ELSEVIER

Information Processing Letters 74 (2000) 15–18

Information Processing Letters

www.elsevier.com/locate/ipl

Rings of polynomial invariants of the alternating group have no finite SAGBI bases with respect to any admissible order

Manfred Göbel [1]

Deutsches Fernerkundungsdatenzentrum, Algorithmen und Prozessoren, Deutsches Zentrum für Luft- und Raumfahrt e.V., 82234 Weßling, Germany

Received 25 July 1999; received in revised form 26 January 2000
Communicated by T. Lengauer

Abstract

It is well known, that the invariant ring $\mathbb{C}[X_1, X_2, X_3]^{A_3}$ of the alternating group A_3 is the "smallest" ring of polynomial invariants of a permutation group with respect to the number of variables and the number of generators, which has no finite SAGBI basis with respect to any admissible order. We show in this note that for any number of variables $n \geqslant 3$ the invariant ring $\mathbb{C}[X_1, \ldots, X_n]^{A_n}$ has no finite SAGBI basis with respect to any admissible order. © 2000 Elsevier Science B.V. All rights reserved.

Keywords: Algorithmic invariant theory; SAGBI bases; Alternating groups; Admissible orders

The structure of SAGBI (Subalgebra Analogue to Gröbner Basis for Ideals) bases [4] for polynomial invariants of permutation groups [5] with respect to the lexicographical order $<_{lex}$ has been investigated in [1]: Roughly speaking, only invariant rings of direct products of symmetric groups have a finite SAGBI basis, which is then, in addition, multilinear. It was shown in [2] that the ring of polynomial invariants of the alternating group A_3 is the "smallest" invariant ring of a permutation group with respect to the number of variables and the number of generators, which has no finite SAGBI basis with respect to any admissible order [6]. Our goal here is to generalize this result and to show that for any $3 \leqslant n \in \mathbb{N}$ the invariant ring $\mathbb{C}[X_1, \ldots, X_n]^{A_n}$ has no finite SAGBI basis with respect to any admissible order.

The setting in this note is the same as in [1,2]. $\mathbb{N}$ 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 $\mathbb{C}[X_1, \ldots, X_n]$ and

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

the G-invariant orbit of $t \in T$. S_n and A_n are the symmetric and alternating group, and $\sigma_1 = X_1 + \cdots +$

[1] Present address: Department of Electronic Systems Engineering, University of Essex, Wivenhoe Park, Colchester CO4 3SQ, United Kingdom (mkgoebel@essex.ac.uk).

PII: S0020-0190(00)00031-4

$X_n, \ldots, \sigma_n = X_1 \cdots X_n$ the elementary symmetric polynomials.

The set of terms T can be ordered in multiple ways. A characterization of all admissible orders $<$, which are such that $t > 1$ for all $1 \neq t \in T$ and $st_1 > st_2$ for all $s, t_1, t_2 \in T$ with $t_1 > t_2$, is given in [3,6]. 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 an admissible order $<$, respectively. A SAGBI basis B of a subalgebra S of $\mathbb{C}[X_1, \ldots, X_n]$ is such that with respect to a fixed admissible order $<$ every head term of an element $f \in S$ can be expressed as a product of head terms of the elements in B [4]. A single reduction step $f \xrightarrow[B]{} g$ is defined as

$$g = f - HC(f)\left(\frac{\psi_1}{HC(\psi_1)}\right)^{e_1} \cdots \left(\frac{\psi_l}{HC(\psi_l)}\right)^{e_l}$$

with

$$HT(f) = \bigl(HT(\psi_1)\bigr)^{e_1} \cdots \bigl(HT(\psi_l)\bigr)^{e_l}$$

for some elements $\psi_1, \ldots, \psi_l \in B$ and $e_1, \ldots, e_l \in \mathbb{N}$ with $0 \leqslant l \in \mathbb{N}$.

We assume in the following that $3 \leqslant n \in \mathbb{N}$, and recall the following two results for the lexicographical order $<_{lex}$.

