PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 135, Number 4, April 2007, Pages 987–995
S 0002-9939(06)08574-1
Article electronically published on October 11, 2006

LOWER DEGREE BOUNDS FOR MODULAR VECTOR INVARIANTS

UĞUR MADRAN

(Communicated by Bernd Ulrich)

ABSTRACT. Let G be a finite group of order divisible by a prime p acting on an $\mathbb{F}$ vector space V, where $\mathbb{F}$ is the field with p elements and $\dim_{\mathbb{F}} V = n$. Consider the diagonal action of G on m copies of V. This note sharpens a lower bound for $\beta(\mathbb{F}[\oplus_m V]^G)$ for groups which have an element of order p whose Jordan blocks have sizes at most 2.

1. INTRODUCTION

Let $\rho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a faithful representation of a finite group G over the field $\mathbb{F}$. For a positive integer $m \in \mathbb{N}$, G acts via ρ on $\mathbb{F}[x_{i,j} \,|\, 1 \le i \le m,\ 1 \le j \le n]$ by algebra automorphisms given by

$$\begin{bmatrix} g \cdot x_{i,1} \\ g \cdot x_{i,2} \\ \vdots \\ g \cdot x_{i,n} \end{bmatrix} = \begin{bmatrix} \alpha_{1,1}(g) & \alpha_{1,2}(g) & \dots & \alpha_{1,n}(g) \\ \alpha_{2,1}(g) & \alpha_{2,2}(g) & \dots & \alpha_{2,n}(g) \\ \vdots & \vdots & & \vdots \\ \alpha_{n,1}(g) & \alpha_{n,2}(g) & \dots & \alpha_{n,n}(g) \end{bmatrix} \begin{bmatrix} x_{i,1} \\ x_{i,2} \\ \vdots \\ x_{i,n} \end{bmatrix}$$

for all $1 \le i \le m$ and $g \in G$, where $\rho(g) = [\alpha_{i,j}(g)] \in \mathrm{GL}(n, \mathbb{F})$.

The subalgebra of invariants

$$\mathbb{F}[x_{1,1}, \dots, x_{m,n}]^G = \{f \in \mathbb{F}[x_{1,1}, \dots, x_{m,n}] \,|\, g \cdot f = f \text{ for all } g \in G\}$$

is the ring of vector invariants. A solution to the problem of finding generators for this invariant ring is a first fundamental theorem for the particular representation $\rho(G)$. For a more detailed introduction to invariants and the problems, we suggest [B], [S1], [S2], [Stu]. As a consequence of a theorem of Noether [N2], $\mathbb{F}[x_{1,1}, \dots, x_{m,n}]^G$ is finitely generated as an $\mathbb{F}$-algebra. Moreover, if $\mathrm{char}\,\mathbb{F}$ does not divide $|G|$, the order of the group, referred to as the *nonmodular case*, generators have degrees at most $|G|$ no matter how large m is. However, there is no such upper bound depending only on the size of the group in the *modular case*, i.e., where $\mathrm{char}\,\mathbb{F} = p$ divides $|G|$. Here we denote by $\beta(m \cdot \rho(G))$ or simply $\beta(G)$ the maximal degree of a generator of $\mathbb{F}[x_{1,1}, \dots, x_{m,n}]^G$. So, $\mathbb{F}[x_{1,1}, \dots, x_{m,n}]^G$ can be generated by invariant polynomials of degree at most $\beta(G)$.

Received by the editors September 9, 2005 and, in revised form, November 11, 2005.
2000 *Mathematics Subject Classification.* Primary 13A50.
Key words and phrases. Modular invariant theory, vector invariants, degree bound.
The author was supported in part by TÜBİTAK.

In the modular case, Richman proved in [R2] that there is a constant α depending only on $|G|$ and the characteristic p of the ground field such that

$$\beta(G) \geq \alpha \cdot m$$

for any finite group and for sufficiently large m. In particular, he also showed that

$$\beta(G) \geq \max\{2, \frac{m}{n-1}, \frac{m}{|G|-1}, \frac{p}{p-1} \cdot \frac{m}{n}\} \tag{1}$$

when $\mathbb{F} = \mathbb{F}_p$ is the prime field, with the refinement that

$$\beta(G) \geq (m-n+2)(p-1) \tag{2}$$

when G contains a pseudoreflection.

