An infinite family of antiprimitive cyclic codes supporting Steiner systems $S(3,8,7^m+1)$

Can Xiang , Chunming Tang and Qi Liu

arXiv:2110.03881v1 [cs.IT] 8 Oct 2021

Abstract

Coding theory and combinatorial t-designs have close connections and interesting interplay. One of the major approaches to the construction of combinatorial t-designs is the employment of error-correcting codes. As we all known, some t-designs have been constructed with this approach by using certain linear codes in recent years. However, only a few infinite families of cyclic codes holding an infinite family of 3-designs are reported in the literature. The objective of this paper is to study an infinite family of cyclic codes and determine their parameters. By the parameters of these codes and their dual, some infinite family of 3-designs are presented and their parameters are also explicitly determined. In particular, the complements of the supports of the minimum weight codewords in the studied cyclic code form a Steiner system. Furthermore, we show that the infinite family of cyclic codes admit 3-transitive automorphism groups.

Index Terms

Linear codes, cyclic codes, combinatorial designs, automorphism groups, Steiner system

I. Introduction

Let GF(q) be a finite field with q elements, where $q=p^m$ with m being a positive integer and p being an prime number. An $[v,k,d]$ linear code $\mathcal{C}$ over GF(q) is a k-dimensional subspace of GF$(q)^v$ with minimum (Hamming) distance d. An $[v,k,d]$ linear code $\mathcal{C}$ is said to be *cyclic* if $(c_0,c_1,\cdots,c_{v-1})\in\mathcal{C}$ implies $(c_{v-1},c_0,c_1,\cdots,c_{v-2})\in\mathcal{C}$.

Let $\mathcal{C}$ be an $[v,k,d]$ cyclic code over GF(q). If $v=q^m-1$ (resp. $v=q^m+1$), the cyclic code $\mathcal{C}$ is called primitive (resp. antiprimitive). If we identify a vector $(c_0,c_1,\cdots,c_{v-1})\in \mathrm{GF}(q)^v$ with the following polynomial

$$\sum_{i=0}^{v-1} c_i x^i \in \mathrm{GF}(q)[x]/(x^v-1),$$

then any cyclic code $\mathcal{C}$ of length v over GF(q) is an ideal of the quotient ring GF$(q)[x]/(x^v-1)$. It is notice that the ring GF$(q)[x]/(x^v-1)$ is a principal ideal ring. Thus, for any cyclic code $\mathcal{C}$ of length v over GF(q), there exists an unique monic divisor $g(x)$ of x^v-1 of the smallest degree such that $\mathcal{C}=\langle g(x)\rangle$. This polynomial $g(x)$ is called the *generator polynomial,* and $h(x)=(x^v-1)/g(x)$ is called the *check* polynomial of $\mathcal{C}$. It is obvious that $k=v-deg(g(x))$ and $\{g(x),xg(x),\cdots,x^{k-1}g(x)\}$ is a basis of $\mathcal{C}$. It is well known that a cyclic code is a special linear code. Although the error correcting capability of cyclic codes may not be as good as some other linear codes in general, cyclic codes have wide applications in storage and communication systems as they have efficient encoding and decoding algorithms [1], [2], [3].

The research of C. Xiang was supported by the Basic Research Project of Science and Technology Plan of Guangzhou city of China under grant number 202102020888 and the National Natural Science Foundation of China under grant number 12171162. The research of C. Tang was supported by National Natural Science Foundation of China under grant number 11871058 and China West Normal University (14E013, CXTD2014-4 and the Meritocracy Research Funds).

C. Xiang is with the College of Mathematics and Informatics, South China Agricultural University, Guangzhou, Guangdong 510642, China (email:cxiangcxiang@hotmail.com).

C. Tang is with School of Mathematics and Information, China West Normal University, Nanchong, Sichuan 637002, China (email: tangchunmingmath@163.com).

Q. Liu is with School of Mathematics and Information, China West Normal University, Nanchong, Sichuan 637002, China (email: liuqijichushuxue@163.com).

Thus, cyclic codes have been attracted much attention in coding theory and a lot of progress has been made (see, for example, [4], [5], [6], [8], [9], [26], [27]).

It is known that linear codes and t-designs are closely related. A t-design can be induced to a linear code (see, for example, [12], [13]). Meanwhile, a linear code $\mathcal{C}$ may induce a t-design under certain conditions. As far as we know, a lot of 2-designs and 3-designs have been constructed from some special linear codes (see, for example, [10], [14], [15], [19], [21]). Recently, an infinity family of linear codes holding 4-designs was settled by Tang and Ding in [23]. It remains open if there is an infinite family of linear codes holding 5-designs. In fact, only a few infinite families of cyclic codes holding an infinite family of 3-designs are reported in the literature. Motivated by this fact, we will consider a class of cyclic codes

$$\mathcal{C}_m = \{(\mathrm{Tr}(au^4 + bu^3))_{u \in U_{q+1}} : a, b \in \mathrm{GF}(q^2)\} \tag{1}$$

over $\mathrm{GF}(q)$ and its dual, where $q = 7^m$ with $m \geq 2$ being a integer, Tr is the trace function from $\mathrm{GF}(q^2)$ to $\mathrm{GF}(q)$ and U_{q+1} is the set of all $(q+1)$-th roots of unity in $\mathrm{GF}(q^2)$, and prove that these codes hold 3-designs. Specifically, the cyclic code $\mathcal{C}_m$ and its dual $\mathcal{C}_m^{\perp}$ admit 3-transitive automorphism groups and the complement of the supports of the minimum weight codewords in $\mathcal{C}_m$ forms a steiner system $S(3, 8, 7^m + 1)$.

The remainder of this paper is arranged as follows. Section II introduces some notation and basics of linear codes and combinatorial t-designs. Section III determines the parameters of the cyclic code $\mathcal{C}_m$ and its dual, and induces some infinite families of 3-designs. Section IV concludes this paper.

II. Preliminaries

As a special linear code, cyclic codes have all properties of linear codes. In order to study cyclic codes in this paper, we need briefly introduce some known results on linear codes and combinatorial t-designs in this section, which will be used later. For convenience, we begin this section by fixing the following notations unless otherwise stated in this paper.

- p is a prime and $q = p^m$ with m being a positive integer.
- $\mathrm{GF}(q)$ is a finite field with q elements and $\mathrm{GF}(q)^* = \mathrm{GF}(q) \setminus \{0\}$.
- Tr is the trace function from $\mathrm{GF}(q^2)$ to $\mathrm{GF}(q)$.
- U_{q+1} is the set of all $(q+1)$-th roots of unity in $\mathrm{GF}(q^2)$.
- $\binom{S}{k}$ is defined as the set consisting of all k-subsets of the set S if S is a set, and the binomial coefficient otherwise.
- $\mathrm{PGL}(2, q)$ is defined as the group of invertible 2×2 matrices with entries in $\mathrm{GF}(q)$, modulo the scalar matrices $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$, where $a \in \mathrm{GF}(q)^*$.

