FACTORIZATION FORMULAE ON COUNTING ZEROS OF DIAGONAL EQUATIONS OVER FINITE FIELDS

WEI CAO AND QI SUN

(Communicated by Wen-Ching Winnie Li)

Abstract. Let \( N \) be the number of solutions \((u_1, \ldots, u_n)\) of the equation
\[ a_1u_1^{d_1} + \cdots + a_nu_n^{d_n} = 0 \]
over the finite field \( \mathbb{F}_q \), and let \( I \) be the number of solutions of the equation
\[ \sum_{i=1}^{n} x_i/d_i \equiv 0 \pmod{m}, 1 \leq x_i \leq d_i - 1. \]
If \( I > 0 \), let \( L \) be the least integer represented by \( \sum_{i=1}^{n} x_i/d_i, 1 \leq x_i \leq d_i - 1. \) \( I \) and \( L \) play important roles in estimating \( N \). Based on a partition of \( \{d_1, \ldots, d_n\} \), we obtain the factorizations of \( I, L \) and \( N \), respectively. All these factorizations can simplify the corresponding calculations in most cases or give the explicit formulae for \( N \) in some special cases.

1. Introduction

Let \( \mathbb{F}_q \) be a finite field of \( q \) elements, where \( q = p^l > 1 \) is a power of an odd prime \( p \). The diagonal equations over \( \mathbb{F}_q \) we consider in this paper are those of the form
\[ a_1u_1^{d_1} + a_2u_2^{d_2} + \cdots + a_nu_n^{d_n} = 0, \]
where \( a_i \in \mathbb{F}_q \setminus \{0\} \) and \( d_i \) are positive integers satisfying that \( d_i > 1 \) and \( d_i|q - 1 \) for all \( i = 1, \ldots, n \). This is the example chosen by Weil in [14] to illustrate his famous conjectures on projective varieties over finite fields, which were proved later by Dwork and Deligne. Let \( N \) denote the number of solutions \((u_1, u_2, \ldots, u_n)\) to (1) in \( \mathbb{F}_q^n \). Weil [14] and Hua and Vandiver [3] obtained independently the formula for \( N \) in terms of character sums including Jacobi sums. However, it is not easy to get the exact value of \( N \) from their formula in general. Therefore, much work has been done either to give the estimates for \( N \) or to seek the more explicit formulae for \( N \) under certain conditions (see [8], [9], [11], [13], [15]). We shall introduce some of the above results in detail in the next section.

In this paper, based on a partition of \( \{d_1, \ldots, d_n\} \), we first obtain the factorizations of the related estimates for \( N \). Then by using the relationship between Jacobi sums and Gauss sums, a similar result for \( N \) is also obtained. In the last section, we show that our results can simplify the corresponding calculations in most cases or give the explicit formulae for \( N \) in some special cases.
2. Preliminaries

Let \( \chi_1, \chi_2, \ldots, \chi_n \) be multiplicative characters on \( \mathbb{F}_q \). We shall drop the use of the word \emph{multiplicative} from now on. In this paper, the Jacobi sum \( j(\chi_1, \chi_2, \ldots, \chi_n) \) is defined as

\[
j(\chi_1, \chi_2, \ldots, \chi_n) = \sum_{c_1 + \cdots + c_n = 0, \ c_i \in \mathbb{F}_q} \chi_1(c_1)\chi_2(c_2)\cdots \chi_n(c_n).
\]

It is well known that the formula for \( N \) can be expressed in terms of character sums (see \[3\], \[14\], or \[4, p. 103\], \[6, p. 291\]):

Theorem 2.1.

\[
N = q^{n-1} + \sum \chi_1(a_1^{-1})\chi_2(a_2^{-1})\cdots \chi_n(a_n^{-1})j(\chi_1, \chi_2, \ldots, \chi_n),
\]

where the sum is over all \( n \)-tuples of characters \( \chi_1, \chi_2, \ldots, \chi_n \) satisfying \( \chi_i = \chi_0 \neq \chi_i \) for \( i = 1, \ldots, n \) and \( \chi_1\chi_2\cdots \chi_n = \chi_0 \), where \( \chi_0 \) denotes the trivial character of \( \mathbb{F}_q \). Moreover,

\[
|N - q^{n-1}| \leq I(d_1, \ldots, d_n)(q-1)q^{(n-2)/2},
\]

where \( I(d_1, \ldots, d_n) \) is the number of integer solutions \( (x_1, \ldots, x_n) \) of the equation

\[
x_1d_1 + \cdots + x_nd_n \equiv 0 \pmod{1}, \quad 1 \leq x_i \leq d_i - 1, \ i = 1, \ldots, n.
\]

A complicated formula for \( I(d_1, \ldots, d_n) \) was obtained independently by Lidl and Niederreiter \[6, p. 293\], R. Stanly (see Small \[7\]), Sun, Wan and Ma \[10\], and Sun \[12\] as follows.

