Applicable Algebra in Engineering, Communication and Computing
https://doi.org/10.1007/s00200-024-00653-7

ORIGINAL PAPER

Obtaining new classes of optimal linear codes by puncturing and shortening optimal cyclic codes

Félix Hernández[1] · **Gerardo Vega**[2]

Received: 19 October 2023 / Revised: 20 February 2024 / Accepted: 24 February 2024

Abstract
In this paper we use the puncturing and shortening techniques on two already-known classes of optimal cyclic codes in order to obtain three new classes of optimal linear codes achieving the Griesmer bound. The weight distributions for these codes are settled. We also investigate their dual codes and show that they are either optimal or almost optimal with respect to the sphere-packing bound. Moreover, these duals contain classes of almost maximum distance separable codes which are shown to be proper for error detection. Further, some of the obtained optimal linear codes are suitable for constructing secret sharing schemes with nice access structures.

Keywords Optimal linear codes · Almost MDS codes · Punctured codes · Shortened codes · Griesmer bound

1 Introduction

Let q be a power of a prime number. Denote by $\mathbb{F}_q$ the finite field with q elements. An $[n, k, d]$ linear code, $\mathcal{C}$, over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$ with minimum Hamming distance d. In this context, the vectors of $\mathcal{C}$ are called *codewords*. We index the coordinates of the codewords in $\mathcal{C}$ with the elements in $\{0, 1, \ldots, n-1\}$. The linear code $\mathcal{C}$ is called *cyclic* if $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ implies $(c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$. In addition, $\mathcal{C}$ is called *optimal* if there is no $[n, k, d']$ code over $\mathbb{F}_q$ with $d' > d$ or its parameters meet a bound on linear codes. On the other hand, $\mathcal{C}$ is called *almost*

✉ 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, 04510 Mexico City, Mexico

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

Published online: 06 April 2024

optimal if there is an optimal $[n, k, d+1]$ code over $\mathbb{F}_q$ or $[n, k, d+1]$ meets a bound on linear codes. Further, a linear code with parameters $[n, k, n-k+1]$ is called *maximum distance separable* (MDS for short), while a linear code with parameters $[n, k, n-k]$ is said to be *almost maximum distance separable* (AMDS for short).

It is well known that there are several ways to construct new linear codes from old ones. For example, we can puncture a code or shorten it (see Sect. 2 for definitions), extend it, we can also concatenate two codes or compute the subfield codes of a given code. In fact, many interesting and important codes have arisen by modifying or combining existing codes (see for example [15, 16, 19, 21, 26, 28, 31, 32]). For instance, in [28] the authors studied the subfield codes and the subfield subcodes for a class of MDS codes, obtaining as a result a class of linear complementary dual codes (LCD codes) and a class of codes supporting 3-designs. Also, several new classes of optimal binary linear codes were derived by puncturing some binary linear codes in [31]. Furthermore, by shortening some Hamming, Simplex, Reed-Muller, and ovoid codes, eleven classes of optimal linear codes were presented in [21].

Recently, a class of optimal three-weight cyclic codes over $\mathbb{F}_q$ achieving the Griesmer bound was presented in [18, Theorem 11]. On the other hand, a class of optimal five-weight cyclic codes over $\mathbb{F}_q$ whose duals are also optimal was reported in [16, Theorem 6]. Shortly thereafter this class of codes was enlarged in [30, Theorem 2]. In fact, the subfield and extended codes for these classes of optimal three- and five-weight cyclic codes were investigated in [19] and [16], respectively, showing that some of the resulting codes are optimal or have the best known parameters.

In this paper we use the puncturing and shortening techniques on the optimal three- and five-weight cyclic codes presented in [18, Theorem 11] and [30, Theorem 2] in order to obtain three classes of optimal linear codes achieving the Griesmer bound. The weight distributions for these codes are settled using Prange's Theorem (see Theorem 4 below). It turns out that the studied codes have two, four, five or six 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 [9], secret sharing schemes [19, 23, 33], combinatorial designs [6], association schemes [4], design of frequency hopping sequences [10], strongly regular graphs [5, 19] and strongly walk-regular graphs [25]. In fact, optimal linear codes with few weights have been reported in [2–4, 6–8, 13, 16–18, 25, 31] and more recently in [14, 15, 19, 23, 24, 28, 30, 32, 34]. Thus, in the context of such reported codes, the codes presented here are new. The duals of the three classes of optimal linear codes are also investigated and it is shown that they are either optimal or almost optimal with respect to the sphere-packing bound. Moreover, these duals contain classes of AMDS codes which are shown to be proper for error detection. Further, some of the obtained optimal linear codes are suitable for constructing secret sharing schemes with nice access structures.

This paper is organized as follows: In Sect. 2 we establish the notation, give some definitions and recall some known results. In particular we recall two already-known classes of optimal cyclic codes over any finite field. In Sects. 3 and 4 we use the puncturing and shortening techniques on the optimal cyclic codes presented in Sect. 2 in order to obtain three new classes of optimal linear codes whose duals are either optimal or almost optimal. Examples of such codes are given. Finally, Sect. 5 is devoted to conclusions.

2 Notation, definitions and known results

Throughout this work we use the following:

Notation. Let $\mathbb{F}_q$ be as before. For an integer $m \geq 2$, let $\mathbb{F}_{q^m}$ be the finite extension of degree m of the finite field $\mathbb{F}_q$. Denote by $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ the trace function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$. The *weight enumerator* of a linear code $\mathcal{C}$ of length n is defined as the polynomial $\sum_{j=0}^{n} A_j(\mathcal{C})z^j$, while the vector $(A_j(\mathcal{C}))_{j=0}^{n}$ is called its *weight distribution*, where $A_j(\mathcal{C})$, with $0 \leq j \leq n$, denotes the number of codewords in $\mathcal{C}$ with Hamming weight j. If $\sharp\{1 \leq j \leq n : A_j(\mathcal{C}) \neq 0\} = M$, 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 $[n, k]$ linear code, then $\mathcal{C}^{\perp}$ is an $[n, n-k]$ linear code. Let $(A_j(\mathcal{C}^{\perp}))_{j=0}^{n}$ be the weight distribution of $\mathcal{C}^{\perp}$, then the first five Pless power moments (see [20, pp. 259–260]) for $\mathcal{C}$ are:

$$\sum_{j=0}^{n} A_j(\mathcal{C}) = q^k ,$$

$$\sum_{j=0}^{n} jA_j(\mathcal{C}) = q^{k-1}(qn - n - A_1(\mathcal{C}^{\perp})) ,$$

