

Weight distributions and weight hierarchies of a family of *p*-ary linear codes

Fei Li¹ · Xiumei Li²

Received: 26 September 2020 / Revised: 7 August 2021 / Accepted: 6 October 2021 / Published online: 29 October 2021 © The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2021

Abstract

The weight distribution and weight hierarchy of a linear code are two important research topics in coding theory. In this paper, by choosing proper defining sets from inhomogeneous quadratic functions over \mathbb{F}_q^2 , we construct a family of three-weight *p*-ary linear codes and determine their weight distributions and weight hierarchies. Most of the codes can be used in secret sharing schemes.

Keywords Linear code \cdot Quadratic form \cdot Weight distribution \cdot Weight hierarchy \cdot Generalized Hamming weight

Mathematics Subject Classification 94B05 · 11T71

1 Introduction

For an odd prime number p and a positive integer e, let \mathbb{F}_q be the finite field with $q = p^e$ elements and \mathbb{F}_q^* be its multiplicative group.

An [n, k, d] p-ary linear code C is a k-dimensional subspace of \mathbb{F}_p^n with minimum (Hamming) distance d. For $0 \leq i \leq n$, 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

Communicated by V. A. Zinoviev.

 Xiumei Li lxiumei2013@qfnu.edu.cn
 Fei Li cczxlf@163.com

¹ Faculty of School of Statistics and Applied Mathematics, Anhui University of Finance and Economics, Bengbu 233041, Anhui, People's Republic of China

The research was supported by Anhui Provincial Natural Science Foundation No. 1908085MA02 and the National Science Foundation of China Grant Nos. 12001312 and 11701001.

² School of Mathematical Sciences, Qufu Normal University, Qufu 273165, Shandong, People's Republic of China

 $1 + A_1 z + A_2 z^2 + \dots + A_n z^n$. The sequence $(1, A_1, \dots, A_n)$ is called the weight distribution of *C*. A code *C* is said to be a *t*-weight code if the number of nonzero A_i in the sequence (A_1, \dots, A_n) is equal to *t*. The weight distribution can give the minimum distance of the code. Moreover, it allows the computation of the error probability of error detection and correction [23].

The weight distribution of a linear code is an important research topic in coding theory. Some researchers devoted themselves to calculating the weight distributions of linear codes [8,14,15,37,49]. Linear codes with a few weights can be applied to secret sharing [50], association schemes [5], combinatorial designs [38], authentication codes [13] and strongly regular graphs [6]. There are some studies about linear codes with a few weights, for which the reader is referred to [22,24,26,33,34,36].

The weight hierarchy of a linear code is another important research topic in coding theory [4,7,16,17,20,45,46,48]. We recall the definition of the generalized Hamming weights of linear codes [45]. For an [n, k, d] code C and $1 \le r \le k$, denote by $[C, r]_p$ the set of all its \mathbb{F}_p -vector subspaces with dimension r. For $H \in [C, r]_p$, define $\text{Supp}(H) = \bigcup_{c \in H} \text{Supp}(c)$, where Supp(c) is the set of coordinates where c is nonzero, that is,

Supp
$$(H) = \{ i : 1 \le i \le n, c_i \ne 0 \text{ for some } c = (c_1, c_2, \dots, c_n) \in H \}.$$

The *r*-th generalized Hamming weight (GHW) $d_r(C)$ of C is defined to be

$$d_r(C) = \min\left\{ |\operatorname{Supp}(H)| : H \in [C, r]_p \right\}, \ 1 \le r \le k.$$

It is easy to see that $d_1(C)$ is the minimum distance d. The weight hierarchy of C is defined as the sequence $(d_1(C), d_2(C), \dots, d_k(C))$. For more details, one is referred to [18]. There are some results about the weight hierarchies of linear codes [3,21,27–29,31,35,47].

Let Tr denote the trace function from \mathbb{F}_q onto \mathbb{F}_p throughout this paper. For $D = \{d_1, d_2, \ldots, d_n\} \subseteq \mathbb{F}_q^*$, a *p*-ary linear code C_D of length *n* is defined by

$$C_{\mathrm{D}} = \left\{ \left(\mathrm{Tr}(xd_1), \mathrm{Tr}(xd_2), \dots, \mathrm{Tr}(xd_n) \right) : x \in \mathbb{F}_q \right\}.$$
(1)

Here *D* is called the defining set of C_D and C_D can be called a trace code. This construction technique is called the defining-set construction of linear codes, which was first proposed by Ding et al. [10]. The defining-set construction is generic in the sense that many classes of known codes can be produced by selecting some proper defining sets. It has attracted a lot of attention, and a huge amount of linear codes with good parameters have been obtained [9,11,12,14,44,49,52].

In recent years, Shi et al. [39-43] refined the technique of the study of trace codes by using ring extensions of a finite field coupled with a linear Gray map and obtained many families of *p*-ary codes with few weights over different finite rings. Most of their obtained codes are optimal and minimal codes, which can be applied to secret sharing schemes (SSS).

Li et al. [25] extended Ding's defining-set construction as follows. Recall that the ordinary inner product of vectors $\mathbf{x} = (x_1, x_2, \dots, x_s), \ \mathbf{y} = (y_1, y_2, \dots, y_s) \in \mathbb{F}_a^s$ is

$$\mathbf{x} \cdot \mathbf{y} = x_1 y_1 + x_2 y_2 + \dots + x_s y_s.$$

A *p*-ary linear code C_D with length *n* can be defined by

$$C_{\rm D} = \left\{ \left({\rm Tr}(\mathbf{x} \cdot \mathbf{d}_1), {\rm Tr}(\mathbf{x} \cdot \mathbf{d}_2), \dots, {\rm Tr}(\mathbf{x} \cdot \mathbf{d}_n) \right) : \mathbf{x} \in \mathbb{F}_q^s \right\},\tag{2}$$

🖉 Springer

where $D = \{d_1, d_2, \dots, d_n\} \subseteq \mathbb{F}_q^s \setminus \{(0, 0, \dots, 0)\}$ is also called the defining set of C_D . Using this construction, some classes of linear codes with few weights have been constructed [2,22,26,30,31].

Tang et al. [44] constructed a *p*-ary linear code C_D in (1) with at most five nonzero weights from inhomogeneous quadratic function and their defining set is $D = \{x \in \mathbb{F}_q^* : f(x) - \text{Tr}(\alpha x) = 0\}$, where $\alpha \in \mathbb{F}_q^*$ and f(x) is a homogeneous quadratic function from \mathbb{F}_q onto \mathbb{F}_p defined by

$$f(x) = \sum_{i=0}^{e-1} \text{Tr}(a_i x^{p^i + 1}), \ a_i \in \mathbb{F}_q.$$
 (3)

In this paper, inspired by the works of [28,44], we choose a defining set contained in \mathbb{F}_q^2 as follows. For $\alpha \in \mathbb{F}_q^*$, set

$$D = D_{\alpha} = \left\{ (x, y) \in \mathbb{F}_{q}^{2} \setminus \{ (0, 0) \} : f(x) + \operatorname{Tr}(\alpha y) = 0 \right\} = \left\{ d_{1}, \dots, d_{n} \right\},$$
(4)

where f(x) is defined in (3) and non-degenerate. So, the corresponding *p*-ary linear codes $C_{\rm D}$ in (2) is

$$C_{\rm D} = \left\{ \left({\rm Tr}(\mathbf{x} \cdot \mathbf{d}_1), {\rm Tr}(\mathbf{x} \cdot \mathbf{d}_2), \dots, {\rm Tr}(\mathbf{x} \cdot \mathbf{d}_n) \right) : \mathbf{x} \in \mathbb{F}_q^2 \right\}.$$
(5)

We mainly determine their weight distributions and weight hierarchies.

The remainder of this paper is organized as follows. Section 2 introduces some basic notation and results about quadratic forms. Section 3 presents the linear codes with three nonzero weights and determines their weight distributions and weight hierarchies. Section 4 summarizes this paper.

2 Preliminaries

In this section, we state some notation and basic facts on quadratic forms and f defined in (3). These results will be used in the rest of the paper.

2.1 Some notation fixed throughout this paper

For convenience, we fix the following notation. For basic results on cyclotomic field $\mathbb{Q}(\zeta_p)$, one is referred to [19].

- Let Tr be the trace function from \mathbb{F}_q to \mathbb{F}_p . Namely, for each $x \in \mathbb{F}_q$,

$$\operatorname{Tr}(x) = x + x^p + \dots + x^{p^{e-1}}.$$

 $- p^* = (-1)^{\frac{p-1}{2}} p.$

- $-\zeta_p = \exp(\frac{2\pi i}{p})$ is a primitive *p*-th root of unity.
- $-\bar{\eta}$ is the quadratic character of \mathbb{F}_{p}^{*} . It is extended by letting $\bar{\eta}(0) = 0$.
- Let \mathbb{Z} be the rational integer ring and \mathbb{Q} be the rational field. Let \mathbb{K} be the cyclotomic field $\mathbb{Q}(\zeta_p)$. The field extension \mathbb{K}/\mathbb{Q} is Galois of degree p-1. The Galois group $\operatorname{Gal}(\mathbb{K}/\mathbb{Q}) = \{\sigma_z : z \in (\mathbb{Z}/p\mathbb{Z})^*\}$, where the automorphism σ_z is defined by $\sigma_z(\zeta_p) = \zeta_p^z$.

$$-\sigma_{z}(\sqrt{p^{*}}) = \bar{\eta}(z)\sqrt{p^{*}}, \text{ for } 1 \le z \le p-1.$$

- Let $\langle \alpha_{1}, \alpha_{2}, \dots, \alpha_{r} \rangle$ denote a space spanned by $\alpha_{1}, \alpha_{2}, \dots, \alpha_{r}$.

