The Subfield Codes of Some Few-Weight Linear Codes
Li Xu, Cuiling Fan, Sihem Mesnager, Rong Luo

Abstract

Subfield codes of linear codes over finite fields have recently received a lot of attention, as some of these codes are optimal and have applications in secret sharing, authentication codes and association schemes. In this paper, the \( q \)-ary subfield codes \( C_{f,g}^{(q)} \) of six different families of linear codes \( C_{f,g} \) are presented, respectively. The parameters and weight distribution of the subfield codes and their punctured codes \( C_{f,g}^{(q)} \) are explicitly determined. The parameters of the duals of these codes are also studied. Some of the resultant \( q \)-ary codes \( C_{f,g}^{(q)}, C_{f,g}^{(\bar{q})} \) and their dual codes are optimal and some have the best known parameters. The parameters and weight enumerators of the first two families of linear codes \( C_{f,g} \) are also settled, among which the first family is an optimal two-weight linear code meeting the Griesmer bound, and the dual codes of these two families are almost MDS codes. As a byproduct of this paper, a family of \([2^{m-2}, 2m + 1, 2^{m-3}]\) quaternary Hermitian self-dual code are obtained with \( m \geq 2 \). As an application, several infinite families of 2-designs and 3-designs are also constructed with three families of linear codes of this paper.

Index Terms
Linear codes, Subfield codes, Weight distribution, Few-weight codes,

I. INTRODUCTION

Let \( p \) be a prime, \( q = p^l \) for a positive integer \( l \). Let \( \mathbb{F}_q \) be the finite field with \( q \) elements. A \( q \)-ary \([n, k, d]_2\) linear code is a \( k \)-dimensional subspace of \( \mathbb{F}_q^n \) with minimum Hamming distance \( d \). An \([n, k, d]_2\) linear code is said to be optimal if no \([n, k, d']_2\) code with \( d' > d \) exists. The generator matrix of \( C \) is a \( k \times n \) matrix \( G \) whose rows form a basis of \( C \) as an \( \mathbb{F}_q \)-vector space, since \( C = \{xG : x \in \mathbb{F}_q^n\} \). The dual code of \( C \) is defined to be its orthogonal subspace \( C^\perp \) with respect to the Euclidean inner product, i.e., \( C^\perp = \{x \in \mathbb{F}_q^n : x \cdot c = 0, \forall c \in C\} \). For some \( i \in \{1, 2, \ldots, n\} \), puncture \( C \) by deleting the same coordinate \( i \) in each codeword, and denote the punctured code by \( \bar{C} \). If \( G \) is a generator matrix for \( C \), then a generator matrix for \( \bar{C} \) is obtained from \( G \) by deleting column \( i \) (and omitting a zero or duplicate rows that may occur).

Let \( A_i \) denote the number of codewords with Hamming weight \( i \) in a code \( C \) of length \( n \). The weight enumerator of \( C \) is defined by \( 1 + A_1 z + A_2 z^2 + \cdots + A_n z^n \). The sequence \((A_0 = 1, A_1, A_2, \cdots, A_n)\) is called the weight distribution of the code. The study of the weight distribution of a linear code is important both in theory and applications due to the following [31]:

- The weight distribution gives the minimum distance of the code, and thus the error correcting capability.
- 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.

A code \( C \) is said to be a \( t \)-weight code if the number of nonzero \( A_i \) in the sequence \((A_1, A_2, \cdots, A_n)\) is equal to \( t \). The construction of linear codes with few weights is also a meaningful research because they have important applications in secret sharing [1], [8], association schemes [4], strongly regular graphs [5] and authentication codes [9]. In finite geometry, hyperovals in \( \text{PG}(2, 2^m) \) and conics in \( \text{PG}(2, q) \) are the same as the MDS codes with two or three weights [17], maximal \((n, h)\)-arcs in \( \text{PG}(2, 2^m) \) and ovoids in \( \text{PG}(3, q) \) are also the same as a special type of two-weights codes [17]. For more information on few-weight linear codes, the reader is referred to [10]–[12].

Li Xu, Cuiling Fan and Rong Luo are with the School of Mathematics, Southwest Jiaotong University, Chengdu, 610031, China (e-mail: xuli1451@163.com; cuilingfan@163.com; luorong@swjtu.edu.cn).
Sihem Mesnager is with the Department of Mathematics, University of Paris VIII, 93526 Saint-Denis, France, University of Paris XIII, CNRS, UMR 7539 LAGA, Sorbonne Paris Cité, 93430 Villetaneuse, France, and Telecom Paris, Polytechnic Institute of Paris, 91120 Palaiseau, France. (e-mail: smesnager@univ-paris8.fr).
Subfield codes were first studied in \cite{6,7} in order to construct the linear codes with good parameters over \( \mathbb{F}_q \) from a linear codes over \( \mathbb{F}_{q^m} \). Recently, some basic results about subfield codes were derived and the subfield codes of ovoid codes were studied in \cite{18}. It was demonstrated that the subfield codes of ovoid codes are very attractive \cite{18}. The subfield codes of some hyperoval codes and conic codes were also studied in \cite{22} and these results were later extended in \cite{49,51}. In \cite{24}, optimal binary linear codes were constructed from maximal arcs. Meanwhile, some known linear codes can be obtained by taking appropriate functions \( f(x), g(x) \), \( x \in \mathbb{F}_{q^m} \), \( y \in \mathbb{F}_q \). In \cite{23}, \( \mathbb{F}_q \) is a conic code when \( q \) is odd, \( f(x) = x^q + \cdots + x^2 + 1 \) and \( g(x) = x^2 + 1 \) \cite{27}. As show in these mentioned papers, subfield codes of linear codes are a significant study object in coding theory, because some of these codes are optimal (or almost optimal) and always have few weights.

Let \( f(x) \) and \( g(x) \) be two different functions from \( \mathbb{F}_{q^m} \) to \( \mathbb{F}_q \), where \( m \) is a positive integer. Denote 

\[
\mathcal{S}_{f,g} = \{(1, x, y) : (x, y) \in \mathbb{F}_q^2, f(x) + g(y) = 0\}
\]

and 

\[
G_{\mathcal{S}_{f,g}} = \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}
\]

which is a \( 3 \times (\# \mathcal{C}) \) matrix over \( \mathbb{F}_q \), where \( \# \mathcal{C} \) is the cardinality of set \( \mathcal{C} = \{(x, y) \in \mathbb{F}_q^2 : f(x) + g(y) = 0\} \).

We construct a linear code \( C_{f,g} \) over \( \mathbb{F}_{q^m} \) with generator matrix 

\[
G_{f,g} = \begin{pmatrix} 0 & 0 \\ 1 & G_{\mathcal{S}_{f,g}} \end{pmatrix}
\]

(1)

Some known linear codes can be obtained by taking appropriate functions \( f(x) \) and \( g(y) \). It turns out that,

- \( C_{f,g} \) is a punctured hyperoval code when \( q \) is even, \( f(x) = x \) and \( g(y) \) is an oval polynomial \cite{27};
- \( C_{f,g} \) is a conic code when \( q \) is odd, \( f(x) = x \) and \( g(y) = y^2 \) \cite{27}.

Throughout this paper, we use \( \text{Tr}_{q^m/q} \) and \( \text{Norm}_{q^m/q} \) to denote the trace and norm functions from \( \mathbb{F}_{q^m} \) onto \( \mathbb{F}_q \), respectively, which are defined by 

\[
\text{Tr}_{q^m/q}(x) = x + x^q + \cdots + x^{q^{m-1}},
\]

\[
\text{Norm}_{q^m/q}(x) = x^{q^m-1}/(q-1),
\]

where \( x \in \mathbb{F}_{q^m} \). Let \( A(x) \) be an almost bent function and \( B(x) \) be a Boolean bent function. In this paper, we focus on six families of linear codes \( C_{f,g} \), where \( f \) and \( g \) are distinct and taken from the set of functions 

\[
\{\text{Tr}_{q^m/q}(x), \text{Tr}_{q^m/q}(x^2), \text{Norm}_{q^m/q}(x), \text{Tr}_{2m/2}(A(x)), \text{Tr}_{2m/2}(B(x))\}.
\]

When \( m = 2 \), \( f(x) = \text{Tr}_{q^2/q}(x) \) and \( g(x) = \text{Norm}_{q^2/q}(x) \), we show that \( C_{f,g} \) is an optimal two-weight code achieving the Griesmer bound, and its dual is an almost MDS code. For general integer \( m \), when \( f(x) = \text{Tr}_{q^m/q}(x) \) and \( g(x) = \text{Tr}_{q^m/q}(x^2) \), \( C_{f,g} \) is shown to have four or five weights, its dual is also an almost MDS code. The subfield codes and the punctured code of the subfield codes of these two families of few-weight codes are also studied. All of these resultant codes are \( q \)-ary few-weight codes, some of them and their dual codes are optimal and some have the best known parameters. Specially, when \( q = 2 \), the binary subfield codes and the punctured codes of four different families of \( C_{f,g} \) are studied with 

\[
\{(\text{Tr}_{2m/2}(x)), (\text{Tr}_{2m/2}(A(x))), (\text{Tr}_{2m/2}(A_1(x))), (\text{Tr}_{2m/2}(A_2(x))).\}
\]

Seven families of few-weight binary linear codes are presented and most of their dual code are optimal respect to the sphere packing bound.

The rest of this paper is arranged as follows. Section \( \text{III} \) recalls some notations and basics of characters, linear codes and some special functions, which will be used in subsequent sections. Section \( \text{III} \) studies the \( q \)-ary subfield codes \( C_{f,g}^{(q)} \) and the punctured code \( \tilde{C}_{f,g}^{(q)} \) of the subfield codes of six different families of \( C_{f,g} \) respectively. The parameters and weight enumerators of the first two families of linear codes \( C_{f,g} \) are also determined. Some of the
resultant $q$-ary few-weight codes and their dual codes are optimal and some have the best known parameters. As a byproduct, a family of $[2^{4m-2}, 2m + 1, 2^{4m-3}]$ quaternary Hermitian self-dual code are obtained, where $m \geq 2$. Section [V] presents several infinite families of 2-designs or 3-designs with some of the codes presented in this paper. Section [V] summarizes this paper.

II. PRELIMINARIES

In this section, we briefly introduce some known results about characters and linear codes over finite fields and some special functions on $\mathbb{F}_{2^m}$, which will be used later in this paper.

A. Characters Over Finite Fields

Let $\mathbb{F}_q$ be a finite field with $q$ elements, where $q$ is a power of a prime $p$. Denote by $\zeta_p$ the primitive $p$-th root of complex unity. The additive character of $\mathbb{F}_q$ is defined as a homomorphism $\chi$ from $\mathbb{F}_q$ into the complex unit group such that $\chi(x + y) = \chi(x)\chi(y)$ for $x, y \in \mathbb{F}_q$. For any $a \in \mathbb{F}_q$, the function defined by

$$\chi_a(x) = \zeta_p^{\text{Tr}_q(\mathbb{F}_q)(ax)}, \quad x \in \mathbb{F}_q$$

is an additive character of $\mathbb{F}_q$. In addition, $\{\chi_a : a \in \mathbb{F}_q\}$ is a group containing all the additive character of $\mathbb{F}_q$. When $a = 0$, we obtain the trivial additive character $\chi_0$, for which $\chi_0(x) = 1$ for all $x \in \mathbb{F}_q$. When $a = 1$, $\chi_1$ is called the canonical additive character of $\mathbb{F}_q$. It’s obvious that $\chi_a(x) = \chi_1(ax)$. A crucial property of the additive characters, called the orthogonality [36], is given as follows:

$$\sum_{x \in \mathbb{F}_q} \chi_1(ax) = \begin{cases} q & \text{for } a = 0, \\
0 & \text{for } a \in \mathbb{F}_q^* \end{cases}$$

where $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$.

A character of the multiplicative group $\mathbb{F}_q^*$ is defined as a homomorphism $\psi$ from $\mathbb{F}_q^*$ into the complex unit group such that $\psi(xy) = \psi(x)\psi(y)$ for all $x, y \in \mathbb{F}_q^*$. $\psi$ is also called multiplicative character of $\mathbb{F}_q$. Let $g$ be a fixed primitive element of $\mathbb{F}_q$. For each $j = 0, 1, \cdots, q - 2$, the function

$$\psi_j \left(g^k\right) = \zeta_{q-1}^j k \quad \text{for } k = 0, 1, \cdots, q - 2$$

defines a multiplicative character of $\mathbb{F}_q$, and every multiplicative character of $\mathbb{F}_q$ is obtained in this way. No matter what $q$ is, the character $\psi_0$ will always represent the trivial multiplicative character, which satisfies $\psi_0(x) = 1$ for all $x \in \mathbb{F}_q^*$. $\eta := \psi_1(1/q) = (q - 1)/2$ is called the quadratic character of $\mathbb{F}_q$. The orthogonality relation of multiplicative characters is given by

$$\sum_{x \in \mathbb{F}_q^*} \psi_j(x) = \begin{cases} q - 1 & \text{for } j = 0, \\
0 & \text{for } j \neq 0. \end{cases}$$

For an additive character $\chi$ and a multiplicative character $\psi$ of $\mathbb{F}_q$, the Gauss sum $G(\psi, \chi)$ over $\mathbb{F}_q$ is defined by

$$G(\psi, \chi) = \sum_{x \in \mathbb{F}_q} \psi(x)\chi(x).$$

We call $G(\eta, \chi)$ the quadratic Gauss sum over $\mathbb{F}_q$ for nontrivial $\chi$. The value of the quadratic Gauss sum is known and documented below.

**Lemma 1** ([36]): Let $q = p^l$ with an odd prime $p$ and a positive integer $l$. Let $\chi$ be the canonical additive character of $\mathbb{F}_q$. Then

$$G(\eta, \chi) = \begin{cases} (-1)^{l-1}\sqrt{q} & \text{if } p \equiv 1 \mod 4, \\
(-1)^{l-1}(\sqrt{-1})^l \sqrt{q} & \text{if } p \equiv 3 \mod 4, \\
(-1)^{l-1}(\sqrt{-1})^{(q+1)/2}\sqrt{q}. \end{cases}$$
Let $\chi$ be a nontrivial additive character of $\mathbb{F}_q$ and let the polynomial $f \in \mathbb{F}_q[x]$ be of positive degree. The character sums of the form
\[
\sum_{c \in \mathbb{F}_q} \chi(f(c))
\]
are sometimes referred to as Weil sums. The problem of evaluating such character sums explicitly is difficult. One usually has to be satisfied with estimates for the absolute value of the sum. In certain special cases, these character sums can be treated, see [36].

When $f$ is a quadratic polynomial and $q$ is odd, the Weil sums have an interesting relationship with quadratic Gauss sums, which is described in the following lemma.

**Lemma 2 ([36]):** Let $\chi$ be a nontrivial additive character of $\mathbb{F}_q$ with $q$ odd, and let $f(x) = a_2 x^2 + a_1 x + a_0 \in \mathbb{F}_q[x]$ with $a_2 \neq 0$. Then
\[
\sum_{c \in \mathbb{F}_q} \chi(f(c)) = \chi \left( a_0 - a_1^2 \left(4a_2\right)^{-1} \right) \eta(a_2) G(\eta, \chi).
\]

The Weil sums can also be evaluated explicitly in case $f$ is a quadratic polynomial and $q$ is even.

**Lemma 3 ([36]):** Let $\chi, b \in \mathbb{F}_q^*$, be a nontrivial additive character of $\mathbb{F}_q$ with $q$ even, and let $f(x) = a_2 x^2 + a_1 x + a_0 \in \mathbb{F}_q[x]$. Then
\[
\sum_{c \in \mathbb{F}_q} \chi_b(f(c)) = \begin{cases} 
\chi_b(a_0) q & \text{if } a_2 = ba_1^2, \\
0 & \text{otherwise.}
\end{cases}
\]

We consider now character sums involving only the quadratic character $\eta$ of $\mathbb{F}_q$, $q$ odd, and having quadratic polynomial arguments, that is, sums of the form
\[
\sum_{c \in \mathbb{F}_q} \eta(f(c))
\]
with $f(x) = a_2 x^2 + a_1 x + a_0 \in \mathbb{F}_q[x]$. The explicit formula is as follows.

**Lemma 4 ([36]):** Let $f(x) = a_2 x^2 + a_1 x + a_0 \in \mathbb{F}_q[x]$ with $q$ odd and $a_2 \neq 0$. Put $d = a_1^2 - 4a_0a_2$. Then
\[
\sum_{c \in \mathbb{F}_q} \eta(f(c)) = \begin{cases} 
-\eta(a_2) & \text{if } d \neq 0, \\
(q-1)\eta(a_2) & \text{if } d = 0.
\end{cases}
\]

Let $f \in \mathbb{F}_q[x]$ be a monic quadratic polynomial, the number of solutions of $f(x) = 0$ in $\mathbb{F}_q$ is given by the following lemma.

**Lemma 5 ([36]):** Let $a_0, a_1 \in \mathbb{F}_q$, where $q = p^l$. Define $N_{a_0,a_1} = \# \{ x \in \mathbb{F}_q : x^2 + a_1 x + a_0 = 0 \}$. Then $N_{a_0,a_1} \in \{0,1,2\}$. More precisely, for $p = 2$,
\[
N_{a_0,a_1} = \begin{cases} 
0 & \text{if } \text{Tr}_{2^l/2}(a_0^2) = 1, \\
1 & \text{if } a_1 = 0, \\
2 & \text{if } \text{Tr}_{2^l/2}(a_0^2) = 0;
\end{cases}
\]

and for $p > 2$,
\[
N_{a_0,a_1} = \begin{cases} 
0 & \text{if } \eta(a_1^2 - 4a_0) = -1, \\
1 & \text{if } a_1^2 - 4a_0 = 0, \\
2 & \text{if } \eta(a_1^2 - 4a_0) = 1.
\end{cases}
\]
B. Finite Projective Geometry

The projective space of dimensional $r$ obtained from $\mathbb{F}_q$ will be denoted by $\text{PG}(r, q)$, where its points are the one-dimensional subspaces of $\mathbb{F}_q^{r+1}$ and its hyperplanes are the $r$-dimensional subspaces of $\mathbb{F}_q^{r+1}$. Obviously any hyperplane can be defined to be $H_u = \{ x \in \mathbb{F}_q^{r+1} : x \cdot u = 0 \}$ for some nonzero vector $u \in \mathbb{F}_q^{r+1}$.

