VECTOR INVARIANTS FOR TWO-DIMENSIONAL ORTHOGONAL GROUPS OVER FINITE FIELDS

YIN CHEN

ABSTRACT. Let $\mathbb{F}_q$ be a finite field of characteristic 2 and $O_2^+(\mathbb{F}_q)$ be the 2-dimensional orthogonal group over $\mathbb{F}_q$. Consider the standard representation V of $O_2^+(\mathbb{F}_q)$ and the ring of vector invariants $\mathbb{F}_q[mV]^{O_2^+(\mathbb{F}_q)}$ for any $m \in \mathbb{N}^+$. We prove a first main theorem for $(O_2^+(\mathbb{F}_q), V)$, i.e., we find a minimal generating set for $\mathbb{F}_q[mV]^{O_2^+(\mathbb{F}_q)}$. As a consequence, we derive the Noether number $\beta_{mV}(O_2^+(\mathbb{F}_q)) = \max\{q-1, m\}$. We construct a free basis for $\mathbb{F}_q[2V]^{O_2^+(\mathbb{F}_q)}$ over a suitably chosen homogeneous system of parameters. We also obtain a generating set for the Hilbert ideal of $\mathbb{F}_q[mV]^{O_2^+(\mathbb{F}_q)}$ which shows that the Hilbert ideal can be generated by invariants of degree $\leqslant q-1 = \frac{|O_2^+(\mathbb{F}_q)|}{2}$, confirming the conjecture of Derksen and Kemper [11, Conjecture 3.8.6 (b)] in this particular case.

1. INTRODUCTION

Let $\mathbb{F}$ be a field, G a finite group and W be a faithful finite-dimensional representation of G over $\mathbb{F}$. The action of G on W induces a linear action on the dual space W^* by $\sigma \cdot x = x \circ \sigma^{-1}$ for $\sigma \in G$ and $x \in W^*$. Extending the action on W^* multiplicatively yields an action of G on $\mathbb{F}[W]$, the symmetric algebra on W^*. We choose $\{x_1, x_2, \ldots, x_n\}$ as a basis of W^*: then $\mathbb{F}[W]$ can be identified with the polynomial ring $\mathbb{F}[x_1, x_2, \ldots, x_n]$. The subalgebra

$$\mathbb{F}[W]^G := \{f \in \mathbb{F}[W] \mid \sigma \cdot f = f, \forall \sigma \in G\}$$

is called the *invariant ring* of G on W.

Fix a representation V of a finite group G and consider $W = mV := V \oplus V \oplus \cdots \oplus V$, the direct sum of m copies of V. Then G acts on W by extending diagonally the action on V. Finding generators for the vector invariant ring $\mathbb{F}[W]^G = \mathbb{F}[mV]^G$ for a classical group G (usually, $\mathbb{F}$ is the field of complex numbers or the field of real numbers) is the central problem in classical invariant theory. According to H. Weyl's famous book [20], a theorem giving a set of explicit generators for $\mathbb{F}[mV]^G$ is referred to as a *first main theorem* for (G, V).

The modular cases where the characteristic of $\mathbb{F}$ divides the order of G are more compli-cated. In 1990, Richman [14] began the study of the vector invariants of C_p acting on its two-dimensional indecomposable representation V_2 in characteristic $p > 0$, giving a conjecture on generators for $\mathbb{F}_p[mV_2]^{C_p}$ with a proof of the case $p = 2$. In 1997, Campbell and Hughes [4] proved that Richman's conjecture was correct. In 2002, Shank and Wehlau [15] gave a minimal generating set for $\mathbb{F}_p[mV_2]^{C_p}$. In 2010, Campbell, Shank and Wehlau [5] proved that the minimal generating set is actually a SAGBI basis for $\mathbb{F}_p[mV_2]^{C_p}$. In 2013, Wehlau [19] gave a new proof for Richman's conjecture via classical invariant theory. Recently, Bonnafé and Kemper [1], Chen [8, 9], Chen and Wehlau [10] also initiated a study of modular invariants of one vector and one covector for some linear groups over finite fields.

The present paper is devoted to study of the vector invariant ring for the two-dimensional or-thogonal group of plus type over a finite field of characteristic 2 with the standard representation.

The following theorem is our main result.

THEOREM 1.1. *Let $\mathbb{F}_q$ be a finite field of characteristic 2 and $O_2^+(\mathbb{F}_q) = \langle \sigma, \tau_a \rangle$ be the 2-dimensional orthogonal group over $\mathbb{F}_q$ generated by $\sigma = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} \right)$ and $\tau_a = \left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix} \right)$, where $a \in \mathbb{F}_q^\times$. Suppose $O_2^+(\mathbb{F}_q)$ acts linearly on the polynomial ring $\mathbb{F}_q[mV] := \mathbb{F}_q[x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_m]$ by $\sigma(x_i) = y_i, \sigma(y_i) = x_i$ and $\tau_a(x_i) = a^{-1} \cdot x_i, \tau_a(y_i) = a \cdot y_i$ for $1 \leqslant i \leqslant m$. Then $\mathbb{F}_q[mV]^{O_2^+(\mathbb{F}_q)}$ is generated by*

$$
\begin{aligned}
\mathcal{N} &= \left\{ N_i = x_i y_i \mid 1 \leqslant i \leqslant m \right\} \\
\mathcal{U} &= \left\{ U_{ij} = x_i y_j + x_j y_i \mid 1 \leqslant i < j \leqslant m \right\} \\
\mathcal{B} &= \left\{ B_\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_m^{\alpha_m} + y_1^{\alpha_1} y_2^{\alpha_2} \cdots y_m^{\alpha_m} \mid \alpha \in \mathbb{N}^m, |\alpha| = q - 1 \right\} \\
\mathcal{D} &= \left\{ d_{I,J} = x_I \cdot y_J + y_I \cdot x_J \mid \emptyset \neq I < J \subseteq \overline{m}, |J| - |I| = 0 \text{ or } q - 1 \right\},
\end{aligned}
$$

where $|\alpha|$, $d_{I,J}$ and $\overline{m}$ are defined as in NOTATION 1.8 below. Moreover, $\mathbb{F}_q[mV]^{O_2^+(\mathbb{F}_q)}$ is gener-ated minimally by $\mathcal{N} \cup \mathcal{B} \cup \mathcal{D}$.

Remark 1.2. Note that $\mathcal{U} \subseteq \mathcal{D}$. We pay special attention to U_{ij} because they will play an important role in our arguments below.

Recall that the polynomial ring $\mathbb{F}[W] = \bigoplus_{d=0}^{\infty} \mathbb{F}[W]_d$ is standard $\mathbb{N}$-graded and G preserves the degrees. Thus the invariant ring $\mathbb{F}[W]^G = \bigoplus_{d=0}^{\infty} \mathbb{F}[W]_d^G$ is also standard $\mathbb{N}$-graded. The number

$$
\beta_W(G) := \min \left\{ e \mid \mathbb{F}[W]^G \text{ is generated by } \bigoplus_{d=0}^{e} \mathbb{F}[W]_d^G \right\}
$$

is called the *Noether number* for (G, W). As a consequence of Theorem 1.1, we derive

COROLLARY 1.3. $\beta_{mV}(O_2^+(\mathbb{F}_q)) = \max\{q-1, m\}$ *for any* $m \in \mathbb{N}^+$.

Remark 1.4. It is worth noting that Symonds [16, Corollary 0.2] recently proved that for any modular representation W of a finite group G, $\beta_W(G) \leqslant \dim(W)(|G|-1)$. For other finite classical groups, we just know that Campbell, Shank and Wehlau [5, Corollary 8.5] in 2010 gave an upper bound for the Noether number $\beta_{mV_2}(\mathrm{SL}_2(\mathbb{F}_p))$, where V_2 is the standard representation of $\mathrm{SL}_2(\mathbb{F}_p)$.

Example 1.5. ($m = 2$) Consider the set $\mathcal{D}$. Note that $1 \leqslant |I| \leqslant m-1$ and $1 \leqslant |J| \leqslant m-1$. In this case, we must have $|I| = |J| = 1$. Since $I < J$, then $I = \{1\}$ and $J = \{2\}$. Thus $\mathcal{U} = \mathcal{D}$. Theorem 1.1 indicates that $\mathbb{F}_q[2V]^{O_2^+(\mathbb{F}_q)} = \mathbb{F}_q[x_1, x_2, y_1, y_2]^{O_2^+(\mathbb{F}_q)}$ is generated by $q+3$ invariants: $N_1 = x_1 y_1, N_2 = x_2 y_2, U_{12} = x_1 y_2 + x_2 y_1$, and $B_k = x_1^k x_2^{q-1-k} + y_1^k y_2^{q-1-k}$ for $0 \leqslant k \leqslant q-1$. (See Section 7 for more examples.)

It follows from Kemper [12, Proposition 16] that $\mathbb{F}_q[2V]^{O_2^+(\mathbb{F}_q) \times O_2^+(\mathbb{F}_q)}$ is a polynomial algebra generated by $\{N_1, N_2, B_0, B_{q-1}\}$. Moreover, we see that $\{N_1, N_2, B_0, B_{q-1}\}$ is a homogeneous system of parameters for $\mathbb{F}_q[2V]^{O_2^+(\mathbb{F}_q)}$, by Campbell and Wehlau [6, Lemma 2.6.3]. Note that the cyclic group C_2 of order 2 is the Sylow 2-subgroup of $O_2^+(\mathbb{F}_q)$ and $\mathbb{F}_q[2V]^{C_2}$ is a hypersurface (so Cohen-Macaulay) algebra (see Campbell and Wehlau [6, Section 1.2]), so it follows from Campbell, Hughes and Pollack [3, Theorem 1] that $\mathbb{F}_q[2V]^{O_2^+(\mathbb{F}_q)}$ is Cohen-Macaulay.

In this paper, we also construct a free basis for $\mathbb{F}_q[2V]^{O_2^+(\mathbb{F}_q)}$ over $\mathbb{F}_q[2V]^{O_2^+(\mathbb{F}_q) \times O_2^+(\mathbb{F}_q)}$ by showing the following second result.

