On the Complexity of Computing Gröbner Bases for Quasi-Homogeneous Systems

Jean-Charles Faugère[*]
Jean-Charles.Faugere@inria.fr

Mohab Safey El Din[*‡]
Mohab.Safey@lip6.fr

Thibaut Verron[†*]
Thibaut.Verron@ens.fr

[*]INRIA, Paris-Rocquencourt Center, PolSys Project
UPMC, Univ. Paris 06, LIP6
CNRS, UMR 7606, LIP6
Case 169, 4, Place Jussieu, F-75252 Paris

[‡]Institut Universitaire de France

[†]École Normale Supérieure,
45, rue d'Ulm, F-75230, Paris

ABSTRACT

Let $\mathbb{K}$ be a field and $(f_1, \ldots, f_n) \subset \mathbb{K}[X_1, \ldots, X_n]$ be a sequence of quasi-homogeneous polynomials of respective weighted degrees $(d_1, \ldots, d_n)$ w.r.t a system of weights $(w_1, \ldots, w_n)$. Such systems are likely to arise from a lot of applications, including physics or cryptography.

We design strategies for computing Gröbner bases for quasi-homogeneous systems by adapting existing algorithms for homogeneous systems to the quasi-homogeneous case. Overall, under genericity assumptions, we show that for a generic zero-dimensional quasi-homogeneous system, the complexity of the full strategy is polynomial in the weighted Bézout bound $\prod_{i=1}^{n} d_i / \prod_{i=1}^{n} w_i$.

We provide some experimental results based on generic systems as well as systems arising from a cryptography problem. They show that taking advantage of the quasi-homogeneous structure of the systems allow us to solve systems that were out of reach otherwise.

Categories and Subject Descriptors

I.1.2 [**Symbolic and Algebraic Manipulation**]: Algorithms; F.2.2 [**Analysis of Algorithms and Problem Complexity**]: Nonnumerical Algorithms and Problems

Keywords

Gröbner bases; Polynomial system solving; Quasi-homogeneous polynomials

1. INTRODUCTION

Polynomial system solving is a very important problem in computer algebra, with a wide range of applications in theory (algorithmic geometry) or in real life (cryptography). For that purpose, Gröbner bases of polynomial ideals are a valuable tool, and practicable computation of the Gröbner bases of any given ideal is a major challenge of modern computer algebra. Since their introduction in 1965, many algorithms have been designed to compute Gröbner bases ([6, 9, 10, 11]), improving the efficiency of the computations.

Systems arising from "real life" problems often have some structure. It has been observed that most of these structures can make the Gröbner basis easier to compute. For example, it is known that homogeneous systems, or systems with an important maximal homogeneous component, are better solved by using a degree-compatible order, and then applying a change of ordering. In this paper, we study a structure slightly more general than homogeneity, called *quasi-homogeneity*. More precisely, we will say that a polynomial $P(X_1, \ldots, X_n)$ is quasi-homogeneous for the *system of weights* $W = (w_1, \ldots, w_n)$, if the polynomial

$$Q(Y_1, \ldots, Y_n) := P(Y_1^{w_1}, \ldots, Y_n^{w_n})$$

is homogeneous. Systems with such a structure are likely to arise for example from physics, where all measures are associated with a dimension which, to some extent, can be seen as a weight.

Let $F = (f_1, \ldots, f_m)$ be a system of polynomials, in a polynomial algebra graded w.r.t the system of weights $W = (w_1, \ldots, w_n)$. In the following, we will assume that F is quasi-homogeneous and generic, or more generally that its quasi-homogeneous components of maximal weighted degree are generic. It is possible to compute directly a Gröbner basis of the ideal generated by F. This strategy consists of running the classical algorithms F_5 ([10]) and FGLM ([11]) on F, while ignoring the quasi-homogeneous structure. However, to the best of our knowledge, there is no general way of evaluating the complexity of that strategy.

Another approach is to compute the *homogenized* system defined by $\widetilde{F} := (f_i(X_1^{w_1}, \ldots, X_n^{w_n}))$, and then compute a Gröbner basis of that system, using the usual strategies for the homogeneous structure. Experimentally, the first step of the computation is much faster than with the naive strategy. However, the number of solutions is increased by a factor of $\prod_{i=1}^{n} w_i$, slowing down the change of ordering, which thus becomes the main bottleneck of the computation.

Furthermore, to the best of our knowledge, the best complexity bounds for this computation are those we obtain for a homogeneous system of the same degree. However, experimentally, the first step of the computation proves faster for a homogenized quasi-homogeneous system with weighted degree $(d_1, \ldots, d_n)$ than for a homogeneous system of total degree $(d_1, \ldots, d_n)$.

Main results. We provide a complexity study of the above strategy, allowing us to quantify this speed-up, as well as to propose a workaround for the change of ordering. Overall, we prove that the known bounds for this strategy can be divided by $\prod_{i=1}^{n} w_i$ for a generic zero-dimensional W-homogeneous system with weights $W = (w_1, \ldots, w_n)$.

More precisely, we assume the system $(f_1, \ldots, f_m)$ to satisfy the two following generic assumptions:

H1. The sequence $f_1, \ldots, f_m$ is regular;

H2. The sequence $f_1, \ldots, f_i$ is in Noether position w.r.t. $X_1, \ldots, X_i$, for any $1 \le i \le m$.

Under hypothesis **H1**, we adapt the classical results of the homogeneous case, using similar arguments based on Hilbert series, to estimate the degree of the ideal and the degree of regularity of the system:

$$\deg(I) = \prod_{i=1}^{n} \frac{d_i}{w_i} \; ; \quad d_{\mathrm{reg}}(F) \le \sum_{i=1}^{n} \left(d_i - w_i \right) + \max\{w_i\}.$$

We study the complexity of the F_5 algorithm through its matrix variant matrix-F_5. This is a usual approach, carried on for example in [14]. With minor changes, the matrix-F_5 algorithm for homogeneous systems can be adapted to quasi-homogeneous systems. A combinatorial result found in [1] shows that the number of columns of the matrices appearing in that variant of matrix-F_5 is approximately smaller by a factor of $\prod_{i=1}^{n} w_i$, when compared to the regular matrix-F_5 algorithm. Overall, we can obtain complexity bounds which are smaller by a factor of P^ω than the bounds we would obtain for a generic homogeneous system with same degrees, where $P = \prod_{i=1}^{n} w_i$ and ω is the exponent of the complexity of matrix multiplication. In the end, we show that for systems satisfying **H1**, our strategy, running F_5 on the homogenized system, dehomogenizing the result, and then running FGLM, performs in time polynomial in $\prod_{i=1}^{n} d_i / \prod_{i=1}^{n} w_i$, that is polynomial in the number of solutions.

Further assuming hypothesis **H2**, we also carry on the precise complexity analyses done in [2] for homogeneous systems, and adapt them to the quasi-homogeneous case to deduce a precise complexity bound for our quasi-homogeneous variant of Matrix-F_5. These new complexity bounds are also smaller by a factor of P^ω than similar bounds for a generic homogeneous system. Even though these bounds still do not match exactly the experimental complexity, they tend to confirm that overall, we are able to compute a LEX Gröbner basis for a generic quasi-homogeneous system in time reduced by a factor of P^ω, when compared with a generic homogeneous system with same degrees.