$$\begin{aligned}\sum_{j=0}^{n} j^2A_j(\mathcal{C}) = q^{k-2}[&(q-1)n(qn-n+1) - (2qn - q - 2n + 2)A_1(\mathcal{C}^{\perp}) \\ &+ 2A_2(\mathcal{C}^{\perp})] ,\end{aligned}$$

$$\begin{aligned}\sum_{j=0}^{n} j^3A_j(\mathcal{C}) = q^{k-3}[&(q-1)n(q^2n^2 - 2qn^2 + 3qn - q + n^2 - 3n + 2) - (3q^2n^2 \\ &- 3q^2n - 6qn^2 + 12qn + q^2 - 6q + 3n^2 - 9n + 6)A_1(\mathcal{C}^{\perp}) \\ &+ 6(qn - q - n + 2)A_2(\mathcal{C}^{\perp}) - 6A_3(\mathcal{C}^{\perp})] ,\end{aligned}$$

$$\begin{aligned}\sum_{j=0}^{n} j^4A_j(\mathcal{C}) = q^{k-4}[&(q-1)n(q^3n^3 - 3q^2n^3 + 6q^2n^2 - 4q^2n + q^2 + 3qn^3 \\ &- 12qn^2 + 15qn - 6q - n^3 + 6n^2 - 11n + 6) - (4q^3n^3 - 6q^3n^2 \\ &+ 4q^3n - q^3 - 12q^2n^3 + 36q^2n^2 - 38q^2n + 14q^2 + 12qn^3 \\ &- 54qn^2 + 78qn - 36q - 4n^3 + 24n^2 - 44n + 24)A_1(\mathcal{C}^{\perp}) \\ &+ (12q^2n^2 - 24q^2n + 14q^2 - 24qn^2 + 84qn - 72q + 12n^2 \\ &- 60n + 72)A_2(\mathcal{C}^{\perp}) - (24qn - 36q - 24n + 72)A_3(\mathcal{C}^{\perp}) \\ &+ 24A_4(\mathcal{C}^{\perp})] .\end{aligned}$$

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

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

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

$$n \geq \sum_{j=0}^{k-1} \left\lceil \frac{d}{q^j} \right\rceil,$$

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

Another well-known bound for linear codes is [20, Theorem 1.12.1]:

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

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

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.

There are several ways to construct new codes from old ones (see [20, Section 1.5]). In the following we recall two of these techniques.

Let $\mathcal{C}$ be a linear code of length n over $\mathbb{F}_q$ and i an integer such that $0 \leq i \leq n-1$. We *puncture* the code $\mathcal{C}$ by deleting the i-th coordinate from each codeword. The resulting code is linear, of length $n-1$ and is denoted by $\mathcal{C}^i$. On the other hand, we *shorten* the code $\mathcal{C}$ by selecting only those codewords having a zero as their i-th component and deleting the i-th component from these codewords. The resulting code is linear, of length $n-1$ and is denoted by $\mathcal{C}_i$.

Remark 1 Let $\mathcal{C}$, $\mathcal{C}^i$ and $\mathcal{C}_i$ be as before. Thus, since $(\mathcal{C}^\perp)^i = (\mathcal{C}_i)^\perp$ (see [20, Theorem 1.5.7 (i)]) and $(\mathcal{C}^\perp)^\perp = \mathcal{C}$, we have that $((\mathcal{C}^\perp)^i)^\perp = \mathcal{C}_i$.

The parameters of a punctured code can be obtained through the following result:

Theorem 3 ([20, Theorem 1.5.1]) *Let $\mathcal{C}$ be an $[n, k, d]$ linear code over $\mathbb{F}_q$ and i an integer such that $0 \leq i \leq n-1$. Let $\mathcal{C}^i$ be the punctured code of $\mathcal{C}$ whose i-th*

coordinate is deleted. If $d > 1$, then $\mathcal{C}^i$ is an $[n-1, k, d^*]$ code where $d^* = d-1$ if $\mathcal{C}$ has a minimum weight codeword with a nonzero i-th coordinate and $d^* = d$ otherwise.

Remark 2 From the previous theorem, it is important to stress that the dimension k, for the two linear codes $\mathcal{C}$ and $\mathcal{C}^i$, remains unchanged.

When certain uniformity conditions hold, the weight distribution of a punctured or shortened code can be determined from the weight distribution of the original code. In order to recall that, let $\mathcal{C}$ be an $[n, k]$ linear code over $\mathbb{F}_q$ and let $\mathcal{M}$ be the $q^k \times n$ matrix whose rows are all codewords in $\mathcal{C}$. Let $\mathcal{M}_j$ be the submatrix of $\mathcal{M}$ consisting of the codewords of weight j. Then we say that the code $\mathcal{C}$ is *homogeneous* provided that for $0 \le j \le n$, each column of $\mathcal{M}_j$ has the same weight (see [20, Sec. 7.6]). Prange proved the following result on homogeneous codes [20, Theorem 7.6.1]:

Theorem 4 (Prange) *Let $\mathcal{C}$ be a homogeneous $[n, k, d]$ linear code over $\mathbb{F}_q$, with $d > 1$, and i an integer such that $0 \le i \le n-1$. Let $\mathcal{C}^i$ and $\mathcal{C}_i$ be the linear codes obtained from the code $\mathcal{C}$ by puncturing and shortening on the i-th coordinate, respectively. Then for $0 \le j \le n-1$ we have*:

$$A_j(\mathcal{C}^i) = \frac{n-j}{n} A_j(\mathcal{C}) + \frac{j+1}{n} A_{j+1}(\mathcal{C}), \quad \text{and} \quad A_j(\mathcal{C}_i) = \frac{n-j}{n} A_j(\mathcal{C}).$$

Let Sym_n denote the *symmetic group* composed of all permutations of the set $\{0, 1, \ldots, n-1\}$. Let $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1}) \in \mathbb{F}_q^n$ and $\sigma \in \mathrm{Sym}_n$. We define $\sigma(\mathbf{v}) \in \mathbb{F}_q^n$ as

$$\sigma(\mathbf{v}) := \left(v_{\sigma(0)}, v_{\sigma(1)}, \ldots, v_{\sigma(n-1)}\right).$$

For a linear code $\mathcal{C}$ of length n, the *permutation automorphism group* of $\mathcal{C}$, $\mathrm{PAut}(\mathcal{C})$, is defined as

$$\mathrm{PAut}(\mathcal{C}) := \left\{\sigma \in \mathrm{Sym}_n \,:\, \sigma(\mathbf{c}) \in \mathcal{C}, \text{ for all } \mathbf{c} \in \mathcal{C}\right\}.$$

Moreover, $\mathrm{PAut}(\mathcal{C})$ is said to be *transitive* if for any two coordinates $i, j \in \{0, 1, \ldots, n-1\}$ there is a permutation $\sigma \in \mathrm{PAut}(\mathcal{C})$ such that $\sigma(i) = j$.

