Turkish Journal of Mathematics

Volume 48 | Number 5 Article 4

9-10-2024

A note on the hull and linear complementary pair of cyclic codes

ZOHREH ALIABADI

TEKGÜL KALAYCI

Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2024) 48: 861 – 873

doi:10.55730/1300-0098.3545

A note on the hull and linear complementary pair of cyclic codes

Zohreh ALIABADI*, **Tekgül KALAYCI**
Department of Mathematics, Faculty of Engineering and Natural Sciences, Sabancı University, İstanbul, Turkiye

Received: 05.04.2023 • **Accepted/Published Online:** 04.06.2024 • **Final Version:** 10.09.2024

Abstract: The Euclidean hull of a linear code C is defined as $C \cap C^{\perp}$, where $C^{\perp}$ denotes the dual of C under the Euclidean inner product. A linear code with the trivial hull is called a linear complementary dual (LCD) code. A pair (C, D) of linear codes of length n over the finite field $\mathbb{F}_q$ is called a linear complementary pair (LCP) of codes if $C \oplus D = \mathbb{F}_q^n$. More generally, a pair (C, D) of linear codes of the same length over $\mathbb{F}_q$ is called a linear ℓ-intersection pair of codes if $C \cap D$ has dimension ℓ as a vector space over $\mathbb{F}_q$. In this paper, we give characterizations of LCD, LCP of cyclic codes and one-dimensional hull cyclic codes of length $q^m - 1$, $m \geq 1$, over $\mathbb{F}_q$ in terms of their basic dual zero sets and their trace representations. We also formulate the hull dimension of a cyclic code of arbitrary length over $\mathbb{F}_q$ with respect to its basic dual zero set. Moreover, we provide a general formula for the dimension ℓ of the intersection of two cyclic codes of arbitrary length over $\mathbb{F}_q$ based on their basic dual zero sets.

Key words: Cyclic codes, hull of linear codes, linear complementary dual codes, linear complementary pair of codes, trace representation, basic dual zero set

1. Introduction

Throughout the paper, $\mathbb{F}_q$ denotes the finite field of q elements, q is a prime power, n is a positive integer such that $\gcd(n, q) = 1$, where $\gcd(n, q)$ denotes the greatest common divisor of n and q, and $\mathbb{F}_q^n$ is the vector space of n-tuples over $\mathbb{F}_q$. A linear code over $\mathbb{F}_q$ of length n and dimension k is a k-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$, and a codeword is an element of the linear code. For a linear code C of length n, the (Euclidean) dual of C, which is denoted by $C^{\perp}$, is defined as

$$C^{\perp} = \{x \in \mathbb{F}_q^n \mid < c, x >= \sum_{i=0}^{n-1} c_i x_i = 0 \text{ for all } c \in C\}.$$

The Euclidean hull of a linear code 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. Obviously, $\mathrm{Hull}(C)$ is also a linear code over $\mathbb{F}_q$. We denote the $\mathbb{F}_q$-dimension of the subspace $\mathrm{Hull}(C)$ of $\mathbb{F}_q^n$ by $h(C)$.

The concept of the hull has been introduced by Assumus and Key in [1] in order to classify finite projective planes. The hull of a linear code has applications in classical linear codes and quantum error-correcting codes, see [11, 15–17, 19]. It turns out that the algorithms for determining permutation equivalence between two codes

*Correspondence: zaliabadi@sabanciniv.edu
2010 *AMS Mathematics Subject Classification:* 94B15, 11T71

and determining the automorphism group of a linear code are more effective when the size of the hull dimension of the code is small.

A zero-dimensional hull linear code is called linear complementary dual (LCD) code, which has been introduced by Massey in [13]. If C is an LCD code of length n over $\mathbb{F}_q$, then $C \oplus C^{\perp} = \mathbb{F}_q^n$. More generally, a pair (C, D) of linear codes of length n over $\mathbb{F}_q$ is called a linear complementary pair (LCP) of codes if $C \oplus D = \mathbb{F}_q^n$. Clearly, if C is an LCD code, then the pair $(C, C^{\perp})$ is LCP of codes.

The study of LCD and LCP of codes has a cryptographic motivation. It has been shown that certain cryptosystems, which are defined via linear codes, are more secure against side-channel attacks (SCA) and fault-injection attacks (FIA) when LCD or LCP of codes are used in their constructions, see [2, 3, 6]. Due to the above-mentioned applications, codes with small hull dimension (especially one-dimensional hull codes) are studied in the recent literature, see [4, 12, 17, 18] and references therein.

As a generalization of linear complementary pairs of codes and hulls, the concept of linear ℓ-intersection pair of codes over a finite field has been introduced in [7]. A pair (C, D) of linear codes is called a linear ℓ-intersection pair of codes if $\dim(C \cap D) = \ell$, where $\dim(C \cap D)$ denotes the $\mathbb{F}_q$-dimension of the subspace $C \cap D$ of $\mathbb{F}_q^n$. In [7], characterizations and constructions of linear ℓ-intersection pairs of codes in terms of the generator and parity check matrices of the codes is provided and as an application, these pairs of codes are used to construct quantum error-correcting codes.

The class of cyclic codes is a particular class of linear codes with an interesting algebraic structure. It is well-known that a cyclic code C of length n over $\mathbb{F}_q$ can be identified with an ideal of the factor ring $\mathbb{F}_q[x]/ < x^n - 1 >$, where $\mathbb{F}_q[x]$ denotes the polynomial ring in one variable x with coefficients in $\mathbb{F}_q$ and $< x^n - 1 >$ denotes the ideal of $\mathbb{F}_q[x]$ generated by the polynomial $x^n - 1$. Since the ring $\mathbb{F}_q[x]/ < x^n - 1 >$ is a principal ideal domain, the ideal of $\mathbb{F}_q[x]/ < x^n - 1 >$ corresponding to C is generated by a unique monic polynomial over $\mathbb{F}_q$ that divides $x^n - 1$, which is called the generator polynomial of C. The parity check polynomial of C is obtained by dividing $x^n - 1$ by the generator polynomial of C. The reciprocal polynomial of the parity check polynomial is the generator polynomial of $C^{\perp}$.

In the literature, the results on the LCD, LCP of cyclic codes, hull dimensions of cyclic codes and linear ℓ-intersection pair of cyclic codes have been obtained by using the generator and parity check polynomials of the codes, to the best of our knowledge. In [21], it has been shown that a cyclic code is LCD if and only if its generator polynomial is self-reciprocal. In [5], it has been shown that a pair of cyclic codes of length n over $\mathbb{F}_q$ is an LCP of codes if and only if their generator polynomials are relatively prime over $\mathbb{F}_q$ and the product of the generator polynomials is $x^n - 1$. Similarly, a linear ℓ-intersection pair of cyclic codes has been characterized in [9] in terms of their generator and parity check polynomials. The possible hull dimensions of a cyclic code of length n over $\mathbb{F}_q$ is formulated in [14] by analysing the irreducible factors of $x^n - 1$ over $\mathbb{F}_q$. In [12], by using the generator polynomial of a cyclic code, one-dimensional hull cyclic codes have been characterized in terms of their defining sets.

In [20], a trace representation of a cyclic code C of length $q^m - 1$, $m \geq 1$, over $\mathbb{F}_q$ has been given by using the basic dual zero set of C. The trace representation of C enables one to obtain the codewords of C explicitly; hence, one can work on the code C in $\mathbb{F}_q^n$ rather than the polynomial representation of C in the ring $\mathbb{F}_q[x]/ < x^n - 1 >$. In this paper, differently from the results in the literature, the characterizations of LCD, LCP of cyclic codes and one-dimensional hull cyclic codes of length $q^m - 1$ over $\mathbb{F}_q$ are given in terms of their

basic dual zero sets, by using the trace representation. Furthermore, a formula for the hull dimension of a cyclic code of arbitrary length in terms of its basic dual zero set is obtained. More generally, a linear ℓ-intersection pair of cyclic codes of the same length is characterized in terms of the basic zero dual sets of the codes.

