The number of solutions of diagonal cubic equations over finite fields

Wenxu Ge*

School of Mathematics and Statistics, North China University of Water Resources and Electric Power, Zhengzhou 450046, P.R.China

Weiping Li

School of Mathematics and Information Sciences, Henan University of Economics and Law, Zhengzhou, 450046, P.R.China

Tianze Wang

School of Mathematics and Statistics, North China University of Water Resources and Electric Power, Zhengzhou, 450046, P.R.China

Abstract

Let \mathbb{F}_q be a finite field of $q = p^k$ elements. For any $z \in \mathbb{F}_q$, let $A_n(z)$ and $B_n(z)$ denote the number of solutions of the equations $x_1^3 + x_2^3 + \cdots + x_n^3 = z$ and $x_1^3 + x_2^3 + \cdots + x_n^3 + zx_{n+1}^3 = 0$ respectively. Recently, using the generator of \mathbb{F}_q^* , Hong and Zhu gave the generating functions $\sum_{n=1}^{\infty} A_n(z)x^n$ and $\sum_{n=1}^{\infty} B_n(z)x^n$. In this paper, we give the generating functions $\sum_{n=1}^{\infty} A_n(z)x^n$ and $\sum_{n=1}^{\infty} B_n(z)x^n$ immediately by the coefficient z. Moreover, we gave the formulas of the number of solutions of equation $a_1x_1^3 + a_2x_2^3 + a_3x_3^3 = 0$ and our formulas are immediately determined by the coefficients a_1, a_2 and a_3 . These extend and improve earlier results.

Keywords: Gauss sum, Jacobi sum, generating function, diagonal cubic equation, exponential sum 2000 MSC: 11T23, 11T24

^{*}Corresponding author

Email addresses: gewenxu@ncwu.edu.cn (Wenxu Ge), wpliyh@163.com (Weiping Li), wtz@ncwu.edu.cn (Tianze Wang)

1. Introduction

Let \mathbb{F}_q be a finite field of $q = p^k$ elements. Let \mathbb{F}_q^* be the multiplicative group of \mathbb{F}_q , i.s. $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. Counting the number of solutions $(x_1, x_2, \cdots, x_n) \in \mathbb{F}_q^n$ of the general diagonal equation

$$a_1 x_1^{d_1} + a_2 x_2^{d_2} + \dots + a_n x_n^{d_n} = b$$

over \mathbb{F}_q is an important and fundamental problem in number theory and finite field. The special case where all the d_i are equal has extensively been studied by many authors (see, for example, [6, 8, 9, 11, 12, 13]).

For any $z \in \mathbb{F}_q$, one lets $A_n(z)$ denote the number of solutions of the following diagonal equation

$$x_1^3 + x_2^3 + \dots + x_n^3 = z$$

over \mathbb{F}_q . When $q = p \equiv 1 \pmod{3}$, Chowla, Cowles and Cowles [2] gave the generating function $\sum_{n=0}^{\infty} A_n(0)x^n$. Myerson [9] extended the Chowla, Cowles and Cowles's result to finite field \mathbb{F}_q . He proved the following result.

Theorem 1.1 ([9]). Let \mathbb{F}_q be a finite field of $q = p^k$ elements with $q \equiv 1 \pmod{3}$. Then

$$\sum_{n=1}^{\infty} A_n(0)x^n = \frac{x}{1-qx} + \frac{(q-1)(2+cx)x^2}{1-3qx^2-qcx^3},$$

where c is uniquely determined by

$$4q = c^2 + 27d^2, c \equiv 1 \pmod{3}$$
 and if $p \equiv 1 \pmod{3}$, then $(c, p) = 1$. (1.1)

Recently, Hong and Zhu [5] consider $A_n(z)$ in finite field \mathbb{F}_q , they proved the following result.

Theorem 1.2 ([5]). Let $z \in \mathbb{F}_q^* = \langle g \rangle$ and $q = p^k \equiv 1 \pmod{3}$ with k being a positive integer. Then

$$\sum_{s=1}^{\infty} A_s(z)x^s = \frac{x}{1-qx} + \frac{2x + (c-2)x^2 - cx^3}{1-3qx^2 - qcx^3}$$

if z is cubic, where c is uniquely determined by (1.1), and

$$\sum_{s=1}^{\infty} A_s(z)x^s = \frac{x}{1-qx} - \frac{x + \frac{1}{2}(4+c+9d\delta_z(d))x^2 + cx^3}{1-3qx^2 - qcx^3}$$

if z is non-cubic, where c and d are uniquely determined by (1.1) with d > 0and

$$\delta_z(q) = \begin{cases} (-1)^{\langle ind_g(d) \rangle_3} \cdot sgn\left(\operatorname{Im}(r_1 + 3\sqrt{3}r_2 \mathbf{i})^k\right), & \text{if } k \equiv 1 \pmod{2}; \\ 0, & \text{if } k \equiv 0 \pmod{2}. \end{cases}$$
(1.2)

where r_1 and r_2 are uniquely determined by

$$4p = r_1^2 + 27r_2^2$$
, $r_1 \equiv 1 \pmod{3}$, $9r_2 \equiv (2N_{\mathbb{F}_q/\mathbb{F}_p}(g)^{\frac{p-1}{3}} + 1)r_1 \pmod{p}$.

Suppose that $z \in \mathbb{F}_q^*$ be non-cubic. Let $B_n(z)$ be the number of solutions of diagonal cubic equation

$$x_1^3 + x_2^3 + \dots + x_n^3 + zx_{n+1}^3 = 0$$

over \mathbb{F}_q . In [5], Hong and Zhu also consider $B_n(z)$. They showed the following result.

