Designs, Codes and Cryptography (2021) 89:1713–1734
https://doi.org/10.1007/s10623-021-00888-2

The projective general linear group $\mathrm{PGL}(2, 2^m)$ and linear codes of length $2^m + 1$

Cunsheng Ding[1] · Chunming Tang[1,2] · Vladimir D. Tonchev[3]

Received: 19 October 2020 / Revised: 19 April 2021 / Accepted: 3 May 2021 / Published online: 21 May 2021

Abstract
Let $q = 2^m$. The projective general linear group $\mathrm{PGL}(2, q)$ acts as a 3-transitive permutation group on the set of points of the projective line. The first objective of this paper is to prove that all linear codes over $\mathrm{GF}(2^h)$ that are invariant under $\mathrm{PGL}(2, q)$ are trivial codes: the repetition code, the whole space $\mathrm{GF}(2^h)^{2^m+1}$, and their dual codes. As an application of this result, the 2-ranks of the (0,1)-incidence matrices of all $3-(q+1, k, \lambda)$ designs that are invariant under $\mathrm{PGL}(2, q)$ are determined. The second objective is to present two infinite families of cyclic codes over $\mathrm{GF}(2^m)$ such that the set of the supports of all codewords of any fixed nonzero weight is invariant under $\mathrm{PGL}(2, q)$, therefore, the codewords of any nonzero weight support a 3-design. A code from the first family has parameters $[q+1, q-3, 4]_q$, where $q = 2^m$, and $m \geq 4$ is even. The exact number of the codewords of minimum weight is determined, and the codewords of minimum weight support a 3-$(q+1, 4, 2)$ design. A code from the second family has parameters $[q+1, 4, q-4]_q$, $q = 2^m$, $m \geq 4$ even, and the minimum weight codewords support a 3-$(q+1, q-4, (q-4)(q-5)(q-6)/60)$ design, whose complementary 3-$(q+1, 5, 1)$ design is isomorphic to the Witt spherical geometry with these parameters. A lower bound on the dimension of a linear code over $\mathrm{GF}(q)$ that can support a 3-$(q+1, q-4, (q-4)(q-5)(q-6)/60)$ design is proved, and it is shown that

---

Communicated by J. W. P. Hirschfeld.

C. Ding's research was supported by the Hong Kong Research Grants Council, Proj. No. 16300418. C. Tang's research was supported by The National Natural Science Foundation of China (Grant No. 11871058) and China West Normal University (14E013, CXTD2014-4 and the Meritocracy Research Funds).

✉ Chunming Tang
tangchunmingmath@163.com

Cunsheng Ding
cding@ust.hk

Vladimir D. Tonchev
tonchev@mtu.edu

1 Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong, China

2 School of Mathematics and Information, China West Normal University, Nanchong 637002, Sichuan, China

3 Department of Mathematical Sciences, Michigan Technological University, Houghton, MI 49931, USA

the designs supported by the codewords of minimum weight in the codes from the second family of codes meet this bound.

Keywords Cyclic code · Linear code · t-design · Projective general linear group · Automorphism group

Mathematics Subject Classification 05B05 · 51E10 · 94B15

1 Introduction

A $t-(v,k,\lambda)$ design is an incidence structure $(X,\mathcal{B})$, where X is a set of v points and $\mathcal{B}$ a set of b k-subsets of X called blocks, such that any t points are contained in exactly λ blocks, where $\lambda > 0$. A t-design is a $t-(v,k,\lambda)$ design for some parameters v, k, λ. A $t-(v,k,\lambda)$ design is also an $s-(v,k,\lambda_s)$ design for every $0 \le s < t$, where

$$\lambda_s = \frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}}\lambda.$$

In particular, the number of blocks is equal to

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

The incidence matrix $A = (a_{i,j})$ of a design $\mathbb{D}$ is a (0,1)-matrix with rows indexed by the blocks, and columns indexed by the points of $\mathbb{D}$, where $a_{i,j} = 1$ if the jth point belongs to the ith block, and $a_{i,j} = 0$ otherwise. If q is a prime power, the q-rank of $\mathbb{D}$ (or $\mathrm{rank}_q\mathbb{D}$) is defined as the rank of its incidence matrix A over a finite field GF(q) of order q: $\mathrm{rank}_q\mathbb{D} = \mathrm{rank}_q A$. Equivalently, the q-rank of a design is the dimension of the linear q-ary code spanned by the rows of its (0,1)-incidence matrix.

A *generalized* incidence matrix of a design $\mathbb{D}$ over a finite field GF(q), or shortly, an GF(q)-incidence matrix of $\mathbb{D}$, is any matrix obtained by replacing the nonzero entries of the (0,1)-incidence matrix of $\mathbb{D}$ with arbitrary nonzero elements of GF(q). The *dimension* of a $t-(v,k,\lambda)$ design $\mathbb{D}$ over GF(q) (or the q-dimension of $\mathbb{D}$, or $\dim_q \mathbb{D}$), is defined in [21] as the minimum among the dimensions of all linear codes of length v over GF(q) that contain the blocks of $\mathbb{D}$ among the supports of codewords of weight w. Equivalently, the q-dimension of $\mathbb{D}$ is equal to

$$\dim_q \mathbb{D} = \min\ \mathrm{rank}_q M,$$

where M runs over the set of all $(q-1)^{bk}$ generalized GF(q)-incidence matrices of $\mathbb{D}$, and b is the number of blocks. Clearly, $\dim_q \mathbb{D} \le \mathrm{rank}_q\mathbb{D}$. For example, if $\mathbb{D}$ is the 4-$(11,5,1)$ design supported by the codewords of minimum weight in the ternary Golay code of length 11 and dimension 6, $\dim_3 \mathbb{D} = 6$, while $\mathrm{rank}_3\mathbb{D} = 11$. A generalization of this definition of the q-dimension of a design is given in [15].

The importance of interactions between groups, linear codes and t-designs has been well recognized for decades. For example, Assmus and Mattson [1] pointed out in 1969 that 5-designs arise from certain extremal self-dual codes, including the extended Golay codes that are closely related to the 5-transitive Mathieu groups. Linear codes that are invariant under groups acting on the set of code coordinates have found important applications for the construction of combinatorial t-designs. Examples of such codes are the Golay codes, the quadratic-residue codes, and the affine-invariant codes [7, Chapter 6].

This paper presents a number of new results about 3-designs arising from linear codes associated with the projective general linear group PGL$(2, q)$.

Let PGL$(2, q)$ be 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 $(c_x)_{x\in \mathrm{PG}(1,q)}$, where $c_x \in$ GF(r) and r is a prime power. In other words, the coordinates of the vectors in GF$(r)^{q+1}$ can be indexed by the points in PG$(1, q)$. Consider the induced action of PGL$(2, q)$ on GF$(r)^{q+1}$ by the left translation:

$$\pi : (c_x)_{x\in \mathrm{PG}(1,q)} \mapsto (c_{\pi(x)})_{x\in \mathrm{PG}(1,q)},$$

where $(c_x)_{x\in \mathrm{PG}(1,q)} \in \mathrm{GF}(r)^{q+1}$ and $\pi \in \mathrm{PGL}(2, q)$. Let $\mathcal{C}$ be a linear code of length $q + 1$ over GF(r). We say that $\mathcal{C}$ is *invariant under* PGL$(2, q)$ if each element of PGL$(2, q)$ carries each codeword of $\mathcal{C}$ into a codeword of $\mathcal{C}$. In other words, $\mathcal{C}$ is invariant under PGL$(2, q)$ if $\mathcal{C}$ admits PGL$(2, q)$ as a subgroup of the permutation automorphism group of $\mathcal{C}$. For a codeword $\mathbf{c} = (c_x)_{x\in \mathrm{PG}(1,q)}$ 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 $\mathcal{B}_w(\mathcal{C}) = \{\mathrm{Supp}(\mathbf{c}) : wt(\mathbf{c}) = w \text{ and } \mathbf{c} \in \mathcal{C}\}$, where $wt(\mathbf{c})$ denotes the Hamming weight of $\mathbf{c}$. $\mathcal{B}_w(\mathcal{C})$ is said to be invariant under PGL$(2, q)$ if the support Supp $\left((c_{\pi(x)})_{x\in \mathrm{PG}(1,q)}\right)$ belongs to $\mathcal{B}_w(\mathcal{C})$ for every $\pi \in$ PGL$(2, q)$ and any codeword $(c_x)_{x\in \mathrm{PG}(1,q)}$ of weight w in $\mathcal{C}$. It is easily seen that if $\mathcal{C}$ is invariant under PGL$(2, q)$, then so is $\mathcal{B}_w(\mathcal{C})$ for each w. Moreover, if $\mathcal{B}_w(\mathcal{C})$ is invariant under PGL$(2, q)$, then (PG$(1, q)$, $\mathcal{B}_w(\mathcal{C})$) holds a 3-design provided $A_w(\mathcal{C}) \neq 0$, since the action of PGL$(2, q)$ on PG$(1, q)$ is 3-transitive (see [2, Propositions 4.6 and 4.8] or [22, Proposition 1.27]). For more related results on linear codes and t-designs, we refer the reader to [7,9].

The first objective of this paper is to investigate the possible parameters of linear codes that are invariant under PGL$(2, q)$. We focus on the case when q and r are powers of 2. We prove in Sect. 4, Theorem 11, that the only linear codes of length $2^m + 1$ over GF(2^h) that are invariant under PGL$(2, q)$ are trivial codes: the zero code, the whole space GF$(2^h)^{2^m+1}$, the repetition code, and its dual code. As an application of this result, the 2-ranks of the (0,1)-incidence matrices of all $3 - (q + 1, k, \lambda)$ designs that are invariant under PGL$(2, q)$ are determined, and it is proved in Theorem 12 that any such design has 2-rank equal to $q+1$ if the block size k is odd, and q if k is even.

The second objective of this paper is to investigate the question whether there are any nontrivial linear codes of length $2^m + 1$ over GF(2^m), such that the set of the supports of all codewords of any fixed nonzero weight is invariant under PGL$(2, q)$. In Sect. 5, we answer this question in the affirmative by presenting two infinite families of cyclic codes of length $2^m + 1$ over GF(2^m), such that the set of the supports of the codewords of any fixed weight is invariant under PGL$_2$(GF(2^m)), therefore, the codewords of any nonzero weight support a 3-design. These codes are obtained as subfield subcodes and trace codes of certain cyclic codes over GF(2^{2m}) and their dual codes (Theorems 21 and 22).

A code from the first family has parameters $[q + 1, q - 3, 4]_q$, where $q = 2^m$, and $m \geq 4$ is even. The exact number of the codewords of minimum weight is determined, and the codewords of minimum weight support a 3-$(q + 1, 4, 2)$ design. To the best knowledge of the authors, this is the first infinite family of linear codes that support an infinite family of $3 - (v, 4, 2)$ designs. The codewords of every other nonzero weight also support 3-designs.

A code from the second family has parameters $[q+1, 4, q-4]$, $q = 2^m$, $m \geq 4$ even. The exact number of the codewords of minimum weight is determined, and the minimum weight codewords support a 3-$(2^m+1, q-4, \lambda)$ design with

$$\lambda = \frac{(q-4)(q-5)(q-6)}{60},$$

whose complementary 3-$(q+1, 5, 1)$ design is shown to be isomorphic to the Witt spherical geometry with these parameters. In Sect. 6, a lower bound on the q-dimension of a 3-$(q+1, (q-4), (q-4)(q-5)(q-6)/60)$ design is proved in Theorem 30, and it is shown that the infinite family of 3-designs described in Theorem 25 meet this bound.

