LINEAR CODES ASSOCIATED WITH THE DESARGUESIAN OVOIDS IN $Q^+(7,q)$

TAO FENG, MICHAEL KIERMAIER, PEIXIAN LIN*, AND KAI-UWE SCHMIDT

ABSTRACT. The Desarguesian ovoids in the orthogonal polar space $Q^+(7,q)$ with q even have first been introduced by Kantor by examining the 8-dimensional absolutely irreducible modular representations of $\mathrm{PGL}(2,q^3)$. We investigate this module for all prime power values of q. The shortest $\mathrm{PGL}(2,q^3)$-orbit O gives the Desarguesian ovoid in $Q^+(7,q)$ for even q and it is known to give a complete partial ovoid of the symplectic polar space $W(7,q)$ for odd q. We determine the hyperplane sections of O. As a corollary, we obtain the parameters $[q^3+1, 8, q^3-q^2-q]_q$ and the weight distribution of the associated $\mathbb{F}_q$-linear code C_O and the parameters $[q^3+1, q^3-7, 5]_q$ of the dual code $C_O^\perp$ for $q \geq 4$. We also show that both codes C_O and $C_O^\perp$ are length-optimal for all prime power values of q.

1. INTRODUCTION

Let q be a prime power and $\mathbb{F}_q$ be the finite field with q elements. An $[n,k]_q$ *code* is a k-dimensional subspace of $\mathbb{F}_q^n$ and an $[n,k,d]_q$ *code* is an $[n,k]_q$ code in which the Hamming weight of every nonzero element of the code is at least d. The *weight distribution* of such a code is the tuple $(A_0, A_1, \ldots, A_n)$, where A_i is the number of codewords in the code with Hamming weight i. The weight distribution of a linear code contains information that is important for error detection and correction [15]. Linear codes with few weights have important applications in cryptography [4, 20], authentication codes [8], and strongly regular graphs [3]. Determining the weight distribution of a linear code is difficult in general and often related to interesting challenging problems in number theory [13].

An ovoid in the orthogonal polar space $Q^+(2n-1, q)$ is a subset of $q^{n-1}+1$ pairwise nonperpendicular points. In the case of $Q^+(7,q)$, Kantor [14] constructed two infinite families ovoids: the *unitary* ovoid for $q \equiv 0, 2 \pmod 3$ with stabilizer $\mathrm{PGU}(3,q)$ and the *Desarguesian* ovoid for even q with stabilizer $\mathrm{PGL}(2,q^3)$. In both cases, the ovoids correspond to the shortest orbit of the respective group action on $\mathrm{PG}(7,q)$. When q is odd, it is shown in [18] that the shortest $\mathrm{PGL}(2,q^3)$-orbit is a complete partial ovoid of the symplectic polar space $W(7,q)$, that is no two of its points are perpendicular and the remaining singular points are perpendicular to at least one of its points.

For a set $O = \{\langle v_1 \rangle, \ldots, \langle v_n \rangle\}$ of n points in $\mathrm{PG}(7,q)$, its associated linear code C has generator matrix whose columns are the vectors $v_1, \ldots, v_n$. Then C is an $[n,k]_q$ code, where $k \leq 8$. It is well known that the weight distribution of C is closely related to the hyperplane sections of O. In [6], the hyperplane sections of the unitary ovoid have been studied, giving the weight distributions of the corresponding linear codes. In this paper,

we study the shortest $\mathrm{PGL}(2, q^3)$-orbit and the associated linear code. We determine the hyperplane sections of the orbit and thus obtain the weight distribution of the associated linear code, which is an $[q^3 + 1, 8, q^3 - q^2 - q]_q$ code. Moreover we show that this code is length-optimal, namely no $[q^3, 8, q^3 - q^2 - q]_q$ code can exist. We note that, in contrast, the codes obtained in [6] have parameters $[q^3 + 1, 8, q^3 - q^2 - 2q]_q$ and q has the restriction $q \equiv -1 \pmod 6$. Also our methods are quite different compared to those in [6].

This paper is organized as follows. In Section 2, we describe the 8-dimensional $\mathbb{F}_q$-module of $\mathrm{PGL}(2, q^3)$. In Section 3, we show that the group $\mathrm{PGL}(2, q^3)$ has four orbits when acting on $\mathrm{PG}(7, q)$ and determine the hyperplane sections with the shortest orbit O. In Section 4, we apply our results to the linear code associated with O and establish length-optimality of this code using linear programming.

2. THE 8-DIMENSIONAL $\mathrm{PGL}(2, q^3)$-MODULE V

Put $V = \mathbb{F}_q \times \mathbb{F}_{q^3} \times \mathbb{F}_{q^3} \times \mathbb{F}_q$. We regard V as an 8-dimensional vector space over $\mathbb{F}_q$ and write its elements in the form (x, y, z, w), where $x, w \in \mathbb{F}_q$ and $y, z \in \mathbb{F}_{q^3}$. For a nonzero vector v of V, we write $\langle v \rangle$ for the projective point that corresponds to v.

Let Tr and N be the trace and norm function from $\mathbb{F}_{q^3}$ to $\mathbb{F}_q$, respectively. We define an alternating form $A : V \times V \to \mathbb{F}_q$ by

$$A\left((x, y, z, w), (x', y', z', w')\right) = xw' - wx' + \mathrm{Tr}(zy' - yz').$$

This form is nondegenerate and confers on $\mathrm{PG}(V)$ the structure of a symplectic polar space $W(7, q)$. We also define a quadratic form $Q : V \to \mathbb{F}_q$ by

$$Q\left((x, y, z, w)\right) = xw + \mathrm{Tr}(yz).$$

This form is also nondegenerate and polarizes to A, that is $A(u, v) = Q(u + v) - Q(u) - Q(v)$. Hence Q confers on $\mathrm{PG}(V)$ the structure of an orthogonal polar space $Q^+(7, q)$.

Define a subset O of $\mathrm{PG}(V)$ by

$$(2.1) \qquad O = \{\langle (1, x, x^{q+q^2}, \mathrm{N}(x)) \rangle : x \in \mathbb{F}_{q^3}\} \cup \{\langle (0, 0, 0, 1) \rangle\}.$$

Then O is a Desarguesian ovoid of $Q^+(7, q)$ if q is even [14] and is a complete partial ovoid of $W(7, q)$ if q is odd [18]. Write $P(x) = \langle (1, x, x^{q+q^2}, \mathrm{N}(x)) \rangle$ for $x \in \mathbb{F}_{q^3}$ and $P(\infty) = \langle (0, 0, 0, 1) \rangle$. This gives a bijection between the points of O and the points of the projective line $\mathrm{PG}(1, q^3)$. It turns out that there is an action of $\mathrm{PGL}(2, q^3)$ on V given by

$$(2.2) \qquad\qquad g : \langle (x, y, z, w) \rangle \mapsto \langle (x', y', z', w') \rangle,$$

where, writing $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$,

$x' = \mathrm{N}(d)x + \mathrm{N}(c)w + \mathrm{Tr}(cd^{q^2+q}y + dc^{q^2+q}z)$,

$y' = bd^{q^2+q}x + ac^{q^2+q}w + ad^{q^2+q}y + bd^{q^2}c^q y^q + bd^q c^{q^2} y^{q^2} + bc^{q^2+q}z + d^q ac^{q^2} z^q + d^{q^2} ac^q z^{q^2}$,

$z' = db^{q^2+q}x + ca^{q^2+q}w + cb^{q^2+q}y + db^{q^2} a^q y^q + db^q a^{q^2} y^{q^2} + da^{q^2+q}z + b^q ca^{q^2} z^q + b^{q^2} ca^q z^{q^2}$,

$w' = \mathrm{N}(b)x + \mathrm{N}(a)w + \mathrm{Tr}(ab^{q^2+q}y + ba^{q^2+q}z)$.

