J. Symbolic Computation (1995) **19**, 285–291

Computing Bases for Rings of Permutation-invariant Polynomials

MANFRED GÖBEL[†]

Wilhelm-Schickard-Institut für Informatik, Universität Tübingen,

Sand 13, 72076 Tübingen, Germany

(Received 12 July 1994)

Let R be a commutative ring with 1, let $R[X_1, \dots, X_n]$ be the polynomial ring in $X_1, \dots, X_n$ over R and let G be an arbitrary group of permutations of $\{X_1, \dots, X_n\}$. The paper presents an algorithm for computing a small finite basis B of the R-algebra of G-invariant polynomials and a polynomial representation of an arbitrary G-invariant polynomial in $R[X_1, \dots, X_n]$ as a polynomial in the polynomials of the finite basis B. The algorithm works independently of the ground ring R, and the basis B contains only polynomials of total degree $\leq max\{n, n(n-1)/2\}$, independent of the size of the permutation group G.

1. Introduction

A classical result in invariant theory due to E. Noether (1916) asserts that for any finite matrix group Γ the ring $K[X_1, \dots, X_n]^\Gamma$ of Γ-invariant polynomials in $K[X_1, \dots, X_n]$ is finitely generated by polynomials of total degree $\leq |\Gamma|$. The proof of Noether's theorem is constructive, but it depends on the fact that the characteristic of the ground field K is zero. The proof fails for fields of prime characteristic and more general ground rings. Noether was aware of this deficiency, and proved later an analogous theorem that $K[X_1, \dots, X_n]^\Gamma$ is always finitely generated as a K-algebra, regardless of whether $|\Gamma|$ is invertible in K or not (Noether, 1926). Unfortunately, the proof is non-constructive and does not produce any bounds on the degree of the generators.

This note restricts the class of group actions to permutation groups G, which play an important rôle in algebra and applications. We present a novel method for computing a finite basis for the ring of G-invariant polynomials that is for most permutation groups G superior to the method of Noether. First, it computes a basis for the ring $R[X_1, \dots, X_n]^G$ of G-invariant polynomials in $R[X_1, \dots, X_n]$ for an arbitrary ground ring R. Second, the basis B contains only polynomials of maximal variable degree $\leq max\{1, n-1\}$ and total degree $\leq max\{n, n(n-1)/2\}$, independent of the size of the permutation group G. The results of this note are already known for rings $K[X_1, \dots, X_n]^G$ with $char(K) = 0$ (see Schmid, 1991: section 9). An alternative approach which gives the same degree bounds may be found in Garsia and Stanton (1984).

[†] E-mail: `goebel@informatik.uni-tuebingen.de`. For Paul and Therese.

0747–7171/95/040285+07 $08.00/0

Our algorithmic approach is a generalization of the classical algorithm for symmetric polynomials presented, for example, in Becker *et al.* (1993), section 10.7, or Sturmfels (1993), section 1.1. The algorithm represents any $f \in R[X_1, \dots, X_n]^G$ as a finite linear combination of the elements of B with symmetric polynomials as coefficients, independent of the given ground ring R.

The plan of the paper is as follows: Section 2 presents the basic definitions and motivates our approach. Section 3 contains a comprehensive description of our reduction algorithm for G-invariant polynomials. We prove degree bounds for the polynomials of the bases B, and illustrate our method by an example. In Section 4 we conclude with some remarks on the complexity of our algorithm, and show that our degree bounds are optimal for permutation groups G from the point of view of worst case complexity. Finally, we deduce a bound for the maximal variable degree of the basis polynomials in dependence of $|G|$.