Theorem 2.2.

\[
I(d_1, \ldots, d_n) = (-1)^n + \sum_{r=1}^{n} (-1)^{n-r} \sum_{1 \leq i_1 < \cdots < i_r \leq n} \frac{d_{i_1} \cdots d_{i_r}}{\text{lcm}[d_{i_1}, \ldots, d_{i_r}]}.
\]

Applying Stickelberger’s congruence for Gauss sums, Wan provided a \( p \)-adic estimate for \( N \), which generalizes the results of Ax \[1\] and Joly \[5\].

Theorem 2.3 (see \[13\]).

\[
N \equiv 0 \pmod{q^{L(d_1, \ldots, d_n)-1}},
\]

where

\[
L(d_1, \ldots, d_n) = \begin{cases} \min\{\sum_{i=1}^{n} x_i/d_i \mid \sum_{i=1}^{n} x_i/d_i \equiv 0 \pmod{1}, 1 \leq x_i \leq d_i - 1\} & \text{if } I(d_1, \ldots, d_n) > 0, \\ n & \text{else.} \end{cases}
\]

Let \( D = \{d_1, \ldots, d_n\} \) and \( A = \{a_1, \ldots, a_n\} \) denote the systems of the degrees and coefficients of \( x_i \) in \( (1) \), respectively. Let \( N(D; A) = N \), the number of solutions
of (1), and define
\[ T(D) = \{(\chi_1, \ldots, \chi_n) | \chi_i^{d_i} = \chi_0 \neq \chi_i \text{ for } i = 1, \ldots, n, \text{ and } \chi_1 \cdots \chi_n = \chi_0\}, \]
\[ R(D) = \{(x_1, \ldots, x_n) | \text{there are } x_i \in \{1, \ldots, d_i - 1\} \text{ for } i = 1, \ldots, n \text{ such that } \frac{x_1}{d_1} + \cdots + \frac{x_n}{d_n} \equiv 0 \pmod{1}\}, \]
\[ J(D; A) = \sum_{(\chi_1, \chi_2, \ldots, \chi_n) \in T(D)} \chi_1^{(a_1^{-1})} \chi_2^{(a_2^{-1})} \cdots \chi_n^{(a_n^{-1})} j(\chi_1, \chi_2, \ldots, \chi_n). \]

Thus (2) can be briefly rewritten as
\[ N(D; A) = q^{n-1} + J(D; A). \]

**Corollary 2.4.** \( J(D; A) \) is an integer. To be precise, we have
\[ J(D; A) = N(D; A) - q^{n-1}. \]

3. A Partition of \( D \) and Main Results

In this section, with the concept of the greatest common divisor, we will first define an equivalence relation on the set \( D \) and then induce an important partition of \( D \). The main results of this paper, based on the partition of \( D \), will be given at the end of the section.

**Definition 3.1.** For any \( a, b \in D \), we say \( a \sim b \) if there exist \( c_1, c_2, \ldots, c_m \in D \) such that \( \gcd(a, c_1) > 1, \gcd(c_1, c_2) > 1, \ldots, \gcd(c_m, b) > 1 \).

Obviously, the relation \( \sim \) on \( D \) is an equivalence relation on \( D \). Since an equivalence relation on a set induces a partition of the set, we have

**Proposition 3.2.** Under the equivalence relation \( \sim \), \( D \) can be partitioned into
\[ D = D_1 \cup \cdots \cup D_r, \]
where \( D_i \) are nonempty, mutually disjoint subsystems of \( D \), and for any \( a, b \in D \), \( a \sim b \) if and only if \( a, b \in D_j \) for some \( 1 \leq j \leq r \).