Theorem 1.3 ([5]). Let $z \in \mathbb{F}_q^*$ be non-cubic and $q = p^k \equiv 1 \pmod{3}$ with k being a positive integer. Then

$$\sum_{s=1}^{\infty} B_s(z) x^s = \frac{qx}{1-qx} - \frac{(q-1)x + \frac{1}{2}(q-1)(c-9d)x^2}{1-3qx^2 - qcx^3},$$

where c and d are uniquely determined by (1.1) with d > 0 and $\delta_z(q)$ is given as in (1.2).

Indeed, The key of these problems is to determine the sign of d. In Hong and Zhu's results, they use the generator of group \mathbb{F}_q^* to determine the sign of d. However, for a large prime p, it is not easy to find a generator of group \mathbb{F}_q^* . In this paper, by calculating the Jacobi sum of finite field, we determine the sign of d immediately by the coefficient z. We give the following two results.

Theorem 1.4. Let \mathbb{F}_q be a finite field of $q = p^k$ elements with $q \equiv 1 \pmod{3}$. Then

$$\sum_{n=1}^{\infty} A_n(z)x^n = \frac{x}{1-qx} + \frac{2x + (c-2)x^2 - cx^3}{1 - 3qx^2 - qcx^3}$$

if z is cubic, and

$$\sum_{n=1}^{\infty} A_n(z)x^n = \frac{x}{1-qx} - \frac{x + \frac{1}{2}(4+c-9d)x^2 + cx^3}{1-3qx^2 - qcx^3}$$

if z is non-cubic, where c and d are uniquely determined by

$$4q = c^2 + 27d^2, c \equiv 1 \pmod{3}, (c, p) = 1, 9d \equiv c(2z^{\frac{q-1}{3}} + 1) \pmod{p}.$$
 (1.3)

Theorem 1.5. Let \mathbb{F}_q be a finite field of $q = p^k$ elements with $q \equiv 1 \pmod{3}$ and $z \in \mathbb{F}_q^*$ be non-cubic. Then we have

$$\sum_{n=0}^{\infty} B_n(z)x^n = \frac{1}{1-qx} - \frac{(q-1)x + \frac{1}{2}(q-1)(c-9d)x^2}{1-3qx^2 - qcx^3},$$

where c and d are uniquely determined by (1.3).

Remark 1.6. When $q \equiv 2 \pmod{3}$, it is known that every element is a cube, so $N_n(z) = q^{n-1}$. If $q \equiv 1 \pmod{3}$ with $p \equiv 2 \pmod{3}$, then Wolfmann [14] gave a formula for $N_n(z)$. By Theorem 16 of [10], we have

$$c = \begin{cases} -2p^{k/2}, & \text{if } k \equiv 0 \pmod{4}; \\ 2p^{k/2}, & \text{if } k \equiv 2 \pmod{4}, \end{cases}$$

and d = 0. Then for this case, Theorem 1.4 and 1.5 immediately follow from Theorem 1.2 and 1.3. So in the rest of this paper, we focus on the case $q \equiv 1 \pmod{3}$ with $p \equiv 1 \pmod{3}$.

For $a_1, a_2, a_3 \in \mathbb{F}_q^*$, let $M_k(a_1, a_2, a_3)$ be the number of solutions of

$$a_1x_1^3 + a_2x_2^3 + a_3x_3^3 = 0$$

over \mathbb{F}_q and let $N_k(a_1, a_2, a_3)$ be the number of solutions of

$$a_1 x_1^3 + a_2 x_2^3 = a_3$$

over \mathbb{F}_q . For the case $q = p \equiv 1 \pmod{3}$, Chowla, Cowles and Cowles [2] showed that $M_1(1, 1, 1) = p^2 + c(p-1)$. As pointed out in [3], the following is essentially included in the derivation of the cubic equation of periods by Gauss [4]: Let a prime $p \equiv 1 \pmod{3}$ and z be non-cubic in \mathbb{F}_p . Then one has

$$M_1(1,1,z) = p^2 + \frac{1}{2}(p-1)(9d-c),$$

where c and d are uniquely determined by (1.1) (except for the sign of d).

Chowla, Cowles and Cowles [3] determined the sign of d for the case of 2 being non-cubic in \mathbb{F}_p .

Theorem 1.7 ([3]). Let a prime $p \equiv 1 \pmod{3}$. If 2 is non-cubic in \mathbb{F}_p , then for any non-cubic element z, one has

$$M_1(1,1,z) = p^2 + \frac{1}{2}(p-1)(9d-c)$$

where c and d are uniquely determined by (1.1) with

$$d \equiv c \pmod{4}$$
 if $4z$ is cubic

and

$$d \equiv -c \pmod{4}$$
 if $2z$ is cubic.

In [5], Hong and Zhu solved the Gauss sign problem. In fact, they gave the following result.

Theorem 1.8 ([5]). Let $z \in \mathbb{F}_q^* = \langle g \rangle$ be non-cubic and $q = p^k \equiv 1 \pmod{3}$. Then

$$M_k(1,1,z) = q^2 + \frac{1}{2}(q-1)(-c - 9\delta_z(q)d),$$

where c and d are uniquely determined by (1.1) with d > 0 and $\delta_z(q)$ is given as in (1.2).

In this paper, we consider $M_k(a_1, a_2, a_3)$, $N_k(a_1, a_2, a_3)$ and determine the sign of d immediately by the coefficients a_1, a_2 and a_3 . We have the following more general results.

