Additive Complementary Pairs of Codes

Sanjit Bhowmick[1], Deepak Kumar Dalai[1]

April 29, 2024

Abstract

An additive code is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^m}^n$ over $\mathbb{F}_{q^m}$, which is not a linear subspace over $\mathbb{F}_{q^m}$. Linear complementary pairs(LCP) of codes have important roles in cryptography, such as increasing the speed and capacity of digital communication and strengthening security by improving the encryption necessities to resist cryptanalytic attacks. This paper studies an algebraic structure of additive complementary pairs (ACP) of codes over $\mathbb{F}_{q^m}$. Further, we characterize an ACP of codes in analogous generator matrices and parity check matrices. Additionally, we identify a necessary condition for an ACP of codes. Besides, we present some constructions of an ACP of codes over $\mathbb{F}_{q^m}$ from LCP codes over $\mathbb{F}_{q^m}$ and also from an LCP of codes over $\mathbb{F}_q$. Finally, we study the constacyclic ACP of codes over $\mathbb{F}_{q^m}$ and the counting of the constacyclic ACP of codes. As an application of our study, we consider a class of quantum codes called Entanglement Assisted Quantum Error Correcting Code (EAQEC codes). As a consequence, we derive some EAQEC codes.

Keywords: Additive codes, Additive complementary pairs of codes, Linear complementary pairs of codes, Constacyclic $\mathbb{F}_q$-linear codes.

2020 AMS Classification Code: 94B05; 11T71.

1 Introduction

Linear complementary pairs (LCP) of codes, which were introduced by Bhasin et al. in [22], are extensively explored for wide application in cryptography (see [2, 6]). Further, we refer to some papers [1, 7, 11] on the LCP of codes over a finite field, and we point out that complementary pairs of codes without linearity properties have an essential role in constructing quantum code (see [23]). Thus, it is a useful context for studying non-linear complementary pairs of codes in coding theory. In particular, we study additive complementary pairs (ACP) of codes that extend the analogous of additive complementary dual (ACD) codes. With this point of view, lots of research has been done for additive complementary dual (ACD) codes (see [24, 25, 26]). LCP of codes is a generalization of linear complementary dual (LCD) codes. The notion of LCD codes was introduced by Massy in [20] and later studied in [8, 9, 10, 11, 21].

*[1]School of Mathematical Sciences, National Institute of Science Education and Research,
An OCC of Homi Bhabha National Institute, Bhubaneswar, Odisha 752050, India. Email: sanjitbhowmick@niser.ac.in; deepak@niser.ac.in

Besides, the study of additive codes has gathered significant attention due to their theoretical significance and practical applications. One prominent application of additive codes lies in quantum error correction, where they are employed to protect quantum information from errors induced by noise or other environmental factors. Additionally, additive codes find utility in secret-sharing schemes, where they facilitate the secure distribution of confidential information among multiple parties, ensuring that only authorized subsets of participants can reconstruct the original secret [18]. Additive codes represent a crucial class of codes within coding theory, introduced by Delsarte et al. [13]. Generally, additive codes are subgroups of the underlying abelian group. Further, Huffman [17] provided an algebraic structure for additive cyclic codes over $\mathbb{F}_4$. Through ongoing research and exploration, the potential of additive codes continues to expand, offering valuable insights and solutions in the realms of information theory, quantum computing, and cryptography (see [14]). Recently, Shi et al. [25] developed a theory of ACD codes over $\mathbb{F}_4$ for trace Euclidean and Hermitian inner products. The authors introduced a nice construction of ACP codes over $\mathbb{F}_4$ from binary codes in the same paper. They also established that ACD codes are potentially related to LCD codes. In the same spirit, Choi et al. [12] studied ACP codes over finite field $\mathbb{F}_{q^m}$ with $m \geq 2$ in a general setup of trace inner product. They also provided new construction of ACP codes with respect to trace-Euclidean, Hermitian, and Galois inner products. This general setup showed that ACD codes are related to LCD codes. In this same paper, they further computed good numerical examples of ACP codes. Motivated by these papers, we study the theory of additive complementary pair (ACP) of codes. We further derive some construction of ACP of codes. This paper establishes a relationship between the LCP of codes and the ACP of codes.

On the other hand, an $\dfrac{\mathbb{F}_q[X]}{(X^n-\lambda)}$-submodule of $\dfrac{\mathbb{F}_{q^m}[X]}{(X^n-\lambda)}$ is a λ-constacyclic $\mathbb{F}_q$-linear additive code over $\mathbb{F}_{q^m}$, where $\lambda \in \mathbb{F}_q^*$ and $m \geq 2$. In paper [5], the authors studied the algebraic structure of λ-costacyclic $\mathbb{F}_q$-linear additive code over $\mathbb{F}_{q^m}$. In the same paper, they developed a theory for self-orthogonal and self-dual negacyclic $\mathbb{F}_q$-linear codes over $\mathbb{F}_{q^l}$. The authors in paper [26] deduced a theory for additive cyclic and cyclic $\mathbb{F}_2$-linear ACD codes over $\mathbb{F}_4$ of odd length for the trace Euclidean and Hermitian inner product. They also provided a characterization for subfield subcodes. Inspired by these papers, we will study the constacyclic $\mathbb{F}_q$-linear ACP of codes and counting of constacyclic $\mathbb{F}_q$-linear ACP of codes.

The paper is organized as follows. In Section 2, firstly, we sketch basic definitions, notations, and results on $\mathbb{F}_q$-linear additive codes over $\mathbb{F}_{q^m}$, and secondly, we recall some useful results for our context from constacyclic $\mathbb{F}_q$-linear additive codes over $\mathbb{F}_{q^m}$. Section 3 deals with the characterization of ACP of codes with respect to the general inner product on $\mathbb{F}_{q^m}^n$. Some constructions of ACP of codes are presented in Section 4. Further, we count a formula for constacyclic ACP of codes in Section 5. Finally, we show an application on EAQEC codes in Section 6 and obtain some examples of EAQEC codes. The paper concludes in Section 7.

2 Some preliminaries

2.1 $\mathbb{F}_q$-linear additive codes

Let $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$ be the finite fields with cardinality q and q^m, respectively, and characteristic p (see for more details [12]). A nonempty subset C of $\mathbb{F}_{q^m}^n$ (where $m > 1$) is called an $\mathbb{F}_q$-linear additive code if C is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^m}^n$. Note that an $\mathbb{F}_q$-linear additive code of $\mathbb{F}_{q^m}^n$ is an $\mathbb{F}_q$-linear code over $\mathbb{F}_{q^m}$ of length n. Now, we define a bilinear mapping

$$\mathcal{B} \ : \mathbb{F}_{q^m}^n \times \mathbb{F}_{q^m}^n \to \mathbb{F}_q \text{ such that}$$
$$((a_1, a_2, \dots, a_n), (b_1, b_2, \dots, a_n)) \mapsto \mathcal{B}((a_1, a_2, \dots, a_n), (b_1, b_2, \dots, a_n)) = \sum_{i=1}^{n} Tr(\mu_i a_i \pi(b_{\sigma(i)})) \tag{1}$$

where $Tr : \mathbb{F}_{q^m} \to \mathbb{F}_q$ is the trace mapping defined by $x \mapsto x + x^q + \cdots + x^{q^{m-1}}$, π is a field automorphism on $\mathbb{F}_{q^m}$ and $\sigma \ : \ \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$ is a permutation with corresponding matrix P such that

$$P_{ij} = \begin{cases} 1 & \text{if } i = \sigma(j); \\ 0 & \text{otherwise,} \end{cases}$$

$M = diag(\mu_1, \mu_2, \dots, \mu_n)$ is an $n \times n$ matrix over $\mathbb{F}_{q^m}$ with $\mu_i \in \mathbb{F}_{q^m}^*$, and $(a_1, a_2, \dots, a_n), (b_1, b_2, \dots, b_n) \in \mathbb{F}_{q^m}^n$. Note that $\mathcal{B}$ is not symmetric in general. $\mathcal{B}$ satisfies the following property

(a) $\mathcal{B}$ is non-degenerate;

(b) $Rad_L(B) = \{a \in \mathbb{F}_{q^m}^n \mid \mathcal{B}(a, x) = 0 \text{ for all } x \in \mathbb{F}_{q^m}^n\}$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^m}^n$;

(c) $Rad_R(B) = \{a \in \mathbb{F}_{q^m}^n \mid \mathcal{B}(y, a) = 0 \text{ for all } y \in \mathbb{F}_{q^m}^n\}$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^m}^n$.

For an $\mathbb{F}_q$-linear additive code C over $\mathbb{F}_{q^m}$, the left-dual of C is denoted as $C^{\perp_L}$, defined by

$$C^{\perp_L} = \{a \in \mathbb{F}_{q^m}^n \mid \mathcal{B}(a, c) = 0 \text{ for all } c \in C\}$$

and the right-dual of C is denoted as $C^{\perp_R}$, defined by

$$C^{\perp_R} = \{a \in \mathbb{F}_{q^m}^n \mid \mathcal{B}(c, a) = 0 \text{ for all } c \in C\}.$$

Note that $C^{\perp_L}$ and $C^{\perp_R}$ are $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^m}^n$. It is not difficult to show that $C^{\perp_L}$ and $C^{\perp_R}$ satisfy the conditions

$$\dim_{\mathbb{F}_q}(C) + \dim_{\mathbb{F}_q}(C^{\perp_L}) = nm \tag{2}$$
$$\dim_{\mathbb{F}_q}(C) + \dim_{\mathbb{F}_q}(C^{\perp_R}) = nm \tag{3}$$
$$(C^{\perp_L})^{\perp_R} = (C^{\perp_R})^{\perp_L} = C. \tag{4}$$

2.2 Constacyclic $\mathbb{F}_q$-linear additive codes

In this subsection, we assume that $\gcd(n, p) = 1$. Suppose that λ is an element of $\mathbb{F}_q^*$ with multiplicative order t. Consequently, $\gcd(nt, p) = 1$ as t is divisor of $q - 1$. Now we spell out some notations for our contexts as follows.

- Set $N = nt$.
- Denote $C_i^{(b)} = \{i, ib, ib^2, \ldots\} \pmod N$ as the b-cyclotomic coset containing i modulo N where $i \in \{0, 1, \ldots, n-1\}$ and b is either q or q^m.
- Denote the cardinality of $C_i^{(b)}$ as $|C_i^{(b)}|$.

