AAECC (2019) 30:75–92
https://doi.org/10.1007/s00200-018-0359-x

ORIGINAL PAPER

Several classes of linear codes and their weight distributions

Xiaoqiang Wang[1] · Dabin Zheng[2] · Hongwei Liu[1]

Received: 25 August 2017 / Revised: 24 April 2018 / Accepted: 11 May 2018 /
Published online: 24 May 2018

Abstract In this paper, several classes of two-weight or three-weight linear codes over $\mathbb{F}_p$ from quadratic or non-quadratic functions are constructed and their weight distributions are determined. From the constructed codes, we obtain some optimal linear codes with respect to the Singleton bound and the Griesmer bound. These two- or three-weight linear codes may have applications in secret sharing, authentication codes, association schemes and strongly regular graphs.

Keywords Linear code · Weight distribution · DO polynomial · Exponential sum · Quadratic form

Mathematics Subject Classification 05A05 · 11T06 · 11T55

1 Introduction

Let $\mathbb{F}_{p^m}$ be a finite field of size p^m, where p is an odd prime. An $[n, k]$ linear code $\mathcal{C}$ over $\mathbb{F}_p$ is a k-dimensional linear subspace of $\mathbb{F}_p^n$. The Hamming weight of a codeword $(c_0, c_1, \ldots, c_{n-1})$ in $\mathcal{C}$ is the number of nonzero c_i for $0 \leq i \leq n-1$. Let A_i denote the

✉ Dabin Zheng
dzheng@hubu.edu.cn

Xiaoqiang Wang
waxiqq@163.com

Hongwei Liu
hwliu@mail.ccnu.edu.cn

[1] School of Mathematics and Statistics, Central China Normal University, Wuhan 430079, China

[2] Hubei Province Key Laboratory of Applied Mathematics, Faculty of Mathematics and Statistics, Hubei University, Wuhan 430062, China

number of nonzero codewords with Hamming weight i in $\mathcal{C}$. The weight enumerator of $\mathcal{C}$ is defined by $1+A_1z+\cdots+A_nz^n$. The sequence $(1, A_1, \ldots, A_n)$ is called the weight distribution of $\mathcal{C}$. The weight distribution of a code not only gives the error correcting ability of the code, but also allows the computation of the error probability of error detection and correction [17]. Therefore, the research of the weight distribution of a linear code is important in both theory and applications.

Let Tr denote the trace function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$. From a subset $D = \{d_1, d_2, \ldots, d_n\} \subset \mathbb{F}_{p^m}$, Ding et al. defined a generic class of linear codes of length $n = |D|$ over $\mathbb{F}_p$ as

$$\mathcal{C}_D = \left\{(\mathrm{Tr}(xd_1), \mathrm{Tr}(xd_2), \ldots, \mathrm{Tr}(xd_n)) \mid x \in \mathbb{F}_{p^m}\right\}. \tag{1}$$

Here D is called the defining set of $\mathcal{C}_D$. This construction is generic in the sense that many classes of known codes could be produced by selecting the defining set D.

As far as we know, this technique was first employed in [3,4] for obtaining good linear codes. Recently, Ding in [5,6] studied linear codes whose defining sets were chosen from some specific classes of 2-designs or (pre)images of certain Boolean functions. In the past three years, many authors worked on this topic. The reader is referred to [5–8,14–16,19,21–23,25–28] and the references therein.

Let f be a polynomial over $\mathbb{F}_{p^m}$. Define

$$D_f = \left\{x \in \mathbb{F}_{p^m}^* \mid \mathrm{Tr}(f(x)) = 0\right\}.$$

Using D_f as a defining set, Zhang et al. in [26] showed the complete weight enumerators of a class of linear codes from a general quadratic polynomial $f(x)$ over $\mathbb{F}_{p^m}$. From [26] we know that the parameters of the linear code $\mathcal{C}_{D_f}$ depend on the rank and determinant of the quadratic form $\mathrm{Tr}(f)$, which are difficult to determine in general.

In fact, from the point of view of geometry, the weight distribution of $\mathcal{C}_{D_f}$ is connected to the size of the intersection of the set D_f and the hyperplane $H_a = \{x \mid \mathrm{Tr}(ax) = 0\}$. If f is a DO polynomial, then D_f is a quadric. When the quadric and hyperplane have the same size, Games in [13] determined the intersection sizes and their corresponding frequencies. In this paper, we will present a class of linear codes from binomial quadratic polynomials over $\mathbb{F}_{p^m}$ and determine their weight distributions explicitly by the application of the theory of quadratic forms over finite fields. Second, motivated by the idea of [29,30], we study a class of linear codes $\mathcal{C}_{D_f}$ from $f = x^{\ell}$ for ℓ satisfying some congruence conditions and derive their weight distributions by converting the exponential sum related to non-quadratic forms to that related to quadratic forms. From the constructed codes, we obtain some optimal linear codes with respect to the Griesmer bound and the Singleton bound.

The remainder of this paper is organized as follows. Section 2 gives some preliminaries on quadratic forms over finite fields. In Sect. 3 we present the weight distributions of a class of linear codes from some special DO polynomials. Section 4 determines the weight distributions of a class of linear codes from some non-quadratic functions. Finally, Sect. 5 concludes this paper.

2 Preliminaries

Let p be an odd prime and $\mathbb{F}_{p^m}$ be a finite field of size p^m. A polynomial $f(x) \in \mathbb{F}_{p^m}[x]$ called a DO polynomial was defined in [11] with the following shape:

$$f(x) = \sum_{i,j=0}^{m-1} a_{ij} x^{p^i + p^j}, \ a_{ij} \in \mathbb{F}_{p^m}.$$

It is clear that $f(x)$ is also a homogeneous quadratic polynomial. A function $Q(x_1, x_2, \ldots, x_m)$ from $\mathbb{F}_p^m$ to $\mathbb{F}_p$ is called a quadratic form if it is a homogenous polynomial of degree two as follows:

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

We fix a basis $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ of $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$ and identify $x = \sum_{i=1}^m x_i \alpha_i$ with the vector $(x_1, x_2, \ldots, x_m) \in \mathbb{F}_p^m$, then $\mathrm{Tr}(f(x))$ is a quadratic form in the coordinates of $\mathbb{F}_p^m$. Moreover, every quadratic form $Q(x)$ from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$ can be represented as

$$Q(x) = \mathrm{Tr}\left(f(x)\right),$$

where $f(x)$ is a DO polynomial defined above. The rank of the quadratic form $Q(x)$ is defined as the codimension of $\mathbb{F}_p$-vector space

$$V = \{z \in \mathbb{F}_{p^m} \mid Q(x+z) - Q(x) - Q(z) = 0, \ \text{for all } z \in \mathbb{F}_{p^m}\},$$

which is denoted by $\mathrm{rank}(Q)$. Then $|V| = p^{m-\mathrm{rank}(Q)}$.

For a quadratic form $Q(x)$ with m variables over $\mathbb{F}_p$, there exists a symmetric matrix A such that $Q(x) = XAX'$, where $X = (x_1, x_2, \ldots, x_m) \in \mathbb{F}_p^m$ and X' denotes the transpose of X. The determinant $\det(Q)$ of $Q(x)$ is defined to be the determinant of A, and $Q(x)$ is nondegenerate if $\det(Q) \neq 0$. It is known that there exists a nonsingular matrix T such that TAT' is a diagonal matrix [18]. Making a nonsingular linear substitution $X = YT$ with $Y = (y_1, y_2, \ldots, y_m)$, we have

$$Q(x) = YTAT'Y' = \sum_{i=1}^{r} a_i y_i^2, \ \ a_i \in \mathbb{F}_p,$$

where $r(\leq m)$ is the rank of $Q(x)$. The following lemma gives a general result on an exponential sum of a quadratic function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$.

