Note on the Number of Solutions of Cubic Diagonal Equations over Finite Fields

HU Shuangnian¹, WANG Shihan², LI Yanyan³, NIU Yujun¹
1. School of Mathematics and Physics, Nanyang Institute of Technology, Nanyang 473004, Henan, China;
2. Faculty of Science and Technology, Beijing Normal University-Hong Kong Baptist University United International College, Zhuhai 519087, Guangdong, China;
3. School of Information Engineering, Nanyang Institute of Technology, Nanyang 473004, Henan, China

© Wuhan University 2023

Abstract: Let $F_q$ be the finite field, $q=p^k$, with $p$ being a prime and $k$ being a positive integer. Let $F_q^*$ be the multiplicative group of $F_q$, that is $F_q^*=F_q\setminus\{0\}$. In this paper, by using the Jacobi sums and an analog of Hasse-Davenport theorem, an explicit formula for the number of solutions of cubic diagonal equation $x_1^3+x_2^3+\cdots+x_n^3=c$ over $F_q$ is given, where $c\in F_q^*$ and $p=1\pmod{3}$. This extends earlier results.

Key words: finite field; rational point; diagonal equations; Jacobi sums

CLC number: O156

0 Introduction

Let $F_q$ be the finite field, $q=p^k$, with $p$ being a prime and $k$ being a positive integer. Let $F_q^*$ be the multiplicative group of $F_q$, that is $F_q^*=F_q\setminus\{0\}$. Counting the number $N(f=0)$ of zeros $(x_1,x_2,\cdots,x_n)\in F_q^*$ of the equation $f(x_1,x_2,\cdots,x_n)=0$ is an important and fundamental topic in number theory and finite field. From Refs. [1,2], we know that there exists an explicit formula for $N(f=0)$ with degree $\deg f\leq 2$. But generally speaking, it is much difficult to give an explicit formula for $N(f=0)$.

Let $k_1,k_2,\cdots,k_n$ be positive integers. A diagonal equation is an equation of the form $a_1x_1^k+\cdots+a_nx_n^k=c$ with coefficients $a_1,\cdots,a_n\in F_q^*$ and $c\in F_q^*$. Counting the number of solutions $(x_1,x_2,\cdots,x_n)\in F_q^*$ of the diagonal equation is a difficult problem. The special case where all the $k_i$ are equal has extensively been studied (see, for instance, Refs. [3-14]). This is the example chosen by Weil[10] to illustrate his renowned conjecture on projective varieties over finite fields.

For any $c\in F_q^*$, let $A_c(0)$ denote the number of zeros $(x_1,x_2,\cdots,x_n)\in F_q^*$ of the following diagonal equation $x_1^k+\cdots+x_n^k=c$ over $F_q$. In 1977, Chowla et al.[10] initiated the investigation of $A_c(0)$ over $F_q$. When $q=p$, it is easy to see that $A_c(0)=p^{k-1}a_1^k$ if $p\not\equiv 2\pmod{3}$. However, when $p=1\pmod{3}$, the situation becomes complicated.
Chowla et al. got that the generating function \( \sum_{n=1}^{\infty} A_n(0)x^n \) is a rational function of \( x \). In 1979, Myerson extended the result in Ref. [3] to the field \( F_q \). When \( q = p^r \), with \( p^r = -1 \) (mod \( d \)) for a divisor \( r \) of \( t \) and \( d|q-1 \), Wolfmann gave an explicit formula of the number of solutions of the equation \( a_1x_1^n + a_2x_2^n + \cdots + a_dx_d^n = c \) over \( F_q \) in 1992, where \( a_1, \ldots, a_d \in F_q^* \) and \( c \in F_q^* \). In 2018, Zhang and Hu determined the number of solutions of the equation \( a_1x_1^n + a_2x_2^n + \cdots + a_dx_d^n = c \) over \( F_{p^m} \) with \( c \in F_{p^m}^* \) and \( p = 1 \) (mod 3). In 2021, by using the generator of \( F_{p^m}^* \), Hong and Zhu gave the generating functions \( \sum_{n=1}^{\infty} A_n(0)x^n \). In 2022, Ge et al. studied the generating functions in a different way.

In this paper, we consider the problem of finding the number of solutions of the diagonal cubic equation \( x_1^3 + x_2^3 + \cdots + x_n^3 = c \) over \( F_{p^m} \) where \( q = p^r \) and \( c \in F_{p^m}^* \).