Remark 3 It is known that a linear code $\mathcal{C}$ is homogeneous if $\mathcal{C}$ has a transitive automorphism group (see [20, Exercise 402]).

Now, observe that if $\mathcal{C}$ is cyclic of length n, then by definition of cyclic code, the permutation $\sigma \in \mathrm{Sym}_n$ defined as

$$\sigma := \begin{pmatrix} 0 & 1 & 2 & \cdots & n-2 & n-1 \\ 1 & 2 & 3 & \cdots & n-1 & 0 \end{pmatrix}$$

is an element of $\mathrm{PAut}(\mathcal{C})$. Therefore, note that for any two coordinates $i, j \in \{0, 1, \ldots, n-1\}$ it holds that $\sigma^{j-i}(i) = j$, where the difference $j - i$ must be taken modulo n. This means that $\mathrm{PAut}(\mathcal{C})$ is transitive (see also [22, Sec. II] and [27, Sec. 3.4]), and therefore, in the light of Remark 3, it is important to keep in mind that all cyclic codes are homogeneous.

The fact that cyclic codes are homogeneous is relevant since this property allows us to construct new linear codes from them, either through the puncturing or shortening techniques, whose weight distribution can be obtained immediately through Prange's Theorem. This is, of course, provided that the weight distribution of the original cyclic codes is known. Furthermore if the cyclic codes, from which the punctured and shortened codes are constructed, have good parameters, then there are good chances that the resulting codes will also have good parameters. With this idea in mind, we end this section by recalling two already-known classes of optimal cyclic codes.

Theorem 5 ([18, Theorem 11]) *Let e_1 and e_2 be integers (see [29, Theorem 1]) and let $\mathcal{C}_{(q,m,e_1,e_2)}$ be the cyclic code of length $n = q^m - 1$ over $\mathbb{F}_q$ given by*

$$\mathcal{C}_{(q,m,e_1,e_2)} := \left\{ \left(a x^{\frac{q^m-1}{q-1} e_1} + \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(b x^{e_2}) \right)_{x \in \mathbb{F}_{q^m}^*} : a \in \mathbb{F}_q, b \in \mathbb{F}_{q^m} \right\}.$$

If $\gcd(\frac{q^m-1}{q-1}, e_2) = 1$ and $\gcd(q-1, me_1 - e_2) = 1$, then $\mathcal{C}_{(q,m,e_1,e_2)}$ is an optimal three-weight $[n, m+1, n-q^{m-1}]$ cyclic code, achieving the Griesmer bound, with weight enumerator

$$1 + n(q-1)z^{n-q^{m-1}} + nz^{q^{m-1}(q-1)} + (q-1)z^n. \tag{1}$$

In addition, if $q > 2$, its dual code is an $[n, n-m-1, 3]$ cyclic code.

Recently, a class of optimal five-weight cyclic codes over $\mathbb{F}_q$ whose duals are also optimal was reported in [16, Theorem 6]. Shortly thereafter this class of codes was enlarged in [30, Theorem 2] and is presented below.

Theorem 6 *Let e_1, e_2 and e_3 be integers and let $\mathcal{D}_{(q,e_1,e_2,e_3)}$ be the cyclic code of length $n = q^2 - 1$ over $\mathbb{F}_q$ given by*

$$\mathcal{D}_{(q,e_1,e_2,e_3)} = \left\{ \mathbf{c}(a,b,c) : a, b \in \mathbb{F}_q, c \in \mathbb{F}_{q^2} \right\},$$

where

$$\mathbf{c}(a,b,c) := \left(a x^{(q+1)e_1} + b x^{(q+1)e_2} + \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(c x^{e_3}) \right)_{x \in \mathbb{F}_{q^2}^*}.$$

If $q > 2$, $\gcd(q+1, e_3) = 1$, $\gcd(q-1, e_2 - e_1) = 1$, and $e_3 \equiv e_1 + e_2 \pmod{q-1}$, then $\mathcal{D}_{(q,e_1,e_2,e_3)}$ is an optimal five-weight $[n, 4, n-q-1]$ cyclic code, achieving the Griesmer bound, with weight enumerator

$$1 + (n-q)(q-1)^2 z^{n-q-1} + 2n(q-1)z^{n-q} + nz^{q(q-1)} + n(q-1)z^{n-1} + 2(q-1)z^n. \tag{2}$$

In addition, its dual code is an optimal $[n, n-4, 4]$ *AMDS cyclic code achieving the sphere-packing bound* (*see* [16, *Theorem* 6]).

3 The punctured and shortened codes of a class of optimal three-weight cyclic codes

Through the following result we present two classes of optimal linear codes whose dual codes are either optimal or almost optimal.

Theorem 7 *Let* i *be an integer such that* $0 \le i \le n-1$, *where* $n = q^m - 1$. *Let* $\mathcal{C}^i_{(q,m,e_1,e_2)}$ *and* $\mathcal{C}_{(q,m,e_1,e_2)i}$ *be the linear codes obtained from the cyclic code* $\mathcal{C}_{(q,m,e_1,e_2)}$ *in Theorem* 5 *by puncturing and shortening on the* i*-th coordinate, respectively. If* $q > 2$, *then the following assertions hold true*:

(A) $\mathcal{C}^i_{(q,m,e_1,e_2)}$ is an optimal four-weight $[n-1, m+1, n-q^{m-1}-1]$ linear code over $\mathbb{F}_q$, achieving the Griesmer bound, with weight enumerator

$$1 + (n-q^{m-1})(q-1)z^{n-q^{m-1}-1} + 2q^{m-1}(q-1)z^{n-q^{m-1}} + (q^{m-1}-1)z^{q^{m-1}(q-1)} + (q-1)z^{n-1}. \tag{3}$$

In addition, the dual code, $\mathcal{C}^{i\perp}_{(q,m,e_1,e_2)}$, *of* $\mathcal{C}^i_{(q,m,e_1,e_2)}$ *is an* $[n-1, n-m-2, 3]$ *linear code which is almost optimal with respect to the sphere-packing bound.*