2. Basics

R (K) is an arbitrary commutative ring (field) with 1, $R[X_1, \dots, X_n]$ is the commutative polynomial ring over R in the indeterminates X_i, T is the set of terms (= power-products of the X_i) in $R[X_1, \dots, X_n]$, $M = \{at \mid a \in R, t \in T\}$ is the set of monomials in $R[X_1, \dots, X_n]$, and $T(f)$, $M(f)$ is the set of terms and monomials occurring in $f \in R[X_1, \dots, X_n]$ with non-zero coefficients, respectively. $AO(T)$ is the set of all admissible orders on T. For a fixed admissible order $<$ on T and $f \in R[X_1, \dots, X_n]$, we let $HT(f)$, $HC(f)$, $HM(f)$ denote the highest term t w.r.t. $<$ in $T(f)$, the coefficient a of t in f and the monomial at of f, respectively. In this paper we fix $<_{lex}$ as the lexicographical order on T.

G denotes any permutation group operating on the n indeterminates $X_1, \dots, X_n$. Any $\pi \in G$ extends in a unique way to an endomorphism of the R-algebra $R[X_1, \dots, X_n]$ defined by $\pi(f) := f(\pi(X_1), \pi(X_2), \dots, \pi(X_n))$. $f \in R[X_1, \dots, X_n]$ is G-invariant, if $f = \pi(f)$ for all $\pi \in G$.

$R[X_1, \dots, X_n]^G$ denotes the R-algebra of G-invariant polynomials in $R[X_1, \dots, X_n]$. $orbit_G(t) = \sum_{s \in \{\pi(t) | \pi \in G\}} s$ is the G-invariant orbit of $t \in T$. $orbit_G(t)$ is a G-invariant polynomial, and if $f \in R[X_1, \dots, X_n]^G$ and $at \in M(f)$, then $M(a \cdot orbit_G(t)) \subseteq M(f)$. S_n and A_n denote the symmetric and the alternating permutation group, respectively.

The multilinear S_n-invariant polynomials $\sigma_i = orbit_{S_n}(X_1 \dots X_i)$, $1 \le i \le n$ are the elementary symmetric polynomials (see van der Waerden, 1971: section 33). $\sigma_1, \dots, \sigma_n$ form a finite SAGBI basis for $R[X_1, \dots, X_n]^{S_n}$ (see Sturmfels, 1993: proof of theorem 1.1.1). The method of SAGBI bases is the natural subalgebra analogue to Gröbner bases for ideals (Kapur and Madlener, 1989; Robbiano and Schweedler, 1990). The following lemma shows, that $R[X_1, \dots, X_n]^G$ has in general no finite SAGBI basis.

LEMMA 2.1. *The invariant ring $R[X_1, X_2, X_3]^{A_3}$ has no finite SAGBI basis.*

PROOF. Assume that $\{\psi_1, \dots, \psi_k\}$ is a finite SAGBI basis of $R[X_1, X_2, X_3]^{A_3}$ with $HT(\psi_i) = X_1^{e_{i_1}} X_2^{e_{i_2}} X_3^{e_{i_3}}$. We must have $e_{i_1} \ge e_{i_2} \ge e_{i_3}$ or $e_{i_1} > e_{i_3} > e_{i_2}$. Let $d = max\{e_{i_j} \mid 1 \le i \le k, 1 \le j \le 3\}$ and let $f = orbit_{A_3}(X_1^{d+1} X_3^d) \in R[X_1, X_2, X_3]^{A_3}$. ψ_i is involved in a reduction of f implies that $e_{i_2} = 0$, i.e. either $HT(\psi_i) = X_1^{e_{i_1}}$ with $d \ge e_{i_1} \ge 0$ or $HT(\psi_i) = X_1^{e_{i_1}} X_3^{e_{i_3}}$ with $d \ge e_{i_1} > e_{i_3} > 0$. In any case, we have to multiply at least two terms $X_1^{e_{i_1}} X_3^{e_{i_3}}$ with $d \ge e_{i_1} > e_{i_3} > 0$ for the reduction of f in order to obtain $HT(f) = X_1^{d+1}X_3^d$. Any such product has a difference of at least two in the exponents of X_1 and X_3 which shows that $HT(f)$ cannot be a product of $HT(\psi_i)$ for $1 \leq i \leq k$ (contradiction). □

In other words the classical algorithm for symmetric polynomials cannot be generalized for polynomials in $R[X_1, \ldots, X_n]^G$. The next section introduces a reduction method which works for arbitrary permutation groups $G \subseteq S_n$.

