Mathematics

https://www.aimspress.com/journal/Math

AIMS Mathematics, 9(9): 25603–25618.
DOI: 10.3934/math.20241250
Received: 11 July 2024
Revised: 24 August 2024
Accepted: 28 August 2024
Published: 03 September 2024

Research article

Separating invariants for certain representations of the elementary Abelian p-groups of rank two

Panpan Jia*, Jizhu Nan and Yongsheng Ma

School of Mathematical Sciences, Dalian University of Technology, Dalian 116024, China

* **Correspondence:** Email: jiapanpan1993@163.com.

Abstract: For a finite group acting linearly on a vector space, a separating set is a subset of the invariant ring that separates the orbits. In this paper, we determined explicit separating sets in the corresponding rings of invariants for four families of finite dimensional representations of the elementary abelian p-groups $(\mathbb{Z}/p)^2$ of rank two over an algebraically closed field of characteristic p, where p is an odd prime. Our construction was recursive. The separating sets consisted only of transfers and norms, and the size of every separating set depended only on the dimension of the representation.

Keywords: elementary abelian p-group; invariant theory; separating invariants
Mathematics Subject Classification: 13A50

1. Introduction

Let $\rho : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a faithful representation of a finite group G over a field $\mathbb{F}$ of arbitrary characteristic. Denote by $V = \mathbb{F}^n$ the n dimensional representation space over $\mathbb{F}$. We write $\mathbb{F}[V]$ for the symmetric algebra $S(V^*)$ over the dual space V^*. The action of G on V induces an action on $\mathbb{F}[V]$: for $f \in \mathbb{F}[V]$ and $\boldsymbol{v} \in V$, the action of $g \in G$ is given by $(g(f))(\boldsymbol{v}) = f(g^{-1}(\boldsymbol{v}))$. The ring of invariants $\mathbb{F}[V]^G$ is defined by

$$\mathbb{F}[V]^G := \{f \in \mathbb{F}[V] \mid g(f) = f \ for\ all\ g \in G\}.$$

Here are some general methods to construct invariants of finite groups. Let $f \in \mathbb{F}[V]$, then the transfer of f is defined by

$$\mathrm{Tr}^G(f) := \sum_{g \in G} g(f).$$

Let $H \leq G$ be a subgroup. Then the relative transfer is defined as

$$\mathrm{Tr}^G_H : \mathbb{F}[V]^H \to \mathbb{F}[V]^G,\ f \mapsto \sum_{gH \in G/H} g(f),$$

where G/H denotes a set of left coset representatives of H in G. Tr^G_H is independent of the choice of the coset representatives. The norm of f is defined by

$$\mathrm{N}^G(f) := \prod_{g\in G} g(f).$$

Note that the transfer, relative transfer and norm are invariant polynomials. If the characteristic of $\mathbb{F}$ divides the group order $|G|$, we speak of the modular case. Otherwise, we are in the nonmodular case, which includes $\mathrm{char}(\mathbb{F}) = 0$.

Separating orbits of a group action on some geometric or algebraic space is likely to have been one of the original motivations of invariant theory. It has regained particular attention following the influential textbook of Derksen and Kemper [1]. Since then, separating invariants have been extensively studied within the last decade.

Definition 1. *A subset $S \subseteq \mathbb{F}[V]^G$ is said to be separating if for any two points $\mathbf{v}, \mathbf{v}' \in V$, we have: If there exists an invariant $f \in \mathbb{F}[V]^G$ with $f(\mathbf{v}) \neq f(\mathbf{v}')$, then there exists an element $h \in S$ with $h(\mathbf{v}) \neq h(\mathbf{v}')$.*

If G is finite, then for $\boldsymbol{v}, \boldsymbol{v}' \in V$ with distinct G-orbits, there exists $f \in \mathbb{F}[V]^G$ such that $f(\boldsymbol{v}) \neq f(\boldsymbol{v}')$. It follows that a subset $S \subseteq \mathbb{F}[V]^G$ is separating if any two G-orbits can be separated by invariants from S for any finite group [2]. While the ring of invariants forms a separating set, computing the ring of invariants for a modular representation is typically a difficult problem. Moreover, separating invariants are better behaved than generating ones. For instance, the Noether degree bound and Weyl theorem hold for separating invariants without any hypothesis on $\mathrm{char}(\mathbb{F})$, see [2, 3]. In [4], Dufresne introduced a geometric notion of separating algebra and gave two geometric formulations of this notion. Geometric separating sets and separating invariants over finite fields were considered in [5, 6]. For more background on separating invariants we direct readers to [7–13].

In the study of explicit separating invariants, it is natural to take p-groups as a starting point. The work of Sezer [14] gives us a good understanding in the case of the cyclic group of order p. Since then, explicit separating invariants have also been calculated for various groups such as cyclic p-groups, the Klein four group, etc [15–19]. The next step is to look at elementary abelian p-groups. With a few notable exceptions, the modular representation theory of an elementary abelian p-group is wild, see for example [20, Theorem 4.4.4]. In the modular case, the degrees of the generators can become arbitrarily big. Therefore, computing the invariants of elementary abelian p-groups in the modular case is particularly difficult and explicit generating sets are available only for a handful of cases. The ring of invariants for all two dimensional representations of $(\mathbb{Z}/p)^r$ and the ring of invariants for all three dimensional representations of $(\mathbb{Z}/p)^2$ have been worked out in [21]. See also [22] for further research. Four families of finite dimensional representations of $(\mathbb{Z}/p)^2$ over an algebraically closed field $\mathbb{F}$ of characteristic p, where p is an odd prime, is given in [23] and their invariant rings have not been computed. In this paper, we give explicit separating sets, including transfers and norms for each representation. Transfers and norms are basic invariants that are easier to obtain. These invariants usually do not suffice to generate the entire ring of invariants $\mathbb{F}[V]^G$ in the modular case. Since the dual of a subrepresentation sits in the dual of higher dimensional representation of $(\mathbb{Z}/p)^2$, this allows us to reduce the problem to separating two points whose coordinates are all the same except a few coordinates. Consequently, we show that the separating set for a representation of $(\mathbb{Z}/p)^2$ can be obtained by adding some transfers and norms to any separating set for the subrepresentation. It is worth pointing out that the size of the separating set depends only on the dimension of the representation. Our work can be viewed as the generalization of the Klein four group (the elementary abelian 2-groups of rank two) [17] to the elementary abelian p-groups of rank two for arbitrary odd prime p. However, the latter case needs more complicated computation and additional separating invariants.

2. Constructing separating invariants

Let $G = \langle\sigma_1, \sigma_2\rangle \cong (\mathbb{Z}/p)^2$ be the elementary abelian p-group of rank two of order p^2, where p is an odd prime. Let $\sigma_3 = \sigma_1\sigma_2$ and H_i denote the subgroup of G which is generated by σ_i for $1 \leq i \leq 3$. The complete list of indecomposable representations of the Klein four group is described in [20, Theorem 4.3.3]. However, the modular representation theory of an elementary abelian p-group of rank two is wild. Here, we study the natural generalization of the irreducible representations of the Klein four group. There are four families of finite dimensional representations of G over an algebraically closed field $\mathbb{F}$ of characteristic odd prime p, which are given in [23]. For each representation in each family, we construct a finite separating set recursively. In the following, I_n denotes the $n \times n$ identity matrix and for any element λ of the field $\mathbb{F}$, J_λ denotes the $n \times n$ Jordan block (lower triangular) with eigenvalues λ.

Type (I) For every even dimension $2n$ there are representations $V_{2n,\lambda}$,

$$\sigma_1 \mapsto \begin{pmatrix} I_n & 0 \\ I_n & I_n \end{pmatrix},$$

$$\sigma_2 \mapsto \begin{pmatrix} I_n & 0 \\ J_\lambda & I_n \end{pmatrix}.$$

Type (II) For every even dimension $2n$ there are representations $V_{2n,\infty}$,

$$\sigma_1 \mapsto \begin{pmatrix} I_n & 0 \\ J_0 & I_n \end{pmatrix},$$

$$\sigma_2 \mapsto \begin{pmatrix} I_n & 0 \\ I_n & I_n \end{pmatrix}.$$

Type (III) For every odd dimension $2n-1$ there are representations $V_{-(2n-1)}$,

$$\sigma_1 \mapsto \begin{pmatrix} I_{n-1} & 0 \\ I_{n-1} & \\ 0_{1\times(n-1)} & I_n \end{pmatrix},$$

$$\sigma_3 \mapsto \begin{pmatrix} I_{n-1} & 0 \\ 0_{1\times(n-1)} & \\ I_{n-1} & I_n \end{pmatrix}.$$

Type (IV) For every odd dimension $2n-1$ there are representations V_{2n-1},

$$\sigma_1 \mapsto \begin{pmatrix} I_n & & 0 \\ 0_{(n-1)\times 1} & I_{n-1} & I_{n-1} \end{pmatrix},$$

$$\sigma_3 \mapsto \begin{pmatrix} \multicolumn{2}{c}{I_n} & 0 \\ I_{n-1} & 0_{(n-1)\times 1} & I_{n-1} \end{pmatrix}.$$

Notice that the matrix group associated with $V_{2n,\infty}$ in type (II) is the same as the matrix group associated with $V_{2n,0}$ in type (I). Therefore, their invariant rings are equal, and a separating set for $V_{2n,0}$ is also a separating set for $V_{2n,\infty}$. Each representation $V_{-(2n-1)}$ in type (III) is isomorphic to a subrepresentation of $V_{2n,p-1}$ in type (I), which we will explain in detail later. So we study the separating sets for types (I) − (III) in Subsection 2.1 and for type (IV) in Subsection 2.2.

