Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 19, Number 2 (2023), pp. 499-513

http://www.ripublication.com/gjpam.htm

Research on Linear Codes Related to Geometric Configurations

Lvping Huang

College of Mathematics and Information,
China West Normal University, Nanchong,
Sichuan-637000, China.

Abstract

Linear codes and their Dual are an important research topic in algebraic coding. As an important class of error correcting codes, they are widely used in secret sharing schemes, combination design, authentication codes and other fields. However, their weight distributions are known only for a very small number of cases. In general the calculation of the weight distribution of linear codes is largely based on the evaluation of some exponential sums over finite fields. In this article, we applied a conic to construct a three-weight linear code on $GF(q)$, q is prime, and obtained their parameters and weight distribution by applying the theory of quadratic forms and the properties of group action.

Keywords: linear codes, Quadratic form, weight distribution, group action, conics.

1. INTRODUCTION

Linear codes over finite fields are widely used for secret schemes [26], strongly regular graphs [4], association schemes [3] and authentication codes [22] due to their linear structure. The main research content of linear codes is their bounds, minimum weight and weight distribution. The bounds of linear codes mainly provide the constraint control relationship between the minimum distance, information bits, and length of the code; Weight distribution refers to the distribution of different weight codewords in linear codes, which not only gives the error correcting ability of the code, but also allows the computation of the error probability of error detection and correction with respect to some error detection and error correction algorithms [22]. Thus the study of

the weight distribution attracts much attention in coding theory, there are many works focus on the determination of the weight distributions of linear codes (see [1]-[11] [18] [23]-[25] [27]-[29]). For more knowledge of linear codes, please refer to the references.

Let p be a prime number, $q = p^m$, m is a positive integer and $GF(q)$ denote the finite field composed of q elements. Let C be a $[n, k, d]$ linear code over a finite field, where n is the length of code C, k is the dimension, and d is the minimum distance. It is the K-dimensional subspace of $GF(q)^n$, Denote by $C^{\perp}$ the dual code of a linear code C. Let A_i denote the number of codewords with Hamming weight i in a code C of length n. The weight enumerator of C is defined by

$$1 + A_1 z + A_2 z^2 + \cdots + A_n z^n$$

The sequence $(1, A_1, A_2, \cdots, A_n)$ is called the weight distribution of the code C. A code C is said to be a t-weight code if the number of nonzero A_i in the sequence $(1, A_1, A_2, \cdots, A_n)$ is equal to t. Clearly, the weight distribution gives the minimum distance of the code.

Let $PG(n, F)$ be the n-dimensional projective space with V as the underlying n-dimensional vector space over the field $\mathbb{F}$. A hypersurface of degree d in $PG(n, F)$ is the set of points satisfying a degree d homogeneous polynomial equation. Let $PG(2, q)$ be the classical projective plane of order q with underlying three-dimensional vector space V over $\mathbb{F}_q$, the finite field of order q. A conic in $PG(2, GF(q))$ is a set of $q + 1$ points of $PG(2, GF(q))$ that are zeros of a nondegenerate homogeneous quadratic form in three variables [2, Section 1.11].

The rest of paper is organized as follows. In Section II, we introduce basic results on Characteristics of finite field and Quadratic form which will be needed in the sequel. In Section III, we present general results about three-weight linear codes, The parameters of the linear code are given by the special properties of the Quadratic form, and the weight distribution of the code is calculated by Group action. Finally, we conclude this paper in Section IV.

2. PRELIMINARIES

This section presents some basic notations, definitions, and necessary auxiliary results for the subsequent section. Let m be a positive integer, $\mathbb{F}_{p^m}$ be the finite field with p^m elements, and $\mathbb{F}_{p^m}[x]$ be the ring of polynomial in variable x. The trace function $Tr_{p^m/p}$ from $\mathbb{F}_{p^m}$ onto $\mathbb{F}_p$ is defined by

$$Tr_{p^m/p}(x) = x + x^p + \cdot + x^{p^m-1}, x \in F_{p^m}$$

Characters Over Finite Fields

Let $\mathbb{F}_q$ be a finite field with q elements, where q is a power of a prime p. Denote by ζ_p the primitive p-th root of complex unity. The additive character of $\mathbb{F}_q$ is defined as a homomorphism χ from $\mathbb{F}_q$ into the complex unit group such that

