AIMS Mathematics, 7(6): 10554–10563.
DOI: 10.3934/math.2022588
Received: 30 November 2021
Revised: 23 February 2022
Accepted: 02 March 2022
Published: 28 March 2022

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

Research article

On the number of solutions of two-variable diagonal sextic equations over finite fields

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

[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 a positive integer, $q = p^k$, and $\mathbb{F}_q$ be the finite field with q elements. In this paper, by using the Jacobi sums, we give an explicit formula for the number of solutions of the two-variable diagonal sextic equations $x_1^6 + x_2^6 = c$ over $\mathbb{F}_q$, with $c \in \mathbb{F}_q^*$ and $p \equiv 1 (\mathrm{mod}\ 6)$. Furthermore, by using the reduction formula for Jacobi sums, the number of solutions of the diagonal sextic equations $x_1^6 + x_2^6 + \cdots + x_n^6 = c$ of $n \geq 3$ variables with $c \in \mathbb{F}_q^*$ and $p \equiv 1 (\mathrm{mod}\ 6)$, can also be deduced.

Keywords: finite fields; rational points; diagonal equations; Jacobi sums
Mathematics Subject Classification: 11T06, 11T24

1. Introduction

Let p be a prime, k a positive integer, $q = p^k$, and let $\mathbb{F}_q$ be the finite field of q elements. Let f be a polynomial over $\mathbb{F}_q$ with n variables, and denote by

$$N(f, q) = N(f(x_1, \cdots, x_n) = 0) = \#\{(x_1, \cdots, x_n) \in \mathbb{F}_q^n \mid f(x_1, \cdots, x_n) = 0\}$$

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

Studying the value of $N(f, q)$ is one of the main topics in the theory of finite fields. Generally speaking, it is difficult to give the explicit formula for $N(f, q)$.

The degree d of the polynomial f plays an important role in the estimate of $N(f, q)$. An upper bound for $N(f, q)$ [14] is given by

$$N(f, q) \leq dq^{n-1}.$$

For any positive integer m, we use $\mathrm{ord}_p m$ to denote the p-adic valuation of m. Suppose that $N(f, q) > 0$, the classical Chevalley-Warning theorem shows that $\mathrm{ord}_p N(f, q) > 0$ if $n > d$. Furthermore, let $\lceil x \rceil$

denote the least integer $\geq x$ and let $q = p^k$, Ax [1] showed that

$$\mathrm{ord}_p N(f, q) \geq k \left\lceil \frac{n-d}{d} \right\rceil.$$

Finding the explicit formula for $N(f, q)$ under certain conditions has attracted researchers for many years. From [13, 14] we know that there exists an explicit formula for $N(f, q)$ satisfying $\deg(f) \leq 2$ over $\mathbb{F}_q$. Some other works were done by Baoulina [2–5], Cao et al. [7, 8], Hua and Vandiver [12], Hu et al. [10, 11], Weil [17], and Zhang and Wan [20, 21].

In 1977, Chowla, Cowles and Cowles [9] got a formula for the number of solutions of the hypersurface

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

over $\mathbb{F}_p$. In 1979, Myerson [15] extended the result in [9] to the field $\mathbb{F}_q$ and studied the number of solutions of the equation

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

over $\mathbb{F}_q$. For $q = p^{2t}$ with $p^r \equiv -1 (\mathrm{mod}\ d)$ for a divisor r of t and $d \mid (q-1)$, Wolfmann [18] gave an explicit formula of the number of solutions of the equation

$$a_1 x_1^d + a_2 x_2^d + \cdots + a_n x_n^d = c$$

over $\mathbb{F}_q$ in 1992, where $a_1, a_2, \ldots, a_n \in \mathbb{F}_q^*$ and $c \in \mathbb{F}_q$. In 2018, Zhang and Hu [19] determined an explicit formula of 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 $p \equiv 1 (\mathrm{mod}\ 3)$ and $c \in \mathbb{F}_p^*$. In 2020, J. Zhao et al. [22, 23] investigated the number of solutions of the forms

$$x_1^4 + x_2^4 = c,$$

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

and

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

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

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

$$f(x_1, x_2, \cdots, x_n) = x_1^6 + x_2^6 + \cdots + x_n^6 - c = 0$$

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

It is well-known that (see [13], p. 105)

$$N(x_1^6 + x_2^6 + \cdots + x_n^6 = c) = N(x_1^{\gcd(6,q-1)} + x_2^{\gcd(6,q-1)} + \cdots + x_n^{\gcd(6,q-1)} = c)$$

over $\mathbb{F}_q$. Let $q = p^k$ with p a prime. If $p = 2$, then $\gcd(6, q-1) = 1$ or 3 depends on k is odd or even. From Corollary 4 in [18], we can obtain the following result.