The paper is organized as follows. In Section 1, we recall the basic definitions and results on cyclic codes and polynomials over finite fields. In Sections 3 and 4, LCD and one-dimensional hull cyclic codes of length q^m-1 over $\mathbb{F}_q$ are studied, respectively. Moreover, the hull of a cyclic code of arbitrary length n over $\mathbb{F}_q$ is formulated. In Section 5, we study the LCP of cyclic codes of length q^m-1 over $\mathbb{F}_q$. Furthermore, a general formula for the dimension ℓ of the intersection of two cyclic codes of arbitrary length over $\mathbb{F}_q$ based on their basic dual zero sets is provided.

2. Preliminaries

We recall that $\mathbb{F}_q$ denotes the finite field of q elements, q is a prime power, n is a positive integer such that $\gcd(n,q)=1$ and $\mathbb{F}_q^n$ is the vector space of n-tuples over $\mathbb{F}_q$. A linear code over $\mathbb{F}_q$ of length n and dimension k is a k-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$, and a codeword is an element of the linear code. In this section, we review cyclic codes, some properties of polynomials over finite fields and trace representation cyclic codes.

2.1. Cyclic codes

A linear code over $\mathbb{F}_q$ of length n is called cyclic, if any cyclic shift of a codeword is again a codeword, i.e., $(c_0,\ldots,c_{n-1})\in C$ implies $(c_{n-1},c_0,\ldots,c_{n-2})\in C$. Clearly, the dual of a cyclic code is also cyclic.

Let C be a linear code of length n over $\mathbb{F}_q$ and c be a codeword. If $c=(c_0,\ldots,c_{n-1})$ is identified with the polynomial $c(x)=\sum_{i=0}^{n-1}c_ix^i$ over $\mathbb{F}_q$, then the code C can be seen as a subset of the ring $\mathbb{F}_q[x]/<x^n-1>$. If C is a cyclic code, then any cyclic shift of a codeword is also a codeword, i.e., the set $\{c(x)\mid c\in C\}$ is an ideal of $\mathbb{F}_q[x]/<x^n-1>$. Since $\mathbb{F}_q[x]/<x^n-1>$ is a principal ideal domain, any ideal of $\mathbb{F}_q[x]/<x^n-1>$ has a unique monic generator.

We recall that for a polynomial $f(x)\in\mathbb{F}_q[x]$ with $f(0)\neq 0$, the polynomial $f^*(x)=\frac{1}{f(0)}x^{\deg f(x)}f(\frac{1}{x})$ is called the reciprocal polynomial of $f(x)$, where $\deg f(x)$ denotes the degree of $f(x)$. A polynomial $f(x)$ is called self-reciprocal if $f(x)=f^*(x)$. Let $g(x)$ be the generator polynomial of a cyclic code C, i.e., $C=<g(x)>$. Then $C^\perp=<h^*(x)>$, where $h(x)=\frac{x^n-1}{g(x)}$ and $h^*(x)$ is the reciprocal polynomial of $h(x)$. The polynomial $h(x)$ is called the parity check polynomial of C. Since the generator polynomial of a cyclic code of length n over $\mathbb{F}_q$ is a factor of x^n-1, we recall the factorization of x^n-1 into monic irreducible polynomials over $\mathbb{F}_q$.

2.2. Factorization of x^n-1

We recall that n and q are relatively prime. Let a be a positive integer. Then the q-cyclotomic coset B_a of a modulo n is defined as follows:

$$B_a=\{a,aq,\ldots,aq^{\delta_a-1}\},$$

where δ_a is the smallest positive integer such that $aq^{\delta_a}\equiv a \pmod n$. Note that the number δ_a is the cardinality of B_a, and it is denoted by $|B_a|$. Clearly, for two positive integers a_1,a_2, either $B_{a_1}=B_{a_2}$ or $B_{a_1}\cap B_{a_2}=\emptyset$. Let $B(n,q)$ be the set of all the q-cyclotomic coset leaders modulo n. Then $\cup_{a\in B(n,q)}B_a=\mathbb{Z}_n$.

That is, the set of q-cyclotomic cosets modulo n forms a partition of $\mathbb{Z}_n$. Let α be a primitive n-th root of unity over $\mathbb{F}_q$. Then the minimal polynomial $m_{\alpha^i}(x)$ of α^i over $\mathbb{F}_q$ is

$$m_{\alpha^i}(x) = \prod_{s \in B_i} (x - \alpha^s).$$

By using the above notation, the factorization of $x^n - 1$ into monic irreducible factors over $\mathbb{F}_q$ can be given as below:

$$x^n - 1 = \prod_{i \in B(n,q)} m_{\alpha^i}(x). \tag{2.1}$$

For our purposes, we need to group the irreducible factors of $x^n - 1$ over $\mathbb{F}_q$ into self-reciprocal polynomials and reciprocal polynomial pairs. The following lemma characterizes the self-reciprocal irreducible factors in terms of q-cyclotomic cosets.

Lemma 2.1 *Let α be a primitive n-th root of unity over $\mathbb{F}_q$. Then $m_{\alpha^i}(x)$ is self-reciprocal if and only if $B_i = B_{-i}$.*

Proof Suppose that $m_{\alpha^i}(x) \in \mathbb{F}_q[x]$ is self-reciprocal. That is, $m_{\alpha^i}(x) = m^*_{\alpha^i}(x)$. This implies that the set of roots of $m^*_{\alpha^i}(x)$ is equal to the set of roots of $m_{\alpha^i}(x)$, i.e., $B_i = B_{-i}$.
Conversely, assume that $B_i = B_{-i}$. This means that α^{-i} is a root of $m_{\alpha^i}(x)$; hence, the minimal polynomial $m^*_{\alpha^i}(x)$ of α^{-i} divides $m_{\alpha^i}(x)$. Since $m^*_{\alpha^i}(x)$ and $m_{\alpha^i}(x)$ are both monic and irreducible, we obtain that $m^*_{\alpha^i}(x) = m_{\alpha^i}(x)$, Hence, the polynomial $m_{\alpha^i}(x)$ is self-reciprocal. □

Let $\{i_1, \ldots, i_t\}$ be the set of all q-cyclotomic coset leaders modulo n, and $T = \{\alpha^{i_j} \mid 1 \leq j \leq t\}$. Suppose $T_1, T_2 \subseteq T$ such that $T_1 = \{\alpha^{i_j} \mid B_j = B_{-j}\}$ and $T_2 = T \setminus T_1$. By Lemma 2.1, for any $\alpha^{i_j} \in T_1$, $m_{\alpha^{i_j}}(x)$ is self-reciprocal. Thus, Equation (2.1) can be rewritten as follows:

$$x^n - 1 = \prod_{\alpha^{i_j} \in T_1} m_{\alpha^{i_j}(x)} \prod_{\alpha^{i_j} \in T_2} m_{\alpha^{i_j}}(x) m^*_{\alpha^{i_j}}(x).$$

2.3. Trace representation of cyclic codes

In this subsection, we consider the case $n = q^m - 1$ for some positive integer m. Let C be a cyclic code of length n over $\mathbb{F}_q$ with the generator polynomial $g(x)$. Let α be a primitive n-th root of unity over $\mathbb{F}_q$ and $\{i_1, \ldots, i_t\}$ be the set of all q-cyclotomic coset leaders modulo n. Suppose that $h(x)$ is the parity check polynomial of C and $S \subseteq \{1, \ldots, t\}$ such that $h^*(x) = \prod_{j \in S} m_{\alpha^{i_j}}(x)$. Then the basic dual zero set of C is defined as

$$\mathrm{BZ}(C^\perp) = \{\alpha^{i_j} \mid j \in S\}.$$

The following theorem gives a trace representation of a cyclic code C of length $q^m - 1$, where $\mathcal{T}_{q^m q^k}$ denotes the relative trace map from $\mathbb{F}_{q^m}$ to $\mathbb{F}_{q^k}$, for a divisor k of m, i.e., $\mathcal{T}_{q^m q^k}(\alpha) = \alpha + \alpha^{q^k} + \cdots + \alpha^{q^{\frac{m}{k}-1}}$ for every $\alpha \in \mathbb{F}_{q^m}$.

