quad\quad$ **end if**
18. $\quad\quad\quad\quad$ **end for**
19. $\quad\quad\quad$ **end for**
20. $\quad\quad$ **end if**
21. $\quad\quad$ Compute $\tilde{\mathscr{M}}_{d,i}$ by Gaussian elimination from $\mathscr{M}_{d,i}$
22. $\quad\quad$ Add to G_i all rows of $\tilde{\mathscr{M}}_{d,i}$ not reducible by $\mathrm{LT}(G_i)$
23. $\quad$ **end for**
24. **end for**
25. **return** $[G_i \,|\, i = 1,\ldots,m]$

The **for** loop of line 14 constructs the matrix $\mathscr{M}_{d,i}$ containing all the polynomials $x_1^{\alpha_1}\cdots x_n^{\alpha_n} f_i$ with $\alpha_1+\cdots+\alpha_n = d-d_i$ (except some that reduce trivially to zero). In order to avoid redundant computations, these are constructed from the rows of the previous matrix $\mathscr{M}_{d-1,i}$ by multiplying all rows by all variables. A row indexed by $(i, x_1^{\alpha_1}\cdots x_j^{\alpha_j})$ with $\alpha_j \neq 0$ can arise from several rows in $\mathscr{M}_{d-1,i}$, we choose to construct it from the row indexed by (i,u) in $\mathscr{M}_{d-1,i}$ with $u = x_1^{\alpha_1}\cdots x_j^{\alpha_j-1}$ and multiply it by x_j, the largest variable occurring in u. This insures that every row comes from exactly one row in the previous matrix.

Example 4. *Algorithm matrix-F_5 over Example 1 constructs the following matrices. In degree 2,*

$$\mathscr{M}_{2,3} = \begin{array}{c} \\ f_1 \\ f_2 \\ f_3 \end{array} \begin{array}{c} \begin{array}{cccccccccc} x^2 & xy & y^2 & xz & yz & z^2 & hx & yh & zh & h^2 \end{array} \\ \begin{pmatrix} 1 & & 1 & -2 & -2 & 1 & & & & 1 \\ 1 & 1 & & & 1 & -1 & & & & -2 \\ 1 & & -1 & & 2 & -2 & & & & \end{pmatrix} \end{array},$$

where only nonzero entries are displayed. Gaussian reduction yields

$$\tilde{\mathscr{M}}_{2,3} = \begin{array}{c} \\ f_1 \\ f_2 \\ f_3 \end{array} \begin{array}{c} \begin{array}{cccccccccc} x^2 & xy & y^2 & xz & yz & z^2 & hx & yh & zh & h^2 \end{array} \\ \begin{pmatrix} 1 & & 1 & -2 & -2 & 1 & & & & 1 \\ & 1 & -1 & 2 & 3 & -2 & & & & -3 \\ & & 2 & -2 & -4 & 3 & & & & 1 \end{pmatrix} \end{array}.$$

From $\tilde{\mathscr{M}}_{2,3}$, it follows that the indices and leading terms of the elements in G_3 are

$$\{((1,1),x^2),((2,1),xy),((3,1),y^2)\}.$$

Next, in degree 3, $\tilde{\mathscr{M}}_{3,3}$ contains (in that order) the columns

$$x^3, x^2y, y^2x, y^3, x^2z, zxy, zy^2, xz^2, yz^2, z^3, x^2h, xyh, y^2h, xzh, yzh, z^2h, h^2x, h^2y, h^2z, h^3$$

and the rows with indices and leading terms

(*ind.*)	$(1,h)$	$(1,z)$	$(1,y)$	$(1,x)$	$(2,h)$	$(2,z)$	$(2,y)$	$(2,x)$	$(3,h)$	$(3,z)$	$(3,y)$	$(3,x)$
(LT)	x^2h	x^2z	x^2y	x^3	xyh	xyz	xy^2	$\underline{y^3}$	y^2h	y^2z	$\underline{xz^2}$	$\underline{yz^2}$

The underlined leading terms are those inserted into G_3 by Algorithm matrix-F_5 in line (22)*. Degree 4 is the first time the F_5 criterion is used. The set Crit of line* (10) *is empty for $i=1$ by convention, but it contains x^2 for $i=2$ and x^2, xy for $i=3$. Thus in line* (16)*, all rows (i,m) with $i=1,2,3$ and m a monomial of degree 2 are added to $\mathscr{M}_{4,2}$ and $\mathscr{M}_{4,3}$, except the rows $(2,x^2)$, $(3,xy)$ and $(3,x^2)$. The matrix $\tilde{\mathscr{M}}_{4,3}$ contains $\binom{7}{4} = 35$ columns and $3\binom{5}{2} - 3 = 27$ rows. The rows that are reduced during the Gaussian elimination and that are added to the Gröbner basis are $((3,y^2),z^4)$. No reduction to 0 has occurred and the Gröbner bases are*

$$G_1 = \{((1,1), x^2+y^2-2xz-2yz+z^2+h^2)\},$$

$$G_2 = G_1 \cup \left\{ \begin{array}{ll} ((2,1), & xy-y^2+2xz+3yz-2z^2-3h^2) \\ ((2,x), & 2y^3-7xyz-3y^2z-2xz^2-yz^2+2z^3+3xh^2+4yh^2+2zh^2) \end{array} \right\},$$

$$G_3 = G_2 \cup \left\{ \begin{array}{ll} ((3,1), & 2y^2-2xz-4yz+3z^2+h^2) \\ ((3,y), & 4xz^2+3yz^2-2z^3+3xh^2+3yh^2-11zh^2) \\ ((3,x), & 3yz^2-6z^3+11xh^2-5yh^2-3zh^2) \\ ((3,y^2), & 3z^4+4xzh^2+12yzh^2-7z^2h^2-12h^4) \end{array} \right\}.$$

The main property of this algorithm is given in the following theorem.

