AAECC (2017) 28:535–547
DOI 10.1007/s00200-017-0319-x

ORIGINAL PAPER

Linear codes from quadratic forms

Xiaoni Du[1] · **Yunqi Wan**[1]

Received: 17 July 2016 / Revised: 16 March 2017 / Accepted: 27 April 2017 /
Published online: 15 May 2017

Abstract Linear codes have been an interesting topic in both theory and practice for many years. In this paper, for an odd prime power q, we present a class of linear codes over finite fields F_q with quadratic forms via a general construction and then determine the explicit complete weight enumerators of these linear codes. Our construction covers some related ones via quadratic form functions and the linear codes may have applications in cryptography and secret sharing schemes.

Keywords Linear code · Weight distribution · Complete weight enumerators · Quadratic form function · Minimal codeword

Mathematics Subject Classification 94B05 · 94A62 · 11E04

1 Introduction

Let p be an odd prime, $m(>1)$, e be positive integers and $q = p^e$. An $[n, k, d]$ linear code $\mathcal{C}$ over the finite field F_q is a k-dimensional subspace of F_q^n with minimum (Hamming) distance d, which determines the error correcting capability of $\mathcal{C}$. Let A_i

X. Du was partially supported by the National Natural Science Foundation of China (Grant Nos. 61462077 and 61662071), the Natural Science Foundation of Shanghai (No. 16ZR1411200) and Anhui Provincial Natural Science Foundation (No. 1608085MF143).

✉ Yunqi Wan
yunqi211@163.com

Xiaoni Du
ymLdxn@126.com

[1] College of Mathematics and Statistics, Northwest Normal University, Lanzhou 730070, Gansu, People's Republic of China

denote the number of codewords with Hamming weight i in a code $\mathcal{C}$ of length n. The weight enumerator of $\mathcal{C}$ is defined by

$$1 + A_1 z + A_2 z^2 + \ldots + A_n z^n.$$

The sequence $(1, A_1, A_2, \ldots, A_n)$ is called the weight distribution of $\mathcal{C}$. The code $\mathcal{C}$ is said to be t-weight if the number of nonzero A_j $(1 \leq j \leq n)$ in the sequence $(A_1, A_2, \ldots, A_n)$ equals t.

The complete weight enumerator of a code $\mathcal{C}$ over F_q enumerates the codewords according to the number of symbols of each kind contained in each codeword. Let $F_q = \{\omega_0, \omega_1, \cdots, \omega_{q-1}\}$ with $\omega_0 = 0$ and $F_q^* = F_q \backslash \{0\}$. For a codeword $\mathbf{c} = (c_0, c_1, \cdots, c_{n-1}) \in F_q^n$, the complete weight enumerator $\omega[\mathbf{c}]$ of $\mathbf{c}$ is defined by

$$\omega[\mathbf{c}] = \omega_0^{k_0} \omega_1^{k_1} \cdots \omega_{q-1}^{k_{q-1}},$$

where $\sum_{j=0}^{q-1} k_j = n, k_j$ is the number of components of $\mathbf{c}$ that equals ω_j. The complete weight enumerator of the code $\mathcal{C}$ is then defined by

$$CWE(\mathcal{C}) = \sum_{\mathbf{c} \in \mathcal{C}} \omega[\mathbf{c}].$$

The weight distribution gives the minimum distance of the code, and hence the error correcting capability. Furthermore, the weight distribution of a code allows the computation of the probability of error detection and correction (see [22] for details). Thus the study of the weight distribution attracts much attention in coding theory and much work is focused on the determination of the weight distributions of linear codes (see [9,10,12,14,16,26,27,32–34] and the references therein). Linear codes can be applied in consumer electronics, communication and data storage system. Linear codes with a few weights are of importance in secret sharing [6,28], authentication codes [13], association schemes [4] and strongly regular graphs [5].

It is easy to see that the complete weight enumerators of binary linear codes are just their weight enumerators, while for the nonbinary case, the weight enumerators can be obtained from their complete weight enumerators. Furthermore, the complete weight enumerators are closely related to the deception probabilities of certain authentication codes constructed from linear codes [11], and used to compute the Walsh transform of monomial functions over finite fields [17]. Thus, a great deal of research [3,7,8,15, 19,23,24,29,30] is devoted to the computation of the complete weight enumerators of specific codes over F_q.

Let $D = \{d_1, d_2, \ldots, d_n\} \subseteq F_{q^m}$. A linear code of length n over F_q is defined by

$$\mathcal{C}_D = \{(Tr_1^m(xd_1), Tr_1^m(xd_2), \ldots, Tr_1^m(xd_n)) : x \in F_{q^m}\}$$

where Tr_1^m is the trace function from F_{q^m} to F_q. The set D is called the defining set of $\mathcal{C}_D$. This construction method was used for obtaining linear codes with a few weights [10,34]. The selection of D directly affects the parameters of the constructed linear

code $\mathcal{C}_D$. How to choose the defining set D for obtaining a good linear code $\mathcal{C}_D$ is an interesting and important problem.