$$\chi(x+y) = \chi(x)\chi(y)$$

for $x, y \in \mathbb{F}_q$. For any $a \in \mathbb{F}_q$, defined additive character of F_q by

$$\chi_a(x) = \zeta_p^{Tr_{q/p}(ax)},\ x \in \mathbb{F}_q$$

In addition, $\chi_a : a \in \mathbb{F}_q$ is a group containing all the additive character of F_q. When $a = 0$, we obtain the trivial additive character χ_0, for which $\chi_0(x) = 1$ for all $x \in \mathbb{F}_q$. When $a = 1$, χ_1 is called the canonical additive character of F_q, and $\chi_a(x) = \chi_1(ax)$. A crucial property of the additive characters, called the orthogonality [11], is given as follows:

$$\sum_{x \in \mathbb{F}_q} \chi_1(ax) = \begin{cases} q & for\ a = 0 \\ 0 & for\ a \in \mathbb{F}_q^* \end{cases}$$

Let $GF(q)^* = GF(q)/\{0\}$. A character ψ of the multiplicative group $GF(q)^*$ is a function from $GF(q)^*$ to C^* such that

$$\psi(xy) = \psi(x)\psi(y)$$

for all $(x, y) \in GF(q)^* \times GF(q)^*$. Define the multiplication of two characters ψ, $\psi'$by $\psi\psi'(x) = \psi(x)\psi'(x)$ for $x \in GF(q)^*$. All the characters of $x \in GF(q)^*$ are given by

$$\psi_j(\alpha^k) = \zeta_{q-1}^{jk} \quad for\ k = 0, 1, \cdots, q-1.$$

where $0 \leq j \leq q-2$. Then all these ψ_j , $0 \leq j \leq q-2$, form a group under the multiplication of characters and are called multiplicative characters of $GF(q)$. In particular, ψ_0 is called the trivial multiplicative character and $\eta = \psi_{(q-1)/2}$ is referred to as the quadratic multiplicative character of $GF(q)$. The orthogonality relation of multiplicative characters is given by

$$\sum_{x \in GF(q)^*} \psi_j(x) = \begin{cases} q-1\ for\ j = 0 \\ 0 \qquad for\ j \neq 0 \end{cases}$$

Let χ be a nontrivial additive character of $GF(q)$ and let $f \in GF(q)[x]$ be a polynomial of positive degree. The character sums of the form

$$\sum_{c \in GF(q)} \chi(f(c))$$

are referred to as Weil sums. The problem of evaluating such character sums explicitly is very difficult in general. In certain special cases, Weil sums can be treated.

Quadratic forms over finite fields

In the following, we recall some necessary preliminaries on quadratic forms over finite fields. A function $f(x)$ from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$ can be viewed as an m-variable polynomial over $\mathbb{F}_p$ if we identify the finite field $\mathbb{F}_{p^m}$ with an m-dimensional vector space $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$. The function f(x) is called a quadratic form if it is a homogenous polynomial of degree two as follows:

$$f(x_1, x_2, \ldots, x_m) = \sum_{1 \le i \le j \le m} a_{ij} x_i x_j, a_{ij} \in \mathbb{F}_p$$

where we fix a basis of $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$ and identify $x \in \mathbb{F}_{p^m}$ with a vector $(x_1, x_2, \cdots, x_m) \in \mathbb{F}_{p^m}$. Then the rank of the quadratic form $f(x)$ is defined as the codimension of $\mathbb{F}_p$-vector space

$$V = \{x \in \mathbb{F}_p \mid f(x+z) - f(x) - f(z) = 0, z \in \mathbb{F}_p\}$$

which is denote by rank $f(x)$. For a quadratic form $f(x)$ with m variables over $\mathbb{F}_p$, p is odd prime, there exists a symmetric matrix A such that $f(x) = XAX^T$, where $X = (x_1, x_2, \cdots, x_m) \in \mathbb{F}_p^m$ and X^T denote the transpose of X. The determinant det(f) of $f(x)$ is defined to be the determinant of A, and $f(x)$ is non-degenerate if $det(f) \neq 0$. There exists a nonsingular matrix M such that MAM^T is a diagonal matrix, making a nonsingular linear substitution $X = YM$ with $Y = (y_1, y_2, \cdots, y_m)$ to the quadratic form $f(x)$, we have

$$f(x) = YMAM^\top Y^\top = \sum_{i=0}^{r} a_i y_i^2, a_i \in \mathbb{F}_p,$$

where r is the rank of $f(x)$.