For permutation groups, the given lower bounds are sharpened by Kemper and Stepanov independently to

$$\beta(G) \geq m(p-1).$$

Campbell and Hughes describe a generating set for the vector invariants of the 2-dimensional representation of the cyclic group of order p over $\mathbb{F}_p$ in [CH], proving a conjecture of Richman.

In this note, extending the result of Richman, we refine the bound (1) by considering the Jordan decomposition of a representation of an element of order p. More precisely, if there exists $\gamma \in G$ of order p such that $\rho(\gamma)$'s Jordan blocks have sizes at most 2 and $\rho(\gamma)$ has r nontrivial Jordan blocks, then

$$\beta(G) \geq \frac{m-n+2r}{r}(p-1), \tag{3}$$

provided $\mathbb{F} = \mathbb{F}_p$.

Note that we do not need any further assumptions on the group G or the representation ρ, e.g., we do not require any symmetry, or G to be cyclic, or any other property which may provide extra theoretical arguments. Moreover, it is known that an invariant ring in the modular case may fail to be Cohen-Macaulay, which makes computations rather difficult.

Since we consider the modular case, there exists an element of order p. The sizes of Jordan blocks of such an element may exceed 2, and these cases will be considered later. Here we consider only the cases where Jordan blocks have sizes at most 2 for two important reasons.

First, the generators of the invariant ring are known under the action of such an element (not the generators of the invariant ring of the whole group). This knowledge enables us to give sharp bounds.

Second, we are able to pass from a result for cyclic groups to a result for an arbitrary group. This is quite important since only little is known in modular invariant theory, and the known results mainly consider either the cyclic group $\mathbb{Z}/p$ or permutation groups.

Despite of the fact that the methods presented in this note are computational, it is possible to extend these computations to get results for arbitrary sized Jordan blocks over arbitrary fields contained in the algebraic closure of the prime field.

The paper is organized as follows. In Section 2, we single out a universal invariant and explain our approach with an important illustration. Jordan decomposition and monomial order depending on that decomposition are given in Section 3. Notations and arguments that simplify the proof of the main result are also collected in this

section. Section 4 is devoted to the proof of the main result. Finally, extensions and sharpness of the main result are briefly discussed in Section 5.

Notation. Let $V = \mathbb{F}^n$ and consider the m-fold direct sum, $\oplus_{i=1}^m V$. The polynomial ring $\mathbb{F}[x_{1,1}, \dots, x_{m,n}]$ can be thought of as the algebra of polynomial functions on $\oplus_m V$, where $\{x_{i,1}, \dots, x_{i,n}\}$ is a basis for V^*, the dual space of the i-th copy of V in $\oplus_m V$, for each $1 \le i \le m$. Hence, we will denote $\mathbb{F}[x_{1,1}, \dots, x_{m,n}]$ simply by $\mathbb{F}[\oplus_m V]$.

Throughout this note $\mathbb{F} = \mathbb{F}_p$ is the prime field of characteristic p and G a finite group of order divisible by p. We suppose $\rho : G \to \mathrm{GL}(n, \mathbb{F})$ is a faithful representation and identify G with its image $\rho(G)$ in $\mathrm{GL}(n, \mathbb{F})$.

Since the action of G preserves the degrees, we will consider only homogeneous polynomials. So, any polynomial appearing in this note is homogeneous unless stated otherwise.

2. Cyclic subgroup

Let $\gamma \in G$ be an element of order p in G. Denote by $H = \langle \gamma \rangle$ the cyclic subgroup of G generated by γ. Then the inclusion $H \subset G \subset \mathrm{GL}(n, \mathbb{F})$ implies that

$$\mathbb{F}[\oplus_m V]^{\mathrm{GL}(n,\mathbb{F})} \subset \mathbb{F}[\oplus_m V]^G \subset \mathbb{F}[\oplus_m V]^H.$$

