VECTORIAL BENT FUNCTIONS AND LINEAR CODES FROM QUADRATIC FORMS

XIANHONG XIE[1], YI OUYANG[2,3] AND MING MAO[4]

Abstract. In this paper, we study the vectorial bentness of an arbitrary quadratic form and construct two classes of linear codes of ≤ 4 weights from the quadratic forms. Let q be a prime power, m be a positive integer and $Q : \mathbb{F}_{q^m} \to \mathbb{F}_q$ be a quadratic form. We first show that Q is a vectorial bent function if and only if Q is non-degenerate and $(q+1)m$ is even (i.e. either q is odd or m is even). Furthermore, if $2 \mid (q+1)m$ and $Q(x) = \sum\limits_{i=0}^{m-1} \mathrm{Tr}_{q^m/q}(a_i x^{q^i+1})$ ($a_i \neq 0$), we show that Q is vectorial bent if and only if the associated additive polynomial $L_Q(x) = \sum_i (a_i + a_{m-i}^{q^i}) x^{q^i}$ is a permutation polynomial over $\mathbb{F}_{q^m}$. If only one $a_i \neq 0$, we recover the constructions of Sidelnikov, Dembowski-Ostrom and Kasami of quadratic vectorial bent functions. We then construct two classes of linear codes $\mathcal{C}'_Q$ and $\mathcal{C}_Q$ over $\mathbb{F}_q$ from Q and completely determine the weight distributions of our codes, showing that they are two-, three- or four-weight codes and contain optimal codes satisfying the Griesmer and Singleton bounds.

Keywords Quadratic forms, Vectorial bent functions, Linear codes, Weight distribution, Griesmer bound.

1. Introduction

Let p be a prime and $q > 1$ be a p-power. Let $Q(x) : \mathbb{F}_{q^m} \to \mathbb{F}_q$ be an arbitrary quadratic form of dimension m over $\mathbb{F}_q$. Our main objectives of this paper are to study the vectorial bentness of Q and to construct and study linear codes from Q.

The importance of bent and vectorial bent functions in coding theory and cryptography is apparent, as can be seen in the survey papers [1, 2, 28] or in many research papers (for example, [3, 6, 8, 9, 29, 30, 37, 38, 42, 44]). This is why we would want to study the bentness of quadratic forms in the first place.

If $q = p$ is odd, it is well-known that a quadratic form Q is a bent function if and only if Q is non-degenerate (see [19, 20, 23]). The general case should be known by the experts for a long time, but we can't find the exact reference in the literature. We first give a proof of this fact: Q is a vectorial bent function if and only if Q is non-degenerate and $(q+1)m$ is even (i.e. either q is odd or m is even). We then investigate the case that $Q(x) = \sum\limits_{i=0}^{m-1} \mathrm{Tr}_{q^m/q}(a_i x^{q^i+1})$ ($a_i \in \mathbb{F}_{q^m}^*$) when $2 \mid (q+1)m$, and show that Q is vectorial bent if and only if the additive polynomial

2010 *Mathematics Subject Classification.* 94B05, 15A63, 94A60.

Corresponding author: Yi Ouyang (yiouyang@ustc.edu.cn).

Partially supported by Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0302904) and Anhui Initiative in Quantum Information Technologies (Grant No. AHY150200).

$L_Q(x) = \sum_i (a_i + a_{m-i}^{q^i})x^{q^i}$ is a permutation polynomial over $\mathbb{F}_{q^m}$. In particular, if $Q(x) = \mathrm{Tr}_{q^m/q}(ax^{q^j+1})$, we obtain necessary and sufficient conditions for Q to be vectorial bent, recover the well-known constructions of Sidelnikov, Dembowski-Ostrom and Kasami, and partially improve the results of Dong et al [14, Theorem 6].

Constructing linear codes with few weights is of special interest in secret sharing [4], authentication codes [10], strongly regular graphs [5] and designing frequency hopping sequences [5]. This has been widely studied by researchers for years (see [11, 16, 18, 21, 22], [24]-[27],[31]-[34], [39]-[43],[45]-[49]). Some special quadratic forms $Q(x)$ have been used to construct $\mathbb{F}_p$-linear codes (see [3, 12, 16, 25, 45, 46]), where the codes are

$$\tilde{C}_Q := \{\tilde{c}_{a,b} = (\mathrm{Tr}_{q^m/p}(aQ(x) - bx))_{x\in\mathbb{F}_{q^m}^*} \mid a, b \in \mathbb{F}_{q^m}\}, \tag{1}$$

$$\tilde{C}'_Q := \{\tilde{c}_{a,b,c} = (\mathrm{Tr}_{q^m/p}(aQ(x) - bx) + c)_{x\in\mathbb{F}_{q^m}} \mid a, b \in \mathbb{F}_{q^m}, c \in \mathbb{F}_p\}. \tag{2}$$

It was shown in [3, 16, 25, 45, 46] that $\tilde{C}_Q$ and $\tilde{C}'_Q$ are five- or six-weight $\mathbb{F}_p$-codes if q is odd and m is even. For even q and $Q(x) = x^{2^j+1} (j \geq 0)$, Ding et al [12] showed that $\tilde{C}_Q$ is three-weight if m is odd or m is even and $j = \frac{m}{2}$. Moreover, Ding et al [9] constructed and studied the binary linear codes

$$\mathcal{C} := \{c_{a,b,c} = (\mathrm{Tr}_{q/2}(aF(x)) + \mathrm{Tr}_{q^m/2}(bx) + c)_{x\in\mathbb{F}_{q^m}^*} : (a, b, c) \in \mathbb{F}_q \times \mathbb{F}_{q^m} \times \mathbb{F}_2\}, \tag{3}$$

where $F : \mathbb{F}_{q^m} \to \mathbb{F}_q$ is a vectorial bent function.

Replacing Q, F by an arbitrary quadratic form and $\mathbb{F}_{q^m}/\mathbb{F}_p$ by any finite field extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ in Eqs. (1), (3), we define two classes of $\mathbb{F}_q$-linear codes $\mathcal{C}_Q$ and $\mathcal{C}'_Q$ from the quadratic form Q as follows:

$$\mathcal{C}_Q := \{c_{a,b} = (aQ(x) - \mathrm{Tr}_{q^m/q}(bx))_{x\in\mathbb{F}_{q^m}^*} \mid a \in \mathbb{F}_q,\ b \in \mathbb{F}_{q^m}\},$$
$$\mathcal{C}'_Q := \{c_{a,b,c} = (aQ(x) - \mathrm{Tr}_{q^m/q}(bx) + c)_{x\in\mathbb{F}_{q^m}} \mid a, c \in \mathbb{F}_q,\ b \in \mathbb{F}_{q^m}\}.$$

The main result of this paper is that we determine the weight distribution of these codes without any restriction on Q. Under any circumference, $\mathcal{C}_Q$ and $\mathcal{C}'_Q$ are codes with few (≤ 4) weights. In particular, we show that both $\mathcal{C}_Q$ and $\mathcal{C}'_Q$ are optimal codes to the Griesmer bound if $m = 2$ and $Q(x) = 0$ only if $x = 0$ and MDS codes if $Q(x) = ax^2 : \mathbb{F}_q \to \mathbb{F}_q$ $(a \neq 0)$, and are not optimal otherwise.

We also present a trick to descend an $\mathbb{F}_q$-code to an $\mathbb{F}_p$-code, whose weight enumerator (and hence parameters) is uniquely determined by the old code, and consequently the optimality will be inherited.

This paper is organized as follows. We first recall basic facts about quadratic forms over a field and then over a finite field in § 2. In § 3 we prove results about the bentness of quadratic forms. In § 4 we are devoted to constructing and studying of our linear codes.

2. Preliminaries

2.1. **Notations and conventions.** Throughout this paper we shall use the following notations.

- p is a prime and $\zeta_p = e^{\frac{2\pi i}{p}}$ is a primitive p-th root of unity;
- For a p-power, $\mathbb{F}_q$ is the finite field of q elements and $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$ is the multiplicative group of $\mathbb{F}_q$;

- For $m > 0$, $\mathrm{Tr}_{q^m/q} = \sum_{t=0}^{m-1} x^{q^t}$ is the trace map from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$;
- For a matrix A, A^T is its transpose. In particular, the transpose of a column vector is a row vector;
- $\mathbb{F}_q^m$ is identified with the column vector space $\mathbb{F}_q^{m\times 1}$.

2.2. **Bent and vectorial bent functions.** We first recall

Definition 1. *The Walsh transform of a function $f : \mathbb{F}_q \to \mathbb{F}_p$ is the function $S_f : \mathbb{F}_q \to \mathbb{C}$ defined by*

$$S_f(b) = \sum_{x\in\mathbb{F}_q} \zeta_p^{f(x)-\mathrm{Tr}_{q/p}(bx)}, \quad b \in \mathbb{F}_q. \tag{4}$$

The function f is called bent if $|S_f(b)|^2 = q$ for all $b \in \mathbb{F}_q$.

Definition 2. *Let $F : \mathbb{F}_{q^m} \to \mathbb{F}_q$ be a vectorial function. The component functions of F for $a \in \mathbb{F}_q^*$ is the function $f_a(x) = \mathrm{Tr}_{q/p}(aF(x)) : \mathbb{F}_{q^m} \to \mathbb{F}_p$, the extended Walsh transform S_F of F is*

$$S_F(a,b) = S_{f_a}(b) = \sum_{x\in\mathbb{F}_{q^m}} \zeta_p^{\mathrm{Tr}_{q/p}(aF(x))-\mathrm{Tr}_{q^m/p}(bx)}, \quad (a,b) \in \mathbb{F}_q^* \times \mathbb{F}_{q^m}. \tag{5}$$

F is called vectorial bent if $|S_F(a,b)|^2 = q^m$ for all $(a,b) \in \mathbb{F}_q^* \times \mathbb{F}_{q^m}$, i.e., if all its component functions f_a are bent.

The characterization and construction of vectorial bent Boolean functions have been extensively studied (see [6, 19, 31, 35, 44]). We shall characterize the quadratic vectorial bent functions.

2.3. **Quadratic forms over finite fields.** The general references for this subsection are [7, 15, 23, 36].

We first assume $\mathbb{F}$ is a field (of any characteristic) and V is a finite dimensional $\mathbb{F}$-vector space. Recall that for a symmetric bilinear form $B : V\times V \to \mathbb{F}$, its radical $\mathrm{rad}(B)$ is a subspace of V defined by

$$\mathrm{rad}(B) = \{v \in V \mid B(v,w) = 0 \text{ for all } w \in V\},$$

and B is called non-degenerate if $\mathrm{rad}(B) = \{0\}$.

Definition 3. *Let $\mathbb{F}$ be a field and V be a finite dimensional $\mathbb{F}$-vector space. A quadratic form Q is a map $V \to \mathbb{F}$ such that $Q(av) = a^2Q(v)$ for all $a \in \mathbb{F}$ and*

$$B(v,w) = B_Q(v,w) := Q(v+w) - Q(v) - Q(w)$$

is a symmetric bilinear form. The dimension of Q is $\dim(Q) := \dim_{\mathbb{F}}(V)$, and the radical of Q is the subspace $\mathrm{rad}(Q) := \{v \in \mathrm{rad}(B) \mid Q(v) = 0\}$. Q is called non-degenerate if $\mathrm{rad}(Q) = \{0\}$ and $\dim_{\mathbb{F}} \mathrm{rad}(B) \le 1$.