Proposition 2.2 *[20, Proposition 2.1] Let α be a primitive n-th root of unity with $n = q^m - 1$. Suppose that C is a cyclic code, where the generator polynomial of $C^\perp$ is equal to $\prod_{j \in S} m_{\alpha^{i_j}}(x)$, i.e., $BZ(C^\perp) = \{\alpha^{i_j} \mid j \in S\}$.*

Then

$$C = \Big\{ \Big(\sum_{j \in S} \mathcal{T}_{q^m q}(\lambda_j x^{i_j}) \Big)_{x \in \mathbb{F}_{q^m}^*} \mid \lambda_j \in \mathbb{F}_{q^m} \Big\}.$$

In connection with the trace representation above, we will use the following theorem for our results.

Theorem 2.3 *([8], Theorem 2.5) For $1 \leq j \leq t$, let $i_j \geq 1$ be positive integers which are in different q-cyclotomic cosets modulo n, where $n = q^m - 1$. For $\lambda_1, \ldots, \lambda_t \in \mathbb{F}_{q^m}$,*

$$\mathcal{T}_{q^m q}(\lambda_1 x^{i_1} + \cdots + \lambda_t x^{i_t}) = 0 \text{ for all } x \in \mathbb{F}_{q^m}$$

if and only if $|B_j| = \delta_j < m$ and $\mathcal{T}_{q^m q^{\delta_j}}(\lambda_j) = 0$ for all $j = 1, \ldots, t$.

3. Linear complementary dual cyclic codes

We recall that the hull of a linear code C is defined as $\mathrm{Hull}(C) = C \cap C^{\perp}$ and we denote the dimension of $\mathrm{Hull}(C)$ by $h(C)$. A linear code C is called linear complementary dual (LCD) if $h(C) = 0$. The characterization of an LCD cyclic code of length $q^m - 1$ with respect to its basic dual zero is given in the following theorem.

Theorem 3.1 *Let $n = q^m - 1$, C be a cyclic code of length n over $\mathbb{F}_q$, α be a primitive n-th root of unity over $\mathbb{F}_q$. Let $\{i_1, \ldots, i_t\}$ be the set of all q-cyclotomic coset leaders modulo n. Then C is LCD if and only if $\alpha^{i_j} \in BZ(C^{\perp})$ implies that either $B_j = B_{-j}$ or $\alpha^{-i_j} \in BZ(C^{\perp})$ for all $1 \leq j \leq t$.*

Proof Suppose that $C =< g(x) >$ and $C^{\perp} =< h^*(x) >$. That is, $g(x)h(x) = x^n - 1$. We also have $\gcd(g(x), h(x)) = 1$, since the polynomial $x^n - 1$ has no repeated factors as $\gcd(n, q) = 1$. These together imply that $g^*(x)h^*(x) = x^n - 1$ and $\gcd(g^*(x), h^*(x)) = 1$. Since $(C^{\perp})^{\perp} = C$ the basic dual zero of $C^{\perp}$ is a set of representatives of the roots of $g(x)$, which is equal to $\mathrm{BZ}(C)$. Suppose on the contrary that C is LCD and there exists $1 \leq j \leq t$ such that $\alpha^{i_j} \in \mathrm{BZ}(C^{\perp})$, $B_j \cap B_{-j} = \emptyset$ and $\alpha^{-i_j} \notin \mathrm{BZ}(C^{\perp})$. We, without loss of generality, assume that $j = 1$. The assumptions $\alpha^{i_1} \in \mathrm{BZ}(C^{\perp})$ and $\alpha^{-i_1} \notin \mathrm{BZ}(C^{\perp})$ imply that $m_{\alpha^{i_1}}(x) \mid h^*(x)$ and $m_{\alpha^{-i_1}}(x) \nmid h^*(x)$, respectively. Since $g^*(x)h^*(x) = x^n - 1$ and $\gcd(g^*(x), h^*(x)) = 1$, we obtain $m_{\alpha^{-i_1}}(x) \mid g^*(x)$, consequently $m_{\alpha^{i_1}}(x) \mid g(x)$. Therefore, $\alpha^{i_1} \in \mathrm{BZ}(C^{\perp}) \cap \mathrm{BZ}(C)$. Assume that $\mathrm{BZ}(C^{\perp}) = \{\alpha^{i_1}\} \cup T_1$ and $\mathrm{BZ}(C) = \mathrm{BZ}((C^{\perp})^{\perp}) = \{\alpha^{i_1}\} \cup T_2$. By Proposition 2.2, the trace representations of C and $C^{\perp}$ are as follows:

$$C = \Big\{ \Big(\mathcal{T}_{q^m q}(\lambda_1 x^{i_1} + \sum_{\alpha^{i_j} \in T_1} \lambda_j x^{i_j}) \Big)_{x \in \mathbb{F}_{q^m}^*} \mid \lambda_j \in \mathbb{F}_{q^m} \Big\},$$

$$C^{\perp} = \Big\{ \Big(\mathcal{T}_{q^m q}(\beta_1 x^{i_1} + \sum_{\alpha^{i_j} \in T_2} \beta_j x^{i_j}) \Big)_{x \in \mathbb{F}_{q^m}^*} \mid \beta_j \in \mathbb{F}_{q^m} \Big\}.$$

We can take $\lambda_h = \beta_l = 0$ for all $\alpha^{i_h} \in T_1$, $\alpha^{i_l} \in T_2$, and $\lambda_1 = \beta_1 = \lambda$ such that $\mathcal{T}_{q^m q^{\delta_j}}(\lambda) \neq 0$. Then we obtain $c = \big(\mathcal{T}_{q^m q}(\lambda x^{i_1})\big)_{x \in \mathbb{F}_{q^m}^*} \in C \cap C^{\perp}$. Since $\mathcal{T}_{q^m q}(\lambda) \neq 0$, $c \neq 0$ by Theorem 2.3. This contradicts the assumption that C is LCD.