2 Preliminaries

2.1 Group actions and *t*-designs

A *permutation group* is a subgroup of the *symmetric group* $\mathrm{Sym}(X)$, where X is a finite set. More generally, an *action* σ of a finite group G on a set X is a homomorphism σ from G to $\mathrm{Sym}(X)$. We denote the image $\sigma(g)(x)$ of $x \in X$ under $g \in G$ by $g(x)$ when no confusion can arise. The *G-orbit* of $x \in X$ is $\mathrm{Orb}_x = \{g(x) : g \in G\}$. The *stabilizer* of x is $\mathrm{Stab}_x = \{g \in G : g(x) = x\}$. The length of the orbit of x is given by

$$|\mathrm{Orb}_x| = |G| \,/\, |\mathrm{Stab}_x| \,.$$

One criterion to measure the level of symmetry is the *degree* of *transitivity* and *homogeneousity* of the group. Recall that a group G acting on a set X is *t-transitive* if for any two ordered t-tuples $(x_1, \ldots, x_t)$, $(x_1', \ldots, x_t')$ of distinct elements from X there is some $g \in G$ such that $\left(x_1', \ldots, x_t'\right) = (g(x_1), \ldots, g(x_t))$. And it is *t-homogeneous* if for any two unordered t-subsets $\{x_1, \ldots, x_t\}$, $\{x_1', \ldots, x_t'\}$ of X there is some $g \in G$ such that $\left\{x_1', \ldots, x_t'\right\} = \{g(x_1), \ldots, g(x_t)\}$.

We recall a well-known general fact (see, e.g. [2, Proposition 4.6]), that for a t-homogeneous group G on a finite set X with $|X| = v$ and a subset B of X with $|B| = k > t$, the pair (X, Orb_B) is a $t-(v, k, \lambda)$ design, where Orb_B is the set of images of B under the group G, $\lambda = \frac{\binom{k}{t}|G|}{\binom{v}{t}|\mathrm{Stab}_B|}$ and Stab_B is the setwise stabilizer of B in X. Let $\binom{X}{k}$ be the set of subsets of X consisting of k elements. A nonempty subset $\mathcal{B}$ of $\binom{X}{k}$ is called *invariant* under G if $\mathrm{Orb}_B \subseteq \mathcal{B}$ for any $B \in \mathcal{B}$. If this is the case, it means that the pair $(X, \mathcal{B})$ is a $t-(v, k, \lambda)$ design admitting G as an automorphism group for some λ. For some recent works on t-designs from group actions, we refer the reader to [19,24].

2.2 Projective general linear groups of degree two

The *projective linear group* $\mathrm{PGL}(2, q)$ *of degree two* 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 $a \in \mathrm{GF}(q)^*$. Note that the group $\mathrm{PGL}(2, q)$ is generated by the matrices $\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}$, $\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, where $a \in \mathrm{GF}(q)^*$ and $b \in \mathrm{GF}(q)$.

Table 1 Subgroups of PGL$(2, q)$

Type	Maximal order	Number of conjugacy classes	Condition
2-group	2^m	–	–
Frobenius	$2^m(2^m-1)$	–	–
Cyclic	2^m+1	one	–
Dihedral	$2(2^m-1)$	one	–
Dihedral	$2(2^m+1)$	one	–
$\mathrm{PGL}_2(\mathrm{GF}(2^{m'}))$	$2^{m'}(4^{m'}-1)$	one	$m' \mid m$
A_4	12	–	$2 \mid m$
A_5	60	–	$2 \mid m$

Here the following convention for the action of PGL$(2, q)$ on the projective line PG$(1, q)$ is used. A matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{PGL}(2, q)$ acts on PG$(1, q)$ by

$$(x_0 : x_1) \mapsto \begin{bmatrix} a & b \\ c & d \end{bmatrix}(x_0 : x_1) = (ax_0 + bx_1 : cx_0 + dx_1), \tag{1}$$

or, via the usual identification of GF$(q) \cup \{\infty\}$ with PG$(1, q)$, by linear fractional transformation

$$x \mapsto \tfrac{ax+b}{cx+d}. \tag{2}$$

This is an action on the left, i.e., for $\pi_1, \pi_2 \in \mathrm{PGL}(2, q)$ and $x \in \mathrm{PG}(1, q)$ the following holds: $\pi_1(\pi_2(x)) = (\pi_1\pi_2)(x)$. The action of PGL$(2, q)$ on PG$(1, q)$ defined in (2) is sharply 3-transitive, i.e., for any distinct $a, b, c \in \mathrm{GF}(q) \cup \{\infty\}$ there is $\pi \in \mathrm{PGL}(2, q)$ taking ∞ to a, 0 to b, and 1 to c. In fact, π is uniquely determined and it equals

$$\pi = \begin{bmatrix} a(b-c) & b(c-a) \\ b-c & c-a \end{bmatrix}.$$

Thus, PGL$(2, q)$ is in one-to-one correspondence with the set of ordered triples (a, b, c) of distinct elements in GF$(q) \cup \{\infty\}$, and in particular

$$|\mathrm{PGL}(2, q)| = (q+1)q(q-1). \tag{3}$$

Two subgroups H_1 and H_2 of a group G are said to be *conjugate* if there is a $g \in G$ such that $gH_1g^{-1} = H_2$. It is easily seen that this conjugate relation is an equivalence relation on the set of all subgroups of G, and is called the conjugacy. The conjugacy classification of subgroups of PGL$(2, q)$ is well known [5]. Table 1 specifies all the subgroups of PGL$(2, q)$ up to conjugacy.

We recall here the classification of sharply 3-transitive finite permutation groups on finite sets of odd cardinality (see for instance [17]).

Theorem 1 *Let G be a sharply 3-transitive permutation group on the finite set X of odd cardinality. Then it is possible to identify the elements of X with the points of the projective line* PG$(1, 2^m)$ *in such a way that $G = \mathrm{PGL}(2, q)$ holds.*

2.3 Linear codes and cyclic codes

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 $\mathcal{C}$:

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

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

$$(\mathbf{a} \cdot \mathcal{C})^\perp = \mathbf{a}^{-1} \cdot \mathcal{C}^\perp, \tag{4}$$

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

There are two classical ways to construct a code over $\mathrm{GF}(r)$ from a given code over $\mathrm{GF}(r^h)$. Let $\mathcal{C}$ be a code of length n over $\mathrm{GF}(r^h)$. Then the *subfield subcode* $\mathcal{C}|_{\mathrm{GF}(r)}$ equals $\mathcal{C} \cap \mathrm{GF}(r)^n$, the set of those codewords of $\mathcal{C}$ all of whose coordinate entries belong to the subfield $\mathrm{GF}(r)$. The *trace code* of $\mathcal{C}$ is given by

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

where $\mathrm{Tr}_{r^h/r}$ denotes the trace function from $\mathrm{GF}(r^h)$ to $\mathrm{GF}(r)$. A celebrated result of Delsarte [6] states that the subfield code $\mathcal{C}^\perp|_{\mathrm{GF}(r)}$ and the trace code $\mathrm{Tr}_{r^h/r}(\mathcal{C})$ are duals of each other, namely,

$$\left(\mathrm{Tr}_{r^h/r}(\mathcal{C})\right)^\perp = \mathcal{C}^\perp\Big|_{\mathrm{GF}(r)}. \tag{5}$$

Conversely, given a linear code $\mathcal{C}$ of length n and dimension k over $\mathrm{GF}(r)$, we define a linear code $\mathrm{GF}(r^h) \otimes \mathcal{C}$ over $\mathrm{GF}(r^h)$ by

$$\mathrm{GF}(r^h) \otimes \mathcal{C} = \left\{\sum_{i=1}^{k} a_i \mathbf{c}_i : (a_1, a_2, \ldots, a_k) \in \mathrm{GF}(r^h)^k\right\}, \tag{6}$$

where $\{\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_k\}$ is a basis of $\mathcal{C}$ over $\mathrm{GF}(r)$. This code is independent of the choice of the basis $\{\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_k\}$ of $\mathcal{C}$, is called the *lifted code* of $\mathcal{C}$ to $\mathrm{GF}(r^h)$. Clearly, $\mathrm{GF}(r^h) \otimes \mathcal{C}$ and $\mathcal{C}$ have the same length, dimension and minimum distance, but different weight distributions. A trivial verification shows that if $(c_0, \ldots, c_{n-1}) \in \mathrm{GF}(r^h) \otimes \mathcal{C}$, then $(c_0^r, \ldots, c_{n-1}^r) \in \mathrm{GF}(r^h) \otimes \mathcal{C}$. Applying [10, Lemma 7], one has

$$\mathrm{Tr}_{r^h/r}\left(\mathrm{GF}(r^h) \otimes \mathcal{C}\right) = \left(\mathrm{GF}(r^h) \otimes \mathcal{C}\right)\Big|_{\mathrm{GF}(r)}.$$

Let n be a positive integer with $\gcd(n, r) = 1$. The *order* $\mathrm{ord}_n(r)$ of r modulo n is the smallest positive integer h such that $r^h \equiv 1 \pmod{n}$. Let $\mathbb{Z}_n$ denote the ring of residue classes of integers modulo n. The r-cyclotomic coset of $e \in \mathbb{Z}_n$ is the set $[e]_{(r,n)} = \{r^i e : 0 \le i \le \mathrm{ord}_n(r) - 1\}$. Then any two r-cyclotomic cosets are either equal or disjoint. A subset E of $\mathbb{Z}_n$ is called r-invariant if the set $\{re : e \in E\}$ equals E, that is, E is the union of some r-cyclotomic cosets. A subset $\widetilde{E} = \{e_1, \ldots, e_t\}$ of an r-invariant set E is called a complete set of representatives of r-cyclotomic cosets of E if $[e_1]_{(r,n)}, \ldots, [e_t]_{(r,n)}$ are pairwise distinct and $E = \cup_{i=1}^t [e_i]_{(r,n)}$.

An $[n,k]_r$ code $\mathcal{C}$ is *cyclic* if $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ implies that $(c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$. Let γ be a primitive n-th root of unity in $\mathrm{GF}(r^h)$, where $h = \mathrm{ord}_n(r)$. It is known [12] that any r-ary cyclic code of length n with $\gcd(n, r) = 1$ has a simple description by means of the trace function.

Theorem 2 *Let $\mathcal{C}$ be an $[n, k]_r$ cyclic code with $\gcd(n, r) = 1$ and γ be a primitive n-th root of unity in $\mathrm{GF}(r^h)$, where $h = \mathrm{ord}_n(r)$. Then there exists a unique r-invariant set $E \subseteq \mathbb{Z}_n$ such that*

$$\mathcal{C} = \left\{ \left(\sum_{i=1}^{t} \mathrm{Tr}_{r^{h_i}/r} \left(a_i \gamma^{e_i j} \right) \right)_{j=0}^{n-1} : a_i \in \mathrm{GF}\left(r^{h_i} \right) \right\},$$

where $\{e_1, \ldots, e_t\}$ is any complete set of representatives of r-cyclotomic cosets of E and $h_i = |[e_i]_{(r,n)}|$. Moreover, $k = |E| = \sum_{i=1}^{t} h_i$.

Theorem 2 states that there is a one-to-one correspondence between cyclic linear codes over $\mathrm{GF}(r)$ with length n and r-invariant subsets of $\mathbb{Z}_n$ with respect to a fixed n-th root of unity γ. We will call the set E in Theorem 2 the *cyclicity-defining set* of $\mathcal{C}$ with respect to γ.

The following corollary is an immediate consequence of Theorem 2.