For $m \ge n$ define the following auxiliary polynomial:

$$f_0 = \sum_{(\alpha_1,\dots,\alpha_n)\in\mathbb{F}^n} (\alpha_1 x_{1,1} + \cdots + \alpha_n x_{1,n})^{p-1} \cdots (\alpha_1 x_{m,1} + \cdots + \alpha_n x_{m,n})^{p-1}, \tag{4}$$

where the sum is over all possible n-tuples $(\alpha_1, \dots, \alpha_n)$. The polynomial f_0 is invariant under the action of $\mathrm{GL}(n, \mathbb{F})$ by [R2, p. 30] and hence

$$f_0 \in \mathbb{F}[\oplus_m V]^{\mathrm{GL}(n,\mathbb{F})} \subset \mathbb{F}[\oplus_m V]^G \subset \mathbb{F}[\oplus_m V]^H. \tag{5}$$

Our aim is to first describe the generators of $\mathbb{F}[\oplus_m V]^H$ and then to write f_0 in terms of these generators. The main result depends on the maximum number of (indecomposable) invariant factors that appear in any summand of a decomposition.

Proposition 1. *Let*

$$f_0 = \sum \alpha_{a_1,\dots,a_\ell} h_1^{a_1} \cdots h_\ell^{a_\ell}\,, \quad \alpha \in \mathbb{F}, a_i \in \mathbb{N}_0, h_i \in \mathbb{F}[\oplus_m V]^H, \tag{6}$$

be a decomposition of f_0 where h_i are among the generators of the invariant ring $\mathbb{F}[\oplus_m V]^H$. Suppose that for any such decomposition, we have $a_1 + \cdots + a_\ell \le N$ whenever $\alpha_{a_1,\dots,a_\ell} \ne 0$. Then

$$\beta(H) \ge \frac{m(p-1)}{N} \tag{7}$$

and moreover,

$$\beta(G) \ge \frac{m(p-1)}{N}. \tag{8}$$

Proof. Since the invariant polynomials h_i are among the generators of $\mathbb{F}[\oplus_m V]^H$, we have $\deg h_i \le \beta(H)$. Therefore, $m(p-1) = \deg f_0 \le N \cdot \beta(H)$ which completes the first part of the proof.

For the second part, assume to the contrary that f_0 can be written as a polynomial in the elements of $\mathbb{F}[\oplus_m V]^G$ having degrees smaller than the above bound. Since $H \le G$ we obtain a contradiction to the first part. □

Remark. This proposition is also an illustration of the main theorem, and here we consider a more simpler situation where the analysis of the invariants appearing in the decomposition (6) is missing.

3. Jordan decomposition and ordering

Without loss of generality, we may assume that γ is in its Jordan canonical form. As stated in the Introduction, we will deal with the case where all Jordan blocks have sizes at most 2 in this paper. Let r be the number of 2×2 blocks, and let s be the number of all blocks, so $s - r$ is the number of trivial blocks. Then, we can write

$$\gamma = \begin{bmatrix} J_1 & & \\ & \ddots & \\ & & J_s \end{bmatrix},$$

where the J_i's are elementary Jordan matrices of order 2×2 or 1×1:

$$J_i = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{or} \quad J_i = [1]\,.$$

We can further assume, by reordering if necessary, that

$$n_1 = n_2 = \cdots = n_r = 2 \text{ and } n_{r+1} = \cdots = n_s = 1,$$

where J_i is an $n_i \times n_i$ matrix.

Definition. Let $\mathcal{I} = \{1, 2, \ldots, m\}$ and $\mathcal{J} = \{1, 2, \ldots, n\}$ be index sets. For a given nonzero monomial $u = \prod x_{i,j}^{e_{i,j}}$ and a nonempty index set $\mathcal{S} \subset \mathcal{I} \times \mathcal{J} = \{(1,1), \ldots, (m,n)\}$, define the $\mathcal{S}$-degree of u as

$$\sum_{(i,j) \in \mathcal{S}} e_{i,j}$$

and denote it by $\deg_{\mathcal{S}} u$. Note that $\deg_{\mathcal{S}} u \leq \deg u$. For simplicity, we also write $\deg_{\mathcal{S}} u$ to denote $\deg_{\mathcal{I} \times \mathcal{S}} u$ for $\mathcal{S} \subset \mathcal{J}$.

