Solving Systems of Polynomial Equations with Symmetries Using SAGBI-Gröbner Bases

Version: July 2, 2009

Jean-Charles Faugère
Jean-Charles.Faugere@inria.fr

Sajjad Rahmany
Sajjad.RAHMANY@lip6.fr

SALSA Project INRIA, Centre Paris-Rocquencourt
UPMC, Univ Paris 06, LIP6
CNRS, UMR 7606, LIP6
UFR Ingénierie 919, LIP6 Passy Kennedy
Boite Courrier 169, 4, Place Jussieu 75252 Paris Cedex 05

ABSTRACT

In this paper, we propose an efficient method to solve polynomial systems whose equations are left invariant by the action of a finite group G. The idea is to simultaneously compute a truncated SAGBI-Gröbner bases (a generalisation of Gröbner bases to ideals of subalgebras of polynomial ring) and a Gröbner basis in the invariant ring $\mathbb{K}[\sigma_1,\ldots,\sigma_n]$ where σ_i is the i-th elementary symmetric polynomial.

To this end, we provide two algorithms: first, from the F_5 algorithm we can derive an efficient and easy to implement algorithm for computing truncated SAGBI–Gröbner bases of the ideals in invariant rings. A first implementation of this algorithm in C enable us to estimate the practical efficiency: for instance, it takes only 92s to compute a SAGBI basis of Cyclic 9 modulo a small prime. The second algorithm is inspired by the FGLM algorithm: from a truncated SAGBI–Gröbner basis of a zero-dimensional ideal we can compute efficiently a Gröbner basis in some invariant rings $\mathbb{K}[h_1,\ldots,h_n]$. Finally, we will show how this two algorithms can be combined to *find the complex roots of* such invariant polynomial systems.

Categories and Subject Descriptors: I.1.2 SYMBOLIC AND ALGEBRAIC MANIPULATION Algorithms Algebraic algorithms

General Terms: Algorithms, Performance, Reliability

Keywords: Gröbner basis, Symmetric Polynomials, SAGBI-Gröbner, Algorithm $F5$, $FGLM$, Invariant ring

1. INTRODUCTION

Solving polynomial equations is a fundamental problem in Computer Algebra; an important subproblem is to solve polynomial systems having some symmetries (for instance when the associated algebraic variety is invariant under the action of some finite group). Several problems can be modeled by such system having this property: for instance the well known cyclic n problem [3] or in Cryptography the NTRU cryptosystem system[14] leads to a system which is invariant by the cyclic group. To the best of our knowledge, it is an open issue how to solve *efficiently* such systems using *exact methods*. In this paper, we consider a yet more restricted problem, namely the problem of finding the zeros of an ideal $I = \langle f_1,\ldots,f_m\rangle \subset \mathbb{K}[x_1,\ldots,x_n]$ such that each f_i is invariant by the action of a finite group G not equal to the symmetric group $\mathfrak{S}_n$.

Of course, for such systems it is always possible to compute a Gröbner basis but this is unsatisfactory because symmetries of the initial system are destroyed during the computation and the number of solutions is a multiple of $|G|$. In [1], Colin proposed to use invariants [4] to reformulate the problem; according to our experience, this method is not always optimal since it is difficult, in practice, to compute the primary and secondary invariants (including the algebraic relations between them); moreover the resulting systems (depending only on the invariants) are, very often, more difficult to solve than the original ones.

The idea presented in this paper is to compute a Gröbner basis in some invariant ring $\mathbb{K}[\sigma_1,\ldots,\sigma_n]$ where σ_i is the i-th elementary symmetric polynomial. To this end, we show that we can use a slightly modified version (algorithm 2) of the FGLM algorithm [11]. To apply the FGLM algorithm we need a normalForm function (in fact an invariant version of the normalForm); such a function can be obtained from the knowledge of a SAGBI-Gröbner basis (abbreviated by SG-basis). Therefore, the main goal of this paper is to describe a new efficient algorithm (algorithm 1) for computing SAGBI-Gröbner basis: we call this algorithm the F_5-invariant algorithm since it an adaptation of the F_5 algorithm [10]. A technical difficulty arise from the fact that, in general, SAGBI-Gröbner are not finite; to overcome this problem we have to apply *simultaneously truncated* version of the F_5-invariant and FGLM-invariant algorithms until we find the (finite) invariant Gröbner basis in $\mathbb{K}[\sigma_1,\ldots,\sigma_n]$. It is important to point out that the size of this Gröbner basis in $\mathbb{K}[\sigma_1,\ldots,\sigma_n]$ is much smaller than the corresponding Gröbner basis in $\mathbb{K}[x_1,\ldots,x_n]$ w.r.t all parameters: number of polynomials, size of the coefficients, number of solutions (an example of such a behavior is given in example 4).

A first implementation of our algorithms has been made in the Maple 12 Computer Algebra system and have been

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
ISSAC'09, July 28–31, 2009, Seoul, Republic of Korea.
Copyright 2009 ACM 978-1-60558-609-0/09/07 ...$5.00.

successfully tried on a number of examples; As reported in section 3.5, a low level implementation (in C) of the new F_5-invariant algorithm enable us to demonstrate the effectiveness of the method.

The paper is organized as follows. In section 2, we will give some basic definitions of invariants rings, we introduce the notion of Sagbi Gröbner bases and the definition of Gröbner basis in invariant rings. In Section 3, we concentrate on our first main goal: we will give an equivalent of the F_5 criterion in the invariant case (proposition 4) and we describe the algorithm for computing SG-basis for ideals in invariant rings of finite matrix groups (algorithm 1). Section 4 provides a FGLM like algorithm for converting a SG-basis into a Gröbner basis. As an application of our algorithms, we will describe in section 5 a general method to compute all the solutions of polynomial equations which are left invariant by the action of a finite group G; we conclude this section by an application to the cyclic n problem.

2. SAGBI-GRÖBNER BASES AND GRÖBNER BASES IN INVARIANT RING.

This section may be skipped by readers familiar with elementary (SAGBI) Gröbner bases theory.

2.1 Frequently used notation

In this paper, we suppose that $\mathbb{K}$ is a field of characteristic zero or p such that $|G|$ and p are coprimes; $R = \mathbb{K}[x_1, \ldots, x_n]$ is the ring of polynomials and we fix an admissible monomial order $\prec$ (only well-orderings of the monomials are considered; for a precise definition of a monomial ordering on R we refer to [8] p. 53). For a polynomial $f \in R$, we denote by $LM_\prec(f)$ (resp. $LT_\prec(f)$ and $LC_\prec(f)$ the leading monomial (resp. the leading term and the leading coefficient) of f with respect to $\prec$. We denote by T, the set of all terms of $x_1, \ldots, x_n$ and by $T(f)$ the set of all terms of f. By extension, for any set F of polynomials, we define $LM_\prec(F) = \{LM_\prec(p) \mid p \in F\}$ and $LT_\prec(F) = \{LT_\prec(p) \mid p \in F\}$.

2.2 Invariants rings

This subsection describes the basic properties of the invariant rings. Let G be a subgroup of $n \times n$ invertible matrices with entries in the field $\mathbb{K}$. We use the notation X, for column vector of the variables $x_1, \ldots, x_n$. A polynomial $f \in R$ is called an *invariant polynomial* if $f(A.X) = f(X)$ for all $A \in G$. The *invariant ring* R^G of G is the set of all invariant polynomials.

