Algorithmica (2023) 85:3973–3995
https://doi.org/10.1007/s00453-023-01173-5

The Subfield and Extended Codes of a Subclass of Optimal Three-Weight Cyclic Codes

Félix Hernández[1] · Gerardo Vega[2]

Received: 23 February 2023 / Accepted: 4 September 2023 / Published online: 25 September 2023

Abstract

A class of optimal three-weight $[q^k - 1, k + 1, q^{k-1}(q - 1) - 1]$ cyclic codes over $\mathbb{F}_q$, with $k \geq 2$, achieving the Griesmer bound, was presented by Heng and Yue (IEEE Trans Inf Theory 62(8):4501–4513, 2016. https://doi.org/10.1109/TIT.2016.2550029). In this paper we study some of the subfield codes of this class of optimal cyclic codes when $k = 2$. The weight distributions of the subfield codes are settled. It turns out that some of these codes are optimal and others have the best known parameters. The duals of the subfield codes are also investigated and found to be almost optimal with respect to the sphere-packing bound. In addition, the covering structure for the studied subfield codes is determined. Some of these codes are found to have the important property that any nonzero codeword is minimal, which is a desirable property that is useful in the design of a secret sharing scheme based on a linear code. Moreover, a specific example of a secret sharing scheme based on one of these subfield codes is given. Finally, a class of optimal two-weight linear codes over $\mathbb{F}_q$, achieving the Griesmer bound, whose duals are almost optimal with respect to the sphere-packing bound is presented. Through a different approach, this class of optimal two-weight linear codes was reported very recently by Heng (IEEE Trans Inf Theory 69(2):978–994, 2023. https://doi.org/10.1109/TIT.2022.3203380). Furthermore, it is shown that these optimal codes can be used to construct strongly regular graphs.

A short version of this paper appeared in the Proceedings of LATIN 2022 [1].

✉ Félix Hernández
felixhdz@ciencias.unam.mx

Gerardo Vega
gerardov@unam.mx

[1] Posgrado en Ciencia e Ingeniería de la Computación, Universidad Nacional Autónoma de México, Mexico City 04510, Mexico

[2] Dirección General de Cómputo y de Tecnologías de Información y Comunicación, Universidad Nacional Autónoma de México, Mexico City 04510, Mexico

Keywords Subfield codes · Extended codes · Optimal linear codes · Secret sharing schemes · Griesmer bound · Sphere-packing bound

1 Introduction

Let $\mathbb{F}_q$ be the finite field with q elements. An $[n, l, d]$ linear code, $\mathcal{C}$, over $\mathbb{F}_q$ is an l-dimensional subspace of $\mathbb{F}_q^n$ with minimum Hamming distance d. It is called *cyclic* if $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ implies $(c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$. Further, the linear code $\mathcal{C}$ is called *optimal* if there is no $[n, l, d']$ code with $d' > d$, and *almost optimal* if there is an optimal $[n, l, d + 1]$ code [1].

Recently, a class of optimal three-weight $[q^k - 1, k + 1, q^{k-1}(q - 1) - 1]$ cyclic codes over $\mathbb{F}_q$ achieving the Griesmer bound was presented in [2], which generalizes a result in [3] from $k = 2$ to arbitrary positive integer $k \geq 2$. Further, the q_0-ary subfield codes of two families of q-ary optimal linear codes were studied in [4], with q_0 being a power of a prime such that q is in turn a power of q_0 (that is, $\mathbb{F}_{q_0}$ is a proper subfield of $\mathbb{F}_q$). Also, some basic results on subfield codes were derived and the subfield codes of ovoid codes were determined in [5]. In addition, the subfield codes of several families of linear codes were obtained in [6], and the subfield codes of hyperoval and conic codes were studied in [7]. The basic idea in these last four references is to consider the subfield code of an optimal, or almost optimal, linear code over $\mathbb{F}_q$ and expect the subfield code over $\mathbb{F}_{q_0}$ to have also good parameters. In all cases, subfield codes with very attractive parameters were found.

Thus, the first objective of this paper is to study the q_0-ary subfield codes for a subclass of the optimal three-weight cyclic codes reported in [2] and determine their weight distributions. It turns out that the studied subfield codes also have three nonzero weights, which is of interest as linear codes with few weights have a wide range of applications in many research fields such as authentication codes [8], secret sharing schemes [9–13], association schemes [14], strongly walk-regular graphs [15, 16], and design of frequency hopping sequences [17]. As we will see, some of the subfield codes are optimal and others have the best known parameters. The duals of the subfield codes are also investigated and found to be almost optimal with respect to the sphere-packing bound.

The second objective is to determine the covering structure for the studied subfield codes. By means of the Ashikhmin–Barg Lemma (see [18]) we show that some of these codes have the important property that all their nonzero codewords are minimal, which is a desirable property that is useful in the design of a secret sharing scheme based on a linear code. Moreover, a specific example of a secret sharing scheme based on one of these subfield codes is given.

Finally, the third objective is to present a class of optimal two-weight linear codes over $\mathbb{F}_q$, achieving the Griesmer bound, whose duals are almost optimal with respect to the sphere-packing bound. This class of codes is obtained by extending some of the optimal three-weight cyclic codes reported in [2]. It is important to highlight that, by means of a different approach, this class of optimal two-weight linear codes was also obtained very recently in [19, Theorem 6.3]. Furthermore, it is shown that these optimal codes can be used to construct strongly regular graphs.

This work is organized as follows: In Sect. 2, we fix some notation and recall some definitions and some known results to be used in subsequent sections. Section 3 is devoted to presenting preliminary results. In Sect. 4 we determine the subfield codes of a subclass of already known optimal three-weight cyclic codes. In Sect. 5, we investigate the covering structure for the studied subfield codes and present a specific example of a secret sharing scheme based on one of these codes. In Sect. 6, a class of optimal two-weight linear codes over any finite field whose duals are almost optimal is presented. Moreover, it is shown that these codes can be used to construct strongly regular graphs. Finally, Sect. 7 is devoted to conclusions.

2 Notation, Definitions and Known Results

Unless otherwise specified, throughout this work we will use the following:
Notation. Let $q_0 = p^t$, where t is a positive integer and p is a prime number. For an integer $r > 1$ we are going to fix $q = q_0^r = p^{tr}$. For an integer $k > 1$, let $\mathbb{F}_{q^k}$ be the finite extension of degree k of the finite field $\mathbb{F}_q$ and let γ be a primitive element of $\mathbb{F}_{q^k}$. Let F be a finite field of characteristic p and E a finite extension of F. Then we will denote by “$\mathrm{Tr}_{E/F}$" the *trace mapping* from E to F, while “Tr" will denote the *absolute trace mapping* from E to the prime field $\mathbb{F}_p$.

The *weight enumerator* of a linear code $\mathcal{C}$ of length n is defined as $1 + A_1 z + \cdots + A_n z^n$, while the sequence $\{1, A_1, \ldots, A_n\}$ is called its *weight distribution*, where A_i $(1 \le i \le n)$ denotes the number of codewords in $\mathcal{C}$ with Hamming weight i. If $\sharp\{1 \le i \le n : A_i \ne 0\} = M$, then $\mathcal{C}$ is called an *M-weight* code.

Let $\mathcal{C}$ be a linear code of length n over $\mathbb{F}_q$. The dual code, $\mathcal{C}^\perp$, of $\mathcal{C}$ is the linear code defined by

$$\mathcal{C}^\perp := \{\mathbf{v} \in \mathbb{F}_q^n : \langle \mathbf{v}, \mathbf{c} \rangle = 0, \text{ for all } \mathbf{c} \in \mathcal{C}\}$$

where $\langle \cdot, \cdot \rangle$ denotes the standard inner product in the vector space $\mathbb{F}_q^n$. It is known that if $\mathcal{C}$ is an $[n, l]$ linear code, then $\mathcal{C}^\perp$ is an $[n, n-l]$ linear code. Moreover, the linear code $\mathcal{C}$ is said to be *projective* if the minimum Hamming distance of $\mathcal{C}^\perp$ is at least 3. Now, denote by the sequence $\{1, A_1^\perp, \ldots, A_n^\perp\}$ the weight distribution of the dual code $\mathcal{C}^\perp$ and fix $m = n(q-1)$. Then, the first four Pless power moments (see [20, pp. 259-260]) for $\mathcal{C}$ are:

$$\sum_{i=1}^{n} A_i = q^l - 1,$$

$$\sum_{i=1}^{n} i A_i = q^{l-1}(m - A_1^\perp),$$

$$\sum_{i=1}^{n} i^2 A_i = q^{l-2}[m(m+1) - (2(m+1) - q)A_1^\perp + 2A_2^\perp],$$

$$\sum_{i=1}^{n} i^3 A_i = q^{l-3}[m(m(m+3)-q+2)-(3m(m-q+3)+q^2-6q+6)A_1^{\perp} +6(m-q+2)A_2^{\perp}-6A_3^{\perp}]. \tag{1}$$

The Pless power moments relate the weight distribution of a linear code to that of its dual code. In this paper we use these identities to determine, given the weight distribution of a linear code, the minimum Hamming distance of its dual code.

When constructing an $[n, l, d]$ code over $\mathbb{F}_q$, from an economical point of view, it is desirable that its length n be minimal for given values of l, d and q. A lower bound for the length n in terms of these values is as follows (see for example [20, Theorem 2.7.4, p. 81]):

Theorem 1 (Griesmer bound) *Let $\mathcal{C}$ be an $[n, l, d]$ linear code over $\mathbb{F}_q$. Then*

$$n \geq \sum_{i=0}^{l-1} \left\lceil \frac{d}{q^i} \right\rceil$$

where $\lceil x \rceil$ denotes the smallest integer greater than or equal to x.

Another well-known bound for linear codes was given in [21, Theorem 6, p. 19].

Theorem 2 (Sphere-packing bound) *An $[n, l, d]$ linear code over $\mathbb{F}_q$ must satisfy*

$$q^l \left(\sum_{i=0}^{\left\lfloor \frac{d-1}{2} \right\rfloor} (q-1)^i \binom{n}{i} \right) \leq q^n$$

where $\lfloor x \rfloor$ denotes the largest integer less than or equal to x.

The sphere-packing bound is useful, for example, to find out if a code with certain parameters exists. In the present work we use it to determine the maximum value that the minimum Hamming distance of a code can take given its length and dimension.