Define the following partition of $\mathcal{J}$ for further use:

$$\begin{aligned} \mathcal{J}_0 &= \{2r+1, 2r+2, \ldots, n\}, \\ \mathcal{J}_1 &= \{1, 3, \ldots, 2r-1\}, \\ \mathcal{J}_2 &= \{2, 4, \ldots, 2r\}, \end{aligned}$$

i.e., all $\mathcal{J}_i$ are disjoint and $\mathcal{J}_0 \sqcup \mathcal{J}_1 \sqcup \mathcal{J}_2 = \mathcal{J}$. Moreover, the first index set, $\mathcal{J}_0$, lists invariant variables which may be split off. Thus

$$\mathbb{F}[x_{i,j} \,|\, i \in \mathcal{I}, j \in \mathcal{J}]^H = \mathbb{F}[x_{i,j} \,|\, i \in \mathcal{I}, j \notin \mathcal{J}_0]^H \otimes \mathbb{F}[x_{i,j} \,|\, i \in \mathcal{I}, j \in \mathcal{J}_0],$$

and in particular we have

$$f_0 = f_1 u_1 + f_2 u_2 + \cdots + f_\ell u_\ell, \tag{9}$$

where $f_k \in \mathbb{F}[x_{i,j} \,|\, i \in \mathcal{I}, j \notin \mathcal{J}_0]^H$ and $u_k = \prod_{i \in \mathcal{I}, j \in \mathcal{J}_0} x_{i,j}^{e_{i,j}}$ for all $1 \leq k \leq \ell$.

Lemma 2. *For each u_k appearing in the above decomposition* (9)*, we have*

$$\deg u_k \geq (p-1)(s-r).$$

Proof. Let v be an arbitrary monomial appearing in f_0. Then, by expanding (4) we obtain the coefficient of v:

$$\sum_{\alpha_1\in\mathbb{F}}\sum_{\alpha_2\in\mathbb{F}}\cdots\sum_{\alpha_n\in\mathbb{F}}\alpha_1^{\deg_{\{1\}} v}\alpha_2^{\deg_{\{2\}} v}\cdots\alpha_n^{\deg_{\{n\}} v}.$$

Since it is not zero, $\deg_{\{j\}} v$ is a nonzero multiple of $(p-1)$ for all j. In particular, $\deg_{\{j\}} v \geq p-1$, and hence $\deg_{\mathcal{J}_0} v \geq (p-1)(s-r)$ (recall that $\mathcal{J}_0$ has $n-2r = s-r$ elements).

Suppose without loss of generality that all u_k appearing in (9) are distinct. For each u_k, there exists at least one monomial v_k appearing in the polynomial f_0 which is divisible by u_k. Otherwise, f_k is zero and u_k does not actually appear in that decomposition. Writing $v_k = w_k u_k$, where the monomial w_k appears in f_k, we note that $\deg_{\mathcal{J}_0} v_k = \deg_{\mathcal{J}_0} w_k + \deg_{\mathcal{J}_0} u_k$. Since $f_k \in \mathbb{F}[x_{i,j} \mid i \in \mathcal{I}, j \notin \mathcal{J}_0]^H$, we get $\deg_{\mathcal{J}_0} w_k = 0$, and hence

$$\deg u_k \geq \deg_{\mathcal{J}_0} u_k = \deg_{\mathcal{J}_0} v_k \geq (p-1)(s-r),$$

establishing the result. □

We will use the graded lexicographical order induced by

$$x_{1,1} \succ x_{1,2} \succ \cdots \succ x_{1,n} \succ x_{2,1} \succ x_{2,2} \succ \cdots \succ x_{m,n}.$$

The leading monomial of a polynomial f will be denoted by $\mathrm{LM}(f)$. The term ordering defined above is compatible with the action of γ in the sense that $\mathrm{LM}(f) \succeq \mathrm{LM}(\gamma(f))$. We direct the reader to [CLO] for a detailed discussion of monomial orders.

Lemma 3.

$$\mathrm{LM}(f_0) = x_{1,1}^{p-1}\cdots x_{m-n+1,1}^{p-1}\cdots x_{m-n+j,j}^{p-1}\cdots x_{m,n}^{p-1}.$$

Proof. First, we claim that the monomial

$$u = x_{1,1}^{p-1}\cdots x_{m-n+1,1}^{p-1}\cdots x_{m-n+j,j}^{p-1}\cdots x_{m,n}^{p-1}$$

appears in the expansion of f_0. Note that the coefficient of u in f_0 is

$$\sum_{(\alpha_1,\ldots,\alpha_n)\in\mathbb{F}^n}\underbrace{\alpha_1^{p-1}\cdots\alpha_1^{p-1}}_{m-n+1 \text{ times}}\alpha_2^{p-1}\cdots\alpha_n^{p-1},$$

which is equal to $(-1)^m \neq 0$. Hence the claim is true.