Theorem 9. *The algorithm matrix-F_5 computes the elements of degree at most D of the reduced Gröbner bases of $\langle f_1,\ldots,f_i\rangle$, $i=1,\ldots,m$. Moreover if $(f_1,\ldots,f_m)$ is a regular sequence then all the matrices $\mathscr{M}_{d,i}$ have full rank.*

Proof. The proof of the first statement follows the algorithm: it is an induction on d and i. For $d=d_1$ and $i=1$, the result is clear. Assuming the induction hypothesis, we now have to prove that the rows of $\mathscr{M}_{d,i}$ generate $\langle f_1,\ldots,f_i\rangle_d$. Then we can deduce that $\mathrm{LT}(\tilde{\mathscr{M}}_{d,i})$ generates $\mathrm{LT}(\langle f_1,\ldots,f_i\rangle_d)$ and the conclusion on G_i follows.

It is thus sufficient to show that for any $\tau\in\mathscr{T}_{d-d_i}$, the polynomial τf_i is generated by the rows of $\mathscr{M}_{d,i}$. If $d\leq d_i$ the result is clear. Otherwise, let j be the highest index such that $x_j\mid\tau$ and let $u=\tau/x_j$. If u is not the index of a row of $\mathscr{M}_{d-1,i}\setminus\mathscr{M}_{d-1,i-1}$ then by the induction hypothesis uf_i is generated by the rows of $\mathscr{M}_{d-1,i-1}$ and therefore τf_i is generated by the rows of $\mathscr{M}_{d,i-1}$. This justifies the selection of rows in the loop over s. Otherwise, τf_i is entered by the algorithm in $\mathscr{M}_{d,i}$, unless $\tau\in\mathrm{LT}(\tilde{\mathscr{M}}_{d-d_i,i-1})$ since then τ is eliminated by the criterion, thanks to Proposition 8.

The second part of the theorem is proved by contradiction. If a row of $\mathscr{M}_{d,i}$ indexed by (i,u) reduces to 0, this means that the algorithm has constructed an identity

$$g_if_i+\cdots+g_1f_1=0.$$

Moreover, the criterion ensures that $g_i\neq 0$ is reduced with respect to $\langle f_1,\ldots,f_{i-1}\rangle$. This contradicts the regularity of $(f_1,\ldots,f_i)$. □

Other useful properties of the algorithm matrix-F_5 that are needed later are gathered in the following Lemma.

Lemma 10. 1. *Any row entered by the algorithm matrix-F_5 into the matrix $\mathscr{M}_{d,i}$ represents a polynomial*

$$g_if_i+\cdots+g_1f_1,$$

where g_i is reduced with respect to $\langle f_1,\ldots,f_{i-1}\rangle$;

2. *if $g\in G_i\setminus G_{i-1}$, then its index s_g has the form (i,t).*

Proof. The first property comes from the proof of the previous theorem. The second one comes from the fact that the algorithm works incrementally with respect to i. □

2.2. Structure theorem for Grevlex Bases with variables in Simultaneous Noether Position

The estimate in Proposition 1 describes precisely the shape of the final Gröbner basis, but it does not take into account any specificity of the F_5 algorithm. Hence we first study in more detail the structure of grevlex bases computed by F_5, giving the shape of the signatures associated to those polynomials. We further restrict to a special situation, namely when the variables are in *simultaneous Noether position*. The following proposition will play a crucial role when estimating precisely the number of operations of the matrix-F_5 algorithm.

Proposition 11. *[Structure of the F_5-bases] Let $(f_1,\ldots,f_m)$ be a homogeneous system for which the variables $(x_1,\ldots,x_n)$ are in simultaneous Noether position. Let $G_1,\ldots,G_m$ be the result of the matrix-F_5 algorithm applied to this system for the grevlex ordering. Then, for all $((j,t),g)\in G_i$, one has $j\leq i$, $\mathrm{LT}(g)\in\mathscr{T}^j$ and $t\in\mathscr{T}^{j-1}$.*

Proof. That $j \leq i$ is a consequence of the incremental nature of the algorithm. Also, since reductions do not change the index and only involve rows with smaller indices, one has that if $((j,t),g) \in G_i$, then $((j,t),g) \in G_j$. Thus by induction it is sufficient to consider $((i,t),g)$. The result on $\mathrm{LT}(g)$ is given by Proposition 7 using the simultaneous Noether position hypothesis.

The property that $t \in \mathscr{T}^{i-1}$ is more deeply related to the way the algorithm F_5 works. We prove it by induction on i and on the degree of t. For $i = 1$, the only element of the basis is $((1,1),f_1)$; it satisfies the property. Let now $i > 1$ and $t \neq 1$. We decompose t as $t = Xu$, where $X \neq 1$ is of minimal degree such that, for some polynomial h, $((i,u),h) \in G_i$. Let $((i,u_1),g_1),\ldots,((i,u_s),g_s)$ be the elements of G_i distinct from h coming from rows with indices smaller than (i,t) (i.e., $u_j < t$). Following Algorithm F_5, the polynomial g is obtained from Xh by reductions in the matrix by h and the g_j's, and $\mathrm{LT}(Xh) \geq \mathrm{LT}(g)$. From line 22 in Algorithm matrix-F_5 we see that $\mathrm{LT}(Xh) > \mathrm{LT}(g)$, so by definition of h there exists an index k and a monomial μ with

$$\mu\,\mathrm{LT}(g_k) = X\,\mathrm{LT}(h).$$

By the minimality of X, we have that $X \mid \mathrm{LT}(g_k)$. Since $g_k \in G_i$, by Proposition 7 this implies $X \in \mathscr{T}^i$ and then also $\mu \in \mathscr{T}^i$. We prove by contradiction that $x_i \nmid X$. Again by the minimality of X, if $x_i \mid X$, then $x_i \nmid \mu$ and therefore $x_i \mid \mathrm{LT}(g_k)$ and $\mu \in \mathscr{T}^{i-1}$. By induction there exists a monomial $\tau \in \mathscr{T}^{i-1}$ such that g_k has index (i,τ). Now we have that $((i,Xu),g)$ is reduced by a row indexed $(i,\mu\tau)$ but this is a contradiction since $\mu\tau \in \mathscr{T}^{i-1}$ is such that $\mu\tau \succ Xu$ for the order grevlex and this would not be a valid row reduction. □

3. Complexity Analysis of F_5

3.1. Number of Polynomials

The following theorem gives quantitative information on the structure of a reduced Gröbner basis (which is independent of the algorithm used to compute it). To the best of our knowledge, it has not been given before.