A. Weight enumerators of linear codes

Let $\mathcal{C}$ be a $[v, k, d]$ linear code over $\mathrm{GF}(q)$. Let A_i denote the number of codewords with Hamming weight i in a code $\mathcal{C}$ for all $0 \leq i \leq v$. The weight enumerator of $\mathcal{C}$ is defined by

$$1 + A_1 z + A_2 z^2 + \cdots + A_v z^v.$$

The sequence $(1, A_1, \ldots, A_v)$ is called the weight distribution of $\mathcal{C}$. A code $\mathcal{C}$ is said to be a t-weight code if the number of nonzero A_i in the sequence $(A_1, A_2, \cdots, A_v)$ is equal to t. A code $\mathcal{C}$ is said to be optimal if its parameters meet certain bounds on linear codes. Denote the dual of $\mathcal{C}$ by $\mathcal{C}^{\perp}$, the minimum distance of $\mathcal{C}^{\perp}$ by $d^{\perp}$ and the weight distribution of $\mathcal{C}^{\perp}$ by $(A_0^{\perp}, A_1^{\perp}, \cdots, A_v^{\perp})$. In order to determine the weight enumerator of $\mathcal{C}$, we will need the *Pless power moments* [20]. The first four Pless power moments identities are given by

$$\begin{aligned}
&\sum_{i=0}^{\nu} A_i = q^k, \\
&\sum_{i=0}^{\nu} i \cdot A_i = q^{k-1}(qv - v - A_1^{\perp}), \\
&\sum_{i=0}^{\nu} i^2 \cdot A_i = q^{k-2}\left[(q-1)v(qv - v + 1) - (2qv - q - 2v + 2)A_1^{\perp} + 2A_2^{\perp}\right], \\
&\sum_{i=0}^{\nu} i^3 \cdot A_i = q^{k-3}((q-1)v(q^2v^2 - 2qv^2 + 3qv - q + v^2 - 3v + 2) \\
&\qquad - (3q^2v^2 - 3q^2v - 6qv^2 + 12qv + q^2 - 6q + 3v^2 - 9v + 6)A_1^{\perp} \\
&\qquad + 6(qv - q - v + 2)A_2^{\perp} - 6A_3^{\perp}).
\end{aligned} \tag{2}$$

B. Automorphism groups of linear codes

Let $\mathcal{C}$ be a $[v, k, d]$ linear code over $\mathrm{GF}(q)$. We denote the set of coordinate positions of codewords of $\mathcal{C}$ by $\mathcal{P}$. Then every codeword $\mathbf{c}$ of $\mathcal{C}$ can be written as $\mathbf{c} = (c_x)_{x\in\mathcal{P}}$. The set of coordinate permutations g that map a code $\mathcal{C}$ to itself forms a group, i.e.,

$$\{g|\ g(c_x)_{x\in\mathcal{P}} = (c_{g^{-1}(x)})_{x\in\mathcal{P}} \in \mathcal{C} \text{ for all } (c_x)_{x\in\mathcal{P}} \in \mathcal{C}\}$$

which called the permutation automorphism group of $\mathcal{C}$ and denoted by $\mathrm{PAut}(\mathcal{C})$. We denote the symmetric group on the set $\mathcal{P}$ by $\mathrm{Sym}(\mathcal{P})$. It is clear that $\mathrm{PAut}(\mathcal{C})$ is the subgroup of $\mathrm{Sym}(\mathcal{P})$ which keeps its invariance of the code C. Define a subgroup of $(\mathrm{GF}(q)^*)^v \rtimes \mathrm{Sym}(\mathcal{P})$ as follows:

$$\{((a_x)_{x\in\mathcal{P}}; g)|\ ((a_x)_{x\in\mathcal{P}}; g)\,(c_x)_{x\in\mathcal{P}} = (a_x c_{g^{-1}(x)})_{x\in\mathcal{P}} \in \mathcal{C} \text{ for all } (c_x)_{x\in\mathcal{P}} \in \mathcal{C}\} \tag{3}$$

where $((a_x)_{x\in\mathcal{P}}; g)$ is a map which maps the code $\mathcal{C}$ to itself. This subgroup is called the monomial automorphism group of $\mathcal{C}$ and denoted by $\mathrm{MAut}(\mathcal{C})$. Let $\mathrm{Gal}(\mathrm{GF}(q))$ be the Galois group of $\mathrm{GF}(q)$ over its prime field. Then the automorphism group $\mathrm{Aut}(\mathcal{C})$ of $\mathcal{C}$ is the subgroup of $(\mathrm{GF}(q)^*)^v \rtimes (\mathrm{Sym}(\mathcal{P}) \times \mathrm{Gal}(\mathrm{GF}(q)))$ as follows:

$$\{((a_x)_{x\in\mathcal{P}}; g, \gamma)|:\ \ ((a_x)_{x\in\mathcal{P}}; g, \gamma)\,(c_x)_{x\in\mathcal{P}} = (a_x \gamma(c_{g^{-1}(x)}))_{x\in\mathcal{P}} \in \mathcal{C} \text{ for all } (c_x)_{x\in\mathcal{P}} \in \mathcal{C}\}$$

where $((a_x)_{x\in\mathcal{P}}; g, \gamma)$ is a map which maps the code $\mathcal{C}$ to itself. It is notice that $\mathrm{PAut}(\mathcal{C}) \subseteq \mathrm{MAut}(\mathcal{C}) \subseteq \mathrm{Aut}(\mathcal{C})$. When q is a prime, $\mathrm{MAut}(\mathcal{C}) = \mathrm{Aut}(\mathcal{C})$. Specifically, $\mathrm{PAut}(\mathcal{C}) = \mathrm{MAut}(\mathcal{C}) = \mathrm{Aut}(\mathcal{C})$ if $\mathcal{C}$ is binary code.

We say that $\mathrm{Aut}(\mathcal{C})$ is *t-homogeneous* (resp. *t-transitive*) if for every pair of t-element sets of coordinates (resp. t-element ordered sets of coordinates), there is an element $((a_x)_{x\in\mathcal{P}}; g, \gamma) \in \mathrm{Aut}(\mathcal{C})$ such that its permutation part g sends the first set to the second set.

C. Combinatorial t-designs and some related results

Let k, t and v be positive integers with $1 \le t \le k \le v$. Let $\mathcal{P}$ be a set with v elements and $\mathcal{B}$ be a set of some k-subsets of $\mathcal{P}$. $\mathcal{B}$ is called the point set and $\mathcal{P}$ is called the block set in general. The incidence structure $\mathbb{D} = (\mathcal{P}, \mathcal{B})$ is called a *t-(v,k,λ) design* (or *t-design*) if every t-subset of $\mathcal{P}$ is contained in exactly λ blocks of $\mathcal{B}$. Let $\binom{\mathcal{P}}{k}$ denote the set consisting of all k-subsets of the point set $\mathcal{P}$. Then the incidence structure $(\mathcal{P}, \binom{\mathcal{P}}{k})$ is a k-$(v,k,1)$ design and is called a *complete design*. The special incidence structure $(\mathcal{P}, \emptyset)$ is called a t-$(v,k,0)$ trivial design for all t and k . A combinatorial t-design is said to be *simple* if its block set $\mathcal{B}$ does not have a repeated block. When $t \ge 2$ and $\lambda = 1$, a t-(v,k,λ) design is called a

Steiner system and denoted by $S(t,k,v)$. The parameters of a combinatorial t-(v,k,λ) design must satisfy the following equation:

$$b=\lambda\frac{\binom{v}{t}}{\binom{k}{t}} \tag{4}$$

where b is the cardinality of $\mathcal{B}$.