**Definition 3.3.** \( D_i \) are called the maximal divisor-connected sets in \( D \).

**Example 3.4.** Suppose \( D = \{2, 3, 4, 5, 7, 8, 15, 49\} \). Then
\[ D = \{2, 4, 8\} \cup \{3, 5, 15\} \cup \{7, 49\}. \]

Correspondingly, the coefficient system \( A \) is partitioned into
\[ A = A_1 \cup \cdots \cup A_r, \]
where \( A_i = \{a_j : d_j \in D_i\} \).

In what follows we will frequently use partitions (9) and (11) without explaining the meanings of \( D_i \) and \( A_i \) again. The following is a basic property of the maximal divisor-connected sets in \( D \).

**Proposition 3.5.** For any \( 1 \leq i \neq j \leq r \), we have \( \gcd(\lcm[D_i], \lcm[D_j]) = 1 \).

**Proof.** Assume that \( \gcd(\lcm[D_i], \lcm[D_j]) \) is divided by some prime number, say \( p \). Then \( p | \lcm[D_i] \) and \( p | \lcm[D_j] \). This implies that there exist \( d_i \in D_i \) and \( d_j \in D_j \), both of which contain the prime divisor \( p \). So we have \( p | \gcd(d_i, d_j) \). This means that \( d_i \) and \( d_j \) lie in the same maximal divisor-connected set, a contradiction. \( \square \)
Likewise, \( T(D_i), \ R(D_i), \ N(D_i; A_i) \) and \( J(D_i; A_i) \) can be defined and the process to define them is not discussed. With the notation and concepts introduced above, we can state the main results of this paper, whose proof will be given in the next section.

**Theorem 3.6.** Suppose \( D \) is of the partition as in (9). Then we have

(a) \( I(D) = \prod_{i=1}^{r} I(D_i) \).

(b) \( L(D) = \sum_{i=1}^{r} L(D_i) \) if \( I(D) > 0 \).

(c) \( N(D; A) = q^{n_i-1} + (q/(q-1))^r \prod_{i=1}^{r} (N(D_i; A_i) - q^{n_i-1}) \).

\[ \text{4. Proof of the main results} \]

**Lemma 4.1.** \( R(D) \) is the direct sum of \( R(D_i) \), that is,

\[ (12) \quad R(D) = \bigoplus_{i=1}^{r} R(D_i). \]

**Proof.** Clearly, \( R(D) \supseteq \bigoplus_{i=1}^{r} R(D_i) \). We show that the converse is also true by induction on \( r \). If \( r = 1 \), the proof is trivial. Assume \( r = 2 \). Suppose \( D_1 = \{ d_1^{(1)}, \ldots, d_{n_1}^{(1)} \} \), \( D_2 = \{ d_1^{(2)}, \ldots, d_{n_2}^{(2)} \} \) and \( (x_1^{(1)}, \ldots, x_{n_1}^{(1)}), (x_1^{(2)}, \ldots, x_{n_2}^{(2)}) \in R(D) \) such that

\[ (13) \quad \frac{x_1^{(1)}}{d_1^{(1)}} + \cdots + \frac{x_{n_1}^{(1)}}{d_{n_1}^{(1)}} + \frac{x_1^{(2)}}{d_1^{(2)}} + \cdots + \frac{x_{n_2}^{(2)}}{d_{n_2}^{(2)}} \equiv 0 \pmod{1}. \]

We need to show \((x_1^{(1)}, \ldots, x_{n_1}^{(1)}), (x_1^{(2)}, \ldots, x_{n_2}^{(2)}) \in R(D_1) \) and \((x_1^{(2)}, \ldots, x_{n_2}^{(2)}) \in R(D_2) \).

