Des. Codes Cryptogr. (2017) 83:691–714
DOI 10.1007/s10623-016-0267-7

Linear codes with few weights from inhomogeneous quadratic functions

Chunming Tang[1] · **Can Xiang**[2] · **Keqin Feng**[3]

Received: 20 March 2016 / Revised: 19 July 2016 / Accepted: 29 July 2016 /
Published online: 10 August 2016

Abstract Linear codes with few weights have been an interesting subject of study for many years, as these codes have applications in secrete sharing, authentication codes, association schemes, and strongly regular graphs. In this paper, linear codes with few weights are constructed from inhomogeneous quadratic functions over the finite field GF(p), where p is an odd prime. They include some earlier linear codes as special cases. The weight distributions of these linear codes are also determined.

Keywords Linear codes · Weight distribution · Quadratic forms · Cyclotomic fields

Mathematics Subject Classification 94A24 · 94B35 · 94B15 · 94A55

1 Introduction

Throughout this paper, let p be an odd prime and let $q = p^m$ for some positive integer m. An $[n, k, d]$ code C over GF(p) is a k-dimensional subspace of GF(p)^n with minimum (Hamming) distance d. Let A_i denote the number of codewords with Hamming weight i in a

Communicated by D. Jungnickel.

✉ Can Xiang
cxiangcxiang@hotmail.com

Chunming Tang
tangchunmingmath@163.com

Keqin Feng
kfeng@math.tsinghua.edu.cn

[1] School of Mathematics and Information, China West Normal University, Nanchong 637002, Sichuan, China

[2] College of Mathematics and Informatics, South China Agricultural University, Guangzhou 510642, China

[3] Department of Mathematical Sciences, Tsinghua University, Beijing 100084, China

code C of length n. The *weight enumerator* of C is defined by $1 + A_1z + A_2z^2 + \cdots + A_nz^n$. The *weight distribution* $(1, A_1, \ldots, A_n)$ is an important research topic in coding theory, as it contains crucial information as to estimate the error correcting capability and the probability of error detection and correction with respect to some algorithms. A code C is said to be a t-weight code if the number of nonzero A_i in the sequence $(A_1, A_2, \ldots, A_n)$ is equal to t.

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 error probability of error detection and correction with respect to some error detection and error correction algorithms (see [14] for details). Thus the study of the weight distribution attracts much attention in coding theory and much work focuses on the determination of the weight distributions of linear codes (see [4–7,9,11] and the references therein). Linear codes can be applied in consumer electronics, communication and data storage system. Linear codes with few weights are of important in secret sharing [3], authentication codes [8,10], association schemes [1] and strongly regular graphs [2].

Let Tr denote the trace function from $\mathrm{GF}(q)$ onto $\mathrm{GF}(p)$ throughout this paper. Let $F(x) \in \mathrm{GF}(q)[x]$, $D = \{x \in \mathrm{GF}(q)^* : \mathrm{Tr}(F(x)) = 0\} = \{d_1, d_2, \ldots, d_n\} \subseteq \mathrm{GF}(q)$ and $n = \#D$. We define a linear code of length n over $\mathrm{GF}(p)$ by

$$C_D = \{(\mathrm{Tr}(xd_1), \mathrm{Tr}(xd_2), \ldots, \mathrm{Tr}(xd_n)) : x \in \mathrm{GF}(q)\}, \tag{1}$$

and call D the *defining set* of this code C_D. By definition, the dimension of the code C_D is at most m.

This construction is generic in the sense that many classes of known codes could be produced by properly selecting the defining set $D \subseteq \mathrm{GF}(q)$. If the defining set D is well chosen, some optimal linear codes with few weights can be obtained. Based on this construction, many linear codes have been constructed since Ding et al. published their paper in 2014 [6]. We refer interested readers to [4,5,7,17–20,22] and the references therein. Particularly, Ding et al. [7] presented the weight distribution of C_D for the case $F(x) = x^2$ and proposed an open problem on how to determine the weight distribution of C_D for general planar functions $F(x)$. Subsequently, Zhou et al. [22] and Tang et al. [19] solved this open problem and gave the weight distribution of C_D from homogeneous quadratic bent functions and weakly regular bent functions with some homogeneous conditions, respectively.

In this paper, we consider linear codes with few weights from inhomogeneous quadratic functions $\mathrm{Tr}(F(x)) = f(x) - \mathrm{Tr}(\alpha x)$ and determine the weight distributions of these linear codes , where $\alpha \in \mathrm{GF}(q)^*$, $f(x)$ is a homogeneous quadratic function from $\mathrm{GF}(q)$ onto $\mathrm{GF}(p)$ and defined by

$$f(x) = \sum_{i=0}^{m-1} \mathrm{Tr}(a_i x^{p^i+1}) \quad (a_i \in \mathrm{GF}(q)). \tag{2}$$

They include some earlier linear codes as special cases [16,21].

The rest of this paper is organized as follows. Section 2 introduces some basic notations and results of group characters, Gauss sums, cyclotomic fields and quadratic forms which will be needed in subsequent sections. Section 3 constructs linear codes with a few weights from inhomogeneous quadratic functions and settles the weight distributions of these linear codes. Section 4 summarizes this paper.

2 Preliminaries

In this section, we state some notations and basic facts on group characters, Gauss sums, cyclotomic fields and quadratic forms. These results will be used in the rest of the paper.

2.1 Some notations fixed throughout this paper

For convenience, we adopt the following notations unless otherwise stated in this paper.

- $p^* = (-1)^{(p-1)/2}p$.
- $\zeta_p = e^{\frac{2\pi\sqrt{-1}}{p}}$ is the primitive p-th root of unity.
- SQ and NSQ denote the set of all squares and nonsquares in $\mathrm{GF}(p)^*$, respectively.
- η and $\bar{\eta}$ are the quadratic characters of $\mathrm{GF}(q)^*$ and $\mathrm{GF}(p)^*$, repsectively. We extend these quadratic characters by letting $\eta(0) = 0$ and $\bar{\eta}(0) = 0$.

2.2 Group characters and Gauss sums

An *additive character* of $\mathrm{GF}(q)$ is a nonzero function χ from $\mathrm{GF}(q)$ to the set of nonzero complex numbers such that $\chi(x + y) = \chi(x)\chi(y)$ for any pair $(x, y) \in \mathrm{GF}(q)^2$. For each $b \in \mathrm{GF}(q)$, the function

$$\chi_b(c) = \zeta_p^{\mathrm{Tr}(bc)} \quad \text{for all } c \in \mathrm{GF}(q) \tag{3}$$

defines an additive character of $\mathrm{GF}(q)$. When $b = 0$, $\chi_0(c) = 1$ for all $c \in \mathrm{GF}(q)$, and is called the *trivial additive character* of $\mathrm{GF}(q)$. The character χ_1 in (3) is called the *canonical additive character* of $\mathrm{GF}(q)$. It is well known that every additive character of $\mathrm{GF}(q)$ can be written as $\chi_b(x) = \chi_1(bx)$ [15, Theorem 5.7].

The Gauss sum $G(\eta, \chi_1)$ over $\mathrm{GF}(q)$ is defined by

$$G(\eta, \chi_1) = \sum_{c\in\mathrm{GF}(q)^*} \eta(c)\chi_1(c) = \sum_{c\in\mathrm{GF}(q)} \eta(c)\chi_1(c) \tag{4}$$

and the Gauss sum $G(\bar{\eta}, \bar{\chi}_1)$ over $\mathrm{GF}(p)$ is defined by

$$G(\bar{\eta}, \bar{\chi}_1) = \sum_{c\in\mathrm{GF}(p)^*} \bar{\eta}(c)\bar{\chi}_1(c) = \sum_{c\in\mathrm{GF}(p)} \bar{\eta}(c)\bar{\chi}_1(c), \tag{5}$$

where $\bar{\chi}_1$ is the canonical additive characters of $\mathrm{GF}(p)$.

The following three lemmas are proved in [15, Theorems 5.15 and 5.33] and [7, Lemma 7], respectively.

Lemma 1 *With the symbols and notations above, we have*

$$G(\eta, \chi_1) = (-1)^{m-1}\sqrt{-1}^{(\frac{p-1}{2})^2 m}\sqrt{q}$$

and

$$G(\bar{\eta}, \bar{\chi}_1) = \sqrt{-1}^{(\frac{p-1}{2})^2}\sqrt{p} = \sqrt{p*}.$$

Lemma 2 *Let χ be a nontrivial additive character of* $\mathrm{GF}(q)$ *with q odd, and let $f(x) = a_2x^2 + a_1x + a_0 \in \mathrm{GF}(q)[x]$ with $a_2 \neq 0$. Then*

$$\sum_{c\in\mathrm{GF}(q)} \chi(f(c)) = \chi(a_0 - a_1^2(4a_2)^{-1})\,\eta(a_2)G(\eta, \chi).$$

2.3 Cyclotomic fields

In this subsection, we state some basic facts on cyclotomic fields. These results will be used in the rest of this paper.

Let $\mathbb{Z}$ be the rational integer ring and Q be the rational field. Some results on cyclotomic field $Q(\zeta_p)$ [13] are given in the following lemma.

Lemma 3 *We have the following basic facts.*

(1) *The ring of integers in $K = Q(\zeta_p)$ is $O_K = \mathbb{Z}(\zeta_p)$ and $\{\zeta_p^i : 1 \leq i \leq p-1\}$ is an integral basis of O_K.*
(2) *The field extension K/Q is Galois of degree $p-1$ and the Galois group $Gal(K/Q) = \{\sigma_a : a \in (\mathbb{Z}/p\mathbb{Z})^*\}$, where the automorphism σ_a of K is defined by $\sigma_a(\zeta_p) = \zeta_p^a$.*
(3) *The field K has a unique quadratic subfield $L = Q(\sqrt{p^*})$. For $1 \leq a \leq p-1$, $\sigma_a(\sqrt{p^*}) = \bar{\eta}(a)\sqrt{p^*}$. Therefore, the Galois group $Gal(L/Q)$ is $\{1, \sigma_\gamma\}$, where γ is any quadratic nonresidue in* GF(p).

From Lemma 3, the conclusion of the following lemma is straightforward and we omit their proofs.

Lemma 4 *With the symbols and notations above, we have the following.*

(I) $\sum_{y\in \mathrm{GF}(p)^*} \sigma_y((p^*)^{-\frac{r}{2}}) = \begin{cases} 0 & \text{if } r \text{ is odd}, \\ (p^*)^{-\frac{r}{2}}(p-1) & \text{if } r \text{ is even}. \end{cases}$
(II) *For any $z \in \mathrm{GF}(p)^*$, then*

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

2.4 Quadratic forms

The field GF(q) is a vector space over GF(p) with dimension m. We fix a basis $v_0, v_1, \ldots, v_{m-1}$ of GF(q) over GF(p). Then each $x \in \mathrm{GF}(q)$ can be uniquely expressed as

$$x = x_0v_0 + x_1v_1 + \cdots + x_{m-1}v_{m-1} \quad (x_i \in \mathrm{GF}(p)).$$

Thus we have the following GF(p)-linear isomorphism $\mathrm{GF}(q) \xrightarrow{\sim} \mathrm{GF}(p)^m$:

$$x = x_0v_0 + x_1v_1 + \cdots + x_{m-1}v_{m-1} \mapsto X = (x_0, x_1, \ldots, x_{m-1}).$$

With this isomorphism, a function $f : \mathrm{GF}(q) \to \mathrm{GF}(p)$ induces a function $F : \mathrm{GF}(p)^m \to \mathrm{GF}(p)$ where for all $X = (x_0, x_1, \ldots, x_{m-1}) \in \mathrm{GF}(p)^m$, $F(X) = f(x)$ where $x = x_0v_0 + x_1v_1 + \cdots + x_{m-1}v_{m-1}$. In this way, the function f defined in (2) induces a quadratic form

$$\begin{aligned} F(X) &= \sum_{i=0}^{m-1} \mathrm{Tr}\left(a_i \left(\sum_{j=0}^{m-1} x_j v_j \right)^{p^i+1} \right) \\ &= \sum_{i=0}^{m-1} \mathrm{Tr}\left(a_i \left(\sum_{j=0}^{m-1} x_j v_j^{p^i} \right) \left(\sum_{k=0}^{m-1} x_k v_k \right) \right) \\ &= \sum_{j=0}^{m-1} \sum_{k=0}^{m-1} \left(\sum_{i=0}^{m-1} \mathrm{Tr}\left(a_i v_j^{p^i} v_k \right) \right) x_j x_k \\ &= XHX^T, \end{aligned} \tag{6}$$

where X^T is the transposition of X, $H = (h_{j,k})$,

$$h_{j,k} = \frac{1}{2} \sum_{i=0}^{m-1} \left(\mathrm{Tr}\left(a_i \left(v_j^{p^i} v_k + v_j v_k^{p^i} \right) \right) \right) \quad \text{for } 0 \leq \mathrm{j, k} \leq \mathrm{m} - 1,$$

and the rank of H is called the rank of the function f defined in (2). We denote the rank of f by r_f. Particularly, $r_f = m$ if and only if f is a bent function.