(B) $\mathcal{C}_{(q,m,e_1,e_2)i}$ is an optimal two-weight $[n-1, m, n-q^{m-1}]$ linear code over $\mathbb{F}_q$, achieving the Griesmer bound, with weight enumerator

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

In addition, the dual code, $\mathcal{C}^{\perp}_{(q,m,e_1,e_2)i}$, *of* $\mathcal{C}_{(q,m,e_1,e_2)i}$ *is an optimal* $[n-1, n-m-1, 2]$ *linear code achieving the sphere-packing bound.*

Proof Part (A): Since $\mathcal{C}_{(q,m,e_1,e_2)}$ is cyclic, then by Theorem 3 and the remark after it, the punctured code $\mathcal{C}^i_{(q,m,e_1,e_2)}$ has parameters $[n-1, m+1, n-q^{m-1}-1]$. Consequently, since the minimum Hamming distance of $\mathcal{C}^i_{(q,m,e_1,e_2)}$ is $n - q^{m-1} - 1 = q^{m-1}(q-1) - 2$, we obtain

$$\begin{aligned}
&\left\lceil \frac{q^{m-1}(q-1)-2}{q^0} \right\rceil + \left\lceil \frac{q^{m-1}(q-1)-2}{q^1} \right\rceil + \cdots + \left\lceil \frac{q^{m-1}(q-1)-2}{q^m} \right\rceil ,\\
&= (q^m - q^{m-1} - 2) + (q^{m-1} - q^{m-2}) + (q^{m-2} - q^{m-3}) + \cdots + (q-1) + 1 ,\\
&= q^m - 2 = n - 1 ,
\end{aligned}$$

which implies that $\mathcal{C}^i_{(q,m,e_1,e_2)}$ is optimal as it achieves the Griesmer bound. Again, since $\mathcal{C}_{(q,m,e_1,e_2)}$ is cyclic, it is homogeneous (see Remark 3 and the discussion after it). Thus, by Theorem 4 and (1), we have that $A_j(\mathcal{C}^i_{(q,m,e_1,e_2)}) = 0$, $0 \le j \le n-1$, except for the following cases

$$\begin{aligned}
A_0(\mathcal{C}^i_{(q,m,e_1,e_2)}) &= A_0(\mathcal{C}_{(q,m,e_1,e_2)}) = 1 ,\\
A_{n-q^{m-1}-1}(\mathcal{C}^i_{(q,m,e_1,e_2)}) &= \frac{(n-q^{m-1}-1)+1}{n} A_{n-q^{m-1}}(\mathcal{C}_{(q,m,e_1,e_2)})\\
&= (n-q^{m-1})(q-1) ,\\
A_{n-q^{m-1}}(\mathcal{C}^i_{(q,m,e_1,e_2)}) &= \frac{n-(n-q^{m-1})}{n} A_{n-q^{m-1}}(\mathcal{C}_{(q,m,e_1,e_2)})\\
&\quad + \frac{(n-q^{m-1})+1}{n} A_{q^{m-1}(q-1)}(\mathcal{C}_{(q,m,e_1,e_2)})\\
&= q^{m-1}(q-1) + q^{m-1}(q-1) = 2q^{m-1}(q-1) ,\\
A_{q^{m-1}(q-1)}(\mathcal{C}^i_{(q,m,e_1,e_2)}) &= \frac{n-(q^{m-1}(q-1))}{n} A_{q^{m-1}(q-1)}(\mathcal{C}_{(q,m,e_1,e_2)})\\
&= q^{m-1} - 1 ,\\
A_{n-1}(\mathcal{C}^i_{(q,m,e_1,e_2)}) &= \frac{(n-1)+1}{n} A_n(\mathcal{C}_{(q,m,e_1,e_2)}) = q - 1 ,
\end{aligned}$$

which is in accordance with (3). Then the weight enumerator of $\mathcal{C}^i_{(q,m,e_1,e_2)}$ follows. Now, owing to (3) and the first four Pless power moments, we obtain that $A_j(\mathcal{C}^{i\perp}_{(q,m,e_1,e_2)}) = 0$, for $1 \le j \le 2$, and

$$A_3(\mathcal{C}^{i\perp}_{(q,m,e_1,e_2)}) = \frac{(q-1)(q-2)(q^m-3)(q^m-4)}{6}.$$

Since $q > 2$, $\mathcal{C}^{i\perp}_{(q,m,e_1,e_2)}$ is an $[n-1, n-m-2, 3]$ linear code. Further, by the sphere-packing bound, it is not difficult to verify that for a code of length $n-1$ and dimension $n-m-2$, its minimum Hamming distance can be at most 4. Therefore, the code $\mathcal{C}^{i\perp}_{(q,m,e_1,e_2)}$ is almost optimal.

Part (B): Since $\mathcal{C}^{\perp}_{(q,m,e_1,e_2)}$ is an $[n, n-m-1]$ linear code, we have, thanks to Remark 2, that the punctured code $(\mathcal{C}^{\perp}_{(q,m,e_1,e_2)})^i$ is an $[n-1, n-m-1]$ linear code. On the other hand, by Remark 1, we have that $\mathcal{C}_{(q,m,e_1,e_2)i} = ((\mathcal{C}^{\perp}_{(q,m,e_1,e_2)})^i)^{\perp}$. In consequence, $\mathcal{C}_{(q,m,e_1,e_2)i}$ has length $n-1$ and dimension $n-1-(n-m-1) = m$. Further, as $\mathcal{C}_{(q,m,e_1,e_2)}$ is homogeneous, we obtain by Theorem 4 and (1) that $A_j(\mathcal{C}_{(q,m,e_1,e_2)i}) = 0$, $0 \le j \le n-1$, except for the following cases

$$\begin{aligned} A_0(\mathcal{C}_{(q,m,e_1,e_2)i}) &= A_0(\mathcal{C}_{(q,m,e_1,e_2)}) = 1\ , \\ A_{n-q^{m-1}}(\mathcal{C}_{(q,m,e_1,e_2)i}) &= \frac{n-(n-q^{m-1})}{n} A_{n-q^{m-1}}(\mathcal{C}_{(q,m,e_1,e_2)}) \\ &= q^{m-1}(q-1)\ , \\ A_{q^{m-1}(q-1)}(\mathcal{C}_{(q,m,e_1,e_2)i}) &= \frac{n-(q^{m-1}(q-1))}{n} A_{q^{m-1}(q-1)}(\mathcal{C}_{(q,m,e_1,e_2)}) \\ &= q^{m-1}-1\ , \end{aligned}$$