For a $q$-ary $[n, k, d]$ linear code $C$ with a generator matrix $G = (g_1 \ldots g_n)$, if we view the columns of $G$ to be projective points (maybe repeated) in $\text{PG}(k-1, q)$, and define $S = \{g_1, \ldots, g_n\}$ to be a multiset. The following lemma states a relationship between weights of codewords in $C$ and hyperplanes in $\text{PG}(k-1, q)$.

**Lemma 6 (13):** Let $u$ be a nonzero vector of $\mathbb{F}_q^n$. The codeword $uG$ has weight $w$ if and only if the hyperplane $H_u$ in $\text{PG}(k-1, q)$ contains $n - w$ points of $S$, i.e., $wt(uG) = n - \#(H_u \cap S)$.

From this lemma, for any $0 < i \leq n$, the number of codewords with weight $i$ in code $C$ is

$$A_i = \#\{ u \in \mathbb{F}_q^n \setminus \{0\} : \#(H_u \cap S) = n - i \}.$$ 

This property plays an important role in determining the weight distribution of linear code $C_{f,g}$ generated by $I$.

C. The Subfield Codes of Linear Codes

Given an $[n, k]$ linear code over $\mathbb{F}_{q^m}$. We construct a new $[n, k']$ code $C^{(q)}$ over $\mathbb{F}_q$ as follows. Let $G$ be a generator matrix of $C$. Take a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Represent each entry of $G$ as an $m \times 1$ column vector of $\mathbb{F}_{q^m}$ with respect to this basis, and replace each entry of $G$ with the corresponding $m \times 1$ column vector of $\mathbb{F}_q$. In this way, $G$ is modified into a $km \times n$ matrix over $\mathbb{F}_q$, which generates the new subfield code $C^{(q)}$ over $\mathbb{F}_q$ with length $n$. It is known that the subfield code $C^{(q)}$ is independent of both the choice of the basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and the choice of the generator matrix $G$ [13].

By definition, the dimension $k'$ of $C^{(q)}$ satisfies $k' \leq mk$. The relationship between the minimal distance of $C^{\perp}$ and that of $C^{(q)\perp}$ is given as follows.

**Lemma 7 (13):** The minimal distance $d^{\perp}$ of $C^{\perp}$ and the minimal distance $d^{(q)\perp}$ of $C^{(q)\perp}$ satisfy

$$d^{(q)\perp} \geq d^{\perp}.$$ 

The trace representation of the $q$-ary subfield code $C^{(q)}$ of $C$ is given in the next lemma.

**Lemma 8 (13):** Let $C$ be an $[n, k]$ linear code over $\mathbb{F}_{q^m}$. Let $G = [g_{ij}]_{1 \leq i \leq k, 1 \leq j \leq n}$ be a generator matrix of $C$. Then the trace representation of the subfield code $C^{(q)}$ is given by

$$C^{(q)} = \left\{ \left( \text{Tr}_{q^m/q} \left( \sum_{i=1}^{k} a_i g_{i1} \right), \ldots, \text{Tr}_{q^m/q} \left( \sum_{i=1}^{k} a_i g_{im} \right) \right) : a_1, \ldots, a_k \in \mathbb{F}_{q^m} \right\}.$$ 

**Remark 1:** It follows from this lemma that the $q$-ary subfield code $C^{(q)}$ of a linear code $C$ over $\mathbb{F}_{q^m}$ is in fact the trace code $\text{Tr}_{q^m/q}(C)$ of $C$, which is different from the subfield subcode well studied in the literature.

D. Pless Power Moments and Two Bounds for Linear Codes

To study the minimal distances of the dual codes of some codes, we need the Pless power moments for linear codes. Let $C$ be a $q$-ary $[n, k]$ code with weight distribution $(1, A_1, \cdots, A_n)$, we denote by $(1, A_1^{\perp}, \cdots, A_n^{\perp})$ the weight distribution of its dual code. The first four Pless power moments on these two weight distributions are given as follows [20].
A function \( f \) where
\[
\sum_{j=0}^{n} A_j = q^k, \\
\sum_{j=0}^{n} jA_j = q^{k-1} \left( qn - n - A_1^1 \right), \\
\sum_{j=0}^{n} j^2 A_j = q^{k-2} (q-1)n(qn - n + 1) - q^{k-2} \left( (2qn - q - 2n + 2)A_1^1 + 2A_2^1 \right), \\
\sum_{j=0}^{n} j^3 A_j = q^{k-3} \left[ (q - 1)n \left( q^2n^2 - 2qn^2 + 3qn - q + n^2 - 3n + 2 \right) \right.
\left. - \left( 3q^2n^2 - 3q^2n - 6qn^2 + 12qn + q^2 - 6q + 3n^2 - 9n + 6 \right) A_1^1 + 6(qn - q - n + 2)A_2^1 - 6A_3^1 \right].
\]

We will also need the following two classical bounds for linear codes [20].

**Lemma 9** (Griesmer bound): Let \( C \) be an \([n, k, d]\) linear code over \( \mathbb{F}_q \) with \( k \geq 1 \). Then
\[
n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil,
\]
where \( \lceil \cdot \rceil \) denotes the ceiling function.

**Lemma 10** (Sphere packing bound): Let \( C \) be an \([n, k, d]\) linear code over \( \mathbb{F}_q \). Then
\[
q^n \geq q^k \sum_{i=0}^{t} \binom{n}{i} (q - 1)^i,
\]
where \( t = \left\lfloor \frac{d-1}{2} \right\rfloor \) and \( \lfloor \cdot \rfloor \) denotes the floor function.

### E. Almost Bent Function and Boolean Bent Function

Let \( f(x) \) be a function from \( \mathbb{F}_{2^m} \) to \( \mathbb{F}_{2^r} \). The Walsh transform of \( f(x) \) at \( (a,b) \in \mathbb{F}_{2^r} \times \mathbb{F}_{2^m} \) is defined as
\[
W_f(a,b) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{Tr}_{2^r/2}(af(x)) + \text{Tr}_{2^m/2}(bx)}.
\]

Specially, when \( t = m \), the Walsh transform of \( f \) is then of the form
\[
W_f(a,b) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\text{Tr}_{2^m/2}(af(x) + bx)}.
\]

A function \( f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m} \) is said to be an almost bent function if \( W_f(a,b) = 0 \) or \( \pm 2^{m-1} \) for any pair \( (a,b) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \). Almost bent functions exist only when \( m \) is odd [2].

When \( t = 1 \), the Walsh transform is then of the form
\[
W_f(1,b) = W_f(b) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{f(x) + \text{Tr}_{2m/2}(bx)}.
\]

A function \( f : \mathbb{F}_{2^m} \to \mathbb{F}_2 \) is said to be a Boolean bent function if \( W_f(b) = \pm 2^{\frac{m}{2}} \) for any \( b \in \mathbb{F}_{2^m} \). Boolean bent functions exist only for even \( m \) [43].

Almost bent and Boolean bent functions play important roles in coding theory, cryptography, sequences, and combinatorics. Many good linear codes over finite fields have been constructed with almost bent and Boolean bent functions [7, 12, 15, 34, 40, 42, 45]. In the present paper, them will be used to construct optimal binary codes with respect to the sphere packing bound.
III. The Subfield Codes of \( C_{f,g} \)

Let \( C_{f,g} \) be the linear code over \( \mathbb{F}_{q^m} \) generated by \( \{1\} \), where \( f \) and \( g \) are two different functions from \( \mathbb{F}_{q^m} \) to \( \mathbb{F}_q \). Due to Lemma 11 the trace representation of the subfield code \( C_{f,g}^{(q)} \) is given by

\[
C_{f,g}^{(q)} = \{ c_{a,b,c} : a \in \mathbb{F}_q, b, c \in \mathbb{F}_{q^m} \},
\]

where

\[
c_{a,b,c} = (\text{Tr}_{q^m/q}(b), (a + \text{Tr}_{q^m/q}(bx + cy))_{(x,y) \in \mathcal{D}}), \quad \mathcal{D} = \{(x, y) \in \mathbb{F}_{q}^{2} : f(x) + g(y) = 0\}.
\]

Let \( \chi \) and \( \chi' \) be the canonical additive characters of \( \mathbb{F}_q \) and \( \mathbb{F}_{q^m} \), respectively, for the rest of the paper.

**Lemma 11:** The code length of the code \( C_{f,g}^{(q)} \) is

\[
n = 1 + q^{2m-1} + \frac{1}{q} \sum_{x \in \mathbb{F}_q} \sum_{x \in \mathbb{F}_{q^m}} \chi(zf(x)) \sum_{y \in \mathbb{F}_{q^m}} \chi(zg(x)).
\]

**Proof:** By the orthogonality of group characters, we have

\[
\#\mathcal{D} = \frac{1}{q} \sum_{(x,y) \in \mathbb{F}_{q}^{2}} \sum_{z \in \mathbb{F}_q} \chi(z(f(x) + g(y))) = q^{2m-1} + \frac{1}{q} \sum_{z \in \mathbb{F}_q} \sum_{(x,y) \in \mathbb{F}_{q^m}^{2}} \chi(zf(x) + zg(y)).
\]

Then \( n = 1 + \#\mathcal{D} = 1 + q^{2m-1} + \frac{1}{q} \sum_{z \in \mathbb{F}_q} \sum_{(x,y) \in \mathbb{F}_{q^m}^{2}} \chi(zf(x)) \sum_{y \in \mathbb{F}_{q^m}} \chi(zg(x)). \)

We define a function \( \delta(x) \) from \( \mathbb{F}_{q^m} \) to \( \{0, 1\} \) as

\[
\delta(x) = \begin{cases} 
0 & \text{if } \text{Tr}_{q^m/q}(x) = 0, \\
1 & \text{if } \text{Tr}_{q^m/q}(x) \neq 0.
\end{cases}
\]

**Lemma 12:** For any \( a \in \mathbb{F}_q \), \( b, c \in \mathbb{F}_{q^m} \), the weight of a codeword \( c_{a,b,c} \) in \( C_{f,g}^{(q)} \) is given by

\[
\text{wt}(c_{a,b,c}) = \begin{cases} 
0 & \text{if } a = b = c = 0, \\
\#\mathcal{D} & \text{if } a \neq 0, b = c = 0, \\
\delta(b) + \frac{q - 1}{q} \#\mathcal{D} - \frac{1}{q} \Upsilon_{a,b,c} & \text{if } b \text{ and } c \text{ are not all } 0,
\end{cases}
\]

where \( \Upsilon_{a,b,c} = \sum_{z \in \mathbb{F}_q} \chi(zx) \sum_{w \in \mathbb{F}_q, (x,y) \in \mathbb{F}_{q^m}^2} \chi(wf(x) + wg(y))\chi'(zbx + zcy). \)

**Proof:** Denote

\[
N_{a,b,c} = \# \{(x, y) \in \mathcal{D} : a + \text{Tr}_q^{q^m}(bx + cy) = 0\}.
\]

By the orthogonality relation of additive characters and the transitivity of trace functions, we have

\[
q N_{a,b,c} = \sum_{(x,y) \in \mathcal{D}} \sum_{z \in \mathbb{F}_q} \chi(z(a + \text{Tr}_q^{q^m}(bx + cy)))
\]

\[
= \#\mathcal{D} + \sum_{(x,y) \in \mathcal{D}} \sum_{z \in \mathbb{F}_q} \chi(za + \text{Tr}_q^{q^m}(zbx + zcy))
\]

\[
= \#\mathcal{D} + \sum_{z \in \mathbb{F}_q} \chi(za) \sum_{(x,y) \in \mathcal{D}} \chi'(zbx + zcy)
\]

\[
= \#\mathcal{D} + \sum_{z \in \mathbb{F}_q} \chi(za) \sum_{(x,y) \in \mathbb{F}_{q^m}^2} \left( \frac{1}{q} \sum_{w \in \mathbb{F}_q} \chi(wf(x) + g(y)) \right) \chi'(zbx + zcy)
\]

\[
= \#\mathcal{D} + \frac{1}{q} \sum_{z \in \mathbb{F}_q} \chi(za) \sum_{(x,y) \in \mathbb{F}_{q^m}^2} \chi'(zbx + zcy) + \frac{1}{q} \sum_{z \in \mathbb{F}_q} \chi(za) \sum_{w \in \mathbb{F}_q} \sum_{(x,y) \in \mathbb{F}_{q^m}^2} \chi(wf(x) + wg(y))\chi'(zbx + zcy),
\]
where \( \#D \) is shown in the proof of Lemma [11]. We deduce that

\[
N_{a,b,c} = \begin{cases} 
\#D & \text{if } a = b = c = 0, \\
0 & \text{if } a \neq 0, b = c = 0, \\
\frac{1}{q}(\#D) + \frac{1}{q^2} \sum_{z \in \mathbb{F}_q^*} \sum_{w \in \mathbb{F}_q^*} \sum_{(x,y) \in \mathbb{F}_2^m} \chi(wf(x) + wg(y))\chi'(zbx + zcy) & \text{if } b \text{ and } c \text{ are not all 0,}
\end{cases}
\]

Hence,

\[
wt(c_{a,b,c}) = \delta(b) + \#D - N_{a,b,c}
\]

\[
= \begin{cases} 
0 & \text{if } a = b = c = 0, \\
\#D & \text{if } a \neq 0, b = c = 0, \\
\delta(b) + \frac{2 - \frac{1}{q}}{q} \#D - \frac{1}{q^2} \Upsilon_{a,b,c} & \text{if } b \text{ and } c \text{ are not all 0,}
\end{cases}
\]

where \( \Upsilon_{a,b,c} = \sum_{z \in \mathbb{F}_q^*} \sum_{(x,y) \in \mathbb{F}_2^m} \chi(wf(x) + wg(y))\chi'(zbx + zcy). \)

Let \( \mathcal{C}^{(q)}_{f,g} \) be the code \( \mathcal{C}^{(q)}_{f,g} \) punctured on the first coordinate. That is,

\[
\mathcal{C}^{(q)}_{f,g} = \{ \tilde{c}_{a,b,c} : a \in \mathbb{F}_q, b, c \in \mathbb{F}_q^m \},
\]

where

\[
\tilde{c}_{a,b,c} = (a + \text{Tr}_q^{m}(bx + cy))(x,y) \in D, \quad D = \{(x,y) \in \mathbb{F}_q^2 : f(x) + g(y) = 0\}.
\]

From the above two lemmas, the following conclusions can be easily drawn.

**Lemma 13:** The code length of \( \mathcal{C}^{(q)}_{f,g} \) is

\[
n = \#D = q^{2m-1} + \frac{1}{q} \sum_{z \in \mathbb{F}_q^*} \sum_{x \in \mathbb{F}_q^m} \chi(zf(x)) \sum_{y \in \mathbb{F}_q^m} \chi(zg(x)).
\]

For any \( a \in \mathbb{F}_q, b, c \in \mathbb{F}_q^m \), the weight of a codeword \( \tilde{c}_{a,b,c} \) in \( \mathcal{C}^{(q)}_{f,g} \) is given by

\[
wt(\tilde{c}_{a,b,c}) = \begin{cases} 
0 & \text{if } a = b = c = 0, \\
\#D & \text{if } a \neq 0, b = c = 0, \\
\frac{2 - \frac{1}{q}}{q} \#D - \frac{1}{q^2} \Upsilon_{a,b,c} & \text{if } b \text{ and } c \text{ are not all 0,}
\end{cases}
\]

where \( \Upsilon_{a,b,c} \) is shown in Lemma [12].

Now we consider six different pairs of functions \( f(x) \) and \( g(x) \) from the set \( \{ \text{Tr}_q^{m}/\text{Tr}_q^{2m}/(x^2), \text{Norm}_{q^2}/\text{Norm}_q(x), \text{Tr}_{2m}/\text{A}(x), B(x) \} \), where \( A(x) \) and \( B(x) \) are almost bent and Boolean bent functions, respectively.

**A. \( f_1(x) = \text{Tr}_{q^2}/\text{Tr}_q^{2m}/(x^2) \) and \( g_1(y) = \text{Norm}_{q^2}/\text{Norm}_q(y) \)**

In this subsection, let \( m = 2 \) and \( f_1(x) = \text{Tr}_{q^2}/\text{Tr}_q^{2m}/(x^2), g_1(y) = \text{Norm}_{q^2}/\text{Norm}_q(y) \). For convenience, abbreviate \( \text{Tr}_{q^2}/\text{Tr}_q^{2m}/(x^2) \) and \( \text{Norm}_{q^2}/\text{Norm}_q(y) \) by \( \text{Tr}(x) \) and \( \text{Norm}(y) \), respectively, for the rest of this subsection.

In order to determine the parameters and weight enumerator of \( \mathcal{C}^{(q)}_{f,g} \), we need the following results.

**Lemma 14:** For any \( \alpha, \beta \in \mathbb{F}_q \), let \( N_{\alpha,\beta}^1 = \#\{ x \in \mathbb{F}_q^2 : \text{Tr}(x) = \alpha, \text{Norm}(x) = \beta \} \). Then for odd \( q \),

\[
N_{\alpha,\beta}^1 = 1 - \eta(\alpha^2 - 4\beta),
\]

and for even \( q \),

\[
N_{\alpha,\beta}^1 = \begin{cases} 
1 & \text{if } \alpha = 0, \\
1 - (-1)^{\text{Tr}_q^{m} (\frac{x}{x^q})} & \text{if } \alpha \neq 0,
\end{cases}
\]

**Proof:** By Vieta theorem, the equation set

\[
\begin{cases} 
\text{Tr}(x) = x + x^q = \alpha, \\
\text{Norm}(x) = x \cdot x^q = \beta
\end{cases}
\]
has the same solutions as the equation \( h(x) = x^2 - \alpha x + \beta = 0 \). Meanwhile, obviously \( x \) and \( x^q \) are two roots of \( h(x) \in \mathbb{F}_q[x] \) over \( \mathbb{F}_{q^2} \). If \( q \) is odd.

- When \( \eta(\alpha^2 - 4\beta) = 0 \), from Lemma 5 the root of \( g(x) \) is \( x = x^q = \beta/2 \in \mathbb{F}_q \). Then \( N_{\alpha,\beta}^1 = 1 \).
- When \( \eta(\alpha^2 - 4\beta) = 1 \), the roots of \( g(x) \) are \( x, x^q \in \mathbb{F}_q \) and \( x \neq x^q \), a contradiction. Thus \( N_{\alpha,\beta}^1 = 0 \).
- When \( \eta(\alpha^2 - 4\beta) = -1 \), the roots of \( g(x) \) are \( x, x^q \in \mathbb{F}_{q^2} \). Then \( N_{\alpha,\beta}^1 = 2 \).