2.1. Separating invariants for types (I)–(III)

We start with the action of G on the representation space $V_{2n,\lambda}$. Let $\boldsymbol{\varepsilon_1},\boldsymbol{\varepsilon_2},\cdots,\boldsymbol{\varepsilon_n}$, $\boldsymbol{\xi_1},\boldsymbol{\xi_2},\cdots,\boldsymbol{\xi_n}$ be the basis for $V_{2n,\lambda}$ with $\sigma_1(\boldsymbol{\varepsilon_i}) = \boldsymbol{\varepsilon_i} + \boldsymbol{\xi_i}$, $\sigma_1(\boldsymbol{\xi_i}) = \boldsymbol{\xi_i}$, $\sigma_2(\boldsymbol{\xi_i}) = \boldsymbol{\xi_i}$ for $1 \leq i \leq n$, $\sigma_2(\boldsymbol{\varepsilon_n}) = \boldsymbol{\varepsilon_n} + \lambda\boldsymbol{\xi_n}$ and $\sigma_2(\boldsymbol{\varepsilon_i}) = \boldsymbol{\varepsilon_i} + \lambda\boldsymbol{\xi_i} + \boldsymbol{\xi_{i+1}}$ for $1 \leq i \leq n-1$. We identify each $\boldsymbol{\varepsilon_i}$ with the column vector with 1 on the i-th coordinate and zero elsewhere, and each $\boldsymbol{\xi_i}$ with the column vector with 1 on the $(n+i)$-th coordinate and zero elsewhere. Let $x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n$ denote the corresponding elements in the dual space $V^*_{2n,\lambda}$. In fact, $x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n$ form the basis for $V^*_{2n,\lambda}$ in the reverse order: we have $\sigma_1^{-1}(x_i) = x_i$, $\sigma_1^{-1}(y_i) = x_i + y_i$, $\sigma_2^{-1}(x_i) = x_i$ for $1 \leq i \leq n$, $\sigma_2^{-1}(y_1) = \lambda x_1 + y_1$ and $\sigma_2^{-1}(y_i) = x_{i-1} + \lambda x_i + y_i$ for $2 \leq i \leq n$. For simplicity we will use the generators σ_i^{-1} instead of σ_i for the rest of the paper and change the notation by writing σ_i for the new generators for $1 \leq i \leq 3$. Note also that $\mathbb{F}[V_{2n,\lambda}] = \mathbb{F}[x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n]$. Pick a point $\boldsymbol{v} = (v_1, v_2, \cdots, v_n, w_1, w_2, \cdots, w_n)$ in $V_{2n,\lambda}$. The surjection $\varphi : V_{2n,\lambda} \to V_{2n-2,\lambda}$ given by $(v_1, v_2, \cdots, v_n, w_1, w_2, \cdots, w_n) \mapsto (v_1, v_2, \cdots, v_{n-1}, w_1, w_2, \cdots, w_{n-1})$ is G-equivariant, as for $g \in G$, $\boldsymbol{v} \in V_{2n,\lambda}$, $g(\varphi(\boldsymbol{v})) = \varphi(g(\boldsymbol{v}))$. Dual to this surjection, the subspace in $V^*_{2n,\lambda}$ generated by $x_1, x_2, \cdots, x_{n-1}, y_1, y_2, \cdots, y_{n-1}$ is closed under the G-action and isomorphic to $V^*_{2n-2,\lambda}$. Hence $\mathbb{F}[V_{2n-2,\lambda}] = \mathbb{F}[x_1, x_2, \cdots, x_{n-1}, y_1, y_2, \cdots, y_{n-1}]$ is a subalgebra in $\mathbb{F}[V_{2n,\lambda}]$.

The following three lemmas are very useful in studying the image of the transfer for modular groups. We will use these formulas repeatedly in the proofs of Lemmas 4–6.

Lemma 1. *Let k be a positive integer. Then $\sum_{0\leq l\leq p-1} l^k \equiv -1$ mod p if $p-1$ divides k and $\sum_{0\leq l\leq p-1} l^k \equiv 0$ mod p, otherwise.*

Proof. See [24, Lemma 9.0.2] for a proof for this statement. □

Lemma 2. *Let k and l be positive integers such that $0 \leq k \leq p-1$, $k \leq l \leq p-1$. There holds*

$$\binom{k}{0}\binom{p-(k+1)}{l-k} + \binom{k+1}{1}\binom{p-(k+2)}{l-(k+1)} + \cdots + \binom{l}{l-k}\binom{p-(l+1)}{0} = \binom{p}{l-k}.$$

Proof. This statement can be proved by induction on k and l and we omit the detailed proof. □

Lemma 3. *(1) Let k be a positive integer such that $1 \leq k \leq p$. Then*

$$\binom{(p+1)(p-1)}{k(p-1)} \equiv 1 \ mod\ p.$$

(2) Let l and k be a positive integer such that $2 \leq l \leq p$ and $1 \leq k \leq l-1$. Then

$$\binom{l(p-1)}{k(p-1)} \equiv 0 \ mod\ p.$$

Proof. It is a simple matter to prove the two identities above by the definition of binomial coefficient. □

From now on all congruences are modulo $\mathbb{F}[x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_{n-1}]$ in Subsection 2.1. The congruences of separating invariants in the following two lemmas will play an important part in the proof of Theorem 1.

Lemma 4. *(1)* $\mathrm{Tr}^G(y_i^{p-1}y_j^{p-1}y_n) \equiv (x_{i-1}x_j - x_ix_{j-1})^{p-1}y_n$ *for* $2 \leq i, j \leq n-1$.
(2) $\mathrm{Tr}^G(y_1^{p-1}y_2^{p-1}y_n) \equiv x_1^{2(p-1)}y_n$.

Proof. Here we only prove for (1). It is easy to verify that $\mathrm{Tr}^G = \mathrm{Tr}^G_H \circ \mathrm{Tr}^H$ for any subgroup H of G. This suggest that we may compute Tr^G by first computing Tr^H and then computing Tr^G_H. Thus we may work with the two smaller groups H and G/H.

By the definition of transfer we have

$$\begin{aligned}
\mathrm{Tr}^{H_1}(y_i^{p-1}y_j^{p-1}y_n) &= \sum_{0\leq l\leq p-1} (lx_i + y_i)^{p-1}(lx_j + y_j)^{p-1}(lx_n + y_n) \\
&\equiv \sum_{0\leq l\leq p-1} (lx_i + y_i)^{p-1}(lx_j + y_j)^{p-1}y_n \\
&\equiv \sum_{0\leq l\leq p-1} \sum_{0\leq s,t\leq p-1} \binom{p-1}{s}\binom{p-1}{t}(lx_i)^s y_i^{p-1-s}(lx_j)^{p-1-t}y_j^t y_n \\
&\equiv \sum_{0\leq l\leq p-1} \sum_{0\leq s,t\leq p-1} \binom{p-1}{s}\binom{p-1}{t} l^{p-1+s-t}x_i^s x_j^{p-1-t} y_i^{p-1-s} y_j^t y_n.
\end{aligned}$$

By Lemma 1, we see that

$$\begin{aligned}
\mathrm{Tr}^{H_1}(y_i^{p-1}y_j^{p-1}y_n) &\equiv \sum_{0\leq l\leq p-1} \sum_{0\leq k\leq p-1} \binom{p-1}{k}^2 l^{p-1}x_i^k x_j^{p-1-k} y_i^{p-1-k} y_j^k y_n \\
&\equiv \sum_{0\leq l\leq p-1} l^{p-1}\Big(\sum_{0\leq k\leq p-1} \binom{p-1}{k}^2 x_i^k x_j^{p-1-k} y_i^{p-1-k} y_j^k y_n\Big) \\
&\equiv -\sum_{0\leq k\leq p-1} x_i^k x_j^{p-1-k} y_i^{p-1-k} y_j^k y_n.
\end{aligned}$$