Linear codes and t-designs are closely related. A t-design $\mathbb{D}=(\mathcal{P},\mathcal{B})$ can be used to construct a linear code over GF(q) for any q as follows. Let $\mathcal{P}=\{q_1,\ldots,q_\nu\}$, $\mathcal{B}=\{B_1,\ldots,B_b\}$. The incidence matrix $M_{\mathbb{D}}:=[m_{ij}]$ of the design $\mathbb{D}=(\mathcal{P},\mathcal{B})$ is a $b\times v$ binary matrix whose entry $m_{ij}=1$ if the point q_j is on the block B_i and $m_{ij}=0$ otherwise. The incidence matrix $M_{\mathbb{D}}$ can be viewed as a matrix over $\mathrm{GF}(q)$ for any q. The *linear code* $\mathsf{C}_q(\mathbb{D})$ over the prime field $\mathrm{GF}(q)$ of the design $\mathbb{D}$ is defined to be the linear subspace of $\mathrm{GF}(q)^v$ spanned by the row vectors of the incidence matrix $M_{\mathbb{D}}$. Linear codes $\mathsf{C}_q(\mathbb{D})$ of designs $\mathbb{D}$ have been extensively investigated (see, for example, [13], [16], [17], [18]).

On the other hand, a linear code $\mathcal{C}$ may produce a t-design which is formed by supports of codewords of a fixed Hamming weight in $\mathcal{C}$. Let $\mathcal{P}(\mathcal{C})=\{0,1,2,\ldots,\nu-1\}$ be the set of the coordinates of codewords in $\mathcal{C}$, where ν is the length of the code $\mathcal{C}$. For a codeword $\mathbf{c}=(c_0,c_1,\ldots,c_{\nu-1})$ in $\mathcal{C}$, the *support* of $\mathbf{c}$ is defined by

$$\mathrm{Supp}(\mathbf{c})=\{i:c_i\neq 0, i\in\mathcal{P}(\mathcal{C})\}.$$

Let $\mathcal{B}_w(\mathcal{C})$ denote the set $\{\{\mathrm{Supp}(\mathbf{c}):wt(\mathbf{c})=w \text{ and } \mathbf{c}\in\mathcal{C}\}\}$, where $\{\{\}\}$ is the multiset notation. For some special code $\mathcal{C}$, the incidence structure $(\mathcal{P}(\mathcal{C}),\mathcal{B}_w(\mathcal{C}))$ could be a t-(v,w,λ) design for some positive integer t and λ. If $(\mathcal{P}(\mathcal{C}),\mathcal{B}_w(\mathcal{C}))$ is a t-design for all w with $0\le w\le\nu$, we say that the code $\mathcal{C}$ *supports t-designs*. By definition, such design $(\mathcal{P}(\mathcal{C}),\mathcal{B}_w(\mathcal{C}))$ could have some repeated blocks, or could be simple, or may be trivial. In this way, many t-designs have been constructed from linear codes (see, for example, [10], [10], [14], [15], [19], [21], [23]). A major way to construct combinatorial t-designs with linear codes over finite fields is the use of linear codes with t-transitive or t-homogeneous automorphism groups (see [10, Theorem 4.18]) and some combinatorial t-designs (see, for example, [7]) were obtained by this way. Very recently, Liu et al.[28] obtained some 3-transitive automorphism groups from a class of BCH codes and derived some combinatorial 3-designs with this way. Another major way to construct t-designs with linear codes is the use of the Assmus-Mattson Theorem (AM Theorem for short) in [10, Theorem 4.14] and the generalized version of the AM Theorem in [22], which was recently employed to construct a number of t-designs (see, for example, [10], [24], [25]). The following theorem is a generalized version of the AM Theorem, which was developed in [22] and will be needed in this paper.

Theorem 1. *[22] Let $\mathcal{C}$ be a linear code over the finite field* $\mathrm{GF}(q)$ *with length ν and minimum distance d. Let $\mathcal{C}^\perp$ denote the dual of $\mathcal{C}$ with minimum distance $d^\perp$. Let s and t be two positive integers such that $t<\min\{d,d^\perp\}$. Let S be a s-subset of the set $\{d,d+1,d+2,\ldots,\nu-t\}$. Suppose that $(\mathcal{P}(\mathcal{C}),\mathcal{B}_\ell(\mathcal{C}))$ and $\left(\mathcal{P}(\mathcal{C}^\perp),\mathcal{B}_{\ell^\perp}(\mathcal{C}^\perp)\right)$ are t-designs for $\ell\in\{d,d+1,d+2,\ldots,\nu-t\}\setminus S$ and $0\le\ell^\perp\le s+t-1$, respectively. Then the incidence structures $(\mathcal{P}(\mathcal{C}),\mathcal{B}_k(\mathcal{C}))$ and $\left(\mathcal{P}(\mathcal{C}^\perp),\mathcal{B}_k(\mathcal{C}^\perp)\right)$ are t-designs for any $t\le k\le\nu$, and particularly,*

- *the incidence structure $(\mathcal{P}(\mathcal{C}),\mathcal{B}_k(\mathcal{C}))$ is a simple t-design for all integers k with $d\le k\le w$, where w is defined to be the largest integer such that $w\le\nu$ and*

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

- *and the incidence structure $\left(\mathcal{P}(\mathcal{C}^\perp),\mathcal{B}_k(\mathcal{C}^\perp)\right)$ is a simple t-design for all integers k with $d\le k\le w^\perp$, where $w^\perp$ is defined to be the largest integer such that $w^\perp\le\nu$ and*

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

III. An infinite family of cyclic codes supporting 3-designs

In this section, our task is to establish the parameters of the cyclic code $\mathcal{C}_m$ defined by (1) and its dual, and prove that these codes hold 3-designs and satisfy 3-transitive automorphism groups. To this end, we shall prove a few more auxiliary results before proving the main results (see Theorems 6, 8 and 14) of this paper.

A. Some auxiliary results

In order to determine the minimum distance of the dual code $\mathcal{C}_m^{\perp}$ of $\mathcal{C}_m$, we need the results in the following three lemmas.

Lemma 2. *Let symbols and notation be the same as before. Let $m \geq 2$ be a positive integer and $q = 7^m$. For any $\{x,y,z\} \in \binom{U_{q+1}}{3}$, we have the following results.*

1) $x+y-2z \neq 0$*;*
2) $x+2y-3z \neq 0$*;*
3) $x+3y-4z \neq 0$*;*
4) $x+4y-5z \neq 0$*;*
5) $x+5y-6z \neq 0$*;.*

Proof. We only give the proof of the first conclusion. The proofs of the other four conclusions are similar to that of the first conclusion and thus omitted.

