A NEW DEGREE BOUND FOR VECTOR INVARIANTS OF SYMMETRIC GROUPS

P. FLEISCHMANN

ABSTRACT. Let R be a commutative ring, V a finitely generated free R- module and $G\ leGL_R(V)$ a finite group acting naturally on the graded symmetric algebra $A = S(V)$. Let $\beta(V, G)$ denote the minimal number m, such that the ring A^G of inva riants can be generated by finitely many elements of degree at most m.
For $G = \Sigma_n$ and $V(n, k)$, the k - fold direct sum of the natural permutat ion module, one knows that $\beta(V(n, k), \Sigma_n) \leq n$, provided that $n!$ is invertible in R. This was used by E.Noether to prove $\beta(V, G) \leq |G|$ if $|G|! \in R^*$.
In this paper we prove $\beta(V(n, k), \Sigma_n) \leq max\{n, k(n-1)\}$ for arbitrary commutative rings R and show equality for $n = p^s$ a prime power and $R = \mathbb{Z}$ or any ring with $n \cdot 1_R = 0$. Our results imply $\beta(V, G) \leq max\{|G|, \text{rank}(V)(|G|-1)\}$ for any ring with $|G| \in R^*$.

1. INTRODUCTION

Let R be a commutative ring, V a finitely generated free R - module and $G \leq GL_R(V)$ a finite group. Then G acts naturally on the symmetric graded algebra

$$A := S_R(V) = \oplus_{i=0}^{\infty} S_R(V)_i$$

where $S_R(V)_i$ denotes the i- th symmetric power of V. Notice that the action of G preserves degrees, hence the algebra A^G of invariants inherits the grading from A. It has been a classical problem of 19^{th} century algebra to construct minimal sets of generators for the ring of invariants A^G or sets of generators with minimal degree. In [3] (1916) E. Noether gave two different constructive proofs for the fact that A^G is finitely generated by invariants of degree at most $|G|$, if $\mathbb{Q} \subseteq R$. Both proofs can be made to work over any ring R having the property that the factorial $|G|!$ of the group order is invertible. (e.g. see [7], [2]).

In [4] (1926), Noether presented a proof for the fact that A^G is finitely generated whenever R is a noetherian ring. No assumption whatsoever on invertibility of $|G|$ is needed but the price one has to pay for this generality is, that the proof is not any more constructive. It essentially uses the fact that submodules of noetherian modules are finitely generated. The first proof in [3] uses a classical result of H. Weyl [8] on vector invariants of the symmetric groups. To state this and to show how it is applied, we have to introduce some notation:

.

Let $V := V(n) = R^{\underline{n}}$ be the free R - module with the natural permutation action of Σ_n on it. For $k \in \mathbb{N}$ we define $V(n,k) := V^{\oplus k} = V \oplus \cdots \oplus V$ to be the k - fold direct sum with diagonal action of Σ_n and $A_R(n,k) := S(V(n,k))$ to be the symmetric R - algebra over $V(n,k)$. Let $\{x_1, ..., x_n\}$ be a basis of $V(n)$ then for $k \in \mathbb{N}$ the set $\{x_{11}, ..., x_{n1}, ..., x_{1k}, ..., x_{nk}\}$ is a basis of $V^{\oplus k}$.
A monomial $X := x_{11}^{a_{11}} \cdot ... \cdot x_{n1}^{a_{n1}} \cdot ... \cdot x_{1k}^{a_{1k}} \cdot ... \cdot x_{nk}^{a_{nk}} \in S(V^{\oplus k})$ is of **multidegree** $md(X) := (d_1, ..., d_k) \in \mathbb{N}^k$ if $d_j = \sum_{i=1}^n a_{ij}$ and of (total) degree $d(X) := \sum_{j=1}^k d_j$. Clearly $A_R(n,k) = \oplus_{\underline{m} \in \mathbb{N}^k} A_R(n,k)_{\underline{m}}$ where $A_R(n,k)_{\underline{m}}$ is the set of R - linear combinations of monomials with multidegree $\underline{m}$ and the $A_R(n,k)_{\underline{m}}$'s are Σ_n - submodules. An element of $A_R(n,k)_{\underline{a}}$ is called homogeneous of multidegree $\underline{m}$.