The *canonical additive character* of $\mathbb{F}_q$ is defined as follows

$$\chi(x) := e^{2\pi\sqrt{-1}\mathrm{Tr}(x)/p} \qquad \text{for all } x \in \mathbb{F}_q.$$

Let $a \in \mathbb{F}_q$. The orthogonality relation for the canonical additive character χ of $\mathbb{F}_q$ is given by (see for example [22, Chapter 5]):

$$\sum_{x \in \mathbb{F}_q} \chi(ax) = \begin{cases} q & \text{if } a = 0, \\ 0 & \text{otherwise.} \end{cases}$$

This property plays an important role in numerous applications of finite fields. Among them, this property is useful for determining the Hamming weight of a given vector over a finite field; for example, if $\mathbf{w}(\cdot)$ stands for the usual Hamming weight function and if $\mathbf{v} = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_q^n$, then

$$\mathbf{w}(\mathbf{v}) = n - \frac{1}{q} \sum_{i=0}^{n-1} \sum_{x \in \mathbb{F}_q} \chi(a_i x). \tag{2}$$

We now recall the class of optimal three-weight cyclic codes for which we are interested in obtaining their subfield and extended codes.

Theorem 3 [2, Theorem 11] *Let e_1 and e_2 be positive integers and let $\mathcal{C}_{(q,k,e_1,e_2)}$ be the cyclic code of length $q^k - 1$ over $\mathbb{F}_q$ given by*

$$\mathcal{C}_{(q,k,e_1,e_2)} = \left\{\mathbf{c}(a, b) : a \in \mathbb{F}_q, b \in \mathbb{F}_{q^k}\right\} \tag{3}$$

where

$$\mathbf{c}(a, b) := \left(a\gamma^{\frac{q^k-1}{q-1}e_1 j} + \mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}\left(b\gamma^{e_2 j}\right)\right)_{j=0}^{q^k-2}.$$

If $\gcd(\frac{q^k-1}{q-1}, e_2) = 1$ and $\gcd(q-1, ke_1 - e_2) = 1$, then $\mathcal{C}_{(q,k,e_1,e_2)}$ is an optimal three-weight $[q^k - 1, k + 1, q^{k-1}(q - 1) - 1]$ cyclic code, achieving the Griesmer bound, with weight enumerator

$$1 + (q - 1)(q^k - 1)z^{q^{k-1}(q-1)-1} + (q^k - 1)z^{q^{k-1}(q-1)} + (q - 1)z^{q^k-1}. \tag{4}$$

In addition, if $q > 2$, its dual code is a $[q^k - 1, q^k - k - 2, 3]$ cyclic code.

Remark 1 In [23, Theorem 1] it was shown that the integers e_1 and e_2 in the previous theorem can be any integers.

Let $\mathcal{C}$ be an $[n, l]$ linear code over $\mathbb{F}_q$. The following describes a way to construct a new $[n, l']$ linear code, $\mathcal{C}^{(q_0)}$, over $\mathbb{F}_{q_0}$ (see [5]). Let G be a generator matrix of $\mathcal{C}$. Take a basis of $\mathbb{F}_q = \mathbb{F}_{q_0^r}$ over $\mathbb{F}_{q_0}$ and represent each entry of G as an $r \times 1$ column vector of $\mathbb{F}_{q_0}^r$ with respect to this basis. Replace each entry of G with the corresponding $r \times 1$ column vector of $\mathbb{F}_{q_0}^r$. With this method, G is modified into an $lr \times n$ matrix over $\mathbb{F}_{q_0}$ generating a new linear code, $\mathcal{C}^{(q_0)}$, over $\mathbb{F}_{q_0}$ of length n, called *subfield code*. It is known that the subfield code $\mathcal{C}^{(q_0)}$ is independent of both the choice of the basis of $\mathbb{F}_q$ over $\mathbb{F}_{q_0}$ and the choice of the generator matrix G of $\mathcal{C}$ (see [5, Theorems 2.1 and 2.6]). Also, it is clear that the dimension l' of $\mathcal{C}^{(q_0)}$ satisfies $l' \leq lr$.

Remark 2 We recall that the *subfield subcode* of a linear code, $\mathcal{C}$, over $\mathbb{F}_q$ is the subset of codewords in $\mathcal{C}$ whose components are all in $\mathbb{F}_{q_0}$ (see for example [20, p. 116]). In consequence, observe that a subfield code and a subfield subcode are different codes in general. In addition, note that the subfield codes defined here are also different from the subfield codes in [24, Subsection 4.1] defined as one-weight irreducible cyclic codes (see Proposition 4.1 therein).

For what follows, we are interested in obtaining the weight distributions for the subfield codes of a subclass of the optimal three-weight cyclic codes in Theorem 3. To that end, the following is a useful result that will allow us to represent the q_0-ary subfield code, $\mathcal{C}^{(q_0)}$, of a q-ary linear code, $\mathcal{C}$, in terms of the trace function.

Lemma 1 [5, Theorem 2.5] *Let $\mathcal{C}$ be an $[n, l]$ linear code over $\mathbb{F}_q$. Let $G = [g_{ij}]_{1\le i\le l, 1\le j\le n}$ be a generator matrix of $\mathcal{C}$. Then, the trace representation of the subfield code $\mathcal{C}^{(q_0)}$ is given by*

$$\mathcal{C}^{(q_0)} := \left\{ \left(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}} \left(\sum_{i=1}^{l} a_i g_{i1} \right), \ldots, \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}} \left(\sum_{i=1}^{l} a_i g_{in} \right) \right) : a_1, \ldots, a_l \in \mathbb{F}_q \right\}.$$

3 Preliminary Results

Throughout this and the next section we are interested in obtaining the weight distributions for the subfield codes of a subclass of the optimal cyclic codes in Theorem 3 when $k = 2$. Thus, for these two sections we fix $k = 2$. That is, $\frac{q^2-1}{q-1} = q + 1$ and $\langle \gamma \rangle = \mathbb{F}_{q^2}^*$.

Note that if $\mathcal{C}_{(q,2,e_1,e_2)}$ is an optimal cyclic code in Theorem 3 then, in accordance with Lemma 1, its subfield code, $\mathcal{C}_{(q,2,e_1,e_2)}^{(q_0)}$, is given by (recall that $q = q_0^r$):

$$\mathcal{C}_{(q,2,e_1,e_2)}^{(q_0)} = \left\{ \mathbf{c}(a, b)^{(q_0)} : a \in \mathbb{F}_q, b \in \mathbb{F}_{q^2} \right\} \tag{5}$$

where

$$\mathbf{c}(a, b)^{(q_0)} := \left(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}} \left(a\gamma^{(q+1)e_1 j} \right) + \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_{q_0}} \left(b\gamma^{e_2 j} \right) \right)_{j=0}^{q^2-2}. \tag{6}$$

Remark 3 Like $\mathcal{C}_{(q,2,e_1,e_2)}$, $\mathcal{C}_{(q,2,e_1,e_2)}^{(q_0)}$ is also a cyclic code of length $q^2 - 1$. Furthermore, if $h_a(x) \in \mathbb{F}_{q_0}[x]$ is the *minimal polynomial* of γ^{-a} (see [21, Ch. 4]) and if d is the smallest positive integer such that $aq_0^d \equiv a \pmod{q^2 - 1}$, then observe that $\deg(h_a(x)) = d$. Therefore, $h_{(q+1)e_1}(x) \neq h_{e_2}(x)$, $h_{(q+1)e_1}(x)h_{e_2}(x)$ is the *parity-check polynomial* of $\mathcal{C}_{(q,2,e_1,e_2)}^{(q_0)}$ (see [21, Ch. 7]), and if l' is its dimension, then $l' = d_1 + d_2$, where d_1 and d_2 are the smallest positive integers such that $(q+1)e_1 q_0^{d_1} \equiv (q+1)e_1 \pmod{q^2 - 1}$ and $e_2 q_0^{d_2} \equiv e_2 \pmod{q^2 - 1}$, respectively (see [22, Part (v) of Theorem 3.33]).

In order to obtain the weight distributions of the subfield codes of the form $\mathcal{C}_{(q,2,e_1,e_2)}^{(q_0)}$, we will need the following preliminary result.

Lemma 2 *Let χ and χ' be the canonical additive characters of $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$, respectively. For $a \in \mathbb{F}_q$ and $b \in \mathbb{F}_{q^2}$, consider the exponential sum*

$$Z(a,b) := \sum_{y\in\mathbb{F}_{q_0}^*} \sum_{x\in\mathbb{F}_{q^2}^*} \chi(yax^{q+1})\chi'(ybx).$$

Then

$$Z(a,b) = \begin{cases} (q_0-1)(q_0^{2r}-1) & \textit{if } a=b=0, \\ -(q_0-1)(q_0^r+1) & \textit{if } a\neq 0 \textit{ and } b=0, \\ -(q_0-1) & \textit{if } a=0 \textit{ and } b\neq 0, \\ -(q_0-1)(q_0^r+1) & \textit{if } (a,b)\neq(0,0) \textit{ and } \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(\frac{b^{q+1}}{a}\right)=0, \\ q_0(q_0^{r-1}-1)+1 & \textit{if } (a,b)\neq(0,0) \textit{ and } \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(\frac{b^{q+1}}{a}\right)\neq 0. \end{cases}$$

Proof Clearly, $Z(0,0) = (q_0-1)(q_0^{2r}-1)$. If $a \neq 0$ and $b=0$, then

$$\begin{aligned} Z(a,0) &= \sum_{y\in\mathbb{F}_{q_0}^*} \sum_{x\in\mathbb{F}_{q^2}^*} \chi(yax^{q+1}) = (q+1)\sum_{y\in\mathbb{F}_{q_0}^*} \sum_{x\in\mathbb{F}_{q}^*} \chi(yax) \\ &= (q+1)\sum_{y\in\mathbb{F}_{q_0}^*}(-1) = -(q+1)(q_0-1) = -(q_0-1)(q_0^r+1). \end{aligned}$$

Further, if $a=0$ and $b\neq 0$,

$$Z(0,b) = \sum_{y\in\mathbb{F}_{q_0}^*} \sum_{x\in\mathbb{F}_{q^2}^*} \chi'(ybx) = \sum_{y\in\mathbb{F}_{q_0}^*}(-1) = -(q_0-1).$$