Corollary 3 *Let n be a positive integer such that $\gcd(n, r) = 1$. Let $\mathcal{C}$ be an $[n, k]_r$ cyclic code with cyclicity-defining set E and $\mathrm{GF}(r^\ell) \otimes \mathcal{C}$ be the lifted code of $\mathcal{C}$ to $\mathrm{GF}(r^\ell)$. Then $\mathrm{GF}(r^\ell) \otimes \mathcal{C}$ is an $[n, k]_{r^\ell}$ cyclic code defined by the cyclicity-defining set E of $\mathcal{C}$. In particular,*

$$\mathrm{GF}(r^h) \otimes \mathcal{C} = \left\{ \left(\sum_{e \in E} a_e \gamma^{je} \right)_{j=0}^{n-1} : a_e \in \mathrm{GF}\left(r^h \right) \right\},$$

where $h = \mathrm{ord}_n(r)$ and γ is a primitive n-th root of unity in $\mathrm{GF}(r^h)$.

Since the set E also defines the code $\mathrm{GF}(r^\ell) \otimes \mathcal{C}$ in Corollary 3, the set E is also called the cyclicity-defining set of the lifted code $\mathrm{GF}(r^\ell) \otimes \mathcal{C}$.

Let n be a positive integer with $\gcd(n, r) = 1$ and $h = \mathrm{ord}_n(r)$. Let U_n be the cyclic multiplicative group of all n-th roots of unity in $\mathrm{GF}(r^h)$. By polynomial interpolation, every function f from U_n to $\mathrm{GF}(r)$ has a unique *univariate polynomial expansion* of the form

$$f(u) = \sum_{i=0}^{n-1} a_i u^i,$$

where $a_j \in \mathrm{GF}(r^h)$, $u \in U_n$.

As a direct result of Theorem 2, we have the following conclusion concerning cyclicity-defining sets of cyclic codes.

Corollary 4 *Let n be a positive integer with $\gcd(n, r) = 1$, $h = \mathrm{ord}_n(r)$ and γ a primitive n-th root of unity in $\mathrm{GF}(r^h)$. Let $\mathcal{C}$ be an $[n, k]_r$ cyclic code with cyclicity-defining set E. Let $f(u) = \sum_{i=0}^{n-1} a_i u^i \in \mathrm{GF}(r^h)[u]$. If $\left(f(\gamma^j) \right)_{j=0}^{n-1} \in \mathcal{C}$ and $a_i \neq 0$, then $i \in E$.*

3 Another representation of the action of PGL(2, q) on the projective line PG(1, 2^m)

In this section we give another representation of the action of $\mathrm{PGL}(2, q)$ on the projective line $\mathrm{PG}(1, 2^m)$. This new representation will play an important role in Sects. 4 and 5.

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

Proposition 5 *Let $q=2^m$. Then the setwise stabilizer $\mathrm{Stab}_{U_{q+1}}$ of U_{q+1} consists of the following three types of linear fractional transformations:*

(I) $u\mapsto u_0u$, *where* $u_0\in U_{q+1}$*;*
(II) $u\mapsto u_0u^{-1}$, *where* $u_0\in U_{q+1}$*;*
(III) $u\mapsto \frac{u+c^qu_0}{cu+u_0}$, *where* $u_0\in U_{q+1}$ *and* $c\in \mathrm{GF}(q^2)^*\setminus U_{q+1}$.

Proof First, the transformations listed in (I)–III) are easily seen to belong to the stabilizer $\mathrm{Stab}_{U_{q+1}}$.

Conversely, let π be a translation in $\mathrm{PGL}_2(\mathrm{GF}(q^2))$ given by $\frac{ax+b}{cx+d}$, where $a,b,c,d\in \mathrm{GF}(q^2)$ and $ad+bc\neq 0$. Then $\pi\in\mathrm{Stab}_{U_{q+1}}$ if and only if the following holds

$$\left(\frac{au+b}{cu+d}\right)^{q+1}=1,\ \text{for all } u\in U_{q+1}. \tag{7}$$

Multiplying both sides of (7) by $(cu+d)^{q+1}$ yields

$$(a^{q+1}+c^{q+1})u^{q+1}+(a^qb+c^qd)u^q+(ab^q+cd^q)u+(b^{q+1}+d^{q+1})=0.$$

Substituting u^{-1} for u^q in the equation above yields

$$(ab^q+cd^q)u^2+(a^{q+1}+b^{q+1}+c^{q+1}+d^{q+1})u+(a^qb+c^qd)=0. \tag{8}$$

Since the quadratic equation in (8) has at least $q+1$ roots: $u\in U_{q+1}$, all its coefficients must be zero, that is

$$\begin{cases} ab^q+cd^q &=0,\\ a^qb+c^qd &=0,\\ a^{q+1}+b^{q+1}+c^{q+1}+d^{q+1} &=0. \end{cases} \tag{9}$$

We investigate the following three cases for (9).

If $b=0$, (9) clearly forces $c=0$. Thus $\pi=u_0x$ for some $u_0\in U_{q+1}$.

If $a=0$, (9) clearly forces $d=0$. Thus $\pi=u_0x^{-1}$ for some $u_0\in U_{q+1}$.

If $ab\neq 0$, we can certainly assume that $a=1$, because $\frac{ax+b}{cx+d}$ and $\frac{x+a^{-1}b}{a^{-1}cx+a^{-1}d}$ determine the same translation. Substituting 1 for a in (9) we conclude that

$$\begin{cases} b+c^qd &=0\\ 1+b^{q+1}+c^{q+1}+d^{q+1} &=0 \end{cases}.$$

This gives $b=c^qd$ and $(c^{q+1}+1)(c^{q+1}+1)=0$. If $c^{q+1}=1$, we would have $ad+bc=0$, a contradiction. It follows that $b=c^qd$, $d^{q+1}=1$ and $c\in\mathrm{GF}(q^2)^*\setminus U_{q+1}$ from $ad+bc\neq 0$. This completes the proof. □

The following result follows from Proposition 5 directly.

Corollary 6 *Let $q=2^m$. Then the setwise stabilizer $\mathrm{Stab}_{U_{q+1}}$ of U_{q+1} is generated by the following three types of linear fractional transformations:*

(I) $u\mapsto u_0u$, *where* $u_0\in U_{q+1}$*;*
(II) $u\mapsto u^{-1}$*;*

(III) $u \mapsto \frac{u+c^q}{cu+1}$, *where* $c \in \mathrm{GF}(q^2)^* \setminus U_{q+1}$.

The following proposition shows that the action of $\mathrm{Stab}_{U_{q+1}}$ on U_{q+1} and the action of $\mathrm{PGL}(2, q)$ on $\mathrm{PG}(1, 2^m)$ are equivalent.

Proposition 7 *Let* $q = 2^m$ *and* $\mathrm{Stab}_{U_{q+1}}$ *the setwise stabilizer of* U_{q+1}*. Then* $\mathrm{Stab}_{U_{q+1}}$ *is conjugate in* $\mathrm{PGL}_2(\mathrm{GF}(2^{2m}))$ *to the group* $\mathrm{PGL}(2, q)$*, and its action on* U_{q+1} *is equivalent to the action of* $\mathrm{PGL}(2, q)$ *on* $\mathrm{PG}(1, 2^m)$.

Proof We begin by proving that the group $\mathrm{Stab}_{U_{q+1}}$ acts sharply 3-transitively on U_{q+1}. It suffices to show that this action is 3-transitive as $\mathrm{PGL}_2(\mathrm{GF}(2^{2m}))$ acts sharply 3-transitively on $\mathrm{PG}(1, 2^{2m})$. Let (u_1, u_2, u_3), (u'_1, u'_2, u'_3) be any two 3-tuples of distinct elements from U_{q+1}. Since the action of $\mathrm{PGL}_2(\mathrm{GF}(2^{2m}))$ on $\mathrm{PG}(1, 2^{2m})$ is 3-transitive, there exists a linear fractional transformation $\frac{ax+b}{cx+d} \in \mathrm{PGL}_2(\mathrm{GF}(2^{2m}))$ such that

$$\frac{au_i + b}{cu_i + d} = u'_i \text{ for } i = 1, 2, 3.$$

This gives

$$\left(\frac{au_i + b}{cu_i + d}\right)^{q+1} = 1, \text{ where } i = 1, 2, 3.$$

Using a similar argument to Proposition 5, we can prove that the transformation given by $u \mapsto \frac{au+b}{cu+d}$ belongs to $\mathrm{Stab}_{U_{q+1}}$, which says that the action of $\mathrm{Stab}_{U_{q+1}}$ on U_{q+1} is 3-transitive. Therefore the action of $\mathrm{Stab}_{U_{q+1}}$ on U_{q+1} is equivalent to the action of $\mathrm{PGL}(2, q)$ on $\mathrm{PG}(1, 2^m)$ by Theorem 1. Now Table 1 shows that $\mathrm{Stab}_{U_{q+1}}$ is conjugate to the subgroup $\mathrm{PGL}(2, q)$ in $\mathrm{PGL}_2(\mathrm{GF}(2^{2m}))$. This completes the proof. □

4 Linear codes invariant under PGL(2, *q*)

The main objective of this section is to classify all linear codes over $\mathrm{GF}(2^h)$ of length $2^m + 1$ that are invariant under $\mathrm{PGL}(2, q)$. As an immediate application, we derive the 2-rank of the incidence matrices of $t - (2^m + 1, k, \lambda)$ designs that are invariant under $\mathrm{PGL}(2, q)$.

Let $\mathcal{C}$ be a $[2^m + 1, k]_{2^h}$ linear code. We can regard U_{2^m+1} as the set of the coordinate positions of $\mathcal{C}$ and write the codeword of $\mathcal{C}$ as $(c_u)_{u \in U_{2^m+1}}$. Then the set of coordinate positions of $\mathcal{C}$ could be endowed with the action of $\mathrm{Stab}_{U_{2^m+1}}$. According to Proposition 7, we only need to find all linear codes over $\mathrm{GF}(2^h)$ of length $2^m + 1$ which are invariant under $\mathrm{Stab}_{U_{2^m+1}}$.

The following lemma gives the polynomial expansion of the linear fractional transformation $\frac{u+c^q}{cu+1}$, where $c \in \mathrm{GF}(q^2)^* \setminus U_{q+1}$.

Lemma 8 *Let* $q = 2^m$ *with* $m \geq 2$ *and* $c \in \mathrm{GF}(q^2)^* \setminus U_{q+1}$*. Then for any* $u \in U_{q+1}$*, the following holds*

$$\frac{u + c^q}{cu + 1} = \sum_{i=1}^{q} c^{i-1} u^i.$$

Proof An easy computation shows that

$$\begin{aligned} \sum_{i=1}^{q} c^{i-1} u^i &= \frac{1+(cu)^q}{1+cu} u \\ &= \frac{u+c^q u^{q+1}}{1+cu} \\ &= \frac{u+c^q}{cu+1}, \end{aligned}$$

which completes the proof. □

The following lemma expresses the coefficients of the polynomial expansion of a function f over U_{q+1} in terms of the sums over U_{q+1} of the product function of f and the power functions u^j.

Lemma 9 *Let f be a function from U_{q+1} to $\mathrm{GF}(q^{2h})$ with $h \geq 1$. Let $\sum_{i=0}^{q} a_i u^i$ be the polynomial expansion of f, where $a_i \in \mathrm{GF}(q^{2h})$. Then $a_i = \sum_{u \in U_{q+1}} f(u)u^{-i}$, where $0 \leq i \leq q$.*

Proof A straightforward computation yields that

$$\sum_{u \in U_{q+1}} u^e = \begin{cases} 1, & \text{if } q+1 \text{ divides } e, \\ 0, & \text{otherwise}, \end{cases} \tag{10}$$

where e is an integer.

