*Discrete Mathematics and Theoretical Computer Science* **3**, 1999, 65–70

# *The Optimal Lower Bound for Generators of Invariant Rings without Finite SAGBI Bases with Respect to Any Admissible Order*

Manfred Göbel†

*DFD-AP, DLR Oberpfaffenhofen, 82234 Weßling, Germany*
Manfred.Goebel@dlr.de

*received 23$^{th}$ April 1998, revised 23$^{th}$ November 1998, accepted 27$^{th}$ January 1999.*

We prove the existence of an invariant ring $\mathbb{C}[X_1, \ldots, X_n]^\Gamma$ generated by elements with a total degree of at most 2, which has no finite SAGBI basis with respect to any admissible order. Therefore, 2 is the optimal lower bound for the total degree of generators of invariant rings with such a property.

**Keywords:** SAGBI basis, Invariant ring, Analysis of algorithms.

In [2], the structure of SAGBI (**S**ubalgebra **A**nalogue to **G**röbner **B**asis for **I**deals [5]) bases for invariant rings of permutation groups with respect to the lexicographical order $<_{lex}$ with $X_1 >_{lex} \ldots >_{lex} X_n$ was investigated. It turned out that only invariant rings of direct products of symmetric groups have a finite SAGBI basis, which is then, in addition, multilinear. Of course, it would be of interest to have such a strong characterization with respect to any other admissible order [4, 6]. To achieve this seems to be all but trivial. One step towards the understanding of the behavior of SAGBI bases for invariant rings with respect to any admissible order is the investigation of important special cases. Recently, the non-finiteness of SAGBI bases for $\mathbb{C}[X_1, X_2, X_3]^{\langle(123)\rangle}$ with respect to any admissible order was proven in [3]. In addition, it was shown that with respect to the number of variables, $\mathbb{C}[X_1, X_2, X_3]^{\langle(123)\rangle}$ is the "smallest" unique example for such a ring of polynomial invariants of a permutation group.

In this note, we show the existence of an invariant ring generated only by polynomial invariants with a total degree of at most 2, which has no finite SAGBI basis with respect to any admissible order. Hence, 2 is the optimal lower bound, because any invariant ring generated by polynomial invariants with a total degree of at most 1 has for trivial reasons a finite SAGBI basis. In addition, we can show that our example has with respect to this property the minimal number of variables 4, if we restrict ourself to polynomial invariants of permutation groups, and the minimal group order 2.

We briefly recall our notation, and then state and prove our result.

†This work was supported by the German Science Foundation (DFG). The author would like to thank Prof. Cohen (Eindhoven) and the anonymous referees for their comments and remarks.

- The natural and complex numbers are denoted by $\mathbb{N}$ and $\mathbb{C}$,
- $K[X_1, \ldots, X_n]$ is the commutative polynomial ring over $K$ in the indeterminates $X_1, \ldots, X_n$,
- $T$ is the set of terms (= power-products of the $X_i$) in $K[X_1, \ldots, X_n]$,
- $GL(K,n)$ denotes the general linear group over $K$,
- $G < GL(K,n)$ a permutation group,
- and $S_n$ the symmetric group of $n$ symbols.

A polynomial $f \in K[X_1, \ldots, X_n]$ is called $\Gamma$-invariant, if

$$f = \pi(f) := f(\sum_{i=1}^{n} a_{1i}X_i, \ldots, \sum_{i=1}^{n} a_{ni}X_i) \quad \forall \pi = (a_{ij})_{1 \leq i,j \leq n} \in \Gamma < GL(K,n). \tag{1}$$

The ring $K[X_1, \ldots, X_n]^\Gamma$ denotes the $K$-algebra of $\Gamma$-invariant polynomials in $K[X_1, \ldots, X_n]$, and

$$orbit_\Gamma(f) = \sum_{p \in \{\pi(f) | \pi \in \Gamma\}} p \tag{2}$$

the $\Gamma$-invariant orbit of $f$. An admissible order $<$ on the set of terms $T$ is such that

$$t > 1 \ \ \forall 1 \neq t \in T \ \text{ and } \ st_1 > st_2 \ \ \forall s, t_1, t_2 \in T \ \text{ with } \ t_1 > t_2 \ \ [4,\ 6]. \tag{3}$$

$HT(f)$ is the leading term of $f \in K[X_1, \ldots, X_n]$ with respect to a given admissible order $<$, and $HC(f)$ denotes its coefficient. A term $t = X_1^{e_1} \ldots X_n^{e_n}$ is called multilinear iff $\{e_1, \ldots, e_n\} \subseteq \{0, 1\}$.

