Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 18, Number 2 (2022), pp. 723-731

http://www.ripublication.com/gjpam.htm

# The linear codes supporting $3-$Design

**Min Guo**[1]

[1]*College of Mathematics and Information, China West Normal University, Nanchong, Sichuan-637000, China.* ,

**Abstract**

Coding theory and combinatorial t-designs have close connections. Some t-designs have been constructed by using certain linear codes in recent years. The objective of this paper is to study 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.
**Keywords:** $t-$design, linear codes, cyclic codes, automorphism group

## 1. T-DESIGN

A $t-(v,k,\lambda)$ $design$, is a pair $(\mathcal{P},\mathcal{B})$ where $\mathcal{P}$ is a set of $v$ elements, called *points*, and $\mathcal{B}$ is a collection of distinct subsets of $\mathcal{P}$ of size $k$, called *blocks*, such that any $t$ points are contained in exactly $\lambda$ blocks, where $\lambda > 0$. A $t-$design is a $t-(v,k,\lambda)$ design for some parameters $v,k,\lambda$. A $t-(v,k,\lambda)$ design is also an $i-(v,k,\lambda_i)$ design for every $0 \leq i < t$, where

$$\lambda_i = \lambda \frac{\binom{v-i}{t-i}}{\binom{k-i}{t-i}}.$$

In a $t-(v,k,\lambda)$ $design$, the number of blocks is

$$b = \lambda_0 = \lambda \frac{\binom{v}{t}}{\binom{k}{t}}.$$

Let $\mathcal{C}$ be a linear code of length $q+1$ over GF$(r)$ and PGL$(2,q)$ the projective general linear group acting as a permutation group on the set of points of the projective line PG$(1,q)$ over a finite field GF$(q)$ with $q$ elements. Every vector in the $(q+1)-$dimensional vector space GF$(r)^{q+1}$

can be written as $(c_x)_{x\in PG(1,q)}$, where $c_x \in \mathrm{GF}(r)$ and $r$ is a prime power. In other words, the coordinates of the vectors in $\mathrm{GF}(r)^{q+1}$ can be indexed by the points in $\mathrm{PG}(1,q)$. We say that $\mathcal{C}$ is *invariant under* $\mathrm{PGL}(2,q)$ if each element of $\mathrm{PGL}(2,q)$ carries each codeword of $\mathcal{C}$ into a codeword of $\mathcal{C}$. In other words, $\mathcal{C}$ is invariant under $\mathrm{PGL}(2,q)$ if $\mathcal{C}$ admits $\mathrm{PGL}(2,q)$ as a subgroup of the permutation automorphism group of $\mathcal{C}$. For a codeword $\mathbf{c} = (c_x)_{x\in PG(1,q)}$ in $\mathcal{C}$, the *support* of $\mathbf{c}$ is defined as

$$\mathrm{Supp}(\mathbf{c}) = \{x \in \mathrm{PG}(1,q) : c_x \neq 0\}.$$

Let $A_w(\mathcal{C}) = |\{\mathbf{c} \in \mathcal{C} : wt(\mathbf{c}) = w\}|$ and $\mathfrak{B}_w(\mathcal{C}) = \{Supp(\mathbf{c}) : wt(\mathbf{c}) = w$ and $\mathbf{c} \in \mathcal{C}\}$, where wt($\mathbf{c}$) denotes the Hamming weight of $\mathbf{c}$. $\mathfrak{B}_w(\mathcal{C})$ is said to be invariant under $\mathrm{PGL}(2,q)$ if the support $Supp((c_{\pi(x)})_{x\in PG(1,q)})$ belongs to $\mathfrak{B}_w(\mathcal{C})$ for every $\pi \in \mathrm{PGL}(2,q)$ and any codeword $(c_x)_{x\in PG(1,q)}$ of weight $w$ in $\mathcal{C}$. It is easily seen that if $\mathcal{C}$ is invariant under $\mathrm{PGL}(2,q)$, then so is $\mathfrak{B}_w(\mathcal{C})$ for each $w$. Moreover, if $\mathfrak{B}_w(\mathcal{C})$ is invariant under $\mathrm{PGL}(2,q)$, then $(\mathrm{PG}(1,q), \mathfrak{B}_w(\mathcal{C}))$ holds a $3-$design provided $A_w(\mathcal{C}) \neq 0$, since the action of $\mathrm{PGL}(2,q)$ on $\mathrm{PGL}(1,q)$ is $3-$transitive.

