Diophantine Approximation
H. P. Schlickewei et al., Editors

ORBIT SUMS AND MODULAR VECTOR INVARIANTS

Serguei A. Stepanov[1,2]
[1] *Department of Mathematics, Bilkent University, 06533 Bilkent, Ankara, Turkey*
[2] *Department of Algebra, V. A. Steklov Mathematical Institute, Russian Academy of Sciences, Ulitsa Gubkina 8, Moscow, GSP-1, 117966 Russia*
sa-stepanov@iitp.ru

To Wolfgang M. Schmidt on the occasion of his 70th birthday

1 Introduction

Let m, n be positive integers, R a commutative ring with the unit element 1, and

$$A_{mn} = R[x_{11}, \dots, x_{m1}; \dots; x_{1n}, \dots, x_{mn}]$$

the algebra of polynomials in mn variables x_{ij} over R. The symmetric group S_n operates on the algebra A_{mn} as a group of R-automorphisms by the rule: $\sigma(x_{ij}) = x_{i,\sigma(j)}$, $\sigma \in G$. Denote by $A_{mn}^{S_n}$ the subalgebra of invariants of the algebra A_{mn} with respect to S_n and define polarized elementary symmetric polynomials $u_{r_1,\dots,r_m} \in A_{mn}^{S_n}$ in n vector variables $(x_{11}, \dots, x_{m1}), \dots, (x_{1n}, \dots, x_{mn})$ by means of the following formal identity

$$\prod_{j=1}^{n}(1 + x_{1j}z_1 + \cdots + x_{mj}z_m) = 1 + \sum_{1 \le r_1 + \cdots + r_m \le n} u_{r_1,\dots,r_m} z_1^{r_1} \cdots z_m^{r_m}.$$

The elements of $A_{mn}^{S_n}$ are usually called *vector invariants* of S_n. If R is Noetherian, it follows from the Hilbert–Noether finiteness theorem [5,7,8] that $A_{mn}^{S_n}$ is a finitely generated commutative R-algebra and A_{mn} is finitely generated as a module over $A_{mn}^{S_n}$; moreover, if every nonzero integer is invertible in R, Weyl's theorem [13] states that the invariants $u_{r_1,\dots,r_m}$ form a complete system of generators of $A_{mn}^{S_n}$ over R. In other words, each element $u \in A_{mn}^{S_n}$ can be written as a polynomial in $u_{r_1,\dots,r_m}$, $1 \le r_1 + \cdots + r_m \le n$, with coefficients in R. The last result was recently generalized by D. Richman [10] and S. A. Stepanov [12] as follows: *if* $|S_n| = n!$ *is invertible in* R, *then* $A_{mn}^{S_n}$ *is generated as an* R*-algebra by the polarized elementary symmetric polynomials* $u_{r_1,\dots,r_m}$, $1 \le r_1 + \cdots + r_m \le n$, *of degree at most* n.

Let $A = R[x_1, \dots, x_N]$ be a finitely generated commutative R-algebra, G a finite group of R-algebra automorphisms of A, and A^G the subalgebra of invariants

Keywords. Polynomial invariants, generalized orbit Chern classes, finite groups, Noether degree bound.

2000 Mathematics subject classification. 11T55, 13A50, 14L24, 16R30, 20G40.

of G. If $z_1, \ldots, z_N$ are commuting variables, then we set

$$P(z_1, \ldots, z_N) = \prod_{\sigma \in G} (1 + \sigma(x_1)z_1 + \sigma(x_2)z_2 + \cdots + \sigma(x_N)z_N).$$

Let $\beta(A^G)$ denote the smallest positive integer β such that A^G can be generated as an R-algebra by polynomials of degree at most β. If each nonzero integer is invertible in R, the Noether result [7] implies that A^G is generated by the coefficients of $P(z_1, \ldots, z_N)$, so that $\beta(A^G) \leq |G|$. The last inequality is known as the *Noether bound*. The above mentioned result of Richman and Stepanov and the standard arguments based on the use of the Reynolds operator and the Noether map (see [11]) show that Noether's bound holds under the condition that $|G|!$ is invertible in R. A recent result of P. Fleischmann [4] demonstrates that Noether's bound remains true under the weaker condition that $|G|$ is invertible in R.

Now let $R = F$ be a field, and G a finite group acting linearly on a vector space V over F of finite dimension n. If the characteristic of F is positive and divides $|G|$, then we speak of the *modular case*. Otherwise, we have the *nonmodular case*, which includes the case of classical invariants over a field of characteristic zero. Almost everything that is usually used in the nonmodular case is missing in the modular case: the Cohen–Macaulay property fails in general, we have no Reynolds operator (averaging over G) and no Molien formula for the Poincaré series. Nevertheless, if F is a field of prime characteristic p, and H a p-subgroup of G, the modular case admits an extensive application of *generalized orbit Chern classes* related to H, especially, orbit traces (*orbit sums* of monomials) and top orbit classes (*orbit norms* of monomials). Let $F = F_p$ be a prime finite field, and $H \leq GL(n, F_p)$ a cyclic group of prime order p acting linearly on V. We set $A_{mn} = F_p[V^m]$ and denote by A_{mn}^H the algebra of vector invariants of A_{mn} with respect to H. It turns out (Theorems 5, 8 and 16) that there exist an F_p-linear space $\tilde{V}$ containing V as a subspace, a cyclic group $\tilde{H}$ of order p closely related to H and acting linearly on $\tilde{V}$, such that every invariant $u \in A_{mn}^H$ can be written as a special F_p-linear combination of orbit sums $S_{\tilde{H}}(f)$, orbit norms $N_{\tilde{H}}(g)$ related to the group $\tilde{H}$, and also their products $S_{\tilde{H}}(f)N_{\tilde{H}}(g)$, for various monomials $f, g \in F_p[\tilde{(V)}^m]$. This is a new point of view in modular invariant theory that reveals an important role of p-subgroups H of G and the associated orbit Chern classes of monomials. It should be pointed out that if H is a cyclic group of prime order p, and $F = F_p$ a prime field, then $S_{\tilde{H}}(f)$ and $N_{\tilde{H}}(g)$ can be calculated explicitly. This gives a possibility to determine a system of generating elements of A_{mn}^H in an explicit form. We also point out that the inclusion $A_{mn}^G \subseteq A_{mn}^H$ implies that the structure of the algebra A_{mn}^G inherits many features of the structure of A_{mn}^H.

The most significant distinction between nonmodular and modular cases is that in contrast to the nonmodular case, the Noether bound does no longer hold in the modular one. In particular, if $r \leq n$ and α are positive integers, F a field of prime characteristic p, and $G = S_n$ the symmetric group of degree n, then the following result holds (G. Kemper [6], Stepanov [12]): *if p^α divides r, then every system of R-algebra generators of $A_{mn}^{S_n}$ contains a generator whose degree is greater than or equal to* $\max\{n, m(p^\alpha - 1)\}$. The last result implies, in particular, that if $R =$ is the ring of integers, then every system of R-algebra generators of $A_{mn}^{S_n}$ contains a generator whose degree is greater than or equal to $\max\{n, m(n-1)/2\}$. This shows that feasibility

of Noether's bound depends essentially on the arithmetic structure of the ring R. It was recently shown by Fleischmann [3] that the lower bound $\max\{n, m(p^\alpha - 1)\}$ is sharp when $m > 1$ and $n = p^\alpha$. In fact, he proved that in this case $\beta(A_{mn}^{S_n}) \leq \max\{n, m(n-1)\}$. The last result can be considered as a refinement of the Campbell–Hughes–Pollack [1] upper bound $\beta(A_{mn}^{S_n}) \leq \max\{n, mn(n-1)/2\}$, which holds over an arbitrary commutative ring R.

Let m, n be positive integers, p a prime number, $F = F_p$ a finite field with $p > 2$ elements, and $V = F_p x_1 + \cdots + F_p x_n$ a vector space over F_p of dimension $n \geq 2$. Let $G \leq GL(n, F_p)$ be a group of order divisible by p, and $H = \langle \gamma \rangle$ a cyclic subgroup of G of order p. Assume that the generating matrix γ of H has the Jordan canonical form

$$\gamma = \begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_s \end{pmatrix}$$

with basic Jordan blocks $J_1, \ldots, J_s$. If $n_1, \ldots, n_s$ are sizes of these basic blocks, then

$$n_1 + n_2 + \cdots + n_s = n,$$

and we can assume without loss of generality that

$$p \geq n_1 \geq n_2 \geq \cdots \geq n_r \geq 2 \quad \text{and} \quad n_{r+1} = \cdots = n_s = 1.$$

Let A_{mn}^G be the algebra of invariants of the polynomial algebra

$$A_{mn} = F_p[V^m] = F_p[x_{11}, \ldots, x_{1n}; \ldots; x_{m1}, \ldots, x_{mn}]$$

with respect to G. In the case when $n_1 = \cdots = n_r = 2$ and $n_{r+1} = \cdots = n_s = 1$, we set

$$N_H^{(0)}(x_{i,2\tau-1}) = \prod_{\alpha \in F_p} \left(x_{i,2\tau-1} + \binom{\alpha}{1} x_{i,2\tau} \right) = x_{i,2\tau-1}^p - x_{i,2\tau-1} x_{i,2\tau}^{p-1},$$

where $1 \leq i \leq m$, $1 \leq \tau \leq r$, and

$$S_H^{(0)}(f) = \sum_{\alpha \in F_p} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \left(x_{i,2\tau-1} + \binom{\alpha}{1} x_{i,2\tau} \right)^{s_{i,\tau p-1}},$$

where

$$f = \prod_{i=1}^{m} \prod_{\tau=1}^{r} x_{i,2\tau-1}^{s_{i,2\tau-1}}$$

is a monomial in $x_{i,2\tau-1}$, for $1 \leq i \leq m$, $1 \leq \tau \leq r$. Finally, if (i_1, j_2), (i_2, j_2) are two different pairs of positive integers, we write

$$(i_1, j_1) \prec (i_2, j_2) \Leftrightarrow i_1 < i_2 \quad \text{or} \quad i_1 = i_2 \text{ and } j_1 < j_2.$$

The purpose of this paper is to extend the arguments of [12] and to prove the following result.

Theorem 1. *Let $H \leq GL(n, F_p)$ be a cyclic group of prime order p generated by γ. If $n \geq 2$ and the sizes $n_1, \ldots, n_s$ of the basis Jordan blocks $J_1, \ldots, J_s$ of the matrix γ satisfy the conditions*

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

then

$$A_{mn}^H = F_p[x_{i,2\tau}, x_{ij}, N_H^{(0)}(x_{i,2\tau-1}), (x_{i_1,2\tau_1-1}x_{i_2,2\tau_2} - x_{i_1,2\tau_1}x_{i_2,2\tau_2-1}), S_H^{(0)}(f')],$$

where $1 \leq i \leq m$, $1 \leq \tau \leq r$, $2r+1 \leq j \leq s$, $1 \leq i_1, i_2 \leq m$, $1 \leq \tau_1, \tau_2 \leq r$ with $(i_1, \tau_1) \prec (i_2, \tau_2)$, and f' runs through the set of monomials f of the above form such that $0 \leq s_{i,2\tau-1} \leq p-1$.

As an easy consequence of Theorem 1 we obtain the following.

Corollary 2. *If additionally $mr > 2$, then every system of generators of A_{mn}^H contains an element of degree at least $mr(p-1)$.*

In the case when G is an arbitrary finite group containing H as a subgroup, we are able to find a lower degree bound for generating elements of the algebra A_{mn}^G.

Theorem 3. *Let $G \leq GL(n, F_p)$ be a finite group whose order is divisible by the characteristic p of F_p, and $H = \langle\gamma\rangle$ a cyclic subgroup of G of prime order p. If $m \geq n \geq 2$, $mr > 2$ and the sizes $n_1, \ldots, n_s$ of the basic Jordan blocks $J_1, \ldots, J_s$ of the matrix γ satisfy the condition*

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

then every system of F_p-algebra generators of $A_{mn}^G = F_p[V^m]^G$ contains a generator whose degree is greater than or equal to $(m - n + 2r)(p-1)/r$.

Theorem 1 provides an explicit construction of generating elements of the algebra A_{mn}^H in terms of orbit sums and orbit norms of monomials. It can be conjectured that the lower degree bound in Corollary 2 is sharp. Theorem 3 improves the lower degree bound

$$\max\left\{2, \frac{m}{n-1}, \frac{m}{|G|-1}, \frac{mp}{n(p-1)}\right\}$$

obtained earlier by Richman [10]. The case when $r = 1$ was studied by Richman [9] (if $p = 2$), and by Campbell and Hughes [2] (if $p > 2$). Our arguments are considerably different from the ones of these authors. In particular, all our constructions are based only on the analysis of orbit Chern classes, without any references to deep results of representation theory or combinatorial analysis. The case when

$$p \geq n_1 \geq \cdots \geq n_\sigma \geq 3,$$

with $1 \leq \sigma \leq s$, requires more complicated calculations and will be considered later. It should be noted that all results of the paper can be easily extended to the case of an arbitrary field F of prime characteristic p.

We now explain briefly the main ideas underlying the proofs of Theorem 1 and 3. The use of orbit sums

$$S_G(f) = \sum_{w \in \{\sigma(f) | \sigma \in G\}} w,$$

where $f \in A_{mn}$ is a monomial, is most efficient in the case when the group G acts on elements of an R-algebra by permutation of the vector variables $x_j = (x_{1j}, x_{2j}, \ldots, x_{mj})$, $1 \leq j \leq n$. In that case each invariant $u \in A_{mn}^G$ is an R-linear combination of the above orbit sums for various monomials f. This important result is a consequence of the following fact: if a monomial f appears in an invariant u with a nonzero coefficient a, then for each $\sigma \in G$ the corresponding monomial $\sigma(f)$ also appears in u with the same coefficient a. Unfortunately, the above property of orbit sums does not longer hold for finite groups of a more general form, in particular, for cyclic groups H generated by matrices of the following form:

$$\gamma = \begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_s \end{pmatrix}$$

with basic Jordan blocks $J_1, J_2, \ldots, J_s$ of sizes $n_1, n_2, \ldots, n_s$ such that $1 < n_\rho < p$ for some $\rho = 1, 2, \ldots, s$. On the other hand, if $n_1 = n_2 = \cdots = n_r = p$ and $n_{r+1} = \cdots = n_s = 1$, then after an appropriate nonsingular linear transformation we can proceed to a new system of vector variables $\tilde{x}_j = (\tilde{x}_{1j}, \tilde{x}_{2j}, \ldots, \tilde{x}_{mj})$, $1 \leq j \leq n$ on which H acts be cyclic permutations.

Let H be the cyclic group of prime order $p > 2$ generated by a nonsingular square matrix γ with Jordan blocks $J_1, J_2, \ldots, J_s$ of sizes $n_1, n_2, \ldots, n_s$, respectively. Assume that $n_1 = n_2 = \cdots = n_r = 2$, $n_{r+1} = \cdots = n_s = 1$, and recall that H acts linearly on the vector space V^m of dimension $m(r+s)$. The proof of Theorem 1 falls into two steps.

