Cryptography and Communications
https://doi.org/10.1007/s12095-025-00861-z

RESEARCH

Asymptotic performance of double circulant and four circulant codes with small hull dimension

Zohreh Aliabadi[1] · Tekgül Kalaycı[2] · Mohammad Zadehdabbagh[3]

Received: 2 August 2025 / Accepted: 26 December 2025

Abstract
We present enumeration formulas for double circulant (DC) codes of length $2m$ and four circulant (FC) codes of length $4m$ over the finite field $\mathbb{F}_q$, with prescribed Euclidean hull dimension, assuming $\gcd(m, q) = 1$. These formulas significantly generalize previous results that were limited to special cases. In particular, we resolve an open problem posed by Zhu and Shi (J. Appl. Math. Comput. 68:1227–1244, 2022) concerning the case of reciprocal pair factors in the factorization of $x^m - 1$ for the enumeration of self-dual and linear complementary dual (LCD) FC codes. Additionally, we correct an enumeration formula used in Zhu and Shi (Bull. Aust. Math. Soc. 98(1):159–166, 2018), leading to an improved bound on the relative distance for LCD FC codes.

Keywords The hull of a code · Quasi-cyclic code · Double circulant code · Four circulant code · Linear complementary dual code · Artin's primitive root conjecture

Mathematics Subject Classification (2010) 94B05 · 11T71

1 Introduction

Throughout the article, $\mathbb{F}_q$ denotes the finite field of q elements, where q is a prime power. A family of $[n, k_n, d_n]$ linear codes $C(n)$ over $\mathbb{F}_q$ is called asymptotically good if the product of the rate R and the relative distance δ is positive, where

✉ Zohreh Aliabadi
zaliabadi@sabanciuniv.edu

Tekgül Kalaycı
tekgulkalayci1@gmail.com

Mohammad Zadehdabbagh
mohameddabagh@aydin.edu.tr

1 Sabancı University, MDBF, Orhanlı, Tuzla, 34956 İstanbul, Turkey

2 Institut für Mathematik, Alpen-Adria-Universität Klagenfurt, Klagenfurt, Austria

3 İstanbul Aydın University, Mechanical Engineering Department, Beşyol, İstanbul, Turkey

Published online: 08 January 2026

$$R = \lim_{n\to\infty} \sup \frac{k_n}{n} \quad \text{and} \quad \delta = \lim_{n\to\infty} \inf \frac{d_n}{n}.$$

The asymptotic behavior of cyclic codes is still an open problem, see [5, 12, 22], and [26]. In contrast, it has been shown that the family of quasi-cyclic (QC) codes is asymptotically good, see [11, 20, 24, 28, 36].

The Euclidean hull of a linear code C over $\mathbb{F}_q$ is defined as the intersection of C with its Euclidean dual. This concept has been introduced by Assumus and Key in [4] for the purpose of classifying finite projective planes. It has since found applications in constructing quantum error-correcting codes and determining permutation equivalence between codes, as discussed in [31] and [37]. Notably, algorithms for determining permutation equivalence between two codes and determining the automorphism group of a linear code tend to be more effective when the hull dimension of the code is small.

The family of linear complementary dual (LCD) codes, introduced by Massey in [27], are the codes characterized by having the trivial hull. These codes have drawn significant attention in recent years, particularly for their applications in cryptography within the context of side-channel and fault-injection attacks, as discussed in [6, 8], and [9].

As 1 represents the next smallest hull dimension, codes with a 1-dimensional hull have also attracted attention. For recent contributions on 1-dimensional hull codes in the literature, we refer to [10, 21], and [37].

The class of quasi-cyclic (QC) codes has been well-studied in coding theory. The algebraic structure of QC codes over finite fields has been investigated in [23] and [25], and the class of 1-generator QC codes has been discussed in [30]. Additionally, LCD QC codes have been characterized in [17], and the hull of 1-generator QC codes has been formulated in [3]. As a particular subclass of 1-generator QC codes, the class of double circulant (DC) codes has also been addressed. Furthermore, the hull of a specific class of 2-generator quasi-cyclic codes, namely, four circulant (FC) codes, has been described.

Asymptotic analyses provide a way to understand how the parameters of families of linear codes behave when the length increases, and to study the existence of infinite families of structured codes with good parameters. Several families of circulant, quasi-cyclic, quasi-twisted, and negacirculant codes, as well as asymptotic bounds for such code families, have been studied in the literature; see, for example, [32–35, 38].

Precise enumeration of a code family is a basic tool for carrying out asymptotic analysis. Enumeration results for self-dual DC and LCD DC codes of length $2m$, with arbitrary m satisfying $\gcd(m, q) = 1$, over $\mathbb{F}_q$ have been presented in [39]. For FC codes, enumerations of self-dual and LCD codes of length $4m$, where $m \mid q^r + 1$ for some $r \in \mathbb{Z}^+$, have also been provided. In this article, we generalize these results by extending the enumeration formulas to DC and FC codes of arbitrary m with any prescribed Euclidean hull dimension. Moreover, we show that LCD DC codes, LCD FC codes, DC codes with a 1-dimensional hull, and FC codes with a 2-dimensional hull are asymptotically good. While the asymptotic behavior of LCD DC and LCD FC codes has already been investigated in the literature [39, 40], we revisit these cases using our new enumeration formulas, which differ from the previous ones; see Remark 1 in Section 3.1 and Remark 2 in Section 3.2 for details. Interestingly, the bounds on the relative distances of these infinite families, all of which have rate $1/2$, satisfy a modified Gilbert-Varshamov bound for linear codes over $\mathbb{F}_q$.

The article is organized as follows. In Section 2, we provide the definitions and known facts required throughout the article. In Section 3, we present the enumerations of DC and FC codes with prescribed hull dimension. In Section 4, we analyze the asymptotic behavior of the aforementioned families of codes with small hull dimensions.

2 Background

In this section, we recall basic definitions and well-known results on linear codes over the finite field $\mathbb{F}_q$, which are required throughout the article.

2.1 Definitions and notation

A q-ary $[n, k]$ linear code, or an $[n, k]$ linear code over $\mathbb{F}_q$, is a k-dimensional linear subspace of the vector space $\mathbb{F}_q^n$, and the elements of C are called codewords. A $k \times n$ matrix G, whose rows form a basis of an $[n, k]$ linear code C over $\mathbb{F}_q$, is called a generator matrix of C.

Let $x = (x_0, \dots, x_{n-1}), y = (y_0, \dots, y_{n-1}) \in \mathbb{F}_q^n$. Then the Hamming distance of x and y is defined as

$$d(x, y) = |\{0 \leq i \leq n-1 \mid x_i \neq y_i\}|.$$

For a q-ary linear code C, the minimum Hamming distance d of C is defined as the minimum of the Hamming distances between two distinct codewords of C, i.e.,

$$d = d(C) = \min_{x \neq y} \{d(x, y) \mid x, y \in C\}.$$

Let C be a linear code of length n over $\mathbb{F}_q$. The (Euclidean) dual of C, which is denoted by $C^\perp$, is defined as

$$C^\perp = \{x \in \mathbb{F}_q^n \mid \langle c, x\rangle = \sum_{i=0}^{n-1} c_i x_i = 0 \text{ for all } c = (c_0, \dots, c_{n-1}) \in C\}.$$

It is known that $C^\perp$ is an $[n, n-k]$ linear code over $\mathbb{F}_q$. An $(n-k) \times n$ generator matrix H for the dual code $C^\perp$ is called a parity check matrix of C.

The Euclidean hull of C over $\mathbb{F}_q$ is defined as the intersection of C with its dual, i.e. $\mathrm{Hull}(C) = C \cap C^\perp$, where $C^\perp$ is the Euclidean dual of C. Note that $\mathrm{Hull}(C)$ is also a linear code over $\mathbb{F}_q$.

If C is a linear code defined over a square field $\mathbb{F}_{q^2}$, then the Hermitian dual of C, which is denoted by $C^{\perp_H}$ is defined as

$$C^{\perp_H} = \{x \in \mathbb{F}_{q^2}^n \mid \langle c, x\rangle_h = \sum_{i=0}^{n-1} c_i \bar{x}_i = 0 \text{ for all } c = (c_0, \dots, c_{n-1}) \in C\},$$

where $\bar{x}_i$ denotes the $\mathbb{F}_q$-conjugate x_i^q of x_i for all $0 \leq i \leq n-1$. Similarly, the Hermitian hull of C is defined as $\mathrm{Hull}_H(C) = C \cap C^{\perp_H}$, which is also a linear code over $\mathbb{F}_{q^2}$. We denote the $\mathbb{F}_q$-dimensions of the Euclidean and Hermitian hulls of C by $h(C)$ and $h_H(C)$, respectively. Note that when C is defined over $\mathbb{F}_q$, the Hermitian inner product coincides with the Euclidean inner product, and hence $h(C) = h_H(C)$.

A q-ary linear code C is called a linear complementary dual (LCD) code, if $\mathrm{Hull}(C) = C \cap C^{\perp} = \{0\}$. The notion of Hermitian LCD codes is defined similarly.

The following proposition determines the Euclidean and Hermitian hull dimensions of linear codes in terms of their generator matrices.

Proposition 1 *[14, Proposition 3.1, 3.2] Let G be a generator matrix of a linear code C and G^T denote the transpose of G.*

i) *If C is a q-ary [n, k] linear code, then $h(C) = k - \mathrm{rank}(GG^T)$.*
ii) *If C is a q^2-ary [n, k] linear code, then $h_H(C) = k - \mathrm{rank}(G\bar{G}^T)$, where $\bar{G}$ is the matrix obtained by taking the conjugate of each entry of G.*

Proposition 2 *[15, Theorem 2.1] For $i \in \{1, 2\}$, let C_i be an $[n, k_i]$ linear code with parity check matrix H_i and generator matrix G_i. Then $\dim(C_1 \cap C_2) = k_1 - \mathrm{rank}(G_1 H_2^T) = k_2 - \mathrm{rank}(G_2 H_1^T)$.*

Proposition 3 *[29, Theorem 2] Let $q \equiv 3 \pmod 4$. If there exists a q-ary self-dual linear code of length n, then n is divisible by 4.*

2.2 Algebraic structure of quasi-cyclic codes

In the subsequent sections of the paper, we suppose that $n = m\ell$, where m, ℓ are positive integers, m is relatively prime to q and $\ell \geq 2$. A q-ary linear code C of length $m\ell$ is called a quasi-cyclic (QC) code of index ℓ if it is invariant under shifting its codewords by ℓ units, and ℓ is the smallest positive integer with this property. Note that the case $\ell = 1$ corresponds to cyclic codes.

