Mathematics

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

AIMS Mathematics, 9(1): 2167–2180.
DOI: 10.3934/math.2024108
Received: 06 November 2023
Revised: 09 December 2023
Accepted: 12 December 2023
Published: 21 December 2023

Research article

Counting rational points of quartic diagonal hypersurfaces over finite fields

Shuangnian Hu[1], Yanyan Li[2] and Rongquan Feng[3,4*]

[1] School of Mathematics and Physics, Nanyang Institute of Technology, Nanyang 473004, China
[2] School of Information and Engineering, Nanyang Institute of Technology, Nanyang 473004, China
[3] School of Mathematics and Statistics, Hainan Normal University, Haikou 571158, China
[4] School of Mathematical Sciences, Peking University, Beijing 100871, China

* **Correspondence:** Email: fengrq@math.pku.edu.cn.

Abstract: Let $\mathbb{F}_q$ be the finite field of order q where $q = p^k$, k is a positive integer and p is an odd prime. Let $\mathbb{F}_q^*$ represent the nonzero elements of $\mathbb{F}_q$. For $f(x_1, \cdots, x_n) \in \mathbb{F}_q[x_1, \cdots, x_n]$, we used $N(f(x_1, \cdots, x_n) = 0)$ to denote the number of $\mathbb{F}_q$-rational points of the affine hypersurface $f(x_1, \cdots, x_n) = 0$. In 2020, Zhao et al. obtained the explicit formulae for $N(x_1^4 + x_2^4 = c)$, $N(x_1^4+x_2^4+x_3^4 = c)$ and $N(x_1^4+x_2^4+x_3^4+x_4^4 = c)$ over $\mathbb{F}_q$, with $c \in \mathbb{F}_q^*$. In this paper, by using Jacobi sums and an analog of the Hasse-Davenport theorem, we arrived at explicit formulae for $N(a_1x_1^4 + a_2x_2^4 = c)$ and $N(b_1x_1^4 + b_2x_2^4 + b_3x_3^4 = c)$ with $a_i, b_j \in \mathbb{F}_q^*(1 \le i \le 2, 1 \le j \le 3)$ and $c \in \mathbb{F}_q$. Furthermore, by using the reduction formula for Jacobi sums, the number of rational points of the quartic diagonal hypersurface $a_1x_1^4 + a_2x_2^4 + \cdots + a_nx_n^4 = c$ of $n \ge 4$ variables with $a_i \in \mathbb{F}_q^*$ $(1 \le i \le n)$, $c \in \mathbb{F}_q$ and $p \equiv 1 \pmod 4$, can also be deduced. These extended and improved earlier results.

Keywords: finite field; rational point; diagonal equation; Jacobi sum
Mathematics Subject Classification: 11T06, 11T24

1. Introduction and main results

Let $\mathbb{F}_q$ be the finite field of order q where $q = p^k$, k is a positive integer and p is an odd prime. Let $\mathbb{F}_q^*$ represent the nonzero elements of $\mathbb{F}_q$. For $f(x_1, \cdots, x_n) \in \mathbb{F}_q[x_1, \cdots, x_n]$, we use $N_q(f; n)$ to denote the number of $\mathbb{F}_q$-rational points of the affine hypersurface $f(x_1, \cdots, x_n) = 0$, namely,

$$N_q(f; n) = N(f(x_1, \cdots, x_n) = 0) = \#\{(x_1, \cdots, x_n) \in \mathbb{F}_q^n | f(x_1, \cdots, x_n) = 0\}.$$

To evaluate the values of $N_q(f; n)$ is a fundamental problem in algebra, number theory and arithmetic geometry. Generally speaking, it is difficult to give explicit formulae for $N_q(f; n)$. An explicit formula for $N_q(f;n)$ is known when $\deg(f) \leq 2$ (see [13]). Finding the explicit formula for $N_q(f;n)$ under certain conditions has attracted many researchers for many years (see, for instance, [2–11, 14–21]).

A special diagonal hypersurface over $\mathbb{F}_q$ is given by an equation of the type

$$a_1x_1^e + a_2x_2^e + \cdots + a_nx_n^e = c,$$

with e being a positive integer, coefficients $a_1, a_2, \cdots, a_n \in \mathbb{F}_q^*$ and $c \in \mathbb{F}_q$. It is clear that

$$N(a_1x_1 + a_2x_2 + \cdots + a_nx_n = c) = q^{n-1}.$$

For $e = 2$, there is an explicit formula for $N(a_1x_1^2 + \cdots + a_nx_n^2 = c)$ in [13]. When $q = p^{2t}$ with $p^r \equiv -1 (\mathrm{mod}\ e)$ for a divisor r of t and $e \mid (q-1)$, Wolfmann [17] gave an explicit formula of the number of rational points of the hypersurface

$$a_1x_1^e + a_2x_2^e + \cdots + a_nx_n^e = c$$

over $\mathbb{F}_q$ in 1992.

For the special case where $a_1 = a_2 = \cdots = a_n = 1$, we denote by

$$M_n^{(e)}(c) = N(x_1^e + x_2^e + \cdots + x_n^e = c).$$

In 1977, Chowla et al. [5] got the generating function $\sum_{n=1}^{\infty} M_n^{(3)}(0)x^n$ over $\mathbb{F}_p$ with $p \equiv 1(\mathrm{mod}\ 3)$. In 1979, Myerson [14] extended the result in [5] to the field $\mathbb{F}_q$, and also showed that the generating function $\sum_{n=1}^{\infty} M_n^{(4)}(0)x^n$ over $\mathbb{F}_q$ with $p \equiv 1(\mathrm{mod}\ 4)$ is a rational function in x.

In 2020, Zhao et al. [19, 20] investigated the number of rational points of the hypersurfaces

$$x_1^4 + x_2^4 = c, \quad x_1^4 + x_2^4 + x_3^4 = c \quad \text{and} \quad x_1^4 + x_2^4 + x_3^4 + x_4^4 = c$$

over $\mathbb{F}_q$, with $c \in \mathbb{F}_q^*$. For any $c \in \mathbb{F}_q$, in 2022, by using the cyclotomic theory and exponential sums, Zhao et al. [21] showed that the generating function $\sum_{n=1}^{\infty} M_n^{(4)}(c)x^n$ is a rational function in x.