Since H defined in (6) is an $m \times m$ symmetric matrix over GF(p) and $r_f = \text{rank } H$, there exists $M \in \mathrm{GL}_m(\mathrm{GF}(p))$ such that $H' = MHM^T$ is a diagonal matrix and

$$H' = diag(\lambda_1, \ldots, \lambda_{r_f}, 0, \ldots, 0)$$

where $\lambda_i \in \mathrm{GF}(p)^*(1 \leq i \leq r_f)$. Let $\Delta = \lambda_1, \ldots, \lambda_{r_f}$. Then the value of $\bar{\eta}(\Delta)$ is an invariant of H under the action of $H \mapsto MHM^T$ where $M \in \mathrm{GL}_m(\mathrm{GF}(p))$. We call $\bar{\eta}(\Delta)$ the sign of the quadratic function f of (2) and is defined by ε_f.

It is clear that the value of r_f is closely related to the value of $\#Z_f$, where the set

$$Z_f = \{x \in \mathrm{GF}(q) : f(x+y) = f(x) + f(y), \forall y \in \mathrm{GF}(q)\}.$$

It is well known that $\#Z_f = p^{m-r_f}$. Note that from Eq. (2) we have

$$f(x+y) = f(x) + f(y) + 2\mathrm{Tr}(L_f(x)y) = f(x) + f(y) + 2\mathrm{Tr}(xL_f(y)), \tag{7}$$

where L_f is a linearized polynominal over GF(q) defined by

$$L_f(x) = \frac{1}{2} \sum_{i=0}^{m-1} \left(a_i + a_{m-i}^{p^i} \right) x^{p^i}.$$

From now on we define $\mathrm{Im}(L_f) = \{L_f(x) : x \in \mathrm{GF}(q)\}$ and $\mathrm{Ker}(L_f) = \{x \in \mathrm{GF}(q) : L_f(x) = 0\}$. If $b \in \mathrm{Im}(L_f)$, we denote $x_b \in \mathrm{GF}(q)$ with satisfying $L_f(x_b) = -\frac{b}{2}$.

From Eq. (7), we have

$$\ker(L_f) = \{x \in \mathrm{GF}(q) : f(x+y) = f(x) + f(y) \text{ for all } y \in \mathrm{GF}(q)\}.$$

Thus $p^{m-r_f} = \#Z_f = \#\mathrm{Ker}(L_f)$, that is, rank $L_f = r_f$. It is obvious that $0 \leq r_f \leq m$.

3 Linear codes from inhomogeneous quadratic functions

We construct linear codes over GF(p) by using inhomogeneous quadratic functions and determine their parameters in this section.

In this paper, the defining set D of the code C_D of (1) is given by

$$D=\{x\in \mathrm{GF}(q)^*:f(x)-\mathrm{Tr}(\alpha x)=0\}, \tag{8}$$

where $\alpha\in\mathrm{GF}(q)^*$ and f is defined in (2). It is clear that the function $f(x)-\mathrm{Tr}(\alpha x)$ used in the defining set D is a inhomogeneous quadratic functions.

Before giving and proving the main results of this paper, we firstly prove a few more auxiliary results which will be needed in proving the main results.

3.1 Some auxiliary results

To prove our main results in this paper, we need the help of a number of lemmas that are described and proved in this subsection.

Lemma 5 *Let the symbols and notations be as above. Let f be a homogeneous quadratic function and $b\in\mathrm{GF}(q)$. Then*

(I) $\sum_{x\in\mathrm{GF}(q)}\zeta_p^{f(x)}=\varepsilon_f p^m (p^*)^{-\frac{r_f}{2}}$ *and*

(II) $\sum_{x\in\mathrm{GF}(q)}\zeta_p^{f(x)-\mathrm{Tr}(bx)}=\begin{cases}0 & \textit{if } b\notin\mathrm{Im}(L_f)\\ \varepsilon_f p^m(p^*)^{-\frac{r_f}{2}}\zeta_p^{-f(x_b)} & \textit{if } b\in\mathrm{Im}(L_f)\end{cases},$

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

Proof (I) The desired conclusion (I) of this lemma then follows from [12, Lemma 1].
(II) If $b\notin\mathrm{Im}(L_f)$, then we have

$$\begin{aligned}
&\left(\sum_{x\in\mathrm{GF}(q)}\zeta_p^{-f(x)}\right)\left(\sum_{y\in\mathrm{GF}(q)}\zeta_p^{f(y)-\mathrm{Tr}(by)}\right)\\
&=\sum_{x\in\mathrm{GF}(q)}\zeta_p^{-f(x)}\sum_{y\in\mathrm{GF}(q)}\zeta_p^{f(x+y)-\mathrm{Tr}(b(x+y))}\\
&=\sum_{x,y\in\mathrm{GF}(q)}\zeta_p^{f(x+y)-f(x)-\mathrm{Tr}(b(x+y))}\\
&=\sum_{x,y\in\mathrm{GF}(q)}\zeta_p^{f(y)+2\mathrm{Tr}(L_f(y)x)-\mathrm{Tr}(b(x+y))} \qquad \text{(By Eq. 7)}\\
&=\sum_{y\in\mathrm{GF}(q)}\zeta_p^{f(y)-\mathrm{Tr}(by)}\sum_{x\in\mathrm{GF}(q)}\zeta_p^{\mathrm{Tr}((L_f(2y)-b)x)}\\
&=0. \qquad \text{(Since } b\notin\mathrm{Im}(L_f))
\end{aligned}$$

From the conclusion (I) of this lemma, we have $\sum_{x\in\mathrm{GF}(q)}\zeta_p^{-f(x)}\neq 0$. Therefore, $\sum_{y\in\mathrm{GF}(q)}\zeta_p^{f(y)-\mathrm{Tr}(by)}=0$.

If $b \in \mathrm{Im}(L_f)$, then there exists $x_b \in \mathrm{GF}(q)$ such that $L_f(x_b) = -\frac{b}{2}$. Thus, we have

$$\begin{aligned}\sum_{x \in \mathrm{GF}(q)} \zeta_p^{f(x)-\mathrm{Tr}(bx)} &= \sum_{x \in \mathrm{GF}(q)} \zeta_p^{f(x)+2\mathrm{Tr}(L_f(x_b)x)} \\ &= \sum_{x \in \mathrm{GF}(q)} \zeta_p^{f(x)+f(x_b)+2\mathrm{Tr}(L_f(x_b)x)-f(x_b)} \\ &= \zeta_p^{-f(x_b)} \sum_{x \in \mathrm{GF}(q)} \zeta_p^{f(x+x_b)} \qquad \text{(By Eq. 7)} \\ &= \zeta_p^{-f(x_b)} \sum_{x \in \mathrm{GF}(q)} \zeta_p^{f(x)} \\ &= \varepsilon_f p^m (p^*)^{-\frac{r_f}{2}} \zeta_p^{-f(x_b)}. \qquad \text{(By the conclusion (I) of this lemma)}\end{aligned}$$

Summarizing all the conclusions above completes the proof of this lemma. □

Lemma 6 *Let $a, b, c \in \mathrm{GF}(p)$ and*

$$S = \sum_{z,w \in \mathrm{GF}(p)} \zeta_p^{az^2+2bzw+cw^2}.$$

Then we have the following.

(I) *If $ac - b^2 \neq 0$, then $S = \bar{\eta}(ac - b^2)p^2(p^*)^{-1}$.*
(II) *If $ac - b^2 = 0$ and $a \neq 0$, then $S = \bar{\eta}(a)p\sqrt{p^*}$.*

Proof (I) The desired conclusion (I) of this lemma then follows from [12, Lemma 1].
(II) If $ac - b^2 = 0$ and $a \neq 0$, then

$$S = \sum_{z,w \in \mathrm{GF}(p)} \zeta_p^{\frac{1}{a}(az+bw)^2} = \sum_{w \in \mathrm{GF}(p)} \sum_{z \in \mathrm{GF}(p)} \zeta_p^{\frac{1}{a}(az+bw)^2} = \sum_{w \in \mathrm{GF}(p)} \sum_{z \in \mathrm{GF}(p)} \zeta_p^{z^2} = \bar{\eta}(a)p\sqrt{p^*},$$

where the last identity follows from Lemmas 1 and 2. This completes the proof of this lemma. □

We require the following lemma which is the standard result on quadratic forms [15, Sect. 6.2].

Lemma 7 *Let g be a homogeneous quadratic function from* $\mathrm{GF}(q)$ *onto* $\mathrm{GF}(p)$ *with the rank r_g and the sign ε_g. For any $t \in \mathrm{GF}(p)^*$, let*

$$N(g = t) = \#\{x \in \mathrm{GF}(q) : g(x) = t\}.$$

Then

$$N(g = t) = \begin{cases} p^{m-1} - \varepsilon_g p^{m-1}(p^*)^{-\frac{r_g}{2}} & if r_g\ is\ even, \\ p^{m-1} + \varepsilon_g \bar{\eta}(-t) p^{m-1}(p^*)^{-\frac{r_f-1}{2}} & if r_g\ is\ odd. \end{cases}$$

Lemma 8 *Let f be a homogeneous quadratic function with the rank r_f and the sign ε_f, $\alpha \in \mathrm{Im}(L_f)$ and $x_\alpha \in \mathrm{GF}(q)$ with satisfying $L_f(x_\alpha) = -\frac{\alpha}{2}$. Let $f(x_\alpha) = 0$ and*

$$A = \#\{x \in \mathrm{GF}(q) : f(x) = a \text{ and } \mathrm{Tr}(\alpha x) = 0\}$$

for any $a \in \mathrm{GF}(p)^*$. Then

$$A = p^{m-2} + \varepsilon_f \bar{\eta}(-a) p^{m-1}(p^*)^{-\frac{r_f-1}{2}}.$$

Proof By definition, we have

$$\begin{aligned}
A &= p^{-2}\sum_{x\in\mathrm{GF}(q)}\left(\sum_{y\in\mathrm{GF}(p)}\zeta_p^{y(f(x)-a)}\right)\left(\sum_{z\in\mathrm{GF}(p)}\zeta_p^{z\mathrm{Tr}(\alpha x)}\right)\\
&= p^{-2}\sum_{x\in\mathrm{GF}(q)}\left(\sum_{z\in\mathrm{GF}(p)}\zeta_p^{z\mathrm{Tr}(\alpha x)}\right)+p^{-2}\sum_{y\in\mathrm{GF}(p)^*}\left(\sum_{z\in\mathrm{GF}(p)}\sum_{x\in\mathrm{GF}(q)}\zeta_p^{y(f(x)-a)+z\mathrm{Tr}(\alpha x)}\right)\\
&= p^{m-2}+p^{-2}\sum_{y\in\mathrm{GF}(p)^*}\sigma_y\left(\sum_{z\in\mathrm{GF}(p)}\zeta_p^{-a}\sum_{x\in\mathrm{GF}(q)}\zeta_p^{f(x)+z\mathrm{Tr}(\alpha x)}\right)\\
&= p^{m-2}+p^{-2}\sum_{y\in\mathrm{GF}(p)^*}\sigma_y\left(\zeta_p^{-a}\sum_{z\in\mathrm{GF}(p)}\zeta_p^{-f(x_\alpha)z^2}\varepsilon_f p^m(p^*)^{-\frac{r_f}{2}}\right) \qquad \text{(By Lemma 5)}\\
&= p^{m-2}+p^{-2}\sum_{y\in\mathrm{GF}(p)^*}\sigma_y\left(\zeta_p^{-a}\varepsilon_f p^{m+1}(p^*)^{-\frac{r_f}{2}}\right) \qquad \text{(Since } f(x_\alpha)=0\text{)}\\
&= p^{m-2}+p^{-2}\bar{\eta}(-a)\varepsilon_f p^{m+1}(p^*)^{-\frac{r_f-1}{2}})\\
&= p^{m-2}+\varepsilon_f\bar{\eta}(-a)p^{m-1}(p^*)^{-\frac{r_f-1}{2}}.
\end{aligned}$$

This completes the proof. □

Lemma 9 *Let the symbols and notations be as above. Let f be a homogeneous quadratic function, $\alpha\in\mathrm{GF}(q)$ and*

$$N_f(\alpha)=\#\{x\in\mathrm{GF}(q):f(x)-\mathrm{Tr}(\alpha x)=0\}.$$

Then we have the following.

