POLYNOMIAL INVARIANTS OF ORTHOGONAL GROUPS OF FINITE CHARACTERISTICS

§1. Introduction.

Lrt $\mathbb{F}_q$ be the Galois field with q elements, and $V=\mathbb{F}_q^n$ be the vector space. Let G be a finite subgroup of $GL(V)$. G induces a linear action on the symmetric algebra $\mathbb{F}_q[x_1,\dots,F_n]$. The invariant subring is

$$\mathbb{F}_q[x_1,\dots,F_n]^G=\{f\in\mathbb{F}_q[x_1,\dots,F_n]:\sigma(f)=f \text{ for all } \sigma\in G\}$$

A problem on Invariant Theory is to find the invariant subrings. If $G=GL_n(\mathbb{F}_q)$ or $SL_n(\mathbb{F}_q)$, the result is due to Dickson[6,1911]. If $G=Sp_{2n}(\mathbb{F}_q)$, it is solved by Carlisle and Kropholler[3;1]. When $G=U_n(\mathbb{F}_{q^2})$, this problem is settled by us in [5]. If $G=O_n(\mathbb{F}_q)$, we have found the invariants for $n\le 4$[4]. In this paper, we will find the invariant subrings of $O_n^+(\mathbb{F}_q)$ for all n, and we also prove that the invariant subring is complete intersection.

Let q be a power of odd prime number and $\mathbb{F}_q$ be the Galois field with q elements. Let $V=\mathbb{F}_q$ and $R=\mathbb{F}_q[x_1,\dots,x_n]$ be the associate symmetric algebra.
Consider the quadratic form

$$Q_n=\epsilon_1x_1^2+\epsilon_2x_2^2+\cdots+\epsilon_nx_n^2,\epsilon_i\in\mathbb{F}_q^\times. \tag{1-1}$$

and let $O_n(\mathbb{F}_q)$ be the orthogonal group associated with the o Q_n. It is well-known that all quadratic forms are equivalent to one of the following two special families:

$$\begin{aligned}Q_n^+&=X_1^2-X_2^2+X_3^2-\cdots+(-1)^nX_{n-1}^2+(-1)^{n+1}X_n^2,\ n\ge 1;\\ Q_n^-&=X_1^2-\epsilon X_2^2+\epsilon X_3^2-\cdots+(-1)^n\epsilon X_{n-1}^2+(-1)^{n+1}\epsilon X_n^2,\quad n\ge 1\end{aligned} \tag{1-2}$$

where ϵ is a non-square in $\mathbb{F}_q^\times$. The diof them are $\delta(Q_n^+)=(-1)^{\lfloor\frac{n}{2}\rfloor}$; $\delta(Q_n^-)=(-1)^{\frac{n}{2}}\epsilon$ if n is even, $\delta(Q_n^-)=(-1)^{\frac{n-1}{2}}$ if n is odd.
Since we are interesting on the orthogonal groups, it is known that there are three types: $O_n^+(\mathbb{F}_q)$, n is even or odd; $O_n^-(\mathbb{F}_q)$, n is even . The orders of these groups are the following:

Proposition 1.1. [7] *The order of the orthogonal groups are*

$$\begin{aligned}|O_n^+(\mathbb{F}_q)|=&\begin{cases}2(q^{n-1}-1)q^{n-2}(q^{n-3}-1)q^{n-4}\cdots(q^2-1)q, & \text{if } n \text{ is odd;}\\ 2(q^{n-1}-q^{\frac{n}{2}-1})(q^{n-2}-1)q^{n-3}\cdots(q^2-1)q, & \text{if } n \text{ is even,}\end{cases}\\ |O_n^-(\mathbb{F}_q)|=&2(q^{n-1}-q^{\frac{n}{2}-1})(q^{n-2}-1)q^{n-3}\cdots(q^2-1)q,\quad \text{if } n \text{ is even.}\end{aligned}$$

The orthogonal group induces a linear action on R. We want to find the invariant subrings $\mathbb{F}_q[x_1,x_2,\dots,x_n]^{O_n(\mathbb{F}_q)}=\{f\in R:\sigma(f)=F \text{ for all } \sigma\in O_n(\mathbb{F}_q)\}$. The answer of the corresponding problem in function fields is

Theorem 1.2. *[2] The invariant subfield is*

$$\mathbb{F}_q(x_1, x_2, \dots, x_n)^{O_n(\mathbb{F}_q)} = \mathbb{F}_q(Q_{n0}, Q_{n1}, \dots, Q_{n,n-1})$$

where

$$Q_{ni} = \epsilon_1 x_1^{q^i+1} + \epsilon_2 x_2^{q^i+1} + \cdots + \epsilon_n x_n^{q^i+1}. \tag{1-3}$$

Notations. (a) Let M be an $m \times n$ matrix, S be a subset of $\{1, 2, \dots, m\}$ and T a subset of $\{1, 2, \cdots, n\}$. Then we denote $M_{S;T}$ to be the submatrix of M obtained by deleting the rows in S and the columns in T. If $S = \{i\}$ and $T = \{j\}$, we always denote M_{ij} instead of $M_{S;T}$.

(b) The Legendre symbol is defined as

$$\left(\frac{\delta}{q}\right) = \delta^{\frac{q-1}{2}} = 1, \text{if } \delta \text{ is a square in } \mathbb{F}_q^\times; \qquad \left(\frac{\delta}{q}\right) = \delta^{\frac{q-1}{2}} = -1, \text{if } \delta \text{ is a non-square in } \mathbb{F}_q^\times. \tag{1-4}$$

(c) We define the weight of variables as follows.

$$\begin{aligned} &\operatorname{wt} x_i = \operatorname{wt} y_i = 1 \text{ for all } i; \\ &\operatorname{wt} X_i = q^i + 1, \operatorname{wt} T = 1. \end{aligned} \tag{1-5}$$

§2. Preliminary Results and the Statement of the Main Theorem for Odd n.

We first consider the infinite dimensional matrix

$$\mathbf{M}(X_0, X_1, X_2, \cdots) = \begin{bmatrix} X_0 & X_1 & X_2 & X_3 & X_4 & \cdots \\ X_1 & X_0^q & X_1^q & X_2^q & X_3^q & \cdots \\ X_2 & X_1^q & X_0^{q^2} & X_1^{q^2} & X_2^{q^2} & \cdots \\ X_3 & X_2^q & X_1^{q^2} & X_0^{q^3} & X_1^{q^3} & \cdots \\ X_4 & X_3^q & X_2^{q^2} & X_1^{q^3} & X_0^{q^4} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{bmatrix}.$$

The (i,j)-entry of $\mathbf{M}$ is $X_{|j-i|}^{q^{\min(i-1,j-1)}}$. Let $\mathbf{M}^{(n)}$ be the submatrix of the first n rows and n columns. We define four sequences f_n, g_n, f_n', g_n' of polynomials which are essential in this paper. In fact, we define g_n' as the quotient of two polynomials, and we will show that they are actually polynomials in Lemma 2.5.

Definition 2.1. *Define* $f_0 = 1, \quad f_n = \det \mathbf{M}^{(n)} \in \mathbb{F}_q[X_0, X_1, \cdots, X_{n-1}], n \geq 1;$
$$f_0' = 1, \quad f_n' = \det \mathbf{M}_{1;n+1}^{(n+1)} \in \mathbb{F}_q[X_0, X_1, \cdots, X_n], n \geq 1.$$

For example, $f_1 = X_0, f_2 = X_0^{q+1} - X_1^2;\ \ f_1' = X_1, f_2' = X_1^{q+1} - X_0^q X_2$. It is easy to see that

$$f_n = -f_{n-2}^{\ q} X_{n-1}^2 + \phi_1(X_0, X_1, \cdots, X_{n-1}), \quad \deg_{X_{n-1}} \phi_1 = 1 \ \text{ for } \ n \geq 3. \tag{2-1}$$

$$f_n' = (-1)^{n+1} f_{n-1}^{\ q} X_n + {f_{n-2}'}^{q} X_{n-1}^{q+1} + \phi_2(X_0, X_1, \cdots, X_{n-1}), \quad \deg_{X_{n-1}} \phi_2 = q \ \text{ for } \ n \geq 3. \tag{2-2}$$

Obviously, f_1 and f_2 are relatively prime. Suppose that f_{n-1} and f_{n-2} are relatively prime. Then from (2-1), it follows that f_n and f_{n-1} are relatively prime. Moreover, from (2-2), we see that

$$f_n \text{ and } f_n' \text{ are relatively prime for all } n. \tag{2-3}$$

Definition 2.2.

$$g_n^+ = \begin{cases} f_n' - f_n^{\frac{q+1}{2}}, & \text{for } n \equiv 0,1 \pmod 4 \\ f_n' + (-f_n)^{\frac{q+1}{2}}, & \text{for } n \equiv 2,3 \pmod 4); \end{cases}$$

$$g_n^- = \begin{cases} f_n' + f_n^{\frac{q+1}{2}}, & \text{for } n \equiv 0,1 \pmod 4 \\ f_n' - (-f_n)^{\frac{q+1}{2}}, & \text{for } n \equiv 2,3 \pmod 4). \end{cases}$$

Definition 2.3. $g_{-1}'^{\pm} = 1; g_0'^{+} = X_0, g_0'^{-} = 1;$

$$g_n'^{\pm} = g_n^{\pm}/(g_{n-2}'^{\mp})^q \quad \textit{for } n \geq 1.$$

Next we show that $g_n'^{\pm}$ are actually polynomials in Lemma 2.5. We first state a Lemma. We will use part (a) here and use part (b) in Lemma 3.8. This Lemma has also appeared in [??], now we give a direct proof.

Lemma 2.4. *Let R be a ring, and $M \in M_n(R)$. We have the following two identities.*
(a) *Let $N = M_{1,n;1,n} \in M_{n-2}(R)$. Then*

$$\det M \cdot \det N = \det M_{nn} \det M_{11} - \det M_{n1} \det M_{1n}.$$

(b) *Let $N' = M_{n-1,n;1,n} \in M_{n-2}(R)$. Then*

$$\det M \cdot \det N' = \det M_{nn} \det M_{n-1,1} - \det M_{n1} \det M_{n-1,n}.$$

Proof. The two identities are easily seen to be equivalent. In fact, let

$$M' = \begin{bmatrix} M_2 \\ M_3 \\ \vdots \\ M_{n-1} \\ M_1 \\ M_n \end{bmatrix}.$$

Apply (b) to M' and get

$$\begin{aligned} \det M' \det N =& \det M'_{nn} \det M'_{n-1,1} - \det M'_{n1} \det M_{n-1,n} \\ (-1)^{n-2} \det M \det N =& (-1)^{n-2} \det M_{nn} \det M_{11} - (-1)^{n-2} \det M_{n1} \det M_{1n}, \end{aligned}$$

(a) follows. So we only prove (b) below. Let M_i be the determinant of the matrix we obtain by deleting the ith row, the last row, the first column and the last column from M. Multiply the $(n-1)$th row of M by M_{n-1} (which is $\det N'$), then add to this row the ith row multiplied by $(-1)^{n-1-i} M_i$ for all $1 \leq i \leq n-2$. We will find that the $(n-1)$th row of M, after the above procedure, becomes $(\,(-1)^n M_{nn}, 0, 0, \ldots, 0, M_{n1})$. Expand $\det M$ along this row now, we get the identity in (b).

Applying Lemma 2.4(a) to $M = \mathbf{M}^{(n)}$, we have

$$f_{n-2}^q f_n = f_{n-1}^{q+1} - f_{n-1}'^{\,2} = -(f_{n-1}' + f_{n-1}^{\frac{q+1}{2}})(f_{n-1}' - f_{n-1}^{\frac{q+1}{2}}) = -g_{n-1}^+ g_{n-1}^-. \tag{2-4}$$

On the other hand, from (2-1) and (2-2) we have, for $n \equiv 0, 1 (\mathrm{mod}\ 4)$,

$$\begin{aligned}
g_n^{\pm} &= f_n' \mp f_n^{\frac{q+1}{2}} \\
&= (-1)^{n+1} f_{n-1}^q X_n + {f'}_{n-2}^{q} X_{n-1}^{q+1} + \phi_2 \mp (-f_{n-2}^q X_{n-1}^2 + \phi_1)^{\frac{q+1}{2}} \\
&= (-1)^{n+1} f_{n-1}^q X_n + [f_{n-2}' \mp (-f_{n-2})^{\frac{q+1}{2}}]^q X_{n-1}^{q+1} + \phi_3(X_0, X_1, \ldots, X_{n-1}) \\
&= (-1)^{n+1} f_{n-1}^q X_n + g_{n-2}^{\mp\, q} X_{n-1}^{q+1} + \phi_3(X_0, X_1, \ldots, X_{n-1}). \qquad (2\text{-}5)
\end{aligned}$$

where $\deg_{X_{n-1}} \phi_3 = q$. The last equality follows from $n-2 \equiv 2, 3 (\mathrm{mod}\ 4)$. It can be checked that the same formula holds for $n \equiv 2, 3 (\mathrm{mod}\ 4)$. (We just need to replace $\pm$ by $\mp$ in the first three lines.)

To prove that $g_n'^{\pm}$ are polynomials, we prove the following

Lemma 2.5. (a) $f_n = (-1)^{\lfloor \frac{n}{2} \rfloor} {g'}_{n-1}^{+} {g'}_{n-1}^{-}$.
(b) $({g'}_{n-2}^{\mp})^q | g_n^{\pm}$.

Proof. We prove by induction on n. Since $g_2^- = (X_1^{q+1} - X_0^q X_2) - (X_1^2 - X_0^{q+1})^{\frac{q+1}{2}}$, so $X_0^q | g_2'^-$. (a) and (b) hold for $n = 1, 2$ trivially. Given $n \geq 3$, suppose these formulae hold for $f_k, k \leq n-1$. We first prove (a). From (2-4),

$$f_{n-2}^q f_n = -g_{n-1}^+ g_{n-1}^-.$$

By inductive hypothesis on (a), $f_{n-2} = (-1)^{\lfloor \frac{n-2}{2} \rfloor} {g'}_{n-3}^{+} {g'}_{n-3}^{-}$, so

$$f_n = (-1)^{\lfloor \frac{n}{2} \rfloor} \frac{g_{n-1}^+}{({g'}_{n-3}^{-})^q} \cdot \frac{g_{n-1}^-}{({g'}_{n-3}^{+})^q} = (-1)^{\lfloor \frac{n}{2} \rfloor} {g'}_{n-1}^{+} {g'}_{n-1}^{-}.$$

Two fractions in the above are polynomials by inductive hypotheses on (b). Now we prove (b). By (2-4) again and by inductive hypotheses on (a),

$$f_{n-1}^q f_{n+1} = -g_n^+ g_n^-,$$
$$f_{n-1}^q = (-1)^{\lfloor \frac{n-1}{2} \rfloor} ({g'}_{n-2}^{+})^q ({g'}_{n-2}^{-})^q.$$

By (2-3) , g_n^+ and g_n^- are relatively prime, so ${g'}_{n-2}^{+}$ divides just one of g_n^+ and g_n^-. Since ${g'}_{n-2}^{+} \in \mathbb{F}_q[X_0, X_1, \cdots, X_{n-2}]$ and observing the X_{n-1}^{q+1}-term in (2-5), we see that ${g'}_{n-2}^{+} | g_n^-$ and$({g'}_{n-2}^{+})^q | g_n^-$.

Lemma 2.6. $g_n'^{\pm} = (-1)^{\lfloor \frac{n}{2} \rfloor} {g'}_{n-2}^{\pm\, q} X_n + \phi_3'(X_0, X_1, \ldots, X_{n-1})$.

Proof. By (2-5), we have

$$\begin{aligned}
g_n'^{\pm} = g_n^{\pm} / ({g'}_{n-2}^{\mp})^q &= (-1)^{n+1} \frac{f_{n-1}^{\ q}}{({g'}_{n-2}^{\mp})^q} X_n + \phi_3'(X_0, X_1, \ldots, X_{n-1}) \\
&= (-1)^{\lfloor \frac{n}{2} \rfloor} {g'}_{n-2}^{\pm\, q} X_n + \phi_3'(X_0, X_1, \ldots, X_{n-1}).
\end{aligned}$$

The last equality follows from Lemma 2.5(a).

Now we introduce the other four sequences of polynomials.

Definition 2.7. *Given $\epsilon \in \mathbb{F}_q^\times$. Define the polynomials*

$$\begin{aligned} F_{n,\epsilon}(X_0,\cdots,X_{n-1};T) &:= f_n(X_0+\epsilon T^2, X_1+\epsilon T^{q+1},\cdots,X_{n-1}+\epsilon T^{q^{n-1}+1}),\\ F'_{n,\epsilon}(X_0,\cdots,X_n;T) &:= f'_n(X_0+\epsilon T^2, X_1+\epsilon T^{q+1},\cdots,X_n+\epsilon T^{q^n+1}),\\ G^\pm_{n,\epsilon}(X_0,\cdots,X_n;T) &:= g^\pm_n(X_0+\epsilon T^2, X_1+\epsilon T^{q+1},\cdots,X_n+\epsilon T^{q^n+1}),\\ G'^{\pm}_{n,\epsilon}(X_0,\cdots,X_n;T) &:= g'^{\pm}_n(X_0+\epsilon T^2, X_1+\epsilon T^{q+1},\cdots,X_n+\epsilon T^{q^n+1}). \end{aligned}$$

We often denote $F_n(T)$ instead of $F_{n,\epsilon}(T)$ for short, if ϵ is understood. Now we give explicit forms for $F_n(T)$ and $F'_n(T)$.

Lemma 2.8. *Let f_{ij} and f'_{ij} be the (i,j)-minor of f_n and f'_n, respectively, $1\le i,\ j\le n$. Then*
(a) $F_n(T) = f_n + \sum_{1\le i,j\le n}(-1)^{i+j}\epsilon\, f_{ij}\ T^{q^{i-1}+q^{j-1}}$,
(b) $F'_n(T) = f'_n + \sum_{1\le i,j\le n}(-1)^{i+j}\epsilon\, f'_{ij}\ T^{q^{i}+q^{j-1}}$.

Proof. (a) Let $\mathbf{T} = (\epsilon T^{q^{i-1}+q^{j-1}})_{n\times n}$, Then $F_n = \det(\mathbf{M}^{(n)}+\mathbf{T})$. Note that $\mathrm{rank}\mathbf{T} = 1$. Hence when we expand the determinant F_n by multilinearity on columns, the terms which two columns of $\mathbf{T}$ are taken must be zero. Then the result can be deduced easily. The proof of (b) is similar.

Now we describe the weight, the T-degrees and the leading coefficients of the polynomials F's and G's.

Lemma 2.9. *Using the definition of weight defined in* (1-4)*, we have that $F_{n,\epsilon}, F'_{n,\epsilon} G_{n,\epsilon}, G'_{n,\epsilon}$ are homogeneous polynomials. The weights are as following.*
(a) $wt\,F_{n,\epsilon} = 2(\frac{q^n-1}{q-1}), wt\,F'_{n,\epsilon} = (q+1)(\frac{q^n-1}{q-1}), wt\,G_{n,\epsilon}^{\ \pm} = (q+1)(\frac{q^n-1}{q-1})$.
(b) $wt\,G'^{\pm}_{n,\epsilon} = \frac{q^{n+1}-1}{q-1}$, *if n is odd* ; $\begin{cases} wt\,G'^{\ +}_{n,\epsilon} = (q^{\frac{n}{2}}+1)(\frac{q^{\frac{n}{2}+1}-1}{q-1}) \\ wt\,G'^{\ -}_{n,\epsilon} = (q^{\frac{n}{2}+1}+1)(\frac{q^{\frac{n}{2}}-1}{q-1}) \end{cases}$ *if n is even.*

Proof. From the definition of F_n, we see that it is homogeneous if f_n is, and $\mathrm{wt}F_n = \mathrm{wt}f_n$. The weight of f_n can be computed from the definition of f_n.

Lemma 2.10. *Regarding the polynomials as polynomial in T, then*
(a) $\deg F_{n,\epsilon} = 2q^{n-1}$, $\quad\deg F'_{n,\epsilon} = q^{n-1}(q+1)$.
(b) $\deg\, G^+_{1,\epsilon} = q - (\frac{\epsilon}{q})$, $\quad\deg G^-_{1,\epsilon} = q + (\frac{\epsilon}{q})$; $\quad\deg\, G^+_{n,\epsilon} = \deg G^-_{n,\epsilon} = q^{n-1}(q+1), n\ge 2$.
(c) $\begin{cases} \deg G'^{+}_{n,\epsilon} = q^n + q^{\frac{n}{2}}, \\ \deg G'^{-}_{n,\epsilon} = q^n - q^{\frac{n}{2}}, \end{cases}$ *if n is even;* $\begin{cases} \deg G'^{+}_{n,\epsilon} = q^n - (\frac{\epsilon}{q})q^{\frac{n-1}{2}}, \\ \deg G'^{-}_{n,\epsilon} = q^n + (\frac{\epsilon}{q})q^{\frac{n-1}{2}}, \end{cases}$ *if n is odd.*

Proof. (a) follows from Lemma 2.8. (b) follows from (a). (c) is proved by induction.

