Designs, Codes and Cryptography
https://doi.org/10.1007/s10623-023-01255-z

Linear codes from arcs and quadrics

Kanat Abdukhalikov[1] · Duy Ho[1]

Received: 9 May 2022 / Revised: 20 May 2023 / Accepted: 27 May 2023

Abstract
Using characterizations of ovals, KM-arcs and elliptic quadrics recently described in polar coordinates, we construct some families of LCD, self-orthogonal, three-weight and four-weight linear codes. We also demonstrate some applications to quantum codes.

Keywords Hyperovals · KM-arcs · Ovoids · Linear codes · LCD codes · Self-orthogonal codes · Quantum codes · Linear codes with few weights

Mathematics Subject Classification 51E15 · 51E21 · 94B05

1 Introduction

In the projective plane $PG(2, q)$, where q is even, a *KM-arc of type t* (also known as a $(q + t, t)$*-arc of type* $(0, 2, t)$) is a set H of $q + t$ points meeting every line in 0, 2 or t points. When $t = 2$, the set H is called a *hyperoval*. Hyperovals are well-studied objects in geometry as they have important applications in symmetric cryptography and coding theory. In standard coordinates, hyperovals can be represented by so-called o-polynomials. From hyperovals and o-polynomials, many good linear codes were obtained, cp. [20, Chapter 12], [29, 43]. The more general KM-arcs were introduced in [32] and further studied in [19, 26, 41, 42]. It appears that linear codes from KM-arcs were not considered before in the literature.

In the projective space $PG(3, q)$ with $q > 2$, an *ovoid* V is a set of $q^2 + 1$ points no three of which are on the same line. The classical example of an ovoid is an *elliptic quadric*, whose points come from a non-degenerate elliptic quadratic form. Linear codes from points of ovoids in standard coordinates were considered in [20, Chapter 13], [22].

This is one of several papers published in *Designs, Codes and Cryptography* comprising the "Special Issue: Finite Geometries 2022".

✉ Duy Ho
duyho92@gmail.com

Kanat Abdukhalikov
abdukhalik@uaeu.ac.ae

[1] UAE University, PO Box 15551, Al Ain, UAE

Published online: 12 June 2023

In this paper, we study linear codes using a newly developed representation of KM-arcs, hyperovals and elliptic quadrics in polar coordinates. This representation was initiated by investigations in [1–4]. Characterizations for KM-arcs and hyperovals were obtained via power sums in [5] and [7], which we will demonstrate to be expedient for constructing linear codes with special properties.

Linear codes with complementary duals (LCD codes) were introduced by Massey in [36]. In recent years, LCD codes became an attractive research interest as they offer solutions to many cryptographic problems, for example against side-channel attacks and fault non-invasive attacks [17]. On the other hand, linear codes with few weights have applications in secret sharing schemes [8, 16] and authentication codes [21, 23]. Using polar presentation of KM-arcs, we obtain new constructions of LCD codes with few weights.

A quantum error-correcting code is a code that protects quantum information from corruption by noise in a way that is similar to how a classical error-correcting code protects information on the classical channel. The theory of stabilizer codes allows the construction of quantum error-correcting codes using classical codes that are self-orthogonal with respect to symplectic, Euclidean and Hermitian inner products.

One of the main problems in quantum coding theory is to find quantum stabilizer codes with optimal parameters. Recently Ball et al. [11, 13, 14] described quantum MDS (maximum distance separable) codes using methods of finite geometry. We further demonstrate the potential of these methods in constructing quantum error-correcting codes. We construct Euclidean and Hermitian self-orthogonal codes based on arcs and other combinatorial objects, which lead, in turn, to quantum codes.

In general, databases of known linear and quantum codes (cp. [27] and external links therein) are only available for $q \leq 10$. Consequently, there is an increasing interest in studying codes over large finite fields, cp. [37, 38]. Constructions of LCD codes, self-orthogonal codes and quantum codes we provided in this paper are considered over large finite fields of characteristic 2. Examples of codes we obtained are either new or with good parameters compared to the literature.

The paper is organized as follows. In Sect. 2, we recall preliminary results from coding theory and finite geometry. In Sect. 3, we consider LCD codes obtained from finite geometries. In Sect. 4, we describe a large family of Euclidean self-orthogonal codes derived from ovals and obtain some examples of quantum codes from this family. In Sect. 5, we consider three-weight and four-weight LCD codes derived from KM-arcs.

2 Preliminaries

2.1 Linear codes, LCD and self-orthogonal codes

Let $\mathbb{F}_q$ be a finite field of q elements. A linear $[n, k]$-code C over $\mathbb{F}_q$ is a k-dimensional vector subspace of $\mathbb{F}_q$. A generator matrix G of C is a $k \times n$ matrix whose rows form a basis of C. The weight $wt(c)$ of a codeword $c \in C$ is the number of nonzero components of c. Let A_i denote the number of codewords with Hamming weight i in C. The weight enumerator of C is defined by

$$A(z) = 1 + A_1 z + A_2 z_2 + \cdots + A_n z_n.$$

The sequence $(1, A_1, A_2, \ldots, A_n)$ is called the weight distribution of the code C. The minimum weight d of all nonzero codewords in C is called the minimum weight of C. An $[n, k, d]$-code is an $[n, k]$-code with the minimum weight d.

We say that two codes are equivalent if one can be obtained from the other by a permutation of the coordinates.

Given a linear code C of length n over $\mathbb{F}_q$ (resp. $\mathbb{F}_{q^2}$), its Euclidean dual code (resp. Hermitian dual code) is denoted by $C^{\perp}$ (resp. $C^{\perp H}$). The codes $C^{\perp}$ and $C^{\perp H}$ are defined by

$$C^{\perp} = \left\{(b_0, b_1, \ldots, b_{n-1}) \in \mathbb{F}_q^n : \sum_{i=0}^{n-1} b_i c_i = 0, \forall (c_0, c_1, \ldots, c_{n-1}) \in C\right\},$$
$$C^{\perp H} = \left\{(b_0, b_1, \ldots, b_{n-1}) \in \mathbb{F}_{q^2}^n : \sum_{i=0}^{n-1} b_i c_i^q = 0, \forall (c_0, c_1, \ldots, c_{n-1}) \in C\right\},$$

respectively.

A linear code C over $\mathbb{F}_q$ is called a *Euclidean linear complementary dual code* (or for short, Euclidean LCD code) if $C \cap C^{\perp} = \{0\}$. A linear code C over $\mathbb{F}_{q^2}$ is called a *Hermitian linear complementary dual code* (Hermitian LCD code) if $C \cap C^{\perp H} = \{0\}$. The following lemma characterizes of Euclidean and Hermitian LCD codes.

Lemma 1 *If G is a generator matrix for the $[n, k]$-linear code C, then C is a Euclidean (resp. Hermitian) LCD code if and only if the $k \times k$ matrix GG^T (resp. $G\bar{G}^T$) is nonsingular.*

A linear code C is called *Euclidean self-orthogonal* (resp. *Hermitian self-orthogonal*) if $C \subseteq C^{\perp}$ (resp. $C \subseteq C^{\perp H}$). The following lemma provides a characterization for self-orthogonal codes.

Lemma 2 *If G is a generator matrix for an $[n, k]$-linear code C, then C is a Euclidean (resp. Hermitian) self-orthogonal code if and only if $GG^T = \mathbf{0}$ (resp. $G\bar{G}^T = \mathbf{0}$).*

The code C is called *Euclidean self-dual* (resp. *Hermitian self-dual)* if $C = C^{\perp}$ (resp. $C = C^{\perp H}$).

2.2 Polar coordinates

In this paper we consider finite fields only in characteristics 2. Let $F = \mathbb{F}_{2^m}$ be a finite field of order $q = 2^m$. Consider F as a subfield of $K = \mathbb{F}_{2^n}$, where $n = 2m$, so K is a two dimensional vector space over F. Let F^* and K^* denote the multiplicative group of F and K, respectively. The *conjugate* of $x \in K$ over F is

$$\bar{x} = x^q.$$

Then the *trace* and the *norm* maps from K to F are

$$T(x) = Tr_{K/F}(x) = x + \bar{x} = x + x^q,$$
$$N(x) = N_{K/F}(x) = x\bar{x} = x^{1+q}.$$

The *unit circle* of K is the set of elements of norm 1:

$$S = \{u \in K \mid u\bar{u} = 1\}.$$

Therefore, S is the multiplicative group of $(q + 1)$st roots of unity in K. Since $F \cap S = \{1\}$, each non-zero element of K has a unique polar coordinate representation $x = \lambda u$ with $\lambda \in F^*$ and $u \in S$. For any $x \in K^*$ we have $\lambda = \sqrt{x\bar{x}}$ and $u = \sqrt{x/\bar{x}}$.

One can define a nondegenerate bilinear form $\langle \cdot, \cdot \rangle : K \times K \to F$ by

$$\langle x, y \rangle = T(x\bar{y}) = x\bar{y} + \bar{x}y.$$

Then the form $\langle \cdot, \cdot \rangle$ is alternating and symmetric, that is, $\langle a, a \rangle = 0$ and $\langle a, b \rangle = \langle b, a \rangle$.

Following [25], consider an element $\mathbf{i} \in K$ with property $T(\mathbf{i}) = \mathbf{i} + \mathbf{i}^q = 1$. Then $K = F(\mathbf{i})$ and $\mathbf{i}$ is a root of a quadratic equation

$$z^2 + z + \delta = 0,$$

where $\delta = N(\mathbf{i}) \in F$. Any element $z \in K$ can be represented as $z = x + y\mathbf{i}$, where $x, y \in F$. For $z = x + y\mathbf{i}$ we have $x = \langle \mathbf{i}, z \rangle$, and $y = \langle 1, z \rangle$.