Two quadratic forms $Q : V \to \mathbb{F}$ and $Q' : W \to \mathbb{F}$ are called equivalent if there exists an $\mathbb{F}$-isomorphism $\sigma : V \to W$ such that $Q(v) = Q'(\sigma(v))$ for all $v \in V$.

Note that if $\mathrm{char}(F) = 2$, then the bilinear form B is also alternating, hence it must be degenerate if $\dim(V)$ is odd, so in this case $\dim_{\mathbb{F}} \mathrm{rad}(B) \ge 1$. In general, we have (see [7, 15])

Lemma 1. *Let Q be a quadratic form over $\mathbb{F}$ and B be its associated bilinear form.*

(1) *If* $\mathrm{char}(\mathbb{F}) \neq 2$ *or if* $\mathrm{char}(\mathbb{F}) = 2$ *and* $\dim(Q)$ *is even, then* Q *is non-degenerate if and only if* B *is non-degenerate.*

(2) *If* $\mathrm{char}(\mathbb{F}) = 2$ *and* $\dim(Q)$ *is odd, then* Q *is non-degenerate if and only if* $\dim(\mathrm{rad}(B)) = 1$ *and* $Q|_{\mathrm{rad}(B)} \neq 0$. *If* $\mathbb{F}$ *is moreover a perfect field, the non-degeneracy condition is equivalent to* $\mathrm{rad}(Q) = \{0\}$.

Take a basis $\{\alpha_1, \cdots, \alpha_m\}$ of V. For $v \in V$, let $X = (X_i)$ be its coordinate vector under this basis. Then $Q : V \to \mathbb{F}$ is equivalent to the quadratic form

$$Q' : \mathbb{F}^m \to \mathbb{F},\ Q'(X) = Q(v).$$

On the other hand, any quadratic form $Q : \mathbb{F}^m \to \mathbb{F}$ can be written as

$$Q(X) = \sum_{1\le i\le j\le m} a_{ij} X_i X_j$$

whose associated bilinear form is

$$B(X,Y) = \sum_{1\le i\le m} 2a_{ii} X_i Y_i + \sum_{1\le i< j\le m} a_{ij}(X_i Y_j + X_j Y_i).$$

Two quadratic forms Q and Q' over $\mathbb{F}^m$ are equivalent if one can transform Q to Q' by non-singular linear substitution of indeterminates, i.e., $Q'(X) = Q(MX)$ where M is an invertible matrix over $\mathbb{F}$.

Proposition 1 ([23], Theorems 6.21 and 6.30)**.** *Suppose* $Q : V \to \mathbb{F}_q$ *is a quadratic form of dimension* m. *Let* $r = m - \dim \mathrm{rad}(Q)$. *Let* W *be a complementary of* $\mathrm{rad}(Q)$ *in* V, *then* $Q|_W$ *is non-degenerate. Hence* Q *is non-degenerate if and only if* $\mathrm{rad}(Q) = \{0\}$. *Moreover, if* Q *is non-degenerate, the followings hold.*

(1) *If* q *is odd, then* $Q(X)$ *is equivalent to a diagonal form* $d_1X_1^2 + \cdots + d_mX_m^2$ $(d_i \in \mathbb{F}_q^*)$, *and* $d_1 \cdots d_m$ *is unique up to a square in* $\mathbb{F}_q^*$.

(2) *If* q *is even, then for odd* m, $Q(X)$ *is equivalent to* $X_1X_2 + X_3X_4 + \cdots + X_{m-2}X_{m-1} + X_m^2$; *for even* m, $Q(X)$ *is equivalent to either* $X_1X_2 + X_3X_4 + \cdots + X_{m-1}X_m$ *or* $X_1X_2 + X_3X_4 + \cdots + X_{m-3}X_{m-2} + X_{m-1}^2 + \lambda X_m^2$ *with* λ *satisfying* $\mathrm{Tr}_{q/2}(\lambda) = 1$.

Remark 1. *We say a quadratic form* $Q : \mathbb{F}_q^m \to \mathbb{F}_q$ *is a standard form if* $Q(X) = Q(X_1, \cdots, X_r)$ *with* $Q(X_1, \cdots, X_r) : \mathbb{F}_q^r \to \mathbb{F}_q$ *is non-degenerate of the form (1) or (2) in the above proposition. For any quadratic form* $Q : V \to \mathbb{F}_q$, *there exists a basis* $\{\alpha_1, \cdots, \alpha_m\}$ *of* V *such that the corresponding quadratic form* Q' *on* $\mathbb{F}_q^m$ *is standard.*

3. Quadratic forms and vectorial bent functions

In the case $q = p > 2$, it was shown that a quadratic function $F : \mathbb{F}_{p^m} \to \mathbb{F}_p$ is bent if and only if the corresponding quadratic form $Q(x)$ is non-degenerate (see [19, 23]). For general q, analogous result should be known by the experts for a while, however we can't find the exact reference. In this section, we shall present and prove the analogous result for general q and then apply this result to specific quadratic forms.

Definition 4. *For a quadratic form* $Q : V \to \mathbb{F}_q$ *and* $u \in \mathbb{F}_q$, *set*

$$N_Q(u) := \#\{v \in V \mid Q(v) = u\}.$$

Lemma 2 ([23], Theorems 6.27 and 6.32)**.** *Let $Q : V \to \mathbb{F}_q$ be a non-degenerate quadratic form of dimension m.*

(1) *If q is odd and Q is equivalent to the diagonal form $Q_m(X) = d_1X_1^2 + \cdots + d_mX_m^2$, let $\varepsilon_Q = \eta_q((-1)^{\frac{m}{2}} d_1 \cdots d_m)$ where η_q is the quadratic character of $\mathbb{F}_q^*$ extending to $\mathbb{F}_q$ by setting $\eta_q(0) = 0$. Then if m is odd,*

$$N_Q(u) = q^{m-1} + q^{\frac{m-1}{2}} \varepsilon_Q \eta_q(u). \tag{6}$$

If m is even,

$$N_Q(u) = \begin{cases} q^{m-1} + q^{\frac{m-2}{2}}(q-1)\varepsilon_Q, & \text{if } u = 0, \\ q^{m-1} - q^{\frac{m-2}{2}}\varepsilon_Q, & \text{if } u \neq 0. \end{cases} \tag{7}$$

(2) *If q is even and m is odd, then*

$$N_Q(u) = q^{m-1}. \tag{8}$$

(3) *If q is even and m is even, let $\varepsilon_Q = 1$ if Q is equivalent to $X_1X_2 + X_3X_4 + \cdots + X_{m-1}X_m$ and $\varepsilon_Q = -1$ if Q is equivalent to $X_1X_2 + X_3X_4 + \cdots + X_{m-1}X_m + X_{m-1}^2 + \lambda X_m^2$ $(\mathrm{Tr}_{q^m/q}(\lambda) = 1)$. Then $N_Q(u)$ has the same formula as in (7).*

Proposition 2. *Let $Q(x) : \mathbb{F}_{q^m} \to \mathbb{F}_q$ be a quadratic form. For $a \in \mathbb{F}_q^*$, $u \in \mathbb{F}_q$ and $b \in \mathbb{F}_{q^m}$, set*

$$N_Q(a, b; u) = \#\{x \in \mathbb{F}_{q^m} \mid aQ(x) - \mathrm{Tr}_{q^m/q}(bx) = u\}.$$

Suppose $\{\alpha_1, \cdots, \alpha_m\}$ is a basis of $\mathbb{F}_{q^m}$ such that the corresponding quadratic form from $\mathbb{F}_q^m$ to $\mathbb{F}_q$ is standard. Let $M = (\mathrm{Tr}_{q^m/q}(\alpha_i\alpha_j))_{1\le i,j\le m}$. Let $\tilde{x} = (\tilde{x}_1, \cdots, \tilde{x}_m) = X^T M$ where X is the coordinate vector of $x \in \mathbb{F}_{q^m}$. Then

(1) *If q is odd, let $Q_r(X_1, \cdots, X_r) = d_1X_1^2 + \cdots + d_rX_r^2$, $u(b) = Q_r(\frac{\tilde{b}_1}{2d_1}, \cdots, \frac{\tilde{b}_r}{2d_r})$. Then*

$$N_Q(a, b; u) = \begin{cases} q^{m-r} N_{Q_r}(au + u(b)), & \text{if } \tilde{b}_j = 0 \text{ for all } j > r, \\ q^{m-1}, & \text{if } \tilde{b}_j \neq 0 \text{ for some } j > r. \end{cases} \tag{9}$$

(2) *If q is even and r is odd, let $Q_r(X_1, \cdots, X_r) = X_1X_2 + \cdots + X_{r-2}X_{r-1} + X_r^2$ and let $u(b) = \tilde{b}_1\tilde{b}_2 + \cdots + \tilde{b}_{r-2}\tilde{b}_{r-1}$ if $r > 1$ and $u(b) = 0$ if $r = 1$. Then*

$$N_Q(a, b; u) = \begin{cases} q^{m-1}, & \text{if } \tilde{b}_r = 0 \text{ or } \tilde{b}_j \neq 0 \text{ for some } j > r, \\ q^{m-1} + \varepsilon_b\ q^{m-\frac{r+1}{2}}, & \text{if } \tilde{b}_r \neq 0 \text{ and } \tilde{b}_j = 0 \text{ for all } j > r. \end{cases} \tag{10}$$

where $\varepsilon_b = 1$ or -1 if the equation $x^2 + \tilde{b}_r x = au + u(b)$ is solvable over $\mathbb{F}_q$ or not.

(3) *If q and r are even, let either $Q_r(X_1, \cdots, X_r) = X_1X_2 + \cdots + X_{r-1}X_r$ or $Q_r(X_1, \cdots, X_r) = X_1X_2 + \cdots + X_{r-1}X_r + X_{r-1}^2 + \lambda X_r^2$, let $u(b) = Q_r(\tilde{b}_1, \cdots \tilde{b}_r)$. Then*

$$N_Q(a, b; u) = \begin{cases} q^{m-r} N_{Q_r}(au + u(b)), & \text{if } \tilde{b}_j = 0 \text{ for all } j > r, \\ q^{m-1}, & \text{if } \tilde{b}_j \neq 0 \text{ for some } j > r. \end{cases} \tag{11}$$

Proof. (1) Under the basis $\{\alpha_1, \cdots, \alpha_m\}$, $aQ(x) - \mathrm{Tr}_{q^m/q}(bx) = u$ is equivalent to

$$\sum_{i=1}^{r} d_i\Big(aX_i - \frac{\tilde{b}_i}{2d_i}\Big)^2 = au + Q_r\Big(\frac{\tilde{b}_1}{2d_1}, \cdots \frac{\tilde{b}_r}{2d_r}\Big) + \sum_{j=r+1}^{m} \tilde{b}_j aX_j.$$

We are led to count the solutions of

$$\sum_{i=1}^{r} d_i X_i^2 = au + u(b) + \sum_{j=r+1}^{m} \tilde{b}_j X_j.$$

If $\tilde{b}_j \neq 0$ for some $j > r$, given $X_{j'} \in \mathbb{F}_q$ for all $j' \neq j$, there is exactly one X_j satisfying the above equation, so $N_Q(a, b; u) = q^{m-1}$ in this case. If $\tilde{b}_j = 0$ for all $j > r$, the number of solutions of $\sum_{i=1}^{r} d_i X_i^2 = au + u(b)$ is clear $q^{m-r} N_{Q_r}(au + u(b))$.