If we set $R_m = \frac{\mathbb{F}_q[x]}{\langle x^m - 1 \rangle}$, then every QC code of length $m\ell$ and index ℓ over $\mathbb{F}_q$ can be considered as an R_m-submodule of R_m^ℓ, and the following map induces a one-to-one correspondence between QC codes of index ℓ in $\mathbb{F}_q^{m\ell}$ and R_m-submodules of R_m^ℓ:

$$\begin{array}{cccc} \phi : & \mathbb{F}_q^{m\ell} & \longrightarrow & R_m^\ell \\ & c = (c_{ij}) & \longmapsto & (c_0(x), c_1(x), \ldots, c_{\ell-1}(x)), \end{array}$$

where

$$c_j(x) := \sum_{i=0}^{m-1} c_{ij} x^i = c_{0j} + c_{1j} x + c_{2j} x^2 + \cdots + c_{m-1,j} x^{m-1} \in R_m$$

for each $0 \leq j \leq \ell - 1$, see [25, Lemma 3.1].

Since m and q are relatively prime, we have the following factorization of $x^m - 1$ into monic irreducible polynomials in $\mathbb{F}_q[x]$

$$x^m - 1 = \prod_{i=1}^{s} g_i(x) \prod_{j=1}^{t} h_j(x) h_j^*(x),$$

where $g_i(x)$ is self-reciprocal for $1 \le i \le s$, $h_j(x)$ and $h_j^*(x)$ are reciprocal pairs for $1 \le j \le t$, and the reciprocal of a monic polynomial $f(x)$ with non-zero constant term is defined as $f^*(x) = f(0)^{-1} x^{\deg(f)} f(x^{-1})$.

Let ξ be a primitive m-th root of unity over $\mathbb{F}_q$, and ξ^{u_i}, ξ^{v_j} and ξ^{-v_j} be roots of $g_i(x)$, $h_j(x)$ and $h_j^*(x)$ respectively, for $1 \le i \le s$ and $1 \le j \le t$. Let

$$\mathbb{G}_i = \frac{\mathbb{F}_q[x]}{\langle g_i(x) \rangle} \cong \mathbb{F}_q(\xi^{u_i}) \quad \text{for} \quad 1 \le i \le s,$$

$$\mathbb{H}'_j = \frac{\mathbb{F}_q[x]}{\langle h_j(x) \rangle} \cong \mathbb{F}_q(\xi^{v_j}) \cong \mathbb{F}_q(\xi^{-v_j}) \cong \frac{\mathbb{F}_q[x]}{\langle h_j^*(x) \rangle} = \mathbb{H}''_j \quad \text{for} \quad 1 \le j \le t.$$

Then by the Chinese Remainder Theorem (CRT), we have the following decomposition of R_m^ℓ

$$R_m^\ell = \left(\bigoplus_{i=1}^{s} \mathbb{G}_i^\ell \right) \bigoplus \left(\bigoplus_{j=1}^{t} \left({\mathbb{H}'_j}^\ell \oplus {\mathbb{H}''_j}^\ell \right) \right).$$

We note that the degree of $\mathbb{G}_i$ over $\mathbb{F}_q$ is even for all i except for the components corresponding to the linear self-reciprocal irreducible factors $x \pm 1$ of $x^m - 1$.

Via the CRT decomposition of R_m^ℓ, a QC code C of length $m\ell$ and index ℓ has the following CRT decomposition

$$C = \left(\bigoplus_{i=1}^{s} C_i \right) \bigoplus \left(\bigoplus_{j=1}^{t} \left(C'_j \bigoplus C''_j \right) \right), \tag{1}$$

where, C_i, C'_j and C''_j are linear codes of length ℓ over the fields $\mathbb{G}_i$, $\mathbb{H}'_j$ and $\mathbb{H}''_j$, respectively, for $1 \le i \le s$ and $1 \le j \le t$. The component codes C_i, C'_j, and C''_j are called the constituents of C.

The dual of a QC code of index ℓ is also a QC code of index ℓ with the following CRT decomposition

$$C^\perp = \left(\bigoplus_{i=1}^{s} C_i^{\perp_H} \right) \bigoplus \left(\bigoplus_{j=1}^{t} \left({C''_j}^\perp \oplus {C'_j}^\perp \right) \right),$$

see [23]. Hence the hull dimension of a q-ary QC code C of length $m\ell$ and index ℓ can be formulated as follows.

$$h(C) = \sum_{i=1}^{s} \deg(g_i(x))\, h_H(C_i) + \sum_{j=1}^{t} \deg(h_j(x)) \left(\dim(C_j' \cap C_j''^{\perp}) + \dim(C_j'' \cap C_j'^{\perp})\right). \quad (2)$$

We refer the reader to [23, 25], for further details on the algebraic structure of QC codes.

If $C = \langle (a_1(x), \ldots, a_\ell(x)) \rangle \subset R_m^\ell$ is a 1-generator QC code of index ℓ, then the constituents of C can be described in terms of the generators of C as follows:

$$\begin{aligned} C_i &= \mathrm{Span}_{\mathbb{G}_i}\{(a_1(\xi^{u_i}), \ldots, a_\ell(\xi^{u_i}))\}, \\ C_j' &= \mathrm{Span}_{\mathbb{H}_j'}\{(a_1(\xi^{v_j}), \ldots, a_\ell(\xi^{v_j}))\}, \\ C_j'' &= \mathrm{Span}_{\mathbb{H}_j''}\{(a_1(\xi^{-v_j}), \ldots, a_\ell(\xi^{-v_j}))\}, \end{aligned} \quad (3)$$

see [16, Lemma 2.1].

2.3 Hull dimensions of double circulant and four circulant codes

We now focus on the Euclidean hulls of certain classes of QC codes. In particular, we recall two results from [3] on the Euclidean hulls of double circulant (DC) and four circulant (FC) codes, which will be used in the following sections.

A 1-generator QC code of index 2 of the form $C = \langle (1, a(x)) \rangle \subset R_m^2$ is called a double circulant (DC) code. In [3], the hull dimension of such 1-generator QC codes, in particular DC codes, is described as follows.

Theorem *1 i) [3, Theorem 3.1] Let $C = \langle (1, a(x)) \rangle \subseteq R_m^2$ be a q-ary DC code of length 2m over $\mathbb{F}_q$. Then*

$$h(C) = \deg\big(\gcd\big(1 + a(x)a(x^{m-1}),\ x^m - 1\big)\big).$$

ii) *[3, Theorem 3.7] There exists a DC code of hull dimension 1 over $\mathbb{F}_q$ if and only if $q \equiv 1 \pmod 4$ or q is even. If there exists a DC code with odd hull dimension over $\mathbb{F}_q$, then $q \equiv 1 \pmod 4$ or q is even.*

A 2-generator QC code of index 4 of the form

$$C = \langle (1, 0, a_1(x), a_2(x)), (0, 1, -a_2(x^{m-1}), a_1(x^{m-1})) \rangle \subset R_m^4$$

is called a four circulant (FC) code. In [3], the hull dimension of an FC code is described as follows.

Theorem 2 *[3, Theorem 4.1] Let $C = \langle (1, 0, a_1(x), a_2(x)), (0, 1, -a_2(x^{m-1}), a_1(x^{m-1})) \rangle \subset R_m^4$ be an FC code of length 4m over $\mathbb{F}_q$. Then*

$$h(C) = 2\deg\left(\gcd\big(1 + a_1(x)a_1(x^{m-1}) + a_2(x)a_2(x^{m-1}),\ x^m - 1\big)\right).$$

In particular, FC codes of odd hull dimension do not exist over any finite field.

For further details and results on families of 1-generator QC codes and FC codes, as well as tables indicating that certain such codes with small hull dimension achieve optimal parameters according to the code tables in [13], we refer the reader to [3].

3 Enumeration

Enumeration of codes with prescribed properties provides information on their distribution and enables asymptotic analysis. In this section, we present enumeration results for DC and FC codes over the finite field $\mathbb{F}_q$ with prescribed Euclidean hull dimension. These results are then used in Section 4 to investigate the asymptotic behavior of DC and FC codes. Our approach is based on the CRT decomposition of QC codes, as described in (1).

3.1 DC codes with prescribed hull dimension

Let $C = \langle(1,\ a(x))\rangle \subseteq R_m^2$ be a q-ary DC code of length $2m$. Then, by the CRT decomposition of C, the constituents of C are [2, 1] linear codes C_i, C'_j, C''_j over their defining fields with generator matrices $(1 \quad a(\xi^{u_i}))$, $(1 \quad a(\xi^{v_j}))$, and $(1 \quad a(\xi^{-v_j}))$, respectively, for $1 \le i \le s$ and $1 \le j \le t$. Since the constituents of C are 1-dimensional linear codes over their defining fields, we have the following.

I) The constituents C_i corresponding to the self-reciprocal factors of $x^m - 1$ satisfy either $h_H(C_i) = 0$ or $h_H(C_i) = 1$ for $1 \le i \le s$.
II) The constituents C'_j and C''_j corresponding to the reciprocal pair factors of $x^m - 1$ satisfy either $C'_j \cap C''^{\perp}_j = \{0\}$ or $C'_j = C''^{\perp}_j$ for $1 \le j \le t$.