2.3 Affine and projective planes in polar presentation

In [1, 2] (see also [10] and references therein), the polar representation of $PG(2, q)$ was introduced using the field K. Consider pairs $(x : z)$, where $x \in K, z \in F, x \neq 0$ or $z \neq 0$, and we identify $(x : z)$ with $(\lambda x : \lambda z)$, $\lambda \in F^*$. Then points of $PG(2, q)$ are

$$\{(x : 1) \mid x \in K\} \cup \{(u : 0) \mid u \in S\}.$$

For $\alpha \in K$, $\beta \in F$, $(\alpha, \beta) \neq (0, 0)$, we define the lines $[\alpha : \beta]$ in $PG(2, q)$ as

$$[\alpha : \beta] = \{(x : z) \in PG(2, q) \mid \langle \alpha, x \rangle + \beta z = 0\}.$$

Pairs $[\alpha : \beta]$ and $[\lambda\alpha : \lambda\beta]$ with $\lambda \in F^*$ define the same lines. The point $(x : z)$ is incident with the line $[\alpha : \beta]$ if and only if $\langle \alpha, x \rangle + \beta z = 0$. The element $u_\infty = (u : 0)$, $u \in S$, will be referred to as the point at infinity in the direction of u. So $[0 : 1]$ indicates the line at infinity.

We define an affine plane $AG(2, q) = PG(2, q) \backslash [0 : 1]$, so points of this affine plane $AG(2, q)$ are $\{(x : 1) \mid x \in K\}$. Associating $(x : 1)$ with $x \in K$ we can identify points of the affine plane $AG(2, q)$ with elements of the field K, and we write $AG(2, q) = K$. Lines of $AG(2, q) = K$ are of the form

$$L(u, \mu) = \{x \in K \mid \langle u, x \rangle + \mu = 0\},$$

where $u \in S$ and $\mu \in F$ (cp. [10, subsection 2.1]).

2.4 Hyperovals, ovals, and Vandermonde sets

We recall sets with the following property first considered by Gács and Weiner [26] (and subsequently by other authors in [15, 39]). Let $1 < t < q$. A set $T = \{y_1, \ldots, y_t\} \subseteq \mathbb{F}_q$ is called a *Vandermonde set* if

$$\pi_k(T) := \sum_{y \in T} y^k = 0,$$

for all $1 \leq k \leq t - 2$. The set T is a *super-Vandermonde set* if it is a Vandermonde set and $\pi_{t-1}(T) = 0$. Some examples of Vandermonde sets can be found in [39, Proposition 1.8].

In the projective plane $PG(2, q)$, where q is even, an *oval* is a set of $q + 1$ points, no three of which are collinear. Any line of the plane meets the oval $\mathcal{O}$ at either 0, 1 or 2 points and is called exterior, tangent or secant, respectively. All the tangent lines to the oval $\mathcal{O}$ concur at the same point N, called the *nucleus* of $\mathcal{O}$. The set $\mathcal{H} = \mathcal{O} \cup N$ becomes a hyperoval. Conversely, by removing any point from hyperoval one gets an oval.

In [5], it was shown that if $\mathcal{O}$ is an oval with points in $AG(2, q) = K$ and nucleus 0, then $\mathcal{O}$ is a super-Vandermonde set. Also, a hyperoval with points in K is a Vandermonde set.

3 LCD codes over $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$, q even

In this section, we consider LCD codes obtained from sets of points in $PG(2, q)$ identified as elements from finite fields. Particular cases are ovals and Vandermonde sets. With a similar approach, we will also consider LCD codes obtained from elliptic quadrics in $PG(3, q)$.

3.1 LCD codes from sets of points in $\mathbb{F}_{q^2}$

Let $V := \{v_1, \dots, v_t\}$ be a set of size t in $K = \mathbb{F}_{q^2}$ with the property

$(*)$ $\sum_{i=1}^{t} v_i = 0$ and $\sum_{i=1}^{t} v_i^{q+1} \neq 0$.

For each $1 \leq i \leq t$, let $x_i, y_i \in F$ be such that $v_i = x_i + y_i \mathbf{i}$.

Theorem 1 *For $\alpha \in \mathbb{F}_{q^2}^*$, let*

$$A = \begin{bmatrix} x_1 & x_2 & x_3 & \dots & x_t & 0 \\ y_1 & y_2 & y_3 & \dots & y_t & 0 \\ 1 & 1 & 1 & \dots & 1 & \alpha \end{bmatrix}.$$

1. *If $\alpha \in \mathbb{F}_q^*$ such that $\alpha + t \neq 0$, then the $[t+1, 3]$-linear code $\mathcal{C}_{\oslash}(V)$ over $\mathbb{F}_q$ with generator matrix A is a Euclidean LCD code.*
2. *If $\alpha \in \mathbb{F}_{q^2}^*$ such that $\alpha^{q+1} + t \neq 0$, then the $[t+1, 3]$-linear code $\mathcal{C}_{\oslash}(V)$ over $\mathbb{F}_{q^2}$ with generator matrix A is a Hermitian LCD code.*

Proof We have

$$\sum_{i=1}^{t} x_i = \sum_{i=1}^{t} \langle \mathbf{i}, v_i \rangle = \sum_{i=1}^{t} (v_i \mathbf{i}^q + v_i^q \mathbf{i}) = \left(\sum_{i=1}^{t} v_i \right) \mathbf{i}^q + \left(\sum_{i=1}^{t} v_i^q \right) \mathbf{i} = 0,$$

and so $\sum_{i=1}^{t} x_i^2 = 0$. Since $\sum_{i=1}^{t} v_i = 0$, it follows that

$$\sum_{i=1}^{t} v_i^2 = \sum_{i=1}^{t} x_i^2 + \mathbf{i}^2 \sum_{i=1}^{t} y_i^2 = 0,$$

and so $\sum_{i=1}^{t} y_i^2 = 0$. Also,

$$\begin{aligned} \sum_{i=1}^{t} x_i^q y_i = \sum_{i=1}^{t} x_i y_i^q = \sum_{i=1}^{t} x_i y_i \\ &= \sum_{i=1}^{t} \langle 1, v_i \rangle \langle \mathbf{i}, v_i \rangle = \sum_{i=1}^{t} (v_i + v_i^q)(v_i \mathbf{i}^q + v_i^q \mathbf{i}) \end{aligned}$$

$$\begin{aligned}&= \sum_{i=1}^{t}(v_i^2\mathbf{i}^q + v_i^{q+1}\mathbf{i}^q + v_i^{q+1}\mathbf{i} + v_i^{2q}\mathbf{i})\\ &= \left(\sum_{i=1}^{t} v_i^2\right)\mathbf{i}^q + \sum_{i=1}^{t} v_i^{q+1} + \left(\sum_{i=1}^{t} v_i^{2q}\right)\mathbf{i}\\ &= 0 + a + 0 = a,\end{aligned}$$

where $a = \sum\limits_{i=1}^{t} v_i^{q+1} \neq 0$.

1. If $\alpha \in \mathbb{F}_q^*$ such that $\alpha + t \neq 0$, then

$$AA^T = \begin{bmatrix} 0 & a & 0 \\ a & 0 & 0 \\ 0 & 0 & \alpha^2 + t \end{bmatrix}$$

   is nonsingular, since $\alpha + t \neq 0$ if and only if $\alpha^2 + t \neq 0$. It follows that $\mathcal{C}_\alpha(V)$ is a Euclidean LCD code over $\mathbb{F}_q$.
2. If $\alpha \in \mathbb{F}_{q^2}^*$ such that $\alpha^{q+1} + t \neq 0$, then

$$A\bar{A}^T = \begin{bmatrix} 0 & a & 0 \\ a & 0 & 0 \\ 0 & 0 & \alpha^{q+1} + t \end{bmatrix}$$

   is nonsingular, and so $\mathcal{C}_\alpha(V)$ is a Hermitian LCD code over $\mathbb{F}_{q^2}$.

□

Corollary 1 *Let V be a super-Vandermonde set of size $q+1$ in K. Then for $\alpha \in \mathbb{F}_q \backslash \{0, 1\}$, the code $\mathcal{C}_\alpha(V)$ is a Euclidean LCD code over $\mathbb{F}_q$. Similarly, for $\alpha \in \mathbb{F}_{q^2}^*$ such that $\alpha^{q+1} \neq 1$, the code $\mathcal{C}_\alpha(V)$ is a Hermitian LCD code over $\mathbb{F}_{q^2}$.*

Corollary 2 *Let $\mathcal{O}$ be an oval of $q+1$ points in K with nucleus at 0. Then for $\alpha \in \mathbb{F}_q \backslash \{0, 1\}$, the code $\mathcal{C}_\alpha(\mathcal{O})$ is a Euclidean LCD MDS code over $\mathbb{F}_q$.*

Remark 1 According to [20, Section 12.2], the code $\mathcal{C}_\alpha(\mathcal{O})$ in Corollary 2 has parameters $[q+2, 3, q]$ and weight enumerator

$$1 + \frac{(q+2)(q^2-1)}{2} z^q + \frac{q(q-1)^2}{2} z^{q+2}.$$

The dual of $\mathcal{C}_\alpha(\mathcal{O})$ has parameters $[q+2, q-1, 4]$.

Remark 2 A particular case of Corollary 2 is when $\mathcal{O}$ is the hyperconic. The resulting code $\mathcal{C}_\alpha(\mathcal{O})$ is equivalent to the code constructed in [18, Lemma 1].