which is in accordance with (4). Then the weight enumerator of $\mathcal{C}_{(q,m,e_1,e_2)i}$ follows. From such weight enumerator we can see that the minimum Hamming distance of $\mathcal{C}_{(q,m,e_1,e_2)i}$ is $n-q^{m-1} = q^{m-1}(q-1)-1$. Thus, we have

$$\begin{aligned} &\left\lceil \frac{q^{m-1}(q-1)-1}{q^0} \right\rceil + \left\lceil \frac{q^{m-1}(q-1)-1}{q^1} \right\rceil + \cdots + \left\lceil \frac{q^{m-1}(q-1)-1}{q^{m-1}} \right\rceil\ , \\ &= (q^m - q^{m-1} - 1) + (q^{m-1} - q^{m-2}) + (q^{m-2} - q^{m-3}) + \cdots + (q^2 - q) + (q-1), \\ &= q^m - 2 = n - 1\ , \end{aligned}$$

which implies that $\mathcal{C}_{(q,m,e_1,e_2)i}$ is optimal by the Griesmer bound. Furthermore, owing to (4) and the first three Pless power moments, we obtain that $A_1(\mathcal{C}^{\perp}_{(q,m,e_1,e_2)i}) = 0$ and

$$A_2(\mathcal{C}^{\perp}_{(q,m,e_1,e_2)i}) = \frac{(q-1)(q-2)(q^m-3)}{2}.$$

Since $q > 2$, $\mathcal{C}^{\perp}_{(q,m,e_1,e_2)i}$ is an $[n-1, n-m-1, 2]$ linear code. Finally, by the sphere-packing bound, it is not difficult to verify that for a code of length $n-1$ and dimension $n-m-1$, its minimum Hamming distance can be at most 2. Hence, the code $\mathcal{C}^{\perp}_{(q,m,e_1,e_2)i}$ is optimal. □

As particular cases of the previous theorem, the following two classes of AMDS codes are obtained.

Corollary 1 *Assume the same notation as in the previous theorem. If $m = 2$ in Theorem 7, then $\mathcal{C}^{i\perp}_{(q,2,e_1,e_2)}$ is an almost optimal $[n-1, n-4, 3]$ AMDS code and $\mathcal{C}^{\perp}_{(q,2,e_1,e_2)i}$ is an optimal $[n-1, n-3, 2]$ AMDS code.*

Proof Direct from the definition of an AMDS code. □

Example 1 The following are some examples of Theorem 7.

(a) Let $(q, m, e_1, e_2) = (4, 4, 6, 8)$ and i an integer such that $0 \le i \le q^m - 2$. Since $\gcd(\frac{q^m-1}{q-1}, e_2) = 1$ and $\gcd(q-1, me_1 - e_2) = 1$, $\mathcal{C}_{(4,4,6,8)}$ belongs to the class of codes in Theorem 5. Thus, owing to Part (A) of Theorem 7, the punctured

code $\mathcal{C}^{i}_{(4,4,6,8)}$ is an optimal four-weight [254, 5, 190] linear code over $\mathbb{F}_4$ with weight enumerator

$$1 + 573z^{190} + 384z^{191} + 63z^{192} + 3z^{254},$$

while its dual code $\mathcal{C}^{i\perp}_{(4,4,6,8)}$ is an almost optimal [254, 249, 3] linear code with respect to the sphere-packing bound. Furthermore, owing to Part (B) of Theorem 7, the shortened code $\mathcal{C}_{(4,4,6,8)i}$ is an optimal two-weight [254, 4, 191] linear code over $\mathbb{F}_4$ with weight enumerator

$$1 + 192z^{191} + 63z^{192},$$

while its dual code $\mathcal{C}^{\perp}_{(4,4,6,8)i}$ is an optimal [254, 250, 2] linear code.

(b) Let $(q, m, e_1, e_2) = (9, 2, 4, 3)$ and i an integer such that $0 \le i \le q^m - 2$. Since $\gcd(\frac{q^m-1}{q-1}, e_2) = 1$ and $\gcd(q - 1, me_1 - e_2) = 1$, $\mathcal{C}_{(9,2,4,3)}$ belongs to the class of codes in Theorem 5. Thus, owing to Part (A) of Theorem 7 and Corollary 1, the punctured code $\mathcal{C}^{i}_{(9,2,4,3)}$ is an optimal four-weight [79, 3, 70] linear code over $\mathbb{F}_9$ with weight enumerator

$$1 + 568z^{70} + 144z^{71} + 8z^{72} + 8z^{79},$$

while its dual code $\mathcal{C}^{i\perp}_{(9,2,4,3)}$ is an almost optimal [79, 76, 3] AMDS linear code with respect to the sphere-packing bound. Moreover, owing to Part (B) of Theorem 7 and Corollary 1, the shortened code $\mathcal{C}_{(9,2,4,3)i}$ is an optimal two-weight [79, 2, 71] linear code over $\mathbb{F}_9$ with weight enumerator

$$1 + 72z^{71} + 8z^{72},$$

while its dual code $\mathcal{C}^{\perp}_{(9,2,4,3)i}$ is an optimal [79, 77, 2] AMDS linear code.

Remark 4 According to the code tables at [12], the dual codes [254, 249, 3] and [79, 76, 3] obtained through Part (A) of Theorem 7 are optimal.

We end this section by showing that the shortened codes in Part (B) of Theorem 7 are minimal. To achieve this, we must first recall what a minimal code is.

For any $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n$, the *support* of $\mathbf{c}$ is defined by the set $\{j : 0 \le j \le n - 1, c_j \ne 0\}$. Furthermore, for any two vectors $\mathbf{c}, \mathbf{c}' \in \mathbb{F}_q^n$, $\mathbf{c}$ is said to *cover* $\mathbf{c}'$ if the support of $\mathbf{c}$ contains that of $\mathbf{c}'$. A nonzero codeword is called *minimal* if it covers only its multiples in a linear code. A linear code is said to be *minimal* if every codeword is minimal.

Minimal linear codes are of interest since these codes are suitable for constructing secret sharing schemes with nice access structures (see for example [19, 23, 33]). Ashikhmin and Barg [1] proved that a sufficient condition for a linear code $\mathcal{C}$ over $\mathbb{F}_q$ to be minimal is that

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

where $\mathbf{w}_{\min}$ and $\mathbf{w}_{\max}$ denote the minimum and maximum nonzero weights in $\mathcal{C}$, respectively. Thus, since

$$\frac{q^{m-1}(q-1)-1}{q^{m-1}(q-1)} > \frac{q-1}{q},$$

we have that any shortened two-weight code $\mathcal{C}_{(q,m,e_1,e_2)i}$, obtained from Part (B) of Theorem 7, is minimal.