Lemma 1. *The invariant ring $\mathbb{C}[X_1, \ldots, X_n]^{A_n}$ has no finite SAGBI basis with respect to $<_{lex}$.*

Proof. See [1]. A_n is not a direct product of symmetric groups. □

Corollary 2 (cf. [1, Section 3]). *The invariant ring $\mathbb{C}[X_1, \ldots, X_n]^{A_n}$ has an infinite SAGBI basis*

$$B = \{\sigma_1, \ldots, \sigma_n\} \cup \Bigl\{orbit_{A_n}\bigl(X_1^{d+n-1} X_2^{d+n-2} \cdots X_{n-2}^{d+2} X_n^{d+1}\bigr) \mid 0 \leqslant d \in \mathbb{N}\Bigr\}$$

with respect to $<_{lex}$. B is minimal as follows: $B \setminus \widehat{B}$ is for any $\emptyset \neq \widehat{B} \subset B$ no SAGBI basis of $\mathbb{C}[X_1, \ldots, X_n]^{A_n}$ with respect to $<_{lex}$.

Next we are going to present our main result.

Theorem 3. *The invariant ring $\mathbb{C}[X_1, \ldots, X_n]^{A_n}$ has no finite SAGBI basis with respect to some admissible order $<$.*

Proof. Assume that $B = \{\psi_1, \ldots, \psi_k\}$ is a finite SAGBI basis of the invariant ring $\mathbb{C}[X_1, \ldots, X_n]^{A_n}$ with respect to $<$ with $HT(\psi_i) = X_1^{e_{i_1}} \cdots X_n^{e_{i_n}}$ and

$$d = \max\bigl\{e_{i_j} \mid 1 \leqslant i \leqslant k, 1 \leqslant j \leqslant n\bigr\}.$$

We can rearrange the variables without loss of generality in such a way that $X_1 \cdots X_i > r_1 \in T(\sigma_i) \setminus \{X_1 \cdots X_i\}$ for $1 \leqslant i \leqslant n$, because $\sigma_1, \ldots, \sigma_n$ is a SAGBI basis of $\mathbb{C}[X_1, \ldots, X_n]^{S_n} \subset \mathbb{C}[X_1, \ldots, X_n]^{A_n}$ with respect to any admissible order [4, Theorem 1.14]. Furthermore, we have $X_i > T(\sigma_1) \setminus \{X_1, \ldots, X_i\}$, because $X_i < X_j$ for some $i < j$ would imply $X_1 \cdots X_{i-1} X_i < X_1 X_{i-1} X_j$ (contradiction), i.e., $X_1 > \cdots > X_n$. By similar reasoning we obtain that $<$ is equal to $<_{lex}$ on $T(\sigma_i)$ for $1 \leqslant i \leqslant n$.

We can assume without loss of generality that $\{\sigma_1, \ldots, \sigma_n\} \subset B$. Let $X_1^{e_1} \cdots X_n^{e_n}$ be the head term of $orbit_{A_n}(t)$ with respect to $<_{lex}$. Because of the structure of $\mathbb{C}[X_1, \ldots, X_n]^{A_n}$, we have to consider only the following cases with respect to $<$:

(1) $|\{e_1, \ldots, e_n\}| \leqslant n - 1$: Then we have

$$orbit_{A_n}(t) = orbit_{S_n}(t),$$

and $HT(orbit_{S_n}(t))$ can be reduced by a unique product of $\sigma_1, \ldots, \sigma_n$.

(2) $e_1 > \cdots > e_n = 0$: Then we have

$$orbit_{A_n}(t) \neq orbit_{S_n}(t),$$

but

$$HT\bigl(orbit_{A_n}(t)\bigr) = HT\bigl(orbit_{S_n}(t)\bigr),$$

i.e., $orbit_{A_n}(t)$ can be reduced by a unique product of $\sigma_1, \ldots, \sigma_{n-1}$.