We need the following lemma for the enrichment of our context. So, we deliver the lemma as follows.

Lemma 2.1. *[5, Lemma 2.1]*

(a) *If* $\gcd(|C_i^{(q)}|, m) = 1$, *then* $C_i^{(q)} = C_i^{(q^m)}$.

(b) *If m is a factor of* $|C_i^{(q)}|$, *then* $|C_i^{(q)}| = m|C_i^{(q^m)}|$ *and* $C_i^{(q)} = C_i^{(q^m)} \cup C_{iq}^{(q^m)} \cup \ldots \cup C_{iq^{m-1}}^{(q^m)}$, *where* $C_{iq^j}^{(q^m)}, 0 \le j \le m-1$ *are pairwise disjoint with same cardinality.*

Let X be an indeterminate over $\mathbb{F}_{q^m}$. Now consider the quotient ring

$$\mathcal{R}_{n,\lambda}^{(q)} = \frac{\mathbb{F}_q[X]}{(X^n - \lambda)} = \bigoplus_{i=0}^{s} \frac{\mathbb{F}_q[X]}{(p_i(X))} = \bigoplus_{i=0}^{s} \mathcal{K}_i \tag{5}$$

where $X^n - \lambda = \prod_{i=0}^{s} p_i(X)$ with each $p_i(X)$ is an irreducible polynomial in $\mathbb{F}_q[X]$, corresponding q-cyclotomic coset $C_{1+tj}^{(q)}$ and $\mathcal{K}_j = \dfrac{\mathbb{F}_q[X]}{(p_j(X))}$ for $0 \le j \le s$. Further, consider the quotient ring

$$\mathcal{R}_{n,\lambda}^{(q^m)} = \frac{\mathbb{F}_{q^m}[X]}{(X^n - \lambda)} = \bigoplus_{i=0}^{\rho} \frac{\mathbb{F}_{q^m}[X]}{(M_i(X))} = \bigoplus_{i=0}^{\rho} \mathcal{I}_i \tag{6}$$

where $X^n - \lambda = \prod_{i=0}^{\rho} M_i(X)$ with each $M_i(X)$ is a polynomial in $\mathbb{F}_{q^m}[X]$ and $\mathcal{I}_j = \dfrac{\mathbb{F}_{q^m}[X]}{(M_j(X))}$ for $0 \le j \le \rho$ with $\rho = r + (s-r)m = ms - (m-1)r$ and

$$M_i(X) = \begin{cases} q_i(X) & \text{if } \ 0 \le i \le r; \\ q_{r+(k-1)m+1}(X) q_{r+(k-1)m+2}(X) \cdots q_{r+km}(X) & \text{if } 1 \le k \le s-r. \end{cases}$$

Here each $q_i(X)$ is an irreducible polynomial in $\mathbb{F}_{q^m}[X]$, corresponding q^m-cyclotomic coset $C_{1+tj}^{(q)}$ for $0 \le j \le s$. Denote $\mathcal{F}_i = \oplus_{h=1}^{m} \mathcal{I}_{r+(i-1)m+h}$, for $1 \le i \le s-r$. For more details to see [5, Section 2].

We next recall that an $\mathbb{F}_q$-linear additive code of length n over $\mathbb{F}_{q^m}$ is defined as an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^m}^n$. In view of the above discussion, we have the following:

Proposition 2.1. *[5, Lemma 3]*

(a) *Each nonempty λ-constacyclic $\mathbb{F}_q$-linear additive code C in $\mathbb{F}_{q^m}^n$ can be uniquely expressed as*

$$C = C_1 \bigoplus C_2 \bigoplus \cdots \bigoplus C_s, \tag{7}$$

where each C_i is a unique $\mathcal{K}_i$-subspace of $\mathcal{I}_i$, for $0 \leq i \leq r$ and C_{r+k} is a unique $\mathcal{K}_i$-subspace of $\mathcal{F}_{r+k}$ for $1 \leq k \leq s-r$.

(b) *Conversely, let D_i be an $\mathcal{K}_i$-subspace of $\mathcal{I}_i$, for $0 \leq i \leq r$ and D_{r+k} be an $\mathcal{K}_i$-subspace of $\mathcal{F}_{r+k}$ for $1 \leq k \leq s-r$. Then the direct sum*

$$D = D_1 \bigoplus D_2 \bigoplus \cdots \bigoplus D_s \tag{8}$$

is an λ-constacyclic $\mathbb{F}_q$-linear additive code over $\mathbb{F}_{q^m}$.

3 Characterization of ACP of codes

For two $\mathbb{F}_q$-linear additive codes over $\mathbb{F}_{q^m}$, C and D, the pair (C, D) is called an additive complementary pair (ACP) of codes if $C \oplus_{\mathbb{F}_q} D = \mathbb{F}_{q^m}^n$. Equivalently, a pair (C, D) is an ACP of codes if and only if $C \cap D = \{0\}$ and $\dim_{\mathbb{F}_q}(C) + \dim_{\mathbb{F}_q}(D) = nm$. Then we have following results.

Lemma 3.1. *Let C and D be two $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_{q^m}^n$. With respect to the inner product B (see Equation (1)), we have the following:*

1) $(C+D)^{\perp_L} = C^{\perp_L} \cap D^{\perp_L}$;
2) $(C+D)^{\perp_R} = C^{\perp_R} \cap D^{\perp_R}$;
3) $C^{\perp_L} + D^{\perp_L} = (C \cap D)^{\perp_L}$;
4) $C^{\perp_R} + D^{\perp_R} = (C \cap D)^{\perp_R}$.

Proof. 1) Let $x \in (C+D)^{\perp_L}$. Then

$$\mathcal{B}(x, a) = 0 \text{ for all } a \in C + D \implies \mathcal{B}(x, c+d) = 0 \text{ for all } c \in C, d \in D.$$

If $d = 0$ then $\mathcal{B}(x, c) = 0$ for all $c \in C \implies x \in C^{\perp_L}$.
Similarly If $c = 0$ then $\mathcal{B}(x, d) = 0$ for all $d \in D, \implies x \in D^{\perp_L}$.
Hence, $x \in C^{\perp_L} \cap D^{\perp_L}$.

For the other direction, let $y \in C^{\perp_L} \cap D^{\perp_L}$.
Then $\mathcal{B}(y, c) = 0$ for all $c \in C$ and $\mathcal{B}(y, d) = 0$ for all $d \in D$. That implies, $\mathcal{B}(x, c+d) = \mathcal{B}(x, c) + \mathcal{B}(x, d) = 0$ for all $c \in C,\ d \in D$. Hence, $x \in (C+D)^{\perp_L}$.

2) It can be proved as in 1).
3) $C^{\perp_L} + D^{\perp_L} = \left((C^{\perp_L} + D^{\perp_L})^{\perp_R}\right)^{\perp_L}$ (see Equation (4)).
Hence, $C^{\perp_L} + D^{\perp_L} = (C \cap D)^{\perp_L}$ (follows from 2).
4) It can be proved as in 3).

$\square$

Then we have the following Theorem.

Theorem 3.2. *Let C and D be two $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_{q^m}^n$. With respect to inner product $\mathcal{B}$ (see Equation (1)), the followings are equivalent.*

1) *the pair (C, D) is an ACP of codes;*

2) *the pair $(C^{\perp_L}, D^{\perp_L})$ is an ACP of codes;*

3) *the pair $(C^{\perp_R}, D^{\perp_R})$ is an ACP of codes.*

Proof. In order to prove that 1), 2) and 3) are equivalent, it is enough to show that 1) and 2) are equivalent. Let us assume that the pair (C, D) is an ACP of codes. Then $C \cap D = \{0\}$ and $\dim_{\mathbb{F}_q}(C) + \dim_{\mathbb{F}_q}(D) = nm$. That is, $C +_{\mathbb{F}_q} D = \mathbb{F}_{q^m}^n$. Then using result in Lemma 3.1[Item 1], we have $C^{\perp_L} \cap D^{\perp_L} = \{0\}$ and from result in Equation (2), we have $\dim_{\mathbb{F}_q}(C^{\perp_L}) + \dim_{\mathbb{F}_q}(D^{\perp_L}) = nm$. Hence, $(C^{\perp_L}, D^{\perp_L})$ is an ACP of codes.

Conversely, suppose that the pair $(C^{\perp_L}, D^{\perp_L})$ is an ACP of codes, which gives that $C^{\perp_L} \cap D^{\perp_L} = \{0\}$ and $C^{\perp_L} +_{\mathbb{F}_q} D^{\perp_L} = \mathbb{F}_{q^m}^n$. From Lemma 3.1, it follows that $C +_{\mathbb{F}_q} D = \mathbb{F}_{q^m}^n$ and $C \cap D = \{0\}$. Hence, (C, D) is an ACP of codes. $\square$

For a matrix $G = (g_{ij})$ with entries $g_{ij} \in \mathbb{F}_{q^m}$, we denote the matrix $Tr(G) = (Tr(g_{ij}))$ over $\mathbb{F}_q$. The following theorem presents an characterizion of an ACP of codes.

Theorem 3.3. *If C and D are two $\mathbb{F}_q$-linear additive codes over $\mathbb{F}_{q^m}$ of length n with generator matrices G_1 and G_2, respectively. If the pair (C, D) is an ACP of codes, then rank $\left(Tr\left(M\begin{pmatrix}\pi(G_1)\\ \pi(G_2)\end{pmatrix}P\right)\right) = n$, where π is a field automorphism on $\mathbb{F}_{q^m}$ and $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ is a permutation with corresponding matrix P such that*

$$P_{ij} = \begin{cases} 1 & \text{if } i = \sigma(j); \\ 0 & \text{otherwise,} \end{cases}$$

$M = diag(\mu_1, \mu_2, \ldots, \mu_n)$ is an $n \times n$ matrix over $\mathbb{F}_{q^m}$ with $\mu_i \in \mathbb{F}_{q^m}^*$.

