Journal of Algorithms and Computation

journal homepage: http://jac.ut.ac.ir

New Algorithm For Computing Secondary Invariants of Invariant Rings of Monomial Groups

Sajjad Rahmany*[1], Abdolali Basiri†[2] and Behzad Salehian Matikolaei[3‡3]

[1, 2,3]School of Mathematics and Computer Science, Damghan University, Department of Mathematics, Damghan University,P.O. Box 36715-364, Damghan, Iran..

ABSTRACT

In this paper, a new algorithm for computing secondary invariants of invariant rings of monomial groups is presented. The main idea is to compute simultaneously a truncated SAGBI- Gröbner basis and the standard invariants of the ideal generated by the set of primary invariants. The advantage of the presented algorithm lies in the fact that it is well-suited to complexity analysis and very easy to implement.

ARTICLE INFO

Article history:
Received 16, December 2016
Received in revised form 04, July 2017
Accepted 29 November 2017
Available online 01, December 2017

Keyword: Invariant Ring, Secondary Invariant, SAGBI-Gröbner basis, Monomial Groups, Algorithm F5-invariant

AMS subject Classification: 05C78.

1 Introduction

Let G be a finite matrix group, linearly acting on a polynomial ring R with n variables over some field $\mathbb{K}$. We denote the action of $\sigma \in G$ on $f \in R$ by $\sigma.f$ and the invariant ring by

$$R^G = \{f \in R : \sigma.f = f, \forall \sigma \in G\}.$$

*rahmany@du.ac.ir
†basiri@du.ac.ir
‡Corresponding author: Behzad Salehian, Email: bsalehian@du.ac.ir

It is clear that R^G is an algebra over $\mathbb{K}$. A famous theorem of Hilbert states that R^G is finitely generated as a $\mathbb{K}$-algebra and also it is well known [8] that there are n algebraically independent homogeneous invariants polynomials $P = \{f_1, \ldots, f_n\} \subset R^G$ such that R^G is finitely generated as a module over sub-algebra $\mathbb{K}[f_1, \ldots, f_n]$. The elements of P are called *primary invariants*. Any minimal system of homogeneous $g_1, \ldots, g_t$ generating R^G as a $\mathbb{K}[f_1, \ldots, f_n]$-module is called a system of *secondary invariants*.
The secondary invariants can be calculated by using the existing algorithms[3, 4, 5, 8]. It is known that most of these algorithms require the computation of a suitable Gröbner basis in polynomial ring R. However, this computation breaks all symmetries, and lead to costly calculations inside the full polynomial ring.
In [9], N.Thiéry circumvents the above shortcoming by relying on the theory of SAGBI-Gröbner bases(a generalization of Gröbner bases to ideals of sub-algebras of polynomial ring). In fact, he provided an algorithm like Buchberger's algorithm for computing truncated SAGBI- Gröbner bases and the standard monomials(i.e. secondary invariants; see proposition 4 in [9]) in the special case of invariant rings of permutation groups. However, according to our experience, this algorithm is not very practical way in order to compute a SAGBI- Gröbner basis [2].
The main aim in this paper is to present a new algorithm for the computation of secondary invariants of invariant rings of monomial groups. The idea is to compute simultaneously a truncated SAGBI- Gröbner basis and the standard invariants of the ideal generated by the set of primary invariants. To compute truncated SAGBI- Gröbner bases, we apply the F5-invariant algorithm which provided by Faugère and Rahmany [2].
A first implementation of our algorithm has been made in the Maple 13 computer algebra system and have been successfully tried on a number of examples. We study here the non-modular case ,i.e., the characteristics of $\mathbb{K}$ does not divide the order of G. Note that according to [5], algorithms for non-modular case are useful also in the modular case.
The paper is organized as follows: In Section 2, we will give some basic definitions and properties of invariants rings of monomial groups. In Section 3, we introduce some notation of SAGBI- Gröbner bases and give a brief exposition of F5-invariant algorithm. In Section 4, we concentrate on our main goal, namely providing an algorithm for computing secondary invariants of invariants rings of monomial groups.

2 The ring of invariants of a monomial group

In this section, we give some basic definitions of invariants rings of monomial groups and describe the main properties of them. For this, we assume that G be a subgroup of $\hat{S}_n$ where

$$\hat{S}_n = \left\{ \Pi. \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix} | \Pi \text{ is an } n \times n \text{ permutation matrix, } a_i \in \mathbb{K} \right\}.$$

Also, we use the notation X, for column vector of the variables $x_1, \ldots, x_n$. In other words:

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Let $A = (a_{ij}) \in G$ and $f \in R$. We define the group action $''.''$ of G on the ring R by:

$$A.f(X) = f(A.X) = f(a_{11}x_1 + \ldots + a_{1n}x_n, \ldots, a_{n1}x_1 + \ldots + a_{nn}x_n).$$