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

\[
N(x_1^3 + x_2^3 + \cdots + x_n^3 = c) = N(x_1 + x_2 + \cdots + x_n = c) = q^n-1
\]

with \( c \in F_{p^m}^* \).

If \( p = 2 \) (mod 3) and \( k \) is an even integer, Hu and Feng presented an explicit formula for \( N(x_1^3 + x_2^3 + \cdots + x_n^3 = c) \) by using the Theorem 1 of Ref. [11]. However, the explicit formula for \( N(x_1^3 + x_2^3 + \cdots + x_n^3 = c) \) is still unknown when \( p = 1 \) (mod 3) and \( c \in F_{p^m}^* \). In this paper, we solve this problem by using Jacobi sums and an analog of Hasse-Davenport theorem.

The main result of this paper can be stated as follows.

**Theorem 1** Let \( k \) be a positive integer and \( q = p^r \) with the prime \( p = 1 \) (mod 3). Let \( \chi \) (resp. \( \alpha \)) be a generator of \( F_q^* \) (resp. \( F_p^* \)). Let \( \lambda \) (resp. \( \chi^j \)) be a multiplicative character of order 3 over \( F_q \) (resp. \( F_p \)) given by \( \lambda(a) = -1 + i\sqrt{3} \) (resp. \( \chi(a) = -1 + i\sqrt{3} / 2 \)). Let \( u \) and \( v \) be the integers uniquely determined by

\[
u^3 + 3v^3 = p, \quad u = -1 \text{ (mod 3)}
\]

and

\[
3v \equiv 2u(2\alpha^{u-3} + 1) \text{ (mod } p)\]

Set

\[
\pi = \chi(2(u + iv\sqrt{3})), \quad \bar{\pi} = \chi^2(2(u - iv\sqrt{3})
\]

Let \( N \) denote the number of rational points of \( x_1^n + x_2^n + \cdots + x_n^n = c \) over \( F_q \). Then

\[
N = q^{n-1} - (-1)^{k-1}q^{-3}(E_1 + E_2 + E_3)
\]

where

\[
E_1 = (-1)^k \sum_{j=0}^{n-1} \pi^{a^{j+3} \bar{\pi}^{j-3}} \sum_{j=0}^{n-1} \pi^{a^{j+3} \bar{\pi}^{j-3}}(n, j)
\]

and

\[
E_2 = \lambda(c) \sum_{j=0}^{n-1} \pi^{a^{j+3} \bar{\pi}^{j-3}} \sum_{j=0}^{n-1} \pi^{a^{j+3} \bar{\pi}^{j-3}}(n, j)
\]

This paper is organized as follows. In Section 1, we present several basic concepts and give some preliminary lemmas. In Section 2, we prove Theorem 1. In Section 3, we supply an example to illustrate the validity of our result.

## 1 Preliminary Lemmas

In this section, we present some useful lemmas that are needed in the proof of Theorem 1. We begin with two definitions.

**Definition 1** Let \( p \) be a prime number and \( q = p^r \) with \( k \) being a positive integer. For any element \( a \in F_q \), the norm of \( a \) relative to \( F_p \) is defined by

\[
N_{F_q/F_p}(a) = a\alpha^r \alpha^{-r} = a^{p-1}
\]

For the simplicity, we write \( N(a) \) for \( N_{F_q/F_p}(a) \). For any \( a \in F_{p^m}^* \), it is clear that \( N(a) \in F_{p^m}^* \). Furthermore, if \( \alpha \) is a primitive element of \( F_{p^m}^* \), then \( N(a) \) is a primitive element of \( F_{p^m}^* \).

**Definition 2** Let \( \lambda_1, \ldots, \lambda_n \) be \( n \) multiplicative characters of \( F_p^* \). The Jacobi sum \( J(\lambda_1, \ldots, \lambda_n) \) is defined by

\[
J(\lambda_1, \ldots, \lambda_n) = \sum_{\gamma_1 \cdots \gamma_n} \lambda_1(\gamma_1) \cdots \lambda_n(\gamma_n)
\]

where the summation is taken over all \( n \)-tuples \( (\gamma_1, \ldots, \gamma_n) \) of elements of \( F_p^* \) with \( \gamma_1 + \cdots + \gamma_n = 1 \).

