Research article

The number of solutions of cubic diagonal equations over finite fields

Shuangnian Hu and Rongquan Feng

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

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

Abstract: Let \( p \) be a prime, \( k \) be a positive integer, \( q = p^k \), and \( \mathbb{F}_q \) be the finite field with \( q \) elements. Let \( \mathbb{F}_q^* \) be the multiplicative group of \( \mathbb{F}_q \), that is \( \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\} \). In this paper, explicit formulae for the numbers of solutions of cubic diagonal equations \( a_1x_1^3 + a_2x_2^3 = c \) and \( b_1x_1^3 + b_2x_2^3 + b_3x_3^3 = c \) over \( \mathbb{F}_q \) are given, with \( a_i, b_j \in \mathbb{F}_q^* \) (\( 1 \leq i \leq 2, 1 \leq j \leq 3 \)), \( c \in \mathbb{F}_q \) and \( p \equiv 1(\text{mod } 3) \). Furthermore, by using the reduction formula for Jacobi sums, the number of solutions of the cubic diagonal equations \( a_1x_1^3 + a_2x_2^3 + \cdots + a_sx_s^3 = c \) of \( s \geq 4 \) variables with \( a_i \in \mathbb{F}_q^* \) (\( 1 \leq i \leq s \)), \( c \in \mathbb{F}_q \) and \( p \equiv 1(\text{mod } 3) \), can also be deduced.

Keywords: finite fields; rational points; diagonal equations; Jacobi sums

Mathematics Subject Classification: 11T06, 11T24

1. Introduction and statement of main result

Let \( p \) be a prime, \( k \) be a positive integer, \( q = p^k \). Let \( \mathbb{F}_q \) be the finite field with \( q \) elements and \( \mathbb{F}_q^* \) represent the nonzero elements of \( \mathbb{F}_q \). Let \( f(x_1, \cdots, x_s) \in \mathbb{F}_q[x_1, \cdots, x_s] \) be a polynomial over \( \mathbb{F}_q \) with \( s \) variables. A solution (or a rational point) of \( f(x_1, \cdots, x_s) \) over \( \mathbb{F}_q \) is an \( s \)-tuple \( (c_1, \cdots, c_s) \in \mathbb{F}_q^s \) such that \( f(c_1, \cdots, c_s) = 0 \). Denote by

\[
N(f, q) = N(f(x_1, \cdots, x_s) = 0) = \# \{(c_1, \cdots, c_s) \in \mathbb{F}_q^s \mid f(c_1, \cdots, c_s) = 0\}
\]

the number of solutions of \( f(x_1, \cdots, x_s) = 0 \) over \( \mathbb{F}_q \).

It is one of the central problems to study the number \( N(f, q) \) of rational points over finite fields. From [14, 15] we know that there exists an explicit formula for \( N(f, q) \) with degree \( \deg(f) \leq 2 \). But generally speaking, it is much difficult to give an explicit formula for \( N(f, q) \). Finding the explicit formula for \( N(f, q) \) under certain conditions has attracted many researchers for many years (See, for instance, [1, 3–13, 16–18, 20–27]).
Let $k_1, \ldots, k_s$ be positive integers. A diagonal equation is an equation of the form

$$a_1x_1^{k_1} + \cdots + a_sx_s^{k_s} = c$$

with coefficients $a_1, \ldots, a_s \in \mathbb{F}_p$ and $c \in \mathbb{F}_q$. The special case where all the $k_i$’s are equal has extensively been studied (see, for example, [7–12, 17, 18, 21–23, 26, 27]).

In 1977, S. Chowla et al. ([7]) investigated a problem about the number of solutions of an equation

$$x_1^3 + x_2^3 + \cdots + x_s^3 = 0$$

over field $\mathbb{F}_p$, where $p$ is a prime with $p \equiv 1(\text{mod } 3)$. In 1979, Myerson [17] extended the result in [7] to the field $\mathbb{F}_q$ and also studied the number of solutions of the equation

$$x_1^4 + x_2^4 + \cdots + x_s^4 = 0$$

over $\mathbb{F}_q$. When $q = p^{2r}$ with $p' \equiv -1(\text{mod } d)$ for a divisor $r$ of $t$ and $d \mid (q-1)$, Wolfmann [22] gave an explicit formula of the number of solutions of the equation

$$a_1x_1^d + a_2x_2^d + \cdots + a_sx_s^d = c$$

over $\mathbb{F}_q$ in 1992, where $a_1, a_2, \ldots, a_s \in \mathbb{F}_q^*$ and $c \in \mathbb{F}_q$. In 2018, Zhang and Hu [23] determined the number of solutions of the equation

$$x_1^3 + x_2^3 + x_3^3 + x_4^3 = c$$

over $\mathbb{F}_p$, with $c \in \mathbb{F}_p^*$ and $p \equiv 1(\text{mod } 3)$.

In 2020, J. Zhao et al. [26, 27] investigated the number of solutions of the equations

$$x_1^3 + x_2^3 = c, \quad x_1^4 + x_2^4 + x_3^3 = c$$

and

$$x_1^4 + x_2^4 + x_3^4 + x_4^4 = c$$

over $\mathbb{F}_q$, with $c \in \mathbb{F}_q^*$.

For any $c \in \mathbb{F}_q$, let $A_n(c)$ and $B_n(c)$ denote the number of solutions of the equations $x_1^3 + x_2^3 + \cdots + x_n^3 = c$ and $x_1^4 + x_2^4 + \cdots + x_n^4 + cx_{n+1}^3 = 0$ over $\mathbb{F}_q$ respectively. In 2021, by using the generator of $\mathbb{F}_q^*$, Hong and Zhu [10] gave the generating functions $\sum_{n=1}^{\infty} A_n(c)x^n$ and $\sum_{n=1}^{\infty} B_n(c)x^n$. In 2022, W. Ge et al. [9] studied these two generating functions in a different way. Moreover, formulas of the number of solutions of equation $a_1x_1^3 + a_2x_2^3 = c$ and $a_1x_1^4 + a_2x_2^4 + a_3x_3^3 = 0$ were also presented in [9].