Theorem 12. *Let $(f_1,\ldots,f_m)$ be a homogeneous system for which the variables $(x_1,\ldots,x_n)$ are in simultaneous Noether position, with $d_1 = \deg(f_1) \leq \cdots \leq d_m = \deg(f_m)$. Let G_i be a reduced Gröbner basis of $(f_1,\ldots,f_i)$ for the grevlex monomial ordering for $1 \leq i \leq m$. Then the number of polynomials of degree d in G_i whose leading term does not belong to $\mathrm{LT}(G_{i-1})$ is bounded by $b_d^{(i)}$, where*

$$B_i(z) = \sum_{d=0}^{\infty} b_d^{(i)} z^d = z^{d_i} \prod_{k=1}^{i-1} \frac{1-z^{d_k}}{1-z}. \tag{8}$$

For fixed i, let $D_i = (d_1-1)+\cdots+(d_{i-1}-1)$. Then the sequence $h_d = b_{d+d_i}^{(i)}$, $0 \leq d \leq D_i$ is positive, symmetric ($h_{D_i-d} = h_d$), unimodal ($h_0 \leq \cdots \leq h_{\lfloor D_i/2 \rfloor} \geq \cdots \geq h_{D_i}$) and log-concave ($h_d^2 \geq h_{d-1}h_{d+1}$).

Example 5. *In Example 4, the series $B_3(z) = z^2(1+z)^2 = z^2+2z^3+z^4$ gives exactly the number of polynomials of degree 2, 3 and 4 in $G_3 \setminus G_2$.*

Proof. The proof is by induction on i. If $i = 1$ then by definition of the Noether position, the basis is reduced to one polynomial with leading term $x_1^{d_1}$ so that in this case $B_1(z) = z^{d_1}$ as expected.

Assuming the property to hold for $i-1$, we now prove it for i. Consider $g \in G_i$, which can be written

$$g = g_i f_i + \cdots + g_1 f_1, \tag{9}$$

for some polynomials g_i. By Proposition 11, we can restrict our attention to g_i with $\mathrm{LT}(g_i)$ belonging to $k[x_1, \ldots, x_{i-1}]$.

Now if $g \in G_i$ has degree d and does not belong to the Gröbner basis of $\langle f_1, \ldots, f_{i-1} \rangle$, the number of possible leading monomials of g_i in such a decomposition is bounded by the number of monomials of degree $d - d_i$ in $k[x_1, \ldots, x_{i-1}]$ that are not leading terms of a polynomial in $\langle f_1, \ldots, f_{i-1} \rangle$, and this is precisely $\mathrm{HF}_{\theta_{i-1}\langle f_1, \ldots, f_{i-1}\rangle}(d - d_i)$ with θ_{i-1} as in Proposition 7. This is a bound on the dimension of a vector space containing these elements of G_i. It is therefore also a bound on their possible number of leading terms, whence the result.

The properties of h_d come from the fact that these properties are true for each of the coefficient sequences of the polynomials $(1 - z^{d_k})/(1 - z)$ and are preserved by multiplication of these polynomials (see, e.g., Stanley (1989)). □

Note that since the series in Theorem 12 is actually a polynomial of degree

$$\delta = \sum_{j=1}^{i} (d_j - 1) + 1,$$

we deduce that this is also a bound on the highest degree of the elements in a reduced grevlex Gröbner basis, thus recovering (Lejeune-Jalabert, 1984, Ch. 3, Cor. 3.5), and from there the result of Lazard (1983) after a generic linear change of variables.

Corollary 13. *For a system with variables in simultaneous Noether position, a bound on the number of operations in k required to compute a Gröbner basis for the grevlex ordering is obtained by taking* $D = \sum_{j=1}^{m} (d_j - 1) + 1$ *in Proposition 1.*

The next section shows that the F_5 algorithm achieves a smaller complexity.

3.2. Upper Bound for F_5

We now give a proof of Theorem 2 from page 3 using the F_5 criterion. Note that the asymptotic character of this result is only relative to n: we obtain an actual bound for any fixed degree δ.

Proof. The outline of the proof is as follows. First, we exploit the information on the shape of the Gröbner basis from Theorem 12 in order to get a good control over the number of operations. Following the structure of the algorithm we get a bound as a sum over $i = 1, \ldots, m$, corresponding to the rows induced by each input polynomial f_i, of sums over d, corresponding to the columns induced by the monomials of a given degree. Next, we observe that the (bound on the) cost of all steps over i is bounded by that devoted to the last polynomial f_m. The situation with respect to degrees is different: there is an intermediate degree where more work takes place. (In fact, we only prove that there is a degree where our bound dominates the other ones, but this behaviour can be observed in practice.) Then, we compute the asymptotic expansion of both this intermediate degree and the (bound on the) number of rows involved in that degree. The final result is obtained by injecting these expansions into the bounds.

Exact bound from the numbers of rows and columns in the top-reduction case. Arithmetic operations are only performed during the Gaussian reductions. If we perform only top-reductions,

for each $1 \le i \le m$ and $\delta \le d \le D$, by Theorems 9 and 12 there are at most $b_d^{(i)}$ polynomials in $\mathscr{M}_{d,i} \setminus \mathscr{M}_{d,i-1}$ that need to be reduced, and they need to be reduced by $\tilde{\mathscr{M}}_{d,i-1}$. By Proposition 11 the leading term of the result is in $\mathscr{T}_d^i$, which implies that at most $\binom{i+d-1}{d}$ rows are involved in this reduction, each row containing $\binom{n+d-1}{d}$ columns. This gives the following bound on the number of arithmetic operations

$$N_{F_5} = \sum_{i=1}^{m} \sum_{d=\delta}^{D} b_d^{(i)} \binom{i+d-1}{d} \binom{n+d-1}{d}. \tag{10}$$

Bound on the number of polynomials in $\mathscr{M}_{d,i} \setminus \mathscr{M}_{d,i-1}$. For an arbitrary d and i, we have

$$b_d^{(i)} \le \frac{B_i(r)}{r^d}, \qquad \text{for any } r > 0$$

which follows from the positivity of the coefficients of B_i (see (8)). This bound holds for arbitrary $r > 0$; it is minimised by choosing for r a root of the derivative of the right-hand side, which is equivalent (using the logarithmic derivative) to taking r such that

$$d = r \frac{B_i'(r)}{B_i(r)}.$$

As $B_i(r) = r^\delta \left(\frac{1-r^\delta}{1-r}\right)^i$ for equations of identical degree δ, this is equivalent to

$$i = 1 + (d-\delta) \cdot \left(\frac{\delta}{1-r^{-\delta}} - \frac{1}{1-r^{-1}} \right)^{-1}. \tag{11}$$

For $d \ge \delta$, the right-hand side of this equation is a differentiable function of r, its derivative is negative, and it has extreme values $+\infty$ and $\frac{d-1}{\delta-1}$. This is then a positive decreasing function of r. This shows that (11) defines r as a function $r(i,d)$ for $i \ge \frac{d-1}{\delta-1}$ and $\delta \le d$, and this function is a positive, decreasing, differentiable function of i.