THEOREM 1.6. *The set*

$$\left\{ U_{12}^i \mid 0 \leqslant i \leqslant \frac{q}{2} \right\} \cup \left\{ B_k \mid 1 \leqslant k \leqslant q-2 \right\} \cup \left\{ B_i B_j \mid 1 \leqslant i, j \leqslant q-2 \text{ and } i+j = q-1 \right\}$$

is a basis for $\mathbb{F}_q[2V]^{O_2^+(\mathbb{F}_q)}$ *as a free* $\mathbb{F}_q[2V]^{O_2^+(\mathbb{F}_q) \times O_2^+(\mathbb{F}_q)}$*-module.*

The Hilbert ideal $\mathfrak{h}_W(G)$ associated with an invariant ring $\mathbb{F}[W]^G$ is the ideal in $\mathbb{F}[W]$ generated by all invariants of positive degree, namely, $\mathfrak{h}_W(G) = (\mathbb{F}[W]_+^G)\mathbb{F}[W]$. Derksen and Kemper [11, Conjecture 3.8.6 (b)] has made the conjecture that $\mathfrak{h}_W(G)$ can be generated by invariants of degree $\leqslant |G|$ for any finite group G and any representation W.

The third purpose of this paper is to find a generating set of $\mathfrak{h}_{mV}(O_2^+(\mathbb{F}_q))$. The following Theorem 1.7 shows that $\mathfrak{h}_{mV}(O_2^+(\mathbb{F}_q))$ can be generated by invariants of degree $\leqslant q-1 = \frac{|O_2^+(\mathbb{F}_q)|}{2}$, confirming the conjecture of Derksen and Kemper in this particular case.

THEOREM 1.7. *The Hilbert ideal $\mathfrak{h}_{mV}(O_2^+(\mathbb{F}_q))$ can be generated by $\mathcal{N} \cup \mathcal{U} \cup \mathcal{B}$.*

This paper is organized as follows: Section 2 contains preliminaries and some basic construc-tions. Our main lemmas, which explain the main idea in the proof of Theorem 1.1, are contained in Section 3. Section 4, together with several technical lemmas in Section 5, gives a complete proof of Theorem 1.1. Section 6 is devoted to giving a proof of Theorem 1.6. In Section 7, we provide more examples to illustrate how large the number of generators in Theorem 1.1 is; a proof of Corollary 1.3 is also given. Section 8 contains a proof of Theorem 1.7. In Section 9, we discuss the orthogonal group of minus type $O_2^-(\mathbb{F}_q)$, and its invariant ring $\mathbb{F}_q[mV]^{O_2^-(\mathbb{F}_q)}$.

We end this introductory section with some notation and conventions.

NOTATION 1.8. We always assume that $\mathbb{F}_q$ is a finite field of characteristic 2. We define $\overline{m} := \{1, 2, \ldots, m\}$. The Greek letters, $\alpha, \beta, \ldots$, denote vectors in $\mathbb{N}^m$. For any vector

$$\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_m) \in \mathbb{N}^m,$$

we define $|\alpha| := \sum_{i=1}^{m} \alpha_i$ and

$$(1.1) \qquad\qquad B_\alpha := x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_m^{\alpha_m} + y_1^{\alpha_1} y_2^{\alpha_2} \cdots y_m^{\alpha_m}.$$

Let $I \subseteq \overline{m}$ be a nonempty subset and $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_m) \in \mathbb{N}^m$ be any vector with $\alpha_i = 0$ for all $i \notin I$. We define $x_I^\alpha := \prod_{i \in I} x_i^{\alpha_i} \in \mathbb{F}_q[mV]$. Similarly, we define $y_J^\beta := \prod_{j \in J} y_j^{\beta_j} \in \mathbb{F}_q[mV]$ for a nonempty subset $J \subseteq \overline{m}$ and any vector β with $\beta_j = 0$ for all $j \notin J$. We also define

$$(1.2) \qquad\qquad d_{I,J}(\alpha, \beta) \;\; := \;\; x_I^\alpha \cdot y_J^\beta + y_I^\alpha \cdot x_J^\beta$$

$$(1.3) \qquad\qquad d_{I,J} \;\; := \;\; d_{I,J}(\overline{1}, \overline{1}) = x_I \cdot y_J + y_I \cdot x_J$$

where $\overline{1}$ is the vector whose the i-th component is 1 for every $i \in I$ (or J) and other components are zero. Given two nonempty subsets $I, J \subseteq \overline{m}$, we say that I *is less than* J, denoted $I < J$, if $i < j$ for all $i \in I$ and all $j \in J$.

2. PRELIMILARIES

Let $\mathbb{F}_q$ denote a finite field of characteristic 2. Recall that a square matrix $A = (a_{ij})$ over any field k is said to be *alternate* if $a_{ij} = -a_{ji}$ and $a_{ii} = 0$. Thus a square matrix over $\mathbb{F}_q$ is alternate if and only if it is symmetric with diagonals zero. Suppose A and B are two $n \times n$ matrices over $\mathbb{F}_q$. We say that A is *congruent* to B, denoted $A \equiv B$, if $A - B$ is an alternate matrix. We choose a fixed element $w \notin \{x^2 + x \mid x \in \mathbb{F}_q\}$. It is well-known that the two-dimensional *orthogonal groups*, up

to isomorphism, are just the following two types:

$$(2.1) \qquad O_2^+(\mathbb{F}_q) \;=\; \left\{ T \in \mathrm{GL}_2(\mathbb{F}_q) \mid T \cdot O^+ \cdot T' \equiv O^+ \right\}$$

$$(2.2) \qquad O_2^-(\mathbb{F}_q) \;=\; \left\{ T \in \mathrm{GL}_2(\mathbb{F}_q) \mid T \cdot O^- \cdot T' \equiv O^- \right\}$$

where $O^+ = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix} \right)$ and $O^- = \left(\begin{smallmatrix} w & 1 \\ 0 & w \end{smallmatrix} \right)$ (see for example, Tang and Wan [17, page 188] or Wan [18]). Note that $|O_2^+(\mathbb{F}_q)| = 2(q-1)$ and $|O_2^-(\mathbb{F}_q)| = 2(q+1)$.

Remark 2.1. The 2-dimensional orthogonal groups over a finite field $\mathbb{F}_q$ of characteristic $p > 2$ have also two isomorphism classes: $O_2^+(\mathbb{F}_q)$ and $O_2^-(\mathbb{F}_q)$, with the orders $2(q-1)$ and $2(q+1)$ respectively. Since p does not divide $2(q-1)$ and $2(q+1)$, the invariants for $O_2^+(\mathbb{F}_q)$ and $O_2^-(\mathbb{F}_q)$ with the standard representations are nonmodular. In this case many classical tools, such as Molien's formula and Noether's bound theorem, can be applied. Thus we ignore this case and emphasize the modular case: $\mathrm{char}(\mathbb{F}_q) = 2$. We also refer to Neusel and Smith [13, page 213], which discusses the generator problem for the invariant ring of $O_2^\pm(\mathbb{F}_p)$ in the nonmodular case.

From now on we always assume that $\mathrm{char}(\mathbb{F}_q) = 2$ and $q = 2^s$ with $s \geqslant 2$. The orthogonal group of plus type $O_2^+(\mathbb{F}_q)$ is generated by

$$(2.3) \qquad \sigma := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } \tau_a := \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix},$$

where $a \in \mathbb{F}_q^\times$. Let V denote the 2-dimensional standard representation of $O_2^+(\mathbb{F}_q)$ over $\mathbb{F}_q$ and $O_2^+(\mathbb{F}_q)$ act on mV diagonally. The action of $O_2^+(\mathbb{F}_q)$ on $\mathbb{F}_q[mV] := \mathbb{F}_q[x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_m]$ is given by

$$(2.4) \qquad \sigma(x_i) = y_i, \qquad \sigma(y_i) = x_i$$

$$(2.5) \qquad \tau_a(x_i) = a^{-1} \cdot x_i, \qquad \tau_a(y_i) = a \cdot y_i$$

for $1 \leqslant i \leqslant m$.

PROPOSITION 2.2. $B_\alpha \in \mathbb{F}_q[mV]^{O_2^+(\mathbb{F}_q)}$ *if and only if* $q - 1$ *divides* $|\alpha|$.

Proof. If $q - 1$ divides $|\alpha|$, then direct calculation shows that $\sigma(B_\alpha) = B_\alpha = \tau_a(B_\alpha)$. Thus B_α is an $O_2^+(\mathbb{F}_q)$-invariant. Conversely, since $\tau_a(B_\alpha) = a^{-|\alpha|} \cdot x_I^\alpha + a^{|\alpha|} \cdot y_I^\alpha = x_I^\alpha + y_I^\alpha$, we have $a^{-|\alpha|} - 1 = 0 = a^{|\alpha|} - 1$. Hence, $q - 1$ divides $|\alpha|$. $\qquad\square$

PROPOSITION 2.3. *The invariant ring* $\mathbb{F}_q[V]^{O_2^+(\mathbb{F}_q)} = \mathbb{F}_q[x, y]^{O_2^+(\mathbb{F}_q)} = \mathbb{F}_q[xy, x^{q-1} + y^{q-1}]$ *is a polynomial algebra.*

Proof. It follows immediately from Kemper [12, Proposition 16]. $\qquad\square$

3. MAIN LEMMA

The following criterion will be very useful for our proof of Theorem 1.1.

LEMMA 3.1. *Let $\mathbb{F}$ be any field and W be an n-dimensional faithful representation of a finite group G over $\mathbb{F}$. Let $H \leqslant G$ be a proper subgroup with $[G:H]^{-1} \in \mathbb{F}$. Suppose $\{f_1, f_2, \ldots, f_m\} \subset \mathbb{F}[W]_+^G \subset \mathbb{F}[W]^H$ is a set of homogeneous polynomials. Let $A = \mathbb{F}[f_1, f_2, \ldots, f_m]$ and $\mathcal{J}$ denote the ideal generated by $\{f_1, f_2, \ldots, f_m\}$ in $\mathbb{F}[W]^H$. We denote the Reynolds operator by:*

$$(3.1) \qquad\qquad \mathcal{R} = \frac{1}{[G:H]} \mathrm{Tr}_H^G : \mathbb{F}[W]^H \longrightarrow \mathbb{F}[W]^G.$$

Suppose $\Delta \cup \{1\}$ is a homogenous generating set of $\mathbb{F}[W]^H$ as an A-module and $\delta \notin A$ for any $\delta \in \Delta$, i.e.,

$$\mathbb{F}[W]^H = A + \sum_{\delta \in \Delta} \delta \cdot A.$$

If $\mathcal{R}(\delta) \in \mathcal{J}$ for all $\delta \in \Delta$, then $\mathbb{F}[W]^G = A$.