2.2 Quadratic form

Viewing \mathbb{F}_q as an \mathbb{F}_p -linear space and fixing $\upsilon_1, \upsilon_2, \ldots, \upsilon_e \in \mathbb{F}_q$ as its \mathbb{F}_p -basis, then for any $x = x_1\upsilon_1 + x_2\upsilon_2 + \cdots + x_e\upsilon_e \in \mathbb{F}_q$ with $x_i \in \mathbb{F}_p$, $i = 1, 2, \ldots, e$, there is an \mathbb{F}_p -linear isomorphism $\mathbb{F}_q \simeq \mathbb{F}_p^e$ defined as:

$$x = x_1\upsilon_1 + x_2\upsilon_2 + \dots + x_e\upsilon_e \mapsto X = (x_1, x_2, \dots, x_e),$$

where $X = (x_1, x_2, ..., x_e)$ is called the coordinate vector of x under the basis $v_1, v_2, ..., v_e$ of \mathbb{F}_q .

A quadratic form g over \mathbb{F}_q with values in \mathbb{F}_p can be represented by

$$g(x) = g(X) = g(x_1, x_2, \dots, x_e) = \sum_{\substack{1 \le i, j \le e \\ = XAX^T}} a_{ij} x_i x_j$$

where $A = (a_{ij})_{n \times n}, a_{ij} \in \mathbb{F}_p, a_{ij} = a_{ji}$ and X^T is the transposition of X. Denote by $R_g = \text{Rank } A$ the rank of g, there exists an invertible matrix M over \mathbb{F}_p such that

$$MAM^{I} = \operatorname{diag}(\lambda_{1}, \lambda_{2}, \ldots, \lambda_{R_{p}}, 0, \ldots, 0)$$

is a diagonal matrix, where $\lambda_1, \lambda_2, \ldots, \lambda_{R_g} \in \mathbb{F}_p^*$. Let $\Delta_g = \lambda_1 \lambda_2 \cdots \lambda_{R_g}$, and $\Delta_g = 1$ if $R_g = 0$. We call $\bar{\eta}(\Delta_g)$ the sign ε_g of the quadratic form g. It is an invariant under nonsingular linear transformations in matrix.

Let

$$F(x, y) = \frac{1}{2} (g(x + y) - g(x) - g(y)).$$

For an *r*-dimensional subspace *H* of \mathbb{F}_q , its dual space H^{\perp_g} is defined by

$$H^{\perp_g} = \left\{ x \in \mathbb{F}_q : F(x, y) = 0, \text{ for any } y \in H \right\}.$$

Restricting the quadratic form g to H, it becomes a quadratic form denoted by $g|_H$ over H in r variables. In this situation, we denote by R_H and ε_H the rank and sign of $g|_H$, respectively.

In the following, we suppose $R_g = e$, i.e., g is a non-degenerate quadratic form. For $\beta \in \mathbb{F}_p$, set

$$\overline{D}_{\beta} = \Big\{ x \in \mathbb{F}_q | g(x) = \beta \Big\},\tag{6}$$

we shall give some lemmas, which are essential to prove our main results.

Lemma 1 [28, Proposition 1] Let g be a non-degenerate quadratic form and H be an rdimensional nonzero subspace of \mathbb{F}_a , then

$$|H \cap \overline{D}_{\beta}| = \begin{cases} p^{r-1} + v(\beta)\overline{\eta}((-1)^{\frac{R_{H}}{2}})\varepsilon_{H}p^{r-\frac{R_{H}+2}{2}}, & \text{if } R_{H} \equiv 0 \pmod{2}, \\ p^{r-1} + \overline{\eta}((-1)^{\frac{R_{H}-1}{2}}\beta)\varepsilon_{H}p^{r-\frac{R_{H}+1}{2}}, & \text{if } R_{H} \equiv 1 \pmod{2}, \end{cases}$$

where $v(\beta) = p - 1$ if $\beta = 0$, otherwise $v(\beta) = -1$.

D Springer

Lemma 2 [28, Proposition 2] Let g be a non-degenerate quadratic form. For each r (0 < 2r < e), there exists an r-dimensional subspace $H \subseteq \mathbb{F}_{p^e}(e > 2)$ such that $H \subseteq H^{\perp_g}$.

Lemma 3 [28, Proposition 3] Let g be a non-degenerate quadratic form and e = 2s > 2. There exists an s-dimensional subspace $H_s \subset \mathbb{F}_{p^e}$ such that $H_s = H_s^{\perp_g}$ if and only if $\varepsilon_g = (-1)^{\frac{e(p-1)}{4}}$.

Lemma 4 [28, Theorem 1] Let g be a non-degenerate quadratic form and β be a nonzero element in \mathbb{F}_p . If e(e > 2) is even, then for the linear codes $C_{\overline{D}_\beta}$ in (1) with defining sets \overline{D}_β defined in (6), we have

$$d_r(C_{\overline{D}_{\beta}}) = \begin{cases} p^{e-1} - p^{e-r-1} - \left((-1)^{\frac{e(p-1)}{4}}\varepsilon_g + 1\right) p^{\frac{e-2}{2}}, & \text{if } 1 \le r \le \frac{e}{2}, \\ p^{e-1} - 2p^{e-r-1} - (-1)^{\frac{e(p-1)}{4}}\varepsilon_g p^{\frac{e-2}{2}}, & \text{if } \frac{e}{2} < r < e, \\ p^{e-1} - (-1)^{\frac{e(p-1)}{4}}\varepsilon_g p^{\frac{e-2}{2}}, & \text{if } r = e. \end{cases}$$

Lemma 5 [28, Theorem 2] Let g be a non-degenerate quadratic form and β be a nonzero element in \mathbb{F}_p . If $\bar{\eta}(\beta) = (-1)^{\frac{(e-1)(p-1)}{4}} \varepsilon_g$ and $e \ (e \ge 3)$ is odd, then for the linear codes $C_{\overline{D}_\beta}$ in (1) with defining sets \overline{D}_β defined in (6), we have

$$d_r(C_{\overline{D}_{\beta}}) = \begin{cases} p^{e-1} - p^{e-r-1}, & \text{if } 1 \le r < \frac{e}{2}, \\ p^{e-1} + p^{\frac{e-1}{2}} - 2p^{e-r-1}, & \text{if } \frac{e}{2} < r < e, \\ p^{e-1} + p^{\frac{e-1}{2}}, & \text{if } r = e. \end{cases}$$

In the following, we present some auxiliary results about f defined in (3), which will play important roles in settling the weight distributions and weight hierarchies. For more details, one is referred to [44].

For any $x \in \mathbb{F}_q$, x can be uniquely expressed as $x = x_1v_1 + x_2v_2 + \cdots + x_ev_e$ with $x_i \in \mathbb{F}_p$. Hence, we have

$$f(x) = \sum_{i=0}^{e-1} \operatorname{Tr}(a_i x^{p^i+1}) = \sum_{i=0}^{e-1} \operatorname{Tr}\left(a_i \left(\sum_{j=1}^{e} x_j \upsilon_j\right)^{p^i+1}\right)$$
$$= \sum_{i=0}^{e-1} \operatorname{Tr}\left(a_i \left(\sum_{j=1}^{e} x_j \upsilon_j^{p^i}\right) \left(\sum_{k=1}^{e} x_k \upsilon_k\right)\right)$$
$$= \sum_{j=1}^{e} \sum_{k=1}^{e} \left(\sum_{i=0}^{e-1} \operatorname{Tr}(a_i \upsilon_j^{p^i} \upsilon_k)\right) x_j x_k = XBX^T,$$

where $X = (x_1, x_2, \dots, x_e)$ and $B = \left(\frac{1}{2}\sum_{i=0}^{e-1} \operatorname{Tr}\left(a_i(v_j^{p^i}v_k + v_jv_k^{p^i})\right)\right)_{e \times e}$. Thus, f is a quadratic form and for any $x, y \in \mathbb{F}_q$, we have

$$F(x, y) = \frac{1}{2} \left(f(x+y) - f(x) - f(y) \right) = \frac{1}{2} \sum_{i=0}^{e-1} \operatorname{Tr} \left(a_i (x^{p^i} y + x y^{p^i}) \right)$$
$$= \frac{1}{2} \sum_{i=0}^{e-1} \operatorname{Tr} \left(a_i x^{p^i} y \right) + \frac{1}{2} \sum_{i=0}^{e-1} \operatorname{Tr} \left(\left(a_i^{p^{-i}} x^{p^{-i}} y \right)^{p^i} \right)$$

Deringer

$$= \frac{1}{2} \sum_{i=0}^{e-1} \operatorname{Tr}\left(a_{i} x^{p^{i}} y\right) + \frac{1}{2} \sum_{i=0}^{e-1} \operatorname{Tr}\left(a_{i}^{p^{e-i}} x^{p^{e-i}} y\right)$$
$$= \operatorname{Tr}\left(\left(a_{0} x + \frac{1}{2} \sum_{i=1}^{e-1} \left(a_{i} + a_{e-i}^{p^{i}}\right) x^{p^{i}}\right) y\right)$$
$$= \operatorname{Tr}\left(yL_{f}(x)\right),$$

where L_f is a linearized polynomial over \mathbb{F}_q defined as

$$L_f(x) = a_0 x + \frac{1}{2} \sum_{i=1}^{e-1} \left(a_i + a_{e-i}^{p^i} \right) x^{p^i}.$$
(7)

Let $\operatorname{Im}(L_f) = \{L_f(x) : x \in \mathbb{F}_q\}$, $\operatorname{Ker}(L_f) = \{x \in \mathbb{F}_q : L_f(x) = 0\}$ denote the image and kernel of L_f , respectively. Noticing that f(x) is non-degenerate, we have $R_f = e$, $\operatorname{Ker}(L_f) = \{0\}$ and $\operatorname{Im}(L_f) = \mathbb{F}_q$. If $L_f(a) = -\frac{b}{2}$, we denote a by x_b .