Lemma 2.11. *Let $\mathrm{lc}\,F$ denote the leading coefficient of $F(T)$. Then*
(a) $\mathrm{lc}\,F_{n,\epsilon} = \epsilon f_{n-1}$, $\quad\mathrm{lc}\,F'_{n,\epsilon} = \epsilon f'_{n-1}$
(b) *If* $(\frac{\epsilon}{q}) = 1$, *then* $\mathrm{lc}\,G^+_{1,\epsilon} = -\frac{1}{2}X_0$ *and* $\mathrm{lc}\,G^-_{1,\epsilon} = 2\epsilon$.
If $(\frac{\epsilon}{q}) = -1$, *then* $\mathrm{lc}\,G^+_{1,\epsilon} = 2\epsilon$ *and* $\mathrm{lc}\,G^-_{1,\epsilon} = -\frac{1}{2}X_0$.
(c) *For $n\ge 2$,*

$$\mathrm{lc}\,G^\pm_{n,\epsilon} = \begin{cases} \epsilon g^\pm_{n-1}, & \text{if } n \text{ is even and } (\frac{-\epsilon}{q}) = 1;\\ \epsilon g^\pm_{n-1}, & \text{if } n \text{ is odd and } (\frac{\epsilon}{q}) = 1;\\ \epsilon g^\mp_{n-1}, & \text{otherwise.}\end{cases}$$

(d) *If n is odd, then*

$$\operatorname{lc} G'^{+}_{n,\epsilon} = \begin{cases} (-1)^{\frac{n+1}{2}}\frac{1}{2}g'^{+}_{n-1}, & \textit{for } (\frac{\epsilon}{q})=1,\\ (-1)^{\frac{n-1}{2}}2\epsilon g'^{-}_{n-1}, & \textit{for } (\frac{\epsilon}{q})=-1; \end{cases} \quad \operatorname{lc} G'^{-}_{n,\epsilon} = \begin{cases} (-1)^{\frac{n-1}{2}}2\epsilon g'^{-}_{n-1}, & \textit{for } (\frac{\epsilon}{q})=1,\\ (-1)^{\frac{n+1}{2}}\frac{1}{2}g'^{+}_{n-1}, & \textit{for } (\frac{\epsilon}{q})=-1. \end{cases}$$

If n is even, then

$$\operatorname{lc} G'^{+}_{n,\epsilon} = \begin{cases} \epsilon g'^{+}_{n-1}, & \textit{for } (\frac{-\epsilon}{q})=1,\\ \epsilon g'^{-}_{n-1}, & \textit{for } (\frac{-\epsilon}{q})=-1; \end{cases} \quad \operatorname{lc} G'^{-}_{n,\epsilon} = \begin{cases} g'^{-}_{n-1}, & \textit{for } (\frac{-\epsilon}{q})=1,\\ g'^{+}_{n-1}, & \textit{for } (\frac{-\epsilon}{q})=-1. \end{cases}$$

Proof. (a) follows from Lemma 2.8. (b) can be checked by direct computation.
(c) If $n \equiv 0 (\text{mod } 4)$, the leading coefficient of $G^{\pm}_n = F'_n \mp F_n^{\frac{q+1}{2}}$ is

$$\epsilon f'_{n-1} \mp (\epsilon f_{n-1})^{\frac{q+1}{2}} = \epsilon[f'_{n-1} \pm \left(\frac{-\epsilon}{q}\right)(-f_{n-1})^{\frac{q+1}{2}}] = \begin{cases} \epsilon g^{\pm}_{n-1}, & \text{for } (\frac{-\epsilon}{q})=1,\\ \epsilon g^{\mp}_{n-1}, & \text{for } (\frac{-\epsilon}{q})=-1, \end{cases}$$

since $n-1 \equiv 3(\text{mod } 4)$.

If $n \equiv 1(\text{mod } 4)$, then the leading coefficient of $G^{\pm}_n = F'_n \mp F_n^{\frac{q+1}{2}}$ is

$$\epsilon f'_{n-1} \mp (\epsilon f_{n-1})^{\frac{q+1}{2}} = \epsilon[f'_{n-1} \mp \left(\frac{\epsilon}{q}\right) f_{n-1}^{\frac{q+1}{2}}] = \begin{cases} \epsilon g^{\pm}_{n-1}, & \text{for } (\frac{\epsilon}{q})=1,\\ \epsilon g^{\mp}_{n-1}, & \text{for } (\frac{\epsilon}{q})=-1, \end{cases}$$

since $n-1 \equiv 0(\text{mod } 4)$.

If $n \equiv 2(\text{mod } 4)$, then the leading coefficient of $G^{\pm}_n = F'_n \pm F_n^{\frac{q+1}{2}}$ is

$$\epsilon f'_{n-1} \pm (-\epsilon f_{n-1})^{\frac{q+1}{2}} = \epsilon[f'_{n-1} \mp \left(\frac{-\epsilon}{q}\right) f_{n-1}^{\frac{q+1}{2}}] = \begin{cases} \epsilon g^{\pm}_{n-1}, & \text{for } (\frac{-\epsilon}{q})=1,\\ \epsilon g^{\mp}_{n-1}, & \text{for } (\frac{-\epsilon}{q})=-1, \end{cases}$$

since $n-1 \equiv 1(\text{mod } 4)$.

If $n \equiv 3(\text{mod } 4)$, then the leading coefficient of $G^{\pm}_n = F'_n \pm F_n^{\frac{q+1}{2}}$ is

$$\epsilon f'_{n-1} \pm (-\epsilon f_{n-1})^{\frac{q+1}{2}} = \epsilon[f'_{n-1} \pm \left(\frac{\epsilon}{q}\right)(-f_{n-1})^{\frac{q+1}{2}}] = \begin{cases} \epsilon g^{\pm}_{n-1}, & \text{for } (\frac{\epsilon}{q})=1,\\ \epsilon g^{\mp}_{n-1}, & \text{for } (\frac{\epsilon}{q})=-1, \end{cases}$$

since $n-1 \equiv 2(\text{mod } 4)$.
(d) The cases $n = 1, 2$ can be checked directly. Suppose $n \geq 3$ is odd and $(\frac{\epsilon}{q}) = 1$. Then by induction,

$$\operatorname{lc} G'^{+}_{n,\epsilon} = \operatorname{lc} G^{+}_{n,\epsilon}/(\operatorname{lc} G'^{-}_{n-2,\epsilon})^q = \epsilon g^{+}_{n-1}/((-1)^{\frac{n-3}{2}}2\epsilon g'^{-}_{n-3})^q = (-1)^{\frac{n+1}{2}}\frac{1}{2}g'^{+}_{n-1}.$$

$$\operatorname{lc} G'^{-}_{n,\epsilon} = \operatorname{lc} G^{-}_{n,\epsilon}/(\operatorname{lc} G'^{+}_{n-2,\epsilon})^q = \epsilon g^{-}_{n-1}/((-1)^{\frac{n-1}{2}}\frac{1}{2}\epsilon g'^{+}_{n-3})^q = (-1)^{\frac{n-1}{2}}2\epsilon g'^{-}_{n-1}.$$

The other cases also proved by induction.

Consider the quadratic form Q_n defined in (1-1) and the polynomials Q_{ni} defined in (1-3). Note that

$$\begin{aligned}&\begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ x_1^q & x_2^q & \cdots & x_n^q \\ \vdots & \vdots & & \vdots \\ x_1^{q^{n-1}} & x_2^{q^{n-1}} & \cdots & x_n^{q^{n-1}} \end{bmatrix} \begin{bmatrix} \epsilon_1 & & & \\ & \epsilon_2 & & \\ & & \ddots & \\ & & & \epsilon_n \end{bmatrix} \begin{bmatrix} x_1 & x_1^q & \cdots & x_1^{q^{n-1}} \\ x_2 & x_2^q & \cdots & x_2^{q^{n-1}} \\ \vdots & \vdots & & \vdots \\ x_n & x_n^q & \cdots & x_n^{q^{n-1}} \end{bmatrix} \\ =& \begin{bmatrix} Q_{n0} & Q_{n1} & Q_{n2} & \cdots & Q_{n,n-1} \\ Q_{n1} & Q_{n0}^q & Q_{n1}^q & \cdots & Q_{n,n-2}^q \\ \vdots & \vdots & \vdots & & \vdots \\ Q_{n,n-1} & Q_{n,n-2}^q & Q_{n,n-3}^{q^2} & \cdots & Q_{n0}^{q^{n-1}} \end{bmatrix} \end{aligned} \tag{2-6}$$

and

$$\begin{aligned}&\begin{bmatrix} x_1^q & x_2^q & \cdots & x_n^q \\ x_1^{q^2} & x_2^{q^2} & \cdots & x_n^{q^2} \\ \vdots & \vdots & & \vdots \\ x_1^{q^{n-1}} & x_2^{q^{n-1}} & \cdots & x_n^{q^{n-1}} \end{bmatrix} \begin{bmatrix} \epsilon_1 & & & \\ & \epsilon_2 & & \\ & & \ddots & \\ & & & \epsilon_n \end{bmatrix} \begin{bmatrix} x_1 & x_1^q & \cdots & x_1^{q^{n-1}} \\ x_2 & x_2^q & \cdots & x_2^{q^{n-1}} \\ \vdots & \vdots & & \vdots \\ x_n & x_n^q & \cdots & x_n^{q^{n-1}} \end{bmatrix} \\ =& \begin{bmatrix} Q_{n1} & Q_{n0}^q & Q_{n1}^q & \cdots & Q_{n,n-2}^q \\ Q_{n2} & Q_{n1}^q & Q_{n0}^{q^2} & \cdots & Q_{n,n-3}^{q^2} \\ \vdots & \vdots & \vdots & & \vdots \\ Q_{n,n} & Q_{n,n-1}^q & Q_{n,n-2}^{q^2} & \cdots & Q_{n1}^{q^{n-1}} \end{bmatrix} \end{aligned} \tag{2-7}$$

Let $D = \det \begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ x_1^q & x_2^q & \cdots & x_n^q \\ \vdots & \vdots & & \vdots \\ x_1^{q^{n-1}} & x_2^{q^{n-1}} & \cdots & x_n^{q^{n-1}} \end{bmatrix}$ and the discriminant $\delta(Q_n) = \epsilon_1\epsilon_2\cdots\epsilon_n$. Taking the determinants of (2-6) and (2-7),we have

$$D^2 \cdot \delta(Q_n) = f_n(Q_{n0}, Q_{n1}, \cdots, Q_{n,n-1})$$

and

$$D^{q+1} \cdot \delta(Q_n) = f_n'(Q_{n0}, Q_{n1}, \cdots, Q_{n,n}).$$

Canceling D from above, we get

$$\begin{aligned} &f_n'(Q_{n0}, Q_{n1}, \cdots, Q_{n,n}) - \delta(Q_n)^{\frac{q-1}{2}} f_n(Q_{n0}, Q_{n1}, \cdots, Q_{n,n-1})^{\frac{q+1}{2}} \\ =&f_n'(Q_{n0}, Q_{n1}, \cdots, Q_{n,n}) - \left(\frac{\delta(Q_n)}{q}\right) f_n(Q_{n0}, Q_{n1}, \cdots, Q_{n,n-1})^{\frac{q+1}{2}} \\ =&0 \quad . \end{aligned} \tag{2-8}$$

where the Legendre symbol is defined in (1-4).

Now we discuss two special families of quadratic forms Q_n^+ and Q_n^- defined in (1-2). From (2-8), we get

Lemma 2.12. $g_n'^{+}(Q_{n0}^+, Q_{n1}^+, \cdots, Q_{nn}^+) = 0$,
$g_n'^{-}(Q_{n0}^-, Q_{n1}^-, \cdots, Q_{nn}^-) = 0$ *for even n.*
$g_n'^{+}(Q_{n0}^-, Q_{n1}^-, \cdots, Q_{nn}^-) = 0$ *for odd n.*

Proof. If $n \equiv 0, 1 (\text{mod } 4)$, then $\delta(Q_n^+) = 1$. So (2-8) says that $(f_n' - f_n^{\frac{q+1}{2}})(Q_{n0}^+, Q_{n1}^+, \cdots, Q_{nn}^+)$ $= 0$. If $n \equiv 2, 3 (\text{mod } 4)$, then $\delta(Q_n^+) = -1$. So $(f_n' - (-1)^{\frac{q-1}{2}} f_n^{\frac{q+1}{2}})(Q_{n0}^+, Q_{n1}^+, \cdots, Q_{nn}^+) = 0$. In any case, by Definition 2.2, $g_n^+(Q_{n0}^+, Q_{n1}^+, \cdots, Q_{nn}^+) = 0$. Since $g_{n-2}'^{\,-}$ involves only $n-1$ variables, and $Q_{n0}^+, Q_{n1}^+, \cdots, Q_{n,n-1}^+$ are algebraically independent, so $g_{n-2}'^{\,-}(Q_{n0}^+, Q_{n1}^+, \cdots, Q_{n,n-2}^+)$ $\neq 0$. Thus $g_n'^{\,+}(Q_{n0}^+, Q_{n1}^+, \cdots, Q_{n,n}^+) = 0$.

The case Q_n^- can be proved similarly. $\delta(Q_n^-) = \begin{cases} (-1)^{\frac{n-1}{2}} & n \text{ is odd;} \\ (-1)^{\frac{n}{2}}\epsilon & n \text{ is even.} \end{cases}$. If $n \equiv 0 (\text{mod} 4)$, then $f_n' - (\frac{\epsilon}{q}) f_n^{\frac{q+1}{2}} = f_n' + f_n^{\frac{q+1}{2}} = g_n^-$; if $n \equiv 2 (\text{mod} 4)$, then $f_n' - (\frac{-\epsilon}{q}) f_n^{\frac{q+1}{2}} = f_n' - (-f_n)^{\frac{q+1}{2}} = g_n^-$; if $n \equiv 1 (\text{mod} 4)$, then $f_n' - f_n^{\frac{q+1}{2}} = g_n^+$; if $n \equiv 3 (\text{mod} 4)$, then $f_n' + f_n^{\frac{q+1}{2}} = g_n^+$.

Lemma 2.13. (a) *For all* $n \geq 1$, $G_{n-1,\epsilon}'^{+}(Q_{n0}^+, Q_{n1}^+, \cdots, Q_{n,n-1}^+; X_n) = 0$, *where* $\epsilon = (-1)^n$;
(b) *For any positive even integer* n, $G_{n-1,\epsilon}'^{+}(Q_{n0}^-, Q_{n1}^-, \cdots, Q_{n,n-1}^-; X_n) = 0$;
(c) *For any positive odd integer* n, $G_{n-1,-\epsilon}'^{-}(Q_{n0}^-, Q_{n1}^-, \cdots, Q_{n,n-1}^-; X_n) = 0$.

Proof. (a) By Lemma 2.12,

$$\begin{aligned}
&G_{n-1,\epsilon}'^{+}(Q_{n0}^+, Q_{n1}^+, \cdots, Q_{n,n-1}^+; X_n) \\
=&g_{n-1}'^{+}(Q_{n0}^+ + \epsilon X_n^2, Q_{n1}^+ + \epsilon X_n^{q+1}, \cdots, Q_{n,n-1}^+ + \epsilon X_n^{q^{n-1}+1}) \\
=&g_{n-1}'^{+}(Q_{n-1,0}^+, Q_{n-1,1}^+, \cdots, Q_{n-1,n-1}^+) \\
=&0.
\end{aligned}$$

(b)

$$\begin{aligned}
&G_{n-1,\epsilon}'^{+}(Q_{n0}^-, Q_{n1}^-, \cdots, Q_{n,n-1}^-; X_n) \\
=&g_{n-1}'^{+}(Q_{n0}^- + \epsilon X_n^2, Q_{n1}^- + \epsilon X_n^{q+1}, \cdots, Q_{n,n-1}^- + \epsilon X_n^{q^{n-1}+1}) \\
=&g_{n-1}'^{+}(Q_{n-1,0}^-, Q_{n-1,1}^-, \cdots, Q_{n-1,n-1}^-) \\
=&0.
\end{aligned}$$

(c)

$$\begin{aligned}
&G_{n-1,-\epsilon}'^{-}(Q_{n0}^-, Q_{n1}^-, \cdots, Q_{n,n-1}^-; X_n) \\
=&g_{n-1}'^{-}(Q_{n0}^- - \epsilon X_n^2, Q_{n1}^- - \epsilon X_n^{q+1}, \cdots, Q_{n,n-1}^- - \epsilon X_n^{q^{n-1}+1}) \\
=&g_{n-1}'^{-}(Q_{n-1,0}^-, Q_{n-1,1}^-, \cdots, Q_{n-1,n-1}^-) \\
=&0.
\end{aligned}$$

Lemma 2.14. (a) *The degree of* X_n *over* $\mathbb{F}_q(Q^+_{n0}, Q^+_{n1}, \cdots, Q^+_{n,n-1})$ *is*

$$\begin{cases} q^{n-1} + q^{\frac{n-1}{2}}, & \text{if } n \text{ is odd;} \\ q^{n-1} - q^{\frac{n}{2}-1}, & \text{if } n \text{ is even.} \end{cases}$$

(b) *The degree of* X_n *over* $\mathbb{F}_q(Q^-_{n0}, Q^-_{n1}, \cdots, Q^-_{n,n-1})$ *is* $q^{n-1} + q^{\frac{n}{2}-1}$ *if* n *is even.*

Proof.

$$\begin{aligned} \mathbb{F}_q(Q_{n0}, Q_{n1}, \cdots, Q_{n,n-1}, X_n) &= \mathbb{F}_q(Q_{n-1,0}, Q_{n-1,1}, \cdots, Q_{n-1,n-1}, X_n) \\ &= \mathbb{F}_q(Q_{n-1,0}, Q_{n-1,1}, \cdots, Q_{n-1,n-2}, X_n). \end{aligned}$$

The last equality follows from Theorem 1.2.

$$\begin{aligned} &[\mathbb{F}_q(Q_{n0}, Q_{n1}, \cdots, Q_{n,n-1}, X_n) : \mathbb{F}_q(Q_{n0}, Q_{n1}, \cdots, Q_{n,n-1})] \\ =&\frac{[\mathbb{F}_q(X_0, X_1, \cdots, X_n) : \mathbb{F}_q(Q_{n0}, Q_{n1}, \cdots, Q_{n,n-1})]}{[\mathbb{F}_q(X_0, X_1, \cdots, X_n) : \mathbb{F}_q(Q_{n0}, Q_{n1}, \cdots, Q_{n,n-1}, X_n)]} \\ =&\frac{[\mathbb{F}_q(X_0, X_1, \cdots, X_n) : F_q(Q_{n0}, Q_{n1}, \cdots, Q_{n,n-1})]}{[\mathbb{F}_q(X_0, X_1, \cdots, X_{n-1}, X_n) : \mathbb{F}_q(Q_{n-1,0}, Q_{n-1,1}, \cdots, Q_{n-1,n-2}, X_n)]} \\ =&|O_n(\mathbb{F}_q)|/|O_{n-1}(\mathbb{F}_q)|. \end{aligned}$$

Now applying Proposition 1.1, we get the followings and the Lemma follows. If $n = 2k+1$ is odd, then

$$\begin{aligned} |O^+_n(\mathbb{F}_q)|/|O^+_{n-1}(\mathbb{F}_q)| &= \frac{2(q^{n-1}-1)q^{n-2}(q^{n-3}-1)q^{n-4}\cdots(q^2-1)q}{2(q^{n-2}-q^{k-1})(q^{n-3}-1)q^{n-4}\cdots(q^2-1)q} \\ &= \frac{(q^{2k}-1)q^{2k-1}}{(q^k-1)q^{k-1}} \\ &= q^k(q^k+1) = q^{n-1} + q^k. \end{aligned}$$

If $n = 2k$ is even, then

$$\begin{aligned} |O^+_n(\mathbb{F}_q)|/|O^+_{n-1}(\mathbb{F}_q)| &= \frac{2(q^{n-1}-q^{k-1})(q^{n-2}-1)q^{n-3}\cdots(q^2-1)q}{2(q^{n-2}-1)q^{n-3}(q^{n-4}-1)q^{n-5}\cdots(q^2-1)q} \\ &= q^{n-1} - q^{k-1}. \end{aligned}$$

If $n = 2k$ is even, then

$$\begin{aligned} |O^-_n(\mathbb{F}_q)|/|O^-_{n-1}(\mathbb{F}_q)| &= \frac{2(q^{n-1}+q^{k-1})(q^{n-2}-1)q^{n-3}\cdots(q^2-1)q}{2(q^{n-2}-1)q^{n-3}(q^{n-4}-1)q^{n-5}\cdots(q^2-1)q} \\ &= q^{n-1} + q^{k-1}. \end{aligned}$$

Proposition 2.15. *Concider the quadratic forms Q_n^+ for all n and Q_n^- for even n. The minimal polynomial of X_n over $\mathbb{F}_q(Q^{\pm}_{n0}, Q^{\pm}_{n1}, \cdots, Q^{\pm}_{n,n-1})$ is*

$$G'^{+}_{n-1,\epsilon}(Q^{\pm}_{n0}, Q^{\pm}_{n1}, \cdots, Q^{\pm}_{n,n-1}; T)/\mathrm{lc}\, G'^{+}_{n-1,\epsilon}$$

where $\epsilon = (-1)^n$ for "Q_n^+" case.

