Computing SAGB-Gröbner Basis of Ideals of Invariant Rings by Using Gaussian Elimination

Sajjad Rahmany, Abdolali Basiri

Abstract—The link between Gröbner basis and linear algebra was described by Lazard [4,5] where he realized the Gröbner basis computation could be achieved by applying Gaussian elimination over Macaulay's matrix.

In this paper, we indicate how same technique may be used to SAGBI-Gröbner basis computations in invariant rings.

Key words—Gröbner basis, SAGBI-Gröbner basis, reduction, Invariant ring, permutation groups.

I. INTRODUCTION

The concept of SAGBI-Gröbner bases (a generalisation of Gröbner bases to ideals of sub algebras of polynomial ring) has been developed by Miller [9,10]. In fact, it is a method to compute bases of ideals of sub algebras in a similar way to computing Gröbner bases for ideals [1,2]. SAGBI-Gröbner bases and Gröbner bases have analogous reduction properties. The main difference is that SAGBI-Gröbner bases need not be finitely generated. Therefore, we restrict our study to partial SAGBI-Gröbner bases up to given degree $D$.

The main goal of this note is to establishes the relation between linear algebra and SAGBI-Gröbner bases (SG-bases) and present an algorithm for computing SG-basis (up to degree $D$) for ideals of invariant rings of permutation groups. For this, we first describe link between SG- bases and linear algebra and then provide an algorithm like Lazard’s algorithm for construction of SG-basis. The advantage of our method lies in this fact that it be compute SG-bases (up to degree $D$) by applying Gaussian elimination on special matrix.

The paper is organized as follows. Section 2 has been divided into two parts: subsection (2.a), we review the necessary mathematical notations and in (2.b) we will give some basic definitions of invariants rings. In section 3, we recall the definition of SG-basis. Also we will present basic properties of SG-basis in invariant rings. In Section 4, we concentrate on our main goal. We will establishes the relation between linear algebra and SG-basis for ideals in invariant rings. In Section 5, We will give an algorithm for computing SG-basis.

II. INVARIANT RINGS

A. Standard notations

In this paper, we suppose that $\mathbb{K}$ is a field of characteristic zero, $R = \mathbb{K}[x_1, \ldots, x_n]$ is the ring of polynomials and monomial order $\prec$ has been fixed. For a polynomial $f \in R$, denote the leading monomial, leading term, and leading coefficient of $f$ with respect to $\prec$ by $LM(f)$, $LT(f)$, and $LC(f)$ respectively. We use the notation $T(f)$ for the set of terms of $f$. We denote by $T$, the set of all terms of $x_1, \ldots, x_n$. By extension, for any set $B$ of polynomials, define $LM(B) = \{LM(p) \mid p \in B\}$ and $LT(B) = \{LT(p) \mid p \in B\}$.

B. Invariants rings

In this subsection, we will give some basic definitions of invariants rings and describe the main properties of them. In the rest of this paper we assume that $G$ be a subgroup of $S_n$ where

$$\hat{S}_n = \{\Pi \in S_n \mid \Pi \text{ is a permutation matrix}\}.$$ 

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

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

Definition 2.1: Let $A = (a_{ij}) \in G$ and $f \in \mathbb{K}[x_1, \ldots, x_n]$. We define $f(A.X) \in \mathbb{K}[x_1, \ldots, x_n]$ by following:

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

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.

Example 2.1: 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 $g(A.X) \neq g(X)$.

It is immediately clear that $R^G$ is not finite dimensional as a vector space $\mathbb{K}$. But we have a decomposition of $R^G$ into its homogeneous components, which are finite dimensional. This decomposition is similar to decomposition of $R$. 

S. Rahmany : Member of the department of Mathematics, Damghan University of Basic Science, Damghan, Iran, e-mail: (see http://www.dubs.ac.ir/contact.html).