It is routine to check that this action gives an embedding of $\mathrm{PGL}(2, q^3)$ into $\mathrm{GL}(V)$, which preserves the form A and, when q is even, also Q, namely we have $A(g(u), g(v)) = A(u, v)$

for all $u, v \in V$ and, when q is even, $Q(g(v)) = Q(v)$ for all $v \in V$. Moreover, the action is transitive on O and maps $P(x)$ to $P\left(\frac{ax+b}{cx+d}\right)$ for each $x \in \mathbb{F}_{q^3} \cup \{\infty\}$.

3. THE HYPERPLANE SECTIONS OF O

Throughout this section, we use the same notation as in Section 2 and denote $\mathrm{PGL}(2, q^3)$ by G. We frequently use without reference that

$$|G| = q^3(q^3 - 1)(q^3 + 1).$$

In this section, we determine the hyperplane sections of O. Each hyperplane of V can be written as $v^\perp$ for some nonzero vector $v \in V$, where

$$v^\perp = \{\langle x \rangle \in \mathrm{PG}(V) : A(x, v) = 0\}.$$

Since O is G-invariant, $g(v)^\perp \cap O$ and $v^\perp \cap O$ have the same size. Hence, it suffices to determine all G-orbits of $\mathrm{PG}(V)$ and then compute $|v^\perp \cap O|$ for one representative v of each orbit.

Throughout this section, we let α be an element of $\mathbb{F}_q$ such that $x^2 - x - \alpha \in \mathbb{F}_q[x]$ is irreducible. The main result of this section is the following.

Theorem 3.1. *There are exactly four G-orbits of $\mathrm{PG}(V)$ having the following properties (where O denotes O_1)*

orbit	size	representative v	$|v^\perp \cap O|$
O_1	$q^3 + 1$	$\langle(1, 0, 0, 0)\rangle$	1
O_2	$q(q^2 + q + 1)(q^3 + 1)$	$\langle(0, 0, 1, 0)\rangle$	$q^2 + 1$
O_3	$\frac{1}{2}q^3(q^3 + 1)(q - 1)$	$\langle(1, 0, 0, 1)\rangle$	$q^2 + q + 1$
O_4	$\frac{1}{2}q^3(q^3 - 1)(q + 1)$	$\langle(1, 0, \alpha, \alpha)\rangle$	$q^2 - q + 1$

Here is an outline of our strategy to prove Theorem 3.1. First it is routine to check that

$$(3.1) \qquad |\langle(1, 0, 0, 0)\rangle^\perp \cap O| = |\{x \in \mathbb{F}_{q^3} : \mathrm{N}(x) = 0\}| = 1,$$

$$(3.2) \qquad |\langle(0, 0, 1, 0)\rangle^\perp \cap O| = 1 + |\{x \in \mathbb{F}_{q^3} : \mathrm{Tr}(x) = 0\}| = q^2 + 1,$$

$$(3.3) \qquad |\langle(1, 0, 0, 1)\rangle^\perp \cap O| = |\{x \in \mathbb{F}_{q^3} : \mathrm{N}(x) = 1\}| = q^2 + q + 1.$$

The fact that O_1 is a G-orbit has been mentioned in Section 2. We first calculate the sizes of O_2 and O_3 by determining the orders of the stabilizers of chosen orbit representatives. This allows us to compute $|v^\perp \cap O|$ for $v \in O_2 \cup O_3$. Then, taking O_4 to be the complement of $O_1 \cup O_2 \cup O_3$ in $\mathrm{PG}(V)$, we compute $|v^\perp \cap O|$ for $\langle v \rangle \in O_4$ using a counting argument. For properly chosen elements $\langle v \rangle \in O_4$, we interpret $|v^\perp \cap O|$ as the number of solutions to some equations over $\mathbb{F}_{q^3}$. This latter information is then used to determine the number of solutions over $\mathbb{F}_{q^3}$ of two equations, which is then used to show that O_4 is indeed a G-orbit.

The remaining part of this section is devoted to the proof of Theorem 3.1.

Lemma 3.2. *The orbit O_2 that contains $\langle(0, 0, 1, 0)\rangle$ has size $q(q^2 + q + 1)(q^3 + 1)$.*

Proof. Suppose that $g \in \mathrm{GL}(2, q^3)$ stabilizes $\langle (0, 0, 1, 0) \rangle$. Writing $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right)$, in view of (2.2) this is the case if and only if there exists $\lambda \in \mathbb{F}_q^*$ such that

$$(3.4) \qquad 0 = \mathrm{Tr}(dc^{q^2+q}),$$

$$(3.5) \qquad 0 = bc^{q^2+q} + d^q ac^{q^2} + d^{q^2} ac^q,$$

$$(3.6) \qquad \lambda = da^{q^2+q} + b^q a^{q^2} c + b^{q^2} a^q c,$$

$$0 = \mathrm{Tr}(ba^{q^2+q}).$$

We now distinguish three cases.

Case 1: $c = 0$. Then the above conditions reduce to $\mathrm{Tr}(ba^{q^2+q}) = 0$ and $da^{q^2+q} = \lambda$. Since $\det(g) \neq 0$ we have $ad \neq 0$. For each pair $(a, \lambda) \in \mathbb{F}_{q^3}^* \times \mathbb{F}_q^*$, there is exactly one $d \in \mathbb{F}_{q^3}$ and q^2 elements $b \in \mathbb{F}_{q^3}$ such that the two conditions are satisfied. Therefore, there are $q^2(q^3 - 1)(q - 1)$ such $g \in \mathrm{GL}(2, q^3)$ and correspondingly $q^2(q - 1)$ elements in G that stabilize $\langle (0, 0, 1, 0) \rangle$.