In this paper, we consider the problem of finding the number of solutions of the diagonal cubic equation

$$f(x_1, x_2, \ldots, x_s) = a_1x_1^3 + a_2x_2^3 + \cdots + a_sx_s^3 - c = 0$$

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

If $p = 3$ and $k$ is an integer, or $p \equiv 2(\text{mod } 3)$ and $k$ is an odd integer, then $\gcd(3, q-1) = 1$. It follows that (see [14] pp.105)

$$N(a_1x_1^3 + a_2x_2^3 + \cdots + a_sx_s^3 = c) = \frac{q^r - 1}{2}$$

$$N(a_1x_1 + a_2x_2 + \cdots + a_sx_s = c) = \frac{q^r - 1}{2}$$
with $a_1, a_2, \ldots, a_s \in \mathbb{F}_q^*$, and $c \in \mathbb{F}_q$.

If $p \equiv 2 \pmod{3}$ and $k$ is an even integer, Hua and Vandiver [13] studied the number of solutions of some trinomial equations over $\mathbb{F}_q$ and Wolfmann [22] also got the number of solutions of certain diagonal equations over $\mathbb{F}_q$. The following result can be deduced from Theorem 1 of [22].

**Theorem 1.1.** Let $p \equiv 2 \pmod{3}$ be a prime, $k$ an even integer, $q = p^k$, $n = \frac{q-1}{3}$, $s \geq 2$ and $c \in \mathbb{F}_q$. Let $\alpha$ be a primitive element of $\mathbb{F}_q$. Denote by $N$ the number of solutions of the equation

$$a_1x_1^3 + a_2x_2^3 + \cdots + a_sx_s^3 = c$$

over $\mathbb{F}_q$. Then

$$N = q^{s-1} + \frac{1}{3}(-1)^{ks/2}q^{s/2-1}(q-1)\sum_{j=0}^{2}(-2)^{\nu(j)}$$

if $c = 0$, and

$$N = q^{s-1} - (-1)^{ks/2+1}q^{s/2-1}\left((-2)^{\nu(j)}q^{1/2} - \frac{1}{3}q^{1/2}(-1)^{k/2}\sum_{j=0}^{2}(-2)^{\nu(j)}\right)$$

if $c \neq 0$, where $\nu(j)$ is the number of $i, 1 \leq i \leq s$, such that $(\alpha^l)^n \equiv (-1)^{l+1}/6; \theta(c)$ is the number of $i, 1 \leq i \leq s$, such that $a_{i}^n = (-c)^n$ and $\tau(j)$ is the number of $i, 1 \leq i \leq s$, such that $a_{i}^n = (\alpha^l)^n$.

However, the explicit formula for $N(a_1x_1^3 + a_2x_2^3 + \cdots + a_sx_s^3 = c)$ is still unknown when $p \equiv 1 \pmod{3}$.

In this paper, we solve this problem by using Jacobi sums and an analog of Hasse-Davenport theorem. We give an explicit formula for the number of solutions of diagonal cubic equations

$$f_1(x_1, x_2) = a_1x_1^3 + a_2x_2^3 - c = 0$$

and

$$f_2(x_1, x_2, x_3) = b_1x_1^3 + b_2x_2^3 + b_3x_3^3 - c = 0$$

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 $p \equiv 1 \pmod{3}$. Note that our approach, which applies Jacobi sums, is not the same as that of Ge et al. [9] and Hong and Zhu [10] which mainly applies Gauss sums. The case with arbitrary $s \geq 4$ variables can be deduced from the reduction formula for Jacobi sums. But we omit the tedious details here.

Let $\alpha \in \mathbb{F}_q^*$ be a fixed primitive element of $\mathbb{F}_q$. For any $\beta \in \mathbb{F}_q^*$, there exists exactly one integer $r \in [1, q - 1]$ such that $\beta = \alpha^r$. Such an integer $r$ is called the index of $\beta$ with the primitive element $\alpha$, and denoted by $\text{ind}_\alpha \beta := r$. For any nonzero integer $m$ and prime number $p$, we define $v_p(m)$ as the greatest integer $t$ such that $p^t$ divides $m$. Then $v_p(m)$ is a nonnegative integer, and $v_p(m) \geq 1$ if and only if $p$ divides $m$.

The results of this paper are stated as follows.

**Theorem 1.2.** Let $k$ be a positive integer and $q = p^k$ with the prime $p \equiv 1 \pmod{3}$. Let $\alpha$ be a primitive element of $\mathbb{F}_q$. Denote by $N_1$ the number of solutions of the equation $a_1x_1^3 + a_2x_2^3 = c$ over $\mathbb{F}_q$. Then

$$N_1 = q - (q - 1)\delta(a_1, a_2)$$
if $c = 0$, and

$$N_1 = \begin{cases} 
q + \frac{(-1)^{\frac{j}{2}}}{2^c} E(u, v, k) + \delta(a_1, a_2), & \text{if } \text{ind}_c ca_1a_2 \equiv 0(\text{mod } 3), \\
q + \frac{(-1)^{\frac{j}{2}}}{2^c} (E(u, v, k) - O(u, v, k)) + \delta(a_1, a_2), & \text{if } \text{ind}_c ca_1a_2 \equiv 1(\text{mod } 3), \\
q + \frac{(-1)^{\frac{j}{2}}}{2^c} (E(u, v, k) + O(u, v, k)) + \delta(a_1, a_2), & \text{if } \text{ind}_c ca_1a_2 \equiv 2(\text{mod } 3)
\end{cases}$$