A standard calculation shows that

$$\begin{aligned} \sum_{u \in U_{q+1}} f(u)u^{-i} &= \sum_{u \in U_{q+1}} u^{-i} \sum_{j=0}^{q} a_j u^j \\ &= \sum_{j=0}^{q} a_j \sum_{u \in U_{q+1}} u^{j-i} \\ &= a_i, \end{aligned}$$

where the last equality comes from (10). The desired conclusion then follows. □

The following lemma gives the first two terms of the polynomial expansion for the function $\left(\frac{u+c^q}{cu+1}\right)^e$ over U_{q+1}.

Lemma 10 *Let $q = 2^m$ with $m \geq 2$, and $c \in \mathrm{GF}(q^2)^* \setminus U_{q+1}$. Let e be an integer such that $1 \leq e \leq q$. Let $a_0 + a_1 u + \cdots + a_q u^q$ be the polynomial expansion of the function from U_{q+1} to $\mathrm{GF}(q^2)$ given by $u \mapsto \left(\frac{u+c^q}{cu+1}\right)^e$. Then $a_0 = 0$ and $a_1 = c^{q(e-1)}$.*

Proof Applying Lemma 9 to the function $f(u) = \left(\frac{u+c^q}{cu+1}\right)^e$, we obtain

$$\begin{aligned} a_1 &= \sum_{u \in U_{q+1}} \left(\frac{u+c^q}{cu+1}\right)^e u^{-1} \\ &= \sum_{u \in U_{q+1}} \left(\frac{u^{-1}+c^q}{cu^{-1}+1}\right)^e u \quad \text{Substituting } u^{-1} \text{ with } u \\ &= \sum_{u \in U_{q+1}} \left(\frac{1+c^q u}{c+u}\right)^e u \\ &= \sum_{u \in U_{q+1}} \left(\frac{u+c}{c^q u+1}\right)^{-e} u \\ &= \sum_{u \in U_{q+1}} u^{-e} \left(\frac{u+c}{c^q u+1}\right) \quad \text{Substituting } \frac{u+c}{c^q u+1} \text{ with } u \\ &= c^{q(e-1)}, \end{aligned}$$

where the last equality follows from Lemmas 8 and 9.

Employing Lemma 9 on $\left(\frac{u+c^q}{cu+1}\right)^e$ again, we have

$$\begin{aligned} a_0 &= \sum_{u \in U_{q+1}} \left(\frac{u+c^q}{cu+1}\right)^e \\ &= \sum_{u \in U_{q+1}} u^e \qquad \text{Substituting } \frac{u+c^q}{cu+1} \text{ with } u \\ &= 0, \end{aligned}$$

where the last equality follows from (10). This completes the proof. □

Now we are ready to prove the main result of this section.

Theorem 11 *Let $q = 2^m$ with $m \geq 2$. If $\mathcal{C}$ is a linear code over* GF(2^h) *of length $2^m + 1$ that is invariant under the permutation action of* PGL$(2, q)$*, then $\mathcal{C}$ must be one of the following:*

(I) *the zero code $\mathcal{C}_0 = \{(0, 0, \ldots, 0)\}$; or*
(II) *the whole space* GF$(2^h)^{q+1}$*, which is the dual of $\mathcal{C}_0$; or*
(III) *the repetition code $\mathcal{C}_1 = \{(c, c, \ldots, c) : c \in \mathrm{GF}(2^h)\}$ of dimension 1; or*
(IV) *the code $\mathcal{C}_1^{\perp}$, given by*

$$\mathcal{C}_1^{\perp} = \left\{(c_0, \ldots, c_q) \in \mathrm{GF}(2^h)^{q+1} : c_0 + \cdots + c_q = 0\right\}.$$

Proof It is evident that the four trivial 2^h-ary linear codes $\mathcal{C}_0$, $\mathcal{C}_0^{\perp}$, $\mathcal{C}_1$ and $\mathcal{C}_1^{\perp}$ of length $2^m + 1$ are invariant under PGL$(2, q)$.

Let $\mathcal{C}$ be a 2^h-ary linear code of length $q + 1$ which is invariant under PGL$(2, q)$, which amounts to saying that $\mathcal{C}$ is invariant under $\mathrm{Stab}_{U_{q+1}}$ by Proposition 7. By Part (I) of Proposition 5, the translation $\pi(u) = u_0 u$ belongs to $\mathrm{Stab}_{U_{q+1}}$, where $u_0 \in U_{q+1}$. This clearly forces $\mathcal{C}$ to be a cyclic code. Let E be the cyclicity-defining set of $\mathcal{C}$. We consider the following four cases for E.

If $E = \emptyset$, then $\mathcal{C} = \mathcal{C}_0$

If $E = \{0\}$, then $\mathcal{C} = \mathcal{C}_1$

If $\{0\} \subsetneq E$, then there exists an $e \in E \setminus \{0\}$. Applying Corollary 3, the lifted code $\mathrm{GF}(q^{2h}) \otimes \mathcal{C}$ to $\mathrm{GF}(q^{2h})$ is the cyclic code over $\mathrm{GF}(q^{2h})$ with respect to the cyclicity-defining set E. We see at once that $\mathrm{GF}(q^{2h}) \otimes \mathcal{C}$ also stays invariant under $\mathrm{Stab}_{U_{q+1}}$ from the definition of lifting of a cyclic code. Combining Corollary 3 with Proposition 5 we obtain $\left(\left(\frac{u+c^{q+1}}{cu+1}\right)^e\right)_{u \in U_{q+1}} \in \mathrm{GF}(q^{2h}) \otimes \mathcal{C}$, where $c \in \mathrm{GF}(q^2)^* \setminus U_{q+1}$. Applying Corollary 4 and Lemma 10 we can assert that $1 \in E$. Thus $\left(\frac{u+c^{q+1}}{cu+1}\right)_{u \in U_{q+1}} \in \mathrm{GF}(q^{2h}) \otimes \mathcal{C}$. Combining Corollary 4 and Lemma 8 we deduce $E = \{0, 1, \cdots, q\}$. We thus get $\mathcal{C} = \mathrm{GF}(2^h)^{q+1} = \mathcal{C}_0^{\perp}$.

If $E \neq \emptyset$ and $0 \notin E$, then there exists an $e \in E \setminus \{0\}$. An analysis similar to that in the proof of the case of $\{0\} \subsetneq E$ shows that $E = \{1, \ldots, q\}$ and $\mathcal{C} = \mathcal{C}_1^{\perp}$. This completes the proof. □

The remainder of this section will be devoted to determining the 2-rank of some special incidence structures. Let $\mathbb{D} = (X, \mathcal{B})$ be an incidence structure. The points of X are usually indexed with $p_1, p_2, \ldots, p_v$, and the blocks of $\mathcal{B}$ are normally denoted by $B_1, B_2, \ldots, B_b$. The *incidence matrix* $M_{\mathbb{D}} = (m_{ij})$ of $\mathbb{D}$ is a $b \times v$ matrix where $m_{ij} = 1$ if $p_j \in B_i$ and $m_{ij} = 0$ otherwise. The p-rank of an incidence structure $\mathbb{D}$ is defined as the rank of its incidence matrix over a finite field of characteristic p and denoted by $\mathrm{rank}_p(\mathbb{D})$. The binary matrix $M_{\mathbb{D}}$ can be viewed as a matrix over GF(q) for any prime power q, and its row vectors span a linear code of length v over GF(q), which is denoted by $\mathcal{C}_q(\mathbb{D})$ and called the *code* of $\mathbb{D}$ over GF(q). The p-rank of incidence structures, i.e., the dimension of the corresponding codes, can be used to classify incidence structures of certain type. For example, the 2-rank and 3-rank of Steiner triple and quadruple systems were intensively studied and employed for counting and classifying Steiner triple and quadruple systems [14], [16], [18] [25], [26], [27], [28].

For any set A and a positive integer k, recall that $\binom{A}{k}$ denotes the set of all k-subsets of A. The following theorem is an important corollary of Theorem 11.

Theorem 12 *Let $\mathcal{B} \subseteq \binom{\mathrm{PG}(1,2^m)}{k}$ such that $m \geq 2$, $1 \leq k \leq 2^m$ and $\mathcal{B}$ is invariant under the action of* $\mathrm{PGL}(2, q)$. *Then the* 2*-rank of the incidence structure* $\mathbb{D} = (\mathrm{PG}(1, 2^m), \mathcal{B})$ *is given by*

$$\mathrm{rank}_2(\mathbb{D}) = \begin{cases} 2^m, & \text{if } k \text{ is even,} \\ 2^m + 1, & \text{if } k \text{ is odd.} \end{cases}$$

Proof Since $\mathcal{B}$ is invariant under the action of $\mathrm{PGL}(2, q)$, then so is the code $\mathcal{C}_2(\mathbb{D})$ of $\mathbb{D}$. It then follows from Theorem 11 that $\mathcal{C}_2(\mathbb{D}) = \mathcal{C}_1^{\perp}$ or $\mathcal{C}_2(\mathbb{D}) = \mathrm{GF}(2)^{2^m+1}$. The desired conclusion then follows. □

5 Linear codes of length $2^m + 1$ with sets of supports invariant under $\mathrm{PGL}(2, q)$

Throughout this section, let $q = 2^m$, and let U_{q+1} be the set of all $(q + 1)$-th roots of unity in $\mathrm{GF}(q^2)$, where $m \geq 2$ is a positive integer. In this section, we describe two families of nontrivial linear codes with the set of the supports of all codewords of any fixed weight being invariant under $\mathrm{PGL}(2, q)$.

We define a cyclic code over $\mathrm{GF}(q^2)$ of length $q + 1$ by

$$\mathcal{C}_{\{3,5\}} = \left\{ \begin{array}{c} \left(a_3u^3 + a_{q-2}u^{q-2} + a_5u^5 + a_{q-4}u^{q-4}\right)_{u\in U_{q+1}} : \\ a_3, a_{q-2}, a_5, a_{q-4} \in \mathrm{GF}(q^2) \end{array} \right\}. \tag{11}$$

We index the coordinates of the codewords in $\mathcal{C}_{\{3,5\}}$ and related codes with the elements in U_{q+1}. It is evident that the dual of $\mathcal{C}_{\{3,5\}}$ is given as

$$\mathcal{C}_{\{3,5\}}{}^{\perp} = \left\{ (c_u)_{u\in U_{q+1}} \in \mathrm{GF}(q^2)^{q+1} : \textstyle\sum_{u\in U_{q+1}} c_u \mathbf{h}_u = \mathbf{0} \right\}, \tag{12}$$

where $\mathbf{h}_u$ is the transpose of the row vector $(u^{-5}, u^{-3}, u^3, u^5)$.