3. The reduction method

We prove in this section that every polynomial $f \in R[X_1, \ldots, X_n]^G$ has a representation as a polynomial over the ground ring R in G-invariant orbits with maximal variable degree $\leq max\{1, n-1\}$ and total degree $\leq max\{n, n(n-1)/2\}$. The proof is constructive and leads to an algorithm which represents f as a finite $R[\sigma_1, \ldots, \sigma_n]$-linear combination of special G-invariant orbits.

DEFINITION 3.1. *Let $t \in T$ and $\pi \in S_n$ such that $\pi(t) = X_1^{e_1} \ldots X_n^{e_n}$ and $e_1 \geq e_2 \geq \ldots \geq e_n$. Then $desc(t) = \pi(t)$ is the descending term of t and $\Omega(t) = \sigma_1^{e_1-e_2} \ldots \sigma_{n-1}^{e_{n-1}-e_n}\sigma_n^{e_n}$ is the elementary symmetric product of t.*

REMARK 3.2. *There exists no infinite chain $t_1, t_2, \ldots \in T$ with $desc(t_i) >_{lex} desc(t_{i+1})$ or $(desc(t_i) = desc(t_{i+1}) \wedge t_i >_{lex} t_{i+1})$ for all $i \in N$, because $<_{lex} \in AO(T)$.*

LEMMA 3.3. *Let $t \in T$. Then $a \cdot t \in M(\Omega(t))$ and $a = 1$.*

PROOF. We have $a \cdot X_1^{e_1} \ldots X_n^{e_n} = a \cdot desc(t) \in M(\Omega(t))$ and so $\Omega(t) = \Omega(X_1^{e_1} \ldots X_n^{e_n}) = \sigma_1^{e_1-e_2} \ldots \sigma_{n-1}^{e_{n-1}-e_n}\sigma_n^{e_n}$. Furthermore,

$$\begin{aligned} HM(\sigma_1^{e_1-e_2} \ldots \sigma_n^{e_n}) &= HM(\sigma_1^{e_1-e_2}) \ldots HM(\sigma_n^{e_n}) \\ &= HM(\sigma_1)^{e_1-e_2} \ldots HM(\sigma_n)^{e_n} \\ &= X_1^{e_1-e_2} \ldots (X_1 \ldots X_n)^{e_n} = X_1^{e_1} \ldots X_n^{e_n}, \end{aligned}$$

i.e. $a = 1$. By symmetry of $\Omega(t)$, the same holds for t. □

LEMMA 3.4. *Let $t = X_1^{e_1} \ldots X_n^{e_n}$ be descending. Then for all $s \in T(\Omega(t) - orbit_G(t))$ the following holds: $desc(t) >_{lex} desc(s)$ or $(desc(t) = desc(s) \wedge t >_{lex} s)$.*

PROOF. By Lemma 3.3 we have $t = HM(\Omega(t))$, and so $desc(t) >_{lex} desc(s)$ or $(desc(t) = desc(s) \wedge t >_{lex} s)$ holds for all $s \in T(\Omega(t) - orbit_G(t))$. □

DEFINITION 3.5. *Let $t = X_1^{e_1} \ldots X_n^{e_n}$, let $\emptyset \neq I \subseteq \{1, \ldots, n\}$, and let m_0 and m_1 denote the minimum and maximum of $\{e_i \mid i \in I\}$, respectively. Then t is k-connected w.r.t. I, if $|I| = k$, $m_1 = max\{e_1, \ldots, e_n\}$, and $\{e_i \mid i \in I\}$ is the set of all integers between m_0 and m_1. t is maximal k-connected, if t is k-connected and not $(k+1)$-connected or $k = n$. A maximal n-connected term t is called special, if either $e_i = 0$ for some $i \in \{1, \ldots, n\}$ or $e_1 = \ldots = e_n = 1$. $orbit_G(t)$ is a special G-invariant orbit, if t is a special term.*

The number of special terms in $R[X_1, \ldots, X_n]$ is finite, and every special term has a maximal variable degree $\leq max\{1, n-1\}$ and a total degree $\leq max\{n, n(n-1)/2\}$.