Quadratic forms have been well studied (see [16]). It should be noted that the rank of a quadratic form over $\mathbb{F}_p$ is the smallest number of variables required to represent the quadratic form, up to nonsingular coordinate transformations. Mathematically, any quadratic form of rank r can be transferred to three canonical forms.

Definition 2.1 *[19] For any finite field $\mathbb{F}_q$, two quadratic form f and g over $\mathbb{F}_q$ are called equivalent if f can be transformed into g by means of a nonsingular linear substitution of indeterminates.*

Equivalence of quadratic forms is easily seen to be an equivalence relation. and if f and g are equivalent, then for any $b \in \mathbb{F}_q$ the equations $f(x_1, x_2, \cdots, x_n) = b$ and

$g(x_1, x_2, \cdots, x_n) = b$ have the same number of solutions in $\mathbb{F}_q^n$. For any finite field $\mathbb{F}_q$ the inter-valued funtion v on $\mathbb{F}_q$ is defined by $v(b) = -1$ for $b \in \mathbb{F}_q^*$ and $v(0) = q - 1$. The following lemma is a well known result about solutions of non-degenerate quadratic forms, which will be used to determine the weight distribution of C.

Lemma 1 *[19]Let f be a non-degenerate quadratic over $\mathbb{F}_q$, q odd, in an even number n of indeterminates. Then for $b \in \mathbb{F}_q$ the number of solutions of the equations $f(x_1, x_2, \cdots, x_n) = b$ in $\mathbb{F}_q^n$ is*

$$q^{n-1} + v(b)q^{\frac{(n-1)}{2}}\eta((-1)^{\frac{n}{2}}\Delta)$$

where η is the quadratic character of $\mathbb{F}_q$ and $\Delta = det(f)$.

Lemma 2 *[19]Let f be a nondegenerate quadratic over $\mathbb{F}_q$, q odd, in an odd number n of indeterminates. Then for $b \in \mathbb{F}_q$ the number of solutions of the equations $f(x_1, x_2, \cdots, x_n) = b$ in $\mathbb{F}_q^n$ is*

$$q^{n-1} + q^{\frac{(n-1)}{2}}\eta((-1)^{\frac{(n-1)}{2}}b\Delta)$$

where η is the quadratic character of $\mathbb{F}_q$ and $\Delta = det(f)$.

Lemma 3 *[19]Let $f \in [x_1, x_2, \cdots, x_n]$, be a nondegenerate quadratic over $\mathbb{F}_q$, q even. If n is odd, then f is eqivalent to*

$$x_1x_2 + x_3x_4 + \cdots + x_{n-2}x_{n-1} + x_n^2,$$

If n is even, Then f is either equivalent to

$$x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n$$

or to a quadratic form of the type

$$x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n + x_{n-1}^2 + x_{n-1}^2 + ax_n^2$$

where $a \in \mathbb{F}_q$ satisfies $Tr_{\mathbb{F}_q}(a) = 1$.

Lemma 4 *[19]Let $\mathbb{F}_q$ be a finite field with q even and let $b \in \mathbb{F}_q$, then for odd n, the number of solutions of the equation*

$$x_1x_2 + x_3x_4 + \cdots + x_{n-2}x_{n-1} + x_n^2 = b,$$

in $\mathbb{F}_q^n$ *is* q^{n-1}. *For n is even, the number of solutions of the equation*

$$x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n = b$$

in $\mathbb{F}_q^n$ *is* $q^{n-1} + v(b)q^{(n-2)/2}$. *For n is even and* $a \in \mathbb{F}_q$ *with* $Tr_{\mathbb{F}_q}(a) = 1$, *the number of solutions of the equation*

$$x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n + x_{n-1}^2 + x_{n-1}^2 + ax_n^2 = b$$

in $\mathbb{F}_q^n$ *is* $q^{n-1} - v(b)q^{(n-1)/2}$.