if $c \neq 0$, where

$$\delta(a_1, a_2) = \begin{cases} 
-2, & \text{if } \text{ind}_c a_1a_2^2 \equiv 0(\text{mod } 3), \\
1, & \text{if } \text{ind}_c a_1a_2^2 \equiv 0(\text{mod } 3),
\end{cases}$$

$$E(u, v, k) := u^k - \sum_{v_2^{(k)} = 1}^k \left( \begin{array}{c} k \\ l \end{array} \right) u^{k-l} v^{3^l}, \quad \sum_{v_2^{(k)} = 2}^k \left( \begin{array}{c} k \\ l \end{array} \right) u^{k-l} v^{3^l},$$

$$O(u, v, k) := \sum_{v_2^{(k)} = 1}^k \left( \begin{array}{c} k \\ l \end{array} \right) u^{k-l} v^{3^{\frac{l+1}{2}}}, - \sum_{v_2^{(k)} = 2}^k \left( \begin{array}{c} k \\ l \end{array} \right) u^{k-l} v^{3^{\frac{2l+1}{2}}}$$

and the integers $u$ and $v$ are uniquely determined such that

$$u^2 + 3v^2 = 4p, \quad u \equiv 1(\text{mod } 3), \quad v \equiv 0(\text{mod } 3) \quad \text{and } 3v \equiv u(2\alpha^{(q-1)/3} + 1)(\text{mod } p)$$

**Theorem 1.3.** Let $k$ be a positive integer and $q = p^k$ with the prime $p \equiv 1(\text{mod } 3)$. Let $\alpha$ be a primitive element of $\mathbb{F}_q$. Denote by $N_2$ the number of solutions of the equation $b_1x_1^2 + b_2x_2^2 + b_3x_3^2 = c$ over $\mathbb{F}_q$. Then

$$N_2 = \begin{cases} 
q^2 - (q - 1) \frac{(-1)^{\frac{j}{2}}}{2^c} E(u, v, k), & \text{if } \text{ind}_c b_1b_2b_3 \equiv 0(\text{mod } 3), \\
q^2 - (q - 1) \frac{(-1)^{\frac{j+1}{2}}}{2^c} (E(u, v, k) - O(u, v, k)), & \text{if } \text{ind}_c b_1b_2b_3 \equiv 1(\text{mod } 3), \\
q^2 - (q - 1) \frac{(-1)^{\frac{j+1}{2}}}{2^c} (E(u, v, k) + O(u, v, k)), & \text{if } \text{ind}_c b_1b_2b_3 \equiv 2(\text{mod } 3)
\end{cases}$$

if $c = 0$, and

$$N_2 = \begin{cases} 
q^2 + \frac{(-1)^{\frac{j}{2}}}{2^c} E(u, v, k) + S(c, b_1, b_2, b_3), & \text{if } \text{ind}_c b_1b_2b_3 \equiv 0(\text{mod } 3), \\
q^2 + \frac{(-1)^{\frac{j+1}{2}}}{2^c} (E(u, v, k) - O(u, v, k)) + S(c, b_1, b_2, b_3), & \text{if } \text{ind}_c b_1b_2b_3 \equiv 1(\text{mod } 3), \\
q^2 + \frac{(-1)^{\frac{j+1}{2}}}{2^c} (E(u, v, k) + O(u, v, k)) + S(c, b_1, b_2, b_3), & \text{if } \text{ind}_c b_1b_2b_3 \equiv 2(\text{mod } 3)
\end{cases}$$

if $c \neq 0$, where $E(u, v, k), O(u, v, k), u, v$ are defined as in Theorem 1.2 and

$$S(c, b_1, b_2, b_3) := \delta(c, b_1, b_2, b_3) + q(\omega(c, b_1, b_2, b_3) + \omega'(c, b_1, b_2, b_3)),$$

with

$$\delta(c, b_1, b_2, b_3) := \begin{cases} 
2q, & \text{if } \text{ind}_c cb_1^2b_2^2b_3 \equiv 0(\text{mod } 3), \\
-q, & \text{if } \text{ind}_c cb_1^2b_2^2b_3 \equiv 0(\text{mod } 3),
\end{cases}$$

$$\omega(c, b_1, b_2, b_3) := \begin{cases} 
2, & \text{if } \text{ind}_c cb_1^2b_2^2b_3 \equiv 0(\text{mod } 3), \\
-1, & \text{if } \text{ind}_c cb_1^2b_2^2b_3 \equiv 0(\text{mod } 3),
\end{cases}$$
and
\[ \omega'(c, b_1, b_2, b_3) := \begin{cases} 2, & \text{if } \text{ind}_a c^2 b_1^2 b_2 b_3 \equiv 0 \pmod{3}, \\ -1, & \text{if } \text{ind}_a c^2 b_1^2 b_2 b_3 \not\equiv 0 \pmod{3}. \end{cases} \]

**Corollary 1.4.** Let \( k \) be a positive integer and \( q = p^k \) with the prime \( p \equiv 1 \pmod{3} \). Let \( \alpha \) be a primitive element of \( \mathbb{F}_q \). Denote by \( N_3 \) (resp. \( N_4 \)) the number of solutions of the equation \( x_1^3 + x_2^3 = 0 \) (resp. \( x_1^3 + x_2^3 + x_3^3 = 0 \)) over \( \mathbb{F}_q \). Then
\[ N_3 = 3q - 2 \]
and
\[ N_4 = q^2 + u(q - 1), \]
where the integer \( u \) is uniquely determined such that
\[ u^2 + 3v^2 = 4p, \ u \equiv 1 \pmod{3}, \ v \equiv 0 \pmod{3} \text{ and } 3v \equiv u(2^q(q-1)/3 + 1) \pmod{p}. \]

Corollary 1.4 is a special case of [17]. If \( k = 1 \), then Corollary 1.4 is a special case of [7].