Now let $G = \{e = g_1, g_2, \ldots, g_n\}$ be an arbitrary finite group of order n and let $W = Rw_1 \oplus \cdots \oplus Rw_k$ be an RG - module of rank k. Consider the Cayley - embedding $G \hookrightarrow \Sigma_n, g \mapsto (g_i \mapsto g_j := gg_i)$. Then

$$\nu : A_R(n,k) \to S_R(W), x_{i\ell} \mapsto g_i(w_\ell)$$

is a G - equivariant algebra epimorphism which preserves degrees. In fact

$$\nu(g(x_{i\ell})) = \nu(x_{j\ell}) = g_j(w_\ell) = gg_i(w_\ell) = g\nu(x_{i\ell}).$$

Now, for completeness, we repeat Noether's original 1916 - argument showing that the restriction

$$\nu : A_R(n,k)^{\Sigma_n} \to S_R(W)^G$$

is surjective, whenever n is invertible in R: In this case, for any $f = f(w_1, \ldots, w_k) \in S_R(V)^G$ we can define

$$F := \frac{1}{n}(f(x_{11}, x_{12}, \ldots, x_{1k}) + \cdots + f(x_{n1}, x_{n2}, \ldots, x_{nk})) \in A_R(n,k)^{\Sigma_n}$$

and get $\nu(F) = \frac{1}{n}(f(g_1(w_1), g_1(w_2), \ldots, g_1(w_k)) + \cdots + f(g_n(w_1), g_n(w_2), \ldots, g_n(w_k))$
$= \frac{1}{n}(g_1 f(w_1, w_2, \ldots, w_k) + \cdots + g_n f(w_1, w_2, \ldots, w_k) = f$.

Let $\beta(W,G)$ denote the minimum number m such that $S_R(W)^G$ is generated by finitely many invariants of degree at most m and $\beta_R(G) := max\{\beta(W,G)\}$, where W ranges through all RG - modules that are finitely generated and free as R - modules. We see immediately that $|G| \in R^*$ implies

$$\beta(W,G) \leq \beta(V(n,k), \Sigma_n).$$

For any $f = f(x_1, \ldots, x_n) \in S(V(n))$ and $\underline{m} = (m_1, \ldots, m_k) \in \mathbb{N}^k$ we define $Pol(f)_{\underline{m}}$ to be the $A_R(n,k)_{\underline{m}}$ - part of the element $f(x_{11} + \cdots + x_{1k}, \ldots, x_{n1} + \cdots + x_{nk})$. Notice that $Pol(f)_{\underline{m}} \in A_R(n,k)^G$ if $f \in S(V(n))^G$ for any $G \leq \Sigma_n$; moreover $Pol(f)_{\underline{m}} = 0$ whenever $\sum_i m_i$ exceedes the degree of $f \in S(V(n))$.
Now Weyl's theorem states that, if $R = K$ is a field containing $\mathbb{Q}$, then

$$A_K(n,k)^{\Sigma_n} = K[Pol(e_i)_{\underline{m}} \mid i = 1, ..., n,\ \underline{m} \in \mathbb{N}^k],$$

where e_i is the i -th elementary - symmetric polynomial. Since $(e_i)_{\underline{m}} = 0$ if $\underline{m} = (m_1, ..., m_k)$ and $\sum_j m_j > i$, $A_K(n,k)^{\Sigma_n}$ is generated by a finite number of elements of degree $\leq n$.

Recently, new proofs for this result have been given by D. Richman and others, which work over any commutative ring R with $n! \in R^*$ (see [2]), In this case Weyls theorem implies $\beta(V(n,k),\Sigma_n) \leq n = |G|$ hence $\beta_R(G) \leq |G|$.
But, as we will see, Weyl's theorem does no longer hold in positive characteristic $\leq n$. Hence although the restriction $\nu : A_R(n,k)^{\Sigma_n} \to S_R(V)^G$ is surjective in the more general situation where only $|G|$ is invertible in R, a proof of $\beta_R(G) \leq |G|$ in this generality is not known at the moment of this writing (see [2] and [6] for proofs in the case of solvable groups).

It is the aim of this paper to analyze vector invariants of Σ_n in the situation where R is an arbitrary commutative ring like for example the ring of rational integers $\mathbb{Z}$.
In [1], Campbell, Hughes and Pollack prove $\beta(V(n,k),\Sigma_n) \leq max\{|G|, k \cdot \left(\begin{array}{c} n \\ 2 \end{array}\right)\}$ and thus obtain $\beta(V,G) \leq max\{|G|, rank(V) \cdot \left(\begin{array}{c} |G| \\ 2 \end{array}\right)\}$ for any commutative ring R with $|G| \in R^*$.

I will prove that $\beta(V(n,k),\Sigma_n) \leq max\{n, k(n-1)\}$ for arbitrary commutative rings R, with equality if $n = p^s$ a prime power and $R = \mathbb{Z}$ or $p \cdot 1_R = 0$. This will imply

$$\beta(V,G) \leq max\{|G|, \mathrm{rank}(V)(|G|-1)\}$$

if $|G|$ is invertible in R. It also implies for the 'global bounds' over $R = \mathbb{Z}$ or $R = K$, a field of characteristic p:

$$\beta_R(\Sigma_{p^s}) = \infty.$$

Hence in this case there is no finite global bound at all, even for the smallest nontrivial group Σ_2.

