AIMS Mathematics, 11(1): 2797–2815.
DOI: 10.3934/math.2026112
Received: 07 October 2025
Revised: 16 December 2025
Accepted: 15 January 2026
Published: 28 January 2026

https://www.aimspress.com/journal/Math

Research article

Weight distributions of subfield codes from special functions

Shanshan Liu, Yan Liu*and Xiaoyu Yu

School of Mathematics and Statistics, Hefei University, Hefei 230601, China.

* **Correspondence:** Email:liuyan2612@126.com.

Abstract: In this paper, we first determine the weight distributions of some subfield codes $C_f^{(p)}$ and punctured codes $C_f^{*(p)}$ constructed from special functions, both of which are few-weight codes. Furthermore, we derive the parameters of their dual codes. Notably, some of these codes and their duals turn out to be optimal or almost distance-optimal. As an application, two classes of 2-designs are constructed from some codes.

Keywords: subfield code; weight distribution; few weight; punctured code; design
Mathematics Subject Classification: 94B05, 11T55, 06E30

1. Introduction

Throughout this paper, let q be a prime power and $\mathbb{F}_{q^m}$ denote the finite field with q^m elements where m is a positive integer. An $[n, k, d]$ linear code C over $\mathbb{F}_{q^m}$ is a k-dimensional subspace of $\mathbb{F}_{q^m}^n$ with minimum Hamming distance d. Defined as $\{\mathbf{y} \in \mathbb{F}_{q^m}^n \mid \mathbf{x} \cdot \mathbf{y} = 0 \text{ for all } \mathbf{x} \in C\}$, the dual code $C^\perp$ of C is an $[n, n-k, d^\perp]$ linear code with minimum Hamming distance $d^\perp$. The dual code $C^\perp$ of an $[n, k, d]$ linear code C over $\mathbb{F}_{q^m}$ is said to be almost distance-optimal if there is no $[n, n-k', d']$ linear code over $\mathbb{F}_{q^m}$ with $n - k' \geq (n-k) + 1$ (i.e., $k' \leq k - 1$) (resp. $d' \geq d^\perp + 1$) that makes it substantially deviate from distance-optimal behavior, or if it either closely approaches meeting a bound for linear codes (in terms of distance optimality) or exhibits performance that is nearly distance-optimal. The punctured code C^* of C is obtained by removing the ith coordinate from each codeword of C. Its generator matrix is derived from C's generator matrix G by deleting column i and discarding any resulting zero or duplicate rows.

For a linear code C, the weight distribution is the sequence $(A_0, A_1, \ldots, A_n)$, where A_i is the number of codewords of Hamming weight i (with $A_0 = 1$). Closely related to the weight distribution is the weight enumerator (or weight counter) of C, defined as the polynomial $W_C(z) = \sum_{i=0}^n A_i z^i$, which compactly encodes the number of codewords of each weight. The code is called a t-weight code if there are exactly t nonzero A_i for $1 \leq i \leq n$. Linear codes with few weights are of particular interest due

to their applications in association schemes, strongly regular graphs [1], combinatorial t-designs [2], and cryptography [3]. Recently, significant progress has been made in constructing such codes and determining their weight distributions using exponential sums and trace representations using defining sets [4], with studies covering various families, including optimal few-weight codes.

In the context of constructing optimal linear codes, the subfield code was first introduced in [5, 6]. Most subfield codes have few weights and good parameters. The next lemma presents the trace representation of the subfield code in terms of the generator matrix of the linear code over $\mathbb{F}_{q^m}$.

Lemma 1.1 ([7, Lemma 1]). *Let $G = (g_{ij}) \in \mathbb{F}_{q^m}^{k\times n}$ be a generator matrix of the linear code C over $\mathbb{F}_{q^m}$. Then the trace representation of the subfield code $C_f^{(q)}$ over $\mathbb{F}_q$ is given by*

$$C_f^{(q)} = \left\{ \left(\mathrm{Tr}_{q^m/q}\left(\sum_{i=1}^{k} a_i g_{i1}\right), \cdots, \mathrm{Tr}_{q^m/q}\left(\sum_{i=1}^{k} a_i g_{in}\right)\right) \mid a_1, \cdots, a_k \in \mathbb{F}_{q^m} \right\},$$

where $\mathrm{Tr}_{q^m/q}$ is the trace function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$.

Building on these foundations, Ding and Heng [8] initiated the study of subfield codes' properties and determined the weight distributions of those derived from elliptic quadric codes and Tits ovoid codes. In [9], Xu et al. first presented a construction framework of three-dimensional linear codes C_f^* with generator matrix

$$G_f^* = \begin{pmatrix} 1 \\ x \\ y \end{pmatrix}_{(x,y)\in S}, \tag{1}$$

where $S = \{(x, y) \in \mathbb{F}_{q^m}^2 \mid f(x, y) = 0\}$, and discussed their subfield codes. Furthermore, consider a $3 \times (\#S + 1)$ matrix

$$G_f = \begin{pmatrix} 0 & \\ 1 & G_f^* \\ 0 & \end{pmatrix}, \tag{2}$$

where $\#S$ denotes the cardinality of S. Then, a $[\#S+1, 3, d]$ linear code can be obtained from the matrix (2), denoted by C_f. Obviously, the punctured code C_f^* is obtained by deleting the first coordinate of C_f, resulting in a $[\#S, 3]$ code with generator matrix G_f^*. Subsequent works further extended this research to subfield codes from various linear codes, optimal cyclic codes [10], and other few-weight linear codes [11, 12].

Inspired by the above work, we investigate the subfield codes $C_f^{(q)}$ and their punctured versions $C_f^{*(q)}$ for three carefully chosen functions:

- $f(x, y) = \mathrm{Tr}_{2^m/2}(x \cdot y) + \mathrm{N}_{2^m/2}(x + y)$;
- $f(x, y) = \mathrm{Tr}_{2^m/2}(x \cdot y)$;
- $f(x, y) = \mathrm{Tr}_{p^3/p}(x^2 + y^2)$, where $p \equiv 3 \pmod 4$.

This paper is organized as follows. Section 2 introduces basic concepts and lemmas related to finite field functions and linear codes. Section 3 studies two types of subfield and punctured codes (with their duals) derived from two specific functions, including their key properties and parameter

advantages illustrated by examples. Section 4 investigates a further subfield code and its punctured code based on another function, confirming excellent parameters through examples. Section 5 presents two classes of 2-designs are derived from several codes. Section 6 concludes the paper with comments.

2. Preliminaries

The trace function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$, denoted as $\mathrm{Tr}_{q^m/q}$, is defined by

$$\mathrm{Tr}_{q^m/q}(x) = \sum_{i=0}^{m-1} x^{q^i} \quad \text{for all } x \in \mathbb{F}_{q^m}.$$

The norm function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ is denoted as $\mathrm{N}_{q^m/q}$. It can be expressed as

$$\mathrm{N}_{q^m/q}(x) = x \cdot x^q \cdot x^{q^2} \cdot \cdots \cdot x^{q^{m-1}} = x^{\frac{q^m-1}{q-1}} \quad \text{for all } x \in \mathbb{F}_{q^m}.$$

Let $q = p^e$ with p a prime and e a positive integer. An *additive character* of $\mathbb{F}_q$ is a nonzero function $\chi : \mathbb{F}_q \to \mathbb{C}^*$, where $\mathbb{C}^*$ is the set of nonzero complex numbers such that

$$\chi(x+y) = \chi(x)\chi(y) \quad \text{for all } x, y \in \mathbb{F}_q.$$

For any $a \in \mathbb{F}_q$, the function

$$\chi_a(x) = \zeta_p^{\mathrm{Tr}_{q/p}(ax)} \quad \text{for } x \in \mathbb{F}_q$$

defines an additive character of $\mathbb{F}_q$, where $\zeta_p = e^{2\pi i/p}$ is a primitive pth root of unity.

If $a = 0$, then $\chi_0(x) = 1$ for all $x \in \mathbb{F}_q$, which is called the *trivial additive character* of $\mathbb{F}_q$; if $a = 1$, χ_1 is called the *canonical additive character* of $\mathbb{F}_q$.

Clearly, $\chi_a(x) = \chi_1(ax)$ for all $x \in \mathbb{F}_q$. Additive characters satisfy the following orthogonality relation:

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

Note that if χ and χ' denote the canonical additive characters of $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$, respectively, then $\chi' = \chi \circ \mathrm{Tr}_{q^m/q}$.