Letting \( l_i = \text{lcm}[D_i] \) \((i = 1, 2)\) and then reducing the fractions yields

\[ (14) \quad \frac{x_1^{(1)}}{l_1} + \frac{x_2^{(1)}}{l_2} \equiv 0 \pmod{1}, \]

where \( x_1 = x_1^{(1)} l_1/d_1^{(1)} + \cdots + x_{n_1}^{(1)} l_1/d_{n_1}^{(1)} \) and \( x_2 = x_1^{(2)} l_2/d_1^{(2)} + \cdots + x_{n_2}^{(2)} l_2/d_{n_2}^{(2)} \). We claim \( l_1 x_1 \) and \( l_2 x_2 \); otherwise the rational number \( x_1/l_1 \) would have two reduced forms with different denominators. So

\[ \frac{x_1^{(1)}}{d_1^{(1)}} + \cdots + \frac{x_{n_1}^{(1)}}{d_{n_1}^{(1)}} \equiv 0 \pmod{1} \quad \text{and} \quad \frac{x_1^{(2)}}{d_1^{(2)}} + \cdots + \frac{x_{n_2}^{(2)}}{d_{n_2}^{(2)}} \equiv 0 \pmod{1}, \]

which means \((x_1^{(1)}, \ldots, x_{n_1}^{(1)}) \in R(D_1) \) and \((x_1^{(2)}, \ldots, x_{n_2}^{(2)}) \in R(D_2) \). Therefore, we proved \( R(D) \subseteq R(D_1) \bigoplus R(D_2) \) for the case \( r = 2 \).

For the case \( r > 2 \), inducting on \( r \) by using the fact that \( \gcd(l_1 \cdots l_{r-1}, l_r) = 1 \) where \( l_i = \text{lcm}[D_i] \) \((i = 1, \ldots, r)\), we can prove \( R(D) \subseteq \bigoplus_{i=1}^{r} R(D_i) \). So \( R(D) = \bigoplus_{i=1}^{r} R(D_i) \). The proof is complete. \( \square \)

There is a direct corollary to Lemma 4.1, which states that \( I(D) \) can be factorized into the product of \( I(D_i) \) and \( L(D) \) can be factorized into the sum of \( L(D_i) \).

**Corollary 4.2** (Factorizations of \( I(D) \) and \( L(D) \)).

\[ (15) \quad I(D) = \prod_{i=1}^{r} I(D_i), \]

and if \( I(D) > 0 \), then

\[ (16) \quad L(D) = \sum_{i=1}^{r} L(D_i). \]
We want to establish the similar relationship between $T(D)$ and $T(D_i)$ as that between $R(D)$ and $R(D_i)$ in Lemma 4.1.

**Lemma 4.3** (see [4, p. 147], [6, pp. 293-294]).

$$j(\chi_1, \chi_2, \ldots, \chi_n) = \frac{q - 1}{q} g(\chi_1) g(\chi_2) \cdots g(\chi_n),$$

where the Gauss sums $g(\chi_j)$ are defined by

$$g(\chi_j) = \sum_{a \in \mathbb{F}_q} \chi_j(a) e^{\text{Tr}_{\mathbb{F}_q}(a)(2\pi i/p)}, \quad j = 1, \ldots, n,$$

with $\text{Tr}_{\mathbb{F}_q}(a)$ being the trace of $a$.

Let $\chi$ be a character on $\mathbb{F}_q$ of order $q - 1$ and set $\chi_i = \chi^{(q-1)/d_i}$. Then $\chi_i$ is a character on $\mathbb{F}_q$ of order $d_i$ ($i = 1, \ldots, n$). It is not hard to verify that there exists a one-to-one correspondence between $T(D)$ and $R(D)$. Therefore, by Lemma 4.1, we have

**Lemma 4.4.** $T(D)$ is the direct sum of $T(D_i)$, that is,

$$T(D) = \bigoplus_{i=1}^{r} T(D_i).$$

To prove Theorem 3.6 (c), we need a lemma on the factorization of $J(D; A)$. Denote by $n_i$ the number of elements in $D_i$ for $1 \leq i \leq r$. The superscripts are used to denote the set to which an element belongs. For example, $(\chi_1^{(i)}, \ldots, \chi_n^{(i)}) \in T(D_i)$, and $a_1^{(i)}, \ldots, a_n^{(i)} \in A_i$, etc.