The last congruence follows since $\binom{p-1}{k}^2 \equiv 1 \bmod p$. Similarly, for each k with $0 \leq k \leq p-1$ we have

$$\begin{aligned}
\mathrm{Tr}^{H_2}(x_i^k x_j^{p-1-k} y_i^{p-1-k} y_j^k y_n) &= \sum_{0\leq l\leq p-1} x_i^k x_j^{p-1-k}(lx_{i-1} + l\lambda x_i + y_i)^{p-1-k}(lx_{j-1} + l\lambda x_j + y_j)^k(lx_{n-1} + l\lambda x_n + y_n) \\
&\equiv \sum_{0\leq l\leq p-1} x_i^k x_j^{p-1-k}(lx_{i-1} + l\lambda x_i + y_i)^{p-1-k}(lx_{j-1} + l\lambda x_j + y_j)^k y_n \\
&\equiv -x_i^k x_j^{p-1-k}(x_{i-1} + \lambda x_i)^{p-1-k}(x_{j-1} + \lambda x_j)^k y_n.
\end{aligned}$$

Thus

$$\mathrm{Tr}^G(y_i^{p-1}y_j^{p-1}y_n) = \mathrm{Tr}^G_{H_1}(\mathrm{Tr}^{H_1}(y_i^{p-1}y_j^{p-1}y_n))$$

$$
\begin{aligned}
&\equiv \mathrm{Tr}^G_{H_1}(-\sum_{0\le k\le p-1} x_i^k x_j^{p-1-k} y_i^{p-1-k} y_j^k y_n)\\
&\equiv \sum_{0\le k\le p-1} x_i^k x_j^{p-1-k}(x_{i-1}+\lambda x_i)^{p-1-k}(x_{j-1}+\lambda x_j)^k y_n\\
&= \sum_{0\le k\le p-1}\ \sum_{0\le s\le p-1-k}\ \sum_{0\le t\le k} \binom{p-1-k}{s}\binom{k}{t}\lambda^{s+t} x_{i-1}^{p-1-k-s} x_i^{k+s} x_{j-1}^{k-t} x_j^{p-1-k+t} y_n.
\end{aligned}
$$

It follows from Lemma 2 that the coefficient of $x_{i-1}^{p-1-l}x_i^l x_{j-1}^{m-1}x_j^{p-m}y_n$ is

$$
\begin{aligned}
&\lambda^{l-m+1}\left(\binom{m-1}{0}\binom{p-m}{l-(m-1)}+\binom{m}{1}\binom{p-(m+1)}{l-m}+\cdots+\binom{l}{l-(m-1)}\binom{p-(l+1)}{0}\right)\\
=&\lambda^{l-m+1}\binom{p}{l-(m-1)}.
\end{aligned}
$$

Moreover, $\binom{p}{l-(m-1)}\equiv 1 \bmod p$ if $l=m-1$ and $\binom{p}{l-(m-1)}\equiv 0 \bmod p$, otherwise. From the above it follows that

$$
\begin{aligned}
\mathrm{Tr}^G(y_i^{p-1}y_j^{p-1}y_n) \equiv& \sum_{0\le k\le p-1}\ \sum_{0\le s\le p-1-k}\ \sum_{0\le t\le k}\binom{p-1-k}{s}\binom{k}{t}\lambda^{s+t}x_{i-1}^{p-1-k-s}x_i^{k+s}x_{j-1}^{k-t}x_j^{p-1-k+t}y_n\\
=&(x_{i-1}^{p-1}x_j^{p-1}+x_{i-1}^{p-2}x_i x_{j-1}x_j^{p-2}+\cdots+x_i^{p-1}x_{j-1}^{p-1})y_n\\
=&(x_{i-1}x_j-x_ix_{j-1})^{p-1}y_n.
\end{aligned}
$$

□

Lemma 5. *(1)* $\mathrm{Tr}^G(y_{n-1}^{(p+1)(p-1)}y_n)\equiv\sum_{1\le k\le p}(x_{n-2}+\lambda x_{n-1})^{(p+1-k)(p-1)}x_{n-1}^{k(p-1)}y_n$.
(2) $\mathrm{N}^{H_3}(x_{n-1}y_n-x_ny_{n-1})\equiv x_{n-1}^p y_n^p - x_{n-1}(x_{n-1}^2-x_{n-2}x_n)^{p-1}y_n$.

Proof. (1) By the definition of transfer, we have

$$
\begin{aligned}
\mathrm{Tr}^{H_1}(y_{n-1}^{(p+1)(p-1)}y_n) &= \sum_{0\le l\le p-1}(lx_{n-1}+y_{n-1})^{(p+1)(p-1)}(lx_n+y_n)\\
&\equiv \sum_{0\le l\le p-1}(lx_{n-1}+y_{n-1})^{(p+1)(p-1)}y_n.
\end{aligned}
$$

By Lemma 1 and Lemma 3(1) we see that

$$
\begin{aligned}
\mathrm{Tr}^{H_1}(y_{n-1}^{(p+1)(p-1)}y_n) &\equiv \sum_{0\le l\le p-1}\ \sum_{0\le k\le p+1}\binom{(p+1)(p-1)}{k(p-1)}l^{k(p-1)}x_{n-1}^{k(p-1)}y_{n-1}^{(p+1-k)(p-1)}y_n\\
&\equiv -\sum_{1\le k\le p+1}x_{n-1}^{k(p-1)}y_{n-1}^{(p+1-k)(p-1)}y_n.
\end{aligned}
$$

For each k with $1\le k\le p+1$,

$$
\mathrm{Tr}^{H_2}(x_{n-1}^{k(p-1)}y_{n-1}^{(p+1-k)(p-1)}y_n) = \sum_{0\le l\le p-1}x_{n-1}^{k(p-1)}(lx_{n-2}+l\lambda x_{n-1}+y_{n-1})^{(p+1-k)(p-1)}(lx_{n-1}+l\lambda x_n+y_n)
$$

$$\equiv \sum_{0\le l\le p-1} x_{n-1}^{k(p-1)}(lx_{n-2}+l\lambda x_{n-1}+y_{n-1})^{(p+1-k)(p-1)}y_n.$$

By Lemma 1 and Lemma 3(1) we have

$$\mathrm{Tr}^{H_2}(x_{n-1}^{k(p-1)}y_{n-1}^{(p+1-k)(p-1)}y_n) \equiv \sum_{0\le l\le p-1}\sum_{0\le s\le p+1-k}\binom{(p+1-k)(p-1)}{s(p-1)} l^{s(p-1)}(x_{n-2}+\lambda x_{n-1})^{s(p-1)}x_{n-1}^{k(p-1)}y_{n-1}^{(p+1-k-s)(p-1)}y_n.$$

For $1 \le k \le p$, we see that $\binom{(p+1-k)(p-1)}{s(p-1)} \equiv 0 \bmod p$ unless $s = p+1-k$ by Lemma 3(2) in which case we have

$$\begin{aligned}\mathrm{Tr}^{H_2}(x_{n-1}^{k(p-1)}y_{n-1}^{(p+1-k)(p-1)}y_n) &\equiv \sum_{0\le l\le p-1} l^{(p+1-k)(p-1)}(x_{n-2}+\lambda x_{n-1})^{(p+1-k)(p-1)}x_{n-1}^{k(p-1)}y_n\\ &\equiv -(x_{n-2}+\lambda x_{n-1})^{(p+1-k)(p-1)}x_{n-1}^{k(p-1)}y_n.\end{aligned}$$

For $k = p+1$, $\mathrm{Tr}^{H_2}(x_{n-1}^{k(p-1)}y_{n-1}^{(p+1-k)(p-1)}y_n) \equiv \sum_{0\le l\le p-1} x_{n-1}^{(p+1-k)(p-1)}y_n \equiv 0$. Thus,

$$\begin{aligned}\mathrm{Tr}^{G}(y_{n-1}^{(p+1)(p-1)}y_n) =&\mathrm{Tr}^{G}_{H_1}(\mathrm{Tr}^{H_1}(y_{n-1}^{(p+1)(p-1)}y_n))\\ \equiv&\mathrm{Tr}^{G}_{H_1}(-\sum_{1\le k\le p+1} x_{n-1}^{k(p-1)}y_{n-1}^{(p+1-k)(p-1)}y_n)\\ \equiv&\sum_{1\le k\le p}(x_{n-2}+\lambda x_{n-1})^{(p+1-k)(p-1)}x_{n-1}^{k(p-1)}y_n.\end{aligned}$$