A *multiplicative character* of $\mathbb{F}_q$ is a nonzero homomorphism $\psi : \mathbb{F}_q^* \to \mathbb{C}^*$ such that

$$\psi(xy) = \psi(x)\psi(y) \quad \text{for all } x, y \in \mathbb{F}_q^*.$$

Let g be a fixed primitive element of $\mathbb{F}_q$ where $\mathbb{F}_q^* = \langle g \rangle$, and let $\zeta_{q-1} = e^{2\pi i/(q-1)}$ be a primitive $(q-1)$th root of unity. All multiplicative characters of $\mathbb{F}_q$ can be expressed as

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

where ψ_0 is called the *trivial multiplicative character*; for odd q, $\psi_{(q-1)/2}$ is the *quadratic character* of $\mathbb{F}_q$, denoted by η. Similarly, the *quadratic character* of $\mathbb{F}_{q^m}$ is denoted by η'.

Multiplicative characters satisfy the following orthogonality relation:

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

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

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

In general, the explicit determination of the Gaussian sum is a difficult problem. In the case of $\psi=\eta$, Gaussian sums are explicitly determined in [13].

Lemma 2.1 ([13]). *Let $q=p^e$ with p an odd prime, and let χ_1 be the canonical additive character of $\mathbb{F}_q$. Then,*

$$G(\eta,\chi_1)=\begin{cases}(-1)^{e-1}\sqrt{q} & \text{if } p\equiv 1 \pmod 4,\\ (-1)^{e-1}\left(\sqrt{-1}\right)^{e-1}\sqrt{q} & \text{if } p\equiv 3 \pmod 4.\end{cases}$$

Let χ be the nontrivial additive character of $\mathbb{F}_q$ and $f\in\mathbb{F}_q[x]$ a positive-degree polynomial. The character sums

$$\sum_{x\in\mathbb{F}_q}\chi(f(x))$$

are called *Weil sums*. For quadratic polynomials over $\mathbb{F}_q$ with odd q, Weil sums are characterized as follows.

Lemma 2.2 ([13]). *Let χ_b be a nontrivial additive character of $\mathbb{F}_q$ with odd q, and let $f(x)=a_2x^2+a_1x+a_0\in\mathbb{F}_q[x]$ with $a_2\neq 0$. Then,*

$$\sum_{c\in\mathbb{F}_q}\chi_b(f(c))=\chi_b\left(a_0-\frac{a_1^2}{4a_2}\right)\eta(a_2)G(\eta,\chi_b).$$

Let $(1,A_1^\perp,\cdots,A_n^\perp)$ denote the weight distribution of its dual code $C^\perp$. Now, recall the Pless power moments, which describe the relationship between the weight distributions of C and $C^\perp$. The first four Pless power moments are given by:

$$\sum_{i=0}^{n}A_i=p^k;$$

$$\sum_{i=0}^{n}iA_i=p^{k-1}\left(pn-n-A_1^\perp\right);$$

$$\sum_{i=0}^{n}i^2A_i=p^{k-2}\left[(p-1)n(pn-n+1)-(2pn-p-2n+2)A_1^\perp+2A_2^\perp\right];$$

$$\sum_{i=0}^{n} i^3 A_i = p^{k-3}\Bigg((p-1)n\left(p^2n^2-2pn^2+3pn-p+n^2-3n+2\right) - \left(3p^2n^2-3p^2n-6pn^2+12pn+p^2-6p+3n^2-9n+6\right)A_1^{\perp} + 6(pn-p-n+2)A_2^{\perp} - 6A_3^{\perp}\Bigg).$$

In this paper, we consider the linear codes C_f over $\mathbb{F}_{q^m}$ with generator matrix (2). According to Lemma 1.1, the subfield code $C_f^{(q)}$ has the following trace representation:

$$C_f^{(q)} = \left\{\mathbf{c}_{a,b,c} = \left(\mathrm{Tr}_{q^m/q}(b),\ \left(a+\mathrm{Tr}_{q^m/q}(bx+cy)\right)_{(x,y)\in S}\right) \mid a\in\mathbb{F}_q,\ b,c\in\mathbb{F}_{q^m}\right\}. \tag{3}$$

In the following sections, we focus on calculating the parameters and weight distributions of the subfield codes and punctured codes as well as their dual codes.

3. Weight distributions of $C_f^{(2)}$ and $C_f^{*(2)}$ with their duals

In this section, take $q=2$. It is easy to observe that the length of the subfield code $C_f^{(2)}$ (resp. the punctured code $C_f^{*(2)}$) is $\#S+1$ (resp. $\#S$). Now, we aim to discuss the weight distributions of $C_f^{(2)}$ and $C_f^{*(2)}$ and to analyze their dual codes. Let $\xi_1 = \mathbb{F}_2\times\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ for short. Set

$$N_{a,b,c} = \#\left\{(x,y)\in S \mid a+\mathrm{Tr}_{2^m/2}(bx+cy)=0\right\} \quad \text{for } (a,b,c)\in\xi_1. \tag{4}$$

For any $(a,b,c)\in\xi_1$, the weight of the codeword $\mathbf{c}_{a,b,c}$ in $C_f^{(2)}$ is equal to

$$\mathrm{wt}(\mathbf{c}_{a,b,c}) = \#S - N_{a,b,c} + \delta(b), \tag{5}$$

where $\delta(x)$ is a function from $\mathbb{F}_{2^m}$ to $\{0,1\}$ defined as:

$$\delta(x) = \begin{cases} 0 & \text{if } \mathrm{Tr}_{2^m/2}(x)=0,\\ 1 & \text{if } \mathrm{Tr}_{2^m/2}(x)\neq 0. \end{cases} \tag{6}$$

3.1. Weight distributions of linear codes from $f(x,y) = \mathrm{Tr}_{2^m/2}(x\cdot y) + \mathrm{N}_{2^m/2}(x+y)$

In this subsection, the lengths and weight distributions of $C_f^{(2)}$ and $C_f^{*(2)}$ are explicitly given for $f(x,y) = \mathrm{Tr}_{2^m/2}(x\cdot y) + \mathrm{N}_{2^m/2}(x+y)$. Below, we prove a few more auxiliary results which will be used to calculate the weight distribution of the codes.

Lemma 3.1. *Let $(a,b,c)\in\xi_1$, and define $\omega_1 = a+\mathrm{Tr}_{2^m/2}(bc)+\mathrm{N}_{2^m/2}(b+c+1)$.*

(i) Let $T_1 = \left\{(a,b,c)\in\mathbb{F}_2\times\mathbb{F}_{2^m}^*\times\mathbb{F}_{2^m} \,\middle|\, \omega_1=0,\ \mathrm{Tr}_{2^m/2}(b)=0\right\}$; then $\#T_1 = 2^{2m-1}-2^m$.

(ii) Let $T_2 = \left\{(a,b,c)\in\mathbb{F}_2\times\mathbb{F}_{2^m}^*\times\mathbb{F}_{2^m} \,\middle|\, \omega_1=0,\ \mathrm{Tr}_{2^m/2}(b)\neq 0\right\}$; then $\#T_2 = 2^{2m-1}$.

(iii) Let $T_3 = \left\{(a,b,c)\in\mathbb{F}_2\times\mathbb{F}_{2^m}^*\times\mathbb{F}_{2^m} \,\middle|\, \omega_1=1,\ \mathrm{Tr}_{2^m/2}(b)\neq 0\right\}$; then $\#T_3 = 2^{2m-1}$.

(iv) Let $T_4 = \left\{(a,b,c) \in \mathbb{F}_2 \times \mathbb{F}_{2^m}^* \times \mathbb{F}_{2^m} \;\middle|\; \omega_1 = 1,\ \mathrm{Tr}_{2^m/2}(b) = 0\right\}$*; then* $\#T_4 = 2^{2m-1} - 2^m$.

(v) Let $T_5 = \left\{(a,0,c) \in \mathbb{F}_2 \times \{0\} \times \mathbb{F}_{2^m}^* \;\middle|\; \omega_1 = 0\right\}$*; then* $\#T_5 = 2^m - 1$.

(vi) Let $T_6 = \left\{(a,0,c) \in \mathbb{F}_2 \times \{0\} \times \mathbb{F}_{2^m}^* \;\middle|\; \omega_1 = 1\right\}$*; then* $\#T_6 = 2^m - 1$.