Therefore, in this case, \( N_{\alpha,\beta}^1 = 1 - \eta(\alpha^2 - 4\beta) \).

If \( q \) is even, the proof is almost the same by Lemma 5 so the details are omitted.

Lemma 15: For any \( a \in \mathbb{F}_q, b \in \mathbb{F}_q^* \), let \( N_{a,b}^2 = \# \{ x \in \mathbb{F}_{q^2} : a + \text{Tr}(x) + b \text{Norm}(x) = 0 \} \). Then \( N_{a,b}^2 \in \{ 1, q+1 \} \), and \( N_{a,b}^2 = 1 \) if and only if \( ab = 1 \).

Proof: By Lemma 4 and Lemma 14, if \( q \) is odd,

\[
N_{a,b}^2 = \sum_{(\alpha, \beta) \in \mathbb{F}_q^2 \atop \alpha + \alpha + \beta = 0} N_{\alpha,\beta}^1
\]

\[
= \sum_{(\alpha, \beta) \in \mathbb{F}_q^2 \atop \alpha + \alpha + \beta = 0} (1 - \eta(\alpha^2 - 4\beta))
\]

\[
= \sum_{\beta \in \mathbb{F}_q} (1 - \eta((a + b\beta)^2 - 4\beta))
\]

\[
= q - \sum_{\beta \in \mathbb{F}_q} \eta(b^2\beta^2 + (2ab - 4)\beta + a^2)
\]

\[
\begin{cases}
q - (q - 1) & \text{if } (2ab - 4)^2 - 4a^2b^2 = 0, \\
q - (-1) & \text{if } (2ab - 4)^2 - 4a^2b^2 \neq 0,
\end{cases}
\]

\[
= \begin{cases}
1 & \text{if } ab = 1, \\
q + 1 & \text{if } ab \neq 1.
\end{cases}
\]

If \( q \) is even,

\[
N_{a,b}^2 = \sum_{(\alpha, \beta) \in \mathbb{F}_q^2 \atop \alpha + \alpha + \beta = 0} N_{\alpha,\beta}^1
\]

\[
= 1 + \sum_{\alpha \in \mathbb{F}_q^*} (1 - (-1)^{\text{Tr}_{q/2}(\frac{\alpha + a}{\alpha})})
\]

\[
= 1 + \sum_{\alpha \in \mathbb{F}_q^*} (1 - (-1)^{\text{Tr}_{q/2}(\frac{\alpha}{\alpha}) + \text{Tr}_{q/2}(\frac{b}{\alpha})})
\]

\[
= q - \sum_{\alpha \in \mathbb{F}_q^*} (-1)^{\text{Tr}_{q/2}(\frac{\alpha}{\alpha}) + \text{Tr}_{q/2}(\frac{b}{\alpha})}
\]

\[
= q - \sum_{\alpha \in \mathbb{F}_q^*} (-1)^{\text{Tr}_{q/2}(\frac{\alpha + a}{\alpha})}
\]

\[
\begin{cases}
q - (q - 1) = 1 & \text{if } ab = 1, \\
q - (-1) = q + 1 & \text{if } ab \neq 1.
\end{cases}
\]

The proof is now completed.

With the preparations above, we now determine the parameters and weight enumerator of \( C_{f_1,g_1} \).

Theorem 1: Let notations be the same as before. Then \( C_{f_1,g_1} \) is an optimal \([q^3 + 1, 3, q^3 - q]\) code achieving the Griesmer bound over \( \mathbb{F}_{q^2} \). Its weight enumerator is

\[
1 + (q^2 - 1)(q^4 - q^3 + q^2)z^{q^3-q} + (q^2 - 1)(q^3 + 1)z^{q^3}.
\]

Its dual \( C_{f_1,g_1}^\perp \) is a \([q^3 + 1, q^3 - 2, 3]\) almost MDS code.
Proof: For \( m = 2 \), \( f_1(x) = \text{Tr}(x) \), \( g_1(y) = \text{Norm}(y) \), by the transitivity of trace functions, we have

\[
\#D = q^3 + \frac{1}{q} \sum_{z \in \mathbb{F}_q^*} \sum_{x \in \mathbb{F}_q^m} \chi(z\text{Tr}(x)) \sum_{y \in \mathbb{F}_q^m} \chi(z\text{Norm}(y)) = q^3,
\]

Then from Lemma 11, the code length of \( C_{f_1,g_1} \) is \( n = q^3 + 1 \).

Let \( S_1 \) be the set of columns of matrix \( G_{f_1,g_1} \). We discuss the value of \( \#(\mathcal{H}_u \cap S_1) \) for any line \( \mathcal{H}_u \) with nonzero \( u = (u_1, u_2, u_3) \in \mathbb{F}_q^3 \) in the following cases.

1. If \( u = (u_1, 0, 0) \) for \( u_1 \in \mathbb{F}_q^* \). Obviously \( \mathcal{H}_u \cap S_1 = \{(0, 1, 0)^T\} \).
2. If \( u = (0, u_2, 0) \) for \( u_2 \in \mathbb{F}_q^* \). Then \( \mathcal{H}_u \cap S_1 = \{(1, 0, y)^T : y \in \mathbb{F}_q^2, \text{Norm}(y) = 0\} = \{(1, 0, 0)^T\} \).
3. If \( u = (0, u_3) \) for \( u_3 \in \mathbb{F}_q^* \). Then \( \mathcal{H}_u \cap S_1 = \{(0, 1, 0)^T\} \cup \{(1, x, 0)^T : x \in \mathbb{F}_q^2, \text{Tr}(x) = 0\} \). Thus \( \#(\mathcal{H}_u \cap S_1) = q + 1 \).
4. If \( u = (u_1, u_2, 0) \) for \( u_1, u_2 \in \mathbb{F}_q^* \). Then \( \mathcal{H}_u \cap S_1 = \{(1, -\frac{u_1}{u_2}, y)^T : y \in \mathbb{F}_q^2, \text{Norm}(y) = -\text{Tr}(\frac{u_1}{u_2})\} \). Thus \( \#(\mathcal{H}_u \cap S_1) = 1 \) if \( \text{Tr}(\frac{u_1}{u_2}) = 0 \), and there are \( (q^2 - 1)(q - 1) \) choices of such \( (u_1, u_2) \in (\mathbb{F}_q^*)^2 \).
5. If \( u = (0, u_2, 0) \) for \( u_2 \in \mathbb{F}_q^* \). Then \( \mathcal{H}_u \cap S_1 = \{(1, x, -\frac{u_2}{u_3})^T : x \in \mathbb{F}_q^2, \text{Tr}(x) = -\text{Norm}(\frac{u_2}{u_3})\} \). Thus \( \#(\mathcal{H}_u \cap S_1) = q + 1 \).
6. If \( u = (u_1, 0, u_3) \) for \( u_1, u_3 \in \mathbb{F}_q^* \). Then \( \mathcal{H}_u \cap S_1 = \{(0, 1, y)^T \cup \{(1, x, -\frac{u_1}{u_3})^T : x \in \mathbb{F}_q^2, \text{Tr}(x) = -\text{Norm}(\frac{u_1}{u_3})\} \). Thus \( \#(\mathcal{H}_u \cap S_1) = 1 \).
7. If \( u = (u_1, u_2, 0) \) for \( u_1, u_2 \in \mathbb{F}_q^* \). Then \( \mathcal{H}_u \cap S_1 = \{(1, -\frac{u_1}{u_2}, y)^T : y \in \mathbb{F}_q^2, \text{Tr}(x) = 0\} \). By Lemma 15, \( \#(x \in \mathbb{F}_q^2, \text{Tr}(x) + \text{Norm}(\frac{u_1}{u_2}) = 0\} \). By Lemma 15, \( \#(\mathcal{H}_u \cap S_1) = q + 1 \).
8. If \( u = (u_1, u_2, u_3) \) for \( u_1, u_2, u_3 \in \mathbb{F}_q^* \). Then \( \mathcal{H}_u \cap S_1 = \{(1, -\frac{u_1}{u_2}, -\frac{u_2}{u_3})^T : y \in \mathbb{F}_q^2, \text{Tr}(y) + \text{Norm}(\frac{u_1}{u_2}) + \text{Norm}(\frac{u_2}{u_3}) = 0\} \). By Lemma 15, \( \#(\mathcal{H}_u \cap S_1) = q + 1 \).

Thus, in this case, \( \#(\mathcal{H}_u \cap S_1) = \{(1, q + 1) \} \) and \( \#(\mathcal{H}_u \in \mathbb{F}_q^3 : \#(\mathcal{H}_u \cap S_1) = 1) = q(q^2 - 1)^2 \).

For any nonzero \( u \in \mathbb{F}_q^3 \), by the foregoing discussions, we deduce that \( \#(\mathcal{H}_u \cap S_1) \in \{1, q + 1\} \), and the number of \( u \in \mathbb{F}_q^3 \) satisfying \( \#(\mathcal{H}_u \cap S_1) = 1 \) is \( q(q^2 - 1)(1 + 1 + q + 1 + q(q^2 - 1)) = (q^2 - 1)(q^3 + 1) \). The minimum distance and weight distribution of code \( C_{f_1,g_1} \) can be obtained directly from Lemma 6.

Note that \( C_{f_1,g_1} \) is of length \( q^3 + 1 \) and dimension \( q^2 - 2 \). Since any two points of \( S_1 \) generate a line in \( \text{PG}(2, q^2) \) and there exist three collinear points, such as \( \{(0, 1, 0)^T, (1, 0, 0)^T, (1, v, 0)^T\} \) for some \( v \in \mathbb{F}_q^2 \) with \( \text{Tr}(v) = 0 \). Hence, the minimum distance of \( C_{f_1,g_1} \) is 3.

Remark 2: When \( q = 2 \), \( C_{f_1,g_1} \) is a quaternary Hermitian self-orthogonal code as every codeword of \( C_{f_1,g_1} \) has weight divisible by two [20].

We give an example to illustrate Theorem 1.

Example 1: Let \( q = 2 \). By [39], \( C_{f_1,g_1} \) is an optimal [9, 3, 6] code over \( \mathbb{F}_4 \) achieving the Griesmer bound with weight enumerator

\[
1 + 36z^6 + 27z^8.
\]

Its dual is a [9, 6, 3] almost MDS code. These coincide with the conclusions of Theorem 1.

Let \( q = 3 \). By [39], \( C_{f_1,g_1} \) is an optimal [28, 3, 24] code over \( \mathbb{F}_9 \) achieving the Griesmer bound with weight enumerator

\[
1 + 504z^2 + 224z^7.
\]

Its dual is a [28, 25, 3] almost MDS code. These also coincide with the conclusions of Theorem 1.

The following theorem documents the \( q \)-ary subfield code of \( C_{f_1,g_1} \), which is denoted by \( C_{f_1,g_1}^{(q)} \).
Theorem 2: Let notations be the same as before. Then the following statements hold.

- If \( q \) is even, \( C_{f_1,g_1}^{(q)} \) is a five-weight \( q \)-ary linear code with parameters \([q^3 + 1, 5, q^3 - q^2 - q]\) and the weight distribution is given in Table II.
- If \( q \) is odd, \( C_{f_1,g_1}^{(q)} \) is a five-weight \( q \)-ary linear code with parameters \([q^3 + 1, 5, q^3 - q^2 - q + 1]\) and the weight distribution is given in Table II.
- The dual \( C_{f_1,g_1}^{(q)\perp} \) is always a \([q^3 + 1, 5, q^3 - 4, 3]\) linear code.

Proof: The code length of \( C_{f_1,g_1}^{(q)} \) is \( q^3 + 1 \) as shown in Theorem I. For any \( a \in \mathbb{F}_q \), \((b, c) \in \mathbb{F}_q^2 \setminus (0, 0)\), by \( f_1(x) = \text{Tr}(x) \), \( g_1(y) = \text{Norm}(y) \), we have

\[
Y_{a,b,c} = \sum_{z \in \mathbb{F}_q^*} \sum_{w \in \mathbb{F}_q^* \setminus \{y \}} \sum_{z \in \mathbb{F}_q^* \setminus \{y \}} \chi(w \text{Tr}(x) + w \text{Norm}(y)) \chi'(zbx + zcy)
\]

\[
= \sum_{z \in \mathbb{F}_q^*} \sum_{w \in \mathbb{F}_q^* \setminus \{y \}} \sum_{z \in \mathbb{F}_q^* \setminus \{y \}} \chi'((w + zb)x) \sum_{y \in \mathbb{F}_q^2} \chi(w \text{Norm}(y) + \text{Tr}(zcy))
\]

\[
= \begin{cases} 
0 & \text{if } w \neq -zb, \\
q^2 \sum_{y \in \mathbb{F}_q^2} \sum_{z \in \mathbb{F}_q^* \setminus \{y \}} \chi(z(a + \text{Tr}(cy) - b \text{Norm}(y))) & \text{if } w = -zb.
\end{cases}
\]

\[
= \begin{cases} 
0 & \text{if } b \in \mathbb{F}_q^2 \setminus \mathbb{F}_q^*, \\
q^3 N_y - q^4 & \text{if } b \in \mathbb{F}_q^2.
\end{cases}
\]

where \( N_y = \#\{y \in \mathbb{F}_q^2 : a + \text{Tr}(cy) - b \text{Norm}(y) = 0\} \) and the last equality holds because for any \( z \in \mathbb{F}_q^* \), there exists some \( w \in \mathbb{F}_q^* \) such that \( w = -zb \) if and only if \( b \in \mathbb{F}_q^* \). From the properties of trace and norm functions,

- when \( c = 0 \), \( a = 0 \), \( N_y = 1 \);
- when \( c = 0 \), \( a \neq 0 \), \( N_y = q + 1 \);
- when \( c \neq 0 \), by Lemma 15,

\[
N_y = \#\{y \in \mathbb{F}_q^2 : a + \text{Tr}(y) - b \text{Norm}(\frac{1}{c}) \text{Norm}(y)\}
\]

\[
= \begin{cases} 
1 & \text{if } ab \text{Norm}(\frac{1}{c}) = -1, \\
q + 1 & \text{if } ab \text{Norm}(\frac{1}{c}) \neq -1,
\end{cases}
\]

\[
= \begin{cases} 
1 & \text{if } \text{Norm}(c) = -ab, \\
q + 1 & \text{if } \text{Norm}(c) \neq -ab.
\end{cases}
\]

Thus,

\[
Y_{a,b,c} = \begin{cases} 
0 & \text{if } b \in \mathbb{F}_q^2 \setminus \mathbb{F}_q^*, \\
q^3 N_y - q^4 & \text{if } b \in \mathbb{F}_q^2, \text{Norm}(c) = -ab, \\
q^3 & \text{if } b \in \mathbb{F}_q^2, \text{Norm}(c) \neq -ab,
\end{cases}
\]

where \( a \in \mathbb{F}_q \), \((b, c) \in \mathbb{F}_q^2 \setminus (0, 0)\).

Since \( \#D = q^3 \), by Lemma 12 for any codeword \( c_{a,b,c} \) in \( C_{f_1,g_1}^{(q)} \), we deduce that

\[
\text{wt}(c_{a,b,c}) = \begin{cases} 
0 & \text{if } a = b = c = 0, \\
q^3 & \text{if } a \neq 0, b = c = 0, \\
q^3 - q^2 & \text{if } b = 0, c \neq 0 \text{ or } b \in \mathbb{F}_q \setminus \mathbb{F}_q, \delta(b) = 0, \\
q^3 - q^2 + 1 & \text{if } b \in \mathbb{F}_q \setminus \mathbb{F}_q, \delta(b) = 1 \\
q^3 - q & \text{if } b \in \mathbb{F}_q^*, \text{Norm}(c) = -ab, \delta(b) = 0, \\
q^3 - q + 1 & \text{if } b \in \mathbb{F}_q^*, \text{Norm}(c) = -ab, \delta(b) = 1, \\
q^3 - q^2 - q & \text{if } b \in \mathbb{F}_q^*, \text{Norm}(c) \neq -ab, \delta(b) = 0, \\
q^3 - q^2 - q + 1 & \text{if } b \in \mathbb{F}_q^*, \text{Norm}(c) \neq -ab, \delta(b) = 1,
\end{cases}
\]

where \( a \in \mathbb{F}_q \), \( b, c \in \mathbb{F}_q^2 \).
When \( q \) is even, for any \( b \in \mathbb{F}_q^2 \), \( \text{Tr}(b) = 0 \) if and only if \( b \in \mathbb{F}_q \). Then we further have

\[
\text{wt}(c_{a,b,c}) = \begin{cases} 
0, & \text{with 1 time,} \\
q^3 - q^2 - q & \text{with } q^4 - 2q^3 + q^2 \text{ time,} \\
q^3 - q^2 & \text{with } q^3 - q \text{ time,} \\
q^3 - q^2 + 1 & \text{with } q^5 - q^4 \text{ time,} \\
q^3 - q & \text{with } q^3 - q^2 \text{ time,} \\
q^3 & \text{with } q - 1 \text{ time.}
\end{cases}
\]

When \( q \) is odd, for any \( b \in \mathbb{F}_q \), \( \text{Tr}(b) = 0 \) if and only if \( b = 0 \), meanwhile, there are \( q - 1 \) different \( b \)'s in \( \mathbb{F}_q^2 \setminus \mathbb{F}_q \) such that \( \text{Tr}(b) = 0 \). Then

\[
\text{wt}(c_{a,b,c}) = \begin{cases} 
0, & \text{with 1 time,} \\
q^3 - q^2 - q + 1 & \text{with } q^4 - 2q^3 + q^2 \text{ time,} \\
q^3 - q^2 & \text{with } q^3 - q \text{ time,} \\
q^3 - q^2 + 1 & \text{with } q^5 - 2q^4 + q^3 \text{ time,} \\
q^3 - q + 1 & \text{with } q^3 - q^2 \text{ time,} \\
q^3 & \text{with } q - 1 \text{ time.}
\end{cases}
\]

The dimension of \( C_{f_1,g_1}^{(q)} \) is 5 as \( A_0 = 1 \).