This paper is organized as follows. In Section 2, we present several basic concepts including the Jacobi sums, and give some preliminary lemmas. In Section 3, we prove Theorems 1.2 and 1.3 and finally, in Section 4, we supply some examples to illustrate the validity of our results.

2. Preliminary lemmas

In this section, we present some auxiliary lemmas that are needed in the proof of Theorems 1.2 and 1.3.

If \( \lambda \) is a multiplicative character of \( \mathbb{F}_q \), then \( \lambda \) is defined for all nonzero elements of \( \mathbb{F}_q \). It is now convenient to extend the definition of \( \lambda \) by setting \( \lambda(0) = 1 \) if \( \lambda \) is the trivial character and \( \lambda(0) = 0 \) otherwise.

For any element \( \alpha \in \mathbb{F}_q = \mathbb{F}_p^k \), the norm of \( \alpha \) relative to \( \mathbb{F}_p \) is defined by (see, for example, [14, 15])
\[ \mathbb{N}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) := \alpha \alpha^p \cdots \alpha^{p^{k-1}} = \alpha^{\frac{q-1}{p-1}}. \]

For the simplicity, we write \( \mathbb{N}(\alpha) \) for \( \mathbb{N}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) \). For any \( \alpha \in \mathbb{F}_q \), it is clear that \( \mathbb{N}(\alpha) \in \mathbb{F}_p \). Furthermore, if \( \alpha \) is a primitive element of \( \mathbb{F}_q \), then \( \mathbb{N}(\alpha) \) is a primitive element of \( \mathbb{F}_p \).

Let \( \chi \) be a multiplicative character of \( \mathbb{F}_p \). Then \( \chi \) can be lifted to a multiplicative character \( \lambda \) of \( \mathbb{F}_q \) by setting \( \lambda(\alpha) = \chi(\mathbb{N}(\alpha)) \). The characters of \( \mathbb{F}_p \) can be lifted to the characters of \( \mathbb{F}_q \), but not all characters of \( \mathbb{F}_q \) can be obtained by lifting a character of \( \mathbb{F}_p \). The following lemma tells us when \( p \equiv 1 \pmod{3} \), then any multiplicative character \( \lambda \) of order 3 of \( \mathbb{F}_q \) can be lifted by a multiplicative character of order 3 of \( \mathbb{F}_p \).

**Lemma 2.1.** [15] Let \( \mathbb{F}_p \) be a finite field and \( \mathbb{F}_q \) be an extension of \( \mathbb{F}_p \). A multiplicative character \( \lambda \) of \( \mathbb{F}_q \) can be lifted by a multiplicative character \( \chi \) of \( \mathbb{F}_p \) if and only if \( \lambda^{p-1} \) is trivial.

Let \( \lambda_1, \ldots, \lambda_s \) be \( s \) multiplicative characters of \( \mathbb{F}_q \). The Jacobi sum \( J(\lambda_1, \cdots, \lambda_s) \) is defined by
\[ J(\lambda_1, \cdots, \lambda_s) := \sum_{y_1 + \cdots + y_s = 1} \lambda_1(y_1) \cdots \lambda_s(y_s), \]
where the summation is taken over all \(s\)-tuples \((\gamma_1, \cdots, \gamma_s)\) of elements of \(\mathbb{F}_q\) with \(\gamma_1 + \cdots + \gamma_s = 1\). It is clear that if \(\sigma\) is a permutation of \([1, \cdots, s]\), then

\[
J(\lambda_{\sigma(1)}, \cdots, \lambda_{\sigma(s)}) = J(\lambda_1, \cdots, \lambda_s).
\]

The readers are referred to [2] and [15] for basic facts on Jacobi sums.

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

**Lemma 2.2.** [15] Let \(\chi_1, \ldots, \chi_s\) be \(s\) multiplicative characters of \(\mathbb{F}_p\), not all of which are trivial. Suppose \(\chi_1, \ldots, \chi_s\) are lifted to characters \(\lambda_1, \ldots, \lambda_s\), respectively, of the finite extension field \(\mathbb{F}_{p^k}\) of \(\mathbb{F}_p\). Then

\[
J(\lambda_1, \cdots, \lambda_s) = (-1)^{(s-1)(k-1)} J(\chi_1, \cdots, \chi_s)^k.
\]

We give the reduction formula for Jacobi sums as follows.

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

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

The value of some needed Jacobi sums are listed in the following two lemmas.

**Lemma 2.4.** [2] Let \(p \equiv 1(\text{mod } 3)\) be a prime, \(q = p^k\), \(\alpha\) be a primitive element of \(\mathbb{F}_q\), and let \(\chi\) be a multiplicative character of order 3 over \(\mathbb{F}_p\). Then

\[
2J(\chi, \chi) = u + iv\sqrt{3},
\]

where the integers \(u\) and \(v\) are uniquely determined such that

\[
u^2 + 3v^2 = 4p, \quad u \equiv 1(\text{mod } 3), \quad v \equiv 0(\text{mod } 3) \text{ and } 3v \equiv u(2\alpha^{(q-1)/3} + 1)(\text{mod } p).
\]

**Lemma 2.5.** [2] Let \(p \equiv 1(\text{mod } 3)\), \(g\) be a primitive element of \(\mathbb{F}_p\) and let \(\chi\) be a multiplicative character of order 3 over \(\mathbb{F}_p\), such that \(\chi(g) = -\frac{\alpha + i\sqrt{3}}{2}\). Let the integers \(u\) and \(v\) be defined as in Lemma 2.4. Then the values of the nine Jacobi sums \(J(\chi^m, \chi^n)\) \((m, n = 0, 1, 2)\) are given in the following Table 1.