Proof. Let assume that $rank\left(Tr\left(M\begin{pmatrix}\pi(G_1)\\ \pi(G_2)\end{pmatrix}P\right)\right) < n$. Then there exists $x (\neq 0) \in \mathbb{F}_q^n$ such that $\left(Tr\left(M\begin{pmatrix}\pi(G_1)\\ \pi(G_2)\end{pmatrix}P\right)\right)x^\top = 0$. This gives that $\left(Tr\left(M\begin{pmatrix}\pi(G_1)\\ 0\end{pmatrix}P\right)\right)x^\top = 0$ and $\left(Tr\left(M\begin{pmatrix}0\\ \pi(G_2)\end{pmatrix}P\right)\right)x^\top = 0$. That implies $\mathcal{B}(x, c) = 0$ for all $c \in C$ and $\mathcal{B}(x, d) = 0$ for all $d \in D$, that is $x \in C^{\perp_L}$ and $x \in D^{\perp_L}$. Hence, $x (\neq 0) \in C^{\perp_L} \cap D^{\perp_L}$. Then $(C^{\perp_L}, D^{\perp_L})$ is not an ACP of codes and that implies (C, D) is not an ACP of codes (see Theorem 3.2). This contradicts the hypothesis that (C, D) is an ACP of codes. Hence $rank\left(Tr\left(M\begin{pmatrix}\pi(G_1)\\ \pi(G_2)\end{pmatrix}P\right)\right) = n$. $\square$

We can have similar result in terms of parity check matrices as in the following Corollary.

Corollary 3.4. *If C and D are two $\mathbb{F}_q$-linear additive codes over $\mathbb{F}_{q^m}$ of length n with parity check matrices H_1 and H_2, respectively. If the pair (C, D) is an ACP of codes then rank* $\left(Tr\left(M\begin{pmatrix}\pi(H_1)\\ \pi(H_2)\end{pmatrix}P\right)\right) = n$*, where π is a field automorphism on $\mathbb{F}_{q^m}$ and $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ is a permutation with corresponding matrix P such that*

$$P_{ij} = \begin{cases} 1 & \text{if } i = \sigma(j); \\ 0 & \text{otherwise,} \end{cases}$$

$M = diag(\mu_1, \mu_2, \ldots, \mu_n)$ is an $n \times n$ matrix over $\mathbb{F}_{q^m}$ with $\mu_i \in \mathbb{F}_{q^m}^*$.

In general, the converse of Theorem 3.3 is not correct. The following example illustrates it.

Example 3.5. *Take $\mathbb{F}_q = \mathbb{F}_2$ and $\mathbb{F}_{q^m} = \mathbb{F}_4$ with π is identity automorphism on $\mathbb{F}_{q^m}$. Let C and D be two $\mathbb{F}_2$-linear additive codes over $\mathbb{F}_4$ of length 3 with generator matrices* $G_1 = \begin{pmatrix} 1 & 1 & 0 \\ \omega & \omega & 0 \\ \omega^2 & 0 & \omega^2 \end{pmatrix}$ *and*

$G_1 = \begin{pmatrix} 1 & 1 & 1 \\ \omega & \omega & \omega \\ \omega & \omega & 0 \end{pmatrix}$*, respectively, where ω is a primitive root of $\mathbb{F}_4$. It is easy to see that $C \cap D \neq \{0\}$, as $(\omega,\ \omega,\ 0) \in C \cap D$. Hence (C, D) is not an ACP of codes. However, rank* $\left(Tr\begin{pmatrix} G_1 \\ G_2 \end{pmatrix}\right) = 3.$

Now, we present a necessary and sufficient condition for an ACP of codes.

Theorem 3.6. *Let C and D be two $\mathbb{F}_q$-linear additive codes over $\mathbb{F}_{q^m}$ of length n with generator matrices G_1 and G_2 and parity check matrices H_1 and H_2, respectively. Assume that* $\dim_{\mathbb{F}_q}(C) + \dim_{\mathbb{F}_q}(D) = mn$*. Then the pair (C, D) is an ACP of codes if and only if rank* $\left(Tr\left(H_2 M \left(\pi\left(G_1\right)P\right)^\top\right)\right) = rank(G_1)$ *and rank* $\left(Tr\left(H_1 M \left(\pi\left(G_2\right)P\right)^\top\right)\right) = rank(G_2)$ *where M and P are defined as in Theorem 3.3.*

Proof. Suppose that $rank\left(Tr\left(H_2 M \left(\pi\left(G_1\right)P\right)^\top\right)\right) = rank(G_1)$ and $rank\left(Tr\left(H_1 M \left(\pi\left(G_2\right)P\right)^\top\right)\right) = rank(G_2)$. To prove (C, D) is an ACP of codes, we need to show that $C \cap D = \{0\}$. Let G_1 be an

$k \times n$ matrix and G_2 be an $nm - k \times n$ matrix. If $x \in C \cap D$ then

$$
\begin{aligned}
& x = \alpha G_1 \text{ and } x = \beta G_2 \text{ where } \alpha \in \mathbb{F}_q^n,\ \beta \in \mathbb{F}_q^{nm-k}, \\
\Longrightarrow\ & \pi(\alpha)\pi(G_1) = \pi(\beta)\pi(G_2),\ \text{ where } \pi \text{ is a field automorphism on } \mathbb{F}_{q^m}, \\
\Longrightarrow\ & \pi(\alpha)\pi(G_1)P = \pi(\beta)\pi(G_2)P,\ \text{ where } \sigma\ :\ \{1,2,\ldots,n\} \to \{1,2,\ldots,n\} \\
& \quad \text{is a permutation with corresponding matrix } P \ \text{ such that} P_{ij} = \begin{cases} 1 & \text{if } i = \sigma(j); \\ 0 & \text{otherwise,} \end{cases} \\
\Longrightarrow\ & M\left(\pi(G_1)P\right)^\top \pi(\alpha)^\top = M\left(\pi(G_2)P\right)^\top \pi(\beta)^\top, \\
& \text{where } M = diag(\mu_1, \mu_2, \ldots, \mu_n) \text{ is an } n \times n \text{ matrix over } \mathbb{F}_{q^m} \text{ with } \mu_i \in \mathbb{F}_{q^m}^*, \\
\Longrightarrow\ & H_2 M\left(\pi(G_1)P\right)^\top \pi(\alpha)^\top = H_2 M\left(\pi(G_2)P\right)^\top \pi(\beta)^\top = 0, \\
& H_1 M\left(\pi(G_2)P\right)^\top \pi(\beta)^\top = H_1 M\left(\pi(G_1)P\right)^\top \pi(\alpha)^\top = 0, \\
\Longrightarrow\ & \pi(\alpha) = 0 \text{ as } rank\left(Tr\left(H_2 M\left(\pi\left(G_1\right)P\right)^\top\right)\right) = rank(G_1), \\
& \pi(\beta) = 0 \text{ as } rank\left(Tr\left(H_1 M\left(\pi\left(G_2\right)P\right)^\top\right)\right) = rank(G_2).
\end{aligned}
$$

Hence, $x = 0$ i.e., $C \cap D = \{0\}$. As by hypothesis $\dim_{\mathbb{F}_q}(C) + \dim_{\mathbb{F}_q}(D) = mn$, the pair (C, D) is an ACP of codes.

Conversely, let us suppose that the pair (C, D) is an ACP of codes. Let $rank\left(Tr\left(H_2 M\left(\pi\left(G_1\right)P\right)^\top\right)\right) < rank(G_1)$. Then there exists $x(\neq 0) \in \mathbb{F}_q^n$ such that $\left(Tr\left(H_2 M\left(\pi\left(G_1\right)P\right)^\top\right)\right) x^\top = 0$. That implies, $\left(Tr\left(H_2 M\left(\pi\left(xG_1\right)P\right)^\top\right)\right) = 0$. That is, $xG_1 \in D$. As already, $xG_1 \in C$, $xG_1(\neq 0) \in C \cap D$, which contradicts the fact that the (C, D) is an ACP of codes. Therefore, $rank\left(Tr\left(H_2 D\pi\left(G_1\right)P\right)^\top\right) = rank(G_1)$. Similarly, we can prove that $rank\left(Tr\left(H_1 M\left(\pi\left(G_2\right)P\right)^\top\right)\right) = rank(G_2)$. $\square$

Example 3.7. *Take $\mathbb{F}_q = \mathbb{F}_2$ and $\mathbb{F}_{q^m} = \mathbb{F}_4$. Let C and D be two $\mathbb{F}_2$-linear additive codes over $\mathbb{F}_4$ of length 3 with generator matrices* $G_1 = \begin{pmatrix} 1 & 1 & 0 \\ \omega & 0 & \omega \\ 0 & \omega & \omega \end{pmatrix}$ *and* $G_2 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ \omega & \omega & \omega \end{pmatrix}$, *respectively, where ω is a primitive root of $\mathbb{F}_4$. Here, we take M, π and σ are all identity. Consider a parity check matrices* $H_1 = \begin{pmatrix} 1 & 1 & 1 \\ \omega & \omega & \omega \\ \omega^2 & \omega^2 & 0 \end{pmatrix}$ *and* $H_2 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ \omega & 0 & \omega \end{pmatrix}$ *of C and D, respectively. Then* $H_2 G_1^\top = \begin{pmatrix} 1 & 0 & \omega \\ 1 & \omega & \omega \\ \omega & 0 & \omega^2 \end{pmatrix}$ *and* $H_1 G_2^\top = \begin{pmatrix} 0 & 1 & \omega \\ 0 & \omega & \omega^2 \\ \omega^2 & 0 & 0 \end{pmatrix}$. *Here,* $Tr(H_1 G_2^\top) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ *and* $Tr(H_2 G_1^\top) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$ *which are having rank 3. Hence, (C, D) is ACP over $\mathbb{F}_4$ (see Theorem 3.6).*

4 Building-up construction for ACP of codes

We first present some constructions of $\mathbb{F}_q$-linear additive code over $\mathbb{F}_{q^m}$ by using a linear code over $\mathbb{F}_{q^m}$. Recall that a linear code over $\mathbb{F}_{q^m}$ of length n is a subspace of $\mathbb{F}_{q^m}^n$. Let $\tilde{G}$ be a $(k \times n)$ generator matrix of a linear code $\tilde{C}$ over $\mathbb{F}_{q^m}$. As $\mathbb{F}_{q^m}$ forms a vector space over $\mathbb{F}_q$, consider $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$, a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Denote

$$G = \begin{pmatrix} \tilde{G} \\ \alpha\tilde{G} \\ \vdots \\ \alpha^{m-1}\tilde{G} \end{pmatrix}. \tag{9}$$