(2) Note that $x_{n-1}y_n - x_ny_{n-1}$ is σ_1-invariant, so the H_3-orbit product of this polynomial is G-invariant. Thus, we have

$$\begin{aligned}\mathrm{N}^{H_3}(x_{n-1}y_n - x_ny_{n-1}) =&\Pi_{0\le l\le p-1}(x_{n-1}(lx_{n-1}+(l\lambda+l)x_n+y_n) - x_n(lx_{n-2}+(l\lambda+l)x_{n-1}+y_{n-1}))\\ =&\Pi_{0\le l\le p-1}(l(x_{n-1}^2 - x_{n-2}x_n) + (x_{n-1}y_n - x_ny_{n-1}))\\ =&(x_{n-1}y_n - x_ny_{n-1})^p - (x_{n-1}y_n - x_ny_{n-1})(x_{n-1}^2 - x_{n-2}x_n)^{p-1}\\ \equiv&x_{n-1}^py_n^p - x_{n-1}(x_{n-1}^2 - x_{n-2}x_n)^{p-1}y_n.\end{aligned}$$

□

Theorem 1. *Let* $\mathbb{F}[V_{2n,\lambda}] = \mathbb{F}[x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n]$. *Then*

$$S_1 = \left\{x_1,\ f_\lambda = \begin{cases}\mathrm{N}^G(y_1) & for\ \lambda \notin \mathbb{F}_p,\\ \mathrm{N}^{H_1}(y_1) & for\ \lambda \in \mathbb{F}_p\end{cases}\right\}$$

is a separating set for $V_{2,\lambda}$. *And* $S_2 = S_1 \bigcup T_2$ *is a separating set for* $V_{4,\lambda}$, *where*

$$T_2 = \left\{x_2,\ \mathrm{N}^G(y_2),\ f_\lambda = \begin{cases}\mathrm{Tr}^G(y_1^{(p+1)(p-1)}y_2) & for\ \lambda \notin \mathbb{F}_p,\\ \mathrm{N}^{H_3}(x_1y_2 - x_2y_1) & for\ \lambda \in \mathbb{F}_p\end{cases}\right\}.$$

Let $n \ge 3$ *and* $S_{n-1} \subseteq \mathbb{F}[V_{2n-2,\lambda}]^G$ *be a separating set for* $V_{2n-2,\lambda}$. *Then* $S_n = S_{n-1} \bigcup T_n$ *is a separating set for* $V_{2n,\lambda}$, *where*

$$T_n = \Big\{x_n,\ \mathrm{N}^G(y_n),\ \mathrm{Tr}^G(y_i^{p-1}y_{i+1}^{p-1}y_n)\ for\ 2 \le i \le n-1,$$

$$f_\lambda = \begin{Bmatrix} \mathrm{Tr}^G(y_{n-1}^{(p+1)(p-1)}y_n) & for\ \lambda \notin \mathbb{F}_p, \\ \mathrm{N}^{H_3}(x_{n-1}y_n - x_ny_{n-1}) & for\ \lambda \in \mathbb{F}_p \end{Bmatrix}.$$

Moreover, a separating set for $V_{2n,0}$ is a separating set for $V_{2n,\infty}$.

Proof. The cases $V_{2,\lambda}$ and $V_{4,\lambda}$ are easy to check so we only prove the case of n. Consider any two points $\boldsymbol{v} = (v_1, \cdots, v_n, w_1, \cdots, w_n)$, $\boldsymbol{v}' = (v'_1, \cdots, v'_n, w'_1, \cdots, w'_n) \in V_{2n,\lambda}$ that do not lie in the same G-orbit, and suppose that $f(\boldsymbol{v}) = f(\boldsymbol{v}')$ for all $f \in S_n$. We will show that there exists $g \in G$ such that $\boldsymbol{v}' = g(\boldsymbol{v})$. This contradicts our assumption that $\boldsymbol{v}$ and $\boldsymbol{v}'$ do not lie in the same G-orbit and this contradiction shows that S_n is a separating set for $V_{2n,\lambda}$. We assume that every invariant in S_n takes the same value on $\boldsymbol{v}$ and $\boldsymbol{v}'$ from now on.

If $(v_1, \cdots, v_{n-1}, w_1, \cdots, w_{n-1})$, $(v'_1, \cdots, v'_{n-1}, w'_1, \cdots, w'_{n-1}) \in V_{2n-2,\lambda}$ do not lie in the same G-orbit, then there exists a polynomial in S_{n-1} that separates the two points because $S_{n-1} \subseteq \mathbb{F}[V_{2n-2,\lambda}]^G$ is separating. Therefore this polynomial separates $\boldsymbol{v}$ and $\boldsymbol{v}'$ as well. Hence by replacing $\boldsymbol{v}'$ with a suitable element in its G-orbit we may assume that $v'_i = v_i$ and $w'_i = w_i$ for $1 \le i \le n-1$. Since $x_n \in T_n$, we may assume that $v'_n = v_n$. Note that with this assumption we must have $w'_n \neq w_n$.

First, by Lemma 4(2), $\mathrm{Tr}^G(y_1^{p-1}y_2^{p-1}y_n)(\boldsymbol{v}) = \mathrm{Tr}^G(y_1^{p-1}y_2^{p-1}y_n)(\boldsymbol{v}')$ implies

$$\begin{aligned} 0 &= \mathrm{Tr}^G(y_1^{p-1}y_2^{p-1}y_n)(\boldsymbol{v}) - \mathrm{Tr}^G(y_1^{p-1}y_2^{p-1}y_n)(\boldsymbol{v}') \\ &= v_1^{2(p-1)}w_n - v_1^{2(p-1)}w'_n \\ &= v_1^{2(p-1)}(w_n - w'_n). \end{aligned}$$

As $w'_n \neq w_n$, we obtain

$$v_1 = 0.$$

Similarly, $\mathrm{Tr}^G(y_i^{p-1}y_{i+1}^{p-1}y_n)(\boldsymbol{v}) = \mathrm{Tr}^G(y_i^{p-1}y_{i+1}^{p-1}y_n)(\boldsymbol{v}')$ implies

$$\begin{aligned} 0 &= \mathrm{Tr}^G(y_i^{p-1}y_{i+1}^{p-1}y_n)(\boldsymbol{v}) - \mathrm{Tr}^G(y_i^{p-1}y_{i+1}^{p-1}y_n)(\boldsymbol{v}') \\ &= (v_{i-1}v_{i+1} - v_i^2)^{p-1}(w_n - w'_n) \end{aligned}$$

for $2 \le i \le n-2$ by setting $j = i+1$ in Lemma 4 (1). Since $v_1 = 0$ and $w'_n \neq w_n$, we get

$$v_2 = v_3 = \cdots = v_{n-2} = 0$$

successively. Since $v_{n-2} = 0$, $\mathrm{Tr}^G(y_{n-1}^{(p+1)(p-1)}y_n)(\boldsymbol{v}) = \mathrm{Tr}^G(y_{n-1}^{(p+1)(p-1)}y_n)(\boldsymbol{v}')$ implies

$$\begin{aligned} 0 &= \mathrm{Tr}^G(y_{n-1}^{(p+1)(p-1)}y_n)(\boldsymbol{v}) - \mathrm{Tr}^G(y_{n-1}^{(p+1)(p-1)}y_n)(\boldsymbol{v}') \\ &= \sum_{1\le k\le p} (v_{n-2}+\lambda v_{n-1})^{(p+1-k)(p-1)}v_{n-1}^{k(p-1)}(w_n - w'_n) \\ &= \sum_{1\le k\le p} \lambda^{(p+1-k)(p-1)}v_{n-1}^{(p+1)(p-1)}(w_n - w'_n) \\ &= (\lambda^{p-1}+\lambda^{2(p-1)}+\cdots+\lambda^{p(p-1)})v_{n-1}^{(p+1)(p-1)}(w_n - w'_n) \\ &= \lambda^{p-1}(\lambda^{p-1}-1)^{p-1}v_{n-1}^{(p+1)(p-1)}(w_n - w'_n) \end{aligned} \tag{2.1}$$

by Lemma 5(1). Notice that $\lambda^{p-1}(\lambda^{p-1}-1)^{p-1}=0$ if and only if $\lambda\in\mathbb{F}_p$, so the following proof falls into two parts depending on whether λ is in $\mathbb{F}_p$ or not.