Note that \( C_{f_1,g_1}^{(q)} \) is of length \( q^3 + 1 \) and dimension \( q^3 - 4 \). It follows from Theorem 1 and Lemma 7 that the minimal distance of \( C_{f_1,g_1}^{(q)} \) satisfies \( d_1^{(q)} \geq 3 \). By the first four Pless power moments, one can derive that \( d_1^{(q)} = 3 \), whether \( q \) is even or odd. Then the proof is completed. ■

**TABLE I:** The weight distribution of \( C_{f_1,g_1}^{(q)} \) with \( q \) even.

| Weight          | Multiplicity |
|-----------------|--------------|
| \( 0 \)         | 1            |
| \( q^3 - q^2 - q \) |              |
| \( q^3 - q^2 \)  |              |
| \( q^3 - q^2 + 1 \) |              |
| \( q^3 - q \)   |              |
| \( q^3 \)       |              |

**TABLE II:** The weight distribution of \( C_{f_1,g_1}^{(q)} \) with \( q \) odd.

| Weight          | Multiplicity |
|-----------------|--------------|
| \( 0 \)         | 1            |
| \( q^3 - q^2 - q + 1 \) |              |
| \( q^3 - q^2 \)  |              |
| \( q^3 - q^2 + 1 \) |              |
| \( q^3 - q + 1 \) |              |
| \( q^3 \)       |              |

**Example 2:** The following examples show that the subfield code \( C_{f_1,g_1}^{(q)} \) is attractive. The optimality are obtained from the code tables at [http://www.coderates.de/](http://www.coderates.de/)

- Let \( q = 2 \). Then \( C_{f_1,g_1}^{(q)} \) has parameters \([9, 5, 2]\), which is almost optimal. Its dual code \( C_{f_1,g_1}^{(q)\perp} \) has parameters \([9, 4, 3]\), which is almost optimal.
- Let \( q = 3 \). Then \( C_{f_1,g_1}^{(q)} \) has parameters \([28, 5, 16]\), which is almost optimal. Its dual code \( C_{f_1,g_1}^{(q)\perp} \) has parameters \([28, 23, 3]\), which is optimal.
- Let \( q = 4 \). Then the dual code \( C_{f_1,g_1}^{(q)\perp} \) has parameters \([65, 60, 3]\), which is optional.
- Let \( q = 5 \). Then the dual code \( C_{f_1,g_1}^{(q)\perp} \) has parameters \([126, 121, 3]\), which is optional.
From Lemma 13 and Theorem 2, we can directly get the following conclusions about the punctured code of the $q$-ary linear code $C_{f_1,g_1}^{(q)}$, which is denoted by $\overline{C}_{f_1,g_1}^{(q)}$.

**Theorem 3:** The punctured code $\overline{C}_{f_1,g_1}^{(q)}$ is a four-weight $q$-ary linear code with parameters $[q^3, 5, q^3 - q^2 - q]$ and the weight enumerator is

$$1 + (q^4 - 2q^3 + q^2)z^{q^3 - q^2 - q} + (q^5 - q^4 + q^3 - q)z^{q^3 - q^2} + (q^3 - q^2)z^{q^3 - q} + (q - 1)z^q.$$

The dual $\overline{C}_{f_1,g_1}^{(q)}$ is a $[q^3, q^3 - 5, 3]$ linear code for $q \geq 3$ and a $[8, 3, 4]$ binary code for $q = 2$.

**Example 3:** The following examples show that the punctured code $C_{f_1,g_1}^{(q)}$ is also attractive. The optimality are obtained from the code tables at [http://www.codetables.de/](http://www.codetables.de/)

- Let $q = 2$. Then $C_{f_1,g_1}^{(q)}$ has parameters $[8, 5, 2]$, which is optimal. Its dual code $\overline{C}_{f_1,g_1}^{(q)}$ has parameters $[8, 3, 4]$, which is optimal.
- Let $q = 3$. Then $C_{f_1,g_1}^{(q)}$ has parameters $[27, 5, 15]$, which is almost optimal. Its dual code $\overline{C}_{f_1,g_1}^{(q)}$ has parameters $[27, 22, 3]$, which is optimal.
- Let $q = 4$. Then the dual code $\overline{C}_{f_1,g_1}^{(q)}$ has parameters $[64, 59, 3]$, which is optimal.
- Let $q = 5$. Then the dual code $\overline{C}_{f_1,g_1}^{(q)}$ has parameters $[125, 120, 3]$, which is optimal.

**Remark 3:** When $q = 4$, $C_{f_1,g_1}^{(q)}$ is a quaternary Hermitian self-orthogonal code as every codeword of $C_{f_1,g_1}$ has weight divisible by two $[20]$.

**B. $f_2(x) = \text{Tr}_{q_1}^{q_2}(x)$ and $g_2(y) = \text{Tr}_{q_1}^{q_2}(y^2)$**

In this subsection, let $m$ be a positive integer and $f_2(x) = \text{Tr}_{q_1/q_2}(x)$, $g_2(y) = \text{Tr}_{q_1/q_2}(y^2)$. Abbreviate $\text{Tr}_{q_1/q_2}(x)$ by $\text{Tr}(x)$ for the rest of this subsection.

In particular, when $m = 1$, $f_2(x) = x$, $g_2(y) = y^2$. Then $C_{f_2,g_2}$ is a $[q + 1, 3, q - 1]$ MDS code which has been studied in [23]. So we focus on the case of $m \geq 2$ in this section.

In order to obtain the parameters and weight enumerator of $C_{f_2,g_2}$, we will make use of the following lemma.

**Lemma 16:** For any $u, v \in \mathbb{F}_{q^m}$, let $N_{u,v}^3 = \#\{y \in \mathbb{F}_{q^m} : \text{Tr}(y^2 + uy + v) = 0\}$. Then for $q = 2^l$,

$$N_{u,v}^3 = \begin{cases} 2q^{m-1} & \text{if } u \in \mathbb{F}_q^*, \text{Tr}_{q_1/q_2}(u) = 0, \\ 0 & \text{if } u \in \mathbb{F}_q, \text{Tr}_{q_1/q_2}(u) = 1, \\ q^{m-1} & \text{if } u \in \mathbb{F}_{q^m}\setminus\mathbb{F}_q^*. \end{cases}$$

and for $q = p^l$ with odd $p$, when $m$ is odd,

$$N_{u,v}^3 = \begin{cases} q^{m-1} & \text{if } \text{Tr}(v - \frac{u^2}{4}) = 0, \\ q^{m-1} + q^{m-2}(-1)^{\frac{(p-1)(m+1)}{4}} & \text{if } \text{Tr}(v - \frac{u^2}{4}) \neq 0, \eta \left(\text{Tr}(v - \frac{u^2}{4})\right) = 1, \\ q^{m} + q^{m-1}(-1)^{\frac{(p-1)(m+1)+4}{4}} & \text{if } \text{Tr}(v - \frac{u^2}{4}) \neq 0, \eta \left(\text{Tr}(v - \frac{u^2}{4})\right) = -1, \end{cases}$$

when $m$ is even,

$$N_{u,v}^3 = \begin{cases} q^{m-1} + (q - 1)q^{m-2}(-1)^{\frac{(m(p-1)+4)}{4}} & \text{if } \text{Tr}(v - \frac{u^2}{4}) = 0, \\ q^{m-1} + q^{m-2}(-1)^{\frac{(m(p-1)+4)}{4}} & \text{if } \text{Tr}(v - \frac{u^2}{4}) \neq 0. \end{cases}$$

**Proof:** By the orthogonality relation of additive characters and the transitivity of trace functions, we have

$$qN_{u,v} = \sum_{y \in \mathbb{F}_{q^m}} \sum_{z \in \mathbb{F}_q} \chi(z(\text{Tr}(y^2 + uy + v)))$$

$$= q^m + \sum_{z \in \mathbb{F}_q^*} \sum_{y \in \mathbb{F}_{q^m}} \chi(zy^2 + zuy + zv).$$
When $q$ is even, by Lemma 3

$$qN_{u,v} = \begin{cases} 
q^m + \chi'(\frac{u}{q^m})q^m & \text{if } u \in \mathbb{F}_q^*, \\
q^m & \text{if } u \in \mathbb{F}_{q^m}\setminus\mathbb{F}_q^*, \\
2q^m & \text{if } u \in \mathbb{F}_q^*, \text{Tr}_{q^m/2}(\frac{u}{q^m}) = 0, \\
0 & \text{if } u \in \mathbb{F}_q^*, \text{Tr}_{q^m/2}(\frac{u}{q^m}) = 1, \\
q^m & \text{if } u \in \mathbb{F}_{q^m}\setminus\mathbb{F}_q^*.
\end{cases}$$

When $q$ is odd, by Lemma 2

$$qN_{u,v} = q^m + \sum_{z \in \mathbb{F}_q^*} \chi'(zv - z^2u^2(4z)^{-1})\eta'(z)G(\eta', \chi')$$

$$= q^m + G(\eta', \chi') \sum_{z \in \mathbb{F}_q^*} \chi' \left( z(v - \frac{u^2}{4}) \right) \eta'(z).$$

If $m$ is odd, we have $\eta'(z) = \eta(z)$ for $z \in \mathbb{F}_q^*$. Then by Lemma 1 we deduce that

$$qN_{u,v} = q^m + G(\eta', \chi') \sum_{z \in \mathbb{F}_q^*} \chi \left( z\text{Tr}(v - \frac{u^2}{4}) \right) \eta(z)$$

$$= \begin{cases} 
q^m + G(\eta', \chi') \sum_{z \in \mathbb{F}_q^*} \eta(z) & \text{if } \text{Tr}(v - \frac{u^2}{4}) = 0, \\
q^m + G(\eta', \chi')G(\eta, \chi)\eta \left( \text{Tr}(v - \frac{u^2}{4}) \right) & \text{if } \text{Tr}(v - \frac{u^2}{4}) \neq 0,
\end{cases}$$

$$= \begin{cases} 
q^m & \text{if } \text{Tr}(v - \frac{u^2}{4}) = 0, \\
q^m + q^\frac{m+1}{2}(-1)^{\frac{1}{4}(p-1)(m+1)} & \text{if } \text{Tr}(v - \frac{u^2}{4}) \neq 0, \eta \left( \text{Tr}(v - \frac{u^2}{4}) \right) = 1, \\
q^m + q^\frac{m+1}{2}(-1)^{\frac{1}{4}(p-1)(m+1)+4} & \text{if } \text{Tr}(v - \frac{u^2}{4}) \neq 0, \eta \left( \text{Tr}(v - \frac{u^2}{4}) \right) = -1.
\end{cases}$$

If $m$ is even, $\eta'(z) = 1$ for any $z \in \mathbb{F}_q^*$. Then by Lemma 1 we deduce that

$$qN_{u,v} = q^m + G(\eta', \chi') \sum_{z \in \mathbb{F}_q^*} \chi' \left( z\text{Tr}(v - \frac{u^2}{4}) \right)$$

$$= q^m + G(\eta', \chi') \sum_{z \in \mathbb{F}_q^*} \chi \left( z\text{Tr}(v - \frac{u^2}{4}) \right)$$

$$= \begin{cases} 
q^m + (q - 1)q^\frac{m+1}{2}(-1)^{\frac{1}{4}(p-1)+4} & \text{if } \text{Tr}(v - \frac{u^2}{4}) = 0, \\
q^m + q^\frac{m+1}{2}(-1)^{\frac{1}{4}(p-1)+4} & \text{if } \text{Tr}(v - \frac{u^2}{4}) \neq 0.
\end{cases}$$

The proof is now completed.

We now settle the parameters and weight enumerator of the linear code $C_{f_2,g_2}$ over $\mathbb{F}_{q^m}$.

**Theorem 4:** Let $q = p^l$. If $m \geq 2$, the following statements hold.

- When $q$ is even, $C_{f_2,g_2}$ is a five-weight linear code over $\mathbb{F}_{q^m}$ with parameters $[q^{2m-1} + 1, 3, q^{2m-1} - 2q^{m-1} + 1]$ and the weight distribution is given in Table [III].
- When both $q$ and $m$ are odd, $C_{f_2,g_2}$ is a five-weight linear code over $\mathbb{F}_{q^m}$ with parameters $[q^{2m-1} + 1, 3, q^{2m-1} - q^{m-1} - q^{\frac{m-1}{2}} + 1]$ and the weight distribution is given in Table [IV].
- When $q$ is odd and $m$ is even, $C_{f_2,g_2}$ is a four-weight linear code over $\mathbb{F}_{q^m}$ with parameters $[q^{2m-1} + 1, 3]$ and weight distribution is given in Table [V].
- The dual $C_{f_2,g_2}^\perp$ is always a $[q^{2m-1} + 1, q^{2m-1} - 2, 3]$ almost MDS code.

**Proof:** From $f_2(x) = \text{Tr}(x)$, $g_2(y) = \text{Tr}(y^2)$, $#D = q^{2m-1} + \frac{1}{q} \sum_{z \in \mathbb{F}_q^*} \sum_{x \in \mathbb{F}_{q^m}} \chi(z\text{Tr}(x)) \sum_{y \in \mathbb{F}_{q^m}} \chi(z\text{Tr}(y^2)) = q^{2m-1}$. 


Then by Lemma \[11\] the code length of $C_{f_2,g_2}$ is $n = q^{2m-1} + 1$.

Similar to the proof of Theorem \[1\] let $S_2$ be the set of columns of matrix $G_{f_2,g_2}$. We discuss the value of $\#(\mathcal{H}_u \cap S_2)$ for any line $\mathcal{H}_u$ with nonzero $u \in \mathbb{F}_q^3$. Let $u_1, u_2, u_3 \in \mathbb{F}_q^m$, combined with Lemma \[16\] we derive the following results.

- When $q$ is even,

$$\#(\mathcal{H}_u \cap S_2) = \begin{cases} 0 & \text{if } u = (u_1, u_2, u_3), \frac{u_3}{u_2} \in \mathbb{F}_q^*, \text{Tr}_2^{q^m} \left( \frac{u_1 u_2}{u_3} \right) = 1, \\
1 & \text{if } u = (u_1, 0, 0), \\
q^{m-1} & \text{if } u = (0, u_2, 0), \\
q^{m-1} & \text{or } u = (u_1, u_2, 0), \\
or u = (0, u_2, 3), \frac{u_3}{u_2} \in \mathbb{F}_q^* \setminus \mathbb{F}_q^2, \\
or u = (u_1, u_2, 3), \frac{u_3}{u_2} \in \mathbb{F}_q^* \setminus \mathbb{F}_q^2, \\
q^{m-1} + 1 & \text{if } u = (0, 0, u_3), \\
or u = (u_1, 0, u_3), \\
2q^{m-1} & \text{if } u = (0, u_2, 3), \frac{u_3}{u_2} \in \mathbb{F}_q^*, \\
or u = (u_1, u_2, 3), \frac{u_3}{u_2} \in \mathbb{F}_q^*, \text{Tr}_2^{q^m} \left( \frac{u_1 u_2}{u_3} \right) = 0. \\
\end{cases}$$

Since

$$\# \left\{ (u_1, u_2, u_3) \in (\mathbb{F}_q^*)^3 : \frac{u_3}{u_2} \in \mathbb{F}_q^*, \text{Tr}_2^{q^m} \left( \frac{u_1 u_2}{u_3} \right) = 0 \right\} = (q^m - 1)(q - 1)(\frac{q^m}{2} - 1).$$

We deduce that

$$\#(\mathcal{H}_u \cap S_2) = \begin{cases} 0 & \text{with } (q^m - 1)(q - 1)\frac{q^m}{2} \text{ times,} \\
1 & \text{with } q^m - 1 \text{ times,} \\
q^{m-1} & \text{with } q^m(q^m - 1)(q^m - q + 1) \text{ times,} \\
q^{m-1} + 1 & \text{with } q^m(q^m - 1) \text{ times,} \\
2q^{m-1} & \text{with } (q^m - 1)(q - 1)\frac{q^m}{2} \text{ times.} \\
\end{cases}$$

- When both $q$ and $m$ are odd,

$$\#(\mathcal{H}_u \cap S_2) = \begin{cases} 1 & \text{if } u = (u_1, 0, 0), \\
q^{m-1} & \text{if } u = (0, u_2, 0), \\
q^{m-1} & \text{or } u = (u_1, u_2, 0), \text{Tr}(\frac{u_1}{u_3}) = 0, \\
or u = (0, u_2, 3), \text{Tr}(\frac{u_3}{4u_2}) = 0, \\
or u = (u_1, u_2, 3), \text{Tr}(\frac{u_1}{u_2} - \frac{u_3}{u_2}) = 0, \\
q^{m-1} + q^{m-1} (-1)^{\frac{(p-1)(m+1)}{4}} & \text{if } u = (0, 0, u_3), \\
or u = (u_1, 0, u_3), \\
q^{m-1} + q^{m-1} (-1)^{\frac{(p-1)(m+1)+4}{4}} & \text{if } u = (u_1, u_2, 0), \text{Tr}(\frac{u_3}{u_2}) \neq 0, \text{Tr}(\frac{u_1}{u_2}) = 1, \\
or u = (0, u_2, 3), \text{Tr}(\frac{u_3}{4u_2}) \neq 0, \text{Tr}(\frac{u_1}{u_2} - \frac{u_3}{4u_2}) = 0, \\
or u = (u_1, u_2, 3), \text{Tr}(\frac{u_1}{u_2} - \frac{u_3}{4u_2}) = 0, \text{Tr}(\frac{u_1}{u_2} - \frac{u_3}{4u_2}) = 0, \\
or u = (0, 0, u_3), \text{Tr}(\frac{u_3}{u_2}) \neq 0, \text{Tr}(\frac{u_1}{u_2}) = 1, \\
or u = (0, u_2, 3), \text{Tr}(\frac{u_3}{4u_2}) = 0, \text{Tr}(\frac{u_1}{u_2} - \frac{u_3}{4u_2}) = 0, \\
or u = (u_1, u_2, 3), \text{Tr}(\frac{u_1}{u_2} - \frac{u_3}{4u_2}) = 0, \text{Tr}(\frac{u_1}{u_2} - \frac{u_3}{4u_2}) = 0, \\
or u = (0, 0, u_3), \text{Tr}(\frac{u_1}{u_2} - \frac{u_3}{4u_2}) = 0, \text{Tr}(\frac{u_1}{u_2} - \frac{u_3}{4u_2}) = 0. \\
\end{cases}$$
The minimum distance and weight distribution of code $C$ now we give an example to illustrate Theorem 4.

Example 4: Let $q = 2, m = 3$. By $[39]$, $C_{f_2,g_2}$ is a $[33,3,25]$ linear code over $F_2^*$ with weight enumerator $1 + 28z^{25} + 56z^{28} + 392z^{29} + 7z^{32} + 28z^{33}$.

