AIMS Mathematics, 11(7): 22097–22113.
DOI: 10.3934/math.2026894
Received: 31 March 2026
Revised: 12 June 2026
Accepted: 22 June 2026
Published: 24 July 2026

https://www.aimspress.com/journal/Math

Research article

Additive conjucyclic codes over $\mathbb{F}_{q^2}$: Trace correspondence and applications to quantum codes

Jingjie Lv[1], Xian Lian[1], Ruihu Li[2] and Hanxu Hou[1,3,*]

[1] School of Electrical Engineering & Intelligentization, Dongguan University of Technology, Dongguan 523808, China
[2] Fundamentals Department, Air Force Engineering University, Xi'an 710051, China
[3] School of Computer Science and Artificial Intelligence, Shenzhen University of Advanced Technology, Shenzhen 518055, China

* **Correspondence:** Email: houhanxu@163.com.

Abstract: Additive conjucyclic codes over $\mathbb{F}_{q^2}$ are closed under the conjugated cyclic shift and play an important role in constructing quantum error-correcting codes (QECCs). However, a systematic algebraic theory for such codes over general finite fields has been lacking. In this paper, we develop a unified framework by establishing a trace-based $\mathbb{F}_q$-linear isomorphism between $\mathbb{F}_{q^2}^n$ and $\mathbb{F}_q^{2n}$. This correspondence shows that additive conjucyclic codes of length n correspond bijectively to q-ary linear cyclic codes of length $2n$, translating their structural analysis to the well-understood setting of cyclic codes. Using this isomorphism, we determine the enumeration of such codes and give explicit forms of their generator matrices. We then introduce an alternating inner product on $\mathbb{F}_{q^2}^n$, which is shown to be compatible with the symplectic inner product on $\mathbb{F}_q^{2n}$ under the trace isomorphism. Based on this inner product, we characterize the dual-containing condition for additive conjucyclic codes and derive explicit parity-check matrices. Finally, we construct q-ary QECCs from dual-containing additive conjucyclic codes. Our results unify and generalize previous studies on quaternary additive conjucyclic codes and present a construction method for q-ary QECCs from additive conjucyclic codes, together with an illustrative example.

Keywords: additive codes; conjucyclic codes; trace map; alternating inner product; quantum error-correcting codes
Mathematics Subject Classification: 11T71, 94B05

List of symbols

For the reader's convenience, we list the main symbols used in this paper:

$\mathbb{F}_{q^2}$	finite field with q^2 elements, q a prime power p
$\bar{\alpha} = \alpha^q$	conjugation in $\mathbb{F}_{q^2}$
$\mathrm{Tr} : \mathbb{F}_{q^2} \to \mathbb{F}_q$	trace map, $\mathrm{Tr}(x) = x + x^q$
β	a fixed primitive element of $\mathbb{F}_{q^2}$
$C^{\perp_e}, C^{\perp_s}, C^{\perp_a}$	Euclidean, symplectic and alternating dual codes of C
σ	right cyclic shift operator, $\sigma(c_0, \ldots, c_{n-1}) = (c_{n-1}, c_0, \ldots, c_{n-2})$
T	right conjucyclic shift operator, $T(c_0, \ldots, c_{n-1}) = (\bar{c}_{n-1}, c_0, \ldots, c_{n-2})$
$\varphi_\beta : \mathbb{F}_{q^2} \to \mathbb{F}_q^2$	$\varphi_\beta(\alpha) = (\mathrm{Tr}(\beta\alpha), \mathrm{Tr}(\bar{\beta}\alpha))$
$\Psi_\beta : \mathbb{F}_{q^2}^n \to \mathbb{F}_q^{2n}$	componentwise extension of φ_β
$\langle \cdot, \cdot \rangle_e$	Euclidean inner product
$\langle \cdot, \cdot \rangle_s$	symplectic inner product on $\mathbb{F}_q^{2m}$
$\langle \cdot, \cdot \rangle_{a,\beta}$	alternating inner product on $\mathbb{F}_{q^2}^n$
$\mathrm{Div}_{\mathbb{F}_q}(x^{2n} - 1)$	set of divisors of $x^{2n} - 1$ over $\mathbb{F}_q$
$g(x)$	generator polynomial of a cyclic code (divisor of $x^{2n} - 1$)
$h(x)$	$(x^{2n} - 1)/g(x)$
$h^*(x)$	reciprocal polynomial of $h(x)$
$\boldsymbol{f}$	coefficient vector of polynomial $f(x)$
τ	linear transformation $\tau(v_0, \ldots, v_{2n-1}) = (-v_n, \ldots, -v_{2n-1}, v_0, \ldots, v_{n-1})$
$\hat{G}$	generator matrix of an additive conjucyclic code C
$\hat{H}_a$	generator matrix of $C^{\perp_{a,\beta}}$ (also parity-check matrix of C)

1. Introduction

Additive codes were first introduced by Delsarte and Levenshtein in 1973 [1]. A seminal contribution by Calderbank et al. [2] established a direct connection between quaternary additive codes and binary quantum error-correcting codes (QECCs). The latter play a crucial role in mitigating environmental and operational decoherence in quantum information, thereby underpinning both quantum communication and quantum computation. In recent years, additive codes have gained increasing interest, as reflected by advances in their structural properties, optimal parameters, among others [3–5].