Lemma 1 (see Theorems 5.15 and 5.33 of [18]) *Let $Q(x)$ be a quadratic function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$ with rank r, and η be the quadratic multiplicative character of $\mathbb{F}_p$. Then*

$$\sum_{x \in \mathbb{F}_{p^m}} \omega_p^{Q(x)} = \eta(\Delta)\delta_{p,r} p^{m-\frac{r}{2}},$$

where ω_p is a pth primitive root of unity, and Δ is the determinant of $Q(x)$, and $\delta_{p,r} = (-1)^{\frac{r(p-1)^2}{8}}$. Moreover, for any $z \in \mathbb{F}_p^*$,

$$\sum_{x \in \mathbb{F}_{p^m}} \omega_p^{zQ(x)} = \eta^r(z)\eta(\Delta)\delta_{p,r} p^{m-\frac{r}{2}}.$$

It is well known that the parameters of an $[n, k, d]$ linear code $\mathcal{C}$ over $\mathbb{F}_p$ satisfy

$$d \leq n - k + 1, \tag{2}$$

and

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{p^i} \right\rceil, \tag{3}$$

where $\lceil x \rceil$ denotes the smallest integer, which is larger than or equal to x. If the equality in (2) holds, then $\mathcal{C}$ is called an optimal code with respect to the Singleton bound. If the equality in (3) holds, then $\mathcal{C}$ is called an optimal code with respect to the Griesmer bound.

Two linear codes $\mathcal{C}$ and $\mathcal{C}'$ of length n over $\mathbb{F}_{p^m}$ are equivalent (see Sect. 1 of Chapter 2 in [20]) if there exist n permutations $\pi_0, \pi_1, \ldots, \pi_{n-1}$ of the p^m elements in $\mathbb{F}_{p^m}$ and a permutation σ of the n coordinate positions such that if $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, then $\sigma(\pi_0(c_0), \pi_1(c_1), \ldots, \pi_{n-1}(c_{n-1})) \in \mathcal{C}'$. That is to say, let G and G' be generator matrices of $\mathcal{C}$ and $\mathcal{C}'$ respectively. The codes $\mathcal{C}$ and $\mathcal{C}'$ are equivalent if there exists a monomial matrix M such that $G' = GM$, where M is a square matrix such that in every row (and in every column) there is exactly one nonzero element in $\mathbb{F}_{p^m}$.

In order to discuss the existence of the solutions for two congruence equations in Sect. 4, we need the following well known facts.

Lemma 2 *Let ϕ, φ, μ be three nonzero elements in $\mathbb{F}_{p^m}$. Then for any congruence equation $\phi x \equiv \varphi \pmod{\mu}$, the equation has solutions if and only if* $\gcd(\phi, \mu) \mid \varphi$. *Moreover, the number of solutions is* $\gcd(\phi, \mu)$.

Lemma 3 *Let h, g be two positive integers. Then*

$$\gcd(p^h + 1, p^g - 1) = \begin{cases} p^{\gcd(h,g)} + 1, & \text{if } \dfrac{g}{\gcd(h,g)} \text{ is even}, \\ 2, & \text{if } \dfrac{g}{\gcd(h,g)} \text{ is odd}. \end{cases}$$

3 Linear codes from DO polynomials

Let $\mathbb{F}_{p^m}$ be a finite field with p^m elements, where p is an odd prime and m is a positive integer. Let Tr denote the trace function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$. Let $f(x)$ be a DO polynomial over $\mathbb{F}_{p^m}$. Recall that

$$D_f = \{x \in \mathbb{F}_{p^m}^* \mid \mathrm{Tr}(f(x)) = 0\} = \{d_1, d_2, \ldots, d_n\} \subset \mathbb{F}_{p^m}^*.$$

Table 1 Weight distribution of $\mathcal{C}_{D_f}$ for an odd r

Hamming weight	Frequency
0	1
$(p-1)p^{m-2}$	$p^m - p^r + p^{r-1} - 1$
$(p-1)(p^{m-2} + p^{\frac{2m-r-3}{2}})$	$\frac{p-1}{2}(p^{r-1} - p^{\frac{r-1}{2}})$
$(p-1)(p^{m-2} - p^{\frac{2m-r-3}{2}})$	$\frac{p-1}{2}(p^{r-1} + p^{\frac{r-1}{2}})$

Table 2 Weight distribution of $\mathcal{C}_{D_f}$ for an even r

Hamming weight	Frequency
0	1
$(p-1)p^{m-2} + \epsilon(p-1)^2 p^{\frac{2m-4-r}{2}}$	$p^m - p^r$
$(p-1)p^{m-2}$	$p^{r-1} + \epsilon(p-1)p^{\frac{r-2}{2}} - 1$
$(p-1)(p^{m-2} + \epsilon p^{\frac{2m-r-2}{2}})$	$(p-1)(p^{r-1} - \epsilon p^{\frac{r-2}{2}})$

From this set, we obtain a linear code proposed in [8] as follows:

$$\mathcal{C}_{D_f} = \{(\mathrm{Tr}(xd_1), \mathrm{Tr}(xd_2), \ldots, \mathrm{Tr}(xd_n)) \mid x \in \mathbb{F}_{p^m}\}. \tag{4}$$

From [10,26], we can get the following lemmas.

Lemma 4 *Let $\mathcal{C}_{D_f}$ be the linear code defined in (4) and n be the length of the codewords in $\mathcal{C}_{D_f}$. Let r be the rank of the quadratic form $Q(x) = \mathrm{Tr}(f(x))$ and its determinant be denoted by Δ. Then*

$$n = \begin{cases} p^{m-1} - 1, & \text{if } r \text{ is odd}, \\ p^{m-1} - 1 + (p-1)\eta(\Delta)\delta_{p,r} p^{m-1-\frac{r}{2}}, & \text{if } r \text{ is even}, \end{cases}$$

where η is the quadratic character of $\mathbb{F}_p$ and $\delta_{p,r}$ is defined in Lemma 1.

Lemma 5 *Let f be a DO polynomial over $\mathbb{F}_{p^m}$ and $\mathrm{Tr}(f)$ be a quadratic form with rank r. Let $\mathcal{C}_{D_f}$ be the linear code defined in (4).*

(1) *If r is odd, then $\mathcal{C}_{D_f}$ is a $[p^{m-1} - 1, m, (p-1)(p^{m-2} - p^{\frac{2m-r-3}{2}})]$ code with the weight distribution in Table 1.*

(2) *If r is even, then $\mathcal{C}_{D_f}$ is a $[p^{m-1} - 1 + \epsilon(p-1)p^{\frac{2m-r-2}{2}}, m]$ code with the weight distribution in Table 2, where $\epsilon = \eta(\Delta)\delta_{p,r}$, Δ is the determinant of $\mathrm{Tr}(f)$, η is the quadratic character of $\mathbb{F}_p$, and $\delta_{p,r}$ is defined in Lemma 1.*

It is observed that the Hamming weight of each codeword in the code $\mathcal{C}_{D_f}$ has a common divisor $p-1$. This indicates that $\mathcal{C}_{D_f}$ may be punctured into a shorter one whose weight distribution is derived from that of the original code. To this end, we define a equivalence relation in the set D_f as follows. For $\beta, \gamma \in D_f$, we say that β

