Electronic Research Archive

http://www.aimspress.com/journal/era

ERA, 31(7): 4303–4312.
DOI: 10.3934/era.2023219
Received: 11 March 2023
Revised: 21 April 2023
Accepted: 08 May 2023
Published: 05 June 2023

Research article

The number of rational points on a class of hypersurfaces in quadratic extensions of finite fields

Qinlong Chen and Wei Cao*

School of Mathematics and Statistics, Minnan Normal University, Zhangzhou 363000, Fujian Province, China

* **Correspondence:** Email: caow2286@mnnu.edu.cn.

Abstract: Let q be an even prime power and let $\mathbb{F}_q$ be the finite field of q elements. Let f be a nonzero polynomial over $\mathbb{F}_{q^2}$ of the form $f = a_1x_1^{m_1} + \cdots + a_sx_s^{m_s} + y_1y_2 + \cdots + y_{n-1}y_n + y_{n-2t-1}^2 + \cdots + y_{n-3}^2 + y_{n-1}^2 + b_ty_{n-2t}^2 + \cdots + b_1y_{n-2}^2 + b_0y_n^2$, where $a_i, b_j \in \mathbb{F}_{q^2}^*$, $m_i \neq 1$, $(m_i, m_k) = 1$, $i \neq k$, $m_i|(q+1)$, $m_i \in \mathbb{Z}^+$, $2|n$, $n > 2$, $0 \leq t \leq \frac{n}{2} - 2$, $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}(b_j) = 1$ for $i, k = 1, \ldots, s$ and $j = 0, 1, \ldots, t$. For each $b \in \mathbb{F}_{q^2}$, let $N_{q^2}(f = b)$ denote the number of $\mathbb{F}_{q^2}$-rational points on the affine hypersurface $f = b$. In this paper, we obtain the formula of $N_{q^2}(f = b)$ by using the Jacobi sums, Gauss sums and the results of quadratic form in finite fields.

Keywords: finite field; polynomial; Jacobi sum; Gauss sum

1. Introduction

Let $\mathbb{F}_q$ be the finite field of q elements with characteristic p, where $q = p^r$, p is a prime number. Let $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$ and $\mathbb{Z}^+$ denote the set of positive integers. Let $s \in \mathbb{Z}^+$ and $b \in \mathbb{F}_q$. Let $f(x_1, \ldots, x_s)$ be a diagonal polynomial over $\mathbb{F}_q$ of the following form

$$f(x_1, \ldots, x_s) = a_1x_1^{m_1} + a_2x_2^{m_2} + \cdots + a_sx_s^{m_s},$$

where $a_i \in \mathbb{F}_q^*$, $m_i \in \mathbb{Z}^+$, $i = 1, \ldots, s$. Denote by $N_q(f = b)$ the number of $\mathbb{F}_q$-rational points on the affine hypersurface $f = b$, namely,

$$N_q(f = b) = \#\{(x_1, \ldots, x_s) \in \mathbb{A}^s(\mathbb{F}_q) \mid f(x_1, \ldots, x_s) = b\}.$$

In 1949, Hua and Vandiver [1] and Weil [2] independently obtained the formula of $N_q(f = b)$ in terms of character sum as follows

$$N_q(f = b) = q^{s-1} + \sum \psi_1\left(a_1^{-1}\right) \cdots \psi_s\left(a_s^{-s}\right) J_q^0(\psi_1, \ldots, \psi_s), \tag{1.1}$$

where the sum is taken over all s multiplicative characters of $\mathbb{F}_q$ that satisfy $\psi_i^{m_i} = \varepsilon$, $\psi_i \neq \varepsilon$, $i = 1, \ldots, s$ and $\psi_1 \cdots \psi_s = \varepsilon$. Here ε is the trivial multiplicative character of $\mathbb{F}_q$, and $J_q^0(\psi_1, \ldots, \psi_s)$ is the Jacobi sum over $\mathbb{F}_q$ defined by

$$J_q^0(\psi_1, \ldots, \psi_s) = \sum_{c_1+\cdots+c_s=0, c_i\in\mathbb{F}_q} \psi_1(c_1)\cdots\psi_s(c_s).$$

Though the explicit formula for $N_q(f = b)$ are difficult to obtain in general, it has been studied extensively because of their theoretical importance as well as their applications in cryptology and coding theory; see [3–9]. In this paper, we use the Jacobi sums, Gauss sums and the results of quadratic form to deduce the formula of the number of $\mathbb{F}_{q^2}$-rational points on a class of hypersurfaces over $\mathbb{F}_{q^2}$ under certain conditions. The main result of this paper can be stated as