The following two lemmas are essential to prove our main results.

Lemma 6 [44, Lemma 5] *Let the symbols and notation be as above and f be defined in (3)* and $b \in \mathbb{F}_q$. Then

(1)
$$\sum_{x \in \mathbb{F}_q} \zeta_p^{f(x)} = \varepsilon_f(p^*)^{\frac{R_f}{2}} p^{e-R_f}.$$

(2)
$$\sum_{x \in \mathbb{F}_q} \zeta_p^{f(x) - \operatorname{Tr}(bx)} = \begin{cases} 0, & \text{if } b \notin \operatorname{Im}(L_f), \\ \varepsilon_f(p^*)^{\frac{R_f}{2}} p^{e-R_f} \zeta_p^{-f(x_b)}, & \text{if } b \in \operatorname{Im}(L_f). \end{cases}$$

where x_b satisfies $L_f(x_b) = -\frac{b}{2}$.

Lemma 7 [44, Lemma 4] With the symbols and notation above, we have the following.

(1)
$$\sum_{y \in \mathbb{F}_p^*} \sigma_y((p^*)^{\frac{r}{2}}) = \begin{cases} 0, & \text{if } r \text{ is odd }, \\ p^r(p^*)^{-\frac{r}{2}}(p-1), & \text{if } r \text{ is even }. \end{cases}$$

(2) For any
$$z \in \mathbb{F}_p^*$$
, then

$$\sum_{y \in \mathbb{F}_p^*} \sigma_y((p^*)^{\frac{r}{2}} \zeta_p^z) = \begin{cases} \bar{\eta}(-z) p^r(p^*)^{-\frac{r-1}{2}}, & \text{if } r \text{ is odd }, \\ -p^r(p^*)^{-\frac{r}{2}}, & \text{if } r \text{ is even }. \end{cases}$$

3 Linear codes from inhomogeneous quadratic functions

In this section, we study the weight distribution and weight hierarchy of C_D in (5), where its defining set is

$$\mathbf{D} = \mathbf{D}_{\alpha} = \left\{ (x, y) \in \mathbb{F}_q^2 \setminus \{ (0, 0) \} : f(x) + \operatorname{Tr}(\alpha y) = 0 \right\},\$$

with $\alpha \in \mathbb{F}_q^*$ and f(x) is defined in (3) and non-degenerate.

🖉 Springer

3.1 The weight distribution of the presented linear code

In this subsection, we first calculate the length of C_D defined in (5) and the Hamming weight of nonzero codewords of C_D .

Lemma 8 Let $\alpha \in \mathbb{F}_q^*$ and D be defined in (4) and C_D be defined in (5). Define n = |D|. Then,

$$n = p^{2e-1} - 1.$$

Proof By the orthogonal property of additive characters, we have

$$n = \frac{1}{p} \sum_{x, y \in \mathbb{F}_q} \sum_{z \in \mathbb{F}_p} \zeta_p^{z\left(f(x) + \operatorname{Tr}(\alpha y)\right)} - 1$$
$$= \frac{1}{p} \sum_{x, y \in \mathbb{F}_q} \left(1 + \sum_{z \in \mathbb{F}_p^*} \zeta_p^{z\left(f(x) + \operatorname{Tr}(\alpha y)\right)} \right) - 1$$
$$= p^{2e-1} + \frac{1}{p} \sum_{z \in \mathbb{F}_p^*} \sum_{y \in \mathbb{F}_q} \zeta_p^{\operatorname{Tr}(z\alpha y)} \sum_{x \in \mathbb{F}_q} \zeta_p^{zf(x)} - 1.$$

The desired conclusion then follows from $\alpha \neq 0$ and $\sum_{y \in \mathbb{F}_q} \zeta_p^{\text{Tr}(z\alpha y)} = 0$.

Lemma 9 Let $\alpha \in \mathbb{F}_q^*$ and D be defined in (4) and C_D be defined in (5). Let $c_{(u,v)}$ be the corresponding codeword in C_D with $(u, v) \in \mathbb{F}_q^2$. We have the following.

- (1) When $v \in \mathbb{F}_q \setminus \mathbb{F}_p^* \alpha$, we have $\operatorname{wt}(c_{(u,v)}) = p^{2e-2}(p-1)$.
- (2) When $v \in \mathbb{F}_p^* \alpha$, we have the following three cases.
 - (2.1) If u = 0, then

$$\operatorname{wt}(c_{(u,v)}) = \begin{cases} p^{2e-2}(p-1), & \text{if } e \text{ is odd }, \\ p^{2e-2}(p-1)\left(1-\varepsilon_f(p^*)^{-\frac{e}{2}}\right), & \text{if } e \text{ is even }. \end{cases}$$

(2.2) If $u \neq 0$ and $f(x_u) = 0$, then

$$wt(c_{(u,v)}) = \begin{cases} p^{2e-2}(p-1), & \text{if } e \text{ is odd }, \\ p^{2e-2}(p-1)\left(1 - \varepsilon_f(p^*)^{-\frac{e}{2}}\right), & \text{if } e \text{ is even }. \end{cases}$$

(2.3) If $u \neq 0$ and $f(x_u) \neq 0$, then

$$\operatorname{wt}(c_{(u,v)}) = \begin{cases} p^{2e-2} \left(p - 1 - \varepsilon_f \bar{\eta}(f(x_u))(p^*)^{-\frac{e-1}{2}} \right), & \text{if } e \text{ is odd }, \\ p^{2e-2} \left(p - 1 + \varepsilon_f(p^*)^{-\frac{e}{2}} \right), & \text{if } e \text{ is even }. \end{cases}$$

Proof Put $N(u, v) = \{(x, y) \in \mathbb{F}_q^2 : f(x) + \text{Tr}(\alpha y) = 0, \text{Tr}(ux + vy) = 0\}$, then the Hamming weight of $c_{(u,v)}$ is n - |N(u, v)| + 1, where *n* is given in Lemma 8. Thus, we just need to evaluate the value of |N(u, v)|.

Deringer

By the orthogonal property of additive characters, we have

$$|N(u, v)| = \frac{1}{p^2} \sum_{x, y \in \mathbb{F}_q} \left(\sum_{z_1 \in \mathbb{F}_p} \zeta_p^{z_1 f(x) + \operatorname{Tr}(z_1 \alpha y)} \sum_{z_2 \in \mathbb{F}_p} \zeta_p^{\operatorname{Tr}(z_2(ux + vy))} \right)$$

$$= \frac{1}{p^2} \sum_{x, y \in \mathbb{F}_q} \left(\left(1 + \sum_{z_1 \in \mathbb{F}_p^*} \zeta_p^{z_1 f(x) + \operatorname{Tr}(z_1 \alpha y)} \right) \left(1 + \sum_{z_2 \in \mathbb{F}_p^*} \zeta_p^{\operatorname{Tr}(z_2(ux + vy))} \right) \right)$$

$$= p^{2e-2} + \frac{1}{p^2} \sum_{z_1 \in \mathbb{F}_p^*} \sum_{x, y \in \mathbb{F}_q} \zeta_p^{z_1 f(x) + \operatorname{Tr}(z_1 \alpha y)} + \frac{1}{p^2} \sum_{z_2 \in \mathbb{F}_p^*} \sum_{x, y \in \mathbb{F}_q} \zeta_p^{\operatorname{Tr}(z_2(ux + vy))}$$

$$+ \frac{1}{p^2} \sum_{z_1 \in \mathbb{F}_p^*} \sum_{z_2 \in \mathbb{F}_p^*} \sum_{x, y \in \mathbb{F}_q} \zeta_p^{z_1 f(x) + \operatorname{Tr}(z_2 ux + z_2 vy + z_1 \alpha y)}$$

$$= p^{2e-2} + p^{-2} \sum_{z_1 \in \mathbb{F}_p^*} \sum_{z_2 \in \mathbb{F}_p^*} \sum_{y \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_q} \zeta_p^{\operatorname{Tr}(z_2 vy + z_1 \alpha y)} \sum_{x \in \mathbb{F}_q} \zeta_p^{z_1 f(x) + \operatorname{Tr}(z_2 ux)}.$$
(8)