Assume that $x+y-2z=0$, then

$$(x+y-2z)^q = \frac{1}{x}+\frac{1}{y}-\frac{2}{z} = \frac{1}{x}+\frac{1}{y}-\frac{4}{2z} = 0.$$

It follows from $x+y=2z$ that

$$\frac{1}{x}+\frac{1}{y}-\frac{4}{x+y} = 0,$$

which means that $(x-y)^2=0$. This is contrary to our assumption that x,y,z are pairwise distinct. Thus, $x+y-2z \neq 0$. This completes the proof. □

Lemma 3. *Let symbols and notation be the same as before. Let $q=7^m$ with $m \geq 2$ being a positive integer and $\{x,y,z\} \in \binom{U_{q+1}}{3}$. Define*

$$\bar{M}(x,y,z) = \begin{bmatrix} 1 & 1 & 1 \\ x & y & z \\ x^7 & y^7 & z^7 \end{bmatrix}. \tag{5}$$

Then

$$|\bar{M}(x,y,z)| = (x-y)(x-z)(y-z)(x+y-2z)(x+2y-3z)(x+3y-4z)(x+4y-5z)(x+5y-6z) \neq 0.$$

Proof. The conclusion follows from Lemma 2. □

Lemma 4. *Let $m \geq 2$ be a positive integer, $q=7^m$ and $(x,y,z,w) \in \mathrm{GF}(q^2)^4$. Define*

$$M(x,y,z,w) = \begin{bmatrix} 1 & 1 & 1 & 1 \\ x & y & z & w \\ x^7 & y^7 & z^7 & w^7 \\ x^8 & y^8 & z^8 & w^8 \end{bmatrix}. \tag{6}$$

Then we have the following results.

1) $|M(x,y,z,w)| = (x-y)(x-z)(x-w)(y-z)(y-w)(z-w)\cdot\prod_{i=1}^{5}(xy+zw+i(xz+wy)+(6-i)(xw+yz))$.

2) *For any* $\{x,y,z\} \in \binom{U_{q+1}}{3}$*, there exists five pairwise distinct* $w \in U_{q+1} \setminus \{x,y,z\}$ *such that* $|M(x,y,z,w)| = 0$*, i.e.,* $\prod_{i=1}^{5}(xy+zw+i(xz+wy)+(6-i)(xw+yz)) = 0$.

Proof. 1) It is easy to prove the first conclusion and we omit its proof.

2) By definitions and Lemma 2, $z+iy+(6-i)x \neq 0$ for any $i \in \{1,2,3,4,5\}$. Denote

$$w_i = \frac{(i-6)yz-xy-ixz}{z+iy+(6-i)x}$$

, where $i \in \{1,2,3,4,5\}$. Note that

$$w_i^q = \frac{(i-6)y^qz^q-x^qy^q-ix^qz^q}{z^q+iy^q+(6-i)x^q} = \frac{((i-6)y^qz^q-x^qy^q-ix^qz^q)\cdot xyz}{(z^q+iy^q+(6-i)x^q))\cdot xyz} = 1/w_i.$$

Thus, $w_i^{q+1} = 1$. This means that $w_i \in U_{q+1}$ for any $i \in \{1,2,3,4,5\}$.

Since $\{x,y,z\} \in \binom{U_{q+1}}{3}$, from $|M(x,y,z,w)| = 0$ and the first conclusion 1) we have

$$\prod_{i=1}^{5}(xy+zw+i(xz+wy)+(6-i)(xw+yz)) = 0.$$

This means that $w = w_i$ with $i \in \{1,2,3,4,5\}$.

Next we will prove that $w_i \neq x,y,z$ for each $i \in \{1,2,3,4,5\}$.

Let $i \in \{1,2,3,4,5\}$. Suppose that $w_i = x$, then

$$\frac{(i-6)yz-xy-ixz}{z+iy+(6-i)x} = x,$$

which yields

$$(i-6)x^2-(i+1)(y+z)x+(i-6)yz = 0,$$

which is the same as

$$(i-6)(x-y)(x-z) = 0.$$

This means that $x = y$ or $x = z$, which is contrary to our assumption that x,y,z are pairwise distinct in U_{q+1}. Thus, $w_i \neq x$. Due to symmetry, $w_i \neq y$ and $w_i \neq z$. Therefore, $w_i \neq x,y,z$ for each $i \in \{1,2,3,4,5\}$.

We now prove that $w_i \neq w_j$ when $i \neq j$ and $i,j \in \{1,2,3,4,5\}$.

Let $i,j \in \{1,2,3,4,5\}$ and $i \neq j$. Suppose that $w_i = w_j$, then

$$\frac{(i-6)yz-xy-ixz}{z+iy+(6-i)x} = \frac{(j-6)yz-xy-jxz}{z+jy+(6-j)x},$$

which yields

$$(i-j)(x-y)(x-z)(y-z) = 0.$$

It then follows from $i \neq j$ that $x = y$ or $x = z$ or $y = z$, which is contrary to our assumption that x,y,z are pairwise distinct in U_{q+1}. Thus, w_1,w_2,w_3,w_4,w_5 are pairwise distinct. This completes the proof. □

The following result plays an important role in calculating the weight distributions of the cyclic code $\mathcal{C}_m$, which is described in the next lemma.

Lemma 5. *Let symbols and notation be the same as before. Let* $m \geq 2$ *be a positive integer,* $q = 7^m$*,* $(a,b) \in \mathrm{GF}(q^2)^2 \setminus \{(0,0)\}$ *and* $f(u) = \mathrm{Tr}(au^4+bu^3)$*. Define*

$$Zero(f) = \{u \in U_{q+1} : f(u) = 0\}.$$

Then $\#Zero(f) \leq 8$*. In particular,* $\#Zero(f) = 8$ *if* $\#Zero(f) \geq 3$.

Proof. Recall that Tr is the trace function from $\mathrm{GF}(q^2)$ to $\mathrm{GF}(q)$. By definition, then

$$f(u) = \mathrm{Tr}(au^4 + bu^3) = \frac{1}{u^4}(au^8 + bu^7 + b^q u + a^q)$$

if $u \in U_{q+1}$. Thus, $\#Zero(f) \leq 8$ and

$$Zero(f) = \{u \in U_{q+1} : au^8 + bu^7 + b^q u + a^q = 0\}.$$

If $\#Zero(f) \geq 3$, we assume that $\{1, -1, u_0\} \subseteq Zero(f)$. Then $f(1) = f(-1) = f(u_0) = 0$, which yields

$$\begin{cases} a^q = -a \\ b^q = -b \\ au_0^8 + bu_0^7 - bu_0 - a = 0. \end{cases} \tag{7}$$

Denote $g(u) = au^8 + bu^7 + b^q u + a^q$. Assume that $a \neq 0$ and denote $c = b/a$. By the first two equations in (7), we have $c^q = (b/a)^q = c$ and

$$g(u) = a(u^8 + \frac{b}{a}u^7 - \frac{b}{a}u - 1) = a(u^8 + cu^7 - cu - 1).$$

Denote

$$h(u) = u^8 + cu^7 - cu - 1.$$

Then it is not hard to verify that u^q and u^{-1} are also the roots of $h(u) = 0$ if u is a root of $h(u) = 0$. Thus, 1, -1, u_0 and $u_0^{-1} = u_0^q$ are also the roots of $h(u) = 0$. Further, from the third equation in (7), we have

$$c = \frac{u_0^8 - 1}{u_0^7 - u_0}.$$

Thus,

$$h(u) = u^8 + \frac{u_0^8 - 1}{u_0^7 - u_0} \cdot u^7 - \frac{u_0^8 - 1}{u_0^7 - u_0} \cdot u - 1.$$