The elementary symmetric polynomials $\sigma_1, \ldots, \sigma_n$ are finite sums of special G-invariant orbits.

DEFINITION 3.6. *Let $t = X_1^{e_1} \ldots X_n^{e_n}$ be non-special and maximal k-connected w.r.t. I. The reduced term of t is defined as $Red(t) = X_1^{d_1} \ldots X_n^{d_n}$ with $d_i = e_i - 1$, $i \in I$ and $d_i = e_i$, otherwise.*

LEMMA 3.7. *Let $t = X_1^{e_1} \ldots X_n^{e_n}$ be non-special and maximal k-connected w.r.t. I and let $u \in T$ such that $t = u \cdot Red(t)$. Then the following holds (see Göbel, 1992: theorem 4.16):*

(i) $desc(t) >_{lex} desc(s)$ for all $s \in T(\Omega(u) \cdot Red(t) - t)$
(ii) $desc(t) >_{lex} desc(s)$ for all $s \in T(\Omega(u) \cdot orbit_G(Red(t)) - orbit_G(t))$.

PROOF. (i) is a consequence of Lemma 3.3 and Definition 3.6. By Lemma 3.3 we have $u \in M(\Omega(u))$. Definition 3.6 ensures that only the term $u \in T(\Omega(u))$ is equal to the power product of the variables belonging to the indices in the index set I. And so, $desc(t) >_{lex} desc(s)$ holds for all other terms $s \in T(\Omega(u) \cdot Red(t) - t)$.

(ii) follows from the definition of the G-invariant orbit, Definition 3.6 and the fact that $\Omega(u) \in R[X_1, \ldots, X_n]^{S_n}$. (i) implies that for all $\pi \in G$ the following holds:

$$desc(t) = desc(\pi(t)) >_{lex} desc(s) \quad \text{for all} \quad s \in T(\Omega(u) \cdot Red(\pi(t)) - \pi(t)) \tag{3.1}$$

Hence, $desc(t) >_{lex} desc(s)$ for all $s \in T(\Omega(u) \cdot orbit_G(Red(t)) - orbit_G(t))$. □

DEFINITION 3.8. *Let $t_0 = t$ be maximal k_0-connected w.r.t. I_0, let $t_i = Red(t_{i-1})$ be maximal k_i-connected w.r.t. I_i for $1 \le i \le r$ and let t_r be a special term, $r \in N$. Then t is maximal $(k_1, \ldots, k_n)$-connected w.r.t. $\Gamma = \{I_0, \ldots, I_r\}$ where k_i is the number of elements $I \in \Gamma$ with $|I| = i$, $1 \le i \le n$.*

For t maximal $(k_1, \ldots, k_n)$-connected w.r.t. $\{I_0, \ldots, I_r\}$ $I_k \subseteq I_l$ holds for $0 \le k \le l \le r$. Special terms are maximal $(0, \ldots, 0)$-connected w.r.t. $\emptyset$.

DEFINITION 3.9. *Let $t = X_1^{e_1} \ldots X_n^{e_n}$ be non-special and maximal $(k_1, \ldots, k_n)$-connected w.r.t. $\Gamma = \{I_0, \ldots, I_r\}$. The total-reduced term of t is defined as $RED(t) = X_1^{d_1} \ldots X_n^{d_n}$ with $d_i = e_i - k$, if k different elements of Γ contain i.*

LEMMA 3.10. *Let $t = X_1^{e_1} \ldots X_n^{e_n}$ be non-special and maximal $(k_1, \ldots, k_n)$-connected w.r.t. Γ and let $u \in T$ such that $t = u \cdot RED(t)$. Then the following holds:*

(i) $desc(t) >_{lex} desc(s)$ for all $s \in T(\Omega(u) \cdot RED(t) - t)$
(ii) $desc(t) >_{lex} desc(s)$ for all $s \in T(\Omega(u) \cdot orbit_G(RED(t)) - orbit_G(t))$.