(1) When $v \in \mathbb{F}_q \setminus \mathbb{F}_p^* \alpha$, the desired conclusion then follows from

$$\sum_{y \in \mathbb{F}_q} \zeta_p^{\operatorname{Tr}(z_2 v y + z_1 \alpha y)} = 0.$$

(2) When $v \in \mathbb{F}_p^* \alpha$, i.e., $\alpha = zv$ for some $z \in \mathbb{F}_p^*$, (8) becomes

$$N(u, v)| = p^{2e-2} + p^{e-2} \sum_{z_1 \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_q} \zeta_p^{z_1 f(x) - z_1 \operatorname{Tr}(zux)}$$

= $p^{2e-2} + p^{e-2} \sum_{z_1 \in \mathbb{F}_p^*} \sigma_{z_1} \left(\sum_{x \in \mathbb{F}_q} \zeta_p^{f(x) - \operatorname{Tr}(zux)} \right).$ (9)

If u = 0, by Lemmas 6 and 7, we have

$$|N(u, v)| = p^{2e-2} + p^{e-2} \sum_{z_1 \in \mathbb{F}_p^*} \sigma_{z_1} \left(\varepsilon_f(p^*)^{\frac{\kappa_f}{2}} p^{e-R_f} \right)$$

= $p^{2e-2} + p^{e-2} \varepsilon_f \sum_{z_1 \in \mathbb{F}_p^*} \sigma_{z_1} ((p^*)^{\frac{e}{2}})$
= $\begin{cases} p^{2e-2}, & \text{if } e \text{ is odd }, \\ p^{2e-2} \left(1 + \varepsilon_f(p^*)^{-\frac{e}{2}}(p-1) \right), & \text{if } e \text{ is even} \end{cases}$

The desired conclusion of (2.1) is obtained. If $u \neq 0$, define c = zu, we have $x_c = zx_u$. By Lemma 6, (9) becomes

$$|N(u, v)| = p^{2e-2} + p^{e-2} \sum_{z_1 \in \mathbb{F}_p^*} \sigma_{z_1} \Big(\varepsilon_f(p^*)^{\frac{R_f}{2}} p^{e-R_f} \zeta_p^{-f(x_c)} \Big)$$
$$= p^{2e-2} + p^{e-2} \varepsilon_f \sum_{z_1 \in \mathbb{F}_p^*} \sigma_{z_1} \Big((p^*)^{\frac{e}{2}} \zeta_p^{-f(x_c)} \Big).$$

The last two conclusions follow directly from Lemma 7.

Table 1 The weight distribution of C_D of Theorem 1 when e is odd	Weight ω	Multiplicity A_{ω}
	0	1
	$p^{2e-2}(p-1)$	$p^{2e} - (p-1)^2 p^{e-1} - 1$
	$p^{2e-2}\left(p-1-p^{-\frac{e-1}{2}}\right)$	$\frac{1}{2}(p-1)^2p^{e-1}(1+p^{-\frac{e-1}{2}})$
	$p^{2e-2}\left(p-1+p^{-\frac{e-1}{2}}\right)$	$\frac{1}{2}(p-1)^2 p^{e-1}(1-p^{-\frac{e-1}{2}})$

Table 2 The weight distribution of C_D of Theorem 1 when *e* is even

Weight ω	Multiplicity A_{ω}
0	1
$p^{2e-2}(p-1)$	$p^{2e} - p^e(p-1) - 1$
$p^{2e-2}(p-1)\left(1-\varepsilon_f(p^*)^{-\frac{e}{2}}\right)$	$(p-1)p^{e-1}\left(1 + \varepsilon_f (p-1)(p^*)^{-\frac{e}{2}}\right)$
$p^{2e-2}(p-1) + \varepsilon_f p^{2e-2}(p^*)^{-\frac{e}{2}}$	$(p-1)^2 p^{e-1} \left(1 - \varepsilon_f(p^*)^{-\frac{e}{2}} \right)$

Remark 1 By Lemma 9, we know that, for $(u, v) \neq (0, 0) \in \mathbb{F}_q^2$, we have wt $(c_{(u,v)}) > 0$. So, the map: $\mathbb{F}_q^2 \to C_D$ defined by $(u, v) \mapsto c_{(u,v)}$ is an isomorphism in linear spaces over \mathbb{F}_p . Hence, the dimension of the code C_D in (5) is equal to 2e.

Lemma 10 Let C_D be defined in (5). Then, the minimal distance of the dual code C_D^{\perp} is at least 2.

Proof We prove it by contradiction. If the minimal distance of the dual code $C_{\rm D}^{\perp}$ is less than 2, then there exists a coordinate *i* such that the *i*-th entry of all of the codewords of $C_{\rm D}$ is 0, that is, $\operatorname{Tr}(ux + vy) = 0$ for all $(u, v) \in \mathbb{F}_q^2$, where $(x, y) \in D$. Thus, by the properties of the trace function, we have (x, y) = (0, 0). It contradicts with $(x, y) \neq (0, 0)$.

Theorem 1 Let $\alpha \in \mathbb{F}_q^*$ and f be a non-degenerate homogeneous quadratic function defined in (3). Let D be defined in (4) and the code C_D be defined in (5). Then the code C_D is a $[p^{2e-1} - 1, 2e]$ linear code over \mathbb{F}_p with the weight distribution in Tables 1 and 2.

Proof By Lemma 8 and Remark 1, the code C_D is a $[p^{2e-1} - 1, 2e]$ linear code over \mathbb{F}_p . Now we shall prove the multiplicities A_{ω_i} of codewords with weight ω_i in C_D . Let us give the proofs of two cases, respectively.

(1) The case that e is odd.

For each $(u, v) \in \mathbb{F}_q^2$ and $(u, v) \neq (0, 0)$. By Lemmas 8 and 9, wt $(c_{(u,v)})$ has only three values, that is,

$$\begin{cases} \omega_1 = (p-1)p^{2e-2}, \\ \omega_2 = p^{2e-2} \left(p - 1 - p^{-\frac{e-1}{2}} \right), \\ \omega_3 = p^{2e-2} \left(p - 1 + p^{-\frac{e-1}{2}} \right). \end{cases}$$

By Lemma 9, we have

$$\begin{split} A_{\omega_1} &= \left| \left\{ (u, v) \in \mathbb{F}_q^2 | \operatorname{wt}(c_{(u,v)}) = (p-1)p^{2e-2} \right\} \right| \\ &= \left| \left\{ (u, v) \in \mathbb{F}_q^2 \setminus \{(0,0)\} | u \in \mathbb{F}_q, v \in \mathbb{F}_q \setminus \mathbb{F}_p^* \alpha \right\} \right| \\ &+ \left| \left\{ (0, v) \in \mathbb{F}_q^2 | v \in \mathbb{F}_p^* \alpha \right\} \right| + \left| \left\{ (u, v) \in \mathbb{F}_q^2 | v \in \mathbb{F}_p^* \alpha, u \neq 0, f(x_u) = 0 \right\} \right| \\ &= q \left(q - (p-1) \right) - 1 + (p-1) + (p-1)(p^{e-1}-1) \\ &= p^{2e} - (p-1)^2 p^{e-1} - 1, \end{split}$$

where we use the fact that the number of nonzero solutions of the equation f(x) = 0 in \mathbb{F}_q is $p^{e-1} - 1$ (see [32, Theorem 6.27]).

By Lemma 10 and the first two Pless power moments [18, p. 259], we obtain the system of linear equations as follows:

$$\begin{cases} A_{\omega_1} = p^{2e} - (p-1)^2 p^{e-1} - 1, \\ A_{\omega_2} + A_{\omega_3} = (p-1)^2 p^{e-1}, \\ \omega_1 A_{\omega_1} + \omega_2 A_{\omega_2} + \omega_3 A_{\omega_3} = p^{2e-1} (p^{2e-1} - 1)(p-1). \end{cases}$$

Solving the system, we get

$$\begin{cases} A_{\omega_1} = p^{2e} - (p-1)^2 p^{e-1} - 1, \\ A_{\omega_2} = \frac{1}{2} (p-1)^2 p^{e-1} \left(1 + p^{-\frac{e-1}{2}} \right), \\ A_{\omega_3} = \frac{1}{2} (p-1)^2 p^{e-1} \left(1 - p^{-\frac{e-1}{2}} \right). \end{cases}$$

This completes the proof of the weight distribution of Table 1.

(2) The case that e is even.

The proof is similar to that of Case (1) and we omit it here. The desired conclusion then follows from Lemmas 8 and 9 and the first two Pless power moments.

Example 1 Let $(p, e, \alpha) = (5, 3, 1)$ and $f(x) = \text{Tr}(x^2)$. Then, the corresponding code C_D has parameters [3124, 6, 2375] and the weight enumerator $1 + 240x^{2375} + 15224x^{2500} + 160x^{2625}$, which is verified by a Magma program.

Example 2 Let $(p, e, \alpha) = (3, 4, 1)$ and $f(x) = \text{Tr}(\theta x^2)$, where θ is a primitive element of \mathbb{F}_q . By Corollary 1 in [44], we have $\varepsilon_f = 1$. Then, the corresponding code C_D has parameters [2186, 8, 1296] and the weight enumerator $1 + 66x^{1296} + 6398x^{1458} + 96x^{1539}$, which is verified by a Magma program.