Now, let φ be the canonical additive character of $\mathbb{F}_{q_0}$ and suppose that $(a,b)\neq(0,0)$. By the transitivity and linearity of the trace function, we have

$$\begin{aligned} Z(a,b) &= \sum_{y\in\mathbb{F}_{q_0}^*} \sum_{x\in\mathbb{F}_{q^2}^*} \varphi\left(y\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(ax^{q+1}\right)\right)\varphi\left(y\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_{q_0}}(bx)\right) \\ &= \sum_{y\in\mathbb{F}_{q_0}^*} \sum_{x\in\mathbb{F}_{q^2}^*} \varphi\left(y\left(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(ax^{q+1}+\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(bx)\right)\right)\right) \\ &= \sum_{y\in\mathbb{F}_{q_0}^*} \sum_{x\in\mathbb{F}_{q^2}^*} \varphi\left(y\left(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(ax^q\left(x+\frac{b^q}{a}\right)+bx\right)\right)\right) \end{aligned}$$

where the last equality holds because $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(bx) = bx + b^q x^q$. Let $B = \mathbb{F}_{q^2} \backslash \{\frac{b^q}{a}\}$. Thus, after applying the variable substitution $x \mapsto w - \frac{b^q}{a}$, we obtain

$$Z(a,b) = \sum_{y \in \mathbb{F}_{q_0}^*} \sum_{w \in B} \varphi\left(y\left(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(a\left(w^q - \frac{b^{q^2}}{a^q}\right)w + b\left(w - \frac{b^q}{a}\right)\right)\right)\right).$$

However, $b^{q^2} = b$ and $a^q = a$. Thus, since $B = \mathbb{F}_{q^2} \setminus \{\frac{b^q}{a}\}$,

$$\begin{aligned}
Z(a,b) &= \sum_{y \in \mathbb{F}_{q_0}^*} \sum_{w \in B} \varphi\left(y\left(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(aw^{q+1} - \frac{b^{q+1}}{a}\right)\right)\right) \\
&= -\sum_{y \in \mathbb{F}_{q_0}^*} \varphi(0) + \sum_{y \in \mathbb{F}_{q_0}^*} \varphi\left(-y\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(\frac{b^{q+1}}{a}\right)\right) \\
&\quad \times \sum_{w \in \mathbb{F}_{q^2}} \varphi\left(y\left(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(aw^{q+1}\right)\right)\right) \\
&= -(q_0 - 1) + \sum_{y \in \mathbb{F}_{q_0}^*} \varphi\left(-y\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(\frac{b^{q+1}}{a}\right)\right) \sum_{w \in \mathbb{F}_{q^2}} \chi\left(yaw^{q+1}\right)
\end{aligned}$$

where χ is the canonical additive character of $\mathbb{F}_q$ (note that $w^{q+1} \in \mathbb{F}_q$). But, since $a, y \neq 0$, we have

$$\begin{aligned}
\sum_{w \in \mathbb{F}_{q^2}} \chi\left(yaw^{q+1}\right) &= 1 + \sum_{w \in \mathbb{F}_{q^2}^*} \chi\left(yaw^{q+1}\right) \\
&= 1 + (q+1) \sum_{w \in \mathbb{F}_q^*} \chi(yaw) = -q.
\end{aligned}$$

Therefore, finally, we obtain

$$\begin{aligned}
Z(a,b) &= -(q_0 - 1) - q \sum_{y \in \mathbb{F}_{q_0}^*} \varphi\left(-y\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(\frac{b^{q+1}}{a}\right)\right) \\
&= \begin{cases} -(q_0 - 1)(q_0^r + 1) & \text{if } \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(\frac{b^{q+1}}{a}\right) = 0, \\ q_0(q_0^{r-1} - 1) + 1 & \text{otherwise.} \end{cases}
\end{aligned}$$

□

4 The Subfield Codes of a Subclass of Optimal Cyclic Codes

By means of the following result we now determine the subfield codes, along with their weight distributions, for a subclass of the optimal three-weight cyclic codes in Theorem 3.

Theorem 4 *Let $r > 1$, e_1 and e_2 be positive integers and let $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$ be the subfield code of length $q_0^{2r} - 1$, over $\mathbb{F}_{q_0}$, given by (5). Assume that $\gcd(q^2 - 1, e_2) = 1$ and $\gcd(q - 1, 2e_1 - e_2) = 1$. Then the following assertions hold true:*

(A) *If $(q - 1)|(q_0 - 1)e_1$, then $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$ is an optimal three-weight cyclic code of length $q_0^{2r} - 1$ and dimension $2r + 1$, over $\mathbb{F}_{q_0}$, that belongs to the class of optimal three-weight cyclic codes in Theorem 3 (therein $k = 2r$ and $q = q_0$).*

(B) *Let $\mathcal{I}$ be an integer such that $\mathcal{I}e_2 \equiv 1 \pmod{q^2 - 1}$. If $(q - 1) \nmid (q_0 - 1)e_1$ and $\mathcal{I}e_1 \equiv 1 \pmod{q - 1}$, then $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$ is a three-weight cyclic code of length $q_0^{2r} - 1$ and dimension $3r$, over $\mathbb{F}_{q_0}$, whose weight enumerator is*

$$\begin{aligned}1 &+ q_0^{r-1}(q_0^{2r} - 1)(q_0 - 1)z^{q_0^{r-1}(q_0^{r+1} - q_0^r - 1)} + (q_0^{2r} - 1)z^{q_0^{2r-1}(q_0 - 1)} \\ &+ q_0^{r-1}(q_0^r - 1)(q_0^r - q_0 + 1)z^{q_0^{r-1}(q_0-1)(q_0^r + 1)}.\end{aligned} \tag{7}$$

In addition, $A_1^{\perp} = A_2^{\perp} = 0$, and

$$A_3^{\perp} = \frac{(q_0^{r+2} - 3q_0^{r+1} + q_0^2 + 3q_0^r - 6q_0 + 6)(q_0^{2r} - 1)(q_0 - 1)}{6}.$$

That is, the dual code, $\mathcal{C}^{(q_0)\perp}_{(q,2,e_1,e_2)}$, of $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$ is a $[q_0^{2r} - 1, q_0^{2r} - 3r - 1, 3]$ cyclic code which is almost optimal with respect to the sphere-packing bound.

Proof First of all, since $\gcd(\frac{q^2-1}{q-1}, e_2) \leq \gcd(q^2 - 1, e_2) = 1$ and $\gcd(q - 1, 2e_1 - e_2) = 1$, observe that $\mathcal{C}_{(q,2,e_1,e_2)}$ indeed belongs to the class of optimal three-weight cyclic codes in Theorem 3 (therein $k = 2$).

Part (A): Let $e_1' = \frac{(q_0-1)e_1}{q-1}$. Clearly $(q + 1)e_1 = \frac{q^2-1}{q_0-1}e_1'$. Let $h_{(q+1)e_1}(x) = h_{\frac{q^2-1}{q_0-1}e_1'}(x)$, $h_{e_2}(x) \in \mathbb{F}_{q_0}[x]$ be the minimal polynomials of $\gamma^{-\frac{q^2-1}{q_0-1}e_1'}$ and γ^{-e_2}, respectively. Hence, in accordance with Remark 3, note that $\deg(h_{(q+1)e_1}(x)) = 1$, because $\frac{q^2-1}{q_0-1}e_1' q_0 \equiv \frac{q^2-1}{q_0-1}e_1' \pmod{q^2 - 1}$. Also, as $\langle\gamma\rangle = \langle\gamma^{-e_2}\rangle = \mathbb{F}^*_{q^2} = \mathbb{F}^*_{q_0^{2r}}$, $\deg(h_{e_2}(x)) = 2r$. In consequence, $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$ has dimension $2r + 1$. In fact, since $\gamma^{(q+1)e_1} = \gamma^{\frac{q_0^{2r}-1}{q_0-1}e_1'} \in \mathbb{F}^*_{q_0}$, note that the code $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$ is given by the set (see (5))

$$\left\{\left(\gamma^{(q+1)e_1 j}\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}(a) + \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_{q_0}}\left(b\gamma^{e_2 j}\right)\right)_{j=0}^{q^2-2} : a \in \mathbb{F}_q, b \in \mathbb{F}_{q^2}\right\}$$

$$= \left\{ \left(a_0 \gamma^{\frac{q_0^{2r}-1}{q_0-1} e_1' j} + \mathrm{Tr}_{\mathbb{F}_{q_0^{2r}}/\mathbb{F}_{q_0}} \left(b\gamma^{e_2 j} \right) \right)_{j=0}^{q_0^{2r}-2} : a_0 \in \mathbb{F}_{q_0}, b \in \mathbb{F}_{q_0^{2r}} \right\}. \quad (8)$$

Clearly $(q_0-1) | (q_0^l - 1)$, for every non-negative integer l (that is, $q_0^l \equiv 1 \pmod{q_0-1}$). Thus, since $\frac{q_0^r-1}{q_0-1} = q_0^{r-1} + q_0^{r-2} + \cdots + q_0 + 1$, $(q_0-1) | (\frac{q_0^r-1}{q_0-1} - r)$. Therefore, as $e_1' = \frac{(q_0-1)e_1}{q_0^r-1}$ and $q-1 = \frac{q_0^r-1}{q_0-1}(q_0-1)$, we have

$$\begin{aligned} \gcd(q_0-1, 2re_1'-e_2) &= \gcd(q_0-1, 2re_1' - e_2 + 2(\frac{q_0^r-1}{q_0-1} - r)e_1') \\ &= \gcd(q_0-1, 2\frac{q_0^r-1}{q_0-1}e_1' - e_2) \\ &= \gcd(q_0-1, 2e_1-e_2) \leq \gcd(q-1, 2e_1-e_2) = 1. \end{aligned}$$

That is, $\gcd(q_0-1, 2re_1'-e_2) = 1$. Moreover, since $\gcd(q^2-1, e_2) = 1$, we also have $\gcd(\frac{q_0^{2r}-1}{q_0-1}, e_2) = 1$. This means, in consequence and in agreement with Theorem 3, that $\mathcal{C}_{(q,2,e_1,e_2)}^{(q_0)}$ is an optimal three-weight cyclic code of length $q_0^{2r}-1$ and dimension $2r+1$ that belongs to such a theorem. In fact, from (8) and (3), note that

$$\mathcal{C}_{(q,2,e_1,e_2)}^{(q_0)} = \mathcal{C}_{(q_0,2r,e_1',e_2)},$$

where $e_1' = \frac{(q_0-1)e_1}{q-1}$.

Part (B): Note that, by Remark 3, $\mathcal{C}_{(q,2,e_1,e_2)}^{(q_0)}$ is cyclic. Now, let $h_{(q+1)e_1}(x), h_{e_2}(x) \in \mathbb{F}_{q_0}[x]$ be as before. Since $(q-1) \nmid (q_0-1)e_1$, observe that r is the smallest positive integer such that $(q+1)e_1q_0^r = (q_0^r+1)e_1q_0^r \equiv (q+1)e_1 \pmod{q_0^{2r}-1}$. Thus, $\deg(h_{(q+1)e_1}(x)) = r$, and since $\deg(h_{e_2}(x)) = 2r$, the dimension of $\mathcal{C}_{(q,2,e_1,e_2)}^{(q_0)}$ is $3r$.

