MATHEMATICS OF COMPUTATION
Volume 71, Number 238, Pages 761–765
S 0025-5718(01)01405-3
Article electronically published on October 25, 2001

FINITE SAGBI BASES FOR POLYNOMIAL INVARIANTS OF CONJUGATES OF ALTERNATING GROUPS

MANFRED GÖBEL

ABSTRACT. It is well-known, that the ring $\mathbb{C}[X_1, \ldots, X_n]^{A_n}$ of polynomial invariants of the alternating group A_n has no finite SAGBI basis with respect to the lexicographical order for any number of variables $n \geq 3$. This note proves the existence of a nonsingular matrix $\delta_n \in GL(n, \mathbb{C})$ such that the ring of polynomial invariants $\mathbb{C}[X_1, \ldots, X_n]^{A_n^{\delta_n}}$, where $A_n^{\delta_n}$ denotes the conjugate of A_n with respect to δ_n, has a finite SAGBI basis for any $n \geq 3$.

1. INTRODUCTION

It was shown in [5] that invariant rings of permutation groups G have a finite SAGBI (**S**ubalgebra **A**nalogue to **G**röbner **B**asis for **I**deals) basis with respect to the lexicographical order iff G is a direct product of symmetric groups. This result is from the computer algebra point of view very discouraging. Only in a few special cases can finite SAGBI bases be used to study such invariant rings and to rewrite their corresponding polynomial invariants. Mainly because of the nonfiniteness of SAGBI bases, which I first noted for invariant rings of the alternating group in three variables, a novel reduction technique for polynomial invariants of permutation groups was experimentally discovered in 1991, described and investigated in [2] and [3], and implemented in [4].

The idea to rewrite elements of invariant rings of permutation groups with finite SAGBI basis goes—as far as I know—back to Weispfenning in 1991. His first advice to me was to reduce polynomial invariants of permutation groups in a similar way as the classical algorithm of Gauß rewrites symmetric functions [1]. This algorithm is based on the fact that the n elementary symmetric polynomials

$$\begin{array}{rcl} \sigma_1 & = & X_1 + \ldots + X_n, \\ \sigma_2 & = & X_1X_2 + \ldots + X_{n-1}X_n, \\ \ldots & & \ldots \\ \sigma_n & = & X_1 \ldots X_n \end{array}$$

are a SAGBI basis with respect to any admissible order [10] for the ring of symmetric functions [8].

Until the end of 1996, my personal impression was that SAGBI bases can play only a very limited rôle for the analysis of invariant rings of permutation groups.

Received by the editor September 7, 1999 and, in revised form, July 19, 2000.
2000 *Mathematics Subject Classification.* Primary 13A50, 12Y05; Secondary 20B35, 14Q99.
Key words and phrases. Algorithmic invariant theory, finite SAGBI bases, alternating groups, rewriting techniques.

In early 1997, Sturmfels brought my attention back to SAGBI bases and explained to me that it is important to study them further. He asked me to investigate the finiteness of SAGBI bases with respect to the lexicographical order for invariant rings of permutation groups similarly to what I had done before for the alternating group in three variables [2, 9]. Shortly after writing [5], I was able to state a conjecture saying that invariant rings of conjugates of permutation groups may have a finite SAGBI bases with respect to the lexicographical order [7]. Furthermore, I was able to prove this conjecture for the alternating group in three variables [6].

What makes this conjecture so significant in the theory of SAGBI bases for invariants of permutation groups? It is, of course, the fact that if we can compute a finite SAGBI basis $\hat{B}$ for the invariant ring of a conjugate of a permutation group G,

1. we can use this basis $\hat{B}$ for a *guided* reduction of the elements of the invariant ring of the permutation group G by applying a simple linear transformation, and
2. we can compute a basis B *with almost SAGBI basis properties* for the invariant ring of the permutation group G.

Putting all this together brings me to the conclusion that Weispfenning's idea to treat invariants of permutation groups by means of SAGBI bases may still have a chance to work simply by applying a certain, well-chosen linear transformation to the given invariant ring of the permutation group G.

This goal of this note is to present a proof for the conjecture of [7] in the case of invariant rings of conjugates of alternating groups for any number of variables. The plan here is as follows: After introducing the basic notation in Section 2, we are going to state and prove our result in Section 3. Eventually, Section 4 concludes with some open problems.

2. Basics

The setting is the same as in [5] and [6]. $\mathbb{N}$ and $\mathbb{C}$ denote the natural and complex numbers. $\mathbb{C}[X_1, \ldots, X_n]$ is the commutative polynomial ring over $\mathbb{C}$ in the indeterminates $X_1, \ldots, X_n$, and T is the set of terms (= power-products of the X_i) in $\mathbb{C}[X_1, \ldots, X_n]$.