(i) At the first step we "blow up" each Jordan block J_ρ, $1 \leq \rho \leq r$, of size $n_\rho = 2$ of the matrix γ to a Jordan block of the largest possible size p. As a result, the generating matrix γ of the group H is transformed into the corresponding square matrix $\tilde{\gamma}$ of size $\nu = (p-1)r + s$, and the group H into the corresponding cyclic group $\tilde{H}$ generated by $\tilde{\gamma}$ and acting on the vector space $\tilde{V}^m$ of dimension $m\nu$. It follows by the above that then one can find new vector variables $\tilde{x}_j = (\tilde{x}_{1j}, \tilde{x}_{2j}, \ldots, \tilde{x}_{mj})$, $1 \leq j \leq \nu$, obtained from the original variables $x_j = (x_{1j}, x_{2j}, \ldots, x_{mj})$ by a non-degenerate linear transformation such that $\tilde{H}$ acts by cyclic permutations of the new vector variables. This property of $\tilde{H}$ allows us to show (Theorem 5) that each invariant v of the algebra $A_{m\nu}^{\tilde{H}}$ is an F_p-linear combination of the orbit sums $S_{\tilde{H}}(f)$, the orbit norms $N_{\tilde{H}}(g)$ and their products $S_{\tilde{H}}(f)N_{\tilde{H}}(g)$ for various monomials $f, g \in A_{m\nu}$.

(ii) At the second step we demonstrate that the appropriate embedding of the algebra A_{mn} into $A_{m\nu}$ results in a fairly simple test (Theorem 8) distinguishing among the $\tilde{H}$-invariants $v \in A_{m\nu}^{\tilde{H}}$ ones invariants with respect to the action of H. The use of this test makes possible an explicit construction of invariants $u \in A_{mn}^H$ as F_p-linear combinations of orbit sums $S_{\tilde{H}}(f)$, orbit norms $N_{\tilde{H}}(g)$ and their products $S_{\tilde{H}}(f)N_{\tilde{H}}(g)$ of a special form.

The idea of the proof of Theorem 3 is as follows. Since $A_{mn}^G \subset A_{mn}^H$, the system of generators of the algebra A_{mn}^H indicated in Theorem 1 contains a corresponding system of generators of the algebra A_{mn}^G. To prove that the latter contains at least one polynomial of a sufficiently high degree we demonstrate that a certain polynomial $f_0 \in A_{mn}$ of a fairly special form, which is invariant under the action of an arbitrary

subgroup of the general linear group $GL(F_p, n)$ (see Section 5), cannot be presented as a polynomial over F_p in elements of moderate degrees of the above mentioned system of generators of the algebra A_{mn}^G, not even as a polynomial over F_p in similar elements of the broader system of generators of the algebra A_{mn}^H.

2 Orbit sums

Let m, n be positive integers, $p \geq 3$ be a prime number, F_p a prime finite field with p elements, $GL(n, F_p)$ the group of invertible $n \times n$ matrices with entries in F_p, and

$$A_{mn} = F_p[x_{11}, \ldots, x_{m1}; \ldots; x_{1n}, \ldots, x_{mn}]$$

the algebra of polynomials in commuting variables $x_{11}, \ldots, x_{m1}; \ldots; x_{1n}, \ldots, x_{mn}$. In the sequel we identify F_p with the set $\{0, 1, \ldots, p-1\}$. If $g \in A_{mn}$ and

$$\sigma = \begin{pmatrix} \sigma_{11} & \sigma_{12} & \cdots & \sigma_{1n} \\ \sigma_{21} & \sigma_{22} & \cdots & \sigma_{2n} \\ \vdots & \vdots & \vdots & \\ \sigma_{n1} & \sigma_{n2} & \cdots & \sigma_{nn} \end{pmatrix}$$

an element of $GL(n, F_p)$, let $\sigma(g)$ denote the image of g under the F_p-algebra endomorphism σ which operates on the basis elements $x_{i1}, \ldots, x_{in}$ of the vector spaces $V_i = F_p x_{i1} + F_p x_{i2} + \cdots + F_p x_{in}$, $1 \leq i \leq m$, as follows:

$$\begin{pmatrix} \sigma(x_{i1}) \\ \sigma(x_{i2}) \\ \vdots \\ \sigma(x_{in}) \end{pmatrix} = \sigma \begin{pmatrix} x_{i1} \\ x_{12} \\ \vdots \\ x_{in} \end{pmatrix} = \begin{pmatrix} \sigma_{11}x_{i1} + \cdots + \sigma_{1n}x_{in} \\ \sigma_{21}x_{i1} + \cdots + \sigma_{2n}x_{in} \\ \vdots \\ \sigma_{n1}x_{i1} + \cdots + \sigma_{nn}x_{in} \end{pmatrix}.$$

Let G be a subgroup of $GL(n, F_p)$, and A_{mn}^G the set of polynomials $u \in A_{mn}$ such that $\sigma(u) = u$ for every $\sigma \in G$. The set A_{mn}^G forms a subalgebra of A_{mn} which is called the *algebra of vector invariants* of G.

Let p be a prime divisor of $|G|$, and $H = \langle \gamma \rangle$ a cyclic subgroup of the group G of order p. In an appropriate basis, the matrix γ has the following Jordan canonical form

$$\gamma = \begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_s \end{pmatrix},$$

where the basic Jordan blocks

$$J_\rho = \begin{pmatrix} 1 & 1 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}, \quad 1 \leq \rho \leq s,$$

are square matrices of sizes $n_1, n_2, \ldots, n_s$, respectively, with $n_1 + n_2 + \cdots + n_s = n$ and $1 \leq n_\rho \leq p$ for all $\rho = 1, 2, \ldots, s$. We can assume without loss of generality that

$$n_1 \geq n_2 \geq \cdots \geq n_r \geq 2 \quad \text{and} \quad n_{r+1} = \ldots = n_s = 1.$$

Let A_{mn}^H be the algebra of polynomials $u \in A_{mn}$ which are invariant under the action of the cyclic group $H = \langle \gamma \rangle$. Our aim is to describe explicitly all the elements of A_{mn}^H. Set $n' = n_1 + \cdots + n_r$ and consider the polynomial algebra

$$A_{mn'} = F_p[x_{ij} \mid 1 \leq i \leq m, 1 \leq j \leq n'].$$

Let $A_{mn'}^H$ be the algebra of invariants of $A_{mn'}$ with respect to H. Since all variables x_{ij}, for $1 \leq i \leq m$, $n'+1 \leq j \leq n$, are invariant under the action of H, then every invariant $u \in A_{mn}^H$ is a polynomial of the form

$$u = u_1 f_1 + u_2 f_2 + \cdots + u_l f_l,$$

where $u_k \in A_{mn'}^H$, and f_k, for $1 \leq k \leq l$, are monomials in $F_p[x_{ij} \mid 1 \leq i \leq m, n'+1 \leq j \leq n]$. This shows that the problem concerning the structure of invariants $u \in A_{mn}^H$ is reduced to the corresponding problem concerning the structure of invariants $u_k \in A_{m,n'}^H$. As a result, we can assume without loss of generality that $n = n'$, $u \in A_{mn}$ and

$$\gamma = \begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_r \end{pmatrix},$$

where $J_1, J_2, \cdots, J_r$ are the basic Jordan blocks of sizes $n_1, n_2, \ldots, n_r$, respectively, with

$$n = n_1 + n_2 + \cdots + n_r \quad \text{and} \quad n_1 \geq n_2 \geq \cdots \geq n_r \geq 2. \tag{1}$$

Set $\nu = rp$ and blow up each of Jordan blocks $J_l, \ldots, J_r$ of the matrix γ to the same Jordan block

$$\tilde{J} = \begin{pmatrix} 1 & 1 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

of size p. As a result, the matrix γ is blown up to the square $(\nu \times \nu)$-matrix

$$\tilde{\gamma} = \begin{pmatrix} \tilde{J} & & & \\ & \tilde{J} & & \\ & & \ddots & \\ & & & \tilde{J} \end{pmatrix}$$

of size ν which operates on each vector space

$$\tilde{V}_i = F_p z_{i1} + F_p z_{i2} + \cdots + F_p z_{i\nu}, \quad \text{for} \quad i = 1, 2 \ldots, m,$$

in the same way as a nonsingular linear transformation of $\tilde{V}_i$. Denote by $\tilde{H}$ the cyclic group of order p generated by $\tilde{\gamma}$ and note that the action of $\tilde{H}$ on the spaces $\tilde{V}_i$, for

$i = 1, 2, \ldots, m$, can be considered as an extension of the action of the group H on the corresponding subspaces V_i of $\tilde{V}_i$, for $i = 1, 2, \ldots, m$. If

$$A_{mv} = F_p[z_{11}, \ldots, z_{m1}; \ldots; z_{1v}, \ldots, z_{mv}]$$

is the algebra of all polynomials over F_p in mv commuting variables $z_{11}, \ldots, z_{1n}; \ldots; z_{1v}, \ldots, z_{mv}$, then every element $\tilde{\sigma}$ of the group $\tilde{H}$ gives an F_p-algebra endomorphism of A_{mv}. Let $A_{mv}^{\tilde{H}}$ denote the subalgebra of invariants of the algebra A_{mv} under the action of $\tilde{H}$. If f is a monomial in A_{mv}, denote by

$$Orb_{\tilde{H}}(f) = \{\tilde{\sigma}(f) \mid \tilde{\sigma} \in \tilde{H}\}$$

the orbit of f with respect to the group $\tilde{H}$. Set $q = |Orb_{\tilde{H}}(F)|$ and note that $q = 1$ or $q = p$. If $Orb_{\tilde{H}}(f)$ is the orbit of a monomial $f \in A_{mv}$ then

$$N_{\tilde{H}}(f) = \prod_{f' \in Orb_{\tilde{H}}(f)} f' \quad \text{and} \quad S_{\tilde{H}}(f) = \sum_{f' \in Orb_{\tilde{H}}(f)} f'$$

are called an *orbit norm* and an *orbit sum* of f with respect to $\tilde{H}$. It is clear that $N_{\tilde{H}}(f)$ and $S_{\tilde{H}}(f)$ are invariant under the action of $\tilde{H}$. Moreover, $N_{\tilde{H}}(f)$ and $S_{\tilde{H}}(f)$ are homogeneous polynomials in A_{mv}. Now we describe explicitly the elements of A_{mv} that are invariant under the action of the cyclic group $\tilde{H}$. At first we prove the following arithmetical result.

Lemma 4. *Let $p \geq 3$ be a prime number, and $l_1, l_2, \ldots, l_p$ integers such that*

$$0 \leq l_\rho \leq p - 1, \quad \textit{for all} \quad \rho = 1, 2, \ldots, p,$$

and

$$l = \sum_{\rho=1}^{p} l_\rho.$$

Then

$$\sum_{\alpha \in F_p} \prod_{\rho=1}^{p} \binom{\alpha}{l_\rho} = \begin{cases} 0 & \text{if } l \leq p - 2, \\ (p-1)/l_1! \cdots l_p! & \text{if } l = p - 1. \end{cases}$$

Proof. As usual, we assume that

$$\binom{\alpha}{l_\rho} = \begin{cases} 1 & \text{if } l_\rho = 0, \\ 0 & \text{if } \alpha < l_\rho. \end{cases}$$

Consider

$$\prod_{\rho=1}^{p} \binom{\alpha}{l_\rho}$$

as a polynomial in $F_p[\alpha]$ of degree l, say,

$$\prod_{\rho=1}^{p} \binom{\alpha}{l_\rho} = c_0 \alpha^l + c_1 \alpha^{l-1} + \cdots + c_l.$$

Now the result is immediate from the relations

$$\sum_{\alpha \in F_p} \alpha^k = \begin{cases} p-1 & \text{if } (p-1) \mid k, \\ 0 & \text{otherwise.} \end{cases}$$

This completes the proof. □

Let

$$f = \prod_{i=1}^{m} \prod_{\tau=1}^{r} \prod_{j=(\tau-1)p+1}^{\tau p-1} z_{ij}^{s_{ij\tau}}$$

be a monomial in the algebra

$$A_{mv} = F_p[z_{ij} \mid 1 \le i \le m, 1 \le j \le v].$$

Assume that f is not invariant under action of the group $\tilde{H}$ and consider the corresponding orbit sum

$$S_{\tilde{H}}(f) = \sum_{\alpha \in F_p} \tilde{\gamma}^{\alpha}(f).$$

Since

$$\tilde{\gamma}^{\alpha}(z_{ij}) = \sum_{l=j}^{\tau p} \binom{\alpha}{l-j} z_{il},$$

for $1 \le i \le m$, $(\tau-1)p+1 \le j \le \tau p$, $1 \le \tau \le r$, we see that

$$S_{\tilde{H}}(f) = \sum_{\alpha \in F_p} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \prod_{j=(\tau-1)p+1}^{\tau p} \left(\sum_{l=0}^{\tau p-j} \binom{\alpha}{l} z_{i,j+l} \right)^{s_{ij\tau}}. \tag{2}$$

Let $\{\tilde{z}_{ij} \mid 1 \le i \le m, 1 \le j \le v\}$ be new variables defined by the following relations

$$\tilde{z}_{i,(\tau-1)p+\alpha+1} = \sum_{l=0}^{\alpha} \binom{\alpha}{l} z_{i,(\tau-1)p+l+1}, \tag{3}$$

for $1 \le i \le m$, $0 \le \alpha \le p-1$ and $1 \le \tau \le r$. This is a nondegenerated linear transformation, so any z_{ij} is an F_p-linear combinations of $\tilde{z}_{ij}$. It follows that every orbit sum $S_{\tilde{H}}(f)$ is an F_p-linear combination of the orbit sums

$$S_{\tilde{H}}(\tilde{f}) = \sum_{\tilde{g} \in Orb(\tilde{f})} \tilde{g},$$

where $\tilde{f}$ is a monomial of the form

$$\tilde{f} = \prod_{i=1}^{m} \prod_{\tau=1}^{r} \prod_{j=(\tau-1)p+1}^{\tau p} \tilde{z}_{ij}^{\tilde{s}_{ij\tau}}.$$

Consider also the orbit norm $N_{\tilde{H}}(\tilde{f}) = \prod_{\tilde{g} \in Orb(\tilde{f})} \tilde{g}$ of the monomial $\tilde{f}$ and observe that $N_{\tilde{H}}(\tilde{f})$ is an element of the algebra $A_{mv}^{\tilde{H}}$. We now note that the elements $\{\tilde{z}_{ij} \mid 1 \le$

$j \le v\}$ defined by (3) form a basis of the space $\tilde{V}_i = F_p z_{i1} + \cdots + F_p z_{iv}$, $1 \le i \le m$, and that for each $\tau = 1, 2, \ldots r$, the group $\tilde{H}$ operates on the basis elements $\tilde{z}_{ij}$, for $(\tau - 1)p + 1 \le j \le \tau p$, by their cyclic permutations. Let $\tilde{f}$ be a monomial in $F_p[\tilde{z}_{ij} \mid 1 \le i \le m, 1 \le j \le v]$ which appears in an invariant $v \in A_{mv}^{\tilde{H}}$ with a nonzero coefficient. Since $\tilde{\gamma}^{\alpha}(v) = v$ for any $\tilde{\gamma}^{\alpha} \in \tilde{H}$, the coefficient of $\tilde{f}$ in v equals the coefficient of $\tilde{\gamma}^{\alpha}(\tilde{f})$ in v. This shows that if $\tilde{f} = \tilde{f}'\tilde{f}''$ and $\tilde{f}'' = N_{\tilde{H}}(\tilde{g})$ for some monomial $\tilde{g} \in F_p[\tilde{z}_{ij} \mid 1 \le i \le m, 1 \le j \le v]$, then v involves the invariant $S_{\tilde{H}}(\tilde{f}')N_{\tilde{H}}(\tilde{g})$. In other words, each invariant $v \in A_{mv}^{\tilde{H}}$ is an F_p-linear combination of the orbit sums $S_{\tilde{H}}(\tilde{f})$, the orbit norms $N_{\tilde{H}}(\tilde{g})$ and also their products $S_{\tilde{H}}(\tilde{f})N_{\tilde{H}}(\tilde{g})$, for various monomials $\tilde{f}, \tilde{g} \in F_p[\tilde{z}_{ij} \mid 1 \le i \le m, 1 \le j \le v]$. On the other hand, every orbit sum $S_{\tilde{H}}(\tilde{f})$ is an F_p-linear combination of orbit sums $S_{\tilde{H}}(f)$ of monomials $f \in A_{mv}$, which shows that any invariant $v \in A_{mv}^{\tilde{H}}$ is an F_p-linear combination of the orbit sums $S_{\tilde{H}}(f)$, the orbit norms $N_{\tilde{H}}(g)$ and also their products $S_{\tilde{H}}(f)N_{\tilde{H}}(g)$, for various monomials $f, g \in A_{mv}$. This gives the following result.

