AIMS Mathematics, 10(6): 13741–13754.
DOI:10.3934/math.2025619
Received: 06 May 2025
Revised: 04 June 2025
Accepted: 09 June 2025
Published: 16 June 2025

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

Research article

Counting solutions to a system of quadratic form equations over finite fields

Xiaodie Luo and Kaimin Cheng*

School of Mathematics and Information, China West Normal University, Nanchong, 637002, China

* **Correspondence:** Email: ckm20@126.com.

Abstract: The problem of counting the number of solutions to equations over finite fields has been a central topic in the study of finite fields. Let q be a prime power, and denote by $\mathbb{F}_q$ the finite field with q elements. In this paper, we address the problem of determining the number of solutions in $\mathbb{F}_q^n$ to a system of quadratic form equations with n unknowns over $\mathbb{F}_q$, a question initially proposed by Carlitz. By employing methods from character sums over finite fields, we derive explicit formulas for the number of solutions to general systems consisting of multiple quadratic forms. Our results provide a complete solution to Carlitz's problem. Separate treatments are provided for the cases of odd and even characteristics.

Keywords: finite fields; quadratic forms; the number of solutions; character sums
Mathematics Subject Classification: 11T06, 11T24

1. Introduction

The study of equations over finite fields forms a cornerstone of modern algebra, with profound connections to number theory, algebraic geometry, and combinatorics. In particular, the problem of counting the number of solutions to such equations has attracted considerable attention in recent decades. Numerous researchers have explored equations of specific forms, yielding a wealth of results. Early studies, such as [5], examined the number of solutions to the equation $a_1X_1^2 + \cdots + a_rX_r^2 = bX_1 \cdots X_r + c$ over a finite field, while [2, 3, 9] investigated certain diagonal equations. More recent contributions include [1], which employed the degree reduction matrix to derive an explicit formula for the number of solutions to a polynomial, and [6, 10, 11], which applied Smith's normalized forms to determine the number of solutions to specific equations. For foundational theories and general results concerning equations over finite fields, we refer the reader to [7, 8]. Nevertheless, determining the exact number of solutions to general polynomial equations or systems of equations remains a highly challenging task.

Let p be a prime and q a power of p, and denote by $\mathbb{F}_q$ the finite field with q elements. For a positive

integer n, a quadratic form in n variables over $\mathbb{F}_q$ is defined as a homogeneous polynomial of degree 2 in $\mathbb{F}_q[X_1, \ldots, X_n]$, or the zero polynomial. Let $Q(X_1, \ldots, X_n)$ be a quadratic form over $\mathbb{F}_q$ and $b \in \mathbb{F}_q$. We refer to the equation $Q(x_1, \ldots, x_n) = b$ as a quadratic form equation over $\mathbb{F}_q$ with n unknowns $x_1, \ldots, x_n$. It is well known that the number of solutions to a single quadratic form equation over $\mathbb{F}_q$ admits a uniform description; see Theorems 6.26, 6.27, and 6.32 in [7].

A natural question then arises: what can be said about the number of solutions in $\mathbb{F}_q^n$ to systems of multiple quadratic form equations? In fact, this problem was first proposed by Carlitz [4], who studied a system consisting of two specific quadratic form equations and derived an explicit formula for the number of solutions in the case of odd characteristic. However, a complete answer to this problem for general systems remains unknown.

Let $m \geq 2$ be an integer, $Q_1(X_1, \ldots, X_n), \ldots, Q_m(X_1, \ldots, X_n)$ be given quadratic forms over $\mathbb{F}_q$, and $b_1, \ldots, b_m \in \mathbb{F}_q$. In this paper, we study the number of solutions in $\mathbb{F}_q^n$ to the following system:

$$\begin{cases} Q_1(x_1, \ldots, x_n) = b_1, \\ Q_2(x_1, \ldots, x_n) = b_2, \\ \quad \vdots \\ Q_m(x_1, \ldots, x_n) = b_m. \end{cases} \tag{1.1}$$

Actually, by employing tools from character sums over finite fields, we obtain explicit formulas for the number of solutions in $\mathbb{F}_q^n$ to the system (1.1), thereby providing a complete solution to the problem originally raised by Carlitz.

The paper is organized as follows: In Section 2, we present some preliminaries on quadratic forms over finite fields. In Section 3, we derive the main results for the case of odd characteristic. Section 4 is devoted to establishing the corresponding results for even characteristics. Finally, in Section 5, we provide examples to illustrate the application of our main results.

2. Preliminaries

Let p be a prime, and q be a power of p. Denote by $\mathbb{F}_q$ the finite field of order q. In this section, we present several basic definitions and results concerning quadratic forms over $\mathbb{F}_q$.

As usual, for a given column vector $X = (X_1, \ldots, X_n)^T$, a linear substitution is defined by $X = CY$, where C is an $n \times n$ matrix over $\mathbb{F}_q$, and $Y = (Y_1, \ldots, Y_n)^T$ is a new column vector of variables. If C is invertible, the substitution is called a nonsingular linear substitution. Two quadratic forms, Q_1 and Q_2, are said to be equivalent if there exists a nonsingular linear substitution transforming Q_1 into Q_2.

Clearly, if Q_1 and Q_2 are equivalent quadratic forms over $\mathbb{F}_q$, then for any $\alpha \in \mathbb{F}_q$, the equations $Q_1(x_1, \ldots, x_n) = \alpha$ and $Q_2(x_1, \ldots, x_n) = \alpha$ have the same number of solutions in $\mathbb{F}_q^n$.

For a quadratic form Q over $\mathbb{F}_q$, the rank of Q, denoted $\mathrm{rank}(Q)$, is defined as the minimal nonnegative integer r such that Q is equivalent to a quadratic form in r variables. It is easy to verify that equivalent quadratic forms have the same rank. In particular, a quadratic form Q in n variables over $\mathbb{F}_q$ is said to be nondegenerate if $\mathrm{rank}(Q) = n$.