EXAMPLE 1. *Consider the cyclic matrix group G generated by matrix $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Clearly, $f = x_1^2 + x_2^2$ is invariant while $g = x_1x_2$ is not invariant, because $g(A.X) \neq g(X)$.*

Even if R^G is not finite dimensional as a $\mathbb{K}$ vector space, we have a decomposition of R^G into its homogeneous components, which are finite dimensional. This decomposition is similar to the decomposition of R. Let R_d denote the vector space of all homogeneous polynomials of degree d, then we have $R = \bigoplus_{d \geq 0} R_d$. The monomials of degree d form a vector space basis of R_d. Now, observe that the action of G preserves the homogeneous components. Hence we obtain also a decomposition of the invariant ring $R^G = \bigoplus_{d \geq 0} R_d^G$. The following Reynolds operator can be used to compute a vector space basis of R^G .

DEFINITION 1. *Let G be a finite group. The* Reynolds operator *of G is the map $\Re : R \longrightarrow R^G$ defined by $\Re_G(f) = \Re(f) = \dfrac{1}{\mid G \mid}\sum_{\sigma \in G} f(\sigma.X)$ for $f \in R$.*

We recall the following properties of the Reynolds operator:

PROPOSITION 1. *([8]) Let $\Re$ be the Reynolds operator of the finite matrix group G.*
(i) $\Re$ *is $\mathbb{K}$-linear.*
(ii) *If $f \in R$, then $\Re(f) \in R^G$.*
(iii) *If $f \in R^G$, then $\Re(f) = f$.*

It is easy to prove that, for any term t the Reynolds operator gives us a homogeneous invariant $\Re(t)$. Such invariants are called *orbit sums*. The set of orbit sums is a vector space basis of R^G, so any invariant can be uniquely written as a linear combination of orbit sums. Now, we give a special representation of invariant polynomials which is used in the next section. For this, we introduce the following terminology.

DEFINITION 2. *A term in LT(R^G) is called an* initial term. *We denote by $\mathcal{T}$ the set of all initial terms.*

LEMMA 1. *Every $f \in R^G$ can be written uniquely as $f = \sum_\alpha c_\alpha \Re(m_\alpha^*)$, where $c_\alpha \in \mathbb{K}$ and m_α^* are initial monomials.*

PROOF. from proposition 1 and definition 2. ☐

In the rest of this paper, we suppose that all representations of invariant polynomials are always in the above form.

2.3 Symmetric Polynomials

Now that we have the definition of invariant polynomial, we can look at the most familiar example of invariant polynomials which called symmetric polynomials.

DEFINITION 3. *A polynomial $f \in R$ is said to be symmetric if it is invariant under the symmetric group $\mathfrak{S}_n$.*

The coefficients of the polynomial $f(z) = (z + x_1) \cdots (z + x_n) = z^n + \sigma_1 z^{n-1} + \ldots + \sigma_n$ with respect to new the variable z are the so called *elementary symmetric polynomials* : $\sigma_1 = x_1 + x_2 + \ldots + x_n, \sigma_2 = x_1x_2 + \ldots + x_{n-1}x_n, \cdots, \sigma_n = x_1 \ldots x_n$. From the elementary symmetric polynomials, we can construct other symmetric polynomials by taking polynomials in $\sigma_1, \ldots, \sigma_n$. This lead us to the well known theorem.

THEOREM 1. *(*Fundamental Theorem of Symmetric polynomials*) Every symmetric polynomial in R can be written uniquely as a polynomial in the elementary symmetric polynomials $\sigma_1, \ldots, \sigma_n$.*

An obvious consequence of the above theorem is that $\mathbb{K}[x_1, \ldots, x_n]^{\mathfrak{S}_n} = \mathbb{K}[\sigma_1, \ldots, \sigma_n]$.

2.4 SAGBI Gröbner basis in Invariant rings

In this subsection, we recall the definition of SG-basis which is an analog of Gröbner basis for ideals in k-subalgebras [12]. Then, we will present basic properties of SG-basis in invariant rings. For the sake of simplicity, we assume that all the *polynomials are homogeneous*. Let $f_1 \ldots, f_m$ be invariant polynomials and I (resp. I^G) represent the ideal generates by $f_1 \ldots, f_m$ in R (resp. R^G)

DEFINITION 4. *[16, 15] A subset $F \subseteq I^G$ is a* SAGBI Gröbner basis (SG-basis) *of I^G if $LT(F)$ generates the initial ideal $\langle LT(I^G)\rangle$ as an ideal over the algebra $\langle LT(R^G)\rangle$. It is called a* partial *SG-basis up to degree D of I^G if $LT(F)$ generates $\langle LT(I^G)\rangle$ up to degree D.*

REMARK 1. *In contrast with ordinary Gröbner basis theory, a SG-basis is not necessarily finite.*

We continue by describing an equivalent of the reduction in R^G.

DEFINITION 5. *Let $f, g, p \in R^G$ with $f, p \neq 0$ and let P be a finite subset of R^G. Then we say that*

$i)$ f SG-reduces *to g modulo p, if $\exists t \in T(f), \exists s \in LM(R^G)$ such that $s.LT(p) = t$ and $g = f - (\frac{a}{Lc(p).Lc(\Re(s))}).\Re_G(s).p$ where a is the coefficient of t in f.*

$ii)$ *f SG-reduces to g modulo P, if f SG-reduces to g modulo p for some $p \in P$.*

From this we obtain straightforwardly the definition of the following concept: SG-reducible *and* SG-NormalForm.

Basic properties of SG-basis are presented in [17, 16, 15]. For the sake of completeness, we will review some of the standard fact on SG-bases.

PROPOSITION 2. *For a subset F of an ideal $I^G \subseteq R^G$ the following properties are equivalent :*
$a)$ F is a SG-basis for I^G.
$b)$ For every $h \in I^G$, SG-NormalForm$(h, F) = 0$.

COROLLARY 1. *A SG-basis for I^G generates I^G as an ideal of R^G.*

It is easy to show that the proposition above continues to hold if we restrict our discussion to SG-basis up to some degree D. Hence, if a SG-basis up to degree D of I^G has already been computed, then this is enough to test the membership in I^G for any polynomial f with $\deg(f) \leq D$.

Now, suppose in addition that $dim(I) = 0$. It is known that $A = R/I$ is a finite $\mathbb{K}$ vector space and that the set $B = \{x^\alpha \mid x^\alpha \notin \langle \mathrm{LT}(I)\rangle\}$ form a basis of A (more precisely, their cosets form a basis). We can obtain the same result for the vector space $A^G = R^G/I^G$. For this, we consider the map

$$\phi \begin{pmatrix} R^G & \longrightarrow & R/I \\ f & \longmapsto & f + I \end{pmatrix}$$

We claim that $\ker(\phi) = I^G$. Clearly I^G lies in the kernel. Conversely, an element f in the kernel has the form $f = h_1 f_1 + \ldots + h_n f_m$ and applying the Reynolds operator $\Re$ yields $f = \Re(f) = \Re(h_1) f_1 + \ldots + \Re(h_n) f_m \in I^G$.

Therefore we have an embedding $R^G/I^G \hookrightarrow R/I$ and conclude that the vector space A^G is of finite dimension. Furthermore, the set $\{\Re(x^\alpha) \mid x^\alpha \notin \langle LT(I^G)\rangle\}$ is a basis of A^G.

REMARK 2. *A term t of $< LT(R^G) >$ is standard if $t \notin < LT(I^G) >$. Orbit sums of a standard term t is called a* standard invariant. *R^G is the direct sum of I^G of the vector space spanned by the standard invariants. Hence, SG-NormalForm of an invariant f, is necessarily a unique linear combination of standard invariants.*

2.5 Gröbner bases in invariant ring.

We introduce the definition and the associated notions of Gröbner basis in some invariant ring. First, we will introduce the notion of invariancy in algebraic geometry. Let $G \subset \mathfrak{S}_n$ be a finite group.

