Gröbner Bases of Ideals Invariant under a Commutative Group: The Non-Modular Case

Jean-Charles Faugère, Jules Svartz
INRIA, Paris-Rocquencourt Center, PolSys Project
UPMC, Univ Paris 06, LIP6
CNRS, UMR 7606, LIP6
{Jean-Charles.Faugere,Jules.Svartz}@lip6.fr

ABSTRACT

We propose efficient algorithms to compute the Gröbner basis of an ideal $I \subset k[x_1, \ldots, x_n]$ globally invariant under the action of a commutative matrix group G, in the non-modular case (where $char(k)$ doesn't divide $|G|$). The idea is to simultaneously diagonalize the matrices in G, and apply a linear change of variables on I corresponding to the base-change matrix of this diagonalization. We can now suppose that the matrices acting on I are diagonal. This action induces a grading on the ring $R = k[x_1, \ldots, x_n]$, compatible with the degree, indexed by a group related to G, that we call G-degree. The next step is the observation that this grading is maintained during a Gröbner basis computation or even a change of ordering, which allows us to split the Macaulay matrices into $|G|$ submatrices of roughly the same size. In the same way, we are able to split the canonical basis of R/I (the staircase) if I is a zero-dimensional ideal. Therefore, we derive *abelian* versions of the classical algorithms F_4, F_5 or FGLM. Moreover, this new variant of F_4/F_5 allows complete parallelization of the linear algebra steps, which has been successfully implemented. On instances coming from applications (NTRU crypto-system or the Cyclic-n problem), a speed-up of more than 400 can be obtained. For example, a Gröbner basis of the Cyclic-11 problem can be solved in less than 8 hours with this variant of F_4. Moreover, using this method, we can identify new classes of polynomial systems that can be solved in polynomial time.

Categories and Subject Descriptors

I.1.2 [**Computing Methodologies**]: Symbolic and Algebraic Manipulation—*Algorithms*

Keywords

Gröbner Basis, Invariant Ideals, Group Action

1. INTRODUCTION

Solving multivariate polynomial systems is a fundamental problem in Computer Algebra, since algebraic systems can arise from many applications (cryptology, robotics, biology, physics, coding theory, etc...). One method to solve such systems is based on Gröbner basis theory. Efficient algorithms to compute Gröbner bases have been proposed, for instance Buchberger's algorithm [1] and Faugère's F_4 or F_5 [4, 5]. If the system has only a finite number of solutions the usual strategy is to compute a Gröbner basis for the DRL ordering, and then perform a change of ordering to obtain a Gröbner basis for the lexicographic ordering with the FGLM algorithm [10]. However, problems coming from applications are often highly structured: in several algebraic problems the set of solutions (the algebraic variety) is invariant under the action of a finite group. The underlying algebraic problem is to compute the variety $V(I)$ associated to an ideal $I \subseteq k[x_1, \ldots, x_n]$ that is *globally* stable under a finite matrix group $G \subset \mathrm{GL}_n(k)$, which means that $\forall f \in I \quad \forall A \in G \quad f^A \in I$. If all the equations are invariant under the action of the group, several approaches have been proposed to solve the system while taking the symmetries into account. In [2] Colin proposes to use invariants [19] to solve the system. This method is very efficient if the Hironaka Decomposition of the ring of invariants is simple, but for the Cyclic-n problem [12] for example, it seems better to use a second method based on SAGBI Gröbner Basis techniques [7]. However, it remains an open issue to solve efficiently the system in the general case. In the biology problem [6] or in the physics problem [9], an approach has been proposed if the group G is the symmetric group or copies of the symmetric group (elements of the form $(\sigma, \ldots, \sigma) \in \mathfrak{S}_m^j$ with $mj = n$.)

MAIN RESULTS. We present efficient algorithms together with complexity analysis to solve polynomial systems which are *globally invariant* under the action of any *commutative* group G. The algorithms are based on three main ideas: first, since the group G is commutative, it is possible to diagonalize the group G, assuming that the characteristic of the field k and $|G|$ are coprime. Thus, up to some linear change of variables, we obtain an ideal $I_{\mathscr{D}}$ invariant under a diagonal group $G_{\mathscr{D}}$ isomorphic to G.

The second idea is to introduce a grading on $R = k[x_1, \ldots, x_n]$ given by the group $G_{\mathscr{D}}$. This grading exists for every finite group H and is indexed on $X(H)$, the set of irreducible linear representations of the group H. The decomposition $R = \bigoplus_{\chi \in X(H)} R_\chi$ is known as the decomposition of R into *isotypic components* (see [17]). In our case, since $G_{\mathscr{D}}$ is diagonal, the set $X(G_{\mathscr{D}})$ is isomorphic to $G_{\mathscr{D}}$ and the isotypic components are generated by monomials. Therefore, we introduce the notion of $G_{\mathscr{D}}$-degree of a polynomial: assuming that $G_{\mathscr{D}}$ is generated by diagonal matrices $Diag(\beta_{i,1}, \ldots, \beta_{i,n})$ of order q_i with $q_1|q_2|\ldots|q_\ell = e$ and that β is a primitive e-root of 1, we say that a polynomial $f \in k[x_1, \ldots, x_n]$ is $G_{\mathscr{D}}$-homogeneous of $G_{\mathscr{D}}$-degree $(d_1, \ldots, d_\ell) \in \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_\ell}$ if $f(\beta_{i,1}x_1, \cdots, \beta_{i,n}x_n) = \beta^{d_i \frac{e}{q_i}} f(x_1, \ldots, x_n)$ for all i. Notice that the action of diagonal groups on polynomials has been used in invariant theory or to speed up Gröbner basis computation in [17, 19, 18, 13]. However, to the best of our knowledge, the impact of such a grading on the complexity of Gröbner bases has not been studied.

Taking into account that the operation of taking the S-polynomial preserves this grading, the final idea is to observe that this can be used to speed up the Gröbner basis computation. More precisely, Macaulay matrix can be decomposed into $|G_{\mathscr{D}}|$ smaller *in-*

ISSAC'13, June 26–29, 2013, Boston, Massachusetts, USA.

dependent matrices, being roughly the same size. In particular, this allows us to split the matrices arising in classical Gröbner basis algorithms based on linear algebra like Macaulay/Lazard algorithm [15], F_4 [4] or F_5 [5]. Therefore, the complexity (in time and in memory) of computing Gröbner bases of such invariant ideals can be decreased in both, theory and practice. In the same way, in the case of a zero-dimensional ideal $I_{\mathscr{D}}$, the canonical basis of the ring $R/I_{\mathscr{D}}$ can also be decomposed in monomials having same $G_{\mathscr{D}}$-degree and thus we are able to split the multiplication matrices arising in FGLM.

In addition, this grading can be used to transform very easily a globally invariant problem into a problem for which all the equations are $G_{\mathscr{D}}$-homogeneous: we show that for each original equation f we can take the $G_{\mathscr{D}}$-homogeneous components of f.

We have implemented, in the computer algebra system Magma, "abelian" versions of the F_5 and *FGLM* algorithms that run several times faster, compared to the same implementation of these classical algorithms. For example, applying FGLM on the Cyclic-10 problem (a system with 34940 solutions), instead of computing 10 multiplication matrices of size 34940, our algorithm computes 900 quasi-square matrices of size at most 348.

In order to compare similar implementations, we have implemented an "abelian" version of F_4 [4] in FGb (C language): computing a Gröbner basis of the Cyclic-10 problem is about 410 times faster with the new approach. Moreover, a grevlex Gröbner basis for the Cyclic-11 problem (184756 solutions) can be computed in less than 8 hours. We also demonstrate that our approach has a significant impact in other fields: NTRU is a well known cryptosystem and the underlying problem can easily be modeled by quadratic equations which are left globally invariant by the action of a cyclic group. We observe a factor of 250 in favor of the new approach for small size problems and more importantly we can solve previously untractable problems. Surprisingly, during these experiments, the linear algebra parts (that is building the matrices and the gaussian elimination parts) can sometimes be so accelerated that the management of the list of critical pairs becomes the most time-consuming part whereas it is usually negligible.

More generally, the algorithms given in this paper can also be used for other kinds of structured polynomial systems like quasi-homogeneous or multi-homogeneous polynomials. Hence we now have a systematic and uniform approach to solve those structured problems. Several further developments can be made on the subject: the Abelian-F_5 and Abelian-FGLM algorithms have to be implemented in C, and it seems possible to obtain a parallelized version of the Abelian-FGLM algorithm. We have already identified new classes of invariant problems which can be solved in polynomial time; for other classes of problems the degree reached during the Gröbner basis computation is much lower than expected and it would be very useful to compute explicitly the Hilbert Series of ideals invariant under a diagonal group.

The organization of the paper is as follows: in section 2, we recall classical notations and explain the relations between the ideals I and $I_{\mathscr{D}}$, and the matrix groups G and $G_{\mathscr{D}}$. In section 3, we explain the grading induced by the diagonal matrix group $G_{\mathscr{D}}$, and introduce the notion of $G_{\mathscr{D}}$-degree of monomials and polynomials. The vector space generated by all monomials having same $G_{\mathscr{D}}$-degree is nothing else than an *isotypic component* ([17]) but since the formulation is simpler in the case of a diagonal group, we introduce the notion of $G_{\mathscr{D}}$-degree of monomials and $G_{\mathscr{D}}$-homogeneous polynomials. Sections 4 and 5 provide variants of the F_5 and FGLM algorithms. The complexity questions are answered in section 6, and benchmarks are made in section 7.