If $\lambda\notin\mathbb{F}_p$, then we have

$$v_{n-1}=0$$

by (2.1). As $\mathrm{N}^G(y_n)=\prod_{0\le k,l\le p-1}(lx_{n-1}+(l\lambda+k)x_n+y_n)$, we have $\mathrm{N}^G(y_n)(\boldsymbol{v})=\prod_{0\le k,l\le p-1}((l\lambda+k)v_n+w_n)$. We define a polynomial

$$P(X):=\prod_{0\le k,l\le p-1}(X+(l\lambda+k)v_n)$$

in $\mathbb{F}[X]$. Notice that $\mathrm{N}^G(y_n)(\boldsymbol{v})=P(w_n)$ and that $P(w_n)=P(w_n+(l\lambda+k)v_n)$ for all $0\le k,l\le p-1$. Since $P(X)$ is a polynomial of degree p^2, it follows that $w_n+(l\lambda+k)v_n$ for $0\le k,l\le p-1$ are the only solutions of $P(X)-P(w_n)=0$. Therefore the equality of $\mathrm{N}^G(y_n)(\boldsymbol{v}')=P(w'_n)$ and $\mathrm{N}^G(y_n)(\boldsymbol{v})=P(w_n)$ implies w_n must be equal to $w'_n+(l\lambda+k)v_n$ for some $0\le k,l\le p-1$. Hence $\boldsymbol{v}'=\sigma_1^k\sigma_2^l(\boldsymbol{v})$. This is a contradiction because $\boldsymbol{v}$ and $\boldsymbol{v}'$ lie in the same G-orbit.

Next we turn to the case $\lambda\in\mathbb{F}_p$. Since $v_{n-2}=0$, then $\mathrm{N}^{H_3}(x_{n-1}y_n-x_ny_{n-1})$ taking the same value on $\boldsymbol{v},\boldsymbol{v}'$ implies

$$\begin{aligned}0&=\mathrm{N}^{H_3}(x_{n-1}y_n-x_ny_{n-1})(\boldsymbol{v})-\mathrm{N}^{H_3}(x_{n-1}y_n-x_ny_{n-1})(\boldsymbol{v}')\\&=(v_{n-1}^pw_n^p-v_{n-1}^{2p-1}w_n)-(v_{n-1}^pw'^p_n-v_{n-1}^{2p-1}w'_n)\\&=v_{n-1}^p(w_n-w'_n)((w_n-w'_n)^{p-1}-v_{n-1}^{p-1})\end{aligned}$$

by Lemma 5(2). If $v_{n-1}\neq0$, then we have $(w_n-w'_n)^{p-1}-v_{n-1}^{p-1}=0$, i.e. $(w_n-w'_n)^{p-1}=v_{n-1}^{p-1}$, i.e. $w_n-w'_n=lv_{n-1}$ for some $1\le l\le p-1$. There must exist k with $0\le k\le p-1$ such that $l\lambda+k=0$. Hence $\boldsymbol{v}'=\sigma_1^k\sigma_2^l(\boldsymbol{v})$. This is a contradiction. So now assume $v_{n-1}=0$. Then $\mathrm{N}^G(y_n)(\boldsymbol{v})=\mathrm{N}^G(y_n)(\boldsymbol{v}')$ implies $(\prod_{0\le l\le p-1}(lv_n+w_n))^p=(\prod_{0\le l\le p-1}(lv_n+w'_n))^p$. Thus $0=(\prod_{0\le l\le p-1}(lv_n+w_n))^p-(\prod_{0\le l\le p-1}(lv_n+w'_n))^p=(\prod_{0\le l\le p-1}(lv_n+w_n)-\prod_{0\le l\le p-1}(lv_n+w'_n))^p$ and therefore $w_n=w'_n+kv_n$ for some $1\le k\le p-1$. Hence $\boldsymbol{v}'=\sigma_1^k(\boldsymbol{v})$. This is also a contradiction.

The final statement follows because the matrix group associated with $V_{2n,\infty}$ is the same as the matrix group associated with $V_{2n,0}$, so their invariant rings are equal, and a separating set for $V_{2n,0}$ is also a separating set for $V_{2n,\infty}$. □

Remark 1. *From the proof of Theorem 1, we see that the separating set for each representation $V_{2n,\lambda}$ we obtained is minimal. Moreover, the size of separating set for $V_{2n,\lambda}$ is $\frac{n(n+3)}{2}$, which only depends on the dimension of the representation. Nevertheless, the maximal degree of an invariant in this set is the group order p^2.*

Since $V_{-(2n-1)}$ is isomorphic to the submodule of $V_{2n,p-1}$ spanned by $\boldsymbol{\varepsilon_1},\cdots,\boldsymbol{\varepsilon_{n-1}}$, $\boldsymbol{\xi_1},\cdots,\boldsymbol{\xi_n}$, where $\boldsymbol{\varepsilon_1},\cdots,\boldsymbol{\varepsilon_n}$, $\boldsymbol{\xi_1},\cdots,\boldsymbol{\xi_n}$ is the basis for $V_{2n,p-1}$. Dual to this inclusion, there is a restriction map $\mathbb{F}[V_{2n,p-1}]^G\to\mathbb{F}[V_{-(2n-1)}]^G$, $f\mapsto f|_{V_{-(2n-1)}}$ which sends separating sets to separating sets by [1, Theorem 2.4.9]. Therefore, in view of Theorem 1, we have the following statement.

Corollary 1. *Let*

$$\mathbb{F}[V_{2n,p-1}]=\mathbb{F}[x_1,x_2,\cdots,x_n,y_1,y_2,\cdots,y_n]$$

and

$$\mathbb{F}[V_{-(2n-1)}]=\mathbb{F}[x_1,x_2,\cdots,x_{n-1},y_1,y_2,\cdots,y_n].$$

Then

$$T_1 = \{y_1\}$$

is a separating set for V_{-1}. Additionally,

$$T_2 = \{x_1,\ \mathrm{N}^{H_1}(y_1),\ \mathrm{N}^{H_3}(y_2)\}$$

is a separating set for V_{-3}. Let $n \geq 3$ and $S_{n-1} \subseteq \mathbb{F}[V_{2n-2,p-1}]^G$ be a separating set for $V_{2n-2,p-1}$. Then the polynomials in $S_n = S_{n-1} \bigcup T_n$ restricted to $V_{-(2n-1)}$ form a separating set for $V_{-(2n-1)}$, where

$$T_n = \{\mathrm{N}^G(y_n),\ \mathrm{N}^{H_3}(x_{n-1}y_n - x_n y_{n-1}),\ \mathrm{Tr}^G(y_i^{p-1}y_{i+1}^{p-1}y_n)\ \textit{for}\ 2 \leq i \leq n-1\}.$$

2.2. *Separating sets for type* (*IV*)

We consider type (I) representations $V_{2n,p-1}$. In view of $\langle \boldsymbol{\xi_1} \rangle \subset V_{2n,p-1}$ is a G-submodule, we have $V_{2n-1} \cong V_{2n,p-1}/\langle \boldsymbol{\xi_1} \rangle$ with basis $\tilde{\boldsymbol{\varepsilon}}_i := \boldsymbol{\varepsilon}_i + \langle \boldsymbol{\xi_1} \rangle$ for $1 \leq i \leq n$, $\tilde{\boldsymbol{\xi}}_i := \boldsymbol{\xi}_i + \langle \boldsymbol{\xi_1} \rangle$ for $2 \leq i \leq n$, and a G-algebra inclusion $\mathbb{F}[V_{2n-1}] = \mathbb{F}[x_1, \cdots, x_n, y_2, \cdots, y_n] \subset \mathbb{F}[V_{2n,p-1}]$. The action of σ_1 and σ_3 on the variables are given by

$$\begin{cases} \sigma_1(x_i) = x_i\ \textit{for}\ 1 \leq i \leq n-1, \\ \sigma_1(y_i) = x_i + y_i\ \textit{for}\ 2 \leq i \leq n \end{cases}$$

and

$$\begin{cases} \sigma_3(x_i) = x_i\ \textit{for}\ 1 \leq i \leq n-1, \\ \sigma_3(y_i) = x_{i-1} + y_i\ \textit{for}\ 2 \leq i \leq n. \end{cases}$$

Pick a point $(v_1, \cdots, v_n, w_2, \cdots, w_n)$ in V_{2n-1}. There is a G-equivariant surjection $V_{2n-1} \to V_{2n-3}$ given by

$$(v_1, \cdots, v_n, w_2, \cdots, w_n) \mapsto (v_1, \cdots, v_{n-1}, w_2, \cdots, w_{n-1}).$$

Hence

$$\mathbb{F}[V_{2n-3}] = \mathbb{F}[x_1, \cdots, x_{n-1}, y_2, \cdots, y_{n-1}]$$

is a subalgebra in $\mathbb{F}[V_{2n-1}]$.

Note that all congruences are modulo $\mathbb{F}[x_1, \cdots, x_n, y_2, \cdots, y_{n-1}]$ in subsection 2.2.