Proof. By Lemma 2.13, X_n satisfies the polynomial $G'^{+}_{n-1,\epsilon}(Q^{\pm}_{n0}, Q^{\pm}_{n1}, \cdots, Q^{\pm}_{n,n-1}; T)$, and by Lemma 2.10, the degree of the field extension is equal to the degree of the polynomial.

Corollary 2.16. *Concider the quadratic forms Q_n^+ for all n and Q_n^- for even n. $G'^{+}_{n-1,\epsilon}(Q^{\pm}_{n0}, Q^{\pm}_{n1}, \cdots, Q^{\pm}_{n,n-1}$ $\mathbb{F}_q[x_1, x_2, \cdots, x_n]^{O_n^{\pm}(\mathbb{F}_q)}[T]$ where $\epsilon = (-1)^n$ for "Q_n^+" case.*

Proof. By [??,Ex. ??].

Definition 2.17. *We define the polynomials $R^{\pm}_{ni}(X_0, \cdots, X_n)$ in the following.*

(i) *If n is even, the polynomial $G'^{+}_{n,-1}(X_0, X_1, \cdots, X_n; T)$ has degree $q^n + q^{\frac{n}{2}}$. Let R^+_{ni} be the coefficient of $T^{q^{n-i}+q^{\frac{n}{2}}}$, $i = 0, 1, \cdots, \frac{n}{2}$.*

(ii) *If n is odd and $(\frac{\epsilon}{q}) = 1$, the polynomial $G'^{+}_{n,\epsilon}(X_0, X_1, \cdots, X_n; T)$ has degree $q^n - q^{\frac{n-1}{2}}$. Let R^+_{ni} be the coefficient of $T^{q^{n-i}-q^{\frac{n-1}{2}}}$, $i = 0, 1, \cdots, \frac{n+1}{2}$.*

(iii) *If n is odd and $(\frac{\epsilon}{q}) = -1$, the polynomial $G'^{+}_{n,\epsilon}(X_0, X_1, \cdots, X_n; T)$ has degree $q^n + q^{\frac{n-1}{2}}$. Let R^-_{ni} be the coefficient of $T^{q^{n-i}+q^{\frac{n-1}{2}}}$, $i = 0, 1, \cdots, \frac{n-1}{2}$; $R^{-}_{n,\frac{n+1}{2}}$ be the constant term.*

Note that $R^{\pm}_{n-1,0}$ is the leading coefficient of $G'^{+}_{n-1,\epsilon}(X_1, \ldots, X_{n-1}; T)$, and $\frac{R^{\pm}_{n-1,i}(X_0, X_1, \cdots, X_{n-1})}{R^{\pm}_{n-1,0}(X_0, X_1, \cdots, X_{n-2})} \in \mathbb{F}_q[x_1, x_2, \cdots, x_n]^{O_n^{\pm}(\mathbb{F}_q)}$ for all i, by Corollary 2.16.

Now we begin to state the first case of our Main Theorem. The proof is postpone to §4. The second case of Main Theorem is stated in §6.

We define a $k \times (k+1)$ matrix $\mathbf{A}^{(k)}$ as

$$\mathbf{A}^{(k)} = \begin{bmatrix} p_{1,2k-1} & p^{q}_{1,2k-3} & p^{q^2}_{1,2k-5} & \cdots & p^{q^{k-2}}_{13} & r^{q^{k-1}}_{12} & r^{q^{k-1}}_{11} \\ p_{2,2k-1} & p^{q}_{2,2k-3} & p^{q^2}_{2,2k-5} & \cdots & r^{q^{k-2}}_{24} & r^{q^{k-2}}_{23} & r^{q^{k-2}}_{22} \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ r_{k,2k} & r_{k,2k-1} & r_{k,2k-2} & \cdots & r_{k,k+2} & r_{k,k+1} & r_{kk} \end{bmatrix} \tag{2-9}$$

where the (i,j)-entry is

$$\begin{cases} p^{q^{j-1}}_{i,2k-2j+1}, & \text{if } j \le k-i \\ r^{q^{k-i}}_{i,k+1+i-j}, & \text{if } j > k-i. \end{cases} \tag{2-10}$$

The entries p_{ij}'s and r_{ij}'s will be defined inductively in the proof of the following Main Theorem.

Theorem $\mathbf{A}_k$. *Let $n = 2k+1$ be a positive odd integer, $Q_n^+ = x_1^2 - x_2^2 + x_3^2 - \cdots + x_{n-2}^2 - x_{n-1}^2 + x_n^2$ be a quadratic form, $O_n^+(\mathbb{F}_q)$ be the orthogonal group associated to Q_n^+. Then*

(a) *The invariant subring is*

$$\begin{aligned}&\mathbb{F}_q[x_1, x_2, \cdots, x_n]^{O_n^+(\mathbb{F}_q)}\\ =&\mathbb{F}_q[Q^+_{n0}, Q^+_{n1}, \cdots, Q^+_{n,n-2}, \tfrac{R^+_{n-1,1}(X_0,X_1,\cdots,X_{n-1})}{R^+_{n-1,0}(X_0,X_1,\cdots,X_{n-2})}, \cdots, \tfrac{R^+_{n-1,k}(X_0,X_1,\cdots,X_{n-1})}{R^+_{n-1,0}(X_0,X_1,\cdots,X_{n-2})}].\end{aligned}$$

(b) *We have an isomorphism*

$$\begin{aligned}\Phi_n : \mathbb{F}_q[X_0, X_1, \cdots, X_{n-2}, Y_1, Y_2, \cdots, Y_k]/\langle K_{n1}, K_{n2}, \cdots, K_{n,k-1}\rangle \longrightarrow\\ \mathbb{F}_q[X_0, X_1, \cdots, X_{n-2}, \tfrac{R^+_{n-1,1}(X_0,X_1,\cdots,X_{n-1})}{R^+_{n-1,0}(X_0,X_1,\cdots,X_{n-2})}, \cdots, \tfrac{R^+_{n-1,k}(X_0,X_1,\cdots,X_{n-1})}{R^+_{n-1,0}(X_0,X_1,\cdots,X_{n-2})}]\end{aligned}$$

defined by

$$\begin{aligned}X_i &\mapsto X_i, && 0 \le i \le n-2\\ Y_j &\mapsto \tfrac{R^+_{n-1,j}(X_0,X_1,\cdots,X_{n-1})}{R^+_{n-1,0}(X_0,X_1,\cdots,X_{n-2})}, && 1 \le j \le k.\end{aligned}$$

where the relations K_{nj} are defined by

$$\begin{bmatrix} K_{n1}\\ K_{n2}\\ \vdots\\ K_{n,k-1}\end{bmatrix} = \mathbf{A}^{(k)}_{k;\emptyset}\begin{bmatrix}1\\ Y_1\\ \vdots\\ Y_k\end{bmatrix}.$$

(c) *The polynomials p_{ij} and $r_{ij} \in \mathbb{F}_q[X_0, X_1, \cdots, X_j]$ are independent of n.*

$$r_{k,2k} = -X_{2k} + \psi(X_0, X_1, \cdots, X_{2k-1}) \quad \textit{for some polynomial } \psi. \tag{2-11}$$

Moreover, they are homogeneous with respect to the weight defined in (1-5) *with*

$$\begin{cases} wt\ p_{ij} = q^{j+1} + q^{\frac{j+1}{2}-i}, & j \textit{ odd;}\\ wt\ r_{ij} = q^j + 1. \end{cases} \tag{2-12}$$

§ 3. Lemmas.

In order to prove the Main Theorem, in this section, we first give some Lemmas.

Lemma 3.1. *For $n \ge 3$ and $i \ge 1$, we have*

$$R^{\pm}_{ni} = (-1)^{\lfloor \frac{n}{2} \rfloor} R^{\pm\, q}_{n-2,i-1} X_n + \phi_{ni}(X_0, X_1, \ldots, X_{n-1}).$$

Proof. Let n be even. Then by Lemma 2.6,

$$G'^+_{n,-1} = (-1)^{\frac{n}{2}} G'^{+\,q}_{n-2,-1}(X_n - T^{q^n+1}) + \phi''_3(X_0, X_1, \ldots, X_{n-1}; T). \tag{3-1}$$

From Lemmas 2.10, 2.11, we see that the leading term of $G'^{+}_{n,-1}$ is $-g'^{\,+}_{n-1}T^{q^n+q^{\frac{n}{2}}}$. Also by the definition of $R^{+}_{n-2,i}$, from (3-1) we have

$$\begin{aligned}
&G'^{+}_{n,-1}\\
=&(-1)^{\frac{n}{2}}\{\sum_{i=0}^{\frac{n}{2}-1} R^{+}_{n-2,i}T^{q^{n-i-2}+q^{\frac{n}{2}-1}} + \sum_j{}^{*}\psi_j(X_0,X_1,\ldots,X_{n-2})T^j\}^q X_n - g'^{\,+}_{n-1}T^{q^n+q^{\frac{n}{2}}}\\
&+\phi_4(X_0,X_1,\ldots,X_{n-1};T)\\
=&-g'^{\,+}_{n-1}T^{q^n+q^{\frac{n}{2}}} + (-1)^{\frac{n}{2}}\sum_{i=1}^{\frac{n}{2}} R^{+\,q}_{n-2,i-1}X_nT^{q^{n-i}+q^{\frac{n}{2}}} + (-1)^{\frac{n}{2}}\sum_j{}^{*}\psi_j^q(X_0,X_1,\ldots,X_{n-2})X_nT^{jq} + \phi_4.
\end{aligned} \tag{3-2}$$

where the sum $\sum^*$ runs over all j such that $j < q^{n-2}+q^{\frac{n}{2}-1}$ and j is not equal to $q^{n-3}+q^{\frac{n}{2}-1}, q^{n-4}+q^{\frac{n}{2}-1},\ldots,2q^{\frac{n}{2}-1}$, so jq is not equal to $q^{n-2}+q^{\frac{n}{2}}, q^{n-3}+q^{\frac{n}{2}},\ldots,2q^{\frac{n}{2}}$. The coefficient of $T^{q^{n-i}+q^{\frac{n}{2}}}, i\geq 1$, is

$$(-1)^{\frac{n}{2}}R^{+\,q}_{n-2,i-1}X_n + \phi_{ni}(X_0,X_1,\ldots,X_{n-1}).$$

Let n be odd and $\left(\frac{\epsilon}{q}\right)=1$. Then

$$\begin{aligned}
G'^{+}_{n,\epsilon} =&(-1)^{\frac{n-1}{2}}G'^{+\,q}_{n-2,\epsilon}(X_n - T^{q^n+1}) + \phi_3''(X_0,X_1,\ldots,X_{n-1};T)\\
=&(-1)^{\frac{n-1}{2}}\{\sum_{i=0}^{\frac{n-1}{2}-1} R^{+}_{n-2,i}T^{q^{n-i-2}-q^{\frac{n-1}{2}-1}} + \sum_j{}^{*}\psi_j(X_0,X_1,\ldots,X_{n-2})T_j\}^q X_n +\\
&(-1)^{\frac{n+1}{2}}\frac{1}{2}g'^{\,+}_{n-1}T^{q^{n-1}+q^{\frac{n-1}{2}}} + \phi_4\\
=&(-1)^{\frac{n+1}{2}}\frac{1}{2}g'^{\,+}_{n-1}T^{q^{n-1}+q^{\frac{n-1}{2}}} + (-1)^{\frac{n-1}{2}}\sum_{i=1}^{\frac{n-1}{2}} R^{+\,q}_{n-2,i-1}X_nT^{q^{n-i}-q^{\frac{n-1}{2}}}\\
&+(-1)^{\frac{n-1}{2}}\sum_j{}^{*}\psi_j^q(X_0,X_1,\ldots,X_{n-2})X_nT^{jq} + \phi_4.
\end{aligned} \tag{3-3}$$

Let n be odd and $\left(\frac{\epsilon}{q}\right)=-1$. Then

$$\begin{aligned}
G'^{+}_{n,\epsilon} =&(-1)^{\frac{n-1}{2}}\{\sum_{i=0}^{\frac{n-1}{2}-1} R^{-}_{n-2,i}T^{q^{n-i-2}-q^{\frac{n-1}{2}-1}} + R^{-}_{n-2,\frac{n-1}{2}} + \sum_j{}^{*}\psi_j(X_0,X_1,\ldots,X_{n-2})T^j\}^q X_n\\
&+(-1)^{\frac{n-1}{2}}2\epsilon g'^{\,-}_{n-1}T^{q^{n-1}+q^{\frac{n-1}{2}}} + \phi_4\\
=&(-1)^{\frac{n-1}{2}}2\epsilon g'^{\,-}_{n-1}T^{q^{n-1}+q^{\frac{n-1}{2}}} + (-1)^{\frac{n-1}{2}}\sum_{i=1}^{\frac{n-1}{2}} R^{-\,q}_{n-2,i-1}X_nT^{q^{n-i}-q^{\frac{n-1}{2}}} + R^{-\,q}_{n-2,\frac{n-1}{2}}\\
&+(-1)^{\frac{n-1}{2}}\sum_j{}^{*}\psi_j^q(X_0,X_1,\ldots,X_{n-2})X_nT^{jq} + \phi_4.
\end{aligned} \tag{3-4}$$

Lemma 3.2. *Under the weight defined in* $(1-5)$, *we have*

$$\text{if } n \text{ is even,} \qquad wt\ R^{+}_{ni} = \frac{q^{n+1}-1}{q-1} - q^{n-i},$$

$$\text{if } n \text{ is odd,} \qquad \begin{cases} wt\ R^{+}_{ni} = \frac{q^{n+1}-1}{q-1} - q^{n-i} + q^{\frac{n-1}{2}}, \\ wt\ R^{-}_{ni} = \frac{q^{n+1}-1}{q-1} - q^{n-i} - q^{\frac{n-1}{2}}, wt\ R^{-}_{n,\frac{n+1}{2}} = \frac{q^{n+1}-1}{q-1}. \end{cases}$$

Proof. By Lemma 2.9.

Lemma 3.3. *For all* $n \in \mathbb{N}$, *we have*

(a) $f_{2k} \equiv (-1)^k X_k^{\frac{2(q^k-1)}{q-1}} (\text{mod } X_0, X_1, \ldots, X_{k-1})$;
(b) $f_{2k+1} \equiv 2X_k^{\frac{2(q^{k+1}-1)}{q-1}} X_{k+1}^{\frac{q^k-1}{q-1}} + 2X_k^{1+\frac{q^{k+1}-1}{q-1}} \cdot f(\text{mod } X_0, X_1, \ldots, X_{k-1})$;
(c) $f'_{2k} \equiv (-1)^{k+1} X_k^{\frac{(q+1)(q^k-1)}{q-1}} (\text{mod } X_0, X_1, \ldots, X_{k-1})$;
(d) $f'_{2k+1} \equiv 2X_k^{\frac{(q^{k+1}-q)}{q-1}} X_{k+1}^{\frac{q^{k+1}-1}{q-1}} + X_k^{\frac{q^{k+1}-1}{q-1}} \cdot f_1(\text{mod } X_0, X_1, \ldots, X_{k-1})$
where f *and* f_1 *are two polynomials.*

Proof. (a) and (c) follow from direct computation. Using the Laplace expansion to the determinants defining f'_{2k} and f'_{2k+1}, we can get (b) and (d).

Lemma 3.4. *For* $n \in \mathbb{N}$, *we have*

(a) $g'^{+}_{2k-1} \equiv (-1)^{\frac{k(k-1)}{2}} X_k^{\frac{q^k-1}{q-1}} (\text{mod } X_0, X_1, \ldots, X_{k-1})$;
(b) $g'^{+}_{2k} \equiv (-1)^{\frac{k(k-1)}{2}} 2X_k^{\frac{q^{k+1}-1}{q-1}} (\text{mod } X_0, X_1, \ldots, X_{k-1})$.
(c) $g'^{-}_{2k} \equiv (-1)^k X_{k+1}^{\frac{q^k-1}{q-1}} (\text{mod } X_0, X_1, \ldots, X_k)$.

Proof. Step 1. By definition 2.1

$$f_{2k+1} \equiv \det \begin{bmatrix} & \mathbf{0} & & & X_k & & & \\ & & & & & X_k^q & & * \\ & & & & \vdots & & X_k^{q^2} & \\ & & & & & & & \ddots \\ X_k & & & & \mathbf{0} & & & X_k^{q^k} \\ X_{k+1} & X_k^q & & & & & & \\ & X_{k+1}^q & X_k^{q^2} & & \vdots & & & \\ & * & \ddots & \ddots & & & \mathbf{0} & \\ & & & X_{k+1}^{q^{k-1}} & X_k^{q^k} & & & \end{bmatrix}$$

Note that the matrix defining f_{2k+1} is symmetric. Expanding it along the $(k+1)$th column, we see that

$$\begin{aligned} f_{2k+1} \equiv & 2X_k^{\frac{q^{k+1}-1}{q-1}} \det B_k (\text{mod } X_0, X_1, \ldots, X_{k-1}). \\ \equiv & 0 (\text{mod } X_0, X_1, \ldots, X_{k-1}, X_k^{\frac{q^{k+1}-1}{q-1}}) \end{aligned} \tag{3-5}$$

where

$$B_k = \begin{bmatrix} X_{k+1} & X_k^q & & & \\ & X_{k+1}^q & X_k^{q^2} & & \mathbf{0} \\ & & \ddots & \ddots & \\ & \mathbf{*} & & \ddots & X_k^{q^{k-1}} \\ & & & & X_{k+1}^{q^{k-1}} \end{bmatrix}.$$

Moreover, we have

$$\det B_k \equiv X_{k+1}^{\frac{q^k-1}{q-1}} (\text{mod } X_0, X_1, \ldots, X_k) \tag{3-6}$$

Step 2.

$$f'_{2k+1} \equiv \det \begin{bmatrix} & & & & X_k^q & & \\ & \mathbf{0} & & & & X_k^{q^2} & * \\ & & & & \vdots & & \ddots \\ & & & & & & x_k^{q^k} \\ X_k & & & & & & \\ X_{k+1} & X_k^q & & & & & \\ & \ddots & \ddots & & \vdots & & \\ * & & \ddots & x_k^{q^k} & & & \mathbf{0} \\ & & & X_{k+1}^{q^k} & X_k^{q^{k+1}} & & \end{bmatrix}$$

Expanding along the $(k+2)$th column, we have

$$f'_{2k+1} \equiv \det D_{k+1} \cdot X_k^{\frac{q(q^k-1)}{q-1}} \pm X_k^{q^{k+1}} \cdot \phi (\text{mod } X_1, X_2, \ldots, X_{k-1})$$

where

$$D_{k+1} = \begin{bmatrix} X_{k+1} & X_k^q & & & \\ & X_{k+1}^q & X_k^{q^2} & & \mathbf{0} \\ & & \ddots & \ddots & \\ & \mathbf{*} & & \ddots & X_k^{q^k} \\ & & & & X_{k+1}^{q^k} \end{bmatrix}$$

Since

$$\det D_{k+1} = X_{k+1}^{\frac{q^{k+1}-1}{q-1}} + X_k^q \cdot \psi,$$

so

$$\begin{aligned} f'_{2k+1} \equiv & (X_{k+1}^{\frac{q^{k+1}-1}{q-1}} + X_k^q \cdot \psi) \cdot X_k^{\frac{q(q^k-1)}{q-1}} \pm X_k^{q^{k+1}} \cdot \phi (\text{mod } X_1, X_2, \ldots, X_{k-1}) \\ \equiv & X_k^{\frac{q^{k+1}-q}{q-1}} X_{k+1}^{\frac{q^{k+1}-1}{q-1}} (\text{mod } X_0, X_1, \ldots, X_k^{\frac{q^{k+1}-1}{q-1}}). \end{aligned} \tag{3-7}$$

By (3.2) and (3.4), we have $g_{2k+1}^{\pm} \equiv X_k^{\frac{q^{k+1}-q}{q-1}} X_{k+1}^{\frac{q^{k+1}-1}{q-1}} (\text{mod } X_0, X_1, \ldots, X_k^{\frac{q^{k+1}-1}{q-1}})$.

Step 3. Now by the definition 2.3, ${g'}_{2k+1}^{\pm} = g_{2k+1}^{\pm}/({g'}_{2k-1}^{\mp})^q$ and induction, the formula for ${g'}_{2k+1}^{\pm}$ is proved.

Step 4. Let $A_k = \begin{bmatrix} X_k & & & * \\ & X_k^q & & \\ & & \ddots & \\ \mathbf{0} & & & x_k^{q^{k-1}} \end{bmatrix}$, $A'_{k-1} = \begin{bmatrix} X_k^q & & & * \\ & X_k^{q^2} & & \\ & & \ddots & \\ \mathbf{0} & & & x_k^{q^{k-1}} \end{bmatrix}$ and $B_{k+1} = \begin{bmatrix} X_k & & & \mathbf{0} \\ & X_k^q & & \\ & & \ddots & \\ * & & & x_k^{q^k} \end{bmatrix}$.