2. LINEAR CHANGE OF VARIABLES

2.1 Frequently used notations

From now on we assume that G is a finite commutative subgroup of $GL_n(k)$, the set of square matrices with coefficients in a field k of characteristic 0 or p such that p and $|G|$ are coprime. $G_{\mathscr{D}}$ will be used to denote a diagonal matrix group, conjugated to G. $R_k = k[x_1,\ldots,x_n]$ is the ring of polynomials with coefficients in k. In the following, we will have to consider a finite simple extension of k that will be denoted $K = k(\xi)$. The set of monomials of R_k (or R_K) will be denoted $\mathscr{M}$. We fix an admissible monomial ordering $\preceq$ on the set of monomials (only admissible orderings are allowed, for a precise definition, we refer to [3] p. 53). For a given degree d, $\mathscr{M}_d$ will be the set of all monomials in R of degree d. For a polynomial in R, $\mathsf{LC}(f)$ (resp $\mathsf{LM}(f)$, $\mathsf{LT}(f)$) denotes the leading coefficient (resp leading monomial, leading term) in f. We have the relation $\mathsf{LT}(f) = \mathsf{LC}(f)\mathsf{LM}(f)$.

2.2 Action of $GL_n(k)$ on $k[x_1,\ldots,x_n]$. Invariant rings.

This subsection describes the basic properties of the action of $GL_n(k)$ on polynomials. We recall that G is a finite subgroup of $GL_n(k)$. Let X be the column vector whose entries are $x_1,\ldots,x_n$. For f a polynomial in R and $A \in G$, let f^A be the polynomial obtained by substituting the components of $A.X$ to $x_1,\ldots,x_n$. Since $(f^A)^B = f^{AB}$, we obtain an action of G on R. Let R_d be the vector space of all homogeneous polynomials of degree d. Then $R = \bigoplus_{d=0}^{\infty} R_d$ and we observe that the action of G preserves the homogeneous components.

Definition 1 *We denote by R^G the set of* invariant polynomials*, that means polynomials invariant under the action of G : $f^A = f$ for every A in G.*

Although we won't work exclusively in the ring R^G of invariant polynomials, we will use several known properties of this set, especially in the complexity section.

Example 1 *The symmetric group $\mathfrak{S}_n$ can be embedded in $GL_n(k)$, and $R^{\mathfrak{S}_n}$ is nothing else than the set of the so called* symmetric polynomials*. Let C_n be the subgroup of $\mathfrak{S}_n$ generated by the n-cycle $\sigma = (12\ldots n)$. C_n is a cyclic group of order n, embedded in $GL_n(k)$ and generated by M_σ.*

$$M_\sigma = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ 1 & 0 & 0 & \ldots & 0 \end{pmatrix}$$

For example if $n = 3$ then $x_1^2x_2 + x_2^2x_3 + x_3^2x_1$ belongs to $R^{C_n} \setminus R^{\mathfrak{S}_n}$.

2.3 From commutative group to diagonal group

This subsection presents one of the main ideas of the paper, although it is very simple. We recall some well known facts about commutative matrix groups.

Theorem 1 *Any finite commutative group is uniquely isomorphic to a product $\mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_\ell\mathbb{Z}$ with $q_1|\ldots|q_\ell$.*

Definition-Proposition 1 *Following the notations of the previous theorem, the integer $e = q_\ell$ is called the* exponent *of the group and is the lowest common multiple of the orders of the elements of the group.*

Theorem 2 *Let G be a finite commutative matrix group, and e be its exponent. Let ξ be a primitive e-th root of 1, in an extension of k and $K = k(\xi)$. The subgroup G is diagonalizable over K, meaning that there exists a matrix P in $GL_n(K)$, such that the group $G_{\mathscr{D}} = P^{-1}GP = \{P^{-1}AP \mid A \in G\}$ is a diagonal group.*

PROOF. Every matrix $A \in G$ satisfies the polynomial $X^e - 1$, which fully splits in K and has simple roots since $char(k) \not| |G|$, so every matrix of G is diagonalizable, and it is well known that a commutative set of diagonalizable matrices is codiagonalizable. ☐

Example 2 *Let k be any field of characteristic 0 or coprime with n. Then if we denote $K = k(\xi)$ where ξ is a primitive n-root of 1 in an extension of k, then the cyclic group C_n defined in example 1 is diagonalizable with the base-change matrix $P = (\xi^{ij})_{i,j\in\{1,\ldots,n\}}$. The matrix associated to the cycle $(1\ldots n)$ becomes the diagonal matrix $D_\sigma = diag(\xi,\ldots,\xi^{n-1},1)$.*

Definition 2 *Let I be an ideal in $R_k = k[x_1,\dots,x_n]$. I is said to be* stable *under the action of G (G-*stable*) if: $\forall f \in I, \forall A \in G \quad f^A \in I$*

Proposition 1 *Let I be a G-stable ideal, and let $G_{\mathscr{D}}$ and P be the diagonal group and the base-change matrix obtained in theorem 2. Then $I_{\mathscr{D}} = K \bigotimes_k \{f^P, f \in I\}$ is an ideal of R_K stable under $G_{\mathscr{D}}$. If $I = \langle f_1,\dots,f_m\rangle_{R_k}$, then $I_{\mathscr{D}} = \langle f_1^P,\dots,f_m^P\rangle_{R_K}$.*

Example 3 *To illustrate the definition, we will use the well known* Cyclic-n problem. *The ideal I of R_k is generated by:*

$$\begin{cases} h_1 = x_1 + \dots + x_n \\ h_2 = x_1x_2 + x_2x_3 + \dots + x_nx_1 \\ \vdots \\ h_{n-1} = x_1x_2\dots x_{n-1} + x_2\dots x_nx_1 + \dots + x_nx_1\dots x_{n-2} \\ h_n = x_1x_2\dots x_{n-1}x_n - 1 \end{cases}$$

The ideal I is obviously invariant under the cyclic group C_n, since each h_i satisfies $h_i^{M_\sigma} = h_i$ and is also stable under the scalar matrix ξI_n with ξ a primitive n-root of 1, since $h_i^{\xi I_n} = \xi^i h_i$. The group G is generated by M_σ and ξI_n. With P the matrix given in example 2, $G_{\mathscr{D}} = P^{-1}GP$, generated by D_σ and ξI_n, is a diagonal group isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. We denote by f_i the polynomials h_i^P, which generate $I_{\mathscr{D}}$: for instance, $f_1 = 3x_3, f_2 = -3x_1x_2 + 3x_3^2, f_3 = x_1^3 + x_2^3 + 3x_1x_2x_3 + x_3^3 - 1$ when $n = 3$. It is easy to prove that for the Cyclic-n problem, the polynomial f_1 is always equal to nx_n.

3. GRADING INDUCED BY A DIAGONAL MATRIX GROUP

In this section, we define the $G_{\mathscr{D}}$-degree of a monomial where $G_{\mathscr{D}}$ is a diagonal matrix group. This $G_{\mathscr{D}}$-degree induces a grading of R_K given by the isomorphism $G_{\mathscr{D}} \simeq \prod \mathbb{Z}/q_i\mathbb{Z}$.

3.1 $G_{\mathscr{D}}$-degree of monomials

Let $G_{\mathscr{D}}$ be a diagonal group of $GL_n(K)$, with diagonal coefficients in $\mathbb{U}_e = \{\xi^0, \xi^1, \dots, \xi^{e-1}\}$, with e the exponent of G and ξ a primitive e-root of 1, as defined in the previous section. Let ϕ be an isomorphism

$$\phi : \begin{pmatrix} G_{\mathscr{D}} & \longrightarrow & \mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_\ell\mathbb{Z} \\ D & \longmapsto & \phi(D) \end{pmatrix}$$

and let D_i be the preimage of $(0,\dots,0,\underset{i}{1},0,\dots,0)$, so D_i generates a subgroup of $G_{\mathscr{D}}$ of cardinality $|q_i|$.

Example 4 *With $G_{\mathscr{D}}$ the group arising in the previous example 3, we take ϕ such that $\phi(D_\sigma) = (1,0) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ and $\phi(\xi I_n) = (0,1)$.*

Proposition 2 *For every monomial $m \in \mathscr{M}$ and for each i, there exists a unique $\mu_i \in \{0,\dots,q_i-1\}$ such that $m^{D_i} = \xi^{\frac{e}{q_i}\mu_i} m$.*

PROOF. Let $m = \prod x_j^{\alpha_j}$ and $D_i = Diag(\beta_1,\dots,\beta_n)$. Since D_i has order q_i, the coefficients β_j are q_i-roots of 1, so can be denoted $\xi^{\ell_j \frac{e}{q_i}}$. Then

$$m_i^D = (\beta_1 x_1)^{\alpha_1} \times \dots \times (\beta_n x_n)^{\alpha_n} = \left(\prod \beta_j^{\alpha_j}\right) m = \xi^{\frac{e}{q_i}\sum \ell_j \alpha_j} m$$

Then we can take $\mu_i = \sum \ell_j \alpha_j \bmod q_i$. Since ξ has order e, $\xi^{\frac{e}{q_i}}$ has order q_i and the unicity of μ_i is clear. $\square$

Instead of considering μ_i in $\{0,\dots,q_i-1\}$, we take μ_i in $\mathbb{Z}/q_i\mathbb{Z}$, which makes sense since $\xi^{\frac{e}{q_i}}$ has order q_i.