Proof. Since $A \subseteq \mathbb{F}[W]^G$, it suffices to show $\mathbb{F}[W]^G \subseteq A$. Note that $\mathcal{R}$ is surjective and degree-preserving, so we need only to show the following *claim*:

$$\mathcal{R}(g) \in A, \text{ for any homogenous element } g \in \mathbb{F}[W]^H.$$

We use the induction on degree of g to prove this claim. Suppose $g \in \mathbb{F}[W]^H$ is any homogenous element and suppose $\mathcal{R}(h) \in A$ for any homogenous element $h \in \mathbb{F}[W]^H$ with $\deg(h) < \deg(g)$. Since $\Delta \cup \{1\}$ is a homogenous generating set of $\mathbb{F}[W]^H$ as an A-module, we may write

$$g = a_0 + \sum_{i=1}^{r} a_i \cdot \delta_i$$

where all $\delta_i \in \Delta$, $a_i \in A$ and $r \in \mathbb{N}^+$. Since every $\mathcal{R}(\delta_i) \in \mathcal{J}$, we may write

$$\mathcal{R}(\delta_i) = g_{i1} f_1 + g_{i2} f_2 + \cdots + g_{im} f_m$$

where $g_{ij} \in \mathbb{F}[W]^H$ are homogenous. Since $\mathcal{R}$ is an $\mathbb{F}[W]^G$-module homomorphism, we have

$$\mathcal{R}(g) = \mathcal{R}^2(g) = \mathcal{R}\left(a_0 + \sum_{i=1}^{r} a_i \cdot \mathcal{R}(\delta_i)\right) = a_0 + \sum_{i=1}^{r} a_i \sum_{j=1}^{m} f_j \cdot \mathcal{R}(g_{ij}).$$

Note that $\deg(f_j) > 0$, so $\deg(g_{ij}) < \deg(g)$ for all $1 \leqslant i \leqslant r$ and $1 \leqslant j \leqslant m$. Thus $\mathcal{R}(g_{ij}) \in A$. Therefore, $\mathcal{R}(g) \in A$ and the claim holds.   □

This lemma leads us to reduce the calculation of $\mathbb{F}_q[mV]^{O_2^+(\mathbb{F}_q)}$ to computing $\mathbb{F}_q[mV]^P$, where P denotes the Sylow 2-subgroup of $O_2^+(\mathbb{F}_q)$. On the other hand, we see that $P \cong C_2$ is the cyclic

group of order 2. It is well-known that any 2-dimensional indecomposable modular representation of the cyclic group $C_p = \langle \sigma \rangle$ of order p is equivalent to the representation defined by

$$\sigma \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

see, for example, Campbell and Wehlau [6, page 105]. Since the invariant rings for equivalent representations are isomorphic, we derive the following result immediately from Richman's Theorem, see Richman [14] or Campbell, Shank and Wehlau [5].

THEOREM 3.2. *Let $\mathbb{F}_q$ be a finite field of characteristic 2 and $P = \langle \sigma \rangle$ be the cyclic group of order 2. Suppose that $\mathbb{F}_q[mV] = \mathbb{F}_q[x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_m]$ is a polynomial algebra on which P acts by permutation, i.e., $\sigma(x_i) = y_i$ and $\sigma(y_i) = x_i$ for all $1 \leqslant i \leqslant m$. Then $\mathbb{F}_q[mV]^P$ is generated by*

$$
\begin{aligned}
\mathcal{L} &= \left\{ L_i = x_i + y_i \mid 1 \leqslant i \leqslant m \right\} \\
\mathcal{N} &= \left\{ N_i = x_i y_i \mid 1 \leqslant i \leqslant m \right\} \\
\mathcal{U} &= \left\{ U_{ij} = x_i y_j + x_j y_i \mid 1 \leqslant i < j \leqslant m \right\} \\
\mathcal{B}' &= \left\{ B_\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_m^{\alpha_m} + y_1^{\alpha_1} y_2^{\alpha_2} \cdots y_m^{\alpha_m} \mid 0 \leqslant \alpha_1, \ldots, \alpha_m \leqslant 1 \right\}.
\end{aligned}
$$

Remark 3.3. Note that in Theorem 3.2, the set $\mathcal{L}$ is contained in $\mathcal{B}'$. Moreover, by Shank and Wehlau [15, Corollary 4.4], $\mathbb{F}_q[mV]^P$ is generated minimally by $\mathcal{L} \cup \mathcal{N} \cup \mathcal{U} \cup \mathcal{B}''$, where

$$\mathcal{B}'' := \left\{ B_\alpha \in \mathcal{B}' \mid |\alpha| \geqslant 3 \right\}.$$

4. PROOF OF THEOREM 1.1

We begin this section with the following well-known result whose proof could be found in Campbell and Wehlau [6, Lemma 9.0.2].

LEMMA 4.1. *Let $q = p^s$ be a prime power and $e \in \mathbb{N}^+$. Then*

$$\sum_{a \in \mathbb{F}_q^\times} a^e = \begin{cases} -1, & \text{if } q - 1 \text{ divides } e, \\ 0, & \text{otherwise}. \end{cases}$$

We define $L^e := L_1^{e_1} L_2^{e_2} \cdots L_m^{e_m}$ and $N^\delta := N_1^{\delta_1} N_2^{\delta_2} \cdots N_m^{\delta_m}$ for any vectors $e = (e_1, e_2, \ldots, e_m) \in \mathbb{N}^m$ and $\delta = (\delta_1, \delta_2, \ldots, \delta_m) \in \mathbb{N}^m$. The following result is an immediate consequence from Campbell and Wehlau [7, Proposition 3.4].

LEMMA 4.2. *For any $B_\alpha, B_\beta \in \mathcal{B}'$, we have*

$$(4.1) \qquad B_\alpha \cdot B_\beta = \sum L^e \cdot N^\delta \cdot B_\gamma + N^{\delta'} \cdot \sum L^{e'} \cdot B_{\gamma'}$$

where two sums are both finite, the vectors $e, e', \delta, \delta' \in \mathbb{N}^m$, and $B_\gamma, B_{\gamma'} \in \mathcal{B}'$.

Proof of the first assertion of Theorem 1.1. We define $\mathcal{S} := \mathcal{N} \cup \mathcal{B} \cup \mathcal{D}$, which will be our desired generating set as $\{f_1, f_2, \ldots, f_m\}$ in Lemma 3.1 and let $\mathcal{J}$ denote the ideal generated by $\mathcal{S}$ in $\mathbb{F}_q[mV]^P$. Then the Reynolds operator

$$(4.2) \quad \mathcal{R} := \mathcal{R}_P^{O_2^+(\mathbb{F}_q)} : \mathbb{F}_q[mV]^P \longrightarrow \mathbb{F}_q[mV]^{O_2^+(\mathbb{F}_q)}, \quad f \mapsto \frac{1}{[O_2^+(\mathbb{F}_q):P]} \sum_{a \in \mathbb{F}_q^\times} \tau_a \cdot f = \sum_{a \in \mathbb{F}_q^\times} \tau_a \cdot f$$

is a surjective homomorphism of $\mathbb{F}_q[mV]^{O_2^+(\mathbb{F}_q)}$-modules.

By Lemma 3.1 and Theorem 3.2, it suffices to show that the image of any non-constant polynomials in $\mathbb{F}_q[mV]^P$ with following form

$$(4.3) \qquad \Big(\prod_{i=1}^m N_i^{\alpha_i}\Big)\Big(\prod_{1 \leqslant i < j \leqslant m} U_{ij}^{\beta_{ij}}\Big)\Big(\prod_{B_\gamma \in \mathcal{B}'} B_\gamma^{e_\gamma}\Big)$$

under $\mathcal{R}$ belongs to $\mathcal{J}$, where $\alpha_i, \beta_{ij}, e_\gamma \in \mathbb{N}$. Note that any $\mathbb{F}_q[\mathcal{S}]$-module generating set Δ of $\mathbb{F}_q[mV]^P$ consists of elements of the above forms, which means that here we actually give a proof for a general result so that the conditions in Lemma 3.1 are satisfied.

Since all $N_i, U_{ij} \in \mathcal{J}$ and $\mathcal{R}$ preserves all $O_2^+(\mathbb{F}_q)$-invariants, it is sufficient to prove that

$$(4.4) \qquad\qquad \mathcal{R}\Big(\prod_{B_\gamma \in \mathcal{B}'} B_\gamma^{e_\gamma}\Big) \in \mathcal{J},$$

where $\deg\Big(\prod_{B_\gamma \in \mathcal{B}'} B_\gamma^{e_\gamma}\Big) > 0$. By Lemma 4.2, we need only to prove the following three cases:

$$(4.5) \qquad\qquad\qquad \mathcal{R}(B_\alpha) \in \mathcal{J},$$

$$(4.6) \qquad\qquad\qquad \mathcal{R}(L^\alpha) \in \mathcal{J},$$

$$(4.7) \qquad\qquad\qquad \mathcal{R}(L^\alpha \cdot B_\beta) \in \mathcal{J},$$

where $B_\alpha, B_\beta \in \mathcal{B}'$ and $L^\alpha = L_1^{\alpha_1} L_2^{\alpha_2} \cdots L_m^{\alpha_m}$ are polynomials with positive degree. Our proof will be completed by applying the following Lemmas 5.4, 5.5 and 5.6 respectively. $\square$

Proof of the second assertion of Theorem 1.1. It is sufficient to show that every element in $\mathcal{N} \cup \mathcal{B} \cup \mathcal{D}$ is indecomposable. The fact that $\mathbb{F}_q[mV]^{O_2^+(\mathbb{F}_q)} \subseteq \mathbb{F}_q[mV]^P$, together with that all N_i and U_{ij} are indecomposable in $\mathbb{F}_q[mV]^P$ (Remark 3.3) implies that all N_i and U_{ij} are indecomposable in $\mathbb{F}_q[mV]^{O_2^+(\mathbb{F}_q)}$. Note that the elements in $\mathcal{D}$ can be separated into two classes:

$$\mathcal{D}_1 = \{d_{I,J} : |J| = |I|\} \text{ and } \mathcal{D}_2 = \{d_{I,J} : |J| = |I| + q - 1\}.$$

For any $B_\alpha \in \mathcal{B}$, assume by way of contradiction that B_α is decomposable. Since $|B_\alpha| = q - 1$ and every element in $\mathcal{D}_2$ has degree $> q - 1$, it does not factor using elements from $\mathcal{D}_2$. Note

that all elements in $\mathcal{N} \cup \mathcal{D}_1$ have even degree, so any product of them has even degree. However, $|B_\alpha| = q - 1$ is odd, thus B_α does not factor using elements from $\mathcal{N} \cup \mathcal{D}_1$. Thus B_α factor using only elements from $\mathcal{B} - \{B_\alpha\}$. Since any element in $\mathcal{B}$ has the same degree, B_α is a linear combination among $\mathcal{B} - \{B_\alpha\}$ over $\mathbb{F}_q$. This contradiction shows that B_α is indecomposable.