Let G be a group of permutations operating on $X_1, \ldots, X_n$, let $\pi \in G$, and let $f \in \mathbb{C}[X_1, \ldots, X_n]$. Then $\pi(f)$ is defined as $f(\pi(X_1), \ldots, \pi(X_n))$, and f is called G-invariant, if $f = \pi(f)$ for all $\pi \in G$. $\mathbb{C}[X_1, \ldots, X_n]^G$ denotes the $\mathbb{C}$-algebra of G-invariant polynomials in $\mathbb{C}[X_1, \ldots, X_n]$,

$$orbit_G(t) = \sum_{s \in \{\pi(t) \mid \pi \in G\}} s$$

the G-invariant orbit of $t \in T$, and S_n and A_n are the symmetric and alternating group operating on the variables $X_1, \ldots, X_n$. $\delta_n = (d_{ij})_{1 \leq i,j \leq n} \in GL(n, \mathbb{C})$ denotes a nonsingular $n \times n$ matrix, $A_n^{\delta_n} = \{\delta_n^{-1} \pi \delta_n \mid \pi \in A_n\}$ the conjugate of A_n with respect to δ_n, and $\delta_n(f)$ is defined as $f(\sum_{j=1}^n d_{1j} X_j, \ldots, \sum_{j=1}^n d_{nj} X_j)$.

Let $<_{lex}$ be the lexicographical order on T with $X_1 >_{lex} \ldots >_{lex} X_n$, and let $HT(f)$ and $HC(f)$ be the head term of $f \in \mathbb{C}[X_1, \ldots, X_n]$, and the coefficient of $HT(f)$ with respect to $<_{lex}$, respectively. A SAGBI basis B of a subalgebra of $\mathbb{C}[X_1, \ldots, X_n]$ is such that with respect to a given admissible order, say $<_{lex}$, every head term of an element in the subalgebra can be expressed as a product of head terms of the elements in B [8]. We assume in the following that $n \geq 3$.

3. A finite SAGBI basis for $\mathbb{C}[X_1, \ldots, X_n]^{A_n^{\delta_n}}$

Theorem 3.1. *The invariant ring $\mathbb{C}[X_1, \ldots, X_n]^{A_n}$ is generated by the set B consisting of the n elementary symmetric polynomials $\sigma_1, \ldots, \sigma_n$ and*

$$\sigma_{n+1} = orbit_{A_n}(X_1^{n-1}X_2^{n-2}\ldots X_{n-2}^2X_n).$$

The total degree of σ_i is i for $1 \leq i \leq n$, and the total degree of σ_{n+1} is $\frac{n(n-1)}{2}$.

Furthermore, $\mathbb{C}[X_1, \ldots, X_n]^{A_n}$ has no finite SAGBI bases with respect to $<_{lex}$, and especially, B is not such a finite SAGBI basis.

Proof. See [3] and [9] for the case $n = 3$, and see [5] for the general case $n \geq 3$. □

Lemma 3.2. *Let $\sigma_1, \ldots, \sigma_{n+1}$ be as in Theorem 3.1, and let $\delta_n \in GL(n, \mathbb{C})$ be defined as*

$$\delta_n = \begin{pmatrix} 1 & \ldots & 0 & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & \ldots & 0 & 1 & 0 & 0 \\ 0 & \ldots & 0 & 0 & 1 & 1 \\ 0 & \ldots & 0 & 0 & -1 & 1 \end{pmatrix}.$$

Then the following hold:

1. $\det(\delta_n) = 2$.
2. $HC(\delta_n(\sigma_i)) = 1$, $HT(\delta_n(\sigma_i)) = X_1X_2\ldots X_i$ *for* $1 \leq i \leq n-2$.
3. $HC(\delta_n(\sigma_{n-1})) = 1$, $HT(\delta_n(\sigma_{n-1})) = X_1X_2\ldots X_{n-2}X_n$.
4. $HC(\delta_n(\sigma_n)) = -1$, $HT(\delta_n(\sigma_n)) = X_1X_2\ldots X_{n-2}X_{n-1}^2$.
5. $HC(\delta_n(\sigma_{n+1})) = -1$, $HT(\delta_n(\sigma_{n+1})) = X_1^{n-1}X_2^{n-2}\ldots X_{n-2}^2X_{n-1}$.

Furthermore, the set $\hat{B} = \{\delta_n(\sigma_1), \ldots, \delta_n(\sigma_{n+1})\}$ is a basis for $\mathbb{C}[X_1, \ldots, X_n]^{A_n^{\delta_n}}$.

Proof. These are obvious consequences of the head term definition and the properties of invariant rings of a conjugate of A_n. □

Table 1 contains—according to Lemma 3.2—the head terms of the elements of the set $\hat{B}$ with respect to $<_{lex}$ for $3 \leq n \leq 6$.