Table 3 Weight distribution of $\mathcal{C}_{\bar{D}_f}$ for an odd r

Hamming weight	Frequency
0	1
p^{m-2}	$p^m - p^r + p^{r-1} - 1$
$p^{m-2} + p^{\frac{2m-r-3}{2}}$	$\frac{p-1}{2}(p^{r-1} - p^{\frac{r-1}{2}})$
$p^{m-2} - p^{\frac{2m-r-3}{2}}$	$\frac{p-1}{2}(p^{r-1} + p^{\frac{r-1}{2}})$

Table 4 Weight distribution of $\mathcal{C}_{\bar{D}_f}$ for an even r

Hamming weight	Frequency
0	1
$p^{m-2} + \epsilon(p-1)p^{\frac{2m-4-r}{2}}$	$p^m - p^r$
p^{m-2}	$p^{r-1} + \epsilon(p-1)p^{\frac{r-2}{2}} - 1$
$p^{m-2} + \epsilon p^{\frac{2m-r-2}{2}}$	$(p-1)(p^{r-1} - \epsilon p^{\frac{r-2}{2}})$

is equivalent to γ if and only if there exists $a \in \mathbb{F}_p^*$ such that $\beta = a\gamma$. The elements chosen from each equivalent class in D_f consist of a set $\bar{D}_f$. It is obvious that

$$D_f = \mathbb{F}_p^* \bar{D}_f = \{ab \ : \ a \in \mathbb{F}_p^*, \ b \in \bar{D}_f\}. \tag{5}$$

Then $\mathcal{C}_{\bar{D}_f}$ is a punctured version of $\mathcal{C}_{D_f}$, whose parameters are given in the following proposition.

Proposition 1 *Let f be a DO polynomial over $\mathbb{F}_{p^m}$ and r be the rank of quadratic form* $\mathrm{Tr}(f)$. *Let $\mathcal{C}_{\bar{D}_f}$ be the linear code defined above, where $\bar{D}_f$ is defined in (5).*

(1) *If r is odd, then $\mathcal{C}_{\bar{D}_f}$ is a $[\frac{p^{m-1}-1}{p-1}, m, p^{m-2} - p^{\frac{2m-r-3}{2}}]$ code with the weight distribution in Table 3.*

(2) *If r is even, then $\mathcal{C}_{\bar{D}_f}$ is a $[\frac{p^{m-1}-1}{p-1} + \epsilon p^{\frac{2m-r-2}{2}}, m]$ code with the weight distribution in Table 4, where $\epsilon = \eta(\Delta)\delta_{p,r}$, Δ is the determinant of* $\mathrm{Tr}(f)$, *η is the quadratic character of $\mathbb{F}_p$ and $\delta_{p,r}$ is defined in Lemma 1.*

From the weight distribution of $\mathcal{C}_{\bar{D}_f}$ above, we obtain some optimal linear codes with respect to the Singleton bound or the Griesmer bound as follows.

Corollary 1 *Let f be a DO polynomial over $\mathbb{F}_{p^m}$ and r be the rank of quadratic form* $\mathrm{Tr}(f)$. *Let $\mathcal{C}_{\bar{D}_f}$ be the linear code defined above.*

(1) *If $r = m = 3$, then $\mathcal{C}_{\bar{D}_f}$ is a $[p+1, 3, p-1]$ code. This code is optimal with respect to the Singleton bound and the Griesmer bound.*

(2) *If $r = m = 4$, and the determinant of* $\mathrm{Tr}(f)$ *is a non-square element in $\mathbb{F}_p^*$, then $\mathcal{C}_{\bar{D}_f}$ is a $[p^2+1, 4, p^2-p]$ code. This code is optimal with respect to the Griesmer bound.*

Proof When $r = m = 3$, from Proposition 1 we know that the length n of $\mathcal{C}_{\bar{D}_f}$ is $p+1$, the dimension k of $\mathcal{C}_{\bar{D}_f}$ is 3, and the minimal distance d is $p-1$. It is easy to verify that these parameters of the code $\mathcal{C}_{\bar{D}_f}$ satisfy the equality in (2) and (3), respectively. Therefore, $\mathcal{C}_{\bar{D}_f}$ is optimal with respect to the Singleton bound and the Griesmer bound. The proof of case (2) is similar, and we omit the details here. □

Remark 1 Section 5 of Chapter 11 in [20] has proved that there exist $[p+1, 3, p-1]$ (cyclic) MDS codes. Corollary 1 only provides a class of MDS code with this parameters by trace representations.

It is well known that an $[n, k]$ linear code is called projective if no two columns of a generator matrix G are linearly dependent, i.e., if the columns of G are pairwise different points in a projective $(k-1)$-dimensional space. A strong regular graph with parameters (v, K, λ, μ) is a finite simple graph with v vertices which is regular of degree K, and any two distinct vertices have λ common neighbours if they are adjacent and μ common neighbours if they are non-adjacent. There are strong connections between projective two-weight codes and strong regular graphs.

Let q be a power of a prime and $\mathbb{F}_q$ be a finite field with q elements. In 1985, Calderbank and Kantor [9] showed that if an $[n, k]$ linear code with weights w_1 and w_2 over $\mathbb{F}_q$ is a projective two-weight code, then we can obtain a strong regular graph with the following parameters (Corollary 3.7 in [2]),

$$\begin{aligned} v &= q^k, \quad K = n(q-1),\\ \lambda &= K^2 + 3K - q(w_1+w_2) - Kq(w_1+w_2) + q^2 w_1 w_2,\\ \mu &= \frac{q^2 w_1 w_2}{q^k} = K^2 + K - kq(w_1+w_2) + q^2 w_1 w_2. \end{aligned}$$

In 2006, Bouyukliev et al. [1] showed that a two-weight code $[q^2+1, 4, q^2-q]$ with weights $w_1 = q^2 - q$ and $w_2 = q^2$ is a projective two-weight code. Hence, from the code in Corollary 1, we can obtain a strong regular graph with parameters $(p^4, p^3 - p^2 + p - 1, p - 2, p^2 - p)$.

Example 1 (1) Let $p = 3$ and $m = 3$. Let $f(x) = x^2, x^4, x^{10} - x^6 - x^2$ or $x^{10} + x^6 - x^2$. Then the code $C_{\bar{D}_f}$ has parameters [4, 3, 2] and the weight enumerator $1 + 12x^2 + 8x^3 + 6x^4$. This code is an MDS code and is optimal with respect to the Griesmer bound.

(2) Let $p = 7$ and $m = 4$. Let $f(x) = x^{50}$ or $\alpha^{11}x^8 + \alpha^{20}x^2$, where α is a primitive element of $\mathbb{F}_{7^4}$. Then the code $C_{\bar{D}_f}$ has parameters [50, 4, 42] and weight enumerator $1 + 2100x^{42} + 300x^{49}$. This code is optimal with respect to the Griesmer bound.