By Shank and Wehlau [15, Corollary 4.4], we have seen that $\prod_{i \in I} x_i + \prod_{i \in I} y_i$ is indecomposable in $\mathbb{F}_q[mV]^P$ for any $I \subseteq \overline{m}$ with $|I| > 2$. Thus choosing a suitable basis for mV, we also deduce that $d_{I,J} = x_I y_J + y_I x_J = \prod_{i \in I} x_i \cdot \prod_{j \in J} y_j + \prod_{i \in I} y_i \cdot \prod_{j \in J} x_j$ is indecomposable in $\mathbb{F}_q[mV]^P$ for any $\emptyset \neq I < J \subseteq \overline{m}$ with $|I| + |J| > 2$. Thus for any $d_{I,J} \in \mathcal{D}$ with $|I| + |J| > 2$, it is indecomposable in $\mathbb{F}_q[mV]^{O_2^+(\mathbb{F}_q)}$. Since any element in $\mathcal{D}$ has degree $\geqslant 2$, we need only to show that the elements in $\mathcal{D}$ with degree 2 are indecomposable. In fact this set of elements of degree 2 just coincides with $\mathcal{U}$. We have seen that every U_{ij} is indecomposable. This completes the proof.   □

5. LEMMAS

We follow the notations in previous section and begin with a simple but useful observation:

LEMMA 5.1. $\mathcal{R}(\mathcal{J}) \subseteq \mathcal{J}$.

Proof. For any $f \in \mathcal{J}$, we may write $f = \sum a_i \cdot f_i$ with $a_i \in \mathcal{S}$ and $f_i \in \mathbb{F}_q[mV]^P$. Since $\mathcal{R}$ is an $\mathbb{F}_q[mV]^{O_2^+(\mathbb{F}_q)}$-module homomorphism, we have $\mathcal{R}(f) = \mathcal{R}(\sum a_i \cdot f_i) = \sum a_i \cdot \mathcal{R}(f_i) \in \mathcal{J}$. Thus $\mathcal{R}(\mathcal{J}) \subseteq \mathcal{J}$.   □

LEMMA 5.2. *Let* $\alpha \in \mathbb{N}^m$ *be any vector with* $|\alpha| > 0$ *and* $B_\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_m^{\alpha_m} + y_1^{\alpha_1} y_2^{\alpha_2} \cdots y_m^{\alpha_m} \in \mathbb{F}_q[mV]^P$. *Then for any* $e \in \mathbb{N}^+$, *we have* $B_\alpha^e \equiv (x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_m^{\alpha_m})^e + (y_1^{\alpha_1} y_2^{\alpha_2} \cdots y_m^{\alpha_m})^e \pmod{\mathcal{J}}$. *In particular,* $L_i^e \equiv x_i^e + y_i^e \pmod{\mathcal{J}}$, *for all* $i \in \overline{m}$.

Proof. Since $|\alpha| > 0$, there exists some $i \in \overline{m}$ such that $\alpha_i > 0$. Without loss of generality, we suppose $\alpha_1 > 0$. Define $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_m^{\alpha_m}$ and $y^\alpha = y_1^{\alpha_1} y_2^{\alpha_2} \cdots y_m^{\alpha_m}$. By the binomial formula, we have

$$B_\alpha^e = (x^\alpha + y^\alpha)^e = (x^\alpha)^e + \left[\sum_{k=1}^{e-1} \binom{e}{e-k} (x^\alpha)^{e-k} (y^\alpha)^k \right] + (y^\alpha)^e.$$

We *claim* that $\sum_{k=1}^{e-1} \binom{e}{e-k} (x^\alpha)^{e-k} (y^\alpha)^k \in \mathcal{J}$. Define $b_k := \binom{e}{e-k} (x^\alpha)^{e-k} (y^\alpha)^k + \binom{e}{k} (x^\alpha)^k (y^\alpha)^{e-k}$ for $1 \leqslant k \leqslant \frac{e-1}{2}$ (when e is odd) and $1 \leqslant k \leqslant \frac{e}{2} - 1$ (when e is even). Further, when e is even, since $\binom{e}{e/2}$ is even, we have $\binom{e}{e/2} (x^\alpha)^{e/2} (y^\alpha)^{e/2} = 0$. Thus it is sufficient to show that every $b_k \in \mathcal{J}$. Since char$(\mathbb{F}_q) = 2$ and $\binom{e}{e-k} = \binom{e}{k}$, $b_k = 0$ whenever $\binom{e}{k}$ is even. Suppose $\binom{e}{k}$ is odd in b_k. Since char$(\mathbb{F}_q) = 2$, then $\binom{e}{k} = 1$ in $\mathbb{F}_q$. Note that $\alpha_1 \geqslant 1$ and $\frac{e-1}{2} \geqslant k \geqslant 1$, we have

$$b_k = (x^\alpha)^{e-k} (y^\alpha)^k + (x^\alpha)^k (y^\alpha)^{e-k}$$

$$
\begin{aligned}
&= (x_1^{\alpha_1(e-k)} x_2^{\alpha_2(e-k)} \cdots x_m^{\alpha_m(e-k)})(y_1^{\alpha_1 k} y_2^{\alpha_2 k} \cdots y_m^{\alpha_m k}) + \\
&\quad (y_1^{\alpha_1(e-k)} y_2^{\alpha_2(e-k)} \cdots y_m^{\alpha_m(e-k)})(x_1^{\alpha_1 k} x_2^{\alpha_2 k} \cdots x_m^{\alpha_m k}) \\
&= N_1 \cdot \Big[(x_1^{\alpha_1(e-k)-1} x_2^{\alpha_2(e-k)} \cdots x_m^{\alpha_m(e-k)})(y_1^{\alpha_1 k-1} y_2^{\alpha_2 k} \cdots y_m^{\alpha_m k}) + \\
&\quad (y_1^{\alpha_1(e-k)-1} y_2^{\alpha_2(e-k)} \cdots y_m^{\alpha_m(e-k)})(x_1^{\alpha_1 k-1} x_2^{\alpha_2 k} \cdots x_m^{\alpha_m k}) \Big] \in \mathcal{J}.
\end{aligned}
$$

Thus the claim follows and $B_\alpha^e \equiv (x^\alpha)^e + (y^\alpha)^e \pmod{\mathcal{J}}$. In particular, when $B_\alpha = L_i = x_i + y_i$, we have $L_i^e \equiv x_i^e + y_i^e \pmod{\mathcal{J}}$. □

LEMMA 5.3. *For any nonempty sets $I, J \subseteq \overline{m}$ and $d_{I,J}(\alpha, \beta) = x_I^\alpha \cdot y_J^\beta + y_I^\alpha \cdot x_J^\beta$ with all exponents $\alpha_i, \beta_j \geqslant 1$, we have $\mathcal{R}(d_{I,J}(\alpha, \beta)) \in \mathcal{J}$.*

Proof. Note that $d_{I,J}(\alpha, \beta)$ is a P-invariant. The proof will be separated into two cases: $I \cap J \neq \emptyset$ and $I \cap J = \emptyset$. For the first case, we suppose that there exists an integer $k \in I \cap J$. Since all $\alpha_i, \beta_j \geqslant 1$, we have

$$
\begin{aligned}
d_{I,J}(\alpha, \beta) &= (x_k^{\alpha_k} y_k^{\beta_k}) \cdot x_{I-\{k\}}^\alpha \cdot y_{J-\{k\}}^\beta + (y_k^{\alpha_k} x_k^{\beta_k}) \cdot y_{I-\{k\}}^\alpha \cdot x_{J-\{k\}}^\beta \\
&= N_k \cdot \Big[(x_k^{\alpha_k-1} y_k^{\beta_k-1}) \cdot x_{I-\{k\}}^\alpha \cdot y_{J-\{k\}}^\beta + (y_k^{\alpha_k-1} x_k^{\beta_k-1}) \cdot y_{I-\{k\}}^\alpha \cdot x_{J-\{k\}}^\beta \Big] \in \mathcal{J}.
\end{aligned}
$$

By Lemma 5.1, $\mathcal{R}(d_{I,J}(\alpha, \beta)) \in \mathcal{J}$ in this case.