Group action

Let group G act on a nonempty set X, and define a equivalence relation on set X, that is, for $x, y \in X$, if there is an element x in G that makes $y = g(x)$, then say $x \sim y$, under this Equivalence relation, the elements of set X are divided into Equivalence class, so the Equivalence class divided into is called orbit, and the orbit containing x is a subset as follows:

$$O_x = \{g(x)|g \in G\}$$

Definition 2.2 *[12] Let* G *act on* X *and let* $x \in X$. *Define the stabilizer of* x *in* G *to be*

$$G_x = \{g \in G : x \cdot g = x\}.$$

Theorem 2.1 *[16] Let* G *act on the set* X. *Then for* $x \in X$,

$$|Orb(x)| = |G : G_x|.$$

Let $\phi \in F[x, y, z]$ be a homogeneous polynomial of degree 2. Then the set $C = \{x \in PG(2, F) : \phi(x) = 0\}$ is called a conic. A conic is called irreducible, or non-degenerate, if the polynomial ϕ cannot be written as a product of two degree 1 polynomials over F and every extension of F. Here we let $Q(2, q)$ be the set of quadrics in $PG(2, q)$, namely, the varieties $V(F)$, where

$$F = ax^2 + by^2 + cz^2 + dxy + eyz + fzx$$

and

$$|V(F)| = (q^6 - 1)/(q - 1)$$

If $V(F)$ is nonsingular, then the quadric is a conic. If $V(F)$ is singular, then F can be reduced to a form in one or two variables. The elements in $V(F)$ are divided into four orbits under the action of $PGL(3, q)$ as follows table[14]:

Table 1: Four orbits of elements of $V(F)$ under the action of group $PGL(3,q)$

	$Canonical$	$Number\ of\ elements\ in\ orbit$
$(i)singular$	$(a)x^2$	q^2+q+1
	$(b)xy$	$q(q+1)(q^2+q+1)/2$
	$(c)x^2+axy+by^2$	$q(q-1)(q^2+q+1)/2$
$(ii)nonsingular$	x^2+yz	q^5-q^2

3. THE WEIGHT DISTRIBUTION OF C

The objective of this section is to present a type of three-weight linear code which generated by conic, and investigate the weight enumerator and complete weight enumerator of this code. Let $q = p^m$ with p a prime. Let V be the conic defined by

$$V = \{(x^2, y^2, z^2, xy, yz, zx) : x, y, z \in GF(q)\},$$

Let C be a linear code over $GF(q)$ with the generator matrix G, is given as follows:

$$G = \begin{pmatrix} x^2 \\ y^2 \\ z^2 \\ xy \\ yz \\ zx \end{pmatrix}_{(x,y,z)\in\mathbb{F}_q^3}$$

which is a $6 \times q^3$ matrix over $GF(q)$, The code word for C is

$$C = \{(f(x,y,z))_{(x,y,z)\in GF(q)^3} : a, b, c, d, e, f \in GF(q)\}$$

where $f(x,y,z) = ax^2+by^2+cz^2+dxy+eyz+fzx$. Obviously, the length of code C is q^3 and the dimension 6, In general, it is difficult to determine the minimal distance of C not to mention the weight distribution. Here we will use the properties of Quadratic form to solve this problem. When q is odd, every Quadratic form is equivalent to a diagonal form.

First, write the Quadratic form $f(x,y,z) = ax^2 + by^2 + cz^2 + dxy + eyz + fzx$ in matrix form , namely

$$f(x,y,z) = \begin{pmatrix} x & y & z \end{pmatrix} \begin{pmatrix} a & \frac{d}{2} & \frac{f}{2} \\ \frac{d}{2} & b & \frac{e}{2} \\ \frac{f}{2} & \frac{e}{2} & c \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

For the above Quadratic form, we want to convert it to diagonal form, which is equivalent to converting its coefficient matrix to Diagonal matrix. Here we take matrix D as follows:

$$D = \begin{pmatrix} 1 & -\frac{d}{2a} & \frac{b(e-2f)}{4ab-d^2} \\ 0 & 1 & \frac{df-2ea}{4ab-d^2} \\ 0 & 0 & 1 \end{pmatrix}$$