Theorem 1.1. *Let $q = 2^r$ with $r \in \mathbb{Z}^+$ and $\mathbb{F}_{q^2}$ be the finite field of q^2 elements. Let $f(X) = a_1x_1^{m_1} + a_2x_2^{m_2} + \cdots + a_sx_s^{m_s}$, $g(Y) = y_1y_2 + y_3y_4 + \cdots + y_{n-1}y_n + y_{n-2t-1}^2 + \cdots + y_{n-3}^2 + y_{n-1}^2 + b_ty_{n-2t}^2 + \cdots + b_1y_{n-2}^2 + b_0y_n^2$, and $l(X, Y) = f(X) + g(Y)$, where $a_i, b_j \in \mathbb{F}_{q^2}^*$, $m_i \neq 1$, $(m_i, m_k) = 1$, $i \neq k$, $m_i|(q+1)$, $m_i \in \mathbb{Z}^+$, $2|n$, $n > 2$, $0 \le t \le \frac{n}{2} - 2$, $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}(b_j) = 1$ for $i, k = 1, \ldots, s$ and $j = 0, 1, \ldots, t$. For $h \in \mathbb{F}_{q^2}$, we have*

(1) *If $h = 0$, then*

$$N_{q^2}(l(X,Y) = 0) = q^{2(s+n-1)} + \sum_{\gamma\in\mathbb{F}_{q^2}^*}\left(\prod_{i=1}^{s}\left(\left(\frac{\gamma}{a_i}\right)_{m_i} m_i - 1\right)\left(q^{s+2n-3} + (-1)^t q^{s+n-3}\right)\right).$$

(2) *If $h \in \mathbb{F}_{q^2}^*$, then*

$$\begin{aligned}&N_{q^2}(l(X,Y) = h)\\ =&q^{2(s+n-1)} + \left(q^{s+2n-3} + (-1)^{t+1}\left(q^2-1\right)q^{s+n-3}\right)\prod_{i=1}^{s}\left(\left(\frac{h}{a_i}\right)_{m_i} m_i - 1\right)\\ &+ \sum_{\gamma\in\mathbb{F}_{q^2}^*\setminus\{h\}}\left[\prod_{i=1}^{s}\left(\left(\frac{\gamma}{a_i}\right)_{m_i} m_i - 1\right)\left(q^{2n+s-3} + (-1)^t q^{n+s-3}\right)\right].\end{aligned}$$

Here,

$$\left(\frac{\gamma}{a_i}\right)_{m_i} = \begin{cases} 1, & \text{if } \frac{\gamma}{a_i} \text{ is a residue of order } m_i, \\ 0, & \text{otherwise.}\end{cases}$$

2. Prerequisites

To prove Theorem 1.1, we need the lemmas and theorems below which are related to the Jacobi sums and Gauss sums.

Definition 2.1. Let χ be an additive character and ψ a multiplicative character of $\mathbb{F}_q$. The Gauss sum $G_q(\psi, \chi)$ in $\mathbb{F}_q$ is defined by

$$G_q(\psi, \chi) = \sum_{x\in\mathbb{F}_q^*} \psi(x)\chi(x).$$

In particular, if χ is the canonical additive character, i.e., $\chi(x) = e^{2\pi i \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)/p}$ where $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(y) = y + y^p + \cdots + y^{p^{r-1}}$ is the absolute trace of y from $\mathbb{F}_q$ to $\mathbb{F}_p$, we simply write $G_q(\psi) := G_q(\psi, \chi)$.

Let ψ be a multiplicative character of $\mathbb{F}_q$ which is defined for all nonzero elements of $\mathbb{F}_q$. We extend the definition of ψ by setting $\psi(0) = 0$ if $\psi \neq \varepsilon$ and $\varepsilon(0) = 1$.

Definition 2.2. Let $\psi_1, \ldots, \psi_s$ be s multiplicative characters of $\mathbb{F}_q$. Then, $J_q(\psi_1, \ldots, \psi_s)$ is the Jacobi sum over $\mathbb{F}_q$ defined by

$$J_q(\psi_1, \ldots, \psi_s) = \sum_{c_1+\cdots+c_s=1, c_i \in \mathbb{F}_q} \psi_1(c_1) \cdots \psi_s(c_s).$$

The Jacobi sums $J_q(\psi_1, \ldots, \psi_s)$ as well as the sums $J_q^0(\psi_1, \ldots, \psi_s)$ can be evaluated easily in case some of the multiplicative characters ψ_i are trivial.

Lemma 2.3. ([10, Theorem 5.19, p. 206]) *If the multiplicative characters $\psi_1, \ldots, \psi_s$ of $\mathbb{F}_q$ are trivial, then*

$$J_q(\psi_1, \ldots, \psi_s) = J_q^0(\psi_1, \ldots, \psi_s) = q^{s-1}.$$

If some, but not all, of the ψ_i are trivial, then

$$J_q(\psi_1, \ldots, \psi_s) = J_q^0(\psi_1, \ldots, \psi_s) = 0.$$

Lemma 2.4. ([10, Theorem 5.20, p. 206]) *If $\psi_1, \ldots, \psi_s$ are multiplicative characters of $\mathbb{F}_q$ with ψ_s nontrivial, then*

$$J_q^0(\psi_1, \ldots, \psi_s) = 0$$

if $\psi_1 \cdots \psi_s$ is nontrivial and

$$J_q^0(\psi_1, \ldots, \psi_s) = \psi_s(-1)(q-1)J_q(\psi_1, \ldots, \psi_{s-1})$$

if $\psi_1 \cdots \psi_s$ is trivial.