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

<table>
<thead>
<tr>
<th>(m) (\setminus) (n)</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>(p)</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>(\frac{1}{2}(u + iv\sqrt{3}))</td>
<td>-1</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>-1</td>
<td>(\frac{1}{2}(u - iv\sqrt{3}))</td>
</tr>
</tbody>
</table>

The following lemma gives the number of solutions of the diagonal equation in terms of Jacobi sums.
Lemma 2.6. \[2\] Let \(k_1, \ldots, k_s\) be positive integers, \(a_1, \ldots, a_s \in \mathbb{F}_q^*\) and let \(c \in \mathbb{F}_q\). Set \(d_i = \gcd(k_i, q - 1)\), and let \(\lambda_i\) be a multiplicative character of order \(d_i\) of \(\mathbb{F}_q^*\), \(i = 1, \ldots, s\). Then the number \(N\) of solutions of the equation \(a_1 x_1^{k_1} + \cdots + a_s x_s^{k_s} = c\) is given by

\[
N = q^{r-1} - (q - 1) \left( \sum_{j=1}^{d_1-1} \lambda_1^{j} (a_1^{-1}) \cdots \lambda_s^{j} (a_s^{-1}) \cdot J(\lambda_1^{j}, \ldots, \lambda_s^{j}) \right)
\]

if \(c = 0\), and by

\[
N = q^{r-1} + \left( \sum_{j=1}^{d_1-1} \lambda_1^{j} (ca_1^{-1}) \cdots \lambda_s^{j} (ca_s^{-1}) \cdot J(\lambda_1^{j}, \ldots, \lambda_s^{j}) \right)
\]

if \(c \neq 0\).

3. Proof of Theorems 1.2 and 1.3

In this section, we give the proof of Theorems 1.2 and 1.3. First, we begin with a lemma.

Lemma 3.1. Let \(p \equiv 1 \pmod{3}\) be a prime, \(q = p^s\), \(\alpha\) be a primitive element of \(\mathbb{F}_q\) and let \(\lambda\) be the multiplicative character of order 3 of \(\mathbb{F}_q\) such that \(\lambda(\alpha) = \frac{-1 + \sqrt{3}}{2}\). Then for any positive integers \(a, b\) and \(\beta \in \mathbb{F}_q^*\), we have

\[
\lambda(\beta) + \lambda(\beta^2) = \begin{cases} 2, & \text{if } \text{ind}_\beta \beta \equiv 0 \pmod{3}, \\ -1, & \text{if } \text{ind}_\beta \beta \not\equiv 0 \pmod{3} \end{cases}
\]

and

\[
\lambda(\beta)(a + ib \sqrt{3})^k + \lambda(\beta^2)(a - ib \sqrt{3})^k = \begin{cases} 2E(a, b, k), & \text{if } \text{ind}_\beta \beta \equiv 0 \pmod{3}, \\ -E(a, b, k) + O(a, b, k), & \text{if } \text{ind}_\beta \beta \equiv 1 \pmod{3}, \\ -E(a, b, k) - O(a, b, k), & \text{if } \text{ind}_\beta \beta \equiv 2 \pmod{3}, \end{cases}
\]

where \(E(a, b, k)\) and \(O(a, b, k)\) are defined as in Theorem 1.2.

Proof. The first part of the lemma is obvious. Now we focus on the proof of the second part of the lemma. One can divide this into the following three cases.

If \(\text{ind}_\beta \beta \equiv 0 \pmod{3}\), then \(\lambda(\beta) = \lambda(\beta^2) = 1\). One has

\[
(a + ib \sqrt{3})^k + (a - ib \sqrt{3})^k
\]

\[
= \sum_{i=0}^{k} \binom{k}{i} a^{k-i} [(ib \sqrt{3})^i + (-ib \sqrt{3})^i]
\]

\[
= 2a^k + \sum_{i=1}^{k} \binom{k}{i} a^{k-i} ((ib \sqrt{3})^i + (-ib \sqrt{3})^i)
\]
\[\begin{align*}
= 2a^k - 2 \sum_{t=1}^{k} \binom{k}{t} a^{k-t} b' 3^z + 2 \sum_{t=2}^{k} \binom{k}{t} a^{k-t} b' 3^z \\
= 2E(a, b, k). \quad (3.1)
\end{align*}\]

If \( \text{ind}_\alpha \beta \equiv 1 \pmod{3} \), then \( \lambda(\beta) = \frac{-1 + i \sqrt{3}}{2} \) and \( \lambda(\beta^2) = \frac{-1 - i \sqrt{3}}{2} \). One has
\[\begin{align*}
\frac{1}{2} \left( (-1 + i \sqrt{3})(a + ib \sqrt{3})^k - (1 + i \sqrt{3})(a - ib \sqrt{3})^k \right) \\
= \frac{1}{2} \left( - (a + ib \sqrt{3})^k - (a - ib \sqrt{3})^k + i \sqrt{3}(a + ib \sqrt{3})^k - i \sqrt{3}(a - ib \sqrt{3})^k \right) \\
= - \frac{1}{2} \left( 2 \sum_{t=0}^{k} \binom{k}{t} a^{k-t} b' 3^z - 2i \sqrt{3} \sum_{t=1}^{k} \binom{k}{t} a^{k-t} b' 3^z \right) \\
= - a^k + \sum_{t=1}^{k} \binom{k}{t} a^{k-t} b' 3^z - \sum_{t=1}^{k} \binom{k}{t} a^{k-t} b' 3^z - \sum_{t=1}^{k} \binom{k}{t} a^{k-t} b' 3^{z+1} \\
+ \sum_{t=2}^{k} \binom{k}{t} a^{k-t} b' 3^{z+1} \\
= - \left( E(a, b, k) + O(a, b, k) \right). \quad (3.2)
\end{align*}\]