In this paper, we consider the problem of finding the explicit formula for the number of rational points of the diagonal quartic hypersurface

$$f(x_1, x_2, \cdots, x_n) = a_1x_1^4 + a_2x_2^4 + \cdots + a_nx_n^4 - c = 0$$

over $\mathbb{F}_q$, where $q = p^k$, $a_1, a_2, \cdots, a_n \in \mathbb{F}_q^*$ and $c \in \mathbb{F}_q$.

If $p \equiv 3(\mathrm{mod}\ 4)$ and k is an odd integer, then $\gcd(4, q-1) = 2$. It follows that (see [12])

$$N(a_1x_1^4 + a_2x_2^4 + \cdots + a_nx_n^4 = c) = N(a_1x_1^2 + a_2x_2^2 + \cdots + a_nx_n^2 = c).$$

Throughout this paper, we let η be the quadratic multiplicative character of $\mathbb{F}_q$. Then from Theorems 6.26 and 6.27 in [13], the following result is deduced.

Theorem 1.1. *Let $q = p^k$ with $p \equiv 3(\mathrm{mod}\ 4)$ and k be an odd integer. Let $\psi(c) = -1$ for $c \in \mathbb{F}_q^*$ and $\psi(0) = q - 1$. Then the number of rational points of the hypersurface*

$$f(x_1, x_2, \cdots, x_n) = a_1x_1^4 + a_2x_2^4 + \cdots + a_nx_n^4 - c$$

over $\mathbb{F}_q$ *is*

$$q^{n-1} + \psi(c)q^{\frac{n-2}{2}}\eta\Big((-1)^{\frac{n}{2}}a_1a_2\cdots a_n\Big)$$

if n is even, and is

$$q^{n-1} + q^{\frac{n-1}{2}}\eta\Big((-1)^{\frac{n-1}{2}}ca_1a_2\cdots a_n\Big)$$

if n is odd.

If $p \equiv 3(\text{mod } 4)$ and k is an even integer, the following result can be derived from [17, Theorem 1].

Theorem 1.2. *Let* $p \equiv 3(\text{mod } 4)$ *be a prime, k an even integer,* $q = p^k$, $s = \frac{q-1}{4}$, $n \geq 2$ *and* $c \in \mathbb{F}_q$. *Let* α *be a primitive element of* $\mathbb{F}_q$. *Denote by N the number of rational points of the hypersurface*

$$a_1x_1^4 + a_2x_2^4 + \cdots + a_nx_n^4 = c$$

over $\mathbb{F}_q$, *then*

$$N = q^{n-1} + \frac{1}{4}(-1)^{kn/2}q^{n/2-1}(q-1)\sum_{j=0}^{3}(-3)^{v(j)}$$

if $c = 0$, *and*

$$N = q^{n-1} - (-1)^{k(n+1)/2}q^{n/2-1}\left[(-3)^{\theta(c)}q^{1/2} - \frac{1}{4}\left(q^{1/2} - (-1)^{k/2}\right)\sum_{j=0}^{3}(-3)^{\tau(j)}\right]$$

if $c \neq 0$, *where* $v(j)$ *is the number of i,* $1 \leq i \leq n$, *such that*

$$(\alpha^j)^s a_i^s = (-1)^{k(p+1)/8};$$

$\theta(c)$ *is the number of i,* $1 \leq i \leq n$, *such that* $a_i^s = (-c)^s$ *and* $\tau(j)$ *is the number of i,* $1 \leq i \leq n$, *such that* $a_i^s = (\alpha^j)^s$.

However, the explicit formula for $N(a_1x_1^4+a_2x_2^4+\cdots+a_nx_n^4 = c)$ is still unknown when $p \equiv 1(\text{mod } 4)$. In this paper, we solve this problem by using the Jacobi sums and an analog of the Hasse-Davenport theorem. We give an explicit formula for the number of rational points of diagonal quartic hypersurface

$$f_1(x_1, x_2) = a_1x_1^4 + a_2x_2^4 - c = 0 \tag{1.1}$$

and

$$f_2(x_1, x_2, x_3) = b_1x_1^4 + b_2x_2^4 + b_3x_3^4 - c = 0 \tag{1.2}$$

over $\mathbb{F}_q$, with $a_1, a_2, b_1, b_2, b_3 \in \mathbb{F}_q^*$, $c \in \mathbb{F}_q$ and the characteristic $p \equiv 1(\text{mod } 4)$. The case with arbitrary $n \geq 4$ variables can be deduced from the reduction formula for Jacobi sums, but we omit the tedious details here.

For a generator α of $\mathbb{F}_q^*$, we define the index of $\beta \in \mathbb{F}_q^*$ with respect to α, denoted by $\text{ind}_\alpha\beta$, to be the unique integer $r \in [1, q-1]$ such that $\beta = \alpha^r$ (see, for instance, [13]). For any nonzero integer n and prime number p, we define $\nu_p(n)$ as the greatest integer t such that p^t divides n. Then $\nu_p(n)$ is a nonnegative integer, and $\nu_p(n) \geq 1$ if and only if p divides n.

To give the main results, we need two concepts as follows.

Definition 1.1. *Let λ be a multiplicative character of $\mathbb{F}_q$. Associated to λ, we define the function S_λ over $\mathbb{F}_q^*$ as follows*

$$S_\lambda(\beta) := \lambda(\beta) + \lambda(\beta^3).$$

Clearly, if λ is the multiplicative character of order 4 of $\mathbb{F}_q$ with $\lambda(\alpha) = i = \sqrt{-1}$, then we have

$$S_\lambda(\beta) = \begin{cases} 2, & \text{if } \mathrm{ind}_\alpha\beta \equiv 0 (\mathrm{mod}\ 4), \\ 0, & \text{if } \mathrm{ind}_\alpha\beta \equiv 1 (\mathrm{mod}\ 4) \text{ or } \mathrm{ind}_\alpha\beta \equiv 3 (\mathrm{mod}\ 4), \\ -2, & \text{if } \mathrm{ind}_\alpha\beta \equiv 2 (\mathrm{mod}\ 4). \end{cases}$$