Therefore, by (2), to determine the number of q-ary DC codes of length $2m$ with an l-dimensional hull, we need to count the [2, 1] linear codes over certain extensions of $\mathbb{F}_q$ satisfying conditions I) and II).

Lemma 4 *The number of solutions of the equation $1 + x^2 = 0$ in $\mathbb{F}_q$ is 1 if q is even, and 2 if $q \equiv 1 \pmod 4$.*

Proof If q is even, then $1 + x^2 = (1 + x)^2$. Clearly, $x = 1$ is the only root of this equation. If $q \equiv 1$ (mod 4), then there exists $\alpha \in \mathbb{F}_q^*$ such that $\alpha^2 = -1$. Hence, α and $-\alpha$ are the roots of $1 + x^2$. □

Lemma 5 *The number of solutions of the equation $1 + x^{q+1} = 0$ in $\mathbb{F}_{q^2}$ is $q + 1$.*

Proof Let $f(x) = 1 + x^{q+1}$. First, note that $f(x)$ has at most $q + 1$ roots in the algebraic closure $\bar{\mathbb{F}}_{q^2}$ of $\mathbb{F}_{q^2}$. We also have $f'(x) = x^q$, where $f'(x)$ denotes the derivative of $f(x)$. Since $\gcd(f, f') = 1$, the solutions of $1 + x^{q+1} = 0$ are distinct. It remains to show that every root of $f(x)$ is in $\mathbb{F}_{q^2}$. Let $f(\alpha) = 0$. Then we have $\alpha^{q+1} = -1$. If q is even, then $-1 = 1$ in $\mathbb{F}_q$, so $(\alpha^{q+1})^{q-1} = 1$, which implies $\alpha \in \mathbb{F}_{q^2}$. If q is odd, then $q - 1$ is even, and thus $\alpha^{q^2-1} = (\alpha^{q+1})^{q-1} = 1$, implying that $\alpha \in \mathbb{F}_{q^2}$. □

Lemma 6 *[1, Lemma 2.10] The number of solutions* $(x_1, y_1, x_2, y_2, \ldots, x_{t-1}, y_{t-1})$ *of the equation* $1 + x_1 y_1 + \cdots + x_{t-1} y_{t-1} = 0$ *in* $\mathbb{F}_q^{2(t-1)}$ *is*

$$q^{2t-3} - q^{t-2}.$$

We recall that the hull dimension l of a q-ary DC code of length $2m$ satisfies the following, see (2).

$$h(C) = \sum_{i=1}^{s} \deg(g_i(x)) h_H(C_i) + \sum_{j=1}^{t} \deg(h_j(x)) \left(\dim(C'_j \cap C''^{\perp}_j) + \dim(C''_j \cap C'^{\perp}_j) \right),$$

where $x^m - 1 = \prod_{i=1}^{s} g_i(x) \prod_{j=1}^{t} h_j(x) h_j^*(x)$, $g_i(x)$ is self-reciprocal for $1 \le i \le s$, $h_j(x)$ and $h_j^*(x)$ are reciprocal pairs for $1 \le j \le t$.

If m is odd, then $x - 1$ is the only self-reciprocal linear factor of $x^m - 1$. If m is even, then $x - 1$ and $x + 1$ are the self-reciprocal linear factors. Let $\deg(g_i(x)) = 2d_i$ for non-linear self-reciprocal factors of $x^m - 1$, and $d'_j = \deg(h_j(x)) = \deg(h_j^*(x))$ for $1 \le j \le t$.

In order to count the number of q-ary DC codes with an l-dimensional hull, we assume that l can be expressed in r different ways as follows,

$$l = a_{1_u} + \sum_{i=2}^{s} 2d_i a_{i_u} + \sum_{j=1}^{t} 2d'_j a'_{j_u} \quad \text{when } m \text{ is odd,} \tag{4}$$

$$l = a_{1_u} + a_{2_u} + \sum_{i=3}^{s} 2d_i a_{i_u} + \sum_{j=1}^{t} 2d'_j a'_{j_u} \quad \text{when } m \text{ is even,} \tag{5}$$

where $a_{i_u}, a'_{j_u} \in \{0, 1\}$ for all $1 \le i \le s$, $1 \le j \le t$, $1 \le u \le r$.

We obtain the following theorem.

Theorem 3 *Let q be a prime power and m be a positive integer relatively prime to q. Suppose that l is a positive integer which can be written as in (4) when m is odd, or as in (5) when m is even. Then the number of l-dimensional hull DC codes of length 2m over* $\mathbb{F}_q$ *is given below.*

i) $\sum_{u=1}^{r} 2^{a_{1_u}} (q-2)^{1-a_{1_u}} \prod_{i=2}^{s} (1+q^{d_i})^{a_{i_u}} (q^{2d_i} - q^{d_i} - 1)^{1-a_{i_u}} \prod_{j=1}^{t} (q^{d'_j} - 1)^{a'_{j_u}} (q^{2d'_j} - q^{d'_j} + 1)^{1-a'_{j_u}}$ *when m is odd and* $q \equiv 1 \pmod 4$.

ii) $\sum_{u=1}^{r} 2^{a_{1_u} + a_{2_u}} (q-2)^{2-a_{1_u} - a_{2_u}} \prod_{i=3}^{s} (1+q^{d_i})^{a_{i_u}} (q^{2d_i} - q^{d_i} - 1)^{1-a_{i_u}} \prod_{j=1}^{t} (q^{d'_j} - 1)^{a'_{j_u}} (q^{2d'_j} - q^{d'_j} + 1)^{1-a'_{j_u}}$ *when m is even and* $q \equiv 1 \pmod 4$.

iii) $\sum_{u=1}^{r} q^{1-a_{1_u}} \prod_{i=2}^{s} (1+q^{d_i})^{a_{i_u}} (q^{2d_i} - q^{d_i} - 1)^{1-a_{i_u}} \prod_{j=1}^{t} (q^{d'_j} - 1)^{a'_{j_u}} (q^{2d'_j} - q^{d'_j} + 1)^{1-a'_{j_u}}$ *when m is odd and q is even, or when* $q \equiv 3 \pmod 4$.

iv) $\sum_{u=1}^{r} q^2 \prod_{i=3}^{s} (1+q^{d_i})^{a_{i_u}} (q^{2d_i} - q^{d_i} - 1)^{1-a_{i_u}} \prod_{j=1}^{t} (q^{d'_j} - 1)^{a'_{j_u}} (q^{2d'_j} - q^{d'_j} + 1)^{1-a'_{j_u}}$ *when m is even and* $q \equiv 3 \pmod 4$.

Proof We have the following number of choices for the constituents of an l-dimensional hull DC code of length $2m$ over $\mathbb{F}_q$.

- If m is odd, then $x-1$ is the only self-reciprocal linear factor of x^m-1. In this case, in the CRT decomposition, there is a [2, 1] linear code, say C_1, over $\mathbb{F}_q$ with a generator matrix $G_1=(1\ c_1)$, see (3). By Proposition 1 *i*), $h(C_1)=1$ if and only if $G_1G_1^T=1+c_1^2=0$. The number of solutions of the equation $1+x^2=0$ in $\mathbb{F}_q$ is 1 when q is even, and 2 when $q\equiv 1 \pmod 4$ by Lemma 4. So, there exists only 1 choice for C_1 when q is even, and there are 2 choices when $q\equiv 1 \pmod 4$ in the case of $h(C_1)=1$. Therefore, there exist $q-1$ choices for C_1 satisfying $h(C_1)=0$ when q is even, and $q-2$ such choices when $q\equiv 1 \pmod 4$. By Proposition 3, there are no linear codes C_1 with $h(C_1)=1$ when $q\equiv 3 \pmod 4$. Hence, all q choices for C_1 satisfy $h(C_1)=0$ in this case. If m is even, then q is odd as $\gcd(m,q)=1$, and hence $x-1$ and $x+1$ are the self-reciprocal linear factors of x^m-1. In this case, in the CRT decomposition, there are two [2, 1] linear codes, say C_1 and C_2, over $\mathbb{F}_q$ with generator matrices $G_1=(1\ c_1)$ and $G_2=(1\ c_2)$, respectively, see (3). By the above argument, we have the following cases when $q\equiv 1 \pmod 4$.

  - In the case of $h(C_1)=h(C_2)=0$, there are $(q-2)^2$ choices for C_1 and C_2.
  - In the case of $h(C_1)=h(C_2)=1$, there are 4 choices for C_1 and C_2.
  - In the case of $h(C_1)\neq h(C_2)$, there are $2(q-2)$ choices for C_1 and C_2.

By Proposition 3, we have q^2 choices for C_1 and C_2 in the case of $h(C_1)=h(C_2)=0$ and no choice in the remaining cases when $q\equiv 3 \pmod 4$.

- The constituents corresponding to the self-reciprocal factors $g_i(x)$ of x^m-1 with $\deg(g_i(x))=2d_i$ are [2, 1] linear codes over $\mathbb{F}_{q^{2d_i}}$, say C_i, where $2\le i\le s$ when m is odd and $3\le i\le s$ when m is even. Let $G_i=(1\ c_i)$ be a generator matrix of C_i. Then $h_H(C_i)=1$ if and only if $G_i\bar{G}_i^T=1+c_i^{q^{d_i}+1}=0$ by Proposition 1 *ii*). Since the number of solutions of the equation $1+x^{q^{d_i}+1}=0$ in $\mathbb{F}_{q^{2d_i}}$ is $q^{d_i}+1$ by Lemma 5, we have $q^{d_i}+1$ choices for C_i when $h_H(C_i)=1$. Hence, we have $q^{2d_i}-q^{d_i}-1$ choices for C_i when $h_H(C_i)=0$.
- The constituents corresponding to the reciprocal pair factors $(h_j(x),h_j^*(x))$ with $\deg(h_j(x))=\deg(h_j^*(x))=d'_j$ are [2, 1] linear codes over $\mathbb{F}_{q^{d'_j}}$, say C'_j and C''_j, for $1\le j\le t$. Let $G'_j=(1\ c'_j)$ and $G''_j=(1\ c''_j)$ be generator matrices of C'_j and C''_j, respectively, for $1\le j\le t$. By Proposition 2, we have $C'_j={C''_j}^{\perp}$ if and only if $\mathrm{rank}(G'_jG''^T_j)=0$. Since $G'_jG''^T_j=1+c'_jc''_j$, the condition $C'_j={C''_j}^{\perp}$ is equivalent to $1+c'_jc''_j=0$. Since the number of solutions $(x_1,y_1)\in\mathbb{F}^2_{q^{d'_j}}$ of the equation $1+x_1y_1=0$ is $q^{d'_j}-1$ by Lemma 6, we have $q^{d'_j}-1$ choices for the pair (C'_j,C''_j) satisfying $C'_j={C''_j}^{\perp}$. Hence, there are $q^{2d'_j}-q^{d'_j}+1$ choices for the pair (C'_j,C''_j) satisfying $C'_j\cap {C''_j}^{\perp}=C''_j\cap {C'_j}^{\perp}=\{0\}$.