Let $Q(x)$ be a quadratic form function from F_{q^m} to F_q. Very recently, for $e = 1$ and $Q(x)$ being a quadratic form function of full rank (quadratic Bent function), Zhou et al. constructed some classes of linear codes over F_p with defining set $D = \{x \in F_{q^m}^* : Q(x) = 0\}$ and examined their weight distribution [34]. Later, Zhang et al. extended Zhou et al.'s construction to F_q for general quadratic form function $Q(x)$ and examined the complete weight enumerators of the codes [31]. In this paper, for the case of clarity, we will denote the defining set D by $D_Q^a = \{x \in F_{q^m}^* : Q(x) = a\}$ for any $a \in F_q$. Firstly, we construct a class of linear codes over F_q with defining set D_Q^a. Then we examine their complete weight enumerators and discuss their application in secret sharing schemes.

2 Quadratic form functions

Identifying F_{q^m} with the m-dimensional F_q-vector space F_q^m, a function $Q(x)$ from F_{q^m} to F_q can be regarded as an m-variable polynomial over F_q. The former is called a quadratic form over F_q if the latter is a homogeneous polynomial of degree two in the form

$$Q(x_1, x_2, \ldots, x_m) = \sum_{1 \le i \le j \le m} a_{ij} x_i x_j,$$

where $a_{ij} \in F_q$. Any choice of a basis $\{\beta_1, \beta_2, \ldots, \beta_m\}$ from F_{q^m} as a vector space over F_q determines an identification $F_q^m \to F_{q^m}$ by $\bar{x} = (x_1, x_2, \ldots, x_m) \mapsto \sum_{i=1}^m x_i \beta_i = x$. We write $\bar{x}$ when an element is to be viewed as a vector in F_q^m, and we write x when the same vector is to be viewed as an element of F_{q^m}. The rank of the quadratic form $Q(x)$ is defined as the codimension of the F_q -vector space

$$V = \{y \in F_{q^m} : Q(x + y) - Q(x) - Q(y) = 0 \text{ for all } x \in F_{q^m}\}.$$

That is $|V| = q^{m-r}$ where r is the rank of $Q(x)$.

In the sequel, we shall give some lemmas that are essential in proving our main results. Before doing this, we first fix some notation.

* $B_{2j}(\bar{x}) = x_1 x_2 + x_3 x_4 + \ldots + x_{2j-1} x_{2j}$ where j is an integer with $0 \le 2j \le m$ (we assume that $B_0 = 0$ when $j = 0$).
* $I(x)$ is a function over F_q defined by $I(x) = -1$ for any $x \in F_q^*$ and $I(0) = q - 1$.
* $\eta(x)$ is the quadratic character of F_q with $\eta(0) = 0$.

Quadratic forms have been well studied (see [20,21,25], for example). Here we follow the treatment in [20] and [21]. It should be noted that the rank of a quadratic form over F_q is the smallest number of variables required to represent the quadratic form, up to nonsingular coordinate transformations. Mathematically, any quadratic form of rank r can be transferred to three canonical forms described in Table 1.

Table 1 Standard types of quadratic form over F_q with rank r and m variables

Type of quadratic form	Parity of r	N_a
I: $B_r(\bar{x})$	Even	$q^{m-1} + I(a)q^{m-\frac{r}{2}-1}$
II: $B_{r-1}(\bar{x}) + \mu x_r^2$	Odd	$q^{m-1} + \eta(\mu a)q^{m-\frac{r+1}{2}}$
III: $B_{r-2}(\bar{x}) + x_{r-1}^2 - \gamma\mu x_r^2$	Even	$q^{m-1} - I(a)q^{m-\frac{r}{2}-1}$

Lemma 1 ([21]) *Let $Q(x)$ be a quadratic form over F_q of rank r in m variables. Under a nonsingular change of coordinates, $Q(x)$ is equivalent to one of the three standard types in Table 1:*
where $\mu \in \{1, \gamma\}$ and γ is a fixed nonsquare in F_q and we denote N_a by

$$N_a = |\{\bar{x} \in F_q^m : \ Q(\bar{x}) = a\}| \quad \text{for all } a \in F_q.$$

Consider a system of equations consisting of a quadratic form and a linear function. The number of solutions depends on the type and rank of the quadratic form. Let $Q(\bar{x})$ be a quadratic form of rank r in m variables in one of the three standard types. Let $L_{\bar{b}}(\bar{x}) = \bar{b}\bar{x}^T = \sum_{i=1}^m b_i x_i$ be a linear function in m variables with $\bar{b} = (b_1, b_2, \ldots, b_m) \in F_q^m \backslash \{\bar{0}\}$, where $\bar{0} = (0, 0, \ldots, 0)$ denotes the all zero vector. For any $a, \ v \in F_q$, we denote by $N(a, v)$ the number of solutions to the system of equations

$$\begin{cases} Q(\bar{x}) = a, \\ L_{\bar{b}}(\bar{x}) = v. \end{cases}$$

The following lemmas will be used to determine the complete weight enumerators of linear codes constructed from general quadratic forms over F_q. Before introducing them, we give some notations for the standard quadratic form $Q(\bar{x})$ defined above. For any vector $\bar{x} = (x_1, x_2, \ldots, x_m)$, denote $\bar{x}' = (x_1, x_2, \ldots, x_r)$ and $\bar{x}'' = (x_{r+1}, x_{r+2}, \ldots, x_m)$, where r is the rank of $Q(\bar{x})$. Thus $Q(\bar{x}) = Q(\bar{x}')$. Let

$$\hat{Q}(\bar{x}) = \begin{cases} Q(\bar{x}), & \text{if } Q(\bar{x}) = B_r(\bar{x}), \\ B_{r-1}(\bar{x}) + \frac{x_r^2}{4\mu}, & \text{if } Q(\bar{x}) = B_{r-1}(\bar{x}) + \mu x_r^2, \\ B_{r-2}(\bar{x}) + \frac{x_{r-1}^2}{4} - \frac{x_r^2}{4\gamma}, & \text{if } Q(\bar{x}) = B_{r-1}(\bar{x}) + x_{r-1}^2 - \gamma x_r^2, \end{cases}$$

where $\mu \in \{1, \gamma\}$ and γ is a fixed nonsquare in F_q. Note that $\hat{Q}(\bar{x})$ is equivalent to $Q(\bar{x})$ under a change of coordinates.