Case 2: $cd \neq 0$. Since $\mathrm{GL}(2, q^3)$ is acting on projective points, we may assume that $d = 1$. Write $u = 1/c$. Then (3.4) and (3.5) reduce to $\mathrm{Tr}(u) = 0$ and $b = -au^q - au^{q^2}$. We deduce that

$$
\begin{aligned}
a^{q^2+q} + b^q a^{q^2} c + b^{q^2} a^q c &= a^{q^2+q} + (-a^q u^{q^2} - a^q u) a^{q^2} u^{-1} + (-a^{q^2} u - a^{q^2} u^q) a^q u^{-1} \\
&= a^{q^2+q} u^{-1} (u - u^{q^2} - u - u - u^q) \\
&= -a^{q^2+q} u^{-1} \mathrm{Tr}(u) = 0,
\end{aligned}
$$

which contradicts (3.6).

Case 3: $c \neq 0$ and $d = 0$. In this case we deduce that $b = 0$ from (3.5). It follows that the left hand side of (3.6) equals zero, a contradiction.

In summary the stabilizer of $\langle (0, 0, 1, 0) \rangle$ in G has order $q^2(q - 1)$. The claim now follows from the orbit stabilizer theorem. $\qquad\square$

Lemma 3.3. *The orbit O_3 that contains $\langle (1, 0, 0, 1) \rangle$ has size $\frac{1}{2} q^3 (q^3 + 1)(q - 1)$.*

Proof. Suppose that $g \in \mathrm{GL}(2, q^3)$ stabilizes $\langle (0, 0, 1, 0) \rangle$. Writing $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right)$, we find from (2.2) that this is the case if and only if there exists an element $\lambda \in \mathbb{F}_q^*$ such that

$$(3.7) \qquad \lambda = \mathrm{N}(c) + \mathrm{N}(d),$$

$$(3.8) \qquad 0 = ac^{q^2+q} + bd^{q^2+q},$$

$$(3.9) \qquad 0 = ca^{q^2+q} + db^{q^2+q},$$

$$(3.10) \qquad \lambda = \mathrm{N}(a) + \mathrm{N}(b).$$

We distinguish three cases.

Case 1: $c = 0$. In this case we get $b = 0$ from (3.8) and the fact $ad - bc \neq 0$. Then (3.9) holds trivially, and (3.7) and (3.10) reduce to $\mathrm{N}(d) = \mathrm{N}(a) = \lambda$. There are $(q^3 - 1)(q^2 + q + 1)$ possible choices for g and hence $q^2 + q + 1$ elements of G that stabilize $\langle (1, 0, 0, 1) \rangle$.

Case 2: $d = 0$. This case is similar to the first case. We have $a = 0$ and find again that there are $q^2 + q + 1$ elements of G that stabilize $\langle (1, 0, 0, 1) \rangle$.

Case 3: $cd \neq 0$. Then (3.8) and $ad - bc \neq 0$ imply that $ab \neq 0$. Write $u = d/c$ and $m = a/b$. Then (3.8) and (3.9) reduce to $m = -u^{q^2+q}$ and $m^{q^2+q} = -u$. It follows that

$$-m = u^{q^2+q} = m^{(q^2+q)(q^2+q)} = m \cdot \mathrm{N}(m)$$

and therefore $\mathrm{N}(m) = -1$. We thus have

$$\mathrm{N}(a) + \mathrm{N}(b) = \mathrm{N}(b)(\mathrm{N}(m) + 1) = 0,$$

which contradicts (3.10).

In summary the stabilizer of $\langle(1, 0, 0, 1)\rangle$ in G has order $2(q^2 + q + 1)$ and the claim now follows from the orbit stabiliser theorem $\qquad\square$

In what follows we put

$$O_4 = \mathrm{PG}(V) \backslash (O_1 \cup O_2 \cup O_3).$$

We shall now show in a series of lemmas that O_4 is indeed a G-orbit containing $\langle(1, 0, \alpha, \alpha)\rangle$. We begin with determining the hyperplane sections of O corresponding to points of O_4.

Lemma 3.4. *For each $v \in O_4$, we have $|v^\perp \cap O| = q^2 - q + 1$.*

Proof. We double count the triples $(\langle v\rangle, \langle x\rangle, \langle y\rangle)$, where $\langle v\rangle \in \mathrm{PG}(V)$ and $\langle x\rangle, \langle y\rangle$ are distinct points of $v^\perp \cap O$. On one hand, the number of such triples is

$$\sum_{v \in \mathrm{PG}(V)} |v^\perp \cap O|(|v^\perp \cap O| - 1).$$

On the other hand, for distinct points $\langle x\rangle, \langle y\rangle$ in O, the size of $\langle x, y\rangle^\perp$ equals $(q^6 - 1)/(q - 1)$ and thus we we thus have

$$(3.11) \qquad \sum_{v \in \mathrm{PG}(V)} |v^\perp \cap O|(|v^\perp \cap O| - 1) = q^3(q^3 + 1)\frac{q^6 - 1}{q - 1}.$$

Similarly, by double counting the pairs $(\langle v\rangle, \langle x\rangle)$, where $\langle v\rangle \in \mathrm{PG}(V)$ and $\langle x\rangle \in v^\perp \cap O$, we obtain

$$(3.12) \qquad \sum_{v \in \mathrm{PG}(V)} |v^\perp \cap O| = (q^3 + 1)\frac{q^7 - 1}{q - 1}.$$

By combining (3.11) and (3.12) with (3.1), (3.2), (3.3) and Lemmas 3.2 and 3.3, we find that

$$\sum_{v \in O_4} |v^\perp \cap O| = \frac{1}{2}q^3(q^3 - 1)(q^3 + 1),$$

$$\sum_{v \in O_4} |v^\perp \cap O|^2 = \frac{1}{2}q^3(q^3 - 1)(q^3 + 1)(q^2 - q + 1).$$

Since O_4 has size $\frac{1}{2}q^3(q^3 - 1)(q + 1)$, we deduce that

$$\sum_{v \in O_4} \left(|v^\perp \cap O| - (q^2 - q + 1)\right)^2 = 0,$$

which completes the proof. $\qquad\square$

The next step will be to determine the number of solutions of certain equations, for which we need the following lemma.

Lemma 3.5. *We have* $\langle(0, 1, -1, 1 + \alpha)\rangle, \langle(1, \alpha, 0, \alpha^2)\rangle \in O_4$.

Proof. By (2.1) it is clear that the two points are not in O_1. It thus suffices to show that the two points are not in $O_2 \cup O_3$. We show that this holds for $P = \langle(0, 1, -1, 1 + \alpha)\rangle$. The other point can be treated similarly.

First suppose for a contradiction that $P \in O_2$. Then there exists $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{GL}(2, q^3)$ that maps $\langle(0, 0, 1, 0)\rangle$ to $\langle(0, 1, -1, 1 + \alpha)\rangle$. By (2.2), there exists $\lambda \in \mathbb{F}_q^*$ such that

$$0 = \mathrm{Tr}(dc^{q^2+q}), \tag{3.13}$$

$$\lambda = bc^{q^2+q} + d^q ac^{q^2} + d^{q^2} ac^q, \tag{3.14}$$

$$-\lambda = da^{q^2+q} + b^q ca^{q^2} + b^{q^2} ca^q, \tag{3.15}$$

$$\lambda(1 + \alpha) = \mathrm{Tr}(ba^{q^2+q}). \tag{3.16}$$

From (3.14) and (3.15) we deduce that $ac \neq 0$. Since $\mathrm{GL}(2, q^3)$ is acting on projective points, we may assume that $c = 1$. Then (3.13) takes the form $\mathrm{Tr}(d) = 0$, hence $d + d^q + d^{q^2} = 0$. Then (3.14) reduces to $b - ad = \lambda$.