Definition 3 *The k-tuple $(\mu_1,\dots,\mu_k) \in \prod \mathbb{Z}/q_i\mathbb{Z}$ is said to be the* $G_{\mathscr{D}}$-degree *of m and is denoted $\mathsf{deg}_{G_{\mathscr{D}}}(m)$, although it depends on the choice of the matrices D_i (more exactly, the choice of ϕ). We denote by $\hat{G} = \prod \mathbb{Z}/q_i\mathbb{Z}$ the set of all $G_{\mathscr{D}}$-degrees.*

Remark 1 *It is yet unclear that every $\mu \in \hat{G}$ is the $G_{\mathscr{D}}$-degree of some monomial. This will be proved in the complexity section.*

Proposition 3 *Since $\mathsf{deg}_{G_{\mathscr{D}}}(m) + \mathsf{deg}_{G_{\mathscr{D}}}(m') = \mathsf{deg}_{G_{\mathscr{D}}}(mm')$ for all $m, m' \in \mathscr{M}$, R can be graded by $R = \bigoplus_{g \in \hat{G}} Vect(\mathscr{M}_g)$, where $\mathscr{M}_g$ is the set of monomials of $G_{\mathscr{D}}$-degree g.*

PROOF. Let $i \in \{1,\dots,k\}, m, m' \in \mathscr{M}$ and μ_i, μ_i' such that $m^{D_i} = \xi^{\frac{e}{q_i}\mu_i} m$ and $m'^{D_i} = \xi^{\frac{e}{q_i}\mu_i'} m'$. Then $(mm')^{D_i} = \xi^{\frac{e}{q_i}(\mu_i + \mu_i')} mm'$. It follows that the $G_{\mathscr{D}}$-degree verifies $\mathsf{deg}_{G_{\mathscr{D}}}(mm') = \mathsf{deg}_{G_{\mathscr{D}}}(m) + \mathsf{deg}_{G_{\mathscr{D}}}(m')$ for all monomials $m, m' \in \mathscr{M}$ and $\mathsf{deg}_{G_{\mathscr{D}}}$ is a monoid morphism between $\mathscr{M}$ and $\hat{G}$ since $\mathsf{deg}_{G_{\mathscr{D}}}(1) = (0,\dots,0)$, $\square$

Remark 2 *If we denote by $\mathscr{M}_{d,g}$ the set of monomials of degree d and $G_{\mathscr{D}}$-degree g, $\mathscr{M}_{d,g}\mathscr{M}_{d',g'} \subseteq \mathscr{M}_{d+d',g+g'}$ for all d, d', g, g'. Therefore $R = \bigoplus_{d \in \mathbb{N}, g \in \hat{G}} Vect(\mathscr{M}_{d,g})$.*

Notice that for computing $\mathsf{deg}_{G_{\mathscr{D}}}(m)$ with $m = \prod x_i^{\alpha_i}$, we just have to know $\mathsf{deg}_{G_{\mathscr{D}}}(x_i)$ since $\mathsf{deg}_{G_{\mathscr{D}}}(m) = \sum \alpha_i \mathsf{deg}_{G_{\mathscr{D}}}(x_i)$. This grading will be used to reduce the sizes of the matrices in the Diagonal-F_5 algorithm.

Example 5 *Let $G_{\mathscr{D}}$ be the matrix group generated by the diagonal matrix $D_\sigma = Diag(\xi, \xi^2, 1)$ where ξ is a primitive third root of 1. Each x_i has $G_{\mathscr{D}}$-degree $i \bmod 3$, so $m = \prod x_j^{\alpha_j}$ has $G_{\mathscr{D}}$-degree $\sum j\alpha_j \bmod 3$. Hence, $x_1x_2x_3$ (resp. $x_1x_2^2$) has $G_{\mathscr{D}}$-degree 0 (resp. 2).*

Example 6 *(cont. of example 3) The $G_{\mathscr{D}}$-degree of x_i is $(i,1)$.*

3.2 $G_{\mathscr{D}}$-homogeneous polynomials

In this subsection, we define the notion of $G_{\mathscr{D}}$-homogeneity. The cornerstone of the Abelian-F_5 algorithm (section 4) is that the S-polynomial of two $G_{\mathscr{D}}$-homogeneous polynomials is $G_{\mathscr{D}}$-homogeneous, which will be proved in theorem 3.

Definition 4 *A polynomial f in R_K is said to be $G_{\mathscr{D}}$-*homogeneous *if all monomials of f share the same $G_{\mathscr{D}}$-degree $(\mu_1,\dots,\mu_k) \in \hat{G}$. In this case, we set $\mathsf{deg}_{G_{\mathscr{D}}}(f) = \mathsf{deg}_{G_{\mathscr{D}}}(\mathsf{LM}(f))$.*

Proposition 4 *If f is $G_{\mathscr{D}}$-homogeneous and m is a monomial, then mf is $G_{\mathscr{D}}$-homogeneous. Moreover, $\mathsf{deg}_{G_{\mathscr{D}}}(mf) = \mathsf{deg}_{G_{\mathscr{D}}}(m) + \mathsf{deg}_{G_{\mathscr{D}}}(f)$.*

PROOF. For any monomial $\tilde{m}$ of f, $\mathsf{deg}_{G_{\mathscr{D}}}(\tilde{m}m) = \mathsf{deg}_{G_{\mathscr{D}}}(\tilde{m}) + \mathsf{deg}_{G_{\mathscr{D}}}(m) = \mathsf{deg}_{G_{\mathscr{D}}}(f) + \mathsf{deg}_{G_{\mathscr{D}}}(m)$, so all monomials of mf share the same $G_{\mathscr{D}}$-degree $\mathsf{deg}_{G_{\mathscr{D}}}(f) + \mathsf{deg}_{G_{\mathscr{D}}}(m) = \mathsf{deg}_{G_{\mathscr{D}}}(mf)$. $\square$

Theorem 3 *Let f, g be two $G_{\mathscr{D}}$-homogeneous polynomials of R_K. The S-polynomial of (f,g), defined by*

$$S(f,g) = \frac{\mathsf{LM}(f) \vee \mathsf{LM}(g)}{\mathsf{LM}(f)} f - \frac{\mathsf{LM}(f) \vee \mathsf{LM}(g)}{\mathsf{LM}(g)} \frac{\mathsf{LC}(f)}{\mathsf{LC}(g)} g$$

is $G_{\mathscr{D}}$-homogeneous of $G_{\mathscr{D}}$-degree $\mathsf{deg}_{G_{\mathscr{D}}}(\mathsf{LM}(f) \vee \mathsf{LM}(g))$. ($\mathsf{LM}(f) \vee \mathsf{LM}(g)$ denotes the lowest common multiple of $\mathsf{LM}(f)$ and $\mathsf{LM}(g)$.)

PROOF. Since $\mathsf{LM}(f)$ and $\mathsf{LM}(g)$ divide $\mathsf{LM}(f) \vee \mathsf{LM}(g)$, both fractions $\frac{\mathsf{LM}(f)\vee\mathsf{LM}(g)}{\mathsf{LM}(f)}$ and $\frac{\mathsf{LM}(f)\vee\mathsf{LM}(g)}{\mathsf{LM}(g)}$ are monomials, therefore by previous proposition, $\frac{\mathsf{LM}(f)\vee\mathsf{LM}(g)}{\mathsf{LM}(g)} \frac{\mathsf{LC}(f)}{\mathsf{LC}(g)} g$ and $\frac{\mathsf{LM}(f)\vee\mathsf{LM}(g)}{\mathsf{LM}(f)} f$ are $G_{\mathscr{D}}$-homogeneous. Moreover, they share the same leading monomial, so they have same $G_{\mathscr{D}}$-degree, which is the $G_{\mathscr{D}}$-degree of $S(f,g)$. We actually proved that $\mathsf{deg}_{G_{\mathscr{D}}}(S(f,g)) = \mathsf{deg}_{G_{\mathscr{D}}}(\mathsf{LM}(f) \vee \mathsf{LM}(g))$. $\square$

Example 7 *Following example 3, it appears that each f_i has $G_{\mathscr{D}}$-degree $(0,i) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ under $G_{\mathscr{D}}$ generated by D_σ and ξI_n.*

3.3 $G_{\mathscr{D}}$-homogeneous ideals

In this subsection, $G_{\mathscr{D}}$ is a diagonal group, and $I_{\mathscr{D}}$ is a $G_{\mathscr{D}}$-stable ideal generated by $f_1,\dots,f_m$. A Gröbner basis computation preserves the $G_{\mathscr{D}}$-degree, but the polynomials f_i are not necessarily $G_{\mathscr{D}}$-homogeneous. Our aim here is to prove that the $G_{\mathscr{D}}$-homogeneous components of the f_i are in $I_{\mathscr{D}}$, and so to compute a Gröbner basis of $I_{\mathscr{D}}$, we take the $G_{\mathscr{D}}$-homogeneous components of generators of $I_{\mathscr{D}}$ as inputs. This operation has a negligible cost since at each degree d, the abelian-F_5 algorithm (presented in the next section) separates the set $\mathscr{M}_d$ into subsets $\mathscr{M}_{d,g}$ of same $G_{\mathscr{D}}$-degree g.

Definition 5 *An ideal J of R_K is said to be* $G_{\mathscr{D}}$-homogeneous *if for any polynomial $f \in J$, its $G_{\mathscr{D}}$-homogeneous components are also in J.*

Theorem 4 *An ideal is $G_{\mathscr{D}}$-homogeneous if and only if it is $G_{\mathscr{D}}$-stable.*

It is obvious that a $G_{\mathscr{D}}$-homogeneous ideal is $G_{\mathscr{D}}$-stable. To prove the other implication, we will first prove a lemma.