Definition 2.1 A polynomial $f \in R$ is called *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.
It is easily seen that R^G is not finite dimensional as a $\mathbb{K}$-vector space. But we have a decomposition of R^G into its homogeneous components, which are finite dimensional. This decomposition is similar to 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 set of monomials of degree d is a vector space basis of R_d. Now, observe that the action G preserves the homogeneous components. Hence we get a decomposition of the invariant ring

$$R^G = \bigoplus_{d \geq 0} R_d^G.$$

An important tool to the calculation of a vector space basis of R_d^G is the Reynolds operator, which is defined as follows
Definition 2.2 Let G be a finite group. The *Reynolds operator* of G is the map $\Re : R \longrightarrow R^G$ defined by the formula

$$\Re(f) = \frac{1}{\mid G \mid} \sum_{\sigma \in G} f(\sigma.X)$$

for $f \in R$.
Following properties of the Reynolds operator is easily verified(see[1], Section 7.3, Proposition 3).
Proposition 2.1 Let $\Re$ be the Reynolds operator of the group G, then
(a) $\Re$ is $\mathbb{K}$-linear in f.
(b) If $f \in R$, then $\Re(f) \in R^G$.
(c) If $f \in R^G$, then $\Re(f) = f$.
It is easy to prove that, for any monomial m the Reynolds operator gives us a homogeneous invariant $\Re(m)$. Such invariants are called *orbit sums*.
The set of all 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 assume a monomial order $<$ has been fixed and $LM(p)$ denote leading monomial of p with respect to $<$.
Definition 2.3. A monomial in $LM(R^G) = \{LM(p) \mid p \in R^G\}$ is called an *initial*.
Using proposition 2.1 and definition 2.3 we can simply derive the following lemma.
Using proposition 2.1 and definition 2.3 we can simply derive the following lemma.
Lemma 2.1 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.
In the rest of this paper, we suppose that all representations of invariant polynomials are in the above form.
SectionSAGBI- Gröbner bases in R^G In this section, we recall the definition of SAGBI-Gröbner bases(SG-bases) which is an analogs of Gröbner basis for ideals in $\mathbb{K}$-sub-algebras [6, 7]. Also, we will present basic properties of SG-basis in invariant rings.
The following symbol will be needed throughout the paper. Let $f_1 \ldots, f_n$ be invariant polynomials and I, I^G represent the ideal generates by $f_1 \ldots, f_n$ in R and R^G respectively. For the sake of simplicity, we assume that all the polynomials are homogeneous. The extension to the non-homogeneous case raise no difficulty.
Definition 3.1. A subset $F \subseteq I^G$ is *SG-basis* for I^G if $LT(F)$ generates the initial ideal $\langle LT(I^G)\rangle$ as an ideal over algebra $\langle LT(R^G)\rangle$. It is a partial SG-basis up to degree D of I^G if $LT(F)$ generates $\langle LTI^G\rangle$ up to the degree D.
Recall that in ordinary Gröbner basis theory every ideal is assured to have a finite Gröbner bases but SG-basis need not be finite.We continue by describing an appropriate reduction for the current context.
Definition 3.2. Let $f, g, p \in R^G$ with $f, p \neq 0$ and let P be a subset of R^G. Then we say

i) f *SG-reduces* to g modulo p by eliminating t(denote by: $f \xrightarrow[SG]{p} g[t]$), if $t \in T(f)$, there exists $s \in LM(R^G)$ with $s.LT(p) = t$, and

$$g = f - (\frac{a}{Lc(p).Lc(\Re(s))}).\Re(s).p$$

where a is the coefficient of t in f.

ii) f SG-reduces to g modulo P(denote by:$f \xrightarrow[SG]{P} g$), if f SG-reduces to g module p for some $p \in P$.

Finally, the definition of *SG-reducible*, *SG-normalform* are straightforward.

Basic properties of SG-basis presented in [2, 9]. We will review some of the standard fact on SG-bases. The proofs of the following proposition and its corollary proceed in the standard way.
Proposition 3.1 The following are equivalent for a subset F of an ideal $I^G \subseteq R^G$:

a) F is an SG-basis for I^G.

b) For every $h \in I^G$, every SG-normal form of h modulo F is 0.