Substitute $b = \lambda + ad$ into the left hand side of (3.15) to obtain

$$da^{q^2+q} + b^q a^{q^2} + b^{q^2} a^q = da^{q^2+q} + (\lambda + a^q d^q)a^{q^2} + (\lambda + a^{q^2} d^{q^2})a^q$$
$$= \mathrm{Tr}(d)a^{q^2+q} + \lambda(a^q + a^{q^2})$$
$$= \lambda(a^q + a^{q^2}).$$

Hence (3.15) reduces to $\lambda(a^q + a^{q^2}) = -\lambda$, and so $a = 1 + \mathrm{Tr}(a)$. Therefore $a \in \mathbb{F}_q$ and $a = 1 + 3a$. This implies that q is odd and $a = -1/2$. Using $b = \lambda + ad$ and $\mathrm{Tr}(d) = 0$, (3.16) then reduces to

$$\tfrac{3}{4}\lambda = \lambda(1 + \alpha).$$

Hence $\alpha = -1/4$. But then $x^2 - x - \alpha = (x - 1/2)^2$, contradicting the assumed irreducibility of this polynomial. This proves that $P \notin O_2$.

Now suppose for a contradiction that $P \in O_3$. Then there exists $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{GL}(2, q^3)$ that maps $\langle(1, 0, 0, 1)\rangle$ to $\langle(0, 1, -1, 1 + \alpha)\rangle$. By (2.2), this implies that there exists $\lambda \in \mathbb{F}_q$ such that

$$0 = \mathrm{N}(c) + \mathrm{N}(d), \tag{3.17}$$

$$\lambda = ac^{q^2+q} + bd^{q^2+q}, \tag{3.18}$$

$$-\lambda = ca^{q^2+q} + db^{q^2+q}, \tag{3.19}$$

$$\lambda(1 + \alpha) = \mathrm{N}(a) + \mathrm{N}(b). \tag{3.20}$$

From (3.17) and $ad - bc \neq 0$ we deduce that $cd \neq 0$. Again we may assume that $c = 1$. Since $\lambda^q = \lambda$, the same holds for the left hand sides of (3.18) and (3.19).

$$a + bd^{q^2+q} = a^q + b^q d^{q^2+1},$$
$$a^{q^2+q} + db^{q^2+q} = a^{q^2+1} + d^q b^{q^2+1}.$$

After rearranging terms, we have

(3.21)
$$a - a^q = d^{q^2}(db^q - bd^q),$$
$$a^{q^2}(a - a^q) = b^{q^2}(db^q - bd^q).$$

from which we find that

$$(b - ad)^{q^2}(a - a^q)(db^q - bd^q) = 0.$$

From $bc - ad \neq 0$ and $c = 1$ and (3.21), we then conclude $a - a^q = 0$ and so $a \in \mathbb{F}_q$.

From $c = 1$ and (3.13) we have $N(d) = -1$. From (3.18) we have $\lambda = a - b/d$ and thus $b/d = a - \lambda$ is in $\mathbb{F}_q$. Hence

$$N(b) = N(d) N(b/d) = -(b/d)^3.$$

By adding up both sides of (3.18) and (3.19), we obtain

$$a + a^2 - (b/d) - (b/d)^2 = 0,$$

or equivalently $(a - b/d)(a + b/d + 1) = 0$. Since $a - b/d = \lambda \neq 0$, we have $a + b/d + 1 = 0$. From (3.20) we then deduce that

$$\begin{aligned}
\alpha &= \frac{N(a) - N(b/d)}{a - b/d} - 1 \\
&= \frac{a^3 - (b/d)^3}{a - b/d} - 1 \\
&= a^2 + ab/d + (b/d)^2 - 1 \\
&= a(a + 1),
\end{aligned}$$

using $a = -b/d - 1$. But then $x^2 - x - \alpha = (x - a)(x + a + 1)$, which again contradicts the irreducibility of this polynomial. This proves that $P \notin O_3$. $\qquad \square$

Corollary 3.6. *We have*

$$|\{x \in \mathbb{F}_{q^3} : \mathrm{Tr}(x) + \mathrm{Tr}(x^{q^2+q}) + 1 + \alpha = 0\}| = q^2 - q,$$
$$|\{x \in \mathbb{F}_{q^3} : N(x) - \mathrm{Tr}(x^{q^2+q})\alpha - \alpha^2 = 0\}| = q^2 - q + 1.$$

Proof. For each point $P = \langle(v_1, v_2, v_3, v_4)\rangle$ in $\mathrm{PG}(V)$, the set $P^\perp \cap (O\backslash\{\langle(0,0,0,1)\rangle\})$ equals

$$\{\langle(1, x, x^{q+q^2}, N(x))\rangle : v_4 - v_1 N(x) + \mathrm{Tr}(v_2 x^{q^2+q} - v_3 x) = 0, x \in \mathbb{F}_{q^3}\}.$$

By taking P as $\langle(0, 1, -1, 1 + \alpha)\rangle$ and $\langle(1, \alpha, 0, \alpha^2)\rangle$, the result follows from Lemmas 3.4 and 3.5 and the fact that $P^\perp$ contains $\langle(0,0,0,1)\rangle$ if and only if $v_1 = 0$. $\qquad \square$

Now we show that O_4 is indeed a G-orbit.

Lemma 3.7. *The set O_4 is a G-orbit of size $\frac{1}{2}(q^3(q^3-1)(q+1))$ and contains $\langle(1, 0, \alpha, \alpha)\rangle$.*

Proof. Suppose that $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{GL}(2, q^3)$ stabilizes $P = \langle(1, 0, \alpha, \alpha)\rangle$. By (2.2), this is the case if and only if there exists $\lambda \in \mathbb{F}_q^*$ such that

$$(3.22) \qquad \lambda = \mathrm{N}(d) + \mathrm{N}(c)\alpha + \mathrm{Tr}(dc^{q^2+q})\alpha,$$

$$(3.23) \qquad 0 = ac^{q^2+q}\alpha + bd^{q^2+q} + (bc^{q^2+q} + d^q ac^{q^2} + d^{q^2} ac^q)\alpha,$$

$$(3.24) \qquad \lambda\alpha = ca^{q^2+q}\alpha + db^{q^2+q} + (da^{q^2+q} + b^q ca^{q^2} + b^{q^2} ca^q)\alpha,$$

$$(3.25) \qquad \lambda\alpha = \mathrm{N}(b) + \mathrm{N}(a)\alpha + \mathrm{Tr}(ba^{q^2+q})\alpha.$$

First observe that $\alpha \neq -1/4$, since otherwise $x^2 - x + 1/4 = (x - 1/2)^2$ is not irreducible. Next we distinguish four cases.