Next, we will show that any monomial v for which $v \succ u$ holds does not appear in the expansion of f_0. If $\deg_{\{i\}\times\mathcal{J}} v \neq p-1$ for some $1 \leq i \leq m$, then v clearly does not appear in f_0 by (4). So, we can assume that $\deg_{\{i\}\times\mathcal{J}} v = p-1$ for all i. Note that, as $v \succ u$ and $\deg_{\{(i,1)\}} u = p-1$ for all $1 \leq i \leq m-n+1$, we have the same for v, i.e., $x_{1,1}^{p-1}\cdots x_{m-n+1,1}^{p-1}$ divides v. Moreover, there exists $j \geq 1$ such that $x_{1,1}^{p-1}\cdots x_{m-n+1,1}^{p-1}\cdots x_{m-n+j,j}^{p-1} | v$ but $x_{m-n+j+1,j+1}^{p-1} \nmid v$ and $x_{m-n+j+1,k} | v$ for some $k < j+1$. But then, $\deg_{\{j+1,\ldots,n\}} v < (p-1)(n-j)$, which implies that there exists $j+1 \leq \ell \leq n$ for which $\deg_{\{\ell\}} v < (p-1)$ holds. Hence, by the same argument used in the first paragraph of the proof of Lemma 2, the coefficient of v in the expansion of f_0 cannot be nonzero, and the lemma follows. □

Remark. As we will use the following in the proof of the main result, we note them here for the convenience of the reader:

$$\begin{aligned}\deg_{\mathcal{J}_0} \mathrm{LM}(f_0) &= (s-r)(p-1),\\ \deg_{\mathcal{J}_1} \mathrm{LM}(f_0) &= (m-n+r)(p-1),\\ \deg_{\mathcal{J}_2} \mathrm{LM}(f_0) &= r(p-1).\end{aligned}$$

4. Main result

Theorem 4. *If $m > n$, and G contains an element of order p whose Jordan blocks have sizes at most 2 with r nontrivial blocks and $s-r$ trivial ones, then any set of generators for the invariant ring $\mathbb{F}[\oplus_m V]^G$ contains an element of degree at least*

$$(p-1)\frac{m-n+2r}{r} \geq 2(p-1)\frac{m}{n},$$

where $\mathbb{F}$ is the prime field with p elements and $V = \mathbb{F}^n$.

To prove the theorem we need the following result from [CH].

Theorem 5 (Conjecture of Richman)**.** *With the notations of the previous section, there are 4 classes of generators for the invariant ring $\mathbb{F}[\oplus_m V]^H$, namely,*

1. $x_{i,j'}, \quad i \in \mathcal{I}$ *and* $j' \in \mathcal{J}_0 \cup \mathcal{J}_2$,
2. $\mathrm{N}(x_{i,j}) = \prod_{\alpha\in\mathbb{F}} \gamma^\alpha(x_{i,j}) = x_{i,j}^p - x_{i,j}x_{i,j+1}^{p-1}, \quad i \in \mathcal{I}$ *and* $j \in \mathcal{J}_1$,
3. $u_{(i,j)(k,l)} = x_{i,j}x_{k,l+1} - x_{i,j+1}x_{k,l}, \quad (i,j) <_{lex} (k,l),\ i,k \in \mathcal{I},\ j,l \in \mathcal{J}_1$,
4. $\mathrm{Tr}(z) = \sum_{\alpha\in\mathbb{F}} \gamma^\alpha(z)$ *such that z divides* $\prod_{i\in\mathcal{I},\, j\in\mathcal{J}_1} x_{i,j}^{p-1}$,

where $(i,j) <_{lex} (k,l)$ means either $i < k$ or $i = k$ and $j < l$.