Corollary 3.1. A SG-basis for I^G generates I^G as an ideal of R^G.
Corollary 3.2 Suppose that F is an SG-basis for $I \subseteq R^G$. Then $f \in R^G$ belongs to $I \Longleftrightarrow f \xrightarrow[SG]{F} 0$.
In [2], Faugère and Rahmany presented an efficient algorithm, called F5-invariant, for computing SG-basis up to degree D of invariant rings of monomial groups. In rest of this section, we give a brief exposition of F5 invariant algorithm. For this, we need the following definition which is an adaptation of Macaulay's matrix [9] in invariant rings:
Definition 3.3 [Macaulay's Matrix Invariant] Let $f_1, \ldots, f_m$ be homogeneous invariant polynomials with $degf_i = d_i$ and $d_1 \leq \ldots \leq d_m$. The Macaulay's matrix invariant $f_1, \ldots, f_m$ of degree d is matrix which rows are all coefficients multiples $\Re(m).f_i$ where m is an initial monomial of degree $d - d_i$ and columns indexed by initial monomials of degree d.
We will use the symbol $M_{d,m}$ to denote Macaulay's matrix invariant.

$$M_{d,m} = \begin{array}{c} \\ \Re(m_1).f_1 \\ \vdots \\ \Re(m_i).f_j \\ \vdots \\ \Re(m_t).f_m \end{array} \begin{array}{c} \begin{array}{cccc} \tilde{m}_1 & \tilde{m}_2 & \ldots & \tilde{m}_k \end{array} \\ \begin{pmatrix} \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \end{pmatrix} \end{array}$$

In fact, the algorithm $F5$-invariant constructs matrices incrementally in the degree and the number of polynomials. Let d be the current degree and i the current number of polynomials(in other words are computing a SG-basis of $\langle f_1, \ldots, f_i \rangle$ truncated in degree d with deg $f_i = d_i$). The algorithm constructs sub matrix $M_{d,i}$ of the Macaulay's matrix invariant and performs a row reduction on them. The incremental step from $i-1$ to i introduces the lines corresponding to $\Re(m).f_i$ for all monomials m of degree $d-d_i$ that do not appear as leading monomials in the $\tilde{M}_{d-d_i,i-1}$($F5$-invariant criterion). The algorithm stops when a large enough D has been reached.
We now describe the $F5$-invariant algorithm. Here the order is any monomial ordering.
We now describe the $F5$-invariant algorithm. Here the order is any monomial ordering.

Algorithm 3.1 Algorithm $F5$-invariant

Input: homogeneous polynomials invariants $(f_1, \ldots, f_m)$ with degrees $d_1 \leq \ldots \leq d_m$; a maximal degree D.

Output:The elements of degree at most D of reduced SG-bases of $(f_1, \ldots, f_m)$ for $i = 1, \ldots, m$.

for i **from** 1 **to** n **do** $G_i := \phi$

for d **from** d_1 **to** D **do**

$M_{d,0} := \phi$, $\tilde{M}_{d,0} := \phi$

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 $[G_i | i = 1, \ldots, m]$

Theorem 3.1. The algorithm $F5$-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 3.1. See [2], section 3.3, theorem 2.

3 An algorithm for computing secondary invariants

In this section we concentrate on our main goal: providing an algorithm for computing secondary invariants of R^G. For this, we assume that the primary invariants $f_1, \ldots, f_n \in R^G$ have been given . In our algorithm, we use the number and the degrees of secondary invariants which can be computed by the following proposition.
Proposition 4.1.
Let $d_1, \ldots, d_n$ be the degree of a primary invariants of R^G. Then

(a) the (minimal) number of secondary invariants equals

$$t = \frac{d_1 \cdots d_n}{|G|}.$$

(b) if $e_1, \ldots e_t$ be the degrees of the secondary invariants then the Hilbert series of R^G equals

$$H(R^G, z) = \frac{z^{e_1} + \cdots + z^{e_t}}{(1 - z^{d_1}) \cdots (1 - z^{d_n})}.$$

Remark 4.1. In the non-modular case, Molien's formula [8] provides complete information about the Hilbert series of R^G.

A result of Nakayama's lemma (see [5] lemma 2.1) state that the g_i are secondary invariants if and only if they generate $\frac{R^G}{I^G}$ as a vector space over $\mathbb{K}$, where I^G is the ideal generated by $f_1, \ldots, f_n$ in R^G. Since the number of g_i is correct, it is equivalent to the condition that the g_i are linearly independent modulo I^G. In fact, the following definition and proposition is the key of our algorithm.

Definition 4.1. Let I^G be an ideal of R^G. An initial monomial m is *standard* if $m \notin \langle LT(I^G)\rangle$. The invariant polynomial $\Re(m)$ of standard monomial m is called a *standard invariant*.

Proposition 4.2. Let $\{f_1, \ldots, f_n\}$ be a set of primary invariants and $I^G = \langle f_1, \ldots, f_n\rangle$ be the ideal generates by $\{f_1, \ldots, f_n\}$ in R^G. Then, the standard invariants w.r.t $\langle f_1, \ldots, f_n\rangle$ form a system of secondary invariants of R^G.