A. Basiri : Member of the department of Mathematics, Damghan University of Basic Science, Damghan, Iran, e-mail: (see http://www.dubs.ac.ir/contact.html). 

Manuscript received October 31, 2009.
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 $d$ are 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

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

A method for calculating a vector space basis of $R^G$ 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 $\mathcal{R} : \mathbb{R} \rightarrow R^G$ defined by the formula

$$\mathcal{R}(f) = \frac{1}{|G|} \sum_{\sigma \in G} \sigma(f.X)$$

for $f \in R$.

Following properties of the Reynolds operator is easily verified.

**Proposition 2.1:** ([3]) Let $\mathcal{R}$ be the Reynolds operator of the finite group $G$.

1. $\mathcal{R}$ is $K$-linear in $f$.
2. If $f \in R$, then $\mathcal{R}(f) \in R^G$.
3. If $f \in R^G$, then $\mathcal{R}(f) = f$.

It is easy to prove that, for any nonmonomial $m$ the Reynolds operator gives us a homogeneous invariant $\mathcal{R}(m)$. Such invariants are called orbit sums.

The set 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 require the following terminology.

**Definition 2.3:** A monomial in $LM(R^G)$ is called an initial.

Using 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 $f = \sum_{\alpha} c_{\alpha} \mathcal{R}(m^*_\alpha)$, where $c_{\alpha} \in K$ and $m^*_\alpha$ are initial monomials.

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

### III. SG-BASIS IN INVARIANT RINGS

In this section, we recall the definition of SG-basis which is an analog of Gröbner basis for ideals in $k$-sub algebras. 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 $I$ be an ideal generated by $f_1, \ldots, f_n$ in $R$ and $R^G$ respectively. For the sake of simplicity, we assume that $I$ is 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 $LT(I^G)$ as an ideal over algebra $(LT(R^G))$. It is a partial SG-basis up to degree $D$ of $I^G$ if $LT(F)$ generates $LT(I^G)$ 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

1. $f$ SG-reduces to $g$ modulo $p$ (written $f \xrightarrow{P} g$), if $\exists a \in T(f), \exists b \in LM(R^G)$ such that $s.LT(p) = t$ and $g = f - (\frac{b}{LT(p)} + Lc).\mathcal{R}(s).p$ where $a$ is the coefficient of $t$ in $f$ and $\mathcal{R}$ is Reynolds operator of $G$.
2. $f$ SG-reduces to $g$ modulo $P$ (written $f \xrightarrow{P} g$), if $f$ SG-reduces to $g$ modulo $p$ for some $p \in P$.

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

Basic properties of SG-basis presented in [9,10,6]. 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 $I^G \subseteq R^G$:

1. $F$ is an SG-basis for $I^G$.
2. For every $h \in I^G$, every SG-normalform 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 $I$ if and only if $f \xrightarrow{SG} 0$.

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

### IV. LINEAR ALGEBRA AND SG-BASIS

The link between Gröbner basis and linear algebra was described by Lazar[4,5] where he realized the Gröbner basis computation could be archived by applying Gaussian elimination over Macaulay’s matrix.

In this section, we indicate how same technique may be used to SG-Gröbner basis computations. Also, we will establishes the relation between linear algebra and SG-Gröbner basis. For this, we assume $I^G$ be an ideal generated by a finite set of invariants polynomials $f_1, \ldots, f_n$ in $R^G$ and $I^G_d$ denote the set of polynomials in $I^G$ which are of degree less or equal than $d$, namely

$$I^G_d = \{ f \in I^G | \text{deg}(f) \leq d \}.$$

It is easy to see that the ideal $I^G$ itself is a subspace of the $K$-vector space $R^G$, and so is $I^G_d$ for each $d \in \mathbb{N}$.