By calculating, We have

$$D'AD = \begin{pmatrix} a & 0 & 0 \\ 0 & \frac{4ab-d^2}{4a} & 0 \\ 0 & 0 & \frac{4abc-d^2c-e^2a-f^2b-edf}{4ab-d^2} \end{pmatrix}$$

where

$$A = \begin{pmatrix} a & \frac{d}{2} & \frac{f}{2} \\ \frac{d}{2} & b & \frac{e}{2} \\ \frac{f}{2} & \frac{e}{2} & c \end{pmatrix}$$

Now we equate quadratic form $f(x, y, z)$ into the standard form $g(x, y, z)$

$$g(x, y, z) = ax^2 + \frac{4ab - d^2}{4a}y^2 + \frac{4abc - d^2c - e^2a - f^2b - edf}{4ab - d^2}z^2$$

In the following content, we will study the parameters and weight distribution of linear codes C through the exponential sum and the related properties of Quadratic form.

Theorem 3.1 *Let $q = p^m$ and p is prime number, $m > 1$. Then C is an three-weight linear code with parameters $[p^{3m}, 6, p^{3m} - 2p^{2m} + p^m]$ over $\mathbb{F}_q$ and the weight enumerator is*

$$1+(q^5+q+1)(q-1)z^{q^3-q^2}+\frac{q(q^2-1)(q^2+q+1)}{2}z^{q^3-2q^2+q}+\frac{q(q-1)(q^2+q+1)}{2}z^{q^3-q}$$

the weight distribution in Table 2.

Proof Firstly, let

$$N_0(a, b, c, d, e, f) = \sharp\{(x, y, z) \in GF(q)^3 : f(x, y, z) = 0\}$$

and

$$N_1(a, b, c, d, e, f) = \sharp\{(x, y, z) \in GF(q)^3 : f(x, y, z) \neq 0\}$$

Table 2: The weight distribution of C for odd m.

$Hamming\ Weight$	$Multiplicity$
0	1
$p^{3m}-p^{2m}$	$(p^{5m}+p^m+1)(p^m-1)$
$p^{3m}-2p^{2m}+p^m$	$p^m(p^{2m}-1)(p^{2m}+p^m+1)/2$
$p^{3m}-p^m$	$p^m(p^m-1)^2(p^{2m}+p^m+1)/2$

where $f(x,y,z)=ax^2+by^2+cz^2+dxy+eyz+fzx$. q is odd, According to Theorem 2.1, the Quadratic form under non degenerate linear transformation is equivalent, and two Quadratic form under equivalent conditions have the same number of solutions. So we replaced calculating the number of zeros for $f(x,y,z)$ with calculating the number of zeros for $g(x,y,z)$ in the $GF(q)$.

When the rank of A is equal to 3, According to Lemma 2.2, it can be inferred that

$$\begin{aligned} N_0(a,b,c,d,e,f) &= N(g(x,y,z)=0:(x,y,z)\in GF(q)^3) \\ &= q^{m-1}+q^{\frac{m-1}{2}}\eta(0\cdot(-1)^{\frac{m-1}{2}}det(g)) \\ &= q^2 \end{aligned}$$

When the $rank(A)=2$, $f(x,y,z)$ is equivalent to a diagonal type $g(x,y,z)=ax^2+\frac{4ab-d^2}{4a}y^2$.

$$\begin{aligned} pN_0(a,b,c,d,e,f) &= \sum_{(x,y,z)\in GF(q)^3}\sum_{h\in GF(p)}\chi(hg(x,y,z)) \\ &= \sum_{h\in GF(p)}\sum_{(x,y,z)\in GF(q)^3}\chi(h(ax^2+\frac{4ab-d^2}{4a}y^2)) \\ &= q\sum_{h\in GF(p)}\sum_{(x,y)\in GF(q)^2}\chi(ahx^2+\frac{4ab-d^2}{4a}hy^2) \end{aligned}$$

let $m(x,y)=ax^2+\frac{4ab-d^2}{4a}y^2$, we calculate the number of zeros of $m(x,y)$. Assume