Lemma 1 *Let $f \in I_{\mathscr{D}}$, and $D \in G_{\mathscr{D}}$, then the $\langle D\rangle$-homogeneous components of f are in $I_{\mathscr{D}}$, where $\langle D\rangle$ is the subgroup generated by D.*

PROOF. Let q be the order of D in $G_{\mathscr{D}}$, and $\xi_D = \xi^{\frac{e}{q}}$. Then, all diagonal coefficients of D are powers of ξ_D. f can be written $\sum_{j=0}^{q-1} f_j$, with $f_j^D = \xi_D^j f_j$; in other words, the f_j are the $\langle D\rangle$-homogeneous components of f. Let $X_f = {}^t(f_0,f_1,\dots,f_{q-1})$, $V = (\xi_D^{ij})_{0\le i,j\le q-1}$, and $Y_f = VX_f$. Since $f_j^{D^i} = \xi_D^{ij} f_j$, the column vector Y_f is equal to ${}^t(f, f^D, \dots, f^{D^{q-1}})$. Since $f \in I_{\mathscr{D}}$ and $I_{\mathscr{D}}$ is $G_{\mathscr{D}}$-stable, all components of Y_f belong to $I_{\mathscr{D}}$. But V is a VanDerMonde invertible matrix, so the components of X_f are obtained from Y_f by linear combinations, and the f_j belong to $I_{\mathscr{D}}$. ☐

PROOF. We now prove theorem 4 by induction on ℓ where $G \simeq \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_\ell\mathbb{Z}$: the case $\ell = 1$ is the lemma. Now assume that $\ell \ge 2$ and let D_i be the matrices generating $G_{\mathscr{D}}$ as defined in section 2. Let $f \in I_{\mathscr{D}}$. By the lemma, the $\langle D_\ell\rangle$-homogeneous components of f are in $I_{\mathscr{D}}$. Denote by $\tilde{G_{\mathscr{D}}}$ the subgroup of $G_{\mathscr{D}}$ generated by $D_1,\dots,D_{\ell-1}$, then $\tilde{G_{\mathscr{D}}} \simeq \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_{\ell-1}\mathbb{Z}$, and $I_{\mathscr{D}}$ is also $\tilde{G_{\mathscr{D}}}$-stable, and by induction the $\tilde{G_{\mathscr{D}}}$-homogeneous components of each $\langle D_\ell\rangle$-homogeneous component of f are in $I_{\mathscr{D}}$, but they are exactly the $G_{\mathscr{D}}$-homogeneous components of f. ☐

Remark 3 *In representation theory, the $G_{\mathscr{D}}$-homogeneous components of a polynomial in $I_{\mathscr{D}}$ are the images of the projections onto each isotypic component. [17]*

Example 8 *Let $G_{\mathscr{D}}$ be the diagonal group of order 2 generated by the matrix $diag(-1,1)$, acting on $R = k[x_1,x_2]$. Suppose that $x_1^3x_2 + x_1^2x_2^2 - x_1 + 1 \in I_{\mathscr{D}}$, with $I_{\mathscr{D}}$ a $G_{\mathscr{D}}$-stable ideal. Then since $\mathsf{deg}_{G_{\mathscr{D}}}(x_i) = i \bmod 2$, $\mathsf{deg}_{G_{\mathscr{D}}}(x_1^3x_2) = \mathsf{deg}_{G_{\mathscr{D}}}(x_1) = 1$ and $\mathsf{deg}_{G_{\mathscr{D}}}(1) = \mathsf{deg}_{G_{\mathscr{D}}}(x_1^2x_2^2) = 0$, so $x_1^3x_2 - x_1$ and $x_1^2x_2^2 + 1$ belong to $I_{\mathscr{D}}$.*

4. ABELIAN-F_5 ALGORITHM

Now, we are able to describe the Abelian-F_5 algorithm, which is a variant of F_5 that takes advantage of the action of the abelian group $G_{\mathscr{D}}$. As usual, $I_{\mathscr{D}}$ is a $G_{\mathscr{D}}$-stable ideal, with $G_{\mathscr{D}}$ a diagonal group isomorphic to $\hat{G}$, the set of $G_{\mathscr{D}}$-degrees. Let $f_1,\dots,f_m$ be $G_{\mathscr{D}}$-homogeneous polynomials generating $I_{\mathscr{D}}$ (according to theorem 4). All computation of the reduced Gröbner basis of $I_{\mathscr{D}}$ would implicitly use the grading $R = \bigoplus_{g\in\hat{G}} R_g$ since it computes S-polynomials. There exist several versions of the F_5-algorithm (see [7, 5]), we present here a variant of the matrix version. The F_5-algorithm constructs matrices degree by degree. At a fixed degree d, it constructs m matrices of the form $M_{d,i}$ for each i between 1 and m, and performs row reduction on them to obtain $\tilde{M_{d,i}}$. In the homogeneous case, $\tilde{m}_1,\dots,\tilde{m}_\nu$ are all monomials of degree d, whereas in the affine case, they are all monomials of degrees between 0 and d. For the sake of simplicity, we assume that all polynomials f_i are homogeneous. The rows are indexed by couples of the form $m_\mu f_j$, the matrix $M_{d,i}$ is deduced from the matrix $\tilde{M_{d,i-1}}$ by adding all rows $m_\mu f_i$ with m_μ describing the set of monomials of degree $d - \deg(f_i)$, except monomials removed by the F_5-criterion (see [7, 5]).

$$
M_{d,i} = \begin{array}{c} \\ m_1 f_1 \\ \vdots \\ m_\mu f_j \\ \vdots \\ m_\gamma f_i \end{array}
\begin{array}{c}
\begin{array}{cccc} \tilde{m}_1 & \tilde{m}_2 & \dots & \tilde{m}_\nu \end{array} \\
\begin{pmatrix} \dots & \dots & \dots & \dots \\ & & & \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ & & & \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix}
\end{array}
$$

The key of the Abelian-F_5 algorithm is the following : the polynomials f_i are $G_{\mathscr{D}}$-homogeneous, and also the polynomials $m_\mu f_i$. Therefore, the only non-zero coefficients of the row indexed by $m_\mu f_i$ are on columns indexed by monomials having same $G_{\mathscr{D}}$-degree. So, instead of building one Macaulay matrix $M_{d,i}$, we will construct $|G_{\mathscr{D}}|$ matrices $M_{d,i,g}$, for all $g \in \hat{G}$.

Abelian-F_5 (homogeneous-case)

Input: The set $\hat{G}$ of $G_{\mathscr{D}}$-degrees, homogeneous and $G_{\mathscr{D}}$-homogeneous polynomials $(f_1,\dots,f_m)$ with degrees $d_1 \le \dots \le d_m$ and a maximal degree D.
Output: the elements of degree at most D of a Gröbner basis of $(f_1,\dots,f_i)$ for $i = 1,\dots,m$.

for i **from** 1 **to** m **do** $\mathscr{G}_i := \emptyset$ **end for**
for d **from** d_1 **to** D **do**
  for g **in** $\hat{G}$ **do**
    $M_{d,0,g} := \emptyset$, $\tilde{M}_{d,0,g} := \emptyset$
    for i **from** 1 **to** m **do**
      case
        $d < d_i)$ $M_{d,i,g} := \tilde{M}_{d,i-1,g}$
        $d = d_i)$ **if** $g = \mathsf{deg}_{G_{\mathscr{D}}}(f_i)$ **then**
            $M_{d,i,g} :=$ add new row f_i to $\tilde{M}_{d,i-1,g}$ with index $(i,1)$
          else
            $M_{d,i,g} := \tilde{M}_{d,i-1,g}$
          end if
        $d > d_i)$ $M_{d,i,g}$:=add new row $m.f_i$ for all monomials m of degree $d - d_i$ with $\mathsf{deg}_{G_{\mathscr{D}}}(m) = g - \mathsf{deg}_{G_{\mathscr{D}}}(f_i)$ that do not appear as leading monomials in the matrix $\tilde{M}_{d-d_i,i-1,u-\mathsf{deg}_{G_{\mathscr{D}}}(f_i)}$ to $\tilde{M}_{d,i-1,g}$ with index (i,m).
      end case
      Compute $\tilde{M}_{d,i,g}$ by Gaussian elimination from $M_{d,i,g}$.
      Add to $\mathscr{G}_i$ all rows of $\tilde{M}_{d,i,g}$ not reducible by $\mathsf{LM}(\mathscr{G}_i)$.
    end for
  end for
end for
return $\mathscr{G}_1,\cdots,\mathscr{G}_m$

Notice that all the loops on $g \in \hat{G}$ are independent, so at each degree d, it is possible to parallelize on $|G|$ different processors to speed up the computations. Assuming that the degrees of the *primary invariants* are relatively prime, we will see in the complexity section 6 that the number of monomials of $\mathscr{M}_d$ having same $G_{\mathscr{D}}$-degree is almost the same for all g. In the affine case, we will prove without any assumption that the monomials of degree between 0 and d are evenly distributed on $\hat{G}$. These considerations allow us to bound the complexity of the computation of a Gröbner basis on such ideals, and we will verify that in practice they make an improvement on the timings (see section 7).