Following proposition give a link between linear base of $I^G_d$ and SG-Gröbner basis.
Proposition 4.1: Let \( F = \{g_1, \ldots, g_l\} \subseteq I^G \). Suppose \( d \in \mathbb{N} \) was fixed and for \( 1 \leq i \leq l \) let
\[
B_i = \{ \mathcal{R}(m) \cdot g_i | deg(\text{LT}(\mathcal{R}(m) \cdot g_i)) \leq d, \text{LT}(g_j) \}\ \cup \\text{LT}(\mathcal{R}(m) \cdot g_i) \text{ for all } j < i \}.
\]
where \( \mathcal{R} \) is Reynolds operator of \( G \). Then following conditions are equivalent
(i) \( F \) is a SG-Gröbner basis up to degree \( d \) of \( I^G \) w.r.t a total degree order.
(ii) \( B = \bigcup_{i=1}^{l} B_i \) is a basis of the \( K \)-vector space \( I^G_d \).

Proof 4.1: Let \( F \) be a SG-Gröbner basis up to degree \( d \) of \( I^G \). We have \( B \subseteq I^G_d \) by choice of the term order. It is clear that the head terms of elements of \( B_i \) are pairwise different for fixed \( 1 \leq i \leq l \).

If there were \( \mathcal{R}(m_1) \cdot g_i \), \( \mathcal{R}(m_2) \cdot g_j \) with \( i < j \) and \( LT(\mathcal{R}(m_1) \cdot g_i) = LT(\mathcal{R}(m_2) \cdot g_j) \) then we would have \( LT(g_j) \upharpoonright LT(\mathcal{R}(m_2) \cdot g_j) \) contrary to the construction of \( B_j \). To prove the linear independence of \( B \), let
\[
p = \sum_{q \in B} \lambda_q q \quad (\lambda_q \in \mathbb{K})
\]
where not all \( \lambda_q \) equal zero. Then \( max\{LT(q) | \lambda_q \neq 0\} = LT(h) \) for exactly one \( h \in B \), and we see that \( LT(h) \) is a term \( p \). So \( p \neq 0 \). It remain to show that \( B \) is a generating system of \( I^G_d \). Let \( f \in I^G_d \). Then \( f \xrightarrow{SG} 0 \). Among all possible reduction chains, consider the one where each reduction step \( f_k \xrightarrow{SG} f_{k+1} \) is a top reduction and has the property \( LT(g_j) \upharpoonright LT(f_k) \) for all \( j < i \). So, \( f_{k+1} = f_k - \mathcal{R}(m_i) \cdot g_i \) such that \( \mathcal{R}(m_i) \cdot g_i \in B_i \). Finally, we can find a representation of \( f \) as sum of orbit sums multiples of elements of \( B \).

Conversely, let \( B \) generate \( I^G_d \). Then for \( f \in I^G_d \) we have \( f = \sum_{q \in B} \lambda_q q \). According to the above observation, there is a \( q \in B \) such that \( LT(q) = LT(f) \). It is means that there exist a \( g_i \in F \) \( ( q = \mathcal{R}(m_i) \cdot g_i \) such that \( LT(g_i) \upharpoonright LT(f) \).

Let us mention one important consequence of the above proposition.In rest of this section, we assume \( I^G \) be an ideal generated by homogeneous polynomials \( f_1, \ldots, f_m \) with \( deg(f_i) = d_i \) and \( d_1 \leq \ldots \leq d_m \). Also, let \( I^G_d \) denote the set of homogeneous polynomials in \( I^G \) which are of degree \( d \).

The characterization of SG-Gröbner basis of the last proposition may be used to make the following.

Corollary 4.1: A set \( F = \{f_1, \ldots, f_k\} \) of homogeneous polynomials is a SG-Gröbner basis for degree \( D \) of \( I^G \) if and only if
\[
\{ \mathcal{R}(m) \cdot f_i | i \in \{1, \ldots, k\}, \text{deg}(\text{LT}(\mathcal{R}(m) \cdot f_i)) = d, \text{LT}(f_j) \}\ \cup \\text{LT}(\mathcal{R}(m) \cdot f_i) \text{ for all } j < i \} \text{ a linear basis for } I^G_d.
\]
According to the above corollary, compute a SG-Gröbner basis in degree \( d \) for ideal \( I^G \) equivalent to find the linear basis for \( I^G_d \). Then, our goal (i.e. compute a SG-Gröbner basis in degree \( d \)) becomes to compute a linear basis for \( I^G_d \).