Definition 1.2. *Let $r,\ s$ and k be positive integers, and we define*

$$E(r,s,k) := r^k - \sum_{\substack{m=1 \\ v_2(m)=1}}^{k} \binom{k}{m} r^{k-m} s^m + \sum_{\substack{m=1 \\ v_2(m)\geq 2}}^{k} \binom{k}{m} r^{k-m} s^m$$

and

$$O(r,s,k) := \sum_{\substack{m=1 \\ v_2(m+1)=1}}^{k} \binom{k}{m} r^{k-m} s^m - \sum_{\substack{m=1 \\ v_2(m+1)\geq 2}}^{k} \binom{k}{m} r^{k-m} s^m.$$

Moreover, let α be a primitive element of $\mathbb{F}_q$ and $\beta \in \mathbb{F}_q^*$. Then associated to $r,\ s$ and k, we define

$$W_{(r,s,k)}(\beta) := \begin{cases} 2E(r,s,k), & \text{if } \mathrm{ind}_\alpha\beta \equiv 0 (\mathrm{mod}\ 4), \\ -2O(r,s,k), & \text{if } \mathrm{ind}_\alpha\beta \equiv 1 (\mathrm{mod}\ 4), \\ -2E(r,s,k), & \text{if } \mathrm{ind}_\alpha\beta \equiv 2 (\mathrm{mod}\ 4), \\ 2O(r,s,k), & \text{if } \mathrm{ind}_\alpha\beta \equiv 3 (\mathrm{mod}\ 4). \end{cases}$$

Now we can state the main results of this paper as follows.

Theorem 1.3. *Let k be a positive integer and $q = p^k$ with $p = 4t + 1$. Let α be a primitive element of $\mathbb{F}_q$, η be the quadratic multiplicative character of $\mathbb{F}_q$ and λ be a multiplicative character of order 4 of $\mathbb{F}_q$ such that $\lambda(\alpha) = i$. Let N_1 denote the number of rational points of the hypersurface over $\mathbb{F}_q$ defined by (1.1). Then*

$$N_1 = q + (q-1)\left((-1)^{tk} S_\lambda(a_1 a_2^3) + \eta(a_1 a_2)\right)$$

if $c = 0$, and

$$N_1 = q - (-1)^{tk} S_\lambda(a_1 a_2^3) - \eta(a_1 a_2) + (-1)^{k+1}\left((-1)^{kt} W_{(u,-v,k)}(\alpha_1) + \sum_{i=2}^{3} W_{(u,-v,k)}(\alpha_i)\right)$$

if $c \neq 0$, with $\alpha_1 = c^2 a_1 a_2$, $\alpha_2 = c a_1^2 a_2$, $\alpha_3 = c a_1 a_2^2$ and the integers u and v being defined uniquely by

$$u^2 + v^2 = p,\ u \equiv -\left(\frac{2}{p}\right) (\mathrm{mod}\ 4) \ \text{ and } \ v \equiv u\alpha^{(q-1)/4} (\mathrm{mod}\ p),$$

where $\left(\frac{2}{p}\right)$ is the Legendre symbol.

Theorem 1.4. *Let k be a positive integer and $q = p^k$ with $p = 4t + 1$. Let α be a primitive element of $\mathbb{F}_q^*$, η be the quadratic multiplicative character of $\mathbb{F}_q$ and λ be a multiplicative character of order 4 of $\mathbb{F}_q$ such that $\lambda(\alpha) = i$. Let N_2 denote the number of rational points of the hypersurface over $\mathbb{F}_q$ defined by (1.2). Then*

$$N_2 = q^2 - (q-1)(-1)^{(t+1)k} \sum_{i=1}^{3} W_{(u,-v,k)}(\beta_i)$$

if $c = 0$, and

$$\begin{aligned} N_2 =& q^2 + (-1)^{(t+1)k} \sum_{i=1}^{3} W_{(u,-v,k)}(\beta_i) + (-1)^{kt} W_{(u^2-v^2,-2uv,k)}(cb_1b_2b_3) \\ &+ q\left((-1)^{kt} \sum_{j=1}^{6} S_\lambda(\gamma_i) + \sum_{j=7}^{9} S_\lambda(\gamma_i) + \eta(cb_1b_2b_3)\right) \end{aligned}$$

if $c \neq 0$, with

$$\begin{aligned} &\beta_1 = b_1b_2b_3^2,\ \ \beta_2 = b_1b_2^2b_3,\ \ \beta_3 = b_1^2b_2b_3,\ \ \gamma_1 = cb_1^3b_2^3b_3, \\ &\gamma_2 = c^2b_1^3b_2^2b_3,\ \ \gamma_3 = cb_1^3b_2b_3^3,\ \ \gamma_4 = c^2b_1^3b_2b_3^2,\ \ \gamma_5 = c^3b_1^3b_2b_3, \\ &\gamma_6 = c^2b_1^2b_2^3b_3,\ \ \gamma_7 = cb_1^3b_2^2b_3^2,\ \ \gamma_8 = c^3b_1^2b_2b_3^2,\ \ \gamma_9 = cb_1^2b_2^2b_3^3 \end{aligned}$$

and the integers u and v being defined as in Theorem 1.3.

This paper is organized as follows. In Section 2, we recall some useful known lemmas that will be needed later. Subsequently, in Section 3, we prove Theorems 1.3 and 1.4. Finally, in Section 4, we supply two examples to illustrate the validity of our results.

2. Preliminary lemmas

In this section, we present some useful lemmas that are needed in the proof of Theorems 1.3 and 1.4.

Let $q = p^k$, where k is a positive integer and p is a prime. For any element $\beta \in E = \mathbb{F}_q$ and $F = \mathbb{F}_p$, the norm of β relative to $\mathbb{F}_p$ is defined by (see, for example, [1, 13])

$$\mathbb{N}_{E/F}(\beta) := \beta\beta^p \cdots \beta^{p^{k-1}} = \beta^{\frac{q-1}{p-1}}.$$

For the simplicity, we write $\mathbb{N}(\beta)$ for $\mathbb{N}_{E/F}(\beta)$. It is clear that if α is a primitive element of $\mathbb{F}_q$, then $\mathbb{N}(\alpha)$ is a primitive element of $\mathbb{F}_p$. Let χ be a multiplicative character of $\mathbb{F}_q$. For any $\alpha \in \mathbb{F}_q$, if $\chi(\alpha) = 1$, then we call the character χ is trivial. Let χ be a multiplicative character of $\mathbb{F}_p$. Then χ can be lifted to a multiplicative character λ of $\mathbb{F}_q$ by setting $\lambda(\beta) = \chi(\mathbb{N}(\beta))$. Any characters of $\mathbb{F}_p$ can be lifted to characters of $\mathbb{F}_q$, but not all the characters of $\mathbb{F}_q$ can be obtained by lifting a character of $\mathbb{F}_p$. The following lemma characterizes all the characters of $\mathbb{F}_q$ that can be obtained by lifting a character of $\mathbb{F}_p$.