$$N_0'=\sharp\{(x,y)\in GF(q)^2:m(x,y)=0\}$$

According to Lemma 2.1, it can be inferred that:

$$\begin{aligned} PN_0' &= \sum_{h\in GF(p)} \sum_{(x,y)\in GF(q)^2} \chi(ahx^2 + \frac{4ab-d^2}{4a}hy^2) \\ &= p(q + v(0)q^{\frac{n-1}{2}}\eta((-1)^{\frac{n}{2}}det(f))) \\ &= p(q + (q-1)\eta(\frac{4ab-d^2}{4})\eta(-1)) \end{aligned}$$

so

$$N_0' = \begin{cases} 2q-1, & for \quad \eta(\frac{4ab-d^2}{4})\eta(-1) = 1 \\ 1, & for \quad \eta(\frac{4ab-d^2}{4})\eta(-1) = -1. \end{cases}$$

in the case

$$N_0(a,b,c,d,e,f) = \begin{cases} 2p^{2m} - p^m, & for \quad \eta(\frac{4ab-d^2}{4})\eta(-1) = 1 \\ p^m, & for \quad \eta(\frac{4ab-d^2}{4})\eta(-1) = -1. \end{cases}$$

When the $rank(A) = 1$, then we have $g(x, y.z) = ax^2$.

$$\begin{aligned} pN_0(a,b,c,d,e,f) &= \sum_{(x,y,z)\in GF(q)^3} \sum_{h\in GF(p)} \chi(hg(x,y,z)) \\ &= \sum_{h\in GF(p)} \sum_{(x,y,z)\in GF(q)^3} \chi(h(ax^2)) \\ &= q^2 \sum_{h\in GF(p)} \sum_{x\in GF(q)} \chi(ahx^2) \end{aligned}$$

Similar to above let $m(x) = ax^2$. Assume

$$N_0'' = \sharp\{x \in GF(q) : m(x) = 0\}$$

Then

$$\begin{aligned} pN_0'' &= \sum_{h\in GF(p)} \sum_{x\in GF(q)} \chi(ahx^2) \\ &= p(q^{n-1} + q^{\frac{n-1}{2}}\eta(0)) \\ &= p \end{aligned}$$

so

$$N_0'' = 1$$

Then

$$N_0(a, b, c, d, e, f) = p^{2m}.$$

When q is even, according to Lemma 2.3, The Quadratic form can be equivalent to different forms according to whether the variable is odd or even.
When the rank of A is equal to 3, According to lemma 2.3 $f(x, y, z)$ is equivalent to

$$h(x, y, z) = xy + z^2,$$

and according to the Lemma 2.4, the number of solutions of the Quadratic form $h(x, y, z)$ is

$$\begin{aligned} N_0(a, b, c, d, e, f) &= N(h(x, y, z) = 0 : (x, y, z) \in GF(q)^3) \\ &= q^{n-1} \\ &= q^2 \end{aligned}$$

When the rank of A is equal to 2, According to lemma 2.3 $f(x, y, z)$ is equivalent to

$$h(x, y) = xy$$

or

$$h(x, y) = xy + az^2$$

where $a \in \mathbb{F}_q$ satisfies $Tr_{\mathbb{F}_q}(a) = 1$. For the first case, the number of solutions of the Quadratic form $h(x, y)$ is

$$\begin{aligned} N(h(x, y) = 0) &= q^{n-1} + v(0)q^{(n-2)/2} \\ &= 2q - 1 \end{aligned}$$

Further calculations have shown that

$$\begin{aligned} pN_0(a, b, c, d, e, f) &= \sum_{(x,y,z)\in GF(q)^3} \sum_{h\in GF(p)} \chi(hf(x, y, z)) \\ &= qpN(h(x, y) = 0) \end{aligned}$$

