A class of affine-invariant codes and their supporting 2-designs

Yan Liu[1,2], Xiwang Cao[3]

Abstract

In this paper, we first introduce a class of linear codes which are affine-invariant. Then we obtain infinite families of 2-designs from them and determine the parameters of these 2-designs by considering the weight distribution of the linear codes.

Key words and phrases: affine-invariant code, cyclic code, 2-design, weight distribution.

MSC: 05B05, 51E10, 94B15, 11T71.

1 Introduction

Let $\mathcal{P}$ be a set of $v \geq 1$ elements and $\mathcal{B}$ be a set of r-subsets of $\mathcal{P}$, where $1 \leq r \leq v$. Let t be a positive integer with $t \leq r$. The pair $(\mathcal{P}, \mathcal{B})$ is called a t-(v, r, λ) design, or simply t-design, if every t-subset of $\mathcal{P}$ is contained in exactly λ elements of $\mathcal{B}$. The elements of $\mathcal{P}$ are called *points* and those of $\mathcal{B}$ are referred to as *blocks*. We usually use b to denote the number of blocks in $\mathcal{B}$. A t-design is called *simple* if $\mathcal{B}$ does not contain repeated blocks and is called *symmetric* if $v = b$. It is clear that t-designs with $r = t$ or $r = v$ always exist. Such t-designs are *trivial*. In this paper, we only consider simple t-designs with $v > r > t$. A t-(v, r, λ) design is referred to as a *Steiner system* $S(t, r, v)$ if $t \geq 2$ and $\lambda = 1$. The following identity is a necessary condition for a t-(v, r, λ) design which can be proved by definition:

$$b\binom{r}{t} = \lambda\binom{v}{t}. \tag{1}$$

Moreover, a necessary condition for the existence of a t-(v, r, λ) design is that

$$\binom{r-i}{t-i} \text{ divides } \lambda\binom{v-i}{t-i}$$

[1]School of Mathematical Sciences, Nanjing University of Aeronautics and Astronautics, Nanjing, 210016, China, liuyan0916@126.com. Y. Liu is supported by the Natural Science Foundation of the Jiangsu Higher Education Institutions of China (No. 19KJB120014) and the National Natural Science Foundation of China (No. 11701498)

[2]College of Mathematics and Physics, Yancheng Institute of Technology, Yancheng, 224003, China.

[3]Corresponding author, School of Mathematical Sciences, Nanjing University of Aeronautics and Astronautics, Nanjing, 210016, China, xwcao@nuaa.edu.cn. X. Cao is supported by the National Natural Science Foundation of China (No. 11771007).

for any integer i with $0 \leq i \leq t$.

Let $\mathcal{C}$ be an $[n, l, d]$ linear code over $\mathbb{F}_p$, where p is a prime. Let $\mathcal{C}^{\perp}$ be the *dual* of $\mathcal{C}$ which is defined by $\mathcal{C}^{\perp} := \{\mathbf{y} \in \mathbb{F}_p^n | \mathbf{x} \cdot \mathbf{y} = 0 \, \text{for any} \, \mathbf{x} \in \mathcal{C}\}$. The *extended code* $\overline{\mathcal{C}}$ of $\mathcal{C}$ is defined by $\overline{\mathcal{C}} = \{(c_0, c_1, \ldots, c_n) \in \mathbb{F}_p^{n+1} : (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C} \, \text{with} \, \sum_{i=0}^{n} c_i = 0\}$. Furthermore, $\mathcal{C}$ is called *cyclic* if for any $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, also $(c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$. A cyclic code of length $n = p^m - 1$ over $\mathbb{F}_p$ for some positive integer m is called a *primitive cyclic code*. A linear code $\mathcal{C}$ in $\mathbb{F}_p^n$ is cyclic if and only if $\mathcal{C}$ is an ideal of the polynomial residue class ring $\mathbb{F}_p[x]/(x^n - 1)$. Since $\mathbb{F}_p[x]/(x^n - 1)$ is a principal ideal ring, every cyclic code corresponds to a principal ideal $(g(x))$ of the multiples of a polynomial $g(x)$ which is the monic polynomial of lowest degree in the ideal. Then $g(x)$ is unique and is called the generator polynomial of $\mathcal{C}$. Let A_i denote the number of codewords with Hamming weight i in $\mathcal{C}$. The sequence $(A_0, A_1, A_2, \ldots, A_n)$ is called the *weight distribution* of $\mathcal{C}$. If we index the coordinates of a codeword by $(0, 1, \cdots, n-1)$, then for any codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ of $\mathcal{C}$, the *support* of $\mathbf{c}$ is defined by

$$Suppt(\mathbf{c}) = \{0 \leq i \leq n-1 : c_i \neq 0\} \subseteq \{0, 1, \cdots, n-1\}.$$

For each i with $A_i \neq 0$, let $\mathcal{B}_i$ denote the set of supports of all the codewords of Hamming weight i in $\mathcal{C}$. Let $\mathcal{P} = \{0, 1, \cdots, n-1\}$. The pair $(\mathcal{P}, \mathcal{B}_i)$ may be a t-(v, k, λ) design for some positive integer λ, which is called a *support design* of this code. In this case, we say that $\mathcal{C}$ holds a t-(v, k, λ) design.

There has been an interplay between codes and t-designs for decades. On one hand, the incidence matrix of any t-design spans a linear code over any finite fields. A lot of progress in this direction has been made in the literature (see [1,4,21,22] for examples). On the other hand, both linear and nonlinear codes may hold t-designs.

There are two standard approaches to obtaining t-designs from linear codes. The first one is to study the automorphism group of a linear code $\mathcal{C}$. If the permutation part of the automorphism group acts t-transitively on the code $\mathcal{C}$, then $\mathcal{C}$ holds t-designs [1]. The second one is to employ Assmus-Mattson Theorem [2]. It should be noted that a generalized Assmus-Mattson theorem is developed recently in [20]. The construction of t-designs from linear codes have been attracted a lot of attention in recent years. In 2017 and 2018, infinite families of 2-designs and 3-designs were obtained from several different classes of linear codes by Ding [7], Ding and Li [8] by applying the Assmus-Mattson Theorem. Besides, Ding presented an infinite family of Steiner systems $S(2, 4, 2^m)$ held by a class of affine-invariant codes in [6]. Recently, Du et al. have derived infinite families of 2-designs from some different classes of affine-invariant codes [11–13]. It is well known that the first linear code supporting a 4-design was the ternary Golay code discovered in 1949 by Golay. However, the question as to whether there is an infinite family of linear codes holding an infinite family of t-designs for $t \geq 4$ remains open for 71 years. Very recently, Tang and Ding [18] settle this long-standing problem by presenting an infinite family of BCH codes holding an infinite family of 4-$(2^{2m+1} + 1, 6, 2^{2m} - 4)$ designs. More constructions of t-designs can be found in [9, 10, 19, 20, 23] and related papers.