4 The punctured codes of a class of optimal five-weight cyclic codes

By means of the following result we present a class of optimal linear codes whose duals are not only optimal but also AMDS.

Theorem 8 *Let i be an integer such that $0 \le i \le n-1$, where $n = q^2 - 1$. Let $\mathcal{D}^i_{(q,e_1,e_2,e_3)}$ be the code obtained from the cyclic code $\mathcal{D}_{(q,e_1,e_2,e_3)}$ in Theorem 6 by puncturing on the i-th coordinate. If $q > 2$, then $\mathcal{D}^i_{(q,e_1,e_2,e_3)}$ is an optimal $[n-1, 4, n-q-2]$ linear code over $\mathbb{F}_q$, achieving the Griesmer bound, with weight enumerator*

$$\begin{aligned} &1 + (n-q)(q-1)(q-2)z^{n-q-2} + 3(n-q)(q-1)z^{n-q-1} \\ &\quad + 3q(q-1)z^{n-q} + (q-1)z^{q(q-1)} + (n-1)(q-1)z^{n-2} + 3(q-1)z^{n-1}. \end{aligned} \tag{5}$$

In addition, the dual code, $\mathcal{D}^{i\perp}_{(q,e_1,e_2,e_3)}$, of $\mathcal{D}^i_{(q,e_1,e_2,e_3)}$ is an optimal $[n-1, n-5, 4]$ AMDS linear code achieving the sphere-packing bound.

Proof Since $\mathcal{D}_{(q,e_1,e_2,e_3)}$ is cyclic, then by Theorem 3 and the remark after it, the punctured code $\mathcal{D}^i_{(q,e_1,e_2,e_3)}$ has parameters $[n-1, 4, n-q-2]$. Consequently, since the minimum Hamming distance of $\mathcal{D}^i_{(q,e_1,e_2,e_3)}$ is $n-q-2 = q(q-1)-3$, we obtain

$$\begin{aligned} &\left\lceil \frac{q(q-1)-3}{q^0} \right\rceil + \left\lceil \frac{q(q-1)-3}{q^1} \right\rceil + \left\lceil \frac{q(q-1)-3}{q^2} \right\rceil + \left\lceil \frac{q(q-1)-3}{q^3} \right\rceil, \\ &= (q^2-q-3) + (q-1) + 1 + 1 = q^2 - 2 = n-1, \end{aligned}$$

which implies that $\mathcal{D}^i_{(q,e_1,e_2,e_3)}$ is optimal as it achieves the Griesmer bound. Further, by Remark 3 and the discussion after it, the cyclic code $\mathcal{D}_{(q,e_1,e_2,e_3)}$ is homogeneous. Thus, by Theorem 4 and (2), we have that $A_j(\mathcal{D}^i_{(q,e_1,e_2,e_3)}) = 0$, $0 \le j \le n-1$, except for the following cases

$$
\begin{aligned}
A_0(\mathcal{D}^i_{(q,e_1,e_2,e_3)}) &= A_0(\mathcal{D}_{(q,e_1,e_2,e_3)}) = 1\ ,\\
A_{n-q-2}(\mathcal{D}^i_{(q,e_1,e_2,e_3)}) &= \frac{(n-q-2)+1}{n} A_{n-q-1}(\mathcal{D}_{(q,e_1,e_2,e_3)})\\
&= (n-q)(q-1)(q-2)\ ,\\
A_{n-q-1}(\mathcal{D}^i_{(q,e_1,e_2,e_3)}) &= \frac{n-(n-q-1)}{n} A_{n-q-1}(\mathcal{D}_{(q,e_1,e_2,e_3)})\\
&\quad + \frac{(n-q-1)+1}{n} A_{n-q}(\mathcal{D}_{(q,e_1,e_2,e_3)})\\
&= (n-q)(q-1) + 2(n-q)(q-1) = 3(n-q)(q-1)\ ,\\
A_{n-q}(\mathcal{D}^i_{(q,e_1,e_2,e_3)}) &= \frac{n-(n-q)}{n} A_{n-q}(\mathcal{D}_{(q,e_1,e_2,e_3)})\\
&\quad + \frac{(n-q)+1}{n} A_{q(q-1)}(\mathcal{D}_{(q,e_1,e_2,e_3)})\\
&= 2q(q-1) + q(q-1) = 3q(q-1)\ ,\\
A_{q(q-1)}(\mathcal{D}^i_{(q,e_1,e_2,e_3)}) &= \frac{n-(q(q-1))}{n} A_{q(q-1)}(\mathcal{D}_{(q,e_1,e_2,e_3)}) = q-1\ ,\\
A_{n-2}(\mathcal{D}^i_{(q,e_1,e_2,e_3)}) &= \frac{(n-2)+1}{n} A_{n-1}(\mathcal{D}_{(q,e_1,e_2,e_3)}) = (n-1)(q-1)\ ,\\
A_{n-1}(\mathcal{D}^i_{(q,e_1,e_2,e_3)}) &= \frac{n-(n-1)}{n} A_{n-1}(\mathcal{D}_{(q,e_1,e_2,e_3)})\\
&\quad + \frac{(n-1)+1}{n} A_n(\mathcal{D}_{(q,e_1,e_2,e_3)})\\
&= (q-1) + 2(q-1) = 3(q-1)\ ,
\end{aligned}
$$

which is in accordance with (5). Then the weight enumerator of $\mathcal{D}^i_{(q,e_1,e_2,e_3)}$ follows. Now, owing to (5) and the first five Pless power moments, we obtain that $A_j(\mathcal{D}^{i\perp}_{(q,e_1,e_2,e_3)}) = 0$, for $1 \le j \le 3$, and

$$
A_4(\mathcal{D}^{i\perp}_{(q,e_1,e_2,e_3)}) = \frac{(q-1)(q+2)(q-2)^2(q^2-3)(q^2-5)}{24}.
$$

Since $q > 2$, $\mathcal{D}^{i\perp}_{(q,e_1,e_2,e_3)}$ is an $[n-1, n-5, 4]$ AMDS linear code. Finally, by the sphere-packing bound, it is not difficult to verify that for a code of length $n-1$ and dimension $n-5$, its minimum Hamming distance can be at most 4. Therefore, the code $\mathcal{D}^{i\perp}_{(q,e_1,e_2,e_3)}$ is optimal. □

Remark 5 Let $\mathcal{D}_{(q,e_1,e_2,e_3)i}$ be the linear code obtained from the cyclic code $\mathcal{D}_{(q,e_1,e_2,e_3)}$ in Theorem 6 by shortening on some coordinate $0 \le i \le q^2-2$. Thus, it is interesting to note that if $q > 2$, then the shortened code $\mathcal{D}_{(q,e_1,e_2,e_3)i}$ has the same parameters and the same weight distribution as the punctured code $\mathcal{C}^i_{(q,2,e_1,e_2)}$ in Part (A) of Theorem 7 (therein $m = 2$).