If all ψ_i are nontrivial, there exists an important connection between Jacobi sums and Gauss sums.

Lemma 2.5. ([10, Theorem 5.21, p. 207]) *If $\psi_1, \ldots, \psi_s$ are nontrivial multiplicative characters of $\mathbb{F}_q$ and χ is a nontrivial additive character of $\mathbb{F}_q$, then*

$$J_q(\psi_1, \ldots, \psi_s) = \frac{G_q(\psi_1, \chi) \cdots G_q(\psi_s, \chi)}{G_q(\psi_1 \cdots \psi_s, \chi)}$$

if $\psi_1 \cdots \psi_s$ is nontrivial and

$$\begin{aligned} J_q(\psi_1, \ldots, \psi_s) &= -\psi_s(-1)J_q(\psi_1, \ldots, \psi_{s-1}) \\ &= -\frac{1}{q}G_q(\psi_1, \chi) \cdots G_q(\psi_s, \chi) \end{aligned}$$

if $\psi_1 \cdots \psi_s$ is trivial.

We turn to another special formula for Gauss sums which applies to a wider range of multiplicative characters but needs a restriction on the underlying field.

Lemma 2.6. ([10, Theorem 5.16, p. 202]) *Let q be a prime power, let ψ be a nontrivial multiplicative character of $\mathbb{F}_{q^2}$ of order m dividing $q+1$. Then*

$$G_{q^2}(\psi) = \begin{cases} q, & \text{if } m \text{ odd or } \frac{q+1}{m} \text{ even,} \\ -q, & \text{if } m \text{ even and } \frac{q+1}{m} \text{ odd.} \end{cases}$$

For $h \in \mathbb{F}_{q^2}$, define $v(h) = -1$ if $h \in \mathbb{F}_{q^2}^*$ and $v(0) = q^2 - 1$. The property of the function $v(h)$ will be used in the later proofs.

Lemma 2.7. ([10, Lemma 6.23, p. 281]) *For any finite field $\mathbb{F}_q$, we have*

$$\sum_{c \in \mathbb{F}_q} v(c) = 0,$$

for any $b \in \mathbb{F}_q$,

$$\sum_{c_1+\cdots+c_m=b} v(c_1)\cdots v(c_k) = \begin{cases} 0, & 1 \leqslant k < m, \\ v(b)\, q^{m-1}, & k = m, \end{cases}$$

where the sum is over all $c_1, \ldots, c_m \in \mathbb{F}_q$ with $c_1 + \cdots + c_m = b$.

The quadratic forms have been studied intensively. A quadratic form f in n indeterminates is called nondegenerate if f is not equivalent to a quadratic form in fewer than n indeterminates. For any finite field $\mathbb{F}_q$, two quadratic forms f and g over $\mathbb{F}_q$ are called equivalent if f can be transformed into g by means of a nonsingular linear substitution of indeterminates.

Lemma 2.8. ([10, Theorem 6.30, p. 287]) *Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$, q even , be a nondegenerate quadratic form. If n is even, then f is either equivalent to*

$$x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n$$

or to a quadratic form of the type

$$x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n + x_{n-1}^2 + ax_n^2,$$

where $a \in \mathbb{F}_q$ satisfies $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a) = 1$.

Lemma 2.9. ([10, Corollary 3.79, p. 127]) *Let $a \in \mathbb{F}_q$ and let p be the characteristic of $\mathbb{F}_q$, the trinomial $x^p - x - a$ is irreducible in $\mathbb{F}_q$ if and only if $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a) \neq 0$.*

Lemma 2.10. ([10, Lemma 6.31, p. 288]) *For even q, let $a \in \mathbb{F}_q$ with $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a) = 1$ and $b \in \mathbb{F}_q$. Then*

$$N_q(x_1^2 + x_1x_2 + ax_2^2 = b) = q - v(b).$$

Lemma 2.11. ([10, Theorem 6.32 , p. 288]) *Let $\mathbb{F}_q$ be a finite field with q even and let $b \in \mathbb{F}_q$. Then for even n, the number of solutions of the equation*

$$x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n = b$$

in $\mathbb{F}_q^n$ *is* $q^{n-1}+v(b)q^{(n-2)/2}$. *For even n and* $a\in\mathbb{F}_q$ *with* $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)=1$, *the number of solutions of the equation*

$$x_1x_2+x_3x_4+\cdots+x_{n-1}x_n+x_{n-1}^2+ax_n^2=b$$

in $\mathbb{F}_q^n$ *is* $q^{n-1}-v(b)q^{(n-2)/2}$.