2. Multiplication in invariant rings

Let R, V, A and G be as in the introduction and $U \leq G$ a subgroup. Then we have the following homomorphism of R - modules:

$$T_U^G : A^U \to A^G, \ a \mapsto \sum_{g \in [G:U]} {}^g a,$$

where $[G:U]$ denotes an arbitrary cross section of (left) U - cosets in G, i.e. $G = \biguplus_{g \in [G:U]} gU$. This is called the **(relative) trace homomorphism**. It preserves (multi) degrees and if the index $|[G:U]|$ is invertible in R, then T_U^G is an epimorphism. (Since $a \in A^U$, its relative trace $T_U^G(a)$ does not depend on the choice of coset representatives).

We will give a 'Mackey formula' for the product of relative traces which is particularly useful in the case of invariant rings of permutation modules.

Let $U, V \leq G$ be subgroups and suppose we are given a a cross section $[U : G : V]$ of U, V double - cosets with $G = \uplus_{g\in[U:G:V]} UgV$ and for each $g \in [U : G : V]$ a cross section $[UgV : V] \subseteq U$ of V - cosets with $UgV = \uplus_{t\in[UgV:V]} tgV$. Then $[UgV : V]$ is also a cross section $[U : U\cap\ {}^gV]$ of $U\cap\ {}^gV$ cosets in U, i.e. $U = \uplus_{t\in[UgV:V]} tU\cap\ {}^gV$. Here, as in the following ${}^gV$ denotes gVg^{-1}.

Proposition 2.1. *Let $U, V \leq G$ be subgroups and $[U : G : V]$ be an arbitrary cross section of $U - V$ - double cosets in G. Then we have for each $a \in A^U$ and $b \in A^V$:*

$$T_U^G(a) \cdot T_V^G(b) = \sum_{g\in[U:G:V]} T^G_{U\cap\ {}^gV}(agb).$$

Proof: First notice that the summands on the right hand side do not depend on the choice of double coset representatives. Indeed if $u \in U$ and $v \in V$, then we have

$$T^G_{U\cap\ {}^{ugv}V}(a(ugvb)) = T^G_{U\cap\ {}^{ug}V}((ua)(ugb)) = T^G_{U\cap\ {}^{ug}V}(u(agb)) = T^G_{U\cap\ {}^{g}V}(agb).$$

Now we choose $[U : G : V]$ and $[UgV : V]$ such that $G = \uplus_{g\in[U:G:V],t\in[U:U\cap\ {}^gV]} tgV$ and conclude $T_U^G(a) \cdot T_V^G(b) = T_U^G(a \cdot T_V^G(b)) = \sum_{d\in[G:U],h\in[G:V]} d[a(hb)] =$ $\sum_{g\in[U:G:V],t\in[U:U\cap\ {}^gV],d\in[G:U]} d[a(tgb)] = \sum_{g\in[U:G:V],t\in[U:U\cap\ {}^gV],d\in[G:U]} dt[a(gb)] =$ $\sum_{g\in[U:G:V]} T^G_{U\cap\ {}^gV}(a(gb))$. $\circ$

From now on we suppose that $G \leq \Sigma_n$ and $V := V(n)$, i.e. that V is a permutation module of G. It is well known that in this case the orbit sums of monomials form a free R - basis of A^G so the formulae above, applied to momomials, completely describe multiplication in A^G.
More precisely, for any monomial $a \in A$ let G_a denote the stablizer $G_a := \{g \in G \mid {}^ga = a\}$ and a_G^+ denote the G - orbit sum $\sum_{g\in[G:G_a]} {}^ga$. (We write a^+ if G is clear from the context). Then we have

Corollary 2.2.

$$a_G^+ \cdot b_G^+ = \sum_{g\in[G_a:G:G_b]} \frac{|G_{agb}|}{|G_a \cap\ {}^gG_b|}(ag(b))_G^+.$$

3. The 'row - lex' order of matrices

Let the set of k - vectors over $\mathbb{N}$ be ordered lexicographically, i.e. by the rule $\underline{a} = (a_1, a_2, ..., a_k) < \underline{b} = (b_1, b_2, ..., b_k)$ if and only if there is $1 \leq j_0 \leq k$ with $a_j = b_j$ for $j < j_0$ and $a_{j_0} < b_{j_0}$. We say that $\underline{b}$ **(strictly) dominates** $\underline{a}$ iff $a_i \leq b_i$ for all $i = 1, \ldots, k$ (with at least one $a_i < b_i$). Notice that $\underline{a} < \underline{b}$ whenever $\underline{b}$ strictly dominates $\underline{a}$ but $\underline{a} < \underline{b}$ does not imply that $\underline{a}$ is dominated by $\underline{b}$ (e.g.