Table III: The weight distribution of $C_{f_2,g_2}$ with $q$ even.

| Weight | Multiplicity |
|--------|--------------|
| $q^{2m-1} - 2q^{m-1} + 1$ | $q^m(q^m - 1)(q - 1)$ |
| $q^{2m-1} - q^{m-1}$ | $q^m(q^m - 1)$ |
| $q^{2m-1} - q^{m-1} + 1$ | $q^m(q^m - q + 1)$ |
| $q^{2m-1}$ | $q^m - 1$ |
| $q^{2m-1} - 2q^{m-1} + 1$ | $q^m(q^m - 1)(q - 1)$ |
TABLE IV: The weight distribution of $C_{f_2,g_2}$ with $q$ odd and $m$ odd.

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

TABLE V: The weight distribution of $C_{f_2,g_2}$ with $q$ odd and $m$ even.

| Weight                  | Multiplicity          |
|-------------------------|-----------------------|
| $q^{2m-1} - q^{m-1} + (q-1)q^{\frac{m-2}{2}}(1) - \frac{m-2}{4} + 4$ | $q^{2m-1}(q^{m-1})(q-1)$ |
| $q^{2m-1} - q^{m-1} + q^{\frac{m-2}{2}}(1) - \frac{m-2}{4} + 4$ | $q^m(q^{m-1})$        |
| $q^{2m-1} - q^{m-1}$     | $q^m(q^{m-1})$        |
| $q^{2m-1}$              | $q^m - 1$             |

Its dual is a [33, 30, 3] almost MDS code. These coincide with the conclusions of Theorem 4.

Let $q = 3$, $m = 3$. By [39], $C_{f_2,g_2}$ is a [244, 3, 232] code over $\mathbb{F}_3^q$ with weight enumerator

$$1 + 6318z^{232} + 702z^{234} + 6318z^{235} + 6318z^{238} + 26z^{243}.$$ 

Its dual is a [244, 241, 3] almost MDS code. These also coincide with the conclusions of Theorem 4.

Define a class of exponential sums as

$$\Omega(a, b, c) = \sum_{z \in \mathbb{F}_q^*} \sum_{y \in \mathbb{F}_q^{m^2}} \chi'(-zyb^2 + zcy), \; a \in \mathbb{F}_q, \; b, c \in \mathbb{F}_q^m.$$ 

**Lemma 17:** For any $a \in \mathbb{F}_q, b \in \mathbb{F}_q^m$ and $c \in \mathbb{F}_q^m$. If $q$ is even, we have

$$\Omega(a, b, c) = \begin{cases} 
q^m & \text{if } c \in \mathbb{F}_q^*, \; \text{Tr}_{q/2}(ab/c) = 0, \\
-q^m & \text{if } c \in \mathbb{F}_q^\times, \; \text{Tr}_{q/2}(ab/c) = 1, \\
0 & \text{if } c \in \mathbb{F}_q^m \setminus \mathbb{F}_q^*.
\end{cases}$$

If both $q$ and $m$ are odd,

$$\Omega(a, b, c) = \begin{cases} 
q^{\frac{m+1}{2}}(-1)^{\frac{[(m-1)(m+1)]}{4}} & \text{if } a + \text{Tr}(c^2_{q^m}) = 0, \\
0 & \text{if } a + \text{Tr}(c^2_{q^m}) \neq 0, \; c'(-b)\eta(a + \text{Tr}(c^2_{q^m})) = 1, \\
q^{\frac{m+1}{2}}(-1)^{\frac{[(m-2)(m+1)]}{4}} & \text{if } a + \text{Tr}(c^2_{q^m}) \neq 0, \; c'(-b)\eta(a + \text{Tr}(c^2_{q^m})) = -1.
\end{cases}$$

If $q$ is odd and $m$ is even,

$$\Omega(a, b, c) = \begin{cases} 
(q-1)q^{\frac{m}{2}}(-1)^{\frac{[(m-1)+4]}{4}} & \text{if } a + \text{Tr}(c^2_{q^m}) = 0, \\
0 & \text{if } a + \text{Tr}(c^2_{q^m}) \neq 0.
\end{cases}$$

**Proof:** When $q$ is even, by Lemma 3 for any $z \in \mathbb{F}_q^*$

$$\sum_{y \in \mathbb{F}_q^{m^2}} \chi'(-zyb^2 + zcy) = \begin{cases} 
q^m & \text{if } b = zc^2, \\
0 & \text{otherwise}.
\end{cases}$$
Then
\[\Omega(a, b, c) = \sum_{z \in \mathbb{F}_q^*} \chi(za) \sum_{y \in \mathbb{F}_q^m} \chi'(zby^2 + zcy)\]
\[= \begin{cases} \chi(\frac{ab}{c^2})q^m & \text{if } c \in \mathbb{F}_q^* \\ 0 & \text{if } c \in \mathbb{F}_q = \mathbb{F}_q^* \end{cases},\]
\[= \begin{cases} q^m & \text{if } c \in \mathbb{F}_q^*, \text{Tr}_{q/2}(\frac{ab}{c^2}) = 0, \\ -q^m & \text{if } c \in \mathbb{F}_q^*, \text{Tr}_{q/2}(\frac{ab}{c^2}) = 1, \\ 0 & \text{if } c \in \mathbb{F}_q = \mathbb{F}_q^*, \end{cases}\]

where the second equality holds because there exists some \( z \in \mathbb{F}_q^* \) such that \( b = zc^2 \) if and only if \( c \in \mathbb{F}_q^* \).

When \( q \) is odd, by Lemma [2]
\[\Omega(a, b, c) = \sum_{z \in \mathbb{F}_q^*} \chi(za) \sum_{y \in \mathbb{F}_q^m} \chi'(-zby^2 + zcy)\]
\[= \sum_{z \in \mathbb{F}_q^*} \chi(za)\chi'(-z^2c^2(-4zb)^{-1})\eta'(-zb)G(\eta', \chi')\]
\[= G(\eta', \chi')\eta'(-b) \sum_{z \in \mathbb{F}_q^*} \chi(za)\chi'(z\frac{c^2}{4b})\eta'(z)\]
\[= G(\eta', \chi')\eta'(-b) \sum_{z \in \mathbb{F}_q^*} \chi \left( za + z\text{Tr}(\frac{c^2}{4b}) \right) \eta'(z).\]

If \( m \) is odd,
\[\Omega(a, b, c) = \begin{cases} G(\eta', \chi')\eta'(-b) \sum_{z \in \mathbb{F}_q^*} \eta(z) & \text{if } a + \text{Tr}(\frac{c^2}{16}) = 0, \\ G(\eta, \chi)G(\eta', \chi')\eta'(-b)\eta \left( a + \text{Tr}(\frac{c^2}{16}) \right) & \text{if } a + \text{Tr}(\frac{c^2}{16}) \neq 0, \\ 0 & \text{if } a + \text{Tr}(\frac{c^2}{16}) = 0, \end{cases}\]
\[= \begin{cases} q^{\frac{m+1}{2}}(-1)^{\frac{(n-1)(m+1)}{4}} & \text{if } a + \text{Tr}(\frac{c^2}{16}) \neq 0, \eta'(-b)\eta \left( a + \text{Tr}(\frac{c^2}{16}) \right) = 1, \\ -1 \end{cases}\]

If \( m \) is even, \( \eta'(-b) = 1 \) for any \( b \in \mathbb{F}_q^* \), then
\[\Omega(a, b, c) = G(\eta', \chi') \sum_{z \in \mathbb{F}_q^*} \chi \left( za + \text{Tr}(\frac{c^2}{4b}) \right)\]
\[= \begin{cases} (q - 1)q^{\frac{m}{2}}(-1)^{\frac{(n-1)(m+1)}{4}} & \text{if } a + \text{Tr}(\frac{c^2}{16}) = 0, \\ q^{\frac{m}{2}}(-1)^{\frac{(n-1)(m+1)}{4}} & \text{if } a + \text{Tr}(\frac{c^2}{16}) \neq 0. \end{cases}\]

The proof is now completed.

We now determine the parameters of the \( q \)-ary subfield code of \( C_{f_2,g_2} \).

**Theorem 5:** Let \( q = p^l \). If \( m \geq 2 \), the following statements hold.

- When \( q \) and \( m \) are even.
  - If \( q = 2^l \), \( C_{f_2,g_2}(\bar{q}) \) is a binary three-weight linear code with parameters \([2^{2m-1} + 1, 2m, 2^{2m-2}]\) and weight distribution in Table [VII]. The dual \( C_{f_2,g_2}^\perp \) is a \([2^{2m-1} + 1, 2^{2m-1} - 2m + 1, 3]\) binary code.
  - If \( q = 2^l, l \geq 2 \), \( C_{f_2,g_2}(\bar{q}) \) is a four-weight \( q \)-ary linear code with parameters \([q^{2m-1} + 1, 2m + 1, (q - 2)q^{2m-2}]\) and the weight distribution in Table [VII]. The dual \( C_{f_2,g_2}^\perp \) is a \([q^{2m-1} + 1, q^{2m-1} - 2m, 3]\) linear code.
- When \( q \) is even and \( m \) is odd.
When

When both \( q \) and \( m \) are odd.

When \( q \) is odd and \( m \) is even.

The dual \( C_{f_2,g_2}^{(q)\perp} \) is always a \([q^{2m-1}+1,q^{2m-1}+2m,3]\) linear code over \( \mathbb{F}_q \).

\begin{itemize}
  \item If \( q = 2^l \), \( l \geq 2 \), the dual \( C_{f_2,g_2}^{(q)\perp} \) is a \([q^{2m-1}+1,q^{2m-1}+2m,3]\) linear code.
  \item When \( q \) is even, we deduce that
    \[
    \sum_{z \in \mathbb{F}_q^m} \chi(z) \sum_{w \in \mathbb{F}_q^m} \sum_{(x,y) \in \mathbb{F}_m^2} \chi(w \text{Tr}(x) + w \text{Tr}(y^2)) \chi'(zbx + zcy)
    \]
    \[
    = \sum_{z \in \mathbb{F}_q^m} \chi(z) \sum_{w \in \mathbb{F}_q^m} \chi'((w + zb)x) \sum_{y \in \mathbb{F}_q^m} \chi'(wcy^2 + zcy)
    \]
    \[
    = \begin{cases}
      0, & \text{if } w \neq -zb, \\
      q^n \sum_{z \in \mathbb{F}_q^m} \chi(z) \sum_{y \in \mathbb{F}_q^m} \chi'(-zby^2 + zcy), & \text{if } w = -zb,
    \end{cases}
    \]
    \[
    = \begin{cases}
      0, & \text{if } b \in \mathbb{F}_q^m \setminus \mathbb{F}_q^* \\
      q^n \Omega(a,b,c), & \text{if } b \in \mathbb{F}_q^*,
    \end{cases}
    \]
    where \( \Omega(a,b,c) \) is shown in Lemma 17.

Since \( \#D = q^{2m-1} \), by Lemma 12 for any codeword \( \mathbf{c}_{a,b,c} \) in \( C_{f_2,g_2}^{(q)} \),

- when \( q \) is even, we deduce that
  \[
  \text{wt}(\mathbf{c}_{a,b,c}) = \begin{cases}
    0, & \text{if } a = b = c = 0, \\
    q^{2m-1}, & \text{if } a \neq 0, b = 0, c = 0, \\
    q^{2m-1} + 1, & \text{if } b \in \mathbb{F}_q^*, c \in \mathbb{F}_q^*, \text{Tr}_2^{q}(ab) = 1, \delta(b) = 0, \\
    (q - 1)q^{2m-2}, & \text{if } b \in \mathbb{F}_q^m \setminus \mathbb{F}_q^*, \delta(b) = 0, \\
    (q - 1)q^{2m-2} + 1, & \text{if } b \in \mathbb{F}_q^m \setminus \mathbb{F}_q^*, \delta(b) = 1, \\
    (q - 2)q^{2m-2}, & \text{if } b \in \mathbb{F}_q^*, c \in \mathbb{F}_q^*, \text{Tr}_2^{q}(ab) = 0, \delta(b) = 0, \\
    (q - 2)q^{2m-2} + 1 & \text{if } b \in \mathbb{F}_q^*, c \in \mathbb{F}_q^*, \text{Tr}_2^{q}(ab) = 0, \delta(b) = 1,
  \end{cases}
  \]
- \( \text{Tr}(x) = \text{Tr}(y^2) \) as show in Theorem 4. For any \( a \in \mathbb{F}_q, (b, c) \in \mathbb{F}_q^2 \setminus \{0, 0\} \), for \( f_2(x) = \text{Tr}(x), g_2(y) = \text{Tr}(y^2) \), we have

- The dual \( C_{f_2,g_2}^{(q)\perp} \) is a \([q^{2m-1}+1,q^{2m-1}+2m,3]\) linear code.

Proof: The code length of \( C_{f_2,g_2}^{(q)} \) is \( q^{2m-1} + 1 \) as show in Theorem 4.
where \( a \in \mathbb{F}_q, b, c \in \mathbb{F}_{q^m} \). If \( 2 \mid m \), for any \( b \in \mathbb{F}_{q^m}^* \), \( \delta(b) = 0 \). Then

\[
wt(c_{a,b,c}) = \begin{cases} 
0 & \text{with 1 time}, \\
q^{2m-1} & \text{with } (q-1)(q^2-q+2)/2 \text{ time}, \\
(q-1)q^{2m-2} & \text{with } q^{2m} - q^3 + 2q^2 - 2q \text{ time}, \\
(q-1)q^{2m-2} + 1 & \text{with } q^{2m+1} - q^{2m} \text{ time}, \\
(q-2)q^{2m-2} & \text{with } q(q-1)^2/2 \text{ time}.
\end{cases}
\]

If \( 2 \nmid m \), for any \( b \in \mathbb{F}_q^* \), \( \delta(b) = 1 \). Then

\[
wt(c_{a,b,c}) = \begin{cases} 
0 & \text{with 1 time}, \\
q^{2m-1} & \text{with } q-1 \text{ time}, \\
q^{2m-1} + 1 & \text{with } q(q-1)^2/2 \text{ time}, \\
(q-1)q^{2m-2} & \text{with } q^{2m} - q \text{ time}, \\
(q-1)q^{2m-2} + 1 & \text{with } q^{2m+1} - q^{2m} - q^3 + 2q^2 - q \text{ time}, \\
(q-2)q^{2m-2} + 1 & \text{with } q(q-1)^2/2 \text{ time}.
\end{cases}
\]

- When both \( q \) and \( m \) are odd, we deduce that

\[
wt(c_{a,b,c}) = \begin{cases} 
0 & \text{if } a = b = c = 0, \\
q^{2m-1} & \text{if } a \neq 0, b = c = 0, \\
(q-1)q^{2m-2} & \text{if } b \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q, \delta(b) = 0, \\
(q-1)q^{2m-2} + 1 & \text{or } b = 0, c \neq 0, \\
(q-1)q^{2m-2} + q^{3m-3}(-1)^{(p-1)(m+1)+4} & \text{or } b \in \mathbb{F}_q^*, a + \text{Tr}(\frac{c^2}{2q}) = 0, \delta(b) = 0, \\
(q-1)q^{2m-2} + q^{3m-3}(-1)^{(p-1)(m+1)+4}/4 + 1 & \text{if } b \in \mathbb{F}_q^*, a + \text{Tr}(\frac{c^2}{2q}) = 0, \delta(b) = 1, \\
(q-1)q^{2m-2} + q^{3m-3}(-1)^{(p-1)(m+1)+4}/4 & \text{or } b \in \mathbb{F}_q^*, a + \text{Tr}(\frac{c^2}{2q}) = 0, \delta(b) = 1, \\
(q-1)q^{2m-2} + q^{3m-3}(-1)^{(p-1)(m+1)+4} & \text{if } b \in \mathbb{F}_q^*, a + \text{Tr}(\frac{c^2}{2q}) = 0, \delta(b) = 1, \\
(q-2)q^{2m-2} + q^{3m-3}(-1)^{(p-1)(m+1)+4} + 1 & \text{if } b \in \mathbb{F}_q^*, a + \text{Tr}(\frac{c^2}{2q}) = 0, \delta(b) = 1.
\end{cases}
\]

If \( p \mid m \),

\[
wt(c_{a,b,c}) = \begin{cases} 
0 & \text{with 1 time}, \\
q^{2m-1} & \text{with } q-1 \text{ time}, \\
(q-1)q^{2m-2} & \text{with } q^{2m} - q^{m+2} + 2q^m - q^m - q \text{ time}, \\
(q-1)q^{2m-2} + 1 & \text{with } q^{2m+1} - q^{2m} \text{ time}, \\
(q-1)q^{2m-2} + q^{3m-3}(-1)^{(p-1)(m+1)+4}/4 & \text{with } (q^{m+2} - 2q^{m+1} + q^m)/2 \text{ time}, \\
(q-1)q^{2m-2} + q^{3m-3}(-1)^{(p-1)(m+1)+4}/4 + 1 & \text{with } (q^{m+2} - 2q^{m+1} + q^m)/2 \text{ time}.
\end{cases}
\]
If \( p \nmid m \),

\[
wt(c_{a,b,c}) = \begin{cases} 
0 & \text{with 1 time,} \\
q^{2m-1} & \text{with } q - 1 \text{ time,} \\
(q - 1)q^{2m-2} & \text{with } q^2m - q - q^m \text{ time,} \\
(q - 1)q^{2m-2} + 1 & \text{with } q^2m + 1 - q^{m+2} + 2q^m + q^m \text{ time,} \\
(q - 1)q^{2m-2} + q^{3m-3} \frac{(1)}{2} \left( 1 - \frac{\ell(p-1)(m+1)+1}{4} \right) + 1 & \text{with } (q^m+2 - 2q^{m+1} + q^m)/2 \text{ time,} \\
(q - 1)q^{2m-2} + q^{3m-3} \frac{(1)}{2} \left( 1 - \frac{\ell(p-1)(m+1)+1}{4} \right) + 1 & \text{with } (q^m+2 - 2q^{m+1} + q^m)/2 \text{ time.}
\end{cases}
\]