(I) *If $\alpha\notin\mathrm{Im}(L_f)$, then $N_f(\alpha)=p^{m-1}$.*
(II) *If $\alpha\in\mathrm{Im}(L_f)$, then*

$$N_f(\alpha)=\begin{cases}
p^{m-1}+\varepsilon_f(p-1)p^{m-1}(p^*)^{-\frac{r_f}{2}} & \text{if } r_f \text{ is even and } f(x_\alpha)=0,\\
p^{m-1}-\varepsilon_f p^{m-1}(p^*)^{-\frac{r_f}{2}} & \text{if } r_f \text{ is even and } f(x_\alpha)\neq 0,\\
p^{m-1} & \text{if } r_f \text{ is odd and } f(x_\alpha)=0,\\
p^{m-1}+1+\varepsilon_f\bar{\eta}(-f(x_\alpha))p^{m-1}(p^*)^{-\frac{r_f-1}{2}} & \text{if } r_f \text{ is odd and } f(x_\alpha)\neq 0,
\end{cases}$$

where x_α satisfies $L_f(x_\alpha)=-\frac{\alpha}{2}$, r_f is the rank of f and ε_f is the sign of f.

Proof By definition, we have

$$\begin{aligned}
N_f(\alpha) &= p^{-1}\sum_{x\in\mathrm{GF}(q)}\sum_{y\in\mathrm{GF}(p)}\zeta_p^{y(f(x)-\mathrm{Tr}(\alpha x))}\\
&= p^{m-1}+p^{-1}\sum_{y\in\mathrm{GF}(p)^*}\sigma_y\left(\sum_{x\in\mathrm{GF}(q)}\zeta_p^{f(x)-\mathrm{Tr}(\alpha x)}\right).
\end{aligned}$$

The desired conclusions then follow from Lemma 4 and the result (II) of Lemma 5. □

Lemma 10 *Let the symbols and notations be as above. Let f be a homogeneous quadratic function with the rank r_f and the sign ε_f, $\beta \in \mathrm{GF}(q)^*$ and*

$$S_1 = \sum_{z\in \mathrm{GF}(p)} \sum_{x\in \mathrm{GF}(q)} \zeta_p^{-z\mathrm{Tr}(\beta x)},$$

$$S_2 = \sum_{z\in \mathrm{GF}(p)} \sum_{x\in \mathrm{GF}(q)} \zeta_p^{f(x)-z\mathrm{Tr}(\beta x)},$$

$$S_3 = \sum_{y\in \mathrm{GF}(p)^*} \sigma_y \left(\sum_{z\in \mathrm{GF}(p)} \sum_{x\in \mathrm{GF}(q)} \zeta_p^{f(x)-z\mathrm{Tr}(\beta x)} \right).$$

Then we have the following:

(I) $S_1 = q$,

(II) $$S_2 = \begin{cases} \varepsilon_f p^{m+1}(p^*)^{-\frac{r_f}{2}} & \text{if} \beta \in \mathrm{Im}(L_f) \mathit{and}\ f(x_\beta) = 0 \\ \varepsilon_f \bar{\eta}(-f(x_\beta)) p^m (p^*)^{-\frac{r_f-1}{2}} & \text{if} \beta \in \mathrm{Im}(L_f) \mathit{and}\ f(x_\beta) \neq 0 \\ \varepsilon_f p^m (p^*)^{-\frac{r_f}{2}} & \text{if} \beta \notin \mathrm{Im}(L_f) \end{cases},$$

(III) *if r_f is even, then*

$$S_3 = \begin{cases} \varepsilon_f (p-1) p^{m+1}(p^*)^{-\frac{r_f}{2}} & \mathit{if} \beta\ \in\ \mathrm{Im}(L_f)\ \mathit{and}\ f(x_\beta) = 0, \\ 0 & \mathit{if}\ \beta\ \in\ \mathrm{Im}(L_f)\ \mathit{and}\ f(x_\beta) \neq 0, \\ \varepsilon_f (p-1) p^m (p^*)^{-\frac{r_f}{2}} & \mathit{if}\ \beta \notin \mathrm{Im}(L_f), \end{cases}$$

if r_f is odd, then

$$S_3 = \begin{cases} 0 & \mathit{if}\ \beta\ \in\ \mathrm{Im}(L_f)\ \mathit{and}\ f(x_\beta) = 0, \mathit{or} \beta \notin \mathrm{Im}(L_f), \\ \varepsilon_f \bar{\eta}(-f(x_\beta))(p-1) p^m (p^*)^{-\frac{r_f-1}{2}} & \mathit{if} \beta\ \in\ \mathrm{Im}(L_f)\ \mathit{and}\ f(x_\beta) \neq 0. \end{cases}$$

where $x_\beta \in \mathrm{GF}(q)$ satisfies $L_f(x_\beta) = -\frac{\beta}{2}$ when $\beta \in \mathrm{Im}(L_f)$.

Proof (I) Note that

$$\sum_{z\in \mathrm{GF}(p)^*} \sum_{x\in \mathrm{GF}(q)} \zeta_p^{\mathrm{Tr}(-z\beta x)} = 0,$$

as $\beta \in \mathrm{GF}(q)^*$. Therefore, we have

$$\begin{aligned} S_1 &= \sum_{x\in \mathrm{GF}(q)} \zeta_p^0 + \sum_{z\in \mathrm{GF}(p)^*} \sum_{x\in \mathrm{GF}(q)} \zeta_p^{-z\mathrm{Tr}(\beta x)} \\ &= q. \end{aligned}$$

(II) By definitions and Part (II) of Lemma 5, we have

$$S_2 = \begin{cases} \sum_{z\in \mathrm{GF}(p)} \varepsilon_f p^m (p^*)^{-\frac{r_f}{2}} \zeta_p^{-f(x_\beta)z^2} & \text{if } \beta \in \mathrm{Im}(L_f), \\ \sum_{x\in \mathrm{GF}(q)} \zeta_p^{f(x)} & \text{if } \beta \notin \mathrm{Im}(L_f). \end{cases}$$

The desired conclusion (II) of this lemma then follows from Lemmas 1 and 2 and Part (I) of Lemma 5.

(III) The desired conclusion then follows directly from Lemma 4 and the result (II) of this lemma.

This completes the proof. □

Lemma 11 *Let the symbols and notations be as above. Let f be a homogeneous quadratic function with rank r_f and the sign ε_f, $\beta \in \mathrm{GF}(q)^*$ and*

$$N_{f,\beta} = \#\{x \in \mathrm{GF}(q) : f(x) = 0 \textit{ and } \mathrm{Tr}(\beta x) = 0\}.$$

Then, for the case r_f being even, we have

$$N_{f,\beta} = \begin{cases} p^{m-2} + \varepsilon_f (p-1) p^{m-1} (p^*)^{-\frac{r_f}{2}} & \textit{if } \beta \in \mathrm{Im}(L_f) \textit{ and } f(x_\beta) = 0, \\ p^{m-2} & \textit{if } \beta \in \mathrm{Im}(L_f) \textit{ and } f(x_\beta) \neq 0, \\ p^{m-2} + \varepsilon_f (p-1) p^{m-2} (p^*)^{-\frac{r_f}{2}} & \textit{if } \beta \notin \mathrm{Im}(L_f), \end{cases}$$

and for the case r_f being odd, we have

$$N_{f,\beta} = \begin{cases} p^{m-2} & \textit{if } \beta \in \mathrm{Im}(L_f) \textit{ and } f(x_\beta) = 0, \textit{or} \beta \notin \mathrm{Im}(L_f), \\ p^{m-2} + \varepsilon_f \bar{\eta}(-f(x_\beta))(p-1) p^{m-2} (p^*)^{-\frac{r_f - 1}{2}} & \textit{if } \beta \in \mathrm{Im}(L_f) \textit{ and } f(x_\beta) \neq 0, \end{cases}$$

where $x_\beta \in \mathrm{GF}(q)$ satisfies $L_f(x_\beta) = -\frac{\beta}{2}$ when $\beta \in \mathrm{Im}(L_f)$.

Proof By definition, we have

$$\begin{aligned} N_{f,\beta} &= p^{-2} \sum_{x \in \mathrm{GF}(q)} \left(\sum_{y \in \mathrm{GF}(p)} \zeta_p^{y f(x)} \right) \left(\sum_{z \in \mathrm{GF}(p)} \zeta_p^{-z \mathrm{Tr}(\beta x)} \right) \\ &= p^{-2} \left(\sum_{z \in \mathrm{GF}(p)} \sum_{x \in \mathrm{GF}(q)} \zeta_p^{-z \mathrm{Tr}(\beta x)} + \sum_{y \in \mathrm{GF}(p)^*} \sigma_y \left(\sum_{z \in \mathrm{GF}(p)} \sum_{x \in \mathrm{GF}(q)} \zeta_p^{f(x) - z \mathrm{Tr}(\beta x)} \right) \right). \end{aligned}$$

The desired conclusion then follows from Lemma 10. □

Lemma 12 *Let f be a homogeneous quadratic function with the rank r_f and the sign ε_f, $\alpha \in \mathrm{GF}(q) \backslash \mathrm{Im}(L_f)$ and $\beta \in \mathrm{GF}(q)^*$. Then we have the following.*

- *There exists $z_0 \in \mathrm{GF}(p)^*$ such that $\alpha - z_0 \beta \in \mathrm{Im}(L_f)$ if and only if $\beta \in \bigcup_{z \in \mathrm{GF}(p)^*} (z\alpha + \mathrm{Im}(L_f))$.*
- *Let $z' \in \mathrm{GF}(p)^*$ and $\beta \in z'\alpha + \mathrm{Im}(L_f)$. Then $\{z \in \mathrm{GF}(p)^* : \alpha - z\beta \in \mathrm{Im}(L_f)\} = \{\frac{1}{z'}\}$.*

Proof The desired conclusion is straightforward. □

Lemma 13 *Let f be a homogeneous quadratic function with the rank r_f and the sign ε_f, $\alpha \in \mathrm{GF}(q)$, $\beta \in \mathrm{GF}(q)^*$ and*

$$S_4 = \sum_{z \in \mathrm{GF}(p)} \sum_{x \in \mathrm{GF}(q)} \zeta_p^{f(x) - \mathrm{Tr}((\alpha - \beta z)x)}.$$

Then we have the following.

(I) *If $\alpha \in \mathrm{Im}(L_f)$, then*

$$S_4 = \begin{cases} \varepsilon_f p^{m+1} (p^*)^{-\frac{r_f}{2}} \zeta_p^{-f(x_\alpha)} & \textit{if } \beta \in \mathrm{Im}(L_f),\ f(x_\beta) = 0 \textit{ and } \mathrm{Tr}(\alpha x_\beta) = 0, \\ 0 & \textit{if } \beta \in \mathrm{Im}(L_f),\ f(x_\beta) = 0 \textit{ and } \mathrm{Tr}(\alpha x_\beta) \neq 0, \\ \varepsilon_f \bar{\eta}(-f(x_\beta)) p^m (p^*)^{-\frac{r_f - 1}{2}} \zeta_p^{-f(x_\alpha) + \frac{(\mathrm{Tr}(\alpha x_\beta))^2}{4 f(x_\beta)}} & \textit{if } \beta \in \mathrm{Im}(L_f) \textit{ and } f(x_\beta) \neq 0, \\ \varepsilon_f p^m (p^*)^{-\frac{r_f}{2}} \zeta_p^{-f(x_\alpha)} & \textit{if } \beta \notin \mathrm{Im}(L_f), \end{cases}$$

where $x_\alpha \in \mathrm{GF}(q)$ satisfies $L_f(x_\alpha) = -\frac{\alpha}{2}$ and $x_\beta \in \mathrm{GF}(q)$ satisfies $L_f(x_\beta) = -\frac{\beta}{2}$.