DEFINITION 6. *The orbit of a point $\boldsymbol{a} = (\boldsymbol{a_1}, \ldots, \boldsymbol{a_n}) \in \mathbb{K}^n$ is the set $\{g.\boldsymbol{a} = (a_{g(1)}, \ldots, a_{g(n)}) \mid g \in G\}$, and is called the G-*orbit *of $\boldsymbol{a}$.*

Note that the group G can act on an affine space $\mathbb{K}^n$ just as easily as it can act on a polynomial ring R. This notion leads to our next definition.

DEFINITION 7. *The set of all G-orbits in $\mathbb{K}^n$ is denoted $\mathbb{K}^n/G$ and called the* orbit space *of G.*

Let $F = \{f_1, \ldots, f_s\}$ be a set of polynomials which are invariant under the action of the group G. Then, the ideal $I =< F >$ is a set which is invariant under the action of G on R, and its variety $\mathbb{V}(F) = \mathbb{V}(I)$ is invariant under the action of G on $\mathbb{K}^n$. If we compute a Gröbner basis to obtain $\mathbb{V}(I)$ from I, we start with a symmetric set but we obtain a Gröbner basis containing asymmetric polynomials, and we are faced with the task of restoring the symmetry, by using the asymmetric set to compute the symmetric variety $\mathbb{V}(I)$. We need the following definition.

DEFINITION 8. *If the variety $\mathbb{V}(I)$ is invariant under the action of finite group G, we define the* relative orbit variety *$\mathbb{V}(I)/G$, whose points are the G-orbits of zeroes of I.*

Intuitively the idea is to compute a Gröbner basis associated with the relative orbit variety $\mathbb{V}(I)/G$ instead of a Gröbner basis of $\mathbb{V}(I)$ itself. It is easy to reconstruct the properties of $\mathbb{V}(I)$ from $\mathbb{V}(I)/G$.

A famous theorem of Hilbert state that R^G is finitely generated. So there exists a finite set of polynomials $\{h_1, \ldots, h_r\}$ such that $R^G = \mathbb{K}[h_1, \ldots, h_r]$. According to this point of view, we can introduce following definition.

DEFINITION 9. *Let $h_1, \ldots, h_r$ be some polynomials which are invariants by the action of the finite group G. Let I be an ideal generated by invariant polynomials. We introduce r new variables $H_1, \ldots, H_r$ and we consider in $\mathbb{K}[x_1, \ldots, x_n, H_1, \ldots, H_r]$ the following ideal:*

$$J = I + \langle H_1 - h_1(x_1, \ldots, x_N), \ldots, H_r - h_r(x_1, \ldots, x_N)\rangle$$

Then, by definition,a Gröbner basis of $J \cap \mathbb{K}[H_1, \ldots, H_r]$ is an invariant Gröbner basis of I in the invariant ring $\mathbb{K}[h_1, \ldots, h_r]$. We denote by $G_{\mathbb{K}[h_1,\ldots,h_r]^G}(I, \prec)$ this basis.

REMARK 3. *In practice, we will choose a weighted monomial ordering in $\mathbb{K}[x_1, \ldots, x_n, H_1, \ldots, H_r]$ with weights $(1, \ldots, 1, \deg(h_1), \ldots, \deg(h_r))$.*

PROPOSITION 3. *An invariant Gröbner basis in the invariant ring $\mathbb{K}[h_1, \ldots, h_r]$ is always finite.*

PROOF. This is obvious from the fact that the invariant Gröbner basis is a Gröbner basis of $J \cap \mathbb{K}[H_1, \ldots, H_r]$. $\square$

REMARK 4. *It is easy to compute an invariant Gröbner basis in the invariant ring $\mathbb{K}[h_1, \ldots, h_r]$ using elimination theory but in that case we have to deal with non symmetric intermediate objects; the goal of the paper is to compute this invariant Gröbner basis without loosing the symmetries.*

REMARK 5. *An important particular case is the following: we consider the symmetric group $\mathfrak{S}_n$ and the invariant ring $\mathbb{K}[x_1,\ldots,x_n]^{\mathfrak{S}_n} = \mathbb{K}[\sigma_1,\ldots,\sigma_n]$ then $G_{\mathbb{K}[\sigma_1,\ldots,\sigma_n]^{\mathfrak{S}_n}}(I,\prec)$ is a symmetric invariant Gröbner basis of an ideal I.*

3. F5-INVARIANT ALGORITHM

In [18], Thiéry give a variant of the Buchberger's algorithm to compute SG-basis up to some degree D of invariant rings of permutation groups. Also, he provided a Buchberger-like criterion to skip the computation of unnecessary S-pairs. Although this criteria avoid many reductions to zero, still many useless pairs remain undetected. Our aim, in this section, is to give a new practical algorithm and a criteria to avoid useless computations.

3.1 Macaulay and F_5-INVARIANT matrices

The following definition is an obvious generalization of Macaulay's matrix in invariant rings:

DEFINITION 10 (MACAULAY'S MATRIX INVARIANT). *Let $f_1,\ldots,f_t$ be homogeneous invariant polynomials with $\deg(f_i) = d_i$ and $d_1 \le \ldots \le d_m$. The Macaulay's matrix invariant $f_1,\ldots,f_m$ of degree d is the matrix whose rows are all the products $\Re(t).f_i$ where t is an initial term of degree $d-d_i$ and the columns are indexed by all initial monomials of degree d (sorted by $\preceq$).*

We will use the symbol $M_{d,m}$ to denote the Macaulay's matrix invariant.

$$M_{d,i} = \begin{array}{c} \\ \Re(t_1).f_1 \\ \vdots \\ \\ \Re(t_i).f_j \\ \vdots \\ \\ \Re(t_l).f_i \end{array} \begin{array}{c} \begin{array}{cccc} \Re(\tilde m_1) & \Re(\tilde m_2) & \ldots & \Re(\tilde m_k) \end{array} \\ \left(\begin{array}{cccc} \cdots & \cdots & \cdots & \cdots \\ & & & \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ & & & \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{array}\right) \end{array}$$

We will present in subsection 3.3 a matrix version of the algorithm F_5 [10] for computing SG-basis.

Similarly to [9] we consider matrix representations of all the polynomials encountered during the F_5 algorithm, and it is convenient to view a matrix $M = (M_{s,t})$ as a map

$$(s,t) \in S \times T' \longrightarrow M_{s,t} \in \mathbb{K}$$

where S is a finite subset of $\mathbb{N}$ and T' a finite subset of $\mathcal{T}$ ordered using a graded ordering. A row indexed by $s = (i,m')$ will be used to label the polynomial $\Re(m').f_i$ or any combination with smaller polynomials: $\Re(m').f_i + \sum_{t\prec m}\Re(t).f_i + \sum_{j<i}\Re(h_j).f_j$. Hence, a row in the matrix $(M_{s,t})$ is specified by its index s, and we identify the vector Row(M,s)=[M$_{s,t}|t \in T$] and the polynomial $\sum_{t\in\mathcal{T}} M_{s,t}.\Re(t)$; the leading term of a row is the leading term the corresponding polynomial. We fix the following notation: Rows$(M) = S$ and LT(M) is the set of leading term of all rows of (M). A valid elementary row operation is $Row(M,s) \longleftarrow Row(M,s) + \lambda.Row(M,s')$ where $\lambda \in \mathbb{K}, s' \in S$ and the additional condition that $s' = (j',u') < (j,u) = s$ (or more explicitly $j' < j$ or ($j = j'$ and $u' \prec u$)). The index of the row is unchanged after a elementary operation. We denoted by $\tilde M_{d,i}$ the result of Gaussian elimination applied to the matrix $M_{d,i}$ using a sequence of valid elementary row operations.