If \( \text{ind}_\alpha \beta \equiv 2 \pmod{3} \), then \( \lambda(\beta) = \frac{-1 - i \sqrt{3}}{2} \) and \( \lambda(\beta^2) = \frac{-1 + i \sqrt{3}}{2} \). One has
\[\begin{align*}
\frac{1}{2} \left( (-1 - i \sqrt{3})(a + ib \sqrt{3})^k + (-1 + i \sqrt{3})(a - ib \sqrt{3})^k \right) \\
= - \sum_{t=0}^{k} \binom{k}{t} a^{k-t} b' 3^z - i \sqrt{3} \sum_{t=1}^{k} \binom{k}{t} a^{k-t} b' 3^z \\
= - a^k + \sum_{t=1}^{k} \binom{k}{t} a^{k-t} b' 3^z - \sum_{t=1}^{k} \binom{k}{t} a^{k-t} b' 3^z + \sum_{t=1}^{k} \binom{k}{t} a^{k-t} b' 3^{z+1} \\
- \sum_{t=2}^{k} \binom{k}{t} a^{k-t} b' 3^{z+1} \\
= - \left( E(a, b, k) - O(a, b, k) \right). \quad (3.3)
\end{align*}\]

The result follows immediately from (3.1)–(3.3). \[\square\]

Now we can turn our attention to prove Theorems 1.2 and 1.3.
Lemma 2.5 and Lemma 3.1, we obtain
\[ \lambda \]
if \( c = 0 \), and
\[ N_1 = q + \sum_{j_1=1}^{2} \sum_{j_2=1}^{2} \lambda(c^{j_1+j_2}a_1^{-j_1}a_2^{-j_2})J(\lambda^{j_1}, \lambda^{j_2}), \]  
(3.5)
if \( c \neq 0 \).

Since \( p \equiv 1(\text{mod } 3) \), it follows that \( \lambda^{p-1} \) is trivial. By Lemma 2.1, the cubic multiplicative character \( \lambda \) can be lifted by a cubic multiplicative character \( \chi \) of \( \mathbb{F}_p \). Combining with the Lemma 2.2, Table 1 of Lemma 2.5 and Lemma 3.1, we obtain
\[ \sum_{j_1=1}^{2} \sum_{j_2=1}^{2} \lambda(a_1^{-j_1}a_2^{-j_2})J(\lambda^{j_1}, \lambda^{j_2}) \]
\[ = (-1)^{j_1}J(\chi, \chi^2)^{j_2}(\lambda(a_1^2a_2) + \lambda(a_1a_2^2)) \]
\[ = -\lambda(a_1^2a_2) + \lambda(a_1a_2^2) \]
\[ = \delta(a_1, a_2), \]  
(3.6)
and
\[ \sum_{j_1=1}^{2} \sum_{j_2=1}^{2} \lambda(c^{j_1+j_2}a_1^{-j_1}a_2^{-j_2})J(\lambda^{j_1}, \lambda^{j_2}) \]
\[ = (-1)^{j_1-1}(\lambda(c^2a_1^2a_2^2)J(\chi, \chi)^k + \lambda(a_1^2a_2)J(\chi, \chi^2)^k + \lambda(a_1a_2^2)J(\chi^2, \chi)^k \]
\[ + \lambda(ca_1a_2)J(\chi^2, \chi^3)^k \]
\[ = -\lambda(a_1^2a_2) + \lambda(a_1a_2^2) + (-1)^{j_1-1}(\lambda(c^2a_1^2a_2^2)J(\chi, \chi)^k + \lambda(ca_1a_2)J(\chi^2, \chi^3)^k) \]
\[ = \delta(a_1, a_2) + \frac{(-1)^{k-1}}{2^k}(\lambda(c^2a_1^2a_2^2)(u + iv\sqrt{3})^k + \lambda(ca_1a_2)(u - iv\sqrt{3})^k) \]
\[ = \begin{cases} 
\frac{(-1)^{k-1}}{2^k}E(u, v, k) + \delta(a_1, a_2), & \text{if } \text{ind}_a ca_1a_2 \equiv 0(\text{mod } 3), \\
\frac{(-1)^k}{2^k}(E(u, v, k) - O(u, v, k)) + \delta(a_1, a_2), & \text{if } \text{ind}_a ca_1a_2 \equiv 1(\text{mod } 3), \\
\frac{(-1)^k}{2^k}(E(u, v, k) + O(u, v, k)) + \delta(a_1, a_2), & \text{if } \text{ind}_a ca_1a_2 \equiv 2(\text{mod } 3).
\end{cases} \]  
(3.7)

Then from (3.4)–(3.7), one can easily deduce the result of Theorem 1.2.  
\[ \Box \]
\textbf{Proof of Theorem 1.3.} By the same argument as in the proof of theorem 1.2, let \( \alpha \) be a primitive element of \( \mathbb{F}_q \) and \( \lambda \) be the multiplicative character of \( \mathbb{F}_p \) of order 3 with \( \lambda(\alpha) = -\frac{1+i\sqrt{3}}{2} \). We deduce that

\[ N_2 = q^2 - (q - 1) \sum_{j_1=1}^{2} \sum_{j_2=1}^{2} \sum_{j_3=1}^{2} \lambda(b_1^{-j_1}b_2^{-j_2}b_3^{-j_3})J(\lambda^{j_1}, \lambda^{j_2}, \lambda^{j_3}) \]  

(3.8)

if \( c = 0 \), and

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

(3.9)

if \( c \neq 0 \).