Theorem 5. *Every invariant of the algebra $A_{mv}^{\tilde{H}}$ is an F_p-linear combination of the orbit sums $S_{\tilde{H}}(f)$, the orbit norms $N_{\tilde{H}}(g)$ and also their products $S_{\tilde{H}}(f)N_{\tilde{H}}(g)$, for various monomials $f, g \in A_{mv}$ of the form*

$$f = \prod_{i=1}^{m}\prod_{\tau=1}^{r}\prod_{j=(\tau-1)p+1}^{\tau p} z_{ij}^{s_{ij\tau}}, \quad g = \prod_{i=1}^{m}\prod_{\tau=1}^{r}\prod_{j=(\tau-1)p+1}^{\tau p} z_{ij}^{t_{ij\tau}}.$$

If $0 \le \lambda < p - 1$ is an integer, then among all possible orbit sums $S_{\tilde{H}}(f) \in A_{mv}$ we select those ones that involve no variable $z_{i,j}$, for $1 \le i \le m$, $(\tau - 1)p + 1 \le j < \tau p - 1 - \lambda$, $1 \le \tau \le r$. Our next aim is to find an exact form of such orbit sums $S_{\tilde{H}}(f)$, for various monomials $f \in A_{mv}$.

Set

$$s_{ij\tau} = \sum_{e=0}^{\eta} s_{ij\tau}^{(e)} p^e, \quad 0 \le s_{ij}^{(e)} \le p - 1,$$

for $0 \le e \le \eta$, $1 \le i \le m$, $(\tau - 1)p + 1 \le j \le \tau p$, $1 \le \tau \le r$, and write f in the following form:

$$f = \prod_{e=0}^{\eta}\prod_{i=1}^{m}\prod_{\tau=1}^{r}\prod_{j=(\tau-1)p+1}^{\tau p} (z_{ij}^{p^e})^{s_{ij\tau}^{(e)}}. \tag{4}$$

Now we define the *weight* of the monomial f and the associated orbit sum $S_{\tilde{H}}(f)$ as follows:

$$w(f) = w(S_{\tilde{H}}(f)) = \sum_{e=0}^{\eta}\sum_{i=1}^{m}\sum_{\tau=1}^{r}\sum_{j=(\tau-1)p+1}^{\tau p} (\tau p - j)s_{ij\tau}^{(e)}.$$

If a monomial f is invariant under the action of $\tilde{H}$, it has the form

$$f = \prod_{e=0}^{\eta}\prod_{i=1}^{m}\prod_{\tau=1}^{r} z_{i,\tau p}^{s_{i,\tau p}^{(e)}}.$$

If f is not invariant under the action of $\tilde{H}$, it follows from (2), (4) and Lemma 4 that the condition $w(f) < p-1$ implies $S_{\tilde{H}}(f) = 0$. On the other hand, if $w(f) > p+\lambda$ and $s_{ij\tau} \geq 1$ at least for one triple (i, j, τ) with $1 \leq i \leq m$, $(\tau-1)p+1 \leq j < \tau p-1-\lambda$, $1 \leq \tau \leq r$, then the invariant $S_{\tilde{H}}(f)$ involves at least one variable z_{ij}, with $1 \leq i \leq m$, $(\tau-1)p+1 \leq j < \tau p-1-\lambda$, $1 \leq \tau \leq r$. This proves the following result.

Proposition 6. *Let $0 \leq \lambda < p-1$, $\mu \geq 1$ be integers, and*

$$f = \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \prod_{j=(\tau-1)p+1}^{\tau p} (z_{ij}^{p^e})^{s_{ij\tau}^{(e)}}$$

a monomial in A_{mv} that is not invariant under the action of $\tilde{H}$. Every orbit norm $N_{\tilde{H}}(f) \in A_{mv}^{\tilde{H}}$ that involves no variable z_{ij}, for $1 \leq i \leq m$, $(\tau-1)p+1 \leq j < \tau p-1-\lambda$, $1 \leq \tau \leq r$, has the following form:

$$N_{\tilde{H}}^{(\lambda)}(f) = \prod_{\alpha \in F_p} \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \prod_{j=\tau p-1-\lambda}^{\tau p} \left(\sum_{l=0}^{\tau p-j-1} \binom{\alpha}{l} z_{i,j+l}^{p^e} \right)^{s_{ij\tau}^{(e)}},$$

and each orbit sum $S_{\tilde{H}}(f) \in A_{mv}^{\tilde{H}}$ that involves no variable z_{ij}, for $1 \leq i \leq m$, $(\tau-1)p+1 \leq j < \tau p-1-\lambda$, $1 \leq \tau \leq r$, has either the form

$$S_{\tilde{H}}^{(\lambda)}(f) = \sum_{\alpha \in F_p} \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \prod_{j=\tau p-1-\lambda}^{\tau p} \left(\sum_{l=0}^{\tau p-j-1} \binom{\alpha}{l} z_{i,j+l}^{p^e} \right)^{s_{ij\tau}^{(e)}}$$

or the form

$$S_{\tilde{H}}^{(\mu,\lambda)}(f) = \sum_{\alpha \in F_p} \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \prod_{j=(\tau-1)p+1}^{\tau p} \left(\sum_{l=0}^{\tau p-j} \binom{\alpha}{l} z_{i,j+l}^{p^e} \right)^{s_{ij\tau}^{(e)}},$$

where $w(f) = p-1+\mu \geq p+\lambda$ and $s_{ij\tau}^{(e)} \geq 1$ at least for one quadruple (e, i, j, τ) such that $0 \leq e \leq \eta$, $1 \leq i \leq m$, $(\tau-1)p+1 \leq j < \tau p-1-\lambda$, $1 \leq \tau \leq r$.

We assume in what follows that

$$n_1 = \cdots = n_r = 2. \tag{5}$$

Under this assumption, the following result is an easy consequence of Proposition 6 with $\lambda = 0$.

Corollary 7. *Let μ be a positive integer, and*

$$f = \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \prod_{j=(\tau-1)p+1}^{\tau p} (z_{ij}^{p^e})^{s_{ij\tau}^{(e)}}$$

a monomial in A_{mn} that is not invariant under the action of $\tilde{H}$. Every orbit norm $N_{\tilde{H}}(f)$ that involves no variable z_{ij}, for $1 \leq i \leq m$, $(\tau-1)p+1 \leq j < \tau p-1$, $1 \leq \tau \leq r$, has the following form:

$$N_{\tilde{H}}^{(0)}(f) = \prod_{\alpha\in F_p}\prod_{e=0}^{\eta}\prod_{i=1}^{m}\prod_{\tau=1}^{r}\left(z_{i,\tau p-1}^{p^e} + \binom{\alpha}{1} z_{i,\tau p}^{p^e}\right)^{s_{i,\tau p-1}^{(e)}} \left(z_{i,\tau p}^{p^e}\right)^{s_{i,\tau p}^{(e)}},$$

and every orbit sum $S_{\tilde{H}}(f)$ that involves no variables z_{ij}, for $1 \le i \le m$, $(\tau-1)p+1 \le j < \tau p - 1$, $1 \le \tau \le r$, has either the form

$$S_{\tilde{H}}^{(0)}(f) = \sum_{\alpha\in F_p}\prod_{e=0}^{\eta}\prod_{i=1}^{m}\prod_{\tau=1}^{r}\left(z_{i,\tau p-1}^{p^e} + \binom{\alpha}{1} z_{i,\tau p}^{p^e}\right)^{s_{i,\tau p-1}^{(e)}} \left(z_{i,\tau p}^{p^e}\right)^{s_{i,\tau p}^{(e)}}$$

or the form

$$S_{\tilde{H}}^{(1)}(f) = \sum_{\alpha\in F_p}\prod_{e=0}^{\eta}\prod_{i=1}^{m}\prod_{\tau=1}^{r}\prod_{j=(\tau-1)p+1}^{\tau p}\left(\sum_{l=0}^{\tau p-j}\binom{\alpha}{l} z_{i,j+l}^{p^e}\right)^{s_{ij\tau}^{(e)}},$$

where $w(f) = p$ and $s_{ij\tau} \ge 1$ at least for one tuple (e, i, j, τ) such that $0 \le e \le \eta$, $1 \le i \le m$, $(\tau-1)p+1 \le j < \tau p - 1$, $1 \le \tau \le r$.

On the other hand, if $S_{\tilde{H}}(f)$ involves at least one variable $z_{i,j}$, for $1 \le i \le m$, $(\tau-1)p+1 \le j < \tau p - 1$, $1 \le \tau \le r$, then $S_{\tilde{H}}(f)$ has the form

$$S_{\tilde{H}}^{(\mu)}(f) = \sum_{\alpha\in F_p}\prod_{e=0}^{\eta}\prod_{i=1}^{m}\prod_{\tau=1}^{r}\prod_{j=(\tau-1)p+1}^{\tau p}\left(\sum_{l=0}^{\tau p-j}\binom{\alpha}{l} z_{i,j+l}^{p^e}\right)^{s_{ij\tau}^{(e)}},$$

where $w(f) = p - 1 + \mu \ge p + 1$ and $s_{ij\tau} \ge 1$ at least for one tuple (e, i, j, τ) such that $0 \le e \le \eta$, $1 \le i \le m$, $(\tau-1)p+1 \le j < \tau p - 1$, $1 \le \tau \le r$.

For each $i = 1, 2, \ldots m$, consider now the embedding

$$\vartheta : V_i \hookrightarrow \tilde{V}_i \tag{6}$$

of the space V_i into the space $\tilde{V}_i$ given by the relations

$$\vartheta(x_{ij}) = \begin{cases} z_{i,\tau p-1} & \text{if } j = 2\tau - 1, \quad 1 \le \tau \le r, \\ z_{i,\tau p} & \text{if } j = 2\tau, \qquad 1 \le \tau \le r \end{cases}$$

and define as follows the action of the cyclic group H on $\tilde{V}_i$. If γ is a generating element of H, its action on elements $(x_{i1}, \ldots, x_{in})$ of V_i is given by

$$\gamma(x_{ij}) = \begin{cases} x_{ij} + x_{i,j+1} & \text{if } j = 2\tau - 1, \quad 1 \le \tau \le r, \\ x_{ij} & \text{if } j \ne 2\tau - 1, \quad 1 \le \tau \le r. \end{cases}$$

In that case, the map $\vartheta : V_i \hookrightarrow \tilde{V}_i$ induces the corresponding action of γ on the space $\tilde{V}_i$ defined by

$$\gamma(z_{ij}) = \begin{cases} z_{ij} + z_{i,j+1} & \text{if } j = \tau p - 1, \quad 1 \le \tau \le r, \\ z_{ij} & \text{if } j \ne \tau p - 1, \quad 1 \le \tau \le r, \end{cases} \tag{7}$$

This yields a unique extension of the action of H on the space $V_i \subseteq \tilde{V}_i$ to its action on the space $\tilde{V}_i$ and defines the corresponding unique extension of the action of H on elements of A_{mn} to its action on elements of the algebra A_{mv}.

On the other hand, if $\tilde{\gamma}$ is a generating element of the group $\tilde{H}$, its action on elements $(z_{i1}, \ldots, z_{iv})$ of the space $\tilde{V}_i$ is given by

$$\tilde{\gamma}(z_{ij}) = \begin{cases} z_{ij} + z_{i,j+1} & \text{if } (\tau-1)p+1 \le j \le \tau p - 1, \quad 1 \le \tau \le r, \\ z_{ij} & \text{if } j = \tau p, \quad 1 \le \tau \le r. \end{cases}$$

Now we consider the invariants $u \in A_{mv}^{\tilde{H}}$ that are also invariant under the action of H.

Theorem 8. *Let $v \in A_{mv}^{\tilde{H}}$ be a polynomial of positive degree. Then v is invariant under action of H if and only if the polynomial v involves no variable z_{ij}, for $1 \le i \le m$, $(\tau-1)p+1 \le j \le \tau p - 2$, $1 \le \tau \le r$.*

Proof. Every invariant $v \in A_{mv}^{\tilde{H}}$ of degree $s \ge 1$ is a sum of its homogeneous components $v_k \in A_{mv}^{\tilde{H}}$ of degree k, for $0 \le k \le s$. This reduces the problem to the case of homogeneous polynomials, so we can assume without loss of generality that v is a homogeneous $\tilde{H}$-invariant.

Suppose that $v \in A_{mv}^{\tilde{H}}$ involves at least one variable z_{ij}, for $1 \le i \le m$, $(\tau-1)p+1 \le j \le \tau p - 2$, $1 \le \tau \le r$, and write

$$v = \sum_{(s_{ij})} v_{(s_{ij})} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \prod_{(\tau-1)p+1 \le j \le \tau p-2} z_{ij}^{s_{ij}},$$

where $v_{(s_{ij})}$ are homogeneous polynomials in

$$F_p[z_{i,\tau p-1}, z_{i,\tau p} \mid 1 \le i \le m, 1 \le \tau \le r],$$

and the sum is over all tuples

$$(s_{ij}) = (s_{ij} \mid 1 \le i \le m, (\tau-1)p+1 \le j \le \tau p - 2, 1 \le \tau \le r)$$

of nonnegative integers s_{ij} such that

$$\sum_{i=1}^{m} \sum_{\tau=1}^{r} \sum_{(\tau-1)p+1 \le j \le \tau p-2} s_{ij} \le s.$$

Let $j_0 \le rp - 2$, $j_0 \ne \tau p - 1, \tau p$, for $1 \le \tau \le r$, be the largest positive integer such that the polynomial v involves no monomial

$$\prod_{i=1}^{m} \prod_{j=1}^{rp} z_{ij}^{s_{ij}}$$

with $s_{ij} \ge 1$, for all $1 \le i \le m$ and $j > j_0$. In that case,

$$v = v_{(0)} + \sum_{(s_{ij}) \ne (0)} v_{(s_{ij})} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \prod_{\substack{1 \le i \le j_0 \\ (\tau-1)p+1 \le j \le \tau p-2 \\ 1 \le \tau \le r}} z_{ij}^{s_{ij}},$$

and the polynomial v contains at least one nonzero term of the form

$$v_{(s_{ij})} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \prod_{\substack{1 \le i \le j_0 \\ (\tau-1)p+1 \le j \le \tau p-2 \\ 1 \le \tau \le r}} z_{ij}^{s_{ij}},$$

involving z_{ij_0} for some $i = 1, 2, \ldots, m$.