When q is odd, it is known that any quadratic form $Q(X_1, \ldots, X_n)$ over $\mathbb{F}_q$ can be written as

$$Q(X_1, \ldots, X_n) = \sum_{1 \leq i,j \leq r} a_{ij} X_i X_j, \text{ where } a_{ij} = a_{ji}.$$

Associated with Q is the $r\times r$ symmetric matrix $A = (a_{ij})$, called the coefficient matrix of Q. We denote by $\det(Q)$ the determinant of the coefficient matrix A.

A quadratic form Q is called diagonal if its coefficient matrix is diagonal. The following lemma is a standard result:

Lemma 2.1. *[7, Theorem 6.21] For q an odd prime power, every quadratic form Q over $\mathbb{F}_q$ is equivalent to a diagonal quadratic form with rank(Q) non-zero entries on the main diagonal.*

For a quadratic form $Q(X_1,\dots,X_n)$ over $\mathbb{F}_q$, we define its diagonal multiplier as $C = c_1c_2\cdots c_r$, where Q is equivalent to a diagonal form $c_1Y_1^2+\cdots+c_rY_r^2$ with each $c_i\neq 0$.

For even q, we have the parallel result:

Lemma 2.2. *[7, Theorem 6.30] Let q be a power of two. Let Q be a quadratic form with rank n over $\mathbb{F}_q$. Each of the following statements holds.*

(a) If n is odd, then Q is equivalent to

$$X_1X_2+X_3X_4+\cdots+X_{n-2}X_{n-1}+X_n^2.$$

(b) If n is even, then Q is equivalent to

$$X_1X_2+X_3X_4+\cdots+X_{n-3}X_{n-2}+bX_{n-1}^2+cX_{n-1}X_n+dX_n^2,$$

for some $b,d\in\mathbb{F}_q$ and $c\in\mathbb{F}_q^*$. Moreover, Q is equivalent to

$$X_1X_2+X_3X_4+\cdots+X_{n-1}X_n,$$

if $b=0$, or $b\neq 0$ and $Tr(dbc^{-2})=0$, and

$$X_1X_2+X_3X_4+\cdots+X_{n-1}X_n+X_{n-1}^2+dbc^{-2}X_n^2,$$

if $b\neq 0$ and $Tr(dbc^{-2})=1$. Here, Tr denotes the trace function from $\mathbb{F}_q$ to $\mathbb{F}_2$.

Let χ be the canonical additive character of $\mathbb{F}_q$ and η be the quadratic multiplicative character of $\mathbb{F}_q$; that is, $\chi(x)=\exp(2\pi i\mathrm{Tr}(x)/p)$ for any $x\in\mathbb{F}_q$, where Tr is the absolute trace from $\mathbb{F}_q$ to its prime field $\mathbb{F}_p$, and

$$\eta(x)=\begin{cases}1, & x \text{ is a nonzero square},\\ -1, & x \text{ is a nonsquare},\\ 0, & x=0.\end{cases}$$

Let g be the quadratic Gauss sum over $\mathbb{F}_q$ defined by

$$g=\sum_{x\in\mathbb{F}_q}\chi(x)\eta(x). \tag{2.1}$$

Its exact value is given by the following lemma.

Lemma 2.3. *[7, Theorem 5.15] Let p be an odd prime and $q = p^s$, with s being a positive integer. Then the quadratic Gauss sum g over $\mathbb{F}_q$ is given by*

$$g = \begin{cases} (-1)^{s-1}q^{1/2}, & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{s-1}i^s q^{1/2}, & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

where i is the imaginary unit. Consequently, $g^2 = \eta(-1)q$.

For the system of Eq (1.1), let $\boldsymbol{b} = (b_1, \ldots, b_m)$, and denote by $N_{\boldsymbol{b}}$ the number of solutions in $\mathbb{F}_q^n$ to (1.1). Consider the following associated system:

$$\begin{cases} Q_1(x_1, \ldots, x_n) - b_1 y^2 = 0, \\ Q_2(x_1, \ldots, x_n) - b_2 y^2 = 0, \\ \quad \vdots \\ Q_m(x_1, \ldots, x_n) - b_m y^2 = 0, \end{cases} \tag{2.2}$$

where y is a new variable distinct from $x_1, \ldots, x_n$. Define $N'_{\boldsymbol{b}}$ as the number of solutions in $\mathbb{F}_q^{n+1}$ to the system (2.2). Observe that for each $y \in \mathbb{F}_q^*$, the map

$$(x_1, \ldots, x_n, y) \mapsto (y^{-1}x_1, \ldots, y^{-1}x_n)$$

induces a bijection from the set of solutions $(x_1, \ldots, x_n, y)$ to (2.2) onto the set of solutions to (1.1). Consequently, we have

$$N_{\boldsymbol{b}} = \frac{1}{q-1}(N'_{\boldsymbol{b}} - N_{\boldsymbol{0}}), \tag{2.3}$$

where $N_{\boldsymbol{0}}$ denotes the number of solutions in $\mathbb{F}_q^n$ to the system (1.1) with $\boldsymbol{b}$ being the zero vector. Thus, to determine $N_{\boldsymbol{b}}$, it suffices to compute the number of solutions in $\mathbb{F}_q^n$ to the system of the type

$$\begin{cases} Q_1(x_1, \ldots, x_n) = 0, \\ Q_2(x_1, \ldots, x_n) = 0, \\ \quad \vdots \\ Q_m(x_1, \ldots, x_n) = 0, \end{cases} \tag{2.4}$$

which will be carried out in Section 3 for the case where q is odd and in Section 4 for the case where q is even.

3. Odd characteristic case

In this section, we investigate the number of solutions to the system (2.4) in $\mathbb{F}_q^n$ for odd q. We begin by introducing a key lemma.