$(1,2,2) < (2,1,1)$). We will identify the set $\mathcal{M} := \mathcal{M}(n,k)$ of monomials in $A := A_R(n,k)$ with the set $Mat_{n,k}(\mathbb{N}_0)$ of nonnegative n,k - matrices using the bijection

$$c : \mathcal{M}(n,k) \to Mat_{n,k}(\mathbb{N}_0),\ x_{11}^{a_{11}} \cdot \ldots \cdot x_{n1}^{a_{n1}} \cdot \ldots \cdot x_{1k}^{a_{1k}} \cdot \ldots \cdot x_{nk}^{a_{nk}} \mapsto (a_{ij}).$$

Now we define a total order on the set $\mathcal{M} := \mathcal{M}(n,k)$ of monomials in the following way (we call this the 'row - lex' order) :
$a = (a_{ij}) < b = (b_{ij})$ if and only if $d(a) < d(b)$ or $d(a) = d(b)$ and $md(a) < md(b)$ or $md(a) = md(b)$ and there is a row index $i_0 \in \mathbb{N}$ such that the row vectors $a_i = b_i$ for all $i < i_0$ and $a_{i_0} < b_{i_0}$. Hence the matrices are ordered first by total degree, then multidegree and, if these coincide by the 'row - lexicographic' order. This amounts to the total order of variables x_{ij} given by $x_{11} > x_{21} > \cdots > x_{n1} > x_{12} > x_{22} \cdots > x_{(n-1)n} > x_{nn}$. Notice that the action of Σ_n on $\mathcal{M}$ corresponds to the permutation of rows of $a = (a_{ij})$ i.e. ${}^{\sigma}a := (a_{\sigma^{-1}(i),j}) = \hat{\sigma} \circ (a_{ij})$ where $\hat{\sigma} := {}^{\sigma}(\delta_{ij})$ is the permutation matrix corresponding to $\sigma \in \Sigma_n$. Moreover the product of monomials is given by componentwise addition of matrix entries

$$ab = c = (c_{ij}) \text{ with } c_{ij} = a_{ij} + b_{ij}$$

hence $md(ab) = md(a) + md(b)$. For $a, b, c \in \mathcal{M}$ we have $ab \geq a$ with equality if and only if $b = 1$ (the zero matrix) and $a < b \iff ac < bc$. For $f = \sum_{a \in \mathcal{M}} r_a a \in A$ we define $HT(f)$ to be the highest monomial a with respect to "$<$", that appears in f with nonzero coefficient r_a. Now we get a preorder (i.e. a transitive relation) on A by defining f to be less than $g \in A$ ($f \prec g$) if and only if $HT(f) < HT(g)$. We also define $f \preceq g \iff f = g$ or $f \prec g$. For $a \in \mathcal{M}$ the orbit sum a^+ will usually be written by displaying its highest element $a = max\ a^G$. We get immediately:

Lemma 3.1. *Let $a, b \in \mathcal{M}$ with $a := max\ a^G$ and $b := max\ b^G$. Then $G_{ab} = G_a \cap G_b$ and*

$$(ab)^+ - a^+ b^+ \prec (ab)^+.$$

Proof: First note that $G_a \cap G_b \subseteq G_{ab}$ so we only have to prove the opposite inclusion. Suppose then that $g \in G$ but $g \notin G_a \cap G_b$. Then without loss of generality we may assume $g \notin G_a$. Hence $ga \prec a$ and $g(ab) = g(a)g(b) \prec ab$. Therefore $g \notin G_{ab}$ and so $G_{ab} = G_a \cap G_b$ and we conclude

$$(ab)^+ - a^+ b^+ = -\{ \sum_{g \in [G_a : G : G_b] \setminus G_a \cdot G_b} \frac{|G_{agb}|}{|G_a \cap {}^{g}G_b|} (ag(b))^+ \}.$$

For any $t \in G$ we have $ta \preceq a$, hence $ta \cdot tgb \preceq a \cdot tgb \preceq a \cdot b$. Let $g \in [G_a : G : G_b]$ and $t(a \cdot g(b)) = max\ (ag(b))^G$. If $ta \cdot tgb \not\prec ab$, then $ta \cdot tgb = ab$, hence $ta = a$ and $tgb = b$ and $g \in G_a\ id\ G_b$. We conclude that all monomials that appear in $(ab)^+ - a^+ b^+$ are stricly less than ab. $\circ$