Then we have

$$f_{2k} \equiv \begin{vmatrix} 0 & A_k \\ A_k^t & 0 \end{vmatrix} = (-1)^k X_k^{\frac{2(q^k-1)}{q-1}} (\text{mod } X_0, X_1, \ldots, X_{k-1}),$$

$$f'_{2k} \equiv \begin{vmatrix} 0 & A'_{k-1} \\ B_{k+1} & 0 \end{vmatrix} = (-1)^{k+1} X_k^{\frac{(q+1)(q^k-1)}{q-1}} (\text{mod } X_0, X_1, \ldots, X_{k-1})$$

By the definition 2.2 of g_n^+, we have

$$g_{2k}^+ \equiv (-1)^{k+1} 2 X_k^{(q+1)\frac{q^k-1}{q-1}} (\text{mod } X_0, X_1, \ldots, X_{k-1}) \tag{3-8}$$

Step 5. Now from Lemma 2.5(a), $f_{2k+1} = (-1)^k g'^{+}_{2k} g'^{-}_{2k}$. Comparing (3-1),(3-2) and (3-3), we get the formula for g_{2k}^-

Lemma 3.5. *For any j such that $1 \le j \le k-1$, we have*

$$g'^{\pm}_{2k-1} \equiv \pm X_j^{\frac{q^k - q^{k-j}}{q-1}} X_{k+j}^{\frac{q^{k-j}-1}{q-1}} (\text{mod } X_0, X_1, \ldots, X_j^{1+\frac{q^k-q^{k-j}}{q-1}}, \ldots, X_{k+j-1})$$

Proof. *Step 1.* It is not difficult to see that

$$f_{2k} \equiv \left| \begin{array}{ccccccccc} & & \ddots & & & & X_{k+j} & & * \\ & & & & & & & \ddots & \\ & & & \ddots & & & & & X_{k+j}^{q^{k-j-1}} \\ \ddots & & & & X_j^{q^{k-j}} & & \mathbf{0} & & \\ & & & & & \ddots & & & \\ & \ddots & & & & X_j^{q^{k-1}} & & & \\ & & X_j^{q^{k-j}} & & \mathbf{0} & & 0 & & \\ & & & \ddots & & & & \ddots & \\ & & & X_k^{q^{k-1}} & & & & & 0 \\ X_{k+j} & & \mathbf{0} & & 0 & & & & \\ & \ddots & & & & \ddots & & & \\ * & X_{k+j}^{q^{k-j-1}} & & & & 0 & & & \end{array} \right|$$

$$\equiv (-1)^{(k+1)(j+1)-1} X_j^{2\frac{q^k-q^{k-j}}{q-1}} X_{k+j}^{2\frac{q^{k-j}-1}{q-1}} (\text{mod } X_0, X_1, \ldots, X_j^{1+\frac{2(q^k-q^{k-j})}{q-1}}, \ldots, X_{k+j-1}) \tag{3-9}$$

Step 2. Observing the matrices defining f_{2k-1} and f'_{2k-1},we see that the exponents of X_{k+j} in f_{2k-1} is $\le \frac{2(q^{k-j-1}-1)}{q-1}$, which in f'_{2k-1} is $\le \frac{q^{k-j}-1}{q-1} + q\frac{q^{k-j-2}-1}{q-1}$. Thus the exponents of X_{k+j}

in $g_{2k-1}^{\pm}$ is $\leq (q+1)(\frac{q^{k-j-1}-1}{q-1})$. On the other hand, by induction hypothesis, the exponents of X_{k+j} in $g_{2k-3}^{\pm}$ is $\frac{q^{k-j-2}-1}{q-1}$. So the exponents of X_{k+j} in $g_{2k-1}'^{\pm}$ is $\leq \frac{q^{k-j}-1}{q-1}$.

Using Lemma 2.5(a) and comparing the exponent of X_{k+j} in (3-9) and in $g_{2k-1}'^{\pm}$, we see that the exponents of X_{k+j} in $g_{2k-1}'^{\pm}$ is equal to $\frac{q^{k-j}-1}{q-1}$. Moreover, $\mathrm{wt} g_{2k-1}^{+} = \mathrm{wt} g_{2k-1}^{-} = \frac{q^{2k}-1}{q-1}$, so they also have the same exponents for X_j. The Lemma follows.

Lemma 3.6.

(a) $G_{2k}'^{+} \equiv (-1)^{k+1} X_{k+1}^{\frac{q^{k+1}-1}{q-1}} T^{2q^k} (\mathrm{mod}\ X_0, X_1, \ldots, X_k)$,

(b) $G_{2k}'^{-} \equiv (-1)^{k} X_{k+1}^{\frac{q^{k}-1}{q-1}} (\mathrm{mod}\ X_0, X_1, \ldots, X_k)$.

Proof. Step 1. Note that

$$f_{2k}' \equiv \begin{vmatrix} \mathbf{0} & A^{(k-1)} \\ B^{(k+1)} & \mathbf{0} \end{vmatrix} (\mathrm{mod}\ X_0, X_1, \ldots, X_{k-1}, X_k^{\frac{q^k-1}{q-1}}\ ) \tag{3-10}$$

where $A^{(k-1)} = \begin{bmatrix} X_k^q & & & * \\ & X_k^{q^2} & & \\ \mathbf{0} & & \ddots & \\ & & & X_k^{q^{k-1}} \end{bmatrix}$ and $B^{(k+1)} = \begin{bmatrix} X_k & & & & & \mathbf{0} \\ X_{k+1} & X_k^q & & & & \\ & X_{k+1}^q & X_k^{q^2} & & & \\ & & \ddots & \ddots & & \\ * & & & \ddots & X_k^{q^{k-1}} & \\ & & & & X_{k+1}^{q^[k-1} & 0 \end{bmatrix}$.

Note that the $(k+1)$th column in (3-5) is zero and $\det A^{(k-1)} = X_k^{\frac{q^k-q}{q-1}}$. Thus to compute all minors f_{ij}' in Lemma 2.8(b) carefully, we find that the only nonzero minor is $f_{k,k+1}'$. And we get

$$F_{2k}' \equiv X_k^{\frac{q^k-q}{q-1}} X_{k+1}^{\frac{q^k-1}{q-1}} T^{2q^k} (\mathrm{mod}\ X_0, X_1, \ldots, X_{k-1}, X_k^{\frac{q^k-1}{q-1}}\ )$$

Step 2. Similar to Step 1. , Using

$$f_{2k} \equiv \begin{vmatrix} \mathbf{0} & A^{(k)} \\ A^{(k)t} & \mathbf{0} \end{vmatrix} (\mathrm{mod}\ X_0, X_1, \ldots, X_{k-1}\ )$$

where $A^{(k)} = \begin{bmatrix} X_k & & & * \\ & X_k^{q^2} & & \\ \mathbf{0} & & \ddots & \\ & & & X_k^{q^{k-1}} \end{bmatrix}$. We use Lemma 2.8 to find F_{2k}. Most minors are zero, we have

$$F_{2k} \equiv X_k^{2\frac{q^k-1}{q-1}} + \sum_{i=0}^{k-1} 2 f_{k+1,i+1} T^{q^k+q^i} + \sum_{i=1}^{k-1} 2 f_{k+2,i+1} T^{q^{k+1}+q^i} + \cdots + 2 f_{2k,k} T^{q^{2k}+q^k}$$
$$(\mathrm{mod}\ X_0, X_1, \ldots, X_{k-1})$$

All the minors appear in the above are multiple of $X_k^{\frac{q^k-1}{q-1}}$, so

$$F_{2k} \equiv 0 (\mathrm{mod}\ X_0, X_1, X_{k-1}, X_k^{\frac{q^k-1}{q-1}}).$$

Step 3. From Steps 1,2, we have

$$G_{2k}^{\pm} \equiv X_k^{\frac{q^k-q}{q-1}} X_{k+1}^{\frac{q^k-1}{q-1}} T^{2q^k} (\bmod X_0, X_1, \ldots, X_{k-1}, X_k^{\frac{q^k-1}{q-1}})$$

By definition of $G_n'^{\pm}$ and induction, the Lemma follows.

Lemma 3.7. (a) $R_{2k,0}^{+} \equiv X_k^{\frac{q^k-1}{q-1}} (\bmod X_0, X_1, \ldots, X_{k-1})$.

(b) $R_{2k,j}^{+} \equiv X_k^{\frac{q^k-1}{q-1}-q^{k-j}} X_{k+j}^{q^{k-j}} (\bmod X_0, X_1, \ldots, \widehat{X}_k, \ldots, \widehat{X}_{k+j}, \ldots, X_{2k}), 1 \le j \le k-1$

(c) $R_{2k,k}^{+} \equiv (-1)^{k+1} X_{k+1}^{\frac{q^{k+1}-1}{q-1}} (\bmod X_0, X_1, \ldots, X_k)$

Proof. By Definition and Lemma 3.6, we have, modulo $\langle X_0, X_1, \ldots, X_{k-1}\rangle$

$$G_{2k}'^{+} = \begin{cases} (F_{2k}' - F_{2k}^{\frac{q+1}{2}})/(G_{2k-2}'^{-})^q \equiv (F_{2k}' - F_{2k}^{\frac{q+1}{2}})/(X_k^{\frac{q^k-1}{q-1}})^q, & k \text{ even} \\ (F_{2k}' + (-F_{2k})^{\frac{q+1}{2}})/(G_{2k-2}'^{-})^q \equiv (F_{2k}' + (-F_{2k})^{\frac{q+1}{2}})/(-X_k^{\frac{q^k-1}{q-1}})^q, & k \text{ odd} \end{cases} \tag{3-11}$$

Note that $R_{2k,j}^{+}$ is the coefficient of $T^{q^{2k-j}+q^k}$ in $G_{2k}'^{+}$.

Step 1. We claim the term $T^{q^{2k-j}+q^k}$ cannot appear in the expansion of $F_{2k}^{\frac{q+1}{2}}$. Let $\mathcal{S}$ be the set of all exponents of T appear in F_{2k}. By (3-6)

$$\begin{aligned} \mathcal{S} =& \mathcal{S}_1 \cup \mathcal{S}_2 \cup \mathcal{S}_3 \cup \{0\}, \\ \mathcal{S}_1 =& \{q^l + q^m : 2k-j+1 \le l \le 2k-1, 0 \le m \le l\} \cup \{q^{2k-j} + q^m : k < m < 2k-j\}, \\ \mathcal{S}_2 =& \{q^{2k-j} + q^m, 0 \le m \le k\}, \\ \mathcal{S}_3 =& \{q^l + q^m : k \le l \le 2k-j-2, 0 \le m \le l\} \cup \{q^{2k-j-1} + q^m : 0 \le m \le k-1\}. \end{aligned}$$

The exponents of T may appears in $F_{2k}^{\frac{q+1}{2}}$ is $\sum_{i=1}^{\alpha} u_i + \sum_{i=1}^{\beta} v_i + \sum_{i=0}^{\gamma} w_3, u_i \in \mathcal{S}_1, v_i \in \mathcal{S}_2, w_i \in \mathcal{S}_3, \alpha_+\beta_+\gamma_\le \frac{q+1}{2}$. Now suppose

$$q^{2k-j} + q^j = \sum_{i=1}^{\alpha} u_i + \sum_{i=1}^{\beta} v_i + \sum_{i=0}^{\gamma} w_3. \tag{3-12}$$

Since $u_i \ge q^{2k-j} + q^j$, so $\alpha = 0$. If $v_1, v_2 \in S_2$, then $v_1 + v_2 > q^{2k-j} + q^k$, hence $\beta = 0, 1$. If $\beta = 1$ and $v_1 = q^{2k-j} + q^k$, then (3-12) holds.

Suppose $v_1 = q^{2k-j} + q^m, m < k$. then $v_1 + * = q^{2k+j} + q^k$ and $q^m + * = q^k$. $*$ is a sum of some w_i. Say

$$q_m + w_1 + \cdots + v_\beta = q^k, \beta \le \frac{q-1}{2}.$$

Let ν be the valuation determined by q. The valuation of the right hand side of the above equation is k, so, in the left hand side, the terms with the minimal valuation must be cancelled. thus the only possibilities is

$$\beta = \frac{q-1}{2} \text{ and } v_1 = \cdots = v_\beta = 2q_m.$$

So $q^m + v_1 + \cdots + v_\beta = q^{m+1}$, and $m = k-1$. Thus we have

$$w_1 = q^{2k-j} + q^{k-1}, v_1 = \cdots = v_{\frac{q-1}{2}} = 2q^{k-1}.$$

Assume that $\beta = 0$. Suppose that there are only $\frac{q-3}{2}$ $w_i's$ which are equal to $2q^{2k-j-1}$. Then

$$\begin{aligned}
\frac{q-3}{2}(2q^{2k-j-1} + w_1 + w_2) &= q^{2k-j} + q^k \\
w_1 + w_2 &= 3q^{2k-j-1} + q^k \\
w_1 + w_2 &\leq 2(q^{2k-j-1} + q^{2k-j-2}) \\
q^{2k-j-1} + q^k &\leq 2q^{2k-j-2} \\
(q-2)q^{2k-j-2} + q^k &\leq 0.
\end{aligned}$$

A contradiction. Thus we have $w_1 = \cdots w_{\frac{q-1}{2}} = 2q^{2k-j-1}, w_{\frac{q+1}{2}} = q^{2k-j-1} + q^k$.

Step 2. In F'_{2k} the coefficient of $T^{q^{2k-j}+q^j}$ is

$$(-1)^{k+j}(f'_{k,2k-j+1} + f'_{2k-j,k+1}) (\text{mod } X_0, X_1, \ldots, \widehat{X}_k, \ldots, \widehat{X}_{k+j}, \ldots, X_{2k})$$

. By direct computations, one can check that

$$\begin{aligned}
f'_{k,2k-j+1} &\equiv 0 (\text{mod } X_0, X_1, \ldots, \widehat{X}_k, \ldots, \widehat{X}_{k+j}, \ldots, X_{2k}) \\
f'_{2k-j,k+1} &\equiv (-1)^{j+1} X_k^{\frac{q^k-q}{q-1} + \frac{q^k-1}{q-1} - q^{k-j}} X_{k+j}^{q^{k-j}} (\text{mod } X_0, X_1, \ldots, \widehat{X}_k, \ldots, \widehat{X}_{k+j}, \ldots, X_{2k}).
\end{aligned}$$

Step 3. Substituting the results in Steps 1 and 2 into (3-6), the Lemma follows.

Lemma 3.8. (a) *Consider the ring homomorphism*

$$\begin{aligned}
\Phi; \mathbb{F}_q[X_0, X_1, \ldots, X_n] &\to \mathbb{F}(Q^+_{n0}, Q^+_{n1}, \ldots, Q^+_{nn}) \\
X_i &\mapsto Q^+_{ni}.
\end{aligned}$$

Then $\ker \Phi = \langle g'^+_n \rangle$.

(b) *Consider the ring homomorphism*

$$\begin{aligned}
\Phi; \mathbb{F}_q[X_0, X_1, \ldots, X_n] &\to \mathbb{F}(Q^-_{n0}, Q^-_{n1}, \ldots, Q^-_{nn}) \\
X_i &\mapsto Q^-_{ni}.
\end{aligned}$$

Then $\ker \Phi = \langle g'^+_n \rangle$, *if n is odd;* $\ker \Phi = \langle g'^-_n \rangle$, *if n is even.*

Proof. Comparing the transcendental degrees of the kernel and the image of Φ, we see that $\ker \phi$ is a principle prime ideal of height one. By Lemma 2.12, $g^\pm_n \in \ker \Phi$ and it is irreducible, so $\ker \Phi = \langle g'^\pm_n \rangle$.

Lemma 3.9. (a) $2\gamma f_{n-2}^{\frac{q(q+1)}{2}} R_{n-1,1}^{+\ q+1} \equiv (-1)^{\frac{q+1}{2}} g_{n-4}^{\pm\ q(q+1)} g_n^{+} (\text{mod } g'^{\,+}_{n-2})$, *where γ is defined in (3-17).*

(b) Define $N = M_{1,n+1;n+1,n+2}^{(n+2)} - \delta_n^{\frac{q+1}{2}} M_{n;n+1}^{(n+1)} M_{n;n}^{(n+1)\ \frac{q+1}{2}}$.

Then $N \equiv g'^{\pm\ q}_{n-2} R^{+}_{n+1,1} (\text{mod } g'^{\,+}_{n-1})$.

Proof.

$$f_n = (-1)^{\lfloor \frac{n}{2} \rfloor} g'^{\,+}_{n-1} g'^{\,-}_{n-1} = (-1)^{\lfloor \frac{n}{2} \rfloor} \frac{g^{+}_{n-1}}{(g'^{\,-}_{n-3})^q} \frac{g^{-}_{n-1}}{(g'^{\,+}_{n-3})^q} = (-1)^{\lfloor \frac{n}{2} \rfloor} \frac{f'^{\,2}_{n-1} - f^{q+1}_{n-1}}{(-1)^{\lfloor \frac{n-2}{2} \rfloor} f_{n-2}^{\ q}}. \tag{3-13}$$

Since

$$f_{n-1} = (-1)^{\lfloor \frac{n-1}{2} \rfloor} g'^{\,+}_{n-2} g'^{\,-}_{n-2} \equiv 0 (\text{mod } g'^{\,+}_{n-2}), \tag{3-14}$$

so from (3-13) and (3-14),

$$f_n \equiv -\frac{f'^{\,2}_{n-1}}{f_{n-2}^{\ q}} (\text{mod } g'^{\,+}_{n-2})$$

and

$$f_{n-2}^{\frac{q(q+1}{2}} f_n^{\frac{q+1}{2}} \equiv (-1)^{\frac{q+1}{2}} f'^{\ q+1}_n (\text{mod } g'^{\,+}_{n-2}). \tag{3-15}$$

Apply Lemma 2.4 to the matrix defining f'_n and by (3-13), we get

$$f^q_{n-2} f'_n = f'_{n-1} M^{(n)\ q}_{n-1;n} - f^q_{n-1} M^{(n+1)}_{1,n;n,n+1} \equiv f'_{n-1} M^{(n)\ q}_{n-1;n} (\text{mod } g'^{\,+}_{n-2}). \tag{3-16}$$

By the definition (2.2) of $g'^{\,+}_{n-2}$, we have

$$f'_{n-2} \equiv \begin{cases} f_{n-2}^{\frac{q+1}{2}} (\text{mod } g'^{\,+}_{n-2}) & n = 2, 3 (\text{mod } 4) \\ (-1)^{\frac{q-1}{2}} f_{n-2}^{\frac{q+1}{2}} (\text{mod } g'^{\,+}_{n-2}) & n = 0, 1 (\text{mod } 4) \end{cases}$$

Define

$$\gamma = -1, \text{if } n \equiv 0, 1 (\text{mod } 4); = (-1)^{\frac{q+1}{2}}, \text{if } n \equiv 2, 3 (\text{mod } 4). \tag{3-17}$$

Then $f'_{n-2} \equiv (-1)^{\frac{q+1}{2}} \gamma f_{n-2}^{\frac{q+1}{2}} (\text{mod } g'^{\,+}_{n-2})$. By (3-14) and (3-15),

$$\begin{aligned} f_{n-2}^{\frac{q(q+1)}{2}} g_n^{+} &= f_{n-2}^{\frac{q(q+1)}{2}} (f'_n + \gamma f_n^{\frac{q+1}{2}}) \equiv f_{n-2}^{\frac{q(q-1)}{2}} f'_{n-1} M^{(n)\ q}_{n-1;n} + \gamma (-1)^{\frac{q+1}{2}} f'^{\ q+1}_{n-1} \\ &= f'_{n-1} \{ f_{n-2}^{\frac{q-1}{2}} M^{(n)}_{n-1;n} + \gamma (-1)^{\frac{q+1}{2}} f'_{n-1} \}^q \end{aligned} \tag{3-18}$$

Moreover,

$$M^{(n)}_{n-1;n} = (-1)^n f'_{n-2} X_{n-1} + \psi = (-1)^n (-1)^{\frac{q+1}{2}} \gamma f_{n-2}^{\frac{q+1}{2}} X_{n-1} + \psi$$

We proceed to compute (3-16),

$$\begin{aligned} f_{n-2}^{\frac{q-1}{2}} M^{(n)}_{n-1;n} + \gamma (-1)^{\frac{q+1}{2}} f'_{n-1} &= (-1)^n (-1)^{\frac{q+1}{2}} \gamma f^q_{n-2} X_{n-1} + \psi + (-1)^{\frac{q+1}{2}} (-1)^n \gamma f^q_{n-2} X_{n-1} + \psi' \\ &= (-1)^{n + \frac{q+1}{2}} \{ 2\gamma f^q_{n-2} X_{n-1} + \xi \} \end{aligned}$$

From (3-18) and (2-2),

$$f_{n-2}^{\frac{q(q+1)}{2}} g_n^+ \equiv (-1)^{\frac{q+1}{2}} 2\gamma f_{n-2}^{q(q+1)} X_{n-1}^{q+1} + \dots .$$

$$g_n^+ = (-1)^{\frac{q+1}{2}} 2\gamma f_{n-2}^{\frac{q(q+1)}{2}} X_{n-1}^{q+1} + \dots$$

Since

$$R'^{+\ q+1}_{n-1,1} = g'^{\pm\ q(q+1)}_{n-4} X_{n-1}^{q+1} + \dots,$$

so

$$2\gamma f_{n-1}^{\frac{q(q+1)}{2}} R^{+\ q+1}_{n-1,1} \equiv (-1)^{\frac{q+1}{2}} g'^{\pm\ q(q+1)}_{n-4} g'^{+}_n (\bmod\ g'^{\ +}_{n-2}).$$

(b) Define

$$\begin{aligned} N &= M^{(n+2)}_{1,n+1;n+1,n+2} - \delta^{\frac{q-1}{2}} M^{(n+1)}_{n;n+1} M^{(n+1)\ \frac{q-1}{2}}_{n;n} \\ &= f_n^q X_{n+1} + \dots \\ &= g'^{+\ q}_{n-2} g'^{-\ q}_{n-2} X_{n+1} + \cdots \\ R^+_{n+1,1} &= R^{+\ q}_{n-1,0} X_{n+1} + \cdots = g'^{\pm\ q}_{n-2} X_{n+1} + \cdots \end{aligned}$$

Thus the result follows.