(2) Let $Q_r(X) = X_1 X_2 + \cdots + X_{r-2} X_{r-1} + X_r^2 = Q_{r-1}(X) + X_r^2$. Let $u(b) = \tilde{b}_1 \tilde{b}_2 + \cdots + \tilde{b}_{r-2} \tilde{b}_{r-1}$. In this case, $aQ(x) - \mathrm{Tr}_{q^m/q}(bx) = u$ is equivalent to

$$Q_{r-1}(aX_1 + \tilde{b}_1, \cdots, aX_{r-1} + \tilde{b}_{r-1}) + (aX_r)^2 + \sum_{j=1}^{m} \tilde{b}_j (aX_j) = au + u(b).$$

We are led to count the solutions of the equation

$$Q_{r-1}(X_1, \cdots, X_{r-1}) + X_r^2 + \tilde{b}_r X_r + \sum_{j=r+1}^{m} \tilde{b}_j X_j = au + u(b).$$

Again if $\tilde{b}_j \neq 0$ for some $j > r$ or if $\tilde{b}_r = 0$, $N_Q(a, b; u) = q^{m-1}$. Now assume $\tilde{b}_r \neq 0$ and $\tilde{b}_j = 0$ for $j > r$. The remaining case is to count the number of solutions of $Q_{r-1}(X_1, \cdots, X_{r-1}) + X_r^2 + \tilde{b}_r X_r = au + u(b)$ with $b_r \neq 0$. For $w \in \mathbb{F}_q$, if $r > 1$, then

$$\begin{aligned} N(w) :=& \#\{(X_i) \in \mathbb{F}_q^r \mid Q_{r-1}(X_1, \cdots, X_{r-1}) + X_r^2 + \tilde{b}_r X_r = w\} \\ =& \sum_{v \in \mathbb{F}_q} \#\{Q_{r-1}(X_i) = v\} \cdot \#\{X_r^2 + \tilde{b}_r X_r = w + v\} \\ =& (q^{r-2} + q^{\frac{r-1}{2}} - q^{\frac{r-3}{2}}) \cdot \#\{X_r^2 + \tilde{b}_r X_r = w\} \\ &+ (q^{r-2} - q^{\frac{r-3}{2}}) \cdot \sum_{v \neq 0} \#\{X_r^2 + \tilde{b}_r X_r = w + v\}. \end{aligned}$$

Since $\#\{X_r \in \mathbb{F}_q \mid X_r^2 + \tilde{b}_r X_r = w\} = 0$ or 2 and clearly $\#\{(X_r, v) \in \mathbb{F}_q^2 \mid X_r^2 + \tilde{b}_r X_r = v\} = q^2$, we get $N(w) = q^{r-1} \pm q^{\frac{r-1}{2}}$ according to $x^2 + b_r x = w$ is solvable or not. If $r = 1$, the result is clear.

(3) Assume $Q_r(X_1. \cdots, X_r) = X_1 X_2 + \cdots + X_{r-1} X_r + X_{r-1}^2 + \lambda X_r^2$. Then in this case, $aQ(x) - \mathrm{Tr}_{q^m/q}(bx) = u$ is equivalent to

$$Q_r(aX_1 + \tilde{b}_1, \cdots, aX_r + \tilde{b}_r) + \sum_{j=r-1}^{m} \tilde{b}_j (aX_j) = au + u(b).$$

The same argument as in (1) gives the answer. The case $Q_r(X_1. \cdots, X_r) = X_1 X_2 + \cdots + X_{r-1} X_r$ is similar. □

Corollary 1. *One always has $N_Q(0) = q^{m-r} N_{Q_r}(0)$. Thus if $N_Q(0)$ is prime to p, then Q must be non-degenerate.*

In particular, if $m = 2$, then Q is non-degenerate with $\varepsilon_Q = -1$ if and only if $N_Q(0) = 1$; Q is non-degenerate with $\varepsilon_Q = 1$ if and only if $N_Q(0) = 2q - 1$.

Remark 2. *From now on, for an arbitrary quadratic form Q such that $r = m - \dim \mathrm{rad}(Q)$, if q is odd or r is even, we let $\varepsilon_Q = \varepsilon_{Q_r}$ where Q_r is given* *in Proposition 2. Certainly if Q is non-degenerate, i.e., $m = r$, then this definition agrees with Lemma 2.*

Theorem 1. *A quadratic form $Q(x) : \mathbb{F}_{q^m} \to \mathbb{F}_q$ is vectorial bent if and only if $Q(x)$ is non-degenerate and either q is odd or m is even.*

Proof. Note that

$$S_Q(a,b) = \sum_{x\in\mathbb{F}_{q^m}} \zeta_p^{\mathrm{Tr}_{q/p}(aQ(x)-\mathrm{Tr}_{q^m/q}(bx))} = \sum_{u\in\mathbb{F}_q} N_Q(a,b;u)\zeta_p^{\mathrm{Tr}_{q/p}(u)}.$$

If $N_Q(a,b;u) = q^{m-1}$ or $q^{m-1} + \varepsilon_b q^{m-\frac{r+1}{2}}$ in Proposition 2, then $S_Q(a,b) = 0$ and $Q(x)$ is not vectorial bent. This means that if Q is degenerate or if q is even and m is odd, then $Q(x)$ is not vectorial bent.

Now we assume Q is non-degenerate and either q is odd or m is even. Then $r = m$, $N_Q(a,b;u) = N_{Q_m}(au + u(b))$, and

$$S_Q(a,b) = \sum_{u\in\mathbb{F}_q} N_{Q_m}(au+u(b))\zeta_p^{\mathrm{Tr}_{q/p}(u)} = \zeta_p^{-\mathrm{Tr}_{q/p}(a^{-1}u(b))} \cdot \sum_{u\in\mathbb{F}_q} N_{Q_m}(au)\zeta_p^{\mathrm{Tr}_{q/p}(u)}.$$

If q is odd and m is odd, by Proposition 2, then

$$\sum_{u\in\mathbb{F}_q} N_{Q_m}(au)\zeta_p^{\mathrm{Tr}_{q/p}(u)} = q^{\frac{m-1}{2}}\varepsilon_Q\eta_q(a)\sum_{u\in\mathbb{F}_q}\eta_q(u)\zeta_p^{\mathrm{Tr}_{q/p}(u)}.$$

The last sum is a Gauss sum, hence $|S_Q(a,b)| = q^{\frac{m}{2}}$ and Q is vectorial bent.

If m is even and q is general, by Proposition 2, then

$$\sum_{u\in\mathbb{F}_q} N_{Q_m}(au)\zeta_p^{\mathrm{Tr}_{q/p}(u)} = q^{\frac{m}{2}}\varepsilon_Q,$$

hence Q is also vectorial bent. □

Remark 3. *Certainly this theorem implies that a quadratic function $F(x)$ is vectorial bent if and only if either q is odd or m is even and the corresponding quadratic form $Q(x)$ is non-degenerate.*

The following theorem is one of the main results in this section.

Theorem 2. *Suppose either q is odd or m is even. Let $a_i \in \mathbb{F}_{q^m}$ $(i = 0, 1, \ldots, m-1)$ and write $a_m = a_0$. Let $Q(x) = \sum_{i=0}^{m-1} \mathrm{Tr}_{q^m/q}(a_i x^{q^i+1})$ and*

$$L_Q(x) = \sum_{i=0}^{m-1}\left(a_i + a_{m-i}^{q^i}\right)x^{q^i}.$$

Then $Q(x)$ is vectorial bent if and only if $L_Q(x) \neq 0$ for $x \in \mathbb{F}_{q^m}^*$, i.e., $L_Q(x)$ is a permutation polynomial over $\mathbb{F}_{q^m}$. In particular, Q is vectorial bent if $\widetilde{L}_Q(x) = \sum_{i=0}^{m-1}\left(a_i + a_{m-i}^{q^i}\right)x^{\frac{q^i-1}{q-1}} \neq 0$ for $x \in \mathbb{F}_{q^m}^*$, i.e., $\gcd(\widetilde{L}_Q(x), x^{q^m-1} - 1) = 1$.

Proof. By Theorem 1, it suffices to show the associated bilinear form

$$B(x,y) = Q(x+y) - Q(x) - Q(y)$$

is non-degenerate. But

$$\begin{aligned}
&B(x,y)\\
&=\sum_{i=0}^{m-1}\mathrm{Tr}_{q^m/q}\Big(a_i(x^{q^i}y+xy^{q^i})\Big)=\sum_{i=0}^{m-1}\mathrm{Tr}_{q^m/q}\Big(y^{q^i}(a_i^{q^i}x^{q^{2i}}+a_ix)\Big)\\
&=\sum_{i=0}^{m-1}\mathrm{Tr}_{q^m/q}\Big(y(a_i^{q^i}x^{q^{2i}}+a_ix)^{q^{m-i}}\Big)=\sum_{i=0}^{m-1}\mathrm{Tr}_{q^m/q}\Big(y(a_i^{q^{m-i}}x^{q^{m-i}}+a_ix^{q^i})\Big)\\
&=\mathrm{Tr}_{q^m/q}\Big(y\sum_{i=0}^{m-1}(a_i+a_{m-i}^{q^i})x^{q^i}\Big)=\mathrm{Tr}_{q^m/q}(yL_Q(x)).
\end{aligned}$$

The non-degeneracy of $\mathrm{Tr}_{q^m/q}$ means that $B(x,y)$ is non-degenerate if and only if $L_Q(x)\neq 0$ for all $x\in\mathbb{F}_{q^m}^*$, i.e., $L_Q(x)$ is a permutation polynomial over $\mathbb{F}_{q^m}$.

If $\widetilde{L}_Q(x)\neq 0$ for $x\in\mathbb{F}_{q^m}^*$, then $L_Q(x)=x\widetilde{L}_Q(x^{q-1})\neq 0$ for $x\in\mathbb{F}_{q^m}^*$, hence Q is vectorial bent. □

Theorem 2 has the following consequence:

Corollary 2. *Suppose $2\nmid q$ or $2\mid m$. Let $Q(x)=\mathrm{Tr}_{q^m/q}(ax^{q^j+1})$ with $a\in\mathbb{F}_{q^m}^*$ and $0\le j<m$.*

(1) *If $j=0$, then $Q(x)$ is vectorial bent if and only if q is odd.*

(2) *If $1\le j<m$ and $j\neq\frac{m}{2}$, let $s=\gcd(2j,m)$. Let $\mathrm{ord}(a)$ be the order of $a\in\mathbb{F}_{q^m}^*$ and $v_2(i)$ be the 2-adic valuation of $i\in\mathbb{Z}$. If $2\mid m$, let*

$$T_{m,j}=\frac{q^m-1}{q^{\frac{s}{2}}+1}.$$

If q is odd, then $Q(x)$ is vectorial bent if and only if one of the following is satisfied:

- $2\nmid m$ *or* $v_2(j)\ge v_2(m)\ge 1$;
- $0\le v_2(j)<v_2(m)-1$ *and* $\mathrm{ord}(a)\nmid T_{m,j}$;
- $v_2(j)=v_2(m)-1\ge 0$ *and either* $\mathrm{ord}(a)\nmid 2T_{m,j}$ *or* $\mathrm{ord}(a)\mid T_{m,j}$.