We have run benchmarks with the FGb library ([16]) and the Magma computer algebra software ([5]), on both generic systems and real-life systems arising in cryptography. Experimentally, in both cases, our strategy seems always faster than ignoring the quasi-homogeneous structure, and the speed-up increases with the considered weights.

Experiments have also shown that the order of the variables can have an impact on the performances of both strategies. Predicting this behavior seems to require more sophisticated tools and may be material for future research.

Prior works. Making use of the structure of polynomial systems to develop faster algorithms has been a general trend over the past few years: see for example [12], [7] or [15]. Polynomial algebras graded with respect to a system of weights have been studied by researchers in commutative algebra. Most notably, the Hilbert series of ideals defined by regular sequences, which we use several times in this paper, is well known, and could be found for example in [21]. The paper [20] defines many structures of polynomial algebras, including weighted gradings, in preparation for future algorithmic developments. Combinatorial objects arising when we try to estimate the number of monomials of a given W-degree are called *Sylvester denumerants*, and studied for example in [1].

When it comes to Gröbner bases, weighted gradings and related orderings have been described in early works such as [4]. However, as far as we know, the impact of a quasi-homogeneous structure on the complexity of Gröbner bases computations had never been studied.

Among the various computer algebra software able to compute Gröbner bases, it seems that only Magma has algorithms dedicated to quasi-homogeneous systems. Given a quasi-homogeneous system, it will detect the appropriate system of weights, and use the W-GREVLEX ordering to compute an intermediate basis before the change of ordering. However, this strategy is only available for quasi-homogeneous systems, while it can be useful in many other cases, for example systems of polynomials defined as the sum of a quasi-homogeneous component and a scalar.

Other computer algebra software (e.g. Singular) allow the user to compute $\tilde{F}$ and to run the Gröbner basis algorithm on it. Since all these algorithms (most often Buchberger, F_4 or F_5) use S-pairs, they will show a similar speed-up. However, the user must notice that the computations may benefit from using a quasi-homogeneous structure of the system, and provide the system of weights.

We do not provide a way to know what is the "appropriate" system of weights for a given system, or even to detect systems which would benefit from taking into account the quasi-homogeneous structure. However, some systems obviously belong to that category (e.g quasi-homogeneous plus scalar), and the system of weights will then be easy to compute.

Structure of the paper. In section 2 we define more precisely quasi-homogeneous systems, and we compute their degree and degree of regularity assuming the above hypotheses. We also take this opportunity to show briefly that these hypotheses are generic. In section 3 we prove that the strategy consisting of modifying the system is correct, we explain how we can adapt matrix-F_5 and FGLM to quasi-homogeneous systems, and then we evaluate the complexity of these algorithms. In section 4, we briefly explain how these results for quasi-homogeneous systems still help in case the system was obtained from a quasi-homogeneous system by specializing one of the variables to 1. We also give an example of such a structure, as well as the associated algorithm. Finally, in section 5, we give some experimental results.

2. QUASI-HOMOGENEOUS SYSTEMS
2.1 Weighted degrees and polynomials

Let $\mathbb{K}$ be a field. We consider the algebra $A := \mathbb{K}[X_1, \ldots, X_n] = \mathbb{K}[\mathbf{X}]$. Even though one usually uses the total degree to grade the algebra A, there are other ways to define such a grading, as seen in [4], for example.

Definition 1. Let $W = (w_1, \ldots, w_n)$ be a vector of positive integers. Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ be a tuple of nonnegative integers. Let the integer $\deg_W(\mathbf{X}^\alpha) = \sum_{i=1}^{n} w_i \alpha_i$ be the *W-degree*, or *weighted degree* of the monomial $\mathbf{X}^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$. Call the vector W a *system of weights*. We denote by $\mathbf{1}$ the system of weights defined by $(1, \ldots, 1)$, associated with the usual grading on A.

One can prove that any grading on $\mathbb{K}[\mathbf{X}]$ comes from such a system of weights ([4, sec. 10.2]). We denote by $(\mathbb{K}[\mathbf{X}], W)$ the W-graded structure on A, and in that case, to clear ambiguities, we use the adjective *W-homogeneous* for elements or ideals, or *quasi-homogeneous* or *weighted homogeneous* if W is clear in the context. The word *homogeneous* will be reserved for $\mathbf{1}$-homogeneous items.

PROPOSITION 1. *Let* $(\mathbb{K}[X_1, \ldots, X_n], W)$ *be a graded polynomial algebra. Then the application*
$$\hom_W : \begin{array}{ccc} (\mathbb{K}[X_1, \ldots, X_n], W) & \to & (\mathbb{K}[t_1, \ldots, t_n], \mathbf{1}) \\ f & \mapsto & f(t_1^{w_1}, \ldots, t_n^{w_n}) \end{array}$$
is an injective graded morphism, and in particular the image of a quasi-homogeneous polynomial is a homogeneous polynomial.

PROOF. It is an easy consequence of the definition of the grading w.r.t a system of weights. □

The above morphism also provides a quasi-homogeneous variant of the GREVLEX ordering (as found for example in [4]), which we

call the W-GREVLEX *ordering*:

$$u <_{W\text{-grevlex}} v \iff \hom_W(v) <_{\text{grevlex}} \hom_W(v)$$

Given a W-homogeneous system F, one can build the homogeneous system $\hom_W(F)$, and then apply classical algorithms ([10, 11]) to that system to compute a GREVLEX (resp. LEX) Gröbner basis of the ideal generated by $\hom_W(F)$. We will prove in section 3 (prop. 7) that this basis is contained in the image of $\hom_W$, and that its pullback is a W-GREVLEX (resp. LEX) Gröbner basis of the ideal generated by F.

Let us end this paragraph with some notations and definitions. The *degree of regularity* of the system F is the highest degree $d_{\text{reg}}(F)$ reached in a run of F_5 to compute a GREVLEX Gröbner basis of $\hom_W(F)$. The *index of regularity* of an ideal I is the degree i_{reg} of the Hilbert series $\text{HS}_{A/I}$, defined as the difference of the degree of its numerator and the degree of its denominator.

Recall that given a homogeneous ideal I, we define its degree D as the degree of the projective variety $V(I)$, as introduced for example in [18]. This definition still holds for the quasi-homogeneous case. In case the projective variety is empty, that is if the affine variety is equal to $\{0\}$, we extend that definition by letting D be the multiplicity of the 0 point, that is the dimension of the $\mathbb{K}$-vector space A/I. Finally, from now on we will only consider *affine* varieties, even when the ideal is quasi-homogeneous. In particular, the dimension of $V(0)$ is n, and that a zero-dimensional variety will be defined by at least n polynomials.

2.2 Degree and degree of regularity

Zero-dimensional regular sequences. As in the homogeneous case, regular sequences are an important case to study, because it is a generic property which allows us to compute several key parameters and good complexity bounds. We first characterize the degree and bound the degree of regularity of a zero-dimensional ideal defined by a regular sequence.