Lemma 2 ([21]) *Let $Q(\bar{x})$ be a quadratic form over F_q of rank r in m variables. Let the notation be the same as before and $\bar{b}'' = 0$.*

(1) When Q is of Type I or Type III,

$$N(a,v)=\begin{cases} q^{m-2}+\epsilon I(a)q^{m-\frac{r}{2}-1}, & \text{if } Q(\bar{b})=0 \text{ and } v=0,\\ q^{m-2}, & \text{if } Q(\bar{b})=0 \text{ and } v\neq 0,\\ q^{m-2}+\epsilon\eta\Big(v^2-4a\hat{Q}(\bar{b})\Big)q^{m-\frac{r}{2}-1}, & \text{if } Q(\bar{b})\neq 0. \end{cases}$$

(2) When Q is of Type II,

$$N(a,v)=\begin{cases} q^{m-2}+\eta(\mu a)q^{m-\frac{r+1}{2}}, & \text{if } Q(\bar{b})=0 \text{ and } v=0,\\ q^{m-2}, & \text{if } Q(\bar{b})=0 \text{ and } v\neq 0,\\ q^{m-2}+I\Big(v^2-4a\hat{Q}(\bar{b})\Big)\eta\Big(\mu\hat{Q}(\bar{b})\Big)q^{m-\frac{r+3}{2}}, & \text{if } Q(\bar{b})\neq 0, \end{cases}$$

where $\epsilon=1$ if $Q(x)$ is equivalent to Type I and $\epsilon=-1$ if $Q(x)$ is equivalent to Type III.

Lemma 3 ([21]) *Let $Q(\bar{x})$ be a quadratic form over F_q of rank r in m variables. Let the notation be the same as before and $\bar{b}''\neq 0$.*

(1) When Q is of Type I or Type III,

$$N(a,v)=q^{m-2}+\epsilon I(a)q^{m-\frac{r}{2}-2}.$$

(2) When Q is of Type II,

$$N(a,v)=q^{m-2}+\eta(\mu a)q^{m-\frac{r+3}{2}}.$$

3 Linear codes from quadratic forms

In this paper, for any $a\in F_q$, the defining set is defined by

$$D_Q^a=\{x\in F_{q^m}: Q(x)=a\}=\{d_1,d_2,\ldots,d_n\}. \tag{1}$$

A linear code of length n over F_q is defined by

$$\mathcal{C}_{D_Q^a}=\{(Tr(xd_1),Tr(xd_2),\ldots,Tr(xd_n)): x\in F_{q^m}\}. \tag{2}$$

Note that for the case of $a=0$, the weight distribution of the linear codes has been discussed in [34] for $Q(x)$ over F_p with $r=m$ and later in [31] for general quadratic form $Q(x)$ over F_q. Thus we consider the complete weight enumerator of the linear code $\mathcal{C}_{D_Q^a}$ only for $a\in F_q^*$.

Theorem 1 *Let g be a generator of F_q^*. If r is even, then the code $\mathcal{C}_{D_Q^a}$ is a $[q^{m-1}-\epsilon q^{m-\frac{r}{2}-1},m]$ linear code with the weight distribution given in Table 2 and its complete weight enumerator is*

Table 2 Weight distribution of the codes $\mathcal{C}_{D_Q^a}$ with r even

Weight	Multiplicity
0	1
$(q-1)(q^{m-2}-\epsilon q^{m-\frac{r}{2}-2})$	q^m-q^r
$q^{m-1}-q^{m-2}$	$\frac{q+1}{2}q^{r-1}+\epsilon\frac{q-1}{2}q^{\frac{r}{2}-1}-1$
$q^{m-1}-q^{m-2}-2\epsilon q^{m-\frac{r}{2}-1}$	$\frac{q-1}{2}(q^{r-1}-\epsilon q^{\frac{r}{2}-1})$