Theorem 1.1. *Let $p = 2$, k an integer, $q = p^k$ and $c \in \mathbb{F}_q^*$. Then*

$$N(x_1^6 + x_2^6 + \cdots + x_n^6 = c) = q^{n-1}$$

if k is odd, and

$$N(x_1^6 + x_2^6 + \cdots + x_n^6 = c) = \begin{cases} q^{n-1} + \xi^{n+1} q^{\frac{n}{2}-1}[2^n q^{\frac{1}{2}} - (q^{\frac{1}{2}} + \xi)\frac{2^n + 2(-1)^n}{3}], & \text{if } c^{\frac{q-1}{3}} = 1, \\ q^{n-1} + \xi^{n+1} q^{\frac{n}{2}-1}[(-1)^n q^{\frac{1}{2}} - (q^{\frac{1}{2}} + \xi)\frac{2^n + 2(-1)^n}{3}], & \text{otherwise} \end{cases}$$

if k is even and $n \geq 2$, with $\xi = (-1)^{\frac{k}{2}+1}$.

If $p = 3$ and k is an integer, or $p \equiv 5 (\mathrm{mod}\ 6)$ and k is an odd integer, then $\gcd(6, q-1) = 2$. It follows from Theorems 6.26 and 6.27 in [14] that the following result is given.

Theorem 1.2. *Let $p = 3$ and k an integer, or $p \equiv 5 (\mathrm{mod}\ 6)$ be a prime and k an odd integer, $q = p^k$ and $c \in \mathbb{F}_q^*$. Then*

$$N(x_1^6 + x_2^6 + \cdots + x_n^6 = c) = q^{n-1} - q^{\frac{n-2}{2}} \eta((-1)^{\frac{n}{2}})$$

if n is even, and

$$N(x_1^6 + x_2^6 + \cdots + x_n^6 = c) = q^{n-1} + q^{\frac{n-1}{2}} \eta((-1)^{\frac{n-1}{2}} c)$$

if n is odd, where η is the quadratic multiplicative character of $\mathbb{F}_q$.

If $p \equiv 5 (\mathrm{mod}\ 6)$ and k is an even integer, Hua and Vandiver [12] studied the number of solutions of some trinomial equations over $\mathbb{F}_q$ and Wolfmann [18] also got the number of solutions of certain diagonal equations over $\mathbb{F}_q$. The following result can be deduced from Corollary 4 of [18].

Theorem 1.3. *Let $p \equiv 5 (\mathrm{mod}\ 6)$ be a prime, k an even integer, $q = p^k$, $n \geq 2$ and $c \in \mathbb{F}_q^*$. Then*

$$N(x_1^6 + x_2^6 + \cdots + x_n^6 = c) = \begin{cases} q^{n-1} + \xi^{n+1} q^{\frac{n}{2}-1}[5^n q^{\frac{1}{2}} - (q^{\frac{1}{2}} + \xi)\frac{5^n + 5(-1)^n}{6}], & \text{if } c^{\frac{q-1}{6}} = 1, \\ q^{n-1} + \xi^{n+1} q^{\frac{n}{2}-1}[(-1)^n q^{\frac{1}{2}} - (q^{\frac{1}{2}} + \xi)\frac{5^n + 5(-1)^n}{6}], & \text{otherwise,} \end{cases}$$

where $\xi = (-1)^{\frac{k}{2}+1}$.

However, the formula for $N(x_1^6 + x_2^6 + \cdots + x_n^6 = c)$ is still unknown when $p \equiv 1 (\mathrm{mod}\ 6)$. 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 case with 2 variables. The case with arbitrary $n \geq 3$ variables can be deduced from the reduction formula for Jacobi sums.