THEOREM 2. *Let $W = (w_1, \ldots, w_n)$ be a system of weights, and $F = (f_1, \ldots, f_m)$ a regular sequence of W-homogeneous polynomials, of respective W-degrees $d_1, \ldots, d_m$. Further assume that the set of solutions is zero-dimensional, that is $m = n$. We denote by I the quasi-homogeneous ideal generated by F. Then we have $\deg(I) = \prod_{i=1}^{n} \frac{d_i}{w_i}$ and $d_{\text{reg}}(F) \leq \sum_{i=1}^{n}(d_i - w_i) + \max\{w_i\}$.*

PROOF. We will determine the degree and degree of regularity of the system from the Hilbert series (or Poincaré series) of the algebra A/I. A classical result which can be found for example in [21, cor. 3.3] states that, for regular sequences, this series is

$$\text{HS}_{A/I}(t) = \frac{(1-t^{d_1})\cdots(1-t^{d_m})}{(1-t^{w_1})\cdots(1-t^{w_n})}. \tag{1}$$

We assumed $n = m$, so the Hilbert series can be rewritten as

$$\text{HS}_{A/I}(t) = \frac{(1+\cdots+t^{d_1-1})\cdots(1+\cdots+t^{d_n-1})}{(1+\cdots+t^{w_1-1})\ldots(1+\cdots+t^{w_n-1})}.$$

In the 0-dimensional case, recall that the Hilbert series is actually a polynomial, and has degree $i_{\text{reg}} = \sum_{i=1}^{n}(d_i - w_i)$. This means that all monomials of W-degree greater than i_{reg} are in the ideal, and as such, that the leading terms of the W-GREVLEX Gröbner basis of F need to divide all the monomials of W-degree greater than i_{reg}. This proves that all the polynomials in the Gröbner basis computed by F_5 have W-degree at most $i_{\text{reg}} + \max\{w_i\}$. And since the F_5 criterion ([10]) ensures that there is no reduction to zero in a run of F_5 on a regular sequence, the algorithm indeed stops in degree at most $i_{\text{reg}} + \max\{w_i\}$.

Furthermore, the degree of the ideal I is equal to the dimension of the vector space A/I, that is the value of the Hilbert series at $t = 1$, that is $\prod_{i=1}^{n} \frac{d_i}{w_i}$. $\square$

Note that except for this inequality, not much is known about the degree of regularity of a quasi-homogeneous system. In particular, the above bound is nothing more than a bound, even in the generic case. Let us introduce some examples of the three cases one can observe with a quasi-homogeneous generic system:

1. $W = (3, 2, 1)$, generic system of W-degree $\mathbf{D} = (6, 6, 6)$: then $d_{\text{reg}} = i_{\text{reg}} + 1 = 13$;
2. $W = (1, 2, 3)$, generic system of W-degree $\mathbf{D} = (6, 6, 6)$: then $d_{\text{reg}} = 15 > i_{\text{reg}} + 1 = 13$;
3. $W = (2, 3)$, generic system of W-degree $\mathbf{D} = (6, 6)$: then $d_{\text{reg}} = 6 < i_{\text{reg}} = 7$.

Only the case 1 is observed with generic homogeneous systems. Furthermore, examples 1 and 2 show that the degree of regularity depends upon the order of the variables (chosen in the description of the system of weights). As the Hilbert series of a generic sequence doesn't depend on that order, it shows that we probably need to find a better tool in order to evaluate more precisely the degree of regularity in the quasi-homogeneous case. However, the above bound already leads to good improvements on the complexity bounds, as we will see in the following sections. Also note that these computations only hold when the system is 0-dimensional, we will discuss that restriction in section 2.3.

Genericity. We now prove that zero-dimensional W-homogeneous sequences of given W-degree are generically regular, under some assumptions on the W-degree. Let us start with the first part of this statement:

LEMMA 3. *Let n be a positive integer, and consider the algebra $A := \mathbb{K}[X_1, \ldots, X_n]$, graded with respect to the system of weights $W = (w_1, \ldots, w_n)$. Regular sequences of length n form a Zariski-open subset of all sequences of quasi-homogeneous polynomials of given W-degree in A.*

PROOF. Let $(d_1, \ldots, d_m)$ be a family of W-degrees, we consider the set $V(\mathbb{K}[\mathbf{a}][\mathbf{X}])$ of all systems of quasi-homogeneous polynomials of W-degree $d_1, \ldots, d_m$, where $\mathbf{a}$ is a set of variables representing the coefficients of the polynomials. We denote by $f_1, \ldots, f_m$ the polynomials of the generic system, and by I the ideal they generate, in $\mathbb{K}[\mathbf{a}][\mathbf{X}]$.

Since the Hilbert series (1) characterizes regular sequences ([21, cor. 3.2]), the sequence (f_i) is regular if and only if the ideal I contains all monomials of W-degree between $i_{\text{reg}}(I) + 1$ and $i_{\text{reg}}(I) + \max\{w_i\}$, where $i_{\text{reg}}(I)$ is given by $\sum(d_i - w_i)$. This expresses that a given set of linear equations has solutions, and so it can be coded as some determinants being non-zero. $\square$

There are some systems of W-degree for which there is no regular sequence. The reason is that because of the weights, for some systems of W-degrees, there exists no or very few monomials. For example, take $n = 2$, $W = (1, 2)$ and $\mathbf{D} = (1, 1)$. All quasi-homogeneous polynomials of W-degree 1 are in $\mathbb{K}X$, so there is no regular sequence of quasi-homogeneous polynomials with these W-degrees.

However, if we only consider "reasonable" systems of W-degrees, that is systems of W-degrees for which there exists a regular sequence, regular sequences form a Zariski-dense subset from the above.

Remark 1. A sufficient condition for example is to take weighted degrees such that d_1 is divisible by w_1, ..., d_n is divisible by w_n. Thus we can define the sequence $X_1^{d_1/w_1}, \ldots, X_n^{d_n/w_n}$, which is regular, and so for such systems of weight, the regularity condition is generic.

We only proved the genericity for quasi-homogeneous sequences of length n, the more general case of a sequence of length $m \leq n$ will be proved in section 2.3 (remark 2).

2.3 Noether position

To compute the degree and degree of regularity of quasi-homogeneous systems of positive dimension, we will assume that the system $F = (f_1, \ldots, f_m)$ we consider is in *Noether position* (as seen in [8, ch. 13, sec. 1] or [3, def. 2]), i.e. the ideal $I = \langle F \rangle$ satisfies the two following conditions:

- for $i \leq m$, the canonical image of X_i in $\mathbb{K}[\mathbf{X}]/I$ is an algebraic integer over $\mathbb{K}[X_{m+1}, \ldots, X_n]$;
- $\mathbb{K}[X_{m+1}, \ldots, X_n] \cap I = 0$.

LEMMA 4. *Let $F = f_1, \ldots, f_m$ be a regular quasi-homogeneous sequence of polynomials in $\mathbb{K}[X_1, \ldots, X_n]$. The sequence F is in Noether position if and only if $F_{\mathrm{ext}} := f_1, \ldots, f_m, X_{m+1}, \ldots, X_n$ is a regular sequence.*

PROOF. Let I be the ideal generated by the f_i's. The geometric characterization of Noether position (see e.g. [19]) shows that the canonical projection onto the m first coordinates

$$\pi : V(I) \to V(\langle X_1, \ldots, X_m \rangle)$$

is a surjective morphism with finite fibers. This implies that the variety $V(\langle F_{\mathrm{ext}} \rangle)$, that is $\pi^{-1}(0)$, is zero-dimensional, and so the sequence is regular.