Additive cyclic codes constitute a distinguished subclass of additive codes, characterized by invariance under cyclic shifts (see Definition 2.1). This structural property facilitates efficient encoding and decoding via shift registers. The algebraic structure of quaternary additive cyclic codes was first investigated by Huffman [6], who established a canonical decomposition for codes of odd length. Subsequently, Bierbrauer [7] extended the theory to additive cyclic codes over arbitrary finite fields. Güneri et al. [8] derived a sufficient condition under which a particular family of additive cyclic codes are complementary dual. The existence of asymptotically good additive cyclic codes was later demonstrated by Shi et al. [9]. More recently, Dastbasteh and Shivji [10] introduced a polynomial representation for additive cyclic codes over $\mathbb{F}_{p^2}$ and derived new binary quantum codes from this framework. Very recently, further developments include the characterization of trace duality and additive complementary pairs for additive cyclic codes over finite chain rings [4].

Similar to additive cyclic codes, additive conjucyclic codes are closed under the conjugated cyclic shift (see Definition 2.2) and can also be utilized to construct QECCs [2]. However, in contrast to the

extensive study of additive cyclic codes, research on additive conjucyclic codes remains remarkably limited. A major obstacle is that these codes do not admit a canonical polynomial representation, which complicates their structural analysis. The additive case was first systematically addressed by Abualrub et al. [11, 12], who developed an algebraic description over $\mathbb{F}_4$ using a linear algebraic approach. Nevertheless, their method relies heavily on the specific properties of $\mathbb{F}_4$ and does not readily generalize to arbitrary q^2-ary alphabets. To date, the literature on additive conjucyclic codes remains sparse, with no unified framework applicable to general finite fields $\mathbb{F}_{q^2}$. This gap motivates the present work, in which we aim to develop a systematic algebraic theory for additive conjucyclic codes over $\mathbb{F}_{q^2}$ by establishing a trace-based isomorphism with q-ary linear cyclic codes. This approach not only reveals the underlying cyclic structure but also facilitates the construction of QECCs via the alternating inner product.

In this paper, we investigate the algebraic structure of additive conjucyclic codes over $\mathbb{F}_{q^2}$. By employing the trace function from $\mathbb{F}_{q^2}$ down to $\mathbb{F}_q$, we establish an isomorphic correspondence between q^2-ary additive conjucyclic codes and q-ary linear cyclic codes. Using this correspondence, we determine the enumeration of such codes and provide explicit forms of their generator matrices. Furthermore, by defining an alternating inner product on $\mathbb{F}_{q^2}^n$, we characterize the dual-containing condition for these codes and derive explicit parity-check matrices, which then yield a construction method for q-ary quantum error-correcting codes from additive conjucyclic codes.

The remainder of this paper is organized as follows. Section 2 introduces the necessary definitions and preliminary results on cyclic codes, conjucyclic codes, as well as the Euclidean and symplectic inner products. A list of the main symbols used throughout the paper is provided at the end of this section. In Section 3, we establish a trace-based correspondence between q^2-ary additive conjucyclic codes and q-ary linear cyclic codes, and give their enumeration and generator matrices. Section 4 defines the alternating inner product on $\mathbb{F}_{q^2}^n$, investigates the dual structure under this inner product, derives explicit parity-check matrices, and presents a construction method for q-ary QECCs from additive conjucyclic codes, together with an illustrative example. Section 5 concludes the paper.

2. Preliminaries

Let $\mathbb{F}_{q^2}$ be a finite field with q^2 elements, where q is a prime power p. Denote by $\mathrm{char}(\mathbb{F}_{q^2}) = p$ the characteristic of $\mathbb{F}_{q^2}$. For any element $\alpha \in \mathbb{F}_{q^2}$, let $\bar{\alpha} = \alpha^q$ denote its conjugation. A linear code with parameters $[n, k]_{q^2}$ is a k-dimensional linear subspace of $\mathbb{F}_{q^2}^n$. An additive code C of length n over $\mathbb{F}_{q^2}$ is a subgroup of the additive group of $\mathbb{F}_{q^2}^n$; if $|C| = M$, we refer to it as an $(n, M)_{q^2}$ additive code. In general, for an arbitrary element $k \in \mathbb{F}_{q^2}$ and a codeword $\mathbf{c} \in C$, the scalar multiple $k\mathbf{c}$ need not lie in C. When C is closed under multiplication by elements of $\mathbb{F}_q$ (i.e., $k\mathbf{c} \in C$ for all $k \in \mathbb{F}_q$ and $\mathbf{c} \in C$), we call C an $\mathbb{F}_q$-linear additive code. In this paper, the term additive code will always refer to an $\mathbb{F}_q$-linear additive code unless stated otherwise.