Combining the above counting arguments with the choices $a_{i_u},a'_{j_u}\in\{0,1\}$ in (4) and (5) yields the result. □

We present the following examples, in which the results have been confirmed using the MAGMA computer algebra system [7].

Example 1 Let $q = 5$ and $m = 8$. Then the factorization of $x^8 - 1$ into monic irreducible polynomials over $\mathbb{F}_5$ is given by

$$x^8 - 1 = (x+1)(x+2)(x+3)(x+4)(x^2+2)(x^2+3).$$

In this factorization, the self-reciprocal factors are $g_1(x) = x+1$ and $g_2(x) = x+4$, while the reciprocal pair factors are $h_1(x) = x+2$, $h_1^*(x) = x+3$, and $h_2(x) = x^2+2$, $h_2^*(x) = x^2+3$. We then have $d_1' = \deg(h_1(x)) = \deg(h_1^*(x)) = 1$ and $d_2' = \deg(h_2(x)) = \deg(h_2^*(x)) = 2$. For $l = 4$, we have $r = 2$ by (5), since

$$4 = a_{1_1} + a_{2_1} + 2d_1'a_{1_1}' + 2d_2'a_{2_1}' = 1 + 1 + 2 \cdot 1 \cdot 1 + 2 \cdot 2 \cdot 0$$

or

$$4 = a_{1_2} + a_{2_2} + 2d_1'a_{1_2}' + 2d_2'a_{2_2}' = 0 + 0 + 2 \cdot 1 \cdot 0 + 2 \cdot 2 \cdot 1.$$

That is, $r = 2$ with $a_{1_1} = a_{2_1} = a_{1_1}' = 1$, $a_{2_1}' = 0$ and $a_{1_2} = a_{2_2} = a_{1_2}' = 0$, $a_{2_2}' = 1$. By Theorem 3 ii), the number of 4-dimensional hull DC codes of length 16 over $\mathbb{F}_5$ is

$$2^2(5-1)(5^4 - 5^2 + 1) + (5-2)^2(5^2 - 5 + 1)(5^2 - 1) = 14152.$$

Example 2 Let $q = 3$ and $m = 13$. Then the factorization of $x^{13} - 1$ into monic irreducible polynomials over $\mathbb{F}_3$ is given by

$$x^{13} - 1 = (x+2)(x^3+x^2+2)(x^3+2x+2)(x^3+x^2+x+2)(x^3+2x^2+2x+2).$$

In this factorization, the self-reciprocal factor is $g_1(x) = x+2$, and the reciprocal pair factors are $h_1(x) = x^3+x^2+2$, $h_1^*(x) = x^3+2x+2$, and $h_2(x) = x^3+x^2+x+2$, $h_2^*(x) = x^3+2x^2+2x+2$. We then have $d_1' = \deg(h_1(x)) = \deg(h_1^*(x)) = 3$ and $d_2' = \deg(h_2(x)) = \deg(h_2^*(x)) = 3$. For $l = 6$, we have $r = 2$ by (4), since

$$6 = a_{1_1} + 2d_1'a_{1_1}' + 2d_2'a_{2_1}' = 0 + 2 \cdot 3 \cdot 0 + 2 \cdot 3 \cdot 1$$

or

$$6 = a_{1_2} + 2d_1'a_{1_2}' + 2d_2'a_{2_2}' = 0 + 2 \cdot 3 \cdot 1 + 2 \cdot 3 \cdot 0.$$

That is, $r = 2$ with $a_{1_1} = a_{1_1}' = 0$, $a_{2_1}' = 1$ and $a_{1_2} = a_{2_2}' = 0$, $a_{1_2}' = 1$. By Theorem 3 *iii*), the number of 6-dimensional hull DC codes of length 26 over $\mathbb{F}_3$ is

$$3(3^3 - 1)(3^6 - 3^3 + 1) + 3(3^6 - 3^3 + 1)(3^3 - 1) = 109668.$$

The following two corollaries are immediate consequences of Theorem 3, which we need in the next section. We have the following enumeration result for LCD DC codes.

Corollary 7 *Let q be a prime power and m be a positive integer relatively prime to q. Then the number of LCD DC codes of length $2m$ over $\mathbb{F}_q$ is given below.*

i) $(q-2)\prod_{i=2}^{s}(q^{2d_i}-q^{d_i}-1)\prod_{j=1}^{t}(q^{2d'_j}-q^{d'_j}+1)$ *when m is odd and* $q \equiv 1 \pmod 4$.
ii) $(q-2)^2\prod_{i=3}^{s}(q^{2d_i}-q^{d_i}-1)\prod_{j=1}^{t}(q^{2d'_j}-q^{d'_j}+1)$ *when m is even and* $q \equiv 1 \pmod 4$.
iii) $(q-1)\prod_{i=2}^{s}(q^{2d_i}-q^{d_i}-1)\prod_{j=1}^{t}(q^{2d'_j}-q^{d'_j}+1)$ *when m is odd and q is even.*
iv) $q\prod_{i=2}^{s}(q^{2d_i}-q^{d_i}-1)\prod_{j=1}^{t}(q^{2d'_j}-q^{d'_j}+1)$ *when m is odd and* $q \equiv 3 \pmod 4$.
v) $q^2\prod_{i=3}^{s}(q^{2d_i}-q^{d_i}-1)\prod_{j=1}^{t}(q^{2d'_j}-q^{d'_j}+1)$ *when m is even and* $q \equiv 3 \pmod 4$.

Proof Since $l=0$, the result follows from Theorem 3 with $r=1$ and $a_{i_1}=a'_{j_1}=0$ for all $1\le i\le s, 1\le j\le t$. □

In light of Theorem 1 *ii*), we obtain the following enumeration result for DC codes with a 1-dimensional hull.

Corollary 8 *Suppose that q is a prime power such that $q \equiv 1 \pmod 4$ or q is even and m is an integer relatively prime to q. Then the number of 1-dimensional hull DC codes of length $2m$ over $\mathbb{F}_q$ is given below.*

i) $2\prod_{i=2}^{s}(q^{2d_i}-q^{d_i}-1)\prod_{j=1}^{t}(q^{2d'_j}-q^{d'_j}+1)$ *when m is odd and* $q \equiv 1 \pmod 4$.
ii) $4(q-2)\prod_{i=3}^{s}(q^{2d_i}-q^{d_i}-1)\prod_{j=1}^{t}(q^{2d'_j}-q^{d'_j}+1)$ *when m is even and* $q \equiv 1 \pmod 4$.
iii) $\prod_{i=2}^{s}(q^{2d_i}-q^{d_i}-1)\prod_{j=1}^{t}(q^{2d'_j}-q^{d'_j}+1)$ *when m is odd and q is even.*

Proof By (2), (4) and (5), we only consider the constituents corresponding to the self-reciprocal linear factors of x^m-1 in order to obtain a DC code with an *l*-dimensional hull with $l=1$. If *m* is odd, then $x-1$ is the only self-reciprocal linear factor of x^m-1. Then parts *i*) and *iii*) follow from Theorem 3 *i*) and *iii*) with $r=1$, $a_{1_1}=1$, $a_{i_1}=a'_{j_1}=0$ for all $2\le i\le s$ and $1\le j\le t$. If *m* is even, then $x+1$ and $x-1$ are the self-reciprocal linear factors. In this case part *ii*) follows from Theorem 3 *ii*) with $r=2$, $a_{1_1}=1$, $a_{i_1}=a'_{j_1}=0$ for all $3\le i\le s$ and $1\le j\le t$ and $a_{2_2}=1$, $a_{1_2}=a_{i_2}=a'_{j_2}=0$ for all $3\le i\le s$ and $1\le j\le t$. □

Remark 1 Enumeration results on self-dual and LCD DC codes can be found in [1, 2], and [39]. These results apply to DC codes whose duals are also DC codes. As discussed in Section 2.2, the dual of a QC code of index ℓ is again a QC code of index ℓ. However, if $C = \langle(1, a(x))\rangle$ is a DC code of length $2m$, that is, a 1-generator QC code of index 2 over $\mathbb{F}_q$, then $C^\perp = \langle(-a(x), 1)\rangle$ is a 1-generator QC code of index 2, but it is not necessarily a DC code. In fact, $C^\perp$ is a DC code if and only if $\gcd(a(x), x^m - 1) = 1$. If $\gcd(a(x), x^m - 1) \neq 1$, then $(1\ 0)$ serves as a generator matrix for one of the constituents, as described in (3). In this case, $(0\ 1)$ is a generator matrix for the corresponding constituent of the dual code, which cannot occur as a constituent of a DC code according to (3). Consequently, such constituents are excluded from the enumeration results in [1, 2], and [39]. In our work, we do not impose the condition that the dual must be a DC code. Instead, we enumerate all DC codes with a prescribed hull dimension, and therefore include these constituents in our counting.

