Int. J. Nonlinear Anal. Appl. 9 (2018) No. 2, 215-221 ISSN: 2008-6822 (electronic) http://dx.doi.org/10.22075/ijnaa.2017.1718.1640



A new algorithm for computing SAGBI bases up to an arbitrary degree

Shahnaz Fakouri, Abdolali Basiri^{*}, Sajjad Rahmany Department of Mathematics and Computer Sciences, Damghan University, Damghan, Iran

(Communicated by M. Eshaghi)

Abstract

We present a new algorithm for computing a SAGBI basis up to an arbitrary degree for a subalgebra generated by a set of homogeneous polynomials. Our idea is based on linear algebra methods which cause a low level of complexity and computational cost. We then use it to solve the membership problem in subalgebras.

Keywords: SAGBI basis, SAGBI algorithm, Subalgebra membership problem, Homogeneous polynomial. 2010 MSC: Primary 8W30; Secondary 13P10.

1. Introduction

The concept of SAGBI bases for subalgebras, was introduced by Robbiano and Sweedler [4] and independently by Kapur and Madlener [1]. Like gröbner basis for an ideal, SAGBI basis for a subalgebra is a convenient basis which can be used to solve the membership problem: Given polynomials f and f_1, \ldots, f_s in the ring $\mathbb{K}[x_1, \ldots, x_n]$, we may ask whether f is an element of the subalgebra $\mathbb{K}[f_1, \ldots, f_s]$ or not. There exist algorithms for solving the subalgebra membership problem without using of SAGBI bases [2], but its complexity is high because of computing of Gröbner bases. If we have a SAGBI basis for a subalgebra we can solve this problem easily by using of subduction algorithm [6], But unfortunately, unlike the Gröbner bases, SAGBI bases may be infinite with respect to a certain term ordering.

^{*}Corresponding author

Email addresses: sh.fakouri@std.du.ac.ir (Shahnaz Fakouri), Basiri@du.ac.ir (Abdolali Basiri), rahmani@du.ac.ir (Sajjad Rahmany)

SAGBI is an abbreviation for Subalgebra Analog to Gröbner Bases for Ideals

In this paper, by just linear algebra methods, we present a new algorithm that computes a SAGBI basis up to an arbitrary degree with respect to a certain term ordering for a subalgebra, even if the subalgebra does not have a finite SAGBI basis with respect to this term ordering. Then we use this algorithm to solve the subalgebra membership problem and give a representation of a member of the subalgebra as a polynomial in the generators of the subalgebra.

The paper is organized as follows. In Section 2, we give some preliminaries of SAGBI bases, in Section 3, we present our algorithm and prove the correctness of this algorithm, finally in Section 4, we use this algorithm to solve the subalgebra membership problem and provide an example to show how the algorithm works.

2. SAGBI bases

In this section, we recall definitions and notations related to the SAGBI bases of subalgebras. Throughout this paper, \mathbb{K} is a field, x_1, \ldots, x_n and y_1, \ldots, y_s are algebraic independent variables over \mathbb{K} , $R = \mathbb{K}[x_1, \ldots, x_n]$ denotes the polynomial ring over \mathbb{K} and \prec is a admissible term ordering on R. We denote by $\langle f_1, \ldots, f_m \rangle$ the ideal generated by the polynomials $f_1, \ldots, f_m \in R$. Let $f = \sum_{\alpha} a_{\alpha} x^{\alpha} \in R$ where $a_{\alpha} \in \mathbb{K}$, then we denote by T(f) the set $\{x^{\alpha} \mid a_{\alpha} \neq 0\}$, while LT(f)is the max(T(f)) respect to \prec . We denote by LC(f), the coefficient of LT(f) in f, and also LM(f) = LC(f)LT(f). For $F \subset R$, we denote by LT(F) the set $\{LT(f) \mid f \in F\}$, by T(F) the union of T(f) where $f \in F$ and T = T(R). The notation |F| is cardinality of F. The total degree deg(t) of $t = x_1^{\alpha_1} \ldots x_n^{\alpha_n} \in T$ is given by $\sum_{i=1}^n \alpha_i$. A polynomial f is called homogeneous if all of members of T(f) have a same degree.