The algorithm $F5$-invariant constructs matrices incrementally degree by degree and equation by equation. Let d be the current degree and i the current number of polynomials; in other words, we are computing a SG-basis of $\langle f_1,\ldots,f_i\rangle$ truncated in degree d. The algorithm constructs a *submatrix* $M_{d,i}$ of the invariant Macaulay matrix and performs row reductions on them. The incremental step from $i-1$ to i introduces the rows corresponding to $\Re(m).f_i$ for all monomials m of degree $d-d_i$, where $d_i = \deg(f_i)$, that do not appear as leading monomials in the $\tilde M_{d-d_i,i-1}$(by application of the F_5 criterion see proposition 4). The algorithm stops when the current degree is bigger than a given bound D.

3.2 F_5-INVARIANT Criterion

The following proposition is the key of the F_5 invariant algorithm.

PROPOSITION 4. *[F_5-invariant criterion] If t is the leading term of Row($\tilde M_{d-d_i,i-1},s$) where $s = (j,u) < (i,1)$ then the row $\Re(t).f_i$ indexed by (i,t) belongs to the vector space generated by the rows of $M_{d,i}$ having smaller index.*

PROOF. The hypothesis is that $t \in LT(\tilde M_{d-d_i,i-1})$, so that $t = LT(h)$ for some $h = \sum_{k=1}^{i-1}\Re(t_k)f_k$. This implies that $\Re(t).f_i = \sum_{k=1}^{i-1}\Re(t_k).f_k.f_i + (\Re(t)-h)f_i$, where the first term belongs to $\langle Row(M_{d,i-1})\rangle$ and the last one is a linear combination of rows of $M_{d,i}$ having smaller index as $LT(\Re(t)-h) \preceq LT(h)$. $\square$

3.3 Matrix F_5-invariant algorithm

We now describe the F_5-invariant algorithm. Here the admissible order is any admissible monomial ordering.

ALGORITHM 1. F_5***-invariant***
Input: *invariants homogeneous polynomials $(f_1,\ldots,f_m)$ with degrees $d_1 \le \ldots \le d_m$; a maximal degree D.*
Output: *the elements of degree at most D of a SG-bases of $(f_1,\ldots,f_m)$ for $i = 1,\ldots,m$.*
for i ***from*** 1 ***to*** n ***do*** $G_i := \emptyset$
for d ***from*** d_1 ***to*** D ***do*** $M_{d,0} := \emptyset$, $\tilde M_{d,0} := \emptyset$
for i ***from*** 1 ***to*** m ***do***
  if $d < d_i$ ***then*** $M_{d,i} := M_{d,i-1}$
  else if $d = d_i$ ***then***
    $M_{d,i}$:= *add new row* f_i *to* $\tilde M_{d,i-1}$ *with index* $(i,1)$
  else
    $M_{d,i}$:=*add new row* $\Re(m).f_i$ *for all monomials*
     m *of degree* $d-d_i$ *that do not appear as leading*
     monomials in the $\tilde M_{d-d_i,i-1}$ *with index* (i,m) *in* $\tilde M_{d,i-1}$.
   Compute $\tilde M_{d,i}$ *by Gaussian elimination from* $M_{d,i}$
   Add to G_i *all rows of* $\tilde M_{d,i}$ *not reducible by* LT(G_i)
return $G_1 \cup \cdots \cup G_m$

THEOREM 2. *The algorithm F_5-invariant computes the elements of degree at most D of the reduced SG-bases of $\langle f_1,\ldots,f_i\rangle$, for $i = 1,\ldots,m$.*

PROOF. We will use induction on d and i. For $d = d_1$ and $i = 1$, the result is clear. Assuming the induction hypothesis, we now simply have to prove that the rows of $M_{d,i}$ generate $\langle f_1,\ldots,f_i\rangle_d$. Then we can deduce that $LT(\tilde M_{d,i})$ generates $LT(\langle f_1,\ldots,f_i\rangle_d)$ and the conclusion on G_i follows. It is thus sufficient to show that for any $m \in \mathcal{T}_{d-d_i}$, the polynomial $\Re(m).f_i$ is generated by the rows of $M_{d,i}$. If $m \in LT(\tilde M_{d-d_i,i-1})$ then by proposition3.2, $\Re(m).f_i$ is generated by rows of the matrix having a smaller index and using the induction hypothesis the result is clear. Otherwise, $\Re(m).f_i$ is entered by the algorithm in $M_{d,i}$. This complete the proof of the theorem. $\square$

3.4 F_5-invariant example

Let G be the alternating group A_3 acting on the variables $X = [x, y, z]$. We consider the ring $\mathbb{K}[x, y, z]^G$ with graded lexicographic order $x > y > z$. The Reynolds operator is given by $\Re(f) = \frac{1}{3}(f(x, y, z) + f(y, z, x) + f(z, x, y))$. Let $I = \langle f_1, f_2 \rangle = \langle \Re(x), \Re(x^2y) - \Re(xyz) \rangle$. Assume that we want to compute the SG-basis of I up to degree 5. We start with $G_2 = \{f_1, f_2\}$. To compute the SG-bases, we proceed degree by degree. Since the first computation is the most simple we may skip the two first steps. In degree 3, we construct the matrix $M_{3,1}$ whose rows are coefficients of the following polynomials:

$$\begin{array}{l} \Re(x^2).f_1 = \frac{1}{9}\Re(x^3) + \frac{1}{9}\Re(x^2y) + \frac{1}{9}\Re(x^2z) \\ \Re(xy).f_1 = \frac{1}{9}\Re(x^2y) + \frac{1}{9}\Re(x^2z) + \frac{1}{3}\Re(xyz) \end{array}$$

with index $(1, x^2)$ and $(1, xy)$ respectively. So

$$M_{3,1} = \begin{array}{c} \\ \Re(x^2).f_1 \\ \Re(xy).f_1 \end{array} \begin{array}{c} \begin{array}{cccc} \Re(x^3) & \Re(x^2y) & \Re(x^2z) & \Re(xyz) \end{array} \\ \begin{pmatrix} \frac{1}{9} & \frac{1}{9} & \frac{1}{9} & 0 \\ 0 & \frac{1}{9} & \frac{1}{9} & \frac{1}{3} \end{pmatrix} \end{array}$$

It is obvious that $\tilde{M}_{3,1} = M_{3,1}$. We obtain $M_{3,2}$ by adding polynomial f_2 to $\tilde{M}_{3,1}$ with index$(2, 1)$:

$$M_{3,2} = \begin{array}{c} \\ \Re(x^2).f_1 \\ \Re(xy).f_1 \\ f_2 \end{array} \begin{array}{c} \begin{array}{cccc} \Re(x^3) & \Re(x^2y) & \Re(x^2z) & \Re(xyz) \end{array} \\ \begin{pmatrix} \frac{1}{9} & \frac{1}{9} & \frac{1}{9} & 0 \\ 0 & \frac{1}{9} & \frac{1}{9} & \frac{1}{3} \\ 0 & 1 & 0 & -1 \end{pmatrix} \end{array}$$

After Gaussian elimination:

$$\tilde{M}_{3,2} = \begin{pmatrix} \frac{1}{9} & \frac{1}{9} & \frac{1}{9} & 0 \\ 0 & \frac{1}{9} & \frac{1}{9} & \frac{1}{3} \\ 0 & 0 & -1 & -4 \end{pmatrix}.$$