Lemma 2.1. [1] *Let $\mathbb{F}_p$ be a finite field and $\mathbb{F}_q$ be an extension of $\mathbb{F}_p$. A multiplicative character λ of $\mathbb{F}_q$ can be lifted by a multiplicative character χ of $\mathbb{F}_p$ if and only if λ^{p-1} is trivial.*

Let $\lambda_1,\cdots,\lambda_n$ be n multiplicative characters of $\mathbb{F}_q$. The Jacobi sum $J(\lambda_1, \cdots, \lambda_n)$ is defined by

$$J(\lambda_1, \cdots, \lambda_n) := \sum_{\gamma_1+\cdots+\gamma_n=1} \lambda_1(\gamma_1)\cdots\lambda_n(\gamma_n),$$

where the summation is taken over all n-tuples $(\gamma_1, \cdots, \gamma_n)$ of elements of $\mathbb{F}_q$ with $\gamma_1 + \cdots + \gamma_n = 1$. It is clear that if σ is a permutation of $\{1, \cdots, n\}$, then

$$J(\lambda_{\sigma(1)}, \cdots, \lambda_{\sigma(n)}) = J(\lambda_1, \cdots, \lambda_n).$$

The readers are referred to [1, 13] for the basic facts on the Jacobi sum.

The following lemma is an analog of the Hasse-Davenport theorem which establishes an important relationship between the Jacobi sums in $\mathbb{F}_q$ and the Jacobi sums in $\mathbb{F}_p$.

Lemma 2.2. [13] *Let $\chi_1, \cdots, \chi_n$ be multiplicative characters of $\mathbb{F}_p$, not all of which are trivial. Suppose $\chi_1, \cdots, \chi_n$ are lifted to characters $\lambda_1, \cdots, \lambda_n$, respectively, of the extension field $\mathbb{F}_q$ of $\mathbb{F}_p$ with degree $[\mathbb{F}_q : \mathbb{F}_p] = k$. Then*

$$J(\lambda_1, \cdots, \lambda_n) = (-1)^{(n-1)(k-1)} J(\chi_1, \cdots, \chi_n)^k.$$

Lemma 2.3. (Reduction formula for the Jacobi sums) [1] *Let $\lambda_1, \cdots, \lambda_{s-1}, \lambda_s$ be s nontrivial multiplicative characters of $\mathbb{F}_q$. If $s \geq 2$, then*

$$J(\lambda_1, \cdots, \lambda_{s-1}, \lambda_s) = \begin{cases} -qJ(\lambda_1, \cdots, \lambda_{s-1}), & \text{if } \lambda_1, \cdots, \lambda_{s-1} \text{ is trivial,} \\ J(\lambda_1, \cdots, \lambda_{s-1}, \lambda_s)J(\lambda_1, \cdots, \lambda_{s-1}), & \text{if } \lambda_1, \cdots, \lambda_{s-1} \text{ is nontrivial.} \end{cases}$$

Lemma 2.4. [1] *Let $p \equiv 1 \pmod 4$ be a prime, q a power of p, α be a generator of $\mathbb{F}_q^*$, and let χ be a multiplicative character of order 4 of $\mathbb{F}_p$ with $\chi(\mathbb{N}(\alpha)) = i$. Then*

$$J(\chi, \chi^2) = u + iv,$$

where the integers u and v are uniquely determined by

$$u^2 + v^2 = p,\ u \equiv -\left(\frac{2}{p}\right) \pmod 4 \ \text{ and } \ v \equiv u\alpha^{(q-1)/4} \pmod p.$$

Lemma 2.5. [1] *Let $p = 4t + 1$ be a prime number. Let g be a primitive element of $\mathbb{F}_p$ and χ be a multiplicative character of order 4 over $\mathbb{F}_p$ such that $\chi(g) = i$. Let the integers u and v be defined as in Lemma 2.4. Then the values of the 16 Jacobi sums $J(\chi^m, \chi^n)$ $(m, n = 0, 1, 2, 3)$ of order 4 are given in Table 1.*

Table 1. The values of the Jacobi sums $J(\chi^m, \chi^n)$.

$m \setminus n$	0	1	2	3
0	p	0	0	0
1	0	$(-1)^t(u + vi)$	$u + vi$	$(-1)^{t+1}$
2	0	$u + vi$	-1	$u - vi$
3	0	$(-1)^{t+1}$	$u - vi$	$(-1)^t(u - vi)$

The following lemma gives a formula for the number of rational points of a diagonal hypersurface in terms of the Jacobi sums.

Lemma 2.6. [1] *Let $k_1, \cdots, k_n$ be positive integers. Let $a_1, \cdots, a_n \in \mathbb{F}_q^*$ and $c \in \mathbb{F}_q$. Set*

$$d_i = \gcd(k_i, q - 1),$$

and let λ_i be a multiplicative character of $\mathbb{F}_q$ of order d_i, for $i = 1, \cdots, n$. Then the number N of rational points of the equation

$$a_1x_1^{k_1} + \cdots + a_nx_n^{k_n} = c$$

over $\mathbb{F}_q$ is given by

$$N = q^{n-1} - (q-1) \sum_{\substack{j_1=1 \\ \lambda_1^{j_1}\cdots\lambda_n^{j_n}\ \text{trivial}}}^{d_1-1} \cdots \sum_{j_n=1}^{d_n-1} \lambda_1^{j_1}(a_1^{-1}) \cdots \lambda_n^{j_n}(a_n^{-1}) J(\lambda_1^{j_1}, \ldots, \lambda_n^{j_n})$$

if $c = 0$, and by

$$N = q^{n-1} + \sum_{j_1=1}^{d_1-1} \cdots \sum_{j_n=1}^{d_n-1} \lambda_1^{j_1}(ca_1^{-1}) \cdots \lambda_n^{j_n}(ca_n^{-1}) J(\lambda_1^{j_1}, \cdots, \lambda_n^{j_n})$$

if $c \neq 0$.