Corollary 3 *Let $\mathcal{O}$ be an oval of $q+1$ points in K with nucleus at 0. Then for $\alpha \in \mathbb{F}_{q^2}^*$ such that $\alpha^{q+1} \neq 1$, the code $\mathcal{C}_\alpha(\mathcal{O})$ is a Hermitian LCD MDS code over $\mathbb{F}_{q^2}$ with parameters $[q+2, 3, q]$.*

Proof The parity-check matrix for the dual code $\mathcal{C}_\alpha(\mathcal{O})^\perp$ is A. Any three columns of A are linearly independent, thus the minimum distance of $\mathcal{C}_\alpha(\mathcal{O})^\perp$ is greater than 3. Hence $\mathcal{C}_\alpha(\mathcal{O})^\perp$ has a minimum distance 4 by the Singleton bound. This implies $\mathcal{C}_\alpha(\mathcal{O})^\perp$ is an MDS code with parameters $[q+2, q-1, 4]$. It follows that $\mathcal{C}_\alpha(\mathcal{O})$ is also an MDS code with parameters $[q+2, 3, q]$. □

Example 1 Ovals are super-Vandermonde sets of size $q+1$. However, it was shown in [5] that there are Vandermonde sets of size $q+1$ which are not ovals. For $q=8$, let $\lambda, \mu \in F^*$ such that $1+\lambda^3+\mu^3=0$. Let

$$H := \{1, \omega, \bar{\omega}, \lambda, \lambda\omega, \lambda\bar{\omega}, \mu, \mu\omega, \mu\bar{\omega}\},$$

where $\omega \in S$ such that $\omega^3=1, \omega \neq 1$. Then H is a Vandermonde set but not an oval, as the line $L(1,0)$ intersects H in three points $1, \lambda$ and μ.

For $\alpha \in \mathbb{F}_8 \backslash \{0,1\}$, the code $\mathcal{C}_\alpha(H)$ over $\mathbb{F}_8$ is a Euclidean LCD code with parameters $[10,3,6]$. This code is almost optimal (since $[10,4,6]_8$ is an optimal code according to [27]).

For $\alpha \in \mathbb{F}_{64}^*$ such that $\alpha^{q+1} \neq 1$, the Hermitian LCD code $\mathcal{C}_\alpha(H)$ over $\mathbb{F}_{64}$ also has parameters $[10,3,6]$. To our knowledge, this code is new.

3.2 LCD cyclic codes from the elliptic quadric

In standard coordinates, a classical ovoid V can be defined as the following set of points:

$$V = \{(0,0,1,0)\} \cup \{(x, y, x^2+xy+ay^2, 1) : x, y \in \mathbb{F}_q\},$$

where $a \in \mathbb{F}_q$ such that the polynomial x^2+x+a has no root in $\mathbb{F}_q$. Such ovoid is called an *elliptic quadric*, as the points come from a non-degenerate elliptic quadratic form.

Let $E \supset K \supset F$ be a chain of finite fields, $|E|=q^4$, $|K|=q^2$, $|F|=q$, $q=2^m$. We note that $PG(3,q)$ can be represented using the field $E=\mathbb{F}_{q^4}$ (cp. [10]). In [6, Theorem 4], it was shown that the set

$$\mathcal{O} = \{u \in E \mid u^{q^2+1}=1\}$$

determines an elliptic quadric in $PG(3,q)$. In [6, Theorem 5], it was shown that an ovoid code $\mathcal{C}$ obtained from an elliptic quadric in $PG(3,q)$ is equivalent to a cyclic code over $\mathbb{F}_q$ with parameters $[q^2+1, 4, q^2-q]$. In the following theorem, we extend this result further by showing that this code $\mathcal{C}$ is an LCD code.

Theorem 2 *An ovoid code $\mathcal{C}$ obtained from an elliptic quadric in $PG(3,q)$ is equivalent to an LCD cyclic code over $\mathbb{F}_q$ with parameters $[q^2+1, 4, q^2-q]$.*

Proof In the proof of [6, Theorem 5], it was shown that $\mathcal{C}^\perp$ is a cyclic $[q^2+1, q^2-3, 4]$-code with generator polynomial (for a definition see [30, Chapter 4])

$$g(x) = (x-\gamma)(x-\gamma^q)(x-\gamma^{q^2})(x-\gamma^{q^3}),$$

where $\gamma \in E$ such that $\gamma^{q^2+1}=1$. Let $g^*(x)=x^{\deg(g)}g(x^{-1})$ be the reciprocal of $g(x)$. We note that $\gamma^{q^3+q^2+q+1}=1$, and so

$$\begin{aligned} g^*(x) &= x^4(x^{-1}-\gamma)(x^{-1}-\gamma^q)(x^{-1}-\gamma^{q^2})(x^{-1}-\gamma^{q^3}) \\ &= (1-x\gamma)(1-x\gamma^q)(1-x\gamma^{q^2})(1-x\gamma^{q^3}) \\ &= (\gamma^{q^2}-x)(\gamma^{q^3}-x)(\gamma-x)(\gamma^q-x) = g(x). \end{aligned}$$

Since $g^*(x)=g(x)$, by [33, Theorem 4], $\mathcal{C}^\perp$ is an LCD code. Therefore $\mathcal{C}$ is also an LCD code. □

Remark 3 By [20, Theorem 13.6], the weight enumerator of $\mathcal{C}$ is

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

4 Euclidean self-orthogonal linear codes from ovals in $\mathbb{F}_{q^2}$, q even

4.1 Self-orthogonal codes from the unit circle

Let $S = \{u \in K \mid u^{q+1} = 1\} = \langle w \rangle = \{1, w, \ldots, w^q\}$ be the unit circle. We note that

$$\sum_{u \in S} u^i = \begin{cases} 0 & \text{if } i \neq 0 \pmod{q+1}, \\ 1 & \text{if } i = 0 \pmod{q+1}. \end{cases}$$

Let $L := \{l_1, \ldots, \text{ł}_t\}$, where $1 \leq l_i \leq q$ for each $1 \leq i \leq t$. Let $\mathbf{v} := (v_1, \ldots, v_t) \in S^t$. Let G be the matrix whose (i, j)-entry is $\left\langle v_i, w^{(j-1)l_i} \right\rangle$, where $1 \leq i \leq t$, $1 \leq j \leq q+1$, that is,

$$G = \begin{bmatrix} \langle v_1, 1 \rangle & \left\langle v_1, w^{l_1} \right\rangle & \ldots & \left\langle v_1, w^{ql_1} \right\rangle \\ \langle v_2, 1 \rangle & \left\langle v_2, w^{l_2} \right\rangle & \ldots & \left\langle v_2, w^{ql_2} \right\rangle \\ \ldots & \ldots & \ldots & \ldots \\ \langle v_t, 1 \rangle & \left\langle v_t, w^{l_t} \right\rangle & \ldots & \left\langle v_t, w^{ql_t} \right\rangle \end{bmatrix}.$$

Let $\mathcal{C}$ be the linear code over $\mathbb{F}_q$ with generator matrix G.

Theorem 3 *If $l_i \neq l_j$ and $l_i + l_j \neq q+1$ for each $i \neq j$, then $\mathcal{C}$ is a Euclidean self-orthogonal code over $\mathbb{F}_q$ with parameters $[q+1, t]$.*

Proof 1. For $1 \leq i \leq t$, let $\mathbf{r}_i$ be the i-th row of G. For $(c_1, \ldots, c_t) \in F^t$, we have

$$c_1\mathbf{r}_1 + c_2\mathbf{r}_2 \cdots + c_t\mathbf{r}_t = \mathbf{0}$$

if and only if $\sum\limits_{i=1}^{t} c_i \left\langle v_i, u^{l_i} \right\rangle = 0$ for each $u \in S$. For $u \in S$, let

$$\begin{aligned} P(u) &= \sum_{i=1}^{t} c_i \left\langle v_i, u^{l_i} \right\rangle = \sum_{i=1}^{t} c_i (v_i^q u^{l_i} + v_i u^{l_i q}) \\ &= \sum_{i=1}^{t} c_i v_i^q u^{l_i} + \sum_{i=1}^{t} c_i v_i u^{l_i q} \\ &= \sum_{i=1}^{t} c_i v_i^q \psi_{l_i}(u) + \sum_{i=1}^{t} c_i v_i \psi_{ql_i}(u), \end{aligned}$$

where each ψ_i is a homomorphism from S to K^* defined by

$$\psi_i : x \mapsto x^i.$$

From the conditions on L, the set $\Psi := \{\psi_i \mid i \in \{l_1, \ldots, l_t, ql_1, \ldots ql_t\}\}$ consists of pairwise distinct homomorphisms and by Artin's Lemma [34, Lemma 2.33], Ψ is a linearly independent set. In particular, if $P(u) = 0$ for each $u \in S$, then $c_i = 0$ for each i. This implies that the rows of G are linearly independent and so $\operatorname{rank}(G) = t$.

