Computer Science Journal of Moldova, vol.**13**, no.3(39), 2005

A note on Computing SAGBI-Gröbner bases in a Polynomial Ring over a Field

Hans Öfverbeck

Abstract

In the paper [2] Miller has made concrete Sweedler's theory for ideal bases in commutative valuation rings (see [5]) to the case of subalgebras of a polynomial ring over a field, the ideal bases are called SAGBI-Gröbner bases in this case. Miller proves a concrete algorithm to construct and verify a SAGBI-Gröbner basis, given a set of generators for an ideal in the subalgebra. The purpose of this note is to present an observation which justifies substantial shrinking of the so called syzygy family of a pair of polynomials. Fewer elements in the syzygy family means that fewer syzygy-polynomials need to be checked in the SAGBI-Gröbner basis construction/verification algorithm, thus decreasing the time needed for computation.

1 Introduction

SAGBI-Gröbner theory is a generalisation of Gröbner theory to subalgebras of a polynomial ring. Thus we consider a fixed subalgebra A of a polynomial ring $k[X] = k[x_1, \ldots, x_n]$ over a field k, and we want to do Gröbner theory in the subalgebra A.

In Gröbner basis theory a so called *S-polynomial* of a pair (f, g) of polynomials is defined as (see the next section for the exact definitions of the notation):

$$S(f, g) = L_1 f - L_2 g, \tag{1}$$

where

$$L_1 = \frac{\mathrm{lcm}(\mathrm{lp}(f), \mathrm{lp}(g))}{\mathrm{lt}(f)}, \qquad L_2 = \frac{\mathrm{lcm}(\mathrm{lp}(f), \mathrm{lp}(g))}{\mathrm{lt}(g)}.$$

In SAGBI-Gröbner basis theory the analogue of a S-polynomial of a pair is the *syzygy family* of a pair (f, g). As the name indicates, the syzygy family usually consists of more than one element, but all the elements have the form (1) for some $(L_1, L_2) \in A^2$ such that $\mathrm{lt}(L_1 f) = \mathrm{lt}(L_2 g)$. The purpose of this note is to prove that when constructing the syzygy family we need only consider polynomials of the form (1) where $(L_1, L_2) \in A^2$ are such that $\mathrm{lp}(g)$ does not divide $\mathrm{lp}(L_1)$ and $\mathrm{lp}(f)$ does not divide $\mathrm{lp}(L_2)$ in $\mathrm{Lp}(A)$.

This yields a substantially smaller syzygy family than what is indicated in [2].

2 Notation

Since the purpose of this note is to refine a result in the article [2] we try to follow the notation there as closely as possible. Let $k[X] = k[x_1, \ldots, x_n]$ be multivariate polynomial ring over a field k. Suppose we have a term order on $k[X]$, then for a polynomial $p \in k[X]$, $\mathrm{lp}(p)$ denotes the leading X-power product of p, $\mathrm{lc}(p)$ the leading coefficient of p, and $\mathrm{lt}(p) = \mathrm{lc}(p)\mathrm{lp}(p)$ the leading term of p. If $S \subseteq k[X]$, then $\mathrm{Lp}(S)$ denotes $\{\mathrm{lp}(s) | s \in S\}$.

If $w = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$ is an X power product then the *multidegree*, $\mathrm{mdeg}(w)$, of w is defined as $\mathrm{mdeg}(w) = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{N}^n$. For a polynomial $f \in k[X]$ we define $\mathrm{mdeg}(f) = \mathrm{mdeg}(\mathrm{lp}(f))$.

For a vector $v = (v_1, \ldots, v_m) \in \mathbb{N}^m$ and a (implicitly ordered) set $S = \{s_1, \ldots, s_m\} \in k[X]$ with m elements we define:

$$S^v = \prod_{j=1}^{m} s_j^{v_j}.$$

Let A be fixed subalgebra of $k[X]$, then $\mathrm{Lp}(A)$ is a multiplicative monoid. For an ideal I in A, $\mathrm{Lp}(I)$ is a monoid-ideal in $\mathrm{Lp}(A)$. A *SAGBI-Gröbner basis* for an ideal I in A is a subset $G \subseteq I$ such that $\mathrm{Lp}(G)$ generates $\mathrm{Lp}(I)$ as a monoid-ideal in $\mathrm{Lp}(A)$.

For an ideal J in $k[X]$ an ordinary Gröbner basis is a subset $G' \subseteq J$ such that $\mathrm{Lp}(G')$ generates J as a monoid ideal in $\mathrm{Lp}(k[X])$. This

corresponds to the special case $A = k[X]$ for SAGBI-Gröbner bases, thus we can say that SAGBI-Gröbner bases are a generalisation of Gröbner bases. On the other hand SAGBI-Gröbner bases are a special case of the even more general bases presented in [5] and [4].