Lemma 3.1. *For an odd prime power q, with χ as the canonical additive character of $\mathbb{F}_q$ and η as the quadratic multiplicative character of $\mathbb{F}_q$, consider a quadratic form $Q(X_1, \ldots, X_n)$ in n variables over $\mathbb{F}_q$ with rank r. Then*

$$\sum_{(x_1,\ldots,x_n)\in\mathbb{F}_q^n} \chi(Q(x_1, \ldots, x_n)) = \eta(\gamma)g^r q^{n-r},$$

where γ is a diagonal multiplier of Q, and g is the quadratic Gauss sum defined as in (2.1)*. In particular, if $r = n$, then*

$$\sum_{(x_1,\ldots,x_n)\in\mathbb{F}_q^n} \chi(Q(x_1, \ldots, x_n)) = \eta(\det(Q))g^n.$$

Proof. First, from Lemma 2.1, we know that there exists a nonsingular linear substitution $X = CY$ that transforms Q into the diagonal form

$$c_1Y_1^2 + \cdots + c_nY_n^2,$$

where $c_i \in \mathbb{F}_q^*$ for any $1 \le i \le r$, and $c_i = 0$ for any $i > r$. It then follows that

$$\begin{aligned}\sum_{(x_1,\ldots,x_n)\in\mathbb{F}_q^n} \chi(Q(x_1, \ldots, x_n)) &= \sum_{(y_1,\ldots,y_n)\in\mathbb{F}_q^n} \chi(c_1y_1^2 + \cdots + c_ny_n^2)\\ &= q^{n-r} \sum_{(y_1,\ldots,y_r)\in\mathbb{F}_q^n} \chi(c_1y_1^2 + \cdots + c_ry_r^2)\\ &= q^{n-r} \prod_{i=1}^{r} \sum_{y_i\in\mathbb{F}_q} \chi(c_iy_i^2).\end{aligned}$$

Let $S = \{x^2 : x \in \mathbb{F}_q^*\}$. One sees that the map $\sigma : x \mapsto x^2$ from $\mathbb{F}_q^*$ onto S is 2-to-1. We also note that

$$\eta(x) + 1 = \begin{cases} 2, & \text{if } x \in S,\\ 0, & \text{if } x \in \mathbb{F}_q^* \setminus S.\end{cases}$$

It implies that for any $c \in \mathbb{F}_q^*$,

$$\begin{aligned}\sum_{y\in\mathbb{F}_q} \chi(cy^2) &= 1 + 2\sum_{y\in S} \chi(cy)\\ &= 1 + \sum_{y\in S} \chi(cy)(\eta(y) + 1) + \sum_{y\in\mathbb{F}_q^*\setminus S} \chi(cy)(\eta(y) + 1)\\ &= 1 + \sum_{y\in\mathbb{F}_q^*} \chi(cy)\eta(y) + \sum_{y\in\mathbb{F}_q^*} \chi(cy)\\ &= \sum_{y\in\mathbb{F}_q^*} \chi(cy)\eta(y) + \sum_{y\in\mathbb{F}_q} \chi(cy)\\ &= \eta(c)g,\end{aligned}$$

where the last equality holds since $\sum_{y\in\mathbb{F}_q} \chi(cy) = 0$. Therefore, we derive that

$$\sum_{(x_1,\ldots,x_n)\in\mathbb{F}_q^n} \chi(Q(x_1, \ldots, x_n)) = q^{n-r} \prod_{i=1}^{r} \sum_{y_i\in\mathbb{F}_q} \chi(c_iy_i^2) = \eta(\gamma)g^r q^{n-r},$$

where $\gamma = c_1 \cdots c_r$ is a diagonal multiplier of the quadratic form Q. This proves the first part of the lemma. Particularly, if $r = n$, then

$$\sum_{(x_1,\ldots,x_n)\in\mathbb{F}_q^n} \chi(Q(x_1,\ldots,x_n)) = \eta(c_1\cdots c_n)g^n. \tag{3.1}$$

Let A be the coefficient matrix of Q, and $\Lambda = \mathrm{diag}(c_1,\ldots,c_n)$. Then we have $\Lambda = C^TAC$. It implies that $\eta(c_1\cdots c_n) = \eta(\det(\Lambda)) = \eta(\det(C)^2\det(A)) = \eta(\det(Q))$. Hence, the second statement follows immediately from (3.1). This completes the proof of Lemma 3.1. □

Before stating the main result, we introduce some notations. Let q be an odd prime power, and let $m \geq 2$ be an integer. Consider m distinct quadratic forms $Q_1(X_1,\ldots,X_n), \ldots, Q_m(X_1,\ldots,X_n)$ in n variables over the finite field $\mathbb{F}_q$. Define a polynomial $d(Z_1,\ldots,Z_m)$ in $\mathbb{F}_q[Z_1,\ldots,Z_m]$ as the determinant of the quadratic form $Z_1Q_1(X_1,\ldots,X_n) + \cdots + Z_mQ_m(X_1,\ldots,X_n)$ in the variables $X_1,\ldots,X_n$. We call $d(Z_1,\ldots,Z_m)$ the associated polynomial of the quadratic forms $Q_1,\ldots,Q_m$. Clearly, $d(Z_1,\ldots,Z_m)$ is either a homogeneous polynomial of degree n or the zero polynomial.

Suppose $d(Z_1,\ldots,Z_m)$ has two nonzero linear factors over $\mathbb{F}_q$, say

$$l_1 = a_1Z_1 + \cdots + a_mZ_m \quad \text{and} \quad l_2 = b_1Z_1 + \cdots + b_mZ_m.$$

We say that l_1 and l_2 are equivalent if the vectors $(a_1,\ldots,a_m)$ and $(b_1,\ldots,b_m)$ are linearly dependent over $\mathbb{F}_q$.