Let $D_1 = \begin{vmatrix} x_1 & x_2 & \dots & x_n \\ x_1^q & x_2^q & \dots & x_n^q \\ \vdots & \vdots & & \vdots \\ x_1^{q^{n-1}} & x_2^{q^{n-1}} & \dots & x_n^{q^{n-1}} \end{vmatrix}$ and $D_2 = \begin{vmatrix} x_1 & x_2 & \dots & x_n \\ x_1^q & x_2^q & \dots & x_n^q \\ \vdots & \vdots & & \vdots \\ \widehat{x_1}^{q^{n-1}} & \widehat{x_2}^{q^{n-1}} & \dots & \widehat{x_n}^{q^{n-1}} \\ x_1^{q^n} & x_2^{q^n} & \dots & x_n^{q^n} \end{vmatrix}$. Then

$$\begin{aligned} M^{(n+2)}_{1,n+1;n+1,n+2} &= D_1 D_2^q \delta_n \\ M^{(n+1)}_{n;n+1} &= D_1 \delta_n D_2 \\ M^{(n+1)}_{n;n} &= D_1^2 \delta_n \end{aligned}$$

so $N(Q_{n0}, \dots, Q_{nn}) = 0$

Lemma 3.10. (a) *Let n be even and $\epsilon = -1$ or n be odd and $\epsilon = 1$.*

(i) $G'^{+}_{n,-1}(Q^+_{n-1,0}, \dots, Q^+_{n-1,0}; X_n) = 0$

(ii) *If a polynomial $\phi(X_0, X_1, X_{n-1}; T) = \sum_{k=0}^N a_k(X_0, \dots, X_{n-1})T^k$ satisfies $\phi(Q^+_{n-1,0},$ $\dots, Q^+_{n-1,0}; X_n) = 0$, then $a_k \in \langle g'^{+}_{n-1} \rangle$.*

(iii) $R^+_{ni} \in \langle g'^{+}_{n-1} \rangle$.

(b) *Let n be odd and $(\frac{\epsilon}{q}) = -1$.*

(i) $G'^{-}_{n,-1}(Q^-_{n-1,0}, \dots, Q^-_{n-1,0}; X_n) = 0$

(ii) *If a polynomial $\phi(X_0, X_1, X_{n-1}; T) = \sum_{k=0}^N a_k(X_0, \dots, X_{n-1})T^k$ satisfies $\phi(Q^-_{n-1,0},$ $\dots, Q^-_{n-1,0}; X_n) = 0$, then $a_k \in \langle g'^{-}_{n-1} \rangle$.*

(iii) $R^-_{ni} \in \langle g'^{-}_{n-1} \rangle$.

Proof. (a)(i)

$$\begin{aligned}
&G'^{+}_{n,\epsilon}(Q^+_{n-1,0}, Q^+_{n-1,1}, \cdots, Q^+_{n-1,n-1}; X_n)\\
=&g'^{+}_n(Q^+_{n-1,0} + \epsilon X_n^2, Q^+_{n-1,1} + \epsilon X_n^{q+1}, \cdots, Q^+_{n-1,n-1} + \epsilon X_n^{q^{n-1}+1})\\
=&g'^{+}_n(Q^+_{n,0}, Q^+_{n,1}, \cdots, Q^+_{n,n-1})\\
=&0.
\end{aligned}$$

(ii) $0 = \phi(Q^+_{n-1,0}, \ldots, Q^+_{n-1,0}; X_n) = \sum_{k=0}^N a_k(Q^+_{n-1,0}, \ldots, Q^+_{n-1,0})T^k$. Since $a_k(Q^+_{n-1,0}, \ldots, Q^+_{n-1,0}) \in \mathbb{F}_q[x_1, \ldots, x_{n-1}]$, hence $a_k(Q^+_{n-1,0}, \ldots, Q^+_{n-1,0}) = 0$ for all k. The statement follows from Lemma 3.9(a).

(iii) Applying (ii) to $G'^{+}_{n,-1}$, we get the result.

The proofs of (b) are similar.

Lemma 3.11. *All the coefficients of G'^{+}_n belong to the $\mathbb{F}_q[X_0, \ldots, X_{n-1}]$-module generated by*

$$\begin{cases} R^+_{n0}, R^+_{n1}, \ldots, R^+_{n,\lfloor\frac{n+1}{2}\rfloor}, & \text{if } n \text{ is enen and } \epsilon = -1; \text{ or } n \text{ is odd and } (\frac{\epsilon}{q}) = 1;\\ R^-_{n0}, R^-_{n1}, \ldots, R^-_{n,\lfloor\frac{n+1}{2}\rfloor}, & \text{if } n \text{ is odd and } (\frac{\epsilon}{q}) = -1 \end{cases}.$$

Proof. Let $\mathcal{M}_n$ be the $\mathbb{F}_q[X_0, \ldots, X_{n-1}]$-module generated by $R^{\pm}_{n0}, R^{\pm}_{n1}, \ldots, R^{\pm}_{n,\lfloor\frac{n+1}{2}\rfloor}$. We'll prove by induction on n. For $n = 1, 2$, it is easy to see check directly.

Let $n > 2$. First suppose n is even and $\epsilon = -1$. Consider (3-2). In this expression $\psi_j(X_0, \ldots, X_{n-2})$ is a coefficient of $G'^{\,+}_{n-2}$, so by the induction hypothesis, we have $\psi_j \in \mathcal{M}_{n-2}$ for all j, i.e.

$$\psi_j(X_0, \ldots, X_{n-2}) = h_{0j}R^+_{n-2,0} + \cdots + h_{\lfloor\frac{n-1}{2}\rfloor,j}R^+_{n-2,\lfloor\frac{n-1}{2}\rfloor}$$

for some $h_{ij} \in \mathbb{F}_q[X_0, \ldots, X_{n-3}]$. Let

$$\psi'_j(X_0, \ldots, X_n) := h^q_{0j}R^+_{n1} + \cdots + h^q_{\lfloor\frac{n-1}{2}\rfloor,j}R^+_{n,\lfloor\frac{n-1}{2}\rfloor+1} \in \mathcal{M}_n \quad .$$

Then by Lemma 3.1,

$$\begin{aligned}
\psi'_j - (-1)^{\lfloor\frac{n}{2}\rfloor}\psi_j^q X_n &= \sum_{i=1}^{\lfloor\frac{n+1}{2}\rfloor} h^q_{i-1,j}(R^+_{n,i} - (-1)^{\lfloor\frac{n}{2}\rfloor}R^{+\,q}_{n-2,i-1}X_n)\\
&= \sum_{i=1}^{\lfloor\frac{n+1}{2}\rfloor} h^q_{i-1,j}\phi_{n,i} \ \in \ \mathbb{F}_q[X_0, \ldots, X_{n-1}].
\end{aligned}$$

So

$$(-1)^{\lfloor\frac{n}{2}\rfloor}\psi_j^q X_n = h^q_{0j}R^+_{n1} + \cdots + h^q_{\lfloor\frac{n-1}{2}\rfloor,j}R^+_{n,\lfloor\frac{n-1}{2}\rfloor+1} + \sum_{i=1}^{\lfloor\frac{n+1}{2}\rfloor} h^q_{i-1,j}\phi_{n,i}.$$

Also

$$(-1)^{\frac{n}{2}}R^{+\,q}_{n-2,i-1}X_n = R^+_{n-2,i} - \phi_{n-2,i}(X_0, \ldots, X_{n-3}).$$

Substituting these into (3-1) and collecting all coefficients of R^+_{ni}, we get

$$G'^{\,+}_{n,-1}(T) = h_0 R^+_{n0} + h_1 R^+_{n1} + \cdots + h_{\lfloor \frac{n+1}{2} \rfloor} R^+_{n,\lfloor \frac{n+1}{2} \rfloor} + \phi'(X_0, \ldots, X_{n-1}, T)$$

where $h_j \in \mathbb{F}_q[X_0, \ldots, X_{n-1}; T]$. We write $\phi'(X_0, \ldots, X_{n-1}; T) = \sum_{k=0}^{N} a_k(X_0, \ldots, X_{n-1})T^k$. Then by Lemma 3.9 $a_k(Q^+_{n-1,0}, \ldots, Q^+_{n-1,n-1}) = 0 \quad \text{for all}\, k$. By Lemma 3.8, $a_k \in \langle g'^{+}_{n-1} \rangle = \langle R^+_{n0} \rangle$. Hence all coefficients of G'^{+}_n belong to $\mathcal{M}_n$.

To prove the other cases, we just need to replace (3-2) by (3-3) and (3-4), and use the same arguments.

A key technical part of the proof in §4 is the use of homogeneous regular sequence. So we first develop some basic properties about regular sequence which will be needed later. See [12].

Proposition 3.12. *If $x_1, x_2, \ldots, x_n \in R$ is a regular sequence, then x_1 is a non-zerodivisor in $R/\langle x_2, x_3, \ldots, x_n \rangle$.*

Proof. It suffices to prove for $n = 2$. So suppose x_1, x_2 is a regular sequence. We want to show that $x_1 r \in \langle x_2 \rangle$ implies $r \in \langle x_2 \rangle$. Assume that $x_1 r = x_2 s$. Because x_2 is a non-zerodivisor in $R/\langle x_1 \rangle$, $s = x_1 s'$ for some $s' \in R$. Then $x_1 r = x_2 x_1 s'$. Since x_1 is a non-zerodivisor in R, we may cancel it from both sides of the equation and get $r = x_2 s' \in \langle x_2 \rangle$.

Lemma 3.13.

(*a*) *If $x_1, x_2, \ldots, x_i, \ldots, x_n \in R$ is a regular sequence, and $x_1, x_2, \ldots, x_{i-1}, x'_i, x_{i+1}, \ldots, x_n \in R$ is a regular sequence, then $x_1, x_2, \ldots, x_{i-1}, x_i x'_i, x_{i+1}, \ldots, x_n$ is a regular sequence.*

(*b*) *If $x_1, x_2, \ldots, x_n \in R$ is a regular sequence, then $x_1^{k_1}, x_2^{k_2}, \ldots, x_n^{k_n}$ is a regular sequence for any $k_1, k_2, \ldots, k_n \in \mathbb{N}$.*

To make the proof in §4 go more smoothly, we establish several lemmas below. The first one is just a direct corollary of Lemma 3.13, but it is a situation we'll often encounter.

Lemma 3.14. *Let $R = F[X_0, X_1, \ldots, X_k, Y_1, Y_2, \ldots, Y_n]$, the polynomial ring of $k+n+1$ variables over a field F. Suppose we have a sequence $S_1, S_2, \ldots, S_m \in R$, $m \le n$, such that*

$$S_i = \sum_{j=1}^{n} a_{ij} Y_j$$

where $a_{ij} \in F[X_0, X_1, \ldots, X_k]$ and

$$a_{ij} \equiv \gamma_{ij} X^{l_{ij}}_{i+j-2} (\text{mod } X_0, X_1, \ldots, X_{i+j-3})$$

for some $\gamma_{ij} \in F^\times$, $l_{ij} \in \mathbb{N}$. (Here we require $k \ge m+n-2$ so that this condition makes sense). Then $X_0, X_1, \ldots, X_{n-2}, S_1, S_2, \ldots, S_m$ is a regular sequence in R.

Proof. Observe that

$$S_1 \equiv \gamma_{1n} X^{l_{1n}}_{n-1} Y_n (\text{mod} \langle X_0, X_1, \ldots, X_{n-2} \rangle) \tag{3-19}$$

$$S_2 \equiv \gamma_{2n} X^{l_{2n}}_{n} Y_n (\text{mod} \langle X_0, X_1, \ldots, X_{n-1} \rangle) \tag{3-20}$$

$$S_2 \equiv \gamma_{2,n-1} X^{l_{2,n-1}}_{n-1} Y_{n-1} (\text{mod} \langle X_0, X_1, \ldots, X_{n-2}, Y_n \rangle) \tag{3-21}$$

$$S_3 \equiv \gamma_{3,n} X_{n+1}^{l_{3,n}} Y_{n-1} (\mathrm{mod}\langle X_0, X_1, \ldots, X_n \rangle) \tag{3-22}$$

$$S_3 \equiv \gamma_{3,n-1} X_n^{l_{3,n-1}} Y_{n-1} (\mathrm{mod}\langle X_0, X_1, \ldots, X_{n-1}, Y_n \rangle) \tag{3-23}$$

$$S_3 \equiv \gamma_{3,n-2} X_{n-1}^{l_{3,n-2}} Y_{n-2} (\mathrm{mod}\langle X_0, X_1, \ldots, X_{n-2}, Y_{n-1}, Y_n \rangle) \tag{3-24}$$

$$\vdots$$

The lemma is proved by applying Lemma 3.11 over and over again. To explain the procedure, we prove the case $m = 3$ explicitly.

From (3-22), $X_1, \ldots, X_{n-1}, X_n, S_3$ is a regular sequence.

From (3-23), $X_1, \ldots, X_{n-1}, Y_n, S_3$ is a regular sequence.

So by (3-20) and Lemma 3.11, $X_1, \ldots, X_{n-2}, X_{n-1}, S_2, S_3$ is a regular sequence.

From (3-23), $X_1, \ldots, X_{n-2}, Y_n, X_{n-1}, S_3$ is a regular sequence.

From (3-24), $X_1, \ldots, X_{n-2}, Y_n, Y_{n-1}, S_3$ is a regular sequence.

So by (3-21) and Lemma 3.13, $X_1, \ldots, X_{n-2}, Y_n, S_2, S_3$ is a regular sequence.

Thus by (3-19) and Lemma 3.13 again, we see that $X_1, \ldots, X_{n-2}, S_1, S_2, S_3$ is a regular sequence.

In the following Lemmas 3.15, 3.16 and 3.17, let $R = R_0 \oplus R_1 \oplus R_2 \oplus \cdots$ be a positively graded ring, and for any $x \in R$, we denote its homogeneous component of the highest degree by $\mathrm{in}(x)$.

Lemma 3.15. *Let $x_1, x_2, \ldots, x_n \in R$ be homogeneous elements with positive degrees. If $x_1, x_2, \ldots, x_n$ is a regular sequence, then $x_1, x_2, \ldots, x_n$ is a regular sequence in any order.*

Proof. Since any permutation is a product of transpositions, it suffices to prove for $n = 2$. So suppose $x_1, x_2 \in R$ are homogeneous elements with positive degrees, and x_1, x_2 is a regular sequence. By Lemma 3.11, we only need to show that x_2 is a non-zerodivisor in R, i.e. $x_2 y = 0$ will imply $y = 0$. We may assume y to be homogeneous. Since x_1, x_2 is a regular sequence, $x_2 y = 0 \in \langle x_1 \rangle$ implies $y = x_1 y_1$ for some $y_1 \in R$, and we may assume y_1 to be homogeneous. If $y_1 = 0$, then we're done; if $y_1 \neq 0$, then $\deg y_1 < \deg y$ because $\deg x_1 > 0$. Now $x_2 y = x_2 x_1 y_1 = 0$, and because x_1 is a non-zerodivisor, $x_2 y_1 = 0$. Repeat the above argument, we have $y_1 = x_1 y_2$ for some homogeneous $y_2 \in R$, and either $y_2 = 0$ or $\deg y_2 < \deg y_1 < \deg y$. Note that since R is positively graded, this process can not be repeated indefinitely. Hence we must have $y = 0$.

Lemma 3.16. *Let $x_1, x_2, \ldots, x_n \in R$, not necessarily homogeneous, and suppose* $\mathrm{in}(x_1), \mathrm{in}(x_2), \ldots, \mathrm{in}(x_n)$ *is a regular sequence. If $s \in \langle x_1, x_2, \ldots, x_n \rangle$, then there exist $y_1, y_2, \ldots, y_n \in R$ such that $s = \sum_{i=1}^n x_i y_i$ and $\deg x_i + \deg y_i \leq \deg s$, $1 \leq i \leq n$.*

Proof. Induction on n. $n = 1$ is obvious, so suppose the statement holds for $n - 1$. Since $s \in \langle x_1, x_2, \ldots, x_n \rangle$, there exist $y_1, y_2, \ldots, y_n \in R$ such that $s = \sum_{i=1}^n x_i y_i$. Among all the possible choices of $y_1, y_2, \ldots, y_n$, choose one such that the number $m := \max\{\deg x_i + \deg y_i \mid 1 \leq i \leq n\}$ is the smallest. We are going to prove by contradiction that in this case, $m \leq \deg s$.

Suppose $m > \deg s$. Let $d_i = m - \deg x_i$, and let y_{i,d_i} be the homogeneous component of degree d_i in y_i. Because $m > \deg s$, we have

$$\sum_{i=1}^n \mathrm{in}(x_i) y_{i,d_i} = 0 \quad ,$$

hence

$$\mathrm{in}(x_n)y_{n,d_n} \in \langle \mathrm{in}(x_1), \mathrm{in}(x_2), \ldots, \mathrm{in}(x_{n-1})\rangle \quad .$$

Because $\mathrm{in}(x_1), \mathrm{in}(x_2), \ldots, \mathrm{in}(x_n)$ is a regular sequence, this implies

$$y_{n,d_n} \in \langle \mathrm{in}(x_1), \mathrm{in}(x_2), \ldots, \mathrm{in}(x_{n-1})\rangle \quad ,$$

hence there exist homogeneous $z_1, z_2, \ldots, z_{n-1} \in R$ such that

$$y_{n,d_n} = \sum_{i=1}^{n-1} \mathrm{in}(x_i) z_i$$

and $\deg z_i + \deg x_i = d_n$, $1 \le i \le n-1$.

Let

$$y_i' = y_i + z_i x_n \quad , \qquad 1 \le i \le n-1 \, ,$$
$$y_n' = y_n - y_{n,d_n} - \sum_{i=1}^{n-1} (x_i - \mathrm{in}(x_i)) z_i \quad .$$

It can be easily checked that $\sum_{i=1}^n x_i y_i' = \sum_{i=1}^n x_i y_i = s$. Note that $\deg y_n' < d_n$, because $\deg(y_n - y_{n,d_n}) < d_n$ and $\deg(x_i - \mathrm{in}(x_i))z_i < \deg x_i + \deg z_i = d_n$. Thus

$$\deg x_n y_n' \le \deg x_n + \deg y_n' < \deg x_n + d_n = m \quad ,$$

and since we suppose $m > \deg s$, we have $\deg(s - x_n y_n') < m$. By the induction hypothesis, there exist $y_1'', y_2'', \ldots, y_{n-1}'' \in R$ such that

$$\sum_{i=1}^{n-1} x_i y_i'' = \sum_{i=1}^{n-1} x_i y_i' = s - x_n y_n'$$

and $\deg x_i + \deg y_i'' \le \deg(s - x_n y_n') < m$, $1 \le i \le n-1$. Let $y_n'' = y_n'$, then $\sum_{i=1}^n x_i y_i'' = s$ and $\deg x_i + \deg y_i'' < m$, $1 \le i \le n$. This contradicts to the minimality of m.

Lemma 3.17. *Let $x_1, x_2, \ldots, x_n \in R$, not necessarily homogeneous. If $\mathrm{in}(x_1), \mathrm{in}(x_2), \ldots, \mathrm{in}(x_n)$ is a regular sequence, then $x_1, x_2, \ldots, x_n$ is a regular sequence.*

Proof. The statement obviously holds for $n = 1$. Suppose it holds for $n-1$. Then we only have to show that x_n is a non-zerodivisor in $R/\langle x_1, x_2, \ldots, x_{n-1}\rangle$.

Suppose $x_n y \in \langle x_1, x_2, \ldots, x_{n-1}\rangle$ in R. By Lemma 3.13, there exist $y_1, y_2, \ldots, y_{n-1} \in R$ such that

$$x_n y = \sum_{i=1}^{n-1} x_i y_i$$

and $\deg x_i + \deg y_i \le \deg x_n y$, $1 \le i \le n-1$. Hence

$$\mathrm{in}(x_n)\mathrm{in}(y) \in \langle \mathrm{in}(x_1), \mathrm{in}(x_2), \ldots, \mathrm{in}(x_{n-1})\rangle \quad .$$

(Note that $\mathrm{in}(x_n)\mathrm{in}(y)$ may be zero). Since $\mathrm{in}(x_1), \mathrm{in}(x_2), \ldots, \mathrm{in}(x_n)$ is a regular sequence, this implies

$$\mathrm{in}(y) \in \langle \mathrm{in}(x_1), \mathrm{in}(x_2), \ldots, \mathrm{in}(x_{n-1})\rangle \quad .$$

Thus there exist homogeneous $z_1, z_2, \ldots, z_{n-1} \in R$ such that

$$\mathrm{in}(y) = \sum_{i=1}^{n-1} \mathrm{in}(x_i) z_i \quad .$$

Let $y' = y - \sum_{i=1}^{n-1} x_i z_i$, then $x_n y' \in \langle x_1, x_2, \ldots, x_{n-1}\rangle$ and $\deg y' < \deg y$. Since R is positively graded, an induction on $\deg y$ will conclude that $y \in \langle x_1, x_2, \ldots, x_{n-1}\rangle$.