3. Proof of Theorems 1.3 and 1.4

In this section, we give the proofs of Theorems 1.3 and 1.4. First, we begin with a lemma.

Lemma 3.1. *Let α be a primitive element of $\mathbb{F}_q$ and λ be a multiplicative character of order 4 of $\mathbb{F}_q = \mathbb{F}_{p^k}$ such that $\lambda(\alpha) = i$. Then for any positive integers r, s and $\beta \in \mathbb{F}_q^*$, we have*

$$\lambda(\beta)(r+si)^k + \lambda(\beta^3)(r-si)^k = W_{(r,s,k)}(\beta),$$

where the function $W_{(r,s,k)}(\beta)$ is defined as in Definition 1.2.

Proof. If $\mathrm{ind}_\alpha\beta \equiv 0 \pmod 4$, then

$$\lambda(\beta) = \lambda(\beta^3) = 1.$$

Thus, one has

$$\begin{aligned}
\lambda(\beta)(r+si)^k + \lambda(\beta^3)(r-si)^k &= (r+si)^k + (r-si)^k \\
&= \sum_{m=0}^{k} \binom{k}{m} r^{k-m}[(si)^m + (-si)^m] \\
&= 2r^k + \sum_{\substack{m=1 \\ m \text{ is even}}}^{k} \binom{k}{m} r^{k-m}[(si)^m + (-si)^m] \\
&= 2r^k - 2\sum_{\substack{m=1 \\ v_2(m)=1}}^{k} \binom{k}{m} r^{k-m}s^m + 2\sum_{\substack{m=1 \\ v_2(m)\geq 2}}^{k} \binom{k}{m} r^{k-m}s^m \\
&= 2E(r,s,k).
\end{aligned}$$

If $\mathrm{ind}_\alpha\beta \equiv 1 \pmod 4$, then

$$\lambda(\beta) = i \text{ and } \lambda(\beta^3) = -i.$$

Thus, one has

$$\begin{aligned}\lambda(\beta)(r+si)^k+\lambda(\beta^3)(r-si)^k &= (r+si)^k i-(r-si)^k i\\ &= \sum_{m=0}^{k}\binom{k}{m}r^{k-m}[s^m i^{m+1}+s^m(-i)^{m+1}]\\ &= 2\sum_{\substack{m=1\\ m \text{ is odd}}}^{k}\binom{k}{m}r^{k-m}s^m i^{m+1}\\ &= -2\sum_{\substack{m=1\\ v_2(m+1)=1}}^{k}\binom{k}{m}r^{k-m}s^m+2\sum_{\substack{m=1\\ v_2(m+1)\geq 2}}^{k}\binom{k}{m}r^{k-m}s^m\\ &= -2O(r,s,k).\end{aligned}$$

If $\mathrm{ind}_\alpha\beta\equiv 2 \pmod 4$, then

$$\lambda(\beta)=\lambda(\beta^3)=-1,$$

and if $\mathrm{ind}_\alpha\beta\equiv 3 \pmod 4$, then

$$\lambda(\beta)=-i \text{ and } \lambda(\beta^3)=i.$$

The results in these two cases can be proved similarly. □

We can now give the proof of Theorem 1.3.

Proof of Theorem 1.3. Let α be a primitive element of $\mathbb{F}_q$ and λ be a multiplicative character of $\mathbb{F}_q$ of order 4 with $\lambda(\alpha)=i$. Since $q\equiv 1 \pmod 4$, then

$$\gcd(4,q-1)=4.$$

Using Lemma 2.6, by setting $\lambda_1=\lambda_2=\lambda$, one can deduce that the number N_1 of rational points

$$a_1x_1^4+a_2x_2^4=c$$

in $\mathbb{F}_q^2$ is given by

$$N_1=q-(q-1)\sum_{\substack{j_1=1\\ \lambda^{j_1}\lambda^{j_2}}}^{3}\sum_{\substack{j_2=1\\ \text{trivial}}}^{3}\lambda(a_1^{-j_1}a_2^{-j_2})J(\lambda^{j_1},\lambda^{j_2}) \tag{3.1}$$

if $c=0$, and by

$$N_1=q+\sum_{j_1=1}^{3}\sum_{j_2=1}^{3}\lambda(c^{j_1+j_2}a_1^{-j_1}a_2^{-j_2})J(\lambda^{j_1},\lambda^{j_2}) \tag{3.2}$$

if $c\neq 0$.

Since $p\equiv 1 \pmod 4$, it follows that λ^{p-1} is trivial. Thus, from Lemma 2.1, we know that the quartic multiplicative character λ can be lifted by a quartic multiplicative character χ of $\mathbb{F}_p$.

Using Lemmas 2.2, 2.5 and 3.1 and Definition 1.1, we have the following two cases, depending on $c=0$ or $c\neq 0$.

If $c = 0$, we derive that

$$\begin{aligned}
&\sum_{\substack{j_1=1\\ \lambda^{j_1}\lambda^{j_2}\,\text{trivial}}}^{3} \sum_{j_2=1}^{3} \lambda(a_1^{-j_1}a_2^{-j_2})J(\lambda^{j_1},\lambda^{j_2})\\
&= \lambda(a_1^3a_2)J(\lambda,\lambda^3) + \lambda(a_1^2a_2^2)J(\lambda^2,\lambda^2) + \lambda(a_1a_2^3)J(\lambda^3,\lambda)\\
&= (-1)^{k-1}\Big(\lambda(a_1^3a_2)J(\chi,\chi^3)^k + \lambda(a_1a_2^3)J(\chi^3,\chi)^k + \lambda(a_1^2a_2^2)J(\chi^2,\chi^2)^k\Big)\\
&= (-1)^{tk-1}\Big(\lambda(a_1^3a_2) + \lambda(a_1a_2^3)\Big) - \lambda(a_1^2a_2^2)\\
&= (-1)^{tk-1}S_\lambda(a_1^3a_2) - \eta(a_1a_2).
\end{aligned} \tag{3.3}$$

Thus, from (3.1) and (3.3), the first part of Theorem 1.3 follows immediately.