Let φ, χ and χ' be the canonical additive characters of $\mathbb{F}_{q_0}$, $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$, respectively. Let $a \in \mathbb{F}_q$, $b \in \mathbb{F}_{q^2}$, and $\mathbf{c}(a,b)^{(q_0)} \in \mathcal{C}_{(q,2,e_1,e_2)}^{(q_0)}$. Hence, from (6) and by the orthogonality relation for the character φ (see (2)), the Hamming weight of the codeword $\mathbf{c}(a,b)^{(q_0)}$, $\mathbf{w}(\mathbf{c}(a,b)^{(q_0)})$, is equal to

$$\begin{aligned} & q^2 - 1 - \frac{1}{q_0} \sum_{y \in \mathbb{F}_{q_0}} \sum_{w \in \mathbb{F}_{q^2}^*} \varphi\left(y \left(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}(aw^{(q+1)e_1}) + \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_{q_0}}\left(bw^{e_2}\right) \right) \right) \\ &= q^2 - 1 - \frac{1}{q_0} \sum_{y \in \mathbb{F}_{q_0}} \sum_{w \in \mathbb{F}_{q^2}^*} \chi(yaw^{(q+1)e_1}) \chi'\left(ybw^{e_2}\right) \\ &= \frac{(q_0-1)(q_0^{2r}-1)}{q_0} - \frac{1}{q_0} \sum_{y \in \mathbb{F}_{q_0}^*} \sum_{w \in \mathbb{F}_{q^2}^*} \chi(yaw^{(q+1)e_1}) \chi'\left(ybw^{e_2}\right). \end{aligned}$$

But $\mathcal{I}e_2 \equiv 1 \pmod{q^2-1}$ and $\mathcal{I}e_1 \equiv 1 \pmod{q-1}$. Thus, after applying the variable substitution $w \mapsto x^{\mathcal{I}}$, we get

$$\begin{aligned}\sum_{y\in\mathbb{F}_{q_0}^*}\sum_{w\in\mathbb{F}_{q^2}^*}\chi(yaw^{(q+1)e_1})\chi'(ybw^{e_2}) &= \sum_{y\in\mathbb{F}_{q_0}^*}\sum_{x\in\mathbb{F}_{q^2}^*}\chi(yax^{(q+1)\mathcal{I}e_1})\chi'(ybx^{\mathcal{I}e_2})\\ &= \sum_{y\in\mathbb{F}_{q_0}^*}\sum_{x\in\mathbb{F}_{q^2}^*}\chi(yax^{(q+1)})\chi'(ybx)\\ &= Z(a,b)\end{aligned}$$

where $Z(a,b)$ is as in Lemma 2. In fact, due to this lemma, we have

$$\mathbf{w}(\mathbf{c}(a,b)^{(q_0)}) = \begin{cases} 0 & \text{if } a=b=0,\\ q_0^{r-1}(q_0-1)(q_0^r+1) & \text{if } a\neq 0 \text{ and } b=0,\\ q_0^{2r-1}(q_0-1) & \text{if } a=0 \text{ and } b\neq 0,\\ q_0^{r-1}(q_0-1)(q_0^r+1) & \text{if } (a,b)\neq(0,0) \text{ and } \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(\frac{b^{q+1}}{a}\right)=0,\\ q_0^{r-1}(q_0^{r+1}-q_0^r-1) & \text{if } (a,b)\neq(0,0) \text{ and } \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(\frac{b^{q+1}}{a}\right)\neq 0,\end{cases}$$

which is in accordance with (7). Now observe that

$$\begin{aligned}A_{q_0^{r-1}(q_0-1)(q_0^r+1)} &= \sharp\{a\in\mathbb{F}_q^*\} + \sharp\{(a,b)\in\mathbb{F}_q^*\times\mathbb{F}_{q^2}^* : \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_{q_0}}\left(\frac{b^{q+1}}{a}\right)=0\}\\ &= (q-1)+(q-1)(q+1)(\frac{q}{q_0}-1)\\ &= q_0^{r-1}(q_0^r-1)(q_0^r-q_0+1).\end{aligned}$$

Similarly, the frequencies of the other weights of $\mathcal{C}_{(q,2,e_1,e_2)}^{(q_0)}$ can be computed and we omit the details here. Then the weight enumerator of $\mathcal{C}_{(q,2,e_1,e_2)}^{(q_0)}$ follows.

Finally, note that $A_1^{\perp}=0$, since otherwise $\mathcal{C}_{(q,2,e_1,e_2)}^{(q_0)}$ would be the null code $\{0\}$. Thus, a direct application of the last two identities in (1) shows that $A_2^{\perp}=0$ and that the value of $A_3^{\perp}$ is the announced one. Lastly, by the sphere-packing bound (see Theorem 2), it is not difficult to verify that for a code of length $q_0^{2r}-1$ and dimension $q_0^{2r}-3r-1$, its minimum Hamming distance can be at most 4. Therefore, the code $\mathcal{C}_{(q,2,e_1,e_2)}^{(q_0)\perp}$ is almost optimal since its minimum Hamming distance is 3. □

Example 1 The following are some examples of Theorem 4.

(a) Let $(q_0,r,e_1,e_2)=(3,2,4,1)$. Then $q=9$ and clearly $(q-1)|(q_0-1)e_1$. Thus, owing to Part (A) of Theorem 4, the subfield code $\mathcal{C}_{(9,2,4,1)}^{(3)}=\mathcal{C}_{(3,4,1,1)}$ is an optimal three-weight cyclic code of length 80 and dimension 5, over $\mathbb{F}_3$, whose weight enumerator is

$$1+160z^{53}+80z^{54}+2z^{80}.$$

(b) Let $(q_0, r, e_1, e_2) = (2, 2, 1, 1)$. Then $q = 4$, $\mathcal{I} = 1$, and clearly $(q-1) \nmid (q_0 - 1)e_1$. Thus, owing to Part (B) of Theorem 4, the subfield code $\mathcal{C}^{(2)}_{(4,2,1,1)}$ is a binary three-weight $[15, 6, 6]$ cyclic code with weight enumerator

$$1 + 30z^6 + 15z^8 + 18z^{10}$$

while its dual code is an almost optimal $[15, 9, 3]$ cyclic code with respect to the sphere-packing bound, with $A_1^{\perp} = A_2^{\perp} = 0$ and $A_3^{\perp} = 5$.

(c) Let $(q_0, r, e_1, e_2) = (3, 2, 1, 1)$. Then $q = 9$, $\mathcal{I} = 1$, and clearly $(q-1) \nmid (q_0 - 1)e_1$. Thus, owing to Part (B) of Theorem 4, the subfield code $\mathcal{C}^{(3)}_{(9,2,1,1)}$ is a three-weight $[80, 6, 51]$ cyclic code over $\mathbb{F}_3$ with weight enumerator

$$1 + 480z^{51} + 80z^{54} + 168z^{60}$$

while its dual code is an almost optimal $[80, 74, 3]$ cyclic code with respect to the sphere-packing bound, with $A_1^{\perp} = A_2^{\perp} = 0$ and $A_3^{\perp} = 640$.

(d) Let $(q_0, r, e_1, e_2) = (2, 4, 2, 2)$. Then $q = 16$ and $\mathcal{I} = 128$. Clearly $(q-1) \nmid (q_0 - 1)e_1$ and $\mathcal{I}e_1 \equiv 1 \pmod{q-1}$. Thus, owing to Part (B) of Theorem 4, the subfield code $\mathcal{C}^{(2)}_{(16,2,2,2)}$ is a binary three-weight $[255, 12, 120]$ cyclic code with weight enumerator

$$1 + 2040z^{120} + 255z^{128} + 1800z^{136}$$

while its dual code is an almost optimal $[255, 243, 3]$ cyclic code with respect to the sphere-packing bound, with $A_1^{\perp} = A_2^{\perp} = 0$ and $A_3^{\perp} = 595$.

Remark 4 According to the code tables at [25], note that the $[15, 6, 6]$ code in (b) is optimal, while the $[80, 6, 51]$ code in (c) and its dual code are optimal. Finally, the $[255, 12, 120]$ code in (d) has the best known parameters.

By fixing $k = 2$, it is important to observe that the condition on the integer e_2 is more restrictive in Theorem 4 ($\gcd(q^2 - 1, e_2) = 1$) than in Theorem 3 ($\gcd(q + 1, e_2) = 1$). This implies, of course, that Theorem 4 can only determine the subfield codes for a subclass of the optimal three-weight cyclic codes in Theorem 3. Specifically, this means that there are optimal three-weight cyclic codes in Theorem 3, whose subfield codes cannot be described through Theorem 4. For example, with the help of a computer, it is not difficult to verify that the subfield code $\mathcal{C}^{(2)}_{(4,2,1,3)}$ is a four-weight binary cyclic code with weight enumerator $1 + 25z^6 + 30z^8 + 3z^{10} + 5z^{12}$ (for this example note that $\gcd(q+1, e_2) = 1$, but $\gcd(q^2-1, e_2) \neq 1$). This subfield code, like the subfield code in (b) Example 1, is optimal. However, unlike the dual of $\mathcal{C}^{(2)}_{(4,2,1,1)}$, the dual of $\mathcal{C}^{(2)}_{(4,2,1,3)}$ is a binary optimal cyclic code with parameters $[15, 9, 4]$. This example let us know that, beyond Theorem 4, there are still other optimal three-weight cyclic codes whose subfield codes have good parameters.

5 The Covering Structure of the Subfield Codes

For any $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_{q_0}^n$, the *support* of $\mathbf{c}$ is defined by the set $\{i : 0 \leq i \leq n-1, c_i \neq 0\}$. Furthermore, for any two vectors $\mathbf{c}, \mathbf{c}' \in \mathbb{F}_{q_0}^n$, $\mathbf{c}$ is said to *cover* $\mathbf{c}'$ if the support of $\mathbf{c}$ contains that of $\mathbf{c}'$. A nonzero codeword is called a *minimal codeword* if it covers only its multiples in a linear code. The set of all minimal codewords in a linear code is called the *covering structure* of the code.

Determining the covering structure of a linear code is in general a difficult but at the same time interesting problem as it is closely related to the construction of secret sharing schemes (see for example [9–13]). In this section we determine the covering structure of the subfield codes in Theorem 4. As we will see, some of these codes have the important property that any nonzero codeword is minimal. These codes are suitable for constructing secret sharing schemes with nice access structures. Moreover, we present a specific example of a secret sharing scheme based on one of these subfield codes.