Then

$$N_0(a, b, c, d, e, f) = 2q^2 - q.$$

For the second case, Similar to the above case, we have

$$\begin{aligned} N(h(x, y) = 0) &= q^{n-1} - v(0)q^{(n-2)/2} \\ &= 1 \end{aligned}$$

therefore

$$N_0(a,b,c,d,e,f) = q.$$

When the $rank(A) = 1$, According to lemma 2.3 and lemma 2.4 $f(x,y,z)$ is equivalent to

$$h(x) = x^2$$

and

$$N(h(x) = 0) = 1$$

Then

$$\begin{aligned} N_0(a,b,c,d,e,f) &= q^2 N(h(x) = 0) \\ &= q^2 \end{aligned}$$

by the discussions above we deduce that

$$Wt(C) = \begin{cases} p^{3m} - p^{2m}, for\ Rank(A) = 3\ or\ Rank(A) = 1 \\ p^{3m} - 2p^{2m} + p^m,\ for\ Rank(A) = 2,\ \eta(\frac{4ab - d^2}{4})\eta(-1) = 1 \\ p^{3m} - p^m,\ for\ Rank(A) = 2,\ \eta(\frac{4ab - d^2}{4})\eta(-1) = -1. \end{cases}$$

We will calculate the weight distribution of code C in the following content. Firstly, The Quadric in PG (2, q) is divided into four categories under the action of $PGL(3,q)$ as follows:

Type I $\mathcal{P}_2 = V(X_0^2 + X_1X_2)$ is a conic, comprising $q+1$ points, no three of which are collinear;

Type II $\Pi_0\mathcal{H}_1 = V(X_0X_1)$ is a line pair u_0, u_1;

Type III $\Pi_0\varepsilon_1 = V(f(X_0, X_1))$) is a single point U_2;

Type IV $\Pi_1\mathcal{P}_0 = V(X_0^2)$ is a single line u_0;

According to Table 1, the orbit sizes of these four types are presented, and the discussions above we deduce that

$$Wt(C) = \begin{cases} 0 & with \quad 1 \quad times \\ p^{3m} - p^{2m} & with \quad (p^{5m} + p^m + 1)(p^m - 1) \quad times \\ p^{3m} - 2p^{2m} + p^m & with \quad p^m(p^{2m} - 1)(p^{2m} + p^m + 1)/2 \quad times \\ p^{3m} - p^m & with \quad p^m(p^m - 1)^2(p^{2m} + p^m + 1)/2 \quad times. \end{cases}$$

Example 5 *Let $\mathcal{C}$ be the linear code in Theorem 3.1.*

(1) If $p = 2$, $m = 2$, then $\mathcal{C}$ has parameters $[64, 6, 36]$ and weight enumerator $1 + 630x^{36} + 3087x^{48} + 378x^{60}$.

(2) If $p = 2$, $m = 3$, then $\mathcal{C}$ has parameters $[512, 6, 392]$ and weight enumerator $1 + 18396x^{392} + 229439x^{448} + 920x^{20} + 14308x^{504}$.

(3) If $p = 3$, $m = 2$, then $\mathcal{C}$ has parameters $[729, 6, 576]$ and weight enumerator $1 + 32760x^{576} + 472472x^{648} + 26208x^{720}$.

These results have been verified by Magma.

4. CONCLUSION

In this article mainly uses quadratic curves to construct a class of linear codes, and calculates the parameters and weight distribution. The first section, we introduces the research background and progress of this kind of linear codes, and introduces the role of weight distribution of linear codes in Coding theory. The second section mainly introduces the relevant lemma. In the third section, the calculation of weight distribution is mainly based on the group characteristics on the Finite field and the relevant properties of Quadratic form. We obtained its weight through the discussion of the rank of the coefficient matrix of Quadratic form, and then the weight distribution is obtained through Group action. Through calculation, we found that the code we constructed is a three weight linear code with parameter $[p^{3m}, 6, p^{3m} - 2p^{2m} + p^m]$ on $GF(q)$.

REFERENCES

[1] C. Tang, Y. Qi, D. Huang, Two-weight and three-weight linear codes from square functions, IEEE Commun. Lett. (2015) **20**, 29-32 .

[2] C. Tang, N. Li, Y. Qi, Z. Zhou, T. Helleseth, Linear codes with two or three weights from weakly regularbent functions, IEEE Trans. Inf. Theory (2016) 62 1166-1176.

[3] Calderbank A R, Goethals J M. Three-weight codes and association schemes. Philips J. Res, (1984), 39: 143-152.