Proof. The action of γ is given explicitly by

$$\gamma(x_{i,j}) = \begin{cases} x_{i,j} + x_{i,j+1} & \text{if } j \in \mathcal{J}_1 = \{1,3,\dots,2r-1\},\\ x_{i,j} & \text{if } j \in \mathcal{J}_2 = \{2,4,\dots,2r\},\end{cases}$$

and as noted earlier, $\mathbb{F}[x_{i,j}]^H = \mathbb{F}[x_{i,j} \,|\, j \notin \mathcal{J}_0]^H \otimes \mathbb{F}[x_{i,j} \,|\, j \in \mathcal{J}_0]$. The result then follows from [CH]. □

We need the following technical lemma.

Lemma 6. *Let $z = \prod_{i\in\mathcal{I},j\in\mathcal{J}_1} x_{i,j}^{e_{i,j}}$ such that $e_{i,j} \leq p-1$ for all i,j. If $\mathrm{Tr}(z) \neq 0$, then $\deg_{\mathcal{J}_2} u \geq p-1$ for any monomial u appearing in $\mathrm{Tr}(z)$.*

Proof. When we expand the $\mathrm{Tr}(z)$, we get the following formula:

$$\mathrm{Tr}(z) = \sum_{\alpha\in\mathbb{F}} \gamma^\alpha(z) = \sum_{\alpha\in\mathbb{F}} \prod_{i\in\mathcal{I},j\in\mathcal{J}_1} \left(x_{i,j} + \binom{\alpha}{1} x_{i,j+1}\right)^{e_{i,j}}.$$

Since

$$\sum_{\alpha\in\mathbb{F}} \alpha^d = \begin{cases} 0, & \text{if } p-1 \nmid d,\\ -1, & \text{if } p-1 \mid d,\end{cases}$$

the $\mathcal{J}_2$-degree of a monomial is a nonzero multiple of $p-1$ and in particular, at least $p-1$. □

Remark. The theorem can be proved using a weaker lemma, where we only require that $\deg_{\mathcal{J}_2} \mathrm{LM}(\mathrm{Tr}(z)) \geq p-1$. In this case, however, we need to redefine the monomial order in a more complicated way which makes it difficult to follow each step in the proof of main theorem.

Proof of Theorem 4. Let

$$f_0 = \sum \alpha_{a_1,\ldots,a_k} h_1^{a_1} h_2^{a_2} \cdots h_k^{a_k}, \tag{10}$$

where the $h_i \in \mathbb{F}[\oplus_m V]^H$ belong to one of the four classes described in Theorem 5. Comparing the degrees of both sides with respect to $\{x_{i,1}, \ldots, x_{i,n}\}$, we conclude that none of the h_i's on the right-hand side belong to the class $\mathrm{N}(x_{i,j})$, as the degree of $\mathrm{N}(x_{i,j})$ is p in this set of variables, whereas f_0 has degree at most $p-1$.

Next, observe that there must exist h_i's belonging to the class $\mathrm{Tr}(z)$. Otherwise, $f_0 \in \mathbb{F}[x_{i,j'}, u_{(i,j)(k,l)}]$, and hence the $\mathcal{J}_1$-degree of $\mathrm{LM}(f_0)$ is at most the $\mathcal{J}_2$-degree of $\mathrm{LM}(f_0)$. This contradicts the fact that

$$\deg_{\mathcal{J}_1} \mathrm{LM}(f_0) = (m-n+r)(p-1) > \deg_{\mathcal{J}_2} \mathrm{LM}(f_0) = r(p-1)$$

as $m > n$.

There exists an exponent sequence $\mathbf{a} = (a_1, \ldots, a_k)$ with $\alpha_{\mathbf{a}} \neq 0$ such that the monomial $\mathrm{LM}(f_0)$ appears in the expansion of $h_1^{a_1} \cdots h_k^{a_k}$. Let $\tau_{\mathbf{a}}$ be the number of h_i's, counted with multiplicities, which belong to the class $u_{(i,j)(k,l)}$, i.e., those belonging to the third class as stated in Theorem 5, and let $\nu_{\mathbf{a}}$ be the number of those belonging to the first class. Hence, $a_1 + \cdots + a_k - \tau_{\mathbf{a}} - \nu_{\mathbf{a}}$ of them belong to the fourth class.