Let L denote the set of pairwise inequivalent nonzero linear factors of $d(Z_1,\ldots,Z_m)$ over $\mathbb{F}_q$, referred to as the linear factor set of $d(Z_1,\ldots,Z_m)$. The cardinality of L, denoted by $|L| = t$, is called the linear index of the quadratic forms $Q_1,\ldots,Q_m$. Clearly, $0 \leq t \leq n$ if $d(Z_1,\ldots,Z_m)$ is not identically zero, and $t = \frac{q^m-1}{q-1}$ if $d(Z_1,\ldots,Z_m) \equiv 0$.

Define the following set

$$V = \left\{(z_1,\ldots,z_m) \in \mathbb{F}_q^m \setminus \{(0,\ldots,0)\} \;\middle|\; l(z_1,\ldots,z_m) = 0 \text{ for some } l \in L\right\},$$

which is called the set of nontrivial linear zeros of $d(Z_1,\ldots,Z_m)$.

We select a maximal subset $\{v_1,\ldots,v_s\} \subseteq V$ such that the vectors are pairwise linearly independent over $\mathbb{F}_q$; these are referred to as the $\mathbb{F}_q$-linearly independent representative set of V. For each linearly independent representative $v_i = (z_{i1},\ldots,z_{im}) \in V$, by Lemma 2.1, the quadratic form $z_{i1}Q_1 + \cdots + z_{im}Q_m$ is equivalent to a diagonal quadratic form, which we denote by

$$c_{i1}Y_1^2 + c_{i2}Y_2^2 + \cdots + c_{ir_i}Y_{r_i}^2,$$

where each coefficient $c_{ij} \in \mathbb{F}_q^*$ for all $1 \leq j \leq r_i$. We denote $C_i = c_{i1}\cdots c_{ir_i}$ and refer to it as a diagonal multiplier of v_i. The integer r_i is called the rank of v_i.

Now we can report the main result of this section as follows.

Theorem 3.1. *For an odd prime power q and an integer $m \geq 2$, let $Q_1,\ldots,Q_m$ be distinct quadratic forms in n variables $X_1,\ldots,X_n$ over $\mathbb{F}_q$, with associated polynomial $d(Z_1,\ldots,Z_m)$. Define V as the set of nontrivial linear zeros of $d(Z_1,\ldots,Z_m)$. Denote by N the number of solutions in $\mathbb{F}_q^n$ to the system* (2.4)*. The following statements hold:*

(a) If V is nonempty with an $\mathbb{F}_q$-linearly independent representative set $\{v_1, \ldots, v_s\}$, then

$$N = \begin{cases} q^{n-m} + (q-1)\mathcal{W} + q^{n/2-m}\mathcal{V}, & \text{if } n \text{ is even}, \\ q^{n-m} + (q-1)\mathcal{W}, & \text{if } n \text{ is odd}, \end{cases}$$

where

$$\mathcal{W} = \sum_{\substack{1 \le i \le s \\ r_i \text{ even}}} q^{n-m-r_i/2}\eta((-1)^{r_i/2}C_i), \mathcal{V} = \sum_{(z_1,\ldots,z_m)\in\mathbb{F}_q^m} \eta((-1)^{n/2}d(z_1, \ldots, z_m)),$$

r_i and C_i are the rank and the diagonal multiplier of v_i, respectively.

(b) If V is empty, then

$$N = \begin{cases} q^{n-m} + q^{n/2-m}\mathcal{V}, & \text{if } n \text{ is even}, \\ q^{n-m}, & \text{if } n \text{ is odd}, \end{cases}$$

where $\mathcal{V}$ is defined as in (a).

Proof. Let χ be the canonical character of $\mathbb{F}_q$. First, using the orthogonality of characters, we express N as

$$N = \sum_{x\in\mathbb{F}_q^n} \left(\frac{1}{q} \sum_{z_1\in\mathbb{F}_q} \chi(z_1Q_1(x)) \cdots \frac{1}{q} \sum_{z_m\in\mathbb{F}_q} \chi(z_mQ_m(x)) \right) = q^{-m} \sum_{(z_1,\ldots,z_m)\in\mathbb{F}_q^m} \sum_{x\in\mathbb{F}_q^n} \chi(z_1Q_1(x) + \cdots + z_mQ_m(x)). \quad (3.2)$$

For $z = (z_1, \ldots, z_m) \in \mathbb{F}_q^m$, define a sum

$$S(z) = \sum_{x\in\mathbb{F}_q^n} \chi(z_1Q_1(x) + \cdots + z_mQ_m(x)).$$

Clearly, $S(\mathbf{0}) = q^n$, where $\mathbf{0}$ denotes the zero vector in $\mathbb{F}_q^m$. Let $d(Z_1, \ldots, Z_m)$ be the associated polynomial of $Q_1, \ldots, Q_m$, and let V be the set of nontrivial linear zeros of $d(Z_1, \ldots, Z_m)$. Then we have

$$\sum_{z\in\mathbb{F}_q^m} S(z) = q^n + \sum_{z\in V} S(z) + \sum_{z\in\mathbb{F}_q^m\setminus(V\cup\{\mathbf{0}\})} S(z). \quad (3.3)$$

Suppose that V is nonempty with an $\mathbb{F}_q$-linearly independent representative set $\{v_1, \ldots, v_s\}$. For each v_i, let C_i and r_i be a diagonal multiplier and the rank of v_i, respectively. It follows that

$$\sum_{z\in V} S(z) = \sum_{i=1}^{s} \sum_{\lambda\in\mathbb{F}_q^*} S(\lambda v_i).$$