As explained above, it looks that not much progress on the construction of t-designs from codes has been made so far. The main objective of this paper is to construct infinite families of 2-designs from linear codes. In addition, we determine the parameters of these 2-designs by considering the weight distribution of the linear codes.

Throughout this paper, let m and k be two positive even integers such that $s = m/d \geq 5$ is odd, where $d = \gcd(m, k)$. Let p be an odd prime and π be a primitive element of the finite field $\mathbb{F}_{p^m}$. Let $q = p^m$, $q_0 = p^d$, then $q = q_0^s$. For a positive divisor i of m, the trace function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_{p^i}$ is defined by $Tr_i^m(x) = \sum_{j=0}^{\frac{m}{i}-1} x^{p^{ij}}$. Let $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ associated with the integer addition modulo n and integer multiplication modulo n operations, where $n = p^m - 1$. For any integer j, $0 \leq j \leq n-1$, the p-cyclotomic coset modulo n containing j is defined by

$$C_j = \{j, pj, p^2 j, \cdots, p^{l_j - 1} j\} \subset \mathbb{Z}_n,$$

where l_j is the minimal positive integer such that $p^{l_j} j \equiv j \pmod{n}$ which is called the *length* of C_j and is denoted by $|C_j|$. The smallest integer in C_j is called the *coset leader* of C_j. Thus the generator polynomial $g(x)$ of a cyclic code $\mathcal{C}$ with length n over $\mathbb{F}_p$ can be written as $g(x) = \prod_j \prod_{s \in C_j} (x - \pi^s)$, where j runs through some coset leaders of p-cyclotomic cosets C_j modulo n. The set $\bigcup_j C_j$ is referred to as the *defining set* of $\mathcal{C}$ which is the union of these p-cyclotomic cosets. Moreover, we have the following result on the length of some special p-cyclotomic cosets.

Lemma 1.1 ([24]) *Let $1 \leq e \leq m-1$. Then*

(1) *when m is odd, $|C_{p^e+1}| = m$;*

(2) *when m is even,*

$$|C_{p^e+1}| = \begin{cases} \frac{m}{2}, & \text{if } e = \frac{m}{2}; \\ m, & \text{otherwise.} \end{cases}$$

A code $\overline{\mathcal{C}}$ of length q^m is an *extended primitive cyclic code* with defining set $\overline{T}$ which is defined by

$$\overline{T} = \begin{cases} \{0\} \bigcup T, & \text{if } 0 \notin T, \\ \{0, n\} \bigcup T, & \text{if } 0 \in T. \end{cases}$$

In this paper, when $p^{2k} + 1$ is larger than $p^m - 1$, we will take it as the residue modulo $p^m - 1$ which will not cause any problems. And it is the same for $p^{4k} + 1$.

Let $\mathcal{C}$ be the cyclic code over $\mathbb{F}_p$ with defining set $T = C_1 \cup C_2 \cup C_{p^{2k}+1} \cup C_{p^{4k}+1}$. It should be noticed that 2, $p^{2k}+1$ and $p^{4k}+1$ are in different cyclotomic cosets from [25]. By Lemma 1.1, we can obtain the dimension of $\mathcal{C}$ is $p^m - 1 - 4m$ since none of 2, $p^{2k}+1$ and $p^{4k}+1$ is in C_1. Besides, we can prove $\overline{\mathcal{C}}^{\perp}$ is affine-invariant. In order to do this, we introduce a partial ordering $\preceq$ on the set $\overline{\mathcal{N}} = \{0, 1, \cdots, n\}$. For any two integers r, s in $\overline{\mathcal{N}}$, we define $r \preceq s$ if $r_i \leq s_i$ for all $0 \leq i \leq m-1$, where $r = \sum_{i=1}^{m-1} r_i p^i$, $0 \leq r_i \leq p-1$ and $s = \sum_{i=1}^{m-1} s_i p^i$, $0 \leq s_i \leq p-1$ are the p-adic expansions of s and r, respectively. By definition, $r \leq s$ if $r \preceq s$. The following is a characterization of affine-invariant codes due to Kasami, Lin and Peterson.

Lemma 1.2 ([14]) *Let $\overline{\mathcal{C}}$ be an extended primitive cyclic code of length p^m over $\mathbb{F}_p$ with defining set $\overline{T}$. Then the code $\overline{\mathcal{C}}$ is affine-invariant if and only if whenever $s \in \overline{T}$ then $r \in \overline{T}$ for all $r \in \overline{\mathcal{N}}$ with $r \preceq s$.*

Besides, we also need the following result due to C. Ding.

Lemma 1.3 ([5], Theorem 6.5) *The dual of an affine-invariant code is also affine-invariant.*

Based on this, we have the following result.

Theorem 1.4 *The linear code $\overline{\mathcal{C}}^{\perp}$ is affine-invariant.*

Proof. First, we will prove $\overline{\mathcal{C}}$ is affine-invariant. By the definition, the defining set of $\mathcal{C}$ is $T = C_1 \cup C_2 \cup C_{p^{2k}+1} \cup C_{p^{4k}+1}$. Since $0 \notin T$, the defining set $\overline{T}$ of $\overline{\mathcal{C}}$ is given by

$$\overline{T} = C_1 \cup C_2 \cup C_{p^{2k}+1} \cup C_{p^{4k}+1} \cup \{0\}.$$

Let $s \in \overline{T}$ and r be any integer in $\overline{\mathcal{N}}$ such that $r \preceq s$. If $r = 0$, then $r \in \overline{T}$. Otherwise, $0 < r \leq s$. If $s \in C_1 \cup C_2$, the Hamming weight of s is 1 and then $r = s$ since $r \preceq s$. So $r \in C_1 \cup C_2 \subset \overline{T}$. If $s \in C_{p^{2k}+1} \cup C_{p^{4k}+1}$, the Hamming weight of s is 2 and then either the Hamming weight of r is 1 or $r = s$ also by $r \preceq s$. In both cases, $r \in \overline{T}$. Then by Lemmas 1.2 and 1.3, we obtain the result. ■

Moreover, by using the well-known Delsarte's Theorem [3], $\mathcal{C}^{\perp}$ can be expressed as

$$\mathcal{C}^{\perp} = \{\mathbf{c}_{(\alpha,\beta,\gamma,\delta)} : \alpha, \beta, \gamma, \delta \in \mathbb{F}_q\},$$

where $\mathbf{c}_{(\alpha,\beta,\gamma,\delta)} = \left(Tr_1^m(\alpha x^{p^{4k}+1} + \beta x^{p^{2k}+1} + \gamma x^2 + \delta x)\right)_{x \in \mathbb{F}_{p^m}^*}$, where $\mathbb{F}_{p^m}^* = \mathbb{F}_{p^m} \setminus \{0\}$. Moreover, by the definition of extended codes and dual codes, $\overline{\mathcal{C}}^{\perp}$ can be expressed as

$$\overline{\mathcal{C}}^{\perp} = \{\mathbf{c}_{(\alpha,\beta,\gamma,\delta,h)} : \alpha, \beta, \gamma, \delta \in \mathbb{F}_{p^m}, h \in \mathbb{F}_p\}, \tag{2}$$

where $\mathbf{c}_{(\alpha,\beta,\gamma,\delta,h)} = (Tr_1^m(\alpha x^{p^{4k}+1} + \beta x^{p^{2k}+1} + \gamma x^2 + \delta x)_{x \in \mathbb{F}_{p^m}} + h)$. To obtain the parameters of the 2-designs derived from $\overline{\mathcal{C}}^{\perp}$, we need to determine the weight distribution of it.