2. For $1 \leq i \leq t$, since $1 \leq l_i \leq q$, we have

$$\sum_{u \in S} \left\langle v_i, u^{l_i} \right\rangle = \sum_{u \in S} \left(v_i^q u^{l_i} + v_i u^{l_i q} \right) = v_i^q \sum_{u \in S} u^{l_i} + v_i \sum_{u \in S} u^{l_i q} = 0.$$

This implies $\sum_{u\in S}\left\langle v_i, u^{l_i}\right\rangle^2=0$. For $1\le i,j\le t, i\ne j$,

$$\begin{aligned}\sum_{u\in S}\left\langle v_i, u^{l_i}\right\rangle\left\langle v_j, u^{l_j}\right\rangle &= \sum_{u\in S}(v_iu^{l_iq}+v_i^qu^{l_i})(v_ju^{l_jq}+v_j^qu^{l_j})\\ &= v_iv_j\sum_{u\in S}u^{l_iq+l_jq}+v_i^qv_j\sum_{u\in S}u^{l_i+l_jq}\\ &\quad+v_iv_j^q\sum_{u\in S}u^{l_iq+l_j}+v_i^qv_j^q\sum_{u\in S}u^{l_i+l_j}\\ &=0,\end{aligned}$$

from the assumption on L. It follows that GG^T is the zero matrix and so $\mathcal{C}$ is a Euclidean self-orthogonal code over $\mathbb{F}_q$. □

Extended codes from Theorem 3 are also self-orthogonal codes. For suitable parameters, we can further obtain self-dual and near-MDS codes, as seen in the following example.

Example 2 Let $m=3$ so that $q=8$. Let $\mathbf{v}=(a,b,c,d)\in S^4$ and $L=\{1,2,3,4\}$. Let

$$G=\begin{bmatrix}\langle a,1\rangle & \langle a,w\rangle & \dots & \left\langle a,w^8\right\rangle & 0\\ \langle b,1\rangle & \left\langle b,w^2\right\rangle & \dots & \left\langle b,w^{16}\right\rangle & 0\\ \langle c,1\rangle & \left\langle c,w^3\right\rangle & \dots & \left\langle c,w^{24}\right\rangle & 0\\ \langle d,1\rangle & \left\langle d,w^4\right\rangle & \dots & \left\langle d,w^{32}\right\rangle & 0\\ 1 & 1 & \dots & 1 & 1\end{bmatrix}.$$

The code $\mathcal{C}$ over $\mathbb{F}_q$ with generator matrix G is a self-dual linear code. Furthermore, $\mathcal{C}$ is near-MDS when it has parameters [10, 5, 5]. Based on calculations from GAP [40] package GUAVA [9], we include some suitable vectors $\mathbf{v}$ for this to occur.

1. $\mathbf{v}=(1,1,1,w^i)$ is not suitable for any i.
2. $\mathbf{v}=(1,1,w,w^i)$, where $i=1,2,7,8$.
3. $\mathbf{v}=(1,w,w,w^i)$, where $i=0,2$.
4. $\mathbf{v}=(1,w,w^2,w^i)$ is not suitable unless $i=2$.
5. $\mathbf{v}=(1,w,w^3,w^i)$ is not suitable for any i.
6. $\mathbf{v}=(1,w,w^4,w^i)$, where $i=0,2,6$.

Remark 4 We note that if $\mathbf{v}=(a,b,c,d)$ is a suitable vector, then so is (a^2,b^2,c^2,d^2). To show that this is true, let $g_{i,j}$ be the (i,j)-entry of G. Let G' be the matrix whose (i,j)-entry is $g_{i,j}^2$. Since the map $x\mapsto x^2$ is a permutation of S, up to permutations of columns, G' is equal to the matrix

$$\begin{bmatrix}\left\langle a^2,1\right\rangle & \left\langle a^2,w\right\rangle & \dots & \left\langle a^2,w^8\right\rangle & 0\\ \left\langle b^2,1\right\rangle & \left\langle b^2,w^2\right\rangle & \dots & \left\langle b^2,w^{16}\right\rangle & 0\\ \left\langle c^2,1\right\rangle & \left\langle c^2,w^3\right\rangle & \dots & \left\langle c^2,w^{24}\right\rangle & 0\\ \left\langle d^2,1\right\rangle & \left\langle d^2,w^4\right\rangle & \dots & \left\langle d^2,w^{32}\right\rangle & 0\\ 1 & 1 & \dots & 1 & 1\end{bmatrix}.$$

Remark 5 Linear codes over $\mathbb{F}_8$ with parameters [10, 5, 5] are optimal according to [27]. In Example 2, the code $\mathcal{C}$ is self-dual, which is not the case for the code presented in [27]. A self-dual $[10,5,5]_8$ code was described in [28] as a random code. Example 2 is a constructive example of a self-dual $[10,5,5]_8$ code.

4.2 Self-orthogonal codes from ovals

Generalising Theorem 3, in this subsection we construct linear codes from arbitrary ovals. For a set $X \subseteq \mathbb{Z}$, denote $X_n := \{x \pmod n) \mid x \in X\}$.

Recall that $q = 2^m$. Let

$$\mathcal{E} := \left\{ \sum_{j=0}^{m-1} 2^j x_j > 0 \mid x_j \in \{0, 1, q\} \right\}.$$

Lemma 3 *Let $\mathcal{O} \subset K$ be an oval with nucleus at* 0*. Let $v, w \in K$ and $i, j \in \mathcal{E}, i \neq j$. If $\{i + j, iq + j\}_{q^2-1} \subset \mathcal{E}$, then $\sum_{u \in \mathcal{O}} \langle v, u^i \rangle \langle w, u^j \rangle = 0$.*

Proof We recall from [5, Theorem 4.7] that $\sum_{u \in \mathcal{O}} u^i = 0$ for each $i \in \mathcal{E}$. The proof follows from the calculation

$$\begin{aligned}\sum_{u \in \mathcal{O}} \left\langle v, u^i \right\rangle \left\langle w, u^j \right\rangle &= \sum_{u \in \mathcal{O}} (vu^{iq} + v^q u^i)(wu^{jq} + w^q u^j) \\ &= \sum_{u \in \mathcal{O}} (vwu^{iq+jq} + v^q wu^{i+jq} + vw^q u^{iq+j} + v^q w^q u^{i+j}) \\ &= vw \sum_{u \in \mathcal{O}} u^{iq+jq} + v^q w \sum_{u \in \mathcal{O}} u^{i+jq} + vw^q \sum_{u \in \mathcal{O}} u^{iq+j} + v^q w^q \sum_{u \in \mathcal{O}} u^{i+j}.\end{aligned}$$

□

Definition 1 A subset L of $\mathcal{E}$ is called *admissible* if $\{l_i + l_j, l_i q + l_j\}_{q^2-1} \subset \mathcal{E}$ whenever $l_i, l_j \in L, l_i \neq l_j$.

Example 3 We describe some examples of admissible sets.

1. If L is an admissible set, then any of its subsets is an admissible set.
2. The set $L_1 = \{2^i \mid 0 \leq i \leq m - 1\}$ is an admissible set.
3. The set $L_2 = \left\{ i(q - 1) \mid 1 \leq i \leq \frac{q}{2} \right\}$ is an admissible set. This follows from the fact that, modulo $q^2 - 1$, nonzero multiples of $(q - 1)$ are of the form $\sum_{j=0}^{m-1} 2^j x_j$, where $x_j \in \{1, q\}$.
4. For $m = 3$, the set $L_3 = \{20, 49\}$ is an admissible set. Furthermore, L_3 cannot be extended to a larger admissible set.

Theorem 4 *Let $\mathcal{O} := \{u_1, \ldots, u_{q+1}\} \subseteq K$ be an oval with nucleus at* 0*. Let $L := \{l_1, \ldots, l_t\}$ be an admissible set of size t. Let $\mathbf{v} := (v_1, \ldots, v_t) \in K^t$, where $v_i \neq 0$ for each i. Let $\mathcal{C}(\mathcal{O}, \mathbf{v}, L)$ be the linear code over $\mathbb{F}_q$ spanned by the vectors*

$$\mathbf{r}_i := (\theta_i(u_1), \theta_i(u_2), \ldots, \theta_i(u_{q+1})),$$

where $1 \leq i \leq t$, and $\theta_i(u_j) = \left\langle v_i, u_j^{l_i} \right\rangle$. Then $\mathcal{C}(\mathcal{O}, \mathbf{v}, L)$ is a Euclidean self-orthogonal code.

Proof By [5, Theorem 4.7], for $1 \leq i \leq t$, we have

$$\sum_{u \in \mathcal{O}} \theta_i(u) = \sum_{u \in \mathcal{O}} \left\langle v_i, u^{l_i} \right\rangle = \sum_{u \in \mathcal{O}} \left(v_i^q u^{l_i} + v_i u^{l_i q} \right) = v_i^q \sum_{u \in \mathcal{O}} u^{l_i} + v_i \sum_{u \in \mathcal{O}} u^{l_i q} = 0,$$

since $l_i \in \mathcal{E}$. This implies $\sum_{u \in \mathcal{O}} \theta_i(u)^2 = 0$. For $1 \leq i, j \leq t, i \neq j$, by Lemma 3,

$$\sum_{u \in \mathcal{O}} \theta_i(u)\theta_j(u) = \sum_{u \in \mathcal{O}} \left\langle v_i, u^{l_i} \right\rangle \left\langle v_j, u^{l_j} \right\rangle = 0.$$

It follows that $\mathcal{C}(\mathcal{O}, \mathbf{v}, L)$ is a Euclidean self-orthogonal code. □

Remark 6 We note that using the set L_2, we obtain linear codes equivalent to codes constructed in Theorem 3.

Example 4 Let $m = 3$ and recall the set $L_3 = \{20, 49\}$ from Example 3. Let $S = \langle w \rangle$ be the unit circle and let $\mathbf{v} = \{1, w^8\}$. Then the code $C = \mathcal{C}(S, \mathbf{v}, L_3)$ is a $[9, 2, 7]$-code. The dual of C has parameters $[9, 7, 2]$ and so C is a near-MDS code.

Let $S = \{w_1, \ldots, w_{q+1}\}$ be the unit circle. We recall from [12] that if k is odd, then the code

$$C_1 = \left\{ (h(w_1) + h(w_1)^q, \ldots, h(w_{q+1}) + h(w_{q+1})^q \mid h \in K[X], \deg h \leq \frac{1}{2}(k-1) \right\}$$

is a $[q + 1, k, q + 2 - k]$ generalized Reed-Solomon code over $\mathbb{F}_q$.