§ 4. Sopme results on Main Theorem.

Now we assume that Theorem A_k and Proposition B_{k-1} hold and want to prove the following Proposition.

Proposition $\mathbf{B}_k$. *Let $n = 2k+1$.* (a) *Define a homomorphism*

$$\tilde{\Phi}_n : \mathbb{F}_q[X_0, X_1, \cdots, X_{n-2}, X_{n-1}, Y_1, Y_2, \cdots, Y_k]/\langle K_{n1}, K_{n2}, \cdots, K_{n,k-1}\rangle \longrightarrow$$
$$\mathbb{F}_q[X_0, X_1, \cdots, X_{n-2}, X_{n-1}, \tfrac{R^+_{n-1,1}(X_0,X_1,\cdots,X_{n-1})}{R^+_{n-1,0}(X_0,X_1,\cdots,X_{n-2})}, \cdots, \tfrac{R^+_{n-1,k}(X_0,X_1,\cdots,X_{n-1})}{R^+_{n-1,0}(X_0,X_1,\cdots,X_{n-2})}],$$

which is defined by

$$\begin{aligned} X_i &\mapsto X_i, && 0 \le i \le n-2 \\ Y_j &\mapsto \tfrac{R^+_{n-1,j}(X_0,X_1,\cdots,X_{n-1})}{R^+_{n-1,0}(X_0,X_1,\cdots,X_{n-2})}, && 1 \le j \le n. \end{aligned}$$

Then

$$\ker \widetilde{\Phi}_n = \langle K_{n1}, K_{n2}, \cdots, K_{n,k-1}, K_{nk}\rangle/\langle K_{n1}, K_{n2}, \cdots, K_{n,k-1}\rangle$$

where K_{ni} are defined as

$$\begin{bmatrix} K_{n1} \\ K_{n2} \\ \vdots \\ K_{nk} \end{bmatrix} = \mathbf{A}^{(k)} \begin{bmatrix} 1 \\ Y_1 \\ \vdots \\ Y_k \end{bmatrix}.$$

(b) $\det\, \mathbf{A}^{(k)}_{\emptyset;1} = -R^+_{n-1,0}$, $\det\, \mathbf{A}^{(k)}_{\emptyset;i} = (-1)^{i+1} R^+_{n-1,i-1}, 2 \le i \le k+1.$
(c) *For any l, $1 \le l \le k-1$,*

$$\det\, \mathbf{A}^{(k)}_{\emptyset;1} \equiv r_{k,k+l} X_l^{\frac{q^k - q^{k-l}}{q-1}} \phi (\mathrm{mod}\ X_0, X_1, \cdots, X_l^{1+\frac{q^k-q^{k-l}}{q-1}}, \cdots, X_{k+l}, \cdots, X_{k-1}).$$

(d)

$$p_{ij} \equiv \alpha_{ij} X_{i+\frac{j+1}{2}}^{q^{\frac{j+1}{2}-i}} (\mathrm{mod}\ X_0, X_1, \cdots, X_{i+\frac{j+1}{2}-1}).$$

$$r_{ij} \equiv \beta_{ij} X_j (\mathrm{mod}\ X_0, X_1, \cdots, X_{j-1}).$$

(e) *Let*

$$\Psi_n : \mathbb{F}_q[X_0, \ldots, X_{n-1}, Y_2, \ldots, Y_{k+1}] \to \mathbb{F}_q[X_0, \ldots, X_{n-1}, (\frac{R^+_{n-1,1}}{R^+_{n-1,0}})^q, \ldots, (\frac{R^+_{n-1,k}}{R^+_{n-1,0}})^q]$$

be the ring homomorphism which sends X_i to X_i and Y_i to $(\frac{R^+_{n-1,i-1}}{R_{n-1,0}})^q$. Then

$$\ker \Psi_n = \langle K'_{n,1}, K'_{n,2}, \ldots, K'_{n,k} \rangle$$

where $K'_{n,1}, K'_{n,2}, \ldots, K'_{n,k}$ are defined as

$$\begin{bmatrix} K'_{n,1} \\ K'_{n,2} \\ \vdots \\ K'_{n,k} \end{bmatrix} = \varphi(\mathbf{A}^{(k)}) \begin{bmatrix} 1 \\ Y_2 \\ Y_3 \\ \vdots \\ Y_{k+1} \end{bmatrix}.$$

And the kernel of the map

$$\mathbb{F}_q[X_0, \ldots, X_n, Y_2, \ldots, Y_{k+1}] \to \mathbb{F}_q[X_0, \ldots, X_n, (\frac{R^+_{n-1,1}}{R^+_{n-1,0}})^q, \ldots, (\frac{R^+_{n-1,k}}{R^+_{n-1,0}})^q]$$

defined by

$$X_i \mapsto X_i, \qquad Y_i \mapsto (\frac{R^+_{n-1,i-1}}{R^+_{n-1,0}})^q$$

is also $\langle K'_{n,1}, K'_{n,2}, \ldots, K'_{n,k} \rangle$.

Proof of (a). *Step 1.* Let

$$\begin{aligned} \Pi\colon \mathbb{F}_q[X_0, \ldots, X_{n-2}, X_{n-1}, Y_1, \ldots, Y_{k+1}]/\langle K_{n1}, \ldots, K_{n,k-1} \rangle \longrightarrow \\ \mathbb{F}_q[X_0, \ldots, X_{n-2}, Y_1, \ldots, Y_{k+1}]/\langle K_{n1}, \ldots, K_{n,k-1} \rangle \end{aligned}$$

be the ring homomorphism which sends X_i to X_i for $0 \le i \le n-2$, Y_j to Y_j for $1 \le j \le k$, and X_{n-1} to 0. Then by Theorem $\mathbf{A}_k$, $\Phi_{2n+2} \circ \Pi = \widetilde{\Phi}_{2n+2}$ and Φ_n is an isomorphism. Thus

$$\begin{aligned} \ker \widetilde{\Phi}_n &= \Pi^{-1}(\ker \Phi_n) \\ &= \ker \Phi_n + \ker \Pi = \ker \Pi \end{aligned}$$

We just need to find K_{nk} such that $\ker \Pi = \langle K_{nk} \rangle$. Here we also define the entries $r_{k,2k}, r_{k,2k-1}$, $\ldots, r_{k,k}$ in the matrix $\mathbf{A}^{(k)}$.

Step 2. From

$$\mathbb{F}_q[x_1, x_2, \cdots, x_n]^{O^+_n(\mathbb{F}_q)} = \mathbb{F}_q[Q^+_{n0}, Q^+_{n1}, \cdots, Q^+_{n,n-2}, \frac{R^+_{n-1,1}(Q^+_{ni})}{R^+_{n-1,0}(Q^+_{ni})}, \cdots, \frac{R^+_{n-1,k}(Q^+_{ni})}{R^+_{n-1,0}(Q^+_{ni})}],$$

where $R^+_{n-1,j}(Q^+_{ni})$ is the abbreviation of $R^+_{n-1,j}(Q^+_{n0},\dots,Q^+_{n,n-1})$, and $Q^+_{n,n-1}\in\mathbb{F}_q[x_1,x_2,\cdots,x_n]^{O^+_n(\mathbb{F}_q)}$, it follows that

$$X_{n-1}\in\mathbb{F}_q[X_0,X_1,\cdots,X_{n-2},\frac{R^+_{n-1,1}}{R^+_{n-1,0}},\cdots,\frac{R^+_{n-1,k}}{R^+_{n-1,0}}]$$

i.e. there exists a polynomial $H(X_0,X_1,\dots,X_{n-2};Y_1,\dots,Y_k)$ such that

$$X_{n-1}=H(X_0,\dots,X_{n-2};\frac{R^+_{n-1,1}}{R^+_{n-1,0}},\dots,\frac{R^+_{n-1,k}}{R^+_{n-1,0}}) \tag{4-1}$$

Among all such polynomials, we choose H to be the one whose total degree in $Y_1,Y_2,\dots,Y_k$ is the smallest.

Step 3. We claim that

$$H \textit{ is linear in } Y_1,Y_2,\dots,Y_k. \tag{4-2}$$

We write

$$H=\sum_{m=0}^{l}\sum_{|\Lambda|=m}h_\Lambda(X_0,X_1,\dots,X_{n-2})\mathbf{Y}^\Lambda$$

where $\Lambda=(\lambda_1,\lambda_2,\cdots,\lambda_k),|\Lambda|=\sum_{i=1}^n\lambda_i,\mathbf{Y}^\Lambda=Y_1^{\lambda_1}Y_2^{\lambda_2}\cdots Y_k^{\lambda_k}$. Obviously $l\neq 0$, because $X_0,X_1,\dots,X_{n-2}$ are independent variables. By Lemma 3.1,

$$H(X_0,\dots,X_{n-2};\frac{R^+_{n-1,1}}{R^+_{n-1,0}},\dots,\frac{R^+_{n-1,k}}{R^+_{n-1,0}})\in\mathbb{F}_q(X_0,\dots,X_{n-2})[X_{n-1}],$$

Let H_l be the $\mathbf{Y}$-degree l part of H. Then the coefficient of X^l_{n-1} is

$$H_l(X_0,\dots,X_{n-2};R^{+\,q}_{n-3,0},\dots,R^{+\,q}_{n-3,k-1})/R^{+\,l}_{n-1,0}$$

So if $l\geq 2$, then by (4-1), $H_l(X_0,\dots,X_{n-2};R^{+\,q}_{n-3,0},\dots,R^{+\,q}_{n-3,k-1})=0$. Let $H'_l(X_0,\dots,X_{n-2};Y_2,\cdots,Y_k)$ be the dehomogenization of H_l with respect to Y_1 regarding it as a polynomial in $Y_1,Y_2,\cdots,Y_n$. Then

$$H'_l(X_0,\dots,X_{n-2},(\frac{R^+_{n-3,1}}{R^+_{n-3,0}})^q,\dots,(\frac{R^+_{n-3,k-1}}{R^+_{n-3,0}})^q)=0.$$

By Proposition $\mathbf{B}_{k-1}$(e) there exist $S'_1,\cdots,S'_{k-1}\in\mathbb{F}_q[X_0,X_1,\cdots,X_{n-2},Y_2,Y_3,\cdots,Y_k]$ such that $H'_l=\sum_{i=1}^{k-1}S'_iK'_{ni}$. By Proposition $\mathbf{B}_{k-1}$(d),

$$X_0,\,X_1\,,\dots,\,X_k\,,K'_{n,1}-p^q_{1,n-2}\,,\;K'_{n,2}-p^q_{2,n-2}\,,\dots,\;K'_{n,k-2}-p^q_{k-2,n-2}\,,\;K'_{n,k-1}-r^q_{k-1,n-1}$$

is a regular sequence in $\mathbb{F}_q[X_0,\dots,X_{n-2},Y_2,\dots,Y_k]$. Since they are homogeneous with respect the weight, by Lemma 3.15

$$K'_{n,1}-p^q_{1,n-2}\,,\;K'_{n,2}-p^q_{2,n-2}\,,\dots,\;K'_{n,k-2}-p^q_{k-2,n-2}\,,\;K'_{n,k-1}-r^q_{k-1,n-1}$$

is a also regular sequence in $\mathbb{F}_q[X_0,\dots,X_{n-2},Y_2,\dots,Y_k]$. Now if we consider the grading defined by total $\mathbf{Y}$-degree then Lemma 3.16 tells us that we may assume $\deg_{\mathbf{Y}}S'_i\leq l-1$.

So let S_i be the homogenization of S_i' with respect to Y_1 regarding it as a polynomial in $Y_1, Y_2, \cdots, Y_k$, we get

$$H_l = \sum_{i=1}^{k-1} (K_{n,i} - p_{i,n}) S_i \ .$$

Therefore $H - \sum_{i=1}^{n} K_{n,i} S_i$ has strictly smaller total degree in $Y_1, \ldots, Y_k$ than H, which is a contradiction because

$$X_{n-1} = (H - \sum_{i=1}^{k-1} K_{n,i} S_i)(X_0, \ldots, X_{n-2}, \tfrac{R^+_{n-1,1}}{R^+_{n-1,0}}, \ldots, \tfrac{R^+_{n-1,k}}{R^+_{n-1,0}}).$$

This proves our claim (4-2) that $l = 1$.

Step 4. (4-1) can be written as

$$X_{n-1} = r'_{k,2k} + r_{k,2k-1} \frac{R^+_{n-1,1}}{R^+_{n-1,0}} + r_{k,2k-2} \frac{R^+_{n-1,2}}{R^+_{n-1,0}} + \cdots + r_{kk} \frac{R^+_{n-1,k}}{R^+_{n-1,0}} \tag{4-3}$$

for some $r'_{k,2k}, r_{ni} \in \mathbb{F}_q[X_0, \ldots, X_{n-2}]$. Since by Lemma 3.2, $\frac{R^+_{n-1,i}}{R^+_{n-1,0}}$ is homogeneous of weight $q^{n-1} + q^{n-i-1}$, comparing the weight of each term, we may assume that $r_{n,n-i-1}$ is homogeneous with weight $q^{n-i-1} + 1$. Moreover, comparing with $\operatorname{wt} X_i$, we see that $r_{ni} \in \mathbb{F}_q[X_0, \ldots, X_i]$.

Let $r_{k,2k} := r'_{k,2k} - X_{n-1}$ and $K_{nk} := r_{k,2k} + r_{k,2k-1} Y_1 + r_{k,2k-2} Y_2 + \cdots + r_{kk} Y_k$. Then $\ker \tilde{\Phi}_n = \langle K_{nk} \rangle$ as desired.

Proof of (b). We compare the coefficients of X_{n-1} from both side of (4-3), and by Lemma 3.1 we see that

$$(-1)^k = r_{k,2k-1} \frac{{R^+_{n-3,0}}^q}{R^+_{n-1,0}} + r_{k,2k-2} \frac{{R^+_{n-3,1}}^q}{R^+_{n-1,0}} + \cdots + r_{kk} \frac{{R^+_{n-3,k}}^q}{R^+_{n-1,0}},$$

i.e.

$$(-1)^k R^+_{n-1,0} = r_{k,2k-1} {R^+_{n-3,0}}^q + r_{k,2k-2} {R^+_{n-3,1}}^q + \cdots + r_{kk} {R^+_{n-3,k}}^q. \tag{4-4}$$

With this, we can calculate $\det \mathbf{A}^{(k)}_{\emptyset;1}$ by expanding along its last row:

$$\begin{aligned} \det \mathbf{A}^{(k)}_{\emptyset;1} &= \textstyle\sum_{i=1}^{k} (-1)^{k+i} r_{k,2k-i} (\det \mathbf{A}^{(k-1)}_{\emptyset;i})^q \\ &= (-1)^{k+1} \textstyle\sum_{i=1}^{k} r_{k,2k-i} {R^+_{n-3,i-1}}^q && \text{(by (b) in case } k-1) \\ &= -R^+_{n-1,0} && \text{(by (4-4).} \end{aligned}$$

To determine the value of $\det \mathbf{A}^{(k)}_{\emptyset;i}$ for $2 \le i \le k+1$, we'll view

$$\mathbf{A}^{(k)} \begin{bmatrix} 1 \\ Y_1 \\ Y_2 \\ \vdots \\ Y_k \end{bmatrix} = 0$$

as a system of linear equations in $Y_1, Y_2, \ldots, Y_k$ with coefficients in the field $\mathbb{F}_q(X_0, \ldots, X_{n-1})$. The fact that $\det \mathbf{A}^{(k)}_{\emptyset;1} = -R^+_{n-1,0} \neq 0$ tells us this system has a unique solution

$$Y_i = (-1)^i \frac{\det \mathbf{A}^{(k)}_{\emptyset;i+1}}{\det \mathbf{A}^{(k)}_{\emptyset;1}} = (-1)^{i+1} \frac{\det \mathbf{A}^{(k)}_{\emptyset;i+1}}{R^+_{n-1,0}},\ 1 \leq i \leq k$$

However, we have already seen that

$$Y_i = \frac{R^+_{n-1,i}}{R^+_{n-1,0}},\ 1 \leq i \leq k\ ,$$

is a solution to the system. Therefore $\det \mathbf{A}^{(k)}_{\emptyset;i} = (-1)^{i+1} R^+_{n-1,i-1}, 2 \leq i \leq k+1$.

Proof of (c). To go further the proof, it is convenient to rename the entries of $\mathbf{A}^{(k)}$ as follows:

$$\mathbf{A}^{(k)} = \begin{bmatrix} a_{0k} & a_{0,k-1} & \cdots & a_{01} & a_{00} \\ a_{1k} & a_{1,k-1} & \cdots & a_{11} & a_{10} \\ \vdots & \vdots & & \vdots & \vdots \\ a_{k-1,k} & a_{k-1,k-1} & \cdots & a_{k-1,1} & a_{k-1,0} \end{bmatrix}.$$

note that

$$a_{ij} = \begin{cases} p^{q^{k-j}}_{i+1,2j-1} \in \mathbb{F}_q[X_0, \cdots, X_{2j-1}], & \text{if } j \geq i+2 \\ r^{q^{k-i-1}}_{i+1,i+j+1} \in \mathbb{F}_q[X_0, \cdots, X_{i+j+1}], & \text{if } j \leq i+1. \end{cases} \tag{4-5}$$

Moreover, from (2-12), we have

$$\operatorname{wt} a_{ij} = q^{k+j} + q^{k-i-1} \tag{4-6}$$

Let $\bar{a}_{ij} \in \mathbb{F}_q[X_l, X_{k+l}]$ be the residue of a_{ij} modulo $\langle X_0, X_1, \cdots, X_l^{1+q^{k-l}(\frac{q^l-1}{q-1})}, \cdots, \hat{X}_{k+l}, \cdots, X_{n-1}\rangle$. We use the notation $\nu(f)$ to denote the largest integer s such that $X_l^s | f$, we set the convention that $\nu(0) = \infty$. Let S_k be the symmetric group on $\{0, 1, 2, , \cdots, k-1\}$. Let $\det \mathbf{A}^{(k)}_{\emptyset;1} = \sum_{\sigma \in S_k} (\pm \prod_{j=0}^{k-1} \bar{a}_{\sigma(j),j})$. To prove (c), we just need to show that

$$\text{(i) For any } \sigma \text{ such that } \sigma(l) \neq k-1, \text{then } \nu(\prod_{j=0}^{k-1} \bar{a}_{\sigma(j),j}) > 1 + q^{k-l}(\frac{q^l-1}{q-1}). \tag{4-7}$$

$$\text{(ii) For any } \sigma \text{ such that } \sigma(l) = k-1, \text{then } \nu(\prod_{\substack{0 \leq j \leq k-1 \\ j \neq l}} \bar{a}_{\sigma(j),j}) \geq q^{k-l}(\frac{q^l-1}{q-1}). \tag{4-8}$$

Before proving the claims (i) and (ii), we first note the following.

$$\text{If } j \leq l, \text{then } \bar{a}_{ij} \in \mathbb{F}_q[X_l] \text{ except that } (i,j) = (k-1, l)$$

by (4-5). Moreover, since $\bar{a}_{ij}$ is homogeneous, so if $\bar{a}_{ij} \neq 0$, it must be some power of X_l and

$$\mathrm{wt}\, X_l = q^l + 1 \mid \mathrm{wt}\, \bar{a}_{ij} = q^{k-i-1}(q^{i+j+1} + 1).$$

Thus we have $l \mid i + j + 1$, say,

$$i + j + 1 = lm \text{ for some odd integer } m, \tag{4-9}$$

and

$$\nu(\bar{a}_{ij}) = \frac{\mathrm{wt}\, \bar{a}_{ij}}{\mathrm{wt}\, X_l} = q^{k-i-1}(\frac{q^{i+j+1} + 1}{q^l + 1}). \tag{4-10}$$

Now we begin to prove Claims (i) and (ii). Let $\pm \prod_{j=0}^{k-1} \bar{a}_{\sigma(j),j}$ be a term in $\det \mathbf{A}^{(k)}_{\emptyset;1}$, $\sigma \in S_k$. Suppose $\sigma(l) \neq k-1$ and $\bar{a}_{\sigma(l),l} \neq 0$. Then

$$\begin{aligned}\nu(\prod_{j=0}^{k-1} \bar{a}_{\sigma(j),j}) \geq & \nu(\bar{a}_{\sigma(l),l}) = q^{k-\sigma(l)-1}(\frac{q^{l+\sigma(l)+1} + 1}{q^l + 1}) \qquad \text{by } (4-10)\\ =& \frac{q^{k+l} + q^{k-\sigma(l)-1}}{q^l + 1}\\ >& \frac{q^k - q^{k-l}}{q - 1}.\end{aligned}$$

by routine checking. Thus the Claim (i) is proved. Now we suppose that $\sigma(l) = k-1$. For any $j = 0, 1, \cdots, l-1$, if $\bar{a}_{\sigma(j),j} \neq 0$, from (4-9), then we have

$$\sigma(j) = m_j l - j - 1.$$

For any h such that $1 \leq h \leq m_j - 1$, find $s_h^{(j)}$ such that

$$\sigma(s_h^{(j)}) = hl - j - 1,\ s_h^{(j)} \neq j. \tag{4-11}$$

Let $\mathcal{S}^{(j)} = \{s_h^{(j)} : 1 \leq h \leq m_j - 1\}$. Note that the sets $\mathcal{S}^{(j)}$'s are disjoint for different j's. If $0 \leq s_h^{(j)} \leq l-1$ for some h, then $\bar{a}_{\sigma(s_h^{(j)}),s_h^{(j)}} = 0$. Otherwise, by (4-9), $l|\sigma(s_h^{(j)}) + s_h^{(j)} + 1 = hl - j - 1 + s_h^{(j)} + 1$, so $l|s_h^{(j)} - j$. But $0 < |s_h^{(j)} - j| < l$, a contradiction. Hence we may assume that $s_h^{(j)} \geq l+1$ for all $0 \leq h \leq m_j - 1$. By (4-6),

$$\mathrm{wt}(\bar{a}_{\sigma(s_h^{(j)}),s_h^{(j)}}) = q^{k+s_h^{(j)}} + q^{k-\sigma(s_h^{(j)})-1} = q^{k+s_h^{(j)}} + q^{k-hl+j}.$$