Lemma 2.12. *Let* $q=2^r$ *and* $h\in\mathbb{F}_{q^2}$. *Let* $g(Y)\in\mathbb{F}_{q^2}[y_1,y_2,\ldots,y_n]$ *be a polynomial of the form*

$$g(Y)=y_1y_2+y_3y_4+\cdots+y_{n-1}y_n+y_{n-2t-1}^2+\cdots+y_{n-3}^2+y_{n-1}^2+b_ty_{n-2t}^2+\cdots+b_1y_{n-2}^2+b_0y_n^2,$$

where $b_j\in\mathbb{F}_{q^2}^*$, $2|n$, $n>2$, $0\le t\le\frac{n}{2}-2$, $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}(b_j)=1$, $j=0,1,\ldots,t$. *Then*

$$N_{q^2}(g(Y)=h)=q^{2(n-1)}+(-1)^{t+1}q^{n-2}v(h). \tag{2.1}$$

Proof. We provide two proofs here. The first proof is as follows. Let $q_1=q^2$. Then by Lemmas 2.7 and 2.10, the number of solutions of $g(Y)=h$ in $\mathbb{F}_{q^2}$ can be deduced as

$$\begin{aligned}
&N_{q^2}(g(Y)=h)\\
=&\sum_{c_1+c_2+\cdots+c_{t+2}=h}N_{q^2}\left(y_1y_2+y_3y_4+\cdots+y_{n-2t-3}y_{n-2t-2}=c_1\right)\\
&\cdot N_{q^2}\left(y_{n-2t-1}y_{n-2t}+y_{n-2t-1}^2+b_ty_{n-2t}^2=c_2\right)\cdots N_{q^2}\left(y_{n-1}y_n+y_{n-1}^2+b_0y_n^2=c_{t+2}\right)\\
=&\sum_{c_1+c_2+\cdots+c_{t+2}=h}\left(q_1^{n-2t-3}+v(c_1)\,q_1^{(n-2t-4)/2}\right)(q_1-v(c_2))\cdots(q_1-v(c_{t+2}))\\
=&\sum_{c_1+c_2+\cdots+c_{t+2}=h}\left(q_1^{n-2t-2}+v(c_1)\,q_1^{(n-2t-2)/2}-v(c_2)\,q_1^{n-2t-3}-v(c_1)\,v(c_2)\,q_1^{(n-2t-4)/2}\right)\\
&\cdot(q_1-v(c_3))\cdots(q_1-v(c_{t+2}))\\
=&\sum_{c_1+c_2+\cdots+c_{t+2}=h}\left(q_1^{n-t-2}+v(c_1)\,q_1^{(n-2)/2}-v(c_2)\,q_1^{n-t-3}+\cdots+(-1)^{t+1}v(c_1)\,v(c_2)\cdots v(c_{t+2})\,q_1^{(n-2t-4)/2}\right)\\
=&q_1^{n-1}+q_1^{(n-2)/2}\sum_{c_1\in\mathbb{F}_{q^2}}v(c_1)+\cdots+(-1)^{t+1}\sum_{c_1+c_2+\cdots+c_{t+2}=h}v(c_1)\,v(c_2)\cdots v(c_{t+2})\,q_1^{(n-2t-4)/2}.
\end{aligned}\tag{2.2}$$

By Lamma 2.7 and (2.2), we have

$$N_{q^2}(g(Y)=h)=q_1^{n-1}+(-1)^{t+1}v(h)q_1^{(n-2)/2}=q^{2(n-1)}+(-1)^{t+1}v(h)q^{n-2}.$$

Next we give the second proof. Note that if f and g are equivalent, then for any $b\in\mathbb{F}_{q^2}$ the equation $f(x_1,\ldots,x_n)=b$ and $g(x_1,\ldots,x_n)=b$ have the same number of solutions in $\mathbb{F}_{q^2}$. So we can get the number of solutions of $g(Y)=h$ for $h\in\mathbb{F}_{q^2}$ by means of a nonsingular linear substitution of indeterminates.

Let $k(X)\in\mathbb{F}_{q^2}[x_1,x_2,x_3,x_4]$ and $k(X)=x_1x_2+x_1^2+Ax_2^2+x_3x_4+x_3^2+Bx_4^2$, where $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}(A)=\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}(B)=1$. We first show that $k(x)$ is equivalent to $x_1x_2+x_3x_4$.

Let $x_3=y_1+y_3$ and $x_i=y_i$ for $i\neq 3$, then $k(X)$ is equivalent to $y_1y_2+y_1y_4+y_3y_4+Ay_2^2+y_3^2+By_4^2$.