If q is even, then $Q(x)$ is vectorial bent if and only if $v_2(j)\le v_2(m)-1$ and $\mathrm{ord}(a)\nmid T_{m,j}$.

(3) *If $j=\frac{m}{2}$ and hence m is even, then $Q(x)$ is vectorial bent if and only if $a\in\mathbb{F}_{q^{m/2}}^*$ or $\mathrm{ord}(a)\nmid 2(q^{\frac{m}{2}}-1)$ if q is odd; and $a\in\mathbb{F}_{q^m}\backslash\mathbb{F}_{q^{m/2}}$ if q is even.*

Proof. We only prove (2), the remaining cases are easy. Note that $L_Q(x)=a^{q^{m-j}}x^{q^{m-j}}+ax^{q^j}$. For $x\in\mathbb{F}_{q^m}^*$, we get $L_Q(x)^{q^j}=ax(1+(ax^{q^j+1})^{q^j-1})$. Then $Q(x)$ is not vectorial bent if and only if there exists $x\in\mathbb{F}_{q^m}^*$ such that $(ax^{q^j+1})^{q^j-1}=-1$.

Let $i=\frac{q^m-1}{\mathrm{ord}(a)}$. Suppose α is a primitive element of $\mathbb{F}_{q^m}$ such that $a=\alpha^i$. Let $t_j=2j/s$ and $t_m=m/s$. Then

- $2\mid t_m$ and $2\nmid t_j$ if and only if $v_2(j)<v_2(m)-1$;
- $2\nmid t_jt_m$ if and only if $v_2(j)=v_2(m)-1$;
- $2\mid t_j$ and $2\nmid t_m$ if and only if $v_2(j)\ge v_2(m)$.

(i) If q is odd, $(ax^{q^j+1})^{q^j-1}=-1$ has a root in $\mathbb{F}_{q^m}^*$ if and only if there exists t such that $(\alpha^{i+(q^j+1)t})^{q^j-1}=-1$, which is equivalent to

$$\frac{q^m-1}{2}-(q^j-1)i\equiv 0\pmod{q^s-1}. \tag{12}$$

Note that $\frac{q^m-1}{2} \equiv 0 \pmod{q^s-1}$ if t_m is even and $\frac{q^m-1}{2} \equiv \frac{q^s-1}{2} \pmod{q^s-1}$ if t_m is odd. Note that $q^j-1 \equiv 0 \pmod{q^s-1}$ if m is odd or if m is even and t_j is even, and $q^j-1 \equiv q^{\frac{s}{2}}-1 \pmod{q^s-1}$ if m is even and t_j is odd.

If m is odd, we always have $\frac{q^m-1}{2}-(q^j-1)i \equiv \frac{q^s-1}{2} \not\equiv 0 \pmod{q^s-1}$. Thus $Q(x)$ is always vectorial bent if m is odd.

If m is even, then s is even and we need to treat three situations:

(A) $2 \mid t_m$ and hence $2 \nmid t_j$. Then

$$\frac{q^m-1}{2}-(q^j-1)i \equiv (q^{\frac{s}{2}}-1)i \pmod{q^s-1}.$$

Then (12) is satisfied if and only if i is a multiple of $q^{\frac{s}{2}}+1$, equivalently $\mathrm{ord}(a) \mid T_{m,j}$. Hence $Q(x)$ is vectorial bent if $\mathrm{ord}(a) \nmid T_{m,j}$.

(B) $2 \nmid t_m t_j$. Then

$$\frac{q^m-1}{2}-(q^j-1)i \equiv \frac{q^s-1}{2}-(q^{\frac{s}{2}}-1)i \pmod{q^s-1}.$$

Then (12) is satisfied if and only if i is the product of $\frac{q^{\frac{s}{2}}+1}{2}$ and an odd number, i.e., $\mathrm{ord}(a) \mid 2T_{m,j}$ and $2 \nmid \frac{2T_{m,j}}{\mathrm{ord}(a)}$. Hence $Q(x)$ is vectorial bent if $\mathrm{ord}(a) \nmid 2T_{m,j}$ or $\mathrm{ord}(a) \mid T_{m,j}$.

(C) $2 \mid t_j$ and hence $2 \nmid t_m$. Then $s \mid j$ and $\frac{q^m-1}{2}-(q^j-1)i \equiv \frac{q^s-1}{2} \pmod{q^s-1}$. Thus $Q(x)$ is always vectorial bent in this case.

(ii) If q is even, then s is even and $1=-1 \in \mathbb{F}_q$. $(ax^{q^j+1})^{q^j-1}=1$ has a root in $\mathbb{F}_{q^m}^*$ if and only if there exists t such that $(\alpha^{i+(q^j+1)t})^{q^j-1}=1$, i.e.,

$$(q^j-1)i \equiv 0 \pmod{q^s-1}. \tag{13}$$

But $q^j-1 \equiv 0 \pmod{q^s-1}$ if $2 \mid t_j$ and is $q^{\frac{s}{2}}-1 \pmod{q^s-1}$ if $2 \nmid t_j$. Thus $Q(x)$ is not vectorial bent if $2 \mid t_j$. If $2 \nmid t_j$, $Q(x)$ is vectorial bent if i is not a multiple of $(q^{\frac{s}{2}}+1)$, i.e., $\mathrm{ord}(a) \nmid T_{m,j}$. □

Remark 4. *We can recover the following well-known constructions of quadratic vectorial bent functions:*

1. *Sidelnikov's Construction is case (1) in the corollary.*
2. *Dembowski-Ostrom's Construction is case (2) for both q and m odd.*
3. *Kasami's Construction is case (3) for q odd, $m=2$ and $a \in \mathbb{F}_q^*$.*

Remark 5. *For $q=2^l$, a sufficient condition for the function $\mathrm{Tr}_{q^m/q}(ax^{2^i+1})$ to be vectorial bent was given in Dong et al ([14, Theorem 6]). In the case $i=lj$, their condition is just $v_2(j) \le v_2(m)-1$, $s=2$ and $\mathrm{ord}(a) \nmid T_{m,j}$.*

We give another example of quadratic vectorial bent functions in the following.

Theorem 3. *Suppose $m=2n$, let $u_1, u_2 \in \mathbb{F}_{q^m}^*$ satisfying $u_1 u_2^{q^n} \in \mathbb{F}_{q^n}$ and $\mathrm{Tr}_{q^n/p}(u_1 u_2^{q^n})=0$. Then*

$$Q_\beta(x) = \mathrm{Tr}_{q^m/q^n}(\beta x^{q^n+1}) + \mathrm{Tr}_{q^m/q^n}(\beta u_1 x)\mathrm{Tr}_{q^m/p}(u_2 x)$$

is vectorial bent if $q=p=2$ and $\beta \in \mathbb{F}_{2^m}-\mathbb{F}_{2^n}$, or $p \ge 3$ and $\mathrm{ord}(\beta) \nmid 2(q^n-1)$.

Proof. Set $q_{a\beta}(x) = \mathrm{Tr}_{q^m/p}(a\beta x^{q^n+1}) + \mathrm{Tr}_{q^m/p}(a\beta u_1 x)\mathrm{Tr}_{q^m/p}(u_2 x)$, $a \in \mathbb{F}_{q^n}^*$. Then $Q_\beta(x)$ is vectorial bent if and only if $q_{a\beta}(x)$ is bent for any $a \in \mathbb{F}_{q^n}^*$ or equivalently, the associated bilinear form

$$B(x,y) = q_{a\beta}(x+y) - q_{a\beta}(x) - q_{a\beta}(y)$$

is non-degenerate. But

$$\begin{aligned} B(x,y) =& \mathrm{Tr}_{q^m/p}(a\beta(x^{q^n}y + xy^{q^n})) + \mathrm{Tr}_{q^m/p}(a\beta u_1 x)\mathrm{Tr}_{q^m/p}(u_2 y) + \mathrm{Tr}_{q^m/p}(a\beta u_1 y) \\ & \times \mathrm{Tr}_{q^m/p}(u_2 x) \\ =& \mathrm{Tr}_{q^m/p}\Big(y\big(ax^{q^n}(\beta+\beta^{q^n}) + u_2\mathrm{Tr}_{q^m/p}(a\beta u_1 x) + a\beta u_1 \mathrm{Tr}_{q^m/p}(u_2 x)\big)\Big) \\ =& \mathrm{Tr}_{q^m/p}(yL_{q_{a\beta}}(x)). \end{aligned}$$

The non-degeneracy of $\mathrm{Tr}_{q^m/p}$ means that $B(x,y)$ is non-degenerate if and only if $L_{q_{a\beta}}(x) \neq 0$ for all $x \in \mathbb{F}_{q^m}^*$, i.e., $L_{q_{a\beta}}(x)$ is a permutation polynomial over $\mathbb{F}_{q^m}$.

Assume $q = p = 2$ and $\beta \in \mathbb{F}_{2^n}$ or $p \geq 3$ and $\mathrm{ord}(\beta) \mid 2(q^n - 1)$, then $\beta + \beta^{q^n} = 0$. Note that $a, u_1 u_2^{q^n} \in \mathbb{F}_{q^n}^*$, then

$$L_{q_{a\beta}}(u_2^{q^n}) = u_2 \mathrm{Tr}_{q^m/p}(a\beta u_1 u_2^{q^n}) + a\beta u_1 \mathrm{Tr}_{q^m/p}(u_2^{q^n+1}) = 0.$$

Thus $L_{q_{a\beta}}(x)$ is not a permutation over $\mathbb{F}_{q^m}$.

Assume $q = p = 2$ and $\beta \in \mathbb{F}_{2^m} - \mathbb{F}_{2^n}$ or $p \geq 3$ and $\mathrm{ord}(\beta) \nmid 2(q^n - 1)$. Take $\gamma = \beta + \beta^{q^n} \in \mathbb{F}_{q^n}^*$. Then $L_{q_{a\beta}}(x) = 0$ can be reduced to one of the following two systems of equations:

$$(A)\begin{cases} a\gamma x^{q^n} + u_2\mathrm{Tr}_{q^m/p}(a\beta u_1 x) = 0, \\ \mathrm{Tr}_{q^m/p}(u_2 x) = 0; \end{cases} \qquad (B)\begin{cases} a\gamma x^{q^n} + u_2\mathrm{Tr}_{q^m/p}(a\beta u_1 x) = al\beta u_1, \\ \mathrm{Tr}_{q^m/p}(u_2 x) = l \in \mathbb{F}_p^*. \end{cases}$$

We claim that $a\gamma x^{q^n} + u_2\mathrm{Tr}_{q^m/p}(a\beta u_1 x)$ is a permutation over $\mathbb{F}_{q^m}$ and the system (B) has no zeros at all in $\mathbb{F}_{q^m}$. Then $L_{q_{a\beta}}(x)$ is a permutation over $\mathbb{F}_{q^m}$.