Note that for any monomial w appearing in the expansion of $h_1^{a_1} \cdots h_k^{a_k}$ we have $\deg_{\mathcal{J}_0 \cup \mathcal{J}_2} w \geq (a_1 + \cdots + a_k - \tau_{\mathbf{a}} - \nu_{\mathbf{a}})(p-1) + \tau_{\mathbf{a}} + \nu_{\mathbf{a}}$ by using Lemma 6. Since $\mathrm{LM}(f_0)$ also appears as a monomial in that expansion, we find

$$(a_1 + \cdots + a_k - \tau_{\mathbf{a}} - \nu_{\mathbf{a}})(p-1) + \tau_{\mathbf{a}} + \nu_{\mathbf{a}} \leq \deg_{\mathcal{J}_0 \cup \mathcal{J}_2} \mathrm{LM}(f_0) = s(p-1).$$

Hence, we can approximate the number of factors in the given summand,

$$a_1 + \cdots + a_k - \tau_{\mathbf{a}} - \nu_{\mathbf{a}} \leq \frac{s(p-1) - \tau_{\mathbf{a}} - \nu_{\mathbf{a}}}{p-1}.$$

Since among h_i's there are $\tau_{\mathbf{a}}$ invariants of degree 2 and $\nu_{\mathbf{a}}$ invariants of degree 1, the product of the remaining h_i's has degree $m(p-1) - 2\tau_{\mathbf{a}} - \nu_{\mathbf{a}}$. Thus, among those h_i's belonging to the class $\mathrm{Tr}(z)$, there exists a generator of degree at least

$$\frac{m(p-1) - 2\tau_{\mathbf{a}} - \nu_{\mathbf{a}}}{(s(p-1) - \tau_{\mathbf{a}} - \nu_{\mathbf{a}})/(p-1)} = (p-1)\frac{m(p-1) - 2\tau_{\mathbf{a}} - \nu_{\mathbf{a}}}{s(p-1) - \tau_{\mathbf{a}} - \nu_{\mathbf{a}}}. \tag{11}$$

Since $x_{i,j}$ does not appear in any other class except the first one, for $j \in \mathcal{J}_0$, we have $\nu_{\mathbf{a}} \geq \deg_{\mathcal{J}_0} u$ for any monomial u appearing in $h_1^{a_1} \cdots h_k^{a_k}$, and hence by Lemma 2,

$$\nu_{\mathbf{a}} \geq (p-1)(s-r). \tag{12}$$

In particular,

$$\frac{m(p-1) - \nu_{\mathbf{a}}}{s(p-1) - \nu_{\mathbf{a}}} > 2, \tag{13}$$

since $m > n = s + r$.

Now, we consider the fraction in (11) as a function of $\tau_{\mathbf{a}}$. By differentiating it (with respect to $\tau_{\mathbf{a}}$) and inequality (13), we see that it is an increasing function of $\tau_{\mathbf{a}}$, and hence takes its minimum when $\tau_{\mathbf{a}} = 0$. Thus, from (11) we get the inequality

$$(p-1)\frac{m(p-1)-2\tau_{\mathbf{a}}-\nu_{\mathbf{a}}}{s(p-1)-\tau_{\mathbf{a}}-\nu_{\mathbf{a}}} \geq (p-1)\frac{m(p-1)-\nu_{\mathbf{a}}}{s(p-1)-\nu_{\mathbf{a}}}. \tag{14}$$

Similarly, by considering the last fraction as a function of $\nu_{\mathbf{a}}$, we see that it is also an increasing function and thus takes its minimum value when $\nu_{\mathbf{a}}$ is minimum. The minimum of $\nu_{\mathbf{a}}$ is $(p-1)(s-r)$ by (12). Thus we obtain

$$(p-1)\frac{m(p-1)-\nu_{\mathbf{a}}}{s(p-1)-\nu_{\mathbf{a}}} \geq (p-1)\frac{(p-1)(m-(s-r))}{(p-1)(s-(s-r))} = (p-1)\frac{m-s+r}{r}. \tag{15}$$

Finally, using the relation $n = r + s$, we get the bound

$$\beta(H) \geq (p-1)\frac{m-n+2r}{r},$$

and by the argument used in the proof of Proposition 1, we can conclude that the same bound holds for G, i.e.,

$$\beta(G) \geq (p-1)\frac{m-n+2r}{r} \geq 2(p-1)\frac{m}{n},$$

where the last inequality is due to $r \leq n/2$. □

5. Concluding remarks and sharpness

The result and the proof of Theorem 4 can be read in two different directions. First, the maximum of degrees of generators depends on the Jordan block decomposition. Even if the representation $\rho(G)$ is irreducible, it is possible to get a reducible representation $\rho(H)$, and actually, this is always the case when $n > p$. Thus, considering the Jordan decomposition of an element of order p is a reasonable step.