There are several ways to construct secret sharing schemes by using linear codes. One of them was proposed by Massey in [11, 12] and is presented below (see [10, 13]).

Let $\mathcal{C}$ be an $[n, l]$ linear code over $\mathbb{F}_{q_0}$. In the *secret sharing scheme based on a linear code* $\mathcal{C}$, the secret $\mathbf{s}$ is an element of $\mathbb{F}_{q_0}$, which is called the secret space. There is a dealer P_0 and $n-1$ parties $P_1, P_2, \ldots, P_{n-1}$ involved in the secret sharing scheme, the dealer being a trusted person. Let $G^{\perp} = (\boldsymbol{g}_0^{\perp}, \boldsymbol{g}_1^{\perp}, \ldots, \boldsymbol{g}_{n-1}^{\perp})$ be a generator matrix of the dual code, $\mathcal{C}^{\perp}$, of $\mathcal{C}$ such that $\boldsymbol{g}_i^{\perp}$ is the i-th column vector of $G^{\perp}$ and $\boldsymbol{g}_i^{\perp} \neq 0$ for $0 \leq i \leq n-1$. Then, the secret sharing scheme based on $\mathcal{C}$ is described as follows:

Step 1) In order to compute the shares with respect to a secret $\mathbf{s}$, the dealer P_0 chooses randomly a vector $\boldsymbol{u} = (u_0, u_1, \ldots, u_{n-l-1}) \in \mathbb{F}_{q_0}^{n-l}$ such that $\mathbf{s} = \boldsymbol{u}\boldsymbol{g}_0^{\perp}$. There are altogether q_0^{n-l-1} such vectors $\boldsymbol{u} \in \mathbb{F}_{q_0}^{n-l}$.

Step 2) The dealer P_0 treats $\boldsymbol{u}$ as an information vector and computes the corresponding codeword $\boldsymbol{t} = \boldsymbol{u}G^{\perp} = (t_0, t_1, \ldots, t_{n-1})$ in $\mathcal{C}^{\perp}$. Then he sends t_i to party P_i as the share for every i $(1 \leq i \leq n-1)$.

Step 3) The secret $\mathbf{s}$ is recovered as follows: since $t_0 = \boldsymbol{u}\boldsymbol{g}_0^{\perp} = \mathbf{s}$, a set of shares $\{t_{i_1}, t_{i_2}, \ldots, t_{i_m}\}$ can determine the secret $\mathbf{s}$ iff $\boldsymbol{g}_0^{\perp}$ is a linear combination of $\{\boldsymbol{g}_{i_1}^{\perp}, \boldsymbol{g}_{i_2}^{\perp}, \ldots, \boldsymbol{g}_{i_m}^{\perp}\}$, where $1 \leq i_1 < i_2 < \cdots < i_m \leq n-1$.

Clearly, if a group of participants $\mathcal{D}$ can recover the secret by combining their shares, then any group of participants containing $\mathcal{D}$ can also recover the secret. The set $\{i_1, i_2, \ldots, i_m\}$ is said to be a *minimal access set* if it can recover the secret $\mathbf{s}$ but none of its proper subsets can do so. The *access structure* of the secret sharing scheme refers to the set of all minimal access sets.

For a linear code $\mathcal{C}$, the following lemma from [11] presents a one-to-one correspondence between the set of minimal access sets of the secret sharing scheme based on $\mathcal{C}$ and the set of minimal codewords in $\mathcal{C}$ whose first coordinate is 1.

Lemma 3 *Let $\mathcal{C}$ be an $[n, l]$ linear code over $\mathbb{F}_{q_0}$. Then, the set $\{i_1, i_2, \ldots, i_m\} \subseteq \{1, 2, \ldots, n-1\}$ with $i_1 < i_2 < \cdots < i_m$ is a minimal access set in the secret sharing* *scheme based on $\mathcal{C}$ iff there is a minimal codeword* $\mathbf{c} = \{c_0, c_1, \ldots, c_{n-1}\}$ *in $\mathcal{C}$ such that the support of* $\mathbf{c}$ *is* $\{0, i_1, i_2, \ldots, i_m\}$ *and* $c_0 = 1$.

If $\mathbf{c}$ is a nonzero codeword whose first coordinate is 1 and the support of the codeword $\mathbf{c}$ is $\{0, i_1, i_2, \ldots, i_m\}$ such that $1 \leq i_1 < i_2 < \cdots < i_m \leq n-1$, we call the set $\{i_1, i_2, \ldots, i_m\}$ the *access support* of the codeword $\mathbf{c}$.

From the discussion above, determining the access structure of the secret sharing scheme based on a linear code $\mathcal{C}$ is equivalent to determining the set of access supports of the minimal codewords in $\mathcal{C}$ whose first coordinate is 1. Thus, in the following we determine the covering structure of the subfield codes in Theorem 4. To that end, the next results found in [18] will be useful.

Lemma 4 *Let $\mathcal{C}$ be a linear code over $\mathbb{F}_{q_0}$ with minimum Hamming distance d. Then, every codeword whose weight is less than or equal to $\frac{dq_0-q_0+1}{q_0-1}$ must be a minimal codeword.*

The following lemma states that if the weights of a linear code are close enough to each other, then all nonzero codewords of the code are minimal.

Lemma 5 (Ashikhmin–Barg Lemma) *Let $\mathcal{C}$ be an $[n, l]$ linear code over $\mathbb{F}_{q_0}$, and let $\mathbf{w}_{\min}$ and $\mathbf{w}_{\max}$ be the minimum and maximum nonzero weights of $\mathcal{C}$, respectively. If*

$$\frac{\mathbf{w}_{\min}}{\mathbf{w}_{\max}} > \frac{q_0-1}{q_0}$$

then all nonzero codewords of $\mathcal{C}$ are minimal.

We remark that the condition in the previous lemma is only a sufficient condition. There are codes such that all their nonzero codewords are minimal without satisfying this condition (see for example [13]).

Now, we are able to give the covering structure of the subfield codes in Theorem 4:

Theorem 5 *Assume the same notation as in Theorem 4. Then the covering structure of a subfield code of the form $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$ is as follows:*

(a) *If $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$ belongs to Part* (A) *of Theorem 4, then all its nonzero codewords with weight $q_0^{2r}-1$ are not minimal, while the other nonzero codewords are minimal.*
(b) *If $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$ belongs to Part* (B) *of Theorem 4, then all its nonzero codewords are minimal.*

Proof Part (a): Clearly, all nonzero codewords with weight $q_0^{2r}-1$ are not minimal as the length of $\mathcal{C}^{(q_0)}_{(q,2,e_1,e_2)}$ is $q_0^{2r}-1$ (see Theorem 4). Now, since $2r > 2$, it is not difficult to verify that

$$q_0^{2r-1}(q_0-1) \leq \frac{q_0^{2r+1} - q_0^{2r} - 2q_0 + 1}{q_0-1}.$$

Thus, since $q_0^{2r-1}(q_0-1)-1 < q_0^{2r-1}(q_0-1)$, it follows from Lemma 4 that the assertion in Part (a) holds.

Part (b): Let $\mathbf{w}_{\min}$ and $\mathbf{w}_{\max}$ be as in Lemma 5. Thus, by (7), $\mathbf{w}_{\min} = q_0^{r-1}(q_0^{r+1} - q_0^r - 1)$ and $\mathbf{w}_{\max} = q_0^{r-1}(q_0-1)(q_0^r+1)$. The result now follows directly from Lemma 5. □

Linear codes whose nonzero codewords are all minimal are suitable for constructing secret sharing schemes with nice access structures as described in the following:

Proposition 1 [13, Proposition 2] *Let $\mathcal{C}$ be an $[n, l]$ linear code over $\mathbb{F}_{q_0}$ and let $G = (\boldsymbol{g}_0, \boldsymbol{g}_1, \ldots, \boldsymbol{g}_{n-1})$ be a generator matrix of $\mathcal{C}$ such that $\boldsymbol{g}_i$ is the i-th column vector of G and $\boldsymbol{g}_i \neq 0$ for $0 \leq i \leq n-1$. If each nonzero codeword of $\mathcal{C}$ is minimal, then the access structure of the secret sharing scheme based on $\mathcal{C}$ is composed of q_0^{l-1} minimal access sets, which is equal to the set of access supports of the nonzero codewords in $\mathcal{C}$ with first coordinate* 1. *In addition, we have the following:*

(a) *If $\boldsymbol{g}_i$ is a scalar multiple of $\boldsymbol{g}_0$, $1 \leq i \leq n-1$, then participant P_i must be in every minimal access set. Such a participant is called a* dictatorial participant.
(b) *If $\boldsymbol{g}_i$ is not a scalar multiple of $\boldsymbol{g}_0$, $1 \leq i \leq n-1$, then participant P_i must be in $(q_0-1)q_0^{l-2}$ out of q_0^{l-1} minimal access sets.*

We end this section by presenting a specific example of a secret sharing scheme based on one of the subfield codes in Theorem 4.