Let $y_2=z_2+z_4$ and $y_i=z_i$ for $i\neq 2$, then $k(X)$ is equivalent to $z_1z_2+z_3z_4+Az_2^2+z_3^2+Az_4^2+Bz_4^2$.

Let $z_1=\alpha_1+A\alpha_2$ and $z_i=\alpha_i$ for $i\neq 1$, then $k(X)$ is equivalent to $\alpha_1\alpha_2+\alpha_3^2+\alpha_3\alpha_4+(A+B)\alpha_4^2$.

Since $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}(A+B)=0$, we have $\alpha_3^2+\alpha_3\alpha_4+(A+B)\alpha_4^2$ is reducible by Lemma 2.9. Then $k(X)$ is equivalent to $x_1x_2+x_3x_4$. It follows that if t is odd, then $g(Y)$ is equivalent to $x_1x_2+x_3x_4+\cdots+x_{n-1}x_n$, and if t is even , then $g(Y)$ is equivalent to $x_1x_2+x_3x_4+\cdots+x_{n-1}x_n+x_{n-1}^2+ax_n^2$ with $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}(a)=1$. By Lemma 2.11, we get the desired result. □

3. Proof of Theorem 1.1

From (1.1), we know that the formula for the number of solutions of $f(X)=0$ over $\mathbb{F}_{q^2}$ is

$$N_{q^2}(f(X)=0)=q^{2(s-1)}+\sum_{j_1=1}^{d_1-1}\cdots\sum_{j_s=1}^{d_s-1}\overline{\psi_1^{j_1}}(a_1)\cdots\overline{\psi_s^{j_s}}(a_s)\,J_{q^2}^0\left(\psi_1^{j_1},\ldots,\psi_s^{j_s}\right),$$

where $d_i=(m_i,q^2-1)$ and ψ_i is a multiplicative character of $\mathbb{F}_{q^2}$ of order d_i. Since $m_i|q+1$, we have $d_i=m_i$. Let $H=\{(j_1,\ldots,j_s)\mid 1\le j_i<m_i,\ 1\le i\le s\}$. It follows that $\psi_1^{j_1}\cdots\psi_s^{j_s}$ is nontrivial for any $(j_1,\ldots,j_s)\in H$ as $(m_i,m_j)=1$. By Lemma 2.4, we have $J_{q^2}^0\left(\psi_1^{j_1},\ldots,\psi_s^{j_s}\right)=0$ and hence $N_{q^2}(f(X)=0)=q^{2(s-1)}$.

Let $N_{q^2}(f(X)=c)$ denote the number of solutions of the equation $f(X)=c$ over $\mathbb{F}_{q^2}$ with $c\in\mathbb{F}_{q^2}^*$. Let $V=\{(j_1,\ldots,j_s)|0\le j_i<m_i,\ 1\le i\le s\}$. Then

$$\begin{aligned}N_{q^2}(f(X)=c)&=\sum_{\gamma_1+\cdots+\gamma_s=c}N_{q^2}\left(a_1x_1^{m_1}=\gamma_1\right)\cdots N_{q^2}\left(a_sx_s^{m_s}=\gamma_s\right)\\&=\sum_{\gamma_1+\cdots+\gamma_s=c}\sum_{j_1=0}^{m_1-1}\psi_1^{j_1}\left(\frac{\gamma_1}{a_1}\right)\cdots\sum_{j_s=0}^{m_s-1}\psi_s^{j_s}\left(\frac{\gamma_s}{a_s}\right).\end{aligned}$$

Since ψ_i is a multiplicative character of $\mathbb{F}_{q^2}$ of order m_i, we have

$$\begin{aligned}N_{q^2}(f(X)=c)&=\sum_{\frac{\gamma_1}{c}+\cdots+\frac{\gamma_s}{c}=1}\sum_{(j_1,\ldots,j_s)\in V}\psi_1^{j_1}\left(\frac{\gamma_1}{c}\right)\psi_1^{j_1}\left(\frac{c}{a_1}\right)\cdots\psi_s^{j_s}\left(\frac{\gamma_s}{c}\right)\psi_s^{j_s}\left(\frac{c}{a_s}\right)\\&=\sum_{(j_1,\ldots,j_s)\in V}\psi_1^{j_1}\left(\frac{c}{a_1}\right)\cdots\psi_s^{j_s}\left(\frac{c}{a_s}\right)\sum_{\frac{\gamma_1}{c}+\cdots+\frac{\gamma_s}{c}=1}\psi_1^{j_1}\left(\frac{\gamma_1}{c}\right)\cdots\psi_s^{j_s}\left(\frac{\gamma_s}{c}\right)\\&=\sum_{(j_1,\ldots,j_s)\in V}\psi_1^{j_1}\left(\frac{c}{a_1}\right)\cdots\psi_s^{j_s}\left(\frac{c}{a_s}\right)J_{q^2}\left(\psi_1^{j_1},\ldots,\psi_s^{j_s}\right).\end{aligned}$$