### 1.1. Linear codes and trace function

Let $\mathrm{GF}(r)$ be the finite field with $r$ elements. An $[n,k]_r$ linear code $\mathcal{C}$ is a k-dimensional vector subspace of $\mathrm{GF}(r)^n$. If it has minimum distance $d$ it is also called an $[n,k,d]_r$ code. The *dual code* $\mathcal{C}^\perp$ of $\mathcal{C}$ is the set of vectors orthogonal to all codewords of $\mathcal{C}$:

$$\mathcal{C}^\perp = \{\mathbf{w} \in GF(r)^n : \langle \mathbf{c}, \mathbf{w}\rangle = 0 \text{ for all } \mathbf{c} \in \mathcal{C}\},$$

where $\langle \mathbf{c}, \mathbf{w}\rangle$ is the usual Euclidean inner product of $\mathbf{c}$ and $\mathbf{w}$. Let $\mathbf{a} = (a_0, ..., a_{n-1}) \in (GF(r)^*)^n$. Here and subsequently, $\mathbf{a} \cdot \mathcal{C}$ stands for the linear code $\{(a_0c_0, ..., a_{n-1}c_{n-1}) : (c_0, ..., c_{n-1}) \in \mathcal{C}\}$. It is a simple matter to check that

$$(\mathbf{a} \cdot \mathcal{C})^\perp = \mathbf{a}^{-1} \cdot \mathcal{C}^\perp, \tag{1}$$

where $\mathbf{a}^{-1} = (a_0^{-1}, ..., a_{n-1}^{-1})$.

The *trace code* of $\mathcal{C}$ is given by

$$\mathrm{Tr}_{r^h/r}(\mathcal{C}) = \{(\mathrm{Tr}_{r^h/r}(c_0), ..., \mathrm{Tr}_{r^h/r}(c_{n-1})) : (c_0, ..., c_{n-1}) \in \mathcal{C}\},$$

where $\mathrm{Tr}_{r^h/r}$ denotes the trace function from $\mathrm{GF}(r)^h$ to $\mathrm{GF}(r)$. A celebrated result of Delsarte states that the subfield code $\mathcal{C}^\perp|_{GF(q)}$ and the trace code $\mathrm{Tr}_{r^h/r}(\mathcal{C})$ are duals of each other, namely,

$$(\mathbf{Tr}_{r^h/r}(\mathcal{C}))^\perp = \mathcal{C}^\perp|_{\mathbf{GF}(q)}. \tag{2}$$

Let $U_{q+1}$ be the subset of the projective line PG$(1, q^2)$ =GF$(q^2) \cup \{\infty\}$ consisting of all the $q+1-$th roots of unity. Denote by $\text{Stab}_{U_{q+1}}$ the setwise stabilizer of $U_{q+1}$ under the action of $\text{PGL}_2(\text{GF}(q^2))$ on PG$(1, q^2)$.

**Corollary 1** *Let $q = 3^m$. Then the setwise stabilizer $Stab_{U_{q+1}}$ of $U_{q+1}$ is generated by the following three types of linear fractional transformations:*
*(i) $u \longmapsto u_0 u$, where $u_0 \in U_{q+1}$;*
*(ii) $u \longmapsto u^{-1}$;*
*(iii) $u \longmapsto \frac{u+c^q}{cu+1}$, where $c \in GF(q^2)^* \backslash U_{q+1}$.*