Lemma 6. *(1)* $\mathrm{Tr}^G(y_i^{p-1}y_j^{p-1}y_n) \equiv (x_{i-1}x_j - x_i x_{j-1})^{p-1}y_n$ *for* $2 \leq i, j \leq n-1$.
(2) $\mathrm{Tr}^G(y_i^{(p+1)(p-1)}y_n) \equiv x_{i-1}^{p-1}x_i^{p-1}(x_{i-1}^{p-1} - x_i^{p-1})^{p-1}y_n$ *for* $2 \leq i \leq n-1$.
(3) $\mathrm{N}^{H_3}(x_{n-1}y_n - x_n y_{n-1}) \equiv x_{n-1}^p y_n^p - x_{n-1}(x_{n-1}^2 - x_{n-2}x_n)^{p-1}y_n$.
(4) $\mathrm{Tr}^G((y_i + \alpha y_{n-1})^{(p+1)(p-1)}y_n) \equiv (x_{i-1} + \alpha x_{n-2})^{p-1}(x_i + \alpha x_{n-1})^{p-1}((x_{i-1} + \alpha x_{n-2})^{p-1} - (x_i + \alpha x_{n-1})^{p-1})^{p-1}y_n$ *for every* $\alpha \in \mathbb{F}\backslash\mathbb{F}_p$ *and* $2 \leq i \leq n-2$.

Proof. The above congruences follow by the same methods as Lemmas 4 and 5. □

Theorem 2. *Let* $\mathbb{F}[V_{2n-1}] = \mathbb{F}[x_1, \cdots, x_n, y_2, \cdots, y_n]$. *Then* $S_1 = \{x_1\}$, $S_2 = \{x_1, x_2, \mathrm{N}^G(y_2)\}$ *and* $S_3 = S_2 \bigcup T_3$ *are separating sets for* V_1, V_3 *and* V_5 *respectively, where*

$$T_3 = \left\{x_3,\ \mathrm{N}^G(y_3),\ \mathrm{Tr}^G(y_2^{(p+1)(p-1)}y_3),\ \mathrm{N}^{H_3}(x_2y_3 - x_3y_2)\right\}.$$

Let $n \geq 4$ and $S_{n-1} \subseteq \mathbb{F}[V_{2n-3}]^G$ be a separating set for V_{2n-3}. Choose an element $\alpha \in \mathbb{F}$ with α not in the prime field $\mathbb{F}_p$. Then $S_n = S_{n-1} \bigcup T_n$ is a separating set for V_{2n-1}, where

$$\begin{aligned} T_n = \Big\{ & x_n,\ \mathrm{N}^G(y_n),\ \mathrm{N}^{H_3}(x_{n-1}y_n - x_ny_{n-1}),\ \mathrm{Tr}^G(y_2^{p-1}y_{n-1}^{p-1}y_n),\\ & \mathrm{Tr}^G(y_i^{p-1}y_{i+1}^{p-1}y_n)\ for\ 2 \leq i \leq n-2,\\ & \mathrm{Tr}^G(y_i^{(p+1)(p-1)}y_n)\ for\ 2 \leq i \leq n-1,\\ & \mathrm{Tr}^G((y_i + \alpha y_{n-1})^{(p+1)(p-1)}y_n)\ for\ 2 \leq i \leq n-2 \Big\}. \end{aligned}$$

Proof. We first prove the cases $n \geq 4$. Consider any two points $\boldsymbol{v} = (v_1, \cdots, v_n, w_2, \cdots, w_n)$, $\boldsymbol{v}' = (v_1', \cdots, v_n', w_2', \cdots, w_n') \in V_{2n-1}$ that do not lie in the same G-orbit, and suppose that $f(\boldsymbol{v}) = f(\boldsymbol{v}')$ for all $f \in S_n$. We show that there exists $g \in G$ such that $\boldsymbol{v}' = g(\boldsymbol{v})$. This contradicts our assumption that $\boldsymbol{v}$ and $\boldsymbol{v}'$ do not lie in the same G-orbit and this contradiction shows that S_n is a separating set for V_{2n-1}. We assume that every invariant in S_n takes the same value on $\boldsymbol{v}$ and $\boldsymbol{v}'$ from now on. We may assume that $v_i' = v_i$ for $1 \leq i \leq n$, $w_i' = w_i$ for $2 \leq i \leq n-1$ and $w_n' \neq w_n$ as the proof of Theorem 1.

Case 1. We assume that there exists $v_i = 0$ for $1 \leq i \leq n-1$ and let j be maximal with this property.

First, $\mathrm{Tr}^G(y_i^{p-1}y_{i+1}^{p-1}y_n)(\boldsymbol{v}) = \mathrm{Tr}^G(y_i^{p-1}y_{i+1}^{p-1}y_n)(\boldsymbol{v}')$ implies

$$\begin{aligned} 0 &= \mathrm{Tr}^G(y_i^{p-1}y_{i+1}^{p-1}y_n)(\boldsymbol{v}) - \mathrm{Tr}^G(y_i^{p-1}y_{i+1}^{p-1}y_n)(\boldsymbol{v}')\\ &= (v_{i-1}v_{i+1} - v_i^2)^{p-1}(w_n - w_n') \end{aligned}$$

for $1 \leq i \leq n-3$ by setting $j = i+1$ in Lemma 6(1). As $w_n' \neq w_n$, this suggests that: If $v_{i-1} = 0$, then $v_i = 0$ for $2 \leq i \leq n-2$. Therefore $j \geq n-2$.

If $j = n-2$, then $v_{n-1} \neq 0$. Again, $\mathrm{Tr}^G(y_i^{p-1}y_{i+1}^{p-1}y_n)(\boldsymbol{v}) = \mathrm{Tr}^G(y_i^{p-1}y_{i+1}^{p-1}y_n)(\boldsymbol{v}')$ implies $(v_{i-1}v_{i+1} - v_i^2)^{p-1}(w_n - w_n') = 0$ for $1 \leq i \leq n-3$. As $w_n' \neq w_n$, so the last equation suggests that: If $v_{i+1} = 0$, then $v_i = 0$ for $1 \leq i \leq n-3$. Since $v_{n-2} = 0$, we get

$$v_1 = v_2 = \cdots = v_{n-2} = 0$$

successively. However, $\mathrm{N}^{H_3}(x_{n-1}y_n - x_ny_{n-1})$ taking the same value on $\boldsymbol{v}, \boldsymbol{v}'$ implies

$$\begin{aligned} 0 &= \mathrm{N}^{H_3}(x_{n-1}y_n - x_ny_{n-1})(\boldsymbol{v}) - \mathrm{N}^{H_3}(x_{n-1}y_n - x_ny_{n-1})(\boldsymbol{v}')\\ &= (v_{n-1}^p w_n^p - v_{n-1}^{2p-1}w_n) - (v_{n-1}^p w'^p_n - v_{n-1}^{2p-1}w_n')\\ &= v_{n-1}^p(w_n - w_n')((w_n - w_n')^{p-1} - v_{n-1}^{p-1}) \end{aligned}$$

by Lemma 6(3). As $v_{n-1} \neq 0$ and $w_n' \neq w_n$, then we have $w_n = w_n' + lv_{n-1}$ for some $1 \leq l \leq p-1$. Hence $\boldsymbol{v}' = \sigma_1^l\sigma_2^l(\boldsymbol{v})$ which is a contradiction.

If $j = n-1$, namely $v_{n-1} = 0$. $\mathrm{Tr}^G(y_2^{p-1}y_{n-1}^{p-1}y_n)$ taking the same value on $\boldsymbol{v}$, $\boldsymbol{v}'$ implies

$$\begin{aligned} 0 &= \mathrm{Tr}^G(y_2^{p-1}y_{n-1}^{p-1}y_n)(\boldsymbol{v}) - \mathrm{Tr}^G(y_2^{p-1}y_{n-1}^{p-1}y_n)(\boldsymbol{v}')\\ &= v_2^{p-1}v_{n-2}^{p-1}(w_n - w_n') \end{aligned}$$

by setting $i = 2$, $j = n-2$ in Lemma 6(1). We have that $v_2 = 0$ or $v_{n-2} = 0$. Whether $v_2 = 0$ or $v_{n-2} = 0$, we have

$$v_1 = v_2 = \cdots = v_{n-2} = 0$$

successively by $\mathrm{Tr}^G(y_i^{p-1}y_{i+1}^{p-1}y_n)(\boldsymbol{v}) = \mathrm{Tr}^G(y_i^{p-1}y_{i+1}^{p-1}y_n)(\boldsymbol{v}')$ for $2 \le i \le n-2$. Furthermore, $\mathrm{N}^G(y_n)(\boldsymbol{v}) = \mathrm{N}^G(y_n)(\boldsymbol{v}')$ implies

$$\begin{aligned} 0 &= \mathrm{N}^G(y_n)(\boldsymbol{v}) - \mathrm{N}^G(y_n)(\boldsymbol{v}') \\ &= \Big(\prod_{0\le l,k\le p-1}(lv_{n-1} + (-l+k)v_n + w_n)\Big) - \Big(\prod_{0\le l,k\le p-1}(lv_{n-1} + (-l+k)v_n + w_n')\Big) \\ &= \Big(\prod_{0\le l,k\le p-1}((-l+k)v_n + w_n)\Big) - \Big(\prod_{0\le l,k\le p-1}((-l+k)v_n + w_n')\Big). \end{aligned}$$

Thus $w_n = w_n' + (-l+k)v_n$ for some $0 \le k, l \le p-1$. Hence $\boldsymbol{v}' = \sigma_1^k\sigma_2^l(\boldsymbol{v})$ which is also a contradiction.