PROOF. (i) is a consequence of Lemma 3.3 and Definition 3.9 (see also Lemma 3.7). By Lemma 3.3 we have $u \in M(\Omega(u))$. Definition 3.9 ensures that only the term $u \in T(\Omega(u))$ is equal to the power product of the variables belonging to the indices in the index sets of Γ. And so, $desc(t) >_{lex} desc(s)$ holds for all other terms $s \in T(\Omega(u) \cdot RED(t) - t)$.

(ii) follows from the definition of the G-invariant orbit, Definition 3.9 and the fact that $\Omega(u) \in R[X_1, \ldots, X_n]^{S_n}$. (i) implies that for all $\pi \in G$ the following holds:

$$desc(t) = desc(\pi(t)) >_{lex} desc(s) \quad \text{for all} \quad s \in T(\Omega(u) \cdot RED(\pi(t)) - \pi(t)) \tag{3.2}$$

Hence, $desc(t) >_{lex} desc(s)$ for all $s \in T(\Omega(u) \cdot orbit_G(RED(t)) - orbit_G(t))$. □

THEOREM 3.11. *If R is any commutative ring and G any subgroup of the $n \times n$ permutation matrices, then the invariant ring $R[X_1, \ldots, X_n]^G$ is generated in degree at most $n(n-1)/2$.*

PROOF. We prove this theorem over the following algorithm which represents an arbitrary $f \in R[X_1, \ldots, X_n]^G$ as a finite $R[\sigma_1, \ldots, \sigma_n]$-linear combination of special G-invariant orbits.

ALGORITHM 3.12.

INPUT $f \in R[X_1, \ldots, X_n]^G$;
$\hat{f} := f$; $p_t := 0$ *for* $t \in T$ *special;*
WHILE $\hat{f} \neq 0$ *DO*
  select $at := aX_1^{e_1} \ldots X_n^{e_n} \in M(\hat{f})$ *such that*
    $desc(t) >_{lex} desc(s)$ *or* $(desc(t) = desc(s) \wedge t >_{lex} s)$ *for all* $s \in T(\hat{f}) \setminus t$;
  IF (t is descending) THEN / Lemma 3.4 */*
    $p_1 := p_1 + a \cdot X_1^{e_1 - e_2} \ldots X_{n-1}^{e_{n-1} - e_n} X_n^{e_n}$;
    $\hat{f} := \hat{f} - a \cdot \Omega(t)$;
  ELSIF (t is non-special) THEN / Lemma 3.10 (ii) */*
    $X_1^{d_1} \ldots X_n^{d_n} := RED(t)$; $\sigma_1^{k_1} \ldots \sigma_n^{k_n} := \Omega(X_1^{e_1 - d_1} \ldots X_n^{e_n - d_n})$;
    $p_{RED(t)} := p_{RED(t)} + a \cdot X_1^{k_1} \ldots X_n^{k_n}$;
    $\hat{f} := \hat{f} - a \cdot \Omega(X_1^{e_1 - d_1} \ldots X_n^{e_n - d_n}) \cdot orbit_G(RED(t))$;
  ELSE $p_t := p_t + a$; $\hat{f} := \hat{f} - a \cdot orbit_G(t)$; *ENDIF;*
  ENDWHILE;
OUTPUT $f = \sum_{t \in T\, special} p_t(\sigma_1, \ldots, \sigma_n) \cdot orbit_G(t)$ *with* $p_t \in R[X_1, \ldots, X_n]$;

The loop invariant is $f = \hat{f} + \sum_{t \in T \text{special}} p_t(\sigma_1, \ldots, \sigma_n) \cdot orbit_G(t)$. By Lemma 3.4 and Lemma 3.10 (ii) every pass through the while-loop removes at least $a \cdot orbit_G(t)$ from $\hat{f}$ and adds only terms s to $\hat{f}$ with $desc(t) >_{lex} desc(s)$ or $(desc(t) = desc(s) \wedge t >_{lex} s)$ for all s. The termination is ensured by Remark 3.2, i.e. $\hat{f} = 0$ will be reached after finitely many cycles. $RED(t)$ is a special term for every $t \in T$, and therefore, f is a finite $R[\sigma_1, \ldots, \sigma_n]$-linear combination of special G-invariant orbits. □