Suppose $\bar{a}_{\sigma(s_h^{(j)}),s_h^{(j)}} = \gamma X_l^\alpha X_{k+l}^\beta, \alpha, \beta \geq 0$. Then we have an equation

$$q^{k+s_h^{(j)}} + q^{k-hl+j} = \alpha(q^l + 1) + \beta(q^{k+l} + 1). \tag{4-12}$$

Suppose the equation (4-12) has no solution, then $\bar{a}_{\sigma(s_h^{(j)}),s_h^{(j)}} = 0$. Thus we assume that (4-12) has an integer solution (α, β). Observe that

$$\alpha(q^l + 1) = (q^{s_h^{(j)}-l} - \beta)(q^{k+l} + 1) + q^{k-hl+j} - q^{s_h^{(j)}-l}. \tag{4-13}$$

The case $q^{s_h^{(j)}-l}-\beta<0$ is impossible since α is nonnegative. If $q^{s_h^{(j)}-l}-\beta\geq 1$, then

$$\alpha \geq \frac{q^{k-hl+j}-q^{s_h^{(j)}-l}+q^{k+l}+1}{q^l+1} \tag{4-14}$$

$$\nu(\prod_{j=0}^{k-1}\bar{a}_{\sigma(j),j}) \geq \nu(\bar{a}_{\sigma(s_h 1^{(j)}),s_h^{(j)}}) = \alpha \geq q^{k-1}(\frac{q^l}{q-1}).$$

The last equalioty follows from (4-14) and direct checking. Thus (4-6) holds. Hence we have $q^{s_h^{(j)}-l}-\beta=0$. From (4-12), we have

$$q^{k-hl+j}-q^{s_h^{(j)}-l}\geq 0 \tag{4-15}$$

and

$$\alpha=\frac{q^{k-hl+j}-q^{s_h^{(j)}-l}}{q^l+1}=q^{s_h^{(j)}-l}(\frac{q^{k-hl+j-s_h^{(j)}+l}-1}{q^l+1}). \tag{4-16}$$

so $l\mid k-hl+j-s_h^{(j)}+l=k+j+l-s_h^{(j)}-hl$ and the quotient is an even integer. Therefore we have

$$s_h^{(j)}=k+j+l-\tau(h)l \tag{4-17}$$

where τ is a one to one map defined on $\{1,2,\cdots,m_j-1\}$ and $\tau(h)\equiv h(\text{mod } 2)$. From (4-12), we have $k-hl+j\geq s_h^{(j)}-l$. This implies that $\tau(h)\geq h$, that is τ is a nondecreasing function. Moreover, from $s_h^{(j)}\leq k-1$, we have $\tau(h)\geq 2$. We consider the sequence $1,\tau(1),\tau^2(1),\tau^3(1),\cdots$. note that this sequence is strictly increasing. In fact, $1<2\leq\tau(1)$, by induction, suppose $\tau^i(1)<\tau^{i+1}(1)$, then $\tau^{i+1}(1)<\tau^{i+2}(1)$ since τ is one to one. The sequence $1<\tau(1)<\tau^2(1)<\cdots<\tau^{r-1}(1)<\tau^r(1)$ will terminate until $\tau^r(1)\geq m_j$.

$$\begin{aligned}
&\nu(\bar{a}_{\sigma(0),0}\bar{a}_{\sigma(1),1}\cdots\widehat{\bar{a}_{\sigma(l),l}}\cdots\bar{a}_{\sigma(k-1),k-1})\\
\geq&\nu(\prod_{j=0}^{l-1}[\bar{a}_{\sigma(j),j}\prod_{h=0}^{m_j-1}\bar{a}_{\sigma(s_h^{(j)}),s_h^{(j)}}])\\
=&\sum_{j=0}^{l-1}[\nu(\bar{a}_{\sigma(j),j})+\sum_{h=0}^{m_j-1}\nu(\bar{a}_{\sigma(s_h^{(j)}),s_h^{(j)}})]\\
\geq&\sum_{j=0}^{l-1}[\nu(\bar{a}_{m_jl-j-1,j})+\sum_{i=0}^{r-1}\nu(\bar{a}_{\tau^i(1)l-j-1,s_{\tau^i(1)}})] \quad \text{by (4-11)}\\
\geq&\sum_{j=0}^{l-1}[\frac{q^{k+j}+q^{k+j-m_jl}}{q^l+1}+\sum_{i=0}^{r-1}\frac{q^{k+j-\tau^i(1)l}-q^{k+j-\tau^{i+1}(1)l}}{q^l+1}] \quad \text{by (4-10), (4-14) and (4-15)}\\
\geq&\sum_{j=0}^{l-1}[q^{k+j}+q^{k+j-l}+q^{k+j-m_jl}-q^{k+j-\tau^r(1)l}]/(q^l+1)\\
\geq&\frac{q^k}{q^l+1}\sum_{j=0}^{l-1}q^j(1+q^{-l}) \quad \text{since } \tau^r(1)\geq m_j\\
=&\frac{q^k}{q^l+1}\frac{q^l-1}{q-1}\frac{q^l+1}{q^l}=\frac{q^{k-l}(q^l-1)}{q-1}.
\end{aligned}$$

Thus claim (ii) is proved.

Proof of (d). The statement is equivelent to $a_{ij} \equiv \alpha_{ij} X_{i+j+1}^{q^{k-i-1}} (\mathrm{mod} X_0, X_1, \ldots, X_{i+j})$. By induction, we may assume that the result holds for $a_{ij}, i < k-1$ or $j < k$. We will prove the cases $a_{ik}, 0 \le i \le k-2$ and $a_{k-1,j}, 0 \le j \le k$. We separate into several cases. We first prove that

$$a_{ik} = p_{i+1,2k-1} \equiv \alpha_i X_{i+k+1}^{q^{k-i-1}} (\mathrm{mod} X_1, \cdots, \widehat{X}_k, \cdots, X_{k+i-1}). \tag{4-18}$$

From $K_{n,i+1}$, we have

$$p_{i+1,2k-1} R^+_{n-1,0} + p^q_{i+1,2k-3} R^+_{n-1,1} + \cdots + p^{q^{k-i-1}}_{i+1,2i+3} R^+_{n-1,n-i-1} + r^{q^{k-i}}_{i+1,2i+2} R^+_{n-1,k-i} + r^{q^{k-i}}_{i+1,2i+1} R^+_{n-1,k-i+1} + \cdots + r^{q^{k-i}}_{i+1,i+1} R^+_{n-1,k} = 0$$

That is,

$$a_{ik} R^+_{n-1,0} + a_{i,k-1} R^+_{n-1,1} + \cdots + a_{i,k-i-1} R^+_{n-1,i+1} + \cdots + a_{i0} R^+_{n-1,k} = 0. \tag{4-19}$$

It is known that, modulo $\langle X_0, \cdots, \widehat{X}_k, \cdots, X_{k+i} \rangle$, we have $R^+_{n-1,j} \equiv 0, 1 \le j \le i$ by Lemma 3.7(b) and $a_{ij} \equiv 0$ for $j \le k-i-2$ by induction hypothesis. So (4-19) implies that

$$a_{ik} R^+_{n-1,0} + a_{i,k-i-1} R^+_{n-1,i+1} = 0 (\mathrm{mod} X_0, \cdots, \widehat{X}_k, \cdots, X_{k+i}) \tag{4-20}$$

Moreover, $R^+_{n-1,0} = g^+_{n-2} \equiv X_k^{\frac{q^k-1}{q-1}}$ by Lemma 3.7(a), $R^+_{n-1,i+1} \equiv X_{k+i+1}^{q^{k-i-1}} X_k^{\frac{q^k-1}{q-1} - q^{k-i-1}}$ by Lemma 3.5, and $a_{i,k-i-1} \equiv X_k^{q^{k-i-1}}$ by induction hypotheses. Substitute these data into (4-20), we get (4-18).

Second, $a_{k-1,k} = r_{k,k-1}$ is followed by (2-11). Since

$$\det \mathbf{A}^{(k)}_{\emptyset;1} \equiv \begin{vmatrix} \gamma_{0,k} X_k^{q^{k-1}} & & & \\ & \gamma_{1,k-1} X_k^{q^{k-2}} & & 0 \\ & & \ddots & \\ & * & & \gamma_{k-1,1} X_k^q \\ & & & & r_{kk} \end{vmatrix}$$

$$\equiv R^+_{2k,0} \equiv X_k^{\frac{q^k-1}{q-1}} (\mathrm{mod}\ X_0, X_1, \cdots, X_{k-1}).$$

Thus $a_{k-1,0} = r_{kk} \equiv X_k (\mathrm{mod}\ X_0, X_1, \cdots, X_{k-1})$. Moreover, since

$$\det \mathbf{A}^{(k)}_{\emptyset;k} \equiv \begin{vmatrix} \gamma_{0,k+1} X_{k+1}^{q^k} & & & \\ & \gamma_{1,k} X_{k+1}^{q^{k-1}} & & 0 \\ & & \ddots & \\ & * & & \gamma_{k-1,2} X_{k+1}^q \\ & & & & r_{k,k+1} \end{vmatrix}$$

$$\equiv R^+_{2k,k} \equiv X_{k+1}^{\frac{q^{k+1}-1}{q-1}} (\mathrm{mod}\ X_0, X_1, \cdots, X_k).$$

Thus $a_{k-1,1} = r_{k,k+1} \equiv X_{k+1} (\mathrm{mod}\ X_0, X_1, \cdots, X_k)$.

At last, the remaining cases are $a_{k-1,l}$ such that $2 \le l \le k-1$. By Lemma 3.5, when we modulo $\langle X_0, X_1, \cdots, X_l^{1+\frac{q^k-q^{k-l}}{q-1}}, \cdots, \widehat{X}_{k+l}, \cdots, X_{n-1}\rangle$, we get

$$\det \mathbf{A}^{(k)}_{\emptyset;1} = R^+_{2k,0} = g'^+_{2k-1} \equiv X_l^{\frac{q^k-q^{k-l}}{q-1}} X_{k+l}^{\frac{q^{k-l}-1}{q-1}}, \tag{4-21}$$

and by (c),

$$\det \mathbf{A}^{(k)}_{\emptyset;1} \equiv r_{k,k+l} X_l^{\frac{q^k-q^{k-l}}{q-1}} \psi. \tag{4-22}$$

Comparing (4-21) and (4-22), we have $r_{k.k+l} \not\equiv 0 (\mathrm{mod}\ X_l)$. But $r_{k,k+l} \in \mathbb{F}_q[X_0, X_1, \cdots, X_{k+l}]$ and $\mathrm{wt}\, r_{k,k+l} = q^{k+l}+1$, so $r_{k,k+l} \equiv X_{k+l}$. Thus all statements in (d) are proved.

Proof of (e). The second statement follows from the first, since $R^+_{n-1,i}$ do not involve X_n. Comparing the transcendental degrees of the domain and the image of Ψ_n, we see that $\ker \Psi_n$ is a prime ideal in $\mathbb{F}_q[X_0, \ldots, X_{n-1}, Y_2, \ldots, Y_{k+1}]$ with height k. By (a), it is obvious that $\langle K'_{n1}, \ldots, K'_{nk}\rangle \subset \ker \Psi_n$. Thus to prove the fist statement, we just need to show that $\langle K'_{n1}, \ldots, K'_{nk}\rangle$ is a prime ideal in $\mathbb{F}_q[X_0, \ldots, X_{n-1}, Y_2, \ldots, Y_{k+1}]$ with the same height, and then they must be equal.

Step 1. In $\mathbb{F}_q[X_0, \ldots, X_{n-1}, Y_2, \ldots, Y_{k+1}][\frac{1}{g'^+_{n-2}}]/\langle K'_{n1}, \ldots, K'_{nk}\rangle$, the relations $K'_{n1}, \ldots, K'_{nk}$ can be written as

$$\varphi(\mathbf{A}^{(k)}_{\emptyset;1}) \begin{bmatrix} Y_2 \\ Y_3 \\ \vdots \\ Y_{k+1} \end{bmatrix} = - \begin{bmatrix} p_{1,n-2} \\ p_{2,n-2} \\ \vdots \\ p_{k-1,n-2} \\ r_{k,n-1} \end{bmatrix}.$$

By (b), $\det \mathbf{A}^{(k)}_{\emptyset;1} = g'^+_{n-2}$. Since we have localized at g'^+_{n-2}, the matrix $\varphi(\mathbf{A}^{(k)}_{\emptyset;1})$ becomes invertible, so we can solve the above relations to express $Y_2, Y_3, \ldots, Y_{k+1}$ in terms of $X_0, \ldots, X_{n-1}$. Therefore

$$\begin{aligned} &\mathbb{F}_q[X_0, \ldots, X_{n-1}, Y_2, \ldots, Y_{k+1}][\frac{1}{g'^+_{n-2}}]/\langle K'_{n1}, \ldots, K'_{nk}\rangle \\ = &\mathbb{F}_q[X_0, \ldots, X_{n-1}][\frac{1}{g'^+_{n-2}}] \end{aligned}$$

is an affine domain with Krull dimension n. Since $\mathbb{F}_q[X_0, \ldots, X_{n-1}, Y_2, \ldots, Y_{k+1}][\frac{1}{g'^+_{n-2}}]$ is an affine domain with Krull dimension $n+n$, $\langle K'_{n1}, \ldots, K'_{nn}\rangle$ is a prime ideal in $\mathbb{F}_q[X_0, \ldots, X_{n-1}, Y_2, \ldots, Y_{k+1}][\frac{1}{g'^+_{n-2}}]$ with height n.

Step 2. From (d) and definition of K'_{ni}, we have $K'_{ni} \equiv X_{k+i} (\mathrm{mod} X_0, \ldots, X_{k+i-1})$. Thus by Lemmas 3.3,3.13 and (b), $X_0, X_1, \ldots, X_{n-2}, g'^+_{n-2}, K'_{n1}, K'_{n2}, \ldots, K'_{nk}$ is a regular sequence in $\mathbb{F}_q[X_0, \ldots, X_{n-1}, Y_2, \ldots, Y_{k+1}]$. They are homogeneous with respect to the weight given in (1.5) and wt $Y_i = q^n - q^{n-i+1}$, then by Lemma 3.15, this sequence is a regular sequence in any order. In particular, g'^{+}_{n-2} is a non-zero divisor in $\mathbb{F}_q[X_0, \ldots, X_{n-1}, Y_2, \ldots, Y_{k+1}]$ $/\langle K'_{n1}, \ldots, K'_{nk}\rangle$ hence

$$\begin{aligned}&\mathbb{F}_q[X_0, \ldots, X_{n-1}, Y_2, \ldots, Y_{k+1}]/\langle K'_{n1}, \ldots, K'_{nk}\rangle \\ &\qquad\hookrightarrow \mathbb{F}_q[X_0, \ldots, X_{n-1}, Y_2, \ldots, Y_{k+1}][\frac{1}{g'^{+}_{n-2}}]/\langle K'_{n1}, \ldots, K'_{nk}\rangle\end{aligned}$$

and thus is also a domain. So $\langle K'_{n1}, \ldots, K'_{nk}\rangle$ is a prime ideal in $\mathbb{F}_q[X_0, \ldots, X_{n-1}, Y_2, \ldots, Y_{k+1}]$, and its height is n, the same as the height of its localization in $\mathbb{F}_q[X_0, \ldots, X_{n-1}, Y_2, \ldots, Y_{k+1}][\frac{1}{g'^{+}_{n-2}}]$. Thus (e) is proved and all the proof of Proposition are complete.

§ 5. The Proof of the Main Theorem for Odd n.

Now we assume Theorem $\mathbf{A}_i$ and Proposition $\mathbf{B}_i$ holds for $i \leq k$. We want to give a

Proof of Theorem $\mathbf{A}_{k+1}$. *Step 1.* First we are going to define $p_{i,n}$, $1 \leq i \leq n$. By Proposition $\mathbf{B}_k$(e),

$$\varphi(\mathbf{A}^{(k)}) \begin{bmatrix} 1 \\ (\frac{R^+_{n-1,1}}{R^+_{n-1,0}})^q \\ (\frac{R^+_{n-1,2}}{R^+_{n-1,0}})^q \\ \vdots \\ (\frac{R^+_{n-1,k}}{R^+_{n-1,0}})^q \end{bmatrix} = 0 \quad \Rightarrow \quad \varphi(\mathbf{A}^{(k)}) \begin{bmatrix} R^{+q}_{n-1,0} \\ R^{+q}_{n-1,1} \\ \vdots \\ R^{+q}_{n-1,k} \end{bmatrix} = 0.$$

By Proposition 2.12 and Lemma 3.9, there exist $p_{i,n} \in \mathbb{F}_q[X_0, \ldots, X_n]$, $1 \leq i \leq n$, such that

$$\varphi(\mathbf{A}^{(n)}) \begin{bmatrix} R^+_{n+1,1} \\ R^+_{n+1,2} \\ \vdots \\ R^+_{n+1,k+1} \end{bmatrix} = - \begin{bmatrix} p_{1,n} \\ p_{2,n} \\ \vdots \\ p_{n,n} \end{bmatrix} R_{n+1,0} \tag{5–1}$$

Moreover, from (a) in case k and Lemma 2.9, we have $p_{i,n}$ is homogeneous of weight $q^{n+1} + q^{n+2-i}$, $1 \leq i \leq n$.

Step 2. From (5-1) we have

$$\begin{bmatrix} p_{1,n} \\ p_{2,n} \\ \vdots \\ p_{k,n} \end{bmatrix} + \varphi(\mathbf{A}^{(k)}) \begin{bmatrix} \frac{R^+_{n+1,1}}{R^+_{n+1,0}} \\ \frac{R^+_{n+1,2}}{R^+_{n+1,0}} \\ \vdots \\ \frac{R^+_{n+1,k+1}}{R^+_{n+1,0}} \end{bmatrix} = 0.$$

So $\langle K_{n+2,1}, K_{n+2,2}, \ldots, K_{n+2,k}\rangle \subset \ker \Phi_{n+2}$.

To prove the opposite inclusion, suppose

$$H(X_0,\ldots,X_n,Y_1,\ldots,Y_{k+1})=\sum_{m=0}^{l}\sum_{|\Lambda|=m}h_\Lambda(X_0,X_1,\ldots,X_n)\mathbf{Y}^\Lambda\in\ker\Phi_{n+2}\ .$$

(Here we use the same notations as (4-2).) We proceed by induction on l. $l=0$ is trivial. So suppose $l\geq 1$. By Proposition 3.1,

$$H(X_0,\ldots,X_n,\frac{R^+_{n+1,1}}{R^+_{n+1,0}},\ldots,\frac{R^+_{n+1,k+1}}{R^+_{n+1,0}})\in\mathbb{F}_q(X_0,\ldots,X_n)[X_{n+1}]\ ,$$

By the similar arguments as given in the proof of Proposition 4.1 (a), there exist $S_i(X_0,\ldots,X_n,Y_2,\ldots,Y_{k+1})\in\mathbb{F}_q[X_0,\ldots,X_n,Y_2,\ldots,Y_{k+1}]$, $1\leq i\leq k$, such that $H-\sum_{i=1}^k K_{n+2,i}S_i\in\ker\Phi_{n+2}$ whose total degree in $Y_1,Y_2,\ldots,Y_{k+1}$ is strictly less than that of F. By the induction hypothesis, $H-\sum_{i=1}^k K_{n+2,i}S_i\in\langle K_{n+2,1},K_{n+2,2},\ldots,K_{n+2,k}\rangle$, hence $H\in\langle K_{n+2,1},K_{n+2,2},\ldots,K_{n+2,k}\rangle$.