The rest of this paper is organized as follows. In Section 2, we introduce some preliminaries. The weight distribution of the linear codes $\overline{\mathcal{C}}^{\perp}$ and the parameters of their supporting 2-designs are determined in Section 3. Section 4 concludes this paper.

2 Preliminaries

In this section, we will introduce some basic facts on 2-designs, exponential sums, cyclotomic fields and quadratic forms. It should be noticed that most of the known results hold for any positive integer m and prime p unless otherwise stated. In the following, we always assume that $n = p^m - 1$ and π is a primitive element of $\mathbb{F}_{p^m}$. The following results given by Ding [5] are very important for us to present the main results of this paper.

Lemma 2.1 ([5], Theorem 6.6) *For each i with $A_i \neq 0$ in an affine-invariant code with length p^m, the supports of the codewords with weight i form a 2-design.*

Lemma 2.2 ([5], Lemma 4.1) *Let $\mathcal{C}$ be a linear code over $\mathbb{F}_p$ with minimum distance d and length n. Let w be the largest integer with $w \leq n$ satisfying*

$$w - \lfloor \frac{w+p-2}{p-1} \rfloor < d.$$

Let $\mathbf{c}_1$ and $\mathbf{c}_2$ be two codewords of weight i with $d \leq i \leq w$ and $Suppt(\mathbf{c}_1) = Suppt(\mathbf{c}_2)$. Then $\mathbf{c}_1 = a\mathbf{c}_2$ for some $a \in \mathbb{F}_p^*$, where $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$.

Let $\zeta_p = e^{\frac{2\pi i}{p}}$ be a primitive p-th root of unity. In the following, we give a well-known fact on Galois group of cyclotomic fields $\mathbb{Q}(\zeta_p)$.

Lemma 2.3 ([17], Propositions 6.3.2 and 13.2.1) *The Galois group of $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$ is $\{\sigma_a | 1 \leq a \leq p-1\}$, where the automorphism σ_a of $\mathbb{Q}(\zeta_p)$ is determined by $\sigma_a(\zeta_p) = \zeta_p^a$. Furthermore, the unique quadratic subfield of $\mathbb{Q}(\zeta_p)$ is $\mathbb{Q}(\sqrt{p^*})$ and $\sigma_a(\sqrt{p^*}) = \eta(a)\sqrt{p^*}$, where η is the quadratic character of $\mathbb{F}_p$ and $p^* = (-1)^{\frac{p-1}{2}}p$.*

Recall that $d = \gcd(m,k)$, $s = m/d$, $q = p^m$ and $q_0 = p^d$. By fixing a basis $v_1, v_2, \ldots, v_s$ of $\mathbb{F}_q$ over $\mathbb{F}_{q_0}$, each $x \in \mathbb{F}_q$ can be uniquely expressed as

$$x = x_1v_1 + x_2v_2 + \cdots + x_sv_s,$$

where $x_i \in \mathbb{F}_{q_0}$ for $1 \leq i \leq s$. Then $\mathbb{F}_q$ is isomorphic to the s-dimensional linear space $\mathbb{F}_{q_0}^s$. In other words, we have the following $\mathbb{F}_p$-linear isomorphism:

$$x = x_1v_1 + x_2v_2 + \cdots + x_sv_s \mapsto X = (x_1, x_2, \ldots, x_s).$$

With this isomorphism, a function f from $\mathbb{F}_q$ to $\mathbb{F}_{q_0}$ induces a function F from $\mathbb{F}_{q_0}^s$ to $\mathbb{F}_{q_0}$. For $X = (x_1, x_2, \ldots, x_s) \in \mathbb{F}_{q_0}^s$, let $F(X) = f(x)$, where $x = x_1v_1 + x_2v_2 + \cdots + x_sv_s$. In this way, for any fixed $\delta \in \mathbb{F}_{p^m}$, $f(x) = Tr_d^m(\delta x)$ induces a linear function $F(X) = \sum_{i=1}^s Tr_d^m(\delta v_i)x_i = A_\delta X^T$, where $A_\delta = (Tr_d^m(\delta v_1), Tr_d^m(\delta v_2), \ldots, Tr_d^m(\delta v_s))$, X^T denotes the transpose of X. Similarly, for any fixed $\alpha, \beta, \gamma \in \mathbb{F}_{p^m}$, $Q_{\alpha,\beta,\gamma}(x) = Tr_d^m(\alpha x^{p^{4k}+1} + \beta x^{p^{2k}+1} + \gamma x^2)$ induces a quadratic form

$$\begin{aligned} F_{\alpha,\beta,\gamma}(X) &= Tr_d^m(\alpha(\sum_{i=1}^s x_iv_i)^{p^{4k}+1} + \beta(\sum_{i=1}^s x_iv_i)^{p^{2k}+1} + \gamma(\sum_{i=1}^s x_iv_i)^2) \\ &= \sum_{i,j=1}^s Tr_d^m(\alpha v_i^{p^{4k}}v_j + \beta v_i^{p^{2k}}v_j + \gamma v_iv_j)x_ix_j \\ &= XH_{\alpha,\beta,\gamma}X^T, \end{aligned} \tag{3}$$

where $H_{\alpha,\beta,\gamma} = (h_{i,j})$ and

$$h_{i,j} = \frac{1}{2}Tr_d^m(\alpha(v_i^{p^{4k}}v_j + v_iv_j^{p^{4k}}) + \beta(v_i^{p^{2k}}v_j + v_iv_j^{p^{2k}})) + Tr_d^m(\gamma v_iv_j), \quad 1 \leq i,j \leq s.$$