Now we assume that v is invariant under the action of H. Since the variables z_{ij}, for $1 \le i \le m$, $(\tau-1)p+1 \le j \le \tau p-2$, $1 \le \tau \le r$, are fixed under action of $\gamma \in H$, we have

$$\gamma(v) = \gamma(v_{(0)}) + \sum_{(s_{ij}) \ne (0)} \gamma(v_{(s_{ij})}) \prod_{i=1}^{m} \prod_{\tau=1}^{r} \prod_{\substack{1 \le i \le j_0 \\ (\tau-1)p+1 \le j \le \tau p-2 \\ 1 \le \tau \le r}} z_{ij}^{s_{ij}}.$$

This shows, in particular, that the coefficients $v_{(s_{ij})}$ of the polynomial v are invariant under the action of H, so

$$\gamma(v) = v_{(0)} + \sum_{(s_{ij}) \ne (0)} v_{(s_{ij})} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \prod_{\substack{1 \le i \le j_0 \\ (\tau-1)p+1 \le j \le \tau p-2 \\ 1 \le \tau \le r}} z_{ij}^{s_{ij}}.$$

On the other hand, since $\tilde{\gamma}(z_{ij}) = \gamma(z_{ij})$ for all $1 \le i \le m$, $j = \tau p-1, \tau p$, $1 \le \tau \le r$, and $\tilde{\gamma}(z_{ij}) = z_{ij} + z_{i,j+1}$, for $1 \le i \le m$, $(\tau-1)p+1 \le j \le \tau p-2$, $1 \le \tau \le r$, then

$$\tilde{\gamma}(v) = v_{(0)} + \sum_{(s_{ij}) \ne (0)} v_{(s_{ij})} \prod_{i=1}^{m} \prod_{\substack{1 \le i \le j_0 \\ (\tau-1)p+1 \le j \le \tau p-2 \\ 1 \le \tau \le r}} (z_{ij} + z_{i,j+1})^{s_{ij}},$$

so the polynomial $\tilde{\gamma}(v)$ contains at least one nonzero term

$$v_{(s_{ij})} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \prod_{\substack{1 \le i \le j_0 \\ (\tau-1)p+1 \le j \le \tau p-2 \\ 1 \le \tau \le r}} z_{i,j+1}^{s_{ij}},$$

which involves z_{i,j_0} and which does not appear in $\gamma(v) = v$. This shows that v cannot be invariant under the action of H. Conversely, if the polynomial $v \in A_{mv}^{\tilde{H}}$ involves no variable z_{ij}, for $1 \le i \le m$, $(\tau-1)p+1 \le j \le \tau p-1$, it is invariant under the action of H, and this completes the proof. □

Let $v \in A_{mv}^{\tilde{H}}$ be a polynomial that is invariant under the action of H. Theorem 5 shows that v is an F_p-linear combinations of $S_{\tilde{H}}^{(0)}(f)$, $S_{\tilde{H}}^{(\mu)}(f)$, $N_{\tilde{H}}^{(0)}(g)$ and also $S_{\tilde{H}}^{(0)}(f)N_{\tilde{H}}^{(0)}(g)$, $S_{\tilde{H}}^{(\mu)}(f)N_{\tilde{H}}^{(0)}(g)$, for various $\mu \ge 1$ and $f, g \in A_{mv}$. Since the polynomials $S_{\tilde{H}}^{(0)}(f)$, $S_{\tilde{H}}^{(1)}(f)$ and $N_{\tilde{H}}^{(0)}(g)$ involve no variable z_{ij}, for $1 \le i \le m$, $(\tau-1)p+1 \le j \le \tau p-2$, $1 \le \tau \le r$, it follows from Theorem 8 that the polynomials $S_{\tilde{H}}^{(0)}(f)$, $S_{\tilde{H}}^{(1)}(f)$ and $N_{\tilde{H}}^{(0)}(g)$ are H-invariants. Now we prove the following result.

Proposition 9. *Let*

$$f = \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \prod_{j=(\tau-1)p+1}^{\tau p} (z_{ij}^{p^e})^{s_{ij\tau}^{(e)}}$$

be a monomial in A_{mv}. *Then* $S_{\tilde{H}}^{(1)}(f)$ *is an* F_p*-linear combination of* H*-invariants of the form*

$$(z_{i_1,\tau_1 p-1}^{p^{e_1}} z_{i_2,\tau_2 p}^{p^{e_2}} - z_{i_1,\tau_1 p}^{p^{e_1}} z_{i_2,\tau_2 p-1}^{p^{e_2}}) \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} (z_{i,\tau p}^{p^e})^{\omega_{i,\tau p}^{(e)}},$$

where $0 \le e_1, e_2 \le \eta$, $1 \le i_1, i_2 \le m$, $1 \le \tau_1, \tau_2 \le r$, $(i_1, \tau_1) \prec (i_2, \tau_2)$, *and* H*-invariants of the form*

$$\prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} (z_{i,\tau p}^{p^e})^{v_{i,\tau p}^{(e)}}.$$

Proof. Let

$$f = \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \prod_{j=(\tau-1)p+1}^{\tau p} (z_{ij}^{p^e})^{s_{ij\tau}^{(e)}}$$

and

$$S_{\tilde{H}}^{(1)}(f) = \sum_{\alpha \in F_p} \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \prod_{j=(\tau-1)p+1}^{\tau p} \left(\sum_{l=0}^{\tau p - j} \binom{\alpha}{l} z_{i,j+l}^{p^e} \right)^{s_{ij\tau}^{(e)}},$$

where $s_{ij\tau}^{(e)} \ge 1$ at least for one quadruple (e, i, j, τ) with $0 \le e \le \eta$, $1 \le i \le m$, $(\tau - 1)p + 1 \le j \le \tau p - 2$, $1 \le \tau \le r$, and $w(f) = p$. Set

$$v_{i,\tau p}^{(e)} = \sum_{j=(\tau-1)p+1}^{\tau p} s_{ij\tau}^{(e)}.$$

Since $S_{\tilde{H}}^{(1)}(f)$ involves no variable z_{ij}, for $1 \le i \le m$, $(\tau - 1)p + 1 \le j \le \tau p - 2$, $1 \le \tau \le r$, then

$$S_{\tilde{H}}^{(1)}(f) = \sum_{\alpha \in F_p} \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \prod_{j=(\tau-1)p+1}^{\tau p} \left(\binom{\alpha}{\tau p - j - 1} z_{i,\tau p-1}^{p^e} + \binom{\alpha}{\tau p - j} z_{i,\tau p}^{p^e} \right)^{s_{ij\tau}^{(e)}}.$$

This shows that

$$S_{\tilde{H}}^{(1)}(f) = \sum_{(e_1,e_2,i_1,i_2,\tau_1,\tau_2)} (a_{i_1 i_2 \tau_1 \tau_2}^{(e_1,e_2)} z_{i_1,\tau_1 p-1}^{p^{e_1}} z_{i_2,\tau_2 - p}^{p^{e_2}} + b_{i_1 i_2 \tau_1 \tau_2}^{(e_1,e_2)} z_{i_1,\tau_1}^{p^{e_1}} z_{i_2,\tau_2 p-1}^{p^{e_2}}) \times \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} (z_{i,\tau p}^{p^e})^{\omega_{i,\tau p}^{(e)}} + a \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} (z_{i,\tau p}^{p^e})^{v_{i,\tau p}^{(e)}},$$

where

$$\omega_{i,\tau p}^{(e)} = \begin{cases} v_{i,\tau p}^{(e)} - 1 & \text{if } (e, i, \tau) = (e_1, i_1, \tau_1), (e_2, i_2, \tau_2); \\ v_{i,\tau p}^{(e)} & \text{if } (e, i, \tau) \ne (e_1, i_1, \tau_1), (e_2, i_2, \tau_2). \end{cases}$$

Since $S_{\tilde{H}}^{(1)}$ is invariant under the action of H, and

$$\gamma(z_{ij}) = \begin{cases} z_{ij} + z_{i,j+1} & \text{if } j = \tau p - 1, \quad 1 \le \tau \le r; \\ z_{ij} & \text{if } j = \tau p, \quad 1 \le \tau \le r, \end{cases}$$

then $a_{i_1 i_2 \tau_1 \tau_2}^{(e_1,e_2)} + b_{i_1 i_2 \tau_1 \tau_2}^{(e_1,e_2)} = 0$ for all $(e_1, e_2, i_1, i_2, \tau_1, \tau_2)$, and therefore

$$S_{\tilde{H}}^{(1)}(f) = \sum_{(e_1,e_2,i_1,i_2,\tau_1,\tau_2)} a_{i_1 i_2 \tau_1 \tau_2}^{(e_1,e_2)} (z_{i_1,\tau_1 p-1}^{p^{e_1}} z_{i_2,\tau_2 p}^{p^{e_2}} - z_{i_1,\tau_1 p}^{p^{e_1}} z_{i_2,\tau_2 p-1}^{p^{e_2}})$$
$$\times \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} (z_{i,\tau p}^{p^e})^{\omega_{i,\tau p}^{(e)}} + a \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} (z_{i,\tau p}^{p^e})^{\upsilon_{i,\tau p}^{(e)}}.$$

This completes the proof. □

Consider the invariants $v \in A_{mv}^{\tilde{H}}$ which are F_p-linear combinations of orbit sums $S_{\tilde{H}}^{(\mu)}(f)$, for monomials f and $\mu \ge 2$. Our next aim is to describe those $v \in A_{mv}^{\tilde{H}}$ that are also invariant under the action of H.

Proposition 10. *Let $v \in A_{mv}^{\tilde{H}}$ be a polynomial that is an F_p-linear combination*

$$v = \sum_{k=1}^{K} a_k S_{\tilde{H}}^{(\mu_k)}(f_k), \qquad a_k \neq 0,$$

of orbit sums $S_{\tilde{H}}^{(\mu_k)}(f_k)$, for various

$$f_k = \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \prod_{j=(\tau-1)p+1}^{\tau p} (z_{ij}^{p^e})^{s_{ij\tau}^{(e,k)}}$$

and $\mu_1 \ge \mu_2 \cdots \ge \nu_K \ge 2$. If v is invariant under the action of H, then $\mu_{k'} = \mu_k$ at least for one pair (k', k) with $k' > k$, and

$$\sum_{j=(\tau-1)p+1}^{\tau p} s_{ij\tau}^{(e,k')} = \sum_{j=(\tau-1)p+1}^{\tau p} s_{ij\tau}^{(e,k)}.$$

Proof. Since $\mu_k \ge 2$, it follows from Corollary 7 that the orbit sum $S_{\tilde{H}}^{(\mu_k)}$ involves at least one variable z_{ij}, for $1 \le i \le m$, $(\tau - 1)p + 1 \le j \le \tau p - 2$, $1 \le \tau \le r$, say, $z_{\iota\kappa}$. On the other hand, since v is invariant under the action of H, Theorem 8 implies that v involves no such variable. This shows that $z_{\iota\kappa}$ should be eliminated by means of other orbit sums occurring in v with nonzero coefficients. In that case the linear combination

$$v = \sum_{k=1}^{K} a_k S_{\tilde{H}}^{(\mu_k)}(f_k)$$

must contain, alongside $S_{\tilde{H}}^{(\mu_k)}$, at least one orbit sum $S_{\tilde{H}}^{(\mu_{k'})}(f_{k'})$, for some

$$f_{k'} = \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \prod_{j=(\tau-1)p+1}^{\tau p} (z_{ij}^{p^e})^{s_{ij\tau}^{(e,k')}}$$

with $k' > k$ and $\mu_{k'} = \mu_k$.

Consider the orbit sums

$$S_{\tilde{H}}^{(\mu_k)}(f_k) = \sum_{\alpha\in F_p} \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \prod_{j=(\tau-1)p+1}^{\tau p} \left(\sum_{l=0}^{\tau p-j} \binom{\alpha}{l} z_{i,j+l}^{p^e} \right)^{s_{ij\tau}^{(e,k)}},$$

$$S_{\tilde{H}}^{(\mu_k)}(f_{k'}) = \sum_{\alpha\in F_p} \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \prod_{j=(\tau-1)p+1}^{\tau p} \left(\sum_{l=0}^{\tau p-j} \binom{\alpha}{l} z_{i,j+l}^{p^e} \right)^{s_{ij\tau}^{(e,k')}}$$

and suppose that, on the contrary,

$$\sum_{j=(\tau-1)p+1}^{\tau p} s_{ij\tau}^{(e,k')} \neq \sum_{j+(\tau-1)p+1}^{\tau p} s_{ij\tau}^{(e,k)},$$

for some triple (e, i, τ). The polynomials $S_{\tilde{H}}^{(\mu_k)}(f_k)$ and $S_{\tilde{H}}^{(\mu_k)}$ are F_p-linear combinations of monomials

$$\left(\sum_{\alpha\in F_p} \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \prod_{j=(\tau-1)p+1}^{\tau p} \prod_{l=0}^{\tau p-j} \binom{\alpha}{l}^{\sigma_{i,j+l,\tau}^{(e,k)}} \right) \times \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \prod_{j=(\tau-1)p+1}^{\tau p} \prod_{l=0}^{\tau p-j} (z_{i,j+l}^{p^e})^{\sigma_{i,j+l,\tau}^{(e,k)}}$$

and

$$\left(\sum_{\alpha\in F_p} \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \prod_{j=(\tau-1)p+1}^{\tau p} \prod_{l=0}^{\tau p-j} \binom{\alpha}{l}^{\sigma_{i,j+l,\tau}^{(e,k')}} \right) \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \times \prod_{j=(\tau-1)p+1}^{\tau p} \prod_{l=0}^{\tau p-j} (z_{i,j+l}^{p^e})^{s_{\sigma_{i,j+l,\tau}^{(e,k')}}},$$

respectively, where

$$\sum_{l=0}^{\tau p-j} \sigma_{i,j+l,\tau}^{(e,k)} = s_{ij\tau}^{(e,k)} \quad \text{and} \quad \sum_{l=0}^{\tau p-j} \sigma_{i,j+l,\tau}^{(e,k')} = s_{ij\tau}^{(e,k')}.$$

Under the above supposition, each monomial of $S_{\tilde{H}}^{(\mu_k)}(f_k)$ involving $z_{\iota\kappa}$ differs from every monomial of $S_{\tilde{H}}^{(\mu_{k'})}(f_{k'})$, so that no monomial of $S_{\tilde{H}}^{(\mu_k)}$ involving $z_{\iota\kappa}$ can be eliminated. This yields a contradiction proving Proposition 10.