Let I be an ideal, a subset G of I is called a Gröbner basis for the ideal I if $\langle LT(G) \rangle = \langle LT(I) \rangle$. By Buchberger theorem [2] for each ideal in R there exists a finite Gröbner basis and we have an algorithm to compute it. Each Gröbner basis is also a generator for the ideal. By the usual polynomial multiplication, the ring R can be considered as a K-algebra. The most familiar example of the subalgebras of R is the subalgebra generated by finite numbers of polynomials f_1, \ldots, f_s . We denote this subalgebra by $\mathbb{K}[f_1, \ldots, f_s]$, i.e.

$$\mathbb{K}[f_1,\ldots,f_s] = \{p(f_1,\ldots,f_r) \mid p \in \mathbb{K}[y_1,\ldots,y_s]\}.$$

The subalgebra $\mathbb{K}[f_1, \ldots, f_s]$ is called homogeneous if all of f_1, \ldots, f_r are homogeneous.

Now we define the SAGBI basis of a \mathbb{K} -subalgebra of R which is equivalent of the Gröbner basis of an ideal of R.

Definition 2.1. Let A be a K-subalgebra of R. Then a set $F \subset A$ is called a SAGBI basis for A, if LT(F) generates the K-subalgebra $\mathbb{K}[LT(A)]$, i.e. $\mathbb{K}[LT(F)] = \mathbb{K}[LT(A)]$.

Note that the subalgebra A is a SAGBI basis for itself, thus each subalgebra always has a SAGBI basis. A SAGBI basis for the K-subalgebra A is a generator set for it. Moreover, if A has a finite SAGBI basis, an explicit representation of an element f of A as a polynomial in members of SAGBI basis, can be found quickly and efficiently by using the subduction algorithm as follows.

```
Subduction Algorithm

Input: A SAGBI basis F for A \subset \mathbb{R}, and A polynomial f \in \mathbb{R}.

Output: An expression of f as a polynomial in elements of F, provided f \in \mathbb{R}.

While f is not a constant in \mathbb{K} do

1. Find f_1, \ldots, f_r \in \mathbb{F}, exponents i_1, \ldots, i_r \in \mathbb{N} and c \in \mathbb{K}^*, s.th

LT(f) = c.LT(f_1)^{i_1} \ldots LT(f_r)^{i_r}, (2.1)

2. If no representation (2.1) exists, then output "f dose not lie in A".STOP

3. Otherwise p := c.y_1^{i_1} \ldots y_r^{i_r} and replace f := f - p(f_1, \ldots, f_r).

Output the polynomial \Sigma p(y_1, \ldots, y_r) + f.
```

For subalgebras that have finite SAGBI basis with respect a term ordering.

Fix a term ordering \prec and a set of polynomials $\{f_1, \ldots, f_s\}$ in $\mathbb{K}[x_1, \ldots, x_n]$ where for each $i, 1 \leq i \leq s$, $LT(f_i) = x^{a_i}$ and set $\mathcal{A} = \{a_1, \ldots, a_s\} \subset \mathbb{N}^n$. Let $\mathbf{A} = \mathbb{K}[f_1, \ldots, f_s]$ be the subalgebra generated by them. Consider the homomorphism from $\mathbb{K}[y_1, \ldots, y_s]$ onto \mathbf{A} defined by $y_i \mapsto f_i$, the kernel of this map is the *toric* ideal $I_{\mathcal{A}}$. There is a criterion for deciding whether the set $F \subset A$ is a SAGBI basis for A with respect to the term ordering \prec , see [6].

Theorem 2.2. Let $\{p_1, \ldots, p_m\}$ be generators of the toric ideal I_A . Then $\mathbf{F} = \{f_1, \ldots, f_s\}$ is a SAGBI basis if and only if the *subduction* algorithm reduces $p_i(f_1, \ldots, f_s)$ via F to a constant for all $i \in \{1, \ldots, s\}$.