3.1 A class of linear codes from some special DO polynomials

From Proposition 1, in order to determine the parameters of the linear code $\mathcal{C}_{\bar{D}_f}$, we need to know the rank and determinant of the quadratic form $\mathrm{Tr}(f)$, and they are

Table 5 Weight distribution of $\mathcal{C}_{\bar{D}_f}$ for an odd m

Hamming weight	Frequency
0	1
p^{m-2}	$p^{m-1}-1$
$p^{m-2}+p^{\frac{m-3}{2}}$	$\frac{p-1}{2}(p^{m-1}-p^{\frac{m-1}{2}})$
$p^{m-2}-p^{\frac{m-3}{2}}$	$\frac{p-1}{2}(p^{m-1}+p^{\frac{m-1}{2}})$

Table 6 Weight distribution of $\mathcal{C}_{\bar{D}_f}$

Hamming weight	Frequency
0	1
p^{m-2}	$p^{m-1}+(-1)^{\frac{m}{2^{v+1}}}(p-1)p^{\frac{m-2}{2}}-1$
$p^{m-2}+(-1)^{\frac{m}{2^{v+1}}}p^{\frac{m-2}{2}}$	$(p-1)(p^{m-1}-(-1)^{\frac{m}{2^{v+1}}}p^{\frac{m-2}{2}})$

difficult to determine in general. In this subsection, we present a class of linear codes from binomial polynomials and determine their weight distributions explicitly.

Proposition 2 *Let $\nu_2(\cdot)$ denote the 2-adic order function. Let i and j be positive integers with $i > j$. Let $f(x) = x^{p^i+1}+x^{p^j+1} \in \mathbb{F}_{p^m}[x]$ and $\mathcal{C}_{\bar{D}_f}$ be the linear code defined above.*

(1) *If m is odd, then $\mathcal{C}_{\bar{D}_f}$ is a $[\frac{p^{m-1}-1}{p-1}, m, p^{m-2}-p^{\frac{m-3}{2}}]$ code with the weight distribution in Table 5.*

(2) *If $v=\nu_2(i)=\nu_2(j)<\nu_2(m)$ and $\nu_2(m)\le \min\{\nu_2(i-j), \nu_2(i+j)\}$, then $\mathcal{C}_{\bar{D}_f}$ is a $[\frac{p^{m-1}-1}{p-1}+(-1)^{\frac{m}{2^{v+1}}}p^{\frac{m-2}{2}}, m]$ code with the weight distribution in Table 6.*

(3) *Let $v=\nu_2(i)=\nu_2(j)$ and $d=\gcd(i+j,m)$. If $v<\nu_2(m)$ and $\nu_2(i+j)<\nu_2(m)\le\nu_2(i-j)$, then $\mathcal{C}_{\bar{D}_f}$ is a $[\frac{p^{m-1}-1}{p-1}+(-1)^{\frac{m-d}{2^{v+1}}}p^{\frac{m+d-2}{2}}, m]$ code with the weight distribution in Table 7.*

(4) *Let $v=\nu_2(i)=\nu_2(j)$ and $d=\gcd(i-j,m)$. If $v<\nu_2(m)$ and $\nu_2(i-j)<\nu_2(m)\le\nu_2(i+j)$, then $\mathcal{C}_{\bar{D}_f}$ is a $[\frac{p^{m-1}-1}{p-1}+(-1)^{\frac{m-d}{2^{v+1}}}p^{\frac{m+d-2}{2}}, m]$ code with the weight distribution in Table 7.*

In order to prove Proposition 2, we need the following lemma.

Lemma 6 (see Theorem 7.3 of [12]) *Let $\nu_2(\cdot)$ denote the 2-adic order function. Let $f\in\mathbb{F}_{p^m}[x]$ be a DO polynomial given in Proposition 2 with $\nu_2(i)=\nu_2(j)<\nu_2(m)$. Then*

$$\eta(\Delta)=\begin{cases}(-1)^{\left(\frac{1}{4}(p-1)^2+1\right)\frac{r}{2}}, & v=0,\\ (-1)^{\frac{r}{2^{v+1}}}, & v>0,\end{cases}$$

where $v=\nu_2(i)$, Δ and r are the determinant and the rank of $\mathrm{Tr}(f)$*, respectively.*

Table 7 Weight distribution of $\mathcal{C}_{\bar{D}_f}$

Hamming weight	Frequency
0	1
$p^{m-2}+(-1)^{\frac{m-d}{2^{\nu+1}}}(p-1)p^{\frac{m+d-4}{2}}$	p^m-p^{m-d}
p^{m-2}	$p^{m-d-1}+(-1)^{\frac{m-d}{2^{\nu+1}}}(p-1)p^{\frac{m-d-2}{2}}-1$
$p^{m-2}+(-1)^{\frac{m-d}{2^{\nu+1}}}p^{\frac{m+d-2}{2}}$	$(p-1)(p^{m-d-1}-(-1)^{\frac{m-d}{2^{\nu+1}}}p^{\frac{m-d-2}{2}})$

Proof of Proposition 2 It is known that the weight distribution of $\mathcal{C}_{\bar{D}_f}$ is related to the determinant and rank of $\mathrm{Tr}(f)$, and they have a connection given in Lemma 6. So, we may obtain the weight distribution of $\mathcal{C}_{\bar{D}_f}$ if we can determine the rank of $\mathrm{Tr}(f)$.

Note that the rank of $\mathrm{Tr}(f)$ equals the codimension of $\mathbb{F}_p$- vector space

$$\left\{x\in\mathbb{F}_{p^m}\mid \mathrm{Tr}(f(x+y)-f(x)-f(y))=\mathrm{Tr}(yL(x))=0,\ \text{for all } y\in\mathbb{F}_{p^m}\right\},$$

where

$$L(x)=x^{p^{2i}}+x^{p^{i+j}}+x^{p^{i-j}}+x. \tag{6}$$

So, the rank of $\mathrm{Tr}(f)$ is equal to the codimension of the null space of $L(x)$.

Cases (1) and (2): From (6) we have

$$(x^{p^{i-j}}+x)^{p^{i+j}}+(x^{p^{i-j}}+x)=0. \tag{7}$$

Set $z=x^{p^{i-j}}+x$. (7) is reduced to

$$z^{p^{i+j}}+z=0. \tag{8}$$

Obviously, $z=0$ is a solution of (8). If $z\neq 0$, then we obtain $z^{p^{i+j}-1}=-1$. Let α be a primitive element of $\mathbb{F}_{p^m}$ and $z=\alpha^s$ for some positive integer s. Then $z^{p^{i+j}-1}=-1$ is reduced to

$$\alpha^{(p^{i+j}-1)s}=\alpha^{\frac{p^m-1}{2}},$$

which is equivalent to

$$(p^{i+j}-1)s\equiv\frac{p^m-1}{2}\ (\mathrm{mod}\ p^m-1). \tag{9}$$

In Cases (1) and (2), it is easy to see that $\gcd(p^{i+j}-1,p^m-1)\nmid\frac{p^m-1}{2}$ since $\nu_2(m)\le\nu_2(i+j)$. By Lemma 2, (9) has no solution for s. It follows that (8) has only one solution $z=0$. Similarly, one can verify that $x^{p^{i-j}}+x=0$ has also only one solution $x=0$ since $\nu_2(m)\le\nu_2(i-j)$. That is to say, the rank of $\mathrm{Tr}(f)$ is m. In the case of m being odd, from Table 3 we get the weight distribution of $\mathcal{C}_{\bar{D}_f}$, which is given in Table 5. In the case of $\nu_2(m) > 0$, from Lemma 6 we have

$$\begin{aligned}\epsilon = \eta(\Delta)\delta_{p,m} &= \begin{cases} (-1)^{\left(\frac{1}{4}(p-1)^2+1\right)\frac{m}{2}}(-1)^{\frac{(p-1)^2m}{8}}, & v=0 \\ (-1)^{\frac{m}{2^{v+1}}}(-1)^{\frac{(p-1)^2m}{8}}, & v>0 \end{cases}\\ &= (-1)^{\frac{m}{2^{v+1}}}.\end{aligned}$$

Substituting this ϵ and $r = m$ into Table 4, we get Table 6.