$$
\begin{aligned}
CWE(\mathcal{C}_{D_Q^a}) &= \omega_0^{q^{m-1}-\epsilon q^{m-\frac{r}{2}-1}} + (q^m-q^r)\prod_{\rho=0}^{q-1}\omega_\rho^{q^{m-2}-\epsilon q^{m-\frac{r}{2}-2}} \\
&+ \left(q^{r-1}+\epsilon(q-1)q^{\frac{r}{2}-1}-1\right)\omega_0^{q^{m-2}-\epsilon q^{m-\frac{r}{2}-1}}\prod_{\rho=1}^{q-1}\omega_\rho^{q^{m-2}} \\
&+ (q^{r-1}-\epsilon q^{\frac{r}{2}-1})\sum_{\beta=1}^{\frac{q-1}{2}}\omega_0^{q^{m-2}+(\frac{-1}{q})\epsilon q^{m-\frac{r}{2}-1}}\omega_{2g^\beta}^{q^{m-2}}\omega_{q-2g^\beta}^{q^{m-2}} \\
&\cdot \prod_{\rho\neq 0,\pm 2g^\beta}\omega_\rho^{q^{m-2}+(\frac{\rho^2-4g^{2\beta}}{q})\epsilon q^{m-\frac{r}{2}-1}} \\
&+ (q^{r-1}-\epsilon q^{\frac{r}{2}-1})\sum_{\beta=1}^{\frac{q-1}{2}}\omega_0^{q^{m-2}-(\frac{-1}{q})\epsilon q^{m-\frac{r}{2}-1}}\prod_{\rho=1}^{q-1}\omega_\rho^{q^{m-2}+(\frac{\rho^2-4g^{2\beta+1}}{q})\epsilon q^{m-\frac{r}{2}-1}}.
\end{aligned}
$$

Proof By Lemma 1, it is obvious that the code $\mathcal{C}_{D_Q^a}$ has length $n = N_a = q^{m-1} - \epsilon q^{m-\frac{r}{2}-1}$ and dimension m. For any codeword $\mathbf{c}_b$ in $\mathcal{C}_{D_Q^a}$, according to the definition, the Hamming weight is equal to

$$WT(\mathbf{c}_b) = N_a - N(a,0).$$

Then, the weight distribution of $\mathcal{C}_{D_Q^a}$ follows from Lemmas 1, 2 and 3.

To obtain the complete weight enumerator of $C_{D_Q^a}$, we need to determine the value distribution of $\mathcal{N}_b(a,v)$ for each $v \in F_q$ when b runs through all the elements in F_{q^m}. Let $\{\alpha_1,\alpha_2,\ldots,\alpha_m\}$ and $\{\beta_1,\beta_2,\ldots,\beta_m\}$ be the dual basis of F_{q^m} over F_q. Using the dual bases, we write $x = x_1\beta_1+x_2\beta_2+\ldots+x_m\beta_m$ and $b = b_1\alpha_1+b_2\alpha_2+\ldots+b_m\alpha_m$ for $x,\ b \in F_{q^m}$ and we write corresponding vectors as $\bar{x} = (x_1,x_2,\ldots,x_m) \in F_q^m$ and $\bar{b} = (b_1,b_2,\ldots,b_m) \in F_q^m$. So, the linear function $Tr_1^m(bx) = v$ is equivalent to $L_{\bar{b}}(\bar{x}) = v$. Let $\mathcal{N}_b(a,v)$ be equal to the number of solutions $\bar{x} \in F_q^m\backslash\{\bar{0}\}$ of the following system of equations:

$$\begin{cases} \hat{Q}(\bar{x}) = a, \\ L_{\bar{b}}(\bar{x}) = v, \end{cases}$$

Table 3 Weight distribution of the codes $\mathcal{C}_{D_Q^a}$ with r odd

Weight	Multiplicity
0	1
$(q-1)\left(q^{m-2}+\eta(\mu a)q^{m-\frac{r+3}{2}}\right)$	$q^m-q^r+\frac{q-1}{2}\left(q^{r-1}-\eta(\mu a)q^{\frac{r-1}{2}}\right)$
$q^{m-1}-q^{m-2}$	$q^{r-1}-1$
$q^{m-2}(q-1)+\eta(\mu a)(q+1)q^{m-\frac{r+3}{2}}$	$\frac{q-1}{2}\left(q^{r-1}+\eta(\mu a)q^{\frac{r-1}{2}}\right)$

Table 4 Weight distribution of the codes $\mathcal{C}_{D_Q^a}$ with $r=\eta(\mu a)=1$

Weight	Multiplicity
0	1
$2q^{m-2}(q-1)$	q^m-q
$2q^{m-1}$	$q-1$

after nonsigular transformation for the quadratic form $Q(x)$ (for simplicity, we still use symbol $\bar{x}$).

Observe that $b=0$ gives the zero codeword and the contribution to the complete weight enumerator is ω_0^n, so below we assume that $b\in F_q^*$. Note that $\bar{b}$ runs through all the elements in $F_q^m\backslash\{\bar{0}\}$ if and only if b runs though all the elements in $F_{q^m}^*$.

Note that g is a generator of F_q^*, i.e., each element of F_q^* can be represented by g^β for some $1\le\beta\le q-1$. When β runs over all the elements of the set $\{1,2,\ldots,\frac{q-1}{2}\}$, $g^{2\beta}$ and $g^{2\beta+1}$ will run over all the quadratic residues and quadratic nonresidues of F_q^*, respectively.