Example 2 The following are some examples of the previous theorem.

(a) Let $(q, e_1, e_2, e_3) = (3, 2, 7, 5)$ and i an integer such that $0 \le i \le q^2 - 2$. Since $\gcd(q+1, e_3) = 1$, $\gcd(q-1, e_2 - e_1) = 1$, and $e_3 \equiv e_1 + e_2 \pmod{q-1}$, $\mathcal{D}_{(3,2,7,5)}$ belongs to the class of codes in Theorem 6. Thus, owing to Theorem 8, the punctured code $\mathcal{D}^i_{(3,2,7,5)}$ is an optimal five-weight [7, 4, 3] linear code over $\mathbb{F}_3$ with weight enumerator

$$1 + 10z^3 + 30z^4 + 18z^5 + 16z^6 + 6z^7,$$

while its dual code $\mathcal{D}^{i\perp}_{(3,2,7,5)}$ is an optimal [7, 3, 4] AMDS linear code.

(b) Let $(q, e_1, e_2, e_3) = (8, 3, 14, 10)$ and i an integer such that $0 \le i \le q^2 - 2$. Since $\gcd(q+1, e_3) = 1$, $\gcd(q-1, e_2 - e_1) = 1$, and $e_3 \equiv e_1 + e_2 \pmod{q-1}$, $\mathcal{D}_{(8,3,14,10)}$ belongs to the class of codes in Theorem 6. Thus, owing to Theorem 8, the punctured code $\mathcal{D}^i_{(8,3,14,10)}$ is an optimal six-weight [62, 4, 53] linear code over $\mathbb{F}_8$ with weight enumerator

$$1 + 2310z^{53} + 1155z^{54} + 168z^{55} + 7z^{56} + 434z^{61} + 21z^{62},$$

while its dual code $\mathcal{D}^{i\perp}_{(8,3,14,10)}$ is an optimal [62, 58, 4] AMDS linear code.

(c) Let $(q, e_1, e_2, e_3) = (9, 5, 2, 7)$ and i an integer such that $0 \le i \le q^2 - 2$. Since $\gcd(q+1, e_3) = 1$, $\gcd(q-1, e_2 - e_1) = 1$, and $e_3 \equiv e_1 + e_2 \pmod{q-1}$, $\mathcal{D}_{(9,5,2,7)}$ belongs to the class of codes in Theorem 6. Thus, owing to Theorem 8, the punctured code $\mathcal{D}^i_{(9,5,2,7)}$ is an optimal six-weight [79, 4, 69] linear code over $\mathbb{F}_9$ with weight enumerator

$$1 + 3976z^{69} + 1704z^{70} + 216z^{71} + 8z^{72} + 632z^{78} + 24z^{79},$$

while its dual code $\mathcal{D}^{i\perp}_{(9,5,2,7)}$ is an optimal [79, 75, 4] AMDS linear code.

When a q-ary $[n, k]$ linear code $\mathcal{C}$ with weight distribution $(A_j(\mathcal{C}))_{j=0}^n$ is used for error detection on a q-ary symmetric channel with symbol error probability ϵ, the probability of undetected error is given by (see [11, Sec. IV])

$$P_{ue}(\mathcal{C}, \epsilon) := \sum_{j=1}^{n} A_j(\mathcal{C}) \left(\frac{\epsilon}{q-1} \right)^j (1-\epsilon)^{n-j}.$$

If $P_{ue}(\mathcal{C}, \epsilon)$ is an increasing function of ϵ on the interval $[0, (q-1)/q]$, then $\mathcal{C}$ is said to be *proper* for error detection. In [11] the error detection capability of AMDS codes was investigated and the authors found the following sufficient condition for an AMDS code to be proper for error detection:

Lemma 1 ([11, Lemma 4]) *Let $\mathcal{C}$ be an $[n, k]$ AMDS code over $\mathbb{F}_q$. Then, $\mathcal{C}$ is proper if*

$$\frac{A_{n-k}(\mathcal{C})}{q-1} \leq \frac{1}{q}\binom{n}{k}.$$

Remark 6 It is not difficult to verify that the AMDS linear codes $\mathcal{C}^{i\perp}_{(q,2,e_1,e_2)}$, $\mathcal{C}^{\perp}_{(q,2,e_1,e_2)i}$ and $\mathcal{D}^{i\perp}_{(q,e_1,e_2,e_3)}$, from Corollary 1 and Theorem 8, satisfy the above condition. Therefore, it is important to remark that these codes are proper for error detection.

5 Conclusions

Let $q > 2$ be a prime power and $m \geq 2$ an integer. In this paper we used the puncturing and shortening techniques on two already-known classes of optimal cyclic codes (Theorems 5 and 6) in order to obtain:

(i) A class of optimal four-weight $[q^m - 2, m+1, q^{m-1}(q-1) - 2]$ linear codes over $\mathbb{F}_q$, achieving the Griesmer bound, whose duals are almost optimal $[q^m - 2, q^m - m - 3, 3]$ linear codes with respect to the sphere-packing bound (Part (A) of Theorem 7). Through the analysis of several examples it is suggested that such duals are optimal (Remark 4).

(ii) A class of optimal two-weight $[q^m - 2, m, q^{m-1}(q-1) - 1]$ linear codes over $\mathbb{F}_q$, achieving the Griesmer bound, whose duals are optimal $[q^m - 2, q^m - m - 2, 2]$ linear codes with respect to the sphere-packing bound (Part (B) of Theorem 7). Further, as pointed out at the end of Sect. 2, these two-weight codes are minimal and therefore suitable for constructing secret sharing schemes with nice access structures.

(iii) A class of optimal $[q^2 - 2, 4, q(q-1) - 3]$ linear codes over $\mathbb{F}_q$, achieving the Griesmer bound, whose duals are optimal $[q^2 - 2, q^2 - 6, 4]$ AMDS linear codes achieving the sphere-packing bound (Theorem 8).