Let \( \chi \) be a multiplicative character of \( F_q^* \). Then \( \gamma \) can be lifted to a multiplicative character \( \lambda \) of \( F_q^* \) by setting \( \lambda(a) = \chi(N(a)) \). The characters of \( F_q^* \) can be lifted to the characters of \( F_{p^m}^* \), but not all the characters of \( F_q^* \) can be obtained by lifting a character of \( F_{p^m}^* \). The following lemma tells us when \( p = 1 \) (mod 3), then any multiplica-
tive character $\lambda$ of order 3 of $F_q$ can be lifted by a multiplicative character of order 3 of $F_p$.

**Lemma 1**[1] Let $F_p$ be a finite field and $F_q$ be an extension of $F_p$. A multiplicative character $\lambda$ of $F_q$ can be lifted by a multiplicative character $\chi$ of $F_p$ if and only if $\lambda^{q-1}$ is trivial.

The following lemma provides an important relationship between the Jacobi sums in $F_q$ and the Jacobi sums in $F_p$.

**Lemma 2**[2] Let $\chi_i, \cdots, \chi_s$ be $n$ multiplicative characters of $F_p$, 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 $F_p$ with $[E:F_p] = k$. Then

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

**Lemma 3**[3] Let $p \equiv 1(\text{mod } 3)$ be a prime and let $\alpha$ be a generator of $F_p'$. Let $\chi$ be a multiplicative character of order 3 over $F_p$ given by $\chi(N(a)) = -1 + i \sqrt{3} / 2$.

Let $n_1$ and $n_2$ be nonnegative integers with $n_1 + n_2 \geq 1$. Set

$$J_{n_1,n_2} = J(\chi, \cdots, \chi, \chi, \cdots, \chi).$$

Then

$$J_{n_1,n_2} = \begin{cases} -\pi^{2(n_1 + n_2 - 3)b} \pi(n_1 + 2n_2 - 3b), & \text{if } n_1 + 2n_2 \equiv 0(\text{mod } 3), \\ \pi^{2(n_1 + n_2 - 2b)(n_1 + 2n_2 - 3b)}, & \text{if } n_1 + 2n_2 \equiv 1(\text{mod } 3), \\ \pi^{2(n_1 + n_2 - b)(n_1 + 2n_2 - 2b)}, & \text{if } n_1 + 2n_2 \equiv 2(\text{mod } 3), \end{cases}$$

where $\pi$ and $\bar{\pi}$ are defined as in Theorem 1.

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

**Lemma 4**[4] Let $k_1, \cdots, k_s$ be positive integers, $a_1, \cdots, a_s, c \in F_p'$. Set $d_i = \gcd(k_i, q - 1)$, and let $\lambda$ be a multiplicative character on $F_q$, of order $d_i$ for $i = 1, \cdots, s$. The number $N$ of solutions of the equation $a_1x_1^d + \cdots + a_sx_s^d = c$ is given by

$$N = q^{-1} + \sum_{j=1}^{d_i - 1} \lambda_j(c)J_{n_i,n_i} \left( \frac{n}{n_1} \right).$$

2 Proof of Theorem 1

In this section, we give the proof of Theorem 1. 

**Proof of Theorem 1** Let $\lambda$ be a multiplicative character on $F_q$ of order 3 with $\lambda(a) = -1 + i \sqrt{3} / 3$. Since $c \in F_q$, by using Lemma 3, we deduce that the number $N$ of solutions $x_1^3 + x_2^3 + \cdots + x_s^3 = c$ in $F_q$ is given by

$$N = q^{-1} + \sum_{j=1}^{d_i - 1} \lambda_j(c)J_{n_i,n_i} \left( \frac{n}{n_1} \right).$$

For integers $0 \leq n_1 \leq n$, $0 \leq n_2 \leq n$ and $n_1 + n_2 = n$, we need to calculate the sum over $j_1, \cdots, j_s$ with $n_1$ of the $j_i$'s equal to 1 and $n_2$ of the $j_i$'s equal to 2. That is

$$j_1 + j_2 + \cdots + j_n = n_1 + 2n_2$$

and

$$J(\lambda_1, \cdots, \lambda_s) = J(\lambda_1, \cdots, \lambda_s, \lambda_1^2, \cdots, \lambda_s^2).$$