For $j = 1, \ldots, k$ let $\underline{1}^{(j)} \in \mathcal{M}$ denote the matrix whose entries are all one in the j - th column and zero elsewhere. Let $a \in \mathcal{M}$ be such that for some column index j and all $i = 1, \ldots, n$ the entries a_{ij} are positive. Then

$$a^+ = \begin{pmatrix} a_{11} & \ldots & a_{1j} - 1 & \ldots & a_{1k} \\ a_{21} & \ldots & a_{2j} - 1 & \ldots & a_{2k} \\ \ldots & \ldots & \ldots & \ldots\ldots & \\ a_{n1} & \ldots & a_{nj} - 1 & \ldots & a_{nk} \end{pmatrix}^+ \cdot \begin{pmatrix} 0 & \ldots & 1 & \ldots & 0 \\ 0 & \ldots & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots\ldots & \\ 0 & \ldots & 1 & \ldots & 0 \end{pmatrix}^+ .$$

Hence A^G can be generated by the $\underline{1}^{(i)}$'s and orbit sums a^+ such that each column of $a \in M$ has a zero entry.
If $G = \Sigma_n$ and $\tilde{a} \in \mathcal{M}$, then $max\ \tilde{a}^G$ has a particularly easy shape: let $(a_1 \geq a_2 \geq \cdots \geq a_n)$ be the family of row vectors of $\tilde{a}$ and consider $b := \begin{pmatrix} b_1 \\ b_2 \\ \cdots \\ b_n \end{pmatrix} \neq a := \begin{pmatrix} a_1 \\ a_2 \\ \cdots \\ a_n \end{pmatrix}$, where the unordered families (a_i) and (b_i) coincide. Let $i_0 := min\{i \mid a_i \neq b_i\}$ then the families $(a_i)_{1 \leq i < i_0}$ and $(b_i)_{1 \leq i < i_0}$ coincide and b_{i_0} must be one of the a_i's with $i > i_0$, hence $b_{i_0} < a_{i_0}$ and $b < a$. We see that a is the maximal element in the orbit $a^{\Sigma_n} = \tilde{a}^{\Sigma_n}$.

4. Indecomposable invariants

The following definition as well as the lemma make sense for arbitrary invariant rings of finite groups:

Definition 4.1. For $d \in \mathbb{N}$ let $\mathrm{R}(d) := R[b \in A^G \mid d(b) < d]$. An element $a \in A^G$ is called **indecomposable** if and only if $a \notin \mathrm{R}(d(a))$ and **decomposable** if $a \in \mathrm{R}(d(a))$. (In particular 0 is decomposable.)

Lemma 4.2. *Let $S \subseteq A^G$ then the following are equivalent:*
(i)*: $A^G = R[S]$;*
(ii)*: For each $a \in \mathcal{M}$ with $a^+ \in A^G \backslash S$ there is $f \in R[S]$ with $f = 0$ or $d(f) \leq d(a)$ such that $a^+ - f$ is decomposable.*

Proof: '(i) $\Rightarrow$ (ii)': We can take $f = a^+$. '(ii) $\Leftarrow$ (i)' : Let $m \in \mathcal{M}$ be of minimal degree d such that $m^+ \in A^G \backslash R[S]$. Then $m^+ \notin S$, so $c := m^+ + f$ is decomposable for some $f \in R[S]$ of degree $\leq d$ or $f = 0$. In any case $d(c) \leq d$ and $c \in \mathrm{R}(d)$, so it is a linear combination of products of elements b^+ of degree $< d$. By minimality of d, each of these b^+'s lies in $R[S]$, hence c and m^+ lie in $R[S]$, a contradiction. So $R[S] = A^G$. $\circ$

Remark 4.3.

$$\beta(V(n,k), G) = max\{d \mid R(d) < A^G\} = min\{d \mid R(d+1) = A^G\}.$$

From not on let $G := \Sigma_n$ and $A := A(n,k)$.

Definition 4.4. Let $\mathcal{B}^1$ denote the R - module spanned by those elements $b^+ \in A^G$ with $b \in \mathcal{M}$ such that the first column vector $\underline{b}^1$ of b lies in $\{0,1\}^{\underline{n}}$ and all rows of b starting with 1 in the first column are of the form $(1, 0, \ldots, 0)$.

Lemma 4.5. *For any $a \in \mathcal{M}$ we have:*

$$a^+ \in (\mathcal{B}^1 \cap A^G_{md(a)}) + \mathrm{R}(d(a^+)).$$

This implies that if $md(a) = (a_1, a_2, \dots, a_k)$ *with* $a_1 > n$ *or* $a_1 = n$ *and* $md(a) \neq (n, 0, 0, \dots, 0)$ *then* a^+ *is decomposable and if* $md(a) = (n, 0, 0, \dots, 0)$ *then* $a^+ - r\underline{1}^{(1)}$ *is decomposable for some* $r \in R$.