Similarly, the cubic multiplicative character \( \lambda \) can be lifted by a cubic multiplicative character \( \chi \) of \( \mathbb{F}_p \). By using the Lemmas 2.2, 2.3, Table 1 of Lemma 2.5 and Lemma 3.1, we get

\[
\sum_{j_1=1}^{2} \sum_{j_2=1}^{2} \sum_{j_3=1}^{2} \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_1^2b_2^2b_3^2)J(\chi, \chi)^kJ(\chi^2, \chi)^k + \lambda(b_1b_2b_3)J(\chi, \chi^2)^kJ(\chi^2, \chi)^k \\
= \left(-\frac{1}{2}\right)^k \left( \lambda(b_1^2b_2^2b_3^2)(u + iv \sqrt{3})^k + \lambda(b_1b_2b_3)(u - iv \sqrt{3})^k \right) \\
= \left\{ \begin{array}{ll}
\left(-\frac{1}{2}\right)^k E(u, v, k), & \text{if } \text{ind}_a b_1b_2b_3 \equiv 0 \text{(mod 3)}, \\
\left(-\frac{1}{2}\right)^{k+1} (E(u, v, k) - O(u, v, k)), & \text{if } \text{ind}_a b_1b_2b_3 \equiv 1 \text{(mod 3)}, \\
\left(-\frac{1}{2}\right)^{k+1} (E(u, v, k) + O(u, v, k)), & \text{if } \text{ind}_a b_1b_2b_3 \equiv 2 \text{(mod 3)}
\end{array} \right.  

(3.10)

and

\[
\sum_{j_1=1}^{2} \sum_{j_2=1}^{2} \sum_{j_3=1}^{2} \lambda(c^{j_1+j_2+j_3}b_1^{-j_1}b_2^{-j_2}b_3^{-j_3})J(\lambda^{j_1}, \lambda^{j_2}, \lambda^{j_3}) \\
= \lambda(b_1b_2b_3)J(\chi, \chi^2)^kJ(\chi^2, \chi)^k + \lambda(b_1^2b_2^2b_3^2)J(\chi, \chi)^kJ(\chi^2, \chi)^k \\
+ \lambda(c^2b_1b_2b_3)J(\chi, \chi^2)^kJ(\chi^2, \chi)^k \\
+ \lambda(c^2b_1b_2b_3)J(\chi, \chi^2)^k + \lambda(c^2b_1b_2b_3)J(\chi^2, \chi)^k \\
= \left(-\frac{1}{2}\right)^k \left( \lambda(b_1b_2b_3)(u + iv \sqrt{3})^k + \lambda(b_1^2b_2^2b_3^2)(u - iv \sqrt{3})^k \right) \\
+ \frac{1}{2^{2k}} (u^2 + 3v^2)^k \left( \lambda(c^2b_1b_2b_3) + \lambda(c^2b_1b_2b_3) \right)
\]
\[ + q \left( \lambda(c b_1^2 b_2 b_3^2) + \lambda(c^2 b_1 b_2^2 b_3) + \lambda(c^2 b_1^2 b_2 b_3) + \lambda(c b_1 b_2^2 b_3^2) \right). \] (3.11)

By second part of Lemma 3.1, we derive that
\[
\left( \frac{-1}{2} \right)^k (\lambda(b_1 b_2 b_3)(u - iv \sqrt{3})^k + \lambda(b_1^2 b_2^2 b_3^2)(u + iv \sqrt{3})^k)
= \begin{cases} 
\left( \frac{-1}{2} \right)^{k+1} E(u, v, k), & \text{if } \text{ind}_{u} b_1 b_2 b_3 \equiv 0 \mod 3, \\
\left( \frac{-1}{2} \right)^k (E(u, v, k) - O(u, v, k)), & \text{if } \text{ind}_{u} b_1 b_2 b_3 \equiv 1 \mod 3, \\
\left( \frac{-1}{2} \right)^k (E(u, v, k) + O(u, v, k)), & \text{if } \text{ind}_{u} b_1 b_2 b_3 \equiv 2 \mod 3.
\end{cases}
\] (3.12)

Note that Lemma 2.4 tells us \( u^2 + 3v^2 = 4p \). Then from the first part of Lemma 3.1, one has
\[
\frac{1}{2^{2k}}(u^2 + 3v^2)^k (\lambda(c b_1^2 b_2 b_3) + \lambda(c^2 b_1 b_2 b_3^2))
= \begin{cases} 
2q, & \text{if } \text{ind}_{u} c b_1^2 b_2^2 b_3 \equiv 0 \mod 3, \\
-q, & \text{if } \text{ind}_{u} c b_1^2 b_2^2 b_3 \not\equiv 0 \mod 3
\end{cases}
\] (3.13)

and
\[
\lambda(c b_1^2 b_2 b_3^2) + \lambda(c^2 b_1 b_2^2 b_3) + \lambda(c^2 b_1^2 b_2 b_3) + \lambda(cb_1 b_2^2 b_3^2)) = \omega(c, b_1, b_2, b_3) + \omega'(c, b_1, b_2, b_3). \] (3.14)

Thus from (3.8)–(3.14), the desired result of Theorem 1.3 follows immediately.

\[ \square \]

4. Some examples

In this section, we present some examples to demonstrate the validity of our results.