The same reasoning on the equation $d = r\frac{B_i'(r)}{B_i(r)}$ shows that $r(i,d)$ is differentiable with respect to d, for $\delta \le d \le \deg B_i$, and that it is positive and increasing.

Bound on the work on the ith polynomial. A bound on the sequence summed in (10) is now obtained by bounding the *differentiable* function of i

$$\frac{B_i(r(i,d))}{r(i,d)^d} \binom{i+d-1}{d} \binom{n+d-1}{d}$$

for $1 \le i \le m$ such that $b_d^{(i)} \ne 0$, i.e., $i \ge \frac{d-1}{\delta-1}$. This is an increasing function of i. Indeed, the last binomial does not depend on i, the previous one is clearly increasing and the logarithmic derivative of the first factor w.r.t. i is

$$\frac{1-r(i,d)^\delta}{1-r(i,d)} = 1 + r(i,d) + \cdots + r(i,d)^{\delta-1} \tag{12}$$

which is positive. Hence, we have the bound

$$N_{F_5} \le m \sum_{d=\delta}^{D} \frac{B_m(r(m,d))}{r(m,d)^d} \binom{m+d-1}{d} \binom{n+d-1}{d}. \tag{13}$$

(Intuitively, the most expensive part of the computation is performed for $i = m$.)

The most expensive degree d. Consider now the summand as a function of d. Its logarithmic derivative in d for fixed r has a simple expression, which vanishes for d root of the equation

$$2\psi(d+m) - 2\psi(d+1) = \log r(m,d), \tag{14}$$

where ψ is the logarithmic derivative of the Γ function (see, e.g., (Abramowitz and Stegun, 1992, Ch. 6)). Thus we now have two equations, (14) and (11) (with $i = m$), relating r, d, m.

As a consequence of the functional equation of the Γ function ($\Gamma(s+1) = s\Gamma(s)$), the left-hand side of (14) can be rewritten using the alternative expression

$$\psi(d+m) - \psi(d+1) = \frac{1}{d+1} + \cdots + \frac{1}{d+m-1}.$$

It follows that Equation (14) defines a unique positive, differentiable function $d(m)$, such that the pair $(d(m), \rho(m))$ with the notation

$$\rho(m) := r(m, d(m)))$$

gives the solution to (11,14) (for $i = m$). Moreover, we have $\rho(m) \geq 1$.

We have now isolated the most expensive step of the algorithm and basically bound all of them by it. The total number of arithmetic operations in k required by algorithm matrix-F_5 is therefore bounded by

$$N_{F_5} \leq m\left(m(\delta-1)+1-(\delta-1)\right)\frac{B_m(\rho(m))}{\rho(m)^{d(m)}}\binom{m+d(m)-1}{d(m)}\binom{m+\ell+d(m)-1}{d(m)}, \tag{15}$$

where we have used the bound on D from Corollary 13 and the hypothesis $n = m + \ell$.

Asymptotic expansions. We now let $m \to \infty$ and obtain the asymptotic behaviour of both ρ and d simultaneously, before injecting into the bound above.

Rewriting (11) yields

$$\frac{d(m)-\delta}{m-1} = \frac{\delta}{1-\rho(m)^{-\delta}} - \frac{1}{1-\rho(m)^{-1}}, \tag{16}$$

from which we define

$$\lambda(m) := \frac{d(m)}{m}.$$

Now, since $\rho(m) \geq 1$, the right-hand side of Equation (16) takes its values between $\frac{\delta-1}{2}$ and $\delta - 1$, which implies that $\lambda(m)$ is bounded as $m \to \infty$.

Thus we can compute the asymptotic behaviour of (14), using the classical expansion

$$\psi(x) = \log(x) - \frac{1}{2x} - \sum_{n=1}^{\infty} \frac{B(2n)}{2n(x^{2n})}, \qquad x \to +\infty \tag{17}$$

where $B(n)$ is the nth Bernoulli number. This gives

$$\rho(m) = \left(1 + \lambda(m)^{-1}\right)^2 + O\left(\frac{1}{m}\right)$$

We can then eliminate $\rho(m)$ from (16) asymptotically:

$$\lambda(m)+O\left(\frac{1}{m}\right)=\frac{\delta}{1-(1+\lambda(m)^{-1})^{-2\delta}}-\frac{1}{1-(1+\lambda(m)^{-1})^{-2}}+O\left(\frac{1}{m}\right)$$

from which we see that as $m\to\infty$, $\lambda(m)$ tends to λ_0 the unique root between $\frac{\delta-1}{2}$ and $\delta-1$ of

$$\lambda_0=\frac{\delta}{1-\left(1+\lambda_0^{-1}\right)^{-2\delta}}-\frac{1}{1-\left(1+\lambda_0^{-1}\right)^{-2}}$$

or equivalently

$$\left(1+\lambda_0^{-1}\right)^{2\delta}=\frac{1}{1-\delta\left(\frac{(\lambda_0+1)^2-{\lambda_0}^2}{(\lambda_0+1)^3-{\lambda_0}^3}\right)}. \tag{18}$$

Now, Equation (14) using (17) gives ρ as a bivariate formal expansion in $1/m$ and $\lambda-\lambda_0$, with

$$\rho=\left(1+\lambda_0^{-1}\right)^2-\frac{2(\lambda_0+1)}{\lambda_0^3}(\lambda-\lambda_0)-\frac{(\lambda_0+1)\,(2\,\lambda_0+1)}{\lambda_0^3}\frac{1}{m}+\sum_{i,j\geq 1}\rho_{i,j}(\lambda_0)\frac{(\lambda-\lambda_0)^i}{m^j}.$$