For the first assertion, take $x, y \in \mathbb{F}_{q^m}$, let

$$a\gamma x^{q^n} + u_2\mathrm{Tr}_{q^m/p}(a\beta u_1 x) = a\gamma y^{q^n} + u_2\mathrm{Tr}_{q^m/p}(a\beta u_1 y).$$

Set $z = \mathrm{Tr}_{q^m/p}(a\beta u_1 x) - \mathrm{Tr}_{q^m/p}(a\beta u_1 y) \in \mathbb{F}_p$, then $y = x + (a\gamma)^{-1}u_2^{q^n} z$ and

$$\begin{aligned} z =& \mathrm{Tr}_{q^m/p}(a\beta u_1(x-y)) = -\mathrm{Tr}_{q^m/p}(a\beta u_1 (a\gamma)^{-1} u_2^{q^n} z) = -z\mathrm{Tr}_{q^n/p}(u_1 u_2^{q^n}) \\ \Rightarrow& z = 0. \end{aligned}$$

Thus $a\gamma x^{q^n} + u_2\mathrm{Tr}_{q^m/p}(a\beta u_1 x)$ is a permutation over $\mathbb{F}_{q^m}$.

The system (B) is equal to

$$\begin{cases} \gamma x^{q^n} = l\beta u_1, \\ \mathrm{Tr}_{q^m/p}(u_2 x) = l, \mathrm{Tr}_{q^m/p}(a\beta u_1 x) = 0; \end{cases} \qquad \begin{cases} a\gamma x^{q^n} = al\beta u_1 - l' u_2, \\ \mathrm{Tr}_{q^m/p}(u_2 x) = l, \mathrm{Tr}_{q^m/p}(a\beta u_1 x) = l', \end{cases}$$

where $l' \in \mathbb{F}_p^*$. For the first system, note that $x = \gamma^{-1} l (\beta u_1)^{q^n}$, then

$$\mathrm{Tr}_{q^m/p}(u_2 x) = l\mathrm{Tr}_{q^m/p}(u_2 \gamma^{-1}(\beta u_1)^{q^n}) = l\mathrm{Tr}_{q^n/p}(u_2 u_1^{q^n}) = l\mathrm{Tr}_{q^n/p}(u_2^{q^n} u_1) = 0. \tag{14}$$

For the second system, we have $x = (al\beta u_1 - l'u_2)^{q^n}(a\gamma)^{-1}$ and

$$\begin{aligned} \mathrm{Tr}_{q^m/p}(u_2 x) =& \mathrm{Tr}_{q^m/p}(u_2(al\beta u_1 - l'u_2)^{q^n}(a\gamma)^{-1}) = \mathrm{Tr}_{q^m/p}(u_2 u_1^{q^n} al \beta^{q^n}(a\gamma)^{-1}) \\ & - \mathrm{Tr}_{q^m/p}(l'(a\gamma)^{-1} u_2^{q^n+1}) = l\mathrm{Tr}_{q^n/p}(u_2 u_1^{q^n}) = 0. \end{aligned} \tag{15}$$

Since $\mathrm{Tr}_{q^m/p}(u_2x) = l \neq 0$, then Eqs. (14) and (15) can't hold and the system (B) has no zeros at all. Hence $L_{q_{a\beta}}(x) = 0$ if and only if $x = 0$. $\square$

4. Constructing codes with few weights from quadratic forms

Let $Q : \mathbb{F}_{q^m} \to \mathbb{F}_q$ be an arbitrary quadratic form. We define two linear codes over $\mathbb{F}_q$ from Q as follows:

$$\mathcal{C}_Q := \{c_{a,b} = (aQ(x) - \mathrm{Tr}_{q^m/q}(bx))_{x\in\mathbb{F}_{q^m}^*} \mid a \in \mathbb{F}_q,\ b \in \mathbb{F}_{q^m}\}, \tag{16}$$

$$\mathcal{C}'_Q := \{c_{a,b,c} = (aQ(x) - \mathrm{Tr}_{q^m/q}(bx) + c)_{x\in\mathbb{F}_{q^m}} \mid a, c \in \mathbb{F}_q,\ b \in \mathbb{F}_{q^m}\}. \tag{17}$$

The main purpose of this section is to determine the weight distribution of these two codes.

Theorem 4. *Assume $Q(x) : \mathbb{F}_{q^m} \to \mathbb{F}_q$ is a quadratic form and $r = m - \dim \mathrm{rad}(Q)$. Suppose $(r, q) \neq (1, 2)$.*

(1) If r is even, then $\mathcal{C}'_Q$ is a four-weight $[q^m, m + 2]$ linear code with weight distribution given in Table 1. Moreover $\mathcal{C}'_Q$ satisfies the Griesmer bound if and only if $m = 2$ and $N_Q(0) = 1$, and in this case $\mathcal{C}'_Q$ is an $[q^2, 4, q^2 - q - 1]_q$-code whose weight enumerator is

$$A_{\mathcal{C}'_Q}(x) = 1 + q^2(q-1)^2x^{q^2-q-1} + (q^3-q)x^{q^2-q} + q^2(q-1)x^{q^2-1} + (q-1)x^{q^2}.$$

Table 1. Weight distribution of $\mathcal{C}'_Q$ for $2 \mid r$

Weight i	*Frequency A_i*
0	*1*
$q^m - q^{m-1}$	$q^{m+2} - q^{r+2} + q^{r+1} - q$
$(q^{m-1} - \varepsilon_Q q^{\frac{2m-r-2}{2}})(q-1)$	$q^r(q-1)$
$q^m - q^{m-1} + \varepsilon_Q q^{\frac{2m-r-2}{2}}$	$q^r(q-1)^2$
q^m	$q-1$

(2) If $r \geq 3$ is odd, then $\mathcal{C}'_Q$ is a four-weight $[q^m, m+2, q^m - q^{m-1} - q^{\frac{2m-r-1}{2}}]$ linear code with weight distribution given in Table 2. If $r = 1$, then $\mathcal{C}'_Q$ is a three-weight $[q^m, m+2, q^m - 2q^{m-1}]$-code whose weight enumerator is $A_{\mathcal{C}'_Q}(x) =$

$$1+\frac{q^3-2q^2+q}{2}x^{q^m-2q^{m-1}} + (q^{m+2}-q^3+2q^2-2q)x^{q^m-q^{m-1}} + \frac{q^3-2q^2+3q-2}{2}x^{q^m}.$$

Moreover, $\mathcal{C}'_Q$ satisfies the Griesmer bound if and only if $m = r = 1$, and in this case, $\mathcal{C}'_Q$ is an $[q, 3, q-2]_q$ MDS code whose weight enumerator is

$$A_{\mathcal{C}'_Q}(x) = 1 + \frac{q^3-2q^2+q}{2}x^{q-2} + (2q^2-2q)x^{q-1} + \frac{q^3-2q^2+3q-2}{2}x^q.$$

Proof. We shall study the weight of $c_{a,b,c} = (aQ(x) - \mathrm{Tr}_{q^m/q}(bx) + c)$, which is $q^m - \#\{x \in \mathbb{F}_{q^m} \mid aQ(x) - \mathrm{Tr}(bx) + c = 0\}$. Note that if $a \neq 0$, then $\mathrm{wt}(c_{a,b,c}) = q^m - N_Q(a, b; -c)$. Note that

Table 2. Weight distribution of $\mathcal{C}_Q'$ for $2 \nmid r \geq 3$

Weight i	*Frequency A_i*
0	1
$q^m - q^{m-1}$	$q^{m+2} - q^r(q-1)^2 - q$
$q^m - q^{m-1} + q^{\frac{2m-r-1}{2}}$	$\frac{1}{2}q^r(q-1)^2$
$q^m - q^{m-1} - q^{\frac{2m-r-1}{2}}$	$\frac{1}{2}q^r(q-1)^2$
q^m	$q-1$

(I) If $a = b = 0$, then $\mathrm{wt}(c_{a,b,c}) = 0$ if $c = 0$ and q^m if $c \neq 0$. This means that there are $q-1$ codewords of weight q^m and 1 codeword of weight 0 in $\mathcal{C}_Q'$ for $a = b = 0$.

(II) If $a = 0$ and $b \neq 0$, then the number of x that $\mathrm{Tr}_{q^m/q}(bx) = c$ is q^{m-1}, so $\mathrm{wt}(c_{a,b,c}) = q^m - q^{m-1}$. This means all codewords that $a = 0$ and $b \neq 0$ in $\mathcal{C}_Q'$ are of weight $q^m - q^{m-1}$, whose number is $q^m(q-1)$.

(III) If $a \neq 0$, by Proposition 2, we see that $c_{a,b,c} = 0$ can only happen in the case that r is odd, q is even and $q^m = q^{m-1} - q^{m-\frac{r+1}{2}}$, i.e., $r = 1$ and $q = 2$. Hence $(a, b, c) \mapsto c_{a,b,c}$ is always injective and $\mathcal{C}_Q'$ has the desired length and dimension.

(1) Assume r is even. Suppose $a \neq 0$. If $\tilde{b}_j \neq 0$ for some $j > r$, then $\mathrm{wt}(c_{a,b,c}) = q^m - q^{m-1}$. There are $(q^m - q^r)(q-1)q$ codewords of this form in $\mathcal{C}_Q'$. Now if $b \in \mathbb{F}_{q^m}$ satisfying $\tilde{b}_j = 0$ for all $j > r$, the number of such b is q^r. For those b, take $\tilde{b} = (\tilde{b}_1, \cdots, \tilde{b}_r)$, then $b \mapsto \tilde{b}$ are one-to-one, $u(b) = u(\tilde{b})$ and

$$\mathrm{wt}(c_{a,b,c}) = \begin{cases} (q-1)(q^{m-1} - q^{\frac{2m-r-2}{2}}\varepsilon_Q), & \text{if } u(\tilde{b}) = ac, \\ q^m - q^{m-1} + q^{\frac{2m-r-2}{2}}\varepsilon_Q, & \text{if } u(\tilde{b}) \neq ac. \end{cases} \tag{18}$$

We call the first weight A and the second weight B.

(1a) Suppose $c = 0$. Then $\#\{\tilde{b} \in \mathbb{F}_q^r \mid u(\tilde{b}) = 0\} = q^{r-1} + q^{\frac{r-2}{2}}\varepsilon_Q$, so the number of (a, b, c) $(a \neq 0,\ c = 0)$ such that $\mathrm{wt}(c_{a,b,c}) = A$ is $(q-1)(q^{r-1} + (q-1)q^{\frac{r-2}{2}}\varepsilon_Q)$; $\#\{b \mid u(b) \neq 0\} = (q-1)(q^{r-1} - q^{\frac{r-2}{2}}\varepsilon_Q)$, so the number of (a, b, c) $(a \neq 0,\ c = 0)$ such that $\mathrm{wt}(c_{a,b,c}) = B$ is $(q-1)^2(q^{r-1} - q^{\frac{r-2}{2}}\varepsilon_Q)$.