Theorem 3.3. *Let $\hat{B} = \{\delta_n(\sigma_1), \ldots, \delta_n(\sigma_{n+1})\}$ be as in Lemma 3.2. Then $\hat{B}$ is a finite SAGBI basis for $\mathbb{C}[X_1, \ldots, X_n]^{A_n^{\delta_n}}$ with respect to $<_{lex}$.*

Table 1. The head terms of the set $\hat{B}$ for different numbers of variables n.

$n = 3$	$n = 4$	$n = 5$	$n = 6$
X_1	X_1	X_1	X_1
X_1X_3	X_1X_2	X_1X_2	X_1X_2
$X_1X_2^2$	$X_1X_2X_4$	$X_1X_2X_3$	$X_1X_2X_3$
$X_1^2X_2$	$X_1X_2X_3^2$	$X_1X_2X_3X_5$	$X_1X_2X_3X_4$
	$X_1^3X_2^2X_3$	$X_1X_2X_3X_4^2$	$X_1X_2X_3X_4X_6$
		$X_1^4X_2^3X_3^2X_4$	$X_1X_2X_3X_4X_5^2$
			$X_1^5X_2^4X_3^3X_4^2X_5$

Proof. We know from Lemma 3.2 that $\hat{B}$ is a basis for $\mathbb{C}[X_1, \ldots, X_n]^{A_n^{\delta_n}}$. Once we know this, we only have to check, according to [8], if $\hat{B}$ is in addition a SAGBI basis. A detailed analysis of the set of head terms

$$\{HT(\delta_n(\sigma_1)), \ldots, HT(\delta_n(\sigma_{n+1}))\}$$

reveals that we only have to verify that the polynomial[1]

$$f = (\delta_n(\sigma_{n+1}))^2 + \delta_n(\sigma_n) \cdot (\delta_n(\sigma_{n-2}))^3 \cdot (\delta_n(\sigma_{n-3}) \ldots \delta_n(\sigma_1))^2 \tag{1}$$

can be reduced to zero by means of $\hat{B}$ to ensure that $\hat{B}$ is a SAGBI basis. From the reduction point of view, f is the only relevant critical polynomial which can be made up from the initial set $\hat{B}$.

Let $g = \delta_n^{-1}(f)$. Then we know that $g \in \mathbb{C}[X_1, \ldots, X_n]^{A_n}$. Thus g can be reduced with [3, algorithm 3.12] and represented as

$$g = p_1(\sigma_1, \ldots, \sigma_n) + p_2(\sigma_1, \ldots, \sigma_n) \cdot \sigma_{n+1} \tag{2}$$

with $p_1, p_2 \in \mathbb{C}[X_1, \ldots, X_n]$. The representation (2) is definitely different from

$$g = \sigma_{n+1}^2 + \sigma_n \cdot \sigma_{n-2}^3(\sigma_{n-3} \ldots \sigma_1)^2$$

obtained simply by computing $\delta_n^{-1}(f)$ via equation (1). Algorithm 3.12 terminates after a finite number $l \in \mathbb{N}$ of reduction steps. At any reduction step we have to subtract a certain product of the basis polynomials $\sigma_1, \ldots, \sigma_{n+1}$, say

$$h_i = c_i \sigma_1^{e_{i_1}} \ldots \sigma_n^{e_{i_n}} \sigma_{n+1}^{e_{i_{n+1}}}$$

with $(e_{i_1}, \ldots, e_{i_n}, e_{i_{n+1}}) \in \mathbb{N}^n \times \{0, 1\}$ and $0 \neq c_i \in \mathbb{C}$ in step $1 \leq i \leq l$. Eventually, after termination of algorithm 3.12, the representation (2) of g has been computed as

$$g = h_1 + \ldots + h_l.$$

Algorithm 3.12 ensures that $h_i \neq h_j$ for $1 \leq i \neq j \leq l$. This implies that

$$\delta_n(h_i) = c_i \delta_n(\sigma_1)^{e_{i_1}} \ldots \delta_n(\sigma_n)^{e_{i_n}} \delta_n(\sigma_{n+1})^{e_{i_{n+1}}} \neq \delta_n(h_j),$$

and, because of our choice of δ_n, that $HT(\delta_n(h_i)) \neq HT(\delta_n(h_j))$ for $1 \leq i \neq j \leq l$. We can now rearrange the sequence $\delta_n(h_1), \ldots, \delta_n(h_l)$ in such a way that

$$HT(\delta_n(h_i)) >_{lex} HT(\delta_n(h_j)) \tag{3}$$

for $1 \leq i < j \leq l$. This new sequence is then by construction able to reduce our polynomial f as follows:

$$f \xrightarrow{\delta_n(h_1)} f_1 \xrightarrow{\delta_n(h_2)} \ldots \xrightarrow{\delta_n(h_{l-1})} f_{l-1} \xrightarrow{\delta_n(h_l)} f_l$$

with $f_1, \ldots, f_{l-1} \in \mathbb{C}[X_1, \ldots, X_n]$ and $f_l = 0$. This reduction sequence has to be a SAGBI basis reduction with respect to $\hat{B}$, because the relations (3) imply

$$HT(\delta_n(h_1)) \in T(f), \;\; HT(\delta_n(h_2)) \in T(f_1), \;\; \ldots, \;\; HT(\delta_n(h_l)) \in T(f_{l-1}).$$

□

[1] Note that we define $(\delta_n(\sigma_{n-3}) \ldots \delta_n(\sigma_1))^2 = 1$, if $n = 3$.