Let $g \in \mathbb{F}_q^*$ 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 $\beta = g^r$. Such r is called the *index* of β with the primitive element g, and denoted by $\mathrm{ind}_g \beta := r$.

For any element $\alpha \in E = \mathbb{F}_{p^k}$ and $F = \mathbb{F}_p$, the norm of α relative to $\mathbb{F}_p$ are defined by (see, for example, [6, 14])

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

For the simplicity, we write $\mathbb{N}(\alpha)$ for $\mathbb{N}_{E/F}(\alpha)$.

The main result of this paper is stated as follows.

Theorem 1.4. *Let t and k be positive integers, $p = 6t + 1$ be a prime, $q = p^k$, and let $\mathbb{F}_q$ be the finite field with q elements. Let $c \in \mathbb{F}_q^*$, g be a primitive element of $\mathbb{F}_q$ and $Z = ind_{\mathbb{N}(g)}2$. Then*

$$N(x_1^6 + x_2^6 = c) = \begin{cases} q - 5 + (-1)^{k-1}(\frac{3u+r}{2^{k-1}} + 12a), & \text{if } \mathrm{ind}_g c \equiv 0 (\mathrm{mod}\ 6), \\ q - 5 + (-1)^k(\frac{r-u-3s-3v}{2^k} + 4a - 12b), & \text{if } \mathrm{ind}_g c \equiv 1 (\mathrm{mod}\ 6), \\ q - 5 + (\frac{-1}{2})^k(3u + 3s + r - 9v), & \text{if } \mathrm{ind}_g c \equiv 2 (\mathrm{mod}\ 6), \\ q - 5 + (-1)^k(\frac{u-r}{2^{k-1}} + 4a), & \text{if } \mathrm{ind}_g c \equiv 3 (\mathrm{mod}\ 6), \\ q - 5 + (\frac{-1}{2})^k(9v + 3u + r - 3s), & \text{if } \mathrm{ind}_g c \equiv 4 (\mathrm{mod}\ 6), \\ q - 5 + (-1)^k(\frac{3v+r+3s-u}{2^k} + 4a + 12b), & \text{if } \mathrm{ind}_g c \equiv 5 (\mathrm{mod}\ 6) \end{cases}$$

when t or k is even, and

$$N(x_1^6 + x_2^6 = c) = \begin{cases} q + 1 + \frac{r+u}{2^{k-1}} + 4a, & \text{if } \mathrm{ind}_g c \equiv 0 (\mathrm{mod}\ 6), \\ q + 1 + \frac{3s+3u+9v-r}{2^k}, & \text{if } \mathrm{ind}_g c \equiv 1 (\mathrm{mod}\ 6), \\ q + 1 + \frac{3v-r-3s-u}{2^k} + 4a + 12b, & \text{if } \mathrm{ind}_g c \equiv 2 (\mathrm{mod}\ 6), \\ q + 1 + \frac{r-3u}{2^{k-1}} - 12a, & \text{if } \mathrm{ind}_g c \equiv 3 (\mathrm{mod}\ 6), \\ q + 1 + \frac{3s-u-3v-r}{2^k} - 12b + 4a, & \text{if } \mathrm{ind}_g c \equiv 4 (\mathrm{mod}\ 6), \\ q + 1 + \frac{3u-9v-r-3s}{2^k}, & \text{if } \mathrm{ind}_g c \equiv 5 (\mathrm{mod}\ 6) \end{cases}$$

when both t and k are odd, where $a + ib\sqrt{3} = (a' + ib'\sqrt{3})^k$, $u + iv\sqrt{3} = (u' + iv'\sqrt{3})^k$, $r + is\sqrt{3} = (r' + is'\sqrt{3})^k$ with a' and b' being integers such that

$$a'^2 + 3b'^2 = p, \quad a' \equiv -1 (\mathrm{mod}\ 3), \quad \textit{and} \quad 3b' \equiv a'(2g^{(q-1)/3} + 1) (\mathrm{mod}\ p),$$

and the integers r', s', u' and v' are given by

$$\begin{cases} u' = r' = 2a', v' = s' = 2b', & \text{if } Z \equiv 0 (\mathrm{mod}\ 3), \\ u' = 3b' - a', r' = -a' - 3b', v' = -a' - b', s' = a' - b', & \text{if } Z \equiv 1 (\mathrm{mod}\ 3), \\ u' = -a' - 3b', r' = 3b' - a', v' = a' - b', s' = -a' - b', & \text{if } Z \equiv 2 (\mathrm{mod}\ 3). \end{cases}$$

This paper is organized as follows. In Section 2, we recall some useful known results which will be needed later. In Section 3, we prove Theorem 1.4 and then present an example to illustrate the validity of our result.