Set $z_{ij}^{(e)} = z_{ij}^{p^e}$ and consider the product

$$f = \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \prod_{j=(\tau-1)p+1}^{\tau p} (z_{ij}^{p^e})^{s_{ij\tau}^{(e)}}$$

as a monomial with respect to $z_{ij}^{(e)}$. Similarly, we consider the associated orbit sum $S_{\tilde{H}}^{(\mu)}(f)$ as a polynomial with respect to $z_{ij}^{(e)}$. We also observe that the weight of every monomial that appears in $S_{\tilde{H}}^{(\mu)}(f)$ with a nonzero coefficient does not exceed μ. A monomial f and the associated orbit sum $S_{\tilde{H}}^{(\mu)}(f)$ are said to be *flat* if $s_{ij\tau}^{(e)} = 0$ or $s_{ij\tau}^{(e)} = 1$, for $0 \le e \le \eta$, $1 \le i \le m$, $(\tau-1)p+1 \le j \le \tau p$, $1 \le \tau \le r$. We note that there is no essential difference between arbitrary orbit sums and flat orbit sums, since each orbit sum $S_{\tilde{H}}^{(\mu)}(f)$ can be obtained from a flat orbit sum by the identification of the corresponding powers $z_{i,(\tau-1)p+l}^{p^e}$, for various (e, i, τ). This shows that the study of orbit sums $S_{\tilde{H}}^{(\mu)}(f)$, for various monomials $f \in A_{mv}$, is reduced to the study of similar orbit sums with flat monomials f. The following result is an immediate consequence of Proposition 10. □

Corollary 11. *Let $v \in A_{mv}^{\tilde{H}}$ be a polynomial of positive degree that is an F_p-linear combination*

$$v = \sum_{k=1}^{K} a_k S_{\tilde{H}}^{(\mu_k)}(f_k), \qquad a_k \neq 0,$$

of flat orbit sums $S_{\tilde{H}}^{(\mu_k)}$, for various

$$f_k = \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \prod_{j=(\tau-1)p+1}^{\tau p} (z_{ij}^{p^e})^{s_{ij\tau}^{(e,k)}},$$

and let $\mu_1 \ge \mu_2 \ge \cdots \ge \mu_K \ge 2$. If v is invariant under the action of H and if two orbit sums $S_{\tilde{H}}^{(\mu_k)}$ and $S_{\tilde{H}}^{(\mu_{k'})}$ such that $\mu_{k'} = \mu_k$ for $k' > k$ appear in v with nonzero coefficients, then the monomial $f_{k'}$ is obtained from f_k by means of substitutions

$$z_{ij}p^e \mapsto z_{i,j+l}^{p^e} \quad \text{and} \quad z_{i'j'}^{p^e} \mapsto z_{i',j'-l}^{p^e},$$

with $(\tau-1)p+1 \le j+l,\ j'-l \le \tau p$, $0 \le e \le \eta$, $1 \le i, i' \le m$, $1 \le \tau \le r$, that preserve weights and degrees of the monomials f_k and $f_{k'}$.

It follows from the stated above that a more general F_p-linear combination

$$v = \sum_{k=1}^{K} a_k S_{\tilde{H}}^{(\mu_k)}(f_k) + \sum_{l=1}^{L} c_l S_{\tilde{H}}^{(\mu_l)}(f_l) N_{\tilde{H}}(g_l), \quad a_k \neq 0, c_l \neq 0, \deg(g_l) \ge 1,$$

is invariant under the action of H only in the case when it has the following special form

$$v = v_0 + \sum_{\lambda=1}^{\Lambda} v_\lambda N_{\tilde{H}}^{(0)}(g_\lambda),$$

where each F_p-linear combination

$$v_\lambda = \sum_{k=1}^{K_\lambda} a_{k\lambda} S_{\tilde{H}}^{(\mu_{k\lambda})}(f_{k\lambda}), \quad \text{for} \quad 0 \le \lambda \le \Lambda,$$

of orbit sums $S_{\tilde{H}}^{(\mu_{k\lambda})}(f_{k\lambda})$ involves no variable z_{ij} with $1 \le i \le m$, $(\tau-1)p+1 \le j \le \tau p-2$, $1 \le \tau \le r$.

Now we are able to give a complete description of the H-invariants $v \in A_{mv}^{\tilde{H}}$ that are F_p-linear combinations of flat orbit sums $S_{\tilde{H}}^{(\mu)}(f)$, for various $\mu \ge 2$ and f. The following result plays a crucial role in constructing a system of generators of the algebra A_{mn}^{H}.

Proposition 12. *Let $v \in A_{mv}^{\tilde{H}}$ be a polynomial of positive degree that is an F_p-linear combination*

$$v = \sum_{k=1}^{K} a_k S_{\tilde{H}}^{(\mu_k)}(f_k), \qquad a_k \neq 0,$$

of flat orbit sums $S_{\tilde{H}}^{(\mu_k)}(f_k)$, for various $\mu_k \ge 2$ and

$$f_k = \prod_{e=0}^{\eta}\prod_{i=1}^{m}\prod_{\tau=1}^{r}\prod_{j=(\tau-1)p+1}^{\tau p}(z_{ij}^{p^e})^{s_{ij\tau}^{(e,k)}}.$$

If v is invariant under the action of H, then v is an F_p-linear combination of polynomials

$$\prod_{\kappa=1}^{\sigma}(z_{i_{2\kappa-1},\tau_{2\kappa-1}p-1}^{p^{e_{2\kappa-1}}}z_{i_{2\kappa},\tau_{2\kappa}p}^{p^{e_{2\kappa}}} - z_{i_{2\kappa-1},\tau_{2\kappa-1}p}^{p^{e_{2\kappa-1}}}z_{i_{2\kappa},\tau_{2\kappa}p-1}^{p^{e_{2\kappa}}})\prod_{e=0}^{\eta}\prod_{i=1}^{m}\prod_{\tau=1}^{r}(z_{i,\tau p}^{p^e})^{\omega_{i,\tau p}^{(e)}},$$

where $0 \le \sigma \le [s/2]$, $(i_{2\kappa-1}, \tau_{2\kappa-1}) \prec (i_{2\kappa}, \tau_{2\kappa})$, and $0 \le \omega_{i,\tau p}^{(e)} \le 1$.

Proof. Since v is invariant under the action of H, it follows from Theorem 8 that v involves only monomials of the form

$$z_{i_1,\tau_1 p-\varepsilon_1}^{p^{e_1}} \cdots z_{i_s,\tau_s p-\varepsilon_s}^{p^{e_s}},$$

with $1 \le s \le \deg v$, $1 \le e_1, \ldots, e_s \le \eta$, $1 \le i_1 \le \cdots \le i_s \le m$, $1 \le \tau_1, \ldots, \tau_s \le r$, and $\varepsilon_1, \ldots, \varepsilon_s \in \{0, 1\}$. Moreover, since v is an F_p-linear combination of flat orbit sums, then $(e_k, i_k, \tau_k) \neq (e_l, i_l, \tau_l)$, for all k and l such that $k \neq l$.

Let

$$g = z_{i_1,\tau_1 p-\varepsilon_1}^{p^{e_1}} \cdots z_{i_s,\tau_s p-\varepsilon_s}^{p^{e_s}}$$

be a monomial of maximal possible weight $\sigma \le s$ that appears in v with a nonzero coefficient $a \in F_p$. We can assume without loss of generality that

$$g = z_{i_1,\tau_1 p-1}^{p^{e_1}} \cdots z_{i_{\sigma-1},\tau_{\sigma-1}p-1}^{p^{e_{\sigma-1}}} z_{i_\sigma,\tau_\sigma p-1}^{p^{e_\sigma}} z_{i_{\sigma+1},\tau_{\sigma+1}p}^{p^{e_{\sigma+1}}} z_{i_{\sigma+2},\tau_{\sigma+2}p}^{p^{e_{\sigma+2}}} \cdots z_{i_s,\tau_s p}^{p^{e_s}}.$$

Since $\gamma(v) = v$, then along with ag the invariant v contains also the polynomial

$$\gamma(ag) = ag + \sum_{\kappa=1}^{\sigma}\frac{a}{\kappa!}\left(z_{i_1,\tau_1 p}^{p^{e_1}}\frac{\partial}{\partial z_{i_1,\tau_1 p-1}^{(e_1)}} + \cdots + z_{i_s,\tau_s p}^{p^{e_s}}\frac{\partial}{\partial z_{i_\sigma,\tau_\sigma p-1}^{(e_\sigma)}}\right)^{\kappa} g,$$

involving several associated extra terms

$$ag_\kappa = \frac{a}{\kappa!}\left(z_{i_1,\tau_1 p}^{p^{e_1}}\frac{\partial}{\partial z_{i_1,\tau_1 p-1}^{(e_1)}} + \ldots + z_{i_s,\tau_s p}^{p^{e_s}}\frac{\partial}{\partial z_{i_s,\tau_s p-1}^{(e_s)}}\right)^{\kappa} g,$$

each of which is a linear combination of monomials $g_{\iota\kappa}$ of the same weight $\sigma - \kappa$. On the other hand, since v is invariant under the action of H it cannot contain the above extra terms, so the invariant v should involve at least one extra monomial g' of the same weight σ that gives a possibility to cancel some of the monomials $g_{\iota\kappa}$. This process of cancellation of extra monomials $g_{\iota\kappa}$ can be described inductively as follows.

Adding and subtracting, if it is necessary, several terms of the form ag' for different monomials g' of the same weight σ we can assume without loss of generality that

$$g' = z_{i_1,\tau_1 p-1}^{p^{e_1}} \cdots z_{i_{\sigma-1},\tau_{\sigma-1} p-1}^{p^{e_{\sigma-1}}} z_{i_\sigma,\tau_\sigma p}^{p^{e_\sigma}} z_{i_{\sigma+1},\tau_{\sigma+1} p-1}^{p^{e_{\sigma+1}}} z_{i_{\sigma+2},\tau_{\sigma+2} p}^{p^{e_{\sigma+2}}} \cdots z_{i_s,\tau_s p}^{p^{e_s}}.$$

Since

$$a(g - g') = a(z_{i_\sigma,\tau_\sigma p-1}^{p^{e_\sigma}} z_{i_{\sigma+1},\tau_{\sigma+1} p}^{p^{e_{\sigma+1}}} - z_{i_\sigma,\tau_\sigma p}^{p^{e_\sigma}} z_{i_{\sigma+1},\tau_{\sigma+1} p-1}^{p^{e_{\sigma+1}}})$$

$$\times z_{i_1,\tau_1 p-1}^{p^{e_1}} \cdots z_{i_{\sigma-1},\tau_{\sigma-1} p-1}^{p^{e_{\sigma-1}}} z_{i_{\sigma+2},\tau_{\sigma+2} p}^{p^{e_{\sigma+2}}} \cdots z_{i_s,\tau_s p}^{p^{e_s}},$$

it follows that

$$a(g - g') = a' z_{i_1,\tau_1 p-1}^{p^{e_1}} \cdots z_{i_{\sigma-1},\tau_{\sigma-1} p-1}^{p^{e_{\sigma-1}}} z_{i_{\sigma+1},\tau_{\sigma+1} p}^{p^{e_{\sigma+1}}} \cdots z_{i_s,\tau_s p}^{p^{e_s}},$$

where

$$a' = a(z_{i_\sigma,\tau_\sigma p-1}^{p^{e_\sigma}} z_{i_{\sigma+1},\tau_{\sigma+1} p}^{p^{e_{\sigma+1}}} - z_{i_\sigma,\tau_\sigma p}^{p^{e_\sigma}} z_{i_{\sigma+1},\tau_{\sigma+1} p-1}^{p^{e_{\sigma+1}}})$$

is an H-invariant. Repeating this procedure we eliminate after finitely many steps all the extra terms ag_κ in the above representation of $\gamma(g)$. As a result we obtain that $\sigma \le [s/2]$ and that v is a F_p-linear combination of invariants

$$\prod_{\kappa=1}^{\sigma} (z_{i_\kappa,\tau_\kappa p-1}^{p^{e_\kappa}} z_{i_{\kappa+1},\tau_{\kappa+1} p}^{p^{e_{\kappa+1}}} - z_{i_\kappa,\tau_\kappa p}^{p^{e_\kappa}} z_{i_{\kappa+1},\tau_{\kappa+1} p-1}^{p^{e_{\kappa+1}}}) \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} z_{i,\tau p}^{\omega_{i,\tau p}^{(e)}}.$$

This finishes the proof. □

Using the above arguments in the case of repeating $z_{i,\tau p-1}^{p^e}$ and $z_{i,\tau p}^{p^e}$ we obtain the following result.

Corollary 13. *Let $v \in A_{mv}^{\tilde{H}}$ be a polynomial of positive degree that is an F_p-linear combination*

$$v = \sum_{k=1}^{K} a_k S_{\tilde{H}}^{(\mu_k)}(f_k), \qquad a_k \neq 0,$$

of orbit sums $S_{\tilde{H}}^{(\mu_k)}(f_k)$, for various $\mu_k \ge 2$ and

$$f_k = \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \prod_{j=(\tau-1)+1}^{\tau p} (z_{ij}^{(e)})^{s_{ij\tau}^{(e)}}.$$

If v is invariant under the action of H, then it is an F_p-linear combination of invariants

$$\prod_{\kappa=1}^{\sigma}(z_{i_{2\kappa-1},\tau_{2\kappa-1}p-1}^{p^{e_{2\kappa-1}}}z_{i_{2\kappa},\tau_{2\kappa}p}^{p^{e_{2\kappa}}}-z_{i_{2\kappa-1},\tau_{2\kappa-1}p}^{p^{e_{2\kappa-1}}}z_{i_{2\kappa},\tau_{2\kappa}p-1}^{p^{e_{2\kappa}}})^{s_{i_{2\kappa-1}i_{2\kappa}\tau_{2\kappa-1}\tau_{2\kappa}}^{(e_{2\kappa-1},e_{2\kappa})}}$$
$$\times\prod_{e=0}^{\eta}\prod_{i=1}^{m}\prod_{\tau=1}^{r}(z_{i,\tau p}^{p^e})^{\omega_{i,\tau p}^{(e)}},$$

with $0\le\sigma\le[s/2]$, $(i_{2\kappa-1},\tau_{2\kappa-1})\prec(i_{2\kappa},\tau_{2\kappa})$, *and* $0\le s_{i_{2\kappa-1}i_{2\kappa}\tau_{2\kappa-1}\tau_\kappa}^{(e_{2\kappa-1},e_{2\kappa})},\omega_{i,\tau p}^{(e)}\le p-1$.