(II) *If* $\alpha \notin \mathrm{Im}(L_f)$, *then*

$$S_4 = \begin{cases} \varepsilon_f p^m (p^*)^{-\frac{r_f}{2}} \zeta_p^{-f(x')} & \textit{if } \beta \in \bigcup_{z \in \mathrm{GF}(p)^*} (z\alpha + \mathrm{Im}(L_f)), \\ 0 & \textit{otherwise} , \end{cases}$$

where $f(x') = -\frac{\alpha - \beta z_0}{2}$ *with* $\beta \in \frac{1}{z_0}\alpha + \mathrm{Im}(L_f)$ *and* $z_0 \in \mathrm{GF}(p)^*$.

Proof (I) It is obvious that there exists $x_\alpha \in \mathrm{GF}(q)$ such that $L_f(x_\alpha) = -\frac{\alpha}{2}$ when $\alpha \in \mathrm{Im}(L_f)$. Let us distinguish the following two cases when $\alpha \in \mathrm{Im}(L_f)$.

- Case $\beta \in \mathrm{Im}(L_f)$.
  It is obvious that there exists $x_\beta \in \mathrm{GF}(q)$ such that $L_f(x_\beta) = -\frac{\beta}{2}$. Thus, $L_f(x_\alpha - zx_\beta) = -\frac{\alpha - z\beta}{2}$. From Lemma 5, we have

$$\begin{aligned} S_4 &= \sum_{z \in \mathrm{GF}(p)} \varepsilon_f p^m (p^*)^{-\frac{r_f}{2}} \zeta_p^{-f(x_\alpha - zx_\beta)} \\ &= \varepsilon_f p^m (p^*)^{-\frac{r_f}{2}} \sum_{z \in \mathrm{GF}(p)} \zeta_p^{-f(x_\alpha) - f(x_\beta)z^2 + 2\mathrm{Tr}(L_f(x_\alpha)x_\beta)z} \\ &= \varepsilon_f p^m (p^*)^{-\frac{r_f}{2}} \sum_{z \in \mathrm{GF}(p)} \zeta_p^{-f(x_\beta)z^2 - \mathrm{Tr}(\alpha x_\beta)z - f(x_\alpha)} \\ &= \begin{cases} \varepsilon_f p^{m+1} (p^*)^{-\frac{r_f}{2}} \zeta_p^{-f(x_\alpha)} & \text{if } f(x_\beta) = 0 \, and \, \mathrm{Tr}(\alpha x_\beta) = 0, \\ 0 & \text{if } f(x_\beta) = 0 \, and \, \mathrm{Tr}(\alpha x_\beta) \neq 0, \\ \varepsilon_f \bar{\eta}(-f(x_\beta)) p^m (p^*)^{-\frac{r_f - 1}{2}} \zeta_p^{-f(x_\alpha) + \frac{(\mathrm{Tr}(\alpha x_\beta))^2}{4f(x_\beta)}} & \text{if } f(x_\beta) \neq 0, \end{cases} \end{aligned} \tag{9}$$

  where the last identity follows by using Lemmas 1 and 2.
- Case $\beta \notin Im(L_f)$. It is clear that $\alpha - \beta z \notin Im(L_f)$ for any $z \in \mathrm{GF}(p)^*$. Therefore, from Lemma 5 we have

$$S_4 = \sum_{x \in \mathrm{GF}(q)} \zeta_p^{f(x) - \mathrm{Tr}(\alpha x))} = \varepsilon_f p^m (p^*)^{-\frac{r_f}{2}} \zeta_p^{-f(x_\alpha)}. \tag{10}$$

Combining (9) and (10), the result (I) of this lemma follows.

(II) The proof is similar to that of Case (I). The desired conclusion then follows from Lemmas 5 and 12.

□

Lemma 14 *Let the symbols and notations be defined in Lemma 13, and let*

$$S_5 = \sum_{y \in \mathrm{GF}(p)^*} \sigma_y \left(\sum_{z \in \mathrm{GF}(p)} \sum_{x \in \mathrm{GF}(q)} \zeta_p^{f(x) - \mathrm{Tr}((\alpha - \beta z)x)} \right).$$

Then we have the following.

(I) *When* $\alpha \in \mathrm{Im}(L_f)$, *we have the following four cases.*

- *If* r_f *is even and* $f(x_\alpha) = 0$, *then*

$$S_5 = \begin{cases} \varepsilon_f (p-1) p^{m+1} (p^*)^{-\frac{r_f}{2}} & \textit{if } f(x_\beta) = 0 \, and \, \mathrm{Tr}(\alpha x_\beta) = 0, \\ 0 & \textit{if } f(x_\beta) = 0 \, and \, \mathrm{Tr}(\alpha x_\beta) \neq 0 \\ & \textit{or } f(x_\beta) \neq 0 \, and \, \mathrm{Tr}(\alpha x_\beta) = 0, \\ \varepsilon_f \bar{\eta}(-1) p^m (p^*)^{-\frac{r_f - 2}{2}} & \textit{if } f(x_\beta) \neq 0 \, and \, \mathrm{Tr}(\alpha x_\beta) \neq 0, \\ \varepsilon_f (p-1) p^m (p^*)^{-\frac{r_f}{2}} & \textit{if } \beta \notin Im(L_f). \end{cases}$$

– *If r_f is even and $f(x_\alpha) \neq 0$, then*

$$S_5 = \begin{cases} -\varepsilon_f p^{m+1}(p^*)^{-\frac{r_f}{2}} & \textit{if } f(x_\beta) = 0 \textit{ and } \mathrm{Tr}(\alpha x_\beta) = 0, \\ 0 & \textit{if } f(x_\beta) = 0 \textit{ and } \mathrm{Tr}(\alpha x_\beta) \neq 0 \\ & \textit{or } f(x_\beta) \neq 0 \textit{ and } E = 0, \\ \varepsilon_f \bar{\eta}(-f(x_\beta)E) p^m (p^*)^{-\frac{r_f-2}{2}} & \textit{if } f(x_\beta) \neq 0 \textit{ and } E \neq 0, \\ -\varepsilon_f p^m (p^*)^{-\frac{r_f}{2}} & \textit{if } \beta \notin Im(L_f), \end{cases}$$

where $E = -f(x_\alpha) + \frac{(\mathrm{Tr}(\alpha x_\beta))^2}{4f(x_\beta)}$.

– *If r_f is odd and $f(x_\alpha) = 0$, then*

$$S_5 = \begin{cases} 0 & \textit{if } f(x_\beta) = 0 \textit{ or } \beta \notin \mathrm{Im}(L_f), \\ \varepsilon_f \bar{\eta}(-f(x_\beta))(p-1)p^m (p^*)^{-\frac{r_f-1}{2}} & \textit{if } f(x_\beta) \neq 0 \textit{ and } \mathrm{Tr}(\alpha x_\beta) = 0, \\ -\varepsilon_f \bar{\eta}(-f(x_\beta)) p^m (p^*)^{-\frac{r_f-1}{2}} & \textit{if } f(x_\beta) \neq 0 \textit{ and } \mathrm{Tr}(\alpha x_\beta) \neq 0. \end{cases}$$

– *If r_f is odd and $f(x_\alpha) \neq 0$, then*

$$S_5 = \begin{cases} \varepsilon_f \bar{\eta}(-f(x_\alpha)) p^{m+1}(p^*)^{-\frac{r_f-1}{2}} & \textit{if } f(x_\beta) = \mathrm{Tr}(\alpha x_\beta) = 0, \\ 0 & \textit{if } f(x_\beta) = 0 \textit{ and } \mathrm{Tr}(\alpha x_\beta) \neq 0 \\ \varepsilon_f \bar{\eta}(-f(x_\alpha))(p-1)p^m (p^*)^{-\frac{r_f-1}{2}} & \textit{if } f(x_\beta) \neq 0 \textit{ and } E = 0, \\ -\varepsilon_f \bar{\eta}(-f(x_\beta)) p^m (p^*)^{-\frac{r_f-1}{2}} & \textit{if } f(x_\beta) \neq 0 \textit{ and } E \neq 0, \\ \varepsilon_f \bar{\eta}(-f(x_\alpha)) p^m (p^*)^{-\frac{r_f-1}{2}} & \textit{if } \beta \notin Im(L_f). \end{cases}$$

where $E = -f(x_\alpha) + \frac{(\mathrm{Tr}(\alpha x_\beta))^2}{4f(x_\beta)}$.

(II) *When $\alpha \notin \mathrm{Im}(L_f)$, we have the following two cases.*

– *If r_f is even, then*

$$S_5 = \begin{cases} -\varepsilon_f p^m (p^*)^{-\frac{r_f}{2}} & \textit{if } \beta \in \bigcup_{z \in \mathrm{GF}(p)^*}(z\alpha + \mathrm{Im}(L_f)) \textit{ and } f(x') \neq 0, \\ (p-1)\varepsilon_f p^m (p^*)^{-\frac{r_f}{2}} & \textit{if } \beta \in \bigcup_{z \in \mathrm{GF}(p)^*}(z\alpha + \mathrm{Im}(L_f)) \textit{ and } f(x') = 0, \\ 0 & \textit{otherwise}\ , \end{cases}$$

where $f(x') = -\frac{\alpha - \beta z_0}{2}$ *with* $z_0 \in \mathrm{GF}(p)^*$ *and* $\beta \in \frac{1}{z_0}\alpha + \mathrm{Im}(L_f)$.

– *If r_f is odd, then*

$$S_5 = \begin{cases} \varepsilon_f \bar{\eta}(-f(x')) p^m (p^*)^{-\frac{r_f-1}{2}} & \textit{if } \beta \in \bigcup_{z \in \mathrm{GF}(p)^*}(z\alpha + \mathrm{Im}(L_f)) \textit{ and } f(x') \neq 0, \\ 0 & \textit{otherwise}\ , \end{cases}$$

where $f(x') = -\frac{\alpha - \beta z_0}{2}$ *with* $\beta \in \frac{1}{z_0}\alpha + \mathrm{Im}(L_f)$ *and* $z_0 \in \mathrm{GF}(p)^*$.

Proof The desired conclusions then follow from Lemmas 13 and 4. □

Lemma 15 *Let f be a homogeneous quadratic function with the rank r_f and the sign ε_f, $\alpha \in \mathrm{GF}(q)$, $\beta \in \mathrm{GF}(q)^*$ and*

$$N_{f,\beta}(\alpha) = \{x \in \mathrm{GF}(q) : f(x) - \mathrm{Tr}(\alpha x) = 0 \textit{ and } \mathrm{Tr}(\beta x) = 0\}.$$

Then we have the following.

(i) *When* $\alpha \in \mathrm{Im}(L_f)$, *we have the following four cases.*

- *If* r_f *is even and* $f(x_\alpha) = 0$, *then*

$$N_{f,\beta}(\alpha) = \begin{cases} p^{m-2} + \varepsilon_f (p-1) p^{m-1} (p^*)^{-\frac{r_f}{2}} & \textit{if } f(x_\beta) = 0 \textit{ and } \mathrm{Tr}(\alpha x_\beta) = 0, \\ p^{m-2} & \textit{if } f(x_\beta) = 0 \textit{ and } \mathrm{Tr}(\alpha x_\beta) \neq 0 \\ & \textit{or } f(x_\beta) \neq 0 \textit{ and } \mathrm{Tr}(\alpha x_\beta) = 0, \\ p^{m-2} + \varepsilon_f \bar{\eta}(-1) p^{m-2} (p^*)^{-\frac{r_f-2}{2}} & \textit{if } f(x_\beta) \neq 0 \textit{ and } \mathrm{Tr}(\alpha x_\beta) \neq 0, \\ p^{m-2} + \varepsilon_f (p-1) p^{m-2} (p^*)^{-\frac{r_f}{2}} & \textit{if } \beta \notin \mathrm{Im}(L_f). \end{cases}$$

- *If* r_f *is even and* $f(x_\alpha) \neq 0$, *then*

$$N_{f,\beta}(\alpha) = \begin{cases} p^{m-2} - \varepsilon_f p^{m-1} (p^*)^{-\frac{r_f}{2}} & \textit{if } f(x_\beta) = 0 \textit{ and } \mathrm{Tr}(\alpha x_\beta) = 0, \\ p^{m-2} & \textit{if } f(x_\beta) = 0 \textit{ and } \mathrm{Tr}(\alpha x_\beta) \neq 0 \\ & \textit{or } f(x_\beta) \neq 0 \textit{ and } E = 0, \\ p^{m-2} + \varepsilon_f \bar{\eta}(-f(x_\beta)E) p^{m-2} (p^*)^{-\frac{r_f-2}{2}} & \textit{if } f(x_\beta) \neq 0 \textit{ and } E \neq 0, \\ p^{m-2} - \varepsilon_f p^{m-2} (p^*)^{-\frac{r_f}{2}} & \textit{if } \beta \notin \mathrm{Im}(L_f), \end{cases}$$

where $E = -f(x_\alpha) + \frac{(\mathrm{Tr}(\alpha x_\beta))^2}{4f(x_\beta)}$.