2. Preliminary lemmas

In this section, we present some useful lemmas that are needed in the proof of Theorem 1.4. For any multiplicative character λ of $\mathbb{F}_q$, it is now convenient to extend the definition of λ by setting $\lambda(0) = 1$ if λ is the trivial character and $\lambda(0) = 0$ otherwise.

Let $\lambda_1, \cdots, \lambda_s$ be s multiplicative characters of $\mathbb{F}_q$, the Jacobi sum $J(\lambda_1, \cdots, \lambda_s)$ is defined by

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

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 σ is a permutation of $\{1, \cdots, s\}$, then

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

Also for any $\alpha \in \mathbb{F}_q^*$, we have that

$$\sum_{\gamma_1+\cdots+\gamma_s=\alpha} \lambda_1(\gamma_1)\cdots\lambda_s(\gamma_s) = (\lambda_1\cdots\lambda_s)(\alpha)J(\lambda_1, \cdots, \lambda_s).$$

The readers are referred to [6] and [14] 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 2.1. [14] *Let $\chi_1, \cdots, \chi_s$ be s multiplicative characters of $\mathbb{F}_p$, not all of which are trivial. Suppose $\chi_1, \cdots, \chi_s$ are lifted to characters $\lambda_1, \cdots, \lambda_s$, respectively, of the finite extension field E of $\mathbb{F}_p$ with $[E : \mathbb{F}_p] = k$. Then*

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

Let χ be a multiplicative character of F and λ be a multiplicative character of E. Recall that χ can be lifted to E 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 the characters of $\mathbb{F}_q$ can be obtained by lifting a character of $\mathbb{F}_p$. The following lemma tells us when $p \equiv 1(\text{mod } 6)$, then the multiplicative character λ of order 6 of $\mathbb{F}_q$ can be lifted by a multiplicative character of order 6 of $\mathbb{F}_p$.

Lemma 2.2. [14] *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 g be a generator of $\mathbb{F}_q^* = \mathbb{F}_{p^k}^*$. Since

$$\mathbb{N}(g)^{p-1} = (g^{\frac{q-1}{p-1}})^{p-1} = g^{q-1} = 1$$

and

$$\mathbb{N}^l(g) = (g^{\frac{q-1}{p-1}})^l \neq 1 \text{ for } 1 \leq l \leq p-1,$$

one knows that $\mathbb{N}(g)$ is a generator of $\mathbb{F}_p^*$. Then we can state the following lemma.

Lemma 2.3. [6] *Let $p \equiv 1(\text{mod } 6)$ be a prime, q a power of p, g be a generator of $\mathbb{F}_q^*$, and let χ be a multiplicative character of order 6 over $\mathbb{F}_p$. Then*

$$J(\chi, \chi^2) = a' + ib'\sqrt{3},$$

where the integers a' and b' are uniquely determined by

$$a'^2 + 3b'^2 = p, \quad a' \equiv -1(\text{mod } 3), \quad \textit{and} \quad 3b' \equiv a'(2g^{(q-1)/3} + 1)(\text{mod } p).$$

Lemma 2.4. [6] *Let $p = 6t+1$ be a prime number. Let g' be the generator of $\mathbb{F}_p^*$ and χ be a multiplicative character of order 6 over $\mathbb{F}_p$ such that $\chi(g') = \frac{1+i\sqrt{3}}{2}$. Let the integers a' and b' be defined as in Lemma 2.3 and the integers u', v', r', s' are given as in Theorem 1.4. The values of the 36 Jacobi sums $J(\chi^m, \chi^n)$ $(m, n = 0, 1, 2, 3, 4, 5)$ are given in the following Table 1.*