If $h(u) = 0$, then

$$(u_0^7 - u^0)(u^8 - 1) - (u_0^8 - 1)(u^7 - u) = 0$$

which is the same as

$$\begin{aligned}(u_0^2 - 1)(u^2 - 1)(u - u_0)(u_0 u - 1) \quad &\cdot (u_0 u + 5u + 2u_0 - 1) \\ &\cdot (u_0 u + 4u + 3u_0 - 1) \\ &\cdot (u_0 u + 3u + 4u_0 - 1) \\ &\cdot (u_0 u + 2u + 5u_0 - 1) \quad = 0.\end{aligned}$$

This means that $h(u) = 0$ has eight roots as follows:

$$1,\ -1,\ u_0,\ u_0^{-1},\ u_1,\ u_2,\ u_3,\ u_4, \tag{8}$$

where

$$\begin{cases} u_1 = \frac{-2u_0+1}{u_0-2} \\ u_2 = \frac{-3u_0+1}{u_0-3} \\ u_3 = \frac{-4u_0+1}{u_0-4} \\ u_4 = \frac{-5u_0+1}{u_0-5}. \end{cases} \tag{9}$$

Note that it is not hard to verify that $u_3 = u_1^{-1}$, $u_4 = u_2^{-1}$ and $u_i^q = 1/u_i$ for any $i \in \{1,2,3,4\}$, which means that $u_i^{q+1} = 1$, i.e., $u_i \in U_{q+1}$ for any $i \in \{1,2,3,4\}$. Thus, the eight roots given by (8) are in U_{q+1}. Moreover, these eight roots in (8) are pairwise distinct. Suppose that $u_1 = u_0$, then we have $u_0^2 = 1$. This means that $u_0 = 1$ or $u_0 = -1$, which is contrary to our assumption that $1, -1, u_0$ are pairwise distinct in U_{q+1}. Thus, $u_1 \neq u_0$. By similar discussions, it is easily obtain that all elements in (8) are pairwise distinct. This completes the proof. $\square$

B. The parameters of cyclic codes

In this subsection, we will determine the parameters of the cyclic code $\mathcal{C}_m$ and its dual $\mathcal{C}_m^{\perp}$, and prove that these codes hold 3-designs.

Theorem 6. *Let $q = 7^m$ with $m \geq 2$ being a positive integer. Then the code $\mathcal{C}_m^{\perp}$ over* GF(q) *has the parameters $[q+1, q-3, 4]$. Furthermore, the minimum weight codewords in $\mathcal{C}_m^{\perp}$ support a 3-$(q+1, 4, 5)$ design.*

Proof. It follows from definitions that the code $\mathcal{C}_m^{\perp}$ has length $q+1$. Let α be a generator of the multiplicative group $\mathrm{GF}(q^2)^*$ and define $\beta = \alpha^{q-1}$. Then $\beta \in U_{q+1}$ is an $q+1$-th primitive root of unity in the field $\mathrm{GF}(q^2)$. Let $g_i(x)$ denote the minimal polynomial of β^i over $\mathrm{GF}(q)$, where $i \in \{3, 4\}$. Note that $g_i(x)$ has only the roots β^i and β^{-i}. We then deduce that $g_3(x)$ and $g_4(x)$ are pairwise distinct irreducible polynomials of degree 2. By definition, the generator polynomial of $\mathcal{C}_m^{\perp}$ is $g_3(x)g_4(x)$ with degree 4. Thus, $\mathcal{C}_m^{\perp}$ has dimension $q+1-4 = q-3$.

Let $U_{q+1} = \{x_1, x_2, x_3 \ldots, x_{q+1}\}$. Define

$$H = \begin{bmatrix} x_1^{-4} & x_2^{-4} & x_3^{-4} & \cdots & x_{q+1}^{-4} \\ x_1^{-3} & x_2^{-3} & x_3^{-3} & \cdots & x_{q+1}^{-3} \\ x_1^{3} & x_2^{3} & x_3^{3} & \cdots & x_{q+1}^{3} \\ x_1^{4} & x_2^{4} & x_3^{4} & \cdots & x_{q+1}^{4} \end{bmatrix}. \tag{10}$$

It is easily observed that

$$\mathcal{C}_m^{\perp} = \{\mathbf{c} \in \mathrm{GF}(q)^{q+1} : \mathbf{c}H^T = \mathbf{0}\}. \tag{11}$$

By Lemma 5 and Equations (10) and (11), we have the minimum distance d of $\mathcal{C}_m^{\perp}$ is at least 4. Next we will prove that $d = 4$.

Let $\{x, y, z, w\} \in \binom{U_{q+1}}{4}$. Without the loss of generality, we assume that

$$x = x_{i_1},\ y = x_{i_2},\ z = x_{i_3},\ w = x_{i_4},$$

where $1 \leq i_1 < i_2 < i_3 < i_4 \leq q+1$. Since $d \geq 4$, the rank of the matrix $M(x, y, z, w)$ equals 3, where $M(x, y, z, w)$ was defined by (6). Let $(u_{i_1}, u_{i_2}, u_{i_3}, u_{i_4}) \in \mathrm{GF}(q)^4$ denote a nonzero solution of

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ x & y & z & w \\ x^7 & y^7 & z^7 & w^7 \\ x^8 & y^8 & z^8 & w^8 \end{bmatrix} \begin{bmatrix} u_{i_1} \\ u_{i_2} \\ u_{i_3} \\ u_{i_4} \end{bmatrix} = \mathbf{0}.$$

Since the rank of the matrix $M(x, y, z, w)$ is 3, all these $u_{i_j} \neq 0$. Define a vector $\mathbf{c} = (c_0, c_1, \ldots, c_n) \in \mathrm{GF}(q)^{n+1}$, where $c_{i_j} = u_{i_j}$ for $j \in \{1, 2, 3, 4\}$ and $c_h = 0$ for all $h \in \{0, 1, \ldots, n\} \setminus \{i_1, i_2, i_3, i_4\}$. It is easily observed that $\mathbf{c}$ is a codeword with Hamming weight 4 in $\mathcal{C}_m^{\perp}$. The set $\{a\mathbf{c} : a \in \mathrm{GF}(q)^*\}$ consists of all such codewords of Hamming weight 4 with nonzero coordinates in $\{i_1, i_2, i_3, i_4\}$. Hence, the code $\mathcal{C}_m^{\perp}$ has minimum distance $d = 4$. Meanwhile, every codeword of Hamming weight 4 in $\mathcal{C}_m^{\perp}$ with nonzero coordinates in $\{i_1, i_2, i_3, i_4\}$ must correspond to the set $\{x, y, z, w\}$. Further, from $|M(x, y, z, w)| = 0$ and Lemma 4, it follows that every codeword of weight 4 and its nonzero multiples in $\mathcal{C}_m^{\perp}$ correspond to five such set $\{x, y, z, w\}$. We then deduce that the codewords of weight 4 in $\mathcal{C}_m^{\perp}$ support a 3-$(q+1, 4, 5)$ design. Thus, the number of the codewords of weight 4 in $\mathcal{C}_m^{\perp}$ is

$$A_4^{\perp} = (q-1) \cdot \frac{\binom{q+1}{3}}{\binom{4}{3}} \cdot 5 = \frac{5(q-1)^2 q(q+1)}{24}.$$

This completes the proof. $\square$

Example 7. *Let $m=2$. Then the code $\mathcal{C}_m^{\perp}$ has the parameters $[50,46,4]$. The number of the codewords of weight 4 in $\mathcal{C}_m^{\perp}$ is $A_4^{\perp}=1176000$. The codewords of weight 4 in $\mathcal{C}_m^{\perp}$ support a 3-$(50,4,5)$ design.*

It is now time to determine the parameters of the cyclic code $\mathcal{C}_m$, which is described in the following theorem.