Then

$$T(\alpha,\beta,\gamma)=\sum_{x\in\mathbb{F}_{p^m}}\zeta_p^{Tr_1^m(\alpha x^{p^{4k}+1}+\beta x^{p^{2k}+1}+\gamma x^2)}=\sum_{X\in\mathbb{F}_{q_0}^s}\zeta_p^{Tr_1^d(XH_{\alpha,\beta,\gamma}X^T)}$$

and

$$S(\alpha,\beta,\gamma,\delta)=\sum_{x\in\mathbb{F}_{p^m}}\zeta_p^{Tr_1^m(\alpha x^{p^{4k}+1}+\beta x^{p^{2k}+1}+\gamma x^2+\delta x)}=\sum_{X\in\mathbb{F}_{q_0}^s}\zeta_p^{Tr_1^d(XH_{\alpha,\beta,\gamma}X^T+A_\delta X^T)}.$$

For a quadratic form $F(X)$ over $\mathbb{F}_{q_0}$, there exists a symmetric matrix A of order s over $\mathbb{F}_{q_0}$ such that $F(X)=XAX^T$, where $X=(x_1,x_2,\ldots,x_s)\in\mathbb{F}_{q_0}^s$. Then there exists a nonsingular matrix H of order s over $\mathbb{F}_{q_0}$ such that HAH^T is a diagonal matrix [15]. The rank of the quadratic form $F(X)$ is defined to be the rank of A which is exactly the codimension of the $\mathbb{F}_{q_0}$-vector space $V=\{x\in\mathbb{F}_{p^m}: Q(x+z)-Q(x)-Q(z)=0\ for\ all\ z\in\mathbb{F}_{p^m}\}$. Under the nonsingular linear substitution $X=ZH$ with $Z=(z_1,z_2,\ldots,z_s)\in\mathbb{F}_{q_0}^s$, $F(X)=ZHAH^TZ^T=\sum_{i=1}^r d_iz_i^2$, where r is the rank of $F(X)$ and $d_i\in\mathbb{F}_{q_0}^*$. Let $\triangle=d_1d_2\cdots d_r$ (we assume $\triangle=0$ when $r=0$). Let η_0 be the quadratic character of $\mathbb{F}_{q_0}$. Then $\eta_0(\triangle)$ is an invariant of A under the action of $H\in GL_s(\mathbb{F}_{q_0})$. Furthermore, quadratic forms over finite fields have the following properties.

Lemma 2.4 *Let $F(X)=XHX^T$ be a quadratic form in s variables of rank r over $\mathbb{F}_{q_0}$, then*

(1) $\sum_{X\in\mathbb{F}_{q_0}^s}\zeta_p^{Tr_1^d(F(X))}=\begin{cases}\eta_0(\triangle)(-1)^{(d-1)r}q_0^{s-\frac{r}{2}}, & p\equiv 1\pmod 4,\\ \eta_0(\triangle)(\sqrt{-1})^{dr}(-1)^{(d-1)r}q_0^{s-\frac{r}{2}}, & p\equiv 3\pmod 4,\end{cases}$

(2) *for $A=(a_1,a_2,\ldots,a_s)\in\mathbb{F}_{q_0}^s$, if $2YH+A=0$ has a solution $Y=B\in\mathbb{F}_{q_0}^s$, then $\sum_{X\in\mathbb{F}_{q_0}^s}\zeta_p^{Tr_1^d(F(X)+AX^T)}=\zeta_p^c\sum_{X\in\mathbb{F}_{q_0}^s}\zeta_p^{Tr_1^d(F(X))}$, where $c=-Tr_1^d(BHB^T)=\frac{1}{2}Tr_1^d(AB^T)\in\mathbb{F}_p$, otherwise $\sum_{X\in\mathbb{F}_{q_0}^s}\zeta_p^{Tr_1^d(F(X)+AX^T)}=0$.*

The first statement of the lemma above can be easily deduced from Lemma 1 in [25] and the second statement is the Lemma 1 in [16].

When s is odd and d is even, the value distribution of the exponential sum $T(\alpha,\beta,\gamma)$ is determined in [25] which is given in Table 1.

Table 1: Value Distribution of $T(\alpha,\beta,\gamma)$

Value	Frequency
p^m	1
$\pm p^{\frac{m}{2}}$	$n_0/2=(p^m-1)(p^{2m+6d}+p^{2m+d}+p^{2m}+p^{m+6d}+p^{6d}-p^{2m+5d}$ $-p^{2m+4d}-p^{m+5d}-p^{m+3d}-p^{m+2d})/2(p^{2d}-1)^2(p^{2d}+1)$
$\pm p^{\frac{m+d}{2}}$	$n_{\pm1,1}=\frac{(p^{m+d}\pm p^{\frac{m+3d}{2}})(p^{2m}-p^{2m-2d}-p^{2m-3d}+p^{m-2d}+p^{m-3d}-1)}{2(p^{2d}-1)}$
$\pm p^{\frac{m+2d}{2}}$	$n_2/2=(p^m-1)(p^{2m+d}+p^{m+d}+p^m+p^{m-d}-p^{2m-d}$ $-p^{2m-2d}-p^{m+2d}-p^{2d})/2(p^{2d}-1)^2$
$\pm p^{\frac{m+3d}{2}}$	$n_{\pm1,3}=\frac{(p^{m-3d}\pm p^{\frac{m-3d}{2}})(p^{m-d}-1)(p^m-1)}{2(p^{2d}-1)}$
$\pm p^{\frac{m+4d}{2}}$	$n_4/2=\frac{(p^m-1)(p^{2m-4d}-p^{m-d}-p^{m-3d}+1)}{2(p^{2d}-1)^2(p^{2d}+1)}$

Moreover, we have the following result.

Lemma 2.5 ([25, 26]) *Following the notations above, we have*

(1) *for any* $(\alpha,\beta,\gamma)\in\mathbb{F}_{p^m}^3\backslash\{(0,0,0)\}$, $rank(H_{\alpha,\beta,\gamma})$ *is at least* $s-4$.