Second, as also stated in the Introduction, we made use of the generators of 2-dimensional vector invariants. Hence, finding generators of higher-dimensional vector invariants would sharpen lower bounds in the general setting. Unfortunately, the generators are not known except for the 2-dimensional and the p-dimensional vector invariants, and a few other special cases.

The bound given in Theorem 4 is sharp in the sense that it is attained, as Theorem 5 shows, for

$$r = 1 \Rightarrow \beta(G) = (p-1)(m-n+2).$$

Moreover, it extends the bound of Richman, given here by (1), since the maximum of the numbers on the right-hand side of (1) is, in general, at most

$$\frac{p}{p-1}\frac{m}{n} \leq 2(p-1)\frac{m}{n}.$$

Finally, there is an analogue of the main result for any field (possibly infinite) contained in the algebraic closure of $\mathbb{F}_p$. More general results, including the cases where $n_1 \geq 3$, are also under consideration and are to be included in [M].

Acknowledgements

This note is a part of the author's Ph.D. thesis, under the supervision of Serguei A. Stepanov at Bilkent University. The author gratefully acknowledges the many helpful suggestions of Larry Smith during the preparation of this note. The author also thanks the anonymous referees who gave very careful readings to previous versions of this note.

References

[B] D. J. Benson, *Polynomial invariants of finite groups*, Cambridge Univ. Press, Cambridge, 1993. MR1249931 (94j:13003)

[CH] H. E. A. Campbell and I. P. Hughes, Vector invariants of $U_2(\mathbf{F}_p)$: a proof of a conjecture of Richman. *Adv. Math.* **126** (1997), no. 1, 1–20. MR1440251 (98c:13007)

[CLO] D. Cox, J. Little and D. O'Shea, *Ideals, varieties, and algorithms*, Springer, New York, 1992. MR1189133 (93j:13031)

[K] G. Kemper, Lower degree bounds for modular invariants and a question of I. Hughes. *Transform. Groups* **3** (1998), no. 2, 135–144. MR1628445 (99f:13004)

[M] U. Madran, Modular Vector Invariants. *Ph.D. Dissertation*, Bilkent Univ., Ankara, to appear. *will be available online through Bilkent University Library Thesis Database.*

[N1] E. Noether, Der Endlichkeitssatz der Invarianten endlicher Gruppen. *Math. Ann.* **77** (1916), 89-92. MR1511848

[N2] E. Noether, Der Endlichkeitssatz der Invarianten endlicher linear Gruppen der Charakteristik *p*. *Nachr. Akad. Wiss. Göttingen* (1926), 28-35.

[R1] D. R. Richman, On vector invariants over finite fields. *Adv. Math.* **81** (1990), no. 1, 30–65. MR1051222 (91g:15020)

[R2] D. R. Richman, Invariants of finite groups over fields of characteristic *p*. *Adv. Math.* **124** (1996), no. 1, 25–48. MR1423197 (97i:13005)

[S1] L. Smith, Polynomial invariants of finite groups, A survey of recent developments. *Bull. Amer. Math. Soc. (N.S.)* **34** (1997), no. 3, 211–250. MR1433171 (98i:13009)

[S2] L. Smith, *Polynomial invariants of finite groups*, A K Peters, Wellesley, MA, 1995. MR1328644 (96f:13008)

[Ste] S. A. Stepanov, Vector invariants of symmetric groups in the case of a field of prime characteristic. Translation in *Discrete Math. Appl.* **10** (2000), no. 5, 455–468. MR1826176 (2002e:13014)

[Stu] B. Sturmfels, *Algorithms in invariant theory*, Springer, Vienna, 1993. MR1255980 (94m:13004)

Department of Mathematics, Bilkent University, Bilkent, 06800 Ankara, Turkey
E-mail address: madran@fen.bilkent.edu.tr
E-mail address: madran@member.ams.org