It can be shown that G is a generator matrix of an $\mathbb{F}_q$-linear additive code, say C, corresponding to the linear code $\tilde{C}$ over $\mathbb{F}_{q^m}$. Next, we will present a construction of ACP of codes from LCP of codes over $\mathbb{F}_{q^m}$. Towards the LCP of codes, we define a general inner product on $\mathbb{F}_{q^m}$, which is the analog of the inner product $\mathcal{B}$ (see Equation (1)), using the bilinear mapping

$$\tilde{\mathcal{B}} \;:\mathbb{F}_{q^m}^n \times \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m} \text{ such that}$$

$$((a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, a_n)) \mapsto \tilde{\mathcal{B}}((a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, a_n)) = \sum_{i=1}^{n} \mu_i a_i \pi(b_{\sigma(i)}) \tag{10}$$

where μ_i, σ, and π are as defined in Equation (1). Notice that, in general, $\tilde{\mathcal{B}}$ is not symmetric. A pair of codes $(\tilde{C}, \tilde{D})$ of length n over $\mathbb{F}_{q^m}$ is called an LCP of codes if $\tilde{C} \oplus_{\mathbb{F}_{q^m}} \tilde{D} = \mathbb{F}_{q^m}^n$. That is, a pair of codes $(\tilde{C}, \tilde{D})$ of length n over $\mathbb{F}_{q^m}$ is LCP if and only if $\tilde{C} \cap \tilde{D} = \{0\}$ and $\dim_{\mathbb{F}_{q^m}}(\tilde{C}) + \dim_{\mathbb{F}_{q^m}}(\tilde{D}) = n$. The following proposition presents a characterization of LCP of codes over $\mathbb{F}_{q^m}$ with respect to the inner product $\tilde{\mathcal{B}}$ (see Equation (10)).

Proposition 4.1. *Let $\tilde{C}$ and $\tilde{D}$ be two linear codes of length n over $\mathbb{F}_{q^m}$ with generator matrices $\tilde{G}_1$, $\tilde{G}_2$ and parity check matrices $\tilde{H}_1$, $\tilde{H}_2$, respectively. Then the followings are equivalent.*

1. *The pair $(\tilde{C}, \tilde{D})$ is LCP.*
2. *The rank* $\left(M \begin{pmatrix} \pi(\tilde{G}_1) \\ \pi(\tilde{G}_2) \end{pmatrix} P \right) = n$.
3. *The rank* $\left(\left(\tilde{H}_2 D\pi\left(\tilde{G}_1\right) P \right)^{\top} \right) = rank(\tilde{G}_1)$ *and rank* $\left(Tr\left(\tilde{G}_1 D\pi\left(\tilde{G}_2\right) P \right)^{\top} \right) = rank(\tilde{G}_2)$. *Additionally,* $\dim_{\mathbb{F}_{q^m}}(\tilde{C}) + \dim_{\mathbb{F}_{q^m}}(\tilde{D}) = n$.

Here, π is a field automorphism on $\mathbb{F}_{q^m}$, $\sigma \;:\; \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ is a permutation with corresponding matrix P such that

$$P_{ij} = \begin{cases} 1 & \text{if } i = \sigma(j); \\ 0 & \text{otherwise,} \end{cases}$$

and $M = diag(\mu_1, \mu_2, \ldots, \mu_n)$ is an $n \times n$ matrix over $\mathbb{F}_{q^m}$ with $\mu_i \in \mathbb{F}_{q^m}^*$ as defined in Equation (1).

The proof of this Proposition is similar to the proof of the Theorem 3.6. Now we will present an

ACP of codes from a given pair of LCP of codes.

Proposition 4.2. *Let $\tilde{C}$, $\tilde{D}$ be two linear codes of length n over $\mathbb{F}_{q^m}$. Let C, D be the codes constructed from $\tilde{C}$, $\tilde{D}$, respectively, as presented in Equation (9). If the pair $(\tilde{C}, \tilde{D})$ is an LCP of codes over $\mathbb{F}_{q^m}$ then (C, D) is an ACP of codes over $\mathbb{F}_{q^m}$.*

Proof. Let $\tilde{G}_1$, $\tilde{G}_2$ be generator matrices of the linear codes $\tilde{C}$, $\tilde{D}$, respectively. Using Equation 9, construct G_1 and G_2 which are generator matrices of C, D, respectively. Since $(\tilde{C}, \tilde{D})$ is an LCP of codes, $\dim_{\mathbb{F}_{q^m}}(\tilde{C}) + \dim_{\mathbb{F}_{q^m}}(\tilde{D}) = n$ and that implies $\dim_{\mathbb{F}_q}(C) + \dim_{\mathbb{F}_q}(D) = mn$. We need to prove that $C \cap D = \{0\}$. In contrary, assume that there exists a non-zero $x \in \mathbb{F}_q^n$ such that $x \in C \cap D$. Then $x = \gamma G_1 = \delta G_2$ for some $\gamma \in \mathbb{F}_q^k$, $\delta \in \mathbb{F}_q^{mn-k}$ where $k = rank(G_1)$ and $mn - k = rank(G_2)$. Then from Equation (9), we have that $x \in \tilde{C} \cap \tilde{D}$. Since x is nonzero vector in $\mathbb{F}_q^n$, it contradicts that $(\tilde{C}, \tilde{D})$ is an LCP. Hence, (C, D) is an ACP of codes. $\square$

Converse of Proposition 4.2 is not correct in general. For this, we demonstrate an example as follows.

Example 4.1. *Take $\mathbb{F}_q = \mathbb{F}_2$ and $\mathbb{F}_{q^m} = \mathbb{F}_4$. Let C and D be two $\mathbb{F}_2$-linear additive codes over $\mathbb{F}_4$ of length 3 with generator matrices $G_1 = \begin{pmatrix} 1 & 1 & 0 \\ \omega & 0 & \omega \\ 0 & \omega & \omega \end{pmatrix}$ and $G_2 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ \omega & \omega & \omega \end{pmatrix}$, respectively, where ω is a primitive root of $\mathbb{F}_4$. Here, (C, D) is ACP over $\mathbb{F}_4$. It is easy to see that $\tilde{C} \cap \tilde{D} \neq \{0\}$, as $(\omega\ 0\ \omega) \in \tilde{C} \cap \tilde{D}$. Therefore, $(\tilde{C}, \tilde{D})$ is not an LCP of codes over $\mathbb{F}_4$.*

For $\mathbf{a} = (a_1, a_2, \ldots, a_n) \in \left(\mathbb{F}_{q^m}^n\right)$ and a code C, define

$$\mathbf{a}C := \{(a_1c_1, a_2c_2, \ldots, a_nc_n) \mid (c_1, c_2, \ldots, c_n \in C)\}.$$

Note that, for $\mathbf{a} \in \left(\mathbb{F}_{q^m}^*\right)^n$, $\mathbf{a}C$ is an $\mathbb{F}_q$-linear additive code if C is an $\mathbb{F}_q$-linear additive code. Recall that a linear code $\tilde{C} := [n, k, d]$ over $\mathbb{F}_{q^m}$ is MDS if $d = n - k + 1$.

Theorem 4.2. *Let $\tilde{C}$, $\tilde{D}$ be two linear codes of length n over $\mathbb{F}_{q^m}$. Let C, D be the codes constructed from $\tilde{C}$, $\tilde{D}$, respectively, as presented in Equation (9). Assume that at least one of codes $\tilde{C}, \tilde{D}$ is MDS and $\dim_{\mathbb{F}_{q^m}}(\tilde{C}) + \dim_{\mathbb{F}_{q^m}}(\tilde{D}) = n$. Then there exists $\mathbf{a} \in \left(\mathbb{F}_{q^m}^*\right)^n$ such that a pair $(\mathbf{a}C, D)$ is an ACP of codes.*

Proof. Since $q^m \geq 4$, by [1, Theorm 5.4], there exists $\mathbf{a} \in \left(\mathbb{F}_{q^m}^*\right)^n$ such that $(\mathbf{a}\tilde{C}, \tilde{D})$ is an LCP of codes over $\mathbb{F}_{q^m}$. By Proposition 4.2, we obtain that $(\mathbf{a}C, D)$ is an ACP of codes. $\square$

Let $\mathbb{F}_q$ be a finite field with $q \geq 3$, x be transcendental over $\mathbb{F}_q$ and $\mathcal{P}_k = \{f \in \mathbb{F}_q[x] : \deg(f) \leq k - 1\}$. For $\mathbf{b} = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_q^n$, where α_is are distinct elements in $\mathbb{F}_q$, let $RS_k(\mathbf{b}) = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \mid f \in \mathcal{P}_k\}$ be a k-dimensional Reed-Solomon code which is MDS. Then $RS_k(\mathbf{b})$ is $[n, k, n-k+1]$ code and $RS_k(\mathbf{b})^\perp$ is a $[n, n-k, k+1]$ code.

Denote $\widehat{RS_k(\mathbf{b})}$ be the $\mathbb{F}_q$-linear additive code corresponding linear code $RS_k(\mathbf{b})$ over $\mathbb{F}_{q^m}$ and $\widehat{RS_k(\mathbf{b})^\perp}$ be the $\mathbb{F}_q$-linear additive code corresponding linear code $RS_k(\mathbf{b})^\perp$over $\mathbb{F}_{q^m}$.

Example 4.3. *From above discussion,* $RS_k(\boldsymbol{b}) = \{(f(\alpha_1), f(\alpha_2), \dots, f(\alpha_n)) \mid f \in \mathcal{P}_k\}$ *be a* k*-dimensional Reed-Solomon code. Then by Theorem 4.2, there exists* $\mathbf{a} \in \left(\mathbb{F}_{q^m}^*\right)^n$ *such that a pair* $(\mathbf{a}\widehat{RS_k(\boldsymbol{b})}, \widehat{RS_k(\boldsymbol{b})}^{\perp})$ *is an ACP of codes over* $\mathbb{F}_{q^m}$*.*

Let $\tilde{C}$ be a linear code over $\mathbb{F}_{q^m}$ of length n with generator matrix $\tilde{G}$. We define two different expansions of $\tilde{C}$ as $\tilde{C}_{ex_1}$ and $\tilde{C}_{ex_2}$ generated by the generator matrices

$$\tilde{G}_{ex_1} = \begin{pmatrix} \lambda & P \\ 0 & \tilde{G} \end{pmatrix} \text{ and } \tilde{G}_{ex_2} = \begin{pmatrix} P' & \tilde{G} \end{pmatrix},$$

respectively, where $\lambda \in \mathbb{F}_{q^m}, P \in \mathbb{F}_{q^m}^n$ and $P'^{\top} \in \mathbb{F}_{q^m}^k$. We now construct an ACP of codes from the expansions of an ACP of codes.