- When \( q \) is odd and \( m \) is even, we deduce that

\[
wt(c_{a,b,c}) = \begin{cases} 
0 & \text{if } a = 0, b = c = 0, \\
q^{2m-1} & \text{if } a \neq 0, b = c = 0, \\
(q - 1)q^{2m-2} & \text{if } b \in \mathbb{F}_q, \delta(b) = 0, \\
(q - 1)q^{2m-2} + 1 & \text{or } b = 0, c \neq 0, \\
(q - 1)q^{2m-2} + (q - 1)q^{3m-4} \frac{(1)}{2} \left( 1 - \frac{\ell(p-1)(m+1)+1}{4} \right) + 1 & \text{if } b \in \mathbb{F}_q, \delta(b) = 1, \\
(q - 1)q^{2m-2} + (q - 1)q^{3m-4} \frac{(1)}{2} \left( 1 - \frac{\ell(p-1)(m+1)+1}{4} \right) + 1 & \text{if } b \in \mathbb{F}_q, a + \text{Tr}(\frac{c^2}{q^2}) = 0, \delta(b) = 0, \\
(q - 1)q^{2m-2} + q^{3m-4} \frac{(1)}{2} \left( 1 - \frac{\ell(p-1)(m+1)+1}{4} \right) + 1 & \text{if } b \in \mathbb{F}_q, a + \text{Tr}(\frac{c^2}{q^2}) = 0, \delta(b) = 1, \\
(q - 1)q^{2m-2} + q^{3m-4} \frac{(1)}{2} \left( 1 - \frac{\ell(p-1)(m+1)+1}{4} \right) + 1 & \text{if } b \in \mathbb{F}_q, a + \text{Tr}(\frac{c^2}{q^2}) \neq 0, \delta(b) = 0, \\
(q - 1)q^{2m-2} + q^{3m-4} \frac{(1)}{2} \left( 1 - \frac{\ell(p-1)(m+1)+1}{4} \right) + 1 & \text{if } b \in \mathbb{F}_q, a + \text{Tr}(\frac{c^2}{q^2}) \neq 0, \delta(b) = 1.
\end{cases}
\]

If \( p \mid m \),

\[
wt(c_{a,b,c}) = \begin{cases} 
0 & \text{with 1 time,} \\
q^{2m-1} & \text{with } q - 1 \text{ time,} \\
(q - 1)q^{2m-2} & \text{with } q^2m - q^{m+2} + q^m - 1 \text{ time,} \\
(q - 1)q^{2m-2} + 1 & \text{with } q^{2m+1} - q^2m \text{ time,} \\
(q - 1)q^{2m-2} + (q - 1)q^{3m-4} \frac{(1)}{2} \left( 1 - \frac{\ell(p-1)(m+1)+1}{4} \right) + 1 & \text{with } q^{m+1} - q^m \text{ time,} \\
(q - 1)q^{2m-2} + q^{3m-4} \frac{(1)}{2} \left( 1 - \frac{\ell(p-1)(m+1)+1}{4} \right) + 1 & \text{with } q^m(q - 1)^2 \text{ time.}
\end{cases}
\]

If \( p \nmid m \),

\[
wt(c_{a,b,c}) = \begin{cases} 
0 & \text{with 1 time,} \\
q^{2m-1} & \text{with } q - 1 \text{ time,} \\
(q - 1)q^{2m-2} & \text{with } q^2m - q - q^m \text{ time,} \\
(q - 1)q^{2m-2} + 1 & \text{with } q^{2m+1} - q^{m+2} + q^m \text{ time,} \\
(q - 1)q^{2m-2} + (q - 1)q^{3m-4} \frac{(1)}{2} \left( 1 - \frac{\ell(p-1)(m+1)+1}{4} \right) + 1 & \text{with } q^m + 1 - q^m \text{ time,} \\
(q - 1)q^{2m-2} + q^{3m-4} \frac{(1)}{2} \left( 1 - \frac{\ell(p-1)(m+1)+1}{4} \right) + 1 & \text{with } q^m(q - 1)^2 \text{ time.}
\end{cases}
\]

When \( q = 2 \) and \( m \) is even, observe that \((q - 2)q^{2m-2} = 0\), the codeword with Hamming weight 0 occurs 2 times if \((a, b, c)\) runs through \(\mathbb{F}_2 \times \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}\). Thus, in this subcase, every codeword in \(C_{f_{2,92}}^{(q)}\) repeats 2 times, the dimension of \(C_{2}^{(q)}\) is 2m. In other subcases, the dimension of \(C_{f_{2,92}}^{(q)}\) is 2m + 1 as \(A_0 = 1\).

The code length and dimension of \(C_{f_{2,92}}^{(q)}\) are obvious. It follows from Theorem 4 and Lemma 7 that the minimal distance of \(C_{f_{2,92}}^{(q)}\) satisfies \(d_2^{(q)} \geq 3\).

- When \( q = 2 \) and \( m \) is odd, \(C_{f_{2,92}}^{(q)}\) is of length \(2^{2m-1} + 1\) and dimension \(2^{2m-1} - 2m\). By the sphere-packing bound of codes, we have

\[
2^{2m-1} + 1 \geq 2^{2m-1} - 2m \left( \sum_{i=0}^{(d_2^{(q)})-1} \left( \begin{array}{c} 2^{2m-1} + 1 \end{array} \right) \right).
\]
Consequently,
\[
2^{2m+1} \geq \left( \sum_{i=0}^{\lfloor \frac{d_2^{(q)\perp}}{2} \rfloor - 1} \left( \begin{array}{c} 2^{2m-1} + 1 \\ i \end{array} \right) \right).
\]

Then it’s easy to verify that \( d_2^{(q)\perp} \leq 4 \). By the first four Pless power moments, one can derive that \( d_2^{(q)\perp} = 4 \).

- For the other subcases, by the first four Pless power moments, we can always derive that \( d_2^{(q)\perp} = 3 \).

The proof is now completed.

### TABLE VI: The weight distribution of \( C_{f_2,g_2}^{(q)} \) with \( q = 2 \) and \( m \) even.

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

### TABLE VII: The weight distribution of \( C_{f_2,g_2}^{(q)} \) with \( q = 2^l \), \( l \geq 2 \) and \( m \) even.

| Weight | Multiplicity |
|--------|--------------|
| 0      | 1            |
| \( (q-2)q^{2m-2} \) | \( q(q-1)^2/2 \) |
| \( (q-1)q^{2m-2} \) | \( q^2m - q^2 + 2q^2 - 2q \) |
| \( (q-1)q^{2m-2} + 1 \) | \( q^{2m+1} - q^2m - q^3 + 2q^2 - q \) |
| \( q^{2m-1} \) | \( (q-1)(q^2 - q + 2)/2 \) |

### TABLE VIII: The weight distribution of \( C_{f_2,g_2}^{(q)} \) with \( q \) even and \( m \) odd.

| Weight | Multiplicity |
|--------|--------------|
| 0      | 1            |
| \( (q-2)q^{2m-2} + 1 \) | \( q(q-1)^2/2 \) |
| \( (q-1)q^{2m-2} \) | \( q^2m - q \) |
| \( (q-1)q^{2m-2} + 1 \) | \( q^{2m+1} - q^2m - q^3 + 2q^2 - q \) |
| \( q^{2m-1} \) | \( q-1 \) |
| \( q^{2m-1} + 1 \) | \( q(q-1)^2/2 \) |

### TABLE IX: The weight distribution of \( C_{f_2,g_2}^{(q)} \) with \( q \) odd, \( m \) odd and \( p | m \).

| Weight | Multiplicity |
|--------|--------------|
| 0      | 1            |
| \( (q-1)q^{2m-2} - q^{2m-2} \) | \( (q^m + 2q^{m+1} + q^m)/2 \) |
| \( (q-1)q^{2m-2} \) | \( q^2m - q^{m+2} + 2q^{m+1} - q^m - q \) |
| \( (q-1)q^{2m-2} + 1 \) | \( q^{2m+1} - q^2m \) |
| \( q^{2m-1} \) | \( (q^m + 2q^{m+1} + q^m)/2 \) |
| \( q^{2m-1} \) | \( q-1 \) |

**Example 5:** The following examples show that the subfield code \( C_{f_2,g_2}^{(q)} \) is attractive. The optimality are obtained from the code tables at [http://www.codetables.de/](http://www.codetables.de/)

- Let \( q = 2 \), \( m = 2 \). Then \( C_{f_2,g_2}^{(q)} \) has parameters \([9, 4, 4]\), which is optimal. Its dual code \( C_{f_2,g_2}^{(q)\perp} \) has parameters \([9, 5, 3]\), which is almost optimal.
- Let \( q = 2 \), \( m = 3 \). Then the dual code \( C_{f_2,g_2}^{(q)\perp} \) has parameters \([33, 26, 4]\), which is optimal.
- Let \( q = 2 \), \( m = 4 \). Then \( C_{f_2,g_2}^{(q)} \) has parameters \([129, 8, 64]\), which is optimal. Its dual code \( C_{f_2,g_2}^{(q)\perp} \) has parameters \([129, 121, 3]\), which is optimal.
Let $q = 4$, $m = 2$. Then the dual code $\mathcal{C}_{f_2,g_2}^{(4)}$ has parameters $[65, 60, 3]$, which is optimal.

Let $q = 3$, $m = 2$. Then the dual code $\mathcal{C}_{f_2,g_2}^{(3)}$ has parameters $[28, 23, 3]$, which is optimal.

Let $q = 5$, $m = 2$. Then the dual code $\mathcal{C}_{f_2,g_2}^{(5)}$ has parameters $[126, 121, 3]$, which is optimal.

From Lemma 13 and Theorem 5 we can directly get the following conclusions.

**Theorem 6**: Let $q = p^l$. If $m \geq 2$, the following statements hold.

- **When $q$ is even.**
  
  - If $q = 2$, $\mathcal{C}_{f_2,g_2}^{(2)}$ is an optimal $[2^{2m-1}, 2m, 2^{2m-2}]$ binary code achieving the Griesmer bound with weight enumerator
    
    $$1 + (2^m - 2)z^{2m-2} + z^{2m-1}.$$  

  The dual $\mathcal{C}_{f_2,g_2}^{(2)}$ is an optimal $[2^{2m-1}, 2^{2m-2} - 2m, 4]$ binary code with respect to the sphere-packing bound.

  - If $q = 2^l$, $l \geq 2$, $\mathcal{C}_{f_2,g_2}^{(q)}$ is a three-weight $q$-ary linear code with parameters $[q^{2m-1}, 2m+1, (q-2)q^{2m-2}]$ and the weight distribution in Table XI. The dual $\mathcal{C}_{f_2,g_2}^{(q)}$ is a $[q^{2m-1}, q^{2m-1} - 2m - 1, 3]$ linear code over $\mathbb{F}_q$.

- **When both $q$ and $m$ are odd.** $\mathcal{C}_{f_2,g_2}^{(q)}$ is a four-weight $q$-ary linear code with parameters $[q^{2m-1}, 2m+1, (q-1)q^{2m-2} - q^{2m-3}/2]$ and the weight distribution in Table XIV. The dual $\mathcal{C}_{f_2,g_2}^{(q)}$ is a $[q^{2m-1}, q^{2m-1} - 2m - 1, 3]$ linear code over $\mathbb{F}_q$.

- **When $q$ is odd and $m$ is even.** $\mathcal{C}_{f_2,g_2}^{(q)}$ is a four-weight $q$-ary linear code with parameters $[q^{2m-1}, 2m+1]$ and the weight distribution in Table XVI. The dual $\mathcal{C}_{f_2,g_2}^{(q)}$ is also a $[q^{2m-1}, q^{2m-1} - 2m - 1, 3]$ linear code over $\mathbb{F}_q$.
Remark 4: Note that, when \( q = 2 \), \( \bar{C}_{f_2,g_2}^{(2)} \) is actually the first order Reed-Muller code \( R(1, 2m - 1) \) \[20]\). When \( q = 4, m \geq 2 \), by XIII every codeword of \( \bar{C}_{f_2,g_2}^{(q)} \) has weight divisible by two, thus it is a \([2^{4m-2}, 2m + 1, 2^{4m-3}]\) quaternary Hermitian self-orthogonal code \[20]\).

**Example 6:** The following examples show that the subfield code \( \bar{C}_{f_2,g_2}^{(q)} \) is attractive. The optimality are obtained from the code tables at [http://www.codetables.de/](http://www.codetables.de/)

- Let \( q = 2, m = 2 \). Then \( \bar{C}_{f_2,g_2}^{(q)} \) has parameters \([8, 4, 4]\), which is optimal. Its dual code \( \bar{C}_{f_2,g_2}^{(q)} \perp \) has parameters \([8, 4, 4]\), which is also optimal.
- Let \( q = 2, m = 3 \). Then \( \bar{C}_{f_2,g_2}^{(q)} \) has parameters \([32, 6, 16]\), which is optimal. Its dual code \( \bar{C}_{f_2,g_2}^{(q)} \perp \) has parameters \([32, 26, 4]\), which is also optimal.
- Let \( q = 2, m = 4 \). Then \( \bar{C}_{f_2,g_2}^{(q)} \) has parameters \([128, 8, 64]\), which is optimal. Its dual code \( \bar{C}_{f_2,g_2}^{(q)} \perp \) has parameters \([128, 120, 4]\), which is optimal.
- Let \( q = 4, m = 2 \). Then the dual code \( \bar{C}_{f_2,g_2}^{(q)} \perp \) has parameters \([64, 59, 3]\), which is optimal.
- Let \( q = 3, m = 3 \). Then the dual code \( \bar{C}_{f_2,g_2}^{(q)} \perp \) has parameters \([243, 236, 3]\), which is optimal.
- Let \( q = 3, m = 2 \). Then the dual code \( \bar{C}_{f_2,g_2}^{(q)} \perp \) has parameters \([27, 22, 3]\), which is optimal.
- Let \( q = 5, m = 2 \). Then the dual code \( \bar{C}_{f_2,g_2}^{(q)} \perp \) has parameters \([125, 120, 3]\), which is optimal.

**Example 6:** The following examples show that the subfield code \( \bar{C}_{f_2,g_2}^{(q)} \) is attractive. The optimality are obtained from the code tables at [http://www.codetables.de/](http://www.codetables.de/)

- Let \( q = 2, m = 2 \). Then \( \bar{C}_{f_2,g_2}^{(q)} \) has parameters \([8, 4, 4]\), which is optimal. Its dual code \( \bar{C}_{f_2,g_2}^{(q)} \perp \) has parameters \([8, 4, 4]\), which is also optimal.
- Let \( q = 2, m = 3 \). Then \( \bar{C}_{f_2,g_2}^{(q)} \) has parameters \([32, 6, 16]\), which is optimal. Its dual code \( \bar{C}_{f_2,g_2}^{(q)} \perp \) has parameters \([32, 26, 4]\), which is also optimal.
- Let \( q = 2, m = 4 \). Then \( \bar{C}_{f_2,g_2}^{(q)} \) has parameters \([128, 8, 64]\), which is optimal. Its dual code \( \bar{C}_{f_2,g_2}^{(q)} \perp \) has parameters \([128, 120, 4]\), which is optimal.
- Let \( q = 4, m = 2 \). Then the dual code \( \bar{C}_{f_2,g_2}^{(q)} \perp \) has parameters \([64, 59, 3]\), which is optimal.
- Let \( q = 3, m = 3 \). Then the dual code \( \bar{C}_{f_2,g_2}^{(q)} \perp \) has parameters \([243, 236, 3]\), which is optimal.
- Let \( q = 3, m = 2 \). Then the dual code \( \bar{C}_{f_2,g_2}^{(q)} \perp \) has parameters \([27, 22, 3]\), which is optimal.
- Let \( q = 5, m = 2 \). Then the dual code \( \bar{C}_{f_2,g_2}^{(q)} \perp \) has parameters \([125, 120, 3]\), which is optimal.

C. \( f_3(x) = \Tr_{2^m}^2(x) \) and \( g_3(y) = \Tr_{2^m}^2(A(y)) \) with \( A(y) \) an almost bent function

In this section, let \( q = 2, m \) be odd and \( f_3(x) = \Tr_{2^m/2(x)}, g_3(y) = \Tr_{2^m/2(A(y))} \), where \( A(y) \) is an almost bent function from \( \mathbb{F}_{2^m} \) to itself. For convenience, abbreviate \( \Tr_{2^m/2(x)} \) by \( \Tr(x) \) for the rest of this subsection.

**Theorem 7:** \( \bar{C}_{f_3,g_3}^{(2)} \) is a five-weight binary code with parameters \([2^{2m-1} + 1, 2m + 1, 2^{2m-2} - 2^{2m-3} + 1]\) and the weight distribution is given in Table \[XVI\]. The dual \( \bar{C}_{f_3,g_3}^{(2)} \) is is an optimal \([2^{2m-1} + 1, 2m, 4]\) binary code with respect to the sphere-packing bound.
Proof: For \( f_3(x) = \text{Tr}(x), \ g_3(y) = \text{Tr}(A(y)) \), by the transitivity of trace functions, we have
\[
\#D = 2^{2m-1} + \frac{1}{2} \sum_{x \in \mathbb{F}_2^m} \chi(\text{Tr}(x)) \sum_{y \in \mathbb{F}_2^m} \chi(\text{Tr}(A(y))) = 2^{2m-1}.
\]

Then from Lemma 11 the code length of \( C_{f_3,g_3}^{(2)} \) is \( n = 2^{2m-1} + 1 \).

For any \( a \in \mathbb{F}_2, \ (b, c) \in \mathbb{F}_2^2 \setminus \{0,0\} \),
\[
\Upsilon_{a,b,c} = \sum_{x \in \mathbb{F}_2} \chi(za) \sum_{w \in \mathbb{F}_2^2 (x,y) \in \mathbb{F}_2^2} \chi(wTr(x) + wTr(A(y))) \chi'(zbx + zcy)
= (-1)^a \sum_{x \in \mathbb{F}_2} \chi'((1+b)x) \sum_{y \in \mathbb{F}_2} \chi'(A(y) + cy)
= \begin{cases} 
0 & \text{if } b \neq 1, \\
(-1)^a 2^m W_A(1, c) & \text{if } b = 1,
\end{cases}
\]
where \( W_A(1, c) = 0 \) or \( \pm 2^{\frac{m+1}{2}} \) from the definition of almost Bent function.