Note that λv_i has a diagonal multiplier $\lambda^{r_i}C_i$ for any $\lambda \in \mathbb{F}_q^*$. Thus, by using Lemma 3.1, we obtain

$$\sum_{z\in V} S(z) = \sum_{i=1}^{s} \sum_{\lambda\in\mathbb{F}_q^*} \eta(\lambda^{r_i}C_i)g^{r_i}q^{n-r_i} = \sum_{i=1}^{s} g^{r_i}q^{n-r_i} \sum_{\lambda\in\mathbb{F}_q^*} \eta(\lambda^{r_i}C_i) = (q-1) \sum_{\substack{1 \le i \le s \\ r_i \text{ even}}} \eta(C_i)g^{r_i}q^{n-r_i}, \quad (3.4)$$

where the last equality holds since

$$\sum_{\lambda\in\mathbb{F}_q^*}\eta(\lambda^{r_i}C_i)=\begin{cases}(q-1)\eta(C_i), & \text{if } r_i \text{ is even},\\ 0, & \text{if } r_i \text{ is odd}.\end{cases}$$

Now we turn attention to the last sum on the right-hand side of (3.3). Note that the quadratic form

$$z_1Q_1(X_1,\ldots,X_n)+\cdots+z_mQ_m(X_1,\ldots,X_n)$$

is of rank n for any $(z_1,\ldots,z_m)\in\mathbb{F}_q^m\setminus V$, and recall that $d(Z_1,\ldots,Z_m)$ is the associated polynomial of $Q_1,\ldots,Q_m$. It follows from Lemma 3.1 that

$$\sum_{z\in\mathbb{F}_q^m\setminus V}S(z)=g^n\sum_{z\in\mathbb{F}_q^m\setminus V}\eta(d(z))=g^n\sum_{z\in\mathbb{F}_q^m}\eta(d(z)), \tag{3.5}$$

since $\eta(0)=0$. In particular, for odd n, consider the sum

$$\mathcal{S}=\sum_{(z_1,\ldots,z_m)\in\mathbb{F}_q^m}\eta(d(z_1,\ldots,z_m)).$$

Let $w\in\mathbb{F}_q^*$ be a non-square element. Then

$$\mathcal{S}=\sum_{(z_1,\ldots,z_m)\in\mathbb{F}_q^m}\eta(d(wz_1,\ldots,wz_m))=\eta(w^n)\mathcal{S}.$$

Since n is odd and $\eta(w)=-1$, we have $\eta(w^n)=-1$, so $\mathcal{S}=-\mathcal{S}$, implying $\mathcal{S}=0$. By substituting (3.4) and (3.5) into (3.3), combining with (3.2), and applying Lemma 2.3, we obtain the first statement of this theorem.

If V is empty, the first sum on the right-hand side of (3.3) vanishes, and the second statement of this lemma follows similarly.

This completes the proof of Theorem 3.1. □

4. Even characteristic case

In this section, we analyze the number of solutions to the system (2.4) in $\mathbb{F}_q^n$ for even q. We start with a useful lemma.

Lemma 4.1. *Suppose q is a power of two. Take χ as the canonical additive character of $\mathbb{F}_q$, and let $Q(X_1,\ldots,X_n)$ be a quadratic form in n variables over $\mathbb{F}_q$ with rank r. Then*

$$\sum_{(x_1,\ldots,x_n)\in\mathbb{F}_q^n}\chi(Q(x_1,\ldots,x_n))=\begin{cases}0, & \text{if } r \text{ is odd},\\ \delta q^{n-r/2}, & \text{if } r \text{ is even},\end{cases}$$

where $\delta=1$ if $Q(X_1,\ldots,X_n)$ is equivalent to $Y_1Y_2+Y_3Y_4+\cdots+Y_{r-1}Y_r$, and $\delta=-1$ otherwise.

Proof. First, we let r be odd. Using Lemma 2.2(a), we can transform the quadratic form $Q(X_1, \ldots, X_n)$ into

$$F(Y_1, \ldots, Y_n) = Y_1Y_2 + Y_3Y_4 + \cdots + Y_{r-2}Y_{r-1} + Y_r^2$$

by a nonsingular linear substitution. Then

$$\begin{aligned}\sum_{(x_1,\ldots,x_n)\in\mathbb{F}_q^n} \chi(Q(x_1, \ldots, x_n)) &= \sum_{(y_1,\ldots,y_n)\in\mathbb{F}_q^n} \chi(F(y_1, \ldots, y_n)) \\ &= q^{n-r} \sum_{(y_1,\ldots,y_r)\in\mathbb{F}_q^n} \chi(y_1y_2 + y_3y_4 + \cdots + y_{r-2}y_{r-1} + y_r^2) \\ &= q^{n-r} \left(\sum_{y_1,y_2\in\mathbb{F}_q} \chi(y_1y_2) \right)^{(r-1)/2} \sum_{y\in\mathbb{F}_q} \chi(y^2).\end{aligned}$$

Note that y^2 is a permutation polynomial of $\mathbb{F}_q$ since q is even. It implies that

$$\sum_{y\in\mathbb{F}_q} \chi(y^2) = \sum_{y\in\mathbb{F}_q} \chi(y) = 0.$$

Hence, we obtain

$$\sum_{(x_1,\ldots,x_n)\in\mathbb{F}_q^n} \chi(Q(x_1, \ldots, x_n)) = 0.$$

Now, let r be even. Similarly, from Lemma 2.2(b), we know that $Q(X_1, \ldots, X_n)$ is equivalent to

$$G(Y_1, \ldots, Y_n) = Y_1Y_2 + Y_3Y_4 + \cdots + Y_{r-1}Y_r,$$

or

$$H(Y_1, \ldots, Y_n) = Y_1Y_2 + Y_3Y_4 + \cdots + Y_{r-1}Y_r + Y_{r-1}^2 + aY_r^2,$$

for some $a \in \mathbb{F}_q$ with $\mathrm{Tr}(a) = 1$. For the first case, we have

$$\begin{aligned}\sum_{(x_1,\ldots,x_n)\in\mathbb{F}_q^n} \chi(Q(x_1, \ldots, x_n)) &= \sum_{(y_1,\ldots,y_n)\in\mathbb{F}_q^n} \chi(G(y_1, \ldots, y_n)) \\ &= q^{n-r} \sum_{(y_1,\ldots,y_r)\in\mathbb{F}_q^n} \chi(y_1y_2 + y_3y_4 + \cdots + y_{r-1}y_r) \\ &= q^{n-r} \left(\sum_{y_1,y_2\in\mathbb{F}_q} \chi(y_1y_2) \right)^{r/2}. \qquad (4.1)\end{aligned}$$