EXAMPLE 3.13. *The Algorithm 3.12 has been implemented in MAS (Kredel, 1992) and has proven to perform well. Let $f = orbit_{A_4}(X_1^4 X_2^3 X_4^2) \in R[X_1, X_2, X_3, X_4]^{A_4}$. Then we obtain* $f = \underbrace{-\sigma_1\sigma_4^2 + 2\sigma_2\sigma_3\sigma_4 + \sigma_1^2\sigma_3\sigma_4 - \sigma_1\sigma_2^2\sigma_4}_{p_1} + \underbrace{\sigma_3}_{p_{X_1^3 X_2^2 X_4}} \cdot orbit_{A_4}(X_1^3 X_2^2 X_4)$.

Summarizing the results of this section, we have found that the Algorithm 3.12 represents any $f \in R[X_1, \ldots, X_n]^G$ as a finite $R[\sigma_1, \ldots, \sigma_n]$-linear combination of special G-invariant orbits, i.e.

$$f = \sum_{t \in T \text{special}} p_t(\sigma_1, \ldots, \sigma_n) \cdot orbit_G(t) \tag{3.3}$$

with $p_t \in R[X_1, \ldots, X_n]$. The algorithm works independently of the ground ring R, and the finite basis B which generates $R[X_1, \ldots, X_n]^G$ consists of all special G-invariant orbits.

4. Concluding remarks

The head term of a polynomial in $R[X_1, \ldots, X_n]^{S_n}$ is always descending w.r.t. $<_{lex}$, i.e. Algorithm 3.12 coincides for the symmetric group S_n exactly with the classical algorithm for symmetric polynomials. This strong relationship can be found again in the following complexity bound for the number of reduction steps.

LEMMA 4.1. *Let $f \in R[X_1, \ldots, X_n]^G$, let d be the maximal variable degree of f, and let $\#(d,n)$ be the number of descending terms $t \in T$ with maximal variable degree $\leq d$. Then at most $\#(d,n) \cdot |S_n|/|G|$ reduction steps are necessary to compute $f = \sum_{t \in T\, special} p_t(\sigma_1, \ldots, \sigma_n) \cdot orbit_G(t)$.*

PROOF. It is easy to verify, that every S_n-invariant orbit is a finite sum of not more than $|S_n|/|G|$ G-invariant orbits. Furthermore, every G-invariant orbit occurring in the reduction process of Algorithm 3.12 has to be reduced only once. Hence, at most $\#(d,n) \cdot |S_n|/|G|$ reduction steps are necessary. □

The next lemma shows that our degree bounds are optimal for permutation groups G from the point of view of worst case complexity.

LEMMA 4.2. *For all $n \geq 1$ exists a R-algebra of G-invariant polynomials $R[X_1, \ldots, X_n]^G$ which has no finite basis of G-invariant polynomials with maximal variable degree $< max\{1, n-1\}$ or total degree $< max\{n, n(n-1)/2\}$.*

PROOF. ($n=1$) trivial. ($n=2$) Let $\{\psi_1, \ldots, \psi_l\}$ be a finite basis of $R[X_1, X_2]^{S_2}$ with maximal variable degree < 1 or total degree < 2 for all ψ_i, i.e. $\psi_i = a_i(X_1 + X_2) + b_i$ with $a_i, b_i \in R$ for $1 \leq i \leq l$. Then there exists a $p \in R[X_1, \ldots, X_l]$ with $R[X_1, X_2]^{S_2} \ni X_1X_2 = p(\psi_1, \ldots, \psi_l)$ and a $\hat{p} \in R[X]$ with $\sigma_2 = X_1X_2 = \hat{p}(X_1 + X_2) = \hat{p}(\sigma_1)$. This implies that σ_1, $\sigma_2 \in R[X_1, X_2]^{S_2}$ are algebraically dependent (contradiction). ($n \geq 3$) Let $\{\psi_1, \ldots, \psi_l\}$ be a finite basis of $R[X_1, \ldots, X_n]^{A_n}$ with maximal variable degree $< (n-1)$ or total degree $< n(n-1)/2$ for all ψ_i. Then ψ_i is S_n-invariant for $1 \leq i \leq l$, because every $t \in T(\psi_i)$ contains at least two equal exponents. Hence, $\{\psi_1, \ldots, \psi_l\}$ cannot be a finite basis of $R[X_1, \ldots, X_n]^{A_n}$ (contradiction). □