Conversely, assume F_{ext} is a regular sequence. Let $i \leq m$, we want to show that X_i is integral over the ring $\mathbb{K}[X_{m+1}, \ldots, X_n]$. Since F_{ext} defines a zero-dimensional ideal, there exists $n_i \in \mathbb{N}$ such that $X_i^{n_i} = \mathrm{LT}(f)$ with $f \in \langle F_{\mathrm{ext}} \rangle$ for the GREVLEX ordering with $X_1 > \cdots > X_n$. By definition of the GREVLEX ordering, we can assume that f simply belongs to I. This shows that every X_i is integral over $\mathbb{K}[X_{i+1}, \ldots, X_n]/I$. We get the requested result by induction on i : first, this is clear if $i = m$. Now assume that we know that $\mathbb{K}[X_i, \ldots, X_n]/I$ is an integral extension of $\mathbb{K}[X_{m+1}, \ldots, X_n]$. From the above, we also know that X_{i-1} is integral over $\mathbb{K}[X_i, \ldots, X_n]$, and so, since the composition of integral homomorphisms is integral, we get the requested result.

Finally, we want to check the second part of the definition of Noether position. Assume that there is a non-zero polynomial in $\mathbb{K}[X_{m+1}, \ldots, X_n] \cap I$, since the ideal is quasi-homogeneous, we can assume this polynomial to be quasi-homogeneous. Either this polynomial is of degree 0, or it is a non-trivial syzygy between $X_{m+1}, \ldots, X_n$. So in any case, it contradicts the regularity hypothesis. $\square$

As we did for regular sequences, we first show how we can evaluate the degree and degree of regularity of a sequence in Noether position, and then we show that the Noether position property is generic under some assumptions on the W-degree of the polynomials.

THEOREM 5. *Let $W = (w_1, \ldots, w_n)$ be a system of weights, and $f_1, \ldots, f_m$ a regular sequence in Noether position, of quasi-homogeneous polynomials of W-degrees $(d_1, \ldots, d_m)$. The same way we did above, we denote by I the ideal generated by the f_i's. Then we have $\deg(I) = \prod_{i=1}^m \frac{d_i}{w_i}$ and $d_{\mathrm{reg}}(I) \leq \sum_{i=1}^m (d_i - w_i) + \max\{w_i\}$.*

PROOF. Let us denote by I' the ideal generated by F_{ext}. The degree of the ideal I' is the same as that of I, because the variety it defines is the intersection of $V(I)$ with some non-zero-divisor hyperplanes. Furthermore, all critical pairs appearing in a run of F_5 on F will also appear in a run of F_5 on F_{ext}, ensuring that $d_{\mathrm{reg}}(F) \leq d_{\mathrm{reg}}(F_{\mathrm{ext}})$.

But since by Noether position, the family F_{ext} defines a zero-dimensional variety, we can use the previous computations to deduce its degree of regularity and the degree of I'. $\square$

LEMMA 6. *Let n be a positive integer, and consider the algebra $A := \mathbb{K}[X_1, \ldots, X_n]$, graded with respect to the system of weights $W = (w_1, \ldots, w_n)$. Systems in Noether position form a Zariski-open subset of all systems of quasi-homogeneous polynomials of given W-degrees in A.*

PROOF. Let $F = (f_1, \ldots, f_m)$ be m generic quasi-homogeneous polynomials, with coefficients in $\mathbb{K}[\mathbf{a}]$. We use the same characterization of a zero-dimensional regular sequence as we did in the proof of Lemma 3. It allows us to express the regularity condition for the sequence $(f_1, \ldots, f_m, X_{m+1}, \ldots, X_n)$ as some determinants being non-zero, which by definition, shows that the condition of being in Noether position is an open condition. $\square$

Since a sequence in Noether position is in particular a regular sequence, we are confronted with the same problem as for the genericity of regular sequences, that is the possible emptiness of the condition. However, it is still true that for "reasonable" systems of W-degrees, i.e. systems of W-degrees for which there exists enough monomials, sequences in Noether position do exist, and thus form a Zariski-dense subset of all sequences. For example, since the sequence $X_1^{d_1/w_1}, \ldots, X_m^{d_m/w_m}$ is in Noether position, the sufficient condition given in Remark 1 is also sufficient to ensure that sequences in Noether position are Zariski-dense.

Remark 2. Any sequence in Noether position is in particular a regular sequence, so Lemma 6 proves that, under the same assumption on the degree, regular sequences of length $m \leq n$ are generic among quasi-homogeneous sequences of given W-degree.

3. COMPUTING GRÖBNER BASES
3.1 Using the standard algorithms on the homogenized system

As we said before, in order to apply the F_5 algorithm to a quasi-homogeneous system, we may run it through $\hom_W$. This is shown by the following proposition.

PROPOSITION 7. *Let $F = (f_1, \ldots, f_m)$ be a family of polynomials in $\mathbb{K}[X_1, \ldots, X_n]$, assumed to be quasi-homogeneous for a system of weights $W = (w_1, \ldots, w_n)$. Let $<_1$ be a monomial order, G the reduced Gröbner basis of $\hom_W(F)$ for this order, and $<_2$ the pullback of $<_1$ through $\hom_W$. Then*

1. *all elements of G are in the image of $\hom_W$;*
2. *the family $G' := \hom_W^{-1}(G)$ is a reduced Gröbner basis of the system F for the order $<_2$.*

PROOF. The morphism $\hom_W$ preserves S-polynomials, in the sense that $\mathrm{S\text{-}Pol}(\hom_W(f), \hom_W(g)) = \hom_W(\mathrm{S\text{-}Pol}(f, g))$. Recall that we can compute a reduced Gröbner basis by running the Buchberger algorithm, which involves only multiplications, additions, tests of divisibility and computation of S-polynomials. Since all these operations are compatible with $\hom_W$, if we run the Buchberger algorithm on both F and $\hom_W(F)$ simultaneously, they will follow exactly the same computations up to application of $\hom_W$. The consequences on the final reduced Gröbner basis follow. $\square$

In practice, if we want to compute a LEX Gröbner basis of F, we generate the system $\widetilde{F} = \hom_W(F)$, we compute a GREVLEX basis $\widetilde{G_1}$ of $\widetilde{F}$ with F_5, and then we compute a LEX Gröbner basis $\widetilde{G_2}$ of $\widetilde{F}$ with FGLM. In the end, we get a LEX Gröbner basis of $\widetilde{F}$, which we turn into a LEX Gröbner basis of F via $\hom_W^{-1}$.

3.2 Direct algorithms

We can now explain why algorithm FGLM becomes a bottleneck with the above strategy. Indeed, we have seen that going through $\hom_W$ increases the Bézout bound of the system by a factor $\prod_{i=1}^n w_i$, and recall that the complexity of the FGLM step is polynomial in that bound.

Here is a workaround. In the above process, we can apply $\hom_W^{-1}$ to the basis $\widetilde{G_1}$ and thus obtain a W-GREVLEX basis G_1 of F. We

can then run FGLM on that basis to obtain a LEX basis of F. Thus, we can avoid the problem of a greater degree of the ideal on the complexity of the FGLM step.

Algorithm F_5 operates by computing S-pairs, and as such, the argument of the proof of proposition 7 can be adapted, showing that going through hom_W is equivalent to running a F_5 algorithm following weighted degree instead of total degree. However, to evaluate the complexity of the F_5 algorithm, we instead study a less-efficient variant called Matrix-F_5 (described for example in [14]), which needs to be adapted to the quasi-homogeneous case. All we need to do is change the algorithm a little, in order to consider directly the variables with their weight. The modified algorithm is algorithm 1 opposite. The function F5CRITERION$(\mu,i,\mathcal{M})$ implements the F_5-criterion described in [10]: it evaluates to false if and only if μ is the leading term of a line of the matrix $\mathcal{M}_{d-d_i,i-1}$. The function ECHELONFORM(M) reduces the matrix M to row-echelon form, not allowing any row swap.