Example 3 Let $(p, e, \alpha) = (3, 4, \theta)$ and $f(x) = \text{Tr}(x^2)$, where θ is a primitive element of \mathbb{F}_q . By Corollary 1 in [44], we have $\varepsilon_f = -1$. Then, the corresponding code C_D has parameters [2186, 8, 1377] and the weight enumerator $1 + 120x^{1377} + 6398x^{1458} + 42x^{1620}$, which is verified by a Magma program.

3.2 The weight hierarchy of the presented linear code

In this subsection, we give the weight hierarchy of C_D in (5).

By Remark 1, we know that the dimension of the code C_D defined in (5) is 2*e*. So, by [31, Proposition 2.1], we give a general formula, that is

$$d_r(C_{\mathrm{D}}) = n - \max\left\{ |H_r^{\perp} \cap \mathrm{D}| : H_r \in [\mathbb{F}_q^2, r]_p \right\}$$
(10)

$$= n - \max\left\{ |H_{2e-r} \cap \mathbf{D}| : H_{2e-r} \in [\mathbb{F}_q^2, 2e-r]_p \right\},$$
(11)

which will be employed to calculate the generalized Hamming weight $d_r(C_D)$. Here $H_r^{\perp} = \left\{ \mathbf{x} \in \mathbb{F}_q^2 : \operatorname{Tr}(\mathbf{x} \cdot \mathbf{y}) = 0, \text{ for any } \mathbf{y} \in H_r \right\}.$

Let H_r be an *r*-dimensional subspace of \mathbb{F}_q^2 and β_1, \ldots, β_r be an \mathbb{F}_p -basis of H_r . Set

$$N(H_r) = \left\{ \mathbf{x} = (x, y) \in \mathbb{F}_q^2 : f(x) + \text{Tr}(\alpha y) = 0, \text{Tr}(\mathbf{x} \cdot \beta_i) = 0, 1 \le i \le r \right\}.$$

Then, $N(H_r) = (H_r^{\perp} \cap D) \cup \{(0, 0)\}$, which concludes that $|N(H_r)| = |H_r^{\perp} \cap D| + 1$. Hence, we have

$$d_r(C_{\rm D}) = n + 1 - \max\left\{ |N(H_r)| : H_r \in [\mathbb{F}_q^2, r]_p \right\}.$$
 (12)

Lemma 11 Let $\alpha \in \mathbb{F}_q^*$ and f be a non-degenerate homogeneous quadratic function defined in (3) with the sign ε_f . H_r and $N(H_r)$ are defined as above. We have the following.

(1) If $\alpha \notin \operatorname{Prj}_2(H_r)$, then $|N(H_r)| = p^{2e-(r+1)}$. (2) If $\alpha \in \operatorname{Prj}_2(H_r)$, then

$$|N(H_r)| = p^{e-(r+1)} \left(q + \varepsilon_f \sum_{(y_1, -u) \in H_r} \sum_{z \in \mathbb{F}_p^*} \sigma_z \left((p^*)^{\frac{e}{2}} \zeta_p^{f(x_{y_1})} \right) \right).$$

Here Prj_2 *is the second projection from* \mathbb{F}_q^2 *to* \mathbb{F}_q *defined by* $(x, y) \mapsto y$ *.*

Proof By the orthogonal property of additive characters, we have

$$p^{r+1}|N(H_r)| = \sum_{\mathbf{x}=(x,y)\in\mathbb{F}_q^2} \sum_{z\in\mathbb{F}_p} \zeta_p^{zf(x)+\operatorname{Tr}(z\alpha y)} \prod_{i=1}^r \sum_{x_i\in\mathbb{F}_p} \zeta_p^{\operatorname{Tr}(x_i(x\cdot\beta_i))}$$

$$= \sum_{\mathbf{x}=(x,y)\in\mathbb{F}_q^2} \sum_{z\in\mathbb{F}_p} \zeta_p^{zf(x)+\operatorname{Tr}(z(\alpha y))} \sum_{\mathbf{y}\in H_r} \zeta_p^{\operatorname{Tr}(x\cdot y)}$$

$$= \sum_{\mathbf{x}=(x,y)\in\mathbb{F}_q^2} \sum_{\mathbf{y}\in H_r} \zeta_p^{\operatorname{Tr}(x\cdot y)} + \sum_{\mathbf{x}=(x,y)\in\mathbb{F}_q^2} \sum_{z\in\mathbb{F}_p^*} \sum_{\mathbf{y}\in H_r} \zeta_p^{zf(x)+\operatorname{Tr}(x\cdot y+z\alpha y)}$$

$$= q^2 + \sum_{\mathbf{x}=(x,y)\in\mathbb{F}_q^2} \sum_{z\in\mathbb{F}_p^*} \sum_{\mathbf{y}\in H_r} \zeta_p^{zf(x)+\operatorname{Tr}(x\cdot y+z\alpha y)},$$

where the last equation comes from

$$\sum_{\mathbf{x}=(x,y)\in\mathbb{F}_q^2} \sum_{\mathbf{y}\in H_r} \zeta_p^{\mathrm{Tr}(\mathbf{y}\cdot\mathbf{x})} = \sum_{\mathbf{x}=(x,y)\in\mathbb{F}_q^2} 1 + \sum_{\mathbf{x}=(x,y)\in\mathbb{F}_q^2} \sum_{(0,0)\neq\mathbf{y}\in H_r} \zeta_p^{\mathrm{Tr}(\mathbf{y}\cdot\mathbf{x})}$$
$$= q^2 + \sum_{(0,0)\neq\mathbf{y}\in H_r} \sum_{\mathbf{x}=(x,y)\in\mathbb{F}_q^2} \zeta_p^{\mathrm{Tr}(\mathbf{y}\cdot\mathbf{x})} = q^2.$$

Springer

Denote $B_{H_r} = \sum_{\mathbf{x}=(x,y)\in\mathbb{F}_q^2} \sum_{z\in\mathbb{F}_p^*} \sum_{y\in H_r} \zeta_p^{zf(x)+\operatorname{Tr}(\mathbf{x}\cdot\mathbf{y}+z\alpha y)}$, then we have $p^{r+1}|N(H_r)| = q^2 + B_{H_r}$

and

$$B_{H_r} = \sum_{\mathbf{x}=(x,y)\in\mathbb{F}_q^2} \sum_{z\in\mathbb{F}_p^*} \sum_{\mathbf{y}\in H_r} \zeta_p^{zf(x)+\operatorname{Tr}(\mathbf{x}\cdot\mathbf{y}+z\alpha y)}$$

$$= \sum_{(x,y)\in\mathbb{F}_q^2} \sum_{z\in\mathbb{F}_p^*} \sum_{(y_1,y_2)\in H_r} \zeta_p^{zf(x)+\operatorname{Tr}(y_1x+y_2y+z\alpha y)}$$

$$= \sum_{(y_1,y_2)\in H_r} \sum_{z\in\mathbb{F}_p^*} \sum_{x\in\mathbb{F}_q} \zeta_p^{zf(x)+\operatorname{Tr}(y_1x)} \sum_{y\in\mathbb{F}_q} \zeta_p^{\operatorname{Tr}(y_2y+z\alpha y)}$$

$$= \sum_{(y_1,y_2)\in H_r} \sum_{z\in\mathbb{F}_p^*} \sum_{x\in\mathbb{F}_q} \zeta_p^{zf(x)+z\operatorname{Tr}(\frac{y_1}{z}x)} \sum_{y\in\mathbb{F}_q} \zeta_p^{z\operatorname{Tr}(\frac{y_2}{z}y+\alpha y)}$$

$$= \sum_{(y_1,y_2)\in H_r} \sum_{z\in\mathbb{F}_p^*} \sum_{x\in\mathbb{F}_q} \zeta_p^{zf(x)+z\operatorname{Tr}(y_1x)} \sum_{y\in\mathbb{F}_q} \zeta_p^{z\operatorname{Tr}(y_2y+\alpha y)}.$$

If $\alpha \notin \operatorname{Prj}_2(H_r)$, then $B_{H_r} = 0$, which follows from $\sum_{y \in \mathbb{F}_q} \zeta_p^{z\operatorname{Tr}(y_2y + \alpha y)} = 0$. If $\alpha \in \operatorname{Prj}_2(H_r)$, by Lemma 6, we have

$$B_{H_r} = q \sum_{(y_1, -\alpha) \in H_r} \sum_{z \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_q} \zeta_p^{zf(x) + z \operatorname{Tr}(y_1 x)}$$

$$= q \sum_{(y_1, -\alpha) \in H_r} \sum_{z \in \mathbb{F}_p^*} \sigma_z \Big(\sum_{x \in \mathbb{F}_q} \zeta_p^{f(x) + \operatorname{Tr}(y_1 x)} \Big)$$

$$= q \sum_{(y_1, -\alpha) \in H_r} \sum_{z \in \mathbb{F}_p^*} \sigma_z \Big(\varepsilon_f(p^*)^{\frac{R_f}{2}} p^{e - R_f} \zeta_p^{f(x_{y_1})} \Big)$$

$$= \varepsilon_f q \sum_{(y_1, -\alpha) \in H_r} \sum_{z \in \mathbb{F}_p^*} \sigma_z \Big((p^*)^{\frac{e}{2}} \zeta_p^{f(x_{y_1})} \Big).$$

So, the desired result is obtained. Thus, we complete the proof.