Now we study the structure of invariants $N_{\tilde H}^{(0)}(f)$ and $S_{\tilde H}^{(0)}(f)$, for various monomials $f\in F_p[z_{i,\tau p-1},z_{i,\tau p}\mid 1\le i\le m,1\le\tau\le r]$. At first we observe that

$$N_{\tilde H}^{(0)}(z_{i,\tau p-1})=z_{i,\tau p-1}^{p}-z_{i,\tau p-1}z_{i,\tau p}^{p-1}\quad\text{and}\quad N_{\tilde H}^{(0)}(z_{i,\tau p})=z_{i,\tau p}^{p}.$$

Hence if

$$f=\prod_{e=0}^{\eta}\prod_{i=1}^{m}\prod_{\tau=1}^{r}(z_{i,\tau p-1}^{p^e})^{s_{i,\tau p-1}^{(e)}}(z_{i,\tau p}^{p^e})^{s_{i,\tau p}^{(e)}},$$

then

$$N_{\tilde H}^{(0)}(f)=\prod_{e=0}^{\eta}\prod_{i=1}^{m}\prod_{\tau=1}^{r}(z_{i,\tau p-1}^{p^{e+1}}-z_{i,\tau p-1}^{p^e}z_{i,\tau p}^{p^e(p-1)})^{s_{i,\tau p-1}}(z_{i,\tau p}^{p^{e+1}})^{s_{i,\tau p}}.$$

We also observe that

$$z_{i_1,\tau_1p-1}^{p^{e_1}}z_{i_2,\tau_2p}^{p^{e_2}}-z_{i_1,\tau_1p}^{p^{e_1}}z_{i_2,\tau_2p-1}^{p^{e_2}}$$
$$=(z_{i_1,\tau_1p-1}^{p^{e_1}}-z_{i_1,\tau_1p-1}^{p^{e_1-1}}z_{i_1,\tau_1p}^{p^{e_1-1}(p-1)})z_{i_2,\tau_2p}^{p^{e_2}}$$
$$-(z_{i_1,\tau_1p}^{p^{e_1-1}}z_{i_2,\tau_2p}^{p^{e_2}}-z_{i_1,\tau_1p-1}^{p^{e_1-1}}z_{i_2,\tau_2p}^{p^{e_2}})z_{i_1,\tau_1p}^{p^{e_1-1}(p-1)}$$
$$=N_{\tilde H}^{(0)}(z_{i_1,\tau_1p-1})^{p^{e_1-1}}z_{i_2,\tau_2p}^{p^{e_2}}-(z_{i_1,\tau_1p}^{p^{e_1-1}}z_{i_2,\tau_2p-1}^{p^{e_2}}-z_{i_1\tau_1p-1}^{p^{e_1-1}}z_{i_2,\tau_2p}^{p^{e_2}})z_{i_1,\tau_1p}^{p^{e_1-1}(p-1)}.$$

Iterating the last relation we find that

$$z_{i_1,\tau_1p-1}^{p^{e_1}}z_{i_2,\tau_2p}^{p^{e_2}}-z_{i_1,\tau_1p}^{p^{e_1}}z_{i_2,\tau_2p-1}^{p^{e_2}}=(z_{i_1,\tau_1p-1}z_{i_2,\tau_2p}-z_{i_1,\tau_1p}z_{i_2,\tau_2p-1})z_{i_1,\tau_1p}^{p^{e_1}-1}z_{i_2,\tau_2p}^{p^{e_2}-1}$$
$$+\left(\sum_{\varepsilon_1=1}^{e_1}N_{\tilde H}^{(0)}(z_{i_1,\tau_1p-1})^{p^{e_1-\varepsilon_1}}z_{i_1,\tau_1p}^{p^{e_1-\varepsilon_1+1}(p^{\varepsilon_1-1}-1)}\right)z_{i_2,\tau_2p}^{p^{e_2}}$$
$$-\left(\sum_{\varepsilon_2=1}^{e_2}N_{\tilde H}^{(0)}(z_{i_2,\tau_2p-1})^{p^{e_2-\varepsilon_2}}z_{i_2,\tau_2p}^{p^{e_1-\varepsilon_2+1}(p^{\varepsilon_2-1}-1)}\right)z_{i_1,\tau_1p}^{p^{e_1}-1}.$$

Taking into account Proposition 9 and Corollary 13 we arrive at the following result.

Proposition 14. *Let* $v \in A_{mv}^{\tilde{H}}$ *be a polynomial of positive degree that is an* F_p*-linear combination of orbit sums* $S_{\tilde{H}}^{(\mu_k)}(f_k)$*, for various* $\mu_k \geq 1$ *and* $f_k \in A_{mv}$*. If* v *is invariant under the action of* H*, then* v *is a polynomial over* F_p *in* H*-invariants* $N_{\tilde{H}}^{(0)}(z_{i,\tau p-1})$, $z_{i,\tau p}$*, for* $1 \leq i \leq m$, $1 \leq r \leq r$*, and* $(z_{i_1,\tau_1 p-1} z_{i_2,\tau_2 p} - z_{i_1,\tau_1 p} z_{i_2,\tau_2 p-1})$*, for* $1 \leq i_1, i_2 \leq m$, $1 \leq \tau_1, \tau_2 \leq r$.

Let again

$$f = \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} (z_{i,\tau p-1}^{p^e})^{s_{i,\tau p-1}^{(e)}} (z_{i,\tau p}^{p^e})^{s_{i,\tau p}^{(e)}}.$$

We set

$$\sum_{e=0}^{\eta} s_{i,\tau p-1}^{(e)} = s_{i,\tau p-1}^{(0)} + t_{i,\tau p-1}^{(0)} p,$$

where $0 \leq s_{i,\tau p-1}^{(0)} \leq p-1$, and write f in the form

$$f = \prod_{i=1}^{m} \prod_{\tau=1}^{r} z_{i,\tau p-1}^{s_{i,\tau p}^{(0)}} (z_{i,\tau p-1}^{p})^{t_{i,\tau p-1}^{(0)}} \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} z_{i,\tau p}^{s_{i,\tau p}^{(e)}}.$$

Since $z_{i,\tau p-1}^{p} = N_{\tilde{H}}^{(0)}(z_{i,\tau p-1}) + z_{i,\tau p-1} z_{i,\tau p}^{p-1}$, it follows that

$$f = \prod_{i=1}^{m} \prod_{\tau=1}^{r} z_{i,\tau p-1}^{s_{i,\tau p-1}^{(0)}} (N_{\tilde{H}}^{(0)}(z_{i,\tau p-1}) + z_{i,\tau p-1} z_{i,\tau p}^{p-1})^{t_{i,\tau p-1}^{(0)}} \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} z_{i,\tau p}^{s_{i,\tau p}^{(e)}}.$$

Iterating the last relation we find that f is an F_p-linear combination of polynomials

$$\prod_{i=1}^{m} \prod_{\tau=1}^{r} z_{i,\tau p-1}^{s_{i,\tau p-1}} z_{i,\tau p}^{t_{i,\tau p}} N_{\tilde{H}}^{(0)}(z_{i,\tau p-1})^{\omega_{i,\tau p-1}},$$

with $0 \leq s_{i,\tau p-1} \leq p-1$. Hence $S_{\tilde{H}}^{(0)}(f)$ is an F_p-linear combination of H-invariants

$$S_{\tilde{H}}^{(0)}(f') \prod_{i=1}^{m} \prod_{\tau=1}^{r} z_{i,\tau p}^{t_{i,\tau p}} N_{\tilde{H}}^{(0)}(z_{i,\tau p-1})^{\omega_{i,\tau p-1}},$$

where

$$f' = \prod_{i=1}^{m} \prod_{\tau=1}^{r} z_{i,\tau p-1}^{s_{i,\tau p-1}}$$

and $0 \leq s_{i,\tau p-1} \leq p-1$, for $1 \leq i \leq m$, $1 \leq \tau \leq r$. Thus we obtain the following result.

Proposition 15. *Let*

$$f = \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} (z_{i,\tau p-1}^{p^e})^{s_{i,\tau p-1}^{(e)}} (z_{i,\tau p}^{p^e})^{s_{i,\tau p}^{(e)}}$$

be a monomial in $F_p[z_{i,\tau p-1}, z_{i,\tau p} \mid 1 \le i \le m, 1 \le \tau \le r]$, *and let*

$$S_{\tilde{H}}^{(0)}(f) = \sum_{\alpha \in F_p} \prod_{e=0}^{\eta} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \left(z_{i,\tau p-1}^{p^e} + \binom{\alpha}{1} z_{i,\tau p}^{p^e} \right)^{s_{i,\tau p-1}^{(e)}} \left(z_{i,\tau p}^{p^e} \right)^{s_{i,\tau p}^{(e)}}$$

be the corresponding orbit sum. Then $S_{\tilde{H}}^{(0)}(f)$ *is a polynomial over* F_p *in* H*-invariants* $N_{\tilde{H}}^{(0)}(z_{i,\tau p-1})$, $z_{i,\tau p}$, *for* $1 \le i \le m$, $1 \le \tau \le r$, *and* $S_{\tilde{H}}^{(0)}(f')$, *for various monomials*

$$f' = \prod_{i=1}^{m} \prod_{\tau=1}^{r} z_{i,\tau p-1}^{s_{i,\tau p-1}}$$

such that $0 \le s_{i,\tau p-1} \le p-1$, *for* $1 \le i \le m$, $1 \le \tau \le r$.

With the use of Theorem 5, Theorem 8, Proposition 14 and Proposition 15 we now arrive at the following result.

Theorem 16. *Let* $v \in A_{mv}^{\tilde{H}}$ *be a polynomial of positive degree that is invariant under the action of* H. *Then* v *is a polynomial over* F_p *in the* H*-invariants* $N_{\tilde{H}}^{(0)}(z_{i,\tau p-1})$, $z_{i,\tau p}$, *for* $1 \le i \le m$, $1 \le \tau \le r$, *the* H*-invariants* $(z_{i_1,\tau_1 p-1} z_{i_2,\tau_2 p} - z_{i_1,\tau_1 p} z_{i_2,\tau_2 p-1})$, *for* $1 \le i_1, i_2 \le m$, $1 \le \tau_1, \tau_2 \le r$, $(i_1, \tau_1) \prec (i_2, \tau_2)$, *and the* H*-invariants* $S_{\tilde{H}}^{(0)}(f')$, *for various monomials*

$$f' = \prod_{i=1}^{m} \prod_{\tau=1}^{r} z_{i,\tau p-1}^{s_{i,\tau p-1}}$$

such that $0 \le s_{i,\tau p-1} \le p-1$.

Finally, we determine an exact form of the polynomials $S_{\tilde{H}}^{(0)}(f')$ for all monomials f' of the above form.

Proposition 17. *Let*

$$f' = \prod_{i=1}^{m} \prod_{\tau=1}^{r} z_{i,\tau p-1}^{s_{i,\tau p-1}}$$

be a monomial of degree $s \ge 1$ *such that* $0 \le s_{i,\tau p-1} \le p-1$, *for* $1 \le i \le m$, $1 \le \tau \le r$. *Then*

$$S_{\tilde{H}}^{(0)}(f') = -\sum_{l=1}^{[s/(p-1)]} \sum_{(\sigma_{i,\tau p-1})} \prod_{i=1}^{m} \prod_{\tau=1}^{r} a_{i,\tau p-1} z_{i,\tau p-1}^{s_{i,\tau p-1}-\sigma_{i,\tau p-1}} z_{i,\tau p}^{\sigma_{i,\tau p-1}},$$

where the inner sum is over all integral tuples $(\sigma_{i,\tau p-1})$ *such that*

$$\sum_{i=1}^{m} \sum_{\tau=1}^{r} \sigma_{i,\tau p-1} = l(p-1) \le s$$

and $0 \le \sigma_{i,\tau p-1} \le s$, *for* $1 \le i \le m$, $1 \le \tau \le r$.

Proof. We set

$$s_i = \sum_{\tau=1}^{r} s_{i,\tau p-1} \quad \text{and} \quad s = \sum_{i=1}^{m} s_i.$$

Since

$$\left(z_{i,\tau p-1} + \binom{\alpha}{1} z_{i,\tau p}\right)^{s_{i,\tau p-1}} = \sum_{\alpha \in F_p} a_{\sigma_{i,\tau p-1}} \alpha^{\sigma_{i,\tau p-1}} z_{i,\tau p-1}^{s_{i,\tau p-1}-\sigma_{i,\tau p-1}} z_{i,\tau p}^{\sigma_{i,\tau p}},$$

where

$$a_{\sigma,\tau p-1} = \binom{s_{i,\tau p-1}}{\sigma_{i,\tau p-1}},$$

then

$$\prod_{\tau=1}^{r} \left(z_{i,\tau p-1} + \binom{\alpha}{1} z_{i,\tau p}\right)^{s_{i,\tau p-1}}$$

$$= \sum_{\sigma_i=0}^{s_i} \alpha^{\sigma_i} \sum_{\sigma_{i,p-1}+\cdots+\sigma_{i,rp-1}=\sigma_i} \prod_{\tau=1}^{r} a_{i,\tau p-1} z_{i,\tau p-1}^{s_{i,\tau p-1}-\sigma_{i,\tau p-1}} z_{i,\tau p}^{\sigma_{i,\tau p-1}}.$$

In that case,

$$\prod_{i=1}^{m} \prod_{\tau=1}^{r} \left(z_{i,\tau p-1} + \binom{\alpha}{1} z_{i,\tau p}\right)^{s_{i,\tau p-1}}$$

$$= \sum_{\sigma=0}^{s} \alpha^{\sigma} \sum_{(\sigma_{i,\tau p-1})} \prod_{i=1}^{m} \prod_{\tau=1}^{r} a_{i,\tau p-1} z_{i,\tau p-1}^{s_{i,\tau p-1}-\sigma_{i,\tau p-1}} z_{i,\tau p}^{\sigma_{i,\tau p-1}}$$

and hence

$$S_{\tilde{H}}^{(0)}(f') = \sum_{\alpha \in F_p} \prod_{i=1}^{m} \prod_{\tau=1}^{r} \left(z_{i,\tau p-1} + \binom{\alpha}{1} z_{i,\tau p}\right)^{s_{i,\tau p-1}}$$

$$= \sum_{\sigma=0}^{s} \sum_{\alpha \in F_p} \alpha^{\sigma} \sum_{(\sigma_{i,\tau p-1})} \prod_{i=1}^{m} \prod_{\tau=1}^{r} a_{i,\tau p-1} z_{i,\tau p-1}^{s_{i,\tau p-1}-\sigma_{i,\tau p-1}} z_{i,\tau p}^{\sigma_{i,\tau p-1}},$$

where the inner sum is over all tuples $(\sigma_{i,\tau p-1})$ such that $0 \le \sigma_{i,\tau p-1} \le s_{i,\tau p-1}$, for $1 \le i \le m$, $1 \le \tau \le r$, and

$$\sum_{i=1}^{m} \sum_{\tau=1}^{r} \sigma_{i,\tau p-1} = \sigma.$$

Now the required result follows from the fact that

$$\sum_{\alpha \in F_p} \alpha^{\sigma} = \begin{cases} p-1, & \text{if } \sigma = l(p-1) \\ 0, & \text{otherwise.} \end{cases}$$

□

3 Proof of Theorem 1 and Corollary 2

Since x_{ij}, for $1 \le i \le m$, $2r+1 \le j \le n$, are invariant under the action of H, every invariant $u \in A_{mn}^H$ is a polynomial of the form

$$u = u_1 f_1 + \cdots + u_l f_l ,$$

where $u_\iota \in A_{m,2r}^H$ and f_k, for $1 \le k \le l$, are monomials in $F_p[x_{i,j} \mid 1 \le i \le m, 2r+1 \le j \le n]$. This shows that we can assume without loss of generality that $u \in A_{m,2r}^H$. Therefore, it suffices to show that

$$A_{m,2r}^H = F_p[x_{i,2\tau-1}, N_H^{(0)}(x_{i,2\tau-1}), (x_{i_1,2\tau_1-1}x_{i_2,2\tau_2} - x_{i_1,2\tau_1}x_{i_2,2\tau_2-1}), S_H^{(0)}(f')],$$

where $1 \le i \le m$, $1 \le \tau \le r$, $1 \le i_1, i_2 \le m$, $1 \le \tau_1, \tau_2 \le r$, and $(i_1, \tau_1) \prec (i_2, \tau_2)$, and f' runs through the set of monomials

$$f' = \prod_{i=1}^{m}\prod_{\tau=1}^{r} x_{i,2\tau-1}^{s_{i,2\tau-1}} \quad \text{with} \quad 0 \le s_{i,2\tau-1} \le p-1.$$