Proof. We will only prove (i) and (ii), as the others can be derived similarly.

(i) From the orthogonal property of the canonical additive character, we have

$$\begin{aligned}\#T_1 &= 2^{m-1} \sum_{\mu \in \mathbb{F}_2} \sum_{b \in \mathbb{F}_{2^m}^*} \chi\left(\mu \mathrm{Tr}_{2^m/2}(b)\right) \\ &= 2^{m-1} \sum_{\mu \in \mathbb{F}_2} \sum_{b \in \mathbb{F}_{2^m}^*} \chi'(\mu b) \\ &= 2^{2m-1} - 2^m.\end{aligned}$$

(ii) The set of triples $(a,b,c) \in \mathbb{F}_2 \times \mathbb{F}_{2^m}^* \times \mathbb{F}_{2^m}$ where $\omega_1 = 0$ has $2^{2m} - 2^m$ elements. It has two distinct subsets: T_1 (with $\mathrm{Tr}_{2^m/2}(b) = 0$) and T_2 (with $\mathrm{Tr}_{2^m/2}(b) \neq 0$). Thus, $\#T_2 = (2^{2m} - 2^m) - \#T_1 = 2^{2m-1}$. □

Define a character sum

$$\Gamma_1^{a,b,c} = \chi(a) \sum_{(x,y) \in \mathbb{F}_{2^m}^2} \chi\left(\mathrm{Tr}_{2^m/2}(x \cdot y) + \mathrm{N}_{2^m/2}(x+y)\right) \chi'(bx + cy), \tag{7}$$

where $(a,b,c) \in \xi_1$. From the orthogonal property of the canonical additive character, we obtain

$$\begin{aligned}\Gamma_1^{a,b,c} &= \chi(a) \sum_{(x,y) \in \mathbb{F}_{2^m}^2} \chi\left(\mathrm{N}_{2^m/2}(x+y)\right) \chi'(x \cdot y + bx + cy) \\ &= \chi(a) \sum_{(s,x) \in \mathbb{F}_{2^m}^2} \chi\left(\mathrm{N}_{2^m/2}(s)\right) \chi'((1+s+b+c)x) \chi'(cs) \\ &= 2^m \chi(a) \chi'(bc) \chi\left(\mathrm{N}_{2^m/2}(b+c+1)\right) \\ &= 2^m (-1)^{\omega_1},\end{aligned}$$

where the second equality follows from $s = x + y$, and ω_1 is as defined in Lemma 3.1.

Theorem 3.2. *The subfield code* $C_f^{(2)}$ *defined in Eq. (3) is a binary linear code with parameters* $[2^{2m-1} - 2^{m-1} + 1, 2m+1, 2^{2m-2} - 2^{m-1}]$*, and its weight distribution is given in Table 1. Its dual code is a binary linear code with parameters* $[2^{2m-1} - 2^{m-1} + 1, 2^{2m-1} - 2^{m-1} - 2m, 3]$.

Table 1. Weight distribution of $C_f^{(2)}$.

Weight	Multiplicity
0	1
2^{2m-2}	$2^{2m-1}-1$
$2^{2m-2}+1$	2^{2m-1}
$2^{2m-2}+2^{m-1}$	$2^{2m-1}-1$
$2^{2m-2}+2^{m-1}+1$	2^{2m-1}
$2^{2m-1}+2^{m-1}$	1

Proof. We begin by determining the length of the code. To this end, we compute $\#S$. Using the orthogonal property of the canonical additive character and $\chi' = \chi \circ \mathrm{Tr}_{2^m/2}$, we have

$$\begin{aligned}
\#S &= \frac{1}{2}\sum_{\kappa\in\mathbb{F}_2}\sum_{(x,y)\in\mathbb{F}_{2^m}^2}\chi\left(\kappa\left(\mathrm{Tr}_{2^m/2}(x\cdot y)+\mathrm{N}_{2^m/2}(x+y)\right)\right)\\
&= 2^{2m-1}+\frac{1}{2}\sum_{(x,y)\in\mathbb{F}_{2^m}^2}\chi\left(\mathrm{Tr}_{2^m/2}(x\cdot y)+\mathrm{N}_{2^m/2}(x+y)\right)\\
&= 2^{2m-1}+\frac{1}{2}\sum_{(s,x)\in\mathbb{F}_{2^m}^2}\chi\left(\mathrm{Tr}_{2^m/2}(x(s-x))+\mathrm{N}_{2^m/2}(s)\right)\\
&= 2^{2m-1}-2^{m-1},
\end{aligned}$$

where $s = x + y$. Thus, the length of $C_f^{(2)}$ is $2^{2m-1} - 2^{m-1} + 1$.

In view of Eq (5), we discuss $N_{a,b,c}$ for $(a, b, c) \in \xi_1$. Clearly, $N_{0,0,0} = \#S$, and $N_{a,0,0} = 0$ for $a \in \mathbb{F}_2$. When b and c are not both zero, using additive character properties,

$$\begin{aligned}
2N_{a,b,c} &= \sum_{\kappa\in\mathbb{F}_2}\sum_{(x,y)\in S}\chi\left(\kappa\big(a+\mathrm{Tr}_{2^m/2}(bx+cy)\big)\right)\\
&= \#S+\sum_{(x,y)\in S}\chi\left(a+\mathrm{Tr}_{2^m/2}(bx+cy)\right)\\
&= \#S+\chi(a)\sum_{(x,y)\in S}\chi'(bx+cy)\\
&= \#S+\chi(a)\sum_{(x,y)\in\mathbb{F}_{2^m}^2}\left(\frac{1}{2}\sum_{\mu\in\mathbb{F}_2}\chi\left(\mu\big(\mathrm{Tr}_{2^m/2}(x\cdot y)+\mathrm{N}_{2^m/2}(x+y)\big)\right)\right)\chi'(bx+cy)\\
&= \#S+\frac{1}{2}\chi(a)\sum_{(x,y)\in\mathbb{F}_{2^m}^2}\chi'(bx+cy)+\frac{1}{2}\Gamma_1^{a,b,c}\\
&= \#S+\frac{1}{2}\Gamma_1^{a,b,c}.
\end{aligned}$$

From the above discussion, we derive the weight of the codeword $\mathbf{c}_{a,b,c}$ in $C_f^{(2)}$ as follows:

$$\mathrm{wt}(\mathbf{c}_{a,b,c}) = \begin{cases} 0 & \text{if } a=b=c=0, \\ 2^{2m-1}-2^{m-1} & \text{if } a\neq 0,\ b=c=0, \\ \delta(b)+2^{2m-2}-2^{m-2}-\frac{1}{4}\Gamma_1^{a,b,c} & \text{if } b,c \text{ not all } 0, \end{cases}$$

$$= \begin{cases} 0 & \text{if } a=b=c=0, \\ 2^{2m-1}-2^{m-1} & \text{if } a=1,\ b=c=0, \\ 2^{2m-2} & \text{if } (a,b,c)\in T_6\cup T_4, \\ 2^{2m-2}+1 & \text{if } (a,b,c)\in T_3, \\ 2^{2m-2}-2^{m-1} & \text{if } (a,b,c)\in T_5\cup T_1, \\ 2^{2m-2}-2^{m-1}+1 & \text{if } (a,b,c)\in T_2, \end{cases}$$

where T_i $(i=1,\ldots,6)$ are defined in Lemma 3.1. This shows that $C_f^{(2)}$ is a binary linear code with parameters $[2^{2m-1}-2^{m-1}+1, 2m+1, 2^{2m-2}-2^{m-1}]$. Applying Lemma 3.1 allows us to immediately determine the frequency of each weight.

At last, it is easy to know that the dual code of $C_f^{(2)}$ has length $2^{2m-1}-2^{m-1}+1$ and dimension $2^{2m-1}-2^{m-1}-2m$. By using the first four power moments, we find that $A_1^{\perp}=A_2^{\perp}=0$, and $A_3^{\perp}>0$. This completes the proof. □

Remark 3.3. Xu et al. studied, in [9], Theorems 7, 9, 12, 14, subfield codes, and the weight distributions of their dual codes for $q=2$ using various functions. We extend the function to $f(x,y)=\mathrm{Tr}_{2^m/2}(x\cdot y)+\mathrm{N}_{2^m/2}(x+y)$ to study the same for $q=2$.