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

$m \setminus n$	0	1	2	3	4	5
0	p	0	0	0	0	0
1	0	$(-1)^t\frac{1}{2}(u'+iv'\sqrt{3})$	$a'+ib'\sqrt{3}$	$(-1)^t(a'+ib'\sqrt{3})$	$\frac{1}{2}(u'+iv'\sqrt{3})$	$-(-1)^t$
2	0	$a'+ib'\sqrt{3}$	$\frac{1}{2}(r'+is'\sqrt{3})$	$a'+ib'\sqrt{3}$	-1	$\frac{1}{2}(u'-iv'\sqrt{3})$
3	0	$(-1)^t(a'+ib'\sqrt{3})$	$a'+ib'\sqrt{3}$	$-(-1)^t$	$a'-ib'\sqrt{3}$	$(-1)^t(a'-ib'\sqrt{3})$
4	0	$\frac{1}{2}(u'+iv'\sqrt{3})$	-1	$a'-ib'\sqrt{3}$	$\frac{1}{2}(r'-is'\sqrt{3})$	$a'-ib'\sqrt{3}$
5	0	$-(-1)^t$	$\frac{1}{2}(u'-iv'\sqrt{3})$	$(-1)^t(a'-ib'\sqrt{3})$	$a'-ib'\sqrt{3}$	$(-1)^t\frac{1}{2}(u'-iv'\sqrt{3})$

The following lemma gives an explicit formula for the number of solutions of the diagonal equation in terms of Jacobi sums.

Lemma 2.5. [6, 12, 17] *Let $k_1, \cdots, k_s$ be positive integers, $a_1, \cdots, a_s, c \in \mathbb{F}_q^*$. Set $d_i = \gcd(k_i, q-1)$, and let λ_i be a multiplicative character on $\mathbb{F}_q$ of order d_i, $i = 1, \cdots, s$. Then the number N of solutions of the equation $a_1x_1^{k_1} + \cdots + a_sx_s^{k_s} = c$ is given by*

$$N = q^{s-1} + \sum_{j_1=1}^{d_1-1} \cdots \sum_{j_s=1}^{d_s-1} \lambda_1^{j_1}(ca_1^{-1}) \cdots \lambda_s^{j_s}(ca_s^{-1}) J(\lambda_1^{j_1}, \cdots, \lambda_s^{j_s}).$$

3. Proof of Theorem 1.4

In this section, we give the proof of Theorem 1.4.

Proof. Let g be a primitive element of $\mathbb{F}_q$ and λ be a multiplicative character of $\mathbb{F}_q$ of order 6 with $\lambda(g) = \frac{1+i\sqrt{3}}{2}$. Since $q \equiv 1 (\mathrm{mod}\ 6)$, then $\gcd(6, q-1) = 6$. Using Lemma 2.5, we have

$$\begin{aligned} N(x_1^6 + x_2^6 = c) &= q + \sum_{j_1=1}^{5}\sum_{j_2=1}^{5} \lambda(c^{j_1+j_2}) J(\lambda^{j_1}, \lambda^{j_2}) \\ &= q + \sum_{1\le i\le 5} \lambda^{2i}(c) J(\lambda^i, \lambda^i) + 2\sum_{1\le i<j\le 5} \lambda^{i+j}(c) J(\lambda^i, \lambda^j). \end{aligned}$$

Since $p \equiv 1 (\mathrm{mod}\ 6)$, it follows that λ^{p-1} is trivial. By Lemma 2.2, the multiplicative character λ can be lifted by a multiplicative character χ of order 6 of $\mathbb{F}_p$. By Lemma 2.1, we obtain

$$N(x_1^6 + x_2^6 = c) = q + (-1)^{k-1}\left(\sum_{1\le i\le 5} \lambda^{2i}(c) J(\chi^i, \chi^i)^k + 2\sum_{1\le i<j\le 5} \lambda^{i+j}(c) J(\chi^i, \chi^j)^k\right). \quad (3.1)$$

Consider the case when t or k is even. Noting that $\lambda(1) = 1$, from (3.1), one has

$$N(x_1^6 + x_2^6 = 1) = q + (-1)^{k-1}\left(\sum_{1\le i\le 5} J(\chi^i, \chi^i)^k + 2\sum_{1\le i<j\le 5} J(\chi^i, \chi^j)^k\right). \quad (3.2)$$