## 2. LINEAR CODES OF LENGTH $3^m + 1$ WITH SETS OF SUPPORTS INVARIANT UNDER PGL$(2, q)$

Let $q = 3^m$ and $U_{q+1} = \{u : u \in GF(q^2), u^{q+1} = 1\}$. Let $\mathcal{C}_m$ be a linear code defined by

$$\mathcal{C}_m = \{(a_4 u^4 + a_5 u^5)_{u \in U_{q+1}} : a_i \in GF(q^2)\}.$$

We define $[k] = \{1, 2, ..., k\}$. The *elementary symmetric polynomial(ESP)* of degree $\ell$ in $k$ variables $u_1, u_2, ..., u_k$, written $\sigma_{k,\ell}$, is defined by

$$\sigma_{k,\ell}(u_1, u_2, ..., u_k) = \sum_{I \subseteq [k], |k| = \ell} \prod_{j \in I} u_j, \tag{3}$$

In commutative algebra, the elementary symmetric polynomials are a type of basic building block for symmetric polynomials, in the sense that any symmetric polynomial can be expressed as a polynomial in elementary symmetric polynomials.

For any $k-$variables symmetric polynomial $f$ with coefficients in GF$(q^2)$, write

$$\mathfrak{B}_{f,q+1} = \{(u_1, u_2, ..., u_k) \in \binom{U_{q+1}}{k} : f(u_1, u_2, ..., u_k) = 0\}. \tag{4}$$

To simplify notation and expressions below, we use $\sigma_{k,\ell}$ to denote $\sigma_{k,\ell}(u_1, u_2, ..., u_k)$ for any $(u_1, u_2, ..., u_k) \in \binom{U_{q+1}}{k}$ whenever $(u_1, u_2, ..., u_k)$ is specified.

**Lemma 2** *Let $q = 3^m$ and $\{u_1, u_2, u_3\} \in \binom{U_{q+1}}{3}$. Then we have $u_1 + u_2 + u_3 \neq 0$.*

***Proof 3*** *Assume that $u_1 + u_2 + u_3 = 0$. Then $u_3 = 2(u_1 + u_2)$, $\frac{1}{u_1} + \frac{1}{u_2} + \frac{1}{u_3} = (u_1 + u_2 + u_3)^q = 0$, $2(u_1 - u_2)^2 = 0$, which is contrary to our assumption that $u_1, u_2, u_3$ are pairwise distinct. Thus, $u_1 + u_2 + u_3 \neq 0$.*

For a positive integer $\ell \leq q+1$, define a $4 \times \ell$ matrix $M_\ell$ by

$$\begin{bmatrix} u_1^{-5} & u_2^{-5} & ... & u_\ell^{-5} \\ u_1^{-4} & u_2^{-4} & ... & u_\ell^{-4} \\ u_1^{+4} & u_2^{+4} & ... & u_\ell^{+4} \\ u_1^{+5} & u_2^{+5} & ... & u_\ell^{+5} \end{bmatrix} \tag{5}$$

where $(u_1, u_2, ..., u_k) \in U_{q+1}$. For $r_1, ..., r_i \in \{\pm 5, \pm 4\}$, let $M_\ell[r_1, ..., r_i]$ denote the submatrix of $M_\ell$ obtained by deleting the rows $(u_1^{r_1}, u_2^{r_1}, ..., u_\ell^{r_1}), ..., (u_1^{r_i}, u_2^{r_i}, ..., u_\ell^{r_i})$ of the matrix $M_\ell$, where $1 \leq i \leq 4$.

**Lemma 4** *Let $M_\ell$ be the matrix given by* (5) *with* $(u_1, u_2, ..., u_\ell) \in \binom{U_{q+1}}{\ell}$. *Consider the system of homogeneous linear equations defined by*

$$M_\ell (x_1, ..., x_\ell)^T = 0. \tag{6}$$

*Then* (6) *has a nonzero solution* $(x_1, ..., x_\ell)$ *in GF*$(q)^\ell$ *if and only if rank*$(M_\ell) < \ell$, *where rank*$(M_\ell)$ *denotes the rank of the matrix* $M_\ell$.

**Lemma 5** *Let* $m$ *be an positive integer and* $M_3$ *be the matrix given by* (5) *with* $(u_1, u_2, u_3) \in \binom{U_{q+1}}{3}$. *Then rank*$(M_3) = 3$.