Now we have obtained one new polynomial $f_3 = -\Re(x^2z) - 4\Re(xyz)$. We add f_3 to G_2. In degree 4 there is no new polynomial so we may skip this step. In degree 5, we construct matrix $M_{5,1}$ whose rows are the coefficients of the following polynomials:

$$\begin{array}{l} \Re(x^4).f_1 = \frac{1}{9}\Re(x^5) + \frac{1}{9}\Re(x^4y) + \frac{1}{9}\Re(x^4z) \\ \Re(x^3y).f_1 = \frac{1}{9}\Re(x^4y) + \frac{1}{9}\Re(x^3y^2) + \frac{1}{9}\Re(x^3yz) \\ \Re(x^3z).f_1 = \frac{1}{9}\Re(x^4z) + \frac{1}{9}\Re(x^3z^2) + \frac{1}{9}\Re(x^3yz) \\ \Re(x^2y^2).f_1 = \frac{1}{9}\Re(x^3y^2) + \frac{1}{9}\Re(x^3z^2) + \frac{1}{9}\Re(x^2y^2z) \\ \Re(x^2yz).f_1 = \frac{1}{9}\Re(x^3yz) + \frac{2}{9}\Re(x^2y^2z) \end{array}$$

So $M_{5,1}$ equal to following matrix (from now we remove $\mathcal{R}$):

$$\begin{array}{c} \\ x^4f_1 \\ x^3yf_1 \\ x^3zf_1 \\ x^2y^2f_1 \\ x^2yzf_1 \end{array} \begin{array}{c} \begin{array}{ccccccc} x^5 & x^4y & x^4z & x^3y^2 & x^3yz & x^3z^2 & x^2y^2z \end{array} \\ \begin{pmatrix} \frac{1}{9} & \frac{1}{9} & \frac{1}{9} & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{9} & 0 & \frac{1}{9} & \frac{1}{9} & 0 & 0 \\ 0 & 0 & \frac{1}{9} & 0 & \frac{1}{9} & \frac{1}{9} & 0 \\ 0 & 0 & 0 & \frac{1}{9} & 0 & \frac{1}{9} & \frac{1}{9} \\ 0 & 0 & 0 & 0 & \frac{1}{9} & 0 & \frac{2}{9} \end{pmatrix} \end{array}$$

It is easy to see $M_{5,1} = \tilde{M}_{5,1}$. We can obtain $M_{5,2}$ by adding the polynomials $\Re(xy).f_2$ and $\Re(x^2).f_2$ to$\tilde{M}_{5,1}$. By using the $F5$-invariant criterion we can remove the row $\Re(x^2).f_2$ from $M_{5,2}$. In other words $M_{5,2}$ is the following matrix

$$\begin{array}{c} \\ x^4f_1 \\ x^3yf_1 \\ x^3zf_1 \\ x^2y^2f_1 \\ x^2yzf_1 \\ xyf_2 \end{array} \begin{array}{c} \begin{array}{ccccccc} x^5 & x^4y & x^4z & x^3y^2 & x^3yz & x^3z^2 & x^2y^2z \end{array} \\ \begin{pmatrix} \frac{1}{9} & \frac{1}{9} & \frac{1}{9} & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{9} & 0 & \frac{1}{9} & \frac{1}{9} & 0 & 0 \\ 0 & 0 & \frac{1}{9} & 0 & \frac{1}{9} & \frac{1}{9} & 0 \\ 0 & 0 & 0 & \frac{1}{9} & 0 & \frac{1}{9} & \frac{1}{9} \\ 0 & 0 & 0 & 0 & \frac{1}{9} & 0 & \frac{2}{9} \\ 0 & 0 & 0 & \frac{1}{9} & \frac{1}{9} & 0 & \frac{-2}{9} \end{pmatrix} \end{array}$$

After triangulation

$$\tilde{M}_{5,2} = \begin{pmatrix} \frac{1}{9} & \frac{1}{9} & \frac{1}{9} & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{9} & 0 & \frac{1}{9} & \frac{1}{9} & 0 & 0 \\ 0 & 0 & \frac{1}{9} & 0 & \frac{1}{9} & \frac{1}{9} & 0 \\ 0 & 0 & 0 & \frac{1}{9} & 0 & \frac{1}{9} & \frac{1}{9} \\ 0 & 0 & 0 & 0 & \frac{1}{9} & 0 & \frac{2}{9} \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{9} & \frac{5}{9} \end{pmatrix}$$

Hence the matrix $\tilde{M}_{5,2}$ give us a new polynomial $f_4 = \Re(x^3z^2) + 5\Re(x^2y^2z)$. The F_5 algorithm stops and returns $[f_1, f_2, f_3, f_4]$.

3.5 Experimental Results - Cyclic n problem

As a proof of concept, a first implementation of the F_5-invariant algorithm has been made in the Maple 12 Computer Algebra systemMAPLE[1]. It is not easy to perform a direct comparison with other software since there is no equivalent procedure in Magma, Cocoa, Macaulay 2 or Singular. For instance, in Singular, the library `sagbi.lib` computes SAGBI bases of subalgebras and we cannot use this library to compute a SG basis of any ideals. Therefore, in Maple, we implement two version of the algorithm: one is a Buchberger's-like algorithm and the second one is the F_5-invariant algorithm (as described in algorithm 1). As a benchmark we use the well known cyclic n problem.

Cyclic n problem. To solve the cyclic n problem [3] we need to find all the (complex) solutions of the following system:

$$(C_n) \quad f_1 = \cdots = f_{n-1} = f_m - 1 = 0$$

where $f_i = \sum_{j=1}^{n} x_j\, x_{j+1} \cdots x_{j+i-1}$ with $x_{n+1} = x_1$, $x_{n+2} = x_2, \ldots$. This system remains invariant when the variables are permuted in a cyclic way and when they are read backwards. More precisely, the system is D_n-invariant where D_n is the dihedral group.

In figure 1, we give the time for computing a SG-basis up to degree 10 of the cyclic n problem (on Intel/XEON 3.20 GHz PC running Linux). Note that we have fix *arbitrarily* the maximal degree $D = 10$ but *there is no need* to compute up so such a degree for this small examples.

Figure 1: Maple implementation: comparison of F5-invariant and Buchberger's-like algorithm for computing a SG-basis truncated in degree 10 for the Cyclic n

Groups	F5-invariant	Buchberger
cyclic 4	309.7 s	716.2 s
cyclic 5	2701.8 s	6830.5 s
cyclic 6	23655 s	∞

As a second proof of concept of the possible efficiency of the method, one of the author has implemented algorithm 1

[1] `http://www.maplesoft.com/`

in C as a part of the FGb program[2]. The main difference with a classical implementation of F_5 is that one has to provide an efficient implementation of the product of terms:

$$\mathfrak{R}(t)\,\mathfrak{R}(t') = \alpha_1\mathfrak{R}(t_1) + \cdots + \alpha_k\mathfrak{R}(t_k)$$

Of course, such an implementation depends strongly on the finite group G; we have thus a dedicated implementation for this operation in the case of the cyclic group C_n. We report in figure 2, CPU timings for the Cyclic n problem modulo a small prime p (the computer is a laptop Dell E6500, 4Go RAM); for the tests we compute a D truncated SG-basis and we choose D big enough so that we can solve the system (that is to say D so that we can apply the FGLM-Invariant algorithm 2). Obviously, there is a huge speedup between the Maple implementation and the low level implementation. The results are very promising since it takes 1m30s to compute a SG-basis for the Cyclic-9 problem. To give an order of magnitude of time of the problem we have included the CPU for computing a Gröbner basis using the F_4[9] implementation in Magma 2.14 (the computer was an Intel/Xeon, 20 Go RAM).