Theorem 1.9. Let \mathbb{F}_q be a finite field of $q = p^k$ elements with the prime $p \equiv 1 \pmod{3}$, and $a_1, a_2, a_3 \in \mathbb{F}_q^*$. Then

$$M_k(a_1, a_2, a_3) = \begin{cases} q^2 + c(q-1), & \text{if } a_1 a_2 a_3 \text{ is cubic;} \\ q^2 + \frac{1}{2}(q-1)(9d-c), & \text{if } a_1 a_2 a_3 \text{ is non-cubic,} \end{cases}$$

where c and d are uniquely determined by

$$4q = c^{2} + 27d^{2}, c \equiv 1 \pmod{3}, (c, p) = 1, 9d \equiv c(2(a_{1}a_{2}a_{3})^{\frac{q-1}{3}} + 1) \pmod{p}.$$
(1.4)

Theorem 1.10. Let \mathbb{F}_q be a finite field of $q = p^k$ elements with the prime $p \equiv 1 \pmod{3}$, and $a_1, a_2, a_3 \in \mathbb{F}_q^*$.

(1) For the case of $a_1a_2a_3$ being cubic, we have

$$N(a_1, a_2, a_3) = \begin{cases} q - 2 + c, & \text{if } a_1 a_2^{-1} \text{ is cubic;} \\ q + 1 + c, & \text{otherwise.} \end{cases}$$

(2) For the case of $a_1a_2a_3$ being non-cubic, we have

$$N(a_1, a_2, a_3) = \begin{cases} q - 2 + \frac{1}{2}(9d - c), & \text{if } a_1 a_2^{-1} \text{ is cubic,} \\ q + 1 + \frac{1}{2}(9d - c), & \text{otherwise,} \end{cases}$$

where c and d are uniquely determined by (1.4).

2. Auxiliary Lemmas

Lemma 2.1 ([7]). Let \mathbb{F}_q be a finite field. Let χ be a nontrivial multiplicative character of \mathbb{F}_q and ψ be a nontrivial additive character of \mathbb{F}_q . Then for any $a \in \mathbb{F}_q$, we have

$$\sum_{x \in \mathbb{F}_q^*} \chi(x) = 0, \quad \sum_{x \in \mathbb{F}_q} \psi(ax) = \begin{cases} q, & \text{if } a = 0; \\ 0, & \text{if } a \neq 0. \end{cases}$$

For any $a \in \mathbb{F}_q^*$, we defined the sums

$$S(a) = \sum_{x \in \mathbb{F}_q} \psi(ax^3)$$

and

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

where χ is a multiplicative character of \mathbb{F}_q and ψ is an additive character of \mathbb{F}_q . Both S(a) and $G(\chi)$ are called Gauss sums.

Lemma 2.2 ([7]). Let χ be a nontrivial multiplicative character and ψ a nontrivial additive character of \mathbb{F}_q . Then $|G(\chi, \psi)| = \sqrt{q}$ and $G(\chi, \psi)G(\overline{\chi}, \psi) = \chi(-1)q$.

Let \mathbb{F}_q be the finite extension of \mathbb{F}_p with $[\mathbb{F}_q : \mathbb{F}_p] = k$. Recall that the trace $\operatorname{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha)$ and norm $\operatorname{N}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha)$ of $\alpha \in \mathbb{F}_q$ over \mathbb{F}_p are defined by

$$\operatorname{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = \alpha + \alpha^p + \dots + \alpha^{p^{k-1}}$$

and

$$N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = \alpha \times \alpha^p \times \cdots \times \alpha^{p^{k-1}} = \alpha^{\frac{q-1}{p-1}}.$$

Lemma 2.3 (Hasse-Davenport Theorem [7]). Let \mathbb{F}_q be the finite extension of \mathbb{F}_p with $[\mathbb{F}_q : \mathbb{F}_p] = k$. Let χ' be a multiplicative character and ψ' an additive character of \mathbb{F}_p , not both of them trivial. Suppose that χ and ψ are the lifts of χ' and ψ' from \mathbb{F}_p to \mathbb{F}_q , i.e. $\chi = \chi' \circ N_{\mathbb{F}_q/\mathbb{F}_p}$ and $\psi = \psi' \circ \operatorname{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$. Then

$$G(\chi, \psi) = (-1)^{k-1} G^k(\chi', \psi').$$

Lemma 2.4 ([7]). Let \mathbb{F}_q be the finite extension of \mathbb{F}_p . Then a multiplicative character χ of \mathbb{F}_q can be lifted by a multiplicative character χ' of \mathbb{F}_p if and only if χ^{p-1} is trivial.

Let $\chi_1, \chi_2, \dots, \chi_s$ be nontrivial multiplicative characters of \mathbb{F}_q . The Jacobi sum in \mathbb{F}_q is defined by

$$J(\chi_1, \chi_2, \cdots, \chi_s) = \sum_{\substack{(x_1, x_2, \cdots, x_s) \in \mathbb{F}_q^s \\ x_1 + x_2 + \cdots + x_s = 1}} \chi_1(x_1) \chi_2(x_2) \cdots \chi_s(x_s).$$

The following gives a relation between Gauss sun and Jacobi sum.

Lemma 2.5 ([7]). Let $\chi_1, \chi_2, \dots, \chi_s$ be nontrivial multiplicative characters of \mathbb{F}_q with the product $\chi_1\chi_2 \cdots \chi_s$ is nontrivial. Let ψ be a nontrivial additive character of \mathbb{F}_q . Then

$$J(\chi_1, \chi_2, \cdots, \chi_s) = \frac{G(\chi_1, \psi) \cdots G(\chi_s, \psi)}{G(\chi_1 \cdots \chi_s, \psi)}.$$

Lemma 2.6 ([10]). Let \mathbb{F}_q be the finite field of $q = p^k$ elements with the prime $p \equiv 1 \pmod{3}$, and z is non-cubic in \mathbb{F}_q^* , Then S(1), S(z) and $S(z^2)$ are the roots of the cubic equation

$$x^3 - 3qx - qc = 0,$$

where c is uniquely determined by

$$4p = c^2 + 27d^2$$
, $c \equiv 1 \pmod{3}$, $(p, c) = 1$.