***Proof 6*** *Suppose that rank*$(M_3) < 3$. *Then det*$(M_3[5]) = AA_1A_2A_3 = 0$, *where* $A = \frac{2\sigma_{3,1}\prod_{1\leq i<j\leq 3}(u_i-u_j)}{\sigma_{3,3}^5}$, $A_1 = (u_1-u_3)^2 + (u_2-u_3)^2$, $A_2 = (u_1-u_2)^2 + (u_2-u_3)^2$, $A_3 = (u_1-u_2)^2 + (u_1-u_3)^2$, *which is contrary to Lemma* 2. *This completes the proof.*

**Lemma 7** *Let* $m$ *be an positive integer and* $M_4$ *be the matrix given by* (5) *with* $(u_1, u_2, u_3, u_4) \in \binom{U_{q+1}}{4}$. *Then rank*$(M_4) = 3$ *if and only if* $\sigma_{4,2} = 0$.

***Proof 8*** *Note that* $det(M_4) = BB_1B_2B_3$,
*where* $B = \frac{2\sigma_{4,2}\prod_{1\leq i<j\leq 4}(u_i-u_j)}{\sigma_{4,4}^5}$, $B_1 = (u_1-u_2)^2(u_3-u_4)^2 + (u_1-u_3)^2(u_2-u_4)^2$, $B_2 = (u_1-u_2)^2(u_3-u_4)^2 + (u_1-u_4)^2(u_2-u_3)^2$, $B_3 = (u_1-u_3)^2(u_2-u_4)^2 + (u_1-u_4)^2(u_2-u_3)^2$.

**Lemma 9** *Let* $f(u) = Tr_{q^2/q}(a_4u^4 + a_5u^5)$ *where* $(a_4, a_5) \in GF(q^2)^2 \backslash \{\mathbf{0}\}$. *Define*

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

*Then* $|zero(f)| \leq 10$. *Moreover,* $|zero(f)| = 10$ *if and only if* $a_4 = \frac{\tau\sigma_{10,1}}{\sqrt{\sigma_{10,10}}}$ *and* $a_5 = \frac{\tau}{\sqrt{\sigma_{10,10}}}$, *where* $\{u_1, ..., u_{10}\} \in \mathfrak{B}_{\sigma_{10,2,q+1}}$ *and* $\tau \in GF(q)^*$. *In particular, the dimension of* $Tr_{q^2/q}(\mathcal{C}_m)$ *equals* 4.

**Proof 10** *When* $u \in U_{q+1}$*, one has*

$$\begin{aligned} f(u) &= Tr_{q^2/q}(a_4u^4 + a_5u^5) \\ &= a_4u^4 + a_5u^5 + (a_4u^4 + a_5u^5)^q \\ &= \frac{1}{u^5}(a_5u^{10} + a_4u^9 + a_4^q u + a_5^q). \end{aligned} \tag{7}$$

*Thus* $|zero(f)| \leq 10$*.*

*Assume that* $|zero(f)| = 10$*. From* (7)*, there exists* $\{u_1, ..., u_{10}\} \in \binom{U_{q+1}}{10}$ *such that* $f(u) = \frac{a_5\Pi_{i=1}^{10}(u+u_i)}{u^5}$*. By Vieta's formular,* $a_5\sigma_{10,1} = a_4$*,* $a_5\sigma_{10,2} = 0, ..., a_5\sigma_{10,8} = 0, a_5\sigma_{10,9} = a_4^q$ *and* $a_5\sigma_{10,10} = a_5^q$*. Thus* $a_5^{q-1} = \sigma_{10,10}, a_5 = \frac{a_5^q}{\sigma_{10,10}} = \frac{\tau}{\sqrt{\sigma_{10,10}}}$*,* $a_4 = \frac{\tau\sigma_{10,1}}{\sqrt{\sigma_{10,10}}}$*, where* $\tau \in GF(q)^*$*.*

*Conversely, assume that* $a_4 = \frac{\tau\sigma_{10,1}}{\sqrt{\sigma_{10,10}}}$*,* $a_5 = \frac{\tau}{\sqrt{\sigma_{10,10}}}$*, where* $\{u_1, ..., u_{10}\} \in \mathfrak{B}_{\sigma_{10,2,q+1}}$ *and* $\tau \in GF(q)^*$*. Then* $f(u) = \frac{a_5\Pi_{i=1}^{10}(u+u_i)}{u^5}$*. Consequently,* $zero(f) = \{u_1, ..., u_{10}\}$ *and* $|zero(f)| \leq 10$*. This completes the proof.*