From Table 1 of Lemma 2.4, we derive that

$$\begin{aligned} \sum_{1\le i\le 5} J(\chi^i, \chi^i)^k &= \left(\tfrac{u'+iv'\sqrt{3}}{2}\right)^k + \left(\tfrac{r'+is'\sqrt{3}}{2}\right)^k + (-1)^k + \left(\tfrac{r'-is'\sqrt{3}}{2}\right)^k + \left(\tfrac{u'-iv'\sqrt{3}}{2}\right)^k \\ &= \tfrac{u+iv\sqrt{3}}{2^k} + \tfrac{r+is\sqrt{3}}{2^k} + (-1)^k + \tfrac{r-is\sqrt{3}}{2^k} + \tfrac{u-iv\sqrt{3}}{2^k} \\ &= \tfrac{1}{2^{k-1}}(u+r) + (-1)^k, \end{aligned} \quad (3.3)$$

and

$$\begin{aligned} 2\sum_{1\le i<j\le 5} J(\chi^i,\chi^j)^k &= 6(a'+ib'\sqrt{3})^k + \tfrac{(u'+iv'\sqrt{3})^k}{2^{k-1}} + 4(-1)^k + \tfrac{(u'-iv'\sqrt{3})^k}{2^{k-1}} + 6(a'-ib'\sqrt{3})^k \\ &= 6(a+ib\sqrt{3}) + \tfrac{u+iv\sqrt{3}}{2^{k-1}} + 4(-1)^k + \tfrac{u-iv\sqrt{3}}{2^{k-1}} + 6(a-ib\sqrt{3}) \\ &= 4\left(3a + \tfrac{u}{2^k} + (-1)^k\right). \end{aligned} \tag{3.4}$$

Thus if $\mathrm{ind}_g c \equiv 0 (\mathrm{mod}\ 6)$, then it follows from (3.2)–(3.4) that

$$N(x_1^6 + x_2^6 = c) = q - 5 + (-1)^{k-1}\left(\frac{3u+r}{2^{k-1}} + 12a\right).$$

From (3.1), we have

$$N(x_1^6 + x_2^6 = g) = q + (-1)^{k-1}\left(\sum_{1\le i\le 5} \lambda^{2i}(g) J(\chi^i,\chi^i)^k + 2\sum_{1\le i<j\le 5} \lambda^{i+j}(g) J(\chi^i,\chi^j)^k\right). \tag{3.5}$$

Noting that $\lambda(g) = \frac{1+i\sqrt{3}}{2}$ and $\lambda^6(g) = 1$, then from Table 1 of Lemma 2.4, we deduce that

$$\begin{aligned} \sum_{1\le i\le 5} \lambda^{2i}(g) J(\chi^i,\chi^i) &= \tfrac{-1+i\sqrt{3}}{2}\left((\tfrac{u'+iv'\sqrt{3}}{2})^k + (\tfrac{r'-is'\sqrt{3}}{2})^k\right) \\ &\quad - \tfrac{1+i\sqrt{3}}{2}\left((\tfrac{r'+is'\sqrt{3}}{2})^k + (\tfrac{u'-iv'\sqrt{3}}{2})^k\right) + (-1)^k \\ &= \tfrac{-1+i\sqrt{3}}{2^{k+1}}(u + iv\sqrt{3} + r - is\sqrt{3}) \\ &\quad - \tfrac{1+i\sqrt{3}}{2^{k+1}}(r + is\sqrt{3} + u - iv\sqrt{3}) + (-1)^k \\ &= \tfrac{3s-3v-r-u}{2^k} + (-1)^k, \end{aligned} \tag{3.6}$$

and

$$2\sum_{1\le i<j\le 5} \chi^{i+j}(g) J(\chi^i,\chi^j) = -4a + 12b + \frac{u+3v}{2^{k-1}} + 4(-1)^k. \tag{3.7}$$

Thus if $\mathrm{ind}_g c \equiv 1 (\mathrm{mod}\ 6)$, from (3.5)–(3.7), one can deduce that

$$N(x_1^6 + x_2^6 = c) = q - 5 + (-1)^k\left(\frac{r-u-3s-3v}{2^k} + 4a - 12b\right).$$