Injecting into Equation (16) yields a bivariate formal power series $\Phi(1/m,\lambda-\lambda_0)=0$ where

$$\Phi(1/m,\lambda-\lambda_0)=\left(\frac{3\,{\lambda_0}^2+3\,\lambda_0+2}{(\lambda_0+1)\,\lambda_0}-\frac{2\left(3\,{\lambda_0}^2+3\,\lambda_0+1\right)}{\lambda_0\,(\lambda_0+1)\,(2\lambda_0+1)}\delta\right)(\lambda-\lambda_0)+$$
$$\left(\frac{3\,{\lambda_0}^3+5\,{\lambda_0}^2+4\,\lambda_0+1}{\lambda_0\,(\lambda_0+1)}-\frac{\left(2\,{\lambda_0}^2+2\,\lambda_0+1\right)}{\lambda_0\,(\lambda_0+1)}\delta\right)\frac{1}{m}+O\left(\frac{\lambda-\lambda_0}{m}\right)$$

The asymptotic implicit function theorem (see, e.g., Gérard and Jurkat (1992)) implies that the asymptotic expansion of $\lambda-\lambda_0$ is given by the formal power series $S\in\mathbb{C}[[1/m]]$ such that $\Phi(1/m,S(1/m))=0$. This series can be computed to arbitrary order, e.g., by indeterminate coefficients or Newton iteration, and for instance we get

$$\lambda(m)=\lambda_0-\frac{(2\,\lambda_0+1)\left(\left(2\,{\lambda_0}^2+2\,\lambda_0+1\right)\delta-3\,{\lambda_0}^3-5\,{\lambda_0}^2-4\,\lambda_0-1\right)}{\left(6\,{\lambda_0}^2+6\,\lambda_0+2\right)\delta-6\,{\lambda_0}^3-9\,{\lambda_0}^2-7\,\lambda_0-2}\frac{1}{m}+O\left(\frac{1}{m^2}\right),$$
$$\rho(m)=\frac{(\lambda_0+1)^2}{{\lambda_0}^2}-\frac{(\lambda_0+1)^2\,(2\,\lambda_0+1)\,(2\,\delta+1)}{{\lambda_0}^2\left(\left(6\,{\lambda_0}^2+6\,\lambda_0+2\right)\delta-6\,{\lambda_0}^3-9\,{\lambda_0}^2-7\,\lambda_0-2\right)}\frac{1}{m}+O\left(\frac{1}{m^2}\right).$$

Final bound. We now inject these estimates into (15) and obtain the final result:

$$N_{F_5}\leq A\,m\left(\frac{\left(\frac{\lambda_0+1}{\lambda_0}\right)^{2\delta}-1}{\frac{1}{{\lambda_0}^2}-\frac{1}{(\lambda_0+1)^2}}\right)^m\left(1+O\left(\frac{1}{m}\right)\right),$$

where A is a constant depending only on δ, λ_0 and ℓ, whose value is given by

$$A = \frac{1-\delta^{-1}}{2\pi} \cdot \frac{\left(1+\lambda_0^{-1}\right)^3 - 1}{(1+\lambda_0)^{1+\ell}}.$$

Inequalities. The proof of Theorem 2 is concluded by showing that the expression abbreviated $B(\delta)$ in the theorem remains within the interval $[\delta^3, 3\delta^3]$.

The lower bound is obtained by observing that, in view of (18),

$$\begin{aligned} B - \delta^3 &= \frac{\delta\lambda_0^2(\lambda_0+1)^2}{1-\delta+3\lambda_0-2\delta\lambda_0+3\lambda_0^2} - \delta^3 \\ &= \frac{\delta(\delta-\lambda_0)(\delta-1-\lambda_0)(\lambda_0+\delta+2\delta\lambda_0+\lambda_0^2)}{1-\delta+3\lambda_0-2\delta\lambda_0+3\lambda_0^2} \\ &= \frac{\delta(\delta-\lambda_0)(\delta-1-\lambda_0)(\lambda_0+\delta+2\delta\lambda_0+\lambda_0^2)}{((1+\lambda_0)^3-\lambda_0^3)(1+\lambda_0^{-1})^{-2\delta}} \end{aligned}$$

and this is nonnegative since λ_0 is smaller than $\delta - 1$.

The upper bound is obtained in two steps: first $B(\delta)/\delta^3$ is shown to be increasing with δ and next its limit as $\delta \to \infty$ is computed. Equation (18) shows that λ_0 is a differentiable function of δ and thus so is B. An expression for $\lambda_0'(\delta)$ is obtained by differentiating (18). Injecting this expression into the derivative of B and simplifying gives the logarithmic derivative of $B(\delta)/\delta^3$:

$$\frac{B'(\delta)}{B(\delta)} - \frac{3}{\delta} = \frac{(3\lambda_0^2+3\lambda_0+1)\ln((1+\lambda_0^{-1})^2) - 3(2\lambda_0+1)}{(2\lambda_0+1)\,\delta}.$$

The numerator depends on λ_0 only. Its positivity is obtained by using the lower bound $\ln(1+x) \geq x - x^2/2 + x^3/3 - x^4/4$ for $x \in (0,1)$, leading to a polynomial that is positive as soon as $\lambda_0 > 1.4$. Since $\lambda_0 \geq (\delta-1)/2$, the monotonicity of $B(\delta)/\delta^3$ is then established by checking the values for the cases $\delta = 2,3,4$ and indeed, we obtain the approximations 2.45, 2.66, 2.73 that conclude this part.

The limit of $B(\delta)/\delta^3$ is obtained in a way similar to the asymptotic expansions above. We first consider the asymptotic behaviour of λ_0 as $\delta \to \infty$. Setting $\lambda_0 = c\delta$ and taking the asymptotic expansion of (18) yields

$$e^{2/c} + O(1/\delta) = \frac{3c}{3c-2} + O(1/\delta).$$

The limiting value of c is therefore the solution of the equation given by the leading term. It can be expressed in terms of the Lambert W function as

$$\lim_{\delta\to\infty} \frac{\lambda_0}{\delta} = \frac{2}{3+W(-3e^{-3})} \simeq 0.708858.$$

In terms of this value of the limit of c, a direct computation gives

$$\lim_{\delta\to\infty} \frac{B(\delta)}{\delta^3} = \frac{-4}{W(-3e^{-3})(3+W(-3e^{-3}))^2} \simeq 2.81405669.$$

This concludes the proof that $B(\delta) \leq 3\delta^3$, with a more precise estimate in place of the factor 3. □

Note that full asymptotic expansions of all the parameters can be derived along the same lines.