The desired conclusions then follow from Lemmas 2 and 3. □

Theorem 2 *Let g be a generator of F_q^*. If r is odd, then the code $\mathcal{C}_{D_Q^a}$ is a $[q^{m-1}+\eta(\mu a)q^{m-\frac{r+1}{2}},m]$ linear code with the weight distribution given in Table 3 and its complete weight enumerator is*

$$
\begin{aligned}
CWE(\mathcal{C}_{D_Q^a}) &= \omega_0^{q^{m-1}+\eta(\mu a)q^{m-\frac{r+1}{2}}}+(q^m-q^r)\prod_{\rho=0}^{q-1}\omega_\rho^{q^{m-2}+\eta(\mu a)q^{m-\frac{r+3}{2}}}\\
&+(q^{r-1}-1)\omega_0^{q^{m-2}+\eta(\mu a)q^{m-\frac{r+1}{2}}}\prod_{\rho=1}^{q-1}\omega_\rho^{q^{m-2}}\\
&+\left(q^{r-1}+\eta(\mu a)q^{\frac{r-1}{2}}\right)\sum_{\beta=1}^{\frac{q-1}{2}}\omega_0^{q^{m-2}-\eta(\mu a)q^{m-\frac{r+3}{2}}}\omega_{2g^\beta}^{q^{m-2}+(q-1)\eta(\mu a)q^{m-\frac{r+3}{2}}}
\end{aligned}
$$

Table 5 Weight distribution of the codes $\mathcal{C}_{D_Q^a}$ with full rank m even

Weight	Multiplicity
0	1
$q^{m-1}-q^{m-2}$	$\frac{q+1}{2}q^{m-1}+\epsilon\frac{q-1}{2}q^{\frac{m}{2}-1}-1$
$q^{m-1}-q^{m-2}-2\epsilon q^{\frac{m}{2}-1}$	$\frac{q-1}{2}(q^{m-1}-\epsilon q^{\frac{m}{2}-1})$

$$\cdot\,\omega_{q-2g^\beta}^{q^{m-2}+(q-1)\eta(\mu a)q^{m-\frac{r+3}{2}}}\prod_{\rho\neq 0,\pm 2g^\beta}\omega_\rho^{q^{m-2}-\eta(\mu a)q^{m-\frac{r+3}{2}}}$$
$$+\frac{q-1}{2}\Big(q^{r-1}-\eta(\mu a)q^{\frac{r-1}{2}}\Big)\prod_{\rho=0}^{q-1}\omega_\rho^{q^{m-2}+\eta(\mu a)q^{m-\frac{r+3}{2}}}.$$

The proof is very similar to that of Theorem 1, so we omitted it here.

Remark As a special case of Theorem 2, if $Q(x)$ is a quadratic form of rank $r=1$, then the code $\mathcal{C}_{D_Q^a}$ does not exist since the length of $\mathcal{C}_{D_Q^a}$ equals zero when $\eta(\mu a)=-1$. While for the case of $\eta(\mu a)=1$, we have that $\mathcal{C}_{D_Q^a}$ is a $[2q^{m-1},m]$ linear code with the weight distribution given in Table 4 and its complete weight enumerator is

$$CWE(\mathcal{C}_{D_Q^a})=\omega_0^{2q^{m-1}}+(q^m-q)\prod_{\rho=0}^{q-1}\omega_\rho^{2q^{m-2}}+2\sum_{\beta=1}^{\frac{q-1}{2}}\omega_{2g^\beta}^{q^{m-1}}\omega_{q-2g^\beta}^{q^{m-1}}.$$

For the quadratic form $Q(x)$ over F_q with full rank $r=m$, we have following two corollaries corresponding to Theorems 1 and 2, respectively.

Corollary 1 *Let $Q(x)$ be a quadratic form of full rank from F_{q^m} to F_q. If m is even, then $\mathcal{C}_{D_Q^a}$ is a two-weight $[q^{m-1}-\epsilon q^{\frac{m}{2}-1},m]$ code over F_q with the weight distribution given in Table 5 and its complete weight enumerator is*

$$\begin{aligned}&CWE(\mathcal{C}_{D_Q^a})\\&=\omega_0^{q^{m-1}-\epsilon q^{\frac{m}{2}-1}}+\Big(q^{m-1}+\epsilon(q-1)q^{\frac{m}{2}-1}-1\Big)\omega_0^{q^{m-2}-\epsilon q^{\frac{m}{2}-1}}\prod_{\rho=1}^{q-1}\omega_\rho^{q^{m-2}}\\&+(q^{m-1}-\epsilon q^{\frac{m}{2}-1})\sum_{\beta=1}^{\frac{q-1}{2}}\omega_0^{q^{m-2}+(\frac{-1}{q})\epsilon q^{\frac{m}{2}-1}}\omega_{2g^\beta}^{q^{m-2}}\omega_{q-2g^\beta}^{q^{m-2}}\\&\cdot\prod_{\rho\neq 0,\pm 2g^\beta}\omega_\rho^{q^{m-2}+(\frac{\rho^2-4g^{2\beta}}{q})\epsilon q^{\frac{m}{2}-1}}\\&+(q^{m-1}-\epsilon q^{\frac{m}{2}-1})\sum_{\beta=1}^{\frac{q-1}{2}}\omega_0^{q^{m-2}-(\frac{-1}{q})\epsilon q^{\frac{m}{2}-1}}\prod_{\rho=1}^{q-1}\omega_\rho^{q^{m-2}+(\frac{\rho^2-4g^{2\beta+1}}{q})\epsilon q^{\frac{m}{2}-1}}.\end{aligned}$$

Table 6 Weight distribution of the codes $\mathcal{C}_{D_Q^a}$ with full rank m odd