- *If* r_f *is odd and* $f(x_\alpha) = 0$, *then*

$$N_{f,\beta}(\alpha) = \begin{cases} p^{m-2} & \textit{if } f(x_\beta) = 0 \textit{ or } \beta \notin \mathrm{Im}(L_f), \\ p^{m-2} + \varepsilon_f \bar{\eta}(-f(x_\beta))(p-1) p^{m-2} (p^*)^{-\frac{r_f-1}{2}} & \textit{if } f(x_\beta) \neq 0 \textit{ and } \mathrm{Tr}(\alpha x_\beta) = 0, \\ p^{m-2} - \varepsilon_f \bar{\eta}(-f(x_\beta)) p^{m-2} (p^*)^{-\frac{r_f-1}{2}} & \textit{if } f(x_\beta) \neq 0 \textit{ and } \mathrm{Tr}(\alpha x_\beta) \neq 0. \end{cases}$$

- *If* r_f *is odd and* $f(x_\alpha) \neq 0$, *then*

$$N_{f,\beta}(\alpha) = \begin{cases} p^{m-2} + \varepsilon_f \bar{\eta}(-f(x_\alpha)) p^{m-1} (p^*)^{-\frac{r_f-1}{2}} & \textit{if } f(x_\beta) = \mathrm{Tr}(\alpha x_\beta) = 0, \\ p^{m-2} & \textit{if } f(x_\beta) = 0 \textit{ and } \mathrm{Tr}(\alpha x_\beta) \neq 0 \\ p^{m-2} + \varepsilon_f \bar{\eta}(-f(x_\alpha))(p-1) p^{m-2} (p^*)^{-\frac{r_f-1}{2}} & \textit{if } f(x_\beta) \neq 0 \textit{ and } E = 0, \\ p^{m-2} - \varepsilon_f \bar{\eta}(-f(x_\beta)) p^{m-2} (p^*)^{-\frac{r_f-1}{2}} & \textit{if } f(x_\beta) \neq 0 \textit{ and } E \neq 0, \\ p^{m-2} + \varepsilon_f \bar{\eta}(-f(x_\alpha)) p^{m-2} (p^*)^{-\frac{r_f-1}{2}} & \textit{if } \beta \notin \mathrm{Im}(L_f). \end{cases}$$

where $E = -f(x_\alpha) + \frac{(\mathrm{Tr}(\alpha x_\beta))^2}{4f(x_\beta)}$.

(II) *When* $\alpha \notin Im(L_f)$, *we have the following two cases.*

- *If* r_f *is even, then*

$$N_{f,\beta}(\alpha) = \begin{cases} p^{m-2} - \varepsilon_f p^{m-2} (p^*)^{-\frac{r_f}{2}} & \textit{if } \beta \in \bigcup_{z \in \mathrm{GF}(p)^*} (z\alpha + \mathrm{Im}(L_f)) \textit{ and } f(x') \neq 0, \\ p^{m-2} + (p-1)\varepsilon_f p^{m-2} (p^*)^{-\frac{r_f}{2}} & \textit{if } \beta \in \bigcup_{z \in \mathrm{GF}(p)^*} (z\alpha + \mathrm{Im}(L_f)) \textit{ and } f(x') = 0, \\ p^{m-2} & \textit{otherwise}, \end{cases}$$

where $f(x') = -\frac{\alpha - \beta z_0}{2}$ *with* $\beta \in \frac{1}{z_0}\alpha + Im(L_f)$ *and* $z_0 \in \mathrm{GF}(p)^*$.

- *If* r_f *is odd, then*

$$N_{f,\beta}(\alpha) = \begin{cases} p^{m-2} + \varepsilon_f \bar{\eta}(-f(x')) p^{m-2} (p^*)^{-\frac{r_f-1}{2}} & \textit{if } \beta \in \bigcup_{z \in \mathrm{GF}(p)^*} (z\alpha + \mathrm{Im}(L_f)) \textit{ and } f(x') \neq 0, \\ p^{m-2} & \textit{otherwise}, \end{cases}$$

where $f(x') = -\frac{\alpha - \beta z_0}{2}$ *with* $\beta \in \frac{1}{z_0}\alpha + \mathrm{Im}(L_f)$ *and* $z_0 \in \mathrm{GF}(p)^*$.

Proof By definition, we have

$$N_{f,\beta}(\alpha) = p^{-2} \sum_{x\in \mathrm{GF}(q)} \left(\sum_{y\in \mathrm{GF}(p)} \zeta_p^{y(f(x)-\mathrm{Tr}(\alpha x))} \right) \left(\sum_{z\in \mathrm{GF}(p)} \zeta_p^{z\mathrm{Tr}(\beta x)} \right)$$
$$= p^{-2} \left(\sum_{z\in \mathrm{GF}(p)} \sum_{x\in \mathrm{GF}(q)} \zeta_p^{z\mathrm{Tr}(\beta x)} + \sum_{y\in \mathrm{GF}(p)^*} \sigma_y \left(\sum_{z\in \mathrm{GF}(p)} \sum_{x\in \mathrm{GF}(q)} \zeta_p^{f(x)-\mathrm{Tr}((\alpha-\beta z)x)} \right) \right).$$

The desired conclusion then follows from Lemma 14 and Part (I) of Lemma 10.

This completes the proof. □

Lemma 16 *Let f be a homogeneous quadratic function with rank r_f and the sign ε_f, $\alpha \in Im(L_f)$ and $x_\alpha \in \mathrm{GF}(q)$ with satisfying $L_f(x_\alpha) = -\frac{\alpha}{2}$. Suppose that $f(x_\alpha) \neq 0$, we define*

$$S_6 = \sum_{z\in \mathrm{GF}(p)} \sum_{w\in \mathrm{GF}(p)} \sum_{x\in \mathrm{GF}(q)} \zeta_p^{f(x)-\frac{1}{4f(x_\alpha)}z^2+w(z-\mathrm{Tr}(\alpha x))}$$

and

$$N_E = \#\left\{ x \in \mathrm{GF}(q) : f(x) - \frac{1}{4f(x_\alpha)}(\mathrm{Tr}(\alpha x))^2 = 0 \right\}.$$

Then we have the following:

(I) $S_6 = \varepsilon_f \bar{\eta}(-f(x_\alpha)) p^{m+1} (p^*)^{-\frac{r_f-1}{2}}$,

(II) $\sum_{y\in \mathrm{GF}(p)^*} \sigma_y(S_6) = \begin{cases} 0 & \text{if } r_f \text{ is even}, \\ \varepsilon_f \bar{\eta}(-f(x_\alpha))(p-1)p^{m+1}(p^*)^{-\frac{r_f-1}{2}} & \text{if} r_f \text{ is odd}, \end{cases}$

(III) $N_E = \begin{cases} p^{m-1} & \text{if} r_f \text{is even}, \\ p^{m-1} + \varepsilon_f \bar{\eta}(-f(x_\alpha))(p-1)p^{m-1}(p^*)^{-\frac{r_f-1}{2}} & \text{if} r_f \text{is odd}. \end{cases}$

Proof (I) By definition, we have

$$S_6 = \sum_{z\in \mathrm{GF}(p)} \sum_{w\in \mathrm{GF}(p)} \zeta_p^{-\frac{1}{4f(x_\alpha)}z^2+wz} \sum_{x\in \mathrm{GF}(q)} \zeta_p^{f(x)-\mathrm{Tr}(w\alpha x)}$$
$$= \varepsilon_f p^m (p^*)^{-\frac{r_f}{2}} \sum_{z\in \mathrm{GF}(p)} \sum_{w\in \mathrm{GF}(p)} \zeta_p^{-\frac{1}{4f(x_\alpha)}z^2+wz-f(x_\alpha)w^2} \quad \text{(By the result (II) of Lemma 5)}$$
$$= \varepsilon_f \bar{\eta}(-f(x_\alpha)) p^{m+1} (p^*)^{-\frac{r_f-1}{2}}. \quad \text{(By Lemma 6)}$$

(II) The desired conclusion then follows from Lemma 4 and Part (I) of this Lemma.

(III) For any $x \in \mathrm{GF}(q)$, we have

$$p^{-2} \sum_{z\in \mathrm{GF}(p)} \left(\sum_{w\in \mathrm{GF}(p)} \zeta_p^{w(z-\mathrm{Tr}(\alpha x))} \right) \left(\sum_{y\in \mathrm{GF}(p)} \zeta_p^{y(f(x)-\frac{1}{4f(x_\alpha)}z^2)} \right)$$
$$= \begin{cases} 1 & \text{if } f(x) - \frac{1}{4f(x_\alpha)}(\mathrm{Tr}(\alpha x))^2 = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore,

$$\begin{aligned}
N_E &= p^{-2} \sum_{x\in \mathrm{GF}(q)} \sum_{z\in \mathrm{GF}(p)} \left(\sum_{w\in \mathrm{GF}(p)} \zeta_p^{w(z-\mathrm{Tr}(\alpha x))} \right) \left(\sum_{y\in \mathrm{GF}(p)} \zeta_p^{y(f(x)-\frac{1}{4f(x_\alpha)}z^2)} \right) \\
&= p^{-2} \sum_{y\in \mathrm{GF}(p)} \sum_{z\in \mathrm{GF}(p)} \sum_{w\in \mathrm{GF}(p)} \sum_{x\in \mathrm{GF}(q)} \zeta_p^{y(f(x)-\frac{1}{4f(x_\alpha)}z^2)+w(z-\mathrm{Tr}(\alpha x))} \\
&= p^{-2} \sum_{z\in \mathrm{GF}(p)} \sum_{w\in \mathrm{GF}(p)} \sum_{x\in \mathrm{GF}(q)} \zeta_p^{w(z-\mathrm{Tr}(\alpha x))} \\
&\quad + p^{-2} \sum_{y\in \mathrm{GF}(p)^*} \sigma_y \left(\sum_{z\in \mathrm{GF}(p)} \sum_{w\in \mathrm{GF}(p)} \sum_{x\in \mathrm{GF}(q)} \zeta_p^{f(x)-\frac{1}{4f(x_\alpha)}z^2+w(z-\mathrm{Tr}(\alpha x))} \right).
\end{aligned}$$

Note that

$$\sum_{z\in \mathrm{GF}(p)} \sum_{w\in \mathrm{GF}(p)} \sum_{x\in \mathrm{GF}(q)} \zeta_p^{w(z-\mathrm{Tr}(\alpha x))} = p^{m+1}.$$

The desired conclusion then follows from the result (II) of this lemma.

This completes the proof. □

Lemma 17 *Let f be a homogeneous quadratic function with rank r_f and the sign ε_f, $\alpha \in Im(L_f)$ and $x_\alpha \in \mathrm{GF}(q)$ with satisfying $L_f(x_\alpha) = -\frac{\alpha}{2}$. Let $f(x_\alpha) \neq 0$,*

$$g(x) = f(x) - \frac{(\mathrm{Tr}(\alpha x))^2}{4f(x_\alpha)}$$

and $N(g = t) = \#\{x \in \mathrm{GF}(q) : g(x) = t\}$ for any $t \in \mathrm{GF}(p)$. Then we have the following results.

(I) $\sum_{x\in \mathrm{GF}(q)} \zeta_p^{g(x)} = \varepsilon_f \bar{\eta}(-f(x_\alpha)) p^m (p^*)^{-\frac{r_f-1}{2}}$.