**Lemma 4.5** (Factorization of $J(D; A)$).

$$J(D; A) = \left( \frac{q}{q - 1} \right)^{r-1} \prod_{i=1}^{r} J(D_i; A_i).$$
Proof. By the discussions above, we have

\[ J(D; A) = \sum_{(x_1, \cdots, x_n) \in T(D)} \chi_1(a_1^{-1}) \cdots \chi_n(a_n^{-1})j(\chi_1, \cdots, \chi_n) \]

\[ = \frac{q-1}{q} \sum_{(x_1, \cdots, x_n) \in \mathcal{D}} \chi_1(a_1^{-1}) \cdots \chi_n(a_n^{-1})g(\chi_1) \cdots g(\chi_n) \]

\[ = \frac{q-1}{q} \sum_{(x_1^{(1)}, \cdots, x_n^{(i)}) \in T(D_i)} r \prod_{i=1}^r \chi_1^{(i)}((a_1^{(i)})^{-1}) \cdots \chi_n^{(i)}((a_n^{(i)})^{-1})g(\chi_1^{(i)}) \cdots g(\chi_n^{(i)}) \]

\[ = \left( \frac{q}{q-1} \right)^{r-1} \prod_{i=1}^r J(D_i; A_i) \]

This completes the proof. \( \square \)

By (8) and (18), one easily gets

**Corollary 4.6.**

\[ N(D; A) = q^{n-1} + \left( \frac{q}{q-1} \right)^{r-1} \prod_{i=1}^r (N(D_i; A_i) - q^{n-1}). \]

In particular, if \( N(D_i; A_i) = q^{n-1} \) for some \( 1 \leq i \leq r \), then

\[ N(D; A) = q^{n-1}. \]

5. Applications

Theorem 3.6(c) shows that the formula (or value) of \( N(D) \) can be obtained by the formulae (or values) of \( N(D_i) \), where \( D_i \) are the maximal divisor-connected sets in \( D \). This may simplify the calculations of \( N(D) \). We will illustrate it by deducing the explicit formulae for the number of solutions to the following two types of equations under certain conditions:

\[ (a_1 x_1^{d_1} + b_1 y_1^{d_1}) + \cdots + (a_n x_n^{d_n} + b_n y_n^{d_n}) = 0 \]

and

\[ (ax^{d_1} + by^{d_1}) + (c_1 z_1^{2} + c_2 z_2^{2} + \cdots + c_n z_n^{2}) = 0. \]

**Theorem 5.1.** Suppose \( D = \{d_1, d_1, d_2, d_2, \ldots, d_n, d_n\} \) with \( \gcd(d_i, d_j) = 1 \) and \( 1 < d_i \mid (q-1) \) for \( 1 \leq i \neq j \leq n \), and \( A = \{a_1, b_1, a_2, b_2, \ldots, a_n, b_n\} \subseteq \mathbb{F}_q \setminus \{0\} \). Then

\[ N(D; A) = q^{2n-1} + q^{n-1}(q-1) \prod_{i=1}^n \delta_{d_i}(-a,b_i^{-1}), \]
where the notation $\delta_d(c)$ with $1 < d \mid (q - 1)$ and $c \in \mathbb{F}_q \setminus \{0\}$ is defined as

\[
\delta_d(c) = \begin{cases} 
  d - 1 & \text{if } x^d = c \text{ is solvable in } \mathbb{F}_q, \\
  -1 & \text{else}.
\end{cases}
\]

In particular, if all equations $x^{d_i} = -a_i b_i^{-1}$ ($i = 1, \ldots, n$) are solvable in $\mathbb{F}_q$, then

\[
N(D; A) = q^{2n-1} + q^{n-1}(q - 1) \prod_{i=1}^{n} (d_i - 1).
\]

**Proof.** Clearly, $D = D_1 \cup \cdots \cup D_n$ where $D_i = \{a_i, d_i\}$ are the maximal divisor-connected sets. By (19), we have

\[
N(D; A) = q^{2n-1} + \left(\frac{q}{q-1}\right)^{n-1} \prod_{i=1}^{n} (N(D_i; A_i) - q).
\]

Note that by $a_i x_i^{d_i} + b_i y_i^{d_i} = 0$, we get $(y_i x_i^{-1})^{d_i} = -a_i b_i^{-1}$ if $x_i y_i \neq 0$. Therefore, it is easy to verify that

\[
N(D_i; A_i) = N((d_i, d_i); (a_i, b_i)) = q + (q - 1)\delta_{d_i}(-a_i b_i^{-1}).
\]

The result follows from (23) and (24). \qed

**Corollary 5.2.** Under the same assumption as in Theorem 5.1 with $A = \{1, -1, 1, -1, \ldots, 1, -1\}$, we have

\[
N(D; A) = q^{2n-1} + q^{n-1}(q - 1) \prod_{i=1}^{n} (d_i - 1).
\]