[4] Calderbank A R, Kantor W M. The geometry of two-weight codes. Bull. London Math. Soc, (1986), 18: 97-122

[5] C. Ding, C. Li, N. Li Z. Zhou, Three-weight cyclic codes and their weight distributions, Discrete Math. (2016) 339 415-427.

[6] E.F. Assmus, J.D. Key, Designs and Their Codes, Cambridge Univ. Press, Cambridge, (1992).

[7] F. Li, Q. Wang, D. Lin, A class of three-weight and five-weight linear codes, Discrete Appl. Math. (2018) **241**, 25-38 .

[8] Feng, Tao, Michael Kiermaier, Peixian Lin and Kai-Uwe Schmidt. Linear codes associated with the Desarguesian ovoids in $Q^+(7,q)$. ArXiv (2022) abs/2208.12919.

[9] G. Luo, X. Cao, S. Xu, J. Mi, Binary linear codes with two or three weights from niho exponents, Cryptogr. Commun. (2018) **10**, 301-318.

[10] G. Jian, Z. Lin, R. Feng, Two-weight and three-weight linear codes based on Weil sums, Finite Fields Appl. (2019) 57 92-107.

[11] Hussain, Fawad. Homological Properties of Invariant Rings of Finite Groups. (2011).

[12] J.W.P. Hirschfeld, Projective Geometries over Finite Fields, 2nd edition, Cambridge Univ. Press,Cambridge, (1998).

[13] J. W. P. Hirschfeld. Projective Geometries over Finite Fields. Oxford University Press,Oxford, (1979), xii+474 pp.

[14] J. W. P. Hirschfeld and J. A. Thas. General Galois Geometries. Oxford University Press, Oxford, (1991), x+407 pp.

[15] Klapper A.: Cross-correlations of quadratic form sequences in odd characteristic, Des. Codes Cryptogr. (1997) 3, 289C305 .

[16] L. Smith. Polynomial invariants of finite groups, volume 6 of Research Notes in Mathematics. A K Peters Ltd., Wellesley, MA, (1995) 29.

[17] Lavrauw M , Popiel T , Sheekey J. Combinatorial invariants for nets of conics in $extPG(2,q)$. Designs, Codes and Cryptography, (2022), 90(9): 2021-2067.

[18] P. Tan, Z. Zhou, D. Tang, T. Helleseth, The weight distribution of a class of two-weight linear codes derived from Kloosterman sums, Cryptogr. Commun. (2018) **10**, 291-299.

[19] R. Lidl and H. Niederreiter, Finite Fields, Cambridge, MA, USA, Cambridge Univ. Press, 1997.(2000)

[20] Simeon B. Finite Geometry and Combinatorial Applications.Cambridge University Press, (2015):11-286

[21] T. Klove, Codes for Error Detection, Hackensack, NJ: world Scientific, (2007).

[22] Wu Huaxiong, Jing Yang and Keqin Feng. The Weight Distributions of Two Classes of Linear Codes From Perfect Nonlinear Functions. ArXiv (2023) abs/2306.06422.

[23] Xu, Guangkui and Xiwang Cao. Linear Codes With Two or Three Weights From Some Functions With Low Walsh Spectrum in Odd Characteristic. ArXiv (2015) abs/1510.01031.

[24] X. Wang, D. Zheng, H. Liu, Several classes of linear codes and their weight distributions, Appl. Algebra Eng. Commun. Comput. (2019) **30**, 75-92.

[25] X. Wang, D. Zheng, The subfield codes of several classes of linear codes, Cryptogr. Commun. (2020) **12**, 1111-1131 .

[26] Yuan J, Ding C. Secret sharing schemes from three classes of linear codes. IEEE Trans Inform Theory, (2006), 52: 206-212

[27] Y. Xia, C. Li, Three-weight ternary linear codes from a family of power functions, Finite Fields Appl. (2017) **46**, 17-37 .

[28] Zhou, Zhengchun, Nian Li, Cuiling Fan and Tor Helleseth. Linear codes with two or three weights from quadratic Bent functions. Designs, Codes and Cryptography (2015) 81 : 283-295.

[29] Z. Heng, Q. Wang, C. Ding: Two families of optimal linear codes and their subfield codes, IEEE Trans. Inf. Theory (2020) **66**(11), 6872-6883.