Theorem 4.4. *Let* $\tilde{C}$ *and* $\tilde{D}$ *be two linear codes over* $\mathbb{F}_{q^m}$ *such that a pair* $(\tilde{C}, \tilde{D})$ *is an ACP of codes (using identity* π*,* σ *and* M *in Proposition 4.1). Then there exist* $\lambda \in \mathbb{F}_{q^m}^*$ *and* $P \in \left(\mathbb{F}_{q^m}^n\right)^*$ *such that the pair* $(\tilde{C}_{ex_1}, \tilde{D}_{ex_2})$ *is an LCP of codes over* $\mathbb{F}_{q^m}$*.*

Proof. Let $\tilde{C}$ and $\tilde{D}$ be two linear codes over $\mathbb{F}_{q^m}$ with generator matrices $\tilde{G}_1$ and $\tilde{G}_2$, respectively. Consider the codes $\tilde{C}_{ex_1}$ and $\tilde{D}_{ex_2}$ with generator matrices $\tilde{G}_{ex_1} = \begin{pmatrix} \lambda & P \\ 0 & \tilde{G}_1 \end{pmatrix}$ and $\tilde{G}_{ex_2} = \begin{pmatrix} P'^{\top} & \tilde{G}_2 \end{pmatrix}$, respectively, where $\lambda \in \mathbb{F}_{q^m}$, non-zero P is an $(1 \times n)$ matrix over $\mathbb{F}_{q^m}$ and P' is an $1 \times (n-k)$ sub-matrix of P. Since, a pair $(\tilde{C}, \tilde{D})$ is an LCP of codes over $\mathbb{F}_{q^m}$, then by Proposition 4.1, $rank \begin{pmatrix} \tilde{G}_1 \\ \tilde{G}_2 \end{pmatrix} = n$. Hence,

$$rank \begin{pmatrix} 0 & \tilde{G}_1 \\ P'^{\top} & \tilde{G}_2 \end{pmatrix} = n. \tag{11}$$

Let $\tilde{C}_1$ be a linear code over $\mathbb{F}_{q^m}$ generated by $\begin{pmatrix} 0 & \tilde{G}_1 \end{pmatrix}$. It is easy to see that $\tilde{C}_1 \cap \tilde{D}_{ex_2} = \{0\}$ by Equation (11). Since, $\tilde{C}_1 + \tilde{D}_{ex_2} \subseteq \tilde{C}_{ex_1} + \tilde{D}_{ex_2}$, $\dim_{\mathbb{F}_{q^m}}(\tilde{C}_1 + \tilde{D}_{ex_2}) \leq \dim_{\mathbb{F}_{q^m}}(\tilde{C}_{ex_1} + \tilde{D}_{ex_2})$ $\implies \dim_{\mathbb{F}_{q^m}}(\tilde{C}_1) + \dim_{\mathbb{F}_{q^m}}(\tilde{D}_{ex_2}) - \dim_{\mathbb{F}_{q^m}}(\tilde{C}_1 \cap \tilde{D}_{ex_2}) \leq \dim_{\mathbb{F}_{q^m}}(\tilde{C}_{ex_1}) + \dim_{\mathbb{F}_{q^m}}(\tilde{D}_{ex_2}) - \dim_{\mathbb{F}_{q^m}}(\tilde{C}_{ex_1} \cap \tilde{D}_{ex_2}) \implies \dim_{\mathbb{F}_{q^m}}(\tilde{C}_{ex_1} \cap \tilde{D}_{ex_2}) \leq 1$.

Further, we choose $\lambda \in \mathbb{F}_{q^m}$ such that $\det \begin{pmatrix} \tilde{G}_{ex_1} \\ \tilde{G}_{ex_2} \end{pmatrix} = \det \begin{pmatrix} \lambda & P \\ 0 & \tilde{G}_1 \\ P'^{\top} & \tilde{G}_2 \end{pmatrix} \neq 0$. Note that there exist such λ satisfying the condition. Then from Proposition 4.1, we have that $\left(\tilde{C}_{ex_1}, \tilde{D}_{ex_2}\right)$ is an LCP of codes over $\mathbb{F}_{q^m}$. $\square$

We denote C_{ex_1} be an $\mathbb{F}_q$-linear additive code over $\mathbb{F}_{q^m}$ corresponding to a linear code $\tilde{C}_{ex_1}$ over $\mathbb{F}_{q^m}$ (see Equation (9)).

Corollary 4.5. *Let* $\tilde{C}$ *and* $\tilde{D}$ *be two linear codes over* $\mathbb{F}_{q^m}$ *such that a pair* $\left(\tilde{C}, \tilde{D}\right)$ *is an LCP of codes (using identity* π*,* σ *and* M *in Proposition 4.1). Then the pair* (C_{ex_1}, D_{ex_2}) *is an ACP of codes over* $\mathbb{F}_{q^m}$*.*

Proof. By Theorem 4.4 with combine Proposition 4.2, we have our results. $\square$

Example 4.6. *Let $\tilde{C}$ and $\tilde{D}$ be two linear codes over $\mathbb{F}_8$ with generator matrices*

$$G_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 \\ 1 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega \\ 1 & \omega^2 & \omega^4 & \omega^6 & \omega & \omega^3 & \omega^5 \\ 1 & \omega^5 & \omega^3 & \omega & \omega^6 & \omega^4 & \omega^2 \end{pmatrix} \text{ and } G_2 = \begin{pmatrix} 1 & 0 & 1 & \omega^6 & \omega^4 & \omega^4 & \omega^6 \\ 0 & 1 & \omega^6 & \omega^4 & \omega^4 & \omega^6 & 1 \end{pmatrix}, \text{ respectively,}$$

where ω is a primitive root of $\mathbb{F}_8$. It can be shown that $\left(\tilde{C}, \tilde{D}\right)$ is an LCP of codes over $\mathbb{F}_8$. By Corollary 4.5, (C_{ex_1}, D_{ex_2}) is an ACP of codes over $\mathbb{F}_8$. However, a generator matrices of $\tilde{C}$ and $\tilde{D}$ of the form

$$G_{ex_1} = \begin{pmatrix} \omega^5 & \omega^6 & \omega^3 & \omega^4 & \omega & \omega^2 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 \\ 0 & 1 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega \\ 0 & 1 & \omega^2 & \omega^4 & \omega^6 & \omega & \omega^3 & \omega^5 \\ 0 & 1 & \omega^5 & \omega^3 & \omega & \omega^6 & \omega^4 & \omega^2 \end{pmatrix} \text{ and } G_{ex_2} = \begin{pmatrix} \omega^6 & 1 & 0 & 1 & \omega^6 & \omega^4 & \omega^4 & \omega^6 \\ \omega^3 & 0 & 1 & \omega^6 & \omega^4 & \omega^4 & \omega^6 & 1 \end{pmatrix}.$$

We further derive a construction of ACP of codes over $\mathbb{F}_{q^m}$ from given m numbers of LCP of codes over $\mathbb{F}_q$ as follows.

Theorem 4.7. *Let $C_i : [n, k_i]$ and $D_i : [n, n-k_i]$ be two linear code over $\mathbb{F}_q$, for $1 \leq i \leq m-1$. If α_i's are distinct elements of $\mathbb{F}_{q^m}^*$ such that $\{\alpha_0, \alpha_1, \ldots, \alpha_{m-1}\}$ are linearly independent over $\mathbb{F}_q$ and (C_i, D_i) is an LCP for $0 \leq i \leq m-1$, then the pair $\left(\sum_{i=0}^{m-1} \alpha_i C_i, \sum_{i=0}^{m-1} \alpha_i D_i\right)$ is an ACP of codes over $\mathbb{F}_{q^m}$.*

Proof. Let $C = \sum_{i=0}^{m-1} \alpha_i C_i$ and $D = \sum_{i=0}^{m-1} \alpha_i D_i$. Now we need to show that $\dim_{\mathbb{F}_q}(C) + \dim_{\mathbb{F}_q}(D) = mn$ and $C \cap D = \{0\}$. From the hypothesis, we have $\dim_{\mathbb{F}_q}(C_i) + \dim_{\mathbb{F}_q}(D_i) = n$ for $0 \leq i \leq m-1$. Hence $\dim_{\mathbb{F}_q}(C) + \dim_{\mathbb{F}_q}(D) = mn$. To prove the second condition, take $x \in C \cap D$. Then $x = \sum_{i=0}^{m-1} \alpha_i c_i$ and $x = \sum_{i=0}^{m-1} \alpha_i d_i$ for some $c_i \in C_i$ and $d_i \in D_i$, where $0 \leq i \leq m-1$. Therefore,

$$\sum_{i=0}^{m-1} \alpha_i c_i = \sum_{i=0}^{m-1} \alpha_i d_i \implies \sum_{i=0}^{m-1} \alpha_i \left(c_i - d_i\right) = 0. \tag{12}$$

Since $\{\alpha_0, \alpha_1, \ldots, \alpha_{m-1}\}$ are linearly independent over $\mathbb{F}_q$, $c_i = d_i$, for all $i : 1 \leq i \leq m-1$. Further as (C_i, D_i) is an LCP for all $i : 1 \leq i \leq m-1$, $c_i = d_i = 0$. Hence, $C \cap D = \{0\}$. $\square$

We next observe the following.