Lemma 2.7 (Theorem 3.1.3 of [1]). Let $p \equiv 1 \pmod{3}$ and χ' be a multiplicative character of order 3 over \mathbb{F}_p . Then

$$J(\chi',\chi') = \frac{c_0 + 3\sqrt{3d_0 i}}{2},$$

where c_0 and d_0 are uniquely determined by

$$4p = c_0^2 + 27d_0^2, \quad c_0 \equiv 1 \pmod{3}, \quad 9d_0 \equiv c_0(2g^{\frac{p-1}{3}} + 1) \pmod{p}$$

with g being the generator of the multiplicative group \mathbb{F}_p^* of non-zero residues (mod p) such that $\chi'(g) = \frac{-1+\sqrt{3}i}{2}$.

In the rest of this paper, we let χ be a multiplicative character of order 3 of \mathbb{F}_q and ψ be the canonical additive character which is defined by

$$\psi(x) = e^{2\pi i \operatorname{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)/p}.$$

We denote $\overline{\chi}$ the conjugate character of χ . For convenience, we let $G(\chi) := G(\chi, \psi)$. By Lemma 2.2, we have $G(\chi)G(\overline{\chi}) = \chi(-1)q = q$ and $|G(\chi)| = |G(\overline{\chi})| = \sqrt{q}$. We have the following three results for the Gauss sums of order 3.

Lemma 2.8. Let \mathbb{F}_q be the finite field of $q = p^k$ elements with the prime $p \equiv 1 \pmod{3}$. If z is non-cubic in \mathbb{F}_q^* , then there is a unique multiplicative character χ of order 3 over \mathbb{F}_q such that

$$\chi(z) = \omega, \quad J(\chi, \chi) = \frac{c + 3\sqrt{3}di}{2}, \quad G^3(\chi) = q \cdot \frac{c + 3\sqrt{3}di}{2},$$

where $\omega = \frac{-1+\sqrt{3}i}{2}$, c and d are uniquely determined by

$$4q = c^2 + 27d^2, c \equiv 1 \pmod{3}, (c, p) = 1, 9d \equiv c(2z^{\frac{q-1}{3}} + 1) \pmod{p}.$$

Proof. Let g' be a generator of the multiplicative group \mathbb{F}_q^* . Note that z is non-cubic. So we have $\operatorname{ind}_{g'} z \equiv \pm 1 \pmod{3}$. If $\operatorname{ind}_{g'} z \equiv 1 \pmod{3}$, we take g = g'; If $\operatorname{ind}_{g'} z \equiv -1 \pmod{3}$, we take $g = (g')^{-1}$. Hence g also a generator of the group \mathbb{F}_q^* and $\operatorname{ind}_g z \equiv 1 \pmod{3}$. Thus we have

$$z^{\frac{q-1}{3}} = \left(g^{\mathrm{ind}_g z}\right)^{\frac{q-1}{3}} = g^{\frac{q-1}{3}\mathrm{ind}_g z} = g^{\frac{q-1}{3}}.$$
 (2.1)

We take the multiplicative character $\chi(\cdot) = e\left(\frac{\operatorname{ind}_g(\cdot)}{3}\right)$. Obviously, we have

$$\chi(z) = e\left(\frac{\mathrm{ind}_g z}{3}\right) = \chi(g) = e\left(\frac{1}{3}\right) = \omega.$$

Since $p \equiv 1 \pmod{3}$, then χ^{p-1} is trivial. By Lemma 2.4, the cubic multiplicative character χ can be lifted by a cubic multiplicative character χ' of \mathbb{F}_p^* . It is easy to see that $N_{\mathbb{F}_q/\mathbb{F}_p}(g) = g^{\frac{q-1}{p-1}}$ is a generator of \mathbb{F}_p^* and

$$\chi(g) = \chi'(\mathcal{N}_{\mathbb{F}_q/\mathbb{F}_p}(g)) = \omega.$$

By Lemma 2.7, we have

$$J(\chi',\chi') = \frac{c_0 + 3\sqrt{3d_0 i}}{2},$$

where c_0 and d_0 are uniquely determined by

$$4p = c_0^2 + 27d_0^2, \quad c_0 \equiv 1 \pmod{3}, \quad 9d_0 \equiv c_0(2(N_{\mathbb{F}_q/\mathbb{F}_p}(g))^{\frac{p-1}{3}} + 1) \pmod{p}.$$

By the Davenport-Hasse Theorem (Lemma 2.3) and Lemma 2.5, we have

$$J(\chi,\chi) = (-1)^{k-1} J^k(\chi',\chi')$$

= $(-1)^{k-1} \left(\frac{c_0 + 3\sqrt{3}d_0i}{2}\right)^k := \frac{c + 3\sqrt{3}di}{2}.$ (2.2)

So we have $4q = 4p^k = c^2 + 27d^2$ and

$$c = 2 \cdot (-1)^{k-1} \operatorname{Re}\left(\frac{c_0 + 3\sqrt{3}d_0 \mathbf{i}}{2}\right)^k = 2 \cdot (-1)^{k-1} \operatorname{Re}\left(\frac{c_0 + 3d_0}{2} + 3d_0\omega\right)^k$$
$$\equiv (-1)^k \left(\frac{c_0 + 3d_0}{2}\right)^k \equiv c_0^k \equiv 1 \pmod{3}.$$

Let $K = \mathbb{Q}(\omega)$. Note that $p \equiv 1 \pmod{3}$. By the prime ideal decomposition of cubic cyclotomic field $K = \mathbb{Q}(\omega)$, we have

$$pO_K = \left(\frac{c_0 + 3\sqrt{3}d_0 \mathbf{i}}{2}\right)O_K \cdot \left(\frac{c_0 - 3\sqrt{3}d_0 \mathbf{i}}{2}\right)O_K := P_1 P_2.$$
(2.3)