Case (3): From (6) we get

$$(x^{p^{i+j}} + x)^{p^{i-j}} + (x^{p^{i+j}} + x) = 0. \tag{10}$$

Set $y = x^{p^{i+j}} + x$. (10) is reduced to

$$y^{p^{i-j}} + y = 0. \tag{11}$$

Then using similar techniques as we prove the number of solutions in (8), we obtain that (11) has only one solution $y = 0$, and $x^{p^{i+j}} + x = 0$ has p^d solutions since $\nu_2(i + j) < \nu_2(m) \le \nu_2(i - j)$, where $d = \gcd(i + j, m)$. So, the rank of $\mathrm{Tr}(f)$ is equal to $m - d$. In this case, from Lemma 6 we have

$$\begin{aligned}\epsilon = \eta(\Delta)\delta_{p,m-d} &= \begin{cases} (-1)^{\left(\frac{1}{4}(p-1)^2+1\right)\frac{m-d}{2}}(-1)^{\frac{(p-1)^2(m-d)}{8}}, & v=0 \\ (-1)^{\frac{m-d}{2^{v+1}}}(-1)^{\frac{(p-1)^2(m-d)}{8}}, & v>0 \end{cases}\\ &= (-1)^{\frac{m-d}{2^{v+1}}}.\end{aligned}$$

Substituting this ϵ and $r = m - d$ into Table 4, we get Table 7.

The proof of Case (4) is similar to that of Case (3). □

Example 2 (1) Let $p = 3, m = 3$ and $f(x) = x^{10} + x^4$ or $x^{28} + x^4$. Then the code $C_{\bar{D}_f}$ has parameters [4, 3, 2] and the weight enumerator $1 + 12x^2 + 8x^3 + 6x^4$. This code is an MDS code and optimal with respect to the Griesmer bound.

(2) Let $p = 3, m = 6$ and $f(x) = x^{28} + x^4$. Then the code $C_{\bar{D}_f}$ has parameters [224, 6, 72] and the weight enumerator $1 + 504x^{72} + 224x^{81}$.

(3) Let $p = 3, m = 12$ and $f(x) = x^{3^9+1} + x^4$ or $x^{3^7+1} + x^4$. Then the code $C_{\bar{D}_f}$ has parameters [87844, 12, 58320] or [82012, 12, 52488] and the weight enumerators $1 + 39528x^{58320} + 472392x^{58563} + 19520x^{59049}$ or $1 + 504x^{52488} + 224x^{59049} + 472392x^{54675}$, respectively.

4 Linear codes from $f = x^\ell$ for ℓ satisfying some congruence conditions

Let $\mathbb{F}_{p^m}$ be a finite field of size p^m, where m is odd and p is an odd prime with $p \equiv 3 \pmod 4$. Let ℓ be an even integer satisfying one of the following conditions:

$$\begin{aligned} &\bullet \quad (p^k+1)\ell \equiv \frac{p^m+1}{2} \pmod{p^m-1}; \\ &\bullet \quad \frac{p^m+1}{2}\ell \equiv p^k+1 \pmod{p^m-1}, \end{aligned} \tag{12}$$

where k is a nonnegative integer. Next, we show that there exists an even integer satisfying one of congruence equations in (12). Since m is odd, by Lemma 3 we have $2 = \gcd(p^k+1, p^m-1) \mid \frac{p^m+1}{2}$ and $2 = \gcd(\frac{p^m+1}{2}, p^m-1) \mid p^k+1$. Then the congruence equations in (12) have solutions for any integer k by Lemma 2. On the other hand, let b be an integer satisfying the first congruence equation. Then $(p^k+1)(b+\frac{p^m-1}{2}) \equiv (p^k+1)b \equiv \frac{p^m+1}{2} \pmod{p^m-1}$. Similarly, if an integer b satisfies the second congruence equation, then $\frac{p^m+1}{2}(b+\frac{p^m-1}{2}) \equiv \frac{p^m+1}{2}b \equiv p^k+1 \pmod{p^m-1}$. These show that if an integer b satisfies one of the congruence equations in (12), then $b+\frac{p^m-1}{2}$ satisfies the corresponding congruence equation. Since $p \equiv 3 \pmod 4$ and m is odd, the number $\frac{p^m-1}{2}$ is odd. Hence, there exists an even integer satisfying each congruence equation in (12).

In this section, we will investigate the weight distribution of a linear code defined by

$$\mathcal{C}_{D_f} = \left\{(\mathrm{Tr}(xd_1), \mathrm{Tr}(xd_2), \ldots, \mathrm{Tr}(xd_n)) \mid x \in \mathbb{F}_{p^m}\right\}, \tag{13}$$

where the defining set D_f is as follows:

$$D_f = \{x \in \mathbb{F}_{p^m}^* \mid \mathrm{Tr}(x^\ell) = 0\} = \{d_1, d_2, \ldots, d_n\}.$$

The following lemma presents the length of the linear code $\mathcal{C}_{D_f}$.

Lemma 7 *Let p be an odd prime with $p \equiv 3 \pmod 4$. Let m be an odd number and ℓ be an even number satisfying one of the conditions in (12). Let $\mathcal{C}_{D_f}$ be the linear code defined in (13). Then the length of the codewords in $\mathcal{C}_{D_f}$ is $p^{m-1}-1$.*

Proof We only prove the case of ℓ satisfying the first condition of (12), i.e., $(p^k+1)\ell \equiv \frac{p^m+1}{2} \pmod{p^m-1}$, and the proof of the case of ℓ satisfying the second condition of (12) is similar.

Let SQ and NSQ denote the set of all square elements and non-square elements in $\mathbb{F}_{p^m}^*$, respectively. Let n be the length of a codeword in $\mathcal{C}_{D_f}$.

$$\begin{aligned} n = \sharp\{x \in \mathbb{F}_{p^m}^* | \mathrm{Tr}(x^\ell) = 0\} &= \frac{p^m - 1}{p} + \frac{1}{p} \sum_{u \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}^*} \omega_p^{u\mathrm{Tr}(x^\ell)} \\ &= \frac{p^m - 1}{p} + \frac{1}{p} \sum_{u \in \mathbb{F}_p^*} \left(\sum_{x \in \mathrm{SQ}} \omega_p^{u\mathrm{Tr}(x^\ell)} + \sum_{x \in \mathrm{NSQ}} \omega_p^{u\mathrm{Tr}(x^\ell)} \right) \\ &= \frac{p^m - 1}{p} + \frac{1}{2p} \sum_{u \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}^*} \left(\omega_p^{u\mathrm{Tr}(x^{\ell(p^k+1)})} + \omega_p^{u\mathrm{Tr}((-1)^\ell x^{\ell(p^k+1)})} \right) \\ &= \frac{p^m - 1}{p} + \frac{1}{p} \sum_{u \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}^*} \omega_p^{u\mathrm{Tr}\left(x^{\frac{p^m+1}{2}}\right)}, \end{aligned} \tag{14}$$

where in the fourth equality, we used the fact that $\{x^{p^k+1} \,|\, x \in \mathbb{F}_{p^m}^*\} = \{x^2 \,|\, x \in \mathbb{F}_{p^m}^*\}$ since $\gcd(p^k + 1, p^m - 1) = 2$.