Algorithm 1: Matrix-F_5 (W-homogeneous version)

Input:
$$\begin{cases} f_1,\ldots,f_m \ W\text{-homogeneous polynomials} \\ \qquad \text{with } W\text{-degrees } d_1,\ldots,d_m \\ d_{\max} \in \mathbb{N} \end{cases}$$

Output: G Gröbner basis of $\langle f_1,\ldots,f_m \rangle$ up to W-degree $d_{\max}$

1   $G \leftarrow \{f_1,\ldots,f_m\}$;
2   **for** $d = 1$ **to** $d_{\max}$ **do**
3     $\mathcal{M}_{d,0} \leftarrow$ matrix with 0 lines;
4   **for** $i = 1$ **to** m **do**
5   **if** $d = d_i$ **then**
6         $\mathcal{M}_{d,i} \leftarrow \widetilde{\mathcal{M}_{d,i-1}} \cup$ line f_i with label $(1,f_i)$;
7   **else if** $d > d_i$ **then**
8         $\mathcal{M}_{d,i} \leftarrow \widetilde{\mathcal{M}_{d,i-1}}$;
9   **for** $j = 1$ **to** n **do**
10   **forall the** lines f of $\widetilde{\mathcal{M}_{d-w_j,i}}$ with label (e,f_i) s.t. the biggest variable dividing e is x_j **do**
11   **for** $k = n$ **downto** j **do**
12   **if** F5CRITERION$(x_k e,i,\mathcal{M})$ **then**
13              $\mathcal{M}_{d,i} \leftarrow \mathcal{M}_{d,i} \cup x_k f$ with label $(x_k e,f_i)$;
14     $\widetilde{\mathcal{M}_{d,m}} \leftarrow$ ECHELONFORM$(\mathcal{M}_{d,m})$;
15   For any line having been reduced to a non-zero polynomial, append it to G ;
16   **return** G

3.3 First complexity bounds

Let $F = (f_1,\ldots,f_n)$ be a system of W-homogeneous polynomials in $\mathbb{K}[X_1,\ldots,X_n]$, and let I be the ideal generated by F, D the degree of I, d_{reg} its degree of regularity and i_{reg} its index of regularity. The classical complexity bounds of Matrix-F_5 (for a regular system) and FGLM are

$$C_{F_5} = O\left(d_{\mathrm{reg}} M_{d_{\mathrm{reg}},W}(n)^\omega\right); \ C_{FGLM} = O\left(nD^3\right),$$

where $M_{d,W}(n)$ stands for the number of monomials of W-degree d in n variables (see for example [2] for F_5 and [11] for FGLM).

Assuming the system F is a regular sequence, we have already seen the following estimates:

$$d_{\mathrm{reg}} \leq i_{\mathrm{reg}} + \max\{w_i\} ; \qquad D = \frac{\prod_{i=1}^n d_i}{\prod_{i=1}^n w_i}.$$

If we compare these values with their equivalent with the system of weights $\mathbf{1}$, we notice a significant gain in theoretical complexity bounds for both the FGLM and F_5 algorithms.

But this gain in complexity for F_5 does not take into account the size of the computed matrices. That size is necessarily reduced, because the number of monomials of given W-degree is much smaller than the number of monomials of given $\mathbf{1}$-degree. The point of the following lemma is to evaluate this gain.

LEMMA 8. *Let $W = (w_1,\ldots,w_n)$ be a system of weights, and for any i, let $W_i = (w_1,\ldots,w_i)$. For any integer d, we denote by $M_{d,W}(n)$ the number of monomials of W-degree d, that is the size of the matrix of W-degree d. Let $\delta := \gcd(W)$, $P := \prod_{i=1}^n w_i$, S_i the integer defined recursively as following:*

$$S_1 = 0, \ S_i = S_{i-1} + w_i \cdot \frac{\gcd(W_{i-1})}{\gcd(W_i)} \ for \ i \geq 2$$

and T_i the integer defined recursively as following:

$$T_1 = 0, \ T_i = T_{i-1} + w_i \cdot \left(\frac{\gcd(W_{i-1})}{\gcd(W_i)} - 1\right) - 1 \ for \ i \geq 2.$$

Then the number of monomials of W-degree d is bounded above and below by:

$$\frac{\delta}{P} M_{d-T_n-n+1,\mathbf{1}}(n) \leq M_{d,W}(n) \leq \frac{\delta}{P} M_{d+S_n-n+1,\mathbf{1}}(n).$$

PROOF. This is a consequence of theorems 3.3 and 3.4 in [1], if we recall that $M_{d,\mathbf{1}}(n) = \binom{d+n-1}{d} = \binom{d+n-1}{n-1}$. $\square$

Note that if $W = \mathbf{1}$, the bounds we get are trivial, which means the complexity bounds we will obtain with them will specialize without any difficulty to the known bounds for the homogeneous case.

Using the notation $S = S_n$, we get this new complexity bound for quasi-homogeneous Matrix-F_5:

$$\begin{aligned} C_{F_5} &= O\left(d_{\mathrm{reg}} M_{d_{\mathrm{reg}},W}(n)^\omega\right) \\ &= O\left(\left(i_{\mathrm{reg}} + \max\{w_i\}\right) \right. \\ &\qquad \left. \cdot \left[\frac{\delta}{P}\binom{i_{\mathrm{reg}} + \max\{w_i\} + S - 1}{n-1}\right]^\omega\right). \end{aligned} \quad (2)$$

On the other hand, the estimate on the degree of a quasi-homogeneous variety gives the following complexity bound for FGLM:

$$C_{FGLM} = O\left(n\left[\frac{\widetilde{D}}{P}\right]^3\right),$$

where $\widetilde{D} = \prod_{i=1}^n d_i$ is the degree of the ideal $\langle \mathrm{hom}_W(F)\rangle$. In the end, for the whole process, we can see that the complexity bound for our direct strategy is smaller by a factor of P^ω, when compared to the strategy of going through hom_W.

3.4 Precise analysis of matrix-F_5

Let us now follow more closely the computations occurring in the Matrix-F_5 algorithm, and obtain more accurate complexity bounds. For this purpose, we take on the computations made in [2, ch. 3], without proving them whenever the proof is an exact transcription of the homogeneous case.

Let $W = (w_1,\ldots,w_n)$ be a system of weights, and $f_1,\ldots,f_m$ a system of quasi-homogeneous polynomials in $\mathbb{K}[X_1,\ldots,X_n]$, which we assume satisfies the hypotheses **H1** and **H2**. We denote by $(d_1,\ldots,d_m)$ the respective W-degrees of the polynomials $f_1,\ldots,f_m$, and we will assume them to allow the existence of such systems.