By Lemma 2.3,

$$N_{q^2}(f(X)=c)=q^{2(s-1)}+\sum_{(j_1,\ldots,j_s)\in H}\psi_1^{j_1}\left(\frac{c}{a_1}\right)\cdots\psi_s^{j_s}\left(\frac{c}{a_s}\right)J_{q^2}\left(\psi_1^{j_1},\ldots,\psi_s^{j_s}\right).$$

By Lemma 2.5,

$$J_{q^2}\left(\psi_1^{j_1},\ldots,\psi_s^{j_s}\right)=\frac{G_{q^2}(\psi_1^{j_1})\cdots G_{q^2}(\psi_s^{j_s})}{G_{q^2}(\psi_1^{j_1}\cdots\psi_s^{j_s})}.$$

Since $m_i | q+1$ and $2 \nmid m_i$, by Lemma 2.6, we have

$$G_{q^2}(\psi_1^{j_1}) = \cdots = G_{q^2}(\psi_s^{j_s}) = G_{q^2}(\psi_1^{j_1} \cdots \psi_s^{j_s}) = q.$$

Then

$$\begin{aligned} & N_{q^2}(f(X)=c) \\ =& q^{2(s-1)} + q^{s-1} \sum_{j_1=1}^{m_1-1} \psi_1^{j_1}\left(\frac{c}{a_1}\right) \cdots \sum_{j_s=1}^{m_s-1} \psi_s^{j_s}\left(\frac{c}{a_s}\right) \\ =& q^{2(s-1)} + q^{s-1} \left(\sum_{j_1=0}^{m_1-1} \psi_1^{j_1}\left(\frac{c}{a_1}\right) - 1\right) \cdots \left(\sum_{j_s=0}^{m_s-1} \psi_s^{j_s}\left(\frac{c}{a_s}\right) - 1\right). \end{aligned}$$

It follows that

$$N_{q^2}(f(X)=c) = q^{2(s-1)} + q^{s-1} \prod_{i=1}^{s} \left(\left(\frac{c}{a_i}\right)_{m_i} m_i - 1\right), \tag{3.1}$$

where

$$\left(\frac{c}{a_i}\right)_{m_i} = \begin{cases} 1, & \text{if } \frac{c}{a_i} \text{ is a residue of order } m_i, \\ 0, & \text{otherwise.} \end{cases}$$

For a given $h \in \mathbb{F}_{q^2}$. We discuss the two cases according to whether h is zero or not.

Case 1: $h = 0$. If $f(X) = 0$, then $g(Y) = 0$; if $f(X) \neq 0$, then $g(Y) \neq 0$. Then

$$\begin{aligned} & N_{q^2}(l(X,Y)=0) \\ =& \sum_{c_1+c_2=0} N_{q^2}(f(X)=c_1)\, N_{q^2}(g(Y)=c_2) \\ =& q^{2(s-1)}\left(q^{2(n-1)} + (-1)^{t+1}(q^2-1)q^{n-2}\right) + \sum_{\substack{c_1+c_2=0 \\ c_1,c_2 \in \mathbb{F}_{q^2}^*}} N_{q^2}(f(X)=c_1)\, N_{q^2}(g(Y)=c_2). \end{aligned} \tag{3.2}$$

By Lemma 2.12, (3.1) and (3.2), we have

$$\begin{aligned} & N_{q^2}(l(X,Y)=0) \\ =& q^{2(s+n-2)} + (-1)^{t+1} q^{2(s-1)+h_n} - (-1)^{t+1} q^{2(s-2)+n} + \sum_{c_1 \in \mathbb{F}_{q^2}^*} \Bigg[q^{2(s+n-2)} - (-1)^{t+1} q^{2(s-2)+n} \\ & + \prod_{i=1}^{s}\left(\left(\frac{c_1}{a_i}\right)_{m_i} m_i - 1\right)\left(q^{2n+s-3} - (-1)^{t+1} q^{n+s-3}\right)\Bigg] \\ =& q^{2(s+n-2)} + (-1)^{t+1} q^{2(s-1)+n} - (-1)^{t+1} q^{2(s-2)+n} + q^{2(s+n-1)} - (-1)^{t+1} q^{2(s-1)+n} - q^{2(s+n-2)} \\ & + (-1)^{t+1} q^{2(s-2)+n} + \sum_{c_1 \in \mathbb{F}_{q^2}^*} \left[\prod_{i=1}^{s}\left(\left(\frac{c_1}{a_i}\right)_{m_i} m_i - 1\right)\left(q^{2n+s-3} - (-1)^{t+1} q^{n+s-3}\right)\right] \\ =& q^{2(s+n-1)} + \sum_{c_1 \in \mathbb{F}_{q^2}^*} \left[\prod_{i=1}^{s}\left(\left(\frac{c_1}{a_i}\right)_{m_i} m_i - 1\right)\left(q^{2n+s-3} - (-1)^{t+1} q^{n+s-3}\right)\right]. \end{aligned} \tag{3.3}$$