It is easy to see that $\gcd(\frac{p^m+1}{2}, p^m - 1) = 2$ since $p \equiv 3 \pmod 4$ and m is odd. So, $\{x^{\frac{p^m+1}{2}} \,|\, x \in \mathbb{F}_{p^m}^*\} = \{x^2 \,|\, x \in \mathbb{F}_{p^m}^*\}$. From Lemma 1, we have

$$\begin{aligned} n &= \frac{p^m - 1}{p} + \frac{1}{p} \sum_{u \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}^*} \omega_p^{u\mathrm{Tr}(x^2)} \\ &= p^{m-1} - 1 + \frac{1}{p} \sum_{u \in \mathbb{F}_p^*} \eta^m(u) \sum_{x \in \mathbb{F}_{p^m}^*} \omega_p^{\mathrm{Tr}(x^2)} \\ &= p^{m-1} - 1. \end{aligned}$$

□

To determine the weight distribution of $\mathcal{C}_{D_f}$, we need to show the value distribution of the set

$$N_\ell(b) = \sharp\{x \in \mathbb{F}_{p^m} \,|\, \mathrm{Tr}(x^\ell + bx) = 0\}$$

for b running over $\mathbb{F}_{p^m}^*$. To this end, we will investigate the relation of the value distribution between $N_\ell(b)$ and the following two sets

$$N_k(b, 1) = \sharp\{x \in \mathbb{F}_{p^m} \,|\, \mathrm{Tr}\left(bx^{p^k+1} + x\right) = 0\}$$

and

$$N_k(1, b) = \sharp\{x \in \mathbb{F}_{p^m} \,|\, \mathrm{Tr}\left(x^{p^k+1} + bx\right) = 0\}$$

for b running through $\mathbb{F}_{p^m}^*$.

Lemma 8 *Let p be a prime with $p \equiv 3 \pmod 4$. Let m be an odd number and ℓ be an even number satisfying one of the conditions in (12). When b runs over $\mathbb{F}_{p^m}^*$, the sets $N_\ell(b)$, $N_k(b,1)$ and $N_k(1,b)$ have the same value distribution as follows:*

$$\begin{cases} p^{m-1}, & p^{m-1}-1 \text{ times}, \\ p^{m-1}-p^{\frac{m-1}{2}}, & \frac{p-1}{2}\left(p^{m-1}-p^{\frac{m-1}{2}}\right) \text{ times}, \\ p^{m-1}+p^{\frac{m-1}{2}}, & \frac{p-1}{2}\left(p^{m-1}+p^{\frac{m-1}{2}}\right) \text{ times}. \end{cases} \tag{15}$$

Proof Let SQ and NSQ denote all square elements and non-square elements in $\mathbb{F}_{p^m}^*$, respectively. It is easy to verify that $\{x^{p^k+1} \mid x \in \mathbb{F}_{p^m}\} = \{x^2 \mid x \in \mathbb{F}_{p^m}\}$ for m being odd. If ℓ satisfies the first condition of (12), then

$$\begin{aligned} N_\ell(b) =& \sharp\left\{x \in \mathbb{F}_{p^m} \mid \mathrm{Tr}(x^\ell + bx) = 0\right\} \\ =& 1 + \sharp\left\{x \in \mathrm{SQ} \mid \mathrm{Tr}(x^\ell + bx) = 0\right\} + \sharp\left\{x \in \mathrm{NSQ} \mid \mathrm{Tr}(x^\ell + bx) = 0\right\} \\ =& 1 + \frac{1}{2}\sharp\left\{x \in \mathbb{F}_{p^m}^* \mid \mathrm{Tr}\left(x^{\frac{p^m+1}{2}} + bx^{p^k+1}\right) = 0\right\} \\ &+ \frac{1}{2}\sharp\left\{x \in \mathbb{F}_{p^m}^* \mid \mathrm{Tr}\left((-1)^\ell x^{\frac{p^m+1}{2}} - bx^{(p^k+1)}\right) = 0\right\}. \end{aligned}$$

Observe that $x^{\frac{p^m+1}{2}} = x$ or $-x$ for x in SQ or NSQ, respectively. Since ℓ is even and m is odd, we have

$$\begin{aligned} N_\ell(b) =& 1 + \frac{1}{2}\sharp\left\{x \in \mathrm{SQ} \mid \mathrm{Tr}\left(x + bx^{p^k+1}\right) = 0\right\} \\ &+ \frac{1}{2}\sharp\left\{x \in \mathrm{NSQ} \mid \mathrm{Tr}\left(-x + bx^{p^k+1}\right) = 0\right\} \\ &+ \frac{1}{2}\sharp\left\{x \in \mathrm{SQ} \mid \mathrm{Tr}\left(x - bx^{p^k+1}\right) = 0\right\} \\ &+ \frac{1}{2}\sharp\left\{x \in \mathrm{NSQ} \mid \mathrm{Tr}\left(-x - bx^{p^k+1}\right) = 0\right\} \\ =& 1 + \frac{1}{2}\sharp\left\{x \in \mathbb{F}_{p^m}^* \mid \mathrm{Tr}\left(x + bx^{p^k+1}\right) = 0\right\} \\ &+ \frac{1}{2}\sharp\left\{x \in \mathbb{F}_{p^m}^* \mid \mathrm{Tr}\left(x - bx^{p^k+1}\right) = 0\right\} \\ =& \frac{1}{2}\sharp\left\{x \in \mathbb{F}_{p^m} \mid \mathrm{Tr}\left(x + bx^{p^k+1}\right) = 0\right\} \\ &+ \frac{1}{2}\sharp\left\{x \in \mathbb{F}_{p^m} \mid \mathrm{Tr}\left(-x - b(-x)^{p^k+1}\right) = 0\right\} \\ =& \sharp\left\{x \in \mathbb{F}_{p^m} \mid \mathrm{Tr}\left(bx^{p^k+1} + x\right) = 0\right\} \\ =& N_k(b,1). \end{aligned} \tag{16}$$

Table 8 Weight distribution of $\mathcal{C}_{D_f}$

Hamming weight	Frequency
0	1
$(p-1)p^{m-2}$	$p^{m-1}-1$
$(p-1)(p^{m-2}+p^{\frac{m-3}{2}})$	$\frac{p-1}{2}(p^{m-1}-p^{\frac{m-1}{2}})$
$(p-1)(p^{m-2}-p^{\frac{m-3}{2}})$	$\frac{p-1}{2}(p^{m-1}+p^{\frac{m-1}{2}})$

This shows that the sets $N_\ell(b)$ and $N_k(b,1)$ have the same value distribution for b running over $\mathbb{F}_{p^m}^*$. Similarly, if ℓ satisfies the second condition of (12), then the sets $N_\ell(b)$ and $N_k(1,b)$ have the same value distribution for b running over $\mathbb{F}_{p^m}^*$.