Let $l = \frac{1}{2}(k - 1)$. Since $k \leq q + 1$, we have $l \leq \frac{q}{2}$.

Lemma 4 *The matrix*

$$G_1 = \begin{bmatrix} \langle 1, w_1 \rangle & \langle 1, w_2 \rangle & \ldots & \left\langle 1, w_{q+1} \right\rangle \\ \langle \mathbf{i}, w_1 \rangle & \langle \mathbf{i}, w_2 \rangle & \ldots & \left\langle \mathbf{i}, w_{q+1} \right\rangle \\ \left\langle 1, w_1^2 \right\rangle & \left\langle 1, w_2^2 \right\rangle & \ldots & \left\langle 1, w_{q+1}^2 \right\rangle \\ \left\langle \mathbf{i}, w_1^2 \right\rangle & \left\langle \mathbf{i}, w_2^2 \right\rangle & \ldots & \left\langle \mathbf{i}, w_{q+1}^2 \right\rangle \\ \ldots & \ldots & \ldots & \ldots \\ \left\langle 1, w_1^l \right\rangle & \left\langle 1, w_2^l \right\rangle & \ldots & \left\langle 1, w_{q+1}^l \right\rangle \\ \left\langle \mathbf{i}, w_1^l \right\rangle & \left\langle \mathbf{i}, w_2^l \right\rangle & \ldots & \left\langle \mathbf{i}, w_{q+1}^l \right\rangle \\ 1 & 1 & \ldots & 1 \end{bmatrix}$$

is a generator matrix of C_1.

Proof Let

$$h(X) = h_0 + h_1 X + \cdots h_l X^l.$$

For each $0 \leq i \leq l$, let

$$h_i = x_i + y_i \mathbf{i}^q.$$

For each $w \in S$, we have

$$\begin{aligned} h(w) + h(w)^q = \langle 1, h(w) \rangle = \sum_{i=0}^{l} \left\langle 1, h_i w^i \right\rangle &= \sum_{i=0}^{l} \left\langle 1, x_i w^i + y_i \mathbf{i}^q w^i \right\rangle \\ &= (h_0 + h_0^q) + \sum_{i=1}^{l} \left\langle 1, x_i w^i \right\rangle + \sum_{i=1}^{l} \left\langle 1, y_i \mathbf{i}^q w^i \right\rangle \\ &= (h_0 + h_0^q) + \sum_{i=1}^{l} x_i \left\langle 1, w^i \right\rangle + \sum_{i=1}^{l} y_i \left\langle \mathbf{i}, w^i \right\rangle, \end{aligned}$$

which shows that each codeword in C_1 is a linear combination of rows of the matrix G_1. □

Let $\mathcal{C} = \mathcal{C}(S, \mathbf{v}, L)$ be the linear code over $\mathbb{F}_q$ defined in Theorem 3, which is a special case of Theorem 4. Let

$$\bar{l} := \max_{1 \le i \le t} l_i .$$

Theorem 5 *If $\bar{l} \le q/2$, then $\mathcal{C}$ is a Euclidean self-orthogonal subcode of a $[q+1, 2\bar{l}+1, q+1-2\bar{l}]_q$ generalized Reed-Solomon code.*

Proof For each $1 \le i \le t$, let $x_i, y_i \in F$ be such that $v_i = x_i + y_i\mathbf{i}$. Then the vector

$$\mathbf{r}_i = (\theta_i(w_1), \theta_i(w_2), \ldots, \theta_i(w_{q+1})),$$

is a linear combination of $(2l_i - 1)$-th row and $(2l_i)$-th row of the matrix G_1 in Lemma 4. The proof now follows. □

Remark 7 For q even, Theorem 5 shows that generalized Reed-Solomon codes with odd dimension contain Euclidean self-orthogonal subcodes. To our knowledge, this was not considered before in the literature. For q odd, some Euclidean self-orthogonal codes contained in generalized Reed-Solomon codes are described in [24].

4.3 Quantum codes from self-orthogonal codes

It is well known that quantum codes can be constructed from self-orthogonal linear codes. We recall from [35] (also [30, p. 667]) the following result.

Theorem 6 *Let q be a prime power and let C_1 be a q-ary $[n, k_1, d_1]$-linear code which contains its Euclidean dual $C_1^{\perp}$. Suppose C_1 can be enlarged to an $[n, k_2, d_2]$-linear code C_2 with $k_2 > k_1 + 1$, i.e. $C_1 \subseteq C_2$. Then a pure q-ary quantum code of parameters $[[n, k_1 + k_2 - n, \min\{d_1, \lceil (1 + 1/q)d_2 \rceil\}]]$ can be constructed.*

Example 5 Let $m = 3$ so that $q = 8$. Let $\mathbf{v} = (v_1, v_2, v_3, v_4) \in S^4$ and $L = \{1, 2, 3, 4\}$. Let

$$G = \begin{bmatrix} \langle v_1, 1 \rangle & \langle v_1, w \rangle & \ldots & \langle v_1, w^8 \rangle \\ \langle v_2, 1 \rangle & \langle v_2, w^2 \rangle & \ldots & \langle v_2, w^{16} \rangle \\ \langle v_3, 1 \rangle & \langle v_3, w^3 \rangle & \ldots & \langle v_3, w^{24} \rangle \\ \langle v_4, 1 \rangle & \langle v_4, w^4 \rangle & \ldots & \langle v_4, w^{32} \rangle \end{bmatrix}.$$

Let C be the linear code over $\mathbb{F}_8$ with generator matrix G. Denote the i-th row of G by $\mathbf{r}_i$. Let D be the subspace of C generated by a subset $\mathbf{d}$ of the rows of G. We have the following diagram of containment:

$$\begin{array}{ccc} C & \supset & D \\ \cap & & \cap \\ C^{\perp} & \subset & D^{\perp} \end{array}$$

Let $C_1 = C^{\perp}$ and $C_2 = D^{\perp}$. Using Theorem 6, we obtain some quantum codes over $\mathbb{F}_8$ in Table 1. We also include codes from [27] over $\mathbb{F}_4$ for comparison.

Table 1 Quantum codes over $\mathbb{F}_8$ of length 9

d	**v**	Parameters	[27]
$\{\mathbf{r}_3\}$	$[1, w, w^2, w]$	$[[9, 4, 3]]_8$	$[[9, 4, 2]]_4$
$\{\mathbf{r}_1, \mathbf{r}_2\}$	$[1, w, w^8, 1]$	$[[9, 3, 3]]_8$	$[[9, 3, 3]]_4$

Table 2 Quantum codes over $\mathbb{F}_8$ of length 10

d	**v**	Parameters	[27]
$\{\mathbf{r}_5\}$	$[1, w, w, w^5]$	$[[10, 4, 3]]_8$	$[[10, 4, 3]]_4$
$\{\mathbf{r}_1, \mathbf{r}_5\}$	$[1, w, w^4, w]$	$[[10, 3, 3]]_8$	$[[10, 3, 3]]_4$
$\{\mathbf{r}_2, \mathbf{r}_4, \mathbf{r}_5\}$	$[1, w, w^3, w^3]$	$[[10, 2, 4]]_8$	$[[10, 2, 4]]_4$

Table 3 Quantum codes over $\mathbb{F}_{16}$ of length 17

d	**v**	Parameters	[27]
$\{\mathbf{r}_2, \mathbf{r}_3, \mathbf{r}_4, \mathbf{r}_5, \mathbf{r}_7, \mathbf{r}_8\}$	$[1, w, w^8, w^7, w^{15}, w^{15}, w^3, w^{10}]$	$[[17, 3, 6]]_{16}$	$[[17, 3, 5-6]]_4$
$\{\mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3, \mathbf{r}_5, \mathbf{r}_6\}$	$[1, w, w^7, w^9, 1, w^{13}, w, w^4]$	$[[17, 4, 5]]_{16}$	$[[17, 4, 5]]_4$
$\{\mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3, \mathbf{r}_7\}$	$[1, w, w^5, w^2, w^3, w^{10}, w^{13}, w^3]$	$[[17, 5, 4]]_{16}$	$[[17, 5, 4-5]]_4$
$\{\mathbf{r}_1, \mathbf{r}_4, \mathbf{r}_5\}$	$[1, w, w^{15}, w^{11}, w^2, w^7, w^8, w^7]$	$[[17, 6, 3]]_{16}$	$[[17, 6, 4-5]]_4$

Example 6 Recall from Example 2 the linear code C over $\mathbb{F}_8$ with generator matrix

$$G = \begin{bmatrix} \langle v_1, 1\rangle & \langle v_1, w\rangle & \dots & \langle v_1, w^8\rangle & 0 \\ \langle v_2, 1\rangle & \langle v_2, w^2\rangle & \dots & \langle v_2, w^{16}\rangle & 0 \\ \langle v_3, 1\rangle & \langle v_3, w^3\rangle & \dots & \langle v_3, w^{24}\rangle & 0 \\ \langle v_4, 1\rangle & \langle v_4, w^4\rangle & \dots & \langle v_4, w^{32}\rangle & 0 \\ 1 & 1 & \dots & 1 & 1 \end{bmatrix}.$$

Denote the i-th row of G by $\mathbf{r}_i$. Let D be the subspace of C generated by a subset $\mathbf{d}$ of the rows of G. Let $C_1 = C^\perp$ and $C_2 = D^\perp$. Using Theorem 6, we obtain some quantum codes over $\mathbb{F}_8$, as described in Table 2.