So, we have an algorithm for computing SAGBI basis, [3]:

```
Input: \{f_1, \ldots, f_n\}

Output: A SAGBI basis F for R = \mathbb{K}[f_1, \ldots, f_s]

F := \{f_1, \ldots, f_s\}, oldF = \emptyset

while F <> oldF do

comput the generating set P for I_A

redP := \{ subduction(P(F) via F \} \setminus \{0\} ;

oldF := F;

F := F \cup oldF;

end do

RETURN F.
```

This algorithm is similar to Buchberger's Algorithm to compute Gröbner bases of ideals for computing SAGBI bases provided SAGBI bases are finite. However there are some conditions for having a finite SAGBI basis [5, 7] but in genral, the question of finding necessary and sufficient conditions for the subalgebra $A \subset R$ to have a finite SAGBI basis is an important open proeblem [6].

Definition 2.3. Let A be a subalgebra of the ring R. Let \prec be a term ordering on R and d be a positive integer. A SAGBI basis up to the degree d with respect to \prec for A is the set of all members of a SAGBI basis with respect to \prec for A which their degrees are equal or less than d.

By this definition, we can present below theorem similar to previous theorem:

Theorem 2.4. By above notations, let $\{p_1, \ldots, p_m\}$ be generators of the toric ideal I_A . Then $F = \{f_1, \ldots, f_k\}$ where $deg(f_j) = d_j$ is a SAGBI basis up to the degree d for A if and only if for each $1 \leq j \leq k$, we have $d_j \leq d$ and for each $1 \leq i \leq m$ such that $deg(p_i(f_1, \ldots, f_k)) \leq d$ the subduction algorithm reduces $p_i(f_1, \ldots, f_k)$ via F to a constant.

Proof . By the definition of SAGBI basis up to the degree d and the previous theorem the proof is straightforward. \Box

3. SAGBI basis up to an arbitrary degree

Let $F = \{f_1, \ldots, f_s\}$ be a finite subset of homogeneous polynomials in R, t be a positive integer and \prec be a admissible term ordering. Our aim, in this section, is to give a new practical algorithm to compute SAGBI basis up to the degree t with respect to \prec for homogeneous subalgebra $\mathbf{K}[f_1, \ldots, f_s]$ by just linear algebra methods. The SAGBI basis up to the degree t help us to solve the subalgebras membership problem and present an expression of f as a polynomial in generators $\{f_1, \ldots, f_s\}$, even if $\mathbb{K}[f_1, \ldots, f_s]$ does not have a finite SAGBI basis with respect to \prec .

We first review some of the standard facts on matrices and Gröbner bases. Let M be a $s \times m$ matrix, and $(\epsilon_i)_{i=1,\dots,m}$ be the canonical basis of \mathbb{K}^m . If $T' = \{t_1, \dots, t_m\}$ is a set of m terms, then we denote by $V_{T'}$ the \neg -submodule of R generated by T'. We define the linear map $\varphi_{T'} : V_{T'} \longrightarrow \mathbb{K}^m$ by $\varphi_{T'}(t_i) = \epsilon_i$. Let $(\alpha_1, \dots, \alpha_m)$ be an element of \mathbb{K}^m . Then $\sum_{i=1}^m \alpha_i t_i$ is an element in R. Therefore, by applying the reciprocal function of $\varphi_{T'}$, denoted it by $\psi_{T'}$, we can consider vectors in \mathbb{K}^m as polynomials in R. If row(M, i), i.e. i-th row of M, is considered as an element of \mathbb{K}^m , then we put

$$Rows(M, T') := \{ \psi_{T'}(row(M, i)) \mid i = 1, \cdots, s \} \setminus \{0\}.$$

Let F be a finite ordered subset of R and $T_{\prec}(F)$ be the ordered set T(F) with respect to an admissible ordering \prec . Then we can construct an $s \times m$ matrix $M^{(F,T(F))}$, where s and m are the |F| and $|T_{\prec}(F)|$, respectively, and the j-th element of the i-th row is the coefficient of the j-th element of $T_{\prec}(F)$ in the i-th element in F.