Next, we show that the sets $N_k(1,b)$ and $N_k(b,1)$ have the same value distribution given in (15). Let

$$N(a,c)=\sharp\{x\in\mathbb{F}_{p^m}\mid \mathrm{Tr}(ax^{p^k+1}+cx)=0\}.$$

Note that m is odd, by Theorem 2 in [24], for a,c running over $\mathbb{F}_{p^m}^*$, the set $N(a,c)$ has the following value distribution,

$$\begin{cases} p^{m-1}+p^{\frac{m-1}{2}}, & \frac{p-1}{2}(p^m-1)\left(p^{m-1}+p^{\frac{m-1}{2}}\right) \text{ times},\\ p^{m-1}, & (p^m-1)(p^{m-1}-1) \text{ times},\\ p^{m-1}-p^{\frac{m-1}{2}}, & \frac{p-1}{2}(p^m-1)\left(p^{m-1}-p^{\frac{m-1}{2}}\right) \text{ times}.\end{cases} \tag{17}$$

For a fixed $a\in\mathbb{F}_{p^m}^*$, if a is a square element in $\mathbb{F}_{p^m}^*$, then there exists $\beta\in\mathbb{F}_{p^m}$ such that $a=\beta^{p^k+1}$, and

$$N(a,c)=\sharp\{x\in\mathbb{F}_{p^m}\mid \mathrm{Tr}(x^{p^k+1}+c\beta^{-1}x)=0\}. \tag{18}$$

If a is a non-square element in $\mathbb{F}_{p^m}^*$, then there exists $\beta\in\mathbb{F}_{p^m}$ such that $-a=\beta^{p^k+1}$, and

$$N(a,c)=\sharp\{x\in\mathbb{F}_{p^m}\mid \mathrm{Tr}(x^{p^k+1}-c\beta^{-1}x)=0\}. \tag{19}$$

From (18) and (19), we know that for a fixed $a\in\mathbb{F}_{p^m}^*$ and c running over $\mathbb{F}_{p^m}^*$, $N(a,c)$ has the same value distribution as that of $N_k(1,b)$ for b running over $\mathbb{F}_{p^m}^*$. Hence, from (17) we obtain that $N_k(1,b)$ has the value distribution given in (15) for b running over $\mathbb{F}_{p^m}^*$. Similarly, $N_k(b,1)$ has the value distribution given in (15) for b running over $\mathbb{F}_{p^m}^*$. By (16), the result follows. □

Now, we give the weight distribution of the linear code $\mathcal{C}_{D_f}$ defined in (13).

Theorem 1 *Let p be an odd prime with $p\equiv 3 \pmod 4$. Let m be an odd number and ℓ be an even number satisfying one of the conditions in (12). Then $\mathcal{C}_{D_f}$ in (13) is a $[p^{m-1}-1, m, (p-1)(p^{m-2}-p^{\frac{m-3}{2}})]$ code with the weight distribution in Table 8.*

Proof We only prove the case of ℓ satisfying the first condition of (12), i.e., $(p^k+1)\ell \equiv \frac{p^m+1}{2} \pmod{p^m-1}$, and the proof of the second case is similar.

Let $\mathcal{C}_{D_f}$ be the linear code defined in (13), and its length n is determined in Lemma 7. For $b \in \mathbb{F}_{p^m}^*$, a codeword in $\mathcal{C}_{D_f}$ is

$$\mathbf{c}_b = (\mathrm{Tr}(bd_1), \mathrm{Tr}(bd_2), \ldots, \mathrm{Tr}(bd_n)),$$

where $d_1, d_2, \ldots, d_n$ are the elements of D_f. Its Hamming weight is as follows:

$$\begin{aligned} wt(\mathbf{c}_b) &= p^{m-1} - 1 - \sharp\{x \in \mathbb{F}_{p^m}^* \mid \mathrm{Tr}(x^\ell) = 0 \text{ and } \mathrm{Tr}(bx) = 0\} \\ &= p^{m-1} - \frac{1}{p^2} \sum_{x \in \mathbb{F}_{p^m}} \sum_{y \in \mathbb{F}_p} \omega_p^{y\mathrm{Tr}(x^\ell)} \sum_{z \in \mathbb{F}_p} \omega_p^{z\mathrm{Tr}(bx)}. \end{aligned}$$

Since $\sum_{x\in\mathbb{F}_{p^m}} \sum_{y\in\mathbb{F}_p} \omega_p^{y\mathrm{Tr}(x^\ell)} = p^m$ and $\sum_{x\in\mathbb{F}_{p^m}} \sum_{z\in\mathbb{F}_p} \omega_p^{z\mathrm{Tr}(bx)} = 0$, then

$$wt(\mathbf{c}_b) = (p-1)p^{m-2} - \frac{1}{p^2} \sum_{x \in \mathbb{F}_{p^m}} \sum_{y \in \mathbb{F}_p^*} \omega_p^{y\mathrm{Tr}(x^\ell)} \sum_{z \in \mathbb{F}_p^*} \omega_p^{z\mathrm{Tr}(bx)}.$$

Set $z = uy$. It is clear that when (y, z) runs through $\mathbb{F}_{p^m}^* \times \mathbb{F}_{p^m}^*$, (u, y) also runs through $\mathbb{F}_{p^m}^* \times \mathbb{F}_{p^m}^*$. It is easy to verify that $N_k(b, 1) = N_k(ub, 1)$ for any $u \in \mathbb{F}_p^*$. We have

$$\begin{aligned} wt(\mathbf{c}_b) &= (p-1)p^{m-2} - \frac{1}{p^2} \sum_{y \in \mathbb{F}_p^*} \sum_{u \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \omega_p^{y\mathrm{Tr}(x^\ell + ubx)} \\ &= 2(p-1)p^{m-2} - \frac{1}{p^2} \sum_{u \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_{p^m}} \sum_{y \in \mathbb{F}_p} \omega_p^{y\mathrm{Tr}(x^\ell + ubx)} \\ &= 2(p-1)p^{m-2} - \frac{1}{p} \sum_{u \in \mathbb{F}_p^*} \sharp\{x \in \mathbb{F}_{p^m} \mid \mathrm{Tr}(x^\ell + ubx) = 0\} \\ &= 2(p-1)p^{m-2} - \frac{1}{p} \sum_{u \in \mathbb{F}_p^*} \sharp\{x \in \mathbb{F}_{p^m} \mid \mathrm{Tr}(ubx^{p^k+1} + x) = 0\} \\ &= \frac{(p-1)}{p}(2p^{m-1} - N_k(b, 1)) \\ &= \frac{(p-1)}{p}(2p^{m-1} - N_\ell(b)). \end{aligned} \tag{20}$$

By Lemma 8 and (20), we get the weight distribution of $\mathcal{C}_{D_f}$. From the fact that $wt(\mathbf{c}_b) > 0$ for any $b \in \mathbb{F}_{p^m}^*$, we deduce that the dimension of $\mathcal{C}_{D_f}$ is m. □

Remark 2 When $k = 0$, it is easy to see that $\ell = 2$ is a solution of the second congruence equation in (12). So, in this case, the linear codes in Theorem 1 and those in [8] are the same.

One can verify that when $p = m = 3$, $\ell = 10$ is a solution of the first and the second congruence equation in (12) for the case $k = 1$ and $k = 2$, respectively. Magma shows that when $p = m = 3$, the linear code in [8] has a generator matrix

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 0 & 0 & 2 \\ 0 & 1 & 0 & 2 & 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 2 & 2 \end{pmatrix}.$$

Accordingly, when $p = m = 3$ and $\ell = 10$, the linear code in Theorem 1 has a generator matrix

$$G_2 = \begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 0 & 0 & 2 \\ 0 & 1 & 0 & 1 & 0 & 2 & 0 & 2 \\ 0 & 0 & 1 & 1 & 0 & 0 & 2 & 2 \end{pmatrix}.$$

From the connection between linear transformations and multiplication of monomial matrices, we have that there is no monomial matrix M in $\mathbb{F}_{3^3}$ such that $G_2 = G_1 M$. This means that there exists ℓ in (12) such that the linear codes in Theorem 1 and those in [8] are not equivalent.

Let $\bar{D}_f$ be a defining set as in (5). The weight distribution of the punctured version of $\mathcal{C}_{D_f}$ is as follows.