3.2 FC codes with prescribed hull dimensions

Let $C = \langle(1, 0, a(x), b(x)), (0, 1, -b(x^{m-1}), a(x^{m-1}))\rangle \subseteq R_m^4$ be a q-ary FC code of length $4m$. By the CRT decomposition of C, the constituents of C are [4, 2] linear codes C_i, C'_j, C''_j over their defining fields with generator matrices

$$\begin{aligned} G_i &= \begin{pmatrix} 1 & 0 & a(\xi^{u_i}) & b(\xi^{u_i}) \\ 0 & 1 & -b(\xi^{-u_i}) & a(\xi^{-u_i}) \end{pmatrix} \text{ for } 1 \le i \le s, \\ G'_j &= \begin{pmatrix} 1 & 0 & a(\xi^{v_j}) & b(\xi^{v_j}) \\ 0 & 1 & -b(\xi^{-v_j}) & a(\xi^{-v_j}) \end{pmatrix} \text{ for } 1 \le j \le t, \\ G''_j &= \begin{pmatrix} 1 & 0 & a(\xi^{-v_j}) & b(\xi^{-v_j}) \\ 0 & 1 & -b(\xi^{v_j}) & a(\xi^{v_j}) \end{pmatrix} \text{ for } 1 \le j \le t, \end{aligned} \tag{6}$$

respectively, see [40] for further details. We have the following.

I) For the constituents C_i corresponding to the self-reciprocal factors of $x^m - 1$, we have

$$G_i \bar{G}_i^T = \begin{pmatrix} 1 + a(\xi^{u_i})a(\xi^{-u_i}) + b(\xi^{u_i})b(\xi^{-u_i}) & 0 \\ 0 & 1 + a(\xi^{u_i})a(\xi^{-u_i}) + b(\xi^{u_i})b(\xi^{-u_i}) \end{pmatrix}$$

for all $1 \le i \le s$. Clearly, $\operatorname{rank}(G_i \bar{G}_i^T)$ is either 2 or 0 for all $1 \le i \le s$. Therefore, by Proposition 1 *ii*), $h_H(C_i)$ is either 0 or 2 for all $1 \le i \le s$.

II) For the constituents corresponding to the reciprocal pair factors of $x^m - 1$, we have

$$G'_j G''^T_j = \begin{pmatrix} 1 + a(\xi^{v_j})a(\xi^{-v_j}) + b(\xi^{v_j})b(\xi^{-v_j}) & 0 \\ 0 & 1 + a(\xi^{v_j})a(\xi^{-v_j}) + b(\xi^{v_j})b(\xi^{-v_j}) \end{pmatrix},$$

for $1 \le j \le t$. Clearly, $\operatorname{rank}(G'_j G''^T_j)$ is either 2 or 0 for all $1 \le j \le t$. By Proposition 2, $\dim(C'_j \cap C''^\perp_j)$ is 0 or 2. Similarly, $\operatorname{rank}(G''_j G'^T_j)$ is 2 or 0, and hence by Proposition 2, $\dim(C''_j \cap C'^\perp_j)$ is 0 or 2. That is, we have either $C'_j = C''^\perp_j$ and $C''_j = C'^\perp_j$, or $C'_j \cap C''^\perp_j = C''_j \cap C'^\perp_j = \{0\}$.

Therefore, by (2), to determine the number of q-ary FC codes of length $4m$ with an l-dimensional hull, we need to count the [4, 2] linear codes over certain extensions of $\mathbb{F}_q$ satisfying conditions I) and II).

The following lemmas are necessary for the enumeration.

Lemma 9 *[1, Lemma 2.7] If q is odd, then the number of solutions (x, y) of the equation* $1 + x^{1+q} + y^{1+q} = 0$ *in* $\mathbb{F}_{q^2}^2$ *is* $q^3 - q$.

Lemma 10 *[1, Corollary 2.9] If q is odd, then the number of solutions (x, y) of the equation* $1 + x^2 + y^2 = 0$ *in* $\mathbb{F}_q^2$ *is* $q - \eta(-1)$, *where*

$$\eta(x) = \begin{cases} 1 & \text{if } x \text{ is a non-zero square,} \\ 0 & \text{if } x = 0, \\ -1 & \text{if } x \text{ is a non-square.} \end{cases}$$

is the quadratic character of $\mathbb{F}_q$.

We recall that the hull dimension l of a q-ary FC code of length $4m$ satisfies the following, see (2).

$$h(C) = \sum_{i=1}^{s} \deg(g_i(x))\, h_H(C_i) + \sum_{j=1}^{t} \deg(h_j(x)) \left(\dim\left(C_j' \cap C_j''^{\perp}\right) + \dim\left(C_j'' \cap C_j'^{\perp}\right)\right),$$

where $x^m - 1 = \prod_{i=1}^{s} g_i(x) \prod_{j=1}^{t} h_j(x) h_j^*(x)$, $g_i(x)$ is self-reciprocal for $1 \le i \le s$, $h_j(x)$ and $h_j^*(x)$ are reciprocal pairs for $1 \le j \le t$.

If m is odd, then $x - 1$ is the only self-reciprocal linear factor of $x^m - 1$. If m is even, then $x - 1$ and $x + 1$ are the self-reciprocal linear factors. Let $\deg(g_i(x)) = 2d_i$ for nonlinear self-reciprocal factors of $x^m - 1$, and $d_j' = \deg(h_j(x)) = \deg(h_j^*(x))$.

Since each constituent of an FC code contributes either 0 or 2 to the hull dimension, we write $h_H(C_i) = 2a_i$, $\dim(C_j' \cap C_j''^{\perp}) = \dim(C_j'^{\perp} \cap C_j'') = 2a_j'$, where $a_i, a_j' \in \{0, 1\}$ for all $1 \le i \le s$ and $1 \le j \le t$ in (2).

In order to count the number of q-ary FC codes with an l-dimensional hull, we assume that l can be expressed in r different ways as follows.

$$l = 2\left(a_{1_u} + \sum_{i=2}^{s} 2d_i a_{i_u} + \sum_{j=1}^{t} 2d_j' a_{j_u}'\right) \quad \text{when } m \text{ is odd,} \tag{7}$$

$$l = 2\left(a_{1_u} + a_{2_u} + \sum_{i=3}^{s} 2d_i a_{i_u} + \sum_{j=1}^{t} 2d_j' a_{j_u}'\right) \quad \text{when } m \text{ is even,} \tag{8}$$

where $a_{i_u}, a_{j_u}' \in \{0, 1\}$ for all $1 \le i \le s$, $1 \le j \le t$, $1 \le u \le r$.

We obtain the following theorem.

Theorem 4 *Let q be a power of an odd prime and m be a positive integer relatively prime to q. Let η denote the quadratic character of $\mathbb{F}_q$. Suppose that l is a positive integer which can be written as in (7) or (8). Then the number of l-dimensional hull FC codes of length $4m$ over $\mathbb{F}_q$ is given below.*

i) $\sum_{u=1}^{r}(q-\eta(-1))^{a_{1u}}(q^2-q+\eta(-1))^{1-a_{1u}}\prod_{i=2}^{s}(q^{3d_i}-q^{d_i})^{a_{iu}}(q^{4d_i}-q^{3d_i}+q^{d_i})^{1-a_{iu}}\prod_{j=1}^{t}(q^{3d'_j}-q^{d'_j})^{a'_{ju}}(q^{4d'_j}-q^{3d'_j}+q^{d'_j})^{1-a'_{ju}}$ *when m is odd.*

ii) $\sum_{u=1}^{r}(q-\eta(-1))^{a_{1u}+a_{2u}}(q^2-q+\eta(-1))^{2-a_{1u}-a_{2u}}\prod_{i=3}^{s}(q^{3d_i}-q^{d_i})^{a_{iu}}(q^{4d_i}-q^{3d_i}+q^{d_i})^{1-a_{iu}}\prod_{j=1}^{t}(q^{3d'_j}-q^{d'_j})^{a'_{ju}}(q^{4d'_j}-q^{3d'_j}+q^{d'_j})^{1-a'_{ju}}$ *when m is even.*

Proof We have the following number of choices for the constituents of an l-dimensional hull FC code of length $4m$ over $\mathbb{F}_q$.

- If m is odd, then $x-1$ is the only self-reciprocal linear factor of x^m-1. In this case, in the CRT decomposition of an FC code, there is a [4, 2] linear code, say C_1, over $\mathbb{F}_q$ with a generator matrix $G_1 = \begin{pmatrix} 1 & 0 & c_1 & e_1 \\ 0 & 1 & -e_1 & c_1 \end{pmatrix}$, see (6). Then

$$G_1G_1^T = \begin{pmatrix} 1+c_1^2+e_1^2 & 0 \\ 0 & 1+c_1^2+e_1^2 \end{pmatrix}.$$

By Proposition 1 *i*), $h(C_1)=2$ if and only if $1+c_1^2+e_1^2=0$. Since there are $q-\eta(-1)$ solutions $(c_1,e_1)\in\mathbb{F}_q^2$ of the equation $1+x^2+y^2=0$ by Lemma 10, there are $q-\eta(-1)$ choices for C_1 in the case of $h(C_1)=2$. Hence, there are $q^2-q+\eta(-1)$ choices for C_1 in the case of $h(C_1)=0$. If m is even, then $x-1$ and $x+1$ are the self-reciprocal linear factors of x^m-1. In this case, in the CRT decomposition of an FC code, we have two [4, 2] linear codes over $\mathbb{F}_q$, say C_1 and C_2, with generator matrices

$$G_1 = \begin{pmatrix} 1 & 0 & c_1 & e_1 \\ 0 & 1 & -e_1 & c_1 \end{pmatrix}, \quad G_2 = \begin{pmatrix} 1 & 0 & c_2 & e_2 \\ 0 & 1 & -e_2 & c_2 \end{pmatrix},$$

respectively. By the above argument, we have the following cases.