Secondly, we suppose $I \cap J = \emptyset$. This situation can be separated into two subcases:

SUBCASE 1. For all $i \in I$ and all $j \in J$, $\alpha_i = 1 = \beta_j$. For any $i \in I$, if there exists an integer $j \in J$ such that $i > j$, then

$$
\begin{aligned}
d_{I,J}(\alpha, \beta) &= d_{I,J} \\
&= (x_i y_j)(x_{I-\{i\}} \cdot y_{J-\{j\}}) + (y_i x_j)(y_{I-\{i\}} \cdot x_{J-\{j\}}) \\
&= (U_{ji} + y_i x_j)(x_{I-\{i\}} \cdot y_{J-\{j\}}) + (U_{ji} + x_i y_j)(y_{I-\{i\}} \cdot x_{J-\{j\}}) \\
&= U_{ji} \cdot (x_{I-\{i\}} \cdot y_{J-\{j\}} + y_{I-\{i\}} \cdot x_{J-\{j\}}) + \\
&\quad \Big[x_{(I-\{i\}) \cup \{j\}} \cdot y_{\{i\} \cup (J-\{j\})} + y_{(I-\{i\}) \cup \{j\}} \cdot x_{\{i\} \cup (J-\{j\})} \Big].
\end{aligned}
$$

Since $U_{ji} \cdot (x_{I-\{i\}} \cdot y_{J-\{j\}} + y_{I-\{i\}} \cdot x_{J-\{j\}}) \in \mathcal{J}$ and $\mathcal{R}(\mathcal{J}) \subseteq \mathcal{J}$, if we want to prove $\mathcal{R}(d_{I,J}) \in \mathcal{J}$, it is sufficient to show that

$$
\mathcal{R}\Big[x_{(I-\{i\}) \cup \{j\}} \cdot y_{\{i\} \cup (J-\{j\})} + y_{(I-\{i\}) \cup \{j\}} \cdot x_{\{i\} \cup (J-\{j\})} \Big] \in \mathcal{J}.
$$

Proceeding in this fashion, we need only to show that

(5.1) $\mathcal{R}(x_I y_J + y_I x_J) \in \mathcal{J}$,

where $I < J$. On the other hand, whenever $I < J$,

$$
\begin{aligned}
\mathcal{R}(x_I y_J + y_I x_J) &= \sum_{a \in \mathbb{F}_q^\times} a^{|J|-|I|} x_I y_J + \sum_{a \in \mathbb{F}_q^\times} a^{|I|-|J|} y_I x_J \\
&= \left(\sum_{a \in \mathbb{F}_q^\times} a^{|J|-|I|} \right) \cdot (x_I y_J + y_I x_J) \\
&= \begin{cases} x_I y_J + y_I x_J, & \text{if } q-1 \text{ divides } |J|-|I|, \\ 0, & \text{otherwise.} \end{cases}
\end{aligned}
$$

The last equation follows from Lemma 4.1. We have to show that $d_{I,J} \in \mathcal{J}$ if $q-1$ divides $|J| - |I|$. By the symmetry of $d_{I,J}$, we may write $|J| - |I| = (q-1) \cdot r$, where $r \in \mathbb{N}$. We use induction on r. If $r = 0$ or 1, we are done. Let $I' \subseteq J$ denote the subset such that $|I'| = |I|$ and $J - I' < I'$. For any $k = 1, 2, \cdots, r$, we let $J_k \subseteq J - I'$ denote the subsets such that $|J_k| = q-1$ and $J_1 < J_2 < \cdots < J_r$. Then

$$
\begin{aligned}
d_{I,J} &= x_I y_{J-I'} y_{I'} + y_I x_{J-I'} x_{I'} \\
&= x_I y_{J_1} y_{J_2} \cdots y_{J_r} y_{I'} + y_I x_{J_1} x_{J_2} \cdots x_{J_r} x_{I'} \\
&= x_I (d_{J_1} + x_{J_1}) y_{J_2} \cdots y_{J_r} y_{I'} + y_I (d_{J_1} + y_{J_1}) x_{J_2} \cdots x_{J_r} x_{I'} \\
&= d_{J_1} (x_I y_{J_2} \cdots y_{J_r} y_{I'} + y_I x_{J_2} \cdots x_{J_r} x_{I'}) + (x_I x_{J_1} y_{J_2} \cdots y_{J_r} y_{I'} + y_I y_{J_1} x_{J_2} \cdots x_{J_r} x_{I'}),
\end{aligned}
$$

where $d_{J_1} := \prod_{j \in J_1} x_j + \prod_{j \in J_1} y_j \in \mathcal{B}$ because $|J_1| = q-1$. To see that $d_{I,J} \in \mathcal{J}$, it suffices to show that $x_{I \cup J_1} y_{J_2} \cdots y_{J_{r-1}} y_{J_r \cup I'} + y_{I \cup J_1} x_{J_2} \cdots x_{J_{r-1}} x_{J_r \cup I'} \in \mathcal{J}$, which actually follows from the induction hypothesis. This finishes the proof for the first subcase.

SUBCASE 2. For some $i \in I$ (resp. $j \in J$), we have $\alpha_i \geqslant 2$ (resp. $\beta_j \geqslant 2$). By the symmetry of $d_{I,J}(\alpha, \beta)$, we suppose that there exists an $i \in I$ such that $\alpha_i \geqslant 2$. For any $j \in J$, we have

$$
\begin{aligned}
d_{I,J}(\alpha, \beta) &= x_I^\alpha \cdot y_J^\beta + y_I^\alpha \cdot x_J^\beta \\
&= (x_i y_j)(x_{I-\{i\}}^\alpha x_i^{\alpha_i - 1})(y_{J-\{j\}}^\beta y_j^{\beta_j - 1}) + (y_i x_j)(y_{I-\{i\}}^\alpha y_i^{\alpha_i - 1})(x_{J-\{j\}}^\beta x_j^{\beta_j - 1}) \\
&= (U_{ij} + y_i x_j)(x_{I-\{i\}}^\alpha x_i^{\alpha_i - 1})(y_{J-\{j\}}^\beta y_j^{\beta_j - 1}) + (U_{ij} + x_i y_j)(y_{I-\{i\}}^\alpha y_i^{\alpha_i - 1})(x_{J-\{j\}}^\beta x_j^{\beta_j - 1}) \\
&= U_{ij} \cdot \left[(x_{I-\{i\}}^\alpha x_i^{\alpha_i - 1})(y_{J-\{j\}}^\beta y_j^{\beta_j - 1}) + (y_{I-\{i\}}^\alpha y_i^{\alpha_i - 1})(x_{J-\{j\}}^\beta x_j^{\beta_j - 1}) \right] + \\
&\quad N_i \cdot \left[(x_{I-\{i\}}^\alpha x_i^{\alpha_i - 2} x_j)(y_{J-\{j\}}^\beta y_j^{\beta_j - 1}) + (y_{I-\{i\}}^\alpha y_i^{\alpha_i - 2} y_j)(x_{J-\{j\}}^\beta x_j^{\beta_j - 1}) \right]
\end{aligned}
$$

which belongs to $\mathcal{J}$, so $\mathcal{R}(d_{I,J}(\alpha, \beta)) \in \mathcal{R}(\mathcal{J}) \subseteq \mathcal{J}$. $\square$

LEMMA 5.4. *For any* $\alpha \in \mathbb{N}^m$ *with* $|\alpha| > 0$ *and* $B_\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_m^{\alpha_m} + y_1^{\alpha_1} y_2^{\alpha_2} \cdots y_m^{\alpha_m}$, *we have* $\mathcal{R}(B_\alpha) \in \mathcal{J}$.

Proof. Indeed,

$$
\begin{aligned}
\mathcal{R}(B_\alpha) &= \sum_{a\in\mathbb{F}_q^\times} a^{-|\alpha|}x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_m^{\alpha_m} + \sum_{a\in\mathbb{F}_q^\times} a^{|\alpha|}y_1^{\alpha_1}y_2^{\alpha_2}\cdots y_m^{\alpha_m} \\
&= \Big(\sum_{a\in\mathbb{F}_q^\times}(a^{-1})^{|\alpha|}\Big)x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_m^{\alpha_m} + \Big(\sum_{a\in\mathbb{F}_q^\times}a^{|\alpha|}\Big)y_1^{\alpha_1}y_2^{\alpha_2}\cdots y_m^{\alpha_m} \\
&= \Big(\sum_{a\in\mathbb{F}_q^\times}a^{|\alpha|}\Big)\cdot B_\alpha \\
&= \begin{cases} B_\alpha, & \text{if } q-1 \text{ divides } |\alpha|, \\ 0, & \text{otherwise.} \end{cases}
\end{aligned}
$$

The last equation follows from Lemma 4.1. We have to prove the *claim* that $B_\alpha \in \mathcal{J}$ for all α with $|\alpha| = (q-1)\cdot r$, where $r\in\mathbb{N}^+$. If $r=1$, this claim holds clearly. Now suppose $r>1$. We may write $B_\alpha = x^{\alpha'}x^{\alpha''} + y^{\alpha'}y^{\alpha''}$, where $|\alpha'|=q-1$ and $|\alpha''|=(q-1)(r-1)$. Then

$$
\begin{aligned}
B_\alpha &= (B_{\alpha'} + y^{\alpha'})x^{\alpha''} + (B_{\alpha'}+x^{\alpha'})y^{\alpha''} \\
&= B_{\alpha'}\cdot(x^{\alpha''}+y^{\alpha''}) + (x^{\alpha'}y^{\alpha''}+y^{\alpha'}x^{\alpha''}).
\end{aligned}
$$

Note that $B_{\alpha'} := x^{\alpha'}+y^{\alpha'} \in \mathcal{B}$. To show $B_\alpha \in \mathcal{J}$, it suffices to show that $x^{\alpha'}y^{\alpha''}+y^{\alpha'}x^{\alpha''} \in \mathcal{J}$. However, $x^{\alpha'}y^{\alpha''}+y^{\alpha'}x^{\alpha''} \in \mathbb{F}_q[mV]^{O_2^+(\mathbb{F}_q)}$, so $x^{\alpha'}y^{\alpha''}+y^{\alpha'}x^{\alpha''} = \mathcal{R}(x^{\alpha'}y^{\alpha''}+y^{\alpha'}x^{\alpha''})$. By Lemma 5.1, we have $\mathcal{R}(x^{\alpha'}y^{\alpha''}+y^{\alpha'}x^{\alpha''}) \in \mathcal{J}$. Thus $B_\alpha \in \mathcal{J}$ and the claim holds. This completes the proof. $\square$

LEMMA 5.5. *For any* $L^\alpha = L_1^{\alpha_1}L_2^{\alpha_2}\cdots L_m^{\alpha_m}$ *with* $|\alpha| > 0$, *we have* $\mathcal{R}(L^\alpha) \in \mathcal{J}$.