(1b) Suppose $c \neq 0$. Then $\#\{\tilde{b} \in \mathbb{F}_q^r \mid u(b) = ac\} = q^{r-1} - q^{\frac{r-2}{2}}\varepsilon_Q$, so the number of (a, b, c) $(ac \neq 0)$ such that $\mathrm{wt}(c_{a,b,c}) = A$ is $(q-1)^2(q^{r-1} - q^{\frac{r-2}{2}}\varepsilon_Q)$; $\#\{\tilde{b} \in \mathbb{F}_q^r \mid u(\tilde{b}) \neq ac\} = q^r - q^{r-1} + q^{\frac{r-2}{2}}\varepsilon_Q$, so the number of (a, b, c) $(ac \neq 0)$ such that $\mathrm{wt}(c_{a,b,c}) = B$ is $(q-1)^2(q^r - q^{r-1} + q^{\frac{r-2}{2}}\varepsilon_Q)$.

Combine (I), (II), (1a) and (1b), then for the case r even, 1 codeword in $\mathcal{C}_Q'$ is of weight 0, $q-1$ codewords are of weight q^m, $(q-1)(q^{r-1} + (q-1)q^{\frac{r-2}{2}}\varepsilon_Q)$ codewords are of weight $A = (q-1)(q^{m-1} - q^{\frac{2m-r-2}{2}}\varepsilon_Q)$, $(q-1)^2(q^{r-1} - q^{\frac{r-2}{2}}\varepsilon_Q)$ codewords are of weight $B = q^m - q^{m-1} + q^{\frac{2m-r-2}{2}}\varepsilon_Q$ and $q^{m+2} - q^{r+2} + q^{r+1} - q$ are of weight $q^m - q^{m-1}$.

Now $\mathcal{C}'_Q$ is either a $[q^m, m+2, q^m - q^{m-1} - q^{\frac{2m-r-2}{2}}]_q$-code if $\varepsilon_Q = -1$ or a $[q^m, m+2, q^m - q^{m-1} - q^{\frac{2m-r}{2}} + q^{\frac{2m-r-2}{2}}]_q$-code if $\varepsilon_Q = 1$. In the first case,

$$g_k(n,d) = \sum_{i=0}^{m+1} \left\lceil \frac{d}{q^i} \right\rceil = q^m + 1 - \frac{q^{m-\frac{r}{2}} - 1}{q-1},$$

which equals $n = q^m$ if and only if $2m - r = 2$, i.e., $m = r = 2$. This is equivalent to $m = 2$ and $N_Q(0) = 1$ by Corollary 1. In the second case, $g_k(n,d) = q^m + 1 - q^{m-\frac{r}{2}}$ which is always $< q^m = n$.

(2A) Assume r is odd and q is even and $(r,q) \neq (1,2)$. For $a \neq 0$, the only case that $N_Q(a,b;-c) \neq q^{m-1}$ is when $\tilde{b}_r \neq 0$ and $\tilde{b}_j = 0$ for $j > r$. The number of such b is $q^{r-1}(q-1)$. Fix $a \in \mathbb{F}_q^*$ and b, as $x \mapsto x^2 + \tilde{b}_r x$ is $2:1$, when c passes through $\mathbb{F}_q$, $-ac + u(b)$ also passes through $\mathbb{F}_q$ and exactly half of them makes the equation $x^2 + \tilde{b}_r x = ac + u(b)$ solvable. Hence there are $\frac{1}{2}(q-1)^2 q^r$ codewords each of weight $q^m - q^{m-1} \pm q^{\frac{2m-r-1}{2}}$ by Proposition 2. Combining with (I) and (II), we get the weight distribution in this case.

(2B) Assume r is odd and q is odd. Suppose $a \neq 0$. We only need to consider the case that $\tilde{b}_j = 0$ for all $j > r$. All other codewords are of weight $q^m - q^{m-1}$. Suppose now that $\tilde{b}_j = 0$ for $j > r$, let $\tilde{b} = (\tilde{b}_1, \cdots, \tilde{b}_r)$, then $b \mapsto \tilde{b}$ is a bijection and $u(b) = u(\tilde{b})$. For those b,

$$\mathrm{wt}(c_{a,b,c}) = \begin{cases} q^m - q^{m-1}, & \text{if } u(\tilde{b}) = ac, \\ q^m - q^{m-1} - q^{\frac{2m-r-1}{2}} \varepsilon_Q & \text{if } u(\tilde{b}) - ac \in \mathbb{F}_q^{*2}, \\ q^m - q^{m-1} + q^{\frac{2m-r-1}{2}} \varepsilon_Q & \text{if } u(\tilde{b}) - ac \in \mathbb{F}_q^* \backslash \mathbb{F}_q^{*2}. \end{cases} \tag{19}$$

We call the second weight A and the third weight B.

(2Ba) Suppose $c = 0$. Then $\#\{\tilde{b} \in \mathbb{F}_q^r \mid u(\tilde{b}) = 0\} = q^{r-1}$, the number of (a,b,c) ($a \neq 0$, $c = 0$) such that $\mathrm{wt}(c_{a,b,c}) = q^m - q^{m-1}$ is $(q-1)q^{r-1}$; $\#\{\tilde{b} \in \mathbb{F}_q^r \mid u(\tilde{b}) \in \mathbb{F}_q^{*2}\} = \frac{q-1}{2}(q^{r-1} + q^{\frac{r-1}{2}} \varepsilon_Q)$, the number of (a,b,c) ($a \neq 0$, $c = 0$) such that $\mathrm{wt}(c_{a,b,c}) = A$ is $\frac{(q-1)^2}{2}(q^{r-1} + q^{\frac{r-1}{2}} \varepsilon_Q)$; $\#\{\tilde{b} \in \mathbb{F}_q^r \mid u(\tilde{b}) \in \mathbb{F}_q^* \backslash \mathbb{F}_q^{*2}\} = \frac{q-1}{2}(q^{r-1} - q^{\frac{r-1}{2}} \varepsilon_Q)$, the number of (a,b,c) ($a \neq 0$, $c = 0$) such that $\mathrm{wt}(c_{a,b,c}) = B$ is $\frac{(q-1)^2}{2}(q^{r-1} - q^{\frac{r-1}{2}} \varepsilon_Q)$.

(2Bb) Suppose $c \neq 0$. Then $\#\{\tilde{b} \mid u(\tilde{b}) = ac\} = q^{r-1} + q^{\frac{r-1}{2}} \varepsilon_Q \eta_q(ac)$, the number of (a,b,c) ($ac \neq 0$) such that $\mathrm{wt}(c_{a,b,c}) = q^r - q^{r-1}$ is

$$\sum_{a \in \mathbb{F}_q^*} \sum_{c \in \mathbb{F}_q^*} (q^{r-1} + q^{\frac{r-1}{2}} \varepsilon_Q \eta_q(ac)) = (q-1)^2 q^{r-1}.$$

The number

$$\#\{\tilde{b} \mid u(\tilde{b}) - ac \in \mathbb{F}_q^{*2}\} = \sum_{d \in \mathbb{F}_q^{*2}} (q^{r-1} + q^{\frac{r-1}{2}} \varepsilon_Q \eta_q(ac + d)),$$

and the number of (a,b,c) ($ac \neq 0$) such that $\mathrm{wt}(c_{a,b,c}) = A$ is

$$\sum_{a \in \mathbb{F}_q^*} \sum_{c \in \mathbb{F}_q^*} \sum_{d \in \mathbb{F}_q^{*2}} (q^{r-1} + q^{\frac{r-1}{2}} \varepsilon_Q \eta_q(ac + d)) = \frac{(q-1)^3}{2} q^{r-1} - \frac{(q-1)^2}{2} q^{\frac{r-1}{2}} \varepsilon_Q.$$

Here we use the fact

$$\sum_{a\in\mathbb{F}_q^*}\sum_{c\in\mathbb{F}_q^*}\sum_{d\in\mathbb{F}_q^{*2}}\eta_q(ac+d)=-\frac{1}{2}(q-1)^2.$$

The number

$$\#\{\tilde{b}\mid u(\tilde{b})-ac\in\mathbb{F}_q^*\backslash\mathbb{F}_q^{*2}\}=\sum_{d\in\mathbb{F}_q^*\backslash\mathbb{F}_q^{*2}}(q^{r-1}+q^{\frac{r-1}{2}}\varepsilon_Q\eta_q(ac+d)),$$

and the number of (a,b,c) $(ac\neq 0)$ such that $\mathrm{wt}(c_{a,b,c})=B$ is

$$\sum_{a\in\mathbb{F}_q^*}\sum_{c\in\mathbb{F}_q^*}\sum_{d\in\mathbb{F}_q^*\backslash\mathbb{F}_q^{*2}}(q^{r-1}+q^{\frac{r-1}{2}}\varepsilon_Q\eta_q(ac+d))=\frac{(q-1)^3}{2}q^{r-1}+\frac{(q-1)^2}{2}q^{\frac{r-1}{2}}\varepsilon_Q.$$

Combining (I), (II), (2Ba) and (2Bb), if q is even and $r\geq 3$ is odd, 1 codeword in $\mathcal{C}'_Q$ is of weight 0, $q-1$ codewords are of weight q^m, $\frac{1}{2}(q-1)^2q^r$ codewords are of weights $q^m-q^{m-1}\pm q^{\frac{2m-r-1}{2}}$ and $q^{m+2}-q^r(q-1)^2-q$ are of weight q^m-q^{m-1}. This is the same weight distribution for even q and odd r.

If $r\geq 3$, we get $g_q(n,d)=q^m+1-\frac{q^{m-\frac{r-1}{2}}-1}{q-1}<q^m$. If $r=1$, $g_q(n,d)=q^m+1-\frac{q^m-1}{q-1}$ which equals q^m if and only if $m=1$. In this case, $\mathcal{C}'_Q$ is a $[q,3,q-2]_q$-code, clearly an MDS code. □

Theorem 5. *Assume $Q(x):\mathbb{F}_{q^m}\to\mathbb{F}_q$ is a quadratic form and $r=m-\dim\mathrm{rad}(Q)$. Assume $(r,q)\neq(1,2)$.*

(1) *If r is even, then $\mathcal{C}_Q$ is a three-weight $[q^m-1,m+1]$ linear code with weight distribution given in Table 3. Moreover, the code $\mathcal{C}_Q$ is optimal with respect to the Griesmer bound if and only if $m=2$ and $N_Q(0)=1$, and in this case $\mathcal{C}_Q$ is a $[q^2-1,3,q^2-q-1]_q$-code whose weight enumerator is*

$$A_{\mathcal{C}_Q}(x)=1+(q+1)(q-1)^2x^{q^2-q-1}+(q^2-1)x^{q^2-q}+(q-1)x^{q^2-1}. \qquad (20)$$

TABLE 3. Weight distribution of $\mathcal{C}_Q$ for $2\mid r$

Weight i	*Frequency A_i*
0	*1*
q^m-q^{m-1}	$q^{m+1}-q^{r+1}+q^r-1$
$(q^{m-1}-\varepsilon_Q q^{\frac{m}{2}-1})(q-1)$	$(q-1)(q^{r-1}+\varepsilon_Q(q-1)q^{\frac{r-2}{2}})$
$q^m-q^{m-1}+\varepsilon_Q q^{\frac{m}{2}-1}$	$(q-1)^2(q^{r-1}-\varepsilon_Q q^{\frac{r-2}{2}})$