Theorem 8. *Let $q=7^m$ with $m\geq 2$ being a integer. Then we have the following results.*

(I) *The code $\mathcal{C}_m$ over* GF(q) *has the parameters $[q+1,4,q-7]$ and the weight enumerator*

$$1+\frac{1}{336}(q-1)^2q(q+1)z^{q-7}+\frac{1}{12}(q-1)q(1+q)(7+5q)z^{q-1}+ \\ \frac{1}{7}(q-1)(1+q)(7+(q-1)q)z^{q}+\frac{7}{16}(q-1)^2q(1+q)z^{q+1}. \tag{12}$$

(II) *The code $\mathcal{C}_m$ and its dual $\mathcal{C}_m^{\perp}$ support 3-designs. Furthermore, the codewords of weight $q-7$ in $\mathcal{C}_m$ hold a 3-$(q+1,q-7,\lambda)$ design, where*

$$\lambda=\frac{(q-7)(q-8)(q-9)}{336}.$$

The complement of this design is a 3-$(q+1,8,1)$ design, i.e., Steiner systems $S(3,8,q+1)$.

Proof. (I) By definition, it is clear that the code $\mathcal{C}_m$ has length $q+1$. By Theorem 6, the dual code $\mathcal{C}_m^{\perp}$ of $\mathcal{C}_m$ has dimension $q-3$. Thus, the dimension of the code $\mathcal{C}_m$ is 4.

Further, by definitions and Lemma 5, the minimum distance of $\mathcal{C}_m$ is $q-7$ and the code $\mathcal{C}_m$ has at most four nonzero weights, i.e.,

$$w_1=q-7,\ w_2=q-1,\ w_3=q,\ w_4=q+1\ .$$

We now determine the number A_{w_i} of the codewords with weight w_i in $\mathcal{C}_m$. Since $\mathcal{C}_m^{\perp}$ has minimum distance $d=4$, the first four Pless Power Moments lead to the following system of equations:

$$\begin{cases} A_{w_1}+A_{w_2}+A_{w_3}+A_{w_4}=q^4-1 \\ w_1A_{w_1}+w_2A_{w_2}+w_3A_{w_3}+w_4A_{w_4}=q^3(q-1)n \\ w_1^2A_{w_1}+w_2^2A_{w_2}+w_3^2A_{w_3}+w_4^2A_{w_4}=q^2(q-1)n(qn-n+1) \\ w_1^3A_{w_1}+w_2^3A_{w_2}+w_3^3A_{w_3}+w_4^3A_{w_4}=q(q-1)n(q^2n^2-2qn^2+3qn-q+n^2-3n+2), \end{cases} \tag{13}$$

where $n=q+1$. Solving the system of equations in (13) yields the weight enumerator in (12).

(II) By the conclusions of (I) and Theorem 6, from Theorem 1 we get that both $\mathcal{C}_m$ and $\mathcal{C}_m^{\perp}$ hold 3-designs. By (12), the number of the codewords with weight $q-7$ in $\mathcal{C}_m$ is

$$A_{q-7}=\frac{1}{336}(q-1)^2q(q+1).$$

Since $q-7$ is the minimum weight of $\mathcal{C}_m$, the number of supports of the codewords of weight $q-7$ is

$$b=\frac{A_{q-7}}{q-1}=\frac{1}{336}(q-1)q(q+1). \tag{14}$$

Then the values of λ follow from Equations (14) and (4).

By definitions, the complement of the supports of the codewords with the minimum weight $q-7$ in $\mathcal{C}_m$ holds a 3-$(q+1,8,\lambda')$ and the number of this supports equals the value of b of (14). Then we deduce that $\lambda'=1$ from

$$b=\frac{1}{336}(q-1)q(q+1)=\lambda'\cdot\frac{\binom{q+1}{3}}{\binom{8}{3}}.$$

This means that the complement of the supports of the minimum weight codewords in $\mathcal{C}_m$ forms a Steiner system $S(3,8,q+1)$. This completes the proof.

□

Example 9. *Let $m=2$. Then the code $\mathcal{C}_2$ has the parameters $[50,4,42]$ and weight enumerator*

$$1+16800z^{42}+2469600z^{48}+808800z^{49}+2469600z^{50},$$

which is verified by a Magma program.

Example 10. *Let $m=3$. Then the code $\mathcal{C}_3$ has the parameters $[344,4,336]$ and weight enumerator*

$$1+41073858z^{336}+5790693384z^{342}+1971662832z^{343}+6037857126z^{344},$$

which is verified by a Magma program.

C. Automorphism groups of cyclic codes

In this subsection, we will show that the cyclic code $\mathcal{C}_m$ and its dual $\mathcal{C}_m^{\perp}$ are invariant under group actions of certain permutation groups which are 3-transitive, i.e., the automorphism groups of those code are 3-transitive. To this end, we use the similar method in Liu et al [28].

Define

$$\mathrm{Stab}_{U_{q+1}}=\left\{\begin{pmatrix}\beta_2^q & \beta_1^q\\ \beta_1 & \beta_2\end{pmatrix}\in \mathrm{PGL}(2,q^2):\ \beta_1,\beta_2\in \mathrm{GF}(q^2),\beta_1^{q+1}\neq\beta_2^{q+1}\right\}. \tag{15}$$

Then we have

$$\mathrm{Stab}_{U_{q+1}}=\begin{pmatrix}u_0 & 1\\ 1 & u_0\end{pmatrix}\mathrm{PGL}(2,q)\begin{pmatrix}u_0 & 1\\ 1 & u_0\end{pmatrix}^{-1} \tag{16}$$

with $u_0\in U_{q+1}\setminus\{\pm1\}$ and the following result which was documented in [28, Proposition 5].

Lemma 11. *[28] Let symbols and notation be the same as before. Let $q=7^m$ with $m\geq 2$ being a positive integer. Then the setwise stabilizer of U_{q+1} can be expressed as $\mathrm{Stab}_{U_{q+1}}$ defined by (15). Moreover, the action of $\mathrm{Stab}_{U_{q+1}}$ on U_{q+1} is equivalent to the action of $\mathrm{PGL}(2,q)$ on the projective line $\mathrm{PG}(1,q)$ and $\mathrm{Stab}_{U_{q+1}}$ is 3-transitive.*

Denote the set

$$\mathcal{SF}:=\left\{\mathrm{Tr}\left(au^4+bu^3\right)\in \mathrm{GF}(q^2)[u]/\langle u^{q+1}-1\rangle : a,b\in \mathrm{GF}(q^2)\right\} \tag{17}$$

and the operator $'\circ'$ is defined by

$$(G\circ f)(u):=(\beta_1u+\beta_2)^{4(q+1)}f\left(\tfrac{\alpha_1u+\alpha_2}{\beta_1u+\beta_2}\right), \tag{18}$$

where $G=\begin{pmatrix}\alpha_1 & \alpha_2\\ \beta_1 & \beta_2\end{pmatrix}^{-1}\in \mathrm{GL}(2,q^2)$ and $f\in\mathcal{PF}$.