Weight	Multiplicity
0	1
$q^{m-1}-q^{m-2}$	$q^{m-1}-1$
$q^{m-2}(q-1)+\eta(\mu a)(q+1)q^{\frac{m-3}{2}}$	$\frac{q-1}{2}\left(q^{m-1}+\eta(\mu a)q^{\frac{m-1}{2}}\right)$
$(q-1)\left(q^{m-2}+\eta(\mu a)q^{\frac{m-3}{2}}\right)$	$\frac{q-1}{2}\left(q^{m-1}-\eta(\mu a)q^{\frac{m-1}{2}}\right)$

Corollary 2 *Let $Q(x)$ be a quadratic form of full rank from F_{q^m} to F_q. If m is odd, then $\mathcal{C}_{D_Q^a}$ is a three-weight $[q^{m-1}+\eta(\mu a)q^{\frac{m-1}{2}}, m]$ code over F_q with the weight distribution given in Table 6 and its complete weight enumerator is*

$$\begin{aligned}CWE(\mathcal{C}_{D_Q^a}) &= \omega_0^{q^{m-1}+\eta(\mu a)q^{\frac{m-1}{2}}} + (q^{m-1}-1)\omega_0^{q^{m-2}+\eta(\mu a)q^{\frac{m-1}{2}}}\prod_{\rho=1}^{q-1}\omega_\rho^{q^{m-2}}\\ &+\left(q^{m-1}+\eta(\mu a)q^{\frac{m-1}{2}}\right)\sum_{\beta=1}^{\frac{q-1}{2}}\omega_0^{q^{m-2}-\eta(\mu a)q^{\frac{m-3}{2}}}\omega_{2g^\beta}^{q^{m-2}+(q-1)\eta(\mu a)q^{\frac{m-3}{2}}}\\ &\cdot\omega_{q-2g^\beta}^{q^{m-2}+(q-1)\eta(\mu a)q^{\frac{m-3}{2}}}\prod_{\rho\neq 0,\pm 2g^\beta}\omega_\rho^{q^{m-2}-\eta(\mu a)q^{\frac{m-3}{2}}}\\ &+\frac{q-1}{2}\left(q^{m-1}-\eta(\mu a)q^{\frac{m-1}{2}}\right)\prod_{\rho=0}^{q-1}\omega_\rho^{q^{m-2}+\eta(\mu a)q^{\frac{m-3}{2}}}.\end{aligned}$$

We conclude this section by providing some examples as an indication of the validity of our results.

Example 1 Let $q=p=3$, $m=6$, $a=1$, and $Q(x)=Tr_{q^6/q}(2x^4+x^2)$, which is a Type I quadratic form with rank 4. Our Magma program shows that $\mathcal{C}_{D_Q^a}$ has parameters [216, 6, 108] and the complete weight enumerator

$$\omega_0^{216}+24\omega_0^{108}\omega_1^{54}\omega_2^{54}+648\omega_0^{72}\omega_1^{72}\omega_2^{72}+56\omega_0^{54}\omega_1^{81}\omega_2^{81}.$$

This agrees with the conclusion of Theorem 1.

Example 2 Let $q=p=3$, $m=5$, $a=1$, and $Q(x)=Tr_{q^5/q}(2x^{10}+x^2)$, which is a Type III quadratic form with rank 4. Our Magma program shows that $\mathcal{C}_{D_Q^a}$ has parameters [90, 5, 54] and the complete weight enumerator

$$\omega_0^{90}+50\omega_0^{36}\omega_1^{27}\omega_2^{27}+162\omega_0^{30}\omega_1^{30}\omega_2^{30}+30\omega_0^{18}\omega_1^{36}\omega_2^{36}.$$

This is consistent with the statement of Theorem 1.

Example 3 Let $q = p = 3$, $m = 3$, $a = 1$, and $Q(x) = Tr_{q^3/q}(2x^4 + x^2)$, which is a Type II quadratic form with rank 1 and $\eta(\mu) = 1$, the Magma program shows that $\mathcal{C}_{D_Q^a}$ has parameters [18, 3, 12] and the complete weight enumerator

$$\omega_0^{18} + 24\omega_0^6\omega_1^6\omega_2^6 + 2\omega_1^9\omega_2^9.$$

This agrees with the conclusion of Theorem 2.

Example 4 Let $p = 3$, $e = 2$, $q = 9$, $m = 4$, $a \in \{1, 2, 4, 5, 7, 8\}$, and $Q(x) = Tr_{q^4/q}(x^{q^2+1})$ be a Type III quadratic form with full rank. The Magma program shows that $\mathcal{C}_{D_Q^a}$ has parameters [738, 4, 648] and the weight enumerator

$$1 + 3608z^{648} + 2952z^{666}.$$

The complete weight enumerator is very cumbersome, limited by the length of the space is no longer listed. This agrees with the conclusion of Corollary 1.

4 Optimal codes

An $[n, k, d]$ code over F_q is called optimal if there is no $[n, k, d + 1]$ or $[n, k + 1, d]$ code over F_q. An $[n, k, d]$ code over F_q is called almost optimal if the $[n, k, d + 1]$ or $[n, k + 1, d]$ code is optimal [18]. Below, we prove that some of the codes in the paper are optimal or almost optimal with respect to the Griesmer bound.