Throughout this article we assume that we have a finite SAGBI basis $F = \{f_1, \ldots, f_m\}$ for the subalgebra A, i.e. $F \subseteq A$ and $\mathrm{Lp}(F)$ generates $\mathrm{Lp}(A)$ as monoid.

When dealing with ideals in the subalgebra A we need an analogue of ordinary reduction which takes into account the fact that we work inside a subalgebra, the analogue is called SI-reduction.

Definition 1 (SI-reduction) *Let $G \subseteq A$. A polynomial $h \in A$* SI-reduces via *G to $h' \in A$ in one step if there is a nonzero term cX^α of h for which there exists $g \in G$ and $a \in A$ such that $\mathrm{lt}(ag) = cX^\alpha$ and $h' = h - ag$. If there is a chain of one-step reductions from h to h'' via G, then we say that h* SI-reduces *to h'' via G.*

3 Shrinking the syzygy family

Consider the intersection, $\langle \mathrm{lp}(g) \rangle \bigcap \langle \mathrm{lp}(h) \rangle$, of the monoid ideals generated by $\mathrm{lp}(g)$ and $\mathrm{lp}(h)$ in $\mathrm{Lp}(A)$. The intersection is again a monoid ideal in $\mathrm{Lp}(A)$, which plays a central part in the definition of the syzygy family:

Definition 2 (Definition 4.1 in [2]) *Given $g, h \in A$ and a generating set $T_{g,h}$ in $\mathrm{Lp}(A)$ for $\langle \mathrm{lp}(g) \rangle \bigcap \langle \mathrm{lp}(h) \rangle$, a* syzygy family *for g and h is a set that contains, for each $t \in T_{g,h}$ a polynomial of the form $a_t g - b_t h$ with $\mathrm{lt}(a_t g) = \mathrm{lt}(b_t h) = \mathrm{lt}(c_t t)$ for some $c_t \in k$.*

Consider Corollary 4.6 in [2]; there we are told that a syzygy family for g and h can be constructed in the following way:

Let $\mathcal{V}$ be a finite generating set of the monoid of nonnegative integer solutions $v = (v_1, v_2, \ldots, v_{2m+2})$ of:

$$v_1 \mathrm{mdeg}(g) + \sum_{j=1}^{m} v_{j+1} \mathrm{mdeg}(f_j) = \sum_{j=1}^{m} v_{m+1+j} \mathrm{mdeg}(f_j) + v_{2m+2} \mathrm{mdeg}(h) \tag{2}$$

where $\{f_1, \ldots, f_m\} = F$ is our SAGBI basis for A.

A minimal generating set of the nonnegative solutions of a diophantine system such as (2) is sometimes called a *Hilbert basis* for the solutions. There exist several algorithms to calculate the Hilbert basis, e.g. those described in [1] and [3], this allows us to effectively compute $\mathcal{V}$.

For an element v of $\mathcal{V}$ we let $v^l = (v_1, \ldots, v_{m+1})$ and $v^r = (v_{m+2}, \ldots, v_{2m+2})$, then v is called the *parent vector* of v^l and v^r. Let

$$\mathcal{V}' = \{v \in \mathcal{V} \,|\, v_1 = v_{2m+2} = 1\}$$

and

$$\mathcal{V}'' = \{u + v \,|\, u \in \mathcal{V}_1, v \in \mathcal{V}_2\}$$

where $\mathcal{V}_1 = \{u \in \mathcal{V} \,|\, u_1 = 1, u_{2m+2} = 0\}$ and $\mathcal{V}_2 = \{v \in \mathcal{V} \,|\, v_1 = 0, v_{2m+2} = 1\}$, and let

$$\mathcal{PV} = \mathcal{V}' \cup \mathcal{V}''.$$

Finally let $G = \{g, f_1, \ldots, f_m\}$ and $H = \{f_1, \ldots, f_m, h\}$, (where $f_1, \ldots, f_m$ are the elements of our SAGBI basis F) then by Corollary 4.6 in [2] a syzygy family for g and h is formed by all polynomials of the form

$$s_v = \mathrm{lc}(H^{v^r}) \cdot G^{v^l} - \mathrm{lc}(G^{v^l}) \cdot H^{v^r}$$

where $v \in \mathcal{PV}$.

The purpose of this note is to prove that in the definition of $\mathcal{PV}$ we can remove the second set from the union and let $\mathcal{PV} = \mathcal{V}'$ and the only price we have to pay for this reduction is to add 0 to the syzygy family.