Proposition 4.3. *Let $\tilde{C} := [n, k]$, $\tilde{D} := [n.n-k]$ be two linear codes over $\mathbb{F}_{q^m}$ with a generator matrix $\tilde{G}$ of $\tilde{C}$ and a parity check matrix $\tilde{H}$ of $\tilde{D}$. Suppose that $\tilde{C}_{ex_1}$, $\tilde{D}_{ex_2}$ are two linear codes with a generator matrix $\tilde{G}_{ex_1} = \begin{pmatrix} 1 & d \\ 0 & \tilde{G} \end{pmatrix}$ of $\tilde{C}_{ex_1}$ and a parity check matrix $\tilde{H}_{ex_2} = \begin{pmatrix} 1 & c \\ 0 & \tilde{H} \end{pmatrix}$ of $\tilde{D}_{ex_2}$,* *where $c \in \tilde{C}_{ex_1}$, $d \in \tilde{C}_{ex_1}^{\top}$. Let C, D be $\mathbb{F}_q$-linear additive codes over $\mathbb{F}_{q^m}$ corresponding to the linear codes $\tilde{C}_{ex_1}$ and $\tilde{D}_{ex_2}$, respectively over $\mathbb{F}_{q^m}$ (as in Equation (9)) If the pair $(\tilde{C}, \tilde{D})$ is an LCP of codes (using identity π, σ and M in Proposition 4.1), then (C, D) is an ACP of codes.*

Proof. From Proposition 4.2, it is enough to show that $(\tilde{C}_{ex_1}, \tilde{D}_{ex_2})$ is an LCP of codes. By the construction of $\tilde{C}_{ex_1}$ and $\tilde{D}_{ex_2}$, we obtain that $\tilde{C}_{ex_1}$ is a linear code of length $n+1$ over $\mathbb{F}_{q^m}$ with dimension $k+1$ and $\tilde{D}_{ex_2}$ is a linear code of length $n+1$ over $\mathbb{F}_{q^m}$ with dimension $n-k$. It implies that $\dim\left(\tilde{C}_{ex_1}\right) + \dim\left(\tilde{D}_{ex_2}\right) = n+1$. Now we have to show that $\tilde{C}_{ex_1} \cap \tilde{D}_{ex_2} = \{0\}$.

Let $x \in \tilde{C}_{ex_1} \cap \tilde{D}_{ex_2}$. This implies $x = \alpha \tilde{G}_{ex_1} = \beta G_2$, where $\alpha \in \mathbb{F}_{q^m}^{k+1}$, $\beta \in \mathbb{F}_{q^m}^{n-k}$ and G_2 is a generator matrix of $\tilde{D}_{ex_2}$. This gives that $\alpha \tilde{G}_{ex_1} \tilde{H}_{ex_2}^{\top} = 0$ as $G_2 \tilde{H}_{ex_2}^{\top} = 0$. Then

$$\alpha \tilde{G}_{ex_1} \tilde{H}_{ex_2}^{\top} = 0 \implies \alpha \begin{pmatrix} 1 & d \\ 0 & \tilde{G} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ d^{\top} & \tilde{H}^{\top} \end{pmatrix} = 0 \implies \alpha \begin{pmatrix} 1 + dc^{\top} & 0 \\ 0 & \tilde{G}\tilde{H}^{\top} \end{pmatrix} = 0.$$

Since $(\tilde{C}, \tilde{D})$ is an LCP of codes (using identity π, σ and M in Proposition 4.1), from Proposition 4.1, we get that $rank\left(\tilde{G}\tilde{H}^{\top}\right) = k$. Hence as $rank\left(\tilde{G}\tilde{H}^{\top}\right) = k$ and $dc^{\top} = 0$, we have $\alpha = 0$ i.e., $x = 0$. □

5 Constacyclic $\mathbb{F}_q$-linear ACP of codes over $\mathbb{F}_{q^m}$

This section focuses on counting formulas for constacyclic $\mathbb{F}_q$-linear ACP of codes over $\mathbb{F}_{q^m}$. Recall that two constacyclic $\mathbb{F}_q$-linear codes C and D over $\mathbb{F}_{q^m}$ form an ACP of codes if $C \bigoplus_{\mathbb{F}_q} D = \mathbb{F}_{q^m}^n$. Let denote $q_i = q^{d_i}$. In the following theorem, we derive necessary and sufficient conditions under which a pair of constacyclic $\mathbb{F}_q$-linear codes over $\mathbb{F}_{q^m}$ form an ACP of codes (using identity π, σ and M in Proposition 4.1).

Theorem 5.1. *Let C and D be two λ-constacyclic $\mathbb{F}_q$-linear additive codes over $\mathbb{F}_{q^m}$, whose Canonical decompositions are given by (7) and (8), respectively. Then the pair (C, D) forms an ACP of codes (using identity π, σ and M in Proposition 4.1) if and only if $C_i \bigoplus_{\mathcal{K}_i} D_i = \mathcal{I}_i$, for $0 \le i \le r$ and $C_{r+k} \bigoplus_{\mathcal{K}_{r+k}} D_{r+k} = \mathcal{F}_{r+k}$, for $1 \le k \le s-r$.*

Proof. The proof can be easily derived using Proposition 2.1. □

In order to study constacyclic $\mathbb{F}_q$-linear ACP of codes over $\mathbb{F}_{q^m}$, we first recall that, $|\mathcal{K}_i| = q^{d_i}$, where $|C_{1+ti}^q| = d_i$ for all $0 \le i \le s$. Further $|\mathcal{I}_i| = (q^m)^{d_i} = |\mathcal{K}_i|^m$, for all $0 \le i \le r$. Also, $|\mathcal{F}_{r+k}| = (q^m)^{d_{r+k}} = |\mathcal{K}_{r+k}|^m$, where $|C_{1+t(r+k)}^q| = d_{r+k}$ for all $1 \le r+k \le s-r$. This implies that $\mathcal{I}_i$ is an $\mathcal{K}_i$-linear space of $\mathcal{K}_i^m$ for $0 \le i \le r$ and $\mathcal{F}_{k+r}$ is an $\mathcal{K}_{k+r}$-linear space of $\mathcal{K}_{r+k}^m$ for $1 \le k \le s-r$. It is well known that the number of $\mathbb{F}_{q^{d_i}}$-subspace of $\mathbb{F}_{q^{d_i}}^m$ is equal to $\sum_{v=0}^{m} \begin{bmatrix} m \\ v \end{bmatrix}_{q_i} =$ $\dfrac{(q_i^m - 1)(q_i^m - q_i) \cdots (q_i^m - q_i^{k-1})}{(q_i^v - 1)(q_i^v - q_i) \cdots (q_i^v - q_i^{v-1})}$. From the above discussion, we have the following theorem.

Theorem 5.2. *The number of λ-constacyclic ACP of codes over $\mathbb{F}_{q^m}$ is equal to*

$$\prod_{i=1}^{s}\left(\sum_{v=0}^{m}\begin{bmatrix} m \\ v \end{bmatrix}_{q_i} q_i^{v(m-v)}\right).$$

Proof. By Theorem 5.1, the pair (C, D) is an ACP if and only if $C_i \bigoplus_{\mathcal{K}_i} D_i = \mathcal{I}_i$, for $0 \le i \le r$ and $C_{r+k} \bigoplus_{\mathcal{K}_{r+k}} D_{r+k} = \mathcal{F}_{r+k}$ for $1 \le k \le s-r$. Equivalently, (C, D) is an ACP if and only if (C_i, D_i) is an LCP for all $0 \le i \le s$. If (C_i, D_i) form an LCP for $0 \le i \le s$, then the number of choices of C_i is equal to

$$\sum_{v=0}^{m}\begin{bmatrix} m \\ v \end{bmatrix}_{q_i}$$

and the number of choices of D_i is equal to

$$\frac{(q_i^m - q_i^v)(q_i^m - q_i^{v+1})\cdots(q_i^m - q_i^{m-1})}{(q_i^{m-v}-1)(q_i^{m-v}-q_i)\cdots(q_i^{m-v}-q_i^{m-v-1})} = q_i^{m-v}.$$

Therefore, the number of ACP of codes (C, D) is

$$\#(C, D) = \prod_{i=1}^{s}\left(\sum_{v=0}^{m}\begin{bmatrix} m \\ v \end{bmatrix}_{q_i} q_i^{v(m-v)}\right).$$

This completes the proof. □

We present a numerical example as follows.

Example 5.3. *Take, $q = 3^2$ and consider cyclic $\mathbb{F}_3$-linear additive code over $\mathbb{F}_{3^2}$ of length 10. In this special case, we have $p = 3, m = 2, \lambda = 1$ and $n = 10$. Next, $X^{10} - 1 = \prod_{i=0}^{3} p_i(X)$, where*

$$\begin{aligned} p_0(X) &= X - 1 = 2 + X \\ p_1(X) &= 1 + X \\ p_2(X) &= 1 + X + X^2 + X^3 + X^4 \\ p_3(X) &= 1 + 2X + X^2 + 2X^3 + X^4 \end{aligned}$$

are irreducible polynomials in $\mathbb{F}_3[X]$. By Theorem 5.2, we deduce that the number of cyclic $\mathbb{F}_3$-linear ACP of codes over $\mathbb{F}_{3^2}$ of length 30 equals

$$\#(C, D) = \prod_{i=0}^{3}\left(\sum_{v=0}^{2}\begin{bmatrix} 2 \\ v \end{bmatrix}_{3^{d_i}} q_i^{v(2-v)}\right) = \prod_{i=0}^{3}(2 + 2q_i) = 4,40,896.$$

6 An application on EAQEC codes

In this section, we construct entanglement assisted quantum error correcting (EAQEC) codes from $\mathbb{F}_q$-linear ACP of codes. At first we present some basic concepts and notations on quantum codes. Let $\mathbb{C}^q$ denote the q-dimensional Hilbert space over the complex field $\mathbb{C}$ and K be a finite field with characteristic p. Any n-qubit state is denoted by $|\mathbf{v}\rangle = \sum_{\mathbf{a}\in K^n} v_{\mathbf{a}}|\mathbf{a}\rangle$ where $v_{\mathbf{a}} \in \mathbb{C}$ with $\sum_{\mathbf{a}\in K^n} |v_{\mathbf{a}}|^2 = 1$ and the set $\{|\mathbf{a}\rangle = |a_1\rangle \otimes \cdots \otimes |a_n\rangle : (a_1, \ldots, a_n) \in K^n\}$. For any two vectors $\mathbf{a} = (a_1, \ldots, a_n)$ and $\mathbf{b} = (b_1, \ldots, b_n)$ of K^n, the corresponding tensor products of n error operators are given by $T(\mathbf{a}) = T(a_1)\otimes\cdots\otimes T(a_n)$ and $R(\mathbf{b}) = R(b_1)\otimes\cdots\otimes R(b_n)$. We define the error set $E_n := \{\gamma^i T(\mathbf{a})R(\mathbf{b}) : 0 \le i \le p-1; \mathbf{a}, \mathbf{b} \in K^n\}$ where γ is a complex primitive p-th root of unity. E_n forms an error group.