(2) *If $r\geq 3$ is odd, then $\mathcal{C}_Q$ is a three-weight $[q^m-1,m+1,q^m-q^{m-1}-q^{\frac{2m-r-1}{2}}]$ linear code with weight distribution given in Table 4. If $r=1$, then $\mathcal{C}_Q$ is a two-weight code whose weight enumerator is*

$$A_{\mathcal{C}_Q}(x)=1+(q-1)^2x^{q^m-2q^{m-1}}+(q^{m+1}-q^2+2q-2)x^{q^m-q^{m-1}}.$$

Moreover for odd r, $\mathcal{C}_Q$ satisfies the Griesmer bound if and only if $m=r=1$ (and $q>2$), in this case $\mathcal{C}_Q$ is a $[q-1,2,q-2]_q$ MDS code whose weight enumerator is

$$A_{\mathcal{C}_Q}(x)=1+(q^2-2q+1)x^{q-2}+(2q-2)x^{q-1}. \qquad (21)$$

TABLE 4. Weight distribution of $\mathcal{C}_Q$ for $r \geq 3$ odd

Weight i	*Frequency A_i*
0	*1*
$q^m - q^{m-1}$	$q^{m+1} - q^{r-1}(q-1)^2 - 1$
$q^m - q^{m-1} + q^{\frac{2m-r-1}{2}}$	$\frac{(q-1)^2}{2}(q^{r-1} - q^{\frac{r-1}{2}})$
$q^m - q^{m-1} - q^{\frac{2m-r-1}{2}}$	$\frac{(q-1)^2}{2}(q^{r-1} + q^{\frac{r-1}{2}})$

Proof. Note that $\mathrm{wt}(c_{a,b}) = \mathrm{wt}(c_{a,b,0})$. Except the case that r is odd and q is even (and $(r,q) \neq (1,2)$), all other cases have already been studied in the proof of Theorem 4. The case $r = 1$ is easy. We now assume $r \geq 3$ is odd and q is even.

Note that $\mathrm{wt}(c_{a,b}) = q^m - q^{m-1}$ if $\tilde{b}_r = 0$ or $\tilde{b}_j \neq 0$ for $j > r$. Now assume $\tilde{b}_r \neq 0$ and $\tilde{b}_j = 0$ for all $j > r$. Then by Proposition 2, $\mathrm{wt}(c_{a,b}) = q^m - q^{m-1} - \varepsilon_b q^{m-\frac{r+1}{2}}$ with $\varepsilon_b = 1$ (resp. -1) if $x^2 + \tilde{b}_r x = u(b) = u(\tilde{b}_1, \cdots, \tilde{b}_{r-1})$ is solvable (resp. non-solvable). Note that $x^2 + \tilde{b}_r x = 0$ is solvable, and the number of $(\tilde{b}_1, \cdots, \tilde{b}_{r-1})$ such that $u(b) = 0$ is $q^{r-2} + (q-1)q^{\frac{r-3}{2}}$ by Lemma 2. The number of $c \in \mathbb{F}_q^*$ such that $x^2 + \tilde{b}_r x = c$ is solvable is $\frac{q}{2} - 1$, and the number of $(\tilde{b}_1, \cdots, \tilde{b}_{r-1})$ such that $u(b) = c$ is $q^{r-2} - q^{\frac{r-3}{2}}$ by Lemma 2. Hence the number of (a,b) such that $\mathrm{wt}(c_{a,b}) = q^m - q^{m-1} - q^{m-\frac{r+1}{2}}$ is

$$(q-1)^2(q^{r-2} + (q-1)q^{\frac{r-3}{2}} + (\frac{q}{2} - 1)(q^{r-2} - q^{\frac{r-3}{2}})) = \frac{1}{2}(q-1)^2(q^{r-1} + q^{\frac{r-1}{2}}).$$

Then the number of (a,b) such that $\mathrm{wt}(c_{a,b}) = q^m - q^{m-1} + q^{m-\frac{r+1}{2}}$ is $\frac{1}{2}(q-1)^2(q^{r-1} - q^{\frac{r-1}{2}})$. Hence the weight distribution is the same as the q odd case.

If $r \geq 3$ is odd, we obtain $g_q(n,d) = q^m - \frac{q^{\frac{2m-r+1}{2}} - 1}{q-1} < q^m - 1$. If $r = 1$, $g_q(n,d) = q^m - \frac{q^m - 1}{q-1}$ which equals $q^m - 1$ if and only if $m = 1$. In this case, $\mathcal{C}_Q$ is an $[q-1, 2, q-2]_q$-code, clearly an MDS code. □

Remark 6. *One should note that some special quadratic forms have been used to construct linear codes defined in* (1), (2) *(see* [3, 12, 16, 25, 45, 46, 48, 49]*). For odd p and even m, it was shown in* [3, 25, 45, 46, 48, 49] *that $\tilde{C}_Q$ and $\tilde{C}'_Q$ are five- and six-weight. For $p = 2$, $Q(x) = x^{2^j+1} (j \geq 0)$, Ding et al.* [12] *showed that the code $\tilde{C}_Q$ has three weights if m is odd or m is even and $j = \frac{m}{2}$. Recently, for even m, Ding et al.* [9] *constructed and studied the binary linear codes defined in* (3), *and showed that it has four nonzero weights.*

Remark 7. *Let $\mathrm{wt}_{\min}$ and $\mathrm{wt}_{\max}$ denote the minimum and maximum Hamming weights of nonzero codewords in $\mathcal{C}'_Q$ or $\mathcal{C}_Q$, respectively. By Theorems 4 and 5, if $q > p$ and $r > 1$, then*

$$\frac{p-1}{p} < \frac{\mathrm{wt}_{\min}}{\mathrm{wt}_{\max}}.$$

Remark 8. *Replacing Q by an arbitrary vectorial function F, one can certainly construct linear codes $\mathcal{C}'_F$ and $\mathcal{C}_F$. It would be interesting to study the weight distribution of $\mathcal{C}'_F$ and $\mathcal{C}_F$ in general.*

Example 1. *Suppose $q=p^l$, $m=2$ and $Q(x)=x^{q+1}$. Clearly $N_Q(0)=1$. Thus by Theorems 4 and 5, $\mathcal{C}'_Q$ and $\mathcal{C}_Q$ are optimal codes over $\mathbb{F}_q$ with respect to the Griesmer bound.*

(1) Let $q=4$ and $Q(x)=x^5$. Then $\mathcal{C}'_Q$ is an optimal $[16,4,11]_4$ linear code with the weight enumerator $1+3x^{16}+60x^{12}+48x^{15}+144x^{11}$. The code $\mathcal{C}_Q$ is an optimal $[15,3,11]_4$ linear code with the weight enumerator $1+15x^{12}+3x^{15}+45x^{11}$.

(2) Let $q=25$ and $Q(x)=x^{26}$. Then the code $\mathcal{C}_Q$ is an optimal three-weight $[624,3,599]_{25}$ linear code with the enumerator $1+624x^{600}+24x^{624}+14976x^{599}$.

Example 2. *Let q be odd and $Q(x)=\mathrm{Tr}_{q^m/q}(x^2)$. Then $Q(x)$ is non-degenerate by Corollary 2.*

(1) If $m=2$, then $Q(x)=x^2+x^{2q}$. Then $Q(x)=0$ if either $x=0$ or $x^{2(q-1)}=-1$. The latter is solvable if and only if $q\equiv 3 \bmod 4$. Hence $N_Q(0)=1$ if and only if $q\equiv 1 \bmod 4$. In this case, then $\mathcal{C}_Q$ and $\mathcal{C}'_Q$ are optimal codes over $\mathbb{F}_q$.

(2) If $m=1$, then $\mathcal{C}_Q$ and $\mathcal{C}'_Q$ are MDS codes over $\mathbb{F}_q$.

4.1. **Descending $\mathbb{F}_q$-codes to $\mathbb{F}_p$-codes.** Suppose $q=p^l$. Given an $[n,k,d]$ $\mathbb{F}_q$-linear code, by regarding $\mathbb{F}_q$ as an l-dimensional $\mathbb{F}_p$-vector space, we can regard the code as an $[nl,kl]$ $\mathbb{F}_p$-linear code, however, the distance of the code is not specified. In this subsection, we give another method to descend an $\mathbb{F}_q$-code to an $\mathbb{F}_p$-code with parameters all determined.

Definition 5. *Assume $q=p^l$ and N is a factor of $p-1$ prime to $\frac{q-1}{p-1}$. Let θ be a primitive $\frac{q-1}{N}$-th root of unity in $\mathbb{F}_q$. Define the $\mathbb{F}_p$-linear map*

$$\Psi_N:\ \mathbb{F}_q\to\mathbb{F}_p^{\frac{q-1}{N}}=\mathbb{F}_p^{\frac{q-1}{N}\times 1},\ \gamma\mapsto\psi_\gamma=(\mathrm{Tr}_{q/p}(\gamma\theta^i))^T_{0\le i<\frac{q-1}{N}}.$$

The code $\mathcal{C}_N:=\mathrm{Im}\Psi_N$.

For a linear code $\mathcal{D}$ over $\mathbb{F}_q$ of length n, $\mathcal{D}_N$ is the linear code over $\mathbb{F}_p$:

$$\mathcal{D}_N:=\{(\psi_{c_1},\cdots,\psi_{c_n})_{1\le i\le n}\mid(c_1,\cdots,c_n)\in\mathcal{D}\}\subseteq\mathbb{F}_p^{\frac{(q-1)}{N}\times n}.$$

Note that $N=1$ if $p=2$. We have

Proposition 3. (1) *Ψ_N is injective and $\mathcal{C}_N$ is an $[\frac{q-1}{N},l,\frac{(p-1)p^{l-1}}{N}]$ constant-weight code over $\mathbb{F}_p$ whose weight enumerator is*

$$A_{\mathcal{C}_N}(x)=1+(q-1)x^{\frac{(p-1)p^{l-1}}{N}}.$$

(2) *If $\mathcal{D}$ is an $[n,k,d]$ linear code over $\mathbb{F}_q$, then $\mathcal{D}_N$ is an $[\frac{n(q-1)}{N},kl,\frac{d(p-1)p^{l-1}}{N}]$ linear code over $\mathbb{F}_p$ whose weight enumerator is*

$$A_{\mathcal{D}_N}(z)=A_{\mathcal{D}}(z^{\frac{(p-1)p^{l-1}}{N}}). \tag{22}$$

(3) *The equivalence of $\mathbb{F}_q$-linear code $\mathcal{D}$ is invariant under the action of linear map Ψ_N.*

Proof. (1) This is well-known, see for example [13].

(2) It is clear that $\mathcal{D}_N$ is an $[\frac{n(q-1)}{N},kl]$ linear code, as the map $c\mapsto(\psi_{c_1},\cdots,\psi_{c_n})$ is injective.

Suppose $c=(c_1,c_2,\dots,c_n)\in\mathcal{D}$ and $\mathrm{wt}(c)=i$. If $c_j=0$, certainly $\psi_{c_j}=0$. If $c_j\neq 0$, by (1), then

$$\mathrm{wt}(\psi_{c_j})=\mathrm{wt}(\mathrm{Tr}_{q/p}(c_j),\mathrm{Tr}_{q/p}(c_j\theta),\cdots,\mathrm{Tr}_{q/p}(c_j\theta^{\frac{q-1}{N}-1}))=\frac{(p-1)p^{l-1}}{N}.$$

Hence, $A_{\mathcal{D}_N}(z) = A_{\mathcal{D}}(z^{\frac{(p-1)p^{l-1}}{N}})$.