**Theorem 11** *Let* $q = 3^m$ *with* $m \geq 3$*. Then the trace code* $Tr_{q^2/q}(\mathcal{C}_m)$ *has parameters* $[q+1, 4, q-9]_q$*.*

**Proof 12** *Note that*

$$\mathbf{c}(a_4, a_5) = Tr_{q^2/q}(a_4u^4 + a_5u^5).$$

*Then the dimension of* $Tr_{q^2/q}(\mathcal{C}_m))$ *is equal to* $4$ *by Lemma* $5$ *and* $6$*.*

**Theorem 13** *Let* $q = 3^m$ *with* $m \geq 3$*. Then the dual code* $(Tr_{q^2/q}(\mathcal{C}_m))^\perp$ *has parameters* $[q+1, q-3, 4]_q$*.*

**Proof 14** *Recall that* $(2)$ *says that*

$$(Tr_{q^2/q}(\mathcal{C}_m))^\perp = \mathcal{C}_m^\perp|_{GF(q)}.$$

*Thus* $\mathcal{C}_m^\perp$ *has dimension* $q-3$ *by Lemma* $6$*. Let* $U_{q+1} = \{x_1, x_2, ..., x_{q+1}\}$*.*

$$H = \begin{bmatrix} x_1^{-5} & x_2^{-5} & ... & x_{q+1}^{-5} \\ x_1^{-4} & x_2^{-4} & ... & x_{q+1}^{-4} \\ x_1^4 & x_2^4 & ... & x_{q+1}^4 \\ x_1^5 & x_2^5 & ... & x_{q+1}^5 \end{bmatrix} \tag{8}$$

$$\mathcal{C}_m^{\perp} = \{\mathbf{c} \in \mathrm{GF}(q)^{q+1} : \mathbf{c}\mathrm{H}^{\top} = \boldsymbol{0}\} \tag{9}$$

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 \\ x_{i_1} & x_{i_2} & x_{i_3} & x_{i_4} \\ x_{i_1}^9 & x_{i_2}^9 & x_{i_3}^9 & x_{i_4}^9 \\ x_{i_1}^{10} & x_{i_2}^{10} & x_{i_3}^{10} & x_{i_4}^{10} \end{bmatrix}$$

*where* $1 \le i_1 < i_2 < i_3 < i_4 \le q+1$. *We have the minimum distance d of* $\mathcal{C}_m^{\perp}$ *is* $\ge 4$ *by Lemma6and Equations* $(8), (9)$. *Next we prove that* $d = 4$. *Let* $\{x_{i_1}, x_{i_2}, x_{i_3}, x_{i_4}\} \in \binom{U_{q+1}}{4}$. *Since* $d \ge 4$, *the rank of* $M$ *is* 3. *Let* $(u_{i_1}, u_{i_2}, u_{i_3}, u_{i_4}) \in \mathrm{GF}(q)^4$ *denote a solution of* $Mx = 0$,

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ x_{i_1} & x_{i_2} & x_{i_3} & x_{i_4} \\ x_{i_1}^9 & x_{i_2}^9 & x_{i_3}^9 & x_{i_4}^9 \\ x_{i_1}^{10} & x_{i_2}^{10} & x_{i_3}^{10} & x_{i_4}^{10} \end{bmatrix} \begin{bmatrix} u_{i_1} \\ u_{i_2} \\ u_{i_3} \\ u_{i_4} \end{bmatrix} = 0 \tag{10}$$

*Since the rank of* $M$ *is* 3, *all those* $u_{i_j} \neq 0$ *Define a vector* $\mathbf{c} = (c_0, c_1, ..., c_n) \in \mathrm{GF}(q)^{n+1}$ $c_{i_j} = u_{i_j} j \in \{1, 2, 3, 4\}$ $c_h = 0$, *where* $\forall h \in \{0, 1, ..., n\} \backslash \{i_1, i_2, i_3, i_4\}$. *It is easy to observe 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* $d = 4$