(3) $e_1, \ldots, e_n \geqslant 1$: Then we have

$$orbit_{A_n}(t) = orbit_{A_n}\bigl(X_1^{e_1-1} \cdots X_n^{e_n-1}\bigr)\sigma_n,$$

and

$$HT\bigl(orbit_{A_n}(t)\bigr) = HT\bigl(orbit_{A_n}\bigl(X_1^{e_1-1} \cdots X_n^{e_n-1}\bigr)\bigr)\sigma_n.$$

(4) $e_1 > \cdots > e_{n-2} > e_n > e_{n-1} = 0$: Then we have

$$orbit_{A_n}(t) \neq orbit_{S_n}(t)$$

and

$$HT\bigl(orbit_{A_n}(t)\bigr) \neq HT\bigl(orbit_{S_n}(t)\bigr).$$

Let $u_i = HT(\sigma_i)$ for $1 \leqslant i \leqslant n$, and let $v_i = HT(\sigma_i - u_i)$ for $1 \leqslant i \leqslant n-1$. This implies that

$v_i | u_{i+1}$ for $1 \leqslant i \leqslant n-1$, and more importantly, that $HT(orbit_{A_n}(t))$ has to be one of the $n-1$ terms $w_{j,e_1,\ldots,e_n}$ defined as follows for $1 \leqslant j \leqslant n-1$:

$$w_{j,e_1,\ldots,e_n} = u_1^{e_1-e_2} \cdots u_{j-1}^{e_{j-1}-e_j} v_j^{e_j-e_{j+1}} u_{j+1}^{e_{j+1}-e_{j+2}} \cdots u_{n-2}^{e_{n-2}-e_n} u_{n-1}^{e_n}. \tag{1}$$

Consequently, $B_{HT} = \{HT(\psi_i) \mid 1 \leqslant i \leqslant k\}$ has to be a subset of

$$\{X_1, \ldots, X_1 \cdots X_n\} \cup \big\{w_{j,e_1,\ldots,e_n} \mid 1 \leqslant j \leqslant n-1, \; 0 = e_{n-1} < e_n < e_{n-2} < \cdots < e_1 \leqslant d\big\}.$$

Further, $w_{i,e_1,\ldots,e_n} \in B_{HT}$ implies $w_{j,e_1,\ldots,e_n} \notin B_{HT}$ for all $1 \leqslant i \neq j \leqslant n-1$. Our goal is now to construct an infinite sequence of head terms $t_0, t_1, t_2, \ldots$ of A_n-invariant orbits such that almost all of these terms are not generated by products of terms in B_{HT}.

Let t_0 be the head term of $orbit_{A_n}(X_1^{n-1} X_2^{n-2} \cdots X_{n-2}^2 X_n)$, i.e., t_0 is equal to $w_{j,n-1,n-2,\ldots,2,0,1}$ for some $1 \leqslant j \leqslant n-1$, and let s_0 be the corresponding v_j in the representation of $w_{j,n-1,n-2,\ldots,2,0,1}$ (cf. Eq. (1)). Furthermore, for $i \geqslant 1$, let $t_i = HT(orbit_{A_n}(t_{i-1}s_{i-1}))$, and let $s_i = s_{i-1}$, if $t_i = t_{i-1}s_{i-1}$, and let $s_i = \pi(t_{i-1})$, where the unique and nontrivial $\pi \in A_n$ is such that $t_i = \pi(t_{i-1}s_{i-1})$, otherwise (see [2, Fig. 1] for an example sequence in $\mathbb{C}[X_1, X_2, X_3]^{A_3}$). Note that the total degree of t_{i_1} is smaller than the total degree of t_{i_2} for any $i_1 < i_2 \in \mathbb{N}$, and that s_i is never a head term of an A_n-invariant orbit for any $i \in \mathbb{N}$. In particular, the term s_i is not a product of terms in

$$W_{i-1} = \{X_1, \ldots, X_1 \cdots X_n\} \cup \{t_0, \ldots, t_{i-1}\},$$

but constructed by permuting an element of W_{i-1}.