Example 3.4. The examples provided below demonstrate that the subfield code $C_f^{(2)}$ possesses excellent parameters. For comparison, the best-known parameters are retrieved from the code tables available at [14].

(1) For $m=2$, $C_f^{(2)}$ is a clearly best-known $[7,5,2]$ binary linear code with weight enumerator $1+7z^2+8z^3+7z^4+8z^5+z^6$. Its dual $C_f^{(2)\perp}$ is an almost distance-optimal code $[7,2,3]$.

(2) For $m=3$, $C_f^{(2)}$ is a best-known $[29,7,12]$ binary linear code with weight enumerator $1+31z^{12}+32z^{13}+31z^{16}+32z^{17}+z^{28}$. Its dual is an almost distance-optimal code $[29,22,3]$.

(3) For $m=4$, $C_f^{(2)}$ is a best-known $[121,9,56]$ binary linear code with weight enumerator $1+127z^{56}+128z^{57}+127z^{64}+128z^{65}+z^{120}$. Its dual is an almost distance-optimal dual code $[121,112,3]$.

Using the relationship between $C_f^{(2)}$ and its punctured code $C_f^{*(2)}$, along with Theorem 3.2, we obtain the following result. The minimum distance of the dual code can be computed with the first four power moments, and the calculation is omitted here.

Theorem 3.5. *The punctured code $C_f^{*(2)}$ is a three-weight $[2^{2m-1}-2^{m-1}, 2m+1, 2^{2m-2}-2^{m-1}]$ binary linear code, and its weight enumerator is*

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

Its dual is a $[2^{2m-1}-2^{m-1}, 2^{2m-1}-2^{m-1}-2m-1, 4]$ *binary linear code.*

Remark 3.6. Xu et al. studied, in [9, Theorems 8, 10, 11, 13, 15], subfield codes and the weight distributions of their dual codes for $q = 2$ using various functions. We extend the function to $f(x, y) = \mathrm{Tr}_{2^m/2}(x \cdot y) + \mathrm{N}_{2^m/2}(x + y)$ to study the same for $q = 2$.

Example 3.7. The examples provided below demonstrate that the punctured code $C_f^{*(2)}$ possesses excellent parameters. For comparison, the best-known parameters are retrieved from the code tables available at [14].

(1) For $m = 3$, $C_f^{*(2)}$ is a binary linear code with parameters and weight enumerator $1 + 63z^{12} + 63z^{16} + z^{28}$[28, 7, 12]. Its dual code is a binary linear code, and both codes attain the best-known parameters[28, 21, 4].

(2) Let $m = 4$. $C_f^{*(2)}$ is a binary linear code with parameters and weight enumerator $1 + 255z^{56} + 255z^{64} + z^{120}$[120, 9, 56]. Its dual is a binary linear code, and both have the best-known parameters[120, 111, 4].

3.2. Weight distributions of linear codes from $f(x, y) = \mathrm{Tr}_{2^m/2}(x \cdot y)$

In this subsection, the lengths and weight distributions of $C_f^{(2)}$ and $C_f^{*(2)}$ are explicitly given for $f(x, y) = \mathrm{Tr}_{2^m/2}(x \cdot y)$. Below, we prove a few more auxiliary results which will be used to calculate the weight distributions of the codes.

Similar to the proof of Lemma 3.1, we omit the proof here.

Lemma 3.8. *Let* $(a, b, c) \in \xi_1$*, and define* $\omega_2 = a + \mathrm{Tr}_{2^m/2}(bc)$.

(i) Let $Q_1 = \left\{(a, b, c) \in \mathbb{F}_2 \times \mathbb{F}_{2^m}^* \times \mathbb{F}_{2^m} \;\middle|\; \omega_2 = 0,\ \mathrm{Tr}_{2^m/2}(b) = 0\right\}$*; then* $\#Q_1 = 2^{2m-1} - 2^m$.

(ii) Let $Q_2 = \left\{(a, b, c) \in \mathbb{F}_2 \times \mathbb{F}_{2^m}^* \times \mathbb{F}_{2^m} \;\middle|\; \omega_2 = 0,\ \mathrm{Tr}_{2^m/2}(b) \neq 0\right\}$*; then* $\#Q_2 = 2^{2m-1}$.

(iii) Let $Q_3 = \left\{(a, b, c) \in \mathbb{F}_2 \times \mathbb{F}_{2^m}^* \times \mathbb{F}_{2^m} \;\middle|\; \omega_2 = 1,\ \mathrm{Tr}_{2^m/2}(b) \neq 0\right\}$*; then* $\#Q_3 = 2^{2m-1}$.

(iv) Let $Q_4 = \left\{(a, b, c) \in \mathbb{F}_2 \times \mathbb{F}_{2^m}^* \times \mathbb{F}_{2^m} \;\middle|\; \omega_2 = 1,\ \mathrm{Tr}_{2^m/2}(b) = 0\right\}$*; then* $\#Q_4 = 2^{2m-1} - 2^m$.

(v) Let $Q_5 = \left\{(a, b, c) \in \mathbb{F}_2 \times \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}^* \mid a = 0,\ b = 0\right\}$*; then* $\#Q_5 = 2^m - 1$.

(vi) Let $Q_6 = \left\{(a, b, c) \in \mathbb{F}_2 \times \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}^* \mid a = 1,\ b = 0\right\}$*; then* $\#Q_6 = 2^m - 1$.

Define a character sum

$$\Gamma_2^{a,b,c} = \chi(a) \sum_{(x,y)\in\mathbb{F}_{2^m}^2} \chi\left(\mathrm{Tr}_{2^m/2}(x \cdot y)\right) \chi'(bx + cy), \tag{8}$$

where $(a, b, c) \in \xi_1$. Using the orthogonal property of the canonical additive character and $\chi' = \chi \circ \mathrm{Tr}_{2^m/2}$, we have

$$\begin{aligned}\Gamma_2^{a,b,c} &= \chi(a) \sum_{(x,y)\in\mathbb{F}_{2^m}^2} \chi\left(\mathrm{Tr}_{2^m/2}(x \cdot y)\right) \chi'(bx + cy) \\ &= \chi(a) \sum_{(x,y)\in\mathbb{F}_{2^m}^2} \chi'(x \cdot y + bx + cy)\end{aligned}$$

$$
\begin{aligned}
&= \chi(a) \sum_{y\in\mathbb{F}_{2^m}} \chi'(cy) \sum_{x\in\mathbb{F}_{2^m}} \chi'((y+b)x) \\
&= 2^m \chi(a)\chi'(bc) \\
&= 2^m (-1)^{\omega_2},
\end{aligned}
$$

where ω_2 is as defined in Lemma 3.8.

Theorem 3.9. *The subfield code $C_f^{(2)}$ defined in Eq (3) is a binary linear code with parameters $[2^{2m-1}+2^{m-1}+1, 2m+1, 2^{2m-2}]$, and its weight distribution is given in Table 2. Its dual code is a binary linear code with parameters $[2^{2m-1}+2^{m-1}+1, 2^{2m-1}+2^{m-1}-2m, 3]$.*

Table 2. Weight distribution of $C_f^{(2)}$.

Weight	Multiplicity
0	1
2^{2m-2}	$2^{2m-1}-1$
$2^{2m-2}+1$	2^{2m-1}
$2^{2m-2}+2^{m-1}$	$2^{2m-1}-1$
$2^{2m-2}+2^{m-1}+1$	2^{2m-1}
$2^{2m-1}+2^{m-1}$	1

Proof. We begin by determining the length of the code. To this end, we compute $\#S$. Using the orthogonal property of the canonical additive character and $\chi' = \chi \circ \mathrm{Tr}_{2^m/2}$, we have

$$
\begin{aligned}
\#S &= \frac{1}{2} \sum_{\kappa\in\mathbb{F}_2} \sum_{(x,y)\in\mathbb{F}_{2^m}^2} \chi\left(\kappa \cdot \mathrm{Tr}_{2^m/2}(x\cdot y)\right) \\
&= 2^{2m-1} + \frac{1}{2} \sum_{(x,y)\in\mathbb{F}_{2^m}^2} \chi\left(\mathrm{Tr}_{2^m/2}(x\cdot y)\right) \\
&= 2^{2m-1} + \frac{1}{2} \sum_{(x,y)\in\mathbb{F}_{2^m}^2} \chi'(x\cdot y) \\
&= 2^{2m-1} + \frac{1}{2} \sum_{y\in\mathbb{F}_{2^m}} \chi'(0) \\
&= 2^{2m-1} + 2^{m-1}.
\end{aligned}
$$

Thus, the length of $C_f^{(2)}$ is $2^{2m-1}+2^{m-1}+1$.