Proposition 3 *Let p be an odd prime with $p \equiv 3 \pmod 4$. Let m be an odd number and ℓ be an even number satisfying one of the conditions in (12). Then $\mathcal{C}_{\bar{D}_f}$ is a $[\frac{p^{m-1}-1}{p-1}, m, p^{m-2} - p^{\frac{m-3}{2}}]$ code with the weight distribution in Table 5.*

From the weight distribution of $\mathcal{C}_{\bar{D}_f}$ above, we have the following corollary.

Corollary 2 *Let $\mathcal{C}_{\bar{D}_f}$ be the linear code defined above. If $m = 3$, then $\mathcal{C}_{\bar{D}_f}$ is a $[p+1, 3, p-1]$ code. This code is optimal with respect to the Singleton bound and the Griesmer bound.*

Example 3 (1) Let $p = 3$ and $m = 3$. Let $\ell = 4$ or 10. Then the code $\mathcal{C}_{\bar{D}_f}$ has parameters [4, 3, 2] and the weight enumerator $1 + 12x^2 + 8x^3 + 6x^4$. This code is optimal with respect to the Griesmer bound and the Singleton bound.

(2) Let $p = 7$ and $m = 3$. Let $\ell = 8$ or 278. Then the code $\mathcal{C}_{\bar{D}_f}$ has parameters [8, 3, 6] and the weight enumerator $1 + 126x^6 + 48x^7 + 168x^8$. This code is optimal with respect to the Griesmer bound and the Singleton bound.

5 Concluding remarks

In this paper, we presented several classes of linear codes with two or three weights and determined their weight distributions. From the punctured version of the constructed linear codes, we obtained some optimal linear codes with respect to the Singleton bound or the Griesmer bound.

Let w_{min} and w_{max} denote the minimum and maximum nonzero weights of a linear code $\mathcal{C}$. Ding and Ding in [8] showed that if the linear code $\mathcal{C}$ with $w_{min}/w_{max} >$

$(p-1)/p$, then the secret sharing scheme based on the dual code $\mathcal{C}^{\perp}$ has the nice access structure. Using similar techniques as in [8], one can verify that when $m \geq 12$ and $r \geq 6$, the codes constructed in the paper satisfy $w_{min}/w_{max} > (p-1)/p$. It then follows that the dual codes $\mathcal{C}_{D_f}^{\perp}$ and $\mathcal{C}_{\bar{D}_f}^{\perp}$ can be employed to obtain secret sharing schemes with interesting access structures.

Acknowledgements The authors would like to thank Prof. Q. Xiang for providing Reference [13], and the reviewers and the editor for their helpful comments and valuable suggestions, which have greatly improved the presentation of this paper. This work of X. Wang and H. Liu was supported by the self-determined research funds of CCNU from the collegess basic research and operation of MOE (Grant No. CCNU18TS028).

References

1. Bouyukliev, I., Fack, V., Winne, J., Willems, W.: Projective two-weight codes with small parameters and their corresponding graphs. Des. Codes Cryptogr. **41**, 59–78 (2006)
2. Calderbank, A.R., Kantor, W.M.: The geometry of two-weight codes. Bull Lond. Math. Soc. **18**, 97–122 (1986)
3. Ding, C., Niederreiter, H.: Cyclotomic linear codes of order 3. IEEE Trans. Inf. Theory **53**(6), 2274–2277 (2007)
4. Ding, C., Luo, J., Niederreiter, H.: Two weight codes punctured from irreducible cyclic codes, In: Li, Y., Ling, S., Niederreiter, H., Wang, H., Xing, C., Zhang, S. (Eds.) Proceedings of the First International Workshop on Coding Theory and Cryptography, World Scientific, Singapore, pp. 119–124 (2008)
5. Ding, C.: Linear codes from some 2-designs. IEEE Trans. Inf. Theory **61**(6), 3265–3275 (2015)
6. Ding, C.: A construction of binary linear codes from Boolean functions. Discrete Math. **339**(9), 2288–2303 (2016)
7. Ding, K., Ding, C.: Binary linear codes with three weights. IEEE Commun. Lett. **18**, 1879–1882 (2014)
8. 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)
9. Faldum, A., Willems, W.: A characterization of MMD codes. IEEE Trans. Inf. Theory **44**(4), 1555–1558 (1998)
10. Klapper, A.: Cross-correlations of quadratic form sequences in odd characteristic. Des. Codes Cryptogr. **3**, 289–305 (1997)
11. Dembowski, P., Ostrom, T.G.: Planes of order n with collineation groups of order n^2. Math. Zeitschrift **193**(3), 239–258 (1968)
12. Draper, S., Hou, X.: Explicit evalution of certain exponential sums of quadratic functions over $\mathbb{F}_{p^m}$, p odd. arXiv:0708.3619
13. Games, R.A.: The geometry of quadrics and correlations of sequences. IEEE Trans. Inf. Theory **32**(2), 423–426 (1986)
14. Heng, Z., Yue, Q.: A class of binary linear codes with at most three weights. IEEE Commun. Lett. **19**, 1488–1491 (2015)
15. Heng, Z., Yue, Q., Li, C.: Three classes of linear codes with two or three weights. Discrete Math. **339**, 2832–2847 (2016)
16. Heng, Z., Yue, Q.: Evaluation of the Hamming weights of a classes of linear codes based on Gauss sums. Des. Codes Cryptogr. **83**(2), 307–326 (2017)
17. Kløve, T.: Codes for Error Detection. World Scientific, Hackensack (2007)
18. Lidl, R., Niederreiter, H.: Finite Fields, Encyclopedia of Mathematics, vol. 20. Cambridge University Press, Cambridge (1983)
19. Li, F., Wang, Q., Lin, D.: A class of three-weight and five-weight linear codes. Discrete Appl Math **241**(31), 25–38 (2018)
20. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error Correcting Codes. Elsevier, Amsterdam (1977)
21. Wang, Q., Ding, K., Xue, R.: Binary linear codes with two weight. IEEE Commun. Lett. **19**, 1097–1100 (2015)

22. Xia, Y., Li, C.: Three-weight ternary linear codes from a family of power functions. Finite Fields Appl. **46**, 17–37 (2017)
23. Xiang, C.: Linear codes from a generic construction. Cryptogr. Commun. **8**, 525–539 (2016)
24. Yuan, J., Carlet, C., Ding, C.: The weight distribution of a class of linear codes from perfect nonlinear functions. IEEE Trans. Inf. Theory **52**(2), 712–717 (2006)
25. Zeng, X., Hu, L., Jiang, W., Yue, Q., Cao, X.: The weight distribution of a class of p-ary cyclic codes. Finite Fields Appl. **16**, 56–73 (2010)
26. Zhang, D., Fan, C., Peng, D., Tang, X.: Complete weight enumerators of some linear codes from quadratic forms. Cryptogr. Commun. **9**, 151–163 (2017)
27. Zheng, D., Bao, J.: Four classes of linear codes from cyclotomic cosets. Des. Codes Cryptogr. **86**, 1007–1022 (2018)
28. Zhou, Z., Li, N., Fan, C., Helleseth, T.: Linear codes with two or three weight from quafratic bent functions. Des. Codes Cryptogr. **81**(2), 283–295 (2016)
29. Zhou, Z., Ding, C.: Seven classes of three-weight cyclic codes. IEEE Trans. Commun. **61**(10), 4120–4126 (2013)
30. Zhou, Z., Ding, C.: A class of three-weight cyclic codes. Finite Fields Appl. **25**, 79–93 (2014)