Proof: We use induction with respect to the $\prec$ relation. Let $a = max\ a^G$ with $d(a^+) = d$ and assume that all b^+ with $b^+ \prec a^+$ (and $md(b) = md(a) = (a_1, \dots, a_k)$) lie already in $\mathcal{B}^1 \cap A^G_{md(a)} + \mathrm{R}(d)$. We can assume that at least one zero appears in the first column of a. Now there are three cases to consider: the first column has three distinct entries, two distinct entries with the non-zero entry bigger than one, and two distinct entries with the non-zero entry equal to one.

So we assume first that $a_{11} \geq a_{21} \geq \dots a_{s1} > c = a_{(s+1)1} = \dots = a_{t1} > 0 = a_{(t+1)1} = \dots = a_{n1}$. Consider

$$a^+ = \begin{pmatrix} a_{11} & \underline{b}_1 \\ a_{21} & \underline{b}_2 \\ \dots & \dots \\ a_{s1} & \underline{b}_s \\ c & \underline{b}_{s+1} \\ c & \underline{b}_{s+2} \\ \dots & \dots \\ c & \underline{b}_t \\ 0 & \underline{b}_{t+1} \\ \dots & \dots \\ 0 & \underline{b}_n \end{pmatrix}^+$$

where the $\underline{b}_i$ are appropriate nonnegative $k-1$ vectors satisfying $\underline{b}_t \leq \dots \leq \underline{b}_{s+1}$ and $\underline{b}_n \leq \dots \leq \underline{b}_{t+1}$. Let $a' = \begin{pmatrix} a_{11}-1 & \underline{b}_1 \\ a_{21}-1 & \underline{b}_2 \\ \dots & \dots \\ a_{s1}-1 & \underline{b}_s \\ c & \underline{0} \\ c & \underline{0} \\ \dots & \dots \\ c & \underline{0} \\ 0 & \underline{b}_{t+1} \\ \dots & \dots \\ 0 & \underline{b}_n \end{pmatrix}$ and $e = \begin{pmatrix} 1 & \underline{0} \\ 1 & \underline{0} \\ \dots & \dots \\ 1 & \underline{0} \\ 0 & \underline{b}_{s+1} \\ 0 & \underline{b}_{s+2} \\ \dots & \dots \\ 0 & \underline{b}_t \\ 0 & \underline{0} \\ \dots & \dots \\ 0 & \underline{0} \end{pmatrix}$ then $a' = max\ {a'}^G$ and $e = max\ e^G$ and we get $a^+ - a'i^+ e^+ = (a'e)^+ - {a'}^+ e^+ \prec a^+$. Hence $a^+ - {a'}^+ e^+ \in \mathcal{B}^1 \cap A^G_{md(a)} + \mathrm{R}(d)$. Obviously ${a'}^+ e^+ \in \mathrm{R}(d)$ so we conclude $a^+ \in \mathcal{B}^1 \cap A^G_{\underline{d}} + \mathrm{R}(d)$.

So we can assume that $a = \begin{pmatrix} c & \underline{b}_1 \\ c & \underline{b}_2 \\ \dots & \dots \\ c & \underline{b}_s \\ 0 & \underline{b}_{s+1} \\ 0 & \underline{b}_{s+2} \\ \dots & \dots \\ 0 & \underline{b}_n \end{pmatrix}$ with $c > 1$ and $\underline{b}_n \leq \dots \leq \underline{b}_{s+1}$.

Now let $a' = \begin{pmatrix} c-1 & \underline{b}_1 \\ c-1 & \underline{b}_2 \\ \dots & \dots \\ c-1 & \underline{b}_s \\ 0 & \underline{0} \\ 0 & \underline{0} \\ \dots & \dots \\ 0 & \underline{0} \end{pmatrix}$ and $e = \begin{pmatrix} 1 & \underline{0} \\ 1 & \underline{0} \\ \dots & \dots \\ 1 & \underline{0} \\ 0 & \underline{b}_{s+1} \\ 0 & \underline{b}_{s+2} \\ \dots & \dots \\ 0 & \underline{b}_n \end{pmatrix}$. Again $a' = max\ a'^G$ and $e = max\ e^G$ and we conclude as above.

Finally we can assume that $a = \begin{pmatrix} 1 & \underline{b}_1 \\ 1 & \underline{b}_2 \\ \dots & \dots \\ 1 & \underline{b}_s \\ 0 & \underline{b}_{s+1} \\ 0 & \underline{b}_{s+2} \\ \dots & \dots \\ 0 & \underline{b}_n \end{pmatrix}$ with $\underline{b}_s \le \dots \le \underline{b}_1$ and $\underline{b}_n \le \dots \le \underline{b}_{s+1}$.