Thus in $K = \mathbb{Q}(\omega)$, we have the unique decomposition

$$q = \left(\frac{c+3\sqrt{3}d\mathbf{i}}{2}\right) \cdot \left(\frac{c-3\sqrt{3}d\mathbf{i}}{2}\right) = \left(\frac{c_0+3\sqrt{3}d_0\mathbf{i}}{2}\right)^k \cdot \left(\frac{c_0-3\sqrt{3}d_0\mathbf{i}}{2}\right)^k.$$

Then c is uniquely determined by $4q = c^2 + 27d^2, c \equiv 1 \pmod{3}, (c, p) = 1.$

Now we begin to determine the sign of d. Note that O_K/P_j is isomorphic to \mathbb{F}_p for j = 1, 2 and $N_{\mathbb{F}_q/\mathbb{F}_p}(g) + P_j$ is a generator of $(O_K/P_j)^*$. $\left(N_{\mathbb{F}_q/\mathbb{F}_p}(g)\right)^{\frac{p-1}{3}} + P_j$ is a cubic root of unity in O_K/P_j . Then there is one of the prime ideals P_1 and P_2 (rewrite it as P), satisfying

$$\left(N_{\mathbb{F}_q/\mathbb{F}_p}(g)\right)^{\frac{p-1}{3}} \equiv \omega(\operatorname{mod} P).$$

Thus we have

$$g^{\frac{q-1}{3}} \equiv \omega(\mathrm{mod}P). \tag{2.4}$$

Define the multiplicative character χ_P on $(O_K/P)^*$ by

$$\chi_P(N_{\mathbb{F}_q/\mathbb{F}_p}(g) + P) = \omega.$$

Thus we view χ' as the character χ_P on the finite field O_K/P by identifying the generator

$$\chi'(N_{\mathbb{F}_q/\mathbb{F}_p}(g)) = \chi_P(N_{\mathbb{F}_q/\mathbb{F}_p}(g) + P) = \omega.$$

Then we have $J(\chi', \chi') = J(\chi_P, \chi_P)$. By Theorem 2.1.14 of [1], we have $J(\chi_P, \chi_P) \equiv 0 \pmod{P}$. Thus we have

$$J(\chi',\chi') \equiv 0 \pmod{P}.$$

So by (2.2), we have

$$J(\chi, \chi) = \frac{c + 3\sqrt{3}di}{2} = \frac{c + 3d(2\omega + 1)}{2} \equiv 0 \pmod{P}$$

Then $3d(2\omega + 1) \equiv -c \pmod{P}$. Multiplying $-(2\omega + 1)$, by (2.4), we have

$$9d \equiv -3d(2\omega+1)^2 \equiv c(2\omega+1) \equiv c(2g^{\frac{q-1}{3}}+1) \pmod{P}.$$

Hence by (2.1) and (2.3), we have

$$9d \equiv c(2g^{\frac{q-1}{3}} + 1) \equiv c(2z^{\frac{q-1}{3}} + 1)(\text{mod}p).$$

Since χ is a multiplicative character of order 3, by Lemma 2.5, we have

$$G^{3}(\chi) = J(\chi,\chi)G(\chi^{2})G(\chi) = J(\chi,\chi)G(\overline{\chi})G(\chi) = qJ(\chi,\chi)$$

This completes the proof of Lemma 2.8.

Lemma 2.9. Let χ be a multiplicative character of order 3 of \mathbb{F}_q . Then for any $a \in \mathbb{F}_q^*$, we have

$$S(a) = \overline{\chi}(a)G(\chi) + \chi(a)G(\overline{\chi}).$$
(2.5)

Proof. Note that χ be the multiplicative character of order 3. Then we have

$$1 + \chi(k) + \overline{\chi}(k) = \begin{cases} 3, & \text{if } k \text{ is cubic;} \\ 0, & \text{if } k \text{ is non-cubic.} \end{cases}$$

Thus for any $a \in \mathbb{F}_q^*$, we have

$$S(a) = \sum_{k \in \mathbb{F}_q^*} \psi(ak^3) = 1 + \sum_{k \in \mathbb{F}_q^*} (1 + \chi(k) + \overline{\chi}(k))\psi(ak)$$

$$= 1 + \sum_{k \in \mathbb{F}_q^*} \psi(ak) + \sum_{k \in \mathbb{F}_q^*} \chi(k)\psi(ak) + \sum_{k \in \mathbb{F}_q^*} \overline{\chi}(k)\psi(ak)$$

$$= \overline{\chi}(a) \sum_{k \in \mathbb{F}_q^*} \chi(ak)\psi(ak) + \chi(a) \sum_{k \in \mathbb{F}_q^*} \overline{\chi}(ak)\psi(ak)$$

$$= \overline{\chi}(a)G(\chi) + \chi(a)G(\overline{\chi}).$$

Lemma 2.10. Let \mathbb{F}_q be the finite field of $q = p^k$ elements with the prime $p \equiv 1 \pmod{3}$. If z is non-cubic in \mathbb{F}_q^* , then

$$S(1)^{2}S(z) + S(z)^{2}S(z^{2}) + S(z^{2})^{2}S(1) = \frac{3}{2}q(9d - c),$$

where c and d are uniquely determined by (1.3).