Now, $T(\mathbf{a})|\mathbf{v}\rangle = |\mathbf{v} + \mathbf{a}\rangle$ and $R(\mathbf{b})|\mathbf{v}\rangle = \gamma^{tr_{\mathbb{F}_q/\mathbb{F}_p}\langle \mathbf{b},\mathbf{v}\rangle}|\mathbf{v}\rangle$. For any error $\mathbf{e} = \gamma^i T(\mathbf{a})R(\mathbf{b})$, we define the quantum weight of $\mathbf{e}$ as

$$w_Q(\mathbf{e}) = \{i : (a_i, b_i) \neq (0, 0)\}.$$

A positive integer d is called the minimum distance of q-ary quantum code Q, if the following are satisfied

- for any $|\mathbf{u}\rangle$, $|\mathbf{v}\rangle$ with $\langle \mathbf{u}, \mathbf{v}\rangle = 0$ such that $\langle \mathbf{u}|\mathbf{e}|\mathbf{v}\rangle = 0$;
- $\mathbf{e} \in E_n(d-1)$, where $E_n(i) = \{\mathbf{e} \in E_n : w_Q(\mathbf{e}) \le i\}$.

A q-ary quantum code with parameters length n, dimension k and minimum distance d is denoted by $[[n, k, d]]_q$. An EAQEC code represented as $[[n, k, d; c]]_q$, encodes k logical qubits into n physical qubits with c copies of maximally entangled states. The performance of an EAQEC code is evaluated through its rate $\frac{k}{n}$ and net rate $\frac{k-c}{n}$, which can be positive, negative or zero. If the net rate of an EAQEC code is zero then it does not mean that no qubits are transmitted by this code. It actually means that a number of bits of entanglement is needed that is equal to the number of bits transmitted. The EAQEC codes with positive net rate are used in Quantum communication where as EAQECCs with negative net rate are used as Catalytic codes in Quantum computing (See [3, 4, 16] for more details). When $c = 0$, the EAQEC code reduced to a standard stabilizer code. EAQEC codes can be regarded as generalized quantum codes.

A construction of EAQEC codes from the classical linear codes is provided by Wilde and Burne in [27].

Proposition 6.1. *[27, Corollary 1] Let $\mathcal{C}_1 : [n, k_1, d_1]$ and $\mathcal{C}_2 : [n, k_2, d_2]$ be two linear codes with parity check matrices H_1 and H_2, respectively. Then there exists an EAQEC code $[[n, k_1 + k_2 - n + c, min\{d_1, d_2\}; c]]_q$, where $c = rank(H_1 H_2^\top)$ is the required number of maximally entangled states.*

Now, we will present a theorem which will be useful for designing EQECC codes later in this section. Towards this, for an $\mathbb{F}_q$-linear additive code C over $\mathbb{F}_{q^m}$ of length n, we define

$$Tr(C) := \{Tr(c) : c \in C\}.$$

Note that $Tr(C)$ is a linear code over $\mathbb{F}_q$ of length n. We call $Tr(C)$ is a Trace code of C. Further, if G is a generator matrix of C, then $Tr(G)$ (defined in Section 3)is a generator matrix of $Tr(C)$.

Theorem 6.1. *Let C and D be two $\mathbb{F}_q$-linear additive codes over $\mathbb{F}_{q^m}$ of length n. If the pair (C, D) is an ACP of codes over $\mathbb{F}_{q^m}$ (using identity π, σ and M in Proposition 4.1), then $(Tr(C), Tr(D))$ is an LCP of codes over $\mathbb{F}_q$. In particular, if C is an additive complementary dual (ACD) codes over $\mathbb{F}_{q^m}$ (using identity π, σ and M in Proposition 4.1), then $Tr(C)$ is an LCD codes over $\mathbb{F}_q$.*

Proof. Let G_1 and G_2 be two generator matrices of C and D, respectively. Since, the pair (C, D) is an ACP of codes over $\mathbb{F}_{q^m}$ (using identity π, σ and M in Proposition 4.1), then by Theorem 3.3, we obtain that $rank\left(Tr\begin{pmatrix} G_1 \\ G_2 \end{pmatrix}\right) = n$. This gives that $rank\begin{pmatrix} Tr(G_1) \\ Tr(G_2) \end{pmatrix} = n$. Since $Tr(G_1)$ and $Tr(G_2)$ are generator matrices of $Tr(C)$ and $Tr(D)$, respectively, from Proposition 4.1, we get $(Tr(C), Tr(D))$ is an LCP of codes over $\mathbb{F}_q$. □

We have the following theorem deducted from Proposition 6.1.

Theorem 6.2. *Let C and D be two $\mathbb{F}_q$-linear additive codes over $\mathbb{F}_{q^m}$ of length n such that $Tr(C) := [n, k_1, d_1]$ and $Tr(D) := [n, k_2, d_2]$. Let parity check matrices of C and D be H_1 and H_2, respectively . Then there exists an EAQEC code $[[n, k_1+k_2-n+c, min\{d_1, d_2\}; c]]_q$ where $c = rank(Tr(H_1)Tr(H_2)^\top)$ is the required number of maximally entangled states.*

Corollary 6.3. *Let (C, D) be an ACP of codes of $\mathbb{F}_{q^m}^n$ such that $Tr(C) := [n, k_1, d_1]$ and $Tr(D) := [n, k_2, d_2]$. Let parity check matrices of C and D be H_1 and H_2, respectively. Then there exists an EAQEC code $[[n, c, min\{d_1, d_2\}; c]]_q$ where $c = rank(Tr(H_1)Tr(H_2)^\top)$ is the required number of maximally entangled states. Moreover, if $D = C^\perp$ with parity check matrix H, then there exists an EAQEC code $[[n, k_1, d_1; n-k_1]]_q$.*

It is well known that $rank(Tr(H)Tr(H)^\top) = \dim(Tr(C^\perp)) - dim(hull(Tr(C)))$ where H is a parity check matrix of C.

Corollary 6.4. *Let C be a $\mathbb{F}_q$-linear additive codes over $\mathbb{F}_{q^m}$ of length n such that $Tr(C) := [n, k, d]$. Let H be a parity check matrix of C. Then there exists an EAQEC code $[[n, k-\dim(hull(Tr(C))), d_H; c]]_q$ where $c = rank(Tr(H)Tr(H)^\top)$ is the required number of maximally entangled states.*

In Table 1, we present some examples of LCD codes corresponding additive code from Theorem 6.1. In Table 1, we we present some examples of EAQEC codes from Trace code of additive code from Corollary 6.4.

No.	Generator of additive codes	Trace Codes $\mathcal{C} := [n, k, d_H]_2$	Remark
1	$\begin{pmatrix} \omega & \omega^2 & 0 & \omega & 0 \\ 0 & \omega & \omega^2 & 0 & \omega \end{pmatrix}$	$[5,\ 2,\ 3]$	not LCD code but optimal
2	$\begin{pmatrix} \omega & \omega^2 & 0 & \omega & \omega & 0 \\ 0 & \omega & \omega^2 & 0 & \omega & \omega \end{pmatrix}$	$[6,\ 2,\ 4]$	not LCD code but optimal
3	$\begin{pmatrix} \omega & 0 & \omega^2 & 0 & \omega & \omega & 0 & 0 \\ 0 & \omega & 0 & \omega^2 & 0 & \omega & \omega & 0 \\ 0 & 0 & \omega & 0 & \omega^2 & 0 & \omega & \omega \end{pmatrix}$	$[8,\ 3,\ 4]$	not LCD code but optimal
4	$\begin{pmatrix} \omega & 0 & \omega^2 & 0 & \omega & \omega & 0 & 0 \\ 0 & \omega & 0 & \omega^2 & 0 & \omega & \omega & 0 \\ 0 & 0 & \omega & 0 & 0 & 0 & \omega & \omega \end{pmatrix}$	$[8,\ 3,\ 3]$	an LCD code but not optimal
5	$\begin{pmatrix} \omega & \omega & 0 & \omega & \omega & 0 & \omega & \omega & 0 \\ 0 & \omega & \omega & 0 & \omega & \omega & 0 & \omega & \omega \end{pmatrix}$	$[9,\ 2,\ 6]$	an LCD code and optimal
6	$\begin{pmatrix} \omega & \omega^2 & 0 & \omega & 0 & \omega & \omega & 0 & 0 \\ 0 & \omega & \omega^2 & 0 & \omega & 0 & \omega & \omega & 0 \\ 0 & 0 & \omega & \omega & 0 & \omega^2 & 0 & \omega^2 & \omega \end{pmatrix}$	$[9,\ 3,\ 3]$	an LCD code and optimal
7	$\begin{pmatrix} \omega & 1 & 0 & \omega & 0 & \omega & \omega & 0 & 0 \\ 0 & \omega & 1 & 0 & \omega & 0 & \omega & \omega & 0 \\ 0 & 0 & \omega & \omega & 0 & \omega^2 & 0 & \omega^2 & \omega \end{pmatrix}$	$[9,\ 3,\ 4]$	an LCD code and optimal
8	$\begin{pmatrix} \omega & \omega & 0 & \omega & \omega & 0 & \omega & \omega^2 & \omega & 0 \\ 0 & \omega & \omega & 0 & \omega & \omega & 0 & \omega & \omega^2 & \omega \end{pmatrix}$	$[10,\ 2,\ 6]$	an LCD code and optimal
9	$\begin{pmatrix} \omega & \omega & 0 & 0 & \omega & 0 & \omega & \omega & 0 & 0 \\ 0 & \omega & \omega & 0 & 0 & \omega^2 & 0 & \omega & \omega & 0 \\ 0 & 0 & \omega & \omega & 0 & 0 & \omega & 0 & \omega^2 & \omega \end{pmatrix}$	$[10,\ 3,\ 5]$	not LCD code and optimal
10	$\begin{pmatrix} \omega & \omega & 0 & 0 & \omega & 0 & \omega & 0 & 0 & 0 \\ 0 & \omega & \omega & 0 & 0 & \omega & 0 & \omega & 0 & 0 \\ 0 & 0 & \omega & \omega & 0 & 0 & \omega^2 & 0 & \omega & 0 \\ 0 & 0 & 0 & \omega & \omega & 0 & 0 & \omega & 0 & \omega \end{pmatrix}$	$[10,\ 4,\ 4]$	an LCD code and optimal
11	$\begin{pmatrix} \omega & \omega & 0 & \omega & \omega & 0 & \omega & \omega & 0 & \omega & 0 \\ 0 & \omega & \omega & 0 & \omega & \omega & 0 & \omega & \omega & 0 & \omega \end{pmatrix}$	$[11,\ 2,\ 7]$	not LCD code and optimal
12	$\begin{pmatrix} \omega & \omega & 0 & 0 & \omega & \omega & 0 & 0 & \omega & 0 & 0 \\ 0 & \omega & \omega & 0 & 0 & \omega & \omega & 0 & 0 & \omega & 0 \\ 0 & 0 & \omega & \omega & 0 & 0 & \omega & \omega^2 & 0 & 0 & \omega \end{pmatrix}$	$[11,\ 3,\ 5]$	an LCD code and optimal