(3) Two $\mathbb{F}_q$-linear codes $\mathcal{D}$ and $\mathcal{D}'$ are equivalent if there exist a permutation π such that $\mathcal{D}' = \{\pi(c) : \ c \in \mathcal{D}\}$. Suppose $\mathcal{D}$ and $\mathcal{D}'$ are equivalent, then one has

$$\begin{tikzcd} \mathcal{D} \arrow[r, "\pi"] \arrow[d, "\Psi_N"] & \mathcal{D}' \arrow[d, "\Psi_N"'] \\ \mathcal{D}_N \arrow[r] & \mathcal{D}'_N \end{tikzcd}$$

Note that $\#\mathcal{D} = \#\mathcal{D}' = \#\mathcal{D}'_N = \#\mathcal{D}_N$, thus there is a permutation between $\mathcal{D}_N$ and $\mathcal{D}'_N$, the equivalence of $\mathcal{D}_N$ and $\mathcal{D}'_N$ can be obtained. $\square$

Let $\mathcal{C}_{Q,N} = (\mathcal{C}_Q)_N$ and $\mathcal{C}'_{Q,N} = (\mathcal{C}'_Q)_N$. Then we immediately have

Corollary 3. *Suppose Q is a non-degenerate quadratic form, N is a factor of $p-1$ prime to $\frac{q-1}{p-1}$. Then $\mathcal{C}_{Q,N}$ and $\mathcal{C}'_{Q,N}$ are optimal with respect to the Griesmer bound if $m = 2$ and $N_Q(0) = 1$ or if $m = r = 1$.*

One can write explicitly the corresponding parameters of $\mathcal{C}_{Q,N}$ and $\mathcal{C}'_{Q,N}$. In particular,

Example 3. *The code $\mathcal{C}'_{Q,1}$ in Example 1(1) is an $[48, 8, 22]_2$ binary code with the weight enumerator $1+3x^{32}+60x^{24}+48x^{30}+144x^{22}$, which has the same parameters with the best known codes in the Database* [17].

5. Conclusion

In this paper, we characterize the quadratic vectorial bent functions and in particular quadratic monomial vectorial bent functions. We construct two classes of linear codes with few weights from quadratic forms, determine their weight enumerators and the optimal codes inside these two classes. Moreover, it can be verified that the linear codes of this paper satisfy the condition of $\frac{\mathrm{wt}_{\min}}{\mathrm{wt}_{\max}} > \frac{p-1}{p}$, so they can be employed to obtain secret sharing schemes with interesting access structures.

References

[1] Carlet, C., Mesnager, S.: Four decades of research on bent functions. Des. Codes Cryptogr. **78**(1), 5-50 (2016)

[2] Carlet, C.: Boolean Functions for Cryptography and Coding Theory. Cambridge, U.K.: Cambridge Univ. Press (2021)

[3] Carlet, C., Ding, C., Yuan, J.: Linear codes from perfect nonlinear mappings and their secret sharing schemes. IEEE Trans. Inf. Theory **51**(6), 2089-2102 (2005)

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

[5] Calderbank, A., Kantor, W.: The geometry of two-weight codes. Bull. Lond. Math. Soc. **18**, 97-122 (1986)

[6] Çeşmelioğlu, A., Meidl, W., Pott, A.: Vectorial bent functions in odd characteristic and their components. Cryptogr. Commun. **12**, 899-912 (2020)

[7] Casselman, W.: Quadratic forms over finite fields. Accessed: April 1, 2018. [Online]. Available: *https://www.math.ubc.ca/ cass/research/pdf/FiniteFields.pdf*

[8] Ding, C.: A construction of binary linear codes from Boolean functions. Discrete Math. **339**, 2288-2303 (2016)

[9] Ding, C., Munemasa, A., Tonchev, V.: Bent vectorial functions, codes and designs. IEEE Trans. Inf. Theory **65**(11), 7533-7541 (2019)

[10] Ding, C., Wang, X.: A coding theory construction of new systematic authentication codes. Theor. Comput. Sci. **330**(1), 81-99 (2005)

[11] Ding, C.: Linear codes from some 2-designs. IEEE Trans. Inf. Theory **61**(6), 3265-3275 (2015)
[12] Ding, C., Li, N., Li, C., Zhou, Z.: Three-weight cyclic codes and their weight distributions. Discrete Math. **39**(2), 415-427 (2016)
[13] Ding, C., Yang, J.: Hamming weights in irreducible cyclic codes. Discrete Math. **313**, 434-446 (2013)
[14] Dong, D., Zhang, X., Qu, L., Fu, S.: A note on vectorial bent functions. Inf. Process. Lett. **113**(22), 866-870 (2013)
[15] Elman, R., Karpenko, N., Merkurjev, A.: The algebraic and geometric theory of quadratic forms. AMS Colloquium Publ. **56**. American Mathematical Society, Providence, RI (2008)
[16] Feng, K., Luo, J.: Value distributions of exponential sums from perfect nonlinear functions and their applications. IEEE Trans. Inf. Theory **53**(9), 3035-3041 (2007)
[17] Grassl, M.: Code Tables. Accessed: Feb. 13, 2019. [Online]. Available: *http://www.codetables.de/*.
[18] Griesmer, J.: A bound for error-correcting codes. IBM J. Res. Develop. **4**(5), 532-542 (1960)
[19] Helleseth, T., Kholosha, A.: Monomial and quadratic bent functions over the finite fields of odd characteristic. IEEE Trans. Inf. Theory **52**(5), 2018-2032 (2006)
[20] Helleseth, T., Kholosha, A.: On the dual of monomial quadratic p-ary bent functions. in Sequence, Subsequences and Consequences, S. Golomb, G. Gong, T. Helleseth and H. Song, Eds. Berlin: Springer-Verlag, **4893**, Lecture Notes in Computer Science, 50-61 (2007)
[21] Helleseth, T.: The weight enumerator polynomials of some classes of codes with composite party-check polynomials. Discrete math. **20**, 21-31 (1977)
[22] Heng, Z., Yue, Q.: Several classes of cyclic codes with either optimal three weights or a few weights. IEEE Trans. Inf. Theory **62**(8), 4501-4513 (2016)
[23] Lidl, R., Niederreiter, R.: Finite Fields. 2nd ed. Cambridge, U.K.: Cambridge Univ. Press (1997)
[24] Liu, L., Xie, X., Li, L., Zhu, S.: The weight distributions of two classes of nonbinary cyclic codes with few weights. IEEE Commun. Lett. **21**(11), 2336-2339 (2017)
[25] Li, C., Ling S., Qu, L.: On the covering structures of two classes of linear codes from perfect nonlinear functions. IEEE Trans. Inf. Theory **55**(1), 70-82 (2009)
[26] Li, C., Zeng, X., Hu, L.: A class of binary cyclic codes with five weights. Sci. China Math. **53**(2), 3279-3286 (2010)
[27] Luo, J., Feng, K.: On the weight distributions of two classes of cyclic codes. IEEE Trans. Inf. Theory **54**(12), 5332-5344, (2008)
[28] Mesnager, S.: Bent Functions: Fundamentals and Results. Switzerland, Springer (2016)
[29] Mesnager, S.: Linear codes with few weights from weakly regular bent functions based on a generic construction. Cryptogr. Commun. **9**(1), 71-84 (2017)
[30] Mesnager, S.: Several new infinite families of bent functions and their duals. IEEE Trans. Inf. Theory **60**(7), 4397-4407 (2014)
[31] Mesnager, S.: Bent vectorial functions and linear codes from o-polynomials. Des. Codes Cryptogr. **77**, 99-116 (2015)
[32] Mesnager, S., Sinak, A.: Several classes of minimal linear codes with few weights from weakly regular plateaued functions. IEEE Trans. Inf. Theory **66**(4), 2296-2310 (2020)
[33] Mesnager, S.: Linear codes from weakly regular plateaued functions and their secret sharing schemes. Des. Codes Cryptogr. **87**(2-3), 463-480 (2019)
[34] Mesnager, S.: Linear codes from functions. A Concise Encyclopedia of Coding Theory CRC Press/Taylor and Francis Group (Publisher), London, New York (2021)
[35] Pott, A., Pasalic, E., Muratovié, A., Bajrié, S.: On the maximum number of bent components of vectorial functions. IEEE Trans. Inf. Theory **64**(1), 403-411 (2018)
[36] Pless, V., Huffman, W.: Handbook of Coding Theory. Amsterdam, The Netherlands: North-Holland, **1**, (1998)
[37] Tang, D., Carlet, C., Zhou, Z.: Binary linear codes from vectorial boolean functions and their weight distribution. Discrete Math. **340**, 3055-3072 (2017)
[38] Tang, C., Zhou, Z., Qi, Y., Zhang, X., Fan, C., Helleseth, T.: Generic construction of bent functions and bent idempotents with any possible algebraic degrees. IEEE Trans. Inf. Theory **63**(10), 6149-6157 (2017)
[39] Tang, C., Li, N., Qi, Y., Zhou, Z., Helleseth, T.: Linear codes with two or three weights from weakly regular bent functions. IEEE Trans. Inf. Theory **62**(3), 1166-1176 (2016)

[40] Vega, G.: Two-weight cyclic codes constructed as the direct sum of two one-weight cyclic codes. Finite Fields Appl. **14**, 785-797 (2008)
[41] Vega, G.: A characterization of a class of optimal three-weight cyclic codes of dimension 3 over any finite field. Finite Fields Appl. **42**, 23-38 (2016)
[42] Wu, Y., Li, N., Zeng, X.: Linear codes from perfect nonlinear functions over finite fields. IEEE Trans. Inf. Theory **68**(1), 3-11 (2020)
[43] Wang, X., Zheng, D., Hu, L., Zeng, X.: The weight distributions of two classes of binary cyclic codes. Finite Fields Appl. **34**, 192-207 (2015)
[44] Xu, Y., Carlet, C., Mesnager, S., Wu, C.: Classification of bent monomials, constructions of bent monomials and upper bounds on the nonlinearity of vectorial functions. IEEE Trans. Inf. Theory **64**(1), 367-383 (2018)
[45] 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)
[46] 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)
[47] 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)
[48] Zeng, X., Hu, L., Jiang, W., Yue, Q., Cao, X.: Weight distribution of a p-ary cyclic codes. Finite Fields Appl. **16**, 56-73 (2010)
[49] Zheng, D., Wang, X., Hu, L., Zeng, X.: The weight distributions of two classes of p-ary cyclic codes. Finite Fields Appl. **29**, 202-224 (2014)

[1]School of Information and Computer, Anhui Agricultural University, Hefei, Anhui 230036, China
Email address: xianhxie@mail.ustc.edu.cn

[2]School of Mathematical Sciences, CAS Wu Wen-Tsun Key Laboratory of Mathematics, University of Science and Technology of China, Hefei, Anhui 230026, China

[3]Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, China
Email address: yiouyang@ustc.edu.cn

[4]Beijing Electronic Science and Technology Institute, Beijing 100070, China
Email address: maomingdky@163.com