Since \( m \) is odd, \( \text{Tr}(1) = m \neq 0 \). By Lemma 12 for any codeword \( c_{a,b,c} \) in \( C_{f_3,g_3}^{(2)} \) we deduce that
\[
\text{wt}(c_{a,b,c}) = \begin{cases} 
0 & \text{if } a = b = c = 0, \\
2^{2m-1} & \text{if } a \neq 0, b = c = 0, \\
2^{2m-2} & \text{if } b = 0, c \neq 0, \\
2^{2m-2} + 1 & \text{if } b \neq 1, \delta(b) = 1, \\
2^{2m-2} - 2^{\frac{3m-3}{2}} + 1 & \text{if } b = 1, a = 0, W_A(1, c) = 2^\frac{m+1}{2}, \\
2^{2m-2} - 2^{\frac{3m-3}{2}} + 1 & \text{if } b = 1, a = 1, W_A(1, c) = 2^\frac{m+1}{2}, \\
2^{2m-2} + 2^{\frac{3m-3}{2}} + 1 & \text{if } b = 1, a = 0, W_A(1, c) = 2^{-\frac{m+1}{2}}, \\
2^{2m-2} + 2^{\frac{3m-3}{2}} + 1 & \text{if } b = 1, a = 1, W_A(1, c) = 2^{-\frac{m+1}{2}}, \\
\end{cases}
\]
with 1 time,
with 2 times,
with \( i_1 \) times,
with \( i_2 \) times,
with \( i_3 \) times.

It’s obvious that \( i_2 = i_3 \) and the dimension of \( C_{f_3,g_3}^{(2)} \) is \( 2m + 1 \) as \( A_0 = 1 \).

Since any two columns of matrix \( G_{f_3,g_3} \) are linear independent. It follows from Lemma 7 that the minimal distance \( d_3^{(2)\perp} \) of \( C_{f_3,g_3}^{(2)\perp} \) satisfies \( d_3^{(2)\perp} \geq 3 \). Then by the first three Pless power moments, one can derive that \( i_1 = 2^{2m} - 2^m \) and \( i_2 = i_3 = 2^{m-1} \).

Note that \( C_{f_3,g_3}^{(2)\perp} \) is of length \( q^{2m-1} + 1 \) and dimension \( q^{2m-1} - 2m \). By the sphere-packing bound of codes, we have
\[
2^{2m-1} + 1 \geq 2^{2m-1} - 2m \left( \sum_{i=0}^{[d_3^{(2)\perp}-1]} \binom{2^{2m-1} + 1}{i} \right).
\]

Consequently,
\[
2^{2m+1} \geq \left( \sum_{i=0}^{[d_3^{(2)\perp}-1]} \binom{2^{2m-1} + 1}{i} \right).
\]
Then it’s easy to verify that $d_3^{(2)\perp} \leq 4$. By the first four Pless power moments, one can derive that $d_3^{(2)\perp} = 4$. 

From Lemma 13 and Theorem 7, we can directly get the following conclusions.

**Theorem 8:** The linear code $\bar{C}_{f_3,g_3}^{(2)}$ is a binary four-weight linear code with parameters $[2^{2m-1},2m+1,2^{2m-2} - 2^{3m-3}]$ and the weight distribution in Table XVII. The dual code $\bar{C}_{f_3,g_3}^{(2)}$ is an optimal $[2^{2m-1},2^{2m-1} - 2m - 1,4]$ binary code with respect to the sphere-packing bound.

| Weight | Multiplicity |
|--------|--------------|
| $2^{2m-2} - 2^{3m-3}$ | $2^{2m-1}$ |
| $2^{2m-2}$ | $2^{2m-2}$ |
| $2^{2m-2} + 2^{3m-2}$ | $2^{2m-1}$ |

**Table XVII:** The weight distribution of $\bar{C}_{f_3,g_3}^{(2)}$.

$D. f_4(x) = \text{Tr}_{2m/2}(A_1(x))$ and $g_4(y) = \text{Tr}_{2m/2}(A_2(y))$ with $A_1, A_2$ are two different almost bent functions

In this section, let $q = 2$, $m$ be odd and $f_4(x) = \text{Tr}_{2m/2}(A_1(x))$, $g_4(y) = \text{Tr}_{2m/2}(A_2(y))$, where $A_1, A_2$ are two different almost bent functions from $\mathbb{F}_{2^m}$ to itself. We mainly focus on the parameters and weight distribution of the punctured code $\bar{C}_{f_4,g_4}^{(2)}$. For convenience, abbreviate $\text{Tr}_{2m/2}(x)$ by $\text{Tr}(x)$ for the rest of this subsection.

**Theorem 9:** The punctured code $\bar{C}_{f_4,g_4}^{(2)}$ is a four-weight binary code with parameters $[2^{2m-1} + W/2,2m+1,2^{2m-2} + W/4 - 2m-1]$, where $W \in \{0,-2m+1,2m+1\}$. The weight distribution is shown in Table XVIII. The dual $\bar{C}_{f_4,g_4}^{(2)\perp}$ is an optimal $[2^{2m-1} + W/2,2^{2m-1} + W/2 - 2m - 1,4]$ binary code with respect to the sphere-packing bound.

**Proof:** The code length of $\bar{C}_{f_4,g_4}^{(2)}$ with $f_4(x) = \text{Tr}(A_1(x))$, $g_4(y) = \text{Tr}(A_2(y))$, is

$$n = \#D = 2^{2m-1} + \frac{1}{2} \sum_{x \in \mathbb{F}_{2^m}} \chi(\text{Tr}(A_1(x))) \sum_{y \in \mathbb{F}_{2^m}} \chi(\text{Tr}(A_2(y))) = 2^{2m-1} + W/2,$$

where $W = W_{A_1}(1,0)W_{A_2}(1,0) = 0$ or $\pm 2m+1$.

For any $a \in \mathbb{F}_2$, $(b,c) \in \mathbb{F}_{2^m} \setminus \{0,0\}$,

$$\Upsilon_{a,b,c} = \sum_{z \in \mathbb{F}_2} \chi(z) \sum_{w \in \mathbb{F}_2} \chi(w \text{Tr}(A_1(x)) + w \text{Tr}(A_2(y))) \chi'(bz + cy)$$

$$= (-1)^a \sum_{x \in \mathbb{F}_{2^m}} \chi'(A_1(x) + bx) \sum_{y \in \mathbb{F}_{2^m}} \chi'(A_2(y) + cy)$$

$$= (-1)^a W',$$

where $W' = W_{A_1}(1,b)W_{A_2}(1,c) = 0$ or $\pm 2m+1$. 

| Weight | Multiplicity |
|--------|--------------|
| $2^{2m-2} - 2^{3m-3}$ | $2^{2m-1}$ |
| $2^{2m-2}$ | $2^{2m-2}$ |
| $2^{2m-2} + 2^{3m-2}$ | $2^{2m-1}$ |

**Table XVIII:** The weight distribution of $\bar{C}_{f_4,g_4}^{(2)}$. 

By Lemma 15 for any codeword \( \mathbf{c}_{a,b,c} \) in \( \tilde{C}^{(2)}_{f,s,g_4} \) we deduce that
\[
\text{wt}(\mathbf{c}_{a,b,c}) = \begin{cases} 
0, & \text{if } a = b = c = 0, \\
2^{m-1} + \frac{W}{2}, & \text{if } a \neq 0, b = c = 0, \\
2^{m-2} + \frac{W}{4}, & \text{if } b \text{ and } c \text{ are not all } 0, W' = 0, \\
2^{m-2} + \frac{W}{4} + 2^{m-1}, & \text{if } b \text{ and } c \text{ are not all } 0, a = 0, W' = -2^{m+1}, \\
2^{m-2} + \frac{W}{4} - 2^{m-1}, & \text{if } b \text{ and } c \text{ are not all } 0, a = 0, W' = 2^{m+1}, \\
2^{m-2} + \frac{W}{4} + 2^{m-1}, & \text{with } i_1 \text{ times}, \\
2^{m-2} + \frac{W}{4} - 2^{m-1}, & \text{with } i_3 \text{ times}.
\end{cases}
\]

It’s obvious that \( i_2 = i_3 \) and the dimension of \( \tilde{C}^{(2)}_{f,s,g_4} \) is \( 2m + 1 \) as \( A_0 = 1 \).

Let \( \tilde{G}_{f,s,g_4} \) be the submatrix obtained by deleting the first column of \( G_{f,s,g_4} \). Since any two columns of matrix \( \tilde{G}_{f,s,g_4} \) are linear independent. It follows from Lemma 7 that the minimal distance of \( \tilde{C}^{(2)}_{f,s,g_4} \) satisfies \( d^1_4(\tilde{C}^{(2)}_{f,s,g_4}) \geq 3 \). Then by the first three Pless power moments, one can derive that \( i_1 = 3 \cdot 2^{2m-1} - 2 + \frac{w^2}{2^{2m+1}} \) and \( i_2 = i_3 = 2^{2m-2} - \frac{w^2}{2^{m+2}} \).

Note that \( \tilde{C}^{(2)}_{f,s,g_4} \) is of length \( 2^{2m-1} + \frac{W}{2} \) and dimension \( 2^{2m-1} + \frac{W}{2} - 2^{m-1} - 2 \). By the sphere-packing bound of codes, we have
\[
2^{2m-1} + \frac{W}{2} \geq 2^{2m-1} + \frac{W}{2} - 2^{m-1} - 2 \sum_{i=0}^{\left\lfloor \frac{d^1_4(\tilde{C}^{(2)}_{f,s,g_4})}{2} \right\rfloor} \left( \binom{2^{m-1} + \frac{W}{2}}{i} \right).
\]

Consequently,
\[
2^{m+1} \geq \left( \sum_{i=0}^{\left\lfloor \frac{d^1_4(\tilde{C}^{(2)}_{f,s,g_4})}{2} \right\rfloor} \binom{2^{m-1} + \frac{W}{2}}{i} \right).
\]

It’s easy to verify that \( d^1_4(\tilde{C}^{(2)}_{f,s,g_4}) \leq 4 \). By the first four Pless power moments, one can derive that \( d^1_4(\tilde{C}^{(2)}_{f,s,g_4}) = 4 \).

\textbf{TABLE XVIII: The weight distribution of } \tilde{C}^{(2)}_{f,s,g_4}.

| Weight | Multiplicity |
|--------|--------------|
| \( 2^{m-2} + \frac{w}{4} - 2^{m-1} \) | 1 |
| \( 2^{m-2} + \frac{w}{4} + 2^{m-1} \) | 27 |
| \( 2^{m-1} + \frac{w}{2} \) | 1 |

The following is a list of known almost bent monomials \( A(x) = x^t \) on \( \mathbb{F}_{2^m} \) for an odd \( m \):

- \( t = 2^r + 1 \), where \( \gcd(r, m) = 1 \) [19];
- \( t = 2^r - 2^r + 1 \), where \( r \geq 2 \) and \( \gcd(m, h) = 1 \) [30];
- \( t = 2^{m-2} + 3 \), where \( m \) is odd [30];
- \( t = 2^{m-2} + 2^{m-1} - 1 \), where \( m \equiv 1 \pmod{4} \) [28], [29];
- \( t = 2^{m-2} + 2^{m-1} - 1 \), where \( m \equiv 3 \pmod{4} \) [28], [29].

All almost bent monomials \( A(x) = x^t \) for \( t \) in the list above are permutation polynomials on \( \mathbb{F}_{2^m} \). Hence, the length of \( \tilde{C}^{(2)}_{f,s,g_4} \) is \( n = 2^{2m-1} \) when at least one of \( A_i(x), i = 1, 2 \), is such a monomial. Substituting the value of \( n \) into Theorem 9 we obtain the following results.
Corollary 1: Let $f_4(x) = \text{Tr}(A_1(x))$, $g_4(y) = \text{Tr}(A_2(y))$, where $A_i(x)$, $i = 1, 2$, are distinct almost bent function and at least one of them is a monomial $x^t$ for some integer $t$ in the list above. Then $\mathcal{C}_{f_4, g_4}^{(2)}$ is a four-weight binary code with parameters $[2^{2m-1}, 2m+1, 2^{2m-2} - 2^{m-1}]$. Its weight enumerator is

$$1 + 2^{2m-2}z^{2^{2m-2} - 2^{m-1}} + (3\cdot 2^{m-1} - 2)z^{2^{2m-2}} + 2^{m-2}z^{2^{2m-2} + 2^{m-1}} + z^{2^{2m-1}}.$$ 

The dual $\mathcal{C}_{f_5, g_5}^{(2)\perp}$ is an optimal $[2^{2m-1}, 2^{2m-1} - 2m - 1, 4]$ binary code with respect to the sphere-packing bound.

E. $f_5(x) = \text{Tr}_{2^m/2}(x)$ and $g_5(y) = B(y)$ with $B(y)$ an Boolean bent function

In this section, let $q = 2$, $m$ be even and $f_5(x) = \text{Tr}_{2^m/2}(x)$, $g_5(y) = B(y)$, where $B(y)$ is an Boolean bent functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. For convenience, abbreviate $\text{Tr}_{2^m/2}(x)$ by $\text{Tr}(x)$ for the rest of this subsection.

Theorem 10: $\mathcal{C}_{f_5, g_5}^{(2)}$ is a five-weight binary code with parameters $[2^{2m-1} + 1, 2m + 1, 2^{2m-2} - 2^{m-4}]$ and the weight distribution is given in Table[IX]. The dual $\mathcal{C}_{f_5, g_5}^{(2)\perp}$ is a $[2^{2m-1} + 1, 2^{2m-1} - 2m, 3]$ binary code.

Proof: For $f_5(x) = \text{Tr}(x)$, $g_5(y) = B(y)$, by the transitivity of trace functions, we have

$$\#D = 2^{2m-1} + 1 + \frac{1}{2} \sum_{x \in \mathbb{F}_{2^m}} \chi(\text{Tr}(x)) \sum_{y \in \mathbb{F}_{2^m}} \chi(B(y)) = 2^{2m-1}.$$ 

Then the code length of $\mathcal{C}_{f_5, g_5}^{(2)}$ is $n = 2^{2m-1} + 1$. For any $a \in \mathbb{F}_2$, $(b, c) \in \mathbb{F}_{2^m} \setminus \{(0, 0)\}$,

$$\mathcal{T}_{a, b, c} = (-1)^a \sum_{x \in \mathbb{F}_{2^m}} \chi'((1 + b)x) \sum_{y \in \mathbb{F}_{2^m}} \chi(B(y) + \text{Tr}(cy))$$

$$= \begin{cases} 0, & \text{if } b \neq 1, \\ (-1)^a 2^m W_B(c), & \text{if } b = 1, \end{cases}$$

where $W_B(c) = \pm 2^\frac{m}{2}$ from the definition of Boolean Bent function.

Since $m$ is even, $\text{Tr}(1) = m = 0$. By Lemma[12], for any codeword $c_{a, b, c}$ in $\mathcal{C}_{f_5, g_5}^{(2)}$, we deduce that

$$\text{wt}(c_{a, b, c}) = \begin{cases} 0, & \text{if } a = b = c = 0, \\ 2^{2m-1}, & \text{if } a = 0, b = c = 0, \\ 2^{2m-2}, & \text{if } b = 0, c = 0, \\ 2^{2m-1}, & \text{if } b = 0, c = 0, \\ 2^{2m-1}, & \text{if } b = 0, c = 0, \\ 2^{2m-1} - 2^{m-4}, & \text{if } b = 1, a = 0, W_B(c) = 2^\frac{m}{2}, \\ 2^{2m-1} - 2^{m-4}, & \text{if } b = 1, a = 1, W_B(c) = -2^\frac{m}{2}, \\ 2^{2m-1} - 2^{m-4}, & \text{if } b = 1, a = 0, W_B(c) = -2^\frac{m}{2}, \\ 2^{2m-1} - 2^{m-4}, & \text{if } b = 1, a = 1, W_B(c) = 2^\frac{m}{2}, \\ 0, & \text{with 1 time}, \\ 2^{2m-1}, & \text{with 1 time}, \\ 2^{2m-2}, & \text{with } 2^{2m} - 2^{m+1} - 2 \text{ times}, \\ 2^{2m-2}, & \text{with } 2^{2m} \text{ times}, \\ 2^{2m-2}, & \text{with } 2^{2m} \text{ times}, \\ 2^{2m-2}, & \text{with } 2^{2m} \text{ times}, \end{cases}$$

the last two values are determined because they have the same value. The dimension of $\mathcal{C}_{f_5, g_5}^{(2)}$ is $2m + 1$ as $A_0 = 1$.

Note that $\mathcal{C}_{f_5, g_5}^{(2)}$ is of length $2^{2m-1} + 1$ and dimension $2^{2m-1} - 2m$. Similar to the proof of Theorem[7] by Lemma[12] and the sphere-packing bound of codes, we have the minimal distance of $\mathcal{C}_{f_5, g_5}^{(2)\perp}$ satisfied $3 \leq d_{\perp}^{(2)} \leq 4$. By the first four Pless power moments, one can derive that $d_{\perp}^{(2)} = 3$. 

"
TABLE XIX: The weight distribution of $C_{f_5, g_5}^{(2)}$.

| Weight                | Multiplicity |
|-----------------------|--------------|
| $0$                   | 1            |
| $2^{2m-2} - 2\frac{3m-4}{2}$ | $2^m$        |
| $2^{2m-2}$            | $2^m$        |
| $2^{2m-2} + 1$        | $2^m$        |
| $2^{2m-2} - 2\frac{3m-4}{2}$ | 1            |
| $2^{2m-1}$            | 1            |

From Lemma [13] and Theorem [10] we can directly get the following conclusions.

**Theorem 11:** The linear code $C_{f_5, g_5}^{(2)}$ is a binary four-weight linear code with parameters $[2^{2m-1}, 2m+1, 2^{2m-2} - 2\frac{3m-4}{2}]$ and the weight distribution in Table XX. The dual code $C_{f_5, g_5}^{(2)\perp}$ is an optimal $[2^{2m-1}, 2^{2m-1} - 2m - 1, 4]$ binary code with respect to the sphere-packing bound.

**TABLE XX:** The weight distribution of $C_{f_5, g_5}^{(2)}$. 

| Weight                | Multiplicity |
|-----------------------|--------------|
| $0$                   | 1            |
| $2^{2m-2} - 2\frac{3m-4}{2}$ | $2^m$        |
| $2^{2m-2}$            | $2^m$        |
| $2^{2m-2} + 2\frac{3m-4}{2}$ | $2^m$        |
| $2^{2m-1}$            | 1            |

F. $f_6(x) = B_1(x)$ and $g_6(y) = B_2(y)$ with $B_1, B_2$ are two different Boolean bent functions

In this section, let $q = 2$, $m$ be even and $f_6(x) = B_1(x)$, $g_6(y) = B_2(y)$, where $B_1, B_2$ are two different Boolean bent functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$.