(2) *Let* n_i *be the number of* $(\alpha,\beta,\gamma)\in\mathbb{F}_{p^m}^3$ *such that* $rank(H_{\alpha,\beta,\gamma})=s-i$ *for* $0\le i\le 4$. *Then*

$$\begin{aligned}
n_0=&(p^m-1)(p^{2m+6d}+p^{2m+d}+p^{2m}+p^{m+6d}+p^{6d}-p^{2m+5d}\\
&-p^{2m+4d}-p^{m+5d}-p^{m+3d}-p^{m+2d})/(p^{2d}-1)^2(p^{2d}+1),\\
n_1=&\frac{p^{m+d}(p^{2m}-p^{2m-2d}-p^{2m-3d}+p^{m-2d}+p^{m-3d}-1)}{p^{2d}-1},\\
n_2=&\frac{(p^m-1)(p^{2m+d}+p^{m+d}+p^m+p^{m-d}-p^{2m-d}-p^{2m-2d}-p^{m+2d}-p^{2d})}{(p^{2d}-1)^2},\\
n_3=&\frac{p^{m-3d}(p^{m-d}-1)(p^m-1)}{p^{2d}-1},\\
n_4=&\frac{(p^m-1)(p^{2m-4d}-p^{m-d}-p^{m-3d}+1)}{(p^{2d}-1)^2(p^{2d}+1)}.
\end{aligned}$$

3 Affine-invariant codes and their supporting designs

In this section, we first determine the weight distribution of $\overline{\mathcal{C}}^{\perp}$. And then we obtain the parameters of their supporting 2-designs. To do this, we need the following lemmas. For any $x=\sum_{i=1}^{s}x_iv_i, y=\sum_{i=1}^{s}y_iv_i\in\mathbb{F}_q$, let $X=(x_1,x_2,\cdots,x_s), Y=(y_1,y_2,\cdots,y_s)\in\mathbb{F}_{q_0}^s$.

$$F_{\alpha,\beta,\gamma}(X+Y)-F_{\alpha,\beta,\gamma}(X)-F_{\alpha,\beta,\gamma}(Y)=2XH_{\alpha,\beta,\gamma}Y^T$$

is equal to

$$\begin{aligned}
&Q_{\alpha,\beta,\gamma}(x+y)-Q_{\alpha,\beta,\gamma}(x)-Q_{\alpha,\beta,\gamma}(y)\\
=&Tr_d^m(y^{p^{4k}}(\alpha^{p^{4k}}x^{p^{8k}}+\beta^{p^{4k}}x^{p^{6k}}+2\gamma^{p^{4k}}x^{p^{4k}}+\beta^{p^{2k}}x^{p^{2k}}+\alpha x))\\
=&Tr_d^m(y^{p^{4k}}\phi_{\alpha,\beta,\gamma}(x)),
\end{aligned}$$

where

$$\phi_{\alpha,\beta,\gamma}(x)=\alpha^{p^{4k}}x^{p^{8k}}+\beta^{p^{4k}}x^{p^{6k}}+2\gamma^{p^{4k}}x^{p^{4k}}+\beta^{p^{2k}}x^{p^{2k}}+\alpha x.$$

For $\varepsilon=\pm1$ and $0\le i\le 4$, according to Table 1, we define

$$N_{\varepsilon,i}=\{(\alpha,\beta,\gamma)\in\mathbb{F}_{p^m}^3\backslash\{(0,0,0)\}\mid T(\alpha,\beta,\gamma)=\varepsilon p^{\frac{m+id}{2}}\}.$$

Lemma 3.1 *For any $a\in\mathbb{F}_p$ and $(\alpha,\beta,\gamma)\in N_{\varepsilon,i}$ with $\varepsilon=\pm1$, $0\le i\le 4$, the number of $\delta\in\mathbb{F}_q$ satisfying*

1) $\phi_{\alpha,\beta,\gamma}(x)=-\delta^{p^k}$ *is solvable (choose one solution, say x_0),*
2) $Tr_1^m(\alpha x_0^{p^{4k}+1}+\beta x_0^{p^{2k}+1}+\gamma x_0^2)=a$

is as

$$\begin{cases}p^{m-id-1}+\varepsilon(p-1)p^{\frac{m-id}{2}-1}, & if\ a=0,\\ p^{m-id-1}-\varepsilon p^{\frac{m-id}{2}-1}, & otherwise.\end{cases}$$

Proof. The proof is similar to that of Lemma 4 in [16]. For completeness, detailed proof is given here. For any fixed $(\alpha,\beta,\gamma,a)\in\mathbb{F}_q^3\times\mathbb{F}_p$, define $n(\alpha,\beta,\gamma,a)$ to be the number of $\delta\in\mathbb{F}_q$ satisfying 1) and 2). From Eq. (3), we know that $XH_{\alpha,\beta,\gamma}X^T=Tr_d^m(\alpha x^{p^{4k}+1}+\beta x^{p^{2k}+1}+\gamma x^2)$. From the discussion above, we have

$$\begin{aligned}
&2XH_{\alpha,\beta,\gamma}+A_\delta=0\\
&\Leftrightarrow 2XH_{\alpha,\beta,\gamma}Y^T+A_\delta Y^T=0,\ for\,all\,Y\in\mathbb{F}_{q_0}^s\\
&\Leftrightarrow Tr_d^m(y^{p^{4k}}\phi_{\alpha,\beta,\gamma}(x))+Tr_d^m(\delta y)=0,\ for\,all\,y\in\mathbb{F}_q\\
&\Leftrightarrow \phi_{\alpha,\beta,\gamma}(x)+\delta^{p^{4k}}=0.
\end{aligned}$$

Let x_0 and x_0' be two distinct solutions of (1) (if exists). We can get $x_0=X_0\cdot V^T$ and $x_0'=X_0'\cdot V^T$ with $X_0,X_0'\in\mathbb{F}_{q_0}^s$ and $V=(v_1,v_2,\cdots,v_s)$. Define $\triangle X_0=X_0'-X_0$ and $\triangle x_0=x_0'-x_0=\triangle X_0\cdot V^T$. Then

$$\phi_{\alpha,\beta,\gamma}(x_0)+\delta^{p^{4k}}=\phi_{\alpha,\beta,\gamma}(x_0')+\delta^{p^{4k}}=0$$

gives

$$2X_0H_{\alpha,\beta,\gamma}+A_\delta=2X_0'H_{\alpha,\beta,\gamma}+A_\delta=0$$

and hence

$$\triangle X_0\cdot H_{\alpha,\beta,\gamma}=0.$$

It follows that

$$\begin{aligned}
&X_0' H_{\alpha,\beta,\gamma} X_0'^T \\
=&(X_0 + \triangle X_0) H_{\alpha,\beta,\gamma} (X_0 + \triangle X_0)^T \\
=&X_0 H_{\alpha,\beta,\gamma} X_0^T + \triangle X_0 \cdot H_{\alpha,\beta,\gamma} (X_0 + \triangle X_0)^T + X_0 H_{\alpha,\beta,\gamma} \cdot \triangle X_0^T \\
=&X_0 H_{\alpha,\beta,\gamma} X_0^T + \triangle X_0 \cdot H_{\alpha,\beta,\gamma} (2X_0 + \triangle X_0)^T \\
=&X_0 H_{\alpha,\beta,\gamma} X_0^T.
\end{aligned}$$

Therefore

$$\begin{aligned}
&Tr_1^m(\alpha x_0'^{p^{4k}+1} + \beta x_0'^{p^{2k}+1} + \gamma x_0'^2) \\
=&Tr_1^d(Tr_d^m(\alpha x_0'^{p^{4k}+1} + \beta x_0'^{p^{2k}+1} + \gamma x_0'^2)) \\
=&Tr_1^d(X_0' H_{\alpha,\beta,\gamma} X_0'^T) \\
=&Tr_1^d(X_0 H_{\alpha,\beta,\gamma} X_0^T) \\
=&Tr_1^d(Tr_d^m(\alpha x_0^{p^{4k}+1} + \beta x_0^{p^{2k}+1} + \gamma x_0^2)) \\
=&Tr_1^m(\alpha x_0^{p^{4k}+1} + \beta x_0^{p^{2k}+1} + \gamma x_0^2).
\end{aligned}$$

Hence, $n(\alpha, \beta, \gamma, a)$ is well defined (independent of the choice of x_0).