Our last lemma combines the degree bound of Noether with our results and deduces a bound for the maximal variable degree in dependence of the order of the permutation group G.

LEMMA 4.3. *Let $char(K) = 0$. Then every polynomial in $K[X_1, \ldots, X_n]^G$ has a representation as a polynomial over the ground field K in special G-invariant orbits with maximal variable degree $\leq max\{k \in N \mid k \leq \sqrt{2|G| + \frac{1}{4}} - \frac{1}{2}\}$.*

PROOF. The basis of Noether for $R[X_1, \ldots, X_n]^G$ consists of all G-invariant orbits with total degree $\leq |G|$. The application of Algorithm 3.12 to any non-special G-invariant orbit in B leads to a representation in special G-invariant orbits with total degree $\leq |G|$, which implies that $R[X_1, \ldots, X_n]^G$ is generated by special G-invariant orbits with total degree $\leq |G|$. Hence, special G-invariant orbits with total degree $\leq |G|$ have maximal variable degree $\leq max\{k \in N \mid k \leq \sqrt{2|G| + \frac{1}{4}} - \frac{1}{2}\}$. □

Acknowledgements

The results of this note are based on the author's diploma thesis written under the supervision of Prof. Dr. Weispfenning (Passau). The author would like to thank Prof. Dr. Küchlin (Tübingen) for his support. Special thanks to Prof. Dr. Sturmfels (Berkeley) and the anonymous referees for their comments and remarks on the first version of this paper.

References

Becker, T., Kredel, H., Weispfenning, V. (1993). *Gröbner Bases: A Computational Approach to Commutative Algebra.* New York: Springer.

Garsia, A., Stanton, D. (1984). Group Actions on Stanley–Reisner Rings and Invariants of Permutation Groups. *Adv. Math.* **51**, 107–201.

Göbel, M. (1992). *Reduktion G-symmetrischer Polynome für beliebige Permutationsgruppen G.* Diploma Thesis, Universität Passau.

Kapur, D., Madlener, K. (1989). A Completion Procedure for Computing a Canonical Basis of a k-Subalgebra. In (Kaltofen, E., Watt, S., eds), pp. 1–11. *Proceedings of Computers and Mathematics 89.* Cambridge, MA: MIT.

Kredel, H. (1990). MAS: Modula-2 Algebra System. In (Gerdt, V. P., Rostovtsev, V. A., Shirkov, D. V., eds), pp. 31–34. *IV International Conference on Computer Algebra in Physical Research.* Singapore: World Scientific Publishing Co.

Noether, E. (1916). Der Endlichkeitssatz der Invarianten endlicher Gruppen. *Mathe. Ann.* **77**, 89–92.

Noether, E. (1926). Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p. *Abh. Akad. Wiss. Göttingen*, 28–35.

Robbiano, L., Schweedler, M. (1990). Subalgebra bases. In (Bruns, W., Simis, A., eds), pp. 61–87. *Commutative Algebra (Lect. Notes Math. 1430).* New York: Springer.

Schmid, B. J. (1991). Finite groups and invariant theory. In (Malliavin, M. P., ed.), pp. 35–66. *Topics in Invariant Theory (Lect. Notes Math. 1478).* New York: Springer.

Sturmfels, B. (1993). *Algorithms in Invariant Theory.* Vienna: Springer.

van der Waerden, B. L. (1971). *Algebra I.* Berlin: Springer.