Case 1: $c = 0$. In this case we have $b = 0$ from (3.23) and $ad - bc \neq 0$. Then (3.24) and (3.25) reduce to $(d/a)\,\mathrm{N}(a) = \mathrm{N}(a)$ and so $a = d$. Hence g is a scalar matrix and corresponds to the identity in G.

Case 2: $d = 0$. Then $c \neq 0$ and we may assume that $c = 1$. Then (3.23) implies $b = -a$. From (3.22) we have $\lambda = \alpha$ and so $\alpha \in \mathbb{F}_q$. From (3.24) we find that $\mathrm{N}(a) = -a\alpha$, which implies $a \in \mathbb{F}_q$. From (3.25) we then find that $a = \alpha/(2\alpha + 1)$ and $\alpha = -1$ upon taking norms. To sum up, we obtain a unique element in G for $\alpha = -1$ and a contradiction otherwise.

Case 3: $cd \neq 0$ and $d^{q^2+q} + \alpha = 0$. Again we may assume that $c = 1$. Since $\mathrm{N}(d) = -\alpha d$, we deduce that $d \in \mathbb{F}_q^*$ and so $d^2 = -\alpha$. As remarked earlier this implies $d \neq \pm 1/2$. Now (3.23) reduces to $a\alpha(1 + 2d) = 0$, so $a = 0$. The other three equations then reduce to $d = b$ and $(2d - 1)(d + 1) = 0$. It follows that $d = -1$ and $\alpha = -1$. Hence we again obtain a unique element in G for $\alpha = -1$ and a contradiction otherwise.

Case 4: $cd(d^{q^2+q} + \alpha) \neq 0$. As usual, we may assume that $c = 1$. Now the conditions are equivalent to

$$(3.26) \qquad \mathrm{N}(d) + \alpha + \mathrm{Tr}(d)\alpha \neq 0,$$

$$(3.27) \qquad a\alpha + bd^{q^2+q} + (b + d^q a + d^{q^2} a)\alpha = 0,$$

$$(3.28) \quad a^{q^2+q}\alpha + db^{q^2+q} + (da^{q^2+q} + b^q a^{q^2} + b^{q^2} a^q)\alpha = \mathrm{N}(b) + \mathrm{N}(a)\alpha + \mathrm{Tr}(ba^{q^2+q})\alpha,$$

$$(3.29) \quad a^{q^2+q}\alpha + db^{q^2+q} + (da^{q^2+q} + b^q a^{q^2} + b^{q^2} a^q)\alpha = \mathrm{N}(d)\alpha + \alpha^2 + \mathrm{Tr}(d)\alpha^2.$$

Put

$$u = \frac{1 + d^q + d^{q^2}}{d^{q^2+q} + \alpha}.$$

Then (3.27) implies that $b = -ua\alpha$, hence $ab \neq 0$. Substitute into (3.28) and divide both sides by $a^{q^2+q}\alpha$ to obtain

$$1 + d + (du^{q^2+q} - u^q - u^{q^2})\alpha = (1 - \mathrm{N}(u)\alpha^2 - \mathrm{Tr}(u)\alpha)a.$$

We plug in the expression of u to see that the left hand side equals

$$(3.30) \qquad \frac{(d + d^2 - \alpha)(\mathrm{N}(d) + \alpha + \mathrm{Tr}(d)\alpha)}{(d^{q^2+1} + \alpha)(d^{q+1} + \alpha)}$$

and the right hand side equals

$$\frac{(\mathrm{N}(d) - 2\alpha\mathrm{Tr}(d^{q^2+q}) - \alpha\mathrm{Tr}(d) - 2\alpha^2 - \alpha)(\mathrm{N}(d) + \alpha + \mathrm{Tr}(d)\alpha)}{\mathrm{N}(d^{q^2+q} + \alpha)}\,a.$$

Hence we have
$$a = \frac{(d^{q^2+q} + \alpha)(d^2 + d - \alpha)}{\mathrm{N}(d) - 2\alpha\,\mathrm{Tr}(d^{q^2+q}) - \alpha\,\mathrm{Tr}(d) - 2\alpha^2 - \alpha}.$$

We now have expressed a and b in terms of d. From (3.30) we find that (3.29) reduces to

$$\alpha(\mathrm{N}(d) + \alpha + \mathrm{Tr}(d)\alpha)\left(\frac{\mathrm{N}(d + d^2 - \alpha)}{(\mathrm{N}(d) - 2\alpha\mathrm{Tr}(d^{q^2+q}) - \alpha\mathrm{Tr}(d) - 2\alpha^2 - \alpha)^2} - 1\right) = 0.$$

Next we deduce that

$$\det(g) = a(d + u\alpha) = \frac{(d^2 + d - \alpha)(\mathrm{N}(d) + \alpha + \mathrm{Tr}(d)\alpha)}{\mathrm{N}(d) - 2\alpha\,\mathrm{Tr}(d^{q^2+q}) - \alpha\,\mathrm{Tr}(d) - 2\alpha^2 - \alpha}.$$

Hence $\det(g) \neq 0$ is equivalent to (3.26). Therefore the conditions on g reduce to the following: $d(d^{q^2+q} + \alpha) \neq 0$, $\mathrm{N}(d) + \alpha + \mathrm{Tr}(d)\alpha \neq 0$, and

(3.31) $\mathrm{N}(d + d^2 - \alpha) - (\mathrm{N}(d) - 2\alpha\,\mathrm{Tr}(d^{q^2+q}) - \alpha\,\mathrm{Tr}(d) - 2\alpha^2 - \alpha)^2 = 0.$

Put
$$x = \mathrm{Tr}(d) + \mathrm{Tr}(d^{q^2+q}) + 1 + \alpha,$$
$$y = \mathrm{N}(d) - \mathrm{Tr}(d^{q^2+q})\alpha - \alpha^2,$$

so that
$$y - \alpha x = \mathrm{N}(d) - 2\alpha\,\mathrm{Tr}(d^{q^2+q}) - \alpha\,\mathrm{Tr}(d) - 2\alpha^2 - \alpha,$$
$$y + \alpha x = \mathrm{N}(d) + \mathrm{Tr}(d)\alpha + \alpha.$$

It is tedious but not difficult to check that $\mathrm{N}(d + d^2 - \alpha) = (y + \alpha x)^2 + xy$, so that (3.31) reduces to $(4\alpha + 1)xy = 0$, which in turn reduces to $xy = 0$ using $\alpha \neq -1/4$. Therefore the conditions on g reduce to

(3.32) $xy = 0,$ $d(d^{q^2+q} + \alpha) \neq 0,$ $\mathrm{N}(d) + \mathrm{Tr}(d)\alpha + \alpha \neq 0.$

First suppose that $x = 0$. By Corollary 3.6 there $q^2 - q$ choices for d such that $x = 0$. We now show that the second and third condition in (3.32) are satisfied for these choices of d unless $\alpha = -1$ and $d = 0$ or -1.