Figure 2: Benchmarks with FGb: F5-Invariant for the Cyclic n problem modulo p

Problem	D truncated F_5-invariant	D	Magma 2.14 F_4-Gröbner Basis
cyclic 7	0.06 s	12	0.3 s
cyclic 8	0.5 s	13	8.4 s
cyclic 9	92.2 s	15	575.3 s
cyclic 10	4788 s	16	$>$16 hrs and $>$16 Gig

4. FGLM- INVARIANT ALGORITHM

The main goal of this section is to show how SG-bases can be used to compute a Gröbner basis which respects the elementary symmetric polynomials σ_i. In fact, we will present a more general algorithm to convert a SG-basis of an arbitrary zero ideal to a Gröbner basis in some invariant ring $\mathbb{K}[h_1, \cdots, h_r]$. From now, we assume that $dim(I) = 0$.

First we give an idea of the algorithm which is very close to the original FGLM algorithm [11]. Assume that we want to compute a Gröbner basis $\mathcal{G}$ of I^G in the invariant ring $\mathbb{K}[h_1, \ldots, h_r]$ for a lexicographical ordering; it is known that $\mathcal{G}$ contains a univariate polynomial in the variable h_r: exists $P = \sum_{i=0}^{m} c_i H_r^i \in \mathbb{K}[H_r]$ such that $P(h_r) \in I^G$. Let $\mathcal{G}$ be a SG-basis of I^G with respect to any term order up to degree D (with D big enough for instance $D \geq \deg(P)$) and $\mathrm{NF}_{\mathcal{G}}$ denote the SG-NormalForm modulo $\mathcal{G}$. To find the coefficients of the univariate polynomial in h_r we consider the following sets:

$$L_k = \{1, H_r, H_r^2, \ldots, H_r^k\} \text{ with } k \in \mathbb{N}.$$
$$V_k = \{1, \mathrm{NF}_{\mathcal{G}}(h_i), \mathrm{NF}_{\mathcal{G}}(h_i^2), \ldots, \mathrm{NF}_{\mathcal{G}}(h_i^k)\} \text{with } k \in \mathbb{N}.$$

The second is obtained from the first set by substituting H_i by $h_i(x_1, \ldots, x_n)$ and taking the SG-NormalForm. By proposition 2 we have that for any $(c_0, \ldots, c_l) \in \mathbb{K}^{l+1}$ $c_0.1 + c_2.h_r + \ldots + c_l.h_r^l \in I^G$ iff $c_0 + c_1.\mathrm{NF}_{\mathcal{G}}(h_r) + \ldots + c_l.\mathrm{NF}_{\mathcal{G}}(h_r^l) = 0$. According to the remark 2, we can express $\mathrm{NF}_{\mathcal{G}}(h_i^j)$ as a unique linear combination of standard invariants for all $j \in \mathbb{N}$. So, all we have to do is to check the linear dependence of V_k with increasing k, until we find the coefficients $c_0, \ldots, c_l$. This coefficients are the coefficients of the desired polynomial.

[2] `http://www.grobner.org/jcf/Software/FGb/index.html`

Now, we will use a similar method and provide an algorithm to convert a SG-basis up to degree D w.r.t $\preceq_1$ of a zero-dimensional ideal to an invariant Gröbner basis w.r.t a second monomial ordering $\preceq_2$. Our algorithm pick terms $t \in T_D(H_1, \ldots, H_r)$ by increasing term order for $\preceq_2$ and looks for linear combination

$$\mathrm{NF}_{\mathcal{G}}(t') + \sum_{u \prec_2 t} c_u \mathrm{NF}_{\mathcal{G}}(u') = 0$$

with the convention that t' (resp. u') is the result of substituting H_i by $h_i(x_1, \ldots, x_n)$ in t (resp. u). If there is no such relation then t is a member of the new staircase. Termination is assured by the fact that the number of terms with total degree less or equal to D is finite. We can now present the FGLM-invariant algorithm.

ALGORITHM 2. ***FGLM-Invariant***

Input: *(i) a SG-basis F up to degree D of I^G w.r.t $\preceq_1$*
(ii) a second monomial ordering $\preceq_2$
(iii) polynomials $(h_1, \ldots, h_r) \in \mathbb{K}[x_1, \ldots, x_n]^G$
Output: *Invariant Gröbner basis up to degree D w.r.t $\preceq_2$ in $\mathbb{K}[h_1, \ldots, h_r]$.*

$L := [\,]$ *// list of terms in $T(H_1, \ldots, H_r)$*
$S := [\,]$ *// staircase for the new ordering $\preceq_2$*
$V := [\,]$ *// V = SG-NormalForm(S)*
$G_D := [\,], t := 1$ *// t is a term in $T(H_1, \ldots, H_r)$*
infinite loop
we replace H_i by h_i in t:
$t' :=$ *replace $H_1, H_2, \ldots$ by $h_1, h_2, \ldots$ in t*
$v :=$ *SG-NormalForm*(t')
$s := \#S$ *// number of elements in S.*
if $v \in$ *Vect*$_{\mathbb{K}}(V)$ **then**
we can find $(\lambda_i) \in \mathbb{K}^s$ *s.t.* $v = \sum_{i=1}^{s} \lambda_i \cdot V_i$
$G_D := G_D \cup \left[t - \sum_{i=1}^{s} \lambda_i \cdot S_i\right]$
else
$S := S \cup [t]$ *and* $V := V \cup [v]$
$L :=$*Sort*$(L \cup [H_i\, t \mid i = 1, \ldots, r], \preceq_2)$
Remove duplicates from L and all multiple of LT$_{\preceq_2}(G_D)$
Remove from L elements of degree $> D$
if $L = \emptyset$ **then return** G_D
$t :=$ *first*(L) *and remove t from L.*

THEOREM 3. *The algorithm FGLM-invariant computes the reduce Gröbner basis up to degree D of I^G w.r.t $\preceq_2$ in the ring R^G .*

PROOF. Let G_D be the output set $\{g_1, \ldots, g_m\}$ of polynomials indexed in the order of their placement into G_D, let s_i be the value of t at the time when g_i was placed into G_D, and let $s_i = LT(g_i)$.

Clearly, $s_1 < \ldots < s_m$, $s_j \nmid s_k$ for $j < k$. Furthermore, $T(g_i) \setminus \{s_i\} \in R$, $(1 \leq i \leq m)$. So, g_i is in normal form modulo $\{g_1, \ldots, g_{i-1}, g_{i+1} \ldots, g_m\}$ and thus modulo $G_D \setminus \{g_i\}$. We have proved that G_D is reduced.

By proposition 2, we also have that $G_D \subseteq I^G$. To see that G_D is a Gröbner basis, we show that for every $f \in I^G$ and $\deg(f) \leq D$ with $s = LT(f)$, there exists $(1 \leq i \leq m)$ such that $s_i \mid s$. Assume for a contradiction that this is not true for some $f_0 \in I^G$ with $s_0 = LT(f_0)$. We may assume that f_0 is in normal form modulo G_D.