Conversely, assume that $\alpha^{i_j} \in \mathrm{BZ}(C^{\perp})$ implies that either $B_j = B_{-j}$ or $\alpha^{-i_j} \in \mathrm{BZ}(C^{\perp})$ for all i_j, $1 \leq j \leq t$. If $B_j = B_{-j}$, then we have $m_{\alpha^{i_j}}(x) = m^*_{\alpha^{i_j}}(x)$ by Lemma 2.1. If $B_j \cap B_{-j} = \emptyset$ and $\alpha^{-i_j} \in \mathrm{BZ}(C^{\perp})$,

then we have $m_{\alpha^{i_j}}(x) \mid h(x)$ and $m^*_{\alpha^{i_j}}(x) \mid h^*(x)$. These together imply that $h^*(x)$ is self-reciprocal. That is, $g(x)h^*(x) = x^n - 1$ and $\gcd(g(x), h^*(x)) = 1$. Therefore, $\mathrm{BZ}(C^\perp) \cap \mathrm{BZ}(C) = \emptyset$. As $C \oplus C^\perp = \mathbb{F}_{q^n}$, we have $\mathrm{BZ}(C) \cup \mathrm{BZ}(C^\perp) = T$. Thus, we assume without loss of generality that $\mathrm{BZ}(C^\perp) = \{\alpha^{i_1}, \ldots, \alpha^{i_s}\}$ and $\mathrm{BZ}(C) = \{\alpha^{i_{s+1}}, \ldots, \alpha^{i_t}\}$. Then by Proposition 2.2, the trace representations of C and $C^\perp$ are as follows:

$$C = \left\{ \left(\mathcal{T}_{q^m q}(\lambda_1 x^{i_1} + \cdots + \lambda_s x^{i_s}) \right)_{x \in \mathbb{F}^*_{q^m}} \mid \lambda_j \in \mathbb{F}_{q^m}, 1 \le j \le s \right\},$$

$$C^\perp = \left\{ \left(\mathcal{T}_{q^m q}(\lambda_{s+1} x^{i_{s+1}} + \cdots + \lambda_t x^{i_t}) \right)_{x \in \mathbb{F}^*_{q^m}} \mid \lambda_j \in \mathbb{F}_{q^m}, s+1 \le j \le t \right\}.$$

Suppose on the contrary that $\mathrm{Hull}(C) \neq \{0\}$. Then there exists $0 \neq c \in \mathrm{Hull}(C)$, and $\lambda_1, \ldots, \lambda_t \in \mathbb{F}_{q^m}$ such that

$$c = \left(\mathcal{T}_{q^m q}(\lambda_1 x^{i_1} + \cdots + \lambda_s x^{i_s}) \right)_{x \in \mathbb{F}^*_{q^m}} = \left(\mathcal{T}_{q^m q}(\lambda_{s+1} x^{i_{s+1}} + \cdots + \lambda_t x^{i_t}) \right)_{x \in \mathbb{F}^*_{q^m}}$$

Equivalently,

$$\left(\mathcal{T}_{q^m q}(\lambda_1 x^{i_1} + \cdots + \lambda_s x^{i_s} - \lambda_{s+1} x^{i_{s+1}} - \cdots - \lambda_t x^{i_t}) \right)_{x \in \mathbb{F}^*_{q^m}} = 0. \tag{3.1}$$

By Theorem 2.3, the equality in (3.1) holds if and only if $|B_j| = \delta_j < m$ and $\mathcal{T}_{q^m q^{\delta_j}}(\lambda_j) = 0$ for all $1 \le j \le t$. We know that the set $\mathrm{BZ}(C^\perp) \cup \mathrm{BZ}(C)$ contains all the leaders of q-cyclotomic cosets modulo n, in particular, the coset leader that contains 1. Since the cyclotomic coset that contains 1 has cardinality m, we have a contradiction. Hence, C is LCD. □

Remark 3.2 *By Theorem 3.1, a cyclic code C of length $q^m - 1$ over $\mathbb{F}_q$ is LCD if and only if for any divisor $m_{\alpha^{i_j}}(x)$ of $h^*(x)$, $m^*_{\alpha^{i_j}}(x)$ is also a divisor of $h^*(x)$. Therefore, C is LCD if and only if $h^*(x)$ is self-reciprocal, which implies*

$$g^*(x) = \frac{x^n - 1}{h^*(x)} = \frac{x^n - 1}{h(x)} = g(x)$$

is self-reciprocal. This has also been observed by Massey in [21] for a cyclic code of arbitrary length n.

Note that in some cases, the condition given in Lemma 2.1 on q-cyclotomic cosets modulo n can be satisfied for all cyclotomic cosets, which leads to the following corollary.

Corollary 3.3 *Let $\{i_1, \ldots, i_t\}$ be the set of all q-cyclotomic coset leaders modulo n. If $B_j = B_{-j}$ for all $1 \le j \le t$, then any cyclic code of length n over $\mathbb{F}_q$ is LCD.*

Proof Since $B_j = B_{-j}$ for all $1 \le j \le t$, by Lemma 2.1, the polynomial $m_{\alpha^{i_j}}(x)$ is self-reciprocal for any $1 \le j \le t$. This means that any factor $g(x)$ of $x^n - 1$ is self-reciprocal. Hence, the cyclic code generated by $g(x)$ is LCD. □

Example 3.4 *Let $q = 2$ and $n = 9$. Then the 2-cyclotomic cosets modulo 9 are $B_0 = \{0\}$, $B_1 = \{1, 2, 4, 5, 7, 8\}$, $B_3 = \{3, 6\}$. Since $B_1 = B_8$ and $B_3 = B_6$, every binary cyclic code of length 9 is LCD*

by Corollary 3.3. Note that the monic irreducible factors of x^9-1 *over* $\mathbb{F}_2$ *are* $x+1$, x^2+x+1 *and* x^6+x^3+1, *which are all self-reciprocal.*
Let $q=3$ *and* $n=10$. *Then the* 3*-cyclotomic cosets modulo* 10 *are* $B_0=\{0\}$, $B_1=\{1,3,7,9\}$, $B_2=\{2,4,6,8\}$, $B_5=\{5\}$. *Since* $B_1=B_9$ *and* $B_2=B_8$, *every ternary cyclic code of length* 10 *is LCD by Corollary 3.3. Note that the monic irreducible factors of* $x^{10}-1$ *over* $\mathbb{F}_3$ *are* $x+1$, $x+2$, $x^4+x^3+x^2+x+1$, $x^4+2x^3+x^2+2x+1$, *which are all self-reciprocal.*

4. One-dimensional hull cyclic codes

In this section, we present a condition for a cyclic code to have a one-dimensional hull in terms of its basic dual zero set. We will use the following theorem.

Theorem 4.1 *([10], Theorem 4.3.7) Let* C_i *be a cyclic code of length* n *over* $\mathbb{F}_q$ *with the generator polynomial* $g_i(x)$ *for* $i=1,2$. *Then* $C_1\cap C_2$ *has generator polynomial* $lcm(g_1(x),g_2(x))$, *where* $lcm(g_1(x),g_2(x))$ *denotes the least common multiple of the polynomials* $g_1(x)$ *and* $g_2(x)$.

Let C be a cyclic code of length q^m-1 over $\mathbb{F}_q$. Suppose that $h_{\mathrm{Hull}(C)}(x)$ is the parity check polynomial of Hull(C) and $S\subseteq\{1,\dots,t\}$ such that $h^*_{\mathrm{Hull}(C)}(x)=\prod_{j\in S}m_{\alpha^{ij}}(x)$. Then $\mathrm{BZ}((\mathrm{Hull}(C))^{\perp})=\{\alpha^{ij}\mid j\in S\}$. By Proposition 2.2, the trace representation of $\mathrm{Hull}(C)$ is as follows:

$$\mathrm{Hull}(C)=\Big\{\Big(\sum_{j\in S}\mathcal{T}_{q^mq}(\lambda_jx^{ij})\Big)_{x\in\mathbb{F}^*_{q^m}}\mid\lambda_j\in\mathbb{F}_{q^m}\Big\}.$$