In the following, we shall determine the weight hierarchy of C_D in (5) by calculating $|N(H_r)|$ in Lemma 11 and $|H_{2e-r} \cap D|$ in (11).

Theorem 2 Let $e \ge 3$ and $\alpha \in \mathbb{F}_q^*$ and f be a non-degenerate homogeneous quadratic function defined in (3) with the sign ε_f . Let D be defined in (4) and the code C_D be defined in (5). Define

$$e_0 = \begin{cases} \frac{e-1}{2}, & \text{if } e \text{ is odd,} \\ \frac{e}{2}, & \text{if } e \text{ is even and } \varepsilon_f = (-1)^{\frac{e(p-1)}{4}}, \\ \frac{e-2}{2}, & \text{if } e \text{ is even and } \varepsilon_f = -(-1)^{\frac{e(p-1)}{4}}. \end{cases}$$

Then we have the following.

(1) When $e - e_0 + 1 \le r \le 2e$, we have

$$d_r(C_{\rm D}) = p^{2e-1} - p^{2e-r}.$$

D Springer

(2) When $0 < r \le e - e_0$, we have

$$d_r(C_{\rm D}) = \begin{cases} p^{2e-1} - p^{2e-r-1} - p^{\frac{3e-3}{2}}, & \text{if } 2 \nmid e \}, \\ p^{2e-1} - p^{2e-r-1} - (p-1)p^{\frac{3e-4}{2}}, & \text{if } 2 \mid e \text{ and } \varepsilon_f = (-1)^{\frac{e(p-1)}{4}}, \\ p^{2e-1} - p^{2e-r-1} - p^{\frac{3e-4}{2}}, & \text{if } 2 \mid e \text{ and } \varepsilon_f = -(-1)^{\frac{e(p-1)}{4}}. \end{cases}$$

Proof (1) When $e - e_0 + 1 \le r \le 2e$, then $0 \le 2e - r \le e_0 + e - 1$. Let $T_{\alpha} = \left\{ x \in \mathbb{F}_q : x \in \mathbb$

 $\operatorname{Tr}(\alpha x) = 0$. It is easy to know that $\dim(T_{\alpha}) = e - 1$. By Lemmas 2 and 3, there exists an e_0 -dimensional subspace J_{e_0} of \mathbb{F}_q such that f(x) = 0 for any $x \in J_{e_0}$. Note that the dimension of the subspace $J_{e_0} \times T_{\alpha}$ is $e_0 + e - 1$. Let H_{2e-r} be a (2e - r)-dimensional subspace of $J_{e_0} \times T_{\alpha}$, then, $|H_{2e-r} \cap D| = p^{2e-r} - 1$. Hence, by (11), we have

$$d_r(C_{\rm D}) = n - \max\left\{ |{\rm D} \cap H| : H \in \left[\mathbb{F}_{p^e}^2, 2e - r\right]_p \right\} = p^{2e-1} - p^{2e-r}.$$

Thus, it remains to determine $d_r(C_D)$ when $0 < r \le e - e_0$.

(2) When $0 < r \le e - e_0$, we discuss case by case.

Case 1 $e(e \ge 3)$ is odd. In this case, $e_0 = \frac{e-1}{2}$ and $e - e_0 = \frac{e+1}{2}$, that is, $0 < r \le \frac{e+1}{2}$. When $0 < r < \frac{e+1}{2}$, let H_r be an *r*-dimensional subspace of \mathbb{F}_q^2 . If $\alpha \in \operatorname{Prj}_2(H_r)$, by Lemmas 7 and 11, we have

$$|N(H_r)| = p^{2e - (r+1)} \left(1 + (-1)^{\frac{(e-1)(p-1)}{4}} \varepsilon_f \bar{\eta}(-1) p^{-\frac{e-1}{2}} \sum_{(y_1, -\alpha) \in H_r} \bar{\eta}(f(x_{y_1})) \right).$$

Now we want to construct H_r such that $|N(H_r)|$ reaches its maximum, that is, the number of such as $(y_1, -\alpha)$ is maximal in H_r and for any $(y_1, -\alpha) \in H_r$, $\bar{\eta}(f(x_{y_1})) = (-1)^{\frac{(e-1)(p-1)}{4}} \varepsilon_f \bar{\eta}(-1)$. The constructing method is as follows.

Taking an element $a \in \mathbb{F}_p^*$ satisfying $\overline{\eta}(a) = (-1)^{\frac{(e-1)(p-1)}{4}} \varepsilon_f \overline{\eta}(-1)$, then, by Lemma 1 (or [32, Theorem 6.27]), we know that the length and the dimension of $C_{\overline{D}_a}$ in (1) are $p^{e-1} + \overline{\eta}(-1)p^{\frac{e-1}{2}}$ and e, respectively. Combining formula (11) with Lemma 5 (or [28, Theorem 3]), we have

$$d_{e-r}(C_{\overline{D}_a}) = p^{e-1} + \bar{\eta}(-1)p^{\frac{e-1}{2}} - \max\left\{ |\overline{D}_a \cap H| : H \in [\mathbb{F}_q, r]_p \right\}$$
$$= p^{e-1} + \bar{\eta}(-1)p^{\frac{e-1}{2}} - 2p^{e-(e-r)-1},$$

which follows that $\max \left\{ |\overline{D}_a \cap H| : H \in [\mathbb{F}_q, r]_p \right\} = 2p^{r-1}$. Thus, there exists an r-dimensional subspace J_r of \mathbb{F}_q such that $|\overline{D}_a \cap J_r| = 2p^{r-1}$. By Lemma 1, we know that $R_{J_r} = 1$ and $\varepsilon_{J_r} = \overline{\eta}(a)$, which concludes that there exists an (r-1)-dimensional subspace J_{r-1} of J_r satisfying $f(J_{r-1}) = 0$ and $\overline{\eta}(f(x)) = (-1)^{\frac{(e-1)(p-1)}{4}} \varepsilon_f \overline{\eta}(-1)$, for each $x \in J_r \setminus J_{r-1}$. Let $\alpha_1, \alpha_2, \ldots, \alpha_{r-1}$ be an \mathbb{F}_p -basis of J_{r-1} . Take an element $\alpha_r \in J_r \setminus J_{r-1}$ and set

$$\mu_1 = \alpha_1 + \alpha_r, \, \mu_2 = \alpha_2 + \alpha_r, \, \dots, \, \mu_{r-1} = \alpha_{r-1} + \alpha_r, \, \mu_r = \alpha_r,$$

clearly, $\mu_1, \mu_2, \ldots, \mu_{r-1}, \mu_r$ is an \mathbb{F}_p -basis of J_r . Define

$$\lambda_1 = (\mu_1, -\alpha), \lambda_2 = (\mu_2, -\alpha), \dots, \lambda_{r-1} = (\mu_{r-1}, -\alpha), \lambda_r = (\mu_r, -\alpha)$$

Deringer

and $V_r = \langle \lambda_1, \lambda_2, ..., \lambda_{r-1}, \lambda_r \rangle$, then V_r is an *r*-dimensional subspace of \mathbb{F}_q^2 . Set $S(-\alpha) = \{(y, z) \in V_r : z = -\alpha\}$, it is easy to know that the cardinal number of $S(-\alpha)$ is p^{r-1} . We assert that $f(y) = f(\alpha_r)$ for any $(y, -\alpha) \in S(-\alpha)$. In fact, $(y, -\alpha)$ has the following unique representation:

$$(y, -\alpha) = x_1\lambda_1 + x_2\lambda_2 + \dots + x_{r-1}\lambda_{r-1} + x_r\lambda_r,$$

= $(x_1\alpha_1 + x_2\alpha_2 + \dots + x_{r-1}\alpha_{r-1} + \alpha_r, -\alpha), x_i \in \mathbb{F}_p,$

thus, we have $y = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_{r-1}\alpha_{r-1} + \alpha_r$, which concludes that $f(y) = f(\alpha_r)$. Take

$$H_r = \Big\langle (L_f(\mu_1), -\alpha), (L_f(\mu_2), -\alpha), \dots, (L_f(\mu_{r-1}), -\alpha), (L_f(\mu_r), -\alpha) \Big\rangle,$$

it is easily seen that H_r is our desired *r*-dimensional subspace of \mathbb{F}_q^2 and its $|N(H_r)|$ reaches the maximum

$$|N(H_r)| = p^{2e - (r+1)} \left(1 + p^{r-1 - \frac{e-1}{2}} \right) = p^{2e - r-1} + p^{\frac{3e-3}{2}}.$$

So, for $0 < r < \frac{e+1}{2}$, the desired result is obtained by Lemma 11 and (12).

