

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 archived 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.

. *Keywords*— 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.

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.

II. INVARIANT RINGS

A. Standard notations

In this paper, we suppose that \mathbb{K} is a field of characteristic zero, $R = \mathbb{K}[x_1, \dots, x_n]$ 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, \dots, 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 \hat{S}_n where

$$\hat{S}_n = \{\Pi \cdot \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix} \mid \Pi \text{ is a permutation matrix}\}.$$

Also, we use the notation X , for column vector of the variables x_1, \dots, 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 $f \in \mathbb{K}[x_1, \dots, x_n]$. We define $f(A.X) \in \mathbb{K}[x_1, \dots, x_n]$ by following:

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

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 than 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 .

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 calculate a vector space basis of R^G is Reynolds operator, which is defined as follows

Definition 2.2: Let G be a finite group. The *Reynolds operator* of G is the map $\mathfrak{R} : R \rightarrow R^G$ defined by the formula

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

for $f \in R$.

Following properties of the Reynolds operator is easily verified.

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

- (a) \mathfrak{R} is K -linear in f .
- (b) If $f \in R$, then $\mathfrak{R}(f) \in R^G$.
- (c) If $f \in R^G$, then $\mathfrak{R}(f) = f$.

It is easy to prove that, for any monomial m the Reynolds operator gives us a homogeneous invariant $\mathfrak{R}(m)$. 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 $f = \sum_{\alpha} c_{\alpha} \mathfrak{R}(m_{\alpha}^*)$, where $c_{\alpha} \in \mathbb{K}$ and m_{α}^* 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 analogs 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, \dots, f_n be invariant polynomials and I, I^G represent the ideal generates by f_1, \dots, 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 $\langle LT(I^G) \rangle$ 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 $\langle LT(I^G) \rangle$ 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 (written $f \xrightarrow{p}_{SG} g$), if $\exists t \in T(f), \exists s \in LM(R^G)$ such that $s.LT(p) = t$ and $g = f - (\frac{a}{Lc(p).Lc(\mathfrak{R}(s))}).\mathfrak{R}(s).p$ where a is the coefficient of t in f and \mathfrak{R} is Reynolds operator of G .
- ii) f *SG-reduces* to g modulo P (written $f \xrightarrow{P}_{SG} g$), 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 $I^G \subseteq R^G$:

- a) F is an SG-basis for I^G .
- b) 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 $I \iff f \xrightarrow{F}_{SG} 0$.

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 Lazard[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, \dots, f_n in R^G and I_d^G denote the set of polynomials in I^G which are of degree less or equal than d , namely

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

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

Following proposition give a link between linear base of I_d^G and SG-Gröbner basis .

Proposition 4.1: Let $F = \{g_1, \dots, g_l\} \subseteq I^G$. Suppose $d \in \mathbb{N}$ was fixed and for $1 \leq i \leq l$ set

$$B_i = \{\mathfrak{R}(m)g_i \mid \deg((LT(\mathfrak{R}(m)g_i))) \leq d, LT(g_j) \nmid LT(\mathfrak{R}(m)g_i) \text{ for all } j < i\}.$$

where \mathfrak{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 \mathbb{K} -vector space I_d^G .

Proof 4.1: let F be a SG-Gröbner basis up to degree d of I^G . We have $B \subseteq I_d^G$ 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 $\mathfrak{R}(m_1)g_i, \mathfrak{R}(m_2)g_j$ with $i < j$ and $LT(\mathfrak{R}(m_1)g_i) = LT(\mathfrak{R}(m_2)g_j)$ then we would have $LT(g_i) \mid LT(\mathfrak{R}(m_2)g_j)$ contrary to the construction of B_j . To prove the linear independence of B , let

$$p = \sum_{q \in B} \lambda_q \cdot q \quad (\lambda_q \in \mathbb{K})$$

where not all λ_q equal zero. Then $\max\{LT(q) \mid \lambda_q \neq 0\} = LT(h)$ 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_d^G . Let $f \in I_d^G$. Then $f \xrightarrow{*F}_{SG} 0$. Among all possible reduction chains, consider the one where each reduction step $f_k \xrightarrow{g_i}_{SG} f_{k+1}$ is a top reduction and has the property $LT(g_j) \nmid LT(f_k)$ for all $j < i$. So, $f_{k+1} = f_k - \mathfrak{R}(m_i)g_i$ such that $\mathfrak{R}(m_i)g_i \in B_i$.