Now let $a' = \begin{pmatrix} 1 & \underline{0} \\ 1 & \underline{0} \\ \dots & \dots \\ 1 & \underline{0} \\ 0 & \underline{b}_{s+1} \\ 0 & \underline{b}_{s+2} \\ \dots & \dots \\ 0 & \underline{b}_n \end{pmatrix}$ and $e = \begin{pmatrix} 0 & \underline{b}_1 \\ 0 & \underline{b}_2 \\ \dots & \dots \\ 0 & \underline{b}_s \\ 0 & \underline{0} \\ 0 & \underline{0} \\ \dots & \dots \\ 0 & \underline{0} \end{pmatrix}$. Again $a' = max\ a'^G$ and $e = max\ e^G$ and we conclude as above.

If $a_1 > n$ or $a_1 = n$ and $md(a) \neq (n, 0, \dots, 0)$ then, by definition, $\mathcal{B}^1 \cap A^G_{md(a)} = 0$ and a^+ must be decomposable. If $md(a) = (n, 0, \dots, 0)$ then $\mathcal{B}^1 \cap A^G_{md(a)} = R\underline{1}^{(1)}$. This finishes the proof. $\circ$

Notice that we also have a right Σ_k - action on A by permuting 'columns' of monomials. On $\mathcal{M}$ this action is described by right multiplication with $k \times n$ - permutation matrices. Hence A is a $R\Sigma_n$ - $R\Sigma_k$ - bimodule; in particular Σ_k also acts on the invariant ring A^G.
Clearly the total degree of a monomial is not changed by column permutations; hence if $a, b \in \mathcal{M}$ are largest in their Σ_n - orbits and a and b lie in the same Σ_k - orbit, then a^+ is decomposable if and only if b^+ is decomposable. This observation leads to the following

Theorem 4.6. *For $j = 1, \dots, k$ let $\underline{1}^{(j)} \in \mathcal{M}$ denote the matrix whose entries are all one in the j - th column and zero elsewhere and define*

$\mathcal{M}_n := \{a^+ \in A^{\Sigma_n} \mid md(a)$ is dominated by $(n-1, \dots, n-1)\} \cup \{\underline{1}^{(j)} \mid 1 \le j \le k\}$.

Then $A^{\Sigma_n} = R[\mathcal{M}_n]$. In particular

$$\beta(V(n,k), \Sigma_n) \le max\{n, k(n-1)\},$$

i.e. A^{Σ_n} can be generated by elements of degree $\le max\{n, k(n-1)\}$.

Proof: By 4.2 it suffices to show that for each element $a \in \mathcal{M}$ with a^+ not in $\mathcal{M}_n$, there is a suitable $f \in R[\mathcal{M}_n]$ with $d(f) \leq d(a)$ or $f = 0$ such that $a^+ - f$ is decomposable. So suppose that a^+ has multidegree $(a_1, \ldots, a_n)$ with total degree d and $a_i \geq n$. Since $\mathcal{M}_n$ and $\mathrm{R}(d)$ are stable under column permutations, we can assume that $i = 1$. Now 4.5 tells us that $a^+ \in (\mathcal{B}^1 \cap A^G_{md(a)}) + \mathrm{R}(d)$ and that if $a_1 > n$ or $a_1 = n$ and $md(a) \neq (n, 0, \ldots, 0)$ a^+ must be decomposable. If $md(a) = (n, 0, \ldots, 0)$ then $a^+ - r \cdot \underline{1}^{(1)}$ is decomposable for some $r \in R$. ∘

As mentioned in the introduction, we will now show that our new degree bound is 'best possible' in the following sense:

Theorem 4.7. *Let $n = p^s$ be the power of a prime p and R be $\mathbb{Z}$ or a ring with $p \cdot 1_R = 0$. Then*

$$\beta(V(n,k), \Sigma_n) = max\{n, k(n-1)\}.$$

Proof: Let $G = \Sigma_n$ and A_R denote A if it is defined over R. Since V is a permutation module, $A_R^{\Sigma_n}$ is a free R - module, spanned by orbit sums of monomials. Hence $A_R^{\Sigma_n} = A_{\mathbb{Z}}^{\Sigma_n} \otimes_{\mathbb{Z}} R$ and we have $\beta(V_R(n,k), \Sigma_n) \leq \beta(V_{\mathbb{Z}}(n,k), \Sigma_n)$. Hence it suffices to show that for each $k \geq 1$ and R with $p \cdot 1_R = 0$ the element a_k^+ with

$$a_k := \begin{pmatrix} 1 & \underline{0} \\ 1 & \underline{0} \\ \ldots & \ldots \\ 1 & \underline{0} \\ 0 & \underline{b}_{n-1} \end{pmatrix}$$