Case 2: $h \in \mathbb{F}_{q^2}^*$. If $f(X) = h$, then $g(Y) = 0$; if $f(X) = 0$, then $g(Y) = h$; if $f(X) \notin \{0, h\}$, then $g(Y) \notin \{0, h\}$. So we have

$$\begin{aligned}
&N_{q^2}(l(X,Y)) = h) \\
=&\sum_{c_1+c_2=h} N_{q^2}\left(f\left(X\right)=c_1\right) N_{q^2}\left(g\left(Y\right)=c_2\right) \\
=&N_{q^2}(f(X)=0)N_{q^2}(g(Y)=h) + N_{q^2}(f(X)=h)N_{q^2}(g(Y)=0) \\
&+\sum_{\substack{c_1+c_2=h \\ c_1,c_2\in\mathbb{F}_{q^2}^*\setminus\{h\}}} N_{q^2}\left(f\left(X\right)=c_1\right) N_{q^2}\left(g\left(Y\right)=c_2\right).
\end{aligned} \tag{3.4}$$

By Lemma 2.12, (3.1) and (3.4),

$$\begin{aligned}
&N_{q^2}(l(X,Y) = h) \\
=&2q^{2(s+n-2)} + (-1)^{t+1} q^{2s+n-2} - (-1)^{t+1} 2q^{2s+n-4} + \left(q^{s+2n-3} + (-1)^{t+1}\left(q^2-1\right)q^{s+n-3}\right)\prod_{i=1}^{s}\left(\left(\frac{h}{a_i}\right)_{m_i} m_i - 1\right) \\
&+\sum_{c_1\in\mathbb{F}_{q^2}^*\setminus\{h\}}\left[q^{2(s+n-2)} - (-1)^{t+1} q^{2s+n-4} + \prod_{i=1}^{s}\left(\left(\frac{c_1}{a_i}\right)_{m_i} m_i - 1\right)\left(q^{2n+s-3} - (-1)^{t+1} q^{n+s-3}\right)\right].
\end{aligned}$$

It follows that

$$\begin{aligned}
&N_{q^2}(l(X,Y) = h) \\
=&2q^{2(s+n-2)} + (-1)^{t+1} q^{2s+n-2} - (-1)^{t+1} 2q^{2s+n-4} + \left(q^{s+2n-3} + (-1)^{t+1}\left(q^2-1\right)q^{s+n-3}\right)\prod_{i=1}^{s}\left(\left(\frac{h}{a_i}\right)_{m_i} m_i - 1\right) \\
&+\sum_{c_1\in\mathbb{F}_{q^2}^*\setminus\{h\}}\left[q^{2(s+n-2)} - (-1)^{t+1} q^{2s+n-4} + \prod_{i=1}^{s}\left(\left(\frac{c_1}{a_i}\right)_{m_i} m_i - 1\right)(q^{2n+s-3} - (-1)^{t+1}q^{n+s-3})\right] \\
=&q^{2(s+n-1)} + \left(q^{s+2n-3} + (-1)^{t+1}\left(q^2-1\right)q^{s+n-3}\right)\prod_{i=1}^{s}\left(\left(\frac{h}{a_i}\right)_{m_i} m_i - 1\right) + \sum_{c_1\in\mathbb{F}_{q^2}^*\setminus\{h\}}\left[\prod_{i=1}^{s}\left(\left(\frac{c_1}{a_i}\right)_{m_i} m_i - 1\right)\right. \\
&\left.\cdot\,(q^{2n+s-3} + (-1)^t q^{n+s-3})\right].
\end{aligned} \tag{3.5}$$

By (3.3) and (3.5), we get the desired result. The proof of Theorem 1.1 is complete. □

4. Corollary and examples

There is a direct corollary of Theorem 1.1 and we omit its proof.

Corollary 4.1. *Under the conditions of Theorem 1.1, if* $a_1 = \cdots = a_s = h \in \mathbb{F}_{q^2}^*$*, then we have*

$$
\begin{aligned}
&N_{q^2}(l(X,Y)=h)\\
=&q^{2(s+n-1)}+\left(q^{s+2n-3}+(-1)^{t+1}\left(q^2-1\right)q^{s+n-3}\right)\prod_{i=1}^{s}(m_i-1)\\
&+\sum_{\gamma\in\mathbb{F}_{q^2}^{*}\setminus\{h\}}\left[\prod_{i=1}^{s}\left(\left(\frac{\gamma}{h}\right)_{m_i}m_i-1\right)\left(q^{2n+s-3}+(-1)^{t}q^{n+s-3}\right)\right],
\end{aligned}
$$

where

$$
\left(\frac{\gamma}{h}\right)_{m_i}=\begin{cases}1, & \text{if } \frac{\gamma}{h} \text{ is a residue of order } m_i,\\ 0, & \text{otherwise.}\end{cases}
$$

Finally, we give two examples to conclude the paper.