**Theorem 15** *Let* $q = 3^m$ *with* $m \ge 3$. *Let* $k$ *be an integer with* $1 \le k \le q+1$ *and* $A_k(Tr_{q^2/q}(\mathcal{C}_m)) > 0$. *Then* $\mathcal{B}_k(Tr_{q^2/q}(\mathcal{C}_m))$ *is invariant under the action of* $Stab_{U_{q+1}}$. *In particular, the incidence structure* $(U_{q+1}, \mathcal{B}_k(Tr_{q^2/q}(\mathcal{C}_m)))$ *is a* $3-$*design.*

**Proof 16** *We only need to show that if* $\mathbf{c} \in Tr_{q^2/q}(\mathcal{C}_m)$ *and* $\pi$ *is a linear fractional transformation listed in Corollary* 1, *then there exists a codeword* $\mathbf{c}' \in Tr_{q^2/q}(\mathcal{C}_m)$ *such that Supp*$(\pi(\mathbf{c}))$ =*Supp*$(\mathbf{c}')$. *Denote by* $\mathbf{c}(a_4, a_5)$ *the codeword* $(Tr_{q^2/q}(a_4u^4 + a_5u^5))_{u \in U_{q+1}}$ *of* $Tr_{q^2/q}(\mathcal{C}_m)$, *where* $(a_4, a_5) \in GF(q^2)$. *We investigate the following three cases for* $\pi$.

*If* $\pi$ *is the transformation given by* $u \longmapsto u_0 u$, *where* $u_0 \in U_{q+1}$, *then it is clear that* $\pi(\mathbf{c}(a_4, a_5)) = \mathbf{c}(a_4u_0^4, a_5u_0^5)$. *Thus Supp*$(\pi(\mathbf{c}(a_4, a_5)))$ =*Supp*$(\mathbf{c}(a_4u_0^4, a_5u_0^5))$.

*If* $\pi$ *is the transformation given by* $u \longmapsto u^{-1}$, *then it is obvious that* $\pi(\mathbf{c}(a_4, a_5)) = \mathbf{c}(a_4, a_5)$. *Thus Supp*$(\pi(\mathbf{c}(a_4, a_5)))$ =*Supp*$(\mathbf{c}(a_4, a_5))$.

*Let* $\pi$ *be the transformation given by* $u \longmapsto \frac{u+c^q}{cu+1}$, *where* $c \in GF(q^2)^* \backslash U_{q+1}$. *Write* $f(u)$ =$Tr_{q^2/q}(a_4u^4 + a_5u^5)$ *and* $A = cu+1$. *Then* $u + c^q = uA^q$. *A standard computation*

*gives*

$$\begin{aligned}
&f(\frac{u+c^q}{cu+1})\\
&=Tr_{q^2/q}(a_4(\frac{u+c^q}{cu+1})^4+a_5(\frac{u+c^q}{cu+1})^5)\\
&=Tr_{q^2/q}(\frac{a_4(u+c^q)^4(cu+1)+a_5(u+c^q)^5}{(cu+1)^5})\\
&=Tr_{q^2/q}(\frac{a_4u^4A^{4q}A+a_5u^5A^{5q}}{A^5})\\
&=\frac{a_4u^4A^{4q}A+a_5u^5A^{5q}}{A^5}+\frac{a_4^qu^{4q}A^4A^q+a_5^qu^{5q}A^5}{A^{5q}}\\
&=\frac{a_4A^{9q}Au^4+a_5A^{10q}u^5+(a_4A^{9q}Au^4+a_5A^{10q}u^5}{A^5A^{5q}})^q\\
&=\frac{1}{A^5A^{5q}}Tr_{q^2/q}(a_4A^{9q}Au^4+a_5A^{10q}u^5)
\end{aligned} \tag{11}$$