4. Practical results

In order to estimate the accuracy or the lack of preciseness of our complexity result, we performed actual Gröbner bases computations for quadratic and cubic systems of n equations in n unknowns, in simultaneous Noether position, with dense coefficients. These results have been obtained on a PC (laptop) with 4 GB of RAM. The F_5 algorithm has been implemented in the C language within the FGb software (Faugère, 2010) and we used this implementation to compute the Gröbner basis and to count the exact number of arithmetic operations (multiplications of integers modulo $p = 65521$). These results show that the estimate of the number of polynomials in the Gröbner basis (Eq. (8), Theorem 12) and the asymptotic bound of N_{F_5} (Eq. (3), Theorem 2) are very precise, but that the quantity N_{F_5} (Equation (10)) could be sharpened. This will be done in a future work.

Accuracy of the asymptotic estimate of N_{F_5}. We plot in Figure 2 the values of N_{F_5} computed from Eq. (10) and its asymptotic estimate given in Theorem 2, Eq. (3). This shows that the asymptotic bound for N_{F_5} is accurate.

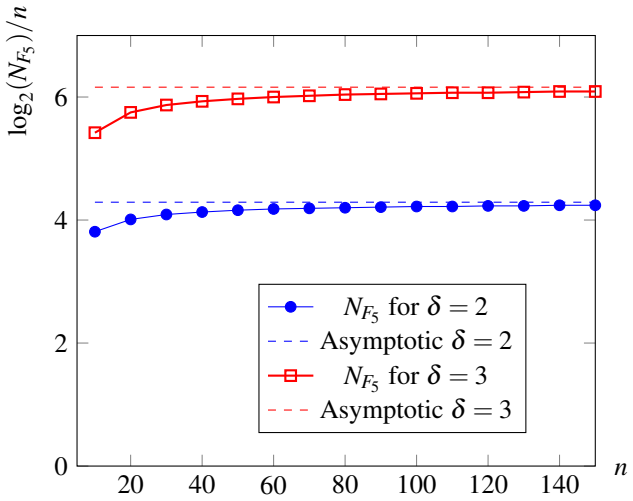

Figure 2: Comparison of N_{F_5} with its asymptotic estimate

Estimation of $b_d^{(i)}$ in Theorem 12, Equation (8). We compare the bound $b_d^{(i)}$, the number of polynomials computed by the matrix F_5 algorithm, and the number of polynomials in the reduced Gröbner basis. It has been shown that F_5 computes "redundant" polynomials that do not belong to the reduced Gröbner basis (see, e.g., Eder et al. (2011)). Moreover, F_5 sometimes reduces less than $b_d^{(i)}$ polynomials. But experimentally, this difference is small. When all the equations have the same degree $d_i = \delta$, the total number of polynomials in our estimation (8) becomes:

$$\text{Polys}_{F_5} = \sum_{i=1}^{m} \sum_{d=\delta}^{D} b_d^{(i)} = \sum_{i=1}^{m} \delta^{i-1} = \frac{\delta^m - 1}{\delta - 1}.$$

Figure 3 shows that this bound is very close to the actual number of polynomials computed by the matrix F_5 algorithm.

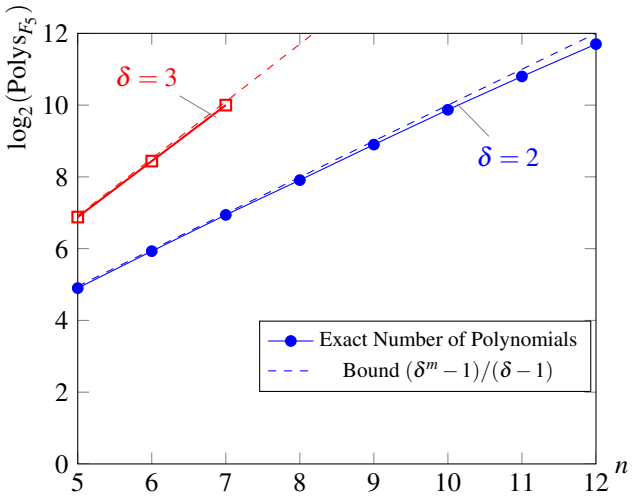

Figure 3: Comparison of the exact/approximated number of polynomials computed by F_5

Estimation of N_{F_5} in Equation (10). In Tables 2 and 3 we report for each n the quantities top F_5 and N_{F_5}, where top F_5 is the experimental number of multiplications for the matrix version of F_5 using only top reductions as described in Section 2.1, and N_{F_5} is given by formula (10). These values are represented graphically on Figures 4 page 22 and 5 page 23.

n	top F_5	full F_5	N_{F_5}
7	$2^{19.83} = 2^{2.83n}$	$2^{20.78} = 2^{2.97n}$	$2^{25.6} = 2^{3.65n}$
8	$2^{22.95} = 2^{2.87n}$	$2^{23.14} = 2^{2.89n}$	$2^{29.7} = 2^{3.72n}$
9	$2^{26.19} = 2^{2.91n}$	$2^{25.39} = 2^{2.82n}$	$2^{33.9} = 2^{3.77n}$
10	$2^{29.38} = 2^{2.94n}$	$2^{27.94} = 2^{2.79n}$	$2^{38.1} = 2^{3.81n}$
11	$2^{32.65} = 2^{2.97n}$	$2^{30.46} = 2^{2.77n}$	$2^{42.3} = 2^{3.84n}$
12	$2^{35.90} = 2^{2.99n}$	$2^{33.20} = 2^{2.77n}$	$2^{46.4} = 2^{3.87n}$
13		$2^{35.86} = 2^{2.76n}$	$2^{50.7} = 2^{3.9n}$
14		$2^{38.70} = 2^{2.76n}$	$2^{54.9} = 2^{3.92n}$
15		$2^{41.52} = 2^{2.79n}$	$2^{59.1} = 2^{3.94n}$
16		$2^{44.43} = 2^{2.78n}$	$2^{63.3} = 2^{3.96n}$