**Lemma 5.3** (see [2] pp. 305). Suppose $q$ is odd and $c_i \in \mathbb{F}_q \setminus \{0\}$ ($i = 1, \ldots, n$). Then

\[
N((2^{\frac{n}{2}}), \ldots, 2^{\frac{n}{2}}; c_1, \ldots, c_n)) = \begin{cases} 
  q^{n-1} + \rho((-1)^{n/2}c_1 \cdots c_n)(q^{n/2} - q^{(n-2)/2}) & \text{if } n \equiv 0 \pmod{2}, \\
  q^{n-1} & \text{if } n \equiv 1 \pmod{2},
\end{cases}
\]

where $\rho$ is a quadratic character on $\mathbb{F}_q$.

We can obtain the formula for the number of solutions to (21), whose proof will be left out because of its similarity to that of Theorem 5.1.

**Theorem 5.4.** Suppose $D = \{d, d, \overbrace{2, \ldots, 2}^{n}\}$ with $d$ odd and greater than 1, $2d \mid (q - 1)$, and $A = \{a, b, c_1, \ldots, c_n\} \subseteq \mathbb{F}_q \setminus \{0\}$. Let $\rho$ be a quadratic character on $\mathbb{F}_q$ and let $\delta_d(-ab^{-1})$ be defined as in (22). Then

\[
N(D; A) = \begin{cases} 
  q^{n+1} + q\delta_{d}(-ab^{-1})\rho((-1)^{n/2}c_1 \cdots c_n)(q^{n/2} - q^{(n-2)/2}) & \text{if } n \equiv 0 \pmod{2}, \\
  q^{n+1} & \text{if } n \equiv 1 \pmod{2}.
\end{cases}
\]

Finally, we present two examples to show that the factorizations of $I(D)$ and $L(D)$ in Corollary 4.2 can also simplify the calculations of $I(D)$ and $L(D).$
Example 5.5. Take the same set $D = \{2, 3, 4, 5, 7, 8, 15, 49\}$ as in Example 3.4. Then by (10) and (15), we have

$$I(2, 3, 4, 5, 7, 8, 15, 49) = I(2, 4, 8) \cdot I(3, 5, 15) \cdot I(7, 49) = 2 \cdot 8 \cdot 6 = 96,$$

and by (10) and (16), we have

$$L(2, 3, 4, 5, 7, 8, 15, 49) = L(2, 4, 8) + L(3, 5, 15) + L(7, 49) = 1 + 1 + 1 = 3.$$

Example 5.6. Let $D$ be defined as in Theorem 5.1. Then

$$I(D) = \prod_{i=1}^{n} I(d_i, d_i) = \prod_{i=1}^{n} (d_i - 1)$$

and

$$L(D) = \sum_{i=1}^{n} L(d_i, d_i) = \sum_{i=1}^{n} 1 = n.$$

The results agree with (3) and (6) by Theorem 5.1.

Acknowledgments

The authors would like to extend their sincere thanks to the referee, who read the manuscript very carefully and gave some valuable suggestions.

References


8. Q. Sun, D. Wan, On the solvability of the equation $\sum_{i=1}^{n} x_i/d_i \equiv 0$ (mod 1) and its application, Proc. Amer. Math. Soc. 100 (1987) 220-224. MR0884454 (88c:11015)

9. Q. Sun, D. Wan, On the diophantine equation $\sum_{i=1}^{n} x_i/d_i \equiv 0$ (mod 1), Proc. Amer. Math. Soc. 112 (1991) 25-29. MR1047608 (91b:11017)

10. Q. Sun, D. Wan, D. Ma, On the Diophantine equation $\sum_{i=1}^{n} x_i/d_i \equiv 0$ (mod 1) and its applications, Chinese Ann. of Math., Ser. B 7 (1986) 232-236. MR0858601 (87j:11023)

11. Q. Sun, On diagonal equations over finite fields, Finite Fields Appl. 3 (1997) 175-179. MR1447073 (97m:11050)

12. Z.W. Sun, Exact $m$-covers and the linear form $\sum_{s=1}^{k} x_s/n_s$, Acta Arith. 81 (1997) 175-198. MR1456240 (98h:11019)