5. ABELIAN-FGLM ALGORITHM

In this section, we explain how to take advantage of the $G_{\mathscr{D}}$-grading to speed up the change of ordering, using a variant of the classical FGLM algorithm [10]. We suppose that $\dim(I_{\mathscr{D}}) = 0$, and that a Gröbner basis $\mathscr{G}_{\preceq_1}$ for an ordering $\preceq_1$ (for instance the DRL ordering) of the ideal $I_{\mathscr{D}} \subset R_K$ has already been computed, and we are interested in computing the Gröbner basis of $I_{\mathscr{D}}$ for an other ordering $\preceq_2$ (for example, the lexicographical ordering). In this section, $\mathbf{Deg}(I_{\mathscr{D}})$ will denote the degree of $I_{\mathscr{D}}$, defined by the dimension of $R/I_{\mathscr{D}}$. The idea of both FGLM and Abelian-FGLM algorithms is to pick up monomials m in $\mathscr{M}$ by increasing order for $\preceq_2$, and look for linear combinations in $R/I_{\mathscr{D}}$ between the Normal Forms $\mathsf{NF}(m,\mathscr{G}_{\preceq_1})$. To this end, these algorithms use linear algebra: we first compute the staircase

$$\mathscr{E} = \{m \in \mathscr{M} \mid m \text{ not reducible by } \mathsf{LM}(\mathscr{G}_{\preceq_1})\}$$

The elements of $\mathscr{E}$ form a basis of $R/I_{\mathscr{D}}$, which has dimension $\mathbf{Deg}(I_{\mathscr{D}})$, the degree of $I_{\mathscr{D}}$. Since $I_{\mathscr{D}}$ is $G_{\mathscr{D}}$-homogeneous, this staircase can be splitted in $|G_{\mathscr{D}}|$ parts, and we will denote by $\mathscr{E}_g$ the set of monomials in $\mathscr{E}$ having $G_{\mathscr{D}}$-degree g. As in the FGLM-algorithm, we use the linear maps given by the multiplication by one variable x_i in $R/I_{\mathscr{D}}$. The main difference lies in the following proposition:

Proposition 5 *Let f be a $G_{\mathscr{D}}$-homogeneous polynomial, and $\mathscr{G}_{\preceq_1}$ be the Gröbner basis of the ideal $I_{\mathscr{D}}$ for $\preceq_1$. Then $\mathsf{NF}(f,\mathscr{G}_{\preceq_1})$ is $G_{\mathscr{D}}$-homogeneous and has same $G_{\mathscr{D}}$-degree as f.*

PROOF. We have seen that being $G_{\mathscr{D}}$-homogeneous is a property stable under S-polynomials operations, so $\mathsf{NF}(f,\mathscr{G}_{\preceq_1})$ is $G_{\mathscr{D}}$-homogeneous. Moreover the only operations used in a Normal-Form computation are of the form $\tilde{f} \leftarrow f - \lambda m h$ with $h \in \mathscr{G}_{\preceq_1}$, $\lambda \in K$ and m a monomial such that $\mathsf{LM}(h) \times m$ is equal to some monomial in f, so $\deg_{G_{\mathscr{D}}}(f) = \deg_{G_{\mathscr{D}}}(\tilde{f})$. $\square$

Diagonal-FGLM algorithm

Input: Multiplication matrices $M_{i,g}$, the sub-staircases $\mathscr{E}_g$, an ordering $\preceq_2$
Output: The Gröbner basis of $I_{\mathscr{D}}$ for $\preceq_2$.

```
L := [(1,0̂,n),(1,0̂,n−1),...,(1,0̂,1)]   // list of 3-uples (j,g,i) symbolizing the monomials S_g[j] × x_i, ordered by increasing order.
S_g := [] for g ∈ Ĝ\{0̂} and S_0̂ = [1].   // subsets of the staircase 𝒮 for the ordering ⪯_2 having same G_𝒟-degree.
V_g := [] for g ∈ Ĝ\{0̂} and V_0̂ = [ᵗ(1,0,...,0)].  // V_g contains the expressions of NF(S_g[j],𝒢_⪯1) in ℰ_g, each vector in V_g has n_g components.
G := []  // The Gröbner basis for ⪯_2
Q_g := I_{n_g} for all g ∈ Ĝ.
 Do
   m := first(L) and remove m from L.
   j := m[1]; g' := m[2]; i := m[3]; g := g' + deg_{G_𝒟}(x_i)
   v := M_{i,g'} V_{g'}[j] // components of NF(x_i S_g[j],𝒢_⪯1) in ℰ_g
   s := #S_g  // number of elements in S_g.
   λ = ᵗ(λ_1,...,λ_{n_g}) := Q_g v
    if λ_{s+1} = ··· = λ_{n_g} = 0  then
      G := G ∪ [m − Σ_{j=1}^{s} λ_j · S_g[j]]
    else
      S_g := S_g ∪ [S_{g'}[j] × x_i]
      V_g := V_g ∪ [v]
      L := Sort(L ∪ [(s+1,g,i) | i = 1,...,n], ⪯_2)
      Remove duplicates from L
      Update(Q_g, λ, v)  // Now Q_g v = ᵗ(0,...,0, 1 (at s+1), 0,...,0)
    end if
   Remove from L all multiples of LM_⪯2(G)
      if L = ∅  then return  G end if
```

Therefore, if m has $G_{\mathscr{D}}$-degree g, $\deg_{G_{\mathscr{D}}}(x_i m) = \deg_{G_{\mathscr{D}}}(x_i) + g$ and $\mathsf{NF}(x_i m,\mathscr{G}_{\preceq_1})$ is of same $G_{\mathscr{D}}$-degree. The map of multiplication by x_i in $\mathsf{Vect}(\mathscr{E})$ can be splitted into the following maps:

$$\begin{array}{rccc} M_{i,g}: & \mathsf{Vect}(\mathscr{E}_g) & \longrightarrow & \mathsf{Vect}(\mathscr{E}_{g+\deg_{G_{\mathscr{D}}}(x_i)}) \\ & f & \longmapsto & \mathsf{NF}(x_i f,\mathscr{G}_{\preceq_1}) \end{array}$$

The Diagonal-FGLM algorithm needs the matrices of multiplication $M_{i,g}$ and proceeds just like FGLM-algorithm:a new monomial to consider (except 1) is of the form $m = x_i m'$, with $m' \preceq_2 m$. Assume that $\deg_{G_{\mathscr{D}}}(m') = g'$, so we already know the expression of $\mathsf{NF}(m',\mathscr{G}_{\preceq_1})$ in terms of $\mathscr{E}_{g'}$, which is a vector V'. It follows that $\mathsf{NF}(m,\mathscr{G}_{\preceq_1})$ is computed by the product $V = M_{i,g'}V'$. Then we have to decide if m belongs to the new staircase in construction $\mathscr{S}$ or if it is the leading monomial of a polynomial of the Gröbner basis for $\preceq_2$. To this end, we use base-change matrices Q_g between $\mathscr{E}_g$ an $\mathscr{S}_g$, the subsets of the staircases having same $G_{\mathscr{D}}$-degree g. If s is the number of elements of the staircase $\mathscr{S}_g = \{u_1 \preceq_2 \cdots \preceq_2 u_s\}$ at the current point of the algorithm, and V_i the vectors corresponding to $\mathsf{NF}(u_i,\mathscr{G}_{\preceq_1})$, then $Q_g V_i$ is equal to the i-th vector of the canonical basis. Since the matrix Q_g is invertible, if all the components but the s first ones of QV are zero, then we deduce a new element of the Gröbner basis $\mathscr{G}_{\preceq_2}$, otherwise m is a new element of $\mathscr{S}_g$ and we have to update Q_g, to map V on the $(i+1)$-th element of the canonical basis. We can now give the pseudocode of the Diagonal-FGLM algorithm, here $\hat{0}$ means the $G_{\mathscr{D}}$-degree $(0,\ldots,0)$. We suppose that $x_1,\ldots,x_n$ is the set of variables, with $x_n \preceq_2 x_{n-1} \preceq_2 \cdots \preceq_2 x_1$, and denote by n_g the number of elements in $\mathscr{E}_g$. Notice that with $\deg_{G_{\mathscr{D}}}(x_i) = \hat{0}$ for each i, we recover the standard FGLM algorithm.

Remark 4 *According to a point of view of representation theory, the sub-staircases $\mathscr{E}_g$ and $\mathscr{S}_g$ can be seen as two distinct bases of an isotypic component of the representation $R/I_{\mathscr{D}}$.*

6. COMPLEXITY QUESTIONS

In this section, we discuss the arithmetic complexity of the algorithms presented before. This complexity will be counted in terms of operations in $K = k(\xi)$.

Remark 5 *[18] A very interesting case is when ξ belongs to k, so $K = k$. Assume that k is the finite group $\mathbb{F}_p$ with p prime. Then*
$\xi \in k \Longleftrightarrow X^e - 1$ splits on $k \Longleftrightarrow \mathbb{Z}/e\mathbb{Z} \subseteq \mathbb{Z}/(p-1)\mathbb{Z} \Longleftrightarrow p \equiv 1[e]$
By Dirichlet's theorem, there are infinitely many such primes and the distribution of such primes is $1/\varphi(e)$, where φ is the Euler's totient function. To compute the Gröbner basis of an ideal over $\mathbb{Q}$, it is more efficient to compute modulo some such primes and use modular methods to recover the original Gröbner basis.

We start by giving without proof a bound on the cost of the two first linear steps:

Proposition 6 *The cost of the diagonalization of the matrix group G is bounded by $O((q_1+\cdots+q_k)n^{\omega})$, with ω the constant of linear algebra. With m polynomials f_i of degree less or equal than d, the cost of computing the f_i^P is bounded by $O(\binom{n+d}{d} ndm \log d \log\log d)$.*

6.1 Dimensions of the subspaces $R_{d,g}$

6.1.1 General facts about the ring of invariants

The first object we are interested in is the ring of invariants $R^{G_{\mathscr{D}}}$, with $G_{\mathscr{D}}$ the diagonal matrix group. Notice that we consider the invariants in a theoretical point of view to obtain complexity bounds, so we don't have to compute them. In this paragraph, we recall some well known facts about R^G, without any assumption on G, excepted that G is a finite matrix group of $GL_n(K)$, $charK$ doesn't divide $|G|$, and G is diagonalizable on K. We follow the presentation of [19]. Although Sturmfels works on $\mathbb{C}$, the results can be easily extended since the characteristic polynomials of matrices in G fully split on K.