*Expanding* $a_4A^{9q}Au^4$ *yields*

$$\begin{aligned}
&a_4A^{9q}Au^4\\
&=a_4(cu+1)^{9q}(cu+1)u^4\\
&=a_4(c^{9q}u^{9q}+1)(cu+1)u^4\\
&=a_4(c^{9q+1}u^{9q+1}+c^{9q}u^{9q}+cu+1)u^4\\
&=a_4(c^{9q+1}u^{-4}+c^{9q}u^{-5}+cu^5+u^4)
\end{aligned} \tag{12}$$

*Expanding* $a_5A^{10q}u^5$ *yields*

$$\begin{aligned}
&a_5A^{10q}u^5\\
&=a_5(cu+1)^{10q}u^5\\
&=a_5(c^{10q}u^{10q}+1)u^5\\
&=a_5(c^{10q}u^{-5}+u^5)
\end{aligned} \tag{13}$$

*Combing*$(9)$ *and* $(10)$ *gives*

$$\begin{aligned}
&Tr_{q^2/q}(a_4A^{9q}Au^4+a_5A^{10q}u^5)\\
&=Tr_{q^2/q}((a_4+a_4^qc^{9+q})u^4+(a_5+a_5^qc^{10}+a_4^qc^9+a_4c)u^5)
\end{aligned} \tag{14}$$

*Plugging* $(11)$ *into* $(8)$ *yields*

$$f(\tfrac{u+c^q}{cu+1})=\tfrac{1}{A^5A^{5q}}Tr_{q^2/q}(a_4'u^4+a_5'u^5)$$

*where* $a'_4 = a_4 + a_4^q c^{9+q}$ *and* $a'_5 = a_5 + a_5^q c^{10} + a_4^q c^9 + a_4 c$.
*This clearly forces Supp*$(\pi(\mathbf{c}(a_4, a_5)))$ =*Supp*$(\mathbf{c}(a'_4, a'_5))$. *The desired conclusion then follows.*

The proof of Theorem 8 gives more, namely

$$\begin{aligned} &Tr_{q^2/q}(a_4(\frac{u+c^q}{cu+1})^4 + a_5(\frac{u+c^q}{cu+1})^5) \\ &= \frac{1}{(cu+1)^5(cu+1)^{5q}} Tr_{q^2/q}(a'_4 u^4 + a'_5 u^5), \end{aligned} \tag{15}$$

where $a_4, a_5 \in GF(q^2), c \in GF(q^2)\backslash U_{q+1}$, $a'_4 = a_4 + a_4^q c^{9+q}$ and $a'_5 = a_5 + a_5^q c^{10} + a_4^q c^9 + a_4 c$.

**Theorem 17** *Let* $q = 3^m$ *with* $m \geq 3$. *Let* $k$ *be an integer with* $1 \leq k \leq q+1$ *and* $A_k(\mathcal{C}_m^\perp) > 0$. *Then* $\mathcal{B}_k(\mathcal{C}_m^\perp)$ *is invariant under the action of Stab*$_{U_{q+1}}$. *In particular, the incidence structure* $(U_{q+1}, \mathcal{B}_k(\mathcal{C}_m^\perp)$ *is a* $3-$*design.*

**Proof 18** $\mathcal{C}_m^\perp|_{GF(q)} = (Tr_{q^2/q}(\mathcal{C}_m))^\perp$
*Let* $\mathbf{w}$ *be any codeword of* $\mathcal{C}_m^\perp|_{GF(q)} = (Tr_{q^2/q}(\mathcal{C}_m))^\perp$ *and* $\pi$ *be any linear fractional translations listed in Corollary* 1. *It is easily seen that if* $\pi$ *is a transformation given by* $u \longmapsto u_0 u$ *or* $u \longmapsto u^{-1}$, *where* $u_0 \in U_{q+1}$, *then*

$$\pi(\mathbf{w}) \in \mathcal{C}_m^\perp|_{GF(q)}. \tag{16}$$

*Assume* $\pi$ *is a translation given by* $u \longmapsto \frac{u+c^q}{cu+1}$, *where* $c \in GF(q^2)^*\backslash U_{q+1}$. *It is obvious that* $\pi(\mathbf{w}) \in (\pi(Tr_{q^2/q}(\mathcal{C}_m)))^\perp$. *From* (12) *we conclude that*

$$\pi(Tr_{q^2/q}(\mathcal{C}_m)) = (\tfrac{1}{(cu+1)^{5q+5}})_{u \in U_{q+1}} \cdot Tr_{q^2/q}(\mathcal{C}_m).$$

$$(\pi(Tr_{q^2/q}(\mathcal{C}_m)))^\perp = ((cu+1)^{5q+5})_{u \in U_{q+1}} \cdot (Tr_{q^2/q}(\mathcal{C}_m))^\perp.$$