If $\vartheta : V_i \hookrightarrow \tilde{V}_i$ is the embedding defined by (6), then ϑ induces the corresponding F_p-algebra monomorphism $\vartheta : A_{m,2r} \to A_{mv}$. Let u be an element of $A_{n,2r}^H$, and $v = \vartheta(u) \in A_{mv}$ the image of u. Then v is invariant under the action of H on A_{mv} defined by (7) as well as under the action of $\tilde{H}$. It follows from Theorem 16 that v is a polynomial in H-invariants $N_{\tilde{H}}^{(0)}(z_{i,\tau p-1})$, $z_{i,\tau p}$, for $1 \le i \le m$, $1 \le \tau \le r$, in H-invariants $(z_{i_1,\tau_1 p-1}z_{i_2,\tau_2 p} - z_{i_1,\tau_1 p}z_{i_2,\tau_2 p-1})$, for $1 \le i_2, i_2 \le m$, $1 \le \tau_1, \tau_2 \le r$, $(i_1, \tau_1) \prec (i_2, \tau_2)$, and in H-invariants $S_{\tilde{H}}^{(0)}(f')$, for various monomials

$$f' = \prod_{i=1}^{m}\prod_{\tau=1}^{r} z_{i,\tau p-1}^{s_{i,\tau p-1}},$$

such that $0 \le s_{i,\tau p-1} \le p-1$. Identifying now $z_{i,\tau p-1}$, $z_{i,\tau p}$ with $x_{i,2\tau-1}$, $x_{i,2\tau}$ via the isomorphism ϑ and taking into account that

$$\vartheta(N_H^{(0)}(x_{i,2\tau-1})) = N_{\tilde{H}}^{(0)}(z_{i,2\tau p-1}), \quad \vartheta(S_H^{(0)}(f')) = S_{\tilde{H}}^{(0)}(f')$$

under this identification, we find that

$$A_{mn}^H = F_p[x_{i,2\tau}, x_{ij}, N_H^{(0)}(x_{i,2\tau-1}), (x_{i_1,2\tau_1-1}x_{i_2,2\tau_2} - x_{i_1,2\tau_1}x_{i_2,2\tau_2-1}), S_H^{(0)}(f')].$$

This proves Theorem 1.

To prove Corollary 2 we consider the polynomial

$$S_H^{(0)}(g') = \sum_{\alpha \in F_p} \prod_{i=1}^{m}\prod_{\tau=1}^{r} \left(x_{i,2\tau-1} + \binom{\alpha}{1} x_{i,2\tau}\right)^{p-1}$$

and show that $S_H^{(0)}(g')$ cannot be expressed as a polynomial over F_p in H-invariants $x_{i,2\tau}$, $N_H^{(0)}(x_{i,2\tau-1})$, $(x_{i_1,2\tau_1-1}x_{i_2,2\tau_2} - x_{i_1,2\tau_1}x_{i_2,2\tau_2-1})$, and $S_H^{(0)}(f')$, where

$$f' = \prod_{i=1}^{m}\prod_{\tau=1}^{r} x_{i,2\tau-1}^{s_{i,2\tau-1}}$$

is a monomial such that $s_{i,2\tau-1} < p-1$ at least for one pair (i,τ) with $1 \le i \le m$, $1 \le \tau \le r$. At first we observe that $S_H^{(0)}(g')$ involves the monomial

$$h' = x_{12}^{p-1} \prod_{\substack{i=1 \\ (i,\tau)\neq(1,1)}}^{m} \prod_{r=1}^{r} x_{i,2\tau-1}^{p-1}$$

of total degree $mr(p-1)$ which occurs in $S_H^{(0)}(g')$ with coefficient -1. Moreover, if

$$f' = \prod_{i=1}^{m} \prod_{\tau=1}^{r} x_{i,2\tau-1}^{s_{i,2\tau-1}} \quad \text{and} \quad S_H^{(0)}(f') \neq 0,$$

then we conclude in view of Proposition 17 that the polynomial $S_H^{(0)}(f')$ involves a monomial of the following form:

$$\prod_{i=1}^{m} \prod_{\tau=1}^{r} x_{i,2\tau-1}^{s_{i,2\tau-1}-\sigma_{i,2\tau-1}} x_{i,2\tau}^{\sigma_{i,2\tau-1}},$$

where $0 \le \sigma_{i,2\tau-1} \le s_{i,2\tau-1}$, and

$$\sum_{i=1}^{m} \sum_{\tau=1}^{r} \sigma_{i,2\tau-1} = p-1.$$

Now we show that no monomial M in $x_{i,2\tau}$, $(x_{i_1,2\tau_1-1}x_{i_2,2\tau_2} - x_{i_1,2\tau_1 2}x_{i_2,2\tau_2-1})$, $N_H^{(0)}(x_{i,2\tau-1})$ and $S_H^{(0)}(f')$, where $\deg f' < mr(p-1)$, occurring in $S_H^{(0)}(g')$ when expanded in terms $x_{i,2\tau-1}$, $x_{i,2\tau}$, for $1 \le i \le m$, $1 \le \tau \le r$, contains the monomial h' with a nonzero coefficient. We observe that $S_H^{(0)}(f')$ is a homogeneous polynomial and therefore each monomial M of this kind has the same total degree $mr(p-1)$ in $x_{i,2\tau}$ and $x_{i,2\tau}$.

If M contains as a factor of some power of $N_H^{(0)}(x_{i,2\tau-1}) = x_{i,2\tau-1}^{p} - x_{i,2\tau-1}x_{i,2\tau}^{p-1}$, then it follows from the rather special form of the polynomials $N_H^{(0)}(x_{i,2\tau-1})$, $S_H^{(0)}(f')$ and $(x_{i_1,2\tau_1-1}x_{i_2,2\tau_2} - x_{i_1,2\tau_2}x_{i_2,2\tau_2-1})$, that the expansion of M in powers of $x_{i,2\tau-1}$ and $x_{i,2\tau}$ is an F_p-linear combination of monomials each of which either involves $x_{i,2\tau-1}^{p}$ or has a total degree of at least p in the variables $x_{i,2\tau}$.

Assume now that M involves a polynomial $S_H^{(0)}(f')$ with $\deg f' < mr(p-1)$. Then using similar arguments we see that each monomial occurring in M with a nonzero coefficient has a total degree at least p in the $x_{i,2\tau}$.

Finally, since $mr > 2$, each monomial M in the variables $x_{i,2\tau}$, for $1 \le i \le m$, $1 \le \tau \le r$, and the invariants $(x_{i_2,2\tau_1}x_{i_2,2\tau_2} - x_{i_1,2\tau_1}x_{i_2,2\tau_2-1})$, for $1 \le i_1, i_2 \le m$, $1 \le \tau_1, \tau_2 \le r$, $(i_1,\tau_1) \prec (i_2,\tau_2)$, that has the total degree $mr(p-1)$ in the variables $x_{i,2\tau-1}$ and $x_{i,2\tau}$ has a total degree at least $mr(p-1)/2 > p-1$ in the variables $x_{i,2\tau}$.

In each of the above cases the monomial h' cannot occur in the monomial M with a nonzero coefficient, and this completes the proof of Corollary 2.

4 A universal invariant

Assume that $m \geq n$ and consider the polynomial

$$f_0 = \sum_{\alpha_1,\ldots,\alpha_n \in F_p} (\alpha_1 x_{11} + \cdots + \alpha_n x_{1n})^{p-1} \cdots (\alpha_1 x_{m1} + \cdots + \alpha_n x_{mn})^{p-1}. \quad (8)$$

At first we show that f_0 is invariant under the action of the general linear group $GL(n, F_p)$. In that case, the polynomial f_0 is also invariant under the action of any subgroup G of $GL(n, F_p)$. It suffices to prove that f_0 is invariant under the action of an arbitrary element of the group G.

Proposition 18. *If σ is an arbitrary element of the group $GL(n, F_p)$, then $\sigma(f_0) = f_0$.*

Proof. Since

$$\sigma((\alpha_1 x_{11} + \cdots + \alpha_n x_{1n})^{p-1} \cdots (\alpha_1 x_{m1} + \cdots + \alpha_n x_{mn})^{p-1})$$

$$= (\alpha_1 \sigma(x_{11}) + \cdots + \sigma(x_{1n})^{p-1} \cdots (\alpha_1 \sigma(x_{m1}) + \cdots + \alpha_n \sigma(x_{mn}))^{p-1}$$

and action of σ permutes the elements of each space $V_i = F_p x_{i1} + \cdots + F_p x_{in}$, for $1 \leq i \leq m$, in the same way, we deduce that

$$\begin{aligned}\sigma(f_0) &= \sum_{\alpha_1,\ldots,\alpha_n \in F_p} (\alpha_1 \sigma(x_{11}) + \cdots + \alpha_n \sigma(x_{1n}))^{p-1} \cdots (\alpha_1 \sigma(x_{m1}) \\ &\quad + \cdots + \alpha_n \sigma(x_{mn}))^{p-1} \\ &= \sum_{\alpha'_1,\ldots,\alpha'_n \in F_p} (\alpha'_1 x_{11} + \cdots + \alpha'_n x_{1n})^{p-1} \cdots (\alpha'_1 x_{m1} + \cdots + \alpha'_n x_{mn})^{p-1} = f_0.\end{aligned}$$

This proves the proposition. □

If F is a polynomial in A_{mn}, let $\pi(F)$ denote its image under the projection

$$\begin{aligned}&\pi(x_{11}, \ldots, x_{1n}; \ldots; x_{m1}, \ldots, x_{mn}) \\ &= (\pi_1(x_{11}, \ldots, x_{1n}); \ldots; \pi_m(x_{m1}, \ldots, x_{mn})),\end{aligned} \quad (9)$$

where

(i) $\pi_i(x_{i1}, \ldots, x_{in}) = (0, \ldots, 0, x_{ii}, 0, \ldots, 0)$, for $i = 1, 2, \ldots, n$;
(ii) $\pi_i(x_{i1}, \ldots, x_{in}) = (x_{i1}, 0, \ldots, 0, 0, \ldots, 0,)$, for $i = n+1, \ldots, m$.

Clearly the map

$$\begin{aligned}&\pi(f(x_{11}, \ldots, x_{1n}; \ldots; x_{m1}, \ldots, x_{mn})) \\ &= f(\pi_1(x_{11}, \ldots, x_{1n}); \ldots; \pi_m(x_{m1}, \ldots, x_{mn}))\end{aligned}$$

defines an F_p-algebra homomorphism.

Denote by $\pi(f_0)$ the image of the polynomial f_0 under the projection π and find an exact form of the polynomial $\pi(f_0)$.

Proposition 19. *If $m \geq n$, then the polynomial $\pi(f_0)$ has the form*

$$\pi(f_0) = (-1)^n \prod_{i=1}^{n} x_{ii}^{p-1} \prod_{i=n+1}^{m} x_{i1}^{p-1}.$$

Proof. At first we observe that

$$\pi(f_0) = \sum_{\alpha_1,\dots,\alpha_n \in F_p} \prod_{i=1}^{n} (\alpha_i x_{ii})^{p-1} \prod_{i=n+1}^{m} (\alpha_1 x_{i1})^{p-1}.$$

In that case,

$$\pi(f_0) = \prod_{i=1}^{n} x_{ii}^{p-1} \prod_{i=n+1}^{m} x_{i1}^{p-1} \left(\sum_{\alpha_1,\dots,\alpha_n \in F_p} \alpha_1^{(m-n+1)(p-1)} \prod_{j=2}^{n} \alpha_j^{p-1} \right),$$

and since $\sum_{\alpha \in F_p} \alpha^{l(p-1)} = -1$ for every positive integer l, then

$$\pi(f_0) = (-1)^n \prod_{i=1}^{n} x_{ii}{}^{p-1} \prod_{i=n+1}^{m} x_{i1}^{p-1}$$

This completes the proof. □

5 Proof of Theorem 3

Let $G \leq GL(n, F_p)$ be a group such that its order $|G|$ is divisible by p, and $H = \langle \gamma \rangle$ a cyclic subgroup of G of order p. Since $H \leq G \leq GL(n, F_p)$, we have

$$A_{mn}^{GL(n,F_p)} \subseteq A_{mn}^{G} \subseteq A_{mn}^{H}.$$

Assume that $m \geq n$ and that the sizes $n_1, \dots, n_s$ of the basic Jordan blocks of the matrix γ satisfy the condition

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

so that $n = 2r + s - r = r + s$.

To prove Theorem 3 it suffices to show that every system of F_p-algebra generators of A_{mn}^{G} contains a generator of degree at least $(m - n + 2r)(p - 1)/r$. Set

$$u_{(i_1,\tau_1),(i_2,\tau_2)} = (x_{i_1,2\tau_1-1} x_{i_2,2\tau_2} - x_{i_1,2\tau_1} x_{i_2,2\tau_2-1})$$

and consider the system of generators

$$B_{mn}^{H} = \{x_{i,2\tau}, x_{ij}, N_H^{(0)}(x_{i_1,2\tau_1-1}), u_{(i_1,\tau_1),(i_2,\tau_2)}, S_H^{(0)}(f')\}$$

of the algebra A_{mn}^{H}, described by Theorem 1. It follows from Corollary 2 that B_{mn}^{H} consists of F_p-algebra generators of the minimal possible degree. Let B_{mn}^{G} be a system of F_p-algebra generators of A_{mn}^{G}. Since $A_{mn}^{G} \subseteq A_{mn}^{H}$, we can assume without loss of generality that $B_{mn}^{G} \subseteq B_{mn}^{H}$. Denote by $\tilde{B}_{mn}^{H}$ a subset of B_{mn}^{H} which consists of the invariants $u \in B_{mn}^{H}$ satisfying the condition

$$\deg u < (m - n + 2r)(p - 1)/2$$

and set $\tilde{B}^G_{mn} = \tilde{B}^H_{mn} \cap B^G_{mn}$. Let $f_0 \in A_{mn}$ be the polynomial defined by (8). Propositions 18 and 19 imply that f_0 is a homogeneous polynomial of degree $m(p-1)$ that is invariant under action of $GL(n, F_p)$. In the case f_0 is also an invariant under the action of G as well as H. The crucial point is that the invariant $f_0 \in A^G_{mn}$ is *indecomposable* in A^H_{mn} with respect to $\tilde{B}^H_{mn}$, i.e., f_0 cannot be written as a polynomial over F_p in vector invariants $u \in \tilde{B}^H_{mn}$. All the more, the invariant f_0 is indecomposable in A^G_{mn} with respect to $\tilde{B}^G_{mn}$, i.e., f_0 cannot be written as a polynomial in invariants $u \in \tilde{B}^G_{mn}$.