We also denote by:

- $A_i = \mathbb{K}[X_1,\ldots,X_i]$, and $A = A_n$;
- S_i the integer defined in Lemma 8, and $S = S_n$;
- $P_i = \prod_{j=1}^i w_j$, and $P = P_n$;
- $I_i = \langle f_1,\ldots,f_i\rangle$, and $I = I_m$;
- $\widetilde{f}_j = \mathrm{hom}_W(f_j)$;
- $\widetilde{I}_i = \langle \widetilde{f}_1,\ldots,\widetilde{f}_i\rangle$, and $\widetilde{I} = \widetilde{I}_m$;
- $D_i = \deg(I_i) = \prod_{j=1}^i (d_j/w_j)$;

- $\widetilde{D}_i = \deg(\widetilde{I}_i) = \prod_{j=1}^{i} d_j$;
- $d_{\text{reg}}^{(i)}$ the degree of regularity of I_i (or of $\widetilde{I}_i$);
- G_i the W-GREVLEX Gröbner basis of I_i as given by Matrix-F_5.

With these notations, we are going to prove the following theorem:

THEOREM 9. *Let $W = (w_1, \ldots, w_n)$ be a system of weights, and $f_1, \ldots, f_m$ ($m \leq n$) a system of W-homogeneous polynomials satisfying H1 and H2. Then the complexity of quasi-homogeneous Matrix-F_5 algorithm (algorithm 1) is:*

$$C_{F_5} = O\left(\sum_{i=2}^{m} (D_{i-1} - D_{i-2}) M_{d_{\text{reg}}^{(i)}, W}(i) M_{d_{\text{reg}}^{(i)}, W}(n) \right)$$

We aim at computing precisely how many lines are reduced in a run of the Matrix-F_5 algorithm, that is, the number of polynomials in the returned Gröbner basis. This is done by the following proposition, which is a weak variant of [3, th. 10]:

PROPOSITION 10. *Let $(f_1, \ldots, f_m)$ be a W-homogeneous system (w.r.t a system of weights W) satisfying the hypotheses H1 and H2. Let G_i be a reduced Gröbner basis of $(f_1, \ldots, f_i)$ for the W-GREVLEX monomial ordering, for $1 \leq i \leq m$. Then the number of polynomials of W-degree d in G_i whose leading term does not belong to $\text{LT}(G_{i-1})$ is bounded by $b_{d,i}$, defined by the generating series*

$$B_i(z) = \sum_{d=0}^{\infty} b_{d,i} z^d = z^{d_i} \prod_{k=1}^{i-1} \frac{1 - z^{d_k}}{1 - z^{w_k}}.$$

PROOF. The proof of [3, th. 10] still holds in the quasi-homogeneous case, using formula (1) for the Hilbert series of a quasi-homogeneous regular sequence. □

So we can obtain a better bound for the number of elementary operations performed in a Matrix-F_5 run. Indeed, $B_i(1)$ represents the number of reduced polynomials in the computation of a Gröbner basis of $(f_1, \ldots, f_i, X_{i+1}, \ldots, X_n)$, that is as many as in the computation of a Gröbner basis of $(f_1, \ldots, f_i)$: since we only perform reductions under the pivot line, [3, prop. 9] shows that the lines coming from $X_{i+1}, \ldots, X_n$ will not add any reduction. Note that the above generating series is the same as the Hilbert series of $\langle f_1, \ldots, f_{i-1}, X_i, \ldots, X_n \rangle$, and so, that its value at $z = 1$ is the degree of that ideal, or D_{i-1}. Therefore, we know that the number of reduced polynomials with label (m, f_i) will be $D_{i-1} - D_{i-2}$ (with convention that $D_0 = 0$).

Now, let g be any polynomial of W-degree d being reduced in a run of the Matrix-F_5 algorithm on $(f_1, \ldots, f_i)$. From [3, prop. 9], we know that the leading term of g, after reduction, is in A_i. So overall, in W-degree d, we reduce by at most as many lines as there are monomials in A_i, that is $M_{d,W}(i)$. Furthermore, each reduction costs at most $O(M_{d,W}(n))$ elementary algebraic operations, since this is the length of the matrix lines. And we perform these reductions up to degree $d_{\text{reg}}^{(i)}$. Note that, if $i = 1$, there clearly isn't any reduction in the computation, and we obtain the following formulas:

$$C_{F_5} = O\left(\sum_{i=2}^{m} (D_{i-1} - D_{i-2}) M_{d_{\text{reg}}^{(i)}, W}(i) M_{d_{\text{reg}}^{(i)}, W}(n) \right) \quad (3)$$

$$= O\left(\sum_{i=2}^{m} \frac{1}{P_i P_n} \left(\frac{\widetilde{D_{i-1}}}{P_{i-1}} - \frac{\widetilde{D_{i-2}}}{P_{i-2}} \right) \right.$$
$$\left. \cdot M_{d_{\text{reg}}^{(i)} + S_i - i + 1, \mathbf{1}}(i) \cdot M_{d_{\text{reg}}^{(i)} + S_n - n + 1, \mathbf{1}}(n) \right)$$

In comparison, the above reasoning for Matrix-F_5 applied to $\widetilde{F}$ would give

$$C_{F_5} = O\left(\sum_{i=2}^{m} \left(\widetilde{D_{i-1}} - \widetilde{D_{i-2}} \right) M_{\widetilde{d_{\text{reg}}}, \mathbf{1}}(i) M_{\widetilde{d_{\text{reg}}}, \mathbf{1}}(n) \right) \quad (4)$$

so that here again, working with quasi-homogeneous polynomials yields a gain or roughly P^3. Note that the exponent 3 (instead of the previous ω) is not really meaningful, because we assumed here that we were using the naive pivot algorithm to perform the Gauss reduction. However, if we assume $\omega = 3$ in the previous computations as well, we observe that our new bound is generally much better than the previous one: figure 1 shows a plot of data obtained both with algorithm 1 and with Matrix-F_5 through $\hom_W$, together with the different bounds we can compute.

Asymptotically, though, the gain does not look important, since the complexity is still $O(nD^3)$ where D is the degree of the ideal and $n \geq m$ the number of variables, or in $O(nd^{3n})$ where d is the greatest d_i.

Remark 3. One may also push the computations a bit further, and obtain an even more accurate bound, expressed in terms of the $b_{d,i}$ (these calculations are done in [2] for the homogeneous case, and can easily be transposed to the quasi-homogeneous case):

$$C_{F_5} = O\left(\sum_{i=1}^{m-1} \sum_{d=0}^{\infty} \frac{b_{d+d_{i+1}, i+1}}{P_{i+1} P_n} \cdot M_{d+d_{i+1}+S_{i+1}-i, \mathbf{1}}(i+1) \right.$$
$$\left. \cdot M_{d+d_{i+1}+S_n-n+1, \mathbf{1}}(n) \right). \quad (5)$$

As an example, we computed that bound as well for a particular case, and included it in figure 1. As one can see, that bound is indeed better than the intermediate evaluation (3), but the difference is low enough to justify using the latter evaluation. Furthermore, the bound (3) expressed in terms of the D_i's is more useful in practice, since it has a closed formula using only the parameters of the system (n, m, d_i and w_i). That allows us to use it in complexity evaluations, in both theory and practice.

Remark 4. As one can see on figure 1, the number of operations needed by Matrix-F_5 on the homogenized system is not significantly higher than the number of operations needed by the quasi-homogeneous variant of Matrix-F_5. That is mostly true because the unmodified algorithm can make use of some of the structure of the quasi-homogeneous systems (for example, columns of zeroes in the matrices).

4. THE AFFINE CASE

We will now consider the case of input that do not necessarily consist of quasi-homogeneous polynomials. One of the methods to find a GREVLEX Gröbner basis of such a system is to apply F_5, considering at W-degree d the set of monomials having W-degree lower than or equal to d. This is equivalent to homogenizing the system, i.e. to adding a variable $X_1 > \cdots > X_n > H$, and applying the classical F_5 algorithm to this homogeneous system. The reverse transformation is done by evaluating each polynomial at $H = 1$.