(II) $$N(g=t) = \begin{cases} p^{m-1} & \textit{if } r_f \textit{ is even and } t = 0, \\ p^{m-1} + \varepsilon_f \bar{\eta}(-t)\bar{\eta}(-f(x_\alpha)) p^{m-1} (p^*)^{-\frac{r_f-2}{2}} & \textit{if } r_f \textit{ is even and } t \neq 0, \\ p^{m-1} + \varepsilon_f \bar{\eta}(-f(x_\alpha))(p-1) p^{m-1} (p^*)^{-\frac{r_f-1}{2}} & \textit{if } r_f \textit{ is odd and } t = 0, \\ p^{m-1} - \varepsilon_f \bar{\eta}(-f(x_\alpha)) p^{m-1} (p^*)^{-\frac{r_f-1}{2}} & \textit{if } r_f \textit{ is odd and } t \neq 0. \end{cases}$$

Proof (I) By definition, we have

$$\begin{aligned}\sum_{x\in \mathrm{GF}(q)} \zeta_p^{g(x)} &= \sum_{x\in \mathrm{GF}(q)} \zeta_p^{f(x)-\frac{(\mathrm{Tr}(\alpha x))^2}{4f(x_\alpha)}}\\ &= \sum_{z\in \mathrm{GF}(p)} \left(\sum_{x\in \mathrm{GF}(q),\mathrm{Tr}(x)=z} \zeta_p^{f(x)-\frac{z^2}{4f(x_\alpha)}} \right)\\ &= \sum_{z\in \mathrm{GF}(p)} \left(\sum_{x\in \mathrm{GF}(q),\mathrm{Tr}(x)=z} \zeta_p^{f(x)-\frac{z^2}{4f(x_\alpha)}} \left(p^{-1} \sum_{w\in \mathrm{GF}(p)} \zeta_p^{w(z-\mathrm{Tr}(\alpha x))} \right) \right)\\ &= p^{-1} \sum_{z\in \mathrm{GF}(p)} \sum_{w\in \mathrm{GF}(p)} \sum_{x\in \mathrm{GF}(q)} \zeta_p^{f(x)-\frac{z^2}{4f(x_\alpha)}+w(z-\mathrm{Tr}(\alpha x))}\\ &= \varepsilon_f \bar{\eta}(-f(x_\alpha)) p^m (p^*)^{-\frac{r_f-1}{2}},\end{aligned}$$

where the last identity follows from Part (I) of Lemma 16.

(II) By Part (I) of this lemma, it is clear that the rank of $g(x)$ is $r_g = r_f - 1$ and the sign of $g(x)$ is $\varepsilon_g = \varepsilon_f \bar{\eta}(-f(x_\alpha))$. Thus the desired conclusion (II) then follows from Lemmas 7 and 16.

This completes the proof.

□

Lemma 18 *Let f be a homogeneous quadratic function with the rank r_f and the sign ε_f, $\alpha \in \mathrm{Im}(L_f)$ and $x_\alpha \in \mathrm{GF}(q)$ with satisfying $L_f(x_\alpha) = -\frac{\alpha}{2}$. Let $f(x_\alpha) \neq 0$,*

$$g(x) = f(x) - \frac{(\mathrm{Tr}(\alpha x))^2}{4f(x_\alpha)}$$

and

$$E = -f(x_\alpha) - \frac{(\mathrm{Tr}(\alpha x))^2}{4f(x)}.$$

When r_f is even, we define

$$\begin{aligned}I_1 &= \#\{x \in \mathrm{GF}(q) : f(x) = \mathrm{Tr}(\alpha x) = 0\},\\ I_2 &= \#\left\{\{x \in \mathrm{GF}(q) : f(x) = 0 \textit{ and } \mathrm{Tr}(\alpha x) \neq 0\} \bigcup \{x \in \mathrm{GF}(q) : f(x) \neq 0 \textit{ and } E = 0\}\right\},\\ I_3 &= \#\{x \in \mathrm{GF}(q) : f(x) \neq 0, E \neq 0 \textit{ and } f(x)\cdot E \in \mathrm{NSQ}\},\\ I_4 &= \#\{x \in \mathrm{GF}(q) : f(x) \neq 0, E \neq 0 \textit{ and } f(x)\cdot E \in \mathrm{SQ}\}.\end{aligned}$$

When r_f is odd, we define

$$\begin{aligned}J_1 &= \#\{x \in \mathrm{GF}(q) : f(x) \neq 0, \bar{\eta}(f(x)) = \bar{\eta}(f(x_\alpha)) \textit{ and } E = 0\},\\ J_2 &= \#\{x \in \mathrm{GF}(q) : f(x) \neq 0 \textit{ and } \bar{\eta}(f(x)) = \bar{\eta}(f(x_\alpha))\},\\ J_3 &= \#\{x \in \mathrm{GF}(q) : f(x) = \mathrm{Tr}(\alpha x) = 0\},\\ J_4 &= \#\{x \in \mathrm{GF}(q) : f(x) = 0 \textit{ and } \mathrm{Tr}(\alpha x) \neq 0\},\\ J_5 &= \#\{x \in \mathrm{GF}(q) : f(x) \neq 0 \textit{ and } E = 0\},\\ J_6 &= \#\{x \in \mathrm{GF}(q) : f(x) \neq 0, E \neq 0 \textit{ and } \bar{\eta}(f(x)) = -\bar{\eta}(f(x_\alpha))\}.\end{aligned}$$

Then we have the following results.

(I) *If r_f is even, then*

$$I_1 = p^{m-2}, \tag{11}$$

$$I_2 = (p-1)p^{m-2}(2 + \varepsilon_f \cdot p(p^*)^{-\frac{r_f}{2}}), \tag{12}$$

$$I_3 = \frac{p-1}{2}p^{m-1}(1 - \varepsilon_f \cdot p(p^*)^{-\frac{r_f}{2}}), \tag{13}$$

$$I_4 = \frac{(p-1)(p-2)}{2}p^{m-2}\left(1 + \varepsilon_f \cdot p(p^*)^{-\frac{r_f}{2}}\right). \tag{14}$$

(II) *If r_f is odd, then*

$$J_1 = (p-1)p^{m-2}\left(1 + \varepsilon_f \bar{\eta}(-f(x_\alpha))(p-1)(p^*)^{-\frac{r_f-1}{2}}\right), \tag{15}$$

$$J_2 = \frac{(p-1)(p-2)}{2}p^{m-2}\left(1 - \varepsilon_f \bar{\eta}(-f(x_\alpha))(p^*)^{-\frac{r_f-1}{2}}\right), \tag{16}$$

$$J_3 = p^{m-2} + \varepsilon_f \bar{\eta}(-f(x_\alpha))(p-1)p^{m-2}(p^*)^{-\frac{r_f-1}{2}}, \tag{17}$$

$$J_4 = (p-1)p^{m-2}\left(1 - \varepsilon_f \bar{\eta}(-f(x_\alpha))(p^*)^{-\frac{r_f-1}{2}}\right), \tag{18}$$

$$J_5 = (p-1)p^{m-2}\left(1 + \varepsilon_f \bar{\eta}(-f(x_\alpha))(p-1)(p^*)^{-\frac{r_f-1}{2}}\right), \tag{19}$$

$$J_6 = \frac{p-1}{2}p^{m-1}\left(1 - \varepsilon_f \bar{\eta}(-f(x_\alpha))(p^*)^{-\frac{r_f-1}{2}}\right). \tag{20}$$

Proof (I) If r_f is even, then we have the following.

- It is clear that Eq. (11) follows directly from Lemma 11.
- By definition, we have

$$\begin{aligned} I_2 &= \#\{x \in \mathrm{GF}(q) : f(x) \neq 0 \ and \ g(x) = 0\} \\ &\quad + \#\{x \in \mathrm{GF}(q) : f(x) = 0 \ and \ \mathrm{Tr}(\alpha x) \neq 0\} \\ &= \#\{x \in \mathrm{GF}(q) : g(x) = 0\} - \#\{x \in \mathrm{GF}(q) : f(x) = 0 \ and \ \mathrm{Tr}(\alpha x) = 0\} \\ &\quad + \#\{x \in \mathrm{GF}(q) : f(x) = 0 \ and \ \mathrm{Tr}(\alpha x) \neq 0\} \\ &= \#\{x \in \mathrm{GF}(q) : g(x) = 0\} + \#\{x \in \mathrm{GF}(q) : f(x) = 0\} - 2\#\{x \in \mathrm{GF}(q) : f(x) \\ &= \mathrm{Tr}(\alpha x) = 0\}. \end{aligned}$$

  Then Eq. (12) follows from Lemmas 17, 9 and 11.
- In Eqs. (13) and (14), we only give the proof for the case $-f(x_\alpha) \in \mathrm{SQ}$ and omit the proof for the case $-f(x_\alpha) \in \mathrm{NSQ}$ whose proof is similar. Suppose that $-f(x_\alpha) \in \mathrm{SQ}$, by definition and

$$-\frac{f(x)E}{f(x_\alpha)} = f(x) - \frac{(\mathrm{Tr}(\alpha x))^2}{4f(x_\alpha)} = g(x)$$

  we get

$$\begin{aligned} I_3 &= \#\{x \in \mathrm{GF}(q) : f(x) \neq 0 \ and \ g(x) \in \mathrm{NSQ}\} \\ &= \#\{x \in \mathrm{GF}(q) : g(x) \in \mathrm{NSQ}\} - \#\{\mathrm{x \in GF(q) : f(x) = 0 \ and \ g(x) \in NSQ}\} \\ &= \#\{x \in \mathrm{GF}(q) : g(x) \in \mathrm{NSQ}\} - \#\{\mathrm{x \in GF(q) : f(x) = 0 \ and \ (Tr(\alpha x))^2 \in NSQ}\} \end{aligned}$$

$$= \#\{x \in \mathrm{GF}(q) : g(x) \in \mathrm{NSQ}\}$$
$$= \frac{p-1}{2} p^{m-1}(1 - \varepsilon_f \cdot p(p^*)^{-\frac{r_f}{2}}),$$

where the last equation follows from Lemma 17. This means that Eq. (13) follows. Similarly, when $-f(x_\alpha) \in \mathrm{SQ}$, Eq. (14) follows from (11) and (12).

(II) If r_f is odd, then we give the proofs of the desired conclusions as follows.

- Since

$$-\frac{E}{4f(x_\alpha)} = \frac{g(x)}{4f(x)},$$

we have

$$\begin{aligned} J_1 &= \#\{x \in \mathrm{GF}(q) : f(x) \neq 0, \bar{\eta}(f(x)) = \bar{\eta}(f(x_\alpha)) \; and \; E = 0\} \\ &= \#\{x \in \mathrm{GF}(q) : g(x) = 0 \; and \; f(x) \neq 0\} \\ &= \#\{x \in \mathrm{GF}(q) : g(x) = 0\} - \#\{x \in \mathrm{GF}(q) : g(x) = f(x) = 0\} \\ &= (p-1)p^{m-2}(1 + \varepsilon_f \bar{\eta}(-f(x_\alpha))(p-1)(p^*)^{-\frac{r_f - 1}{2}}), \end{aligned}$$

where the last equation follows from Lemmas 17 and 11. This means that Eq. (15) follows.

- By definition, we have

$$\begin{aligned} J_2 &= \#\{x \in \mathrm{GF}(q) : f(x) \neq 0 \; and \; \bar{\eta}(f(x)) = \bar{\eta}(f(x_\alpha))\} \\ &\quad -\#\{x \in \mathrm{GF}(q) : f(x) \neq 0, \bar{\eta}(f(x)) = \bar{\eta}(f(x_\alpha)) \; and \; E = 0\} \\ &= \#\{x \in \mathrm{GF}(q) : f(x) \neq 0 \; and \; \bar{\eta}(f(x)) = \bar{\eta}(f(x_\alpha))\} \\ &\quad -\#\{x \in \mathrm{GF}(q) : E = 0 \; and \; f(x) \neq 0\}. \end{aligned}$$

Then Eq. (16) follows from Lemma 7 and (15).

- Equation (17) follows directly from Lemma 11.
- By definition, we have

$$J_4 = \#\{x \in \mathrm{GF}(q) : f(x) = 0\} - \#\{x \in \mathrm{GF}(q) : f(x) = \mathrm{Tr}(\alpha x) = 0\}.$$

The desired conclusion in (18) then follows from Lemma 9 and Eq. (17).