Example 7 Let $m = 4$ so that $q = 16$. Let $S = \langle w\rangle$ be the unit circle. Let $\mathbf{v} = (v_1, v_2, \dots, v_8) \in S^8$ and $L = \{1, 2, \dots, 8\}$. Let

$$G = \begin{bmatrix} \langle v_1, 1\rangle & \langle v_1, w\rangle & \dots & \langle v_1, w^{16}\rangle \\ \langle v_2, 1\rangle & \langle v_2, w^2\rangle & \dots & \langle v_2, w^{32}\rangle \\ \dots & \dots & \dots & \dots \\ \langle v_8, 1\rangle & \langle v_8, w^8\rangle & \dots & \langle v_8, w^{128}\rangle \end{bmatrix}.$$

Let C be the linear code over $\mathbb{F}_{16}$ with generator matrix G. Denote the i-th row of G by $\mathbf{r}_i$. Let D be the subspace of C generated by a subset $\mathbf{d}$ of the rows of G. Let $C_1 = C^\perp$ and $C_2 = D^\perp$. Using Theorem 6, we obtain some quantum codes of length 17 over $\mathbb{F}_{16}$, as described in Table 3.

Example 8 Let $m = 4$ so that $q = 16$. Let $S = \langle w\rangle$ be the unit circle. Let $\mathbf{v} = (v_1, v_2, \dots, v_8) \in S^8$ and $L = \{1, 2, \dots, 8\}$. Let

Table 4 Quantum codes over $\mathbb{F}_{16}$ of length 18

$\mathbf{d}$	$\mathbf{v}$	Parameters	[27]
$\{\mathbf{r}_1, \mathbf{r}_3, \mathbf{r}_5, \mathbf{r}_6, \mathbf{r}_8, \mathbf{r}_9\}$	$[1, w, w^3, w^3, w^9, w^6, w^8, w^9]$	$[[18, 3, 6]]_{16}$	$[[18, 3, 5-6]]_4$
$\{\mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_5, \mathbf{r}_7, \mathbf{r}_9\}$	$[1, w, w^8, w^5, w^5, w^{10}, w^{10}, w^{14}]$	$[[18, 4, 5]]_{16}$	$[[18, 4, 5-6]]_4$
$\{\mathbf{r}_2, \mathbf{r}_5, \mathbf{r}_6, \mathbf{r}_9\}$	$[1, w, 1, w^6, w^4, w^{14}, w^8, w^{14}]$	$[[18, 5, 4]]_{16}$	$[[18, 5, 5]]_4$
$\{\mathbf{r}_4, \mathbf{r}_5, \mathbf{r}_9\}$	$[1, w, w^2, w^7, w^6, w^{13}, w, w^9]$	$[[18, 6, 4]]_{16}$	$[[18, 6, 5]]_4$

$$G = \begin{bmatrix} \langle v_1, 1\rangle & \langle v_1, w\rangle & \dots & \left\langle v_1, w^{16}\right\rangle & 0 \\ \langle v_2, 1\rangle & \left\langle v_2, w^2\right\rangle & \dots & \left\langle v_2, w^{32}\right\rangle & 0 \\ \dots & \dots & \dots & \dots & \dots \\ \langle v_8, 1\rangle & \left\langle v_8, w^8\right\rangle & \dots & \left\langle v_8, w^{128}\right\rangle & 0 \\ 1 & 1 & \dots & 1 & 1 \end{bmatrix}.$$

Let C be the linear code over $\mathbb{F}_{16}$ with generator matrix G. Denote the i-th row of G by $\mathbf{r}_i$. Let D be the subspace of C generated by a subset $\mathbf{d}$ of the rows of G. Let $C_1 = C^\perp$ and $C_2 = D^\perp$. Using Theorem 6, we obtain some quantum codes of length 18 over $\mathbb{F}_{16}$, as described in Table 4.

Remark 8 In Examples 5, 6, 7 and 8, the choices for $\mathbf{d}$ and the coordinates of $\mathbf{v}$ (excluding the first two coordinates) are random. In Tables 1, 2, 3 and 4, we only included random choices that produce quantum codes with highest distance within our GAP calculations. We also note that different choices of $\mathbf{d}$ and $\mathbf{v}$ can result in codes with same parameters.

Remark 9 In general, there are no databases for quantum codes over $\mathbb{F}_q$ for $q > 4$. The quantum codes over $\mathbb{F}_8$ and $\mathbb{F}_{16}$ we obtained in Examples 5, 6, 7 and 8 are new, to our knowledge.

5 Linear codes from KM-arcs

5.1 Three-weight codes from KM-arcs

We recall that in the projective plane $PG(2, q)$, where q is even, a *KM-arc of type t* is a set H of $q + t$ points meeting every line in 0, 2 or t points. If H is a KM-arc of type t in $PG(2, q)$, $2 < t < q$, then

1. q is even and t is a divisor of q, cp. [32];
2. each point of H is on exactly one t-secant and every other line through this point is a 2-secant of H, cp. [32];
3. there are $q/t + 1$ different t-secants to H, and they are concurrent at a unique point called the *t-nucleus* of H, cp. [26];
4. all other lines contain 0 or 2 points of H, cp. [32].

We further note that, by direct counting, the number of 2-secants and 0-secants are $\frac{q(q+t)}{2}$ and $q - \frac{q}{t} + \frac{q(q-t)}{2}$, respectively.

Let $n := q + t$. Let $H := \{u_1, \dots, u_n\}$ be a KM-arc of type t with points in K and nucleus at 0. For each i, we rewrite $u_i = x_i + y_i\mathbf{i}$. Let C be an $[n, 3]$-code over $\mathbb{F}_q$ with generator matrix

$$G = \begin{bmatrix} x_1 & x_2 & \dots & x_n \\ y_1 & y_2 & \dots & y_n \\ 1 & 1 & \dots & 1 \end{bmatrix}.$$

We will assume $t > 2$, since the case $t = 2$ (corresponding to hyperovals) was considered in [20]. In the next theorem, we study the weight enumerator and the minimum distance of of $C^{\perp}$.

Theorem 7 *Let $t > 2$. Then C is a three-weight $[n, 3, q]$-code over $\mathbb{F}_q$ with weight enumerator*

$$A(z) = 1 + A_{n-t}z^{n-t} + A_{n-2}z^{n-2} + A_n z^n,$$

where

$$A_{n-t} = (q-1)\left(\frac{q}{t} + 1\right),$$

$$A_{n-2} = (q-1)\frac{q(q+t)}{2},$$

and

$$A_n = (q-1)\left(q - \frac{q}{t} + \frac{q(q-t)}{2}\right).$$

The minimum distance of $C^{\perp}$ is 3.

Proof By [20, Theorem 2.36] (also compare [20, Section 12.2]), the only possible weights of C is $n, n-2, n-t$. Let the weight enumerator of C be

$$A(z) = 1 + A_{n-t}z^{n-t} + A_{n-2}z^{n-2} + A_n z^n.$$

For convenience, we denote A_{n-t}, A_{n-2}, A_n by X, Y, Z, respectively. We note that C is a projective code, that is, the minimum distance of $C^{\perp}$ is greater than 2 (cp. [20, p. 85]). The first three Pless power moments of C (compare [20, Section 2.3], [31, Section 7.3]) give the following system of equations

$$\begin{cases} 1 + X + Y + Z = q^3 \\ (n-t)X + (n-2)Y + nZ = q^2(q-1)n \\ (n-t)^2X + (n-2)^2Y + n^2Z = q(q-1)n(qn-n+1) \end{cases}$$

Solving the system gives us the weight enumerator of C.

We now consider the weight enumerator $A^{\perp}(z)$ of the dual $C^{\perp}$, which is a $[q+t, q+t-3]$-code. From the MacWilliams Identity,

$$\begin{aligned} q^3A^{\perp}(z) &= (1+(q-1)z)^n A\left(\frac{1-z}{1+(q-1)z}\right) \\ &= (1+(q-1)z)^n \left(1 + X\frac{(1-z)^q}{(1+(q-1)z)^q} + Y\frac{(1-z)^{n-2}}{(1+(q-1)z)^{n-2}}\right. \\ &\quad \left. + Z\frac{(1-z)^n}{(1+(q-1)z)^n}\right) \\ &= (1+(q-1)z)^n + X(1-z)^q(1+(q-1)z)^t \\ &\quad + Y(1-z)^{n-2}(1+(q-1)z)^2 + Z(1-z)^n. \end{aligned}$$

We have

$$(1+(q-1)z)^n = \sum_{i=0}^{n} \binom{n}{i} (q-1)^i z^i,$$
$$Z(1-z)^n = \sum_{i=0}^{n} \binom{n}{i} Z(-z)^i.$$

Also, following the calculations in [20, p. 316, 317], we have

$$X(1-z)^q(1+(q-1)z)^t = \sum_{l=0}^{n} \left(\sum_{i+j=l} \binom{q}{i}\binom{t}{j}(-1)^i(q-1)^j \right) Xz^l,$$
$$Y(1-z)^{n-2}(1+(q-1)z)^2 = \sum_{l=0}^{n} \left(\sum_{i+j=l} \binom{n-2}{i}\binom{2}{j}(-1)^i(q-1)^j \right) Yz^l.$$

It follows that

$$\begin{aligned} q^3A_1^{\perp} &= n(q-1) + (t(q-1)-q)X + (2(q-1)-(n-2))Y - nZ \\ &= 0, \\ q^3A_2^{\perp} &= \binom{n}{2}(q-1)^2 + \left(\binom{t}{2}(q-1)^2 - qt(q-1) + \binom{q}{2}\right) X \\ &\quad + \left((q-1)^2 - (n-2)2(q-1) + \binom{n-2}{2}\right) Y + \binom{n}{2} Z \\ &= 0, \\ q^3A_3^{\perp} &= \binom{n}{3}(q-1)^3 + \left(\binom{t}{3}(q-1)^3 - q\binom{t}{2}(q-1)^2 + \binom{q}{2}t(q-1) - \binom{q}{3}\right) X \\ &\quad + \left(0 - \binom{n-2}{1}(q-1)^2 + \binom{n-2}{2}2(q-1) - \binom{n-2}{3}\right) Y - \binom{n}{3} Z. \end{aligned}$$

Then

$$\begin{aligned} 6q^3A_3^{\perp} &= q^5t^2 + q^4t^3 - 3q^5t - 4q^4t^2 - q^3t^3 + 2q^5 + 5q^4t + 3q^3t^2 - 2q^4 - 2q^3t \\ &= q^3(q-1)(q+t)(t-1)(t-2). \end{aligned}$$

Since $t > 2$, we have $A_3^{\perp} > 0$ and so the minimum distance of $C^{\perp}$ is 3. □

Remark 10 From [20, Theorem 2.36], alternatively one can easily see that the numbers A_{n-t}, A_{n-2}, A_n are $(q-1)$ times the number of t-secants, 2-secants and 0-secants to a KM-arc. We thank one of the reviewers for pointing this out.