Table 2: Quadratic equations ($\delta = 2$)

This time, we observe a significant gap between the exact values and our bound. Remember that the bound in Equation (10) is computed assuming that $b_d^{(i)}$ polynomials in $\mathscr{M}_{d,i} \backslash \mathscr{M}_{d,i-1}$ are reduced (which is exact for dense polynomials); that they are reduced by $|\mathscr{T}_d^i|$ rows, and that each of these rows has $|\mathscr{T}_d^n|$ non-zero coefficients. But in practice each of the $b_d^{(i)}$ rows needs not be reduced by all of the $|\mathscr{T}_d^i|$ rows, and some of the $|\mathscr{T}_d^n|$ entries in each row are zero. For instance, a row with index $(4, x_3)$ contains no monomial depending only on x_1, x_2, and hence needs not be reduced by the $|\mathscr{T}_3^2|$ rows whose leading term depend only on x_1 and x_2. Another reason is that each row in degree d comes from a row in degree $d-1$, and has as many non-zero

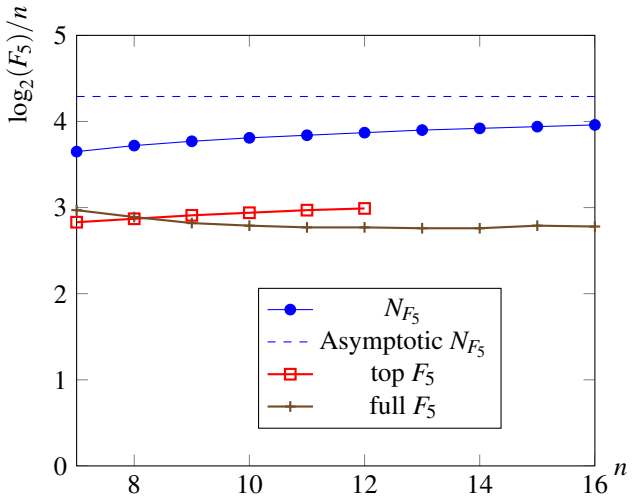

Figure 4: Experiments with $\delta = 2$

n	top F_5	full F_5	N_{F_5}
5	$2^{20.06} = 2^{4.01n}$	$2^{22.01} = 2^{4.40n}$	$2^{24.2} = 2^{4.84n}$
6	$2^{24.93} = 2^{4.16}$	$2^{25.85} = 2^{4.31n}$	$2^{30.1} = 2^{5.02n}$
7	$2^{29.87} = 2^{4.27}$	$2^{29.78} = 2^{4.25n}$	$2^{36.1} = 2^{5.16n}$
8	$2^{34.86} = 2^{4.36}$	$2^{33.98} = 2^{4.25n}$	$2^{42.1} = 2^{5.26n}$
9	$2^{39.88} = 2^{4.43n}$	$2^{38.39} = 2^{4.27n}$	$2^{48.15} = 2^{5.35n}$
10		$2^{41.91} = 2^{4.29n}$	$2^{54.19} = 2^{5.42n}$

Table 3: Cubic equations ($\delta = 3$)

coefficients (before reduction) as the row in degree $d-1$. Hence the matrices $\mathscr{M}_{d,i}$ are sparse matrices. This phenomenon is amplified when the degree d and the number of variables n grow, and explains the gap between our bound and the experiments. We did not find a way to capture this phenomenon in our bound yet, also because we compute a worst-case bound that has to capture all the non-generic behaviors.

Top reduction vs full reduction. Tables 2 and 3 also contain the quantity full F_5, which is the exact number of multiplications for Algorithm F_5' as described in the original article (Faugère, 2002); this algorithm is a matrix version of F_5 where a full reduction is used over the rows, instead of only a top reduction: for each row, reductions are performed not only for the leading term, but also for all the remaining coefficients. Experimental results show that this strategy becomes quickly efficient as n grows, which is due to the fact, observed empirically, that the rows in the matrices are sparser with this algorithm than with top reduction only.

Acknowledgement

This work was partly supported by the HPAC grant of the French National Research Agency (HPAC ANR-11-BS02-013).

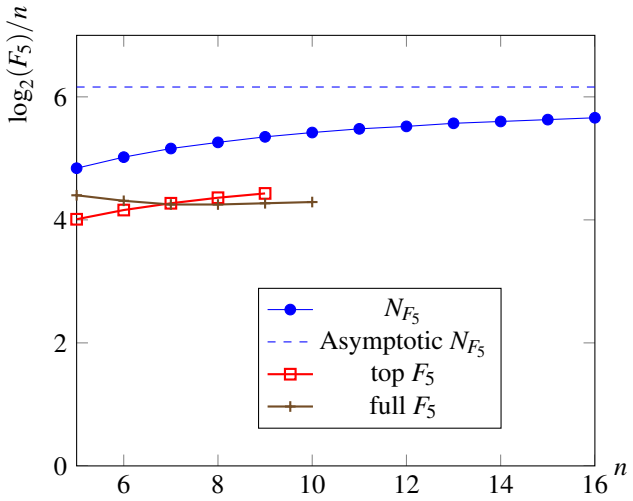

Figure 5: Experiments with $\delta = 3$

We thank the anonymous referees for their careful reading and helpful comments.

References

Abramowitz, M., Stegun, I. A. (Eds.), 1992. Handbook of mathematical functions with formulas, graphs, and mathematical tables. Dover Publications Inc., New York, reprint of the 1972 edition.

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

Buchberger, B., 1965. Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Phd thesis, University of Innsbruck, Austria.

Coppersmith, D., Winograd, S., Mar. 1990. Matrix multiplication via arithmetic progressions. Journal of Symbolic Computation 9 (3), 251–280.

Cox, D., Little, J., O'Shea, D., 1997. Ideals, Varieties, and Algorithms, 2nd Edition. Springer-Verlag, New York.

Cox, D. A., Little, J., O'Shea, D., 2005. Using Algebraic Geometry. Vol. 185 of Graduate Texts in Mathematics. Springer.

Dubé, T. W., Aug. 1990. The structure of polynomials ideals and Gröbner bases. SIAM J. Comput. 19 (4), 750–773.