- Note that

$$-\frac{E}{4f(x_\alpha)} = \frac{g(x)}{4f(x)}.$$

Therefore, we have

$$\begin{aligned} J_5 &= \#\{x \in \mathrm{GF}(q) : f(x) \neq 0 \; and \; g(x) = 0\} \\ &= \#\{x \in \mathrm{GF}(q) : g(x) = 0\} - \#\{x \in \mathrm{GF}(q) : f(x) = \mathrm{Tr}(\alpha x) = 0\}. \end{aligned}$$

The desired conclusion in (19) then follows from Lemma 17 and Eq. (17).

- The desired conclusion in (20) then follows directly from (16), (17), (18) and (19).

This completes the proof of this lemma.

□

Lemma 19 *Let f be a homogeneous quadratic function with the rank r_f and the sign ε_f, $\alpha \in \mathrm{Im}(L_f)$ and $x_\alpha \in \mathrm{GF}(q)$ satisfying $L_f(x_\alpha) = -\frac{\alpha}{2}$ and $f(x_\alpha) = 0$. Then*

Table 1 The weight distribution of C_D of Theorem 1 when r_f is even and $f(x_\alpha)\neq 0$

Weight w	Multiplicity A_w
0	1
$(p-1)p^{m-2}$	$p^{r_f-2}+\frac{p-1}{2}p^{r_f-1}\left(1-\varepsilon_f\cdot p(p^*)^{-\frac{r_f}{2}}\right)-1$
$p^{m-2}\left(p-1-\varepsilon_f\cdot p(p^*)^{-\frac{r_f}{2}}\right)$	$(p-1)p^{r_f-2}\left(2+\varepsilon_f\cdot p(p^*)^{-\frac{r_f}{2}}\right)$
$p^{m-2}\left(p-1-2\varepsilon_f\cdot p(p^*)^{-\frac{r_f}{2}}\right)$	$\frac{(p-1)(p-2)}{2}p^{r_f-2}\left(1+\varepsilon_f\cdot p(p^*)^{-\frac{r_f}{2}}\right)$
$p^{m-2}(p-1)\left(1-\varepsilon_f(p^*)^{-\frac{r_f}{2}}\right)$	$p^m-p^{r_f}$

- $\#\{x\in \mathrm{GF}(q): f(x)\neq 0, \mathrm{Tr}(\alpha x)=0 \textit{ and } -f(x)\in \mathrm{SQ}\}=\frac{\mathrm{p}-1}{2}\mathrm{p}^{\mathrm{m}-2}\left(1+\varepsilon_{\mathrm{f}}\cdot \mathrm{p}(\mathrm{p}^*)^{-\frac{\mathrm{r_f}-1}{2}}\right)$,
- $\#\{x\in \mathrm{GF}(q): f(x)\neq 0, \mathrm{Tr}(\alpha x)=0 \textit{ and } -f(x)\in \mathrm{NSQ}\}=\frac{\mathrm{p}-1}{2}\mathrm{p}^{\mathrm{m}-2}\left(1-\varepsilon_{\mathrm{f}}\cdot \mathrm{p}(\mathrm{p}^*)^{-\frac{\mathrm{r_f}-1}{2}}\right)$,
- $\#\{x\in \mathrm{GF}(q): f(x)\mathrm{Tr}(\alpha x)\neq 0 \textit{ and } -f(x)\in \mathrm{SQ}\}=\frac{(\mathrm{p}-1)^2}{2}\mathrm{p}^{\mathrm{m}-2}$,
- $\#\{x\in \mathrm{GF}(q): f(x)\mathrm{Tr}(\alpha x)\neq 0 \textit{ and } -f(x)\in \mathrm{NSQ}\}=\frac{(\mathrm{p}-1)^2}{2}\mathrm{p}^{\mathrm{m}-2}$.

Proof The desired conclusions then follow from Lemma 8. □

3.2 Main results and their proofs

The following two theorems are the main results of this paper.

Theorem 1 *Let f be a homogeneous quadratic function with rank r_f and the sign ε_f, $\alpha\in\mathrm{Im}(L_f)$ and $x_\alpha\in\mathrm{GF}(q)$ satisfying $L_f(x_\alpha)=-\frac{\alpha}{2}$. Let D be defined in (8). Then the set C_D of (1) is an $[n,m]$ linear code over $\mathrm{GF}(p)$ with the weight distribution in Tables 1, 2, 3 and 4, where*

$$n=\begin{cases} p^{m-1}(1-\varepsilon_f(p^*)^{-\frac{r_f}{2}})-1 & \textit{if } r_f \textit{ is even and } f(x_\alpha)\neq 0,\\ p^{m-1}(1+\varepsilon_f(p-1)(p^*)^{-\frac{r_f}{2}})-1 & \textit{if } r_f \textit{ is even and } f(x_\alpha)=0,\\ p^{m-1}(1+\varepsilon_f\bar{\eta}\left(-f(x_\alpha))(p^*)^{-\frac{r_f-1}{2}}\right)-1 & \textit{if } r_f \textit{ is odd and } f(x_\alpha)\neq 0,\\ p^{m-1}-1 & \textit{if } r_f \textit{ is odd and } f(x_\alpha)=0. \end{cases} \tag{21}$$

Proof By definition, the code length of C_D is $n=|D|=N_f(\alpha)-1$, where $N_f(\alpha)$ was defined by Lemma 9. This means that Eq. (21) follows.

For each $\beta\in\mathrm{GF}(q)^*$, define

$$\mathbf{c}_\beta=(\mathrm{Tr}(\beta d_1),\ \mathrm{Tr}(\beta d_2),\ \ldots,\ \mathrm{Tr}(\beta d_n)), \tag{22}$$

where $d_1, d_2, \ldots, d_n$ are the elements of D. Then the Hamming weight $\mathrm{wt}(\mathbf{c}_\beta)$ of $\mathbf{c}_\beta$ is

$$\mathrm{wt}(\mathbf{c}_\beta)=N_f(\alpha)-N_{f,\beta}(\alpha), \tag{23}$$

where $N_f(\alpha)$ and $N_{f,\beta}(\alpha)$ were defined before. By Lemmas 9 and 15, we have $\mathrm{wt}(\mathbf{c}_\beta)=N_f(\alpha)-N_{f,\beta}(\alpha)>0$ for each $\beta\in\mathrm{GF}(q)^*$. This means that the code C_D has q distinct codewords. Hence, the dimension of the code C_D is m.

Table 2 The weight distribution of C_D of Theorem 1 when r_f is even and $f(x_\alpha)=0$

Weight w	Multiplicity A_w
0	1
$(p-1)p^{m-2}$	$p^{r_f-2}\Big(1+\varepsilon_f\cdot(p-1)p(p^*)^{-\frac{r_f}{2}}\Big)-1$
$(p-1)p^{m-2}\Big(1+\varepsilon_f\cdot p(p^*)^{-\frac{r_f}{2}}\Big)$	$(p-1)p^{r_f-2}\Big(2-\varepsilon_f\cdot p(p^*)^{-\frac{r_f}{2}}\Big)$
$p^{m-2}\Big(p-1+\varepsilon_f\cdot(p-2)p(p^*)^{-\frac{r_f}{2}}\Big)$	$(p-1)^2p^{r_f-2}$
$p^{m-2}(p-1)\Big(1+\varepsilon_f\cdot(p-1)(p^*)^{-\frac{r_f}{2}}\Big)$	$p^m-p^{r_f}$

Table 3 The weight distribution of C_D of Theorem 1 when r_f is odd and $f(x_\alpha)\neq 0$

Weight w	Multiplicity A_w
0	1
$(p-1)p^{m-2}$	$p^{r_f-2}\Big(1+\varepsilon_f\bar{\eta}(-f(x_\alpha))\Big)(p-1)(p^*)^{-\frac{r_f-1}{2}})-1$
$p^{m-2}\Big(p-1+\varepsilon_f\bar{\eta}(-f(x_\alpha))p(p^*)^{-\frac{r_f-1}{2}}\Big)$	$(p-1)p^{r_f-2}\Big(1-\varepsilon_f\bar{\eta}(-f(x_\alpha))(p^*)^{-\frac{r_f-1}{2}}\Big)$
$p^{m-2}\Big(p-1+\varepsilon_f\bar{\eta}(-f(x_\alpha))(p^*)^{-\frac{r_f-1}{2}})$	$(p-1)p^{r_f-2}(1+\varepsilon_f\bar{\eta}(-f(x_\alpha)\Big)(p-1)(p^*)^{-\frac{r_f-1}{2}})$
$p^{m-2}\Big(p-1+\varepsilon_f\bar{\eta}(-f(x_\alpha))(p+1)(p^*)^{-\frac{r_f-1}{2}}\Big)$	$\frac{(p-1)(p-2)}{2}p^{r_f-2}\Big(1-\varepsilon_f\bar{\eta}(-f(x_\alpha))(p^*)^{-\frac{r_f-1}{2}}\Big)$
$p^{m-2}(p-1)\Big(1+\varepsilon_f\bar{\eta}(-f(x_\alpha)\Big)(p^*)^{-\frac{r_f-1}{2}})$	$\frac{(p-1)}{2}p^{r_f-1}\Big(1-\varepsilon_f\bar{\eta}(-f(x_\alpha)\Big)(p^*)^{-\frac{r_f-1}{2}})+p^m-p^{r_f}$

Table 4 The weight distribution of C_D of Theorem 1 when r_f is odd and $f(x_\alpha)=0$

Weight w	Multiplicity A_w
0	1
$p^{m-2}\Big(p-1-\varepsilon_f(p-1)(p^*)^{-\frac{r_f-1}{2}}\Big)$	$\frac{p-1}{2}p^{r_f-2}\Big(1+\varepsilon_f\cdot p(p^*)^{-\frac{r_f-1}{2}}\Big)$
$p^{m-2}\Big(p-1+\varepsilon_f(p-1)(p^*)^{-\frac{r_f-1}{2}}\Big)$	$\frac{p-1}{2}p^{r_f-2}\Big(1-\varepsilon_f\cdot p(p^*)^{-\frac{r_f-1}{2}}\Big)$
$p^{m-2}\Big(p-1+\varepsilon_f(p^*)^{-\frac{r_f-1}{2}}\Big)$	$\frac{(p-1)^2}{2}p^{r_f-2}$
$p^{m-2}\Big(p-1-\varepsilon_f(p^*)^{-\frac{r_f-1}{2}}\Big)$	$\frac{(p-1)^2}{2}p^{r_f-2}$
$p^{m-2}(p-1)$	$p^{r_f-1}+p^m-p^{r_f}-1$

Next we shall prove the the multiplicities A_{w_i} of codewords with weight w_i in C_D. Let us give the proofs of four cases, respectively.

(1) The case that r_f is even and $f(x_\alpha)\neq 0$.
We only give the proof for the case $-f(x_\alpha)\in$ SQ and omit the proof for the case $-f(x_\alpha)\in$ NSQ whose proof is similar. Suppose that $-f(x_\alpha)\in$ SQ. For each $\beta\in$

GF$(q)^*$, then from Lemmas 9 and 15 we obtain the Hamming weight

$$\mathrm{wt}(\mathbf{c}_\beta) = N_f(\alpha) - N_{f,\beta}(\alpha) = \begin{cases} B_1 & \text{if } f(x_\beta) = \mathrm{Tr}(\alpha x_\beta) = 0 \, or \, f(x_\beta)\cdot E \in \mathrm{NSQ}, \\ B_1 - Bp & \text{if } f(x_\beta) = 0 \, and \, \mathrm{Tr}(\alpha x_\beta) \neq 0 \, or \, f(x_\beta) \neq 0 \, and \, E = 0, \\ B_1 - 2Bp & \text{if } f(x_\beta)\cdot E \in \mathrm{SQ}, \\ B_1 - B(p-1) & \text{if } \beta \notin Im(L_f), \end{cases}$$

where $B_1 = p^{m-2}(p-1)$ and $B = p^{m-2}\varepsilon_f(p^*)^{-\frac{r_f}{2}}$. Define

$$w_1 = B_1, w_2 = B_1 - Bp, w_3 = B_1 - 2Bp, w_4 = B_1 - 2B(p-1).$$

Let

$$M_1 = \#\{\beta \in \mathrm{GF}(q) : f(x_\beta) = \mathrm{Tr}(\alpha x_\beta) = 0\} + \#\{\beta \in \mathrm{GF}(q) : f(x_\beta)\cdot E \in \mathrm{NSQ}\}$$

Since the rank of the linear mapping GF$(q) \to$ GF(q) $(x_\beta \mapsto -2L_f(x_\beta))$ is r_f, the dimension of their kernel is $m - r_f$. Therefore,

$$\begin{aligned} M_1 &= p^{r_f-m}\#\{x \in \mathrm{GF}(q) : f(x) = \mathrm{Tr}(\alpha x) = 0\} \\ &\quad + p^{r_f-m}\#\{x \in \mathrm{GF}(q) : f(x)\cdot E \in \mathrm{NSQ}\} \\ &= p^{r_f-2} + \frac{p-1}{2}p^{r_f-1}(1 - \varepsilon_f \cdot p(p^*)^{-\frac{r_f}{2}}). \qquad \text{(By Lemma 18)} \end{aligned}$$

Note that $f(0) = \mathrm{Tr}(\alpha \cdot 0) = 0$. Then

$$\begin{aligned} A_{w_1} &= \#\{\beta \in \mathrm{GF}(q) : \mathrm{wt}(\mathbf{c}_\beta) = (p-1)p^{m-2}\} \\ &= M_1 - 1 \\ &= p^{r_f-2} + \frac{p-1}{2}p^{r_f-1}(1 - \varepsilon_f \cdot p(p^*)^{-\frac{r_f}{2}}) - 1. \end{aligned}$$

Similarly, the values of A_{w_2}, A_{w_3} and A_{w_4} can be calculated. This completes the proof of the weight distribution of Table 1.