Since s_0 is not divisible by any s_i $(1 \leq i \leq m)$, there exists i such that $s_0 = t_i$. $(t_{i-1} \prec_2 s_0 = t_i)$

Let $s'_0 \in T(f_0) \setminus s_0$. Then $s'_0 \prec_2 s_0$, and s'_0 is not divisible by any term of LT(G_D) (since f_0 is in NormalForm modulo G_D). Hence, it is easy to see that $s'_0 \prec_2 t_{i-1}$, and thus s'_0 is in T. Hence, $T(f_0) \setminus s_0 \subset T$ and it follows that the $if-condition$ must detect that $LT(f_0)$ is in Vect$_{\mathbb{K}}(V)$, a contradiction. □

REMARK 6. *There exists a D_0 such that $G_D = G_{D_0}$ for all $D \geq D_0$. In fact, in the radical case, G_{D_0} is a Gröbner basis for the relative orbit variety $\mathbb{V}(I)/G$. Also, we can obtain an invariant Gröbner basis by applying the mapping $H_i \mapsto h_i(x_1, \ldots, x_n)$ to G_{D_0}.*

REMARK 7. *Thanks to the algorithm FGLM-invariant algorithm and theorem[1], we can compute a symmetric invariant Gröbner basis by considering $h_i = \sigma_i$ in the previous algorithm.*

EXAMPLE 2. *Consider the cyclic matrix group G of order 4 generated by $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. It is easy to check that $R^G = \mathbb{K}[h_1, h_2, h_3]$ where $h_1 = x^2 + y^2, h_2 = x^2y^2$ and $h_3 = xy(x^2 - y^2)$ (see for instance [8] ch 7). Let us consider the following invariant system:*

$$\begin{cases} f_1 = x^4 + y^4 - 1 = 0 \\ f_2 = x^3y^3(x^6 - y^6) - 2 = 0 \end{cases}$$

If we compute a Gröbner basis of $I = < f_1, f_2 >$ (w.r.t. the lexicographic order), we find the following polynomial in x :

$$4x^{48} - 24x^{44} + 69x^{40} - 125x^{36} + 156x^{32}$$
$$- 138x^{28} + 70x^{24} + 12x^{20} - 39x^{16} + 15x^{12} + 16 = 0$$

so, we have to find the roots of a polynomial of degree 48. Using the above algorithm, we can compute a Gröbner basis for the relative orbit variety of $\mathbb{V}(I)/G$. For this, we compute a SG-basis up to degree 12 (w.r.t. to the DRL ordering) and thanks to the algorithm FGLM-invariant, we find the following Gröbner basis of I^G:

$$G_0 = \{h_3^3 - 3h_2h_3 + 4, h_1^2 - 2h_2 - 1, 2h_2^2 + h_3^2 - h_2\}.$$

In fact, G_0 is a Gröbner basis for relative orbit variety $\mathbb{V}(I)/G$.

The major difficulty in the above method is the computation of a good generating set $\{h_1, \ldots, h_r\}$. In [13], G. Kemper provided algorithms for this purpose. When the elementary symmetric functions σ_i are left invariant by G we can avoid this problem by working in the ring $\mathbb{K}[\sigma_1, \ldots, \sigma_n]$; in the next section, we apply the method to systems which are invariant by the dihedral group.

5. A METHOD FOR FINDING ALL SOLUTIONS OF THE CYCLIC PROBLEM

The aim of this section is to propose an algorithm to compute the complex solution of a *zero dimensional* algebraic system. Application to the cyclic n problem is given in section 5.2 as an illustration of the method.

5.1 General algorithm

Assume that we want to solve in $\mathbb{C}$ a polynomial system $f_1 = \cdots = f_m = 0$ such that all the polynomials f_i are invariant under the action of the finite group G; moreover we assume that $\sigma_1, \ldots, \sigma_n$ the elementary symmetric functions are left invariant by G. In other words, according to remark 2, we can express σ_i as a unique linear combination of the standard invariants for all $i \in \{1, \ldots, n\}$.

To obtain a Gröbner basis in $\mathbb{K}[\sigma_1, \ldots, \sigma_n]$ we want to apply the invariant FGLM algorithm so that we need a SG-NormalForm function; this SG-NormalForm is available as soon as we have computed a SG-Gröbner basis up to some degree D. Of course, we don't know in advance the value of D so that we have to proceed incrementally degree by degree. Termination is assured by this fact that a finite Gröbner basis exists in $\mathbb{K}[\sigma_1, \ldots, \sigma_n]$.

Assume that we obtain a representation of all the possible values of $\sigma_1, \ldots, \sigma_n$ (for instance a lexicographical Gröbner basis $\mathcal{G}$ in $\mathbb{K}[\sigma_1, \ldots, \sigma_n]$). By solving the equation $X^n - \sigma_1 X^{n-1} + \ldots + (-1)^n \sigma_n = 0$. we are able to recover all the solutions for $x_n, x_{n-1}, \ldots$. The main drawback of this method is that we also obtain parasite solutions which are not solutions of the original system (for each solution obtained from $\mathcal{G}$ we obtain $n!$ candidate solutions); a pseudo algorithm (Algorithm 4) is given in the next section to remove this spurious solutions. The global strategy to solve the system is the following:

ALGORITHM 3. *(Invariant Zero-dimensional Solving)*
Input: $F = [f_1, \ldots, f_m]$
Output: *solutions of F in $\bar{\mathbb{K}}$*
$D := \min_i \deg(f_i)$
infinite loop
 // Apply F_5-invariant algorithm: choose $\prec_1 = \prec_{\text{DRL}}$
 G_D :=*SG-Gröbner basis of F up to degree D*
 // Apply FGLM-invariant algorithm: choose $\prec_2 = \prec_{\text{DRL}}$
 G'_D :=*invariant Gröbner basis up to degree D in $\mathbb{K}[\sigma_1, \ldots, \sigma_n]$*
 if *$\langle G'_D \rangle$ is zero dimensional* ***then***
  // Apply the standard FGLM[11] algorithm
  $\mathcal{G}$:= compute a lexicographical Gröbner basis of G'_D
  // Apply algorithm 4 to eliminate spurious solutions
  $\mathcal{S}ol$:=Keep valid solutions described by $\mathcal{G}$
  return *$\mathcal{S}ol$*
 $D := D + 1$

REMARK 8. *In practice, it is very easy to check that G'_D generates a zero-dimensional ideal: we check that for all $i \in \{1, \ldots, n\}$ we can find $g \in G'_D$ such that LT$(g) = x_i^{k_i}$ for some $k_i \in \mathbb{N}$.*

5.2 Filtering parasite solutions

The aim of this section is to propose a method to remove the parasite solutions in the previous algorithm 3. Let I be the ideal of R generated by the equations $f_1 = \cdots = f_m = 0$ and $J_{\mathfrak{S}_n}$ be the ideal generated by $G_{\mathbb{K}[\sigma_1,\ldots,\sigma_n]^{\mathfrak{S}_n}}(I, \prec)$ in $R^{\mathfrak{S}_n}$ (see definition 9 and remark 5). We denote by $\mathbb{V}(I)$ (resp. $\mathbb{V}(J_{\mathfrak{S}_n})$) the corresponding variety. Suppose that we have a solution $(\sigma_1, \ldots, \sigma_n) \in \mathbb{V}(J_{\mathfrak{S}_n})$. Now we consider the roots $a = (a_1, \ldots, a_n)$ of the polynomial $f(z) = X^n - \sigma_1 X^{n-1} + \ldots + (-1)^n \sigma_n$. Any permutation of the roots $\delta.a = (a_{\delta(1)} \ldots, a_{\delta(n)})$ is not necessarily a solution of the original system; in fact, we have to find a member δ of the set of right cosets of G in $\mathfrak{S}_n$ (denoted by $\mathfrak{S}_n/G$) such that $\delta \cdot (a_1 \ldots, a_n) \in \mathbb{V}(I)$. The following pseudo algorithm computes such a permutation δ for every arbitrary arrangement of $a_1, \ldots, a_n$.