Proof. Let $I = \{i \mid \alpha_i \neq 0\} \subseteq \overline{m}$. Then

$$
\begin{aligned}
L^\alpha &= \prod_{i\in I} L_i^{\alpha_i} \\
&= \prod_{i\in I}(x_i+y_i)^{\alpha_i} \\
&\equiv \prod_{i\in I}(x_i^{\alpha_i}+y_i^{\alpha_i}) \pmod{\mathcal{J}} \quad \text{(by Lemma 5.2)} \\
&= \sum_{K\subseteq I}(x_K^\alpha\cdot y_{K^c}^{\alpha_c} + y_K^\alpha\cdot x_{K^c}^{\alpha_c}),
\end{aligned}
$$

where $K^c = I - K$ denotes the complement of K in I, and the sum runs over the representatives of the quotient set of the power set of I on the equivalence relation: $K_1 \sim K_2$ if and only if $K_2 = K_1^c$. It follows from Lemmas 5.3 and 5.4 that the image of every $x_K^\alpha\cdot y_{K^c}^{\alpha_c} + y_K^\alpha\cdot x_{K^c}^{\alpha_c}$ under $\mathcal{R}$ belongs to $\mathcal{J}$. Hence, $\mathcal{R}(L^\alpha) \in \mathcal{J}$. $\square$

LEMMA 5.6. *For any B_β and $L^\alpha = L_1^{\alpha_1} L_2^{\alpha_2} \cdots L_m^{\alpha_m}$ with $|\alpha| > 0, |\beta| > 0$, we have $\mathcal{R}(L^\alpha \cdot B_\beta) \in \mathcal{J}$.*

Proof. As in the proof of Lemma 5.5, we have $L^\alpha \equiv \sum_{K \subseteq I}(x_K^\alpha \cdot y_{K^c}^{\alpha_c} + y_K^\alpha \cdot x_{K^c}^{\alpha_c})$ (mod $\mathcal{J}$). Thus to show that $\mathcal{R}(L^\alpha \cdot B_\beta) \in \mathcal{J}$, it is sufficient to show that the image of every $(x^\beta + y^\beta)(x_K^\alpha \cdot y_{K^c}^{\alpha_c} + y_K^\alpha \cdot x_{K^c}^{\alpha_c})$ belongs to $\mathcal{J}$. On the other hand,

$$(x^\beta + y^\beta)(x_K^\alpha \cdot y_{K^c}^{\alpha_c} + y_K^\alpha \cdot x_{K^c}^{\alpha_c}) = (x^\beta x_K^\alpha \cdot y_{K^c}^{\alpha_c} + y^\beta y_K^\alpha \cdot x_{K^c}^{\alpha_c}) + (x_K^\alpha \cdot y_{K^c}^{\alpha_c} y^\beta + y_K^\alpha \cdot x_{K^c}^{\alpha_c} x^\beta).$$

Applying Lemmas 5.3 and 5.4 we see that $\mathcal{R}(x^\beta x_K^\alpha \cdot y_{K^c}^{\alpha_c} + y^\beta y_K^\alpha \cdot x_{K^c}^{\alpha_c})$ and $\mathcal{R}(x_K^\alpha \cdot y_{K^c}^{\alpha_c} y^\beta + y_K^\alpha \cdot x_{K^c}^{\alpha_c} x^\beta)$ both belong to $\mathcal{J}$. The proof is completed.   □

6. PROOF OF THEOREM 1.6

Let $R := \mathbb{F}_q[N_1, N_2, B_0, B_{q-1}]$ and $R' := \mathbb{F}_q[N_1, N_2]$. We have seen that $R = \mathbb{F}_q[2V]^{O_2^+(\mathbb{F}_q) \times O_2^+(\mathbb{F}_q)}$ and $\{N_1, N_2, B_0, B_{q-1}\}$ is a homogeneous system of parameters for $\mathbb{F}_q[2V]^{O_2^+(\mathbb{F}_q)}$. We define

$$\mathcal{M} := \left\{ U_{12}^i \mid 0 \leq i \leq \frac{q}{2} \right\} \cup \left\{ B_k \mid 1 \leq k \leq q-2 \right\} \cup \left\{ B_i \cdot B_j \mid 1 \leq i, j \leq q-2 \text{ and } i+j = q-1 \right\}.$$

PROPOSITION 6.1. *For $1 \leq k \leq q-2$, we have $B_k \cdot U_{12} = N_2 \cdot B_{k+1} + N_1 \cdot B_{k-1} \in \sum_{k=1}^{q-2} R \cdot B_k$.*

Proof. Indeed, $B_k \cdot U_{12} = (x_1^k x_2^{q-1-k} + y_1^k y_2^{q-1-k})(x_1 y_2 + x_2 y_1) = (x_1^{k+1} y_2 x_2^{q-1-k} + y_2^{q-1-k} x_2 y_1^{k+1}) + (x_1^k x_2^{q-k} y_1 + y_1^k y_2^{q-k} x_1) = N_2 \cdot B_{k+1} + N_1 \cdot B_{k-1} \in \sum_{k=1}^{q-2} R \cdot B_k$.   □

PROPOSITION 6.2. $U_{12}^{\frac{q}{2}+1} \in \sum_{i=0}^{\frac{q}{2}} R' \cdot U_{12}^i$.

Proof. Note that $q = 2^s$ with $s \geq 2$. If $s = 2$, then $q = 4$. It is easy to check that $U_{12}^3 = U_{12}^2 + N_1 N_2 U_{12}$. This statement follows in this special case. Now we suppose $s \geq 3$ and define

$$V_j := x_1^{\frac{q}{2}+1-2j} y_2^{\frac{q}{2}+1-2j} + y_1^{\frac{q}{2}+1-2j} x_2^{\frac{q}{2}+1-2j}$$

for $j = 0, 1, 2, \ldots, \frac{q}{4}$. In particular, $V_{\frac{q}{4}} = U_{12}$ and $V_{\frac{q}{4}-1} = U_{12}^3 = U_{12}^2 + N_1 N_2 U_{12}$. Then for $i = 0, 1, 2, \ldots, \frac{q}{4} - 2$, we have

$$
\begin{aligned}
V_j &= x_1^{\frac{q}{2}+1-2j} y_2^{\frac{q}{2}+1-2j} + y_1^{\frac{q}{2}+1-2j} x_2^{\frac{q}{2}+1-2j} \\
&= (x_1^{\frac{q}{2}-1-2j} y_2^{\frac{q}{2}-1-2j} + y_1^{\frac{q}{2}-1-2j} x_2^{\frac{q}{2}-1-2j})(x_1^2 y_2^2 + y_1^2 x_2^2) + \\
&\quad (y_1^{\frac{q}{2}-1-2j} x_2^{\frac{q}{2}-1-2j} x_1^2 y_2^2 + x_1^{\frac{q}{2}-1-2j} y_2^{\frac{q}{2}-1-2j} y_1^2 x_2^2) \\
&= V_{j+1} U_{12}^2 + (N_1 N_2)^2 V_{j+2}.
\end{aligned}
$$

Thus, $V_0 = V_1 U_{12}^2 + (N_1 N_2)^2 V_2 = (V_2 U_{12}^2 + (N_1 N_2)^2 V_3) U_{12}^2 + (N_1 N_2)^2 V_2 = \cdots = U_{12}^{\frac{q}{2}} + f$, where $f \in \sum_{i < \frac{q}{2}} R' \cdot U_{12}^i$. Hence, $U_{12}^{\frac{q}{2}+1} = (x_1^{\frac{q}{2}} y_2^{\frac{q}{2}} + x_2^{\frac{q}{2}} y_1^{\frac{q}{2}})(x_1 y_2 + x_2 y_1) = (x_1^{\frac{q}{2}+1} y_2^{\frac{q}{2}+1} + y_1^{\frac{q}{2}+1} x_2^{\frac{q}{2}+1}) + (x_1^{\frac{q}{2}} x_2 y_1 y_2^{\frac{q}{2}} + y_1^{\frac{q}{2}} y_2 x_1 x_2^{\frac{q}{2}}) = V_0 + N_1 N_2 V_1 = U_{12}^{\frac{q}{2}} + f$, for some $f \in \sum_{i < \frac{q}{2}} R' \cdot U_{12}^i$. Therefore, $U_{12}^{\frac{q}{2}+1} \in \sum_{i=0}^{\frac{q}{2}} R' \cdot U_{12}^i$, as desired.   □

LEMMA 6.3. *For any $n \in \mathbb{N}^+$, $v_n := y_1^n x_2^n + x_1^n y_2^n \in \sum_{f \in \mathcal{M}} R \cdot f$.*

Proof. We use induction on n. If $n = 1$, then $v_1 = U_{12}$ and the lemma follows immediately. Suppose $n \geqslant 2$, then $v_n = (y_1^{n-1} x_2^{n-1} + x_1^{n-1} y_2^{n-1})(y_1 x_2 + x_1 y_2) + (x_1^{n-1} y_2^{n-1} y_1 x_2 + y_1^{n-1} x_2^{n-1} x_1 y_2) = v_{n-1} U_{12} + N_1 N_2 v_{n-2}$. By the induction hypothesis and Proposition 6.2, we have $v_n \in \sum_{f \in \mathcal{M}} R \cdot f$. $\square$

PROPOSITION 6.4. *For $1 \leqslant k \leqslant i \leqslant q - 2$, we have $B_k \cdot B_i \in \sum_{f \in \mathcal{M}} R \cdot f$.*

Proof. If $k + i = q - 1$, then $B_k \cdot B_i \in \mathcal{M}$. Now we consider the case when $k + i < q - 1$. Note that

$$
\begin{aligned}
B_k \cdot B_i &= (x_1^k x_2^{q-1-k} + y_1^k y_2^{q-1-k})(x_1^i x_2^{q-1-i} + y_1^i y_2^{q-1-i}) \\
&= (x_1^{k+i} x_2^{2q-2-k-i} + y_1^{k+i} y_2^{2q-2-k-i}) + (x_1^k x_2^{q-1-k} y_1^i y_2^{q-1-i} + y_1^k y_2^{q-1-k} x_1^i x_2^{q-1-i}) \\
&= (B_{k+i} + y_1^{k+i} y_2^{q-1-k-i}) x_2^{q-1} + (B_{k+i} + x_1^{k+i} x_2^{q-1-k-i}) y_2^{q-1} + \\
&\quad N_1^k N_2^{q-1-i} (x_2^{i-k} y_1^{i-k} + y_2^{i-k} x_1^{i-k}) \\
&= B_{k+i} B_0 + N_2^{q-1-k-i}(y_1^{k+i} x_2^{k+i} + x_1^{k+i} y_2^{k+i}) + N_1^k N_2^{q-1-i}(x_2^{i-k} y_1^{i-k} + y_2^{i-k} x_1^{i-k}).
\end{aligned}
$$

By Lemma 6.3, v_{k+i} and v_{i-k} both belong to $\sum_{f \in \mathcal{M}} R \cdot f$, so does $B_k \cdot B_i$. Similar arguments can be applied to the case when $k + i > q - 1$. $\square$

Now we are ready to prove Theorem 1.6.