If 1) is satisfied, that is, $\phi_{\alpha,\beta,\gamma}(x) + \delta^{p^{4k}} = 0$ has solution(s) in $\mathbb{F}_q$ which yields that $2XH_{\alpha,\beta,\gamma} + A_\delta = 0$ has solution(s). Note that $rank(H_{\alpha,\beta,\gamma}) = s - i$. Therefore, $2XH_{\alpha,\beta,\gamma} + A_\delta = 0$ has $q_0^i = p^{id}$ solutions with $X \in \mathbb{F}_{q_0}^s$, which is equivalent to $\phi_{\alpha,\beta,\gamma}(x) + \delta^{p^{4k}} = 0$ has p^{id} solution(s) in $\mathbb{F}_q$. Conversely, for any $x_0 \in \mathbb{F}_q$, we can determine δ by $\delta = -(\phi_{\alpha,\beta,\gamma}(x_0))^{p^{m-4k}}$. Let $N(\alpha, \beta, \gamma, a)$ be the number of x_0 satisfying 2). Then we have $n(\alpha, \beta, \gamma, a) = N(\alpha, \beta, \gamma, a)/p^{id}$.

For any $\lambda \in \mathbb{F}_{q_0}^*$ and $(\alpha, \beta, \gamma) \in N_i$, by Eq. (3), we have $F_{\lambda\alpha,\lambda\beta,\lambda\gamma}(X) = \lambda \cdot F_{\alpha,\beta,\gamma}(X)$ and $rank(H_{\lambda\alpha,\lambda\beta,\lambda\gamma}) = rank(H_{\alpha,\beta,\gamma}) = s - i$. From Lemma 2.4, we know that

$$T(\lambda\alpha, \lambda\beta, \lambda\gamma) = \sum_{X \in \mathbb{F}_{q_0}^s} \zeta_p^{Tr_1^d(XH_{\lambda\alpha,\lambda\beta,\lambda\gamma}X^T)} = \eta_0(\lambda)^{s-i} T(\alpha, \beta, \gamma). \tag{4}$$

Then by the definition of $N(\alpha,\beta,\gamma,a)$, we have

$$\begin{aligned}
N(\alpha,\beta,\gamma,a) &= \frac{1}{p}\sum_{x\in\mathbb{F}_q}\sum_{\lambda\in\mathbb{F}_p}\zeta_p^{\lambda Tr_1^m(\alpha x^{p^{4k}+1}+\beta x^{p^{2k}+1}+\gamma x^2-a)}\\
&= p^{m-1}+\frac{1}{p}\sum_{\lambda\in\mathbb{F}_p^*}\zeta_p^{-\lambda a}\sum_{x\in\mathbb{F}_q}\zeta_p^{Tr_1^m(\lambda\alpha x^{p^{4k}+1}+\lambda\beta x^{p^{2k}+1}+\lambda\gamma x^2)}\\
&= p^{m-1}+\frac{1}{p}\sum_{\lambda\in\mathbb{F}_p^*}\zeta_p^{-\lambda a}T(\lambda\alpha,\lambda\beta,\lambda\gamma)\\
&= p^{m-1}+\frac{1}{p}T(\alpha,\beta,\gamma)\sum_{\lambda\in\mathbb{F}_p^*}\eta_0(\lambda)^{s-i}\zeta_p^{-\lambda a}\\
&= p^{m-1}+\frac{1}{p}T(\alpha,\beta,\gamma)\sum_{\lambda\in\mathbb{F}_p^*}\zeta_p^{-\lambda a}\\
&= \begin{cases} p^{m-1}+\frac{p-1}{p}T(\alpha,\beta,\gamma), & \text{if } a=0,\\ p^{m-1}-\frac{1}{p}T(\alpha,\beta,\gamma), & \text{otherwise.}\end{cases}
\end{aligned}$$

where the fourth equality holds from (4) for any $\lambda\in\mathbb{F}_p^*$ and the fifth equality holds since d is even. The proof is completed by substituting the value of $T(\alpha,\beta,\gamma)$ into the equality above. ■

Remark. Define $\omega=\#\{(\alpha,\beta,\gamma,\delta)\in\mathbb{F}_q^4|S(\alpha,\beta,\gamma,\delta)=0\}$. From Lemma 2.5 (1), we know that if $(\alpha,\beta,\gamma)\neq(0,0,0)$, then $rank(H_{\alpha,\beta,\gamma})=s-i$ for some $i\in\{0,1,2,3,4\}$. Moreover, $2XH_{0,0,0}+A_\delta=0$ is solvable if and only if $\delta=0$. Then

$$\omega=p^m-1+(p^m-p^{m-d})n_1+(p^m-p^{m-2d})n_2+(p^m-p^{m-3d})n_3+(p^m-p^{m-4d})n_4.$$

Furthermore, by Lemma 3.1, we can obtain the value distribution of $S(\alpha,\beta,\gamma,\delta)$ for $i\in\{0,1,2,3,4\}$, $\varepsilon=\pm1$ and $j\in\mathbb{F}_p^*$ as in Table 2.

Table 2: Value Distribution of $S(\alpha,\beta,\gamma,\delta)$

Value	Frequency
0	ω
p^m	1
$\varepsilon p^{\frac{m+id}{2}}$	$p^{m-id-1}+\varepsilon(p-1)p^{\frac{m-id}{2}-1}$
$\varepsilon\zeta_p^j p^{\frac{m+id}{2}}$	$p^{m-id-1}-\varepsilon p^{\frac{m-id}{2}-1}$

Based on the discussion above, we will determine the weight distribution of $\overline{\mathcal{C}}^\perp$ in the following.