**Lemma 1** *Let $G = \langle(12)(34)\rangle$. Then $\mathbb{C}[X_1, X_2, X_3, X_4]^G$ is generated by*

$$B = \{\, X_1 + X_2,\ X_1X_2,\ X_3 + X_4,\ X_3X_4,\ X_1X_4 + X_2X_3\}. \tag{4}$$

**Proof** A close look at the $G$-invariant orbits of $\mathbb{C}[X_1, X_2, X_3, X_4]^G$ via the reduction technique described in [1] shows that we only have to find a representation of $orbit_G(X_1^2X_3)$, $orbit_G(X_1X_3^2)$, $orbit_G(X_1^2X_4)$, and $orbit_G(X_1X_4^2)$ in terms of the elements of $B$. We have

$$\begin{aligned}
orbit_G(X_1^2X_3) &= (X_1 + X_2)(X_1X_3 + X_2X_4) - (X_1X_2)(X_3 + X_4), \\
orbit_G(X_1X_3^2) &= (X_3 + X_4)(X_1X_3 + X_2X_4) - (X_3X_4)(X_1 + X_2), \\
orbit_G(X_1^2X_4) &= (X_1 + X_2)(X_1X_4 + X_2X_3) - (X_1X_2)(X_3 + X_4), \text{ and} \\
orbit_G(X_1X_4^2) &= (X_3 + X_4)(X_1X_3 + X_2X_4) - (X_3X_4)(X_1 + X_2), \\
&\text{with} \\
X_1X_3 + X_2X_4 &= (X_1 + X_2)(X_3 + X_4) - (X_1X_4 - X_2X_3).
\end{aligned}$$

For any other non-multilinear special $orbit_G(X_1^{e_1}X_2^{e_2}X_3^{e_3}X_4^{e_4})$ not listed so far, we have $e_1, e_2 > 0$ or $e_3, e_4 > 0$, i.e. we can rewrite these orbits as

$$(X_1X_2)orbit_G(X_1^{e_1-1}X_2^{e_2-1}X_3^{e_3}X_4^{e_4}) \tag{5}$$

or

$$(X_3X_4)orbit_G(X_1^{e_1}X_2^{e_2}X_3^{e_3-1}X_4^{e_4-1}). \tag{6}$$

This completes the proof of the lemma. □

**Lemma 2** *Let $G = \langle(12)(34)\rangle$. Then $\mathbb{C}[X_1, \ldots, X_n]^G$ has no finite SAGBI basis with respect to $<_{lex}$.*

**Proof** The permutation group $G$ is not a direct product of symmetric groups. So, following [2], $\mathbb{C}[X_1, X_2, X_3, X_4]^G$ can not have a finite SAGBI basis with respect to $<_{lex}$. □

**Theorem 3** *Let $G = \langle(12)(34)\rangle$. Then $\mathbb{C}[X_1, X_2, X_3, X_4]^G$ has no finite SAGBI basis with respect to any admissible order $<$.*

**Proof** Assume that $\mathbb{C}[X_1, X_2, X_3, X_4]^G$ has a finite SAGBI basis $B$ with respect to $<$, and assume further w.l.o.g. that $X_1 > X_2$, $X_3 > X_4$, and $X_1 > X_3$. Then we have either $X_2 > X_3$, or $X_3 > X_2$. And further, the basis $B$ contains the multilinear $G$-invariant orbits

$$\{\, X_1 + X_2,\ X_1X_2,\ X_1X_4 + X_2X_3,\ X_3 + X_4,\ X_3X_4\} \tag{7}$$

and a finite number of non-multilinear $G$-invariant orbits of the form

$$\psi_{e_1,e_2} = X_1^{e_1}X_4^{e_2} + X_2^{e_1}X_3^{e_2} \tag{8}$$

with $e_1 \neq e_2 \geq 1$. Note that the leading term of $\psi = X_1X_4 + X_2X_3$ is with respect to $<$ not determined so far. Our goal is now to construct an infinite sequence of leading terms $t_0, t_1, t_2, \ldots$ of $G$-invariant orbits such that almost all of these terms are not generated by products of leading terms of the polynomials in $B$. Let

$$t_0 = \begin{cases} HT(orbit_G(X_1X_4^2)), \text{if } HT(\psi) = X_1X_4 \\ HT(orbit_G(X_2^2X_3)), \text{otherwise,} \end{cases}$$