Example 2 Let $(q_0, r, e_1, e_2) = (2, 2, 1, 1)$. Then $q = 4$ and by (b) Example 1 we know that the subfield code $\mathcal{C}^{(2)}_{(4,2,1,1)}$ is a binary three-weight [15, 6, 6] cyclic code with weight enumerator $1+30z^6+15z^8+18z^{10}$. We take $\mathbb{F}_{16} = \mathbb{F}_2(\gamma)$ with $\gamma^4+\gamma+1=0$. With this choice, and by using the notation in Remark 3, $h_5(x) = x^2+x+1$ and $h_1(x) = x^4+x^3+1$ (see [21, p. 99]). Therefore, $(x^{15}-1)/h_5(x)h_1(x) = x^9 + x^6+x^5+x^4+x+1$ and $h_5(x)h_1(x) = x^6+x^3+x^2+x+1$ are the generator and parity-check polynomials of $\mathcal{C}^{(2)}_{(4,2,1,1)}$, respectively. In consequence, the generator matrices, G and $G^{\perp}$, for $\mathcal{C}^{(2)}_{(4,2,1,1)}$ and its dual are:

$$G=\begin{bmatrix} 1&1&0&0&1&1&1&0&0&1&0&0&0&0&0\\ 0&1&1&0&0&1&1&1&0&0&1&0&0&0&0\\ 0&0&1&1&0&0&1&1&1&0&0&1&0&0&0\\ 0&0&0&1&1&0&0&1&1&1&0&0&1&0&0\\ 0&0&0&0&1&1&0&0&1&1&1&0&0&1&0\\ 0&0&0&0&0&1&1&0&0&1&1&1&0&0&1 \end{bmatrix}, \quad G^{\perp}=\begin{bmatrix} 0&0&0&0&0&0&0&0&1&0&0&1&1&1&1\\ 0&0&0&0&0&0&0&1&0&0&1&1&1&1&0\\ 0&0&0&0&0&0&1&0&0&1&1&1&1&0&0\\ 0&0&0&0&0&1&0&0&1&1&1&1&0&0&0\\ 0&0&0&0&1&0&0&1&1&1&1&0&0&0&0\\ 0&0&0&1&0&0&1&1&1&1&0&0&0&0&0\\ 0&0&1&0&0&1&1&1&1&0&0&0&0&0&0\\ 0&1&0&0&1&1&1&1&0&0&0&0&0&0&0\\ 1&0&0&1&1&1&1&0&0&0&0&0&0&0&0 \end{bmatrix}.$$

Thus, in the secret sharing scheme based on $\mathcal{C}^{(2)}_{(4,2,1,1)}$, 14 participants and a dealer are involved. Owing to Lemma 3, Part (b) of Theorem 5, and Proposition 1, there are altogether $q_0^{l-1} = 2^5 = 32$ minimal access sets:

{4, 5, 6, 7, 8, 9, 11, 12, 13} {1, 2, 3, 4, 6, 7, 8, 10, 14} {1, 4, 10, 11, 14} {2, 5, 7, 8, 13}

$$\begin{array}{l}
\{2,3,4,6,10,11,12,13,14\}\ \{1,2,3,7,10,11,13\}\ \{5,7,9,12,14\}\ \{6,7,10,11,12\}\\
\{1,2,4,5,6,8,12,13,14\}\ \{1,2,4,8,9,10,11,12,13\}\ \{1,2,5,11,12\}\ \{1,4,5,6,9\}\\
\{1,3,4,5,7,11,12,13,14\}\ \{1,3,4,6,7,9,10,12,13\}\ \{2,4,7,9,10\}\ \{1,6,8,10,13\}\\
\{1,3,7,8,9,10,11,12,14\}\ \{1,2,3,5,6,7,9,13,14\}\ \{2,3,8,10,12\}\ \{3,9,10,13,14\}\\
\{2,3,5,6,8,9,11,12,14\}\ \{2,6,7,8,9,10,11,13,14\}\ \{3,4,5,8,14\}\ \{3,5,6,11,13\}\\
\{1,2,3,4,5,7,8,9,11\}\ \{1,3,5,6,7,8,12\}\ \{3,4,6,8,9,10,11\}\ \{2,4,5,6,7,11,14\}\\
\{4,7,8,10,12,13,14\}\ \{1,2,6,9,10,12,14\}\ \{1,5,8,9,11,13,14\}\ \{2,3,4,5,9,12,13\}\,.
\end{array}$$

Moreover, in accordance with Part (b) of Proposition 1, note that any participant P_i $(1 \leq i \leq 14)$ appears in $(q_0-1)q_0^{l-2} = 16$ out of $q_0^{l-1} = 32$ minimal access sets.

In order to appreciate the use of the previous minimal access sets, suppose that we wish to “split" a 4-bit secret, $\mathbf{s}$, into 4-bit shares for fourteen parties $P_1, P_2, \ldots, P_{14}$. Following [11], $\mathbf{s} \in \mathrm{GF}(2^4) = \mathbb{F}_{16} := \{0,1,2,\ldots,9,a,b,c,d,e,f\}$ and suppose $\mathbf{s} = b = [1011]$. The dealer randomly chooses four codewords $\mathbf{c}_1$, $\mathbf{c}_2$, $\mathbf{c}_3$ and $\mathbf{c}_4$, in the dual code of $\mathcal{C}^{(2)}_{(4,2,1,1)}$, with the condition that each bit in the secret $\mathbf{s}$ matches the first component of one of these four codewords. Suppose that the dealer's choice is:

$$\begin{aligned}
\mathbf{c}_1 &= [100101110111111],\\
\mathbf{c}_2 &= [000000000000000],\\
\mathbf{c}_3 &= [100010111101011],\\
\mathbf{c}_4 &= [110100100100010].
\end{aligned}$$

By means of these codewords the dealer now proceeds to generate the 4-bit shares for the fourteen parties:

$$\begin{array}{ccccccccccccccc}
\boxed{\begin{matrix}1\\0\\1\\1\end{matrix}} & \boxed{\begin{matrix}0\\0\\0\\1\end{matrix}} & \boxed{\begin{matrix}0\\0\\0\\0\end{matrix}} & \boxed{\begin{matrix}1\\0\\0\\1\end{matrix}} & \boxed{\begin{matrix}0\\0\\1\\0\end{matrix}} & \boxed{\begin{matrix}1\\0\\0\\0\end{matrix}} & \boxed{\begin{matrix}1\\0\\1\\1\end{matrix}} & \boxed{\begin{matrix}1\\0\\1\\0\end{matrix}} & \boxed{\begin{matrix}0\\0\\1\\0\end{matrix}} & \boxed{\begin{matrix}1\\0\\1\\1\end{matrix}} & \boxed{\begin{matrix}1\\0\\0\\0\end{matrix}} & \boxed{\begin{matrix}1\\0\\1\\0\end{matrix}} & \boxed{\begin{matrix}1\\0\\0\\0\end{matrix}} & \boxed{\begin{matrix}1\\0\\1\\1\end{matrix}} & \boxed{\begin{matrix}1\\0\\1\\0\end{matrix}}\\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow\\
b & 1 & 0 & 9 & 2 & 8 & b & a & 2 & b & 8 & a & 8 & b & a\\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow\\
\mathbf{s} & P_1 & P_2 & P_3 & P_4 & P_5 & P_6 & P_7 & P_8 & P_9 & P_{10} & P_{11} & P_{12} & P_{13} & P_{14}
\end{array}$$

In this way, the share for party P_1 is 1, the share for party P_2 is 0, and so on. Finally, note that any of the above minimal access sets can recover the secret $\mathbf{s} = b$. For example, by using the shares for the minimal access set $\{1, 4, 5, 6, 9\}$, we get $1+2+8+b+b = b$.

6 A Class of Optimal Two-Weight Linear Codes

Let $\mathcal{C}$ be an $[n, l, d]$ linear code over $\mathbb{F}_q$. The *extended code*, $\widehat{\mathcal{C}}$, of $\mathcal{C}$ is the linear code defined by (see for example [20, p. 14])

$$\widehat{\mathcal{C}} := \left\{(c_1, \ldots, c_{n+1}) \in \mathbb{F}_q^{n+1} : (c_1, \ldots, c_n) \in \mathcal{C} \text{ with } c_1 + \cdots + c_n + c_{n+1} = 0\right\}.$$

It is known that $\widehat{\mathcal{C}}$ is an $[n+1, l, \widehat{d}]$ code, where $\widehat{d} = d$ or $d+1$. Let $\widehat{\mathcal{C}}^{\perp}$ be the dual code of $\widehat{\mathcal{C}}$ and let $\widehat{A}_i$ and $\widehat{A}_i^{\perp}$, with $1 \leq i \leq n+1$, denote the number of codewords with Hamming weight i in $\widehat{\mathcal{C}}$ and $\widehat{\mathcal{C}}^{\perp}$, respectively.

Through the following result we present a class of optimal two-weight linear codes over any finite field whose duals are almost optimal.

Theorem 6 *Let $\widehat{\mathcal{C}}_{(q,k,e_1,e_2)}$ be the extended code of the cyclic code $\mathcal{C}_{(q,k,e_1,e_2)}$ in Theorem 3. If $e_1 = 0$ (see Remark 1), then the extended code $\widehat{\mathcal{C}}_{(q,k,0,e_2)}$ is an optimal two-weight $[q^k, k+1, q^{k-1}(q-1)]$ linear code over $\mathbb{F}_q$, achieving the Griesmer bound, with weight enumerator*

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

In addition, $\widehat{A}_1^{\perp} = \widehat{A}_2^{\perp} = 0$, and

$$\widehat{A}_3^{\perp} = \frac{q^k(q^k-1)(q-1)(q-2)}{6}.$$

Therefore, if $q > 2$, then $\widehat{\mathcal{C}}_{(q,k,0,e_2)}$ is projective and its dual code, $\widehat{\mathcal{C}}^{\perp}_{(q,k,0,e_2)}$, is a $[q^k, q^k - k - 1, 3]$ linear code which is almost optimal with respect to the sphere-packing bound.

Proof Recall that each codeword of the cyclic code $\mathcal{C}_{(q,k,0,e_2)}$ is of the form

$$\mathbf{c}(a,b) = \left(a + \mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}\left(bx^{e_2}\right)\right)_{x \in \mathbb{F}^*_{q^k}}, \quad \text{with } a \in \mathbb{F}_q \text{ and } b \in \mathbb{F}_{q^k}.$$

For each codeword $\mathbf{c}(a,b)$ in $\mathcal{C}_{(q,k,0,e_2)}$, let $\widehat{\mathbf{c}}(a,b)$ denote the corresponding extended codeword in $\widehat{\mathcal{C}}_{(q,k,0,e_2)}$.