And we compute that

$$\sum_{y_1,y_2\in\mathbb{F}_q} \chi(y_1y_2) = \sum_{y_1\in\mathbb{F}_q} \sum_{y_2\in\mathbb{F}_q} \chi(y_1y_2) = q + \sum_{y_1\in\mathbb{F}_q^*} \sum_{y_2\in\mathbb{F}_q} \chi(y_1y_2) = q. \qquad (4.2)$$

Substituting (4.2) into (4.1) yields the desired result of this case. For the latter case, we have

$$\sum_{(x_1,\ldots,x_n)\in\mathbb{F}_q^n} \chi(Q(x_1, \ldots, x_n)) = \sum_{(y_1,\ldots,y_n)\in\mathbb{F}_q^n} \chi(H(y_1, \ldots, y_n))$$

$$= q^{n-r} \sum_{(y_1,\ldots,y_r)\in\mathbb{F}_q^n} \chi(y_1y_2 + y_3y_4 + \cdots + y_{r-1}y_r + y_{r-1}^2 + ay_r^2)$$

$$= q^{n-r} \left(\sum_{y_1,y_2\in\mathbb{F}_q} \chi(y_1y_2) \right)^{(r-2)/2} \sum_{y_1,y_2\in\mathbb{F}_q} \chi(y_1^2 + y_1y_2 + ay_2^2). \tag{4.3}$$

We need to evaluate the last sum of (4.3). On the one hand,

$$\begin{aligned} \sum_{y_1,y_2\in\mathbb{F}_q} \chi(y_1^2 + y_1y_2 + ay_2^2) &= \sum_{y_1\in\mathbb{F}_q} \chi(y_1^2) + \sum_{y_1\in\mathbb{F}_q,y_2\in\mathbb{F}_q^*} \chi(y_1^2 + y_1y_2 + ay_2^2) \\ &= \sum_{y_1\in\mathbb{F}_q,y_2\in\mathbb{F}_q^*} \chi(y_2^2((y_1/y_2)^2 + y_1/y_2 + a)) \\ &= \sum_{t\in\mathbb{F}_q,y\in\mathbb{F}_q^*} \chi(y^2(t^2 + t + a)). \end{aligned}$$

On the other hand, we note that $\mathrm{Tr}(a) = 1$, and then $t^2 + t + a \neq 0$ for any $t \in \mathbb{F}_q$. It implies that

$$\sum_{y_1,y_2\in\mathbb{F}_q} \chi(y_1^2 + y_1y_2 + ay_2^2) = \sum_{t\in\mathbb{F}_q} \left(\sum_{y\in\mathbb{F}_q} \chi((t^2 + t + a)y^2) - 1 \right) = -\sum_{t\in\mathbb{F}_q} 1 = -q. \tag{4.4}$$

Therefore, by substituting (4.2) and (4.4) into (4.3), we arrive at the final result of this case.

This proves Lemma 4.1. □

We now state the main result of this section.

Theorem 4.1. *Suppose q is a power of two and $m \geq 2$ is an integer. Consider $Q_1, \ldots, Q_m$ as distinct quadratic forms in n variables $X_1, \ldots, X_n$ over $\mathbb{F}_q$. For a vector $z = (z_1, \ldots, z_m) \in \mathbb{F}_q^m$, define the quadratic form $Q(z)$ in variables $X_1, \ldots, X_n$ over $\mathbb{F}_q$ by $Q(z) = z_1Q_1 + \cdots + z_mQ_m$. For each $0 \leq r \leq n$, define T_r as the set of vectors $z \in \mathbb{F}_q^m$ such that $Q(z)$ has rank r, and define T_r' as the subset of $z \in \mathbb{F}_q^m$ such that $Q(z)$ has rank r and is equivalent to $Y_1Y_2 + Y_3Y_4 + \cdots + Y_{r-1}Y_r$. Then the number N of solutions in $\mathbb{F}_q^n$ to the system* (2.4) *is*

$$N = q^{n-m} \left(|T_0| + \sum_{1\leq r\leq\lfloor n/2\rfloor} \left(2|T_{2r}'| - |T_{2r}|\right) q^{-r} \right),$$

where $|S|$ represents the number of elements in the set S.

Proof. Let χ be the canonical character of $\mathbb{F}_q$. From the definition of T_r, we can partition $\mathbb{F}_q^m$ into $\mathbb{F}_q^m = \bigcup_{r=0}^n T_r$. For $z = (z_1, \ldots, z_m) \in \mathbb{F}_q^m$, let $Q(z) = z_1Q_1 + \cdots + z_mQ_m$. By (3.2), we then have

$$N = q^{-m} \sum_{(z_1,\ldots,z_m)\in\mathbb{F}_q^m} \sum_{x\in\mathbb{F}_q^n} \chi(z_1Q_1(x) + \cdots + z_mQ_m(x)) = q^{-m} \sum_{r=0}^{n} \sum_{z\in T_r} \chi(Q(z)). \tag{4.5}$$