It is obvious that if $(c_u)_{u\in U_{q+1}} \in \mathcal{C}_{\{3,5\}}$ (resp., $(c_u)_{u\in U_{q+1}} \in \mathcal{C}_{\{3,5\}}{}^{\perp}$), then $\left(c_u^q\right)_{u\in U_{q+1}} \in \mathcal{C}_{\{3,5\}}$ (resp., $\left(c_u^q\right)_{u\in U_{q+1}} \in \mathcal{C}_{\{3,5\}}{}^{\perp}$). From [10, Lemma 7] we deduce that

$$\mathrm{Tr}_{q^2/q}\left(\mathcal{C}_{\{3,5\}}\right) = \mathcal{C}_{\{3,5\}}\big|_{\mathrm{GF}(q)}, \tag{13}$$

and

$$\mathrm{Tr}_{q^2/q}\left(\mathcal{C}_{\{3,5\}}{}^{\perp}\right) = \mathcal{C}_{\{3,5\}}{}^{\perp}\Big|_{\mathrm{GF}(q)}. \tag{14}$$

In fact, $\mathcal{C}_{\{3,5\}}$ is the lifted code of $\mathrm{Tr}_{q^2/q}\left(\mathcal{C}_{\{3,5\}}\right)$ to $\mathrm{GF}(q^2)$ and has cyclicity-defining set $\{3, 5, q-2, q-4\}$. Similarly, $\mathcal{C}_{\{3,5\}}^{\perp}$ is the lifted code of $\mathrm{Tr}_{q^2/q}\left(\mathcal{C}_{\{3,5\}}{}^{\perp}\right)$ to $\mathrm{GF}(q^2)$. The reader is referred to Theorem 2 and Corollary 3 for further clarification.

In order to describe the supports of the codewords of $\mathrm{Tr}_{q^2/q}\left(\mathcal{C}_{\{3,5\}}\right)$ and $\mathcal{C}_{\{3,5\}}{}^{\perp}\big|_{\mathrm{GF}(q)}$, we need to employ symmetric polynomials and elementary symmetric polynomials. A polynomial f is said to be symmetric if it is invariant under any permutation of its variables. The *elementary symmetric polynomial* (*ESP*) of degree ℓ in k variables $u_1, u_2, \cdots, u_k$, written $\sigma_{k,\ell}$, is defined by

$$\sigma_{k,\ell}(u_1, \ldots, u_k) = \sum_{I\subseteq[k],|I|=\ell} \prod_{j\in I} u_j, \tag{15}$$

where $[k] = \{1, 2, \ldots, k\}$. Already known to Newton, the fundamental theorem of symmetric polynomials asserts that any symmetric polynomial is a polynomial in the elementary symmetric polynomials. For any k-variable symmetric polynomial f with coefficients in $\mathrm{GF}(q^2)$, write

$$\mathcal{B}_{f,q+1} = \left\{ \{u_1, \ldots, u_k\} \in \binom{U_{q+1}}{k} : f(u_1, \ldots, u_k) = 0 \right\}. \tag{16}$$

In general, it is difficult to determine $|\mathcal{B}_{f,q+1}|$. However, it was shown in [20] that

$$|\mathcal{B}_{\sigma_{5,2},q+1}| = \begin{cases} \frac{1}{10}\binom{q+1}{3}, & \text{if } m \text{ is even}, \\ 0, & \text{if } m \text{ is odd}. \end{cases} \tag{17}$$

To determine the parameters of $\mathrm{Tr}_{q^2/q}\left(\mathcal{C}_{\{3,5\}}\right)$ and $\mathcal{C}_{\{3,5\}}{}^{\perp}|_{\mathrm{GF}(q)}$, we prove several lemmas below. To simplify notation and expressions below, we use $\sigma_{k,\ell}$ to denote $\sigma_{k,\ell}(u_1, \ldots, u_\ell)$ for any $\{u_1, \ldots, u_k\} \in \binom{U_{q+1}}{k}$ whenever $\{u_1, \ldots, u_k\}$ is specified.

Lemma 13 *Let $\sigma_{3,1}, \sigma_{3,2}, \sigma_{3,3}$ be the ESPs given by (15) with $\{u_1, u_2, u_3\} \in \binom{U_{q+1}}{3}$. Then*

(I) $\sigma_{3,1}\sigma_{3,2} + \sigma_{3,3} = (u_1 + u_2)(u_2 + u_3)(u_3 + u_1)$;
(II) $\sigma_{3,1}\sigma_{3,2} + \sigma_{3,3} \neq 0$; *and*
(III) $\sigma_{3,2}^2 + \sigma_{3,1}\sigma_{3,3} = \sigma_{3,3}^2\left(\sigma_{3,1}^2 + \sigma_{3,2}\right)^q$.

Proof The proofs are straightforward and omitted.

Lemma 14 *Let $q = 2^m$ with m even. Let $\sigma_{3,1}, \sigma_{3,2}, \sigma_{3,3}$ be the ESPs given by (15) with $\{u_1, u_2, u_3\} \in \binom{U_{q+1}}{3}$. Then*

(I) $\sigma_{3,1}^2 + \sigma_{3,2} \neq 0$; *and*
(II) $\sigma_{3,2}^2 + \sigma_{3,1}\sigma_{3,3} \neq 0$.

Proof The proof can be found in [20].

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

$$\begin{bmatrix} u_1^{-5} & u_2^{-5} & \cdots & u_\ell^{-5} \\ u_1^{-3} & u_2^{-3} & \cdots & u_\ell^{-3} \\ u_1^{+3} & u_2^{+3} & \cdots & u_\ell^{+3} \\ u_1^{+5} & u_2^{+5} & \cdots & u_\ell^{+5} \end{bmatrix}, \tag{18}$$

where $u_1, \ldots, u_\ell \in U_{q+1}$. For $r_1, \ldots, r_i \in \{\pm 5, \pm 3\}$, let $M_\ell[r_1, \ldots, r_i]$ denote the submatrix of M_ℓ obtained by deleting the rows $(u_1^{r_1}, u_2^{r_1}, \ldots, u_\ell^{r_1}), \ldots, (u_1^{r_i}, u_2^{r_i}, \ldots, u_\ell^{r_i})$ of the matrix M_ℓ, where $1 \leq i \leq 4$.

Lemma 15 *Let M_ℓ be the matrix given by (18) with $\{u_1, \ldots, u_\ell\} \in \binom{U_{q+1}}{\ell}$. Consider the system of homogeneous linear equations defined by*

$$M_\ell(x_1, \ldots, x_\ell)^T = 0. \tag{19}$$

Then (19) has a nonzero solution $(x_1, \ldots, x_\ell)$ in $\mathrm{GF}(q)^\ell$ if and only if $\mathrm{rank}(M_\ell) < \ell$, where $\mathrm{rank}(M_\ell)$ denotes the rank of the matrix M_ℓ.

Proof The proof is similar to that in [20, Lemma 29] and thus omitted. □

Lemma 16 *Let m be an even positive integer and M_3 be the matrix given by (18) with $\{u_1, u_2, u_3\} \in \binom{U_{q+1}}{3}$. Then* $\mathrm{rank}(M_3) = 3$.

Proof Suppose that $\mathrm{rank}(M_3) < 3$. Then $\det(M_3[5]) = \frac{\prod_{1\le i<j\le 3}(u_i+u_j)^2}{\sigma_{3,3}^5}\left(\sigma_{3,1}^2+\sigma_{3,2}\right)^2 = 0$, which is contrary to Lemma 14. This completes the proof.

Lemma 17 *Let m be an even positive integer and M_4 be the matrix given by (18) with $\{u_1, \ldots, u_4\} \in \binom{U_{q+1}}{4}$. Then* $\mathrm{rank}(M_4) = 3$ *if and only if* $\sigma_{4,2}^2 + \sigma_{4,1}\sigma_{4,3} = 0$.

Proof Note that

$$\det(M_4) = \frac{\prod_{1\le i<j\le 4}(u_i+u_j)^2}{\sigma_{4,4}^5}\left(\sigma_{4,2}^2+\sigma_{4,1}\sigma_{4,3}\right)^2,$$

which completes the proof. □

The following lemma is immediate from [20, Lemmas 18 and 20].

Lemma 18 *Let $q = 2^m$ with m even and $\{u_1, u_2, u_3\} \in \binom{U_{q+1}}{3}$. Let $a = \sigma_{3,1}^2 + \sigma_{3,2}$, $b = \sigma_{3,1}\sigma_{3,2}+\sigma_{3,3}$ and $c = \sigma_{3,2}^2+\sigma_{3,1}\sigma_{3,3}$. Then the quadratic polynomial au^2+bu+c has exactly two roots u_4, u_5 in U_{q+1} such that $\{u_1, u_2, u_3, u_4, u_5\} \in \binom{U_{q+1}}{5}$. Moreover, $\{u_1, u_2, u_3, u_4\}$ satisfies $\sigma_{4,2}^2 + \sigma_{4,1}\sigma_{4,3} = 0$.*

Lemma 19 *Let $q = 2^m$ with m even and M_4 be the matrix given by (18) with $\{u_1, \ldots, u_4\} \in \binom{U_{q+1}}{4}$. If there exists a vector $(x_1, \ldots, x_4) \in (\mathrm{GF}(q)^*)^4$ such that $M_4(x_1, \ldots, x_4)^T = 0$, then $\{u_1, \ldots, u_4\} \in \mathcal{B}_{\sigma_{4,2}^2+\sigma_{4,1}\sigma_{4,3},q+1}$, where $\mathcal{B}_{\sigma_{4,2}^2+\sigma_{4,1}\sigma_{4,3},q+1}$ is defined by (16).*

Proof The proof is similar to that in [20, Lemma 34] and thus omitted. □

The minimum-weight codewords in $\mathrm{Tr}_{q^2/q}\left(\mathcal{C}_{\{3,5\}}\right)$ are described in the following lemma.

Lemma 20 *Let $f(u) = \mathrm{Tr}_{q^2/q}\left(au^5 + bu^3\right)$ where $(a, b) \in \mathrm{GF}(q^2)^2 \setminus \{\mathbf{0}\}$. Define*

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

Then $|\mathrm{zero}(f)| \le 5$. Moreover, $|\mathrm{zero}(f)| = 5$ if and only if $a = \frac{\tau}{\sigma_{5,5}(u_1,\ldots,u_5)}$ and $b = \frac{\tau\sigma_{5,1}^2(u_1,\ldots,u_5)}{\sigma_{5,5}(u_1,\ldots,u_5)}$, where $\{u_1, \ldots, u_5\} \in \mathcal{B}_{\sigma_{5,2},q+1}$ and $\tau \in \mathrm{GF}(q)^*$. In particular, the dimension of $\mathrm{Tr}_{q^2/q}\left(\mathcal{C}_{\{3,5\}}\right)$ equals 4.

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

$$f(u) = \frac{1}{u^5}\left(\sqrt{a}u^5 + \sqrt{b}u^4 + \sqrt{b^q}u + \sqrt{a^q}\right)^2. \tag{20}$$

Thus $|\mathrm{zero}(f)| \le 5$.

Assume that $|\mathrm{zero}(f)| = 5$. From (20), there exists $\{u_1, \ldots, u_5\} \in \binom{U_{q+1}}{5}$ such that $f(u) = \frac{a\prod_{i=1}^5(u+u_i)^2}{u^5}$. By Vieta's formula, $a\sigma_{5,1}^2 = b$, $a\sigma_{5,2}^2 = 0$, $a\sigma_{5,3}^2 = 0$, $a\sigma_{5,4}^2 = b^q$ and $a\sigma_{5,5}^2 = a^q$. One obtains $a = \frac{\tau}{\sigma_{5,5}}$ from $a^{q-1} = \sigma_{5,5}^2$, where $\tau \in \mathrm{GF}(q)^*$. Thus $b = \frac{\tau\sigma_{5,1}^2}{\sigma_{5,5}}$.