If $c \neq 0$, we obtain

$$\begin{aligned}
&\sum_{j_1=1}^{3}\sum_{j_2=1}^{3} \lambda(c^{j_1+j_2}a_1^{-j_1}a_2^{-j_2})J(\lambda^{j_1},\lambda^{j_2})\\
&= \lambda(a_1^3a_2)J(\lambda,\lambda^3) + \lambda(a_1^2a_2^2)J(\lambda^2,\lambda^2) + \lambda(a_1a_2^3)J(\lambda^3,\lambda)\\
&\quad + \lambda(c^2a_1^3a_2^3)J(\lambda,\lambda) + \lambda(c^2a_1a_2)J(\lambda^3,\lambda^3) + \lambda(c^3a_1^3a_2^2)J(\lambda,\lambda^2)\\
&\quad + \lambda(ca_1a_2^2)J(\lambda^3,\lambda^2) + \lambda(c^3a_1^2a_2^3)J(\lambda,\lambda^2) + \lambda(ca_1^2a_2)J(\lambda^2,\lambda^3)\\
&= (-1)^{tk-1}S_\lambda(a_1^3a_2) - \eta(a_1a_2) + (-1)^{k-1}\Big(\lambda(c^2a_1^3a_2^3)J(\chi,\chi)^k\\
&\quad + \lambda(c^2a_1a_2)J(\chi^3,\chi^3)^k + \lambda(c^3a_1^3a_2^2)J(\chi,\chi^2)^k + \lambda(ca_1a_2^2)J(\chi^3,\chi^2)^k\\
&\quad + \lambda(c^3a_1^2a_2^3)J(\chi,\chi^2)^k + \lambda(ca_1^2a_2)J(\chi^2,\chi^3)^k\Big)\\
&= (-1)^{tk-1}S_\lambda(a_1^3a_2) - \eta(a_1a_2) + (-1)^{k-1}\Big((-1)^{tk}(\lambda(c^2a_1^3a_2^3)(u+vi)^k\\
&\quad + \lambda(c^2a_1a_2)(u-vi)^k) + \lambda(c^3a_1^3a_2^2)(u+vi)^k + \lambda(ca_1a_2^2)(u-vi)^k\\
&\quad + \lambda(c^3a_1^2a_2^3)(u+vi)^k + \lambda(ca_1^2a_2)(u-vi)^k\Big)\\
&= (-1)^{tk-1}S_\lambda(a_1^3a_2) - \eta(a_1a_2) + (-1)^{k+1}\Big((-1)^{tk}W_{(u,-v,k)}(c^2a_1a_2)\\
&\quad + W_{(u,-v,k)}(ca_1a_2^2) + W_{(u,-v,k)}(ca_1^2a_2)\Big).
\end{aligned} \tag{3.4}$$

Thus, from (3.2) and (3.4), the desired result follows immediately. □

Now, we can turn our attention to prove Theorem 1.4.

Proof of Theorem 1.4. By the same argument as in the proof of Theorem 1.3, let α be a primitive element of $\mathbb{F}_q$ and λ be the multiplicative character of $\mathbb{F}_q$ of order 4 with $\lambda(\alpha) = i$. One has

$$N_2 = q^2 - (q-1)\sum_{j_1=1}^{3}\sum_{\substack{j_2=1\\ \lambda^{j_1}\lambda^{j_2}\lambda^{j_3}\ \text{trivial}}}^{3}\sum_{j_3=1}^{3} \lambda(b_1^{-j_1}b_2^{-j_2}b_3^{-j_3})J(\lambda^{j_1},\lambda^{j_2},\lambda^{j_3}) \tag{3.5}$$

if $c = 0$, and

$$N_2 = q^2 + \sum_{j_1=1}^{3}\sum_{j_2=1}^{3}\sum_{j_3=1}^{3} \lambda(c^{j_1+j_2+j_3}b_1^{-j_1}b_2^{-j_2}b_3^{-j_3})J(\lambda^{j_1},\lambda^{j_2},\lambda^{j_3}) \tag{3.6}$$

if $c \neq 0$.

Clearly, the quartic multiplicative character λ can be lifted by a quartic multiplicative character χ of $\mathbb{F}_p$. Thus, from Lemmas 2.2, 2.3, 2.5 and 3.1 and Definition 1.2, one gets that

$$\begin{aligned}
&\sum_{j_1=1}^{3}\ \sum_{\substack{j_2=1\\ \lambda^{j_1}\lambda^{j_2}\lambda^{j_3}\text{trivial}}}^{3}\ \sum_{j_3=1}^{3}\lambda(b_1^{-j_1}b_2^{-j_2}b_3^{-j_3})J(\lambda^{j_1},\lambda^{j_2},\lambda^{j_3})\\
&= \lambda(b_1^3b_2^3b_3^2)J(\chi^2,\chi^2)^kJ(\chi,\chi)^k + \lambda(b_1^3b_2^2b_3^3)J(\chi^3,\chi)^kJ(\chi,\chi^2)^k\\
&\quad + \lambda(b_1^2b_2^3b_3^3)J(\chi^3,\chi)^kJ(\chi,\chi^2)^k + \lambda(b_1^2b_2b_3)J(\chi,\chi^3)^kJ(\chi^2,\chi^3)^k\\
&\quad + \lambda(b_1b_2^2b_3)J(\chi,\chi^3)^kJ(\chi^2,\chi^3)^k + \lambda(b_1b_2b_3^2)J(\chi^2,\chi^2)^kJ(\chi^3,\chi^3)^k\\
&= (-1)^{(t+1)k}[\lambda(b_1^3b_2^3b_3^2)(u+vi)^k + \lambda(b_1b_2b_3^2)(u-vi)^k + \lambda(b_1^3b_2^2b_3^3)(u+vi)^k\\
&\quad + \lambda(b_1b_2^2b_3)(u-vi)^k + \lambda(b_1^2b_2^3b_3^3)(u+vi)^k + \lambda(b_1^2b_2b_3)(u-vi)^k]\\
&= (-1)^{(t+1)k}\Big(W_{(u,-v,k)}(b_1b_2b_3^2) + W_{(u,-v,k)}(b_1b_2^2b_3) + W_{(u,-v,k)}(b_1^2b_2b_3)\Big). \qquad (3.7)
\end{aligned}$$

Then, from (3.5) and (3.7), the first part of Theorem 1.4 follows immediately.