However, this process makes it harder to compute the complexity of the F_5 algorithm. The main reason is that dehomogenizing does not necessarily preserve W-degree, and as a consequence, it is no longer true that running the Matrix-F_5 algorithm up to W-degree d provides us with a basis, truncated at W-degree d. What remains true though is that past some W-degree, we may obtain a Gröbner basis for the entire ideal.

Generally, we want to avoid *degree falls* in the run of F_5, that is, reductions where the W-degree of the reductee is less than the W-degrees of the polynomials forming the S-pair. This phenomenon is similar to reductions to zero in the quasi-homogeneous case. It can be ruled out by considering only systems which are *regular in the affine sense* (as found in [2] for gradings in total degree).

Definition 2. Let W be a system of weights, and $(f_1, \ldots, f_n)$ be a system of not-necessarily W-homogeneous polynomials. We denote
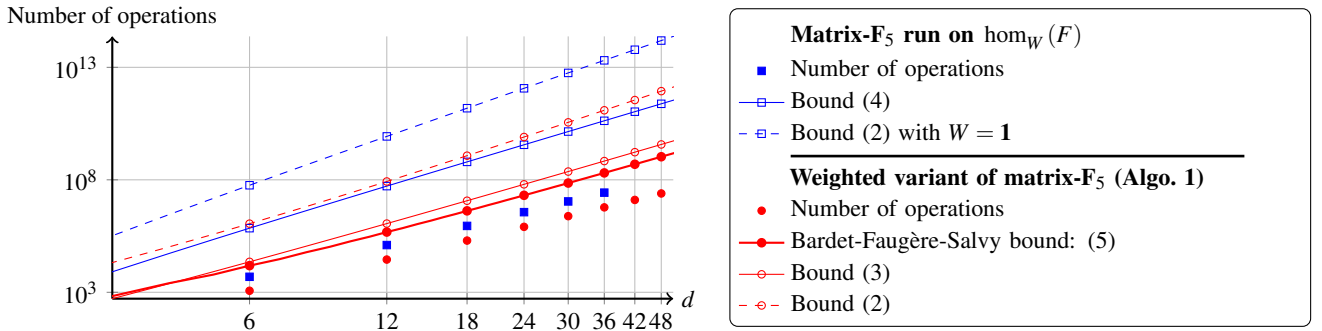
Figure 1: Bounds and values, on a log-log scale, for the number of arithmetic operations performed in Matrix-F_5 for a generic system with $W = (1, 2, 3)$ and $\mathbf{D} = (d, d, d)$

by h_i the quasi-homogeneous component of highest W-degree in f_i, for any $1 \le i \le n$. We say that the sequence (f_i) is *regular in the affine sense* when the sequence (h_i) is regular (in the quasi-homogeneous sense). We define the *degree of regularity* of the ideal $\langle f_i \rangle$ as the degree of regularity of the ideal $\langle h_i \rangle$.

Since a degree fall in a run of F_5 is precisely a reduction to zero in the highest W-degree quasi-homogeneous components of the system, we know that the F_5 criterion rules out all degree falls in a run of F_5 on such a regular system. In turns, it ensures that for such a system, running Matrix-F_5 up to degree d returns a d-Gröbner basis of F.

Hence we can study the complexity of F_5 by looking at a run of Matrix-F_5 on the homogenized system. As an example, we prove the following theorem:

THEOREM 11. *Let $W = (w_1, \dots, w_n)$ be a system of weights, and let $f_1, \dots, f_m$ be a generic system of polynomials of the form $f_i = g_i + \lambda_i$, with g_i W-homogeneous of W-degré d_i and $\lambda_i \in \mathbb{K}$. Let D be the degree of the system, d_{reg} its degree of regularity, and δ the gcd of the d_i's. We can compute a W-GREVLEX Gröbner basis of this system in time*

$$O\left(\frac{d_{\text{reg}}}{\delta^\omega} M_{d,W}(n)^\omega \right),$$

or in other words, we can divide the known complexity of the F_5 process on such a system by δ^ω.

PROOF. The idea is that when we homogenize the system, we can choose any suitable weight for H, not necessarily 1. More precisely, we can set the weight of H to be δ, so that the homogenized polynomials become $f_i^h = g_i + \lambda_i H^{d_i/\delta}$.

Thus, assuming the computations made at section 2.2 still hold, we have the same improvements on the bound on d_{reg} and on the size of matrices as before, and thus we have the wanted result.

Note that even if the initial system is generic, the homogenized system is not. However, one can check that if the initial system was regular in the affine sense, the homogenized system is still regular. Indeed, it's enough to check that no reduction to zero occur in a Matrix-F_5 run, but it is clear, since such a reduction would in particular be a degree fall. Also, the property of being in Noether position for the m first variables is clearly kept upon homogenizing.

As such, generically, our homogenized system is regular and in Noether position, so the previous computations indeed still hold. □

5. EXPERIMENTAL RESULTS

We have run some benchmarks[1], using the FGb library and the Magma algebra software. We present these results in Tables 1a

---

[1] All the systems we used are available online on http://www-polsys.lip6.fr/~jcf/Software/benchsqhomog.html.

and 1b. The examples are chosen with increasing n (number of variables and polynomials), two different classes of systems of weights W and systems of W-degrees D. With these conditions, we built a generic system of polynomials f_i in $\mathbb{F}_{65521}[\mathbf{X}]$, such that all monomials appearing in f_i have W-degree at most d_i. The last examples are systems arising in the study of the Discrete Logarithm Problem, when trying to compute the decompositions of points on an elliptic curve (see [17]). In both cases, we use a shortened notation for the systems of weights and the degrees, where for example $(2^3, 1^2)$ means $(2, 2, 2, 1, 1)$. The magma benchmarks were run on a machine with 128 GB RAM and 3 GHz CPU, running Magma v.2.17-1. The FGb benchmarks were run on a laptop with 16 GB RAM and 3 GHz CPU.

For each system, we compared our strategy ("qh") with the default strategy ("std"), for both steps. The algorithms used by the FGb library are F_5 and an implementation of FGLM taking advantage of the sparsity of the matrices ([13]). The algorithms used by Magma are F_4 and the classical FGLM. The complexity of sparse-FGLM depends on the number of solutions of the system and on the shape of the input basis, while the complexity of classical FGLM depends only on the number of solutions. This explains why we can see a speed-up on the FGLM step in FGb, even though the degree is unchanged.

6. REFERENCES

[1] G. Agnarsson. On the Sylvester denumerants for general restricted partitions. In *Proceedings of the Thirty-third Southeastern International Conference on Combinatorics, Graph Theory and Computing (Boca Raton, FL, 2002)*, volume 154, pages 49–60, 2002.

[2] M. Bardet. *Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie.* Thesis, Université Pierre et Marie Curie - Paris VI, Dec. 2004.

[3] M. Bardet, J.-C. Faugère, and B. Salvy. On the complexity of the F_5 Gröbner basis algorithm. Private communication, 2012.

[4] T. Becker and V. Weispfenning. *Gröbner bases*, volume 141 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1993. A computational approach to commutative algebra, In cooperation with Heinz Kredel.