ALGORITHM 4. ***Filtering solutions***
Input: $(a_1 \dots, a_n)$ *roots of* $f(z) = 0$ *and* G *a group*
Output: *a permutation* δ *such that* $\delta.(a_1 \dots, a_n)$ *is a solution*
$G' :=$ *Gröbner basis of* $[x_1 - a_1, \dots, x_n - a_n]$
For $\delta \in \mathfrak{S}_n/G$ ***do***
$g_1 := f_1(\delta \cdot (X)), \dots, g_n = f_m(\delta \cdot (X))$
$L := \{\mathit{NormalForm}(g_i, G') \mid i = 1, \dots, n\}$
if $L = \{0\}$ ***then return*** δ

5.3 Application to the cyclic n problem

In that case the finite group is the dihedral group. We apply the algorithm 3 to compute a symmetric invariant Gröbner basis in $\mathbb{K}[\sigma_1, \dots, \sigma_n]$. This done by first computing a truncated SG-basis of the following very sparse ideal using the F_5 invariant algorithm:

$$I^{D_n} = \langle \Re(x_1), \Re(x_1 x_2), \dots, \Re(x_1 x_2 \cdots x_n) - 1 \rangle . \quad (1)$$

EXAMPLE 3. *We consider the cyclic* 5 *problem* (C_5)*. Using the* F_5*-invariant algorithm, we compute a SG-basis of the ideal* I^{D_n} *up to degree* 8*; then, thanks to the algorithm FGLM-invariant, we first obtain a Gröbner basis w.r.t the DRL ordering*

$$G_{\mathbb{K}[\sigma_1,\dots,\sigma_5]^{\mathfrak{S}_5}}(I, \prec) := \begin{bmatrix} {\sigma_2}^3 + 5\,{\sigma_3}^2, {\sigma_2}^2 \sigma_3 - 25\,\sigma_2, \\ \sigma_2\,{\sigma_3}^2 - 25\,\sigma_3, {\sigma_3}^3 + 5\,{\sigma_2}^2, \\ \sigma_1, \sigma_4, \sigma_5 - 1 \end{bmatrix}$$

and then by applying again the standard FGLM algorithm we obtain a lexicographical Gröbner basis:

$$\mathcal{G} := [\ \sigma_5 - 1, \sigma_4, \sigma_3^6 + 3125,\ \sigma_3, 125\sigma_2 + \sigma_3^4, \sigma_1\ ]$$

It is easy to see that

$$\mathbb{V}_{\mathbb{C}}(\mathcal{G}) = \{(0, -5\omega^2, -5\omega^3, 0, 1), (0, 0, 0, 0, 1)\}$$

where ω *is a fifth root of unity.*
Case 1. *The roots of* $f_\omega = X^5 - 5\omega^2 X^3 + 5\omega^3 X^2 - 1$ *are* $\omega, \omega, \omega, \frac{-3-\sqrt{5}}{2}\omega, \frac{-3+\sqrt{5}}{2}\omega$*. Using algorithm 4 with* $G = D_5$*, we get the following arrangement of roots.*

$$(x_1, x_2, x_3, x_4, x_5) = (\omega, \omega, \omega, \frac{-3-\sqrt{5}}{2}\omega, \frac{-3+\sqrt{5}}{2}\omega)$$

Case 2. *The roots of* $f_2 = X^5 - 1$ *are* $1, \omega, \omega^2, \omega^3, \omega^4$*. In the same way, we find the following arrangement of roots*

$$(x_1, x_2, x_3, x_4, x_5) = (1, \alpha, \alpha^2, \alpha^3, \alpha^4)$$

where α *is either* $e^{\frac{2i\pi}{5}}$ *or* $e^{\frac{4i\pi}{5}}$*.*

EXAMPLE 4. *We compare the size of the lexicographical (resp. symmetric invariant lexicographical) Gröbner basis for the cyclic* $7, 8$ *problems:*

	#Solutions	#polynomials	Max length of a poly
C_7 lex	924	35	132
inv C_7 lex	57	4	9
C_8 lex	dim 1	57	2545
inc C_8 lex	dim 1	15	548

6. CONCLUSION

We have presented a method based on SAGBI Gröbner basis to find the complex roots of polynomial systems whose equations are left invariant by the action of a finite group. Thanks to this approach we can use the symmetries of such systems to speedup the computation and reduce the size of the computed objects. The experimental tests showed promising results.

7. ACKNOWLEDGMENTS

The authors would like to thank Guénaël for useful discussions.

8. REFERENCES

[1] A.Colin. Solving a system of algebraic equations with symmetries. *Pure and applied algebra*, 117-118:195–215, 1997.
[2] G. A.Conca, J.Herzog. Sagbi bases and application to blow-up algebras. *Reine Angew.Math*, pages 113–138, 1996.
[3] G. Björk. Functions of modulus 1 on $\mathbf{Z}_n$, whose Fourier transforms have constant modulus, and “cyclic n-roots”. In J.S. Byrnes and J.F. Byrnes, editor, *Recent Advances in Fourier Analysis and its Applications*, volume 315 of *Ser. C: Math. Phys. Sci., Kluwer*, pages 131–140. NATO Adv. Sci. Inst., 1989.
[4] B.Sturmfels. *Algorithms in Invariant Theory*. Springer-Verlag, Wien,New York, 1993.
[5] Buchberger B. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* PhD thesis, Innsbruck, 1965.
[6] Buchberger B. An Algorithmical Criterion for the Solvability of Algebraic Systems. *Aequationes Mathematicae*, 4(3):374–383, 1970. (German).
[7] Buchberger B. A Criterion for Detecting Unnecessary Reductions in the Construction of Gröbner Basis. In *Proc. EUROSAM 79*, volume 72 of *Lect. Notes in Comp. Sci.*, pages 3–21. Springer Verlag, 1979.
[8] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties and Algorithms*. Undergraduate Texts in Mathematics. Springer Verlag, New York, 3rd ed. 2007. corr. 2nd printing, 2008, xvi edition, 2007. 560 p.
[9] Faugère J.C. A new efficient algorithm for computing Gröbner bases (F4). *Journal of Pure and Applied Algebra*, 139(1–3):61–88, June 1999.
[10] Faugère J.C. A new efficient algorithm for computing Gröbner bases without reduction to zero F5. In T. Mora, editor, *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, pages 75–83. ACM Press, July 2002.
[11] Faugère, J.C., Gianni, P., Lazard, D. and Mora T. Efficient Computation of Zero-Dimensional Gröbner Basis by Change of Ordering. *Journal of Symbolic Computation*, 16(4):329–344, October 1993.
[12] G.Kapur and K.Madlener. A completion procedure for computing a canonical basis for a k-subalgebra. *Computers and mathematics*, pages 1–11, June 1989.
[13] G.Kemper. *Computational Invariant Theory*. Springer-Verlag, New York, 2002.
[14] J. Hoffstein, J. Pipher, and J. Silverman. Ntru: a ring-based public key cryptosystem. In *ANTS III*, volume 1423, pages 267–288. Springer Verlag, 1998.
[15] J.L.Miller. Analogues of Gröbner bases in polynomial rings over a ring. *Journal Of Symbolic Computation*, 21(2):139–153, June 1996.
[16] J.L.Miller. Effective algorithms for intrinsically computing SAGBI-Gröbner bases in a polynomial ring over a filed. *Groebner bases and application (Linz)*, pages 421–433, February 1998.
[17] L.Robbiano and M. Sweedler. Subalgebra bases. *Commutative algebra*, pages 61–87, 1990.
[18] N.M. Thiéry. Computing minimal generating sets of invariant rings of permutation groups with SAGBI-Gröbner basis. *International Conference DM-CCG, Discrete Model-Combinatorics, Computation and Geometry*, pages 84–89, July 2002.