Let $\beta\in\mathbb{F}_{q^m}$ be a normal element over $\mathbb{F}_q$, i.e., the set $\{\beta,\beta^q,\dots,\beta^{q^{m-1}}\}$ forms a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Then for each $\lambda_j\in\mathbb{F}_{q^m}$, there exist unique elements $c_{\lambda_{j_0}},\dots,c_{\lambda_{j_{m-1}}}$ of $\mathbb{F}_q$ such that $\lambda_j=\sum_{u=0}^{m-1}c_{\lambda_{j_u}}\beta^{q^u}$. Hence, we get

$$\big(\mathcal{T}_{q^mq}(\lambda_jx^{ij})\big)_{x\in\mathbb{F}^*_{q^m}}=c_{\lambda_{j_0}}\big(\mathcal{T}_{q^mq}(\beta x^{ij})\big)_{x\in\mathbb{F}^*_{q^m}}+\cdots+c_{\lambda_{j_{m-1}}}\big(\mathcal{T}_{q^mq}(\beta^{q^{m-1}}x^{ij})\big)_{x\in\mathbb{F}^*_{q^m}}$$

for all $j\in S$. This implies that $\mathrm{Hull}(C)$ is spanned by the vectors $\big(\mathcal{T}_{q^mq}(\beta^{q^r}x^{ij})\big)_{x\in\mathbb{F}^*_{q^m}}$ for $j\in S$, $0\le r\le m-1$, i.e.,

$$\mathrm{Hull}(C)=\mathrm{span}\big\{\big(\mathcal{T}_{q^mq}(\beta^{q^r}x^{ij})\big)_{x\in\mathbb{F}^*_{q^m}}\mid j\in S,0\le r\le m-1\big\}.\tag{4.1}$$

Therefore, in order to determine $h(C)$, we need to find the number of linearly independent vectors in the spanning set given by (4.1). We have the following lemma.

Lemma 4.2 *Let* β *be a normal element of* $\mathbb{F}_{q^m}$ *over* $\mathbb{F}_q$. *Suppose that* k,l *are positive integers with* $B_k\cap B_l=\emptyset$. *Then the vectors* $\big(\mathcal{T}_{q^mq}(\beta x^k)\big)_{x\in\mathbb{F}^*_{q^m}}$ *and* $\big(\mathcal{T}_{q^mq}(\beta x^l)\big)_{x\in\mathbb{F}^*_{q^m}}$ *are linearly independent over* $\mathbb{F}_q$.

Proof: The proof is by contradiction. Suppose that the vectors $\big(\mathcal{T}_{q^mq}(\beta x^k)\big)_{x\in\mathbb{F}^*_{q^m}}$ and $\big(\mathcal{T}_{q^mq}(\beta x^l)\big)_{x\in\mathbb{F}^*_{q^m}}$ are linearly dependent over $\mathbb{F}_q$. Then there exist nonzero $c_1,c_2\in\mathbb{F}_q$ such that

$$c_1\big(\mathcal{T}_{q^mq}(\beta x^k)\big)_{x\in\mathbb{F}^*_{q^m}}+c_2\big(\mathcal{T}_{q^mq}(\beta x^l)\big)_{x\in\mathbb{F}^*_{q^m}}=\big(\mathcal{T}_{q^mq}(c_1\beta x^k+c_2\beta x^l)\big)_{x\in\mathbb{F}^*_{q^m}}=0.$$

This implies that there exists $0 \neq a_x \in \mathbb{F}_{q^m}$ such that $c_1x^k\beta + c_2x^l\beta = (c_1x^k + c_2x^l)\beta = a_x^q - a_x = b_x$, for each $x \in \mathbb{F}_{q^m}$. Since β is a normal element of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, the element b_x has a unique expression of the form $b_x = \sum_{u=0}^{m-1} d_{x_u}\beta^{q^u}$, where $d_{x_u} \in \mathbb{F}_q$. This implies that $c_1x^k + c_2x^l = d_{x_0} \in \mathbb{F}_q$ for all $x \in \mathbb{F}_q$. Therefore, $\mathcal{T}_{q^mq}((c_1x^k + c_2x^l)\beta) = (c_1x^k + c_2x^l)\mathcal{T}_{q^mq}(\beta) = 0$. Since $\beta \in \mathbb{F}_{q^m}$ is normal over $\mathbb{F}_q$, $\mathcal{T}_{q^mq}(\beta) \neq 0$, which means $c_1x^k + c_2x^l = 0$ for all $x \in \mathbb{F}_{q^m}$. Assume without loss of generality that $c_1 \neq 0$ and let $x = 1$. Then $c_1 = -c_2$. If we let $x = \theta$, where θ is a primitive element of $\mathbb{F}_{q^m}$, then $c_1x^k + c_2x^l = c_1(\theta^k - \theta^l) = 0$. As $c_1 \neq 0$, we obtain $\theta^k - \theta^l = 0$. That is, $\theta^{k-l} = 1$, which implies that $k \equiv l \bmod (q^m - 1)$. This contradicts the assumption that $B_k \cap B_l = \emptyset$. Hence, the result follows.

Theorem 4.3 *For $n = q^m - 1$, let C be a cyclic code of length n. Let $\{i_1, \ldots, i_t\}$ be the set of all leaders of q-cyclotomic cosets modulo n, and $T = \{\alpha^{i_j} \mid 1 \leq j \leq t\}$. Then $h(C) = 1$ if and only if $BZ(C^\perp)$ satisfies the following:*

i) There exists a unique $\alpha^{i_j} \in BZ(C^\perp)$ such that $|B_j| = 1$, $B_j \cap B_{-j} = \emptyset$ and $\alpha^{-i_j} \notin BZ(C^\perp)$.

ii) $BZ(C^\perp) = T_1 \cup \{\alpha^{i_j}\}$, where $T_1 \subset T$ satisfies for any $\alpha^{i_h} \in T_1$, we have either $B_h = B_{-h}$ or $\alpha^{-i_h} \in T_1$.

Proof: Let $n = q^m - 1$, a code $C =< g(x) >$ be cyclic of length n, and $h(x)$ be the parity check polynomial of C. Let $\{i_1, \ldots, i_t\}$ be the set of all leaders of q-cyclotomic cosets modulo n, and $T = \{\alpha^{i_j} \mid 1 \leq j \leq t\}$.

Suppose that i) and ii) hold. We first show that $\mathrm{BZ}((\mathrm{Hull}(C))^\perp) = \mathrm{BZ}((C \cap C^\perp)^\perp) = \{\alpha^{i_j}\}$. By Theorem 4.1, we know that $\mathrm{Hull}(C) = C \cap C^\perp =< \mathrm{lcm}(g(x), h^*(x)) >=< \mathrm{lcm}(\frac{x^n-1}{h(x)}, h^*(x)) >$. By ii), we can write $h^*(x) = m_{\alpha^{i_j}}(x)t(x)$, where $t(x) = \prod_{\alpha^{i_h} \in T_1} m_{\alpha^{i_h}}(x)$. Similar to the proof of Theorem 3.1, we can see that $t(x)$ is self-reciprocal. This implies that $h(x) = m^*_{\alpha^{i_j}}(x)t(x)$, and hence $\gcd(g(x), h^*(x)) = m_{\alpha^{i_j}}(x)$. Then we have $\mathrm{lcm}(g(x), h^*(x)) = \frac{g(x)h^*(x)}{\gcd(g(x),h^*(x))} = \frac{x^n-1}{m^*_{\alpha^{i_j}}(x)}$. That is, $\mathrm{Hull}(C) =< \frac{x^n-1}{m^*_{\alpha^{i_j}}(x)} >$, which implies that $\mathrm{BZ}((\mathrm{Hull}(C))^\perp) = \{\alpha^{i_j}\}$. By Proposition 2.2, the trace representation of $\mathrm{Hull}(C)$ is as follows:

$$\mathrm{Hull}(C) = \left\{ \left(\mathcal{T}_{q^mq}(\lambda x^{i_j})\right)_{x \in \mathbb{F}^*_{q^m}} \mid \lambda \in \mathbb{F}_{q^m} \right\}. \tag{4.2}$$