Proof of Theorem 1.6. Since $\mathbb{F}_q[2V]^{O_2^+(\mathbb{F}_q)}$ is Cohen-Macaulay and $\mathbb{F}_q[2V]^{O_2^+(\mathbb{F}_q) \times O_2^+(\mathbb{F}_q)}$ is a polynomial algebra, it follows that $\mathbb{F}_q[2V]^{O_2^+(\mathbb{F}_q)}$ is a free $\mathbb{F}_q[2V]^{O_2^+(\mathbb{F}_q) \times O_2^+(\mathbb{F}_q)}$-module of rank $2(q - 1) = |O_2^+(\mathbb{F}_q)|$, see for example [8, Lemma 2.1]. We observe that $|\mathcal{M}| = 2(q - 1)$. Thus to prove Theorem 1.6, we need only to show that for any $g \in \mathbb{F}_q[2V]^{O_2^+(\mathbb{F}_q)}$, we have $g \in \sum_{f \in \mathcal{M}} R \cdot f$. By Example 1.5, it is sufficient to show that $U_{12}^{\alpha_0} \cdot B_1^{\alpha_1} \cdot B_2^{\alpha_2} \cdots B_{q-2}^{\alpha_{q-2}} \in \sum_{f \in \mathcal{M}} R \cdot f$, for any nonzero vector $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{q-2}) \in \mathbb{N}^{q-1}$. By Proposition 6.1, it suffices to show that $U_{12}^{\alpha_0} \in \sum_{f \in \mathcal{M}} R \cdot f$ and $B_1^{\alpha_1} \cdot B_2^{\alpha_2} \cdots B_{q-2}^{\alpha_{q-2}} \in \sum_{f \in \mathcal{M}} R \cdot f$ for any $\alpha_0 \in \mathbb{N}$ and any $(\alpha_1, \ldots, \alpha_{q-2}) \in \mathbb{N}^{q-2}$. The two cases follow from Proposition 6.2 and Proposition 6.4 respectively. $\square$

7. MORE EXAMPLES AND PROOF OF COROLLARY 1.3

Example 7.1. ($\mathbb{F}_q[3V]^{O_2^+(\mathbb{F}_q)}$) Note that in this case, $1 \leqslant |I| \leqslant m - 1 = 2$ and $1 \leqslant |J| \leqslant m - 1 = 2$. Since $s \geqslant 2$, $q = 2^s \geqslant 4$ and $q - 1 \geqslant 3$. Thus $|I| - |J| = 0$ in $\mathcal{D}$. It follows that either $|I| = |J| = 1$ or $|I| = |J| = 2$. Since $I < J$, we must have $|I| = |J| = 1$. Hence, $\mathcal{U} = \mathcal{D}$. Theorem 1.1 tells us that $\mathbb{F}_q[3V]^{O_2^+(\mathbb{F}_q)}$ is generated by the following invariants:

$$
\mathcal{N} = \left\{ N_1, N_2, N_3 \right\}
$$

$$\mathcal{U} = \left\{ U_{12}, U_{13}, U_{23} \right\}$$
$$\mathcal{B} = \left\{ x_1^k x_2^t x_3^{q-1-k-t} + y_1^k y_2^t y_3^{q-1-k-t} \mid 0 \leqslant k, t \leqslant q-1 \right\}.$$

It is not hard to see that $|\mathcal{B}| = q + (q-1) + (q-2) + \cdots + 2 + 1 = \frac{q(q+1)}{2}$. Thus $|\mathcal{S}| = |\mathcal{N}| + |\mathcal{U}| + |\mathcal{B}| = \frac{q(q+1)}{2} + 6$. For instance, when $q = 4$, $|\mathcal{S}| = 16$ and when $q = 8$, $|\mathcal{S}| = 42$.

Example 7.2. $(m \geqslant 4)$ For $\mathbb{F}_q[4V]^{O_2^+(\mathbb{F}_q)}$, there are no $d_{I,J} \in \mathcal{D}$ such that $q - 1 = |J| - |I|$. However, we have one element $x_1 x_2 y_3 y_4 + y_1 y_2 x_3 x_4 \in \mathcal{D} - \mathcal{U}$. When $m \geqslant 5$, for $\mathbb{F}_q[mV]^{O_2^+(\mathbb{F}_q)}$, there exists $d_{I,J} \in \mathcal{D}$ such that $q - 1 = |J| - |I|$. For example, we take $q = 2^2 = 4$ and $m = 5$. Then $x_1 y_2 y_3 y_4 y_5 + y_1 x_2 x_3 x_4 x_5 \in \mathcal{D}$.

Proof of Corollary 1.3. Note that $q = 2^s \geqslant 4$. Proposition 2.3, Example 1.5 and Example 7.1 show that $\beta_{mV}(O_2^+(\mathbb{F}_q)) = q - 1$ for $m = 1, 2, 3$ respectively. Now we suppose $m > 3$. If $m \leqslant q - 1$, then any generator from $\mathcal{B}$ can make $\beta_{mV}(O_2^+(\mathbb{F}_q)) = q - 1$ holds. If $m > q - 1$ and $m = 2n$ is even, then $d_{I,J} \in \mathcal{D}$ with $I = \{1, 2, \ldots, n\}$ and $J = \{n+1, n+2, \ldots, m\}$, implies that $\beta_{mV}(O_2^+(\mathbb{F}_q)) = m$. If $m > q - 1$ and m is odd, then $m - (q - 1)$ is even. We may assume that $m - (q - 1) = 2n$. Then $d_{I,J} \in \mathcal{D}$ with $I = \{1, 2, \ldots, n\}$ and $J = \{n+1, n+2, \ldots, 2n, 2n+1, \ldots, m\}$, implies that $\beta_{mV}(O_2^+(\mathbb{F}_q)) = m$. $\qquad\square$

8. PROOF OF THEOREM 1.7

Proof of Theorem 1.7. Let $\mathcal{D}_1 = \{d_{I,J} : |J| = |I|\}$ and $\mathcal{D}_2 = \{d_{I,J} : |J| = |I| + q - 1\}$. Then $\mathcal{U} \subseteq \mathcal{D}_1$ and $\mathcal{D} = \mathcal{D}_1 \cup \mathcal{D}_2$. By Theorem 1.1, it is sufficient to show that any element in $\mathcal{D}$ is contained in $\mathfrak{A}$, the ideal generated by $\mathcal{N} \cup \mathcal{U} \cup \mathcal{B}$ in $\mathbb{F}_q[mV]$. Our arguments will be completed by showing two subcases: $\mathcal{D}_1 \subseteq \mathfrak{A}$ and $\mathcal{D}_2 \subseteq \mathfrak{A}$.

SUBCASE 1: For any $d_{I,J} \in \mathcal{D}_1$, we suppose the degree of $d_{I,J}$ is $2n$. We use induction on n. When $n = 1$, we may write $d_{I,J} = x_i y_j + y_i x_j$ with $1 \leqslant i < j \leqslant m$. Thus $d_{I,J} = U_{ij} \in \mathfrak{A}$. Now consider any $n > 1$. Let i_1 be the minimal integer in I and j_1 be the minimal integer in J. Note that $i_1 < j_1$, then $d_{I,J} = x_I \cdot y_J + y_I \cdot x_J = x_{i_1} y_{j_1} (x_{I-\{i_1\}} \cdot y_{J-\{j_1\}}) + y_{i_1} x_{j_1} (y_{I-\{i_1\}} \cdot x_{J-\{j_1\}}) = (U_{i_1 j_1} + y_{i_1} x_{j_1})(x_{I-\{i_1\}} \cdot y_{J-\{j_1\}}) + y_{i_1} x_{j_1} (y_{I-\{i_1\}} \cdot x_{J-\{j_1\}}) \equiv_{\mathfrak{A}} (y_{i_1} x_{j_1}) \cdot d_{I-\{i_1\}, J-\{j_1\}}$. Since $d_{I-\{i_1\}, J-\{j_1\}}$ has degree $2(n-1)$, the induction hypothesis implies that $d_{I-\{i_1\}, J-\{j_1\}} \in \mathfrak{A}$. Thus $d_{I,J} \in \mathfrak{A}$.