In the similar way, one can deduce that

$$N(x_1^6 + x_2^6 = c) = \begin{cases} q - 5 + (\frac{-1}{2})^k(3u + 3s + r - 9v), & \text{if } \mathrm{ind}_g c \equiv 2 (\mathrm{mod}\ 6), \\ q - 5 + (-1)^k(\frac{u-r}{2^{k-1}} + 4a), & \text{if } \mathrm{ind}_g c \equiv 3 (\mathrm{mod}\ 6), \\ q - 5 + (\frac{-1}{2})^k(9v + 3u + r - 3s), & \text{if } \mathrm{ind}_g c \equiv 4 (\mathrm{mod}\ 6), \\ q - 5 + (-1)^k(\frac{3v-u+r+3s}{2^k} + 4a + 12b), & \text{if } \mathrm{ind}_g c \equiv 5 (\mathrm{mod}\ 6). \end{cases}$$

The case when both t and k are odd can also be proved by the same argument. □

Remark. (Reduction formula for Jacobi sums) [6] Let $\chi_1, \cdots, \chi_k$ be k nontrivial multiplicative characters of $\mathbb{F}_q$. If $k \geq 2$, then

$$J(\chi_1, \cdots, \chi_k) = \begin{cases} -qJ(\chi_1, \cdots, \chi_{k-1}), & \text{if } \chi_1 \cdots \chi_{k-1} \text{ is trivial,} \\ J(\chi_1 \cdots \chi_{k-1}, \chi_k)J(\chi_1, \cdots, \chi_{k-1}), & \text{if } \chi_1 \cdots \chi_{k-1} \text{ is nontrivial.} \end{cases}$$

One can use the reduction formula for Jacobi sums to give an explicit formula for the number of solutions of the diagonal sextic equation

$$x_1^6 + x_2^6 + \cdots + x_n^6 = c$$

of $n \geq 3$ variables over $\mathbb{F}_{p^k}$, with $c \in \mathbb{F}_{p^k}^*$ and $p \equiv 1 (\mathrm{mod}\ 6)$. But we omit the tedious details here.

By concluding this section, we present an example to demonstrate the validity of Theorem 1.4.

Example. Let $q = 19^3$. We consider the numbers of solutions of the sextic equation

$$x_1^6 + x_2^6 = c$$

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

Since 2 is a primitive root modulo 19, we have $Z = \mathrm{ind}_2 2 = 1$. Let g be a generator of $\mathbb{F}_{19^3}^*$ such that

$$\mathbb{N}(g) = g^{\frac{19^3-1}{19-1}} = 2.$$

That means

$$g^{\frac{19^3-1}{3}} = (g^{\frac{19^3-1}{19-1}})^{\frac{19-1}{3}} = 2^6.$$

The integers a' and b' are determined by

$$a'^2 + 3b'^2 = 19, \quad a' \equiv -1 (\mathrm{mod}\ 3) \ \text{ and } \ 3b' \equiv 15a' (\mathrm{mod}\ 19).$$

We can get that $a' = -4$, $b' = -1$. Since $Z \equiv 1 (\mathrm{mod}\ 3)$, we obtain that $r' = 7$, $s' = -3$, $u' = 1$ and $v' = 5$. Thus we have $a = -28$, $b = -45$, $r = -224$, $s = -360$, $u = -224$ and $v = -360$. By Theorem 1.4, one can get that

$$N(x_1^6 + x_2^6 = c) = \begin{cases} 6636, & \text{if } \mathrm{ind}_g c \equiv 0 (\mathrm{mod}\ 6), \\ 6264, & \text{if } \mathrm{ind}_g c \equiv 1 (\mathrm{mod}\ 6), \\ 6264, & \text{if } \mathrm{ind}_g c \equiv 2 (\mathrm{mod}\ 6), \\ 7308, & \text{if } \mathrm{ind}_g c \equiv 3 (\mathrm{mod}\ 6), \\ 7344, & \text{if } \mathrm{ind}_g c \equiv 4 (\mathrm{mod}\ 6), \\ 7344, & \text{if } \mathrm{ind}_g c \equiv 5 (\mathrm{mod}\ 6). \end{cases}$$