We can now turn our attention to prove the second part of Theorem 1.4. Clearly,

$$\begin{aligned}
&\sum_{j_1=1}^{3}\sum_{j_2=1}^{3}\sum_{j_3=1}^{3}\lambda(c^{j_1+j_2+j_3}b_1^{-j_1}b_2^{-j_2}b_3^{-j_3})J(\lambda^{j_1},\lambda^{j_2},\lambda^{j_3})\\
&= (-1)^{(t+1)k}\Big(W_{(u,-v,k)}(b_1b_2b_3^2) + W_{(u,-v,k)}(b_1b_2^2b_3) + W_{(u,-v,k)}(b_1^2b_2b_3)\Big)\\
&\quad + \lambda(c^3b_1^3b_2^3b_3^3)J(\chi^2,\chi)^kJ(\chi,\chi)^k + \lambda(cb_1b_2b_3)J(\chi^2,\chi^3)^kJ(\chi^3,\chi^3)^k\\
&\quad + (-1)^kqJ(\chi,\chi^3)^k[\lambda(cb_1^3b_2^3b_3) + \lambda(c^3b_1b_2b_3^3) + \lambda(c^2b_1^3b_2^2b_3) + \lambda(c^2b_1b_2^2b_3^3)\\
&\quad + \lambda(cb_1^3b_2b_3^3) + \lambda(c^3b_1b_2^3b_3) + \lambda(c^2b_1^3b_2b_3^2) + \lambda(c^2b_1b_2^3b_3^2)\\
&\quad + \lambda(c^3b_1^3b_2b_3) + \lambda(cb_1b_2^3b_3^3) + \lambda(c^2b_1^2b_2^3b_3) + \lambda(c^2b_1^2b_2b_3^3)]\\
&\quad + (-1)^kqJ(\chi^2,\chi^2)^k[\lambda(cb_1^3b_2^2b_3^2) + \lambda(c^3b_1b_2^2b_3^2) + \lambda(c^3b_1^2b_2b_3^2) + \lambda(cb_1^2b_2^3b_3^2)\\
&\quad + \lambda(cb_1^2b_2^2b_3^3) + \lambda(c^3b_1^2b_2^2b_3)] + (-1)^kqJ(\chi^2,\chi^2)^k\lambda(c^2b_1^2b_2^2b_3^2). \qquad (3.8)
\end{aligned}$$

By Lemmas 2.5 and 3.1 and Definition 1.2, we derive that

$$\begin{aligned}
&\lambda(c^3b_1^3b_2^3b_3^3)J(\chi^2,\chi)^kJ(\chi,\chi)^k + \lambda(cb_1b_2b_3)J(\chi^2,\chi^3)^kJ(\chi^3,\chi^3)^k\\
&= (-1)^{kt}[\lambda(c^3b_1^3b_2^3b_3^3)(u^2-v^2+2uvi)^k + \lambda(cb_1b_2b_3)(u^2-v^2-2uvi)^k]\\
&= (-1)^{kt}W_{(u^2-v^2,-2uv,k)}(cb_1b_2b_3). \qquad (3.9)
\end{aligned}$$

Using Lemma 2.5, one has

$$(-1)^kqJ(\chi,\chi^3)^k = (-1)^{tk}q \text{ and } (-1)^kqJ(\chi^2,\chi^2)^k = q. \qquad (3.10)$$

Thus, from (3.6), (3.8)–(3.10) and Definition 1.1, the desired result of the second part of Theorem 1.4 follows immediately. □

4. Examples

In this section, we present two examples to demonstrate the validity of Theorems 1.3 and 1.4. We have validated these two examples by using the Magma which is a powerful algebraic computation program package.

Example 4.1. Let $p = 5$ and $k = 5$. It can be checked easily that 2 is a primitive element of $\mathbb{F}_5$. Choose a primitive element ω of $\mathbb{F}_{5^5}$ with $\mathbb{N}(\omega) = 2$. We consider the numbers of rational points $(x_1, x_2) \in \mathbb{F}_{5^5}^2$ of the quartic hypersurfaces

$$x_1^4 + \omega^2 x_2^4 = 0 \text{ and } x_1^4 + \omega^2 x_2^4 = \omega$$

over $\mathbb{F}_{5^5}$.

Now, the Legendre symbol

$$\left(\frac{2}{5}\right) = -1 \text{ and } \omega^{\frac{5^5-1}{4}} = \mathbb{N}(\omega) = 2.$$

Thus, the integers u and v are determined by

$$u^2 + v^2 = 5,\ u \equiv 1 (\text{mod } 4) \text{ and } v \equiv 2u (\text{mod } 5).$$

Then, one has $u = 1,\ v = 2$. Thus, by Theorem 1.3, we obtain

$$N(x_1^4 + \omega^2 x_2^4 = 0) = 12497 \text{ and } N(x_1^4 + \omega^2 x_2^4 = \omega) = 3040.$$

Example 4.2. Let $p = 13$ and $k = 2$. We know that 2 is a primitive element of $\mathbb{F}_{13}$. Choose a primitive element ω of $\mathbb{F}_{13^2}$ with $\mathbb{N}(\omega) = 2$. We consider the numbers of rational points $(x_1, x_2, x_3) \in \mathbb{F}_{13^2}^3$ of the quartic hypersurfaces

$$x_1^4 + \omega x_2^4 + \omega^2 x_3^4 = 0 \text{ and } x_1^4 + \omega x_2^4 + \omega^2 x_3^4 = \omega$$

over $\mathbb{F}_{13^2}$.