Any term t_i has a representation as $w_{j_i,e_{i_1},\ldots,e_{i_n}}$ for some $1 \leqslant j_i \leqslant n-1$. This is because t_0 has such a representation, and s_0 is equal to the v_{j_0} used in the representation of t_0; by assuming that t_{i-1} has such a representation, and that s_{i-1} uses the same $v_{j_{i-1}}$ as t_{i-1} in its representation, we obtain immediately that t_i has such a representation, and that s_i uses the same v_{j_i} as t_i in its representation.

Our selection of the s_i ensures that the sequence of head terms $t_0, t_1, t_2, \ldots$ in $\mathbb{C}[X_1, \ldots, X_n]^{A_n}$ has *by construction* the following properties: First, $t_i = w_{j_i,e_{i_1},\ldots,e_{i_n}}$ is never a product of terms in W_{i-1} for any $i \in \mathbb{N}$, because the exponents of each product of terms in W_{i-1} are unable to match simultaneously all exponents of t_i. And second, all head terms in $\mathbb{C}[X_1, \ldots, X_n]^{A_n}$ can be expressed as a product of terms in $W = \{X_1, \ldots, X_1 \cdots X_n\} \cup \{t_0, t_1, t_2, \ldots\}$, because, when building the sequence, the step from t_i to t_{i+1} is always performed by multiplying with the smallest possible "problem" term s_i. In other words, the sequence $t_0, t_1, t_2, \ldots$ covers all irreducible head terms with respect to $<$.

Altogether, this implies that any t_i with a sufficiently large total degree has no expression as a product of terms of the finite set B_{HT}. Hence, there exists no finite SAGBI basis of $\mathbb{C}[X_1, \ldots, X_n]^{A_n}$ with respect to $<$ (contradiction). □

Corollary 4. *Let the admissible order $<$, and let the sequence $t_0, t_1, t_2, \ldots$ be as in the proof of Theorem* 3. *The invariant ring $\mathbb{C}[X_1, \ldots, X_n]^{A_n}$ has an infinite SAGBI basis*

$$B = \{\sigma_1, \ldots, \sigma_n\} \cup \big\{orbit_{A_n}(t_i) \mid i \in \mathbb{N}\big\}$$

with respect to $<$. B is minimal as follows: $B \setminus \widehat{B}$ is for any $\emptyset \neq \widehat{B} \subset B$ no SAGBI basis of $\mathbb{C}[X_1, \ldots, X_n]^{A_n}$ with respect to $<$.

Note that Theorem 3 holds not only for the field $\mathbb{C}$ but for any ring R, because our arguments are based on A_n-invariant orbits.

Acknowledgement

The author would like to thank Patrick Maier (Saarbrücken) for his comments and remarks.

References

[1] M. Göbel, A constructive description of SAGBI bases for polynomial invariants of permutation groups, J. Symbolic Comput. 26 (1998) 261–272.

[2] M. Göbel, The "smallest" ring of polynomial invariants of a permutation group which has no finite SAGBI bases with respect to any admissible order, Theoret. Comput. Sci. 225 (1–2) (1999) 177–184.

[3] L. Robbiano, Term orderings on the polynomial ring, in: B. Caviness (Ed.), European Conference on Computer Algebra, EUROCAL'85, Linz, Austria, Proceedings, Vol. 2: Research Contributions, Lecture Notes in Comput. Sci., Vol. 204, Springer, Berlin, April 1985, pp. 513–517.

[4] L. Robbiano, M. Sweedler, Subalgebra bases, in: W. Bruns, A. Simis (Eds.), Commutative Algebra, Lecture Notes in Comput. Sci., Vol. 1430, Springer, Berlin, 1990, pp. 61–87.
[5] L. Smith, Polynomial Invariants of Finite Groups, A.K. Peters, Ltd., Wellesley, MA, 1995.
[6] V. Weispfenning, Admissible orders and linear forms, ACM SIGSAM Bull. 21 (2) (1987) 16–18.