Let β be a normal element of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Then for any $\lambda \in \mathbb{F}_{q^m}$ there exist $c_{\lambda_0}, \ldots, c_{\lambda_{m-1}} \in \mathbb{F}_q$ such that $\lambda = c_{\lambda_0}\beta + c_{\lambda_1}\beta^q + \cdots + c_{\lambda_{m-1}}\beta^{q^{m-1}}$. Hence, we get

$$\left(\mathcal{T}_{q^mq}(\lambda x^{i_j})\right)_{x \in \mathbb{F}^*_{q^m}} = c_{\lambda_0}\left(\mathcal{T}_{q^mq}(\beta x^{i_j})\right)_{x \in \mathbb{F}^*_{q^m}} + \cdots + c_{\lambda_{m-1}}\left(\mathcal{T}_{q^mq}(\beta^{q^{m-1}} x^{i_j})\right)_{x \in \mathbb{F}^*_{q^m}}.$$

This implies that $\mathrm{Hull}(C)$ is spanned by the vectors $\left(\mathcal{T}_{q^mq}(\beta^{q^r} x^{i_j})\right)_{x \in \mathbb{F}^*_{q^m}}$ for $0 \leq r \leq m-1$, i.e.,

$$\mathrm{Hull}(C) = \mathrm{span}\left\{ \left(\mathcal{T}_{q^mq}(\beta^{q^r} x^{i_j})\right)_{x \in \mathbb{F}^*_{q^m}} \mid 0 \leq r \leq m-1 \right\}$$

by the equality in (4.2). By i), $|B_j| = 1$, i.e., $j \equiv jq^r \bmod (q^m - 1)$ for all $0 \leq r \leq m-1$. Hence, for all $0 \leq r \leq m-1$, the equality $\left(\mathcal{T}_{q^mq}(\beta^{q^r} x^{i_j})\right)_{x \in \mathbb{F}^*_{q^m}} = \left(\mathcal{T}_{q^mq}(\beta x^{i_j})\right)_{x \in \mathbb{F}^*_{q^m}}$ holds. That is, $\mathrm{Hull}(C) = \mathrm{span}\left\{ \left(\mathcal{T}_{q^mq}(\beta x^{i_j})\right)_{x \in \mathbb{F}^*_{q^m}} \right\}$. Since β is a normal element of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, we have $\mathcal{T}_{q^mq}(\beta) \neq 0$. Then the vector $\left(\mathcal{T}_{q^mq}(\beta x^{i_j})\right)_{x \in \mathbb{F}^*_{q^m}} \neq 0$ by Theorem 2.3, and hence $h(C) = 1$.

Conversely, suppose on the contrary that $h(C) = 1$, and there exist representatives i_j such that $\mathrm{BZ}(C^\perp) = T_1 \cup \{\alpha^{i_1}, \alpha^{i_2}\}$, $B_{i_j} \cap B_{-i_j} = \emptyset$, $|B_{i_j}| = 1$ and $\{\alpha^{-i_j}\} \neq \mathrm{BZ}(C^\perp)$ for $j = 1, 2$. Similar to the proof of Theorem 3.1, we obtain $\mathrm{BZ}((\mathrm{Hull}(C))^\perp) = \{\alpha^{i_1}, \alpha^{i_2}\}$. By Proposition 2.2, we have the following trace representation of $\mathrm{Hull}(C)$:

$$\mathrm{Hull}(C) = \left\{ \left(\mathcal{T}_{q^m q}(\lambda_1 x^{i_1} + \lambda_2 x^{i_2}) \right)_{x \in \mathbb{F}_{q^m}^*} \mid \lambda_1, \lambda_2 \in \mathbb{F}_{q^m} \right\}.$$

Then we have

$$\begin{aligned} \mathrm{Hull}(C) &= \mathrm{span}\left\{ \left(\mathcal{T}_{q^m q}(\beta^{q^r} x^{i_1}) \right)_{x \in \mathbb{F}_{q^m}^*}, \left(\mathcal{T}_{q^m q}(\beta^{q^r} x^{i_2}) \right)_{x \in \mathbb{F}_{q^m}^*} \mid 0 \leq r \leq m-1 \right\}. \\ &= \mathrm{span}\left\{ \left(\mathcal{T}_{q^m q}(\beta x^{i_1}) \right)_{x \in \mathbb{F}_{q^m}^*}, \left(\mathcal{T}_{q^m q}(\beta x^{i_2}) \right)_{x \in \mathbb{F}_{q^m}^*} \right\}, \end{aligned}$$

where the last equality follows from the assumption that $|B_{i_1}| = |B_{i_2}| = 1$. We also have $h(C) = 1$ by assumption, which implies that all the vectors in the spanning set of $\mathrm{Hull}(C)$ are linearly dependent. Using Lemma 4.2, we obtain $B_{i_1} = B_{i_2}$. Hence, the result follows.

Corollary 4.4 *There exist no binary and ternary one-dimensional hull cyclic codes of length $q^m - 1$.*

Proof If C is a one-dimensional hull cyclic code over $\mathbb{F}_q$, then by Theorem 4.3, $\mathrm{BZ}(C^\perp) = T_1 \cup \{\alpha^{i_j}\}$, where $B_j \cap B_{-j} = \emptyset$, $|B_j| = 1$ and $\alpha^{-i_j} \notin \mathrm{BZ}(C^\perp)$. This implies that $i_j \equiv 2i_j \mod (2^m - 1)$, when $q = 2$. Thus, $(2^m - 1) \mid i_j$, i.e, $i_j = 2^m - 1$, a contradiction to the assumption that $i_j < 2^m - 1$.

Similarly, we have $i_j \equiv 3i_j \mod (3^m - 1)$, when $q = 3$. Thus, $(3^m - 1) \mid 2i_j$, i.e., $\alpha^{2i_j} = 1$. Since $i_j < q^m - 1$, we conclude that $\alpha^{i_j} = -1$, which implies that $\alpha^{-i_j} = -1$. Hence, we have $i_j \equiv -i_j \mod (3^m - 1)$, which contradicts the assumption that $B_j \cap B_{-j} = \emptyset$. □

Remark 4.5 *The characterization of one-dimensional hull cyclic codes in terms of their defining sets is given in [12], whereas our characterization is given in terms of basic dual zero sets of cyclic codes. In [12], the authors also obtain the nonexistence result given in Corollary 4.4 as a consequence of their characterization.*

Let C be a cyclic code of length n, where $\gcd(n, q) = 1$. Suppose that $\mathrm{BZ}(C^\perp) = T_1 \cup T_2$, where T_1 is as in Theorem 4.3, and $T_2 = \mathrm{BZ}(C^\perp) \setminus T_1$. Then similar to the proof of Theorem 4.3, we can write

$$\mathrm{BZ}((\mathrm{Hull}(C))^\perp) = T_2.$$

This means that

$$h^*_{\mathrm{Hull}(C)}(x) = \prod_{\alpha^{i_j} \in T_2} m_{\alpha^{i_j}}(x),$$

where $h_{\mathrm{Hull(C)}}(x)$ is the parity check polynomial of the code $\mathrm{Hull}(C)$. As a result, we arrive at the following theorem, which generalizes Theorem 4.3 to the hull of cyclic codes of arbitrary length n.

Theorem 4.6 *Let $C =< g(x) >$ be a cyclic code of length n over $\mathbb{F}_q$. Let $\{i_1, \ldots, i_t\}$ be the set of all leaders of q-cyclotomic cosets modulo n, and $T = \{\alpha^{i_j} \mid 1 \leq j \leq t\}$. Suppose that $BZ(C^\perp) = T_1 \cup T_2$, and the following holds.*

i) For any $\alpha^{i_j} \in T_1$, *either* $B_j = B_{-j}$ *or* $\alpha^{-i_j} \in T_1$.

ii) For any $\alpha^{i_j} \in T_2$, $B_j \cap B_{-j} = \emptyset$ *and* $\alpha^{-i_j} \notin T_2$.