In the following we determine the parameters and weight enumerator of $\widehat{\mathcal{C}}_{(q,k,0,e_2)}$. By definition, the extended code $\widehat{\mathcal{C}}_{(q,k,0,e_2)}$ has length $q^k - 1 + 1 = q^k$ and has the same dimension as $\mathcal{C}_{(q,k,0,e_2)}$. Further, in [2, Theorems 7 and 11] it is shown that the Hamming weight of a codeword in $\mathcal{C}_{(q,k,0,e_2)}$ is given by

$$\mathbf{w}(\mathbf{c}(a,b)) = \begin{cases} 0 & \text{if } a = b = 0, \\ q^k - 1 & \text{if } a \neq 0 \text{ and } b = 0, \\ q^{k-1}(q-1) & \text{if } a = 0 \text{ and } b \neq 0, \\ q^{k-1}(q-1) - 1 & \text{if } (a,b) \neq (0,0). \end{cases}$$

Thus, in order to obtain the weight enumerator for $\widehat{\mathcal{C}}_{(q,k,0,e_2)}$ we will compute the sum of coordinates of a codeword $\mathbf{c}(a,b)$ in each of the above cases. First, note that

$$\sum_{x \in \mathbb{F}^*_{q^k}} a = (q^k - 1)a \equiv -a \pmod{q}.$$

Also, since $\gcd(\frac{q^k-1}{q-1}, e_2) = 1$ and $\gcd(q-1, e_2) = 1$, we have that $\gcd(q^k-1, e_2) = 1$. Hence,

$$\sum_{x\in\mathbb{F}_{q^k}^*} \mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}\left(bx^{e_2}\right) = \sum_{x\in\mathbb{F}_{q^k}^*} \mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(bx) = q^{k-1}\sum_{x\in\mathbb{F}_q^*} x = 0.$$

Therefore,

$$\sum_{x\in\mathbb{F}_{q^k}^*}\left(a + \mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}\left(bx^{e_2}\right)\right) = \begin{cases} 0 & \text{if } a = b = 0, \\ -a & \text{if } a \neq 0 \text{ and } b = 0, \\ 0 & \text{if } a = 0 \text{ and } b \neq 0, \\ -a & \text{if } (a, b) \neq (0, 0). \end{cases}$$

Consequently,

$$\mathbf{w}(\widehat{\mathbf{c}}(a, b)) = \begin{cases} 0 & \text{if } a = b = 0, \\ q^k & \text{if } a \neq 0 \text{ and } b = 0, \\ q^{k-1}(q-1) & \text{if } a = 0 \text{ and } b \neq 0, \\ q^{k-1}(q-1) & \text{if } (a, b) \neq (0, 0). \end{cases}$$

Moreover, since $A_{q^k-1} = (q-1)$ (see (4)), we conclude that $\widehat{A}_{q^k} = (q-1)$. Also, as $A_{q^{k-1}(q-1)} = (q^k-1)$ and $A_{q^{k-1}(q-1)-1} = (q^k-1)(q-1)$, we have

$$\widehat{A}_{q^{k-1}(q-1)} = (q^k-1) + (q^k-1)(q-1) = q(q^k-1).$$

This completes the proof of the parameters and weight enumerator of the code $\widehat{\mathcal{C}}_{(q,k,0,e_2)}$.

Now, observe that

$$\left\lceil \frac{q^{k-1}(q-1)}{q^0} \right\rceil + \left\lceil \frac{q^{k-1}(q-1)}{q} \right\rceil + \cdots + \left\lceil \frac{q^{k-1}(q-1)}{q^k} \right\rceil$$
$$= (q^k - q^{k-1}) + (q^{k-1} - q^{k-2}) + \cdots + (q-1) + 1 = q^k$$

which implies that $\widehat{\mathcal{C}}_{(q,k,0,e_2)}$ is optimal as it achieves the Griesmer bound (see Theorem 1).

In addition, a direct application of the last three identities in (1) shows that $\widehat{A}_1^{\perp} = \widehat{A}_2^{\perp} = 0$ and that the value of $\widehat{A}_3^{\perp}$ is the announced one. Clearly, if $q > 2$, then $\widehat{A}_3^{\perp} \neq 0$ and $\widehat{\mathcal{C}}_{(q,k,0,e_2)}$ is a projective code. Finally, by the sphere-packing bound, it is not difficult to verify that for a code of length q^k and dimension $q^k - k - 1$, its minimum Hamming distance can be at most 4. Therefore, the code $\widehat{\mathcal{C}}_{(q,k,0,e_2)}^{\perp}$ is almost optimal. □

Remark 5 A class of optimal projective two-weight linear codes with the same parameters and weight distribution as the codes in Theorem 6 was recently presented in [19, Theorem 6.3]. However, unlike what was done here, this class of codes is obtained by considering a particular type of almost difference sets. Moreover, at the end of [19, Section VI] the author correctly asserts that the extended code of any cyclic code in Theorem 3 has parameters $[q^k, k+1, q^{k-1}(q-1)-1]$ and three nonzero weights. These three-weight codes are not optimal. However, by allowing $e_1 = 0$ in Theorem 3, Theorem 6 shows us that the extended code obtained is a two-weight linear code which results to be optimal.

Example 3 The following are some examples of the previous theorem.

(a) Let $(q, k, e_2) = (3, 2, 1)$. Thus, owing to Theorem 6, the extended code $\widehat{\mathcal{C}}_{(3,2,0,1)}$ is an optimal two-weight $[9, 3, 6]$ linear code over $\mathbb{F}_3$ with weight enumerator

$$1 + 24z^6 + 2z^9$$

on the other hand, its dual code is an almost optimal $[9, 6, 3]$ linear code with respect to the sphere-packing bound, with $\widehat{A}_1^{\perp} = \widehat{A}_2^{\perp} = 0$ and $\widehat{A}_3^{\perp} = 24$.

(b) Let $(q, k, e_2) = (4, 2, 8)$. Thus, owing to Theorem 6, the extended code $\widehat{\mathcal{C}}_{(4,2,0,8)}$ is an optimal two-weight $[16, 3, 12]$ linear code over $\mathbb{F}_4$ with weight enumerator

$$1 + 60z^{12} + 3z^{16}$$

on the other hand, its dual code is an almost optimal $[16, 13, 3]$ linear code with respect to the sphere-packing bound, with $\widehat{A}_1^{\perp} = \widehat{A}_2^{\perp} = 0$ and $\widehat{A}_3^{\perp} = 240$.

(c) Let $(q, k, e_2) = (5, 3, 9)$. Thus, owing to Theorem 6, the extended code $\widehat{\mathcal{C}}_{(5,3,0,9)}$ is an optimal two-weight $[125, 4, 100]$ linear code over $\mathbb{F}_5$ with weight enumerator

$$1 + 620z^{100} + 4z^{125}$$

on the other hand, its dual code is an almost optimal $[125, 121, 3]$ linear code with respect to the sphere-packing bound, with $\widehat{A}_1^{\perp} = \widehat{A}_2^{\perp} = 0$ and $\widehat{A}_3^{\perp} = 31000$.

(d) Let $(q, k, e_2) = (3, 5, 7)$. Thus, owing to Theorem 6, the extended code $\widehat{\mathcal{C}}_{(3,5,0,7)}$ is an optimal two-weight $[243, 6, 162]$ linear code over $\mathbb{F}_3$ with weight enumerator

$$1 + 726z^{162} + 2z^{243}$$

on the other hand, its dual code is an almost optimal $[243, 237, 3]$ linear code with respect to the sphere-packing bound, with $\widehat{A}_1^{\perp} = \widehat{A}_2^{\perp} = 0$ and $\widehat{A}_3^{\perp} = 19602$.

Remark 6 According to the code tables at [25], all the dual codes in the previous example are optimal.

It is well known that projective two-weight linear codes are closely related to finite projective spaces and strongly regular graphs. What is remarkable is that results from one area can immediately be translated into the other two (see [16]). In the following we use the projective two-weight linear codes in Theorem 6 in order to determine the strongly regular graphs associated to them.

A *graph* is a set V of vertices provided with a symmetric relation $\sim$ on V called *adjacency*, such that no $v \in V$ is adjacent to itself. A pair of adjacent vertices $v_1, v_2 \in V$ form an *edge* and, under these conditions, v_1 is said to be a *neighbor* of v_2 and vice versa.

Let N, K, λ and μ be integers. A graph with N vertices is said to be *strongly regular* with parameters (N, K, λ, μ) if it is regular of degree K (that is, each vertex has exactly K neighbors), and any two distinct vertices have λ common neighbors if they are adjacent and μ common neighbors if they are nonadjacent.

Calderbank and Kantor [16] proposed a way to construct strongly regular graphs using projective two-weight linear codes. Let $\mathbf{w}_1$ and $\mathbf{w}_2$ be the weights of a q-ary projective two-weight linear code $\mathcal{C}$ of length n and dimension l with generator matrix G. To $\mathcal{C}$ we associate a graph as follows. Take as vertices the elements of the vector space $\mathbb{F}_q^l$, where two different vertices v_1 and v_2 are adjacent iff $v_1 - v_2$ is a multiple of a column in G. The graph obtained in this way is strongly regular [16, Theorems 3.1 and 3.2] with the following parameters [16, Corollary 3.7]:

$$N = q^l, \ K = n(q-1), \ \mu = \frac{q^2\mathbf{w}_1\mathbf{w}_2}{q^l}$$
$$\lambda = K^2 + 3K - q(\mathbf{w}_1 + \mathbf{w}_2) - Kq(\mathbf{w}_1 + \mathbf{w}_2) + q^2\mathbf{w}_1\mathbf{w}_2.$$

As a direct consequence of the above, we have the following:

Theorem 7 *Assume the same notation as in Theorem 6. If $q > 2$, then the extended code $\widehat{\mathcal{C}}_{(q,k,0,e_2)}$ generates a strongly regular graph with parameters $(q^{k+1}, q^k(q-1), q^k(q-2), q^k(q-1))$.*

We end this section by presenting an example of the construction of a strongly regular graph from one of the extended codes in Theorem 6.

Example 4 Let $(q, k, e_2) = (3, 2, 1)$. By (a) Example 3 we know that the extended code $\widehat{\mathcal{C}}_{(3,2,0,1)}$ is a projective two-weight [9, 3, 6] linear code over $\mathbb{F}_3$. Owing to Theorem 7, the code $\widehat{\mathcal{C}}_{(3,2,0,1)}$ generates a strongly regular graph with parameters (27, 18, 9, 18). In order to construct this graph we need a generator matrix for $\widehat{\mathcal{C}}_{(3,2,0,1)}$. Since $\mathcal{C}_{(3,2,0,1)}$ is cyclic, it is not difficult to verify (see for example [21, Ch. 7, Sec. 3]) that a generator matrix for this code is given by

$$G = \begin{bmatrix} 2\ 1\ 2\ 2\ 0\ 1\ 0\ 0 \\ 0\ 2\ 1\ 2\ 2\ 0\ 1\ 0 \\ 0\ 0\ 2\ 1\ 2\ 2\ 0\ 1 \end{bmatrix}.$$

Moreover, it is known that a generator matrix for $\widehat{\mathcal{C}}_{(3,2,0,1)}$ can be derived from any generator matrix of $\mathcal{C}_{(3,2,0,1)}$ by adding an extra column such that the sum of the elements of each row equals 0. Therefore,

$$\widehat{G} = \begin{bmatrix} 2\ 1\ 2\ 2\ 0\ 1\ 0\ 0\ 1 \\ 0\ 2\ 1\ 2\ 2\ 0\ 1\ 0\ 1 \\ 0\ 0\ 2\ 1\ 2\ 2\ 0\ 1\ 1 \end{bmatrix} \tag{9}$$