Conversely, assume that $a = \frac{\tau}{\sigma_{5,5}}$ and $b = \frac{\tau\sigma_{5,1}^2}{\sigma_{5,5}}$, where $\{u_1, \ldots, u_5\} \in \mathcal{B}_{\sigma_{5,2},q+1}$ and $\tau \in \mathrm{GF}(q)^*$. Then $f(u) = \frac{a\prod_{i=1}^5(u+u_i)^2}{u^5}$. Consequently, $\mathrm{zero}(f) = \{u_1, \ldots, u_5\}$ and $|\mathrm{zero}(f)| = 5$. This completes the proof. □

Theorem 21 *Let $q = 2^m$ with $m \geq 4$ being an even integer. Then the subfield subcode ${\mathcal{C}_{\{3,5\}}}^{\perp}|_{\mathrm{GF}(q)}$ has parameters $[q+1, q-3, 4]_q$.*

Proof Recall that (5) says that

$$ {\mathcal{C}_{\{3,5\}}}^{\perp}\Big|_{\mathrm{GF}(q)} = \left(\mathrm{Tr}_{q^2/q}(\mathcal{C}_{\{3,5\}})\right)^{\perp}. $$

Thus ${\mathcal{C}_{\{3,5\}}}^{\perp}|_{\mathrm{GF}(q)}$ has dimension $q-3$ by Lemma 20.

Since m is even, we have $d \geq 4$ by Lemma 16. Applying Lemmas 18 and 19, we assert that there must exist a codeword of weight 4. Consequently, $d = 4$. □

As Theorem 21 showed, the subfield subcode ${\mathcal{C}_{\{3,5\}}}^{\perp}|_{\mathrm{GF}(q)}$ almost meets the Griesmer bound.

Theorem 22 *Let $q = 2^m$ with $m \geq 4$ being even. Then the trace code $\mathrm{Tr}_{q^2/q}\left(\mathcal{C}_{\{3,5\}}\right)$ has parameters $[q+1, 4, q-4]_q$.*

Proof Note that any codeword of $\mathrm{Tr}_{q^2/q}\left(\mathcal{C}_{\{3,5\}}\right)$ can be written as

$$ \mathbf{c}(a_3, a_5) = \mathrm{Tr}_{q^2/q}(a_3 u^3 + a_5 u^5). $$

Then the dimension of $\mathrm{Tr}_{q^2/q}\left(\mathcal{C}_{\{3,5\}}\right)$ is equal to 4 by Lemma 20. The desired conclusion on the minimum weight for even m then follows from (17) and Lemma 20. This completes the proof. □

The invariance of the set of the supports of all the codewords of any fixed weight in $\mathrm{Tr}_{q^2/q}\left(\mathcal{C}_{\{3,5\}}\right)$ under the action of PGL$(2, q)$ is established by the following theorem.

Theorem 23 *Let $q = 2^m$ with $m \geq 2$. Let k be an integer with $1 \leq k \leq q+1$ and $A_k\left(\mathrm{Tr}_{q^2/q}\left(\mathcal{C}_{\{3,5\}}\right)\right) > 0$. Then $\mathcal{B}_k\left(\mathrm{Tr}_{q^2/q}\left(\mathcal{C}_{\{3,5\}}\right)\right)$ is invariant under the action of* $\mathrm{Stab}_{U_{q+1}}$. *In particular, the incidence structure $\left(U_{q+1}, \mathcal{B}_k\left(\mathrm{Tr}_{q^2/q}\left(\mathcal{C}_{\{3,5\}}\right)\right)\right)$ is a 3-design when $k > 3$.*

Proof We only need to show that if $\mathbf{c} \in \mathrm{Tr}_{q^2/q}\left(\mathcal{C}_{\{3,5\}}\right)$ and π is a linear fractional transformation listed in Corollary 6, then there exists a codeword $\mathbf{c}' \in \mathrm{Tr}_{q^2/q}\left(\mathcal{C}_{\{3,5\}}\right)$ such that $\mathrm{Supp}(\pi(\mathbf{c})) = \mathrm{Supp}(\mathbf{c}')$. Denote by $\mathbf{c}(a_3, a_5)$ the codeword $\left(\mathrm{Tr}_{q^2/q}(a_3 u^3 + a_5 u^5)\right)_{u \in U_{q+1}}$ of $\mathrm{Tr}_{q^2/q}\left(\mathcal{C}_{\{3,5\}}\right)$, where $a_3, a_5 \in \mathrm{GF}(q^2)$. We investigate the following three cases for π.

If π is the transformation given by $u \mapsto u_0 u$, where $u_0 \in U_{q+1}$, then it is clear that $\pi(\mathbf{c}(a_3, a_5)) = \mathbf{c}(a_3 u_0^3, a_5 u_0^5)$. Thus $\mathrm{Supp}\,(\pi(\mathbf{c}(a_3, a_5))) = \mathrm{Supp}\left(\mathbf{c}(a_3 u_0^3, a_5 u_0^5)\right)$.

If π is the transformation given by $u \mapsto u^{-1}$, then it is obvious that $\pi(\mathbf{c}(a_3, a_5)) = \mathbf{c}(a_3, a_5)$. Thus $\mathrm{Supp}\,(\pi(\mathbf{c}(a_3, a_5))) = \mathrm{Supp}\,(\mathbf{c}(a_3, a_5))$.

Let π be the translation given by $u \mapsto \frac{u+c^q}{cu+1}$ where $c \in \mathrm{GF}(q^2)^* \setminus U_{q+1}$. Write $f(u) = \mathrm{Tr}_{q^2/q}(a_3u^3 + a_5u^5)$ and $A = cu + 1$. Then $u + c^q = uA^q$. A standard computation gives

$$\begin{aligned}
&f\left(\tfrac{u+c^q}{cu+1}\right)\\
&= \mathrm{Tr}_{q^2/q}\left(a_3\left(\tfrac{u+c^q}{cu+1}\right)^3 + a_5\left(\tfrac{u+c^q}{cu+1}\right)^5\right)\\
&= \mathrm{Tr}_{q^2/q}\left(\tfrac{a_3(u+c^q)^3(cu+1)^2+a_5(u+c^q)^5}{(cu+1)^5}\right)\\
&= \mathrm{Tr}_{q^2/q}\left(\tfrac{a_3A^{3q}A^2u^3+a_5A^{5q}u^5}{A^5}\right)\\
&= \tfrac{a_3A^{3q}A^2u^3+a_5A^{5q}u^5}{A^5} + \tfrac{a_3^qA^3A^{2q}u^{3q}+a_5^qA^5u^{5q}}{A^{5q}}\\
&= \tfrac{a_3A^{8q}A^2u^3+a_5A^{10q}u^5+a_3^qA^8A^{2q}u^{3q}+a_5^qA^{10}u^{5q}}{A^5A^{5q}}\\
&= \tfrac{a_3A^{8q}A^2u^3+a_5A^{10q}u^5+\left(a_3A^{8q}A^2u^3+a_5A^{10q}u^5\right)^q}{A^5A^{5q}}\\
&= \tfrac{1}{A^5A^{5q}}\mathrm{Tr}_{q^2/q}\left(a_3A^{8q}A^2u^3 + a_5A^{10q}u^5\right).
\end{aligned} \tag{21}$$

Expanding $a_3A^{8q}A^2u^3$ yields

$$\begin{aligned}
&a_3A^{8q}A^2u^3\\
&= a_3(c^{8q}u^{8q} + 1)(c^2u^2 + 1)u^3\\
&= a_3u^3(c^{8q+2}u^{8q+2} + c^{8q}u^{8q} + c^2u^2 + 1)\\
&= a_3(u^3 + c^{8q+2}u^{-3} + c^2u^5 + c^{8q}u^{-5}).
\end{aligned} \tag{22}$$

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

$$\begin{aligned}
&a_5A^{10q}u^5\\
&= a_5(c^{10q}u^{10q} + 1)u^5\\
&= a_5(u^5 + c^{10q}u^{-5}).
\end{aligned} \tag{23}$$

Combining (22) and (23) gives

$$\begin{aligned}
&\mathrm{Tr}_{q^2/q}\left(a_3A^{8q}A^2u^3 + a_5A^{10q}u^5\right)\\
&= \mathrm{Tr}_{q^2/q}\left(\left(a_3 + a_3^qc^{8+2q}\right)u^3 + \left(a_5 + a_5^qc^{10} + a_3c^2 + a_3^qc_8\right)u^5\right).
\end{aligned} \tag{24}$$

Plugging (24) into (21) yields

$$f\left(\frac{u+c^q}{cu+1}\right) = \frac{1}{A^5A^{5q}}\mathrm{Tr}_{q^2/q}\left(a_3'u^3 + a_5'u^5\right),$$

where $a_3' = a_3 + a_3^qc^{8+2q}$ and $a_5' = a_5 + a_5^qc^{10} + a_3c^2 + a_3^qc_8$. This clearly forces $\mathrm{Supp}\,(\pi(\mathbf{c}(a_3, a_5))) = \mathrm{Supp}\left(\mathbf{c}(a_3', a_5')\right)$. The desired conclusion then follows. □

The proof of Theorem 23 gives more, namely

$$\begin{aligned}
&tr_{q^2/q}\left(a_3\left(\tfrac{u+c^q}{cu+1}\right)^3 + a_5\left(\tfrac{u+c^q}{cu+1}\right)^5\right)\\
&= \tfrac{1}{(cu+1)^5(cu+1)^{5q}}\mathrm{Tr}_{q^2/q}\left(a_3'u^3 + a_5'u^5\right),
\end{aligned} \tag{25}$$

where $a_3, a_5 \in \mathrm{GF}(q^2)$, $c \in \mathrm{GF}(q^2) \setminus U_{q+1}$, $a_3' = a_3 + a_3^qc^{8+2q}$ and $a_5' = a_5 + a_5^qc^{10} + a_3c^2 + a_3^qc_8$.

The following theorem shows the invariance of the set of the supports of all the codewords of any fixed weight in $\mathcal{C}_{\{3,5\}}{}^{\perp}|_{\mathrm{GF}(q)}$ under the action of $\mathrm{PGL}(2, q)$.

Theorem 24 *Let $q = 2^m$ with $m \geq 2$. Let k be any integer with $1 \leq k \leq q+1$ and $A_k\left(\mathcal{C}_{\{3,5\}}{}^{\perp}|_{\mathrm{GF}(q)}\right) > 0$. Then $\mathcal{B}_k\left(\mathcal{C}_{\{3,5\}}{}^{\perp}|_{\mathrm{GF}(q)}\right)$ is invariant under the action of* $\mathrm{Stab}_{U_{q+1}}$. *In particular, the incidence structure $\left(U_{q+1}, \mathcal{C}_{\{3,5\}}{}^{\perp}|_{\mathrm{GF}(q)}\right)$ is a 3-design when $k > 3$.*

Proof Recall that by (5) we have

$$\mathcal{C}_{\{3,5\}}{}^{\perp}\Big|_{\mathrm{GF}(q)} = \left(\mathrm{Tr}_{q^2/q}(\mathcal{C}_{\{3,5\}})\right)^{\perp}.$$

Let $\mathbf{w}$ be any codeword of $\mathcal{C}_{\{3,5\}}{}^{\perp}|_{\mathrm{GF}(q)} = \left(\mathrm{Tr}_{q^2/q}(\mathcal{C}_{\{3,5\}})\right)^{\perp}$ and π be any linear fractional translations listed in Corollary 6. It is easily seen that if π is a transformation given by $u \mapsto u_0 u$ or $u \mapsto 1/u$, where $u_0 \in U_{q+1}$, then

$$\pi(\mathbf{w}) \in \mathcal{C}_{\{3,5\}}{}^{\perp}\Big|_{\mathrm{GF}(q)}. \tag{26}$$