Using calculations similar to those in Eqs (4) and (5) with detailed derivations omitted, the weight

of the codeword $\mathbf{c}_{a,b,c}$ in $C_f^{(2)}$ is:

$$\mathrm{wt}(\mathbf{c}_{a,b,c}) = \begin{cases} 0 & \text{if } a=b=c=0, \\ 2^{2m-1}+2^{m-1} & \text{if } a\neq 0,\ b=c=0, \\ \delta(b)+2^{2m-2}+2^{m-2}-\frac{1}{4}\Gamma_2^{a,b,c} & \text{if } b,c \text{ not all } 0, \end{cases}$$

$$= \begin{cases} 0 & \text{if } a=b=c=0, \\ 2^{2m-1}+2^{m-1} & \text{if } a=1,\ b=c=0, \\ 2^{2m-2} & \text{if } (a,b,c)\in Q_5\cup Q_1, \\ 2^{2m-2}+1 & \text{if } (a,b,c)\in Q_2, \\ 2^{2m-2}+2^{m-1} & \text{if } (a,b,c)\in Q_6\cup Q_4, \\ 2^{2m-2}+2^{m-1}+1 & \text{if } (a,b,c)\in Q_3. \end{cases}$$

where Q_i $(i=1,\ldots,6)$ are defined in Lemma 3.8. This means that $C_f^{(2)}$ is a binary linear code with parameters $[2^{2m-1}+2^{m-1}+1, 2m+1, 2^{2m-2}]$. Applying Lemma 3.8 immediately gives the frequency of each weight.

Finally, it is easy to see that the dual code of $C_f^{(2)}$ has length $2^{2m-1}+2^{m-1}+1$ and dimension $2^{2m-1}+2^{m-1}-2m$. Using the first four power moments, we find that $A_1^\perp = A_2^\perp = 0$, and $A_3^\perp > 0$. This completes the proof. □

Remark 3.10. Xu et al. studied, in [9], Theorems 7, 9, 12, 14, subfield codes and the weight distributions of their dual codes for $q=2$ using various functions. We extend the function to $f(x,y)=\mathrm{Tr}_{2^m/2}(x\cdot y)$ to study the same for $q=2$.

Example 3.11. The examples provided below demonstrate that the subfield code $C_f^{(2)}$ possesses excellent parameters. For comparison, the best-known parameters are retrieved from the code tables available at [14].

(1) For $m=2$, $C_f^{(2)}$ is a clearly best-known $[11,5,4]$ binary linear code with weight enumerator $1+7z^4+8z^5+7z^6+8z^7+z^{10}$. Its dual is an almost distance-optimal code $[11,6,3]$.
(2) For $m=3$, $C_f^{(2)}$ is a clearly best-known $[37,7,16]$ binary linear code with weight enumerator $1+31z^{16}+32z^{17}+31z^{20}+32z^{21}+z^{36}$. Its dual is an almost distance-optimal code $[37,30,3]$.
(3) For $m=4$, $C_f^{(2)}$ is a best-known $[137,9,64]$ binary linear code with weight enumerator $1+127z^{64}+128z^{65}+127z^{72}+128z^{73}+z^{136}$. Its dual is an almost distance-optimal code $[137,128,3]$.

Using the relationship between $C_f^{(2)}$ and its punctured code $C_f^{*(2)}$, together with Theorem 3.9 and the first four power moments, we immediately derive the following result. The minimum distance of the dual code can be computed with the first four power moments, and the calculation is omitted here.

Theorem 3.12. *The punctured code $C_f^{*(2)}$ is a three-weight $[2^{2m-1}+2^{m-1}, 2m+1, 2^{2m-2}]$ binary linear code, and its weight enumerator is*

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

Its dual is a $[2^{2m-1}+2^{m-1}, 2^{2m-1}+2^{m-1}-2m-1, 4]$ binary linear code.

Remark 3.13. Xu et al. studied, in [9, Theorems 8, 10, 11, 13, 15], subfield codes and the weight distributions of their dual codes for $q = 2$ using various functions. We extend the function to $f(x, y) = \mathrm{Tr}_{2^m/2}(x \cdot y)$ to study the same for $q = 2$.

Example 3.14. The examples provided below demonstrate that the punctured code $C_f^{*(2)}$ possesses excellent parameters. For comparison, the best-known parameters are retrieved from the Code Tables available at [14].

(1) For $m = 2$, $C_f^{*(2)}$ is a binary linear code with parameters and weight enumerator $1 + 15z^4 + 15z^6 + z^{10}[10, 5, 4]$. Its dual is a binary linear code, and both codes attain the best-known parameters $[10, 5, 4]$.
(2) For $m = 3$, $C_f^{*(2)}$ is a binary linear code with parameters and weight enumerator $1+63z^{16}+63z^{20}+z^{36}[36, 7, 16]$. Its dual is a binary linear code, and both codes attain the best-known parameters $[36, 29, 4]$.
(3) For $m = 4$, $C_f^{*(2)}$ is a binary linear code with parameters and weight enumerator $1 + 255z^{64} + 255z^{72} + z^{136}[136, 9, 64]$. Its dual is a binary linear code, and both codes attain the best-known parameters $[136, 127, 4]$.

4. Weight distributions of $C_f^{(p)}$ and $C_f^{*(p)}$ with their duals

In this section, we set $q = p$ (where $p \equiv 3 \pmod 4$) and $m = 3$. It is easy to observe that the length of the subfield code $C_f^{(p)}$ (resp. the punctured code $C_f^{*(p)}$) is $\#S + 1$ (resp. $\#S$). The function $f(x, y)$ is defined as $f(x, y) = \mathrm{Tr}_{p^3/p}(x^2 + y^2)$. Here, we aim to discuss the weight distributions of $C_f^{(p)}$ and $C_f^{*(p)}$, and to analyze their dual codes. Let $\xi_2 = \mathbb{F}_p \times \mathbb{F}_{p^3} \times \mathbb{F}_{p^3}$ for short. Set

$$N'_{a,b,c} = \#\left\{(x, y) \in S \mid a + \mathrm{Tr}_{p^3/p}(bx + cy) = 0\right\} \quad \text{for any } (a, b, c) \in \xi_2. \tag{9}$$

For any $(a, b, c) \in \xi_2$, the weight of the codeword $\mathbf{c}_{a,b,c}$ in $C_f^{(p)}$ is given by

$$\mathrm{wt}(\mathbf{c}_{a,b,c}) = \#S - N'_{a,b,c} + \delta'(b), \tag{10}$$

where $\delta'(x)$ is a function from $\mathbb{F}_{p^3}$ to $\{0, 1\}$ defined as:

$$\delta'(x) = \begin{cases} 0 & \text{if } \mathrm{Tr}_{p^3/p}(x) = 0, \\ 1 & \text{if } \mathrm{Tr}_{p^3/p}(x) \neq 0. \end{cases} \tag{11}$$

Next, we will study the weight distributions of $C_f^{(p)}$ and $C_f^{*(p)}$, and analyze their dual codes. To this end, we will prove some auxiliary results below, which will help us calculate the weight distributions of the aforementioned codes.

Lemma 4.1. *Let $(b, c) \in \mathbb{F}_{p^3} \times \mathbb{F}_{p^3}$, and define $\omega_3 = \mathrm{Tr}_{p^3/p}(b^2 + c^2)$.*

(i) Let $R_1 = \left\{(b, c) \in \mathbb{F}_{p^3} \times \mathbb{F}_{p^3} \mid \omega_3 = 0,\ \mathrm{Tr}_{p^3/p}(b) = 0\right\}$; then $\#R_1 = p^4 - p^3 + p^2$.

(ii) Let $R_2 = \left\{(b, c) \in \mathbb{F}^*_{p^3} \times \mathbb{F}^*_{p^3} \mid \omega_3 = 0,\ \mathrm{Tr}_{p^3/p}(b) = 0\right\}$; then $\#R_2 = p^4 - p^3 + p^2 - 1$.

(iii) Let $R_3 = \left\{(b,c) \in \mathbb{F}_{p^3} \times \mathbb{F}_{p^3} \mid \omega_3 = 0,\ \mathrm{Tr}_{p^3/p}(b) \neq 0\right\}$; then $\#R_3 = p^5 - p^4$.