Case 2. We assume that $v_i \ne 0$ for $1 \le i \le n-1$. Then $\mathrm{Tr}^G(y_i^{(p+1)(p-1)}y_n)(\boldsymbol{v}) = \mathrm{Tr}^G(y_i^{(p+1)(p-1)}y_n)(\boldsymbol{v}')$ implies

$$\begin{aligned} 0 &= \mathrm{Tr}^G(y_i^{(p+1)(p-1)}y_n)(\boldsymbol{v}) - \mathrm{Tr}^G(y_i^{(p+1)(p-1)}y_n)(\boldsymbol{v}') \\ &= v_{i-1}^{p-1}v_i^{p-1}(v_{i-1}^{p-1} - v_i^{p-1})^{p-1}w_n - v_{i-1}^{p-1}v_i^{p-1}(v_{i-1}^{p-1} - v_i^{p-1})^{p-1}w_n' \\ &= v_{i-1}^{p-1}v_i^{p-1}(v_{i-1}^{p-1} - v_i^{p-1})^{p-1}(w_n - w_n') \end{aligned}$$

for $2 \le i \le n-1$ by Lemma 6(2). So we have

$$v_1^{p-1} = v_2^{p-1} = \cdots = v_{n-1}^{p-1} \ne 0.$$

We claim that

$$\frac{v_i}{v_{i+1}} = \frac{v_{n-2}}{v_{n-1}} = \gamma \in \mathbb{F}_p^*$$

for $1 \le i \le n-3$. Given this, $\mathrm{N}^{H_3}(x_{n-1}y_n - x_ny_{n-1})$ taking the same value on $\boldsymbol{v}, \boldsymbol{v}'$ implies

$$\begin{aligned} 0 &= \mathrm{N}^{H_3}(x_{n-1}y_n - x_ny_{n-1})(\boldsymbol{v}) - \mathrm{N}^{H_3}(x_{n-1}y_n - x_ny_{n-1})(\boldsymbol{v}') \\ &= (v_{n-1}^p w_n^p - v_{n-1}(v_{n-1}^2 - v_{n-2}v_n)^{p-1}w_n) - (v_{n-1}^p {w'}_n^p - v_{n-1}(v_{n-1}^2 - v_{n-2}v_n)^{p-1}w_n') \\ &= (v_{n-1}^p w_n^p - v_{n-1}(v_{n-1}^2 - \gamma v_{n-1}v_n)^{p-1}w_n) - (v_{n-1}^p {w'}_n^p - v_{n-1}(v_{n-1}^2 - \gamma v_{n-1}v_n)^{p-1}w_n') \\ &= v_{n-1}^p(w_n - w_n')((w_n - w_n')^{p-1} - (v_{n-1} - \gamma v_n)^{p-1}) \end{aligned}$$

by Lemma 6(3). Thus, there exists some $1 \le l \le p-1$ such that $w_n - w_n' = lv_{n-1} - l\gamma v_n$. There must exist k with $0 \le k \le p-1$ such that $-l + k + l\gamma = 0$. Then $\boldsymbol{v}' = \sigma_1^k\sigma_2^l(\boldsymbol{v})$. This is a contradiction.

Now we prove for the claim. For $1 \le i \le n-2$, We define

$$\gamma_i := \frac{v_i}{v_{n-1}}.$$

It is obvious that $\gamma_i \in \mathbb{F}_p^*$. Because of $\mathrm{Tr}^G((y_i + \alpha y_{n-1})^{(p+1)(p-1)}y_n)(\boldsymbol{v}) = \mathrm{Tr}^G((y_i + \alpha y_{n-1})^{(p+1)(p-1)}y_n)(\boldsymbol{v}')$, we have that

$$\begin{aligned} 0 &= \mathrm{Tr}^G((y_i + \alpha y_{n-1})^{(p+1)(p-1)}y_n)(\boldsymbol{v}) - \mathrm{Tr}^G((y_i + \alpha y_{n-1})^{(p+1)(p-1)}y_n)(\boldsymbol{v}') \\ &= (v_{i-1} + \alpha v_{n-2})^{p-1}(v_i + \alpha v_{n-1})^{p-1}((v_{i-1} + \alpha v_{n-2})^{p-1} - (v_i + \alpha v_{n-1})^{p-1})^{p-1}w_n \\ &\quad - (v_{i-1} + \alpha v_{n-2})^{p-1}(v_i + \alpha v_{n-1})^{p-1}((v_{i-1} + \alpha v_{n-2})^{p-1} - (v_i + \alpha v_{n-1})^{p-1})^{p-1}w_n' \end{aligned}$$

$$= (v_{i-1}+\alpha v_{n-2})^{p-1}(v_i+\alpha v_{n-1})^{p-1}((v_{i-1}+\alpha v_{n-2})^{p-1}-(v_i+\alpha v_{n-1})^{p-1})^{p-1}(w_n - w'_n)$$

by Lemma 6(4). Since $v_1^{p-1} = v_2^{p-1} = \cdots = v_{n-1}^{p-1} \neq 0$ and $\alpha \in \mathbb{F}\backslash\mathbb{F}_p$, we have that $v_{i-1} + \alpha v_{n-2} \neq 0$ and $v_i + \alpha v_{n-1} \neq 0$. Since $w_n \neq w'_n$, we obtain that

$$(v_{i-1} + \alpha v_{n-2})^{p-1} - (v_i + \alpha v_{n-1})^{p-1} = 0. \tag{2.2}$$

Substituting $\gamma_i = \frac{v_i}{v_{n-1}}$ into (2.2), and because of $v_{n-1}^{p-1} \neq 0$ and $\gamma_{n-2}^{p-1} = 1$ we get

$$(\alpha + \frac{\gamma_{i-1}}{\gamma_{n-2}})^{p-1} - (\alpha + \gamma_i)^{p-1} = 0.$$

Consider the following polynomial

$$Q(X) := (X + \frac{\gamma_{i-1}}{\gamma_{n-2}})^{p-1} - (X + \gamma_i)^{p-1}$$

in $\mathbb{F}_p[X]$. It is obvious that the degree of $Q(X)$ is strictly less than $p - 1$. We next show that there are at least $p - 1$ different roots of $Q(X)$ and consequently $Q(X) = 0$.

Since $Q(\alpha) = (\alpha + \frac{\gamma_{i-1}}{\gamma_{n-2}})^{p-1} - (\alpha + \gamma_i)^{p-1} = 0$, $\alpha + \frac{\gamma_{i-1}}{\gamma_{n-2}} \neq 0$ and $\alpha + \gamma_i \neq 0$, then we have

$$((\alpha + \frac{\gamma_{i-1}}{\gamma_{n-2}})/(\alpha + \gamma_i))^{p-1} = 1.$$

Set

$$M_a = a(\alpha + \frac{\gamma_{i-1}}{\gamma_{n-2}})/(\alpha + \gamma_i) \tag{2.3}$$

for each $a \in \mathbb{F}_p\backslash\{\pm 1\}$. It is easy to see that $M_a \in \mathbb{F}_p$ and $M_a \neq -1$. Indeed, if $M_a = -1$, then $\alpha = -(a\frac{\gamma_{i-1}}{\gamma_{n-2}} + \gamma_i)/(a + 1) \in \mathbb{F}_p$, which contradicts $\alpha \in \mathbb{F}\backslash\mathbb{F}_p$.