  - In the case of $h(C_1)=h(C_2)=0$, there are $(q^2-q+\eta(-1))^2$ choices for C_1 and C_2.
  - In the case of $h(C_1)=h(C_2)=2$, there are $(q-\eta(-1))^2$ choices for C_1 and C_2.
  - In the case of $h(C_1)\neq h(C_2)$, there are $(q-\eta(-1))(q^2-q+\eta(-1))$ choices for C_1 and C_2.

- The constituents corresponding to the self-reciprocal factors $g_i(x)$ of x^m-1 with $\deg(g_i(x))=2d_i$ are [4, 2] linear codes C_i over $\mathbb{F}_{q^{2d_i}}$, where $2\le i\le s$ when m is odd and $3\le i\le s$ when m is even. Let

$$G_i = \begin{pmatrix} 1 & 0 & c_i & e_i \\ 0 & 1 & -e_i^{q^{d_i}} & c_i^{q^{d_i}} \end{pmatrix}$$

be a generator matrix of C_i, see (6). Then $h_H(C_i) = 2$ if and only if $\mathrm{rank}(G_i\bar{G}_i^T) = 0$ by Proposition 1 *ii*). Since

$$G_i\bar{G}_i^T = \begin{pmatrix} 1 + c_i^{q^{d_i}+1} + e_i^{q^{d_i}+1} & 0 \\ 0 & 1 + c_i^{q^{d_i}+1} + e_i^{q^{d_i}+1} \end{pmatrix},$$

and the number of solutions $(x, y) \in \mathbb{F}^2_{q^{2d_i}}$ of the equation $1 + x^{q^{d_i}+1} + y^{q^{d_i}+1} = 0$ is $q^{3d_i} - q^{d_i}$ by Lemma 9, there are $q^{3d_i} - q^{d_i}$ choices for C_i when $h_H(C_i) = 2$. Hence, there are $q^{4d_i} - q^{3d_i} + q^{d_i}$ choices for C_i when $h_H(C_i) = 0$.

- The constituents corresponding to the reciprocal pair factors $(h_j(x), h_j^*(x))$ with $\deg(h_j(x)) = \deg(h_j^*(x)) = d_j'$ are [4, 2] linear codes over $\mathbb{F}_{q^{d_j'}}$, say C_j' and C_j'', for $1 \le j \le t$. Let

$$G_j' = \begin{pmatrix} 1 & 0 & c_j' & e_j' \\ 0 & 1 & -f_j' & k_j' \end{pmatrix}, \qquad G_j'' = \begin{pmatrix} 1 & 0 & k_j' & f_j' \\ 0 & 1 & -e_j' & c_j' \end{pmatrix}$$

be generator matrices of C_j' and C_j'', respectively, see (6). By Proposition 2, we have $C_j' = C_j''^{\perp}$ if and only if $\mathrm{rank}(G_j'G_j''^T) = 0$. Equivalently,

$$G_j'G_j''^T = \begin{pmatrix} 1 + c_j'k_j' + e_j'f_j' & 0 \\ 0 & 1 + c_j'k_j' + e_j'f_j' \end{pmatrix} = 0,$$

which is equivalent to $1 + c_j'k_j' + e_j'f_j' = 0$. Since the number of solutions $(x_1, y_1, x_2, y_2) \in \mathbb{F}^4_{q^{d_j'}}$ of the equation $1 + x_1y_1 + x_2y_2 = 0$ is $q^{3d_j'} - q^{d_j'}$ by Lemma 6, there are $q^{3d_j'} - q^{d_j'}$ choices for the pair (C_j', C_j'') satisfying $C_j' = C_j''^{\perp}$. Hence, there are $q^{4d_j'} - q^{3d_j'} + q^{d_j'}$ choices for the pair (C_j', C_j'') satisfying $C_j' \cap C_j''^{\perp} = C_j'' \cap C_j'^{\perp} = \{0\}$. Combining the above counting arguments with the choices $a_{i_u}, a_{j_u}' \in \{0, 1\}$ in (7) and (8) yields the result. □

Remark 2 In [40, Theorem 4.3], an enumeration result for LCD FC codes is given. When comparing it with our Theorem 4 in the case $l = 0$, the results do not fully align. Unlike the case of DC codes, see Remark 1, where discrepancies may arise depending on whether DC codes whose duals are not DC are included or excluded, no such issue occurs for FC codes due to their structure. Therefore, the mismatch is not due to a counting distinction of that kind, but rather due to a gap in the formula given in [40]. After a careful examination, we identified the missing detail and corrected the enumeration result for LCD FC codes as follows.

Corollary 11 *Let q be an odd prime power. Then the number of LCD FC codes of length 4m over* $\mathbb{F}_q$ *is given below.*

i) $(q^2 - q + \eta(-1)) \prod_{i=2}^{s}(q^{4d_i} - q^{3d_i} + q^{d_i}) \prod_{j=1}^{t}(q^{4d_j'} - q^{3d_j'} + q^{d_j'})$ *when m is odd.*
ii) $(q^2 - q + \eta(-1))^2 \prod_{i=3}^{s}(q^{4d_i} - q^{3d_i} + q^{d_i}) \prod_{j=1}^{t}(q^{4d_j'} - q^{3d_j'} + q^{d_j'})$ *when m is even.*

Proof Since $l=0$, the result follows from Theorem 4 with $r=1$, $a_{i_1}=a'_{j_1}=0$ for all $1\leq i\leq s, 1\leq j\leq t$. □

The following corollary is an immediate consequence of Theorem 4, which we need in the next section. We have the following enumeration result for 2-dimensional hull FC codes.

Corollary 12 *Let q be an odd prime power. Then the number of 2-dimensional hull FC codes of length 4m over* $\mathbb{F}_q$ *is given below.*

i) $(q-\eta(-1))\prod_{i=2}^{s}(q^{4d_i}-q^{3d_i}+q^{d_i})\prod_{j=1}^{t}(q^{4d'_j}-q^{3d'_j}+q^{d'_j})$ *when m is odd.*
ii) $2(q-\eta(-1))(q^2-q+\eta(-1))\prod_{i=3}^{s}(q^{4d_i}-q^{3d_i}+q^{d_i})\prod_{j=1}^{t}(q^{4d'_j}-q^{3d'_j}+q^{d'_j})$ *when m is even.*

Proof By (2), (7) and (8), we only consider the constituents corresponding to the self-reciprocal linear factors of x^m-1 to obtain an FC code with an *l*-dimensional hull with $l=2$. If *m* is odd, then $x-1$ is the only self-reciprocal linear factor of x^m-1. Then part *i*) follows from Theorem 4 *i*) with $r=1$, $a_{1_1}=1$, $a_{i_1}=a'_{j_1}=0$ for all $2\leq i\leq s$ and $1\leq j\leq t$. If *m* is even, then $x+1$ and $x-1$ are the self-reciprocal linear factors. In this case part *ii*) follows from Theorem 4 *ii*) with $r=2$, $a_{1_1}=1$, $a_{i_1}=a'_{j_1}=0$ for all $2\leq i\leq s, 1\leq j\leq t$ and $a_{2_2}=1$, $a_{1_2}=a_{i_2}=a'_{j_2}=0$ for all $3\leq i\leq s, 1\leq j\leq t$. □

We present the following examples, in which the results have been confirmed using the MAGMA computer algebra system [7].

Example 3 Let $q=3$ and $m=8$. Then the factorization of x^8-1 into monic irreducible polynomials over $\mathbb{F}_3$ is given by

$$x^8-1=(x+1)(x+2)(x^2+1)(x^2+x+2)(x^2+2x+2).$$

In this factorization, the self-reciprocal factors are $g_1(x)=x+1$, $g_2(x)=x+2$, and $g_3(x)=x^2+1$, while the reciprocal pair factors are $h_1(x)=x^2+x+2$, $h_1^*(x)=x^2+2x+2$. We then have $d_3=\deg(g_3(x))/2=1$, $d'_1=\deg h_1(x)=\deg(h_1^*(x))=2$. By Corollary 11 *ii*), the number of LCD FC codes of length 32 over $\mathbb{F}_3$ is

$$(3^2-3-1)^2(3^4-3^3+3)(3^8-3^6+3^2)=8323425.$$

For $l=8$, we have $r=2$ by (8), since

$$8=2\left(a_{1_1}+a_{2_1}+2d_3a_{3_1}+2d'_1a'_{1_1}\right)=2(1+1+2\cdot 1\cdot 1+2\cdot 2\cdot 0)$$

or

$$8=2\left(a_{1_2}+a_{2_2}+2d_3a_{3_2}+2d'_1a'_{1_2}\right)=2(0+0+2\cdot 1\cdot 0+2\cdot 2\cdot 1).$$

That is, $r = 2$ with $a_{1_1} = a_{2_1} = a_{3_1} = 1$, $a'_{1_1} = 0$ and $a_{1_2} = a_{2_2} = a_{3_2} = 0$, $a'_{1_2} = 1$. By Theorem 4 *ii*), the number of 8-dimensional hull FC codes of length 32 over $\mathbb{F}_3$ is

$$(3+1)^2(3^3-3)(3^8-3^6+3^2)+(3^2-3-1)^2(3^4-3^3+3)(3^6-3^2) = 3268944.$$

Remark 3 In [39, Theorem 3.10] and [39, Theorem 3.11] the enumeration formulas of Euclidean self-dual FC codes and Euclidean LCD FC codes are given, under the condition that all the irreducible factors of $x^m - 1$ are self-reciprocal, and the case $x^m - 1$ has reciprocal pair factors is left open. Corollary 11 answers this open problem for LCD FC codes. More generally, Theorem 4 provides an enumeration not only for LCD FC and Euclidean self-dual FC codes but FC codes with arbitrary hull dimension for arbitrary *m*.

4 Asymptotic performance

This section analyzes the asymptotic behavior of DC and FC codes with small hull dimensions, namely LCD DC codes, LCD FC codes, DC codes with a 1-dimensional hull, and FC codes with a 2-dimensional hull. Although the asymptotic behavior of LCD DC and LCD FC codes was previously studied in [39, Theorem 5.5] and [40, Theorem 5.2] respectively, we include these cases for completeness, as our enumeration formulas differ from the formulas presented in the earlier studies, see Remarks 1 and 2.