(iv) Let $R_4 = \left\{(b,c) \in \mathbb{F}_{p^3} \times \mathbb{F}_{p^3} \mid \omega_3 \neq 0,\ \mathrm{Tr}_{p^3/p}(b) = 0\right\}$; then $\#R_4 = p^5 - p^4 + p^3 - p^2$.

(v) Let $R_5 = \left\{(b,c) \in \mathbb{F}_{p^3} \times \mathbb{F}_{p^3} \mid \omega_3 \neq 0,\ \mathrm{Tr}_{p^3/p}(b) \neq 0\right\}$; then $\#R_5 = p^6 - 2p^5 + p^4$.

(vi) Let $R_6 = \left\{(b,c) \in \mathbb{F}_{p^3} \times \mathbb{F}_{p^3} \mid \omega_3 = 0\right\}$; then $\#R_6 = p^5 - p^3 + p^2$.

(vii) Let $R_7 = \left\{(b,c) \in \mathbb{F}_{p^3} \times \mathbb{F}_{p^3} \mid \mathrm{Tr}_{p^3/p}(b) = 0\right\}$; then $\#R_7 = p^5$.

Proof. The conclusion of (vii) follows directly from the definition. Additionally, the cardinalities $\#R_2$ to $\#R_5$ can be derived using set theory based on the following relationships: $R_2 = (R_6 \cap R_7) \setminus \{(0,0)\}$, $R_3 = R_6 \setminus R_7$, $R_4 = R_7 \setminus R_6$, and $R_5 = (R_6 \cup R_7)^c$. Thus, we only need to prove (i) and (vi).

By utilizing the orthogonal property of the canonical additive character, together with $\chi' = \chi \circ \mathrm{Tr}_{p^3/p}$ and Lemma 2.2, we have:

(i)

$$\begin{aligned}
\#R_1 &= \frac{1}{p^2} \sum_{\kappa \in \mathbb{F}_p} \sum_{\mu \in \mathbb{F}_p} \sum_{b \in \mathbb{F}_{p^3}} \chi\left(\mathrm{Tr}_{p^3/p}\left(\kappa b^2 + \mu b\right)\right) \sum_{c \in \mathbb{F}_{p^3}} \chi\left(\mathrm{Tr}_{p^3/p}\left(\kappa c^2\right)\right) \\
&= \frac{1}{p^2} \sum_{\kappa \in \mathbb{F}_p} \sum_{\mu \in \mathbb{F}_p} \sum_{b \in \mathbb{F}_{p^3}} \chi'(\mu b)\chi'(\kappa b^2) \sum_{c \in \mathbb{F}_{p^3}} \chi'(\kappa c^2) \\
&= p^4 + \frac{1}{p} \sum_{\kappa \in \mathbb{F}_p^*} \eta'(\kappa)^2 G(\chi', \eta')^2 \\
&= p^4 - p^3 + p^2.
\end{aligned}$$

(vi)

$$\begin{aligned}
\#R_6 &= \frac{1}{p} \sum_{(b,c) \in \mathbb{F}_{p^3}^2} \sum_{\kappa \in \mathbb{F}_p} \chi\left(\kappa\, \mathrm{Tr}_{p^3/p}(b^2 + c^2)\right) \\
&= p^5 + \frac{1}{p} \sum_{\kappa \in \mathbb{F}_p^*} \sum_{(b,c) \in \mathbb{F}_{p^3}^2} \chi\left(\kappa\, \mathrm{Tr}_{p^3/p}(b^2) + \kappa\, \mathrm{Tr}_{p^3/p}(c^2)\right) \\
&= p^5 + \frac{1}{p} \sum_{\kappa \in \mathbb{F}_p^*} \sum_{b \in \mathbb{F}_{p^3}} \chi'\left(\kappa b^2\right) \sum_{c \in \mathbb{F}_{p^3}} \chi'\left(\kappa c^2\right) \\
&= p^5 + \frac{1}{p} \sum_{\kappa \in \mathbb{F}_p^*} \eta'(\kappa)^2 G(\chi', \eta')^2 \\
&= p^5 - p^3 + p^2.
\end{aligned}$$

□

Define a character sum

$$\Gamma_3^{a,b,c} = \sum_{\kappa \in \mathbb{F}_p^*} \chi(\kappa a) \sum_{\mu \in \mathbb{F}_p^*} \sum_{(x,y) \in \mathbb{F}_{p^3}^2} \chi\left(\mu \mathrm{Tr}_{p^3/p}(y^2) + \mu \mathrm{Tr}_{p^3/p}(x^2)\right) \chi(\kappa b x + \kappa c y), \tag{12}$$

where $(a, b, c) \in \xi_2$ for any such triple. Using the orthogonal property of the canonical additive character, along with $\chi' = \chi \circ \mathrm{Tr}_{p^3/p}$ and Lemma 2.2, we have

$$\begin{aligned}
\Gamma_3^{a,b,c} &= \sum_{\kappa\in\mathbb{F}_p^*} \chi(\kappa a) \sum_{\mu\in\mathbb{F}_p^*} \sum_{(x,y)\in\mathbb{F}_{p^3}^2} \chi\Big(\mu\,\mathrm{Tr}_{p^3/p}(y^2) + \mu\,\mathrm{Tr}_{p^3/p}(x^2)\Big)\chi\Big(\kappa bx + \kappa cy\Big) \\
&= \sum_{(\kappa,\mu)\in\mathbb{F}_p^{*2}} \chi(\kappa a) \sum_{x\in\mathbb{F}_{p^3}} \chi'\big(\mu x^2 + \kappa bx\big) \sum_{y\in\mathbb{F}_{p^3}} \chi'\big(\mu y^2 + \kappa cy\big) \\
&= \sum_{(\kappa,\mu)\in\mathbb{F}_p^{*2}} \chi(\kappa a)\,\eta'(\mu)^2 \chi'\Big(-\frac{\kappa^2(b^2+c^2)}{4\mu}\Big) G(\chi',\eta')^2 \\
&= \sum_{(\kappa,\mu)\in\mathbb{F}_p^{*2}} \chi\Big(\kappa a - \mathrm{Tr}_{p^3/p}\Big(\frac{\kappa^2(b^2+c^2)}{4\mu}\Big)\Big)\eta'(\mu)^2\, G(\chi',\eta')^2 \\
&= G(\chi',\eta')^2 \sum_{(\kappa,\mu)\in\mathbb{F}_p^{*2}} \chi\Big(\kappa a - \mathrm{Tr}_{p^3/p}\Big(\frac{\kappa^2(b^2+c^2)}{4\mu}\Big)\Big) \\
&= \begin{cases} -p^3(p-1)^2 & \text{if } a = 0,\ \omega_3 = 0, \\ p^3(p-1) & \text{if } a = 0,\ \omega_3 \neq 0, \text{ or } a \neq 0,\ \omega_3 = 0, \\ -p^3 & \text{if } a \neq 0,\ \omega_3 \neq 0, \end{cases}
\end{aligned}$$

where ω_3 is as defined in Lemma 4.1.

Theorem 4.2. *The subfield code $C_f^{(p)}$ defined in Eq (3) is a linear code over $\mathbb{F}_p$ with parameters $[p^5 - p^3 + p^2 + 1, 7, p^5 - p^4 - p^3 + p^2]$, and its weight distribution is presented in Table 3. Its dual code $C_f^{(p)\perp}$ is also a linear code over $\mathbb{F}_p$ with parameters $[p^5 - p^3 + p^2 + 1, p^5 - p^3 + p^2 - 6, 3]$.*

Table 3. The Weight distribution of $C_f^{(p)}$.

Weight	Multiplicity
0	1
$p^5 - p^3 + p^2$	$p - 1$
$p^5 - p^4 - p^3 + 2p^2$	$p^6 - 2p^5 + 2p^4 - 2p^3 + p^2$
$p^5 - p^4 - p^3 + 2p^2 + 1$	$p^7 - 3p^6 + 3p^5 - p^4$
$p^5 - p^4$	$p^4 - p^3 + p^2 - 1$
$p^5 - p^4 + 1$	$p^5 - p^4$
$p^5 - p^4 - p^3 + p^2$	$2p^5 - 3p^4 + 3p^3 - 2p^2 - p + 1$
$p^5 - p^4 - p^3 + p^2 + 1$	$2p^6 - 4p^5 + 2p^4$

Proof. We begin by determining the length of the code. To compute $\#S$, note that $\#S = \#R_6$, so we can directly conclude that the length of $C_f^{(p)}$ is $p^5 - p^3 + p^2 + 1$.