Now consider

$$\frac{(\alpha + \frac{\gamma_{i-1}}{\gamma_{n-2}})(a + 1)}{(\alpha + \gamma_i)(M_a + 1)} = \frac{a\alpha + \alpha + a\frac{\gamma_{i-1}}{\gamma_{n-2}} + \frac{\gamma_{i-1}}{\gamma_{n-2}}}{M_a\alpha + \alpha + M_a\gamma_i + \gamma_i} \in \mathbb{F}_p^*. \tag{2.4}$$

Equation (2.4) suggests that $(a\alpha + \alpha + a\frac{\gamma_{i-1}}{\gamma_{n-2}} + \frac{\gamma_{i-1}}{\gamma_{n-2}})^{p-1} = (M_a\alpha + \alpha + M_a\gamma_i + \gamma_i)^{p-1}$ and we see that $(M_a\alpha + \alpha + M_a\gamma_i + \gamma_i)^{p-1} = (a\alpha + \alpha + a\frac{\gamma_{i-1}}{\gamma_{n-2}} + \gamma_i)^{p-1}$ by (2.3). Thus $(a\alpha + \alpha + a\frac{\gamma_{i-1}}{\gamma_{n-2}} + \frac{\gamma_{i-1}}{\gamma_{n-2}})^{p-1} = (a\alpha + \alpha + a\frac{\gamma_{i-1}}{\gamma_{n-2}} + \gamma_i)^{p-1}$, i.e.

$$0 = (a\alpha + \alpha + a\frac{\gamma_{i-1}}{\gamma_{n-2}} + \frac{\gamma_{i-1}}{\gamma_{n-2}})^{p-1} - (a\alpha + \alpha + a\frac{\gamma_{i-1}}{\gamma_{n-2}} + \gamma_i)^{p-1} = Q(a\alpha + \alpha + a\frac{\gamma_{i-1}}{\gamma_{n-2}})$$

for each $a \in \mathbb{F}_p\backslash\{\pm 1\}$. For any $a_1 \neq a_2 \in \mathbb{F}_p\backslash\{\pm 1\}$, $a_1\alpha + \alpha + a_1\frac{\gamma_{i-1}}{\gamma_{n-2}} \neq a_2\alpha + \alpha + a_2\frac{\gamma_{i-1}}{\gamma_{n-2}}$. Moreover, $Q(0) = 0$. Therefore there are at least $p - 1$ different roots of $Q(X)$. We have proved $Q(X) = 0$.

Substituting $-\gamma_i$ into $Q(X) = 0$ we obtain

$$\gamma_i = \frac{\gamma_{i-1}}{\gamma_{n-2}},$$

i.e.

$$\frac{v_{i-1}}{v_i} = \frac{v_{n-2}}{v_{n-1}}$$

for $2 \leq i \leq n-2$. This establish the claim.

Now, we prove the cases $1 \leq n \leq 3$. Obviously, $\mathbb{F}[V_1]^G = \mathbb{F}[x_1]$. Since $\{x_1, x_2, \mathrm{N}^G(y_2)\}$ forms a homogeneous system of parameters for $\mathbb{F}[V_3]^G$ and the product of their degrees is equal to the order of G, it follows from [1, Theorem 3.9.4] that $\mathbb{F}[V_3]^G = \mathbb{F}[x_1, x_2, \mathrm{N}^G(y_2)]$. Naturally $S_2 = \{x_1, x_2, \mathrm{N}^G(y_2)\}$ is a separating set for V_3. Then, $S_3 = S_2 \bigcup T_3$ is a separating set for V_5, where

$$T_3 = \left\{x_3,\ \mathrm{N}^G(y_3),\ \mathrm{Tr}^G(y_2^{(p+1)(p-1)}y_3),\ \mathrm{N}^{H_3}(x_2y_3 - x_3y_2)\right\}.$$

The proof is analogous to the proof for $n \geq 4$. □

Remark 2. *Theorem 2 yields a minimal separating set for each representation V_{2n-1}. Moreover, the size of separating set for V_{2n-1} is $\frac{n(3n-2)}{2}$, which depends only on the dimension of the representation. Incidently, the maximal degree of an invariant in this set is the group order p^2.*

3. Conclusions

In this paper, we determine explicit separating sets for four families of finite dimensional representations of the elementary abelian p-groups of rank two $(\mathbb{Z}/p)^2$ over an algebraically closed field of characteristic p, where p is an odd prime. The size of every separating set depends only on the dimension of the representation.

Author contributions

Panpan Jia: Conceptualization, Methodology, Writing-original draft preparation, Writing-review and editing; Jizhu Nan: Methodology, Writing-review and editing, Funding acquisition; Yongsheng Ma: Methodology, Writing-review and editing. All authors have read and approved the final version of the manuscript for publication.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (No.12171194).

Conflict of interest

The authors declare no conflicts of interest in this paper.

References

1. H. Derksen, G. Kemper, *Computational Invariant Theory*, Berlin: Springer-Verlag, 2002. https://doi.org/10.1007/978-3-662-04958-7_3

2. J. Draisma, G. Kemper, D. Wehlau, Polarization of separating invariants, *Canad. J. Math.*, **60** (2008), 556–571. https://doi.org/10.4153/cjm-2008-027-2

3. G. Kemper, Separating invariants, *J. Symbolic Comput.*, **44** (2009), 1212–1222. https://doi.org/10.1016/j.jsc.2008.02.012

4. E. Dufresne, Separating invariants and finite reflection groups, *Adv. Math.*, **221** (2009), 1979–1989. https://doi.org/10.1016/j.aim.2009.03.013

5. G. Kemper, A. Lopatin, F. Reimers, Separating invariants over finite fields, *J. Pure Appl. Algebra*, **226** (2022), 106904. https://doi.org/10.1016/j.jpaa.2021.106904

6. Y. Chen, R. J. Shank, D. L. Wehlau, Modular invariants of finite gluing groups, *J. Algebra*, **566** (2021), 405–434. https://doi.org/10.1016/j.jalgebra.2020.08.034

7. E. Dufresne, J. Elmer, M. Kohls, The Cohen-Macaulay property of separating invariants of finite groups, *Transform. Groups*, **14** (2009), 771–785. https://doi.org/10.1007/s00031-009-9072-y

8. M. Kohls, H. Kraft, Degree bounds for separating invariants, *Math. Res. Lett.*, **17** (2010), 1171–1182. https://doi.org/10.4310/mrl.2010.v17.n6.a15

9. J. Elmer, M. Kohls, Separating invariants for the basic $\mathbb{G}_a$-actions, *Proc. Amer. Math. Soc.*, **140** (2012), 135–146. https://doi.org/10.1090/s0002-9939-2011-11273-5

10. E. Dufresne, J. Elmer, M. Sezer, Separating invariants for arbitrary linear actions of the additive group, *Manuscripta Math.*, **143** (2014), 207–219. https://doi.org/10.1007/s00229-013-0625-y

11. E. Dufresne, J. Jeffries, Separating invariants and local cohomology, *Adv. Math.*, **270** (2015), 565–581. https://doi.org/10.1016/j.aim.2014.11.003

12. M. Domokos, Degree bound for separating invariants of abelian groups, *Proc. Amer. Math. Soc.*, **145** (2017), 3695–3708. https://doi.org/10.1090/proc/13534

13. F. Reimers, Separating invariants of finite groups, *J. Algebra*, **507** (2018), 19–46. https://doi.org/10.1016/j.jalgebra.2018.03.022

14. M. Sezer, Constructing modular separating invariants, *J. Algebra*, **322** (2009), 4099–4104. https://doi.org/10.1016/j.jalgebra.2009.07.011

15. M. D. Neusel, M. Sezer, Separating invariants for modular p-groups and groups acting diagonally, *Math. Res. Lett.*, **16** (2009), 1029–1036. https://doi.org/10.4310/mrl.2009.v16.n6.a11

16. M. Sezer, Explicit separating invariants for cyclic p-groups, *J. Combin. Theory Ser. A*, **118** (2011), 681–689. https://doi.org/10.1016/j.jcta.2010.05.003

17. M. Kohls, M. Sezer, Separating invariants for the Klein four group and cyclic groups, *Internat. J. Math.*, **24** (2013), 1350046. https://doi.org/10.1142/s0129167x13500468

18. F. Reimers, Separating invariants for two copies of the natural S_n-action, *Commun. Algebra*, **48** (2020), 1584–1590. https://doi.org/10.1080/00927872.2019.1691575

19. A. Lopatin, F. Reimers, Separating invariants for multisymmetric polynomials, *Proc. Amer. Math. Soc.*, **149** (2021), 497–508. https://doi.org/10.1090/proc/15292

20. D. J. Benson, *Representations and Cohomology I*, Cambridge: Cambridge University Press, 1991. https://doi.org/10.1017/cbo9780511623622

21. H. E. A. Campbell, R. J. Shank, D. L. Wehlau, Rings of invariants for modular representations of elementary abelian p-groups, *Transform. Groups*, **18** (2013), 1–22. https://doi.org/10.1007/s00031-013-9207-z

22. T. Pierron, R. J. Shank, Rings of invariants for the three-dimensional modular representations of elementary abelian p-groups of rank four, *Involve*, **9** (2016), 551–581. https://doi.org/10.2140/involve.2016.9.551

23. J. Elmer, P. Fleischmann, On the depth of modular invariant rings for the groups $C_p \times C_p$, *Progr. Math.*, **278** (2010), 45–61. https://doi.org/10.1007/978-0-8176-4875-6_4

24. H. E. A. Campbell, D. L. Wehlau, *Modular Invariant Theory*, Berlin: Springer-Verlag, 2011. https://doi.org/10.1090/surv/094/06