Assume π is a translation given by $u \mapsto \frac{u+c^q}{cu+1}$ where $c \in \mathrm{GF}(q^2)^* \setminus U_{q+1}$. It is obvious that $\pi(\mathbf{w}) \in \left(\pi\left(\mathrm{Tr}_{q^2/q}(\mathcal{C}_{\{3,5\}})\right)\right)^{\perp}$. From (25) we conclude that

$$\pi\left(\mathrm{Tr}_{q^2/q}(\mathcal{C}_{\{3,5\}})\right) = \left(\frac{1}{(cu+1)^{5q+5}}\right)_{u \in U_{q+1}} \cdot \mathrm{Tr}_{q^2/q}(\mathcal{C}_{\{3,5\}}).$$

By (4) we have that

$$\left(\pi\left(\mathrm{Tr}_{q^2/q}(\mathcal{C}_{\{3,5\}})\right)\right)^{\perp} = \left((cu+1)^{5q+5}\right)_{u \in U_{q+1}} \cdot \left(\mathrm{Tr}_{q^2/q}(\mathcal{C}_{\{3,5\}})\right)^{\perp}.$$

Consequently,

$$\pi(\mathbf{w}) \in \left((cu+1)^{5q+5}\right)_{u \in U_{q+1}} \cdot \left(\mathrm{Tr}_{q^2/q}(\mathcal{C}_{\{3,5\}})\right)^{\perp}. \tag{27}$$

Combining (26) and (27) with Corollary 6 we can assert that the set of all the supports of $\mathcal{C}_{\{3,5\}}{}^{\perp}|_{\mathrm{GF}(q)}$ stays invariant under $\mathrm{Stab}_{U_{q+1}}$. This completes the proof. □

The remainder of this section is devoted to determining the parameters of certain 3-designs held in the subfield subcodes $\mathcal{C}_{\{3,5\}}{}^{\perp}|_{\mathrm{GF}(q)}$ and the trace codes $\mathrm{Tr}_{q^2/q}(\mathcal{C}_{\{3,5\}})$.

Theorem 25 *Let $q = 2^m$ with $m \geq 4$ even. Then the incidence structure*

$$\left(U_{q+1}, \mathcal{B}_{q-4}\left(\mathrm{Tr}_{q^2/q}\left(\mathcal{C}_{\{3,5\}}\right)\right)\right)$$

is a $3-(q+1, q-4, \lambda)$ design with

$$\lambda = \frac{(q-4)(q-5)(q-6)}{60},$$

and its complementary incidence structure is a $3-(q+1, 5, 1)$ design.

Proof By Theorems 23 and 22, $\left(U_{q+1}, \mathcal{B}_{q-4}\left(\mathrm{Tr}_{q^2/q}\left(\mathcal{C}_{\{3,5\}}\right)\right)\right)$ is a $3-(q+1, q-4, \lambda)$ design. To determine the value of λ, we consider its complementary design. Lemma 20 shows that the complementary incidence structure of

$$\left(U_{q+1}, \mathcal{B}_{q-4}\left(\mathrm{Tr}_{q^2/q}\left(\mathcal{C}_{\{3,5\}}\right)\right)\right)$$

is isomorphic to the incidence structure of $(U_{q+1}, \mathcal{B}_{\sigma_{5,2},q+1})$, which is a $3-(2^m+1,5,1)$ design by [20, Theorem 5]. It the follows that

$$\lambda = \frac{\binom{q+1-3}{5}}{\binom{q+1-3}{5-3}} = \frac{(q-4)(q-5)(q-6)}{60}.$$

This completes the proof. □

The complementary design $\bar{\mathbb{D}}$ of the 3-design $\mathbb{D}$ from Theorem 25 has parameters 3-$(2^m + 1, 5, 1)$. These parameters correspond to a spherical geometry design [2, Volume I, page 193]. If a linear code $\mathcal{C}$ supports a t-design $\mathbb{D}$, it is in general an open question how to construct a linear code $\mathcal{C}'$ that supports the complementary design of $\mathbb{D}$. We note that an isomorphic version of the complementary $3-(2^m+1,5,1)$ design $\bar{\mathbb{D}}$ of the design $\mathbb{D}$ from Theorem 25 is supported by a linear code described in [20]. According to Magma experiments, $\bar{\mathbb{D}}$ is isomorphic to a spherical geometry design with the same parameters when $m \in \{4, 6\}$. The following theorem asserts that the $3-(2^m+1,5,1)$ design $\bar{\mathbb{D}}$ is isomorphic to the spherical geometry design found by Witt [23] in general. For a short description of the spherical geometry designs found by Witt [23] we refer the reader to [2, Volume I, 6.9 and 6.10, page 193].

Theorem 26 *Let $q = 2^m$ with $m \geq 4$ even. Then the complementary design $\bar{\mathbb{D}}$ of the 3-design $\mathbb{D}$ from Theorem 25 is isomorphic to the Witt spherical geometry design [23] with parameters $3-(2^m+1,5,1)$.*

Proof By definition, $\bar{\mathbb{D}} = \left(U_{q+1}, \bar{\mathcal{B}}\right)$, where $\bar{\mathcal{B}}$ is given by

$$\bar{\mathcal{B}} = \left\{ B \in \binom{U_{q+1}}{5} : \left(U_{q+1} \setminus B\right) \in \mathcal{B}_{q-4}\left(\mathrm{Tr}_{q^2/q}\left(\mathcal{C}_{\{3,5\}}\right)\right) \right\}.$$

Theorem 23 now implies that $\bar{\mathcal{B}}$ is invariant under $\mathrm{Stab}_{U_{q+1}}$. Applying Proposition 7 we conclude that $\bar{\mathbb{D}}$ is isomorphic to a $3-(2^m+1,5,1)$ design $(\mathrm{PG}(1, 2^m), \mathcal{B})$ with $\mathcal{B}$ being invariant under $\mathrm{PGL}(2, q)$. Hence we can write $\mathcal{B}$ as $\mathcal{B} = \dot{\cup}_{i=1}^{\ell} \mathrm{Orb}_{B_i}$, where $B_i \in \binom{\mathrm{PG}(1,2^m)}{5}$ and Orb_{B_i} is the $\mathrm{PGL}(2, q)$-orbit of B_i. Let Stab_{B_i} denote the stabilizer of B_i under the action of $\mathrm{PGL}(2, q)$ on $\binom{\mathrm{PG}(1,2^m)}{5}$. Let B be any 5-subset of $\mathrm{PG}(1, 2^m)$. Let us recall that $|\mathrm{Stab}_B| \in \{1, 4, 60\}$ and all 5-subsets B of $\mathrm{PG}(1, 2^m)$ with $|\mathrm{Stab}_B| = 60$ form exactly one $\mathrm{PGL}(2, q)$-orbit (see Huber05). A trivial verification shows that the 5-subset $\mathrm{PG}(1, 4) = \mathrm{GF}(4) \cup \{\infty\}$ of $\mathrm{PG}(1, 2^m)$ is stabilized by $\mathrm{PGL}_2(\mathrm{GF}(4))$. As the cardinality of the group $\mathrm{PGL}_2(\mathrm{GF}(4))$ is 60 we have $\left|\mathrm{Orb}_{\mathrm{PG}(1,4)}\right| = |\mathrm{PGL}(2, q)|/60$ and $\left\{B \in \binom{\mathrm{PG}(1,2^m)}{5} : |\mathrm{Stab}_B| = 60\right\} = \mathrm{Orb}_{\mathrm{PG}(1,4)}$. Let us observe that $\left|\mathrm{Orb}_{B_i}\right| = |\mathrm{PGL}(2, q)|/60$, $|\mathrm{PGL}(2, q)|/4$, or $|\mathrm{PGL}(2, q)|$ and there is exactly one orbit $\mathrm{Orb}_{\mathrm{PG}(1,4)}$ with size $= |\mathrm{PGL}(2, q)|/60$. It follows that $\ell = 1$ and $\mathcal{B} = \mathrm{Orb}_{\mathrm{PG}(1,4)}$ from $|\mathcal{B}| = |\mathrm{PGL}(2, q)|/60$. The desired conclusion then follows from the definition of spherical geometry designs (see for instance [2, Volume I, page 193]). □

Theorem 27 *Let $q = 2^m$ with $m \geq 4$ being even. Then, the incidence structure*

$$\left(U_{q+1}, \mathcal{B}_4\left(\mathcal{C}_{\{3,5\}}{}^{\perp}\Big|_{\mathrm{GF}(q)}\right)\right)$$

supported by the minimum-weight codewords in $\mathcal{C}_{\{3,5\}}{}^{\perp}\big|_{\mathrm{GF}(q)}$ is a $3-(q+1,4,2)$ design.

Proof By Theorems 24 and 21, $\left(\mathcal{U}_{q+1}, \mathcal{B}_4\left(\mathcal{C}_{\{3,5\}}{}^{\perp}|_{\mathrm{GF}(q)}\right)\right)$ is a $3-(q+1,4,\lambda)$ design. It remains to determine the value of λ. But combining Lemmas 19 and 18 yields directly that it is a $3-(q+1,4,2)$ design. □

It would be interesting to determine parameters for more 3-designs held in $\mathrm{Tr}_{q^2/q}\left(\mathcal{C}_{\{3,5\}}\right)$ and $\mathcal{C}_{\{3,5\}}{}^{\perp}|_{\mathrm{GF}(q)}$. To the best knowledge of the authors, Theorem 27 documents the first infinite family of linear codes supporting an infinite family of $3-(v,4,2)$ designs. According to [4, Table 4.37, page 83], a class of $3-(q+1,4,2)$ designs with $q \equiv 1 \pmod 3$ were found by Hughes [13]. We checked with Magma [3] that in the cases $m=4$ and $m=6$, the 3-(17, 4, 2) design from Theorem 27 and the design with these parameters found in [13] are isomorphic. In case the two $3-(q+1,4,2)$ designs are isomorphic for every even $m \geq 4$, the contribution of Theorem 27 will be a coding-theoretic construction of the $3-(q+1,4,2)$ designs.

Example 28 Let $q = 2^4$. Then $\mathrm{Tr}_{q^2/q}(\mathcal{C}_{\{3,5\}})$ has parameters $[17,4,12]_{16}$ and weight enumerator

$$1 + 1020z^{12} + 24480z^{15} + 15555z^{16} + 24480z^{17},$$

and

$$\left(\mathcal{U}_{q+1}, \mathcal{B}_{q-4}\left(\mathrm{Tr}_{q^2/q}\left(\mathcal{C}_{\{3,5\}}\right)\right)\right)$$

is a $3-(17,12,22)$ design.

The code $\mathcal{C}_{\{3,5\}}{}^{\perp}|_{\mathrm{GF}(q)}$ has parameters $[17,13,4]_{16}$ and weight enumerator

$$\begin{aligned}
&1 + 5100z^4 + 42840z^5 + 2244000z^6 + 50669520z^7 + 949969350z^8 + \\
&\quad 14262976200z^9 + 171117027840z^{10} + 1633451574240z^{11} + \\
&\quad 12250821846060z^{12} + 70677865367400z^{13} + 302905113919200z^{14} + \\
&\quad 908715349415760z^{15} + 1703841278658465z^{16} + 1503389363654520z^{17},
\end{aligned}$$

and $\left(\mathcal{U}_{q+1}, \mathcal{B}_4\left(\mathcal{C}_{\{3,5\}}{}^{\perp}|_{\mathrm{GF}(q)}\right)\right)$ is a $3-(17,4,2)$ design.