Remark 11 When $t = 2$, calculations for the weight enumerator in Theorem 7 still hold. In this case, C is a two-weight code with weight enumerator

$$1 + (q-1)\frac{(q+2)(q+1)}{2} z^q + (q-1)\frac{q(q-1)}{2} z^{q+2}.$$

We have $A_3^{\perp} = 0$ and by the Singleton bound, the minimum distance of $C^{\perp}$ is 4.

Remark 12 The case $q = 8, t = 4$ produces a linear code C over $\mathbb{F}_8$ with parameters $[12, 3, 8]$. This code is almost optimal according to [27]. The dual $C^{\perp}$ has parameters $[12, 9, 3]$ which is almost-MDS.

5.2 Four-weight LCD codes from KM-arcs

Recall $q = 2^m$, $F = \mathbb{F}_q$, $K = \mathbb{F}_{q^2}$. Let $r = 2^h$, where $h \mid m$. Let $F' = \mathbb{F}_r$, and $K' = \mathbb{F}_{r^2}$. We recall the relative trace map $Tr_{F/F'} : F \to F'$, where

$$Tr_{F/F'}(x) = x^{q/r} + x^{q/r^2} + \cdots + x^r + x.$$

Let $V_1 := \{x \in F \mid Tr_{F/F'}(x) = 1\}$.

We recall from [7, Theorem 4] a construction of KM-arcs in polar coordinates, which is equivalent to the construction of Gács and Weiner [26]. Assume m/h is odd. Let $H' \subset K'$ be an oval with nucleus at 0. Let $V_c := cV_1$ for some $c \in K^*$. Then $H := \{\lambda u \mid 1/\lambda \in V_c, u \in H'\}$ is a KM-arc in K of type $t = q/r$ with t-nucleus at 0.

Let $n := q + t$ and let the elements of H be v_i, where $1 \le i \le n$. For each i, let $v_i = x_i + y_i\mathbf{i}$. We can apply Theorem 1 to obtain LCD codes over $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$ from the set H as follows.

Theorem 8 *Let $\alpha \in \mathbb{F}_q^*$. Let $C = C_\alpha(H)$ be a linear code over $\mathbb{F}_q$ with generator matrix*

$$G = \begin{bmatrix} x_1 & x_2 & \dots & x_n & 0 \\ y_1 & y_2 & \dots & y_n & 0 \\ 1 & 1 & \dots & 1 & \alpha \end{bmatrix}.$$

Then C is a four-weight Euclidean LCD $[n+1, 3, q]$-code. The weight enumerator of C is

$$A(z) = 1 + A_{n-t}z^{n-t} + A_{n-1}z^{n-1} + A_n z^n + A_{n+1}z^{n+1}$$

where

$$A_{n-t} = (q-1)\left(\frac{q}{t} + 1\right),$$
$$A_{n-1} = (q-1)\frac{q(q+t)}{2},$$
$$A_n = (q-1)\left(q - \frac{q}{t}\right),$$

and

$$A_{n+1} = (q-1)\frac{q(q-t)}{2}.$$

Proof 1. Since H' is an oval, it is a Vandermonde set, and so $\sum_{i=1}^{n} v_i = 0$. In view of Theorem 1, to prove that C is a Euclidean LCD code it is sufficient to prove that $\sum_{i=1}^{n} v_i^{q+1} \neq 0$. We have

$$\sum_{i=1}^{n} v_i^{q+1} = \sum_{1/\lambda \in V_c} \lambda^2 \sum_{u \in H'} u^{q+1}.$$

We first show that $\sum_{1/\lambda \in V_c} \lambda^2 \neq 0$, by showing that $\sum_{\lambda \in V_1} \lambda^{q-2} \neq 0$. For $\lambda \in V_1$, we have

$$Tr_{F/F'}(\lambda) = \lambda^{q/r} + \lambda^{q/r^2} + \cdots + \lambda^r + \lambda = 1.$$

Rewrite

$$\sum_{\lambda\in V_1}\lambda^{q-2}=\sum_{\lambda\in V_1}\lambda^{\frac{q}{r}-2}\lambda^{\frac{q}{r}(r-1)}=\sum_{\lambda\in V_1}\lambda^{\frac{q}{r}-2}\left(\lambda^{q/r^2}+\cdots+\lambda+1\right)^{r-1}.$$

We note that $r=2^h$ so that $r-1=\sum\limits_{i=0}^{h-1}2^i$. Then

$$A=\lambda^{\frac{q}{r}-2}\left(\lambda^{q/r^2}+\cdots+\lambda+1\right)^{r-1}=\lambda^{\frac{q}{r}-2}\prod_{i=0}^{h-1}\left(\lambda^{q/r^2}+\cdots+\lambda+1\right)^{2^i}.$$

Let λ^d be a term in the expansion of A. Then

$$0\le d\le 2\frac{q}{r}-\frac{q}{r^2}-2.$$

From parts 1 and 2 of the proof of [7, Lemma 7], for d in this range, $\sum\limits_{\lambda\in V_1}\lambda^d\neq 0$ if and only if $d=q/r-1$. Since the term $\lambda^{q/r-1}$ appears in the expansion of A, it follows that $\sum\limits_{\lambda\in V_1}\lambda^{q-2}\neq 0$. Then

$$\sum_{1/\lambda\in V_c}\lambda^2=\sum_{\lambda\in V_1}\frac{1}{c^2\lambda^2}=\frac{1}{c^2}\sum_{\lambda\in V_1}\lambda^{q-2}\neq 0.$$

On the other hand, since H' is an oval, $\sum_{u\in H'}u^{r+1}\neq 0$. For $u\in H'\subset K'$, we have $u^{r^2}=u$, and since m/h is odd,

$$u^{q+1}=u^{r^{m/h}+1}=u^{r+1}.$$

Then

$$\sum_{u\in H'}u^{q+1}=\sum_{u\in H'}u^{r+1}\neq 0.$$

By Theorem 1, it follows that C is a Euclidean LCD code.

2. Let $\bar{H}$ be the set of points in $PG(2,q)$ with homogeneous coordinates given by the columns of G. Then $\bar{H}=H\cup\{(0:0:1)\}$. Since H is a KM-arc of type t, every line in $PG(2,q)$ intersects $\bar{H}$ at 0, 1, 2 or $t+1$ points. By [20, Theorem 2.36], the only possible weights of C are $n+1, n, n-1, n-t$ and so C is a four-weight code.

Let $\mathbf{c}$ be a codeword of C. Then

$$\mathbf{c}=[b_1\ b_2\ b_3]G,$$

where $b_1,b_2,b_3\in\mathbb{F}_q$. We observe that the i-th coordinate of $\mathbf{c}$ is zero if and only if the point $(x_i:y_i:1)$ is on the line L determined by the equation $b_1x+b_2y+b_3=0$. In particular, for $l\in\{0,1,2,t+1\}$, the codeword $\mathbf{c}$ has weight $n+1-l$ if and only if the line L contains l points of $\bar{H}$. On the other hand, triples (b_1,b_2,b_3) and $(\lambda b_1,\lambda b_2,\lambda b_3)$ with $\lambda\in\mathbb{F}_q^*$ determine the same line. It follows that the number of codewords of C with weight $n+1-l$ is equal to $(q-1)$ times the number of l-secants to $\bar{H}$.

We note that the number of $(t+1)$-secants, 2-secants, 1-secants and 0-secants to $\bar{H}$ are $\frac{q}{t}+1$, $\frac{q(q+t)}{2}$, $q-\frac{q}{t}$ and $\frac{q(q-t)}{2}$, respectively. The weight enumerator of C now follows from counting the l-secants to $\bar{H}$. □

Theorem 9 *Let $\alpha \in \mathbb{F}_{q^2}^*$. Let $C = C_\alpha(H)$ be a linear code over $\mathbb{F}_{q^2}$ with generator matrix*

$$G = \begin{bmatrix} x_1 & x_2 & \dots & x_n & 0 \\ y_1 & y_2 & \dots & y_n & 0 \\ 1 & 1 & \dots & 1 & \alpha \end{bmatrix}.$$

Then C is a four-weight Hermitian LCD $[n+1, 3, q]$-code. The weight enumerator of C is

$$A(z) := 1 + A_{n-t}z^{n-t} + A_{n-1}z^{n-1} + A_n z^n + A_{n+1}z^{n+1}$$

where

$$\begin{aligned} A_{n-t} &= (q^2-1)\left(\frac{q}{t}+1\right), \\ A_{n-1} &= (q^2-1)\frac{q(q+t)}{2}, \\ A_n &= (q^2-1)\left(q^2 - \frac{q}{t} + (q^2-q)(q+t)\right), \end{aligned}$$

and

$$A_{n+1} = (q^2-1)\left(q^4 - (q+t)\left(q^2 - \frac{q}{2}\right)\right).$$

Proof Similar to part 1 in the proof of Theorem 8, it can be shown that C is a Hermitian LCD code. In the remainder of the proof, we show that C is a four-weight code and calculate the weight enumerator of C.