4. Conlusions

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 formula for the number of solutions of the two-variable diagonal sextic equations $x_1^6 + x_2^6 = c$ over $\mathbb{F}_q$, with $c \in \mathbb{F}_q^*$ and $p \equiv 1 (\mathrm{mod}\ 6)$, where p is the characteristic of $\mathbb{F}_q$. Furthermore, by using the reduction formula for Jacobi sums, the number of solutions of the diagonal sextic equations $x_1^6 + x_2^6 + \cdots + x_n^6 = c$ of $n \geq 3$ variables with $c \in \mathbb{F}_q^*$ and $p \equiv 1 (\mathrm{mod}\ 6)$, 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

1. J. Ax, Zeros of polynomials over finite fields, *Amer. J. Math.*, **86** (1964), 255–261. http://dx.doi.org/10.2307/2373163
2. I. Baoulina, On the number of solutions of the equation $a_1x_1^{m_1} + \cdots + a_nx_n^{m_n} = bx_1 \cdots x_n$ in a finite field, *Acta Appl. Math.*, **89** (2005), 35–39. http://dx.doi.org/10.1007/s10440-004-5583-7
3. I. Baoulina, Generalizations of the Markoff-Hurwitz equations over finite fields, *J. Number Theory*, **118** (2006), 31–52. http://dx.doi.org/10.1016/j.jnt.2005.08.009
4. I. Baoulina, On the equation $(x_1^{m_1} + \cdots + x_n^{m_n})^k = ax_1 \cdots x_n$ over a finite field, *Finite Fields Appl.*, **13** (2007), 887–895. http://dx.doi.org/10.1016/j.ffa.2006.09.011
5. I. Baoulina, Solutions of equations over finite fields: Enumeration via bijections, *J. Algebra Appl.*, **15** (2016), 1650136. http://dx.doi.org/10.1142/S021949881650136X
6. B. Berndt, R. Evans, K. Williams, *Gauss and Jacobi sums*, Wiley-Interscience, New York, 1998.
7. W. Cao, On generalized Markoff-Hurwitz-type equations over finite fields, *Acta Appl. Math.*, **112** (2010), 275–281. http://dx.doi.org/10.1007/s10440-010-9568-4
8. W. Cao, Q. Sun, On a class of equations with special degrees over finite fields, *Acta Arith.*, **130** (2007), 195–202. http://dx.doi.org/10.4064/aa130-2-8
9. S. Chowla, J. Cowles, M. Cowles, On the number of zeros of diagonal cubic forms, *J. Number Theory*, **9** (1977), 502–506. http://dx.doi.org/10.1016/0022-314X(77)90010-5

10. 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://dx.doi.org/10.1016/j.jnt.2015.04.006

11. 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://dx.doi.org/10.1142/S1005386717000475

12. L. K. Hua, H. S. Vandiver, On the number of solutions of some trinomial equations in a finite field, *PNAS*, **35** (1949), 477–581. http://dx.doi.org/10.1073/pnas.35.8.477

13. K. Ireland, M. Rosen, *A classical introduction to modern number theory*, 2 Eds., Springer-Verlag, New York, 1990.

14. R. Lidl, H. Niederreiter, *Finite fields*, 2 Eds., Cambridge University Press, Cambridge, 1997.

15. G. Myerson, On the number of zeros of diagonal cubic forms, *J. Number Theory*, **11** (1979), 95–99. http://dx.doi.org/10.1016/0022-314X(79)90023-4

16. C. Small, *Arithmetic of finite fields*, Marcel Dekker, New York, 1991.

17. A. Weil, Number of solutions of equations in finite field, *Bull. Amer. Math. Soc.*, **55** (1949), 497–508. http://dx.doi.org/10.1090/S0002-9904-1949-09219-4

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

19. W. Zhang, J. Hu, The number of solutions of the diagonal cubic congruence equation mod p, *Math. Rep.*, **20** (2018), 73–80.

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

21. J. Zhang, D. Wan, Complete symmetric polynomials over finite fields have many rational zeros, *Sci. Sin. Math.*, **51** (2021), 1677–1684. http://dx.doi.org/10.1360/ssm-2020-0328

22. 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://dx.doi.org/10.3934/math.2020175

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

AIMS Press