6 On the q-dimension of $3-(q+1, q-4, (q-4)(q-5)(q-6)/60)$ and $3-(q+1,4,2)$ designs

In this section, we discuss the q-dimension of the 3-designs documented in Sect.5. Recall the q-dimension of t-designs introduced in [21] and the introduction of this paper. An obvious upper bound on the q-dimension is the dimension of the supporting code. We will use the following lemma to derive a lower bound.

Lemma 29 *Let* $f(x) = x^3 - 60x^2 - 61x - 60$. *Then* $f(x) > 0$ *for every* $x \geq 62$, *and* $f(x) < 0$ *for* $0 \leq x \leq 61$.

Proof The derivative $f'(x) = 3x^2 - 120x - 61$ has roots $20 \pm \sqrt{3783}/3$. It follows that $f(x)$ is decreasing on the interval $(20-\sqrt{3783}/3, 20+\sqrt{3783}/3)$, and increasing on the interval $(20+\sqrt{3783}/3, \infty)$. Note that $\sqrt{3783}/3 \approx 20.5$. Hence, $f(x)$ is decreasing on the interval $(0, 40)$, and increasing on the interval $(41, \infty)$. Since

$$f(0) = f(61) = -60, \ \ f(62) = 3846,$$

the lemma follows.

Theorem 30 *Suppose that* $\mathbb{D}$ *is a 3-*$(q+1, q-4, (q-4)(q-5)(q-6)/60)$ *design, where* q *is a prime power. If* $q > 63$ *then*

$$\dim_q \mathbb{D} \geq 4,$$

where $\dim_q \mathbb{D}$ *is the dimension of* $\mathbb{D}$ *over the finite field* $\mathrm{GF}(q)$ *of order* q.

Proof The number of blocks of $\mathbb{D}$ is

$$b = \frac{(q+1)q(q-1)}{60} = \frac{q^3 - q}{60}. \tag{28}$$

If $\mathcal{C}$ is a linear code over $\mathrm{GF}(q)$ of length $q+1$, such that every block of $\mathbb{D}$ is the support of a codeword of weight $q-4$, $\mathcal{C}$ must contain at least $b(q-1)$ codewords of weight $q-4$. It is sufficient to show that

$$b(q-1) > q^3 - 1, \tag{29}$$

which would imply that $|\mathcal{C}| \geq q^4$, hence, the dimension of $\mathcal{C}$ is greater that or equal to 4. Substituting b in (29) by the right-hand side of eq. (28) implies that the inequality (29) is equivalent to

$$q^3 - 60q^2 - 61q - 60 > 0. \tag{30}$$

Since $q > 63$, the inequality (30) holds by Lemma 29. □

As a corollary of Theorem 30, we have the following.

Theorem 31 *The 3-*$(q+1, q-4, (q-4)(q-5)(q-6)/60)$ *design* $\mathbb{D}$ *from Theorem 25 has dimension 4 over* $\mathrm{GF}(2^m)$ *for every even* $m \geq 6$.

Proof The blocks of the design $\mathbb{D}$ are supprts of minimum weight codwords in the $[q+1, 4, q-4]_q$ code $\mathcal{C}$ with $q = 2^m$, $m \geq 4$ even, from Theorem 22. Since the dimension of $\mathcal{C}$ is 4, it follows that $\dim_q \mathbb{D} \leq 4$. On the other hand, according to Theorem 30, $\dim_q \mathbb{D} \geq 4$ for $q = 2^m \geq 64$, that is, for every even $m \geq 6$. □

In the smallest case, $m = 4$, the 3-(17, 12, 22) design $\mathbb{D}$ supported by the $[17, 4, 12]_{2^4}$ code $\mathcal{C}$ from Theorem 22 does not satisfy the hypothesis of Theorem 30, thus, we only have $\dim_{16} \mathbb{D} \leq \dim \mathcal{C} = 4$.

It turns out that the subfield subcode $\mathcal{C}' = \mathcal{C}|_{\mathrm{GF}(4)}$ of the $[17, 4, 12]_{2^4}$ code $\mathcal{C}$ is a $[17, 4, 12]_4$ code with weight distribution

$$A_0 = 1, \ A_{12} = 204, \ A_{16} = 51.$$

The 68 distinct supports of codewords of weight 12 in $\mathcal{C}'$ are the blocks of a 3-(17, 12, 22) design $\mathbb{D}'$ identical with the design $\mathbb{D}$ supported by $\mathcal{C}$. Since

$$3 \cdot 68 > 3 \cdot 4^3,$$

it follows that

$$\dim_4 \mathbb{D}' = 4.$$

A lower bound 4 on the q-dimension of a 3-$(q+1, 4, 2)$ design for any prime power $q > 26$ can be proved as in Theorem 30. However, this bound is far below the upper bound provided by the dimension $q-3$ of the supporting code from Theorem 21. The following analysis of the $3-(17, 4, 2)$ design, the smallest design in the infinite family of 3-designs from Theorem 27, suggests that the q-dimension is likely to be equal to the dimension of the supporting code.

The $[17, 13, 4]_{16}$ code $\mathcal{C}$ from Theorem 21 is a cyclic code with generator polynomial $x^4 + x^3 + \beta^{10}x^2 + x + 1$, where β is a primitive element of GF(16). The following vector is a codeword of weight 4:

$$u = (1, 0, \beta^5, \beta^5, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0).$$

The twelve cyclic shifts of u form a 12×17 matrix M of rank 12 in echelon form. Clearly, replacing the nonzero entries of M by arbitrary nonzero elements of GF(16) changes M to another matrix of rank 12. It follows that the rank of every generalized GF(16)-incidence matrix of the $3-(17, 4, 2)$ design $\mathbb{D}$ from Theorem 27 is greater than or equal to 12. Thus, we have the following.

Theorem 32 *Let* $\mathbb{D}$ *be the* $3-(17, 4, 2)$ *design before. Then*

$$12 \le \dim_{16} \mathbb{D} \le 13.$$

7 Summary and concluding remarks

The main contributions of this paper are the following:

- A complete classification of linear codes over GF(2^h) of length $2^m + 1$ that are invariant under the action of the projective general group PGL(2, q) is established in Theorem 11.
- The 2-ranks of $3-(2^m+1, k, \lambda)$ designs that are invariant under the action of PGL(2, q) are determined in Theorem 12.
- A family of trace codes and a family of subfield subcodes, such that the set of the supports of all codewords of any fixed weight being invariant under PGL(2, q), are constructed in Theorems 23 and 24.
- The parameters of the 3-designs supported by the codewords of minimum weight in these linear codes are presented in Theorems25 and 27.
- It is proved in Theorem 26 that the complementary design $\bar{\mathbb{D}}$ of the 3-design $\mathbb{D}$ from Theorem 25 is isomorphic to the Witt spherical geometry with parameters $3-(2^m + 1, 5, 1)$ [23].
- A lower bound on the q-dimension of of 3-designs with parameters 3-$(q+1, (q-4), (q-4)(q-5)(q-6)/60)$, $q > 63$, is derived in Theorem 30, and it is shown that an infinite family of 3-designs described in Theorem 25 meet this bound.

We remark that the methodology of this paper may be extended to codes of length $p^m + 1$ over GF(p), where p is an odd prime. New linear codes supporting new t-designs may be found.

Acknowledgements The authors are grateful to the reviewers and the Editors for their comments and suggestions that improved the presentation of this paper.

References

1. Assmus Jr. E.F., Mattson Jr. H.F.: New 5-designs. J. Comb. Theory **6**, 122–151 (1969).
2. Beth T., Jungnickel D., Lenz H.: Design Theory. Cambridge University Press, Cambridge (1999).
3. Bosma W., Cannon J.: Handbook of Magma Functions. University of Sydney, School of Mathematics and Statistics, Sydney (1999).

4. Colbourn C.J., Dinitz J.F.: Handbook of Combinatorial Designs, 2nd edn. Chapman & Hall/CRC, Boca Raton (2007).
5. Dickson L.E.: Linear Groups: With an Exposition of the Galois Field Theory. Teubner, Leipzig (1901).
6. Delsarte P.: On subfield subcodes of modified Reed-Solomon codes. IEEE Trans. Inform. Theory **21**(5), 575–576 (1975).
7. Ding C.: Designs from Linear Codes. World Scientific, Singapore (2018).
8. Ding C., Tang C.: Infinite families of near MDS codes holding t-designs. IEEE Trans. Inform. Theory **66**(9), 5419–5428 (2020).
9. Du X., Wang R., Fan C.: Infinite families of 2-designs from a class of cyclic codes. J. Comb. Des. **28**(3), 157–170 (2020).
10. Giorgetti M., Previtali A.: Galois invariance, trace codes and subfield subcodes. Finite Fields Appl. **16**(2), 96–99 (2010).
11. Huber M.: The classification of flag-transitive Steiner 3-designs. Adv. Geom. **5**(2), 195–221 (2005).
12. Huffman W.C., Pless V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003).
13. Hughes D.R.: On t-designs and groups. Am. J. Math. **87**(4), 761–778 (1965).
14. Jungnickel D., Magliveras S.S., Tonchev V.D., Wassermann A.: The classification of Steiner triple systems on 27 points with 3-rank 24. Des. Codes Cryptogr. **87**, 831–839 (2019).
15. Jungnickel D., Tonchev V.D.: New invariants for incidence structures. Des. Codes Cryptogr. **68**, 163–177 (2013).
16. Jungnickel D., Tonchev V.D.: Counting Steiner triple systems with classical parameters and prescribed rank. J. Comb. Theory Ser. A **162**, 10–33 (2019).
17. Passman D.S.: Permutation Groups. Benjamin, New York (1968).
18. Shi M., Xu L., Krotov D.S.: The number of the non-full-rank Steiner triple systems. J. Comb. Des. **27**(10), 571–585 (2019).
19. Tang C.: Infinite families of 3-designs from APN functions. J. Comb. Des. **28**(2), 97–117 (2020).
20. Tang C., Ding C.: An infinite family of linear codes supporting 4-designs. IEEE Trans. Inform. Theory **67**(1), 244–254 (2021).
21. Tonchev V.D.: Linear perfect codes and a characterization of the classical designs. Des. Codes Cryptogr. **17**, 121–128 (1999).
22. Tonchev V.D.: Codes. In: Colbourn C.J., Dinitz J.H. (eds.) Handbook of Combinatorial Designs, 2nd edn, pp. 677–701. CRC Press, New York (2007).
23. Witt E.: Über Steinersche Systeme. Abh. Math. Sem. Hamburg **12**, 265–275 (1938).
24. Xiang C., Ling X., Wang Q.: Combinatorial t-designs from quadratic functions. Des. Codes Cryptogr. **88**(3), 553–565 (2020).
25. Zinoviev D.V.: The number of Steiner triple systems $S(2^m-1,3,2)$ of rank 2^m-m+2 over $\mathbb{F}_2$. Discrete Math. **339**, 2727–2736 (2016).
26. Zinoviev V.A., Zinoviev D.V.: Steiner triple systems $S(2^m-1,3,2)$ of rank 2^m-m+1 over $\mathbb{F}_2$. Probl. Inf. Transm. **48**, 102–126 (2012).
27. Zinoviev V.A., Zinoviev D.V.: Structure of Steiner triple systems $S(2^m-1,3,2)$ of rank 2^m-m+2 over $\mathbb{F}_2$. Probl. Inf. Transm. **49**, 232–248 (2013).
28. Zinoviev V.A., Zinoviev D.V.: Remark on Steiner triple systems $S(2^m-1,3,2)$ of rank 2^m-m+1 over $\mathbb{F}_2$ published in Probl. Peredachi Inf., 2012, no. 2. Probl. Inf. Transm. **49**, 107–111 (2013).