Theorem 3.2 *Let m and k be two positive even integers such that $m/\gcd(m,k)\geq 5$ is odd. Then $\overline{\mathcal{C}}^\perp$ is a linear code over $\mathbb{F}_p$ with length p^m and dimension $4m+1$. Furthermore, the weight distribution of it is given in Table 3.*

Table 3: Weight distribution of $\overline{\mathcal{C}}^{\perp}$

Weight (i)	Frequency (A_i)
0	1
p^m	$p-1$
$p^{m-1}(p-1)$	$p\omega$
$(p-1)(p^{\frac{m}{2}}-1)p^{\frac{m}{2}-1}$	$p^m n_{1,0}$
$(p-1)(p^{\frac{m}{2}}+1)p^{\frac{m}{2}-1}$	$p^m n_{-1,0}$
$(p-1)p^{m-1} \pm p^{\frac{m}{2}-1}$	$(p-1)p^m n_{\pm 1,0}$
$(p-1)(p^{\frac{m-d}{2}}-1)p^{\frac{m+d}{2}-1}$	$p^{m-d} n_{1,1}$
$(p-1)(p^{\frac{m-d}{2}}+1)p^{\frac{m+d}{2}-1}$	$p^{m-d} n_{-1,1}$
$(p-1)p^{m-1} \pm p^{\frac{m+d}{2}-1}$	$(p-1)p^{m-d} n_{\pm 1,1}$
$(p-1)(p^{\frac{m-2d}{2}}-1)p^{\frac{m+2d}{2}-1}$	$p^{m-2d} n_{1,2}$
$(p-1)(p^{\frac{m-2d}{2}}+1)p^{\frac{m+2d}{2}-1}$	$p^{m-2d} n_{-1,2}$
$(p-1)p^{m-1} \pm p^{\frac{m+2d}{2}-1}$	$(p-1)p^{m-2d} n_{\pm 1,2}$
$(p-1)(p^{\frac{m-3d}{2}}-1)p^{\frac{m+3d}{2}-1}$	$p^{m-3d} n_{1,3}$
$(p-1)(p^{\frac{m-3d}{2}}+1)p^{\frac{m+3d}{2}-1}$	$p^{m-3d} n_{-1,3}$
$(p-1)p^{m-1} \pm p^{\frac{m+3d}{2}-1}$	$(p-1)p^{m-3d} n_{\pm 1,3}$
$(p-1)(p^{\frac{m-4d}{2}}-1)p^{\frac{m+4d}{2}-1}$	$p^{m-4d} n_{1,4}$
$(p-1)(p^{\frac{m-4d}{2}}+1)p^{\frac{m+4d}{2}-1}$	$p^{m-4d} n_{-1,4}$
$(p-1)p^{m-1} \pm p^{\frac{m+4d}{2}-1}$	$(p-1)p^{m-4d} n_{\pm 1,4}$

Proof. It is easy to obtain the length and dimension from the discussion above. By Eq. (2), for each nonzero codeword $\mathbf{c}_{(\alpha,\beta,\gamma,\delta,h)} = (c_0, c_1, \ldots, c_{p^m-1})$ in $\overline{\mathcal{C}}^{\perp}$, the weight of it is

$$w(\mathbf{c}_{(\alpha,\beta,\gamma,\delta,h)}) = p^m - I(\alpha,\beta,\gamma,\delta,h), \tag{5}$$

where

$$\begin{aligned} I(\alpha,\beta,\gamma,\delta,h) &= \frac{1}{p}\sum_{i=0}^{p^m-1}\sum_{y\in\mathbb{F}_p}\zeta_p^{yc_i} \\ &= \frac{1}{p}\sum_{y\in\mathbb{F}_p}\sum_{x\in\mathbb{F}_{p^m}}\zeta_p^{y\cdot Tr(\alpha x^{p^{4k}+1}+\beta x^{p^{2k}+1}+\gamma x^2+\delta x+h)} \\ &= \frac{1}{p}\sum_{y\in\mathbb{F}_p}\zeta_p^{yh}\sum_{x\in\mathbb{F}_{p^m}}\zeta_p^{y\cdot Tr(\alpha x^{p^{4k}+1}+\beta x^{p^{2k}+1}+\gamma x^2+\delta x)} \\ &= p^{m-1} + \frac{1}{p}\sum_{y\in\mathbb{F}_p^*}\zeta_p^{yh}\sigma_y(S(\alpha,\beta,\gamma,\delta)). \end{aligned} \tag{6}$$

Then by Table 2, we have

$$\sigma_y(S(\alpha,\beta,\gamma,\delta)) = \begin{cases} S(\alpha,\beta,\gamma,\delta), & \text{if } S(\alpha,\beta,\gamma,\delta) \in \{0, p^m, \varepsilon p^{\frac{m+id}{2}}\} \ for\ i \in \{0,1,2,3,4\}; \\ \varepsilon\zeta_p^{yj} p^{\frac{m+id}{2}}, & \text{if } S(\alpha,\beta,\gamma,\delta) = \varepsilon\zeta_p^{j} p^{\frac{m+id}{2}} \ for\ i \in \{0,1,2,3,4\}. \end{cases}$$

Then by Eq. (6), we obtain Table 4 which describes the values of $I(\alpha,\beta,\gamma,\delta,h)$ and the corresponding conditions. Consequently, by Eq. (5) and Table 4, we have the weight

Table 4: Value of $I(\alpha,\beta,\gamma,\delta,h)$, $j \in \mathbb{F}_p$

Value	Corresponding Condition
0	$S(\alpha,\beta,\gamma,\delta) = p^m, h = 0$
p^m	$S(\alpha,\beta,\gamma,\delta) = p^m, h \neq 0$
p^{m-1}	$S(\alpha,\beta,\gamma,\delta) = 0$
$p^{m-1} - \varepsilon p^{\frac{m+id}{2}-1}$	$S(\alpha,\beta,\gamma,\delta) = \varepsilon\zeta_p^j p^{\frac{m+id}{2}}, h + j \neq 0$
$p^{m-1} + \varepsilon p^{\frac{m+id}{2}-1}(p-1)$	$S(\alpha,\beta,\gamma,\delta) = \varepsilon\zeta_p^j p^{\frac{m+id}{2}}, h + j = 0$

distribution of $\overline{\mathcal{C}}^{\perp}$ in Table 3.■

Since $\overline{\mathcal{C}}^{\perp}$ is affine-invariant, then by Lemma 2.1, we have the following theorem.

Theorem 3.3 *Let m and k be two positive even integers such that $m/\gcd(m,k) > 5$ is odd. Then the supports of codewords with weight $i > 0$ in $\overline{\mathcal{C}}^{\perp}$ form a 2-design, provided that $A_i \neq 0$.*

The parameters of the 2-designs will be determined in the following theorem.