Lemma 4 *[18] (Griesmer Bound) Let $\mathcal{C}$ be an $[n, k, d]$ code over F_q with $k \geq 1$. Then*

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil.$$

Theorem 3 *Let the notation be the same as before. Then we have*

(1) If $Q(x)$ is a Type II quadratic form with rank $r = \eta(\mu a) = 1$, $\mathcal{C}_{D_Q^a}$ is optimal.
(2) If $Q(x)$ is a Type III quadratic form with rank $r = m = 2$, $\mathcal{C}_{D_Q^a}$ is almost optimal.
(3) For the other cases, the gap between the length of codes and the Griesmer bound increases together with the dimension.

Proof (1) If $Q(x)$ be a Type II quadratic form with $r = \eta(\mu a) = 1$, then $\mathcal{C}_{D_Q^a}$ has parameters $[2q^{m-1}, m, 2q^{m-2}(q-1)]$. So it follows from Lemma 4 that

$$\begin{aligned} n - \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil &= 2q^{m-1} - \left\lceil 2q^{m-2}(q-1) \right\rceil - \ldots - \lceil 2(q-1) \rceil - \left\lceil 2(1 - \frac{1}{q}) \right\rceil \\ &= 2q^{m-1} - (2q^{m-2}(q-1)) - \ldots - (2(q-1)) - 2 \\ &= 0. \end{aligned}$$

This completes the proof of (1).

(2) The proof is very similar to that of (1), so we omit it here.
(3) We only prove the case that $Q(x)$ be a Type II quadratic form with $\eta(\mu a) = 1$ and $r \neq 1$, since the other cases can be proved with the similar idea. Theorem 2 means that the code $\mathcal{C}_{D_Q^a}$ has parameters $[q^{m-1} + q^{m-\frac{r+1}{2}}, m, q^{m-1} - q^{m-2}]$. Then it follows from Lemma 4 that

$$\begin{aligned} n - \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil &= q^{m-1} + q^{m-\frac{r+1}{2}} - \left\lceil q^{m-1} - q^{m-2} \right\rceil \\ &\quad - \ldots - \lceil q - 1 \rceil - \left\lceil 1 - \frac{1}{q} \right\rceil \\ &= q^{m-1} + q^{m-\frac{r+1}{2}} - (q^{m-1} - q^{m-2}) - \ldots - (q-1) - 1 \\ &= q^{m-\frac{r+1}{2}}. \end{aligned}$$

This completes the proof of (3). □

5 Minimal codewords in $\mathcal{C}_{D_Q^a}$

The support of a vector $\mathbf{c} = (c_0, \ldots, c_{n-1}) \in F_q^n$ is defined as

$$\{0 \leq i \leq n-1 : c_i \neq 0\}.$$

We say that a vector $\mathbf{x}$ covers a vector $\mathbf{y}$ if the support of $\mathbf{x}$ contains that of $\mathbf{y}$ as a proper subset.

A minimal codeword of a linear code $\mathcal{C}$ is a nonzero codeword that does not cover any other nonzero codeword of $\mathcal{C}$. It is an interesting problem to construct codes whose nonzero codewords are all minimal since such linear codes can be employed to construct secret sharing schemes with interesting access structures [28]. For minimal codewords, we have following results [1,2]:

Lemma 5 *In an $[n, k, d]$ code $\mathcal{C}$, let w_{min} and w_{max} be the minimum and maximum nonzero weights, respectively. If*

$$\frac{w_{min}}{w_{max}} > \frac{q-1}{q},$$

then all nonzero codewords of $\mathcal{C}$ are minimal.

In this section, we will show that for most of quadratic forms $Q(x)$ and q and a, each of codewords of $\mathcal{C}_{D_Q^a}$ given by (2) is minimal.

If $Q(x)$ is equivalent to Type I, then for $\mathcal{C}_{D_Q^a}$ we have

$$\frac{w_{min}}{w_{max}} = \frac{q^{m-1} - q^{m-2} - 2q^{m-\frac{r}{2}-1}}{q^{m-1} - q^{m-2}} > \frac{q-1}{q}$$

if $r = 4$ and $q \geq 5$, or if $r \geq 6$. When $Q(x)$ is equivalent to Type III, we have

$$\frac{w_{min}}{w_{max}} = \frac{q^{m-1} - q^{m-2}}{q^{m-1} - q^{m-2} + 2q^{m-\frac{r}{2}-1}} > \frac{q-1}{q}$$

for all even $r \geq 4$.

Similarly, if $r \geq 5$ is odd, we have $\frac{w_{min}}{w_{max}} > \frac{q-1}{q}$.

By Lemma 5, for certain smaller r and if $m \geq r \geq 5$ for all odd prime power q, the linear codes $\mathcal{C}_{D_Q^a}$ we constructed satisfy the condition $\frac{w_{min}}{w_{max}} > \frac{q-1}{q}$, and can be employed to obtain secret sharing schemes with nice access structures. We omit the details here since it is similar to that of [10].

6 Conclusion

In this paper, we presented a family of linear codes with defining set D_Q^a, where $a \in F_q$ and $Q(x)$ is any quadratic form, and determined their complete weight enumerators. Our results are extensions of earlier related works and some of the code we derived are optimal or almost optimal codes. We also discussed the application of the linear codes in secret sharing.

Acknowledgements The authors acknowledge the patient referees for their valuable and constructive comments which helped to improve this work.