Let *C*(*n*) be a family of *q*-ary $[n, k_n, d_n]$ linear codes. The rate and relative distance of *C*(*n*) are defined as

$$R = \lim_{n\to\infty} \sup \frac{k_n}{n}, \quad \text{and} \quad \delta = \lim_{n\to\infty} \inf \frac{d_n}{n},$$

respectively. The family *C*(*n*) is called asymptotically good if $R\delta > 0$.

An integer *g* is called a primitive root modulo *m* if it generates the group of units U_m of the ring $\mathbb{Z}_m$. Artin's conjecture on primitive roots, which was proved in [18] under the Generalized Riemann Hypothesis, states that any non-square positive integer is a primitive root modulo infinitely many primes *m*. This implies that for a non-square *q*, there exist infinitely many primes *m* such that $x^m - 1$ factors into two irreducible polynomials over $\mathbb{F}_q$ as $x^m - 1 = (x-1)(x^{m-1} + \cdots + x + 1) = (x-1)g(x)$. In this case, the non-zero codewords of the cyclic code of length *m* generated by the polynomial *g*(*x*) are called the constant vectors.

We recall that the weight of a polynomial $u(x) \in R_m$ is the number of terms in *u*(*x*) and the weight of an element $\vec{u}(x) = (u_0(x), \ldots, u_{\ell-1}(x)) \in R_m^\ell$ is the sum of the weights of its coordinates.

We need the following lemma.

Lemma 13 *[2, Lemma 6] Let q be a non-square odd prime power and m be a prime such that $x^m - 1$ has only two irreducible factors over $\mathbb{F}_q$. If $0 \neq u(x) \in R_m^2$ has weight less than m, then there are at most q polynomials a(x) such that $u(x) \in C_a = \langle (1, a(x)) \rangle$.*

The q-ary entropy function is defined by

$$H_q(t) = t\log_q(q-1) - t\log_q(t) - (1-t)\log_q(1-t) \text{ for } 0 < t < 1 - \frac{1}{q}.$$

This function is used in the estimation of the volume of high-dimensional Hamming balls when the base field is $\mathbb{F}_q$. The result we use is that the volume of the Hamming ball of radius *tm* (i.e., the number of vectors of weight at most *tm*) is up to subexponential terms, $q^{mH_q(t)}$, when $0 < t < 1 - \frac{1}{q}$ and *m* goes to infinity, see [19, Lemma 2.10.3].

In our proofs, we employ the classical expurgated random coding technique to demonstrate that sequences of codes from the families under consideration possess sufficiently large minimum distance. To analyze their asymptotic behavior, we estimate the number of codes with small minimum distance and establish the existence of codes with suitably large minimum distance within each family.

Throughout the analysis, we use the notation $f(m) = O(g(m))$ to indicate that there exists a constant $C > 0$ such that $|f(m)| \leq C|g(m)|$ for all sufficiently large m. This provides a convenient way to express that the growth of $f(m)$ is bounded above by that of $g(m)$, up to a constant factor.

Theorem 5 *i)* *Let q be a non-square prime power. Then under Artin's conjecture, there are infinite families of q-ary LCD DC codes of relative distance* $\delta \geq H_q^{-1}(\frac{1}{2})$. *In particular, this family of codes is asymptotically good.*

ii) *Let q be a non-square prime power, which is even or* $q \equiv 1 \pmod 4$. *Then under Artin's conjecture, there are infinite families of q-ary 1-dimensional hull DC codes of relative distance* $\delta \geq H_q^{-1}(\frac{1}{2})$. *In particular, this family of codes is asymptotically good.*

Proof Let q be fixed and *m* be a prime that satisfies Artin's conjecture for q. Then $x^m - 1 = (x-1)g(x)$, where *g*(*x*) is a self-reciprocal irreducible polynomial of degree $m-1$ over $\mathbb{F}_q$.

i) Let

$$\Gamma_m = |\{C \mid C \text{ is a } q\text{-ary } [2m, m] \text{ LCD DC code}\}|,$$

and let δ denote the relative distance of the family of [2*m*, *m*] LCD DC codes. Then, by Corollary 7 *i*), *iii*), and *iv*), we have

$$\Gamma_m = (q-2)(q^{m-1} - q^{\frac{m-1}{2}} - 1), \text{ if } q \equiv 1 \pmod 4,$$
$$\Gamma_m = (q-1)(q^{m-1} - q^{\frac{m-1}{2}} - 1), \text{ if } q \text{ is even},$$
$$\Gamma_m = q(q^{m-1} - q^{\frac{m-1}{2}} - 1), \text{ if } q \equiv 3 \pmod 4.$$

In all three cases, we have $\Gamma_m = O(q^m) \quad$ as $m \to \infty$. Let γ_m denote the number of DC codes of length 2*m* containing a codeword of weight at most $d \sim 2m\delta_0$, where $0 < \delta_0 < 1$ is fixed. Then, by Lemma 13 and [19, Lemma 2.10.3], we have $\gamma_m = O\left(q^{2mH_q(\delta_0)}\right)$. To show the existence of codes with minimum distance at least *d*, it suffices to show that $\gamma_m/\Gamma_m \to 0$ as $m \to \infty$. Since $\Gamma_m = O(q^m)$, we obtain $\frac{\gamma_m}{\Gamma_m} = O\left(q^{m(2H_q(\delta_0)-1)}\right)$, which tends to zero as $m \to \infty$ whenever $H_q(\delta_0) < \frac{1}{2}$. Since this holds for every δ_0 satisfying $H_q(\delta_0) < \frac{1}{2}$, by the definition of the asymptotic relative distance we obtain $\delta \geq H_q^{-1}\left(\frac{1}{2}\right)$. Therefore, this family is asymptotically good.

ii) Let

$$\Lambda_m = |\{C \mid C \text{ is a } q\text{-ary } [2m, m] \text{ 1-dimensional hull DC code}\}|.$$

Then by Corollary 8 *i*) and *iii*), we have

$$\Lambda_m = 2(q^{m-1} - q^{\frac{m-1}{2}} - 1), \text{ if } q \equiv 1 \pmod 4,$$
$$\Lambda_m = (q^{m-1} - q^{\frac{m-1}{2}} - 1), \text{ if } q \text{ is even}.$$

In both cases, $\Lambda_m = O(q^m) \quad \text{as } m \to \infty$. The proof for the remaining part follows similarly to that of part *i*). □

Remark 4 The lower bound on the relative distances of the infinite families of q-ary LCD DC and 1-dimensional hull DC codes obtained in Theorem 5 meets the Gilbert-Varshamov bound on q-ary linear codes of rate 1/2, see [19, Theorem 2.10.8].

In [40, Theorem 5.2] a bound on the relative distance of the family of LCD FC codes is given. After revising the enumeration result in [40, Theorem 5.2] and Corollary 11, we improve the bound on the relative distance.

We need the following lemma.

Lemma 14 *[40, Lemma 5.1] Let q be a non-square prime power, m be prime such that* $x^m - 1$ *has only two irreducible factors over* $\mathbb{F}_q$*. Let* $\tilde{u}(x) = (u_1(x), u_2(x), u_3(x), u_4(x)) \in R_m^4$ *and suppose that* $u_1(x)\tilde{u_1}(x) + u_2(x)\tilde{u_2}(x)$ *is not a constant vector, where* $\tilde{u_i}(x) \equiv u_i(x^{m-1}) \pmod{x^m - 1}$ *for* $i = 1, 2$*. Then there are at most* q^2 *FC codes C over* R_m *such that* $u(x) \in C$.

We have the following theorem.

Theorem 6 *Let q be a non-square prime power. Then under Artin's conjecture, there are infinite families of q-ary LCD FC and 2-dimensional hull FC codes of relative distance* $\delta \geq H_q^{-1}(\frac{1}{2})$*. In particular, these families of codes are asymptotically good.*

Proof Let q be fixed, and let m be an odd prime such that $x^m - 1 = (x-1)g(x)$, where $g(x)$ is a self-reciprocal irreducible polynomial of degree $m-1$ over $\mathbb{F}_q$. Consider the family of $[4m, 2m]$ LCD FC codes.

Let

$$\Gamma_m = |\{C \mid C \text{ is a } q\text{-ary } [4m, 2m] \text{ LCD FC code}\}|,$$

and let δ denote the relative distance of this family. Then by Corollary 11, we have

$$\Gamma_m = \left(q^2 - q + \eta(-1)\right)\left(q^{4\left(\frac{m-1}{2}\right)} - q^{3\left(\frac{m-1}{2}\right)} + q^{\frac{m-1}{2}}\right).$$

As $m \to \infty$, this yields $\Gamma_m = O\left(q^2 q^{4\left(\frac{m-1}{2}\right)}\right) = O(q^{2m})$.

Let γ_m denote the number of [4*m*, 2*m*] FC codes containing a codeword of weight at most $d \sim 4m\delta_0$, where $0 < \delta_0 < 1$ is fixed. Then, by Lemma 14 and [19, Lemma 2.10.3], we have $\gamma_m = O\left(q^{4mH_q(\delta_0)}\right)$.

To show the existence of codes with minimum distance at least *d*, it suffices to show that $\gamma_m/\Gamma_m \to 0$ as $m \to \infty$. Since $\Gamma_m = O(q^{2m})$, we obtain $\frac{\gamma_m}{\Gamma_m} = O\left(q^{m(4H_q(\delta_0)-2)}\right)$, which tends to zero as $m \to \infty$ whenever $H_q(\delta_0) < \frac{1}{2}$. Since this holds for every δ_0 satisfying $H_q(\delta_0) < \frac{1}{2}$, by the definition of the asymptotic relative distance we obtain $\delta \geq H_q^{-1}\left(\frac{1}{2}\right)$.