   It is routine to check that $d^{q^2+q} + \alpha = -(1 + d + d^q)(1 + d)$ and $\mathrm{N}(d) + \mathrm{Tr}(d)\alpha + \alpha = -\mathrm{N}(1 + d + d^q)$. The condition $1 + d + d^q = 0$ is equivalent to $d = 1 + \mathrm{Tr}(d)$ and thus to $2d = -1$. Hence the second and third conditions in (3.32) are equivalent to $d(1 + d)(2d + 1) \neq 0$. If $2d + 1 = 0$, then q is odd and $d = -1/2$ and $x = 0$ forces $\alpha = -1/4$, a contradiction. If $d = 0$ or $d = -1$, then $\alpha = -1$. Hence, for $x = 0$, we obtain $q^2 - q$ suitable elements of G, unless $\alpha = -1$, in which case we obtain $q^2 - q - 2$ such elements.

   Note that the third condition in (3.32) is equivalent to $y + \alpha x \neq 0$. Thus $x = 0$ forces $y \neq 0$ (this also holds for $\alpha = -1$ and $d = 0$ or -1). Suppose now that $y = 0$. By contraposition this forces $x \neq 0$. By Corollary 3.6 there $q^2 - q + 1$ choices for d such that $y = 0$. We now show that the second and third condition in (3.32) are satisfied for these choices of d.

   It is clear that $d \neq 0$, and so $d^{q^2+q} + \alpha \neq 0$ by the fact $\mathrm{N}(d) = (\mathrm{Tr}(d^{q^2+q}) + \alpha)\alpha$. Hence the second condition in (3.32) holds. Since $x \neq 0$, we have $y + \alpha x \neq 0$ and so the

third condition in (3.32) is also satisfied. Hence, for $y = 0$, we obtain $q^2 - q + 1$ suitable elements of G

In summary the four cases give exactly $2(q^2 - q + 1)$ elements in G that stabilize $\langle v \rangle$, from which the claim follows. $\qquad\square$

Theorem 3.1 now follows by combining Lemmas 3.2, 3.3, 3.4, and 3.7.

4. THE LINEAR CODE OF THE SET O

It is well known that up to linear equivalence, spanning multisets of points in $\mathrm{PG}(\mathbb{F}_q^k) \cong \mathrm{PG}(k-1, q)$ correspond to linear codes over $\mathbb{F}_q$ of dimension k in which no coordinate is identically zero. Thereby, the hyperplanes correspond to the projective equivalence classes of the nonzero codewords and the hyperplane sections correspond to the Hamming weights. An early publication of this observation is [2, Thm. 1.11] and a good overview is given in [9].

To make this correspondence precise, let $\mathcal{P}$ be a multiset of n points $\langle v_1 \rangle, \ldots, \langle v_n \rangle$ spanning $\mathrm{PG}(\mathbb{F}_q^k)$. With $\mathcal{P}$ we associate the $[n, k]_q$ code C generated by the matrix G with the columns $v_1, \ldots, v_n$. While this code depends on the chosen point representatives and the order of the points, it is unique up to linear equivalence. Conversely every equivalence class of $[n, k]_q$ codes in which no coordinate is identically zero corresponds to a multiset of n points spanning $\mathrm{PG}(\mathbb{F}_q^k)$. A hyperplane $H = v^\perp$ of $\mathrm{PG}(\mathbb{F}_q^k)$ corresponds to the set of $q - 1$ nonzero scalar multiples of $v^\top G$, which are all codewords of C. The (common) Hamming weight of these $q - 1$ codewords is given by the number of points in $\mathcal{P}$ that are not contained in H.

Now based on the notation of Section 2, we are going to describe and investigate the code C_O associated with the point set $\mathcal{P} = O$ in $\mathrm{PG}(\mathbb{F}_q^8)$. Explicitly, the code C_O is generated by

$$G_O = \begin{bmatrix} g(x_1) & g(x_2) & \cdots & g(x_{q^3}) & e_8 \end{bmatrix},$$

where $e_8 = (0, 0, 0, 0, 0, 0, 0, 1)^\top$ and

$$g(x) = (1, \mathrm{Tr}(x), \mathrm{Tr}(\theta x), \mathrm{Tr}(\theta^2 x), \mathrm{Tr}(x^{q+q^2}), \mathrm{Tr}(\theta x^{q+q^2}), \mathrm{Tr}(\theta^2 x^{q+q^2}), \mathrm{N}(x))^\top$$

with θ being a primitive element of $\mathbb{F}_{q^3}$. Then C has length $q^3 + 1$ and dimension 8, using the fact that O spans $\mathrm{PG}(\mathbb{F}_q^8)$. The weight distribution (and therefore the minimum distance) of C_O follows from the above discussion and the hyperplane sections given in Theorem 3.1.

Theorem 4.1. *The code C_O has parameters $[q^3 + 1, 8, q^3 - q^2 - q]_q$ and the following weight distribution*

weight	multiplicity
0	1
$q(q^2 - q - 1)$	$\frac{1}{2}q^3(q^3 + 1)(q - 1)^2$
$q^2(q - 1)$	$q(q^6 - 1)$
$q(q^2 - q + 1)$	$\frac{1}{2}q^3(q^3 - 1)(q^2 - 1)$
q^3	$(q^3 + 1)(q - 1)$

TABLE 1. THE CODES C_O FOR SMALL q

q	parameters	weight distribution
2	$[9, 8, 2]_2$	$(0^1 2^{36} 4^{126} 6^{84} 8^9)$
3	$[28, 8, 15]_3$	$(0^1 15^{1512} 18^{2184} 21^{2808} 27^{56})$
4	$[65, 8, 44]_4$	$(0^1 44^{18720} 48^{16380} 52^{30240} 64^{195})$
5	$[126, 8, 95]_5$	$(0^1 95^{126000} 100^{78120} 105^{186000} 125^{504})$
7	$[344, 8, 287]_7$	$(0^1 287^{2123856} 294^{823536} 301^{2815344} 343^{2064})$
8	$[513, 8, 440]_8$	$(0^1 440^{6435072} 448^{2097144} 456^{8241408} 512^{3591})$
9	$[730, 8, 639]_9$	$(0^1 639^{17029440} 648^{4782960} 657^{21228480} 729^{5840})$

For small q, the parameters and the weight distribution of the code C_O are given explicitly in Table 1.

Next we discuss optimality properties of C_O with respect to the theory in [10]. For a linear code C with parameters $[n, k, d]_q$, the following notions of optimality are defined in [10]:

- C is *length-optimal* (*n-optimal*) if no linear $[n - 1, k, d]_q$ code exists;
- C is *dimension-optimal* (*k-optimal*) if no linear $[n, k + 1, d]_q$ code exists;
- C is *distance-optimal* (*d-optimal*) if no linear $[n, k, d + 1]_q$ code exists;
- C is *shortening-optimal* (*S-optimal*) if no linear $[n + 1, k + 1, d]_q$ code exists;
- C is *puncturing-optimal* (*P-optimal*) if no linear $[n + 1, k, d + 1]_q$ code exists.