Let $\bar{G}=\begin{pmatrix}\beta_2^q & \beta_1^q\\ \beta_1 & \beta_2\end{pmatrix}^{-1}\in \mathrm{GL}(2,q^2)$ and denote

$$\overline{\mathrm{Stab}}_{U_{q+1}}=\left\{\begin{pmatrix}\beta_2^q & \beta_1^q\\ \beta_1 & \beta_2\end{pmatrix}\in \mathrm{GL}(2,q^2):\ \beta_1,\beta_2\in \mathrm{GF}(q^2),\beta_1^{q+1}\neq\beta_2^{q+1}\right\}. \tag{19}$$

Next we will show that the linear space $\mathcal{PS}$ under the action of the group $\overline{\mathrm{Stab}}_{U_{q+1}}$ is invariant. To this end, we need the results in the following two lemmas.

Lemma 12. *Let $q=7^m$ with $m\geq 2$ being a positive integer. Let $\bar{G}=\begin{pmatrix}\beta_2^q & \beta_1^q\\ \beta_1 & \beta_2\end{pmatrix}^{-1}\in \mathrm{GL}(2,q^2)$ and $f\in\mathcal{SF}$. Then $\bar{G}\circ f\in\mathcal{SF}$.*

Proof. Denote $f_1 = \mathrm{Tr}(au^4) \in \mathrm{GF}(q^2)[u]/\langle u^{q+1}-1\rangle$ and $f_2 = \mathrm{Tr}(bu^3) \in \mathrm{GF}(q^2)[u]/\langle u^{q+1}-1\rangle$. We only need to prove $(\bar{G}\circ f_1)(u) \in \mathcal{SF}$ and $(\bar{G}\circ f_2)(u) \in \mathcal{SF}$ for any $(a,b) \in \mathrm{GF}(q^2)^2$.

For any $a \in \mathrm{GF}(q^2)$, from definitions we have

$$\begin{aligned}
&(\bar{G}\circ f_1)(u)\\
&= (\beta_1 u+\beta_2)^{4(q+1)} f_1\left(\tfrac{\beta_2^q u+\beta_1^q}{\beta_1 u+\beta_2}\right),\\
&= \mathrm{Tr}\left(a\cdot(\beta_1 u+\beta_2)^{4q}(\beta_1 u+\beta_2)^4\cdot\tfrac{(\beta_2^q u+\beta_1^q)^4}{(\beta_1 u+\beta_2)^4}\right)\\
&= \mathrm{Tr}\left(a\cdot(\beta_1^q u^{-1}+\beta_2^q)^4\cdot u^4(\beta_2^q+\beta_1^q u^{-1})^4\right)\\
&= \mathrm{Tr}\left(au^4\cdot(\beta_1^q u^{-1}+\beta_2^q)^8\right)
\end{aligned} \tag{20}$$

Note that $7|\binom{8}{i}$ for any $i \in \{2,3,4,5,6\}$. Therefore, from the Binomial Theorem we have

$$\begin{aligned}
u^4\cdot(\beta_1^q u^{-1}+\beta_2^q)^8 &= \sum_{i=0}^{8}\binom{8}{i}\beta_1^{qi}\beta_2^{q(8-i)}u^{4-i},\\
&= \beta_2^{8q}u^4+\beta_2^{7q}\beta_1^q u^3+\beta_1^{8q}u^{-4}+\beta_2^q\beta_1^{7q}u^{-3}\\
&= \beta_2^{8q}u^4+\beta_2^{7q}\beta_1^q u^3+(\beta_1^8 u^4)^q+(\beta_2\beta_1^7 u^3)^q
\end{aligned} \tag{21}$$

Applying the above equation (21) to (20), we get

$$(\bar{G}\circ f_1)(u) = \mathrm{Tr}\left(a(\beta_2^{8q}u^4+\beta_2^{7q}\beta_1^q u^3)+a^{1/q}(\beta_1^8 u^4+\beta_2\beta_1^7 u^3)\right) \in \mathcal{SF}. \tag{22}$$

Using the similar method on f_1 to f_2, we can easily obtain

$$(\bar{G}\circ f_2)(u) = \mathrm{Tr}\left(b(\beta_1\beta_2^{7q}u^4+\beta_2^{7q+1}u^3)+b^{1/q}(\beta_1^7\beta_2^{1/q}u^4+\beta_1^{q+7}u^3)\right) \in \mathcal{SF} \tag{23}$$

for any $b \in \mathrm{GF}(q^2)$. The desired conclusion then follows from Equations (22) and (23). □

According to Lemma 12 and the definition of $'\circ'$ in (18), we can easily obtain the following result and we omit its proof.

Lemma 13. *Let symbols and notation be the same as before. Let $q = 7^m$ with $m \geq 2$ being a positive integer and E be the 2×2 identity matrix. For any $\overline{G}_1, \overline{G}_2 \in \overline{\mathrm{Stab}}_{U_{q+1}}$ and $f_1, f_2 \in \mathcal{SF}$, we have $\overline{G}_1\circ f_1 \in \mathcal{SF}$, $E\circ f_1 = f_1$, $(\overline{G}_1\overline{G}_2)\circ f_1 = \overline{G}_1\circ(\overline{G}_2\circ f_1)$, and $\overline{G}_1\circ(a'f_1+b'f_2) = a'\overline{G}_1\circ f_1+b'\overline{G}_2\circ f_2$ for all $a',b' \in \mathrm{GF}(q)$.*

Let $\mathrm{GF}(q)^{U_{q+1}}$ denote the vector space consisting of all elements $(c_u)_{u\in U_{q+1}}$, where $c_u \in \mathrm{GF}(q)$. The action of the semidirect product $(\mathrm{GF}(q)^*)^{U_{q+1}} \rtimes \mathrm{Stab}_{U_{q+1}}$ on $\mathrm{GF}(q)^{U_{q+1}}$ is defined by

$$\left((a_u)_{u\in U_{q+1}};g\right)(c_u)_{u\in U_{q+1}} = (a_u c_{g^{-1}(u)})_{u\in U_{q+1}}.$$

Then the multiplication in $(\mathrm{GF}(q)^*)^{U_{q+1}} \rtimes \overline{\mathrm{Stab}}_{U_{q+1}}$ is given by

$$\left((a_u)_{u\in U_{q+1}};g_1\right)\left((b_u)_{u\in U_{q+1}};g_2\right) = \left((c_u)_{u\in U_{q+1}};g_1g_2\right),$$

where $c_u = a_u b_{g_1^{-1}(u)}$.

The following theorem is one of the main result in this paper. It show that the code $\mathcal{C}_m$ and its dual admit 3-transitive automorphism group.