SUBCASE 2: For any $d_{I,J} \in \mathcal{D}_2$, we let $I = \{i_1, \ldots, i_k\}$ and $J = \{j_1, \ldots, j_k, j_{k+1}, \ldots, j_{k+q-1}\}$, where $1 \leqslant i_1 < \cdots < i_k < j_1 < \cdots < j_{k+q-1} \leqslant m$. We may write

$$d_{I,J} = \prod_{i=i_1}^{i_k} x_i \cdot \prod_{j=j_1}^{j_k} y_j \cdot \prod_{j=j_{k+1}}^{j_{k+q-1}} y_j + \prod_{i=i_1}^{i_k} y_i \cdot \prod_{j=j_1}^{j_k} x_j \cdot \prod_{j=j_{k+1}}^{j_{k+q-1}} x_j$$

$$= \prod_{i=i_1}^{i_k} x_i \cdot \prod_{j=j_1}^{j_k} y_j \cdot \prod_{j=j_{k+1}}^{j_{k+q-1}} y_j + \prod_{i=i_1}^{i_k} y_i \cdot \prod_{j=j_1}^{j_k} x_j \cdot (B_{\overline{1}} + \prod_{j=j_{k+1}}^{j_{k+q-1}} y_j)$$

$$\equiv \left(\prod_{i=i_1}^{i_k} x_i \cdot \prod_{j=j_1}^{j_k} y_j + \prod_{i=i_1}^{i_k} y_i \cdot \prod_{j=j_1}^{j_k} x_j \right) \cdot \prod_{j=j_{k+1}}^{j_{k+q-1}} y_j, \quad \mod (\mathfrak{A}).$$

Since $\prod_{i=i_1}^{i_k} x_i \cdot \prod_{j=j_1}^{j_k} y_j + \prod_{i=i_1}^{i_k} y_i \cdot \prod_{j=j_1}^{j_k} x_j \in \mathcal{D}_1$, it follows from the first subcase that $d_{I,J} \in \mathfrak{A}$. Therefore, $\mathcal{D}_2 \subseteq \mathfrak{A}$, completing the proof. $\qquad\square$

9. Remarks on $O_2^-(\mathbb{F}_q)$ and $\mathbb{F}_q[mV]^{O_2^-(\mathbb{F}_q)}$

In the last section we discuss $O_2^-(\mathbb{F}_q)$ and $\mathbb{F}_q[mV]^{O_2^-(\mathbb{F}_q)}$. To our knowledge, there are no suitable references concerning a detailed description for generators of the group $O_2^-(\mathbb{F}_q)$ in terms of matrix language.

First of all, we need to find out generators of $O_2^-(\mathbb{F}_q)$, which are more complicated than $O_2^+(\mathbb{F}_q)$. Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in O_2^-(\mathbb{F}_q)$ be any element. By the definition, we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} w & 1 \\ 0 & w \end{pmatrix}\begin{pmatrix} a & c \\ b & d \end{pmatrix} - \begin{pmatrix} w & 1 \\ 0 & w \end{pmatrix} = \begin{pmatrix} aw & a+bw \\ cw & c+dw \end{pmatrix}\begin{pmatrix} a & c \\ b & d \end{pmatrix} - \begin{pmatrix} w & 1 \\ 0 & w \end{pmatrix}$$

$$= \begin{pmatrix} a^2w + b^2w + w + ab & acw + bdw + ad + 1 \\ acw + bdw + bc & c^2w + d^2w + w + cd \end{pmatrix}$$

is an alternating matrix, i.e.,

$$(9.1) \qquad\qquad a^2w + b^2w + w + ab = 0$$

$$(9.2) \qquad\qquad c^2w + d^2w + w + cd = 0$$

$$(9.3) \qquad\qquad ad + bc + 1 = 0.$$

CASE 1. Suppose $a = 0$, it follows from Eq. (9.1) and Eq. (9.3) that $b^2 = 1$ and $c = b$. Since $b \in \mathbb{F}_q^\times$ and the order of $\mathbb{F}_q^\times$ is odd, we have $b = c = 1$. It follows from Eq. (9.2) that $d^2w = d$. If $d = 0$, we obtain an orthogonal matrix

$$\sigma := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

If $d \neq 0$, then $d = w^{-1}$ and we have another orthogonal matrix

$$\tau_0 := \begin{pmatrix} 0 & 1 \\ 1 & w^{-1} \end{pmatrix}.$$

CASE 2. Suppose $a \neq 0$, it follows from Eq. (9.3) that $d = \frac{bc+1}{a}$. Combining Eqs. (9.2) and (9.1), we have

$$(9.4) \qquad\qquad a^2w + c^2w + w + ac = 0.$$

Adding Eq. (9.4) to Eq. (9.1), we obtain $(b^2 + c^2)w = a(b+c)$. If $b = c$, we have a family of orthogonal matrices

$$\tau_a := \begin{pmatrix} a & b \\ b & a + bw^{-1} \end{pmatrix},$$

and if $b \neq c$ we have

$$\varepsilon_a := \begin{pmatrix} a & b \\ aw^{-1} + b & a \end{pmatrix}$$

where b is defined by $a^2 w + b^2 w + w + ab = 0$. Note that $\varepsilon_b = \sigma \cdot \tau_a$ for all $a \in \mathbb{F}_q$. Thus $O_2^-(\mathbb{F}_q)$ consists of the following matrices: $\left\{ 1, \sigma, \tau_a, \sigma \cdot \tau_a \mid a \in \mathbb{F}_q \right\}$.

Secondly, we consider the invariant ring $\mathbb{F}_q[mV]^{O_2^-(\mathbb{F}_q)}$. Magma calculations [2] suggest that $\mathbb{F}_q[V]^{O_2^-(\mathbb{F}_q)} = \mathbb{F}_q[x,y]^{O_2^-(\mathbb{F}_q)}$ might be a polynomial algebra with two generators Q and E, of degrees 2 and $q+1$ respectively. We define

$$(9.5) \qquad\qquad E \quad := \quad xy^q + x^q y$$

$$(9.6) \qquad\qquad Q \quad := \quad \mathrm{Tr}^{O_2^-(\mathbb{F}_q)}(x^2).$$

We *claim* that $\mathbb{F}_q[V]^{O_2^-(\mathbb{F}_q)} = \mathbb{F}_q[E, Q]$. Since $|O_2^-(\mathbb{F}_q)| = \deg(E) \cdot \deg(Q)$, we need only to show that the Jacobian determinant

$$\det \begin{pmatrix} \frac{\partial E}{\partial x} & \frac{\partial E}{\partial y} \\ \frac{\partial Q}{\partial x} & \frac{\partial Q}{\partial y} \end{pmatrix} \neq 0,$$

by Kemper [12, Proposition 16]. We write $Q = x^2 + uxy + vy^2$ for some $u, v \in \mathbb{F}_q$. Since Q is an $O_2^-(\mathbb{F}_q)$-invariant, a simple computation shows that $u \neq 0$. Thus

$$\det \begin{pmatrix} \frac{\partial E}{\partial x} & \frac{\partial E}{\partial y} \\ \frac{\partial Q}{\partial x} & \frac{\partial Q}{\partial y} \end{pmatrix} = \begin{pmatrix} y^q & x^q \\ uy & ux \end{pmatrix} = u \cdot E \neq 0,$$

which shows the claim. For the case $m = 2$ and some small q, Magma calculations [2] suggest that $\mathbb{F}_q[2V]^{O_2^-(\mathbb{F}_q)}$ can be generated by $q+5$ invariants: N_1', N_2', U_{12}, and B_k' for $0 \leq k \leq q+1$. This evidence suggests that the approach used in the calculation of $\mathbb{F}_q[mV]^{O_2^+(\mathbb{F}_q)}$ might be applied to study the invariant ring $\mathbb{F}_q[mV]^{O_2^-(\mathbb{F}_q)}$.

ACKNOWLEDGMENTS

References

[1] Bonnafé, C., Kemper, G.: Some complete intersection symplectic quotients in positive characteristic: invariants of a vector and a covector. J. Algebra **335**, 96–112 (2011).

[2] Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system I: the user language. J. Symbolic Comput. **24**, 235–265 (1997).

[3] Campbell, H. E. A., Hughes, I.P, Pollack, R.D.: Rings of invariants and p-Sylow subgroups. Canad. Math. Bull. **34**, 42–47 (1991).

[4] Campbell, H. E. A., Hughes, I.P.: Vector invariants of $U_2(\mathbb{F}_p)$: a proof of a conjecture of Richman. Adv. Math. **126**, 1–20 (1997).

[5] Campbell, H. E. A., Shank, R.J., Wehlau, D.L.: Vector invariants for the two-dimensional modular representation of a cyclic group of prime order. Adv. Math. **225**, 1069–1094 (2010).

[6] Campbell, H. E. A., Wehlau, D.L.: Modular Invariant Theory. Encyclopaedia of Mathematical Sciences, vol. 139. Springer, New York (2011).

[7] Campbell, H. E. A., Wehlau, D.L.: The second main theorem vector for the modular regular representation of C_2. Adv. Math. **252**, 641–651 (2014).

[8] Chen, Y.: On modular invariants of a vector and a covector. Manuscripta Math. **144**, 341–348 (2014).

[9] Chen, Y.: Modular invariants of finite affine linear groups. To appear in Bull. Braz. Math. Soc. (2017). doi: https://doi.org/10.1007/s00574-017-0050-z.

[10] Chen, Y., Wehlau, D.L.: Modular invariants of a vector and a covector: a proof of a conjecture of Bonnafe-Kemper. J. Algebra **472**, 195–21 (2017).

[11] Derksen, H., Kemper, G.: Computational Invariant Theory. Encyclopaedia of Mathematical Sciences, vol. 130. Springer, New York (2002).

[12] Kemper, G.: Calculating invariant rings of finite groups over arbitrary fields. J. Symbolic Comput. **21**, 351–366 (1996).

[13] Neusel, M.D., Smith, L.: Invariant Theory of Finite Groups. Mathematics Surveys and Monographs, vol. 94. Amer. Math. Soc., Providence (2002).

[14] Richman, D.R.: On vector invariants over finite fields. Adv. Math. **81**, 30–65 (1990).

[15] Shank, R.J., Wehlau, D.L.: Computing modular invariants of p-groups. J. Symbolic Comput. **34**, 307–327 (2002) .

[16] Symonds, P.: On the Castelnuovo-Mumford regularity of rings of polynomial invariants. Ann. Math. **174**, 499–517 (2011).

[17] Tang, Z., Wan, Z.-X.: A matrix approach to the rational invariants of certain classical groups over finite fields of characteristic two. Finite Fields Appl. **12**, 186–210 (2006).

[18] Wan, Z.-X.: Geometry of Classical Groups over Finite Fields. Science Press, Beijing (2002).

[19] Wehlau, D.L.: Invariants for the modular cyclic group of prime order via classical invariant theory. J. Eur. Math. Soc. **15**, 775–803 (2013).

[20] Weyl, H.: The classical groups: their invariants and representations. Princeton Landmarks in Mathematics, fifteenth printing. Princeton University Press, Princeton (1997).

School of Mathematics and Statistics, Northeast Normal University, Changchun 130024, P.R. China

E-mail address: ychen@nenu.edu.cn