Note that Theorem 3.3 holds not only for $\mathbb{C}$, but for any field of characteristic zero.

The argument of the proof is not restricted to f in equation (1), but works for any other polynomial in $\mathbb{C}[X_1,\dots,X_n]^{A_n^{\delta_n}}$. The polynomial $\delta_n(\sigma_{n+1})$ occurs only linearly in the representation of f. Hence a representation with this property can be obtained for any polynomial in $\mathbb{C}[X_1,\dots,X_n]^{A_n^{\delta_n}}$.

Corollary 3.4. *Let $f \in \mathbb{C}[X_1,\dots,X_n]^{A_n^{\delta_n}}$. Then f has a representation as*

$$f = \hat{p_1}(\delta_n(\sigma_1),\dots,\delta_n(\sigma_n)) + \hat{p_2}(\delta_n(\sigma_1),\dots,\delta_n(\sigma_n)) \cdot \delta_n(\sigma_{n+1})$$

with $\hat{p_1}, \hat{p_2} \in \mathbb{C}[X_1,\dots,X_n]$ with respect to the SAGBI basis $\hat{B}$.

4. Conclusion—open problem

We have presented a δ_n such that $\mathbb{C}[X_1,\dots,X_n]^{A_n^{\delta_n}}$ has a finite SAGBI basis for any $n \geq 3$. This finite basis can now be used for a guided reduction and rewriting of elements in $\mathbb{C}[X_1,\dots,X_n]^{A_n}$ instead of e.g., [3].

Of course, it would be of interest to characterize all $\delta_n \in GL(n,\mathbb{C})$ leading to a finite SAGBI basis for the invariant ring $\mathbb{C}[X_1,\dots,X_n]^{A_n^{\delta_n}}$. How this can be done is even in the case $n = 3$ nontrivial and open.

Acknowledgments

This work was done during the author's time at the German Remote Sensing Data Center (Oberpfaffenhofen). The author would like to thank Prof. Lars B. Wahlbin (Ithaca), Patrick Maier (Saarbrücken), Jochen Walter (Freiburg) and one anonymous referee for their comments and remarks.

References

1. Becker, T., Weispfenning, V., in Cooperation with Kredel, H. (1993). Gröbner Bases: A Computational Approach to Commutative Algebra. Springer MR **95c:**13018
2. Göbel, M. (1992). Reduktion G-symmetrischer Polynome für beliebige Permutationsgruppen G. Diplomarbeit. Universität Passau
3. Göbel, M. (1995). Computing Bases for Permutation-Invariant Polynomials. Journal of Symbolic Computation 19, 285–291 MR **96f:**13006
4. Göbel, M. (1997). The Invariant Package of MAS. In: Comon, H., (ed.), Rewriting Techniques and Applications, 8th Intl. Conf., RTA-97, volume 1232 of *LNCS*, Springer, 327–330 MR **98i:**68015
5. Göbel, M. (1998). A Constructive Description of SAGBI Bases for Polynomial Invariants of Permutation Groups. Journal of Symbolic Computation 26, 261–272 MR **99f:**13002
6. Göbel, M. (1999). The "Smallest" Ring of Polynomial Invariants of a Permutation Group which has No Finite SAGBI Bases with respect to Any Admissible Order. Theoretical Computer Science 225(1–2), 177–184 MR **2000f:**13007
7. Göbel, M, Walter, J. (1999). Bases for Polynomial Invariants of Conjugates of Permutation Groups. Journal of Algorithms 32(1), 58–61 CMP 99:14
8. Robbiano, L., Sweedler, M. (1990). Subalgebra Bases. In: Bruns, W., Simis, A. (eds.), Commutative Algebra (Lect. Notes Math. 1430). Springer, 61-87 MR **91f:**13027
9. Sturmfels, B. (1995). Gröbner Bases and Convex Polytopes. AMS University Lecture Series, Vol. 8, Providence RI MR **97b:**13034
10. Weispfenning, V. (1987). Admissible Orders and Linear Forms. ACM SIGSAM Bulletin 21/2, 16–18

Dettenbachstrasse 16, 94154 Neukirchen vorm Wald, Germany
E-mail address: goebel@informatik.uni-tuebingen.de