and let $s_0 = X_4$, if $t_0 = X_1X_4^2$, $s_0 = X_2X_3$, if $t_0 = X_2X_3^2$, $s_0 = X_2$, if $t_0 = X_2^2X_3$, and $s_0 = X_1X_4$ otherwise. Furthermore, for $i \geq 1$, define $t_i = HT(orbit_G(t_{i-1}s_{i-1}))$, and let $s_i = s_{i-1}$, if $t_i = t_{i-1}s_{i-1}$, and let

$$s_i = \begin{cases} X_1^{e_1}X_4^{e_2}, & \text{if } t_{i-1} = X_2^{e_1}X_3^{e_2} \\ X_2^{e_1}X_3^{e_2}, & \text{otherwise.} \end{cases}$$

For all $i \in \mathbb{N}$, we have $t_i$ is $X_1^{e_1}X_4^{e_2}$ or $X_2^{e_1}X_3^{e_2}$ with $1 \leq e_1 < e_2$, if $HT(\psi) = X_1X_4$, and with $e_1 > e_2 \geq 1$, otherwise (see Figure 1 on the following page for an example sequence). The total degree of $t_{i_1}$ is always smaller than the total degree of $t_{i_2}$ for $i_1 < i_2 \in \mathbb{N}$, and $s_i$ is never a leading term of a $G$-invariant orbit for all $i \in \mathbb{N}$.

Our selection of the $s_i, i \in \mathbb{N}$ ensures that the sequence of leading terms $t_0, t_1, t_2, \ldots$ in $\mathbb{C}[X_1, X_2, X_3, X_4]^G$ has by construction the following properties: First, $t_i$ is never a product of terms in

$$W_{i-1} = \{X_1, X_1X_2, HT(\psi), X_3, X_3X_4\} \cup \{t_0, \ldots, t_{i-1}\} \quad \forall i \in \mathbb{N}. \tag{9}$$

Each product of terms in $W_{i-1}$ matching the exponent of $X_4$ ($X_3$) is unable to match simultaneously the exponent of $X_1$ ($X_2$), if $t_i = X_1^{e_1}X_4^{e_2}$ ($X_2^{e_1}X_3^{e_2}$). Second, all other leading terms in $\mathbb{C}[X_1, X_2, X_3, X_4]^G$ have an expression as a product of terms in $W = \{X_1, X_1X_2, HT(\psi), X_3, X_3X_4\} \cup \{t_0, t_1, t_2, \ldots\}$.

Altogether, this implies that any $t_i$ with a sufficiently large total degree has no expression as a product of leading terms of the polynomials in the finite set $B$. Hence, there exists no finite SAGBI basis of $\mathbb{C}[X_1, X_2, X_3, X_4]^G$ with respect to $<$ (contradiction). □

Figure 1 illustrates the way of the sequence $t_0$, $t_1$, $t_2$, …thru the terms in question with respect to a given admissible order $<$. The upper (lower) half of the figure shows the first couple of $X_1^{e_1} X_4^{e_2}$ ($X_2^{e_1} X_3^{e_2}$) terms denoted by $e_1..e_2$ ($.e_1 e_2.$) with $0 < e_1 < e_2$. We can see in this example that $t_0 = X_1 X_4^2$ ($s_0 = X_4$), $t_1 = X_2 X_3^3$ ($s_1 = X_2 X_3^2$), $t_2 = X_2^2 X_3^5$ ($s_2 = X_2 X_3^2$), $t_3 = X_1^3 X_4^7$ ($s_3 = X_1^2 X_4^5$), $t_4 = X_1^5 X_4^{12}$ ($s_4 = X_1^2 X_4^5$), and so on. The set $W = \{X_1, X_1X_2, X_1X_4, X_3, X_3X_4\} \cup \{t_0, t_1, t_2, \ldots\}$