Applying Lemma 4.1 into (4.5), we obtain

$$N = q^{-m} \sum_{\substack{0\leq r\leq n \\ r \text{ even}}} \sum_{z\in T_r} \delta_{r,z} q^{n-r/2} = q^{n-m} \sum_{\substack{0\leq r\leq n \\ r \text{ even}}} \sum_{z\in T_r} \delta_{r,z} q^{-r/2},$$

where $\delta_{r,z} = 1$, if $Q(z)$ is equivalent to $Y_1Y_2 + Y_3Y_4 + \cdots + Y_{r-1}Y_r$, and otherwise $\delta_{r,z} = -1$. Then N can be simplified to

$$N = q^{n-m}\left(|T_0| + \sum_{1\le r\le\lfloor n/2\rfloor} (2|T'_{2r}| - |T_{2r}|)\, q^{-r}\right),$$

as desired. Theorem 4.1 is proved. □

5. Concluding remarks and examples

In this paper, we investigate the number of solutions to systems of quadratic form equations over finite fields, deriving explicit formulas for the solution counts, thereby addressing one of Carlitz's problems; see Theorems 3.1 and 4.1. Our results, while not always straightforward, offer a novel algorithm for computing the number of solutions. For instance, in Theorem 3.1, one must first determine the set V of nontrivial linear zeros of the associated polynomial $d(Z_1, \ldots, Z_m)$ for the quadratic forms $Q_1, \ldots, Q_m$, then identify a linearly independent representative subset $\{v_1, \ldots, v_s\} \subseteq V$, and compute the rank and diagonal multiplier of each v_i. The desired result is then obtained using our formula. Similarly, for Theorem 4.1, one must determine the sizes of the sets T_{2r} and T'_{2r}, which depend on the quadratic forms $Q_1, \ldots, Q_m$. However, deriving closed-form formulas for $|T_{2r}|$ and $|T'_{2r}|$ remains a significant challenge.

Below, we present several examples to illustrate the application of our theorems.

5.1. Example 5.1

Let $\mathbb{F}_9 = \mathbb{F}_3(a)$, where a is a defining element of $\mathbb{F}_9$ over $\mathbb{F}_3$ satisfying $a^2 = a + 1$. We apply Theorem 3.1 to determine the number of solutions to the following system over $\mathbb{F}_9$:

$$\begin{cases} Q_1 = x_1^2 + x_1x_2 + 2x_3x_4 + x_3^2 + x_5^2 = 1, \\ Q_2 = x_1x_2 + x_2x_3 + x_4^2 + 2x_4x_5 + 2x_5^2 = 2. \end{cases} \tag{5.1}$$

To compute the number of solutions to system (5.1), we consider two auxiliary systems:

$$\begin{cases} Q'_1 = x_1^2 + x_1x_2 + 2x_3x_4 + x_3^2 + x_5^2 - x_6^2 = 0, \\ Q'_2 = x_1x_2 + x_2x_3 + x_4^2 + 2x_4x_5 + 2x_5^2 - 2x_6^2 = 0, \end{cases} \tag{5.2}$$

with N_1 solutions in $\mathbb{F}_9^6$, and

$$\begin{cases} Q_1 = x_1^2 + x_1x_2 + 2x_3x_4 + x_3^2 + x_5^2 = 0, \\ Q_2 = x_1x_2 + x_2x_3 + x_4^2 + 2x_4x_5 + 2x_5^2 = 0, \end{cases} \tag{5.3}$$

with N_2 solutions in $\mathbb{F}_9^5$.

5.1.1. Solutions to system (5.2)

To determine N_1, we proceed as follows:

Step 1. Compute the associated polynomial and factorize it over $\mathbb{F}_9$:

$$d(Z_1, Z_2) = \det(Z_1Q'_1 + Z_2Q'_2) = Z_1(Z_1 + Z_2)(Z_1 - Z_2)(Z_1^3 - Z_1^2Z_2 + Z_2^3).$$

Step 2. Select linearly independent representatives of the linear zero set of $d(Z_1, Z_2)$, given by $v_1 = (0, 1)$, $v_2 = (1, -1)$, and $v_3 = (1, 1)$.
Step 3. For each v_i, compute the rank and the diagonal multiplier of the corresponding quadratic form in the standard way:

- For $v_1 = (0, 1)$, the quadratic form Q'_2 has the equivalent diagonal form $Y_1^2 + Y_2^2 + Y_3^2 + Y_4^2 - Y_5^2$, with rank 5 and diagonal multiplier -1.
- For $v_2 = (1, -1)$, the quadratic form $Q'_1 - Q'_2$ has the equivalent diagonal form $Y_1^2 + Y_2^2 + Y_3^2 - Y_4^2 - Y_5^2$, with rank 5 and diagonal multiplier 1.
- For $v_3 = (1, 1)$, the quadratic form $Q'_1 + Q'_2$ has the equivalent diagonal form $Y_1^2 + Y_2^2 - Y_3^2 - Y_4^2 - Y_5^2$, with rank 5 and diagonal multiplier -1.

Step 4. Compute $\mathcal{W}$, obtaining $\mathcal{W} = 0$.
Step 5. Calculate $\mathcal{V}$ as:

$$\mathcal{V} = \sum_{(z_1,z_2)\in\mathbb{F}_9^2} \eta(-d(z_1, z_2)) = 24,$$

where η is the quadratic character of $\mathbb{F}_9$.
Step 6. Substitute the computed values into Theorem 3.1, yielding

$$N_1 = 9^{6-2} + 9^{6/2-2} \cdot 24 = 6777,$$

solutions for system (5.2).

5.1.2. Solutions to system (5.3)

To determine N_2, we follow a similar procedure:
Step 1. Compute the associated polynomial and factorize it over $\mathbb{F}_9$:

$$d(Z_1, Z_2) = \det(Z_1 Q_1 + Z_2 Q_2) = Z_1(Z_1 + Z_2)(Z_1^3 - Z_1^2 Z_2 + Z_2^3).$$

Step 2. Select linearly independent representatives of the linear zero set of $d(Z_1, Z_2)$, given by $v_1 = (0, 1)$ and $v_2 = (1, -1)$.
Step 3. For each v_i, compute the rank and multiplier of the corresponding quadratic form:

- For $v_1 = (0, 1)$, the quadratic form Q_2 has the equivalent diagonal form $Y_1^2 + Y_2^2 + Y_3^2 + 2Y_4^2$, with rank 4 and diagonal multiplier -1.
- For $v_2 = (1, -1)$, the quadratic form $Q_1 - Q_2$ has the equivalent diagonal form $Y_1^2 + Y_2^2 + 2Y_3^2 + 2Y_4^2$, with rank 4 and diagonal multiplier 1.