Proof. Since $p \equiv 1 \pmod{3}$, the non-zero cubic elements form a multiplicative subgroup H of order $\frac{1}{3}(q-1)$ and index 3 which partitions \mathbb{F}_q^* into three cosets H, zH and z^2H . Then for any $a \in z^jH$, we have $S(a) = S(z^j)$ and $S(az) = S(z^{j+1})$. Thus we have

$$\sum_{a \in \mathbb{F}_q^*} S(a)^2 S(az) = \sum_{a \in H} S(a)^2 S(az) + \sum_{a \in zH} S(a)^2 S(az) + \sum_{a \in zH} S(a)^2 S(az)$$
$$= \frac{1}{3} (q-1) \left(S(1)^2 S(z) + S(z)^2 S(z^2) + S(z^2)^2 S(1) \right). \quad (2.6)$$

On the other hand, by Lemma 2.8, there is a unique multiplicative character χ of order 3 over \mathbb{F}_q such that

$$\chi(z) = \frac{-1 + \sqrt{3}i}{2}, \quad G^3(\chi) = q \cdot \frac{c + 3\sqrt{3}di}{2},$$

where c and d are uniquely determined by (1.3). By Lemmas 2.1 and 2.9, we have

$$\begin{split} &\sum_{a\in\mathbb{F}_q^*} S(a)^2 S(az) \\ &= \sum_{a\in\mathbb{F}_q^*} (\overline{\chi}(a)G(\chi) + \chi(a)G(\overline{\chi}))^2 (\overline{\chi}(az)G(\chi) + \chi(az)G(\overline{\chi})) \\ &= (q-1)\left(\overline{\chi}(z)G^3(\chi) + \chi(z)G^3(\overline{\chi})\right) \\ &= q(q-1)\left(\frac{-1-\sqrt{3}i}{2} \cdot \frac{c+3\sqrt{3}di}{2} + \frac{-1+\sqrt{3}i}{2} \cdot \frac{c-3\sqrt{3}di}{2}\right) \\ &= \frac{1}{2}q(q-1)(9d-c). \end{split}$$
(2.7)

Then Lemma 2.10 immediately follows from (2.6) and (2.7).

3. Proofs of Theorems 1.4 and 1.5

In this section, we prove Theorem 1.4 and 1.5. First, we begin with the proof of Theorem 1.5.

Proof of Theorem 1.5. By Remark 1.6, we only need to consider the case $q \equiv 1 \pmod{3}$ with $p \equiv 1 \pmod{3}$. By Lemma 2.1, we have

$$B_n(z) = \frac{1}{q} \sum_{a \in \mathbb{F}_q} \sum_{\substack{(x_1, x_2, \cdots, x_{n+1}) \in \mathbb{F}_q^{s+1}}} \psi \left(a(x_1^3 + \cdots + x_n^3 + zx_{n+1}^3) \right)$$

= $q^n + \frac{1}{q} \sum_{a \in \mathbb{F}_q^*} (S(a))^n S(az).$

Then

$$\sum_{n=0}^{\infty} B_n(z) x^n = \sum_{n=0}^{\infty} q^n x^n + \frac{1}{q} \sum_{a \in \mathbb{F}_q^*} S(az) \sum_{n=0}^{\infty} (S(a))^n x^n$$
$$= \frac{1}{1-qx} + \frac{1}{q} \sum_{a \in \mathbb{F}_q^*} \frac{S(az)}{1-S(a)x}.$$

Since $p \equiv 1 \pmod{3}$, the non-zero cubic elements form a multiplicative subgroup *H* of order $\frac{1}{3}(q-1)$ and index 3. Then by the proof of Lemma 2.10, we have

$$\begin{split} &\sum_{n=0}^{\infty} B_n(z) x^n \\ &= \frac{1}{1-qx} + \frac{1}{q} \left(\sum_{a \in H} \frac{S(az)}{1-S(a)x} + \sum_{a \in zH} \frac{S(az)}{1-S(a)x} + \sum_{a \in z^2H} \frac{S(az)}{1-S(a)x} \right) \\ &= \frac{1}{1-qx} + \frac{q-1}{3q} \left(\frac{S(z)}{1-S(1)x} + \frac{S(z^2)}{1-S(z)x} + \frac{S(1)}{1-S(z^2)x} \right) \\ &= \frac{1}{1-qx} + \frac{q-1}{3q} \cdot \frac{\alpha - (\alpha^2 - \beta)x + \gamma x^2}{1-\alpha x + \beta x^2 - \delta x^3}, \end{split}$$

Where $\alpha = S(1) + S(z) + S(z^2)$, $\beta = S(1)S(z) + S(z)S(z^2) + S(z^2)S(1)$, $\gamma = S(1)^2S(z) + S(z)^2S(z^2) + S(z^2)^2S(1)$ and $\delta = S(1)S(z)S(z^2)$. By Lemmas 2.6 and 2.10, we have

$$\alpha = 0, \beta = -3q, \gamma = \frac{3}{2}q(9d - c), \delta = qc.$$

Thus we have

$$\sum_{n=0}^{\infty} B_n(z)x^n = \frac{1}{1-qx} + \frac{q-1}{3q} \cdot \frac{-3qx + \frac{3}{2}q(9d-c)x^2}{1-3qx^2 - qcx^3}$$
$$= \frac{1}{1-qx} - \frac{(q-1)x + \frac{1}{2}(q-1)(c-9d)x^2}{1-3qx^2 - qcx^3}.$$

This completes the proof of the Theorem 1.5.