References

1. Ashikhmin, A., Barg, A.: Minimal vectors in linear codes. IEEE Trans. Inf. Theory **44**(5), 2010–2017 (1998)
2. Ashikhmin, A., Barg, A., Cohen, G., Huguet, L.: Variations on minimal codewords in linear codes. Appl. Algebra Algebraic Algorithms Error-Correcting Codes **948**, 96–105 (1995)
3. Blake, I.F., Kith, K.: On the complete weight enumerator of Reed–Solomon codes. SIAM J. Discrete Math. **4**(2), 164–171 (1991)
4. Calderbank, A.R., Goethals, J.M.: Three-weight codes and association schemes. Philips J. Res. **39**, 143–152 (1984)
5. Calderbank, A.R., Kantor, W.M.: The geometry of two-weight codes. Bull. Lond. Math. Soc. **18**, 97–122 (1986)
6. Carlet, C., Ding, C., Yuan, J.: Linear codes from perfect nonlinear mappings and their secret sharing schemes. IEEE Trans. Inf. Theory **51**, 2089–2102 (2005)
7. Chu, W., Colbourn, C.J., Dukes, P.: On constant composition codes. Discrete Appl. Math. **154**(6), 912–929 (2006)
8. Ding, C.: Optimal constant composition codes from zero-difference balanced functions. IEEE Trans. Inf. Theory **54**(12), 5766–5770 (2008)
9. Ding, C.: Linear codes from some 2-designs. IEEE Trans. Inf. Theory **61**, 3265–3275 (2015)
10. 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)
11. Ding, C., Helleseth, T., Klove, T., Wang, X.: A generic construction of Cartesian authentication codes. IEEE Trans. Inf. Theory **53**(6), 2229–2235 (2007)
12. Ding, C., Liu, Y., Ma, C., Zeng, L.: The weight distribution of the duals of cyclic codes with two zeros. IEEE Trans. Inf. Theory **57**(12), 8000–8006 (2011)
13. Ding, C., Wang, X.: A coding theory construction of new systematic authentication codes. Theor. Comput. Sci. **330**, 81–99 (2005)

14. Ding, C., Yang, J.: Hamming weights in irreducible cyclic codes. Discret Math. **313**(4), 434–446 (2013)
15. Ding, C., Yin, J.: A construction of optimal constant composition codes. Des. Codes Cryptogr. **40**(2), 157–165 (2006)
16. Feng, K., Luo, J.: Weight distribution of some reducible cyclic codes. Finite Fields Appl. **14**, 390–409 (2008)
17. Helleseth, T., Kholosha, A.: Monomial and quadratic bent functions over the finite field of odd characteristic. IEEE Trans. Inf. Theory **52**, 2018–2032 (2006)
18. Huffman, W.C., Pless, V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003)
19. Kith K.: Complete weight enumeration of Reed-Solomon codes, Masters thesis, Department of Electrical and Computing Engineering, University of Waterloo, Waterloo, Ontario, Canada (1989)
20. Klapper, A.: Cross-correlations of geometric sequences in characteristic two. Des. Codes Cryptogr. **3**(4), 347–377 (1993)
21. Klapper, A.: Cross-correlations of quadratic form sequences in odd characteristic. Des. Codes Cryptogr. **11**(3), 289–305 (1997)
22. Kløve, T.: Codes for Error Detection. World Scientific, Singapore (2007)
23. Kuzmin A., Nechaev A.: Complete weight enumerators of generalized Kerdock code and linear recursive codes over Galois ring. In: Workshop on Coding and Cryptography, pp. 333–336 (1999)
24. Li, C., Yue, Q., Fu, F.: Complete weight enumerators of some cyclic codes, Des. Codes Cryptogr. doi:10.1007/s10623-015-0091-5
25. Lidl, R., Niederreiter, H.: Finite Fields Encyclopedia of Mathematics 20. Cambridge University Press, Cambridge (1983)
26. Tang, C., Li, N., Qi, Y., Zhou, Z., Helleseth, T.: Two-weight and three-weight linear codes from weakly regular bent functions. IEEE Trans. Inf. Theory **62**(3), 1166–1176 (2016)
27. Xu, G., Cao, X.: Linear codes with two or three weights from some functions with low Walsh spectrum in odd characteristic. arXiv: 1510.01031 (2015)
28. Yuan, J., Ding, C.: Secret sharing schemes from three classes of linear codes. IEEE Trans. Inf. Theory **52**, 206–212 (2006)
29. Yang, S., Yao, Z.: Complete weight enumerators of some linear codes. arxiv: 1505.06326v1 (2015)
30. Yang, S., Yao, Z.: Complete weight enumerators of a family of three-weight linear codes. Des. Codes Cryptogr. doi:10.1007/s10623-016-0191-x
31. Zhang, D., Fan, C., Peng, D., Tang X.: Complete weight enumerators of some linear codes from quadratic forms. Cryptogr. Commun. doi:10.1007/s12095-016-0190-9
32. Zhou, Z., Ding, C.: Seven classes of three-weight cyclic codes. IEEE Trans. Commun. **61**(10), 4120–4126 (2013)
33. Zhou, Z., Ding, C.: A class of three-weight cyclic codes. Finite Field Appl. **25**, 79–93 (2014)
34. Zhou, Z., Li, N., Fan, C., Helleseth, T.: Linear codes with two or three weights from quadratic bent functions. Des. Codes Cryptogr. doi:10.1007/s10623-015-0144-9