There are the following implications:

$$C \text{ is } n\text{-optimal} \implies C \text{ is } k\text{-optimal and } d\text{-optimal};$$
$$C \text{ is } P\text{-optimal} \implies C \text{ is } d\text{-optimal};$$
$$C \text{ is } S\text{-optimal} \implies C \text{ is } k\text{-optimal}.$$

Suitable examples show that there are no other implications among the five optimality notions. If a code is optimal with respect to all five of the above optimality concepts, then it is called *strongly optimal*. By the stated implications, strong optimality already follows from n-, S- and P-optimality.

For $q = 2$, C_O is the binary parity check code with the parameters $[9, 8, 2]_2$, which is an MDS-code and in particular n-optimal. Moreover, it is P-optimal, but not S-optimal as there exists the $[10, 9, 2]_2$ binary parity check code.

We now consider the case $q \geq 3$. The *i*th *Krawtchouk polynomial* (with parameters q and n) is the polynomial

$$K_i = \sum_{j=0}^{i} (-1)^j (q - 1)^{(i-j)} \binom{x}{j} \binom{n - x}{i - j}$$

of degree i in $\mathbb{R}[x]$. For each polynomial $f \in \mathbb{R}[x]$ of degree at most n there are unique $f_0, f_1, \ldots, f_n \in \mathbb{R}$ such that

$$f = \sum_{i=0}^{n} f_i K_i,$$

which is known as the *Krawtchouk expansion* of f. Next we quote the well known linear programming bound (see [17], for example).

Theorem 4.2. *Let C be a code of length n and minimum distance d over an alphabet of size q. Let $f \in \mathbb{R}[x]$ be a polynomial with Krawtchouk expansion $f = \sum_{i=0}^{n} f_i K_i$ such that $f_i \geq 0$ for all $i \in \{0, 1, \ldots, n\}$ and $f(i) \leq 0$ for all $i \in \{d, d+1, \ldots, n\}$. Then we have*

$$|C| \leq f(0)/f_0.$$

We now apply Theorem 4.2 to show that C_O is n-optimal for all q.

Theorem 4.3. *Let C be a code of length q^3 and minimum distance at least $q^3 - q^2 - q$ over a q-ary alphabet for $q \geq 3$. Then*

$$|C| \leq \frac{1}{2} \frac{q^5(q^2 - q - 1)(q^3 - q^2 + q - 2)(q^2 + 1)}{q^4 - 2q^3 - q^2 + 3}.$$

In particular $|C| < q^8$ and so no $[q^3, 8, q^3 - q^2 - q]_q$ code exists.

Proof. Write

$$z_1 = q^3 - q^2 - q, \quad z_2 = q^3 - q^2 + q - 2, \quad z_3 = q^3 - q^2 + q - 1, \quad \text{and} \quad n = q^3.$$

We have $0 < z_1 < z_2 < z_3 < n$, so the polynomial $f(x) = (x - z_1)(x - z_2)(x - z_3)(x - n)$ has no repeated roots. Note that C has minimum distance at least z_1 and length n. Since $f(0) > 0$, we therefore have $f(i) \leq 0$ for all $i \in \{d, d+1, \ldots, n\}$. The Krawtchouk expansion of f is

$$f = f_0 K_0 + f_1 K_1 + f_2 K_2 + f_3 K_3 + f_4 K_4,$$

where

$$f_0 = \frac{2}{q}(q - 1)(q^4 - 2q^3 - q^2 + 3),$$

$$f_1 = \frac{2}{q^4}(q - 1)(q^6 + q^5 - 10q^3 + 3q + 12),$$

$$f_2 = \frac{2}{q^4}(q^5 + 5q^4 - 9q^3 - 6q^2 - 18q + 36),$$

$$f_3 = \frac{6}{q^4}(q^3 + q^2 + 3q - 12),$$

$$f_4 = \frac{24}{q^4}.$$

Since $q \geq 3$, all these coefficients are nonnegative. Then Theorem 4.2 gives the desired bound for $|C|$. $\square$

Theorem 4.3 gives the following corollary.

Corollary 4.4. *The code C_O is n-optimal for all q.*

For $q \in \{3, 4, 5\}$, we can say a bit more.

Theorem 4.5. *The code C_O is strongly optimal for $q \in \{3, 4\}$ and S-optimal for $q = 5$.*

Proof. The nonexistence of the corresponding codes can be looked up at the online tables [5]. We illustrate the typical reasoning behind the entries in the case $q = 3$.

Assume that C_O is not P-optimal. Then there exists a $[29, 8, 16]_3$ code C. Its residual (obtained by shortening C in the support of a codeword of weight 16) is a $[13, 7, \geq 6]_3$ code [12, Thm. 2.7.1]. Puncturing in a single position yields a $[12, 7, \geq 5]_3$ code. However according to the sphere packing bound, a ternary code of length 12 and minimum distance at least 5 contains at most 1838 codewords, which is a contradiction.

Now assume that C_O is not S-optimal. Then there exists a $[29, 9, 15]_3$ code C. Its dual $C^\perp$ is a $[29, 20, d^\perp]_3$ code with minimum distance $d^\perp \leq 6$ by the sphere packing bound. Let $c \in C^\perp$ be a codeword of minimum nonzero weight. Shortening C in a set of 6 positions containing the support of c gives a $[23, \geq 4, \geq 15]_3$ code. After puncturing in two positions we get a $[21, \geq 4, \geq 13]_3$ code, which implies the existence of a $[21, 4, 13]_3$-code. This code does not exist by [11, Thm. 3.2]. $\qquad\square$

We remark that for $q = 5$, the code C_O might also be P-optimal (and hence strongly optimal), since according to [5] the existence of a linear $[127, 8, 45]_5$ code is open.

Based on the above investigation, we dare to state the following conjecture.

Conjecture 1. *The code C_O is strongly optimal for all $q \geq 3$.*

We close this section with some remarks on codes obtained by puncturing C_O. Let T be a set of t coordinate positions of C_O. Deleting all coordinates in T in each codeword of C_O, we obtain a linear code C_O^T of length $q^3 + 1 - t$. If t is strictly less than $q^3 - q^2 - q$ (the minimum distance of C_O), then the dimension of C_O^T is still 8 and the minimum distance of C_O^T is at least $q^3 - q^2 - q - t$.

One can show that, for $t \leq \lfloor (q - 3)/2 \rfloor$ and $q \geq 5$, the code C_O^T has minimum distance exactly $q^3 - q^2 - q - t$ and is still n-optimal. To prove this, it is enough to take $t = \lfloor (q - 3)/2 \rfloor$ and to use the same approach as that in the proof of Theorem 4.2 with

$$z_1 = q^3 - q^2 - q - t, \quad z_2 = q^3 - q^2 + q - 2 - t, \quad z_3 = q^3 - q^2 + q - 1 - t, \quad \text{and} \quad n = q^3 - t$$

to show that no linear code with parameters $[q^3 - t, 8, \geq q^3 - q^2 - q - t]_q$ can exist.