Then $BZ((Hull(C))^{\perp}) = T_2$ *and* $h(C) = \sum_{\alpha^{i_j} \in T_2} |B_j|$.

5. Linear complementary pair of cyclic codes

A pair (C, D) of linear codes of length n over the finite field $\mathbb{F}_q$ is called a linear complementary pair (LCP) of codes if $\mathbb{F}_q^n = C \oplus D$. The LCP of codes can be considered a generalization of LCD codes. Namely, if C is an LCD code, then the pair $(C, C^{\perp})$ is LCP of codes. The following lemma is required to obtain the main result of this section.

Lemma 5.1 *Let* C *and* D *be two cyclic codes of length* n *over* $\mathbb{F}_q$. *Then*

$$BZ((C \cap D)^{\perp}) = BZ(C^{\perp}) \cap BZ(D^{\perp}).$$

Proof Let $g_C(x)$, $g_D(x)$, and $g(x)$ denote the generator polynomials of C, D and $C \cap D$, and $h_C(x)$, $h_D(x)$ and $h(x)$ denote their parity check polynomials, respectively. Take $\alpha^{i_j} \in \mathrm{BZ}((C \cap D)^{\perp})$. Suppose that $0 \neq c \in C \cap D$, and $c(x)$ is the polynomial corresponding to the codeword c. Since $c \in C \cap D$, we have $c(x)h(x) = c(x)h_C(x) = c(x)h_D(x) = 0$. This implies that $c^*(x)h^*(x) = c^*(x)h_C^*(x) = c^*(x)h_D^*(x) = 0$. As $\alpha^{i_j} \in \mathrm{BZ}((C \cap D)^{\perp})$, there exists $q(x) \in \mathbb{F}_q[x]$ such that $h^*(x) = m_{\alpha^{i_j}}(x)q(x)$. Then

$$c^*(x)m_{\alpha^{i_j}}(x)q(x) = c^*(x)h_C^*(x) = c^*(x)h_D^*(x) = 0.$$

Since $c(x) \neq 0$, we obtain that $m_{\alpha^{i_j}}(x) \mid h_C^*(x)$, and $m_{\alpha^{i_j}}(x) \mid h_D^*(x)$. Hence, $\alpha^{i_j} \in \mathrm{BZ}(C^{\perp}) \cap \mathrm{BZ}(D^{\perp})$, i.e., $\alpha^{i_j} \in \mathrm{BZ}((C \cap D)^{\perp}) \subseteq \mathrm{BZ}(C^{\perp}) \cap \mathrm{BZ}(D^{\perp})$.

We prove the reverse inclusion by contradiction. Suppose that $\alpha^{i_j} \in \mathrm{BZ}(C^{\perp}) \cap \mathrm{BZ}(D^{\perp})$ and $\alpha^{i_j} \notin \mathrm{BZ}((C \cap D)^{\perp})$. Then $m_{\alpha^{i_j}}(x) \nmid h^*(x)$, i.e., there exist $q(x), r(x) \in \mathbb{F}_q[x]$ such that $h^*(x) = m_{\alpha^{i_j}}(x)q(x) + r(x)$ with $0 \neq r(x)$ and $\deg r(x) < \deg m_{\alpha^{i_j}}(x)$. Take $0 \neq c \in C \cap D$, and consider the corresponding polynomial $c(x)$. Since $c \in C \cap D$, we have $c(x)h^*(x) = ch_C^*(x) = 0$. As $\alpha^{i_j} \in \mathrm{BZ}(C^{\perp})$, the polynomial $m_{\alpha^{i_j}}(x)$ divides $h_C^*(x)$. That is, there exists $q_1(x) \in \mathbb{F}_q[x]$ such that $h_C^*(x) = m_{\alpha^{i_j}}(x)q_1(x)$. Then

$$0 = c(x)m_{\alpha^{i_j}}(x)q_1(x) = c(x)m_{\alpha^{i_j}}(x)q(x) + c(x)r(x).$$

Thus,

$$c(x)r(x) = c(x)m_{\alpha^{i_j}}(x)(q_1(x) - q(x)),$$

and as $c(x) \neq 0$,

$$r(x) = m_{\alpha^{i_j}}(x)(q(x) - q_1(x)).$$

This implies that $m_{\alpha^{i_j}}(x) \mid r(x)$, which contradicts $\deg r(x) < m_{\alpha^{i_j}}(x)$. Therefore, $\alpha^{i_j} \in \mathrm{BZ}((C \cap D)^{\perp})$, i.e., $\mathrm{BZ}(C^{\perp}) \cap \mathrm{BZ}(D^{\perp}) \subseteq \mathrm{BZ}((C \cap D)^{\perp})$. □

The following theorem characterizes the LCP of cyclic codes (C, D) of length $q^m - 1$ over $\mathbb{F}_q$ in terms of the basic dual zeros of C and D.

Theorem 5.2 *Let $n = q^m - 1$, C and D be cyclic codes of length n. Let $\{i_1, \ldots, i_t\}$ be the set of all leaders of q-cyclotomic cosets modulo n, and $T = \{\alpha^{i_j} \mid 1 \leq j \leq t\}$. Then the pair (C, D) is an LCP of codes if and only if $BZ(C^\perp) = T \setminus BZ(D^\perp)$.*

Proof Assume that the pair (C, D) is an LCP of codes, and there exists $\alpha^{i_j} \in \mathrm{BZ}(C^\perp)$ and $\alpha^{i_j} \notin T \setminus \mathrm{BZ}(D^\perp)$, i.e., $\alpha^{i_j} \in \mathrm{BZ}(C^\perp) \cap \mathrm{BZ}(D^\perp)$. Let $\mathrm{BZ}(C^\perp) = \{\alpha^{i_j}\} \cup T_1$ and $\mathrm{BZ}(D^\perp) = \{\alpha^{i_j}\} \cup T_2$. Similar to the proof of Theorem 3.1, we can see that there exists $\lambda \in \mathbb{F}_{q^m}$ such that $\mathcal{T}_{q^m q}(\lambda) \neq 0$ and $0 \neq c = \left(\mathcal{T}_{q^m q}(\lambda x^{i_j})\right)_{x \in \mathbb{F}_{q^m}^*} \in C \cap D$. This contradicts the assumption that the pair (C, D) is LCP.

Conversely, suppose on the contrary that $\mathrm{BZ}(C^\perp) = T \setminus \mathrm{BZ}(D^\perp)$ and the pair (C, D) is not LCP. As $\mathrm{BZ}(C^\perp) = T \setminus \mathrm{BZ}(D^\perp)$, we, without loss of generality, assume that $\mathrm{BZ}(C^\perp) = \{\alpha^{i_1}, \ldots, \alpha^{i_s}\}$ and $\mathrm{BZ}(D^\perp) = \{\alpha^{i_{s+1}}, \ldots, \alpha^{i_t}\}$. Let $0 \neq c \in C \cap D$. Similar to the proof of Theorem 3.1, there exist $\lambda_1, \ldots, \lambda_t \in \mathbb{F}_{q^m}$ such that

$$c = \left(\mathcal{T}_{q^m q}(\lambda_1 x^{i_1} + \cdots + \lambda_s x^{i_s})\right)_{x \in \mathbb{F}_{q^m}^*} = \left(\mathcal{T}_{q^m q}(\lambda_{s+1} x^{i_{s+1}} + \cdots + \lambda_t x^{i_t})\right)_{x \in \mathbb{F}_{q^m}^*}.$$