Example 4.1. Let \( q = 13^4 \). One can check that 2 is a primitive element of \( \mathbb{F}_{13} \). Let \( \omega \) be a primitive element of \( \mathbb{F}_q \) such that \( \mathbb{N}(\omega) = \omega^{\frac{13^4 - 1}{13 - 1}} = 2 \). We consider the numbers of solutions of the cubic equations
\[ x_1^3 + \omega^2 x_2^3 = 0 \]
and
\[ x_1^3 + \omega x_2^3 = \omega \]
over \( \mathbb{F}_q \).

Since \( \omega^{\frac{13^4 - 1}{13 - 1}} = (\omega^{\frac{13^3 - 1}{13 - 1}})^{\frac{13^4}{13^3}} = 2^4 \), the integers \( u \) and \( v \) in Lemma 2.4 are determined by
\[ u^2 + 3v^2 = 52, \ u \equiv 1 \mod 3, \ v \equiv 0 \mod 3 \] and \( 3v \equiv u(2 \times 2^4 + 1) \mod 13 \).

We can get that \( u = -5 \) and \( v = -3 \). Therefore, by Theorem 1.2, we have
\[ N(x_1^3 + \omega^2 x_2^3 = 0) = 1 \]
and
\[ N(x_1^3 + \omega x_2^3 = \omega) = 28899. \]
Example 4.2. Let $q = 31^2$. One can check that 3 is a primitive element of $\mathbb{F}_{31}$. Let $\omega$ be a primitive element of $\mathbb{F}_q$ such that $\mathbb{N}(\omega) = \omega^{\frac{31^2 - 1}{3}} = 3$. We consider the numbers of solutions of the cubic equations
$$\omega^4 x_1^3 + x_2^3 + \omega x_3^3 = 0$$
and
$$\omega^4 x_1^3 + x_2^3 + \omega x_3^3 = \omega$$
over $\mathbb{F}_q$.

Since $\omega^{\frac{31^2 - 1}{3}} = (\omega^{\frac{31^1 - 1}{3}})^{\frac{31}{3}} = 3^{10}$, the integers $u$ and $v$ are determined by
$$u^2 + 3v^2 = 124, \quad u \equiv 1(\text{mod } 3), \quad v \equiv 0(\text{mod } 3) \text{ and } 3v \equiv u(2 \times 3^{10} + 1)(\text{mod } 31).$$

We get $u = 4$ and $v = 6$. Thus by Theorem 1.3, we deduce that
$$N(\omega^4 x_1^3 + x_2^3 + \omega x_3^3 = 0) = 936001$$
and
$$N(\omega^4 x_1^3 + x_2^3 + \omega x_3^3 = \omega) = 920625.$$

Example 4.3. Let $q = 7^3$. It is clear that 3 is a primitive element of $\mathbb{F}_7$. Let $\omega$ be a primitive element of $\mathbb{F}_q$ such that $\mathbb{N}(\omega) = \omega^{\frac{7^3 - 1}{7}} = 3$. We consider the the numbers of solutions of the cubic equations
$$x_1^3 + \omega^2 x_2^3 + \omega^3 x_3^3 = 0$$
and
$$x_1^3 + \omega^2 x_2^3 + \omega^3 x_3^3 = \omega$$
over $\mathbb{F}_q$.

Similarly, since $\omega^{\frac{7^3 - 1}{7}} = (\omega^{\frac{7^2 - 1}{7}})^{\frac{7}{7}} = 3^2$, the integers $u$ and $v$ are determined by
$$u^2 + 3v^2 = 28, \quad u \equiv 1(\text{mod } 3), \quad v \equiv 0(\text{mod } 3) \text{ and } 3v \equiv u(2 \times 3^2 + 1)(\text{mod } 7).$$

We deduce that $u = 1$ and $v = -3$. Thus by Theorem 1.3, we have
$$N(x_1^3 + \omega^2 x_2^3 + \omega^3 x_3^3 = 0) = 111835$$
and
$$N(x_1^3 + \omega^2 x_2^3 + \omega^3 x_3^3 = \omega) = 117666.$$

5. Conclusions

Studying the number of solutions of the polynomial equation $f(x_1, x_2, \cdots, x_n) = 0$ over $\mathbb{F}_q$ is one of the main topics in the theory of finite fields. 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 the Hasse-Davenport theorem for Jacobi sums, we give an explicit formulae for the numbers of solutions of cubic diagonal equations $a_1 x_1^3 + a_2 x_2^3 = c$ and $b_1 x_1^3 + b_2 x_2^3 + b_3 x_3^3 = c$ over $\mathbb{F}_q$ are given, with $a_i, b_j \in \mathbb{F}_q^*$ ($1 \leq i \leq 2, 1 \leq j \leq 3$), $c \in \mathbb{F}_q$ and $p \equiv 1(\text{mod } 3)$. Furthermore, by using the reduction formula for Jacobi sums, the number of solutions of the cubic diagonal equations $a_1 x_1^3 + a_2 x_2^3 + \cdots + a_s x_s^3 = c$ of $s \geq 4$ variables with $a_i \in \mathbb{F}_q^*$ ($1 \leq i \leq s$), $c \in \mathbb{F}_q$ and $p \equiv 1(\text{mod } 3)$, can also be deduced.
Acknowledgments

The Authors express their gratitude to the anonymous referee for carefully examining this paper and providing a number of important comments and suggestions. This research was supported by the National Science Foundation of China (No. 12026223 and No. 12026224) and by the National Key Research and Development Program of China (No. 2018YFA0704703).

Conflict of interest

We declare that we have no conflict of interest.

References


© 2023 the Author(s), licensee AIMS Press. This is an open access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0)