Eder, C., Faugère, J.-C., Apr. 2014. A survey on signature-based Gröbner basis computations.
URL `http://hal.inria.fr/hal-00974810`

Eder, C., Gash, J., Perry, J., July 2011. Modifying Faugère's F5 algorithm to ensure termination. ACM Commun. Comput. Algebra 45, 70–89.

Faugère, J.-C., 1999. A new efficient algorithm for computing Gröbner bases (F_4). Journal of Pure and Applied Algebra 139 (1-3), 61–88.

Faugère, J.-C., 2002. A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). In: Mora, T. (Ed.), ISSAC 2002. ACM Press, pp. 75–83, proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, July 07–10, 2002, Université de Lille, France.

Faugère, J.-C., September 2010. FGb: A Library for Computing Gröbner Bases. In: Fukuda, K., Hoeven, J., Joswig, M., Takayama, N. (Eds.), Mathematical Software - ICMS 2010. Vol. 6327 of Lecture Notes in Computer Science. Springer Berlin / Heidelberg, Berlin, Heidelberg, pp. 84–87.

Faugère, J. C., Gianni, P., Lazard, D., Mora, T., 1993. Efficient computation of zero-dimensional Gröbner bases by change of ordering. Journal of Symbolic Computation 16 (4), 329–344.

Faugère, J.-C., Joux, A., 2003. Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases. In: Boneh, D. (Ed.), Crypto'2003. No. 2729 in Lecture Notes in Computer Science. Springer-Verlag, pp. 44–60.

Faugère, J.-C., Rahmany, S., 2009. Solving Systems of Polynomial Equations with Symmetries Using SAGBI-Gröbner Bases. In: Kaltofen, E. (Ed.), ISSAC '09: Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation, Seoul Korea, ACM. pp. 151–158.

Gérard, R., Jurkat, W. B., 1992. Asymptotic implicit function theorems. Part I: the preparation theorem and division theorem. Asymptotic Analysis 6, 45–71.

Giusti, M., 1984. Some effectivity problems in polynomial ideal theory. In: Eurosam 84. Vol. 174 of Lecture Notes in Computer Science. Springer, Berlin, pp. 159–171, Cambridge, 1984.

Giusti, M., 1985. A note on the complexity of constructing standard bases. In: Eurocal'85. Vol. 204 of Lecture Notes in Computer Science. Springer-Verlag, pp. 411–412.

Giusti, M., 1988. Combinatorial dimension theory of algebraic varieties. Journal of Symbolic Computation 6 (2-3), 249–265, special issue on Computational Aspects of Commutative Algebra.

Giusti, M., Hägele, K., Lecerf, G., Marchand, J., Salvy, B., Sep. 2000. Computing the dimension of a projective variety: the projective Noether Maple package. Journal of Symbolic Computation 30 (3), 291–307.

Giusti, M., Heintz, J., 1993. La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial. In: Computational Algebraic Geometry and Commutative Algebra (Cortona, 1991). Vol. XXXIV of Sympos. Math. Cambridge Univ. Press, Cambridge, pp. 216–256.

Giusti, M., Lecerf, G., Salvy, B., Mar. 2001. A Gröbner free alternative for polynomial system solving. Journal of Complexity 17 (1), 154–211.

Hashemi, A., Lazard, D., 2011. Sharper complexity bounds for zero-dimensional Gröbner bases and polynomial system solving. International Journal of Algebra and Computation 21 (05), 703–713.

Huỳnh, D. T., 1986. A superexponential lower bound for Gröbner bases and Church-Rosser commutative Thue systems. Information and Control 68 (1-3), 196–206.

Krick, T., Pardo, L. M., 1996. A computational method for Diophantine approximation. In: Algorithms in Algebraic Geometry and Applications (Santander, 1994). Vol. 143 of Progr. Math. Birkhäuser, Basel, pp. 193–253.

Lakshman, Y. N., 1991. A single exponential bound on the complexity of computing Gröbner bases of zero-dimensional ideals. In: Effective Methods in Algebraic Geometry (Castiglioncello, 1990). Vol. 94 of Progr. Math. Birkhäuser Boston, Boston, MA, pp. 227–234.

Lakshman, Y. N., Lazard, D., 1991. On the complexity of zero-dimensional algebraic systems. In: Effective Methods in Algebraic Geometry (Castiglioncello, 1990). Vol. 94 of Progr. Math. Birkhäuser Boston, Boston, MA, pp. 217–225.

Lazard, D., 1983. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In: Computer algebra. Vol. 162 of Lecture Notes in Computer Science. Springer, Berlin, pp. 146–156, proceedings Eurocal'83, London, 1983.

Le Gall, F., 2014. Powers of tensors and fast matrix multiplication. In: ISSAC '14.

Lejeune-Jalabert, M., 1984. Effectivité de calculs polynomiaux. Université de Grenoble I, cours de DEA 84–85.

Macaulay, F. S., 1902. On some formulæ in elimination. Proceedings of the London Mathematical Society 33 (1), 3–27.

Macaulay, F. S., 1916. The algebraic theory of modular systems. Cambridge Mathematical Library. Cambridge University Press, Cambridge, revised reprint edition in 1994.

Mayr, E. W., Meyer, A. R., 1982. The complexity of the word problems for commutative semigroups and polynomial ideals. Advances in Mathematics 46 (3), 305–329.

Möller, H. M., Mora, F., 1984. Upper and lower bounds for the degree of Groebner bases. In: Eurosam 84. Vol. 174 of Lecture Notes in Computer Science. Springer, Berlin, pp. 172–183.

Stanley, R. P., 1989. Log-concave and unimodal sequences in algebra, combinatorics, and geometry. In: Graph theory and its applications: East and West (Jinan, 1986). Vol. 576 of Annals of the New York Academy of Sciences. New York Academy of Sciences, New York, pp. 500–535.

Storjohann, A., 2000. Algorithms for matrix canonical forms. Phd thesis, Department of Computer Science, ETH, Zürich.

Stothers, A., 2010. On the complexity of matrix multiplication. Ph.D. thesis, University of Edinburgh.

Vassilevska Williams, V., 2012. Multiplying matrices faster than Coppersmith-Winograd. In: STOC'12—Proceedings of the 2012 ACM Symposium on Theory of Computing. ACM, New York, pp. 887–898.

von zur Gathen, J., Gerhard, J., 2003. Modern Computer Algebra, 2nd Edition. Cambridge University Press, New York.