*Consequently,*

$$\pi(\mathbf{w}) \in ((cu+1)^{5q+5})_{u \in U_{q+1}} \cdot (Tr_{q^2/q}(\mathcal{C}_m))^\perp. \tag{17}$$

**Example 19** $\mathcal{C}_3$ *is a* $[28, 4, 24]$ *cyclic linear code over GF*$(3^3)$ *and its dual code* $\mathcal{C}_3^\perp$ *is a* $[28, 24, 4]$ *cyclic linear code over GF*$(3^3)$.

**Example 20** $\mathcal{C}_4$ *is a* $[82, 4, 72]$ *cyclic linear code over GF*$(3^4)$ *and its dual code* $\mathcal{C}_4^\perp$ *is a* $[82, 78, 4]$ *cyclic linear code over GF*$(3^4)$.

**Example 21** $\mathcal{C}_5$ *is a* $[244, 4, 240]$ *cyclic linear code over GF*$(3^5)$. $\mathcal{C}_6$ *is a* $[730, 4, 720]$ *cyclic linear code over GF*$(3^6)$.

## 3. CONCLUDING REMARKS

In this paper, we investigated a class of cyclic codes $\mathrm{Tr}_{q^2/q}(\mathcal{C}_m)$ over $GF(3^q)$, and determined their parameters. The results showed that the code $\mathrm{Tr}_{q^2/q}(\mathcal{C}_m)$ has nonzero weight and supports $3-$designs. Meanwhile, the dual code of $\mathrm{Tr}_{q^2/q}(\mathcal{C}_m)$ also supports $3-$designs, and the automorphism group of the code $\mathrm{Tr}_{q^2/q}(\mathcal{C}_m)$ and its dual $(\mathrm{Tr}_{q^2/q}(\mathcal{C}_m))^{\perp}$ are $3-$transitive.

## REFERENCES

[1] T. Beth, D. Jungnickel, H. Lenz, Design Theory, Cambridge University Press, Cambridge,1999.

[2] C.Tang,C.Ding,An infinite family of linear codes supporting 4-designs,IEEE Trans.Inform.Theory 67(1),244-254,2021.

[3] C.Ding,Designs from Linear Codes,World Scientific,Singapore,2018.

[4] C.Ding,C.Tang,V.D.Tonchev,The Projective General Linear Group PGL$(2, 2^m)$ and Linear Codes of Length $2^m + 1$,Des.Codes Cryptogr.89(7),1713-1734,2021

[5] C.Xiang,C.Tang,Q.Liu,An infinite family of antiprimitive cyclic codes supporting Steiner system S$(3, 8, 7^m + 1)$.arXiv:2110.03881, 2021.

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

[7] 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.

[8] C. Ding, C. Tang, "Infinite families of near MDS codes holding t-designs," IEEE Trans. Inform. Theory, vol. 66, no. 9, pp. 5419-C5428, 2020.

[9] E. F. Assmus Jr. and H. F. Mattson Jr., "New 5-designs," J. Comb. Theory Ser. A, vol. 6, no. 2, pp 122-C151, 1969.

[10] C. Ding, "Infinite families of 3-designs from a type of five-weight code," Des. Codes Cryptogr., vol. 86, no. 3, pp. 703-C719, 2018.

[11] C. Ding and C. Tang, "Combinatorial t-designs from special functions," Cryptography and Communications, vol. 12, no. 5, pp. 1011-C 1033, 2020.

[12] R. Lidl and H. Niederreiter, Finite Fields. Cambridge: Cambridge University Press, 1997.

[13] 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-C1268, 1998.