Finally, we can find a representation of f as sum of orbit sums multiples of elements of B .

Conversely, let B generate I_d^G . Then for $f \in I_d^G$ we have $f = \sum_{q \in B} \lambda_q \cdot q$

According to the above observation, there is a $q \in B$ such that $LT(q) = LT(f)$. It is means that there exist a $g_i \in F$ ($q = \mathfrak{R}(m)g_i$) such that $LT(g_i) \mid LT(f)$.

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, \dots, f_m with $\deg(f_i) = d_i$ and $d_1 \leq \dots \leq d_m$. Also, let I_d^G 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 $F = \{f_1, \dots, f_k\}$ of homogeneous polynomials is a SG-Gröbner basis for degree D of I^G if and only if

$$\{\mathfrak{R}(m)f_i \mid i \in \{1, \dots, k\}, \deg((LT(\mathfrak{R}(m)f_i))) = d, LT(f_j) \nmid LT(\mathfrak{R}(m)f_i) \text{ for all } j < i\}$$

a linear basis for I_d^G . According to the above corollary, compute a SG-Gröbner basis in degree d for ideal I^G is equivalent to find the linear basis for I_d^G . Then, our goal (i.e. compute a SG-Gröbner basis in degree d) becomes to compute a linear basis for I_d^G .

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, \dots, f_m of degree d is matrix which rows are all coefficients multiples $\mathfrak{R}(m).f_i$ where m is an initial monomial of degree $d - d_i$ and columns indexed by initial monomials of degree d (stored by \prec).

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

$$M_{d,m} = \begin{matrix} \mathfrak{R}(\tilde{m}_1).f_1 \\ \vdots \\ \mathfrak{R}(m_i).f_j \\ \vdots \\ \mathfrak{R}(m_t).f_m \end{matrix} \begin{pmatrix} \mathfrak{R}(\tilde{m}_1) & \mathfrak{R}(\tilde{m}_2) & \dots & \mathfrak{R}(\tilde{m}_k) \\ \dots & \dots & \dots & \dots \end{pmatrix}$$

It is easy to see that, Macaulay's matrix invariant is a representation of vector space I_d^G 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 $\tilde{M}_{d,m}$ 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 $\tilde{M}_{d,m}$ 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 $Row(\tilde{M}_{d,m})$ be the set of polynomials corresponding with all rows of $\tilde{M}_{d,m}$. 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, \dots, f_m) with degrees $d_1 \leq \dots \leq d_m$; a maximal degree D

output: The elements of degree at most D of SG-bases of (f_1, \dots, f_m) .

$G := \emptyset$

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

Compute $\tilde{M}_{d,m}$ by Gaussian elimination from $M_{d,m}$.

Set $L_d := \{p \in Row(\tilde{M}_{d,m}) \mid LT(p) \notin LT(M_{d,m})\}$

$G := G \cup L_d$

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

- [1] Buchberger B., *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, Innsbruck, 1965
- [2] Buchberger B., *Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems*, Aequationes Math., 4, pages 374–383, 1970.
- [3] David A. Cox and John B. Little and Don O’Shea, *Ideals, Varieties, and Algorithms : An introduction to computational algebraic geometry and commutative algebra*, Undergraduate Texts in Mathematics. Springer Verlag, New York, 3rd ed.2007.
- [4] D.Lazard, *Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations*, Computer algebra (London, 1983), Lecture Notes in Comput. Sci.162.
- [5] D.Lazard, *Solving systems of algebraic equations*, ACM SIGSAM Bulletin, 35, pages 11–37, 2001.
- [6] Faugère, J-C. and Rahmany, S., *Solving systems of polynomial equations with symmetries using SAGBI-Gröbner bases*, ISSAC 2009.
- [7] F.S. Macaulay *On Some formulae in elimination*, proceedings of the London Mathematical Society, 33, page3–27, 1902.
- [8] F.S. Macaulay, *The Algebraic Theory of Modular Systems*, Cambridge Mathematical Librar, Cambridge University Press, 1916.
- [9] J.L.Miller, *Analogues of Gröbner bases in polynomial rings over a ring*, Journal of Symbolic Computation, 21(2), 139–153, 1996.
- [10] J.L.Miller, *Effective algorithm for intrinsically computing SAGBI-Gröbner bases in polynomial ring over a field*, Groebner bases and application (Linz),421–433, 1998.