Example 4.2. *Let* $\mathbb{F}_{2^{10}}=\langle\alpha\rangle=\mathbb{F}_2[x]/(x^{10}+x^3+1)$ *where* α *is a root of* $x^{10}+x^3+1$. *Suppose* $l(X,Y)=\alpha^{33}x_1^3+x_2^{11}+y_3^2+\alpha^{10}y_4^2+y_1y_2+y_3y_4$. *Clearly,* $\mathrm{Tr}_{\mathbb{F}_{2^{10}}/\mathbb{F}_2}(\alpha^{10})=1$, $m_1=3$, $m_2=11$, $s=2$, $n=4$, $t=0$, $a_2=1$. *By Theorem 1.1, we have*

$$
N_{2^{10}}(l(X,Y)=0)=1024^5+(32^7+32^3)\times 20=1126587102265344.
$$

Example 4.3. *Let* $\mathbb{F}_{2^{12}}=\langle\beta\rangle=\mathbb{F}_2[x]/(x^{12}+x^6+x^4+x+1)$ *where* β *is a root of* $x^{12}+x^6+x^4+x+1$. *Suppose* $l(X,Y)=x_1^5+x_2^{13}+y_3^2+\beta^{10}y_4^2+y_1y_2+y_3y_4$. *Clearly,* $\mathrm{Tr}_{\mathbb{F}_{2^{12}}/\mathbb{F}_2}(\beta^{10})=1$, $m_1=5$, $m_2=13$, $s=2$, $n=4$, $t=0$, $a_1=a_2=1$. *By Corollary 4.1, we have*

$$
N_{2^{12}}(l(X,Y)=1)=2^{5\times 12}+(64^7-64^3\times 4095)\times 48=1153132559312355328.
$$

Acknowledgments

This work was jointly supported by the Natural Science Foundation of Fujian Province, China under Grant No. 2022J02046, Fujian Key Laboratory of Granular Computing and Applications (Minnan Normal University), Institute of Meteorological Big Data-Digital Fujian and Fujian Key Laboratory of Data Science and Statistics.

Conflict of interest

The authors declare there is no conflicts of interest.

References

1. L. K. Hua, H. S. Vandiver, Characters over certain types of rings with applications to the theory of equations in a finite field, *Proc. Natl. Acad. Sci. USA*, **35** (1949), 94–99. https://doi.org/10.1073/pnas.35.2.94
2. A. Weil, Numbers of solutions of equations in finite fields, *Bull. Amer. Math. Soc.*, **55** (1949), 497–508. https://doi.org/10.1090/S0002-9904-1949-09219-4
3. B. Berndt, R. Evans, K. Williams, *Gauss and Jacobi Sums*, Wiley-Interscience, New York, 1998.

4. W. Cao, Q. Sun, On a class of equations with special degrees over finite fields, *Acta Arith.*, **130** (2007), 195–202. https://doi.org/10.4064/aa130-2-8

5. S. N. Hu, X. E. Qin, J. Y. Zhao, Counting rational points of an algebraic variety over finite fields, *Results Math.*, **74** (2019), 37, 21 pp. https://doi.org/10.1007/s00025-019-0962-6

6. Q. Sun, D. Q. Wan, On the solvability of the equation $\sum_{i=1}^{n} \frac{x_i}{d_i} \equiv 0(\mathrm{mod} 1)$ and its application, *Proc. Amer. Math. Soc.*, **100** (1987), 220–224. https://doi.org/10.1090/S0002-9939-1987-0884454-6

7. Q. Sun, D. Q. Wan, On the Diophantine equation $\sum_{i=1}^{n} \frac{x_i}{d_i} \equiv 0(\mathrm{mod} 1)$, *Proc. Amer. Math. Soc.*, **112** (1991), 25–29. https://doi.org/10.1090/S0002-9939-1991-1047008-8

8. Q. Sun, P. Z. Yuan, On the number of solutions of diagonal equations over a finite field, *Finite Fields Appl.*, **2** (1996), 35–41. https://doi.org/10.1006/ffta.1996.0003

9. J. Wolfmann, The number of solutions of certain diagonal equations over finite fields, *J. Number Theory*, **42** (1992),247–257. https://doi.org/10.1016/0022-314X(92)90091-3

10. R. Lidl, H. Niederreiter, *Finite Fields*, 2nd Eds., Cambridge University Press, Cambridge, 1997. https://doi.org/10.1017/CBO9780511525926