V. MACAULAY’S MATRIX INVARIANT AND LAZARD’S ALGORITHM

In this section, we will propose new method for computing SG-Gröbner basis in degree \( d \) for ideals in invariant rings of finite groups. The advantage of this method lies in the fact that it be achieve by applying Gaussian elimination on a special matrix. Now, we provide the following definition which is an adaptation of Macaulay’s matrix [7,8] in invariant rings.

Definition 5.1: The Macaulay’s matrix invariant \( f_1, \ldots, f_m \) of degree \( d \) is matrix which are all coefficients multiples \( \mathcal{R}(m) \cdot f_i \) where \( m \) is an initial monomial of degree \( d - d_i \) and columns indexed by initial monomials of degree \( d \) stored by \( \cdot \).

We use the symbol \( M_{d,m} \) to denote Macaulay’s matrix invariant.

\[
\text{We use the symbol } M_{d,m} \text{ to denote Macaulay’s matrix invariant.}
\]

\[
\begin{pmatrix}
\mathcal{R}(\tilde{m}_1) & \mathcal{R}(\tilde{m}_2) & \ldots & \mathcal{R}(\tilde{m}_k) \\
\mathcal{R}(m_1) \cdot f_1 & \ldots & \ldots & \ldots \\
\vdots & \ldots & \ldots & \ldots \\
\mathcal{R}(m_1) \cdot f_j & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots \\
\mathcal{R}(m_1) \cdot f_m & \ldots & \ldots & \ldots \\
\end{pmatrix}
\]

It is easy to see that, Macaulay’s matrix invariant is a representation of vector space \( I^G_d \) by an array of coefficients and also the following facts are straightforward

1. The leading terms of a row is the leading term the corresponding polynomial.
2. The result of applying a row operation on \( M_{d,m} \) gives a matrix whose rows generate the same ideal.

In fact, above representation is used to describe connection between SG-Gröbner basis and linear basis of an ideal. To find this relation, we will state the following definition and lemma. The proof of the lemma proceed in the standard way.

Definition 5.2: We denote by \( M_{d,m} \) the result of Gaussian elimination applied to the matrix \( M_{d,m} \) using a sequence of the elementary rows operations.

Lemma 5.1: The set of the all polynomials correspond with rows of \( M_{d,m} \) such that leading monomials of these not appear as leading monomials of polynomials correspond with rows \( M_{d,m} \) is a SG-Gröbner basis of degree \( d \) for ideal \( I^G \).

Now, suppose \( \text{Row}(M_{d,m}) \) be the set of polynomials corresponding with all rows of \( M_{d,m} \). By using above lemma, we can introduce a new algorithm for computing SG-Gröbner basis up to degree \( D \) of homogeneous ideals which is similar to Lazard’s algorithm.

Algorithm 5.1: Algorithm For computing SG-basis

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 SG-bases of \( (f_1, \ldots, f_m) \).

\( G := \emptyset \)

for \( d \) from \( d_1 \) to \( D \) do

Compute \( M_{d,m} \) by Gaussian elimination from \( M_{d,m} \).

Set \( L_d := \{ p \in \text{Row}(M_{d,m}) | LT(p) \notin LT(M_{d,m}) \} \)

\( G := G \cup L_d \)

return \( G \)
VI. CONCLUSION

A first implementation of above algorithm has been made in maple 12 computer algebra system and have been successfully tried on a number of examples. The advantage of this algorithm lies in this fact that it is very easy to implement and well suited to complexity analysis.

REFERENCES