When $r = \frac{e+1}{2}$, let H_r be an *r*-dimensional subspace of \mathbb{F}_q^2 . By Lemmas 7 and 11, we have $|N(H_r)| \leq 2p^{\frac{3(e-1)}{2}}$, which concludes that

$$d_r(C_{\rm D}) \ge p^{2e-1} - 2p^{\frac{3(e-1)}{2}}$$

by formula (12). On the other hand, by formula (11), we have

$$d_r(C_{\rm D}) = p^{2e-1} - 1 - \max\left\{ \left| H_{\frac{3e-1}{2}} \cap {\rm D} \right| : H_{\frac{3e-1}{2}} \in \left[\mathbb{F}_q^2, \frac{3e-1}{2} \right]_p \right\}.$$

Now we want to construct a $\frac{3e-1}{2}$ -dimensional subspace $H_{\frac{3e-1}{2}}$ of \mathbb{F}_q^2 such that $|H_{\frac{3e-1}{2}} \cap \mathbf{D}| \ge 2p^{\frac{3(e-1)}{2}} - 1$, which concludes that

$$d_r(C_{\rm D}) \le p^{2e-1} - 2p^{\frac{3(e-1)}{2}}.$$

In fact, by the proof of (1), we know that the dimension of $J_{\frac{e-1}{2}}$ is $\frac{e-1}{2}$, then the dimension of $J_{\frac{e-1}{2}}^{\perp_f}$ is $\frac{e+1}{2}$. Taking $(u, v) \in D$, where $u \in J_{\frac{e-1}{2}}^{\perp_f}$ and $f(u) \neq 0$, define $H_{\frac{3e-1}{2}} = (J_{\frac{e-1}{2}} \times T_{\alpha}) \oplus ((u, v))$, then $H_{\frac{3e-1}{2}}$ is our desired subspace of \mathbb{F}_q^2 . So, for $r = \frac{e+1}{2}$, we have

$$d_r(C_{\rm D}) = p^{2e-1} - 2p^{\frac{3(e-1)}{2}}.$$

Case 2 $e(e \ge 3)$ is even and $\varepsilon_f = (-1)^{\frac{e(p-1)}{4}}$. In this case, $e_0 = \frac{e}{2}$ and $e - e_0 = \frac{e}{2}$, that is, $0 < r \le \frac{e}{2}$.

Suppose H_r is an *r*-dimensional subspace of \mathbb{F}_q^2 and $\alpha \in \operatorname{Prj}_2(H_r)$. Recall that v(0) = p-1and v(x) = -1 for $x \in \mathbb{F}_p^*$ defined in Lemma 1. By Lemmas 7 and 11, we have

$$|N(H_r)| = p^{e-(r+1)} \left(q + \varepsilon_f \sum_{(y_1, -u) \in H_r} \sum_{z \in \mathbb{F}_p^*} \sigma_z \left((p^*)^{\frac{e}{2}} \zeta_p^{f(x_{y_1})} \right) \right)$$

🖄 Springer

$$= p^{2e-(r+1)} \left(1 + p^{-\frac{e}{2}} \sum_{(y_1, -\alpha) \in H_r} v(f(x_{y_1})) \right).$$

Let J_r be a subspace of $J_{\frac{e}{2}}$ with a basis $\mu_1, \mu_2, \ldots, \mu_r$. Take

$$H_r = \Big\langle (L_f(\mu_1), -\alpha), (L_f(\mu_2), -\alpha), \dots, (L_f(\mu_{r-1}), -\alpha), (L_f(\mu_r), -\alpha) \Big\rangle,$$

then $|N(H_r)|$ reaches its maximum

$$|N(H_r)| = p^{2e - (r+1)} \left(1 + (p-1)p^{r-1 - \frac{e}{2}} \right) = p^{2e - r - 1} + (p-1)p^{\frac{3e - 4}{2}}$$

So, for $0 < r \le \frac{e}{2}$, the desired result is obtained by Lemma 11 and (12).

Case 3 $e(e \ge 3)$ is even and $\varepsilon_f = -(-1)^{\frac{e(p-1)}{4}}$. In this case, $e_0 = \frac{e-2}{2}$ and $e - e_0 = \frac{e}{2} + 1$, that is, $0 < r \le \frac{e}{2} + 1$.

Suppose H_r is an *r*-dimensional subspace of \mathbb{F}_q^2 and $\alpha \in \operatorname{Prj}_2(H_r)$. By Lemmas 7 and 11, we have

$$|N(H_r)| = p^{2e - (r+1)} \Big(1 - p^{-\frac{e}{2}} \sum_{(y_1, -\alpha) \in H_r} v(f(x_{y_1})) \Big).$$

Taking an element $a \in \mathbb{F}_p^*$, then, by Lemma 1 (or [32, Theorem 6.26]), we know that the length and the dimension of $C_{\overline{D}_a}$ in (1) are $p^{e-1} + p^{\frac{e-2}{2}}$ and *e*, respectively.

When $0 < r \le \frac{e}{2}$, combining formula (11) with Lemma 4, we have

$$d_{e-r}(C_{\overline{D}_a}) = p^{e-1} + p^{\frac{e-2}{2}} - \max\left\{ |\overline{D}_a \cap H| : H \in [\mathbb{F}_q, r]_p \right\}$$
$$= p^{e-1} - 2p^{e-(e-r)-1} + p^{\frac{e-2}{2}},$$

which follows that $\max\left\{|\overline{D}_a \cap H| : H \in [\mathbb{F}_q, r]_p\right\} = 2p^{r-1}$. Thus, there exists an *r*-dimensional subspace J_r of \mathbb{F}_q such that $|\overline{D}_a \cap J_r| = 2p^{r-1}$. By Lemma 1, we know that $R_{J_r} = 1$ and $\varepsilon_{J_r} = \overline{\eta}(a)$, which concludes that there exists an (r-1)-dimensional subspace J_{r-1} of J_r satisfying $f(J_{r-1}) = 0$ and $\overline{\eta}(f(x)) = (-1)^{\frac{(e-1)(p-1)}{4}} \varepsilon_f$, for each $x \in J_r \setminus J_{r-1}$. Let $\alpha_1, \alpha_2, \ldots, \alpha_{r-1}$ be an \mathbb{F}_p -basis of J_{r-1} . Take an element $\alpha_r \in J_r \setminus J_{r-1}$ and set

$$\mu_1 = \alpha_1 + \alpha_r, \, \mu_2 = \alpha_2 + \alpha_r, \, \dots, \, \mu_{r-1} = \alpha_{r-1} + \alpha_r, \, \mu_r = \alpha_r,$$

it's obvious that $\mu_1, \mu_2, \ldots, \mu_{r-1}, \mu_r$ is an \mathbb{F}_p -basis of J_r . Take

$$H_r = \Big\langle (L_f(\mu_1), -\alpha), (L_f(\mu_2), -\alpha), \dots, (L_f(\mu_{r-1}), -\alpha), (L_f(\mu_r), -\alpha) \Big\rangle,$$

then $|N(H_r)|$ reaches its maximum

$$|N(H_r)| = p^{2e - (r+1)} \left(1 + p^{r-1 - \frac{e}{2}} \right) = p^{2e - r - 1} + p^{\frac{3e - 4}{2}}.$$

So, for $0 < r \le \frac{e}{2}$, the desired result is obtained by Lemma 11 and (12).

When $r = \frac{e}{2} + 1$, combining formula (11) with Lemma 4, we have

$$d_{e-r}(C_{\overline{D}_a}) = p^{e-1} + p^{\frac{e-2}{2}} - \max\left\{ |\overline{D}_a \cap H| : H \in [\mathbb{F}_q, r]_p \right\}$$

= $p^{e-1} - p^{e-(e-r)-1},$

D Springer

which follows that $\max \left\{ |\overline{D}_a \cap H| : H \in [\mathbb{F}_q, \frac{e}{2} + 1]_p \right\} = p^{\frac{e}{2}} + p^{\frac{e-2}{2}}$. Thus, there exists an *r*-dimensional subspace J_r of \mathbb{F}_q such that $|\overline{D}_a \cap J_r| = p^{\frac{e-2}{2}} + p^{\frac{e}{2}}$. By the proof of Lemma 4 (or [28, Theorem 1]), we know that $R_{J_r} = 2$ and $\varepsilon_{J_r} = \overline{\eta}((-1)^{\frac{e}{2}-1})\varepsilon_f$. So, there exists an (r-2)-dimensional subspace J_{r-2} of J_r satisfying $f(J_{r-2}) = 0$. Let $\alpha_1, \alpha_2, \ldots, \alpha_{r-2}$ be an \mathbb{F}_p -basis of J_{r-2} . Choose two elements $\gamma_1, \gamma_2 \in J_r \setminus J_{r-2}$ such that $\alpha_1, \ldots, \alpha_{r-2}, \gamma_1, \gamma_2$ is an \mathbb{F}_p -basis of J_r . Set

$$\mu_1 = \alpha_1 + \gamma_2, \dots, \mu_{r-2} = \alpha_{r-2} + \gamma_2, \mu_{r-1} = \gamma_1 + \gamma_2, \mu_r = \gamma_2,$$

it's easy to see that $\mu_1, \mu_2, \dots, \mu_{r-1}, \mu_r$ is an \mathbb{F}_p -basis of J_r . Take $H_r = \left((L_f(\mu_1), -\alpha), (L_f(\mu_2), -\alpha), \dots, (L_f(\mu_{r-1}), -\alpha), (L_f(\mu_r), -\alpha) \right)$, then $|N(H_r)|$ reaches its maximum

$$|N(H_r)| = p^{2e - (r+1)} \left(1 + p^{r-1 - \frac{e}{2}} \right) = 2p^{\frac{3e-4}{2}} = p^{2e - r-1} + p^{\frac{3e-4}{2}}$$

So, for $r = \frac{e}{2} + 1$, the desired result is obtained.