For the $[4m, 2m]$ FC code family, the rate is $R = \frac{2m}{4m} = \frac{1}{2}$. Therefore, $R\delta > 0$, and this family is asymptotically good.

In a similar manner, if

$$\Lambda_m = \left|\{C \mid C \text{ is a } q\text{-ary } [4m, 2m] \text{ 2-dimensional hull FC code}\}\right|,$$

then by Corollary 12, we have

$$\Lambda_m = \left(q - \eta(-1)\right)\left(q^{4\left(\frac{m-1}{2}\right)} - q^{3\left(\frac{m-1}{2}\right)} + q^{\frac{m-1}{2}}\right) = O(q^{2m}),$$

as $m \to \infty$. The proof for the remaining part follows in the same way as for the family of LCD FC codes. □

Remark 5 The lower bound on the relative distance of the infinite families of q-ary LCD FC and 2-dimensional hull FC codes obtained in Theorem 6, meets the Gilbert-Varshamov bound for *q*-ary linear codes of rate 1/2, see [19, Theorem 2.10.8].

5 Conclusion

In this work, we provide enumeration formulas for DC codes of length $2m$ and FC codes of length $4m$ over $\mathbb{F}_q$, where $\gcd(m, q) = 1$, with prescribed Euclidean hull dimension. Our results extend previous work by allowing arbitrary values of m and general hull dimensions. Earlier studies, such as [39, Theorems 3.10 and 3.11], considered only special cases where all irreducible factors of $x^m - 1$ are self-reciprocal, leaving the case involving reciprocal pair factors unresolved. Moreover, enumeration was limited to specific families, such as Euclidean self-dual and Euclidean LCD DC and FC codes, without addressing codes with arbitrary hull dimensions. Our formulas overcome these limitations and resolve the open problem posed in [39].

We also correct the enumeration formula given in [40, Theorem 5.2] and, as a consequence, improve the lower bound on the relative distance of LCD FC codes, as stated in Corollary 11. Using our formulas, we demonstrate that families of LCD DC codes, LCD FC codes, DC codes with a 1-dimensional hull, and FC codes with a 2-dimensional hull are asymptotically good. In particular, these code families, all of rate $1/2$, satisfy a modified Gilbert-Varshamov bound for linear codes over $\mathbb{F}_q$.

Acknowledgements The authors would like to thank Patrick Solé and Buket Özkaya for valuable discussions and Nurdagül Anbar for her suggestions that improved the quality of the presentation of the paper. This study was supported by the Scientific and Technological Research Council of Turkey (TUBITAK) under Grant Number 223N065. Z.A. thanks to TUBITAK for their support. T. K. is supported by the FWF Project P 35138.

Author Contributions All the authors contributed equally to the manuscript.

Funding Open access funding provided by the Scientific and Technological Research Council of Türkiye (TÜBİTAK).

Data Availability No datasets were generated or analysed during the current study.

Declarations

Competing Interests The authors declare no competing interests.

References

1. Alahmadi, A., Güneri, C., Özkaya, B., Shoaib, H., Solé, P.: On complementary dual multinegacirculant codes. Cryptogr. Commun. **12**, 101–113 (2020)
2. Alahmadi, A., Özdemir, F., Solé, P.: On self-dual double circulant codes. Des. Codes Cryptogr. **86**, 1257–1265 (2018)
3. Aliabadi, Z., Güneri, C., Kalaycı, T.: On the hull and complementarity of 1-generator quasi-cyclic codes and four-circulant codes. J. Algebra Appl. **24**(13–14), Paper No. 2541016, 16 pp (2025)
4. Assmus, E.F., Key, J.D.: Affine and projective planes. Discrete Math. **83**(2–3), 161–187 (1990)
5. Assmus, E.F., Mattson, H.F., Turyn, R.: Cyclic Codes. AF Cambridge Research Labs, Bedford, MA, USA, Summary Science Report AFCRL–66–348 (1966)
6. Bhasin, S., Danger, J.L., Guilley, S., Najm, Z., Ngo, X.T.: Linear complementary dual code improvement to strengthen encoded circuit against hardware Trojan horses. In: IEEE Int. Symp. Hardware Oriented Security and Trust, pp. 82–87 (2015). IEEE
7. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symbolic Comput. **24**, 235–265 (1997)
8. Bringer, J., Carlet, C., Chabanne, H., Guilley, S., Maghrebi, H.: Orthogonal direct sum masking: a smartcard friendly computation paradigm in a code, with built-in protection against side-channel and fault attacks. In: WISTP 2014, Lect. Notes Comput. Sci. 8501, pp. 40–56 (2014). Springer
9. Carlet, C., Guilley, S.: Complementary dual codes for counter-measures to side-channel attacks. Adv. Math. Commun. **10**(1), 131–150 (2016)
10. Carlet, C., Li, C., Mesnager, S.: Linear codes with small hulls in semi-primitive case. Des. Codes Cryptogr. **87**(12), 3063–3075 (2019)
11. Chen, C.L., Peterson, W.W., Weldon, E.J., Jr.: Some results on quasi-cyclic codes. Inf. Control **15**, 407–423 (1969)
12. Evra, S., Kowalski, E., Lubotzky, A.: Good cyclic codes and the uncertainty principle. Enseign. Math. **63**(3–4), 305–332 (2017)
13. Grassl, M.: Bounds on the minimum distance of linear codes and quantum codes. Online available at http://www.codetables.de

14. Guenda, K., Jitman, S., Gulliver, T.A.: Constructions of good entanglement-assisted quantum error correcting codes. Des. Codes Cryptogr. **86**, 121–136 (2018)
15. Guenda, K., Gulliver, T.A., Jitman, S., Thipworawimon, S.: Linear ℓ-intersection pairs of codes and their applications. Des. Codes Cryptogr. **88**, 133–152 (2020)
16. Güneri, C., Özbudak, F.: The concatenated structure of quasi-cyclic codes and an improvement of Jensen's Bound. IEEE Trans. Inform. Theory **59**(2), 979–985 (2013)
17. Güneri, C., Özkaya, B., Solé, P.: Quasi-cyclic complementary dual codes. Finite Fields Appl. **42**, 67–80 (2016)
18. Hooley, C.: On Artin's conjecture. J. Reine Angew. Math. **225**, 209–220 (1967)
19. Huffman, W.C., Pless, V.: Fundamentals of Error Correcting Codes. Cambridge University Press, Cambridge (2003)
20. Kasami, T.: An upper bound on $\frac{k}{n}$ for affine-invariant codes with fixed $\frac{d}{n}$. IEEE Trans. Inform. Theory **15**(1), 174–176 (1969)
21. Li, C., Zeng, P.: Constructions of linear codes with one-dimensional hull. IEEE Trans. Inform. Theory **65**(3), 1668–1676 (2019)
22. Lin, S., Weldon, E.J., Jr.: Long BCH codes are bad. Inf. Control **11**, 445–451 (1967)
23. Ling, S., Solé, P.: On the algebraic structure of quasi-cyclic codes III: generator theory. IEEE Trans. Inform. Theory **51**, 2692–2700 (2005)
24. Ling, S., Solé, P.: Good self-dual quasi-cyclic codes exist. IEEE Trans. Inform. Theory **49**(4), 1052–1053 (2003)
25. Ling, S., Solé, P.: On the algebraic structure of quasi-cyclic codes I: finite fields. IEEE Trans. Inform. Theory **47**(7), 2751–2760 (2001)
26. Martinez-Perez, C., Willems, W.: Is the class of cyclic codes asymptotically good? IEEE Trans. Inform. Theory **52**, 696–700 (2006)
27. Massey, J.L.: Linear codes with complementary duals. Discrete Math. **106–107**, 337–342 (1992)
28. Mi, J.F., Cao, X.W.: Asymptotically good quasi-cyclic codes of fractional index. Discrete Math. **341**, 308–314 (2018)
29. Pless, V.: On the uniqueness of the Golay codes. J. Comb. Theory **5**, 215–228 (1968)
30. Seguin, G.E.: A class of 1-generator quasi-cyclic codes. IEEE Trans. Inform. Theory **50**, 1745–1753 (2004)
31. Sendrier, N.: Finding the permutation between equivalent codes: the support splitting algorithm. IEEE Trans. Inform. Theory **46**(4), 1193–1203 (2000)
32. Shi, M.J., Bian, X.P., Solé, P.: Double circulant codes from cubic cyclotomy. Finite Fields Appl. **104**, Paper No. 102593, 19 pp (2025)
33. Shi, M.J., Zhu, H.W., Qian, L.Q., Sok, L., Solé, P.: On self-dual and LCD double circulant and double negacirculant codes over $\mathbb{F}_q + u\mathbb{F}_q$. Cryptogr. Commun. **12**(1), 53–70 (2020)
34. Shi, M.J., Huang, D.T., Sok, L., Solé, P.: Double circulant LCD codes over $\mathbb{Z}_4$. Finite Fields Appl. **58**, 133–144 (2019)
35. Shi, M.J., Qian, L.Q., Solé, P.: On self-dual negacirculant codes of index two and four. Des. Codes Cryptogr. **86**(11), 2485–2494 (2018)
36. Shi, M.J., Qian, L., Liu, Y., Solé, P.: Good self-dual generalized quasi-cyclic codes exist. Inform. Process. Lett. **118**, 21–24 (2017)
37. Sok, L.: On linear codes with one-dimensional Euclidean hull and their applications to EAQECCs. IEEE Trans. Inform. Theory **68**(7), 4329–4343 (2022)
38. Wu, R.S., Shi, M.J.: A modified Gilbert-Varshamov bound for self-dual quasi-twisted codes of index four. Finite Fields Appl. **62**, Paper No. 101627, 11 pp (2020)
39. Zhu, H., Shi, M.J.: Several classes of asymptotically good quasi-twisted codes with a low index. J. Appl. Math. Comput. **68**, 1227–1244 (2022)
40. Zhu, H., Shi, M.J.: On linear complementary dual four circulant codes. Bull. Aust. Math. Soc. **98**(1), 159–166 (2018)