and $\underline{b}_{n-1} = (n-1, \ldots, n-1) \in \mathbb{N}_0^{k-1}$ is indecomposable in $A(n,k)^G$. We use induction on k. We have $a_1^+ = e_{n-1}$; notice that $A_R(n,1)^{\Sigma_n} = R[e_1, \ldots, e_n]$ is a polynomial ring generated by the elementary symmetric polynomials $e_i, i = 1, \ldots, n$, which are algebraically independent; hence the indecomposability of a_1^+ is a consequence of the main theorem on symmetric functions. Assume now that a_{k-1}^+ is indecomposable but a_k^+ is not. Then

$$a_k^+ \in \sum_{\underline{0} \neq \underline{d}_k} A(n,k)^G_{\underline{d}_k} \cdot A(n,k)^G_{\underline{n-1}_k - \underline{d}_k},$$

where $\underline{n-1}_k = (n-1, \ldots, n-1) \in \mathbb{N}^k$ and the $\underline{d}_k$ are strictly dominated by $\underline{n-1}_k$. Now we consider the G - equivariant ring epimorphism $s : A_R(n,k) \to A_R(n,k-1)$ which is the identity on the $x_{i\ell}$ for $\ell < k$ and maps x_{ik} to 1 for $i = 1, \ldots, n$. Notice that for $b \in \mathcal{M}$, $s(b^+) = \frac{|G_{s(b)}|}{|G_b|}(s(b))^+_G$. In particular $s(a_k^+) = \frac{|G_{a_{k-1}}|}{|G_{a_k}|} a_{k-1}^+ = a_{k-1}^+$. It is easy to see from 4.5 that each $h^+ \in A^G_{(0,\ldots,0,i)}$ with $0 < i \leq n-1$ is a linear combination of products of elements of the form b_j^+ with $b_j = \begin{pmatrix} \underline{0} & 1 \\ \underline{0} & 1 \\ \ldots & \ldots \\ \underline{0} & 0 \\ \underline{0} & 0 \end{pmatrix}$ with $0 < j < n$ ones and $n-j$ zeros in the last column. We get $G_{s(b_j)} = G$ and hence $\frac{|G_{s(b_j)}|}{|G_{b_j}|} = |b_j^G| = \begin{pmatrix} n \\ j \end{pmatrix} \equiv 0 \ mod(p)$ by Lucas' congruences, hence $s(h^+) = 0$ for

each $h^+ \in A^G_{(0,\dots,0,i)}$ with $0 < i < n$.
Clearly we have $s(A(n,k)^G_{\underline{d}_k}) \subseteq A(n,k-1)^G_{\underline{d}_{k-1}}$, hence

$$a^+_{k-1} = s(a^+_k) \in \sum_{\underline{0} \neq \underline{d}_{k-1}} A(n,k-1)^G_{\underline{d}_{k-1}} \cdot A(n,k-1)^G_{\underline{n-1}_{k-1} - \underline{d}_{k-1}}.$$

Since $s(A(n,k)^G_{(0,\dots,0,i)}) = 0$ for $0 < i \leq n-1$, all 'surviving' summands must have $\underline{d}_{k-1} = (d_1, \dots, d_{k-1})$ different from $(0, \dots, 0)$ and strictly dominated by $(n-1, \dots, n-1)$. But this implies that a^+_{k-1} is decomposable, which is a contradiction. $\circ$

References

[1] H.E.A. Campbell, I.Hughes, R.D. Pollack, *Vector invariants of symmetric groups*, Canad. Math. Bull. **33**, 391-397, (1990).

[2] S.Hu, M.Kang, *Efficient generation of the ring of invariants*, J. Algebra, **180**, 341-364, (1996).

[3] E. Noether, *Der Endlichkeitssatz der Invarianten endlicher Gruppen*, Math. Ann. **77**, 89-92, (1916).

[4] E. Noether, *Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p*, Nachr. Ges. Wiss. Göttingen (1926), 28-35, in 'Collected Papers', pp.485-492, Springer Verlag, Berlin (1983).

[5] D. Richman, *Explicit generators of the invariants of finite groups*, Adv. Math. to appear.

[6] L. Smith, *E. Noether's bound in the invariant theory of finite groups*, Arch. Math. **66**, 89-92, (1995).

[7] L. Smith, *Polynomial Invariants of Finite Groups*, A.K. Peters Ltd., (1995).

[8] H. Weyl, *The Classical Groups*, 2^{nd} Edition, Princeton Univ. Press, Princeton (1953).

Current address: Institute for Experimental Mathematics University of Essen Ellernstr. 29, 45326 Essen, Germany

E-mail address: peter @ exp-math.uni-essen.de