Proof of Theorem 1.4. By the proof of Theorem 1.3 in [5], it is easy to see that

$$B_n(z) = A_n(0) + (q-1)A_n(z).$$

Thus we have

$$A_n(z) = \frac{1}{(q-1)}(B_n(z) - A_n(0)).$$

If z is non-cubic, then by Theorems 1.1 and 1.5, we have

$$\sum_{n=1}^{\infty} A_n(z) x^n = \frac{1}{(q-1)} \left(\sum_{n=1}^{\infty} B_n(z) x^n - \sum_{n=1}^{\infty} A_n(0) x^n \right)$$
$$= \frac{1}{(q-1)} \left(\frac{1}{1-qx} - \frac{(q-1)x + \frac{1}{2}(q-1)(c-9d)x^2}{1-3qx^2 - qcx^3} - B_0(z) \right)$$
$$- \frac{1}{(q-1)} \left(\frac{x}{1-qx} + \frac{(q-1)(2+cx)x^2}{1-3qx^2 - qcx^3} \right)$$
$$= \frac{x}{1-qx} - \frac{x + \frac{1}{2}(4+c-9d)x^2 + cx^3}{1-3qx^2 - qcx^3}.$$

If z is cubic, we have $B_n(z) = A_{n+1}(0)$. By Theorem 1.1, we have

$$\sum_{n=1}^{\infty} A_n(z) x^n = \frac{1}{(q-1)} \left(\sum_{n=1}^{\infty} A_{n+1}(0) x^n - \sum_{n=1}^{\infty} A_n(0) x^n \right)$$
$$= \frac{1}{(q-1)} \left(\frac{1}{x} \sum_{n=1}^{\infty} A_n(0) x^n - A_1(0) - \sum_{n=1}^{\infty} A_n(0) x^n \right)$$
$$= \frac{1}{(q-1)} \left(\frac{1-x}{x} \sum_{n=1}^{\infty} A_n(0) x^n - 1 \right)$$
$$= \frac{x}{1-qx} + \frac{2x + (c-2)x^2 - cx^3}{1-3qx^2 - qcx^3}.$$

This completes the proof of the Theorem 1.4.

4. Proofs of Theorems 1.9 and 1.10 and an example

In this section, we prove Theorem 1.9 and 1.10. First, we begin with the proof of Theorem 1.9.

Proof of Theorem 1.9.

By Lemma 2.1, we have

$$M_k(a_1, a_2, a_3) = \frac{1}{q} \sum_{m \in \mathbb{F}_q} \sum_{(x_1, x_2, x_3) \in \mathbb{F}_q^3} \psi\left(m(a_1 x_1^3 + a_2 x_2^3 + a_3 x_3^3)\right)$$
$$= q^2 + \frac{1}{q} \sum_{m \in \mathbb{F}_q^*} S(a_1 m) S(a_2 m) S(a_3 m).$$

Then by Lemma 2.9, for any multiplicative character χ of order 3, we have

$$\begin{split} M_k(a_1, a_2, a_3) &= q^2 + \frac{1}{q} \sum_{m \in \mathbb{F}_q^*} \left[\prod_{j=1}^3 \left(\overline{\chi}(ma_j) G(\chi) + \chi(ma_j) G(\overline{\chi}) \right) \right] \\ &= q^2 + \frac{1}{q} \sum_{m \in \mathbb{F}_q^*} \left[\overline{\chi}(a_1 a_2 a_3) G^3(\chi) + \chi(a_1 a_2 a_3) G^3(\overline{\chi}) \right] \\ &+ G(\chi) (\chi(a_1^{-1} a_2^{-1} a_3) + \chi(a_1^{-1} a_2 a_3^{-1}) + \chi(a_1 a_2^{-1} a_3^{-1})) \sum_{m \in \mathbb{F}_q^*} \overline{\chi}(m) \\ &+ G(\overline{\chi}) (\chi(a_1^{-1} a_2 a_3) + \chi(a_1 a_2^{-1} a_3) + \chi(a_1 a_2 a_3^{-1})) \sum_{m \in \mathbb{F}_q^*} \chi(m) \\ &= q^2 + \frac{q - 1}{q} \left[\overline{\chi}(a_1 a_2 a_3) G^3(\chi) + \chi(a_1 a_2 a_3) G^3(\overline{\chi}) \right]. \end{split}$$

If $a_1a_2a_3$ is cubic, thus we have $\chi(a_1a_2a_3) = \overline{\chi}(a_1a_2a_3) = 1$. then by Lemma 2.8, we have

$$M_k(a_1, a_2, a_3) = q^2 + \frac{q-1}{q} (G^3(\chi) + G^3(\overline{\chi}))$$

= $q^2 + (q-1) \left[\frac{c+3\sqrt{3}di}{2} + \frac{c-3\sqrt{3}di}{2} \right]$
= $q^2 + c(q-1).$

If $a_1a_2a_3$ is non-cubic, then by Lemma 2.8, we can take multiplicative character χ of order 3 satisfying

$$\chi(a_1 a_2 a_3) = \frac{-1 + \sqrt{3}i}{2}, \quad G^3(\chi) = q \cdot \frac{c + 3\sqrt{3}di}{2},$$

where c and d are uniquely determined by (1.4). Thus we have

$$M_k(a_1, a_2, a_3) = q^2 + (q - 1) \left(\frac{-1 - \sqrt{3}i}{2} \cdot \frac{c + 3\sqrt{3}di}{2} + \frac{-1 + \sqrt{3}i}{2} \cdot \frac{c - 3\sqrt{3}di}{2} \right)$$
$$= q^2 + \frac{1}{2}(q - 1)(9d - c).$$