Table 1: Some LCD codes

No.	Generator of additive codes	Trace Codes	EAQEC codes from Corollary 6.4 $[[n, k-dim(hull(\mathcal{C})), d_H; n-k-dim(hull(\mathcal{C}))]]_2$	Existing EAQEC codes
1	$\begin{pmatrix} \omega & \omega^2 & 0 \\ 0 & \omega & \omega^2 \end{pmatrix}$	$[3,\ 2,\ 2]$	$[[3,\ 2,\ 2;\ 1]]_2$	$[[3,\ 2,\ 2;\ 1]]_2$[15]
2	$\begin{pmatrix} \omega & 1 & 0 & 1 & \omega & \omega^2 \\ 0 & \omega & 0 & 1 & 1 & \omega \\ 1 & 1 & \omega^2 & 1 & \omega & 1 \\ 0 & 1 & 0 & \omega^2 & \omega & \omega^2 \end{pmatrix}$	$[6,\ 4,\ 2]$	$[[6,\ 2,\ 2;\ 0]]_2$	$[[6,\ 2,\ 2;\ 0]]_2$[15]
3	$\begin{pmatrix} \omega^2 & 1 & 0 & 1 & 1 & \omega^2 \\ 0 & \omega & 0 & 1 & 1 & \omega \\ 1 & 1 & \omega^2 & 1 & 1 & \omega^2 \\ 0 & 1 & 0 & \omega^2 & 0 & \omega \\ 0 & 0 & 0 & 0 & \omega & \omega^2 \end{pmatrix}$	$[6,\ 5,\ 2]$	$[[6,\ 4,\ 2;\ 0]]_2$	$[[6,\ 2,\ 2;\ 0]]_2$[15]
4	$\begin{pmatrix} \omega & 1 & 0 & 1 & 1 & \omega^2 & \omega \\ 0 & \omega & 0 & 0 & \omega & 1 & \omega \\ 1 & 1 & \omega^2 & 1 & \omega^2 & \omega & 1 \\ 0 & 1 & 0 & \omega^2 & \omega & \omega & \omega^2 \end{pmatrix}$	$[7,\ 4,\ 3]$	$[[7,\ 1,\ 3;\ 0]]_2$	$[[7,\ 1,\ 3;\ 0]]_2$[15]
6	$\begin{pmatrix} \omega & \omega & 0 & \omega & \omega & 0 & \omega & \omega & 0 \\ 0 & \omega & \omega & 0 & \omega & \omega & 0 & \omega & \omega \end{pmatrix}$	$[9,\ 2,\ 6]$	$[[9,\ 2,\ 6;\ 7]]_2$	$[[9,\ 2,\ 6;\ 7]]_2$[19]
7	$\begin{pmatrix} \omega & \omega^2 & 0 & \omega & \omega^2 & 0 & \omega & \omega^2 & 0 & \omega & \omega^2 & 0 & \omega & \omega^2 & 0 \\ 0 & \omega & \omega^2 & 0 & \omega & \omega^2 & 0 & \omega & \omega^2 & 0 & \omega & \omega^2 & 0 & \omega & \omega^2 \end{pmatrix}$	$[15,\ 2,\ 10]$	$[[15,\ 2,\ 10;\ 13]]_2$	$[[15,\ 2,\ 10;\ 13]]_2$[19]

Table 2: Some EAQEC codes

7 Conclusion

In this work, we study the characterization and construction of an ACP of codes of length n over $\mathbb{F}_{q^m}$. Moreover, we obtain a condition for an additive pairs of codes to be an ACP of codes. Furthermore, we provide a necessary and sufficient condition for an ACP of codes. Finally, we obtain an ACP of codes from given linear complementary pairs of codes. In addition, as an immediate consequence, we exhibited some optimal binary LCD codes and corresponding EAQCC codes.

Acknowledgement

The authors would like to thank Markus Grassl for their comments and suggestions which us to improve our manuscript.

References

[1] S. Bhowmick, D. K. Dalai, and S. Mesnager. On Linear Complementary Pairs of Algebraic Geometry Codes over Finite Fields. In *arXiv:2311.01008v1* , 2023.

[2] J. Bringer, C. Carlet, H. Chabanne, S. Guilley, and H. Maghrebi. Orthogonal direct sum masking - A smartcard friendly computation paradigm in a code, with built-in protection against side-channel and fault attacks. In *Information Security Theory and Practice. Securing the Internet of Things WISTP 2014, Crete, Greece. Proceedings*, volume 8501 of *Lecture Notes in Computer Science*, pages 40–56. Springer, 2014.

[3] T. Brun, I. Devetak, M. H. Hsieh. Correcting quantum errors with entanglement. *Science*, **314**:436–439, 2006.

[4] A. R. Calderbank, P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, **54**(2):1098–1105, 1996.

[5] Y. Cao, X. Chang, Y. Cao. Constacyclic $\mathbb{F}_q$-linear codes over $\mathbb{F}_{q^l}$. *Appl. Algebra Eng. Commun. Comput.*, **26**:369-388, 2015.

[6] C. Carlet and S. Guilley. Complementary dual codes for counter-measures to side-channel attacks. *Advances in Mathematics of Communications*, **10**(1):131–150, 2016.

[7] C. Carlet, C. Güneri, F. Özbudak, B. Özkaya, and P. Solé. On linear complementary pairs of codes. *IEEE Trans. Inf. Theory*, **64**(10):6583–6589, 2018.

[8] C. Carlet, S. Mesnager, C. Tang, Y. Qi, and R. Pellikaan. Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$. *IEEE Trans. Inf. Theory*, **64**(4):3010–3017, 2018.

[9] C. Carlet, S. Mesnager, C. Tang, and Y. Qi. Euclidean and hermitian LCD MDS codes. *Designs, Codes and Cryptography*, **86**(11):2605–2618, 2018.

[10] C. Carlet, S. Mesnager, C. Tang, and Y. Qi. On σ-LCD codes. *IEEE Trans. Inf. Theory*, **65**(3):1694–1704, 2019.

[11] C. Güneri, B. Özkaya, and S. Sayici. On linear complementary pair of n D cyclic codes. *IEEE Commun. Lett.*, 22(12):2404–2406, 2018.

[12] W. H. Choi, C. Güneri, J. L. Kim, F. Özbudak. Theory of additive complementary dual codes, constructions and computations. *Finite Fileds Appl.*, **92**:102303, 2023.

[13] P. Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Res.Rep. Suppl.*, 1973.

[14] M. F. Ezerman, S. Ling and P. Sole. Additive asymmetric quantum codes. *IEEE Transactions on Information Theory*, **57**: 5536–5550, 2011.

[15] M. Grassl. Bounds on the minimum distance of entanglement-assisted qubit quantum codes. *http://eaqecc.codetables.de/qubit.php*, (online).

[16] M. Grassl, F. Huber and A. Winter. Entropic Proofs of Singleton Bounds for Quantum Error-Correcting Codes. *IEEE Transactions on Information Theory*, **68**(6): 3942–3952, 2022.

[17] W. C. Huffman. On the theory of $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes. *Advances in Mathematics of Communications*, **7**: 349–378, 2013.

[18] J. L. Kim and N. Lee. Secret sharing schemes based on additive codes over GF(4). *Appl. Algebra Eng. Commun. Comput.*, **28**: 79–97, 2017.

[19] L. Lu, R. Li, L. Guo and Q. Fu. Maximal entanglement entanglement-assisted quantum codes constructed from linear codes. *Quantum Information Processing*, **14**: 165–182, 2015.

[20] J. L. Massey. Linear codes with complementary duals. *Discrete Mathematics*, **106-107**:337–342, 1992.

[21] S. Mesnager, C. Tang, and Y. Qi. Complementary dual algebraic geometry codes. *IEEE Trans. Inf. Theory*, **64**(4):2390–2397, 2018.

[22] X. T. Ngo, S. Bhasin, J. Danger, S. Guilley, and Z. Najm. Linear complementary dual code improvement to strengthen encoded circuit against hardware trojan horses. In *IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2015, Washington, DC, USA, 5-7 May 2015*, pages 82–87. IEEE Computer Society, 2015.

[23] E. M. Rains Nonbinary quantum codes. *IEEE Trans. Inform. Theory*, **45**:1828-1832, 1999.

[24] M. Shi, S. Liu, J. L. Kim, and P. Solé. LCD and ACP codes over a noncommutative non-unital ring with four elements. *Cryptogr. Commun.*, **14**:627-640, 2022.

[25] M. Shi, S. Liu, J. L. Kim, and P. Solé. Additive complementary dual codes over $\mathbb{F}_4$. *Des., Codes Cryptogr.*, **91**:273-284, 2022.

[26] M. Shi, S. Liu, F. Özbudak, and P. Solé. Additive cyclic complementary dual codes over $\mathbb{F}_4$. *Finite Fileds Appl.*, **75**:102087, 2022.

[27] M. M. Wilde, T. A. Brun. Optimal entanglement formulas for entanglement-assisted quantum

coding. Phys. Rev. A, **77**(064302):1-4, 2008.