Theorem 3.4 *Let m and k be two positive even integers such that $s \geq 5$ is odd where $s = m/\gcd(m,k)$. Let $\mathcal{B}_i$ be the set of the supports of the codewords in $\overline{\mathcal{C}}^{\perp}$ with weight $1 \leq i \leq p^m$, where $A_i \neq 0$. Then $\overline{\mathcal{C}}^{\perp}$ gives 2-(p^m, i, λ_i) designs provided that $A_i \neq 0$ if $d > 2$ or $s > 5$, where $d = \gcd(m,k)$ and $\lambda_i = \frac{A_i\binom{i}{2}}{(p-1)\binom{p^m}{2}}$.*

Proof. From Table 3, the minimum and maximum weight of $\overline{\mathcal{C}}^{\perp}$ are $(p-1)(p^{m-1} - p^{\frac{m+4d}{2}-1})$ and p^m, respectively. In the following, we consider the condition of Lemma 2.2.

$$\begin{aligned}
&\lfloor\frac{p^m+p-2}{p-1}\rfloor - p^m + (p-1)(p^{m-1} - p^{\frac{m+4d}{2}-1}) \\
=&\frac{p^m+p-2}{p-1} - p^{m-1} - p^{\frac{m+4d}{2}} + p^{\frac{m+4d}{2}-1} \\
=&\frac{p^{m-1} - p^{\frac{m+4d}{2}+1} + p^{\frac{m+4d}{2}} + p - 2}{p-1} + p^{\frac{m+4d}{2}-1} \\
=&\frac{p^{\frac{m+4d}{2}+1}(p^{\frac{d}{2}(s-4)-2} - 1) + p^{\frac{m+4d}{2}} + p - 2}{p-1} + p^{\frac{m+4d}{2}-1}
\end{aligned}$$

is positive when $s > 5$ or $d > 2$. Therefore, the number of different supports of all codewords with weight $1 \leq i \leq p^m$ is equal to $\frac{A_i}{p-1}$ by Lemma 2.2, where A_i is the frequency described in Table 3. Then the conclusion follows from the theorem above and Eq. (1). ■

Remark. As shown above, the parameters of the 2-designs are completely determined by the weight distribution of $\overline{\mathcal{C}}^{\perp}$. Since the weight distribution are different from that of the codes in the references regarding the similar problem, the 2-designs constructed in the paper have new parameters.

4 Conslusion

In this paper, we gave a coding theoretical construction of infinite families of 2-designs. Since the parameters of these 2-designs depend on the weight distributions of $\overline{\mathcal{C}}^{\perp}$, we first investigate the weight distribution based on the value distribution of certain exponential sum obtained in [25] and then obtain the parameters of their supporting 2-designs. The reader is invited to consider the t-designs derived from its dual $\overline{\mathcal{C}}$ and whether t-designs for $t > 2$ can be constructed from these linear codes by Assmus-Mattson theorem or other methods.

Acknowledgements The authors are very grateful to the three anonymous reviewers for their comments which improved the presentation and quality of this paper.

References

[1] E. F. Assmus Jr., J. D. Key, Designs and their codes, Cambridge: Cambridge University Press, 1992.

[2] E. F. Assmus Jr., H. F. Mattson Jr., New 5-designs, J. Comb. Theory, 6, 1969, 122-151.

[3] P. Delsarte, On subfield subcodes of modified Reed-Solomon codes, IEEE Trans. Inf. Theory, 21(5), 1975, 575-576.

[4] C. Ding, Codes from difference sets, World Scientific, Singapore, 2015.

[5] C. Ding, Designs from linear codes, World Scientific, 2018.

[6] C. Ding, An infinite family of Steiner systems S(2, 4, 2^m) from cyclic codes, J. Comb. Des., 26(3), 2018, 127-144.

[7] C. Ding, Infinite families of 3-designs from a type of five-weight code, Des. Codes Cryptogr., 86(3), 2018, 703-719.

[8] C. Ding, C. Li, Infinite families of 2-designs and 3-designs from linear codes, Discrete Math., 40(10), 2017, 2415-2431.

[9] C. Ding, C. Tang, Infinite families of near MDS codes holding t-designs, arXiv: 1010.08265.

[10] C. Ding, Z. Zhou, Parameters of 2-designs from some BCH codes, Codes, Cryptography and Information Security, Lecture Notes in Computer Science, Vol. 10194, S. El Hajji, A. Nitaj, and E. M. Souidi (Editors), Springer, Heidelberg, 2017, 110-127.

[11] X. Du, R. Wang, C. Tang, Infinite families of 2-designs from two classes of linear codes, arXiv: 1903.07459.

[12] X. Du, R. Wang, C. Tang, Q. Wang, Infinite families of 2-designs from linear codes, Appl. Algebr. Eng. Comm., 2020, DOI: 10.1007/s00200-020-00438-8.

[13] X. Du, R. Wang, C. Fan, Infinite families of 2-designs from a class of cyclic codes, J. Comb. Des., 26(3), 2019, 1-14.

[14] T. Kasami, S. Lin, W. Peterson, Some results on cyclic codes which are invariant under the affine group and their applications, Inform Control, 11, 1968, 475-496.

[15] R. Lidl, H. Niederreiter, Finite fieds, Addison-Wdsley Publishing Inc., 1983.

[16] J. Luo, K. Feng, On the weight distribution of two classes of cyclic codes, IEEE Trans. Inf. Theory, 54(12), 2008, 5332-5344.

[17] K. Ireland, M. Rosen, A classical introduction to modern number theory, Springer, 1990.

[18] C. Tang, C. Ding, An infinite family of linear codes supporting 4-designs, arXiv: 2001.00158.

[19] C. Tang, C. Ding, M. Xiong, Steiner systems $S(2, 4, \frac{3m-1}{2})$ and 2-designs from ternary linear codes of length $\frac{3m-1}{2}$, Des. Codes Crypogr., 87(12), 2019, 2793-2811.

[20] C. Tang, C. Ding, M. Xiong, Codes, differentially δ-uniform functions and t-designs, IEEE Trans. Inf. Theory, 66(6), 2020, 3691-3703.

[21] V.D. Tonchev, Codes and designs, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, Vol. II, Elsevier, Amsterdam, 1998, 1229-1268.

[22] V.D. Tonchev, Codes, in: C.J. Colbourn, J.H. Dinitz (Eds.), Handbook of Combinatorial Designs, second edition, CRC Press, New York, 2007, 677-701.

[23] R. Wang, X. Du, C. Fan, Infinite families of 2-designs from a class of non-binary Kasami cyclic codes, arXiv: 1912.04745.

[24] G. Xu, X. Cao, S. Xu, Optimal p-ary cyclic codes with minimum distance four from monomials, Cryptography and Communications, 8(4), 2016, 541-554.

[25] D. Zheng, X. Wang, X. Zeng, L. Hu, The weight distribution of a family of p-ary cyclic codes, Des. Codes Crypogr., 75(2), 2013, 263-275.

[26] Z. Zhou, C. Ding, J. Luo, A. Zhang, A family of five-weight cyclic codes and their weight enumerators, IEEE Trans. Inf. Theory, 59(10), 2013, 6674-6682.