Denote by η the cardinality of $\tilde{B}^H_{mn}$ and enumerate the elements u of $\tilde{B}^H_{mn}$ by the numbers $1, 2, \ldots, \eta$. Assume for the contrary that f_0 is a polynomial over F_p in elements of $u_1, \ldots, u_\eta \in \tilde{B}^H_{mn}$ and write

$$f_0 = \sum_{\substack{1 \le \delta_1 + \cdots + \delta_\eta \le m(p-1) \\ \delta_1 \deg u_1 + \cdots + \delta_\eta \deg u_\eta = m(p-1)}} a_{\delta_1, \ldots, \delta_\eta} u_1^{\delta_1} \cdots u_\eta^{\delta_\eta}, \tag{10}$$

Comparing degrees of the monomials which appear in both sides of the last identity (with respect to each of the variables $x_{11}, \ldots, x_{m1}; \ldots; x_{1n}, \ldots, x_{mn}$), then taking into account that f_0, $u_1, \ldots, u_\eta$ are homogeneous polynomials in $x_{11}, \ldots, x_{m1}; \ldots; x_{1n}, \ldots, x_{mn}$, and $\deg f_0 = m(p-1)$, $\deg_{x_{ij}} f_0 = p - 1$, for $1 \le i \le m$, $1 \le j \le n$, we find that $0 \le \delta_\rho \le p - 1$, for $1 \le \rho \le \eta$, and $\delta_1 + \cdots + \delta_\eta > 1$; moreover, we see that

$$\deg_{x_{ij}} u_\rho \le p - 1,$$

for all $1 \le i \le m$, $1 \le j \le n$ and $1 \le \rho \le \eta$. Now we assume that

$$\{1, 2, \ldots, \eta\} = I_1 \cup I_2 \cup I_3 \cup I_4 \cup I_5,$$

and $u_\epsilon = S^{(0)}_H(f'_\epsilon)$, for $\epsilon \in I_1$; $u_\kappa = N^{(0)}_H(x_{i,2\tau-1})$, for $\kappa \in I_2$, $1 \le i = i(\kappa) \le m$, and $1 \le \tau = \tau(\kappa) \le r$; $u_\lambda = u_{(i_1,\tau_1),(i_2,\tau_2)}$, for $\lambda \in I_3$, $1 \le i_1 = i_1(\lambda), i_2 = i_2(\lambda) \le m$, $1 \le \tau_1 = \tau_1(\lambda), \tau_2 = \tau_2(\lambda) \le r$, and $(i_1, \tau_1) \prec (i_2, \tau_2)$; $u_\mu = x_{i,2\tau}$, for $\mu \in I_4$, $1 \le i = i(\mu) \le m$, and $1 \le \tau = \tau(\mu) \le r$; $u_\nu = x_{ij}$, for $\nu \in I_5$, $1 \le i = i(\nu) \le m$, and $2r + 1 \le j = j(\nu) \le n$. The relation (10) takes the following form:

$$\begin{aligned} f_0 = \sum a_{\delta_1, \ldots, \delta_\eta} & \prod_{\epsilon \in I_1} (S^{(0)}_H(f'_\epsilon))^{\delta_\epsilon} \prod_{\kappa \in I_2} (N^{(0)}_H(x_{i(\kappa),2\tau(\kappa)-1}))^{\delta_\kappa} \\ & \times \prod_{\lambda \in I_3} (u_{(i_1(\lambda),\tau_1(\lambda)),(i_2(\lambda),\tau_2(\lambda))})^{\delta_\lambda} \prod_{\mu \in B_4} x^{\delta_\mu}_{i(\mu),2\tau(\mu)} \prod_{\nu \in I_5} x^{\delta_\nu}_{i(\nu),j(\nu)}, \end{aligned} \tag{11}$$

where the sum on the right-hand side is over all nonnegative integers $\delta_1, \ldots, \delta_\delta$ satisfying the condition

$$\sum_{\epsilon \in I_1} \delta_\epsilon \deg S^{(0)}_H(f'_\epsilon) + \sum_{\kappa \in I_2} \delta_\kappa \deg N^{(0)}_H(x_{i(\kappa),2\tau(\kappa)-1}) + \sum_{\lambda \in I_3} 2\delta_\lambda + \sum_{\mu \in I_4} \delta_\mu + \sum_{\nu \in I_5} \delta_\nu$$

$$= m(p-1).$$

Now we prove that equality (11) is impossible by showing that the monomial

$$\prod_{i=1}^{n} x_{ii}^{p-1} \prod_{i=n+1}^{m} x_{i1}^{p-1}$$

appears in the left-hand side of (11), but does not appear in its right-hand side. Let π be the F_p-algebra homomorphism defined by (9). Then Proposition 19 implies

$$\pi(f_0) = (-1)^n \prod_{i=1}^{n} x_{ii}^{p-1} \prod_{i=n+1}^{m} x_{i1}^{p-1}.$$

On the other hand, we have

$$\pi(N_H^{(0)}(x_{i,2\tau-1})) = \begin{cases} x_{2\tau-1,2\tau-1}^{p}, & \text{if } i = 2\tau-1,\ 1 \le \tau \le r \\ x_{i1}^{p}, & \text{if } n+1 \le i \le m \\ 0, & \text{otherwise,} \end{cases}$$

$$\pi(u_{(i,\sigma),(k,\tau)}) = \begin{cases} x_{2\sigma-1,2\sigma-1}x_{2\tau,2\tau}, & \text{if } i = 2\sigma-1,\ k = 2\tau,\ 1 \le \sigma \le \tau \le r \\ -x_{2\sigma,2\sigma}x_{2\tau-1,2\tau-1}, & \text{if } i_1 = 2\sigma,\ k = 2\tau-1,\ 1 \le \sigma < \tau \le r \\ -x_{k1}x_{2\sigma,2\sigma}, & \text{if } n+1 \le k \le m,\ \tau = 1,\ 1 \le \sigma \le r \\ 0, & \text{otherwise,} \end{cases}$$

and if

$$f' = \prod_{i=1}^{m} \prod_{\tau=1}^{r} x_{i,2\tau-1}^{s_{i,2\tau-1}},$$

then it follows by Proposition 17,

$$\pi(S_H^{(0)}(f')) = -\prod_{\tau=1}^{r} x_{2\tau-1,2\tau-1}^{s_{2\tau-1,2\tau-1}} x_{2\tau,2\tau}^{s_{2\tau,2\tau-1}},$$

where $\sum_{\tau=1}^{r} s_{2\tau,2\tau-1} = l(p-1)$ for some positive integer $l \le m$.

Applying the F_p-algebra homomorphism π to both sides of the relation (11) we obtain

$$\begin{aligned} \prod_{i=1}^{2r} x_{ii}^{p-1} \prod_{i=n+1}^{m} x_{i1}^{p-1} = {} & \prod_{\epsilon \in I_1} \left(\prod_{\tau=1}^{r} x_{2\tau-1,2\tau-1}^{s_{2\tau-1,2\tau-1}^{(\epsilon)}} x_{2\tau,2\tau}^{s_{2\tau,2\tau-1}^{(\epsilon)}} \prod_{i=n+1}^{m} x_{i1}^{s_{i1}^{(\epsilon)}} \right)^{\delta_\epsilon} \\ & \times \prod_{\kappa \in I_2} \left(\prod_{\tau=1}^{r} (x_{2\tau-1,2\tau-1}^{p})^{s_{2\tau-1,2\tau-1}^{(\kappa)}} \prod_{i=n+1}^{m} (x_{i1}^{p})^{s_{i1}^{(\kappa)}} \right)^{\delta_\kappa} \\ & \times \prod_{\lambda \in J_3} \left(\prod_{\rho=1}^{r} \prod_{\sigma=1}^{r} (x_{2\rho-1,2\rho-1}x_{2\sigma,2\sigma})^{s_{2\rho-1,2\sigma}^{(\lambda)}} \right. \\ & \left. \times \prod_{i=n+1}^{m} \prod_{\tau=1}^{r} (x_{i1}x_{2\tau,2\tau})^{s_{i,2\tau}^{(\lambda)}} \right)^{\delta_\lambda} \prod_{\mu \in I_4} \left(\prod_{\tau=1}^{r} x_{2\tau,2\tau}^{s_{2\tau,2\tau}^{(\mu)}} \right)^{\delta_\mu}, \end{aligned} \tag{12}$$

where

$$\sum_{\tau=1}^{r} s^{(\epsilon)}_{2\tau-1,2\tau} = l(p-1), \quad \sum_{\tau=1}^{r} s^{(\kappa)}_{2\tau-1,2\tau-1} = 1, \quad \sum_{i=n+1}^{m} s^{(\kappa)}_{ii} = 1,$$

$$\sum_{\rho=1}^{r}\sum_{\sigma=1}^{r} s^{(\lambda)}_{2\rho-1,2\sigma} = 1, \quad \sum_{i=n+1}^{m}\sum_{\tau=1}^{r} s^{(\lambda)}_{i,2\tau} = 1,$$

$$\sum_{\tau=1}^{r} s^{(\mu)}_{2\tau,2\tau} = 1, \quad \sum_{i=1}^{m}\sum_{j=2r+1}^{n} s^{(\nu)}_{ij} = 1$$

and $s^{(\kappa)}_{2\tau-1,2\tau-1} + s^{(\kappa)}_{ii} \leq 1$ and $s^{(\lambda)}_{2\rho-1,2\sigma} + s^{(\lambda)}_{i,2\tau} \leq 1$. If $s^{(\kappa)}_{2\tau-1,2\tau-1}\delta_\kappa \geq 1$ or $s^{(\kappa)}_{i1}\delta_\kappa \geq 1$, for some (τ, κ), (i, κ), then degree of the right-hand side of (12) with respect to $x_{2\tau,2\tau}$ or x_{i1} is at least p, which is impossible. This shows that $\delta_\kappa = 0$ for all $\kappa \in I_2$.

Set

$$L_1 = \sum_{\epsilon\in I_1}\sum_{i=n+1}^{m} \delta_\epsilon s^{(\epsilon)}_{i,1}, \quad L_3 = \sum_{\lambda\in I_3}\sum_{i=n+1}^{m} \delta_\lambda s^{(\lambda)}_{i,2\tau},$$

$$M_1 = \sum_{\epsilon\in I_1}\sum_{\tau=1}^{r} \delta_\epsilon s^{(\epsilon)}_{2\tau-1,2\tau-1}, \quad M_3 = \sum_{\lambda\in I_3}\sum_{\rho=1}^{r}\sum_{\sigma=1}^{r} \delta_\lambda s^{(\lambda)}_{2\rho-1,2\sigma}$$

and

$$N_1 = \sum_{\epsilon\in I_1}\sum_{\tau=1}^{r} \delta_\epsilon s^{(\epsilon)}_{2\tau,2\tau-1}, \quad N_4 = \sum_{\mu\in I_4}\sum_{\tau=1}^{r} \delta_\mu s^{(\mu)}_{2\tau,2\tau}.$$

Comparing total degrees of the left-hand side and the right-hand side of relation (12) with respect to x_{i1}'s, $x_{2\tau-1,2\tau-1}$'s and $x_{2\tau,2\tau}$'s, respectively, we obtain

$$L_1 + L_3 = (m-n)(p-1), \quad M_1 + M_3 = r(p-1)$$

and

$$N_1 + L_3 + M_3 + N_4 = r(p-1).$$

We observe also that the condition

$$\sum_{\tau=1}^{r} s^{(\epsilon)}_{2\tau,2\tau-1} \geq l(p-1) \geq p-1$$

implies $N_1 \geq (p-1)\sum_{\epsilon\in I_1}\delta_\epsilon$. Set $\theta = \sum_{\epsilon\in I_1}\delta_\epsilon$ and note that $\theta \leq r$. Now we consider the following possibilities:

Case 1. If $\vartheta = r$, then $L_3 = M_3 = N_4 = 0$ and therefore

$$\prod_{i=1}^{2r} x_{ii}^{p-1} \prod_{i=n+1}^{m} x_{i1}^{p-1} = \prod_{\epsilon\in I_1}\left(\prod_{i=n+1}^{m} x_{i1}^{s_{i1}} \prod_{\tau=1}^{r} x_{2\tau-1,2\tau-1}^{s^{(\epsilon)}_{2\tau-1,2\tau-1}} x_{2\tau,2\tau}^{s^{(\epsilon)}_{2\tau,2\tau-1}}\right)^{\tau_\mu}.$$

Comparing total degrees of both sides of the last equality and taking into account that

$$\deg S^{(0)}_H(f'_\epsilon) < \frac{(m-n+2r)(p-1)}{r}$$

we obtain $(m-n+2r)(p-1) < (m-n+2r)(p-1)$. This yields a contradiction.

Case 2. Let $\vartheta < r$. Since

$$L_1 + L_3 + M_1 + M_3 + N_1 = (m-n+r)(p-1) + N_1,$$
$$L_3 + M_3 \le r(p-1) - N_1, \quad N_1 \ge \theta(p-1)$$

and since by assumption,

$$L_1 + M_1 + N_1 < \theta \frac{(m-n+2r)(p-1)}{r},$$

then

$$(m-n+r)(p-1) + N_1 < \theta \frac{(m-n+2r)(p-1)}{r} + M_1 + M_3.$$

In that case,

$$(m-n+r)(p-1) < \theta \frac{(m-n+r)(p-1)}{r} + (r-\theta)(p-1)$$

and hence $(r-\theta)(m-n+r)(p-1) < (r-\theta)r(p-1)$. Since $m \ge n$, we arrive at a contradiction, which completes the proof of Theorem 3.

References

1. Campbell, H.E.A., Hughes, I., Pollack, R.D.: Vector invariants of symmetric groups. *Can. Math. Bull.* **33**, 391–397 (1990)
2. Campbell, H.E.A., Hughes, I.P.: Vector invariants of $U_2(F_p)$: a proof of a conjecture of Richman. *Adv. Math.* **126**, 1–20 (1997)
3. Fleischmann, P.: A new degree bound for the vector invariants of symmetric groups. *Trans. Am. Math. Soc.* **350**, 1703–1712 (1998)
4. Fleischmann, P.: The Noether bound in invariant theory of finite groups. *Adv. Math.* **156**, 23–32 (2000)
5. Hilbert, D.: Über die vollen Invariantensysteme. *Math. Ann.* **42**, 313–373 (1893)
6. Kemper, G.: Lower degree bounds for modular invariants and a question of I. Hughes. *Transform. Groups* **3**, 135–144 (1998)
7. Noether, E.: Der Endlichkeitssatz der Invarianten endlicher Gruppen. *Math. Ann.* **77**, 89–92 (1916)
8. Noether, E.: Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Characteristik p. *Nachr. Ges. Wiss. Göttingen* **1926**, 28–35 (1926)
9. Richman, D.: On vector invariants over finite fields. *Adv. Math.* **81**, 30–65 (1990)
10. Richman, D.: Invariants of finite groups over fields of characteristic p. *Adv. Math.* **124**, 25–48 (1996)
11. Smith, L.: *Polynomial Invariants of Finite Groups*. A.K. Peters, Wellesley (1995)
12. Stepanov, S.A.: Vector invariants of symmetric groups in prime characteristic. *Discrete Math. Appl.* **10**, 455–468 (2000)
13. Weyl, H.: *The Classical Groups*, 2nd edn. Princeton University Press, Princeton (1953)