This completes the proof of the Theorem 1.9. *Proof of Theorem 1.10.* We have

$$\begin{split} M_k(a_1, a_2, a_3) &= \sum_{\substack{(x_1, x_2, x_3) \in \mathbb{F}_q^3 \\ a_1 x_1^3 + a_2 x_2^3 + a_3 x_3^3 = 0}} 1 \\ &= \sum_{\substack{(x_1, x_2) \in \mathbb{F}_q^2, x_3 \in \mathbb{F}_q^* \\ a_1 x_1^3 + a_2 x_2^3 + a_3 x_3^3 = 0}} 1 + \sum_{\substack{(x_1, x_2) \in \mathbb{F}_q^2 \\ a_1 x_1^3 + a_2 x_2^3 = 0}} 1 \\ &= \sum_{\substack{(x_1, x_2) \in \mathbb{F}_q^2, x_3 \in \mathbb{F}_q^* \\ a_1 (-x_1 x_3^{-1})^3 + a_2 (-x_2 x_3^{-1})^3 = a_3}} 1 + \sum_{\substack{x_1 \in \mathbb{F}_q^*, x_2 \in \mathbb{F}_q \\ a_1 x_1^3 + a_2 x_2^3 = 0}} 1 + 1 \\ &= (q - 1) \sum_{\substack{(x_1, x_2) \in \mathbb{F}_q^2 \\ a_1 x_1^3 + a_2 x_2^3 = a_3}} 1 + (q - 1) \sum_{\substack{x \in \mathbb{F}_q \\ x^3 = -a_1 a_2^{-1}}} 1 + 1 \\ &= (q - 1) N_k(a_1, a_2, a_3) + 1 + (q - 1) \sum_{\substack{x \in \mathbb{F}_q \\ x^3 = -a_1 a_2^{-1}}} 1. \end{split}$$

If $a_1 a_2^{-1}$ is cubic, the number of solutions of the equation $x^3 = -a_1 a_2^{-1}$ is exactly 3. Thus we have

 $M_k(a_1, a_2, a_3) = (q-1)N_k(a_1, a_2, a_3) + 1 + 3(q-1) = (q-1)N_k(a_1, a_2, a_3) + 3q-2.$

If $a_1 a_2^{-1}$ is non-cubic, the equation $x^3 = -a_1 a_2^{-1}$ has no solution. Thus we have

$$M_k(a_1, a_2, a_3) = (p-1)N_k(a_1, a_2, a_3) + 1.$$

Hence Theorem 1.10 immediately follows from Theorem 1.9.

Example 4.1. We take $\mathbb{F}_{7^2} := \mathbb{F}_7[u]/(u^2+1)$. One can check that u+1 is non-cubic in $\mathbb{F}_7[u]/(u^2+1)$ and $(u+1)^{\frac{7^2-1}{3}} = 4$. If the integers c and

d satisfying that $4 \cdot 7^2 = c^2 + 27d^2, c \equiv 1 \pmod{3}, (c, p) = 1, 9d \equiv c(2(u + 1)^{\frac{q-1}{3}} + 1) \pmod{p}$, then c = 13, d = -1. Thus we have

$$N_2(1, 1, u+1) = 7^2 - 2 + \frac{1}{2}(-9 - 13) = 36$$

and

$$M_2(1, 1, u+1) = 49^2 + \frac{1}{2}(-9 - 13) = 1873.$$

We list the solutions of equation $x_1^3 + x_2^3 = u + 1$ over $\mathbb{F}_7[u]/(u^2+1)$ as belove:

$$\begin{aligned} &(1,3u); (1,5u); (1,6u); (2,3u); (2,5u); (2,6u); (4,3u); (4,5u); (4,6u); \\ &(u+4,3u+6); (u+4,5u+3); (u+4,6u+5); (2u+1,3u+6); (2u+1,5u+3); \\ &(2u+1,6u+5); (4u+2,3u+6); (4u+2,5u+3); (4u+2,6u+5), \end{aligned}$$

and one can get the remaining 18 solutions by exchanging coordinates.

Acknowledgments

The authors are partially supported by the National Natural Science Foundation of China (Grant No. 11871193, 12071132) and the Natural Science Foundation of Henan Province (No. 202300410031).

References

References

- B. C. Berndt, R. J. Evans and K. S. Williams, Gauss and Jacobi Sums, Canad. Math. Soc. Ser. Monogr. Adv. Texts, John Wiley & Sons, New York, 1998.
- [2] S. Chowla, J. Cowles and M. Cowles, On the number of zeros of diagonal cubic forms, J. Number Theory 9 (1977), no. 4, 502-506.
- [3] S. Chowla, J. Cowles and M. Cowles, The number of zeroes of $x^3 + y^3 + cz^3$ in certain finite fields, J. Reine Angew. Math. 299(300) (1978), 406-410.
- [4] C. F. Gauss, Disquisitiones Arithmeticae, Yale University, New Haven, 1966.

- [5] S. F. Hong and C. X. Zhu, On the number of zeros of diagonal cubic forms over finite fields, Forum Mathematicum 33 (2021), 697-708.
- [6] J. R. Joly, Équations et variétés algébriques sur un corps fini, Enseign. Math. (2) 19 (1973), 1-117.
- [7] R. Lidl and H. Niederreiter, Finite Fields, 2nd ed., Encyclopedia Math. Appl. 20, Cambridge University, Cambridge, 1997.
- [8] B. Morlaye, Equations diagonales non homogènes sur un corps fini, C. R. Acad. Sci. Paris Sèr. A 272 (1971), 1545-1548.
- [9] G. Myerson, On the numbers of zeros of diagonal cubic forms, J. Number Theory 11 (1979), no. 1, 95-99.
- [10] G. Myerson, Period polynomials and Gauss sums for finite fields, Acta Arith. 39 (1981), no. 3, 251-264.
- [11] D. Q. Wan, Zeros of diagonal equations over finite fields, Proc. Amer. Math. Soc. 103 (1988), no. 4, 1049-1052.
- [12] A. Weil, Numbers of solutions of equations in finite fields, Bull. Amer. Math. Soc. 55 (1949), 497-508.
- [13] J. Wolfmann, The number of solutions of certain diagonal equations over finite fields, J. Number Theory 42 (1992), no. 3, 247-257.
- [14] J. Wolfmann, New results on diagonal equations over finite fields from cyclic codes, in: Finite fields: Theory, Applications, and Algorithms, Contemp. Math. 168, American Mathematical Society, Providence (1994), 387-395.