Theorem 1 (Refinement of Corollary 4.6 in [2])
Let $G = \{g, f_1, \ldots, f_m\}$ and $H = \{f_1, \ldots, f_m, h\}$, let $\mathcal{V}$ be a finite generating set for the monoid of nonnegative solutions of the system of equations (2) and let $\mathcal{PV} = \mathcal{V}'$. Then the set S consisting of 0 and all polynomials of the form $s_v = \mathrm{lc}(H^{v^r}) \cdot G^{v^l} - \mathrm{lc}(G^{v^l}) \cdot H^{v^r}$, where the parent vector v of v^l and v^r lies in $\mathcal{V}'$, is a syzygy family for g and h.

Proof. According to Definition 2 a syzygy family for g and h is only required to contain *a* polynomial $a_t g - b_t h$ for each $t \in T_{g,h}$, thus if we can replace the polynomial $a_t g - b_t h$ with a simpler one: $a'_t g - b'_t h$ still having $\mathrm{lt}(a'_t g) = \mathrm{lt}(b'_t h) = c_t t$ for some $c_t \in k$, then we still have a syzygy family for g and h. In view of Corollary 4.6 from [2] we need only prove that for each power product t appearing as the leading power product of a polynomial $\mathrm{lc}(H^{v^r}) \cdot G^{v^l}$, where $v \in \mathcal{V}''$, there exist $a_t, b_t \in A$, $c_t \in k \backslash \{0\}$ such that $\mathrm{lt}(a_t g) = \mathrm{lt}(b_t h) = c_t t$ and $a_t g - b_t h = 0$. Let $v = u + w$ where $u \in \mathcal{V}_1$ and $w \in \mathcal{V}_2$ and let $t = \mathrm{lp}(G^{v^l}) = \mathrm{lp}(H^{v^r})$. Since u and w are solutions of (2) we know that:

$$\begin{aligned} \mathrm{lp}(G^{u^l}) &= \mathrm{lp}(H^{u^r}), \\ \mathrm{lp}(G^{w^l}) &= \mathrm{lp}(H^{w^r}). \end{aligned} \tag{3}$$

Since $u \in \mathcal{V}_1$ and $w \in \mathcal{V}_2$ their left and right halves have the form $u^l = (1, u_2, \ldots, u_{m+1})$ and $w^r = (w_{m+2}, \ldots, w_{2m+1}, 1)$, thus if we let $u' = (u_2, \ldots, u_{m+1})$ and $w' = (w_{m+2}, \ldots, w_{2m+1})$ we get:

$$\begin{aligned} G^{u^l} &= g F^{u'}, \\ H^{w^r} &= F^{w'} h. \end{aligned} \tag{4}$$

Let $a_t = F^{u'} F^{w'} h$ and $b_t = F^{u'} F^{w'} g$. Then $a_t, b_t \in A$ and:

$$\mathrm{lt}(a_t g) = \mathrm{lt}(b_t h) = \mathrm{lt}(F^{u'} F^{w'} g h) = \mathrm{lt}(g F^{u'}) \mathrm{lt}(F^{w'} h) = \mathrm{lt}(G^{u^l}) \mathrm{lt}(H^{w^r})$$

where the last equality follows from (4). Since $\mathrm{lp}(H^{w^r}) = \mathrm{lp}(G^{w^l})$ according to (3), we can deduce that $\mathrm{lt}(H^{w^r}) = c_t \mathrm{lt}(G^{w^l})$ for some nonzero constant $c_t \in k$. Thus

$$\mathrm{lt}(G^{u^l}) \mathrm{lt}(H^{w^r}) = c_t \mathrm{lt}(G^{u^l}) \mathrm{lt}(G^{w^l}) = c_t \mathrm{lt}(G^{u^l + w^l}) = c_t \mathrm{lt}(G^{v^l}) = c'_t t$$

where $c'_t \in k \setminus \{0\}$, the next last equality is due to $v = u + w$ and the last equality follows from our definition $t = \mathrm{lp}(G^{v^l})$. Hence $a_t g - b_t h$ is an element of the syzygy family corresponding to t. Finally we note that

$$a_t g - b_t h = F^{u'} F^{w'} h g - F^{u'} F^{w'} g h = 0.$$

□

The practical use of the syzygy family is to check if a given set is a SAGBI-Gröbner basis, much like S-polynomials are used to check if a set is a Gröbner basis. More precisely a set $G \subseteq A$ is a SAGBI-Gröbner basis if and only if all polynomials in all syzygy families of pairs in G SI-reduce to zero via G, cf. Theorem 5.1 and Algorithm 3 in [2]. A zero SI-reduced remainder indicates that no violation of the SAGBI-Gröbner condition is found for this particular syzygy-polynomial, thus we can remove the extra zero indicated in Corollary 1 from the syzygy family without making the syzygy family less useful. The refinement of Algorithm 2 in [2] becomes:

Algorithm 1

Input: $g, h \in A$, *a finite SAGBI basis* F *for* A
Output: A syzygy family $\mathrm{SyzFam}(g,h)$ *for* g *and* h
Initialisation: $\mathrm{SyzFam}(g,h) := \emptyset$, $\mathcal{PV} := \emptyset$
Compute a generating set $\mathcal{V}$ *for the solutions of system (2).*
$\mathcal{PV} := \{v \in \mathcal{V} : c_0 = d_0 = 1\}$
For Each $v \in \mathcal{PV}$*:*
$\quad s_v := \mathrm{lc}(H^{v^r}) \cdot G^{v^l} - \mathrm{lc}(G^{v^l}) \cdot H^{v^r}$
$\mathrm{SyzFam}(g,h) := \bigcup_{v \in \mathcal{PV}} \{s_v\}$

An implementation of this algorithm is included in the author's Maple package for SAGBI and SAGBI-Gröbner computations, see [6]. For calculating the Hilbert bases the Maple package uses Dmitrii V. Pasechnik's implementation of the algorithm described in [3].

As an application of Algorithm 1 we consider example 4.7 and 5.2 in [2].

Example 1 *Let* $A = \mathbb{Q}[x^2, xy] \subseteq \mathbb{Q}[x,y]$ *and use the degree lexicographical order with* $x > y$. *The set* $F = \{x^2, xy\}$ *is a SAGBI basis for* A. *Let* $g = x^3y + x^2$ *and* $h = x^4 + x^2y^2$ *in* A. *A Hilbert basis for the set of solutions of the equation (2) is:*

$$v^{(1)} = (0,0,1,0,1,0), \quad v^{(2)} = (0,1,0,1,0,0), \quad v^{(3)} = (0,2,0,0,0,1),$$
$$v^{(4)} = (1,0,0,1,1,0), \quad v^{(5)} = (1,1,0,0,1,1), \quad v^{(6)} = (2,0,0,0,2,1).$$

Thus $\mathcal{PV} = \{v^{(5)}\}$*, so by Algorithm 1 a syzygy family for* (g, h) *is* $\{G^{(1,1,0)} - H^{(0,1,1)}\} = \{-x^3y^3 + x^4\}$.

In the original version of this example (example 4.7 in [2]) the syzygy family was $\{-x^5y^3 + x^6, -x^3y^3 + x^4\}$ *instead. It should however be noted (as proved in example 5.2, [2]) that the extra syzygy polynomial* $-x^5y^3 + x^6$ *SI-reduces to zero over* $\{g, h\}$*. Thus this extra polynomial does not affect the final result of the SAGBI-Gröbner basis computations. That the extra syzygy polynomial does not effect the further computations is a consequence of Theorem 1.*

References

[1] Evelyne Contejean and Hervé Devie. An efficient incremental algorithm for solving systems of linear Diophantine equations. *Inform. and Comput.*, 113(1):143–172, 1994.

[2] J. Lyn Miller. Effective algorithms for intrinsically computing SAGBI-Gröbner bases in a polynomial ring over a field. In *Gröbner bases and applications (Linz, 1998)*, volume 251 of *London Math. Soc. Lecture Note Ser.*, pages 421–433. Cambridge Univ. Press, Cambridge, 1998.

[3] Dmitrii V. Pasechnik. On computing Hilbert bases via the Elliot-MacMahon algorithm. *Theoret. Comput. Sci.*, 263(1-2):37–46, 2001. Combinatorics and computer science (Palaiseau, 1997).

[4] Lorenzo Robbiano. On the theory of graded structures. *J. Symbolic Comput.*, 2(2):139–170, 1986.

[5] Moss Sweedler. Ideal bases and valuation rings. Manuscript, 1988.

[6] Hans Öfverbeck. *HilbertSagbiSg, Maple packages for Hilbert, SAGBI and SAGBI-Gröbner basis calculations.*, 2005. `http://www.maths.lth.se/matematiklu/personal/hans/maple`.

Hans Öfverbeck,

Received December 9, 2005

Centre for Mathematical Sciences
Lund University
Box 118, SE-221 00 Lund
Sweden
E–mail: *hans@maths.lth.se*