Theorem 5 *[19] The invariant ring R_K^G is Cohen-Macaulay : there exist a set of n homogeneous polynomials $\theta_1,..,\theta_n$ and t other invariant polynomials $\eta_1,..,\eta_t$ such that $R_K^G = \bigoplus_{i=1}^t \eta_i \mathbb{K}[\theta_1,\ldots,\theta_n]$.*

The set of polynomials θ_i is called a set of *primary invariants* of G and the set of η_j a set of *secondary invariants* of G. A consequence of the previous theorem is the following proposition

Proposition 7 *[19] The Hilbert (Molien) series of the ring R_K^G is*

$$H(R_K^G,z) = \sum_{d=0}^{\infty} z^d \dim(R_{K,d}^G) = \frac{\sum_{i=0}^t z^{deg(\eta_i)}}{\prod_{j=1}^n (1-z^{deg(\theta_j)})}$$

Proposition 8 *[19] The set of secondary invariants depends on the chosen set of primary invariants, moreover the degrees of the primary invariants and the number of secondary invariants are related by the formula :* $t = \prod_j \mathsf{deg}(\theta_j)/|G|$

Now, we want to give an estimation of the size of R_d^G (set of invariant polynomials of degree d) compared to R_d. To give an estimation of the complexities of Abelian-F_5 and Abelian-FGLM algorithms, we are interested in two quantities.

Definition 6 *We define the* density *of R_d^G in R_d and the density of R^G in R by*

$$\delta(R_d^G) = \frac{\dim(R_d^G)}{\dim(R_d)} \qquad \text{and} \qquad \delta(R^G) = \lim_{D\to+\infty} \frac{\sum_{d=0}^D \dim(R_d^G)}{\sum_{d=0}^D \dim(R_d)}$$

The goal of this subsection is to prove the following theorem:

Theorem 6 *The density $\delta(R^G)$ is well defined and is equal to $1/|G|$. If a set of primary invariants of R^G can be chosen such that their degrees are relatively prime, the density $\delta(R_d^G)$ has the limit $\delta(R^G) = 1/|G|$ as d tends to infinity.*

PROOF. Denote by α_i the degree of θ_i, and by α the greatest common divisors of the α_i. We are interested in an asymptotic estimation of the coefficient in z^d in the Hilbert series of R_K^G. For now, denote by $f(z)$ the power series $1/(\prod_{j=1}^n(1-z^{\alpha_j}))$, and $[z^d]f(z)$ the coefficient in z^d in the expansion of f. Clearly, $[z^d]f(z) = 0$ if α doesn't divide d. Then, if $\alpha|d$, $[z^d]f(z) = [z^{d/\alpha}]\frac{1}{\prod_{j=1}^n(1-z^{\alpha_j/\alpha})}$. Since the integers α_i/α have no common factor, it follows that 1 is the unique pole of multiplicity n in the previous rational function, the other poles having a smaller multiplicity. Following the idea of [11] Theorem 4.9, p.256, we obtain that

$$\begin{aligned}[z^{d/\alpha}]\frac{1}{\prod_{j=1}^n(1-z^{\alpha_j/\alpha})} &= [z^{d/\alpha}]\frac{1}{(1-z)^n\prod_{j=1}^n(\sum_{\ell=0}^{(\alpha_j/\alpha)-1} z^\ell)} \\ &= \gamma\binom{d/\alpha+n-1}{n-1}\end{aligned}$$

with γ the coefficient of $\frac{1}{1-z^n}$ in the partial fraction expansion:

$1/\gamma = \lim_{z\to1}\prod_{j=1}^n(\sum_{\ell=0}^{(\alpha_j/\alpha)-1} z^\ell) = \prod_{j=1}^n \alpha_j/\alpha^n$

Since $\binom{d/\alpha+n-1}{n-1} \underset{d\to+\infty}{\sim} (d/\alpha)^{n-1}$, we have obtained that:

$$[z^d]f(z) = \begin{cases} 0 & \text{if } \alpha \nmid d \\ \frac{\alpha d^{n-1}}{\prod_j \alpha_j} + o(d^{n-1}) & \text{if } \alpha \mid d \end{cases}$$

We are now able to give the density of R^G :

$\sum_{d=0}^D \dim R_d^G \underset{D\to+\infty}{\sim} t\sum_{0\le d\le D, \alpha|d} \frac{\alpha d^{n-1}}{\prod_j \alpha_j} \underset{D\to+\infty}{\sim} \frac{t}{\prod_j \alpha_j}\sum_{d=0}^D d^{n-1}$

But $\sum_{d=0}^D \dim R_d \underset{D\to+\infty}{\sim} \sum_{d=0}^D d^{n-1}$, and by applying proposition 8, we conclude that $\delta(R_K^G) = 1/|G|$. Assume now that $\alpha = 1$, then $[z^d]f(z) = \frac{d^{n-1}}{\prod \alpha_i} + o(d^{n-1})$, so $[z^d]H(R^G,z) = \frac{td^{n-1}}{\prod \alpha_i} + o(d^{n-1})$, and the second part of the theorem follows. □

Remark 6 *If the degrees of the primary invariants have a common factor, the second part of the theorem is false. The following (trivial) example illustrates this fact.*

Example 9 *Let $G = \{\mathsf{Diag}(\pm1,\pm1)\}$ Then $\mathbb{K}[x,y]^G = \mathbb{K}[x^2,y^2]$, and all the densities $\delta(R_d^G)$ are zero for odd d.*

6.1.2 Application to diagonal groups

Now we go back to the situation where G is a diagonal group isomorphic to $\prod_{i=1}^k \mathbb{Z}/q_i\mathbb{Z}$. Recall that $\mathscr{M}_{d,g}$ is the set of monomials of degree d and $G_\mathscr{D}$-degree g. We denote by $\hat{0} = (0,\ldots,0)$ the $G_\mathscr{D}$-degree of 1. Then $R_d^G = \mathrm{Vect}_K(\mathscr{M}_{d,\hat{0}})$, and $\dim(R_d^G) = |\mathscr{M}_{d,\hat{0}}|$.

Definition 7 *Following definition 6, we define the densities $\delta(R_g)$ and $\delta(R_{d,g})$ for any $g \in \hat{G}$ as*

$$\delta(R_{d,g}) = \frac{\dim(R_{d,g})}{\dim(R_d)} = \frac{|\mathscr{M}_{d,g}|}{|\mathscr{M}_d|} \text{ and } \delta(R_g) = \lim_{D\to+\infty}\frac{\sum_{d=0}^D|\mathscr{M}_{d,g}|}{\sum_{d=0}^D|\mathscr{M}_d|}$$

Theorem 7 *The density $\delta(R_g)$ is well defined and is equal to $1/|G|$. If a set of primary invariants of R^G can be chosen such that their degrees are relatively prime, the density $\delta(R_{d,g})$ has limit $\delta(R^G) = 1/|G|$ as d tends to infinity.*

PROOF. First of all assume that all the sets $\mathscr{M}_g$ are non-empty, and let $m_g \in \mathscr{M}_g$ for all $g \in \hat{G}$. Denote by d_{m_g} its degree. Then $\mathscr{M}_g$ can be written $\mathscr{M}_g = m_g\mathscr{M}_{\hat{0}} \sqcup \{m \in \mathscr{M}_g \mid m_g \nmid m\}$. Therefore, for d big enough, $\mathscr{M}_{d,g} = m_g\mathscr{M}_{d-d_{m_g},\hat{0}} \sqcup \{m \in \mathscr{M}_{d,g} \mid m_g \nmid m\}$. Assuming the condition of the degrees of the primary invariants, we obtain by theorem 6

$$\frac{|\mathscr{M}_{d,g}|}{|\mathscr{M}_d|} = \underbrace{\frac{|\mathscr{M}_{d-d_{m_g},\hat{0}}|}{|\mathscr{M}_{d-d_{m_g}}|}}_{\underset{d\to\infty}{\to}1/|G|}\frac{|\mathscr{M}_{d-d_{m_g}}|}{|\mathscr{M}_d|} + \underbrace{\frac{|\{m \in \mathscr{M}_{d,g} \mid m_g \nmid m\}|}{|\mathscr{M}_d|}}_{\underset{d\to\infty}{\to}0}$$

and the second part of the theorem is proved. In the same way, we conclude by sketching the proof of theorem 6 that

$$\delta(R_g) = \begin{cases} 1/|G| & \text{if } \mathscr{M}_g \neq \emptyset \\ 0 & \text{if } \mathscr{M}_g = \emptyset \end{cases}$$

But by definition, $\sum \delta(R_g) = 1$, so we proved that every set $\mathscr{M}_g$ is non-empty and $\delta(R_g) = 1/|G|$. □

Remark 7 *We have seen that* asymptotically*, the sets $\mathscr{M}_{d,g}$ have roughly the same size (with the assumption on the degrees of the primary invariants) and that the same result holds without assumption on the sets $\cup_{d=0}^D\mathscr{M}_{d,g}$, and the sizes of these sets correspond to the number of columns in the matrices of the abelian-F_5 algorithm, in the homogeneous or affine case. Actually, these sets are very fast evenly distributed, as we will see in section 7. To perform a complexity analysis, we will suppose that this is the case.*

6.2 Application to the complexity of abelian-F_5 and abelian-FGLM algoritms

6.2.1 Abelian-F_5 algorithm

To analyse the efficiency of our algorithm to compute a Gröbner basis of $I_\mathscr{D}$, we have to compare the complexity of the classical F_5 algorithm on I and $I_\mathscr{D}$ and the abelian-F_5 algorithm on $I_\mathscr{D}$. In order to bound the complexity of F_5 we bound the complexity of the so called Macaulay/Lazard algorithm [15], consisting in building a row echelon form of the Macaulay's matrix; this computation can be seen as a redundant variant of the F_5 algorithm. Since the base-change matrix P defined in section 2 induces an isomorphism between the homogenous components of same degree of I and $I_\mathscr{D}$, assuming they are homogeneous, so these ideals have same Hilbert series. Therefore, the index of regularity (homogeneous case) or the degree of regularity (affine case) are the same. For a good introduction to these notions, see [16]. From the Lazard algorithm [15] it is possible to derive a complexity bound of the computation of a Gröbner basis of zero dimensional homogeneous system.

Theorem 8 *[16] Let $\mathbf{F} = (f_1,\ldots,f_m) \in R^m$ be a family of homogeneous polynomials generating a zero-dimensional ideal. The complexity of computing a Gröbner basis for the DRL ordering of the ideal $\langle\mathbf{F}\rangle$ is bounded by*

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

where ω is the constant of linear algebra.