Step 3. To prove that $\mathbb{F}_q[X_0,\ldots,X_n,Y_1,\ldots,Y_{k+1}]/\langle K_{n+2,1},\ldots,K_{n+2,k}\rangle$ is a UFD, it is enough to show that

$$\mathbb{F}_q[X_0,\ldots,X_n,Y_1,\ldots,Y_{k+1}]/\langle g'^{\,+}_{n-2},K_{n+2,1},\ldots,K_{n+2,k}\rangle\text{is an integral domain.}$$

In fact, in $\mathbb{F}_q[X_0,\ldots,X_n,Y_1,\ldots,Y_{k+1}]/\langle K_{n+2,1},\ldots,K_{n+2,k}\rangle$, the relations $K_{n+2,1},\ldots,K_{n+2,k}$ take the form

$$\begin{bmatrix}p_{1,n}\\ \vdots\\ p_{k,n}\end{bmatrix}+\varphi(\mathbf{A}^{(k)})\begin{bmatrix}Y_1\\ \vdots\\ Y_{k+1}\end{bmatrix}=0,$$

or

$$\varphi(\mathbf{A}^{(k)}_{\emptyset;1})\begin{bmatrix}Y_2\\ \vdots\\ Y_{k+1}\end{bmatrix}=-\begin{bmatrix}p_{1,n}+p^q_{1,n-2}Y_1\\ \vdots\\ p_{k-1,n}+p^q_{k-1,n-2}Y_1\\ p_{k,n}+r^q_{k,n-1}Y_1\end{bmatrix}$$

By Proposition $\mathbf{B}$(d),(b), $\det\mathbf{A}^{(k)}_{\emptyset;1}=g'^{\,+}_{n-2}$, so in $\mathbb{F}_q[X_0,\ldots,X_n,Y_1,\ldots,Y_{k+1}][\frac{1}{g'^{\,+}_{n-2}}]\ /\langle K_{n+2,1},\ldots,K_{n+2,k}\rangle$, $\varphi(\mathbf{A}^{(k)}_{\emptyset;1})$ is invertible and we can solve $Y_2,\ldots,Y_{k+1}$ in terms of $X_0,\ldots,X_n$, Y_1. Hence

$$\mathbb{F}_q[X_0,\ldots,X_n,Y_1,\ldots,Y_{k+1}][\frac{1}{g'^{\,+}_{n-2}}]/\langle K_{n+2,1},\ldots,K_{n+2,k}\rangle=\mathbb{F}_q[X_0,\ldots,X_n,Y_1][\frac{1}{g'^{\,+}_{n-2}}]$$

is a UFD. If we can show that $\mathbb{F}_q[X_0,\ldots,X_n,Y_1,\ldots,Y_{k+1}]/\langle g'^{\,+}_{n-2},K_{n+2,1},\ldots,K_{n+2,k}\rangle$ is an integral domain, or equivalently, that $g'^{\,+}_{n-2}$ is a prime element in $\mathbb{F}_q[X_0,\ldots,X_n,Y_1,\ldots,Y_{k+1}]$ $/\langle K_{n+2,1},\ldots,K_{n+2,k}\rangle$, then, by Nagata lemma [8], $\mathbb{F}_q[X_0,\ldots,X_n,Y_1,\ldots,Y_{k+1}]/\langle K_{n+2,1},\ldots,K_{n+2,k}\rangle$ would be a UFD.

Step 4. In order to prove a ring R to be a domain, we just need to find a non-zerodivisor $u\in R$ and show that $R[u^{-1}]$ is a domain, since R can be embedded in $R[u^{-1}]$. In our situation, the "u" we found is g'_{n-4}. So, in the following, we are going to show that

(i) g'_{n-4} is a non-zerodivisor in $\mathbb{F}_q[X_0,\dots,X_n,Y_1,\dots,Y_{k+1}]/\langle {g'}^{+}_{n-2}, K_{n+2,1},\dots,K_{n+2,k}\rangle$,
(ii) $\mathbb{F}_q[X_0,\dots,X_n,Y_1,\dots,Y_{k+1}][\frac{1}{{g'}^{+}_{n-4}}]/\langle {g'}^{+}_{n-2}, K_{n+2,1},\dots,K_{n+2,k}\rangle$ is a domain.

Step 5. We want to prove the claim (i). $k=1$ is trivial, so suppose $k\geq 2$. By Proposition $\mathbf{B}_K$ (a) and Lemma 3.12, in our case $n=2k$ is even, so $K_{n+2,i}-p_{in}\equiv X_{k+i}(\mathrm{mod} X_0,\dots,X_{k+i-1})$, and

$$X_0\,,\,X_1\,,\dots,\,X_k\,,\,K_{n+2,1}-p_{1,n}\,,\,K_{n+2,2}-p_{2,n}\,,\dots,\,K_{n+2,k}-p_{k,n}$$

is a regular sequence in $\mathbb{F}_q[X_0,\dots,X_n,Y_1,\dots,Y_{k+1}]$. Consider the grading determined by total degree in $Y_1,\cdots,Y_{k+1}$ and apply Lemma 3.14, we know that

$$X_0\,,\,X_1\,,\dots,\,X_k\,,\,K_{n+2,1}\,,\,K_{n+2,2}\,,\dots,\,K_{n+2,k}$$

is a regular sequence in $\mathbb{F}_q[X_0,\dots,X_n,Y_1,\dots,Y_{k+1}]$. By Lemma 3.3,

$$X_0\,,\,X_1\,,\dots,\,X_{k-2}\,,\,g'_{n-4}\,,\,g'_{n-2}\,,\,K_{n+2,1}\,,\,K_{n+2,2}\,,\dots,\,K_{n+2,k}$$

is a regular sequence in $\mathbb{F}_q[X_0,\dots,X_n,Y_1,\dots,Y_{k+1}]$. Finally, consider the weight defined in (1-5) and apply Lemma 2.15, we conclude that

$$X_0\,,\,X_1\,,\dots,\,X_{k-2}\,,\,{g'}^{+}_{n-4}\,,\,{g'}^{+}_{n-2}\,,\,K_{n+2,1}\,,\,K_{n+2,2}\,,\dots,\,K_{n+2,k}$$

is a regular sequence in any order in $\mathbb{F}_q[X_0,\dots,X_n,Y_1,\dots,Y_{k+1}]$. In particular, ${g'}^{+}_{n-4}$ is a non-zerodivisor in

$$\mathbb{F}_q[X_0,\dots,X_n,Y_1,\dots,Y_{k+1}]/\langle {g'}^{+}_{n-2}, K_{n+2,1},\dots,K_{n+2,k}\rangle\ .$$

Step 6. In $\mathbb{F}_q[X_0,\dots,X_n,Y_1,\dots,Y_{k+1}][\frac{1}{{g'}^{+}_{n-4}}]/\langle {g'}^{+}_{n-2}, K_{n+2,1},\dots,K_{n+2,k}\rangle$, the relations $K_{n+2,1}$, $\dots,K_{n+2,k-1}$ can be written in the form

$$\begin{bmatrix} p_{1,n}+p^{q}_{1,n-2}Y_1+p^{q^24}_{1,n-4}Y_2\\ p_{2,n}+p^{q}_{2,n-2}Y_1+p^{q^2}_{2,n-4}Y_2\\ \vdots\\ p_{k-2,n}+p^{q}_{k-2,n-2}Y_1+p^{q^2}_{k-2,n-4}Y_2\\ p_{k-1,n}+p^{q}_{k-1,n-2}Y_1+r^{q^2}_{k-1,n-3}Y_2 \end{bmatrix}+\varphi^2(\mathbf{A}^{(k-1)}_{\emptyset;1})\begin{bmatrix} Y_3\\ Y_4\\ \vdots\\ Y_{k+1}\end{bmatrix}=0. \tag{5–3}$$

By (d) in case k, $\det\mathbf{A}^{(k-1)}_{\emptyset;1}={g'}^{+}_{n-4}$. Since we have already localized at ${g'}^{+}_{n-4}$, $\varphi^2(\mathbf{A}^{(k-1)}_{\emptyset;1})$ would be invertible, so from (5-3) , $Y_3,Y_4,\dots,Y_{n+1}$ can be solved in terms of the other variables . Moreover, the relation between Y_1 and Y_2 is

$$R^{+\,q}_{n-1,1}Y_1-R^{+\,q}_{n-1,0}Y_2-R^{+\,q}_{n-1,1}\frac{R^{+}_{n+1,1}}{R^{+}_{n+1,0}}+R^{+\,q}_{n-1,0}\frac{R^{+}_{n+1,2}}{R^{+}_{n+1,0}}=0.$$

Thus let

$$\widetilde{K}_{n+2,k}:=\frac{-R^{+\,q}_{n-1,1}R^{+}_{n+1,1}}{R^{+}_{n+1,0}}+R^{+\,q}_{n-1,1}Y_1,$$

we have

$$\begin{aligned}&\mathbb{F}_q[X_0,\ldots,X_n,Y_1,\ldots,Y_{k+1}][\frac{1}{g'^{+}_{n-4}}]/\langle g'^{+}_{n-2},K_{n+2,1},\ldots,K_{n+2,k}\rangle\\ =&\mathbb{F}_q[X_0,\ldots,X_n,Y_1,Y_2][\frac{1}{g'^{+}_{n-4}}]/\langle g'^{+}_{n-2},\widetilde{K}_{n+2,n}\rangle.\end{aligned}$$

By Lemma 3.1, the relation $g'^{\,+}_{n-2}$ can also be solved to express X_{n-2} in terms of the other variables, thus

$$\begin{aligned}D:=&\mathbb{F}_q[X_0,\ldots,X_n,Y_1,Y_2][\frac{1}{g'^{\,+}_{n-4}}]/\langle g'^{\,+}_{n-2}\rangle\\ =&\mathbb{F}_q[X_0,\ldots,\hat{X}_{n-2},\ldots,X_n,Y_1,Y_2][\frac{1}{g'^{\,+}_{n-4}}]\end{aligned}$$

is a UFD. Therefore if we can proof that $\widetilde{K}_{n+2,k}$ is irreducible in D, then we are done.

Step 7. Remembering that $R^{+}_{n-1,0}=g'^{\,+}_{n-2}$, it is easy to see that $R^{+}_{n-1,1}$ is irreducible in D. Hence

$$\widetilde{K}_{n+2,k}\text{ is irreducible in }D\iff R^{+}_{n-1,1}\frac{R^{+\,q}_{n-1,1}R^{+}_{n+1,1}}{R^{+}_{n+1,0}}\text{ in }D\ .$$

But from Lemma 3.9, we have

$$R^{+}_{n+1,0}=g'^{+}_{n}=-\frac{(R^{+}_{n-1,1})^{q+1}}{g'^{+\,q}_{n-4}}\text{ in }D\ .$$

and

$$R^{+\,2}_{n-1,1}R^{+}_{n+1,1}\text{ in }D\ .$$

Let $R^{*}_{n}=\mathbb{F}_q[Q^{+}_{n0},Q^{+}_{n1},\cdots,Q^{+}_{n,n-2},\frac{R^{\pm}_{n-1,1}(X_0,X_1,\cdots,X_{n-1})}{R^{\pm}_{n-1,0}(X_0,X_1,\cdots,X_{n-2})},\cdots,\frac{R^{\pm}_{n-1,n}(X_0,X_1,\cdots,X_{n-1})}{R^{\pm}_{n-1,0}(X_0,X_1,\cdots,X_{n-2})}]$. Moreover, since $R^{+}_{n-1,i}$ is linear in $X_{n-1},Q_{n-1,n}$ belongs to the quotient field of R^{*}_{n}. Hence the quotient field of R^{*}_{n} is $\mathbb{F}_q(x_1,x_2,\ldots,x_n)^{O_n(\mathbb{F}_q)}$. Because the monic minimal polynomial of x_n belongs to $R^{*}_{n}[T]$ by Lemma 3.4. $\mathbb{F}_q(x_1,x_2,\ldots,x_n)^{O_n(\mathbb{F}_q)}$is integral over R^{*}_{n}. By Steps $3\sim 7$, R^{*}_{n} is a UFD, hence is integrally closed. Thus $\mathbb{F}_q(x_1,x_2,\ldots,x_n)^{O_n(\mathbb{F}_q)}=R^{*}_{n}$

The proof of the Theorem $\mathbf{A}_{k+1}$ is thus complete.

§ 6. The Statemaen of the Main Theorem for Even n.

Theorem C$_k$. *Let $n=2k$ be a positive even integer, $Q^{+}_{n}=x_1^2-x_2^2+x_3^2-\cdots-x_{n-2}^2+x_{n-1}^2-x_n^2$ be a quadratic form, $O^{+}_{n}(\mathbb{F}_q)$ be the orthogonal group associated to Q^{+}_{n}. Then*

(a) *The invariant subring is*

$$\begin{aligned}&\mathbb{F}_q[x_1,x_2,\cdots,x_n]^{O^{+}_{n}(\mathbb{F}_q)}\\ =&\mathbb{F}_q[Q^{+}_{n0},Q^{+}_{n1},\cdots,Q^{+}_{n,n-2},\frac{R^{+}_{n-1,1}(X_0,X_1,\cdots,X_{n-1})}{R^{+}_{n-1,0}(X_0,X_1,\cdots,X_{n-2})},\cdots,\frac{R^{+}_{n-1,k}(X_0,X_1,\cdots,X_{n-1})}{R^{+}_{n-1,0}(X_0,X_1,\cdots,X_{n-2})}].\end{aligned}$$

(b) *We have an isomorphism*

$$\Phi_n : \mathbb{F}_q[X_0, X_1, \cdots, X_{n-2}, Y_1, Y_2, \cdots, Y_k]/\langle K_{n1}, K_{n2}, \cdots, K_{n,k-1}\rangle \longrightarrow$$
$$\mathbb{F}_q[X_0, X_1, \cdots, X_{n-2}, \tfrac{R^+_{n-1,1}(X_0,X_1,\cdots,X_{n-1})}{R^+_{n-1,0}(X_0,X_1,\cdots,X_{n-2})}, \cdots, \tfrac{R^+_{n-1,k}(X_0,X_1,\cdots,X_{n-1})}{R^+_{n-1,0}(X_0,X_1,\cdots,X_{n-2})}]$$

defined by

$$\begin{aligned} X_i &\mapsto X_i, && 0 \le i \le n-2 \\ Y_j &\mapsto \tfrac{R^+_{n-1,j}(X_0,X_1,\cdots,X_{n-1})}{R^+_{n-1,0}(X_0,X_1,\cdots,X_{n-2})}, && 1 \le j \le k. \end{aligned}$$

where the relations K_{nj} are defined by

$$\begin{bmatrix} K_{n1} \\ K_{n2} \\ \vdots \\ K_{n,k-1} \end{bmatrix} = \mathbf{C}^{(k)}_{k;\emptyset} \begin{bmatrix} 1 \\ Y_1 \\ \vdots \\ Y_k \end{bmatrix}.$$

where

$$\mathbf{C}^{(k)} = \begin{bmatrix} p'_{1,2k-2} & p'^q_{1,2k-4} & p'^{q^2}_{1,2k-6} & \cdots & p'^{q^{k-2}}_{12} & r'^{q^{k-1}}_{11} & r'^{q^{k-1}}_{10} \\ p'_{2,2k-2} & p'^q_{2,2k-4} & p'^{q^2}_{2,2k-6} & \cdots & r'^{q^{k-2}}_{23} & r'^{q^{k-2}}_{22} & r'^{q^{k-2}}_{21} \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ r'_{k,2k-1} & r'_{k,2k-2} & r'_{k,2k-3} & \cdots & r'_{k,k+1} & r'_{k,k} & r'_{k,k-1} \end{bmatrix}$$

(c) *The polynomials p_{ij} and $r_{ij} \in \mathbb{F}_q[X_0, X_1, \cdots, X_j]$ are independent of n.*

$$r_{k,2k-1} = -X_{2k-1} + \psi(X_0, X_1, \cdots, X_{2k-2}) \quad \textit{for some polynomial } \psi.$$

Moreover, they are homogeneous with respect to the weight defined in (1-5) *with*

$$\begin{cases} wt\ p_{ij} = q^{j+1} + q^{\frac{j+1}{2}-i}, & j \text{ even;} \\ wt\ r_{ij} = q^j + 1. \end{cases}$$

Proposition $\mathbf{D}_k$. *Let $n = 2k$.* (a) *Define a homomorphism*

$$\tilde{\Phi}_n : \mathbb{F}_q[X_0, X_1, \cdots, X_{n-2}, X_{n-1}, Y_1, Y_2, \cdots, Y_k]/\langle K_{n1}, K_{n2}, \cdots, K_{n,k-1}\rangle \longrightarrow$$
$$\mathbb{F}_q[X_0, X_1, \cdots, X_{n-2}, X_{n-1}, \tfrac{R^+_{n-1,1}(X_0,X_1,\cdots,X_{n-1})}{R^+_{n-1,0}(X_0,X_1,\cdots,X_{n-2})}, \cdots, \tfrac{R^+_{n-1,k}(X_0,X_1,\cdots,X_{n-1})}{R^+_{n-1,0}(X_0,X_1,\cdots,X_{n-2})}],$$

which is defined by

$$\begin{aligned} X_i &\mapsto X_i, && 0 \le i \le n-2 \\ Y_j &\mapsto \tfrac{R^+_{n-1,j}(X_0,X_1,\cdots,X_{n-1})}{R^+_{n-1,0}(X_0,X_1,\cdots,X_{n-2})}, && 1 \le j \le n. \end{aligned}$$

Then

$$\ker \widetilde{\Phi}_n = \langle K_{n1}, K_{n2}, \cdots, K_{n,k-1}, K_{nk}\rangle / \langle K_{n1}, K_{n2}, \cdots, K_{n,k-1}\rangle$$

where K_{ni} are defined as

$$\begin{bmatrix} K_{n1} \\ K_{n2} \\ \vdots \\ K_{nk} \end{bmatrix} = \mathbf{C}^{(k)} \begin{bmatrix} 1 \\ Y_1 \\ \vdots \\ Y_k \end{bmatrix}.$$

(b) $\det\ \mathbf{C}^{(k)}_{\emptyset;1} = R^+_{n-1,0}, \quad \det\ \mathbf{C}^{(k)}_{\emptyset;i} = (-1)^{i+1} R^+_{n-1,i-1}, 2 \leq i \leq k+1.$

(c) *For any l, $1 \leq l \leq k-1$,*

$$\det\ \mathbf{C}^{(k)}_{\emptyset;1} \equiv r_{k,k+l} X_l^{\frac{q^k - q^{k-l}}{q-1}} \phi (\text{mod } X_0, X_1, \cdots, X_l^{1+\frac{q^k-q^{k-l}}{q-1}}, \cdots, X_{k+l}, \cdots, X_{k-1}).$$

(d)

$$p'_{ij} \equiv \alpha_{ij} X_{i+\frac{j}{2}}^{q^{\frac{j+1}{2}-i}} (\text{mod } X_0, X_1, \cdots, X_{i+\frac{j}{2}-1}).$$

$$r'_{ij} \equiv \beta_{ij} X_j (\text{mod } X_0, X_1, \cdots, X_{j-1}).$$

(e) *Let*

$$\Psi_n : \mathbb{F}_q[X_0, \ldots, X_{n-1}, Y_2, \ldots, Y_{k+1}] \to \mathbb{F}_q[X_0, \ldots, X_{n-1}, (\frac{R^+_{n-1,1}}{R^+_{n-1,0}})^q, \ldots, (\frac{R^+_{n-1,k}}{R^+_{n-1,0}})^q]$$

be the ring homomorphism which sends X_i to X_i and Y_i to $(\frac{R^+_{n-1,i-1}}{R_{n-1,0}})^q$. Then

$$\ker \Psi_n = \langle K'_{n,1}, K'_{n,2}, \ldots, K'_{n,k}\rangle$$

where $K'_{n,1}, K'_{n,2}, \ldots, K'_{n,k}$ are defined as

$$\begin{bmatrix} K'_{n,1} \\ K'_{n,2} \\ \vdots \\ K'_{n,k} \end{bmatrix} = \varphi(\mathbf{C}^{(k)}) \begin{bmatrix} 1 \\ Y_2 \\ Y_3 \\ \vdots \\ Y_{k+1} \end{bmatrix}.$$

And the kernel of the map

$$\mathbb{F}_q[X_0, \ldots, X_n, Y_2, \ldots, Y_{k+1}] \to \mathbb{F}_q[X_0, \ldots, X_n, (\frac{R^+_{n-1,1}}{R^+_{n-1,0}})^q, \ldots, (\frac{R^+_{n-1,k}}{R^+_{n-1,0}})^q]$$

defined by

$$X_i \mapsto X_i, \qquad Y_i \mapsto (\frac{R^+_{n-1,i-1}}{R^+_{n-1,0}})^q$$

is also $\langle K'_{n,1}, K'_{n,2}, \ldots, K'_{n,k}\rangle$.

The proof are almost the same as that of the odd cases, hence we omit it.

REFERENCES

[1] D. Benson, Polynomialinvariants of finite groups, London Mathematics Society Lecture Noote Series 190, Cambridge University Press,1993.
[2] D. Carlisle and P. Kropholler, Rational invariants of certain orthogonal and unitary groups, Bull. London Math. Soc. 24(1992), 57-60.
[3] D. Carlisle and P. Kropholler, Modular invariants of finite symplectic groups, Preprint.
[4] H. Chu, Polynomial invariants of four-dimensional orthogonal groups, Commnication in Algebra 29(2001),1153-1164.
[5] H. Chu and S-Y Jow, Polynomial invariants of finite unitary groups, submitted.
[6] L. Dickson, A fundamental system of invariants of the general modular linear group with a solution of the form problem, Trans. A.M.S.12(1911),75-98.
[7] N. Jacobson, Basic Algebra, vol 1, W.H.Freeman and Com, 1984.
[8] I. Kaplansky, Commutative rings, The university of Chicago Press, Chicago, 1974.