Since $\lambda$ is a multiplicative character on $F_q$ of order 3 and $p \equiv 1(\text{mod } 3)$, thus $\lambda^{q-1}$ is trivial. Then from Lemma 1, we can deduce that the cubic multiplicative character $\lambda$ of $F_q$ can be lifted by a cubic multiplicative character $\chi$ of $F_p$. By using Lemma 2 and Lemma 3, one get

$$J(\lambda, \lambda, \lambda, \lambda, \lambda) = (-1)^{k-1} J(\chi, \cdots, \chi, \chi, \cdots, \chi)^k.$$ 

So that

$$N = q^{r-1} + (-1)^{k-1} \sum_{n_1,n_2} \lambda^{n_1+2n_2}(c)J_{n_i,n_i} \left( \frac{n}{n_1} \right).$$

Using Lemma 3 for the value of $J_{n_i,n_i}$, considering the three cases $n_1 + 2n_2 = 0, 1, 2(\text{mod } 3)$ separately, we obtain

$$\sum_{n_1,n_2} \lambda^{n_1+2n_2}(c)J_{n_i,n_i} \left( \frac{n}{n_1} \right) = \sum_{n_1,n_2} (-1)^{k} \pi^{4(n_1 + n_2 - 2b)} \pi^{4(n_1 + 2n_2 - 3b)} \left( \frac{n}{n_1} \right) = E_1,$$

and

$$\sum_{n_1,n_2} \lambda^{n_1+2n_2}(c)J_{n_i,n_i} \left( \frac{n}{n_1} \right) = \sum_{n_1,n_2} \pi^{4(n_1 + n_2 - 2b)} \pi^{4(n_1 + 2n_2 - 3b)} \left( \frac{n}{n_1} \right) = E_2.$$ 

Then the desired result

$$N = q^{r-1} + (-1)^{k-1}(E_1 + E_2 + E_3)$$

follows immediately.
3 Example

In this section, we present an example to demonstrate the validity of our result Theorem 1.

**Example 1** Let \( \alpha \) be a generator of \( F_7^* \). Now we use Theorem 1 to obtain the number of zeros of the cubic equation:

\[
x_1^3 + x_2^3 + x_3^3 + x_4^3 = \alpha.
\]

It is easy to see that \( 3 \) is a generator of \( F_7^* \), and then we obtain \( N(\alpha) = \alpha^{(7^2 - 7 - 1)} = 3 \). That means

\[
\alpha^{(7^2 - 7 - 1)} = (\alpha^{(7^2 - 7 - 1)})^2 = 3^2.
\]

Since \( 3 \equiv 2 \pmod{7} \), then the integers \( u \) and \( v \) are determined by \( u^2 + 3v^2 = 7 \), \( u = -1 \pmod{3} \) and \( 3v = u(2 \cdot 3^2 + 1) \pmod{7} \), that is

\[
u = 2, \quad v = 1.
\]

Thus

\[
\pi = \chi(2)(u + iv\sqrt{3}) = \chi(3^2)(u + iv\sqrt{3}) = \left(\frac{-1 + i\sqrt{3}}{2}\right)(2 + i\sqrt{3}) = \frac{1 - i3\sqrt{3}}{2}
\]

and

\[
\hat{\pi} = \frac{1 + i3\sqrt{3}}{2}.
\]

Further,

\[
E_1 = (-1)^3 \sum_{j \equiv 1 \pmod{3}} \pi^{2j + 4 - 23\beta} \frac{4}{j} = 6\pi\hat{\pi} = 294,
\]

\[
E_2 = \lambda(\alpha) \sum_{j \equiv 1 \pmod{3}} \pi^{2j + 4 - 23\beta} \frac{4}{j} = \lambda(\alpha)(4\pi^2\hat{\pi}^4 + \pi^2\hat{\pi}^2)
\]

\[
= \frac{931 - 11813\sqrt{3}}{2},
\]

and

\[
E_3 = \lambda(\alpha^2) \sum_{j \equiv 1 \pmod{3}} \pi^{2j + 4 - 23\beta} \frac{4}{j} = \lambda(\alpha^2)(\pi^2\hat{\pi}^4 + 4\pi\hat{\pi}^2)
\]

\[
= \frac{931 + 11813\sqrt{3}}{2}.
\]

Thus by Theorem 1, we get

\[
N(x_1^3 + x_2^3 + x_3^3 + x_4^3 = \alpha) = q^3 - (E_1 + E_2 + E_3) = 116424.
\]

References