Now, the Legendre symbol

$$\left(\frac{2}{13}\right) = -1 \text{ and } \omega^{\frac{13^2-1}{4}} = \mathbb{N}(\omega)^3 = 2^3.$$

Thus, the integers u and v are determined by

$$u^2 + v^2 = 13,\ u \equiv 1 (\text{mod } 4) \text{ and } v \equiv 2^3 u (\text{mod } 13).$$

Therefore,

$$u = -3,\ v = 2.$$

By Theorem 1.4, we have

$$N(x_1^4 + \omega x_2^4 + \omega^2 x_3^4 = 0) = 26881 \text{ and } N(x_1^4 + \omega x_2^4 + \omega^2 x_3^4 = \omega) = 28164.$$

5. Conlusions

Studying the number of rational points of the polynomial equation

$$f(x_1, x_2, \cdots, x_n) = 0$$

over $\mathbb{F}_q$ is a fundamental problem in algebra, number theory and arithmetic geometry. Generally speaking, it is difficult to give an explicit formula for the number of solutions of the equation

$$f(x_1, x_2, \cdots, x_n) = 0.$$

There are many researchers who concentrated on finding the formula for the number of solutions of

$$f(x_1, x_2, \cdots, x_n) = 0$$

under certain conditions. Exponential sums are important tools for solving problems involving the number of solutions of the equation

$$f(x_1, x_2, \cdots, x_n) = 0$$

over $\mathbb{F}_q$. In this paper, by using the Jacobi sums and an analog of the Hasse-Davenport theorem, we arrived at explicit formulae for

$$N(a_1x_1^4 + a_2x_2^4 = c)$$

and

$$N(b_1x_1^4 + b_2x_2^4 + b_3x_3^4 = c),$$

with

$$a_i, b_j \in \mathbb{F}_q^*(1 \le i \le 2, 1 \le j \le 3)$$

and $c \in \mathbb{F}_q$. Furthermore, by using the reduction formula for Jacobi sums, the number of rational points of the quartic diagonal hypersurface

$$a_1x_1^4 + a_2x_2^4 + \cdots + a_nx_n^4 = c$$

of $n \ge 4$ variables with

$$a_i \in \mathbb{F}_q^*(1 \le i \le n),\ c \in \mathbb{F}_q$$

and $p \equiv 1 (\mathrm{mod}\ 4)$, can also be deduced.

Use of AI tools declaration

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

Acknowledgments

This research was supported by the National Science Foundation of China (Nos. 12026223, 12026224 and 12231015), the National Key Research and Development Program of China (No. 2018YFA0704703), the Natural Science Foundation of Beijing (No. M23017), the Natural Science Foundation of Henan Province (No. 232300420123) and the Research Center of Mathematics and Applied Mathematics, Nanyang Institute of Technology.

Conflict of interest

We declare that we have no conflicts of interest.

References

1. B. C. Berndt, R. J. Evans, K. S. Williams, *Gauss and Jacobi sums*, Wiley, 1998.
2. W. Cao, On generalized Markoff-Hurwitz-type equations over finite fields, *Acta Appl. Math.*, **112** (2010), 275–281. http://doi.org/10.1007/s10440-010-9568-4
3. W. Cao, Q. Sun, On a class of equations with special degrees over finite fields, *Acta Arith.*, **130** (2007), 195–202. http://doi.org/10.4064/aa130-2-8
4. L. Carlitz, Pairs of quadratic equations in a finite field, *Amer. J. Math.*, **76** (1954), 137–154. https://doi.org/10.2307/2372405
5. S. Chowla, J. Cowles, M. Cowles, On the number of zeros of diagonal cubic forms, *J. Number Theory*, **9** (1977), 502–506. http://doi.org/10.1016/0022-314X(77)90010-5
6. S. Hong, C. Zhu, On the number of zeros of diagonal cubic forms over finite fields, *Forum Math.*, **33** (2021), 697–708. http://doi.org/10.1515/forum-2020-0354
7. S. Hu, S. Hong, W. Zhao, The number of rational points of a family of hypersurfaces over finite fields, *J. Number Theory*, **156** (2015), 135–153. http://doi.org/10.1016/j.jnt.2015.04.006
8. S. Hu, X. Qin, J. Zhao, Counting rational points of an algebraic variety over finite fields, *Results Math.*, **74** (2019), 37. https://doi.org/10.1007/s00025-019-0962-6
9. S. Hu, J. Zhao, The number of rational points of a family of algebraic varieties over finite fields, *Algebra Colloq.*, **24** (2017), 705–720. http://doi.org/10.1142/S1005386717000475
10. H. Huang, W. Gao, W. Cao, Remarks on the number of rational points on a class of hypersurfaces over finite fields, *Algebra Colloq.*, **25** (2018), 533–540. https://doi.org/10.1142/S1005386718000366
11. L. K. Hua, H. S. Vandiver, On the number of solutions of some trinomial equations in a finite field, *Proc. Natl. Acad. Sci.*, **35** (1949), 477–481. http://doi.org/10.1073/pnas.35.8.477
12. K. Ireland, M. Rosen, *A classical introduction to modern number theory*, 2 Eds., Springer-Verlag, 1990.
13. R. Lidl, H. Niederreiter, *Finite fields*, 2 Eds., Cambridge University Press, 1996. http://doi.org/10.1017/CBO9780511525926
14. G. Myerson, On the number of zeros of diagonal cubic forms, *J. Number Theory*, **11** (1979), 95–99. http://doi.org/10.1016/0022-314X(79)90023-4
15. D. Wan, J. Zhang, Complete symmetric polynomials over finite fields have many rational zeros, *Sci. Sin. Math.*, **51** (2021), 1677–1684. http://doi.org/10.1360/ssm-2020-0328
16. A. Weil, Number of solutions of equations in finite field, *Bull. Amer. Math. Soc.*, **55** (1949), 497–508. http://doi.org/10.1090/S0002-9904-1949-09219-4
17. J. Wolfmann, The number of solutions of certain diagonal equations over finite fields, *J. Number Theory*, **42** (1992), 247–257. http://doi.org/10.1016/0022-314x(92)90091-3

18. J. Zhang, D. Wan, Rational points on complete symmetric hypersurfaces over finite fields, *Discrete Math.*, **11** (2020), 112072. http://doi.org/10.1016/j.disc.2020.112072

19. J. Zhao, S. Hong, C. Zhu, The number of rational points of certain quartic diagonal hypersurfaces over finite fields, *AIMS Math.*, **5** (2020), 2710–2731. http://doi.org/10.3934/math.2020175

20. J. Zhao, Y. Zhao, Y. Niu, On the number of solutions of two-variable diagonal quartic equations over finite fields, *AIMS Math.*, **5** (2020), 2979–2991. http://doi.org/10.3934/math.2020192

21. J. Zhao, Y. Feng, S. Hong, C. Zhu, On the number of zeros of diagonal quartic forms over finite fields, *Forum Math.*, **34** (2022), 385–405. http://doi.org/10.1515/forum-2021-0196