Definition 3.1. Let F be a finite subset of R and \prec be a admissible ordering. We define $T_{\prec}(F)$ to be the ordered set of T(F) with respect to \prec , $M := M^{(F,T(F))}$ and $\tilde{M} = Gaussian \ Elimination[\mathbb{K}](M)$. That Gaussian Elimination makes a copy of the Matrix M and reduces it to row echelon form (upper triangular form).

Definition 3.2. Let $F = \{f_1, \ldots, f_s\}$, where $degree(f_i) = d_i$. We define

$$M(F) = \{ f_1^{\alpha_1} f_2^{\alpha_2} \dots f_s^{\alpha_s} \mid (\alpha_1, \dots, \alpha_s) \in \mathbf{N}^s \}$$

to be the monomials in F. If $\alpha_1 d_1 + \cdots + \alpha_s d_s = d$, we say M(F) has degree d, and demonstrate it by $M(F)^d$.

Now we can present our main theorem:

Theorem 3.3. Let $F = \{f_1, \ldots, f_s\}$ be the set of homogeneous polynomials where $deg(f_i) = d_i$, d be a positive integer and \prec be an admissible term ordering. Consider the set F' be a SAGBI basis up to degree d for the subalgebra $\mathbb{K}[f_1, \ldots, f_s]$, $D = M(F')^{d+1}$, the set mon be the monomials with degree d + 1 in $\mathbb{K}[x_1, \ldots, x_n]$ and the matrix M as $M^{(D, mon_{\prec})}$, then the union of F' with the members of $Rows(\tilde{M}, mon_{\prec})$ which has obtained by row reduction operations will be a SAGBI basis up to degree d + 1 for the subalgebra $\mathbb{K}[f_1, \ldots, f_s]$.

Proof. Set $\mathcal{A} = \{a_1, \ldots, a_s\}$, by theorem 2.4, we need to show for each member p of the generating set of the toric ideal $I_{\mathcal{A}}$ which $deg(p(f_1, \ldots, f_s)) \leq d + 1$ the polynomial $p(f_1, \ldots, f_s)$ will be subduced via F to a constant. Since F' is a SAGBI basis up to the degree d and F contains F', if $deg(p(f_1, f_s)) \leq d$ then $p(f_1, \ldots, f_s)$ will be subduced via F to a constant. So the proof is completed by showing that for each p satisfied in $deg(p(f_1, \ldots, f_s)) = d + 1$, the polynomial $p(f_1, \ldots, f_s)$ will be subduced to a constant.

As above notations, the rows of the matrix M are indexed by the ordered set mon_{\prec} (all monomials in $\{x_1, \ldots, x_n\}$ with degree d + 1) and it's columns are indexed by all monomials with degree d + 1constructed by the members of F'. Since the matrix \tilde{M} is the reduced form of M as row echelon form (upper triangular form), so the rows of \tilde{M} obtained by row addition operation, are all reduced polynomials $p(f_1, \ldots, f_s)$ with degree d + 1 that p_s are the algebraic relations between the leading terms of the members of F'. In fact p_s are members of the generating set of the toric ideal I_A which $deq(p(f_1, \ldots, f_s)) = d + 1$ and the proof will be completed. \Box

This theorem can be used to construct an algorithm for computing SAGBI bases of homogeneous subalgebras.

```
 \begin{array}{l} \textbf{SAGBI Algorithm} \\ \textbf{Input: } A = \mathbb{K}[f_1, \ldots, f_s], \text{ a homogeneous subalgebra in } R \ , t, \text{ a positive integer and } \prec, \text{ a term order} \\ \textbf{Output: } F', \text{ a SAGBI basis up to degree } t \ \text{for } A \ \text{with respect to } \prec \\ F := [f_i \mid degree(f_i) \leq t] \\ d := 1 \\ F' := F; \\ \textbf{While } d \leq t \ \textbf{do} \\ D := M(F')^d; \\ mon := [x_1^{\alpha_1} \dots x_n^{\alpha_n} \mid (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n, \alpha_1 + \dots + \alpha_n = d], \text{ the monomials} \\ \text{with degree } d \ \text{in } \mathbb{K}[x_1, \dots, x_n]. \\ M := M^{(D, mon_{\prec})}; \\ rows := \left\{ \text{the numbers of } Rows(\tilde{M}, mon_{\prec}) \text{that obtained by row addition operations} \right\} \\ F' := F' \cup rows; \\ d := d + 1; \\ \textbf{Return } F' \end{aligned}
```