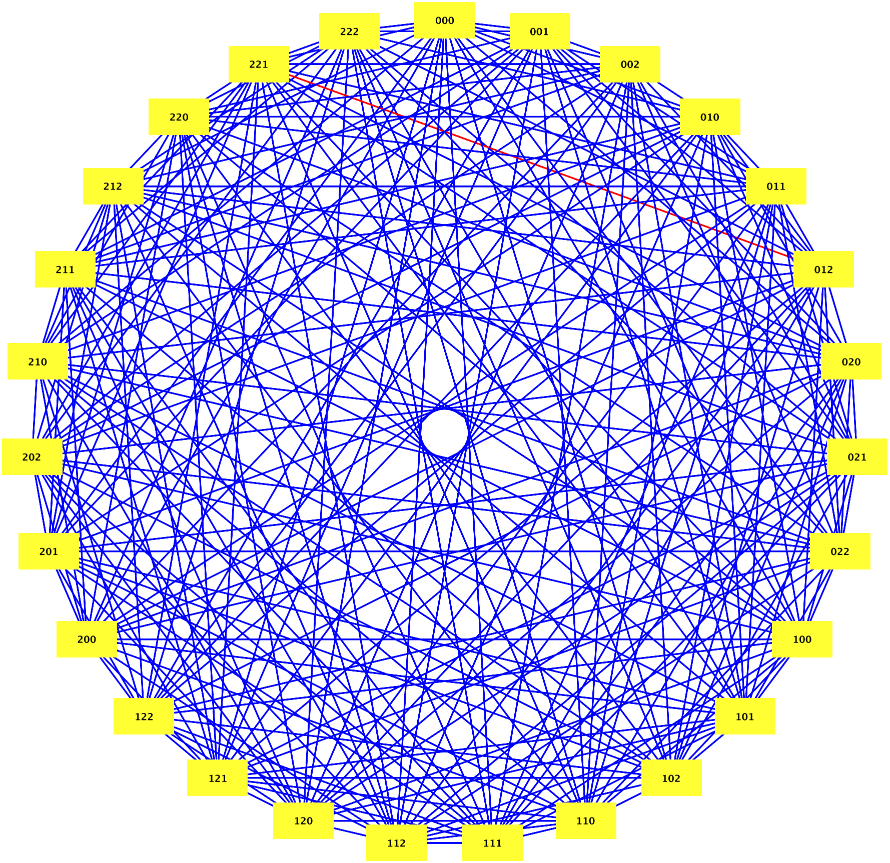

Fig. 1 The (27, 18, 9, 18) strongly regular graph obtained from the extended code $\widehat{\mathcal{C}}_{(3,2,0,1)}$. The vertices 012 and 221 are adjacent or neighbors because $2(012-221) = 212$ appears in the third column of the matrix $\widehat{G}$ in (9). On the contrary, the vertices 012 and 000 are nonadjacent because the difference $012 - 000 = 012$ does not appear as a multiple of a column in such a matrix

is a generator matrix for $\widehat{\mathcal{C}}_{(3,2,0,1)}$.

Following the method described above, the vertices of the graph are the 27 vectors of $\mathbb{F}_3^3 = \{000, 001, 002, \ldots, 222\}$. Further, two different vertices are adjacent iff their difference is a multiple of a column in $\widehat{G}$. Figure 1 shows the strongly regular graph obtained in this way from the extended code $\widehat{\mathcal{C}}_{(3,2,0,1)}$. The graph was plotted using Maple 17.

7 Conclusions

In this paper we studied the q_0-ary subfield codes of a subclass of optimal three-weight cyclic codes of length $q^2 - 1$ and dimension 3 that belongs to the class of codes in Theorem 3. We proved that some of these subfield codes are optimal three-weight cyclic codes of length $q^2 - 1$ and dimension $2r + 1$ (where $q = q_0^r$) that belong, again, to the class of optimal three-weight cyclic codes in Theorem 3 (Part (A) of Theorem 4). For the other subfield codes studied here we showed that they are three-weight cyclic codes of length $q^2 - 1$ whose dimension is now $3r$ (Part (B) of Theorem 4). For the latter subfield codes, we also determined the minimum Hamming distance for their duals, and with this, we concluded that these duals are almost optimal with respect to the sphere-packing bound. Furthermore, it was shown that some subfield codes in Part (B) of Theorem 4 are optimal and others have the best known parameters according to the code tables at [25] (Example 1 and Remark 4). However, as pointed out at the end of Sect. 4, there is evidence of the existence of other subfield codes with good parameters. Therefore, as further work, it would be interesting to study those other subfield codes.

In adittion, as an application of linear codes with few weights, the covering structure of the subfield codes in Theorem 4 was determined (Theorem 5) and used to present a specific example of a secret sharing scheme based on one of these subfield codes at the end of Sect. 5 (Example 2).

Finally, by extending some of the optimal three-weight cyclic codes in Theorem 3, a class of optimal two-weight linear codes over $\mathbb{F}_q$, achieving the Griesmer bound, whose duals are almost optimal with respect to the sphere-packing bound was presented (Theorem 6). Through the analysis of several examples it is suggested that such duals are optimal (Example 3 and Remark 6). We also used the extended codes in Theorem 6 to construct strongly regular graphs (Theorem 7 and Example 4). It is important to note that the parameters and weight distribution of the codes in Theorem 6 are the same as those of a class of codes in Example SU1 in [16] (therein $l = k + 1$ and $t = k$). Also, as pointed out in Remark 5, they are the same for the class of codes in [19, Theorem 6.3]. Thus, as future work, it would be interesting to show if these codes are equivalent to each other.

Author Contributions All authors contributed equally to the conceptualisation, writing, and refinement of this manuscript.

Funding This manuscript is partially supported by PAPIIT-UNAM IN107423. The first author has also received research support from CONAHCyT, México.

Declarations

Conflict of interest Both authors declare that they have no conflict of interest.

References

1. Hernández, F., Vega, G.: On the subfield codes of a subclass of optimal cyclic codes and their covering structures. In: Castañeda, A., Rodríguez-Henríquez, F. (eds.) LATIN 2022: Theoretical Informatics, pp. 255–270. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-20624-5_16
2. Heng, Z., Yue, Q.: Several classes of cyclic codes with either optimal three weights or a few weights. IEEE Trans. Inf. Theory **62**(8), 4501–4513 (2016). https://doi.org/10.1109/TIT.2016.2550029
3. Vega, G.: A characterization of a class of optimal three-weight cyclic codes of dimension 3 over any finite field. Finite Fields Their Appl. **42**, 23–38 (2016). https://doi.org/10.1016/j.ffa.2016.07.001
4. Heng, Z., Wang, Q., Ding, C.: Two families of optimal linear codes and their subfield codes. IEEE Trans. Inf. Theory **66**(11), 6872–6883 (2020). https://doi.org/10.1109/TIT.2020.3006846
5. Ding, C., Heng, Z.: The subfield codes of ovoid codes. IEEE Trans. Inf. Theory **65**(8), 4715–4729 (2019). https://doi.org/10.1109/TIT.2019.2907276
6. Carlet, C., Charpin, P., Zinoviev, V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. **15**, 125–156 (1998). https://doi.org/10.1023/A:1008344232130
7. Heng, Z., Ding, C.: The subfield codes of hyperoval and conic codes. Finite Fields Their Appl. **56**, 308–331 (2019). https://doi.org/10.1016/j.ffa.2018.12.006
8. Ding, C., Wang, X.: A coding theory construction of new systematic authentication codes. Theor. Comput. Sci. **330**(1), 81–99 (2005). https://doi.org/10.1016/j.tcs.2004.09.011
9. Carlet, C., Ding, C., Yuan, J.: Linear codes from perfect nonlinear mappings and their secret sharing schemes. IEEE Trans. Inf. Theory **51**(6), 2089–2102 (2005). https://doi.org/10.1109/TIT.2005.847722
10. Li, C., Qu, L., Ling, S.: On the covering structures of two classes of linear codes from perfect nonlinear functions. IEEE Trans. Inf. Theory **55**(1), 70–82 (2009). https://doi.org/10.1109/TIT.2008.2008145
11. Massey, J.L.: Minimal codewords and secret sharing. In: Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory, pp. 276–279 (1993)
12. Massey, J.L.: Some applications of coding theory in cryptography. In: Codes and Ciphers: Cryptography and Coding IV, pp. 33–47 (1995)
13. Yuan, J., Ding, C.: Secret sharing schemes from three classes of linear codes. IEEE Trans. Inf. Theory **52**(1), 206–212 (2006). https://doi.org/10.1109/TIT.2005.860412
14. Calderbank, A.R., Goethals, J.-M.: Three-weight codes and association schemes. Philips J. Res. **39**(4–5), 143–152 (1984)
15. Shi, M., Solé, P.: Three-weight codes, triple sum sets, and strongly walk regular graphs. Des. Codes Cryptogr. **87**, 2395–2404 (2019). https://doi.org/10.1007/s10623-019-00628-7
16. Calderbank, R., Kantor, W.M.: The geometry of two-weight codes. Bull. Lond. Math. Soc. **18**(2), 97–122 (1986). https://doi.org/10.1112/blms/18.2.97
17. Ding, C., Yin, J.: Sets of optimal frequency-hopping sequences. IEEE Trans. Inf. Theory **54**(8), 3741–3745 (2008). https://doi.org/10.1109/TIT.2008.926410
18. Ashikhmin, A., Barg, A.: Minimal vectors in linear codes. IEEE Trans. Inf. Theory **44**(5), 2010–2017 (1998). https://doi.org/10.1109/18.705584
19. Heng, Z.: Projective linear codes from some almost difference sets. IEEE Trans. Inf. Theory **69**(2), 978–994 (2023). https://doi.org/10.1109/TIT.2022.3203380
20. Huffman, W.C., Pless, V.: Fundamentals of Error-Correcting Codes. Cambridge Univ. Press, Cambridge (2003)
21. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam (1977)
22. Lidl, R., Niederreiter, H.: Finite Fields. Cambridge Univ. Press, Cambridge (1983)
23. Vega, G.: An extended characterization of a class of optimal three-weight cyclic codes over any finite field. Finite Fields Their Appl. **48**, 160–174 (2017). https://doi.org/10.1016/j.ffa.2017.07.010
24. Schmidt, B., White, C.: All two-weight irreducible cyclic codes? Finite Fields Their Appl. **8**(1), 1–17 (2002). https://doi.org/10.1006/ffta.2000.0293
25. Grassl, M.: Bounds on the minimum distance of linear codes and quantum codes. http://www.codetables.de. Accessed 2 Feb 2023