Theorem 14. *Let $q = 7^m$ with $m \geq 2$ being a positive integer. Define the subgroup G_i of $(\mathrm{GF}(q)^*)^{U_{q+1}} \rtimes \mathrm{Stab}_{U_{q+1}}$ by*

$$G_i = \left\{\left(\left((\beta_1 u+\beta_2)^{4i(q+1)}\right)_{u\in U_{q+1}};\begin{pmatrix}\beta_2^q & \beta_1^q\\ \beta_1 & \beta_2\end{pmatrix}^{-1}\right) : \beta_1,\beta_2 \in \mathrm{GF}(q^2), \beta_1^{q+1} \neq \beta_2^{q+1}\right\},$$

where $i \in \{1,-1\}$. *Then we have the following results.*

1) G_1 *is a subgroup of the monomial automorphism group* $\mathrm{MAut}(\mathcal{C}_m)$. *Moreover, the automorphism group of* $\mathcal{C}_m$ *is* 3*-transitive.*
2) G_{-1} *is a subgroup of the monomial automorphism group* $\mathrm{MAut}(\mathcal{C}_m^{\perp})$ *and the automorphism group of* $\mathcal{C}_m$ *is* 3*-transitive.*

Proof. 1) By the definitions in (1) and (17),

$$\mathcal{C}_m = \left\{ (f(u))_{u \in U_{q+1}} : f \in \mathcal{SF} \right\}.$$

Then the desired conclusion follows from definitions and Lemmas 13, 3 and 11.

2) The desired conclusion follows from the first conclusion of this theorem.

□

IV. Concluding remarks

In this paper, we investigated a class of cyclic codes $\mathcal{C}_m$ over $\mathrm{GF}(7^m)$ and completely determined their parameters. The results showed that the code $\mathcal{C}_m$ has four nonzero weights and supports 3-designs. Meanwhile, the dual code of $\mathcal{C}_m$ also supports 3-designs, and the automorphism group of the code $\mathcal{C}_m$ and its dual $\mathcal{C}_m^{\perp}$ are 3-transitive. Specifically, the complements of the supports of the minimum weight codewords in $\mathcal{C}_m$ form a Steiner system $S(3,8,7^m+1)$. Using the similar method of this paper and [28], we remark that it may obtain some new cyclic codes admitting 3-transitive automorphism groups and determine their parameters by properly choosing the value of q and the exponents of u in (1).

References

[1] R. T. Chien, "Cyclic decoding procedure for the Bose-Chaudhuri-Hocquenghem codes", *IEEE Trans. Inform. Theory*, vol. 10, no. 4, pp. 357–363, 1964.

[2] G. D. Forney, "On decoding BCH codes," *IEEE Trans. Inform. Theory,* vol. 11, no. 4, pp. 549–557, 1995.

[3] E. Prange, "Some cyclic error-correcting codes with simple decoding algorithms," Air Force Cambridge Research Center-TN-58-156, Cambridge, Mass., April 1958.

[4] C. Ding, T. Helleseth, "Optimal Ternary Cyclic Codes From Monomials," *IEEE Trans. Inform. Theory*, vol. 59, no. 9, pp. 5898-5904, 2013.

[5] Z. Zhou, C. Ding, "Seven Classes of Three-Weight Cyclic Codes," *IEEE Trans. Commun.*, vol. 61, no. 10, pp. 4120-4126, 2013.

[6] C. Li, C. Ding, S. Li, "LCD Cyclic Codes Over Finite Fields," *IEEE Trans. Inform. Theory*, vol. 63, no. 7, pp. 4344-4356, 2017.

[7] H. Liu, C. Ding, "Infinite families of 2-designs from GA1(q) actions," arXiv:1707.02003, 2017.

[8] C. Ding, "A sequence construction of cyclic codes over finite fields," *Cryptogr. Commun.*, vol. 10, no. 2, pp. 319-341, 2018.

[9] Z. Zha, L. Hu, Y. Liu, X. Cao, "Further results on optimal ternary cyclic codes," *Finite Fields Their Appl.* , vol.75, pp. 101898, 2021.

[10] C. Ding, *Designs from Linear Codes*. Singapore: World Scientific, 2018.

[11] C. Ding, C. Tang, "Infinite families of near MDS codes holding t-designs," *IEEE Trans. Inform. Theory*, vol. 66, no. 9, pp. 5419–5428, 2020.

[12] C.Ding, C. Tang, V.D. Tonchev, "Linear codes of 2-designs associated with subcodes of the ternary generalized Reed-Muller codes," *Des. Codes Cryptogr.*, vol. 88, no. 4, pp. 625-641, 2020.

[13] C. Ding, C. Tang, "The linear codes of t-designs held in the Reed-Muller and Simplex codes," arXiv:2008.09935, 2020.

[14] C. Ding, "Infinite families of 3-designs from a type of five-weight code," *Des. Codes Cryptogr.*, vol. 86, no. 3, pp. 703–719, 2018.

[15] C. Ding, C. Li, "Infinite families of 2-designs and 3-designs from linear codes," *Discrete Math.*, vol. 340, no. 10, pp. 2415–2431, 2017.

[16] C. Ding, *Codes from Difference Sets*. Singapore: World Scientific, 2015.

[17] V. D. Tonchev, "Codes and designs," In Handbook of Coding Theory, vol. II, V. S. Pless and W. C. Huffman, eds., Elsevier, Amsterdam, pp. 1229–1268, 1998.

[18] V. D. Tonchev, "Codes," In Handbook of Combinatorial Designs, 2nd edition, C. J. Colbourn and J. H. Dinitz, eds., CRC Press, New York, pp. 677–701, 2007.

[19] C. Ding, "An infinite family of Steiner systems from cyclic codes," *Journal of Combinatorial Designs*, vol. 26, pp. 127–144, 2018.

[20] W. C. Huffman, V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge: Cambridge University Press, 2003.

[21] C. Tang, C. Ding, M. Xiong, "Steiner systems $S(2,4,\frac{3^m-1}{2})$ and 2-designs from ternary linear codes of length $\frac{3^m-1}{2}$," *Des. Codes Cryptogr.*, vol. 87, no. 12, pp. 2793–2811, 2019.

[22] C. Tang, C. Ding, M. Xiong, "Codes, differentially δ-uniform functions, and t-designs," *IEEE Trans. Inform. Theory*, vol. 66, no. 6, pp. 3691–3703, 2020.

[23] C. Tang, C. Ding, "An infinite family of linear codes supporting 4-designs," *IEEE Trans. Inform. Theory*, vol. 67, no. 1, pp. 244-254, 2021.

[24] X. Du, R. Wang, C. Tang, Q. Wang, "Infinite families of 2-designs from two classes of binary cyclic codes with three nonzeros", arXiv:1903.08153, 2019.

[25] X. Du, R. Wang, C. Tang, Q. Wang, “Infinite families of 2-designs from two classes of linear codes”, arXiv:1903.07459, 2019.
[26] H. Yan, “A class of primitive BCH codes and their weight distribution.” *Appl. Algebra Eng. Commun. Comput.* vol. 29, no. 1, pp. 1–11, 2018.
[27] H. Yan, H. Liu, C. Li, et al., “Parameters of LCD BCH codes with two lengths”, *Adv. Math. Commun.*, vol. 12, no. 3, pp. 579-594, 2018.
[28] Q. Liu, C. Ding, S. Mesnager, C. Tang, V.D. Tonchev, “On infinite families of narrow-sense antiprimitive BCH codes admitting 3-transitive automorphism groups and their consequences”, arXiv:2109.09051, 2021.