In this algorithm, in each step there may be some zero rows in the matrix \tilde{M} that are ineffective, for reducing the number of this rows we present below proposition and improve presented algorithm.

Proposition 3.4. Under the assumption of the presented theorem, if in d-th step of the algorithm the new polynomial $f = \sum_{i=1}^{k} c_j F_j$, where $F_j \in M(F')^d$, is added to the SAGBI basis F' and for some $1 \leq m \leq k$, F_m belongs to $F = \{f_1, \ldots, f_s\}$, then for each $d' \geq d$ the set of non zero rows of \tilde{M} constructed by $M(F')^{d'}$ is equal with the set of non zero rows of \tilde{M} constructed by $M(F')^{d'}$.

Proof. Since \tilde{M} is upper triangular form, so it is easily seen that the leading terms of F_m and $f - c_m F_m = \sum_{j \neq m} c_j F_j$ are equal. And if for some d' and $q \in R$ we have qF_m belongs to $M(F')^{d'}$ then qf and qF_1, \ldots, qF_k also belong to it (because the degrees of f and F_1, \ldots, F_k are equal). These follow that the leading terms of qF_m and $q\Sigma_{j\neq m}c_jF_j$ are equal and the row indexed by qf will be equal with the row $qc_mF_m + q\Sigma_{j\neq m}c_jF_j$ constructed by row reduction operations hence we have a zero row in the matrix \tilde{M} . \Box

4. Subalgebra membership problem and example

In later section, an algorithm was presented that computes a SAGBI basis up to an chosen degree for the given subalgebra, in this section by an example we show how this algorithm works and use this algorithm for solving the subalgebra membership problem.

Lemma 4.1. (Robbiano and Sweedler, [5]): Let $G = \{g_1(X), \ldots, g_t(X)\}$ be a SAGBI basis up tp degree d with respect to \prec . Then for each $f \in A$ of degree $\leq d$, the subduction algorithm comput a polynomial $F \in \mathbb{K}[y_1, \ldots, y_t]$ such that $f(X) = F(g_1(X), \ldots, g_t(X))$.

By this lemma, we are sure that by computing SAGBI basis up to degree d for subalgebra A, we can answer this guestion whether a polynomial f with degree d is in R or not.

Example 4.2. Consider the subalgebra

$$\mathbf{R} = \mathbb{K}[x_1 + x_2 + x_3, x_1x_2 + x_1x_3 + x_2x_3, x_1x_2x_3, (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)]$$

R is the subalgebra of polynomials which are invariant under the cyclic permutation $x_1 \mapsto x_2, x_2 \mapsto x_3, x_3 \mapsto x_1$. Let \prec be the lexicographic term order with $x_1 \succ x_2 \succ x_3$. R has not finite SAGBI basis with respect to \prec , see [6].

Consider the homogenous polynomial $f = x_1^2 x_3 + x_2^2 x_3 + x_3^2 x_1 + x_3^2 x_2 + x_1^2 x_2 + x_2^3 x_1$, we know this

belongs to subalgebra R, since it is invariant under the given permutation. We want to demonstrate it by our algorithm.

Degree(f) = 3, so the input of SAGBI algorithm are the generators of R and the number 3, output of algorithm will be SAGBI basis up to degree 3 for the subalgebra R.