[5] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

System	deg(I)	t_{F_5} (qh)	t_{F_5} (std)	Speed-up for F_5	t_{FGLM} (qh)	t_{FGLM} (std)	Speed-up for FGLM
Generic $n=7$, $W=(1^4,2^3)$, $\mathbf{D}=(4^7)$	2048	2.7 s	3.4 s	1.2	0.4 s	1.1 s	2.6
Generic $n=8$, $W=(1^4,2^4)$, $\mathbf{D}=(4^8)$	4096	12.3 s	22.5 s	1.8	2.4 s	7.3 s	3.0
Generic $n=9$, $W=(1^5,2^4)$, $\mathbf{D}=(4^9)$	16384	314.9 s	778.5 s	2.5	119.6 s	327.8 s	2.7
Generic $n=7$, $W=(2^5,1^2)$, $\mathbf{D}=(4^7)$	512	0.1 s	0.3 s	3.2	0.1 s	0.1 s	1.7
Generic $n=8$, $W=(2^6,1^2)$, $\mathbf{D}=(4^8)$	1024	0.4 s	1.6 s	4.2	0.2 s	0.3 s	1.9
Generic $n=9$, $W=(2^7,1^2)$, $\mathbf{D}=(4^9)$	2048	1.6 s	8 s	4.9	0.6 s	1.2 s	2.0
Generic $n=10$, $W=(2^8,1^2)$, $\mathbf{D}=(4^{10})$	4096	7.5 s	40.4 s	5.4	2.4 s	6.2 s	2.6
Generic $n=11$, $W=(2^9,1^2)$, $\mathbf{D}=(4^{11})$	8192	33.3 s	213.5 s	6.4	17.5 s	41.2 s	2.4
Generic $n=12$, $W=(2^{10},1^2)$, $\mathbf{D}=(4^{12})$	16384	167.9 s	1135.6 s	6.8	115.8 s	246.7 s	2.1
Generic $n=13$, $W=(2^{11},1^2)$, $\mathbf{D}=(4^{13})$	32768	796.7 s	6700 s	8.4	782.7 s	1645.1 s	2.1
Generic $n=14$, $W=(2^{12},1^2)$, $\mathbf{D}=(4^{14})$	65536	5040.1 s	∞	∞	5602.3 s	NA	NA
DLP Edwards $n=4$, $W=(2^3,1)$, $\mathbf{D}=(8^4)$	512	0.1 s	0.1 s	1	0.1 s	0.1 s	1
DLP Edwards $n=5$, $W=(2^4,1)$, $\mathbf{D}=(16^5)$	65536	935.4 s	6461.2 s	6.9	2164.4 s	6935.6 s	3.2

(a) Benchmarks with FGb

System	deg(I)	t_{F_4} (qh)	t_{F_4} (std)	Speed-up for F_4	t_{FGLM} (qh)	t_{FGLM} (std)	Speed-up for FGLM
Generic $n=7$, $W=(1^4,2^3)$, $\mathbf{D}=(4^7)$	2048	7.9 s	14 s	1.7	214.2 s	222.7 s	1
Generic $n=8$, $W=(1^4,2^4)$, $\mathbf{D}=(4^8)$	4096	62.6 s	138.3 s	2.2	1774.7 s	1797.1 s	1
Generic $n=9$, $W=(1^5,2^4)$, $\mathbf{D}=(4^9)$	16384	3775.5 s	8830.5 s	2.3	∞	∞	NA
Generic $n=7$, $W=(2^5,1^2)$, $\mathbf{D}=(4^7)$	512	0.2 s	0.7 s	3.5	45.5 s	45.6 s	1
Generic $n=8$, $W=(2^6,1^2)$, $\mathbf{D}=(4^8)$	1024	1 s	6.2 s	6.2	512.3 s	515.6 s	1
Generic $n=9$, $W=(2^7,1^2)$, $\mathbf{D}=(4^9)$	2048	6 s	88.1 s	14.7	7965 s	8069.4 s	1
Generic $n=10$, $W=(2^8,1^2)$, $\mathbf{D}=(4^{10})$	4096	42.4 s	911.8 s	21.5	∞	∞	NA
Generic $n=11$, $W=(2^9,1^2)$, $\mathbf{D}=(4^{11})$	8192	292.5 s	12126.4 s	41.5	∞	∞	NA
Generic $n=12$, $W=(2^{10},1^2)$, $\mathbf{D}=(4^{12})$	16384	2463.2 s	146774.7 s	59.6	∞	∞	NA
Generic $n=13$, $W=(2^{11},1^2)$, $\mathbf{D}=(4^{13})$	32768	∞	∞	NA	∞	∞	NA
DLP Edwards $n=4$, $W=(2^3,1)$, $\mathbf{D}=(8^4)$	512	1 s	1 s	1	1 s	27 s	27
DLP Edwards $n=5$, $W=(2^4,1)$, $\mathbf{D}=(16^5)$	65536	6044 s	56105 s	9.3	∞	∞	NA

(b) Benchmarks with Magma

Table 1: Benchmarks with FGb and Magma for some affine systems

[6] B. Buchberger. A theoretical basis for the reduction of polynomials to canonical forms. *ACM SIGSAM Bull.*, 10(3):19–29, 1976.

[7] A. Dickenstein and I. Z. Emiris. Multihomogeneous resultant matrices. In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, pages 46–54, New York, 2002. ACM.

[8] D. Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[9] J.-C. Faugére. A new efficient algorithm for computing Gröbner bases (F_4). *J. Pure Appl. Algebra*, 139(1-3):61–88, 1999. Effective methods in algebraic geometry (Saint-Malo, 1998).

[10] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, pages 75–83 (electronic) , New York, 2002. ACM.

[11] J. C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *J. Symbolic Comput.*, 16(4):329–344, 1993.

[12] J.-C. Faugère and A. Joux. Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases. In *Advances in cryptology—CRYPTO 2003*, volume 2729 of *Lecture Notes in Comput. Sci.*, pages 44–60. Springer, Berlin, 2003.

[13] J.-C. Faugère and C. Mou. Sparse FGLM algorithms. Preprint available at http://hal.inria.fr/hal-00807540.

[14] J.-C. Faugère and S. Rahmany. Solving systems of polynomial equations with symmetries using SAGBI-Gröbner bases. In *ISSAC 2009—Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation*, pages 151–158. ACM, New York, 2009.

[15] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree $(1,1)$: algorithms and complexity. *J. Symbolic Comput.*, 46(4):406–437, 2011.

[16] J.-C. Faugère. FGb: A Library for Computing Gröbner Bases. In K. Fukuda, J. Hoeven, M. Joswig, and N. Takayama, editors, *Mathematical Software - ICMS 2010*, volume 6327 of *Lecture Notes in Computer Science*, pages 84–87, Berlin, Heidelberg, September 2010. Springer Berlin / Heidelberg.

[17] J.-C. Faugère, P. Gaudry, L. Huot, and G. Renault. Using symmetries in the index calculus for elliptic curves discrete logarithm. Cryptology ePrint Archive, Report 2012/199, 2012.

[18] R. Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[19] J. S. Milne. Algebraic geometry (v5.22), 2012. Available at www.jmilne.org/math/.

[20] L. Robbiano. On the theory of graded structures. *J. Symbolic Comput.*, 2(2):139–170, 1986.

[21] R. P. Stanley. Hilbert functions of graded algebras. *Advances in Math.*, 28(1):57–83, 1978.