Thus,

$$\mathcal{T}_{q^m q}(\lambda_1 x^{i_1} + \cdots + \lambda_s x^{i_s} - \lambda_{s+1} x^{i_{s+1}} - \cdots - \lambda_t x^{i_t}) = 0 \quad \text{for all } x \in \mathbb{F}_{q^m}^*.$$

By assumption, $\mathrm{BZ}(C^\perp) \cup \mathrm{BZ}(D^\perp)$ contains all the leaders of q-cyclotomic cosets modulo $q^m - 1$, in particular, the coset leader that contains 1, which is of cardinality m. Hence, we obtain a contradiction to Theorem 2.3. □

Remark 5.3 *Let (C, D) be an LCP of cyclic codes of length n. By Theorem 5.2, we have $BZ(C^\perp) = T \setminus BZ(D^\perp)$. Then we have*

$$x^n - 1 = \prod_{\alpha^{i_j} \in \mathrm{BZ(C^\perp)}} m_{\alpha^{i_j}}(x) \prod_{\alpha^{i_j} \in \mathrm{BZ(D^\perp)}} m_{\alpha^{i_j}}(x) = h_C^*(x) h_D^*(x),$$

by Equation (2.1). That is,

$$x^n - 1 = g_C(x) g_D(x).$$

This implies that $g_C(x)$ and $g_D(x)$ are relatively prime, which has been also observed in [5, Remark 2.3].

A pair (C, D) of linear codes is called linear ℓ-intersection pair of codes if $\dim(C \cap D) = \ell$. Note that if (C, D) is an LCP of codes of length n, then (C, D) is a 0-intersection pair of codes with $n = \dim(C) + \dim(D)$. We then have the following theorem, which generalizes Theorem 5.2 to any linear ℓ-intersection pair of cyclic codes with arbitrary length n.

Theorem 5.4 *Let C and D be cyclic codes of length n over $\mathbb{F}_q$. Then*

$$\ell = \dim(C \cap D) = \sum_{\alpha^{i_j} \in T_1} |B_j|,$$

where $T_1 \subseteq T$ such that $BZ(C^\perp) \cap BZ(D^\perp) = T_1$.

Proof Let $\mathrm{BZ}(C^{\perp}) \cap \mathrm{BZ}(D^{\perp}) = T_1$. By Lemma 5.1, we have $T_1 = \mathrm{BZ}((C \cap D)^{\perp})$. This means that

$$h^*_{C\cap D}(x) = \prod_{\alpha^{i_j} \in T_1} m_{\alpha^{i_j}}(x),$$

where $h_{C\cap D}(x)$ is the parity check polynomial of $C \cap D$. Therefore, we obtain

$$\ell = \dim(C \cap D) = \deg h_{C\cap D}(x) = \sum_{\alpha^{i_j} \in T_1} |B_j|.$$

□

Acknowledgment

The authors would like to thank Cem Güneri for pointing out the problem and helpful discussions, and Nurdagül Anbar for her suggestions that improve the quality of the presentation of the paper. T. K. is supported by The Scientific and Technological Research Council of Türkiye (TÜBİTAK) Project under Grant 120F309.

References

[1] Assmus EF, Key JD. Affine and projective planes. Discrete Mathematics 1990; 83 (2-3): 161-187. https://doi.org/10.1016/0012-365X(90)90003-Z

[2] Ngo XT, Bhasin S, Danger JL, Guilley S, Najm Z. Linear complementary dual code improvement to strengthen encoded circuit against hardware Trojan horses. IEEE International Symposium on Hardware Oriented Security and Trust 2015; 82-87. https://doi.org/10.1109/HST.2015.7140242

[3] 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. WISTP, Lecture Notes in Computer Science. Berlin, Heidelberg, Germany: Springer, 2014; 8501: 40-56. https://doi.org/10.1007/978-3-662-43826-8_4

[4] Carlet C, Li C, Mesnager S. Linear codes with small hulls in semi-primitive case. Designs, Codes and Cryptography 2019; 87 (12): 3063-3075. https://doi.org/10.1007/s10623-019-00663-4

[5] Carlet C, Güneri C, Özbudak F, Özkaya B, Solé P. On linear complementary pairs of codes. IEEE Transactions on Information Theory 2018; 64 (10): 6583-6589. https://doi.org/10.1109/TIT.2018.2796125

[6] Carlet C, Guilley S. Complementary dual codes for counter-measures to side-channel attacks. Advances in Mathematics of Communications 2014; 10 (1): 131-150. https://doi.org/10.3934/amc.2016.10.131

[7] Guenda K, Gulliver TA, Jitman S, Thipworawimon, S. Linear ℓ-intersection pairs of codes and their applications. Designs, Codes and Cryptography 2020; 88 (1): 133-152. https://doi.org/10.1007/s10623-019-00676-z

[8] Güneri C. Artin-Schreier curves and weights of two-dimensional cyclic codes. Finite Fields and Their Applications 2004; 10 (4): 481-505. https://doi.org/10.1016/j.ffa.2003.10.002

[9] Hossain MA, Bandi R. Linear ℓ-intersection pairs of cyclic and quasi-cyclic codes over a finite field $\mathbb{F}_q$. Journal of Applied Mathematics and Computing 2023; 69 (4): 2901-2917. https://doi.org/10.1007/s12190-023-01861-z

[10] Huffman WC, Pless WC. Fundamentals of Error-Correcting Codes. Cambridge, UK: Cambridge University Press, 2003. https://doi.org/10.1017/CBO9780511807077

[11] Leon JS. Computing automorphism groups of error-correcting codes. IEEE Transactions on Information Theory 1982; 28 (3): 496-511. https://doi.org/10.1109/TIT.1982.1056498

[12] Li C, Zeng P. Constructions of linear codes with one-dimensional hull. IEEE Transactions on Information Theory 2019; 65 (3): 1668-1676. https://doi.org/10.1109/TIT.2018.2863693

[13] Massey JL. Linear codes with complementary duals. Discrete Mathematics 1992; 106-107: 337-342. https://doi.org/10.1016/0012-365X(92)90563-U

[14] Sangwisut E, Jitman S, Ling S, Udomkavanich P. Hulls of cyclic and negacyclic codes over finite fields. Finite Fields and Their Applications 2015; 33: 232-257. https://doi.org/10.1016/j.ffa.2014.12.008

[15] Sendrier N. Finding the permutation between equivalent codes: the support splitting algorithm. IEEE Transactions on Information Theory 2000; 46 (4): 1193-1203. https://doi.org/10.1109/18.850662

[16] Sendrier N, Skersys G. On the computation of the automorphism group of a linear code. Proceedings IEEE International Symposium on Information Theory 2001; 13. https://doi.org/10.1109/ISIT.2001.935876

[17] Sok L. On linear codes with one-dimensional Euclidean hull and their applications to EAQECCs. IEEE Transactions on Information Theory 2022; 68 (7): 4329-4343. https://doi.org/10.1109/TIT.2022.3152580

[18] Sok L. A new construction of linear codes with one-dimensional hull. Designs, Codes and Cryptography 2022; 90 (12): 2823-2839. https://doi.org/10.1007/s10623-021-00991-4

[19] Thipworawimon S, Jitman S. Hulls of linear codes revisited with applications. Journal of Applied Mathematics and Computing 2020; 62 (1-2): 325-340. https://doi.org/10.1007/s12190-019-01286-7

[20] Wolfmann J. New bounds on cyclic codes from algebraic curves. Coding Theory and Applications 1988; 388: 47-62. https://doi.org/10.1007/BFb0019846

[21] Yang X, Massey JL. The condition for a cyclic code to have a complementary dual. Discrete Mathematics 1994; 126 (1-3): 391-393. https://doi.org/10.1016/0012-365X(94)90283-6