Step 4. Compute $\mathcal{W}$, obtaining

$$\mathcal{W} = 9^{5-2-2}(\eta(2) + \eta(1)) = 18.$$

Step 5. The calculation of $\mathcal{V}$ is not required, as $n = 5$ is odd.
Step 6. Substitute the computed values into Theorem 3.1, yielding

$$N_2 = 9^{5-2} + (9 - 1) \cdot 18 = 873,$$

solutions for system (5.3).

5.1.3. Solutions to system (5.1)

Using the relationship given by (2.3), the number of solutions to system (5.1) is

$$N = \frac{N_1 - N_2}{8} = \frac{6777 - 873}{8} = 738.$$

5.2. Example 5.2

Let $\mathbb{F}_4 = \{0, 1, w, w^2\}$, where w is a primitive cube root of unity. We apply Theorem 4.1 to determine the number N of solutions in $\mathbb{F}_4^7$ to the following system over $\mathbb{F}_4$:

$$\begin{cases} Q_1 = x_1^2 + x_2x_3 + x_2^2 + wx_3x_4 + x_4^2 + w^2x_4x_5 + x_6^2 + x_7^2 = 0, \\ Q_2 = wx_1x_2 + w^2x_2x_3 + x_3^2 + wx_4^2 + x_5^2 + x_4x_5 + w^2x_6^2 + w^2x_7^2 = 0. \end{cases} \tag{5.4}$$

To compute the number of solutions to (5.4), we proceed as follows:
Step 1. For each $(z_1, z_2) \in \mathbb{F}_4^2$, define the quadratic form:

$$Q(z_1, z_2) = z_1Q_1 + z_2Q_2.$$

Step 2. Classify $Q(z_1, z_2)$ by its rank. For each $(z_1, z_2) \in \mathbb{F}_4^2$, compute the rank of the quadratic form $Q(z_1, z_2)$. In finite fields of even characteristic, the rank of a quadratic form can be determined using a standard method, as described in [7, Lemma 6.29 and Theorem 6.30]. Specifically, a non-singular linear transformation can be applied to convert the quadratic form into a canonical form, and the rank is given by the number of variables with non-zero coefficients in this canonical form.
Step 3. Determine the sets T_r and T_r' as defined in Theorem 4.1. Through computation, we obtain:

$$T_7 = \{(0, 1), (0, w), (0, w^2), (1, 0), (1, 1), (w, 0), (w, w), (w^2, 0), (w^2, w^2)\},$$

$$T_6 = \{(1, w), (1, w^2), (w, 1), (w, w^2), (w^2, 1), (w^2, w)\},$$

$$T_6' = \{(1, w^2), (w, 1), (w^2, w)\}, \text{and } T_0 = \{(0, 0)\},$$

with all other T_r and T_r' being empty.
Step 4. Substitute the computed values of $|T_r|$ and $|T_r'|$ into Theorem 4.1, yielding the number of solutions $N = 1024$ for system (5.4).

Author contributions

Xiaodie Luo and Kaimin Cheng: Conceptualization, Methodology, Validation, Writing-original draft, Writing-review & editing. All authors contributed equally to this work.

Use of Generative-AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgment

The authors would like to thank the anonymous referees for their insightful and valuable comments, which significantly enhanced the paper's presentation. The second author thanks Arne Winterhof for his hospitality and support during the second author's visit to RICAM.

This research was partially supported by the China Scholarship Council Fund (Grant No. 202301010002) and the Scientific Research Innovation Team Project of China West Normal University (Grant No. KCXTD2024-7).

Conflict of interest

The authors declare that they have no conflicts of interest.

References

1. W. Cao, A special degree reduction of polynomials over finite fields with applications, *Int. J. Number Theory*, **7** (2011), 1093–1102. https://doi.org/10.1142/S1793042111004277
2. W. Cao, Q. Sun, A deduction for counting the number of zeros of general diagonal equation over finite fields, *Finite Fields Th. Appl.*, **12** (2006), 681–692. https://doi.org/10.1016/j.ffa.2005.07.001
3. W. Cao, Q. Sun, On a class of equations with special degrees over finite fields, *Acta Arith.*, **130** (2007), 195–202. https://doi.org/10.4064/aa130-2-8
4. L. Carlitz, Pairs of quadratic equations in a finite field, *Am. J. Math.*, **76** (1954), 137–154. https://doi.org/10.2307/2372405
5. L. Carlitz, Certain special equations in a finite field, *Monatsh. Math.*, **58** (1954), 5–12. https://doi.org/10.1007/BF01478558
6. 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. https://doi.org/10.1016/j.jnt.2015.04.006
7. R. Lidl, H. Niederreiter, *Finite fields*, Cambridge: Cambridge University Press, 1996. https://doi.org/10.1017/CBO9780511525926
8. W. M. Schmidt, *Equations over finite fields: an elementary approach*, Berlin: Springer, 2006. https://doi.org/10.1007/BFb0080437
9. S. Qi, On diagonal equations over finite fields, *Finite Fields Th. Appl.*, **3** (1997), 175–179. https://doi.org/10.1006/ffta.1996.0173
10. J. Zhao, Y. Feng, S. Hong, C. Zhu, On the number of zeros of diagonal quartic forms over finite fields, *Forum Math.*, **34** (2022), 385–405. https://doi.org/10.1515/forum-2021-0196
11. G. Zhu, S. Hong, On the number of rational points of certain algebraic varieties over finite fields, *Forum Math.*, **35** (2023), 1511–1532. https://doi.org/10.1515/forum-2022-0324