The proof of the previous theorem is obtained by analyzing size and rank of the Macaulay's matrix, and by the fact that a row echelon form of a matrix of size (ℓ,c) and rank r can be computed in times $O(\ell c r^{\omega-2})$. In the case of an ideal $\mathbf{F}$ invariant under a diagonal group $G_{\mathscr{D}}$, we have seen that such a matrix can be slitted into $|G_{\mathscr{D}}|$ parts, and previous analysis of the size of the sets $\mathscr{M}_{d,g}$ in theorem 7 proves that, under parallelization on the computations of row echelon form of the $|G_{\mathscr{D}}|$ submatrices, the following theorem holds:

Theorem 9 *Let $\mathbf{F} = (f_1, \ldots, f_m) \in R^m$ be a family of homogeneous polynomials generating a 0-dimensional ideal, invariant under a diagonal group $G_{\mathscr{D}}$ such that a set of primary invariants of $G_{\mathscr{D}}$ can be chosen with degrees relatively prime. The complexity of computing a Gröbner basis for the DRL ordering of the ideal $\langle \mathbf{F} \rangle$ is bounded by*

$$O\Big(\frac{m}{|G_{\mathscr{D}}|^{\omega}}\binom{n+d_{reg}(\mathbf{F})}{d_{reg}(\mathbf{F})}^{\omega}\Big)$$

Remark 8 *In the affine case, it seems that a bound similar to theorem 8 could be obtained (see [16], page 53), therefore we could obtain a similar improvement than in theorem 9.*

6.2.2 Abelian-FGLM algorithm

Let $I_{\mathscr{D}}$ be a zero-dimensional ideal invariant under the diagonal group $G_{\mathscr{D}}$. We have to consider the two parts of the algorithm to give a complexity estimation : the construction of the multiplication's matrices $M_{i,g}$ and the loop in FGLM. We denote by $\mathbf{Deg}(I_{\mathscr{D}})$ the degree of the ideal $I_{\mathscr{D}}$.

Theorem 10 *Under the hypothesis that the monomials of $\mathscr{E}$ are evenly distributed over the staircases $\mathscr{E}_g$ (which is verified in practice), it is possible to obtain the reduced Gröbner basis $\mathscr{G}_{\preceq_2}$ from $\mathscr{G}_{\preceq_1}$ of $I_{\mathscr{D}}$ with $O(\frac{n}{|G_{\mathscr{D}}|^2}\mathbf{Deg}(I_{\mathscr{D}})^3)$ arithmetics operations in K.*

PROOF. We follow the notations of [10].

• To compute the multiplication matrices, we have to compute the normal forms $NF(m, \mathscr{G}_{\preceq_1})$ for all $m \in B(\mathscr{G}_{\preceq_1}) \cup M(\mathscr{G}_{\preceq_1})$. For at most $n\mathbf{Deg}(I_{\mathscr{D}})$ of these monomials, arithmetic computations are needed and since the staircases $\mathscr{E}_g$ have size about $\mathbf{Deg}(I_{\mathscr{D}})/G_{\mathscr{D}}$, each of these normal forms can be computed with $O((\frac{\mathbf{Deg}(I_{\mathscr{D}})}{|G_{\mathscr{D}}|})^2)$ arithmetic operations in K.

• In the same way, the loop in the FGLM algorithm presented in section 5 has to be done at most $n\mathbf{Deg}(I_{\mathscr{D}})$ times. The cost of the linear operations was $O(\mathbf{Deg}(I_{\mathscr{D}})^2)$ in the original FGLM algorithm [10] but it is reduced to $O(\mathbf{Deg}(I_{\mathscr{D}})^2/|G_{\mathscr{D}}|^2)$ here since the square matrices have a number of lines and columns divided by about $|G_{\mathscr{D}}|$. □

6.3 Polynomial complexity

Suppose that $g_1, \ldots, g_m$ are affine polynomials of R of degree 2, which are individually invariant under the cyclic-n group. Usually, computing a Gröbner basis of $I = \langle g_1, \ldots, g_m \rangle$ is exponential, but we will see that we can obtain a Gröbner basis of $I_{\mathscr{D}}$ in polynomial time in n and m. With $P = (\xi^{ij})$, and $f_i = g_i^P$, each f_i is invariant under $D_\sigma = diag(\xi, \xi^2, \ldots, \xi^{n-1}, 1)$ and f_i has $G_{\mathscr{D}}$-degree 0.

Lemma 2 *The support of each f_i is contained in $\{1, x_n, x_n^2\} \cup \{x_i x_{n-i}, \mid 1 \le i \le \lfloor (n-1)/2 \rfloor\}$.*

PROOF. Each x_i has $G_{\mathscr{D}}$-degree i mod n, so $\deg_{G_{\mathscr{D}}}(x_i x_j) = i + j \bmod n$, and the only monomials of degree 2 having $G_{\mathscr{D}}$-degree 0 are $x_i x_{n-i}$. The only monomial of degree 1 and $G_{\mathscr{D}}$-degree 0 is x_n, and 1 is also of $G_{\mathscr{D}}$-degree 0. □

Theorem 11 *A Gröbner Basis for every monomial ordering of a system of m equations invariant under $D_\sigma = diag(\xi, \ldots, \xi^{n-1}, 1)$ can be computed in polynomial time in $n+m$.*

PROOF. We set $y_i = x_i x_{n-i}$ for each $i \in \{0, \ldots, \lfloor (n-1)/2 \rfloor\}$ to linearize the equations, and perform a Gauss elimination on the equations. The result is a Gröbner Basis since the leading monomials of any pair of the obtained polynomials are coprime. The matrix we have to reduce has m lines and $\lfloor (n+5)/2 \rfloor$ columns, and the complexity is polynomial in $n+m$. □

Remark 9 *Similar results can be obtained for other groups and systems. This will be discussed in an extended version of this paper.*

7. EXPERIMENTS

In this section, we report some experiments that show the improvements given by our approach on the computation of Gröbner bases of ideals invariant under a commutative group. We first present sizes of the sets $\mathscr{M}_{d,g}$ and $\mathscr{E}_g$, and then give timings obtained with an implantation of the algorithm Abelian-F_4. A web page has been made for other softwares and benchmarks, see [8].

7.1 Sizes of the sets $\mathscr{M}_g$ or $\mathscr{E}_g$

In this subsection, we suppose that G is the cyclic group generated by the matrix M_σ presented in example 1. Therefore $G_{\mathscr{D}}$ is the group generated by the diagonal matrix with diagonal coefficients $(\xi, \xi^2, \ldots, \xi^{n-1}, 1)$. We want to compare the size of $\mathscr{M}_{d,g}$ with $|\mathscr{M}_d|/n$ (recall that n is the order of $G_{\mathscr{D}}$). To this end we compute the relative standard deviation of the sets $|\mathscr{M}_{d,g}|$ to $|\mathscr{M}_d|/n$, for several n and d. The formula is $\sigma_{d,n} = \frac{\sqrt{\frac{1}{n}\sum_{g \in G_{\mathscr{D}}}(|\mathscr{M}_{d,g}| - |\mathscr{M}_d|/n)^2}}{|\mathscr{M}_d|/n}$. The following table presents some values of $\sigma_{d,n}$. We see that the monomials are very fast evenly distributed over $g \in \hat{G}$. In the same way,

d/n	2	3	4	5	10	15
3	0.00	0.14	0.00	0.09	0.00	0.01
4	0.20	0.00	0.10	0.09	0.02	0.01
5	0.00	0.09	0.00	0.02	0.00	0.00
10	0.09	0.00	0.02	0.00	0.00	0.00

Table 1: Repartition of the monomials under $G_{\mathscr{D}}$

the stairs $\mathscr{E}_g$ that appear in the abelian-FGLM algorithm have about same size. Table 2 presents some zero dimensional ideals together with the size of the group and the size of the stairs. The final column is the relative standard deviation between $|\mathscr{E}_g|$ and $|\mathscr{E}|/|G_{\mathscr{D}}|$.

n	$\lvert\mathscr{E}\rvert$	$\lvert G_{\mathscr{D}}\rvert$	$\lvert\mathscr{E}_g\rvert/\lvert G_{\mathscr{D}}\rvert$	Max $\lvert\mathscr{E}_g\rvert$	$\sigma_{\mathscr{E}}$
5	70	25	2.80	6	0.286
6	156	36	4.33	6	0.133
7	924	49	18.86	24	0.045
10	34940	100	349.40	354	0.0043
11	184756	121	1526.91	1536	0.00060

Table 2: Cyclic-n: Repartition of the monomials into $\mathscr{E}_g$

From the experimental side, applying the F_4 algorithm on the cyclic 9 problem we obtain, in degree 15, a matrix of size 72558×93917; applying the abelian-F_4 algorithm we obtain 9 independent matrices of roughly the same size: $8340 \times 10703, 8180 \times 10544$, 8122×10484, $7804 \times 10171, 7993 \times 10358, 8042 \times 10404, 7796 \times 10162$, 7967×10369 and 8314×10722.