 $F = \{x_1 + x_2 + x_3, x_1x_2 + x_1x_3 + x_2x_3, x_1x_2x_3, (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)\}.$ d = 1 $F' = \{x_1 + x_2 + x_3, x_1x_2 + x_1x_3 + x_2x_3, x_1x_2x_3, (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)\}$ $d = 1 \le 3 \text{ so } D = M(F)^1 = [f_1]$ $mon = [x_1, x_2, x_3]$ $M = f_1 \left(\begin{array}{ccc} 1 & 1 & 1 \end{array} \right)$ $rows = \{\}$ $F' = \{x_1 + x_2 + x_3, x_1x_2 + x_1x_3 + x_2x_3, x_1x_2x_3, (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)\}$ $d = 2 \le 3 \text{ so } D = M(F)^2 = [f_1^2, f_2]$ $mon = [x_1^2, x_1x_2, x_2^2, x_1x_3, x_2x_3, x_3^2]$ $M = \begin{cases} f_1^2 \left(\begin{array}{ccc} 1 & 2 & 1 & 2 & 2 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{cases} \right)$

 $mon = [x_1^3, x_1^2x_2, x_1x_2^2, x_2^3, x_1^2x_3, x_1x_2x_3, x_2^2x_3, x_1x_3^2, x_2x_3^2, x_3^3]$

							$x_1 x_2 x_3$				
M =	f_{1}^{3}	(1)	3	3	1	3	6	3	3	3	$1 \rangle$
	$f_{1}f_{2}$	0	1	1	0	1	3	1	1	1	0
	$f_4 - f_1 f_2$	0	0	-2	0	-2	-3	0	0	-2	0
	$-2f_{3}$	$\int 0$	0	10	0	0	-2	0	10	0	0 /

 $rows = \{f_4 - f_1 f_2\}$

 $F' = \{x_1 + x_2 + x_3, x_1x_2 + x_1x_3 + x_2x_3, x_1x_2x_3, (x_1 - x_2)(x_1 - x_3)(x_2 - x_3), -2x_1x_2^2 - 2x_1^2x_3 - 3x_1x_2x_3 - 2x_2x_3^2\}$

d = 4 > 3 so algorithm returns F' as a SAGBI basis up to degree 3 for R.

The rows of latest matrix are all products of members of SAGBI basis with degree 3, so we can subduce the polynomial f by these. By this subduction we have $f = f_1 f_2 - 3f_3$.

Now it remains when the polynomial f is not homogeneous, for checking this case consider the following definition:

Definition 4.3. Given a polynomial $f \in \mathbb{K}[x_1, \ldots, x_n]$ of degree s, let f_k be the sum of all terms of f of degree k. Then each f_k is homogeneous and $f = \sum_{1 \le k \le s} f_k$. We call f_k the kth homogeneous component of f.

If the polynomial f of degree s was not homogeneous, we consider f as a sum of its homogeneous components and set $d = [d_1, \ldots, d_t] = [degree(f_k), 1 \le k \le s]$. Then by SAGBI algorithm, we compute SAGBI basis up to degree s, and for each i where $1 \le i \le t$ in i-th step of algorithm subduce the homogeneous component of degree d_i as explained example. Finally the sum of these subductions will be subduction of polynomial f.

5. Acknowledgments

The authors would like to thank Damghan university for supporting this research.

References

- [1] D. Kapur and K. Madlener, A completion procedure for computing canonical basis for a k-subalgebra, Computers and Mathematics, Springer, New York, NY, 1989. 1–11.
- [2] J.B. Little and D. O'Shea, Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, Undergraduate texts in mathematics, Springer, New-York, 2007.
- [3] J.L. Miller, Analogs of Gröbner bases in polynomial rings over a ring, J. Symb. Comput. 21 (1996) 139–153.
- [4] L. Robbiano and M. Sweedler, Ideal and subalgebra coefficients, Proc. Amer. Math Soc. 126 (1998) 2213–2219.
- [5] L. Robbiano and M. Sweedler, Subalgebra bases, Springer, Berlin, Heidelberg, 1990, 61–87.
- [6] B. Sturmfels, Gröbner Bases and Convex Polytopes, Vol. 8. American Mathematical Soc., 1996.
- [7] A. Torstensson, Canonical bases for subalgebras on two generators in the univariate polynomial ring, Beitr. Algebra Geom. 43 (2002) 565–577.