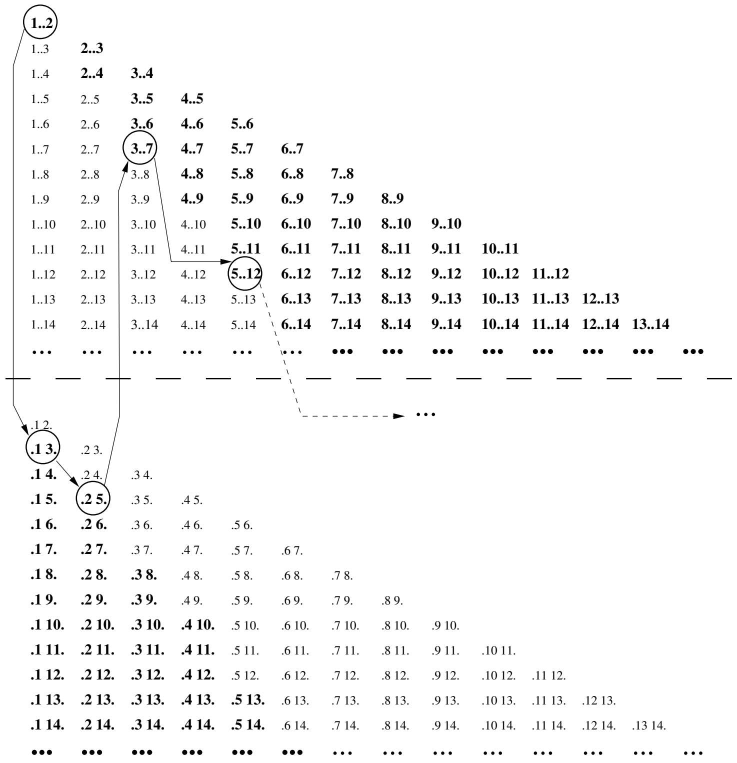


**Fig. 1:** The leading term pattern for a given admissible order $<$.

separates the terms in the set $\{X_1^{e_1} X_4^{e_2}, X_2^{e_1} X_3^{e_2} \mid 0 < e_1 < e_2\}$ into leading terms (font: times-bold) and other terms (font: times-roman) such that either $X_1^{e_1} X_4^{e_2}$ or $X_2^{e_1} X_3^{e_2}$ is a leading term, and such that any other leading term in $\mathbb{C}[X_1, X_2, X_3, X_4]^G$ is a product of terms in $W$.

The invariant ring $\mathbb{C}[X_1, \ldots, X_n]^\Gamma$ is generated by polynomials with a total degree of at most 1 implies that $\Gamma$ is the trivial group, and that the generators are $X_1$, …, $X_n$. Hence, 2 is the smallest possible and therefore optimal lower bound for the generators of an invariant ring without a finite SAGBI with respect to any admissible order. Furthermore, we must have $|\Gamma| \geq 2$ for any $\mathbb{C}[X_1, \ldots, X_n]^\Gamma$ with this property, i.e. our example is minimal with respect to the group order, because $|G| = 2$.

**Lemma 4** *Let $n < 4$, and let $\mathbb{C}[X_1, \ldots, X_n]^G$ be generated by elements with a total degree of at most $2$. Then $\mathbb{C}[X_1, \ldots, X_n]^G$ has a finite SAGBI basis.*

**Proof** $G$ is either $S_1$, $S_1 \times S_1$, $S_2$, $S_1 \times S_2$, $S_2 \times S_1$, or $S_1 \times S_1 \times S_1$, i.e. $\mathbb{C}[X_1, \ldots, X_n]^G$ has a finite SAGBI basis (Cf. [2]). □

Hence, $\mathbb{C}[X_1, X_2, X_3, X_4]^G$ with $G = \langle(12)(34)\rangle$ is, in addition, minimal with respect to the number of variables, if we restrict ourself to polynomial invariants of permutation groups. Note that these results hold not only for the field $\mathbb{C}$ but for any ring $R$, because our arguments are based on $G$-invariant orbits.

## References

[1] M. Göbel, Computing Bases for Permutation-Invariant Polynomials, *Journal of Symbolic Computation*, 19, 285–291, 1995.

[2] M. Göbel, A Constructive Description of SAGBI Bases for Polynomial Invariants of Permutation Groups. *Journal of Symbolic Computation*, 26, 261–272, 1998.

[3] M. Göbel, The “Smallest” Ring of Polynomial Invariants of a Permutation Group which has No Finite SAGBI Bases w.r.t. Any Admissible Order, *Theoretical Computer Science*, to appear, 1998.

[4] L. Robbiano, Term Orderings on the Polynomial Ring, in: B. Caviness (ed.), *European Conference on Computer Algebra, EUROCAL'85*, Proceedings Vol. 2: Research Contributions, volume 204 of *LNCS*, Springer, Linz, Austria, 513–517, 1985.

[5] L. Robbiano and M. Sweedler, Subalgebra Bases, In: W. Bruns and A. Simis (eds.), *Commutative Algebra*, Lect. Notes Math. 1430, Springer, 61–87, 1990.

[6] V. Weispfenning, Admissible Orders and Linear Forms, *ACM SIGSAM Bulletin*, 21:2, 16–18, 1987.