With this proposition, our goal becomes to compute the standard invariants of I^G. Therefore, we can calculate the partial SG-basis up to the degree e_t (i.e. maximum degree of secondary invariants) by algorithm $F5$-invariant and in the process of computation yields the complete information about the standard invariants (i.e.secondary invariants). We now present an algorithm for finding secondary invariants. We use the same notations of section 2.

Algorithm 4.1. Algorithm for computing secondary invariants

Input: A set of primary invariants(Homogeneous polynomials invariants

$(f_1, \ldots, f_n)$ with degrees $d_1 \leq \ldots \leq d_n$.

output: The secondary invariants.

calculate the number and the degrees $e_1, \ldots, e_t$ by Proposition(**??**)

standard:= $\emptyset$;

for i **from** 1 to t **do**

N_i= the set of initial monomials of degree e_i of R^G.

$standard_i := N_i \backslash LT(\tilde{M}_{e_i,n})$

(matrix $\tilde{M}_{e_i,n}$ has been calculated in the process of finding the SG-basis up to the degree e_t in algorithm $F5$-invariant)

standard:=$standard_i \cup$ standard;

return standard;

Let us look at an example now.
Example 4.1. Let G be cyclic group generated by the matrix

$$A = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

The Hilbert series is calculated by Molien's formula to be

$$H(R^G, z) = \frac{(z^3 + z^2 - z + 1)}{(1+z)^2(1+z^2)(1-z)^3}.$$

Magma delivers the following primary invariants:

$$f_1 = x^2 + y^2$$

$$f_2 = z^2$$

$$f_3 = x^4 + y^4$$

According to lemma 4.1 there exist four secondary invariants g_1, g_2, g_3, g_4 with degrees e_1, e_2, e_3, e_4 which are computed by formula

$$H(R^G, z)(1 - z^{d_1})(1 - z^{d_2})(1 - z^{d_3}) = z^{e_1} + z^{e_2} + z^{e_3} + z^{e_4}.$$

After replacing, we obtain $e_1 = 0, e_2 = e_3 = 3, e_4 = 4$. Now we can apply the above algorithm for finding secondary invariants. In degree 3, we obtain $N = \{x^2z, xyz\}$, and $LT(\tilde{M}_{3,3}) = \{\}$. So the set of standard monomials of degree 3 is $\{x^2z, xyz\}$. In degree 4, we have $N = \{x^4, x^3y, x^2y^2, x^2z^2, z^4\}$, and $LT(\tilde{M}_{4,3}) = \{x^4, x^2y^2, x^2z^2, z^4\}$. So monomial x^3y is standard monomial of degree 4 and the desired secondary invariants are

$$g_1 = 1,\ g_2 = \Re(x^2z),\ g_3 = \Re(xyz),\ g_4 = \Re(x^3y).$$

4 Concluding remarks

We have presented a method based on SAGBI- Gröbner basis to find the secondary invariants of invariant rings of monomial groups.Thanks to our approach, we can use the symmetries of primary invariants . In fact, we limit our calculations inside the invariant rings and also to avoid additional computations in the full polynomial ring. Another advantage of our algorithm lies in the fact that it can be obtained from the efficient algorithm F5-invariant.

References

[1] Cox, J.D., D.O'shea, Ideals, Varieties and algorithms, Springer-Verleg, New Yourk, 1997.

[2] Faugère, J.C., S. Rahmany, Solving systems of polynomial equations with symmetries using sagbi-Gröbner bases, in: T. Mora(ED.), ISSAC, ACM Press, 2009.

[3] Kemper, G., A. Steel, Some Algorithms in Invariant Theory of Finite Groups, in: P. Dräxler, G.O. Michler, C. M. Ringel, eds, Computational Methods for Representations of Groups and Algebras, Euroconference in Essen, April 1-5 1997, number 173 in Progress in Mathematics, Birkhuser, Basel, 1999.

[4] Kemper, G., Calculating Invariant Rings of Finite Groups over Arbitrary Fields, J. Symbolic Computation 21 (1996), 351-366.

[5] Kemper, G., Computational Invariant Theory, The Curves Seminar at Queen's, Volume XII, in: Queen's Papers in Pure and Applied Math. 114 (1998), 3-26.

[6] Miller, J., Effective algorithm for intrinsically computing sagbi-gröbner bases in polynomial ring over a field, Gröbner bases and application (Linz)(1998) 421-433.

[7] Miller, J., Analogues of Gröbner bases in polynomial rings over a ring, Journal of Symbolic Computation 21(2) (1996) 139-153.

[8] Sturmfels, B., Algorithms in invariant theory, Speringer-Verleg, Wien, New Yourk, 1993.

[9] Thièry, N.M., Computing minimal generating sets of invariant rings of permutation groups with sagbi-gröbner basis, in: International Conference DM-CCG, Discrete Model-Combinatorics, Computation and Geometry,2002, pp. 84-89.