The weight distributions for these classes of codes were determined explicitly. Moreover, if $m = 2$, then the dual codes in (i) and (ii) are AMDS (Corollary 1). Furthermore, all the AMDS codes presented in this paper are proper for error detection (Remark 6). Finally, as pointed out at the beginning of this work, the classes of optimal linear codes presented here seems to be new.

Acknowledgements The authors want to express their gratitude to the anonymous referees for their valuable suggestions. This manuscript is partially supported by PAPIIT-UNAM IN107423. The first author has also received research support from CONAHCyT, México.

Declarations

Conflict of interest The authors declare that they have no Conflict of interest.

References

1. 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
2. Ball, S., Montanucci, E.: Affine blocking sets, three-dimensional codes and the Griesmer bound. Discrete Math. **307**(13), 1600–1608 (2007). https://doi.org/10.1016/j.disc.2006.09.011
3. Bouyukliev, I.G.: Classification of Griesmer codes and dual transform. Discrete Math. **309**(12), 4049–4068 (2009). https://doi.org/10.1016/j.disc.2008.12.002
4. Calderbank, A.R., Goethals, J.M.: Three-weight codes and association schemes. Philips J. Res. **39**(4–5), 143–152 (1984)
5. Calderbank, R., Kantor, W.M.: The geometry of two-weight codes. Bull. London Math. Soc. **18**(2), 97–122 (1986). https://doi.org/10.1112/blms/18.2.97
6. Ding, C.: Linear codes from some 2-designs. IEEE Trans. Inf. Theory **61**(6), 3265–3275 (2015). https://doi.org/10.1109/TIT.2015.2420118
7. Ding, C., Luo, J., Niederreiter, H.: Two-weight codes punctured from irreducible cyclic codes. In: Li, Y., Ling, S., Niederreiter, H., Wang, H., Xing, C., Zhang, S. (eds.) Proc. 1st Int. Workshop Coding Theory Cryptogr., pp. 119–124. World Scientific, Singapore (2008). https://doi.org/10.1142/9789812832245_0009
8. Ding, C., Niederreiter, H.: Cyclotomic linear codes of order 3. IEEE Trans. Inf. Theory **53**(6), 2274–2277 (2007). https://doi.org/10.1109/TIT.2007.896886
9. 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
10. 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
11. Dodunekova, R., Dodunekov, S., Klove, T.: Almost-MDS and near-MDS codes for error detection. IEEE Trans. Inf. Theory **43**(1), 285–290 (1997). https://doi.org/10.1109/18.567708
12. Grassl, M.: Bounds on the minimum distance of linear codes and quantum codes. http://www.codetables.de. Last accessed Jun 12, (2023)
13. Hellesth, T.: Projective codes meeting the Griesmer bound. Discrete Math. **106–107**, 265–271 (1992). https://doi.org/10.1016/0012-365X(92)90553-R
14. 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
15. Heng, Z., Ding, C.: The subfield codes of some [q + 1, 2, q] MDS codes. IEEE Trans. Inf. Theory **68**(6), 3643–3656 (2022). https://doi.org/10.1109/TIT.2022.3151721
16. 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
17. Heng, Z., Wang, W., Wang, Y.: Projective binary linear codes from special Boolean functions. Appl. Algebra Eng. Commun. **32**, 521–552 (2021). https://doi.org/10.1007/s00200-019-00412-z
18. 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
19. Hernández, F., Vega, G.: The subfield and extended codes of a subclass of optimal three-weight cyclic codes. Algorithmica **85**, 3973–3995 (2023). https://doi.org/10.1007/s00453-023-01173-5
20. Huffman, W.C., Pless, V.: Fundamentals of error-correcting codes. Cambridge Univ. Press, Cambridge, U.K. (2003)

21. Liu, Y., Ding, C., Tang, C.: Shortened linear codes over finite fields. IEEE Trans. Inf. Theory **67**(8), 5119–5132 (2021). https://doi.org/10.1109/TIT.2021.3087082
22. Luo, Y., Xing, C., Yuan, C.: Optimal locally repairable codes of distance 3 and 4 via cyclic codes. IEEE Trans. Inf. Theory **65**(2), 1048–1053 (2019). https://doi.org/10.1109/TIT.2018.2854717
23. Mesnager, S., Qian, L., Cao, X., Yuan, M.: Several families of binary minimal linear codes from two-to-one functions. IEEE Trans. Inf. Theory **69**(5), 3285–3301 (2023). https://doi.org/10.1109/TIT.2023.3236955
24. Ouyang, J., Liu, H., Wang, X.: Several classes of p-ary linear codes with few weights. Appl. Algebra Eng. Commun. Comput. **34**, 691–715 (2023). https://doi.org/10.1007/s00200-021-00527-2
25. 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
26. Solomon, G., Stiffler, J.: Algebraically punctured cyclic codes. Inf. Control. **8**(2), 170–179 (1965). https://doi.org/10.1016/S0019-9958(65)90080-X
27. Tan, P., Fan, C., Ding, C., Tang, C., Zhou, Z.: The minimum locality of linear codes. Des. Codes Cryptogr. **91**, 83–114 (2023). https://doi.org/10.1007/s10623-022-01099-z
28. Tang, C., Wang, Q., Ding, C.: The subfield codes and subfield subcodes of a family of MDS codes. IEEE Trans. Inf. Theory **68**(9), 5792–5801 (2022). https://doi.org/10.1109/TIT.2022.3163813
29. 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
30. Vega, G., Hernández, F.: The complete weight distribution of a subclass of optimal three-weight cyclic codes. Cryptogr. Commun. **15**, 317–330 (2023). https://doi.org/10.1007/s12095-022-00601-7
31. Wang, X., Zheng, D., Ding, C.: Some punctured codes of several families of binary linear codes. IEEE Trans. Inf. Theory **67**(8), 5133–5148 (2021). https://doi.org/10.1109/TIT.2021.3088146
32. Xiang, C., Tang, C., Ding, C.: Shortened linear codes from APN and PN functions. IEEE Trans. Inf. Theory **68**(6), 3780–3795 (2022). https://doi.org/10.1109/TIT.2022.3145519
33. 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
34. Zhang, X., Du, X., Jin, W.: Weight distributions of two classes of linear codes with five or six weights. Discrete Math. **345**(7), 112881 (2022). https://doi.org/10.1016/j.disc.2022.112881