7.2 Abelian-F_4 implementation

A first implementation of the Abelian-F_4-algorithm [4] has been made. The algorithm constructs $|G_{\mathscr{D}}|$ matrices at each degree, using the usual strategy of F_4. Notice that only the construction of the matrices and the operations of row-reduction on them have been parallelized, the handle of the list of critical pairs is still sequential. Surprisingly, the linear algebra can sometimes be so accelerated that this handling can become the most time-consuming part whereas it is usually negligible. Therefore we report in the following tables two timings or ratios in each column: the timings are related to $F_4^{A,n}$, which is the new abelian algorithm parallelized on n cores. The first one is the total timing and the second one is only the parallelized part (that is to say, building the matrices and the linear algebra parts). The other columns contain the ratios between

F_4^A or F_4 and $F_4^{A,n}$. F_4 means the standard F_4 applied on I and F_4^A the standard F_4 applied on $I_{\mathscr{D}}$. F_4^M is the F_4 of Magma, and there is only the ratio for the total timing. In each case except table 7, the group G acting on I is the cyclic group C_n generated by the matrix M_σ defined in example 1, and $G_{\mathscr{D}}$ is the group generated by the diagonal matrix $\mathrm{diag}(\xi,\xi^2,\ldots,1)$. Notice that we have to reach big-sized problems to have a significant impact. In table 3, we consider n randomized equations of degree 3 stable under C_n, which give rise to equations of $G_{\mathscr{D}}$-degree 0 in $I_{\mathscr{D}}$. Table 4 presents n equations of degree 2, half of these equations in $I_{\mathscr{D}}$ are of $G_{\mathscr{D}}$-degree 0, and half of $G_{\mathscr{D}}$-degree 1. In this case, the computation on $I_{\mathscr{D}}$ becomes polynomial in n and the handling of the critical pairs is the most time-consuming part. All computations have been made on a computer with 4 Intel(R) Xeon(R) CPU E5-4620 0 @ 2.20GHz with 387 GB of RAM, on a field where $X^{|G|}-1$ fully splits (most of the time $\mathbb{F}_{65521}$), according to remark 5.

n	$F_4^{A,n}$ total; // part	$F_4^A/F_4^{A,n}$ tot;p.p	$F_4/F_4^{A,n}$ tot;p.p	$F_4^{\mathrm{M}}/F_4^{A,n}$ tot
8	3.46s;2.48s	2.2;2.7	33.0;45.4	22
9	77.04s;64.21s	7.3;8.6	67.8;81.0	50
10	762s;672s	10.0;11.3	160.9;182.1	134
11	22162s;20425s	13.0;14.0	∞	∞

Table 3: n cubic equations of $G_{\mathscr{D}}$-degree 0

n	$F_4^{A,n}$ total; // part	$F_4^A/F_4^{A,n}$ tot;p.p	$F_4/F_4^{A,n}$ tot;p.p
25	0.25s;0.06s	1.9;4.5	56.60;230.0
30	0.58s;0.11s	1.5;4.6	80.79;415.1
35	0.86s;0.11s	1.9;8.5	228.5;1755
40	1.55s;0.21s	2.0;8.5	300.6;2174
50	3.96s;0.45s	2.6;13.3	753.8;6504
60	10.85s;0.96s	2.8;17.2	1294;14330

Table 4: n quadratic equations of $G_{\mathscr{D}}$-degree 0 or 1

Table 5 presents equations coming from a cryptographic application : the cryptosystem NTRU [14]. The underlying problem is the following: given $h \in \mathbb{F}_p[x]$, we are looking for a polynomial $f \in \mathbb{F}_p[x]$ of degree $n-1$ and coefficients in $\{0,1\}$ such that $g = fh \bmod x^n - 1$ has also its coefficients in $\{0,1\}$. Denote $f = \sum_{i=0}^{n-1} f_i x^i$ and $g = \sum_{i=0}^{n-1} g_i x^i$, then the g_i's are linear forms in the f_i's verifying $g_i^{M_\sigma} = g_{\sigma(i)}$. Since the conditions of f_i and g_i to be in $\{0,1\}$ can be written $f_i^2 - f_i = g_i^2 - g_i = 0$, the system consists of $2n$ quadratic equations in the f_i's generating an ideal globally stable under the action of C_n. The speed-up between F_4 and $F_4^{A,n}$ is roughly 250 with 24 variables, and the use of $F_4^{A,n}$ has a significant impact since we can achieve bigger problems. In this case the handling of the critical pairs is also the most time-consuming part.

n	$F_4^{A,n}$ total; // part	$F_4^A/F_4^{A,n}$ tot;p.p	$F_4/F_4^{A,n}$ tot;p.p
21	4.52s;1.21s	4.0;11.9	90.15;334.0
23	11.16s;1.87s	3.3;17.2	115.2;686.1
24	128s;14.3s	5.2;36.5	241.1;2149.
25	218s;31.0s	5.8;32.5	∞
28	1214s;192s	7.1;36.1	∞

Table 5: NTRU equations

Table 6 presents timings on the Cyclic-n problem, we see that Cyclic-11 could be solved in less than 8 hours although it is untractable with F_4. Table 7 is an example of ideals generating by random polynomials of degree 3 invariant under the group $C_{k_1} \times C_{k_2}$, each subgroup C_k acting on k variables. We see that the algorithm is more efficient where $k_1 = k_2$, which makes sense since the size of the group is $k_1 k_2$.

Acknowledgments. This work was supported in part by the HPAC grant (ANR ANR-11-BS02-013) and by the EXACTA grant (ANR-09-BLAN-0371-01) of the French National Research Agency.

n	$F_4^{A,n}$ total; // part	$F_4^A/F_4^{A,n}$ tot;p.p	$F_4/F_4^{A,n}$ tot;p.p	$F_4^{\mathrm{M}}/F_4^{A,n}$ tot
8	0.50s;0.40s	2.5;2.7	7.8;9.3	6.0
9	10.21s;7.71s	4.3;5.4	37.0;48.4	30.5
10	334s;290s	13.2;14.8	411.0;472.3	207
11	27539s;25454s	∞	∞	∞

Table 6: The Cyclic-n problem

k_1,k_2	F_4^{A,k_1k_2} tot; // p.p	$F_4^A/F_4^{A,k_1k_2}$ tot;p.p	$F_4/F_4^{A,k_1k_2}$ tot;p.p	$F_4^{\mathrm{M}}/F_4^{A,k_1k_2}$ tot
4,4	2.0s;1.3s	2.4;3.2	61.8;94.6	37
6,2	2.9s;2.4s	2.2;2.5	76.4;91.4	44
5,5	70s;43s	11.8;16.2	∞	∞
6,4	92s;76s	17.7;19.8	∞	∞
8,2	107s;100s	12.1;12.3	∞	∞

Table 7: $n = k_1 + k_2$ cubic equations invariant under $C_{k_1} \times C_{k_2}$

8. REFERENCES

[1] B. Buchberger. Bruno buchberger's phd thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. *Journal of Symbolic Computation*, 41(3-4):475 – 511, 2006. Logic, Mathematics and Computer Science: Interactions in honor of Bruno Buchberger (60th birthday).

[2] A. Colin. Solving a system of algebraic equations with symmetries. *J. Pure Appl. Algebra*, 117/118:195–215, 1997. Algorithms for algebra (Eindhoven, 1996).

[3] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, New York, third edition, 2007. An introduction to computational algebraic geometry and commutative algebra.

[4] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases (F4). *Journal of Pure and Applied Algebra*, 139(1–3):61–88, June 1999.

[5] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In *Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, ISSAC '02, pages 75–83, New York, NY, USA, 2002. ACM.

[6] J.-C. Faugère, M. Hering, and J. Phan. The membrane inclusions curvature equations. *Advances in Applied Mathematics*, 31(4):643–658, June 2003.

[7] J.-C. Faugère and S. Rahmany. Solving systems of polynomial equations with symmetries using SAGBI-Gröbner bases. In *ISSAC '09: Proceedings of the 2009 international symposium on Symbolic and algebraic computation*, ISSAC '09, pages 151–158, New York, NY, USA, 2009. ACM.

[8] J.-C. Faugère and J. Svartz. Software and benchmarks. http://www-polsys.lip6.fr/~jcf/Software/benchssym.html.

[9] J.-C. Faugère and J. Svartz. Solving polynomial systems globally invariant under an action of the symmetric group and application to the equilibria of n vortices in the plane. In *ISSAC '12: Proceedings of the 2012 International Symposium on Symbolic and Algebraic Computation*, ISSAC '12, pages 170–178, New York, NY, USA, 2012. ACM. accepted.

[10] J.C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering. *Journal of Symbolic Computation*, 16(4):329–344, 1993.

[11] P. Flajolet and R. Sedgewick. *Analytic combinatorics*. Cambridge University Press, 2009.

[12] G. Björck. Functions of modulus 1 on Zn , whose Fourier transforms have constant modulus, and "cyclic n-roots". *NATO, Adv. Sci. Inst. Ser. C, Math. Phys. Sci.*, 315:131–140, 1990. Recent Advances in Fourier Analysis and its applica tions.

[13] K. Gatemann. Symbolic solution polynomial equation systems with symmetry. In *Proceedings of the international symposium on Symbolic and algebraic computation*, ISSAC '90, pages 112–119, New York, NY, USA, 1990. ACM.

[14] J. Hoffstein, J. Pipher, and J.H. Silverman. Ntru: a ring-based public key cryptosystem. In *Algorithmic number theory (Portland, OR, 1998)*, volume 1423 of *Lecture Notes in Comput. Sci.*, pages 267–288. Springer, Berlin, 1998.

[15] D. Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In *Computer Algebra, EUROCAL'83*, volume 162 of *LNCS*, pages 146–156. Springer, 1983.

[16] P-J. Spaenlehauer. *Solving multi-homogeneous and determinantal systems. Algorithms - Complexity - Applications.* PhD thesis, Université Paris 6, 2012.

[17] R. P. Stanley. Invariants of finite groups and their applications to combinatorics. *Bull. Amer. Math. Soc. (new series)*, 1:475–511, 1979.

[18] S. Steidel. Gröbner bases of symmetric ideals. *Journal of Symbolic Computation*, 54(0):72 – 86, 2013.

[19] B. Sturmfels. *Algorithms in Invariant Theory*. Texts and Monographs in Symbolic Computation. SpringerWienNewYork, Vienna, second edition, 2008.