Following the same computational approach as in Eqs (4) and (5), analogous calculations apply to Eqs (9) and (10). As a consequence, the weight of the codeword $\mathbf{c}_{a,b,c}$ in $C_f^{(p)}$ is derived as follows

(detailed steps are omitted):

$$\mathrm{wt}(\mathbf{c}_{a,b,c}) = \begin{cases} 0 & \text{if } a=b=c=0, \\ p^5-p^3+p^2 & \text{if } a\neq 0,\ b=c=0, \\ \delta'(b)+p^4(p-1)+\frac{1}{p^2}\left[(p-1)(p^3-p^4)-\Gamma_3^{a,b,c}\right] & \text{if } b,c \text{ not all } 0, \end{cases}$$

$$= \begin{cases} 0 & \text{if } a=b=c=0, \\ p^5-p^3+p^2 & \text{if } a\neq 0,\ b=c=0, \\ p^5-p^4-p^3+2p^2 & \text{if } a\neq 0,\ (b,c)\in R_4, \\ p^5-p^4-p^3+2p^2+1 & \text{if } a\neq 0,\ (b,c)\in R_5, \\ p^5-p^4 & \text{if } a=0,\ (b,c)\in R_2, \\ p^5-p^4+1 & \text{if } a=0,\ (b,c)\in R_3, \\ p^5-p^4-p^3+p^2 & \text{if } a=0,\ (b,c)\in R_4 \\ & \quad \text{or } a\neq 0,\ (b,c)\in R_2, \\ p^5-p^4-p^3+p^2+1 & \text{if } a=0,\ (b,c)\in R_5 \\ & \quad \text{or } a\neq 0,\ (b,c)\in R_3, \end{cases}$$

where R_i $(i = 2, \ldots, 5)$ are defined in Lemma 4.1. Thus, $C_f^{(p)}$ is a linear code with parameters $[p^5 - p^3 + p^2 + 1, 7, p^5 - p^4 - p^3 + p^2]$, and applying Lemma 4.1 immediately gives the frequency of each weight.

Finally, it is easy to see that the dual code $C_f^{(p)\perp}$ has length $p^5 - p^3 + p^2 + 1$ and dimension $p^5 - p^3 + p^2 - 6$. Using the first four power moments, we find that $A_1^\perp = A_2^\perp = 0$, and $A_3^\perp > 0$. This completes the proof. □

Example 4.3. The examples provided below demonstrate that the subfield code $C_f^{(p)}$ possesses excellent parameters. For comparison, the best-known parameters are retrieved from the code tables available at [14].
For $p = 3$, $C_f^{(3)}$ is a ternary linear code with weight enumerator $1+304z^{144}+648z^{145}+360z^{153}+648z^{154}+62z^{162}+162z^{163}+2z^{225}$ $[226, 7, 144]$. Its dual is attains the best-known parameters $[226, 219, 3]$.

Using the relationship between $C_f^{(p)}$ and its punctured code $C_f^{*(p)}$, together with Theorem 4.2 and the first four power moments, we immediately derive the following result. The minimum distance of the dual code can be computed with the first four power moments, and the calculation is omitted here.

Theorem 4.4. *The punctured code $C_f^{*(p)}$ is a four-weight linear code over $\mathbb{F}_p$ with parameters $[p^5 - p^3 + p^2, 7, p^5 - p^4 - p^3 + p^2]$, and its weight distribution is presented in Table 4. Its dual is a linear code over $\mathbb{F}_p$ with parameters $[p^5 - p^3 + p^2, p^5 - p^3 + p^2 - 7, 3]$.*

Table 4. The Weight distribution of $C_f^{*(p)}$.

Weight	Multiplicity
0	1
$p^5 - p^3 + p^2$	$p - 1$
$p^5 - p^4 - p^3 + 2p^2$	$p^7 - 2p^6 + p^5 + p^4 - 2p^3 + p^2$
$p^5 - p^4$	$p^5 - p^3 + p^2 - 1$
$p^5 - p^4 - p^3 + p^2$	$2p^6 - 2p^5 - p^4 + 3p^3 - 2p^2 - p + 1$

Example 4.5. The examples provided below demonstrate that the punctured code $C_f^{*(p)}$ possesses excellent parameters. For comparison, the best-known parameters are retrieved from the Code Tables available at [14].
For $p = 3$, $C_f^{*(p)}$ is a best-known $[225, 7, 144]$ ternary linear code with weight enumerator $1+952z^{144}+1008z^{153}+224z^{162}+2z^{225}$. Its dual is a ternary linear code, and both share the best-known parameters $[225, 218, 3]$.

5. Constructing t-designs

Let t, n, κ, λ be positive integers with $t \leq \kappa \leq n$. An incidence structure $\mathbb{D} = (\mathcal{P}, \mathcal{B})$ is called a t-(n, κ, λ) design or simply a t-design if it satisfies two core conditions: $\mathcal{P}$ is a set of n elements called points, $\mathcal{B}$ is a family of κ-element subsets of $\mathcal{P}$ called blocks, and every t-element subset of $\mathcal{P}$ is contained in exactly λ blocks from $\mathcal{B}$. This design satisfies the combinatorial identity $\binom{n}{t}\lambda = \binom{\kappa}{t}b$, where $b = |\mathcal{B}|$ and b denote the total number of blocks. Key variants include the simple t-design (with no repeated blocks in $\mathcal{B}$) and the Steiner system, which is a t-design with $t \geq 2$ and $\lambda = 1$ and is denoted $S(t, \kappa, n)$. For an $[n, k, d]$ linear code C over $\mathbb{F}_q$, its coordinate set is $\mathcal{P} = \{p_1, p_2, \ldots, p_n\}$, and the support set of a codeword $\boldsymbol{c} \in C$ is defined as $\text{supp}(\boldsymbol{c}) = \{i \mid c_i \neq 0, i \in \mathcal{P}\}$. Let κ be a code weight with $A_\kappa \neq 0$, where A_κ counts the number of weight-κ codewords in C, and let $\mathcal{B}_\kappa$ be the family of support sets from all weight-κ codewords in C. If $(\mathcal{P}, \mathcal{B}_\kappa)$ forms a t-(n, κ, λ) design, the code C is said to hold a t-(n, κ, λ) support design (denoted $\mathbb{D}_\kappa(C)$), or equivalently, the support sets of weight-κ codewords in C form a t-design.

By Assmus and Mattson [15], the following theorem suffices for a linear code and its dual to form simple t-designs.

Theorem 5.1 (Assmus–Mattson Theorem)**.** *Let C be an $[n, k, d]$ code over $\mathbb{F}_q$, with $d^\perp$ as the minimum distance of $C^\perp$. Let w be the largest integer $\leq n$ satisfying*

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

and $w^\perp$ defined analogously by replacing d with $d^\perp$. Let $(A_i)_{i=0}^n$ and $(A_i^\perp)_{i=0}^n$ be the weight distributions of C and $C^\perp$, respectively. For a positive integer $t < d$, let s be the number of $i \in [1, n-t]$ with $A_i^\perp \neq 0$. If $s \leq d - t$, then the following assertions hold:

- *Weight-i codewords of C form a t-design if $A_i \neq 0$, and $d \leq i \leq w$;*

- *Weight-i codewords of $C^{\perp}$ form a t-design if $A_i^{\perp} \neq 0$, and $d^{\perp} \leq i \leq \min\{n-t, w^{\perp}\}$.*

Theorem 5.2. *Let $f(x,y) = \mathrm{Tr}_{2^m/2}(x \cdot y) + \mathrm{N}_{2^m/2}(x+y)$ and $m \geq 3$. The codewords of Hamming weight $2^{2m-2} - 2^{m-1}$ or 2^{2m-2} in $C_f^{*(2)}$ form a 2-design. Moreover, for all κ with $4 \leq \kappa \leq 2^{2m-1} - 2^{m-1}$, the Hamming weight-$\kappa$ codewords in $C_f^{*(2)^{\perp}}$ form this 2-design.*

Proof. Through the integration of Theorem 3.5 and Theorem 5.1, we arrive at the conclusions for this 2-design. □