(2) The case that r_f is even and $f(x_\alpha) = 0$.
The proof is similar to Case 1) and we omit it here. The desired conclusion then follows from Lemmas 9 and 11.

(3) The case that r_f is odd and $f(x_\alpha) \neq 0$.
The proof is similar to Case 1) and we omit it here. The desired conclusion then follows from Lemmas 9 and 18.

(4) The case that r_f is odd and $f(x_\alpha) = 0$.
The proof is similar to case 1) and we omit it here. The desired conclusion then follows from Lemmas 9 and 19.

□

For special cases of Theorem 1, the following two corollaries are direct consequences of Theorem 1.

Corollary 1 *Let* $u \in \mathrm{GF}(q)^*$, $f(x) = \mathrm{Tr}(ux^2)$ *and* $\alpha \in \mathrm{GF}(q)^*$. *Then*

- $\alpha \in \mathrm{Im}(L_f)$,
- $\varepsilon_f = (-1)^{m-1}\,\eta(-u)$,
- $r_f = m$,
- $L_f(x) = ux$,

Table 5 The weight distribution of C_D of Theorem 2 when r_f is even

Weight w	Multiplicity A_w
0	1
$p^{m-2}(p-1)\left(1-\varepsilon_f(p^*)^{-\frac{r_f}{2}}\right)$	$(p-1)p^{r_f-1}\left(1+\varepsilon_f(p-1)(p^*)^{-\frac{r_f}{2}}\right)$
$p^{m-2}(p-1)+\varepsilon_f p^{m-2}(p^*)^{-\frac{r_f}{2}}$	$(p-1)^2p^{r_f-1}\left(1-\varepsilon_f(p^*)^{-\frac{r_f}{2}}\right)$
$p^{m-2}(p-1)$	$p^m-(p-1)p^{r_f}-1$

- $x_\alpha = -\frac{\alpha}{2u}$ *and* $f(x_\alpha) = \frac{1}{4}\mathrm{Tr}(\frac{\alpha^2}{u})$.

Thus, using this function f, we can construct linear code C_D with the parameter and weight distribution given by Theorem 1.

Corollary 2 *Let* $v \in \mathrm{GF}(q)^*$, $\mathrm{Tr}(v^2) \neq 0$, $f(x) = \mathrm{Tr}(x^2) - \frac{1}{\mathrm{Tr}(v^2)}(\mathrm{Tr}(vx))^2$, $\alpha \in \mathrm{GF}(q)^*$ *and* $\mathrm{Tr}(v\alpha) = 0$. *Then*

- $\alpha \in \mathrm{Im}(L_f)$,
- $\varepsilon_f = (-1)^{m-1}\,\eta(-1)\bar{\eta}(-\mathrm{Tr}(v^2))$,
- $r_f = m-1$,
- $L_f(x) = x - \frac{v}{\mathrm{Tr}(v^2)}\mathrm{Tr}(vx)$.

Thus, we can construct linear code C_D with the parameter and weight distribution given by Theorem 1.

For special cases of Corollary 1, we give the following two examples.

Example 1 Let $(u, p, m) = (1, 3, 4)$, $\alpha \in \mathrm{GF}(q)^*$ and $\mathrm{Tr}(\alpha) \neq 0$. Then the code C_D has parameters $[29, 4, 18]$ and weight enumerator $1 + 44z^{18} + 30z^{21} + 6z^{24}$, which is verified by the Magma program.

Example 2 Let $(u, p, m) = (1, 3, 5)$ and $\alpha \in \mathrm{GF}(p)^*$. Then the code C_D has parameters $[71, 5, 42]$ and weight enumerator $1 + 30z^{42} + 60z^{45} + 90z^{48} + 42z^{51} + 20z^{54}$, which is verified by the Magma program.

For special cases of Corollary 2, we give the following two examples.

Example 3 Let $(v, p, m) = (1, 3, 5)$, g be a generator of $\mathrm{GF}(q)^*$ with the minimal polynomial $x^5 + 2x + 1$. Let $\alpha = g^2$. Then the code C_D has parameters $[89, 5, 54]$ and weight enumerator $1 + 44z^{54} + 162z^{60} + 30z^{63} + 6z^{72}$, which is verified by the Magma program.

Example 4 Let $(v, p, m) = (1, 3, 4)$, g be a generator of $\mathrm{GF}(q)^*$ with the minimal polynomial $x^4 + 2x^3 + 2$. Let $\alpha = g^5$. Then the code C_D has parameters $[17, 4, 6]$ and weight enumerator $1 + 4z^4 + 8z^9 + 66z^{12} + 2z^{15}$, which is verified by the Magma program.

Theorem 2 *Let f be a homogeneous quadratic function with rank r_f and the sign ε_f. let $\alpha \notin \mathrm{Im}(L_f)$ and D be defined in (8). Then the set C_D of (1) is an $[n, m]$ linear code over* $\mathrm{GF}(p)$ *with the weight distribution in Tables 5* and *6, where* $n = p^{m-1} - 1$.

Proof The proof is similar to Case (1) of Theorem 1 and we omit it here. We point out that:

Table 6 The weight distribution of C_D of Theorem 2 when r_f is odd

Weight w	Multiplicity A_w
0	1
$p^{m-2}\left(p-1-\varepsilon_f(p^*)^{-\frac{r_f-1}{2}}\right)$	$\frac{(p-1)^2}{2}p^{r_f-1}\left(1+\varepsilon_f(p^*)^{-\frac{r_f-1}{2}}\right)$
$p^{m-2}\left(p-1+\varepsilon_f(p^*)^{-\frac{r_f-1}{2}}\right)$	$\frac{(p-1)^2}{2}p^{r_f-1}\left(1-\varepsilon_f(p^*)^{-\frac{r_f-1}{2}}\right)$
$p^{m-2}(p-1)$	$p^m-(p-1)^2p^{r_f-1}-1$

– when r_f is even, the desired conclusion then follows from Lemma 14,
– when r_f is odd, the desired conclusion then follows from Lemmas 14 and 7.

This completes the proof. □

As special cases of Theorem 2, the following corollary is a direct consequence of Theorem 2.

Corollary 3 *Let* $v \in \mathrm{GF}(q)^*$, $\mathrm{Tr}(v^2) \neq 0$, $f(x) = \mathrm{Tr}(x^2) - \frac{1}{\mathrm{Tr}(v^2)}(\mathrm{Tr}(vx))^2$, $\alpha \in \mathrm{GF}(q)^*$ *and* $\mathrm{Tr}(v\alpha) \neq 0$. *Then*

– $\alpha \notin \mathrm{Im}(L_f)$,
– $\varepsilon_f = (-1)^{m-1}\,\eta(-1)\bar{\eta}(-\mathrm{Tr}(v^2))$,
– $r_f = m-1$,
– $L_f(x) = x - \frac{v}{\mathrm{Tr}(v^2)}\mathrm{Tr}(vx)$.

Thus, we can construct linear code C_D with the parameter and weight distribution given by Theorem 2.

As special cases of Corollary 3, we give the following two examples.

Example 5 Let $(v, p, m) = (1, 3, 5)$ and $\alpha \in \mathrm{GF}(p)^*$. Then the code C_D has parameters $[26, 5, 15]$ and weight enumerator $1+24z^{15}+44z^{18}+12z^{21}$, which is verified by the Magma program.

Example 6 Let $(v, p, m) = (1, 3, 4)$ and $\alpha \in \mathrm{GF}(p)^*$. Then the code C_D has parameters $[80, 4, 51]$ and weight enumerator $1 + 120z^{51} + 80z^{54} + 42z^{60}$, which is verified by the Magma program.

4 Concluding remarks

In this paper, inspired by the works of [7,22], inhomogeneous quadratic functions were used to construct linear codes with few nonzero weights over finite fields. It was shown that the presented linear codes have at most five nonzero weights. The weight distributions of the codes were also determined and some of constructed linear codes are optimal in the sense that their parameters meet certain bound on linear codes. The work of this paper extended the main results in [7,22].

Acknowledgements The authors are very grateful to the reviewers and the Editor, for their comments and suggestions that improved the presentation and quality of this paper. The research of K. Feng was supported by NSFC No. 11471178, 11571007 and the Tsinghua National Lab. for Information Science and Technology. The research of C. Tang was supported by NSFC No. 11401480, 11531002. C. Tang also acknowledges support from 14E013 and CXTD2014-4 of China West Normal University.

References

1. Calderbank A.R., Goethals J.M.: Three-weight codes and association schemes. Philips J. Res. **39**, 143–152 (1984).
2. Calderbank A.R., Kantor W.M.: The geometry of two-weight codes. Bull. Lond. Math. Soc. **18**, 97–122 (1986).
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. Ding C.: Linear codes from some 2-designs. IEEE Trans. Inf. Theory **61**(6), 3265–3275 (2015).
5. Ding C.: A construction of binary linear codes from Boolean functions. Discret. Math. **339**(9), 2288–2303 (2016).
6. Ding K., Ding C.: Binary linear codes with three weights. IEEE Commun. Lett. **18**(11), 1879–1882 (2014).
7. 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).
8. Ding C., Wang X.: A coding theory construction of new systematic authentication codes. Theor. Comput. Sci. **330**, 81–99 (2005).
9. Ding C., Yang J.: Hamming weights in irreducible cyclic codes. Discret. Math. **313**(4), 434–446 (2013).
10. Ding C., Helleseth T., Klove T., Wang X.: A generic construction of Cartesian authen- tication codes. IEEE Trans. Inf. Theory **53**(6), 2229–2235 (2007).
11. 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).
12. Feng K., Luo J.: Value distribution of exponential sums from perfect nonlinear functions and their applications. IEEE Trans. Inf. Theory **53**(9), 3035–3041 (2007).
13. Ireland K., Rosen M.: A classical introduction to modern number theory. In: Graduate Texts in Mathematics, vol. 84, 2nd edn. Springer, New York (1990).
14. Klve T.: Codes for Error Detection. World Scientific, Hackensack (2007).
15. Lidl R., Niederreiter H.: Finite Fields. Cambridge University Press, Cambridge (1997).
16. Li F., Wang Q., Lin D.: A class of three-weight and five-weightlinear codes, arXiv:1509.06242v1 (2015).
17. Mesnager S.: Linear codes with few weights from weakly regular bent functions based on a generic construction. IACR Cryptol. **2015**, 1103 (2015).
18. Qi Y., Tang C., Huang D.: Binary linear codes with few weights. IEEE Commun. Lett. **20**(2), 208–211 (2016).
19. 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).
20. Tang C., Qi Y., Huang D.: Two-weight and three-weight linear codes from square functions. IEEE Commun. Lett. **20**(1), 29–32 (2016).
21. Xiang C., Tang C., Feng K.: A class of linear codes with a few weights, arXiv:1512.07103v1 (2015).
22. Zhou Z., Li N., Fan C., Helleseth T.: Linear codes with two or three weights from quadratic bent functions, Des. Codes Cryptogr. 1–13 (2015).