**Theorem 12:** $C_{f_6, g_6}^{(2)}$ is a five-weight binary linear code with parameters $[2^{2m-1} + W + 1, 2m + 1, 2^{2m-2} + W - 2^{m-2}]$, where $W = \pm 2^m$. The weight distribution is given in Table XXX. The dual $C_{f_6, g_6}^{(2)\perp}$ is a $[2^{2m-1} + W + 1, 2^{2m-1} + W - 2m, 3]$ binary code.

**Proof:** For $f_6(x) = B_1(x)$, $g_6(y) = B_2(y)$, by the transitivity of trace functions, we have

$$\#D = 2^{2m-1} + \frac{1}{2} \sum_{x \in \mathbb{F}_{2^m}} \chi(B_1(x)) \sum_{y \in \mathbb{F}_{2^m}} \chi(B_2(y)) = 2^{2m-1} + \frac{W}{2},$$

where $W = W_{B_1}(0)W_{B_2}(0) = \pm 2^m$. Then the code length of $C_{f_6, g_6}^{(2)}$ is $n = 2^{2m-1} + \frac{W}{2} + 1$. For any $a \in \mathbb{F}_2$, $(b, c) \in \mathbb{F}_{2^m}^2 \setminus \{(0, 0)\}$,

$$\Upsilon_{a,b,c} = (-1)^a \sum_{x \in \mathbb{F}_{2^m}} (-1)^{B_1(x) + \text{Tr}(bx)} \sum_{y \in \mathbb{F}_{2^m}} (-1)^{B_2(y) + \text{Tr}(cy)}$$

$$= (-1)^a W',$$

where $W' = W_{B_1}(b)W_{B_2}(c) = \pm 2^m$. 
By Lemma 12 for any codeword $c_{a,b,c}$ in $C_{f_0:g_0}^{(2)}$ we deduce that

$$wt(c_{a,b,c}) = \begin{cases} 
0, & \text{if } a = b = c = 0, \\
2^{m-1} + \frac{W}{2}, & \text{if } a \neq 0, b = c = 0, \\
2^{m-2} + \frac{W}{4} - 2^{m-2}, & \text{if } b \text{ and } c \text{ are not all } 0, a = 0, W' = 2^m, \delta(b) = 0, \\
& \text{or } a = 1, W' = -2^m, \delta(b) = 0, \\
2^{m-2} + \frac{W}{4} - 2^{m-2} + 1, & \text{if } b \text{ and } c \text{ are not all } 0, a = 0, W' = 2^m, \delta(b) = 1, \\
& \text{or } a = 1, W' = -2^m, \delta(b) = 1, \\
2^{m-2} + \frac{W}{4} + 2^{m-2}, & \text{if } b \text{ and } c \text{ are not all } 0, a = 0, W' = 2^m, \delta(b) = 0, \\
& \text{or } a = 1, W' = 2^m, \delta(b) = 0, \\
2^{m-2} + \frac{W}{4} + 2^{m-2} + 1, & \text{if } b \text{ and } c \text{ are not all } 0, a = 0, W' = 2^m, \delta(b) = 1, \\
& \text{or } a = 1, W' = 2^m, \delta(b) = 1, \\
0, & \text{with } 1 \text{ time,} \\
2^{m-1} + \frac{W}{2}, & \text{with } 1 \text{ time,} \\
2^{m-2} + \frac{W}{4} - 2^{m-2}, & \text{with } i_1 \text{ times,} \\
2^{m-2} + \frac{W}{4} - 2^{m-2} + 1, & \text{with } i_2 \text{ times,} \\
2^{m-2} + \frac{W}{4} + 2^{m-2}, & \text{with } i_3 \text{ times,} \\
2^{m-2} + \frac{W}{4} + 2^{m-2} + 1, & \text{with } i_4 \text{ times.}
\end{cases}$$

It’s obvious that $i_1 = i_3, i_2 = i_4$ and the dimension of $C_{f_0:g_0}^{(2)}$ is $2m + 1$ as $A_0 = 1$. Since any two columns of matrix $G_{f_0:g_0}$ are linear independent. It follows from Lemma 7 that the minimal distance of $C_{f_0:g_0}^{(2)}$ satisfies $d_{6}^{(2)} \geq 3$. Then by the first three Pless power moments, one can derive that $i_1 = i_3 = 2^{2m-1} - 1$ and $i_2 = i_4 = 2^{2m-1} - 2$.

Note that $C_{f_0:g_0}^{(2)}$ is of length $2^{2m-1} + 1$ and dimension $2^{2m-1} - 2m$. Similar to the proof of Theorem 7 by Lemma 12 and the sphere-packing bound of codes, we have the minimal distance of $C_{f_0:g_0}^{(2)}$ satisfied $3 \leq d_{6}^{(2)} \leq 4$. By the first four Pless power moments, one can derive that $d_{6}^{(2)} = 3$.

**TABLE XXI: The weight distribution of $C_{f_0:g_0}^{(2)}$.**

| Weight            | Multiplicity |
|-------------------|--------------|
| $2^{m-2} + \frac{W}{4} - 2^{m-2}$ | 1 |
| $2^{m-2} + \frac{W}{4} - 2^{m-2} + 1$ | $2^{m-1} - 1$ |
| $2^{m-2} + \frac{W}{4} + 2^{m-2}$ | $2^{m-1} - 1$ |
| $2^{m-2} + \frac{W}{4} + 2^{m-2} + 1$ | $2^{m-1} - 1$ |
| $2^{m-1} + \frac{W}{2}$ | 1 |

From Lemma 13 and Theorem 12 we can directly get the following conclusions.

**Theorem 13:** The linear code $C_{f_0:g_0}^{(2)}$ is a binary three-weight linear code with parameters $[2^{2m-1} + \frac{W}{2}, 2m + 1, 2^{2m-2} + \frac{W}{4} - 2^{m-2}]$ and the weight distribution in Table XXII The dual code $\tilde{C}_{f_0:g_0}^{(2)}$ is an optimal $[2^{2m-1} + \frac{W}{2}, 2^{2m-1} + \frac{W}{2} - 2m - 1, 4]$ binary code with respect to the sphere-packing bound.

**TABLE XXII: The weight distribution of $\tilde{C}_{f_0:g_0}^{(2)}$.**

| Weight            | Multiplicity |
|-------------------|--------------|
| $2^{m-2} + \frac{W}{4} - 2^{m-2}$ | 1 |
| $2^{m-2} + \frac{W}{4} + 2^{m-2}$ | 1 |
| $2^{m-1} + \frac{W}{2}$ | 1 |
IV. APPLICATION IN t-DESIGNS

Let $\kappa$ and $n$ be positive integers such that $1 \leq \kappa \leq n$. Let $\mathcal{P}$ be a set of $n$ elements and let $\mathcal{B}$ be a set of $\kappa$-subsets of $\mathcal{P}$. Let $t$ be a positive integer with $t \leq \kappa$. The pair $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is an incidence structure, where the incidence relation is the set membership. The incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is called a $t-(n, \kappa, \lambda)$ design, or simply a $t$-design, if every $t$-subset of $\mathcal{P}$ is contained in exactly $\lambda$ elements of $\mathcal{B}$. The elements of $\mathcal{P}$ are called points, and those of $\mathcal{B}$ are referred to as blocks. A $t$-design is said to be simple if $\mathcal{B}$ does not contain any repeated blocks. A $t-(n, \kappa, \lambda)$ design is called a Steiner system if $t \geq 2$ and $\lambda = 1$, and is denoted by $S(t, \kappa, \lambda)$. Let $b$ denote the number of blocks in $\mathcal{B}$. The parameters of a $t-(n, \kappa, \lambda)$ design satisfy the following equation:

$$\binom{n}{t} \lambda = \binom{\kappa}{t} b.$$

A construction of $t$-designs with linear codes goes as follows. Let $\mathcal{C}$ be a $[n, k, d]$ linear code over $\mathbb{F}_q$. Let the coordinates of a codeword of $\mathcal{C}$ be indexed by $(0, 1, \cdots, n-1)$ and define $\mathcal{P}(\mathcal{C}) = \{0, 1, \cdots, n-1\}$. For a codeword $\mathbf{e} = (c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}$, the support of $\mathbf{e}$ is defined by $\text{supp}(\mathbf{e}) = \{i : c_i \neq 0, i \in \mathcal{P}(\mathcal{C})\}$. Let $\mathcal{B}_\kappa(\mathcal{C})$ denote the set of the supports of all codewords with Hamming weight $\kappa$ in $\mathcal{C}$ without repeated blocks. If the incidence structure $\mathcal{D}_\kappa = (\mathcal{P}(\mathcal{C}), \mathcal{B}_\kappa(\mathcal{C}))$ is a $t-(n, \kappa, \lambda)$ design for some positive integers $t$ and $\lambda$, where $1 \leq \kappa \leq n$ and $A_\kappa \neq 0$, we say that the code $\mathcal{C}$ holds a $t$-design or the supports of the codewords of weight $\kappa$ in $\mathcal{C}$ hold a $t$-design.

The following theorem, which was developed by Assmus and Mattson in [2], provides a necessary condition for a linear code and its dual to hold simple $t$-designs.

**Theorem 14** (Assmus-Mattson Theorem): Let $\mathcal{C}$ be a $[n, k, d]$ code over $\mathbb{F}_q$. Let $d^\perp$ denote the minimum distance of $\mathcal{C}^\perp$. Let $w$ be the largest integer satisfying $w \leq n$ and

$$w - \left\lfloor \frac{w + q - 2}{q - 1} \right\rfloor < d.$$

Define $w^\perp$ analogously using $d^\perp$. Let $(A_i)_{i=0}^n$ and $(A_i^\perp)_{i=0}^n$ denote the weight distribution of $\mathcal{C}$ and $\mathcal{C}^\perp$, respectively. Fix a positive integer $t$ with $t < d$, and let $s$ be the number of $i$ with $A_i^\perp \neq 0$ for $1 \leq i \leq n-t$. Suppose $s \leq d-t$. Then

- the codewords of weight $i$ in $\mathcal{C}$ hold a $t$-design provided $A_i \neq 0$ and $d - i \leq w$,
- the codewords of weight $i$ in $\mathcal{C}^\perp$ hold a $t$-design provided $A_i^\perp \neq 0$ and $d^\perp - i \leq \min\{n-t, w^\perp\}$.

**Theorem 15:** The codewords of Hamming weight $q^3 - q$ in the code $C_{f_1,g_1}$ hold a $2 - (q^3 + 1, q^3 - q, (q - 1)(q^3 - q - 1))$ design. The complementary design of this code is a $2 - (q^3 + 1, q+1, 1)$ design, i.e., a Steiner system $S(2, q+1, q^3 + 1)$. The minimum weight codewords in $C_{f_1,g_1}^\perp$ hold a $2 - (q^3 + 1, 3, \lambda)$ design, where

$$\lambda = \frac{6A_3^\perp}{q^3(q^2 - 1)(q^3 + 1)}$$

and $A_3^\perp$ denotes the number of codewords of weight 3 in $C_{f_1,g_1}^\perp$.

**Proof:** The desired conclusions follow from Theorem 14 and the Assmus-Mattson Theorem. In addition, the quantity $A_3^\perp$ can be computed with the MacWilliams identity and the weight enumerator of $C_{f_1,g_1}^\perp$.

**Theorem 16:** Let $m \geq 2$. The codewords of Hamming weight $2^{2m-2}$ in the code $C_{f_2,g_2}^{(2)}$ hold a $3 - (2^{2m-1}, 2^{2m-2}, 2^{2m-3} - 1)$ design. For even positive integer $\kappa$ with $4 \leq \kappa \leq 2^{2m-1} - 4$, the codewords of Hamming weight $\kappa$ in the code $C_{f_2,g_2}^{(2)}$ hold a $3$-design.

**Proof:** By Remark 4, $C_{f_2,g_2}^{(2)}$ is binary Reed-Muller code $\mathcal{R}(1, 2m - 1)$. It is known the binary Reed-Muller code $\mathcal{R}(1, 2m - 1)$ hold 3-designs [17]. The desired conclusion then follows.

**Theorem 17:** Let $q = 2$. Then the codewords of Hamming weight $2^{2m-2} + \frac{W}{2} - 2^{m-2}$ or $2^{2m-2} + \frac{W}{2} + 2^{m-2}$, where $W = \pm 2^m$, in the code $C_{f_6,g_6}^{(2)}$ hold a 2-design. For any $4 \leq \kappa \leq 2^{2m-1} + \frac{W}{2}$, the codewords of Hamming weight $\kappa$ in the code $C_{f_6,g_6}^{(2)}$ hold a 2-design.

**Proof:** The desired conclusions follow from Theorem 13 and the Assmus-Mattson Theorem.
V. CONCLUDING REMARKS

The main contributions of this paper are the following:

- A family of \([q^3+1, 3, q^3-q]\) two-weight linear code \(C_{f_1,g_1}\) over \(\mathbb{F}_{q^2}\) meeting the Griesmer bound was presented. The dual is a \([q^3+1, q^3-2, 3]\) almost MDS code. When \(q = 2\), \(C_{f_1,g_1}\) is a quaternary Hermitian self-orthogonal code (see Theorem 1 Remark 2).
- A family \([q^{2m-1}+1, 3]\) linear codes with four or five weights over \(\mathbb{F}_{q^m}\) for any positive integer \(m\) was presented. The minimal distance depends on \(q\) and \(m\), the dual is always a \([q^{2m-1}+1, q^{2m-1}-2, 3]\) almost MDS codes (see Theorem 4).
- The \(q\)-ary subfield codes and the punctured code of the subfield codes of above two families of few-weight codes were investigated. The parameters of these codes and their dual are determined. Some of the resultant codes are optimal and some have the best known parameters (see Theorems 2 3 5 6 and Examples 2 3 5 6).
- A family of \([2^{4m-2}, 2m+1, 2^{4m-3}]\) quaternary Hermitian self-dual code was obtained, where \(m \geq 2\) (see Remark 4).
- Seven families of few-weight binary linear codes were presented using almost bent and Boolean bent functions. Most of their dual codes are optimal respect to the sphere packing bound (see Theorems 7 13).
- Several infinite families of 2-designs or 3-designs were constructed with three families of linear codes of this paper (see Theorems 15 16 and 17).

The trace, norm, almost bent and Boolean bent functions were used in this paper. By choosing other functions \(f(x)\) and \(g(x)\) with good properties to construct the generator matrix \(G_{f,g}\), it may be possible to get more few-weight codes with optimal parameters.

ACKNOWLEDGMENTS

The first author would like to thank Prof. Zhengchun Zhou for his useful discussion and many good suggestions for this paper.

REFERENCES

[1] R. Anderson, C. Ding, T. Helleseth, and T. Kløve, “How to build robust shared control systems,” Des., Codes Cryptogr., vol. 15, no. 2, pp. 111-124, Nov. 1998.
[2] E. F. Assmus, Jr. and H. F. Mattson, Jr., “New 5-designs,” J. Combinat. Theory, vol. 6, no. 2, pp. 122-151, Mar. 1969.
[3] S. Ball, Finite Geometry and Combinatorial Applications, Cambridge University Press, Cambridge, 2015.
[4] A. R. Calderbank and W. M. Kantor, “The geometry of two-weight codes,” Bull. London Math. Soc., vol. 18, no. 2, pp. 105-138, 1986.
[5] R. Calderbank and W. M. Kantor, “The geometry of two-weight codes,” Bull. London Math. Soc., vol. 18, no. 2, pp. 97-122, Mar. 1986.
[6] A. Canteaut, P. Charpin and H. Dobbertin, “Weight divisibility of cyclic codes, highly nonlinear functions on \(\mathbb{F}_{2^n}\), and crosscorrelation of maximum-length sequences,” SIAM Disc. Math., vol. 13, no. 1, pp. 105-138, 2000.
[7] C. Carlet, P. Charpin and V. Zinoviev, “Codes, bent functions and permutations suitable for DES-like cryptosystems;” Des. Codes Cryptogr., vol. 15, no. 2, pp. 125-156, 1998.
[8] C. Carlet, C. Ding and J. Yuan, “Linear codes from perfect nonlinear mappings and their secret sharing schemes,” IEEE Trans. Inf. Theory, vol. 51, no. 6, pp. 2089-2102, 2005.
[9] C. Ding and X. Wang, “A coding theory construction of new systematic authentication codes,” Theor. Comput. Sci., vol. 330, no. 1, pp. 81-99, Jan. 2005.
[10] C. Ding and H. Niederreiter, “Cyclotomic linear codes of order 3,” IEEE Trans. Inf. Theory, vol. 53, no. 6, pp. 2274-2277, Jun. 2007.
[11] K. Ding and C. Ding, “Binary linear codes with three weights,” IEEE Commun. Lett., vol. 18, no. 11, pp. 1879-1882, Nov. 2014.
[12] C. Ding, “Linear codes from some 2-designs,” IEEE Trans. Inf. Theory, vol. 60, no. 6, pp. 3265-3275, 2015.
[13] C. Ding, Y. Liu, C. Ma and L. Zeng, “The weight distributions of the duals of cyclic codes with two zeros,” IEEE Trans. Inf. Theory, vol. 57, no. 12, pp. 8000-8006, 2011.
[14] K. Ding and C. Ding, “A class of two-weight and three-weight codes and their applications in secret sharing;” IEEE Trans. Inf. Theory, vol. 61, no. 11, pp. 5835-5842, 2015.
[15] C. Ding, “A construction of binary linear codes from Boolean functions,” Discret. Math., vol. 339, no. 9, pp. 2288-2303, 2016.
[16] C. Ding, C. Li, N. Li and Z. Zhou, “Three-weight cyclic codes and their weight distributions,” Discret. Math., vol. 339, no. 2, pp. 415-427, 2016.
[17] C. Ding, Designs from Linear Codes, World Scientific, Singapore, 2018.
[18] C. Ding and Z. Heng, “The subfield codes of ovoid codes,” IEEE Trans. Inf. Theory, vol. 65, no. 8, pp. 4715-4729, Aug. 2019.
[19] R. Gold, “Maximal recursive sequences with 3-valued recursive cross-correlation functions (Corresp.),” IEEE Trans. Inf. Theory, vol. 14, no. 1, pp. 154-156, Jan. 1968.
[58] D. Zheng, X. Wang, Y. Li and M. Yuan, “Subfield codes of linear codes from perfect nonlinear functions and their duals,” arXiv:2012.06105.