Theorem 5.3. *Let $f(x,y) = \mathrm{Tr}_{2^m/2}(xy)$ and $m \geq 2$. The Hamming weight $2^{2m-2} + 2^{m-1}$ or 2^{2m-2} codewords in $C_f^{*(2)}$ form a 2-design . Moreover, for all κ with $4 \leq \kappa \leq 2^{2m-1} + 2^{m-1}$, the Hamming weight-$\kappa$ codewords in $C_f^{*(2)^{\perp}}$ form this 2-design.*

Proof. The combination of Theorem 3.12 and Theorem 5.1 gives the desired conclusions for this 2-design. □

6. Conclusions

This paper extends the framework proposed in [9] for constructing three-dimensional linear codes C_f over $\mathbb{F}_{q^m}$ that are parameterized by functions. Specifically, we investigate the weight distributions of the subfield code $C_f^{(2)}$, the punctured code $C_f^{*(2)}$, and their dual codes for the case $q = 2$. For $q = p$ (where $p \equiv 3 \pmod 4$ and $m = 3$), we conduct a similar analysis on the weight distributions of the subfield code $C_f^{(p)}$, the punctured code $C_f^{*(p)}$, and their dual codes. Codes with favorable parameters are rare, and relevant examples are provided in Examples 3.4, 3.7, 3.11, 3.14, 4.3, and 4.5. Furthermore, through our careful comparison, many of the obtained codes either have new parameters or are inequivalent to the known subfield codes (see Table 5). Lastly, two classes of 2-designs are derived from several codes presented in this work.

Table 5. Some known subfield codes in the literature.

q-Ary	$[n,k,d]$ Codes	Conditions	Ref.
q-ary	$[q^3+1, 5, q^3-q^2-q]$	q is even and $m=3$	[9] Thm. 3
p-ary	$[p^2(p^2-1)+2, 4, p^2(p+1)(p-2)+1]$	$m=2$	[16] Thm. 3.3
p-ary	$[p^m+1, 2m+1, p^{m-1}(p-1) - p^{\frac{m-1}{2}}]$	$m>1$ is odd	[17] Thm.16
p-ary	$[p^{2m}+1, 3m+1, p^{2m-1}(p-1) - p^{m-1}]$	$m>1$	[8] Thm. 4.6
p-ary	$[p^{2m}+1, 3m+1, (p^{2m-1}-p^{m-1})(p-1)]$	$m>1$	[8] Thm.4.7
p-ary	$[p^m+1, m+1, (p-1)p^{m-1}]$	$m>1$	[18] Thm. V.1
p-ary	$[p^m+1, 2m, p^{m-1}(p-1) - p^{\frac{m-1}{2}}]$	p and m are odd	[18] Thm. VI.7
binary	$[2^m+1, m+1, 2]$	$m>1$	[18] Thm. VII.4
binary	$[2^m+2, m+2, 2]$	$m>1$	[17] Thm. 11
binary	$[2^m+2, 2m+1, 2^{m-1} - 2^{\frac{m-1}{2}}]$	$m>1$	[17] Thm. 13
binary	$[2^m+2, 2m+1, 2^{m-1} - 2^{\frac{m+d-2}{2}}]$	$v_2(m) \leq v_2(i-j)$ $d = \gcd(m, i-j)$	[7] Thm. 10
binary	$[2^m+1, 2m+1, 2^{m-1} - 2^{\frac{m+2d-2}{2}}]$	$v_2(m) \geq v_2(i-j)+1$ $d = \gcd(m, i-j)$	[7] Thm. 18
binary	$[2^{2m-1}+1, 2m, 2^{2m-2}]$	$m>1$ is even	[9] Thm. 7
binary	$[2^{2m-1}+1, 2m+1, 2^{2m-2} - 2^{\frac{3m-3}{2}}+1]$	$m>1$ is odd	[9] Thm. 9
binary	$[2^{2m-1}+1, 2m+1, 2^{2m-2} - 2^{\frac{3m-4}{2}}]$	$m>1$ is even	[9] Thm. 12

Author contributions

Shanshan Liu, Yan Li, and Xiaoyu Yu: Writing –Review & Editing. All authors have read and approved the final version of the manuscript for publication.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

This research is supported by the University Natural Science Research Project of Anhui Province under Grant 2024AH051503, the Talent Research Fund Project of Hefei University under Grant 24RC17, and the Scientific Research Project of Anhui Provincial Department of Education under Grant 2025AHGXZK30090.

Conflict of interest

All authors declare no conflicts of interest in this paper.

References

1. C. Carlet, C. Ding, J. Yuan, Linear Codes from Perfect Nonlinear Mappings and Their Secret Sharing Schemes, *IEEE Trans. Inf. Theory,* **51** (2005), 2089–2102. https://doi.org/10.1109/TIT.2005.847722
2. C. Ding, Linear Codes from Some 2-Designs, *IEEE Trans. Inf. Theory,* **61** (2015), 3265–3275. https://doi.org/10.1109/TIT.2015.2420118
3. R. Calderbank, W. M. Kantor, The Geometry of Two-Weight Codes, *Bull. London Math. Soc.,* **18** (1986), 97–122. https://doi.org/10.1112/blms/18.2.97
4. Y. Ding, S. Zhu, A Family of Linear Codes with Few Weights and Their Subfield Codes, *Cryptogr. Commun.,* **17** (2025), 207–238. https://doi.org/10.1007/s12095-024-00753-8
5. A. Canteaut, P. Charpin, H. Dobbertin, Weight Divisibility of Cyclic Codes, Highly Nonlinear Functions on $\mathbb{F}_{2^m}$, and Crosscorrelation of Maximum-Length Sequences, *SIAM J. Discrete Math.,* **13** (2000), 105–138. https://doi.org/10.1137/S0895480198350057
6. C. Carlet, P. Charpin, V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, *Designs, Codes, Cryptogr.,* **15** (1998), 125–156. https://doi.org/10.1023/A:1008344232130
7. X. Wang, D. Zheng, The subfield codes of several classes of linear codes, *Cryptogr. Commun.,* **12** (2020), 1111–1131. https://doi.org/10.1007/s12095-020-00432-4
8. C. Ding, Z. Heng, The Subfield Codes of Ovoid Codes, *IEEE Trans. Inf. Theory,* **65** (2019), 4715–4729. https://doi.org/10.1109/TIT.2019.2907276

9. L. Xu, C. Fan, S. Mesnager, R. Luo, H. Yan, Subfield codes of several few-weight linear codes parameterized by functions and their consequences, *IEEE Trans. Inf. Theory,* **70** (2024), 3941–3964. https://doi.org/10.1109/TIT.2023.3328932
10. F. Hernández, G. Vega, The Subfield and Extended Codes of a Subclass of Optimal Three-Weight Cyclic Codes, *Algorithmica,* **85** (2023), 3973–3995. https://doi.org/10.1007/s00453-023-01173-5
11. X. Qiao, X. Du, W. Yuan, Several classes of linear codes with AMDS duals and their subfield codes, *Cryptogr. Commun.,* **16** (2024), 1429–1448. https://doi.org/10.1007/s12095-024-00729-8
12. Y. Wu, Optimal few-weight codes and their subfield codes, *J. Algebra Appl.,* **23** (2024), 2450248. https://doi.org/10.1142/S0219498824502487
13. R. Lidl, H. Niederreiter. Finite Fields. Cambridge University Press, 1997.
14. *M. Grassl, Bounds on the minimum distance of linear codes and quantum codes*, Markus Grassl, 2007. Available from: `http://www.codetables.de`
15. E. F. Assmus, H. F. Mattson, New 5-designs, *J. Combinat. Theory,* **6** (1969), 122–151. https://doi.org/10.1016/S0021-9800(69)80115-8
16. X. Ran, R. Luo, Two classes of subfield codes of linear codes, *arXiv preprint arXiv:2211.00426,* (2022). https://doi.org/10.48550/arXiv.2211.00426
17. Z. Heng, C. Ding, The subfield codes of hyperoval and conic codes, *Finite Fields Appl.,* **56** (2019), 308–331. https://doi.org/10.1016/j.ffa.2018.12.006
18. Z. Heng, C. Ding, The Subfield Codes of Some $[q+1, 2, q]$ MDS Codes, *IEEE Trans. Inf. Theory,* **68** (2022), 3643–3656. https://doi.org/10.1109/TIT.2022.3151721

AIMS Press