4 Concluding remarks

In this paper, inspired by the works of [28,44], we constructed a family of three-weight linear codes using a special inhomogeneous quadratic function, and determined their weight distributions and weight hierarchies. Compared with the codes Tang et al. constructed in [44], the obtained codes in this paper have different weight distributions. They are also different from the weight distributions in the classical families in [11,51,52]. In our case, we note that the quadratic form f defined in (3) is non-degenerate. It is an open problem to determine the weight hierarchy of the code when f is degenerate.

Let w_{\min} and w_{\max} denote the minimum and maximum nonzero weight of our obtained code $C_{\rm D}$ defined in (5), respectively. If $e \ge 3$, then it can be easily checked that

$$\frac{w_{\min}}{w_{\max}} > \frac{p-1}{p}$$

By the results in [1] and [50], we know that every nonzero codeword of C_D is minimal and most of the codes we constructed are suitable for constructing secret sharing schemes with interesting properties.

Acknowledgements The authors are very grateful to the reviewers and the editors, for their comments and suggestions that improved the presentation and quality of this paper.

References

- Ashikhmin A., Barg A.: Minimal vectors in linear codes. IEEE Trans. Inf. Theory 44(50), 2010–2017 (1998).
- Ahn J., Ka D., Li C.: Complete weight enumerators of a class of linear codes. Des. Codes Cryptogr. 83(1), 83–99 (2017).
- Beelen P.: A note on the generalized Hamming weights of Reed-Muller codes. Appl. Algebra Eng. Commun. 30, 233–242 (2019).
- Bras-Amorós M., Lee K., Vico-Oton A.: New lower bounds on the generalized Hamming weights of AG codes. IEEE Trans. Inf. Theory 60(10), 5930–5937 (2014).
- Calderbank A.R., Goethals J.M.: Three-weight codes and association schemes. Philips J. Res. 39, 143–152 (1984).

- Calderbank A.R., Kantor W.M.: The geometry of two-weight codes. Bull. Lond. Math. Soc. 18, 97–122 (1986).
- Cheng J., Chao C.: On generalized Hamming weights of binary primitive BCH codes with minimum distance one less than a power of two. IEEE Trans. Inf. Theory 43(1), 294–298 (1997).
- Choi S.T., Kim J.Y., No J.S., Chung H.: Weight distribution of some cyclic codes. In: Proceedings of the International Symposium on Information Theory, pp. 2911–2913 (2012).
- 9. Ding C.: A construction of binary linear codes from Boolean functions. Discret. Math. 9, 2288–2303 (2016).
- Ding C., Niederreiter H.: Cyclotomic linear codes of order 3. IEEE Trans. Inf. Theory 53(6), 2274–2277 (2007).
- Ding K., Ding C.: A class of two-weight and three-weight codes and their applications in secret sharing. IEEE Trans. Inf. Theory 61(11), 5835–5842 (2015).
- 12. Ding K., Ding C.: Binary linear codes with three weights. IEEE Commun. Lett. 18(11), 1879–1882 (2014).
- Ding C., Helleseth T., Kløve T., Wang X.: A generic construction of Cartesian authentication codes. IEEE Trans. Inf. Theory 53(6), 2229–2235 (2007).
- Ding C., Li C., Li N., Zhou Z.: Three-weight cyclic codes and their weight distributions. Discret. Math. 339(2), 415–427 (2016).
- Ding C., Liu Y., Ma C., Zeng L.: The weight distributions of the duals of cyclic codes with two zeros. IEEE Trans. Inf. Theory 57(12), 8000–8006 (2011).
- Heijnen P., Pellikaan R.: Generalized Hamming weights of q-ary Reed-Muller codes. IEEE Trans. Inf. Theory 44(1), 181–196 (1998).
- Helleseth T., Kløve T., Ytrehus O.: Codes, weight hierarchies, and chains. In: Singapore Iccs/isita 92 Communications on the Move IEEE (1992).
- Huffman W.C., Pless V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003).
- Ireland K., Rosen M.: A classical introduction to modern number theory. In: Graduate Texts in Mathematics, vol. 84, 2nd edn. Springer, New York (1990).
- Janwa H., Lal A.K.: On the generalized Hamming weights of cyclic codes. IEEE Trans. Inf. Theory 43(1), 299–308 (1997).
- Jian G., Feng R., Wu H.: Generalized Hamming weights of three classes of linear codes. Finite Fields Appl. 45, 341–354 (2017).
- Jian G., Lin C., Feng R.: Two-weight and three-weight linear codes based on Weil sums. Finite Fields Appl. 57, 92–107 (2019).
- 23. Kløve T.: Codes for Error Detection. World Scientific, Hackensack (2007).
- Kong X., Yang S.: Complete weight enumerators of a class of linear codes with two or three weights. Discret. Math. 342(11), 3166–3176 (2019).
- Li C., Bae S., Yang S.: Some results on two-weight and three-weight linear codes. Adv. Math. Commun. 13(1), 195–211 (2019).
- Li C., Yue Q., Fu F.: A construction of several classes of two-weight and three-weight linear codes. Appl. Algebra Eng. Commun. 28(1), 1–20 (2018).
- Li F.: A class of cyclotomic linear codes and their generalized Hamming weights. Appl. Algebra Eng. Commun. 29, 501–511 (2018).
- Li F.: Weight hierarchy of a class of linear codes relating to non-degenerate quadratic forms. IEEE Trans. Inf. Theory 67(1), 124–129 (2021).
- Li F., Li X.: Weight hierarchies of a family of linear codes associated with degenerate quadratic forms, arXiv:1804.06866 (2018).
- Li F., Li X.: Weight distributions of several families of 3-weight binary linear codes, arXiv:2002.01853v2 (2020).
- Li F., Li X.: Weight distributions and weight hierarchies of two classes of binary linear codes. Finite Fields Appl. 73, 101865 (2021).
- 32. Lidl R., Niederreiter H.: Finite Fields. Cambridge University Press, New York (1997).
- Liu H., Liao Q.: Several classes of linear codes with a few weights from defining sets over 𝔽_p + u𝔽_p. Des. Codes Cryptogr. 87(1), 15–29 (2017).
- 34. Liu Y., Liu Z.: On some classes of codes with a few weights. Adv. Math. Commun. 12(2), 415–428 (2018).
- Liu Z., Wang J.: Notes on generalized Hamming weights of some classes of binary codes. Cryptogr. Commun. 10, 645–657 (2020).
- Luo G., Cao X.: Five classes of optimal two-weight linear codes. Cryptogr. Commun. 10, 1119–1135 (2018).

- Luo J., Feng K.: On the weight distribution of two classes of cyclic codes. IEEE Trans. Inf. Theory 54(12), 5332–5344 (2008).
- Olmez O.: A link between combinatorial designs and three-weight linear codes. Des. Codes Cryptogr. 86, 817–833 (2018).
- Shi M., Guan Y., Solé P.: Two new families of two-weight codes. IEEE Trans. Inf. Theory 63(10), 6240– 6246 (2017).
- Shi M., Liu Y., Solé P.: Optimal two weight codes from trace codes over 𝔽₂ + u𝔽₂. IEEE Commun. Lett. 20(12), 2346–2349 (2016).
- Shi M., Wu R., Liu Y., Solé P.: Two and three weight codes over F_p + uF_p. Cryptogr. Commun. 9(5), 637–646 (2017).
- Shi M., Liu Y., Solé P.: Optimal two weight codes from trace codes over a non-chain ring. Discret. Appl. Math. 219, 176–181 (2017).
- Shi M., Wu R., Qian L., Lin S., Solé P.: New Classes of *p*-ary few weights codes. Bull. Malays. Math. Sci. Soc. 42(4), 1393–1412 (2019).
- Tang C., Xiang C., Feng K.: Linear codes with few weights from inhomogeneous quadratic functions. Des. Codes Cryptogr. 83(3), 691–714 (2017).
- Wei V.K.: Generalized Hamming weights for linear codes. IEEE Trans. Inf. Theory 37(5), 1412–1418 (1991).
- Wan Z.: The weight hierarchies of the projective codes from nondegenerate quadrics. Des. Codes Cryptogr. 4(4), 283–300 (1994).
- Xiong M., Li S., Ge G.: The weight hierarchy of some reducible cyclic codes. IEEE Trans. Inf. Theory 62(7), 4071–4080 (2016).
- Yang M., Li J., Feng K., Lin D.: Generalized Hamming weights of irreducible cyclic codes. IEEE Trans. Inf. Theory 61(9), 4905–4913 (2015).
- Yang S., Yao Z., Zhao C.: The weight distributions of two classes of p-ary cyclic codes with few weights. Finite Fields Appl. 44, 76–91 (2017).
- Yuan J., Ding C.: Secret sharing schemes from three classes of linear codes. IEEE Trans. Inf. Theory 52(1), 206–212 (2006).
- 51. Zhou Z., Ding C.: A class of three-weight cyclic codes. Finite Fields Appl. 25, 79-93 (2014).
- Zhou Z., Li N., Fan C., Helleseth T.: Linear codes with two or three weights from quadratic bent functions. Des. Codes Cryptogr. 81(2), 283–295 (2016).

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.