Let $\bar{H}$ be the set of points in $PG(2, q^2)$ with homogeneous coordinates given by the columns of G. We note that the homogeneous coordinates of points from $\bar{H}$ can be chosen from $\mathbb{F}_q$. Since H is a KM-arc of type t in $PG(2, q)$, every line in $PG(2, q^2)$ intersects $\bar{H}$ at $0, 1, 2$ or $t+1$ points. By [20, Theorem 2.36], the only possible weights of C are $n+1, n, n-1, n-t$ and so C is a four-weight code.

We now consider the number of l-secants to $\bar{H}$ in $PG(2, q^2)$, for $l \in \{0, 1, 2, t+1\}$. Since two points of $\bar{H}$ determine a unique line in $PG(2, q^2)$ (which is lifted from a line in $PG(2, q)$), the number of $(t+1)$-secants to $\bar{H}$ is equal to the number of t-secants to $H \subset PG(2, q)$, which is $\frac{q}{t} + 1$. Also, the number of 2-secants to $\bar{H}$ is $\frac{q(q+t)}{2}$.

For each point P of $\bar{H} \backslash \{(0:0:1)\}$, there are $q^2 - q$ lines intersecting $\bar{H}$ at only P. Also, there are $q^2 - q/t$ lines intersects $\bar{H}$ at only $(0:0:1)$. Hence, the total number of 1-secants to $\bar{H}$ is

$$q^2 - \frac{q}{t} + (q^2 - q)(q+t).$$

It follows that the number of 0-secants to $\bar{H}$ is

$$q^4 - (q+t)(q^2 - \frac{q}{2}).$$

Similar to part 2 in the proof of Theorem 8, for $l \in \{0, 1, 2, t+1\}$, the number of codewords of C with weight $n+1-l$ is equal to (q^2-1) times the number of l-secants to $\bar{H}$. The weight enumerator of C now follows. □

Acknowledgements The authors would like to thank the anonymous reviewers for their detailed comments, especially for pointing out the connection between the secants to a KM-arc and the weight enumerator of the linear code in Theorem 7. This allowed us to extend Theorems 8 and 9 in the revised version.
This work was supported by UAEU grant G00003490.

Declarations

Data Deposition Information Not applicable.

References

1. Abdukhalikov K.: Bent functions and line ovals. Finite Fields Appl. **47**, 94–124 (2017).
2. Abdukhalikov K.: Hyperovals and bent functions. Eur. J. Comb. **79**, 123–139 (2019).
3. Abdukhalikov K.: Short description of the Lunelli-Sce hyperoval and its automorphism group. J. Geom. **110**, Paper No. 54, 8 (2019).
4. Abdukhalikov K.: Equivalence classes of Niho bent functions. Des. Codes Cryptogr. **89**, 1509–1534 (2021).
5. Abdukhalikov K., Ho D.: Vandermonde sets, hyperovals and Niho bent functions. Adv. Math. Commun. https://doi.org/10.3934/amc.2021048.
6. Abdukhalikov K., Ho D.: Extended cyclic codes, maximal arcs and ovoids. Des. Codes Cryptogr. **89**, 2283–2294 (2021).
7. Abdukhalikov K., Ho D.: Polar coordinates view on KM-arcs. Gr. Comb. **37**, 1467–1490 (2021).
8. Anderson R., Ding C., Helleseth T., Kløve T.: How to build robust shared control systems. Des. Codes Cryptogr. **15**, 111–124 (1998).
9. Baart R., Boothby T., Cramwinckel J., Fields J., Joyner D., Miller R., Minkes E., Roijackers E., Ruscio L., Tjhai C.: GUAVA: a GAP package, version 3.17, 05/09/2022.
10. Ball S.: Polynomials in Finite Geometries. Surveys In Combinatorics, 1999 (Canterbury). **267** pp. 17-35 (1999).
11. Ball S.: Some constructions of quantum MDS codes. Des. Codes Cryptogr. **89**, 811–821 (2021).
12. Ball S.: The Grassl-Rötteler cyclic and consta-cyclic MDS codes are generalised Reed-Solomon codes. arXiv:org/abs/2112.11896.
13. Ball S., Vilar R.: The geometry of Hermitian self-orthogonal codes. J. Geom. **113**(1), Paper No. 7, 12 pp. (2022).
14. Ball S., Centelles A., Huber F.: Quantum error-correcting codes and their geometries. Ann. Inst. Henri Poincare Comb. Phys. Interact. To appear. arXiv:2007.05992.
15. Blokhuis A., Marino G., Mazzocca F., Polverino O.: On almost small and almost large super-Vandermonde sets in GF(q). Des. Codes Cryptogr. **84**, 197–201 (2017).
16. Carlet C., Ding C., Yuan J.: Linear codes from perfect nonlinear mappings and their secret sharing schemes. IEEE Trans. Inform. Theory. **51**, 2089–2102 (2005).
17. Carlet C., Guilley S.: Complementary dual codes for counter-measures to side-channel attacks. Adv. Math. Commun. **10**, 131–150 (2016).
18. Carlet C., Mesnager S., Tang C., Qi Y.: Euclidean and Hermitian LCD MDS codes. Des. Codes Cryptogr. **86**, 2605–2618 (2018).
19. De Boeck M., Van de Voorde G.: A linear set view on KM-arcs. J. Algebr. Comb. **44**, 131–164 (2016).
20. Ding C.: Designs from Linear Codes. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ (2019).
21. Ding C., Helleseth T., Kløve T., Wang X.: A generic construction of Cartesian authentication codes. IEEE Trans. Inform. Theory **53**, 2229–2235 (2007).
22. Ding C., Heng Z.: The subfield codes of ovoid codes. IEEE Trans. Inform. Theory **65**, 4715–4729 (2019).
23. Ding C., Wang X.: A coding theory construction of new systematic authentication codes. Theor. Comput. Sci. **330**, 81–99 (2005).
24. Fang X., Liu M., Luo J.: New MDS Euclidean self-orthogonal codes. IEEE Trans. Inform. Theory. **67**, 130–137 (2021).
25. Fisher J., Schmidt B.: Finite Fourier series and ovals in PG$(2, 2^h)$. J. Aust. Math. Soc. **81**, 21–34 (2006).
26. Gács A., Weiner Z.: On $(q + t, t)$-arcs of type $(0, 2, t)$. Des. Codes Cryptogr. **29**, 131–139 (2003).
27. Grassl M.: Bounds on the minimum distance of linear codes and quantum codes. http://www.codetables.de.
28. Grassl M., Gulliver T.A.: On circulant self-dual codes over small fields. Des. Codes Cryptogr. **52**, 57–81 (2009).
29. Heng Z., Ding C.: The subfield codes of hyperoval and conic codes. Finite Fields Appl. **56**, 308–331 (2019).
30. Huffman W., Kim J., Solé P.: Concise Encyclopedia of Coding Theory. CRC Press, Taylor and Francis Group, London, New York (2021).

31. Huffman W., Pless V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003).
32. Korchmáros G., Mazzocca F.: On $(q+t)$-arcs of type $(0, 2, t)$ in a Desarguesian plane of order q. Math. Proc. Camb. Philos. Soc. **108**, 445–459 (1990).
33. Li C., Ding C., Li S.: LCD cyclic codes over finite fields. IEEE Trans. Inform. Theory **63**, 4344–4356 (2017).
34. Lidl R., Niederreiter H.: Finite Fields. Encyclopedia of Mathematics and its Applications, vol. 20, 2nd edn Cambridge University Press, Cambridge (1997).
35. Ling S., Luo J., Xing C.: Generalization of Steane's enlargement construction of quantum codes and applications. IEEE Trans. Inform. Theory. **56**, 4080–4084 (2010).
36. Massey J.L.: Linear codes with complementary duals. Discret. Math. **106**, 337–342 (1992).
37. Shi M., Sok L., Solé P., Çalkavur S.: Self-dual codes and orthogonal matrices over large finite fields. Finite Fields Appl. **54**, 297–314 (2018).
38. Sok L., Shi M., Solé P.: Constructions of optimal LCD codes over large finite fields. Finite Fields Appl. **50**, 138–153 (2018).
39. Sziklai P., Takáts M.: Vandermonde sets and super-Vandermonde sets. Finite Fields Appl. **14**, 1056–1067 (2008).
40. The GAP Group: GAP: Groups, Algorithms, and Programming, Version 4.12.2; 2022. https://www.gap-system.org.
41. Vandendriessche P.: Codes of Desarguesian projective planes of even order, projective triads and (q+t, t)-arcs of type (0,2, t). Finite Fields Appl. **17**, 521–531 (2011).
42. Vandendriessche P.: On KM-arcs in small Desarguesian planes. Electron. J. Comb. **24**, Paper 1.51, 11 (2017).
43. Wang Q., Heng Z.: Near MDS codes from oval polynomials. Discret Math.. **344**, Paper No. 112277, 10 (2021).

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.