5. THE DUAL CODE $C_O^\perp$

We now investigate the dual code $C_O^\perp$ of C_O of length $q^3 + 1$ and dimension $q^3 - 7$.

Theorem 5.1. *The code $C_O^\perp$ has parameters $[q^3 + 1, q^3 - 7, d]_q$, where*

$$d = \begin{cases} 9 & \text{for } q = 2; \\ 6 & \text{for } q = 3; \\ 5 & \text{for } q \geq 4. \end{cases}$$

Moreover the number of codewords in $C_O^\perp$ of weight 5 is

$$\frac{1}{120}(q - 3)(q - 2)(q - 1)q^3(q^6 - 1).$$

Proof. Let $(A_i)_i$ and $(A_i')_i$ be the weight distributions of C_O and $C_O^\perp$, respectively. By the MacWilliams identity we have

$$A_j' = \frac{1}{|C|} \sum_{i=0}^n K_j(i) A_i \quad \text{for each } j.$$

Now $(A_i)_i$ is given in Theorem 4.1 and a computation reveals that $A'_1 = A'_2 = A'_3 = A'_4 = 0$ and that A'_5 equals the corresponding expression in the statement of the theorem. This shows that $A'_5 \neq 0$ for $q \geq 4$. For $q = 3$ we have $A'_5 = 0$ and we compute $A'_6 = 6552$. For $q = 2$, the code C_O is the binary parity check code of length 9 whose dual is the binary repetition code of length 9 and minimum distance 9. $\qquad\square$

Theorem 5.2. *The code $C_O^\perp$ is n-optimal for all q.*

Proof. The claim is clear for $q = 2$. For $q = 3$, shortening a $[27, 20, 6]_3$ code in 12 positions would result in a $[17, \geq 8, \geq 6]_3$ code, which does not exist by [19].

Now let $q \geq 4$ and suppose that C is a code of length q^3 and minimum distance 5 over $\mathbb{F}_q$. A Hamming sphere of radius 2 in $\mathbb{F}_q^{q^3}$ is of size

$$\sum_{i=0}^{2} \binom{q^3}{i}(q-1)^i = \tfrac{1}{2}q^8 - q^7 + \tfrac{1}{2}q^6 - \tfrac{1}{2}q^5 + 2q^4 - \tfrac{3}{2}q^3 + 1.$$

Since $q \geq 4$, one checks that this is strictly larger than q^7. Hence by the sphere packing bound we have $|C| < q^{q^3-7}$. Hence no $[q^3, q^3 - 7, 5]_q$ code can exist. This implies n-optimality of $C_O^\perp$. $\qquad\square$

For $q = 2$, the code $C_O^\perp$ is S-optimal, but not P-optimal. Moreover from the tables [5] we find the following. For $q = 3$, the code $C_O^\perp$ is P-optimal, but S-optimality is open. For $q = 4$, the code $C_O^\perp$ is not S-optimal and P-optimality is open. For $q = 5$, both S- and P-optimality is open.

References

[1] J. Bierbrauer, Introduction to Coding Theory, 2nd ed. Boca Raton, FL, USA: CRC Press, 2017.

[2] R. C. Burton, An application of convex sets to the construction of error correcting codes and factorial designs. PhD thesis. University of North Carolina, 1964.

[3] A. R. Calderbank and W. M. Kantor, The geometry of two-weight codes. Bull. Lond. Math. Soc. 18(2) (1986), 97–122.

[4] C. Carlet, C. Ding and J. Yuan, Linear codes from perfect nonlinear mappings and their secret sharing schemes, IEEE Trans. Inf. Theory 51(6) (2005), 2089–2102.

[5] www.codetables.de

[6] B. N. Cooperstein, Hyperplane sections of Kantor's unitary ovoids. Des. Codes Cryptogr. 23(2) (2001), 185–195.

[7] Ph. Delsarte, An algebraic approach to the association schemes of coding theory. Philips Res. Rep. Supp. 10, 1973.

[8] C. Ding, T. Helleseth, T. Kløve and X. Wang.: A generic construction of Cartesian authentication codes. IEEE Trans. Inf. Theory 53(6) (2007), 2229–2235.

[9] S. Dodunekov and J. Simonis Codes and projective multisets. Electronic Journal of Combinatorics 5, #R37 (1998).

[10] S. Dodunekov and J. Simonis, Constructions of Optimal Linear Codes. Numbers, information and complexity (Bielefeld, 1998), 245–263, Kluwer Acad. Publ., Boston, MA, 2000.

[11] R. Hill and D. E. Newton, Optimal ternary linear codes, Des. Codes Cryptogr. 2(2) (1992), 137–142.

[12] W. C. Huffman, V. Pless, Fundamentals of error-correcting codes, Cambridge University Press, 2003.

[13] I. Honkala and A. Tietäväinen, Codes and number theory,in Handbook of Coding Theory, Vol. II, V. S. Pless and W. C. Huffman (Eds.), pp. 1143–1194. Elsevier, 1998.

[14] W. M. Kantor, Ovoids and Translation Planes, Canad. J. Math. 34(5) (1982), 1195–1207.

[15] Kløve T.: Codes for Error Detection. World Scientfic, Singapore, 2007.

[16] R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, 1997.

[17] F. J. MacWilliams, N. J. A. Sloane, The Theory of Error-Correcting Codes, North Holland, 1977.

[18] V. Pepe, Desarguesian and unitary complete partial ovoids. J. Algebraic Combin. 37(3) (2013), 503–522.

[19] M. van Eupen, Four nonexistence results for ternary linear codes. IEEE Trans. Inf. Theory 41(3) (1995), 800–805.

[20] J. Yuan and C. Ding, Secret sharing schemes from three classes of linear codes, IEEE Trans. Inf. Theory 52(1) (2006), 206–212.

SCHOOL OF MATHEMATICAL SCIENCES, ZHEJIANG UNIVERSITY, 38 ZHEDA ROAD, HANGZHOU 310027, ZHEJIANG, P.R CHINA

Email address: `tfeng@zju.edu.cn`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BAYREUTH, UNIVERSITÄTSSTR. 30, 95447 BAYREUTH, GERMANY

Email address: `michael.kiermaier@uni-bayreuth.de`

SCHOOL OF MATHEMATICAL SCIENCES, ZHEJIANG UNIVERSITY, 38 ZHEDA ROAD, HANGZHOU 310027, ZHEJIANG, P.R CHINA

Email address: `lpx@zju.edu.cn`

DEPARTMENT OF MATHEMATICS, PADERBORN UNIVERSITY, WARBURGER STR. 100, 33098 PADERBORN, GERMANY.

Email address: `kus@math.upb.de`