For a vector $\boldsymbol{u} = (u_0, u_1, \ldots, u_{n-1}) \in \mathbb{F}_q^n$, define its Hamming weight as $w_h(\boldsymbol{u}) = \mathrm{card}\{i \mid u_i \neq 0,\ 0 \leq i \leq n-1\}$. For a q-ary linear or additive code C of length n, the minimum Hamming weight is given by

$$w_h(C) = \min\{w_h(\boldsymbol{u}) \mid \boldsymbol{u} \in C,\ \boldsymbol{u} \neq \mathbf{0}\}.$$

If $n = 2m$, for $0 \leq j \leq m-1$, define the symplectic weight of $\boldsymbol{u}$ as $w_s(\boldsymbol{u}) = \mathrm{card}\{j \mid (u_j, u_{m+j}) \neq (0, 0)\}$.

The minimum symplectic weight of C is then defined as

$$w_s(C) = \min\{w_s(\boldsymbol{u}) \mid \boldsymbol{u} \in C,\ \boldsymbol{u} \neq \mathbf{0}\}.$$

We now introduce the definition of cyclic codes.

Definition 2.1. Let C be a linear or additive code of length n over $\mathbb{F}_q$. If for every codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in C$, its right cyclic shift

$$\sigma(\mathbf{c}) = (c_{n-1}, c_0, \ldots, c_{n-2}) \tag{2.1}$$

also belongs to C, then C is called a q-ary cyclic code of length n.

Let $\mathbb{R} = \mathbb{F}_q[x]/\langle x^n - 1\rangle$ be the quotient ring. Define an $\mathbb{F}_q$-module isomorphism $\phi : \mathbb{F}_q^n \to \mathbb{R}$ by

$$\phi(c_0, c_1, \ldots, c_{n-1}) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}.$$

It is easy to see that C is a q-ary linear cyclic code of length n if and only if $\phi(C)$ is an ideal of $\mathbb{R}$. Since $\mathbb{R}$ is a principal ideal ring, there exists a one-to-one correspondence between monic divisors of $x^n - 1$ in $\mathbb{F}_q[x]$ and q-ary linear cyclic codes of length n. Thus, the factorization of $x^n - 1$ is essential for classifying such codes. If a linear cyclic code C is generated by a monic divisor $g(x)$ of $x^n - 1$, we call $g(x)$ the generator polynomial of C; for convenience, we denote C by $\langle g(x)\rangle$ throughout.

The definition of conjucyclic codes is analogous.

Definition 2.2. Let C be a q^2-ary linear or additive code of length n. For any codeword $\boldsymbol{c} = (c_0, c_1, \ldots, c_{n-1}) \in C$, if its right conjucyclic shift

$$T(\boldsymbol{c}) = (\bar{c}_{n-1}, c_0, \ldots, c_{n-2}) \tag{2.2}$$

lies in C, then C is called a q^2-ary conjucyclic code of length n.

We now introduce several inner products and their associated dual codes, which will be used throughout this paper.

For two vectors $\boldsymbol{u} = (u_0, u_1, \ldots, u_{n-1})$ and $\boldsymbol{v} = (v_0, v_1, \ldots, v_{n-1})$ in $\mathbb{F}_q^n$, the Euclidean inner product is defined as

$$\langle \boldsymbol{u}, \boldsymbol{v}\rangle_e = \sum_{i=0}^{n-1} u_i v_i.$$

If $n = 2m$, the symplectic inner product is given by

$$\langle \boldsymbol{u}, \boldsymbol{v}\rangle_s = \sum_{i=0}^{m-1} (u_i v_{m+i} - u_{m+i} v_i). \tag{2.3}$$

The corresponding Euclidean and symplectic dual codes of a code C are respectively defined as

$$C^{\perp_e} = \{\boldsymbol{v} \in \mathbb{F}_q^n \mid \langle \boldsymbol{u}, \boldsymbol{v}\rangle_e = 0,\ \forall \boldsymbol{u} \in C\},\ \ C^{\perp_s} = \{\boldsymbol{v} \in \mathbb{F}_q^{2m} \mid \langle \boldsymbol{u}, \boldsymbol{v}\rangle_s = 0,\ \forall \boldsymbol{u} \in C\}.$$

3. Algebraic correspondence and generator description

In this section, we first show that there exists a bijective correspondence between q^2-ary additive conjucyclic codes of length n and q-ary linear cyclic codes of length $2n$.

Let $\mathrm{Tr} : \mathbb{F}_{q^2} \to \mathbb{F}_q$ denote the trace map defined by $\mathrm{Tr}(x) = x + x^q$ for all $x \in \mathbb{F}_{q^2}$. For a fixed primitive element $\beta \in \mathbb{F}_{q^2}$, define a mapping $\varphi_\beta : \mathbb{F}_{q^2} \to \mathbb{F}_q^2$ by

$$\varphi_\beta(\alpha) = (\mathrm{Tr}(\beta\alpha),\ \mathrm{Tr}(\bar{\beta}\alpha)). \tag{3.1}$$

Proposition 3.1. *The map φ_β in* (3.1) *is an $\mathbb{F}_q$-linear isomorphism.*

Proof. For any $k_1, k_2 \in \mathbb{F}_q$ and $\alpha_1, \alpha_2 \in \mathbb{F}_{q^2}$, we have

$$\begin{aligned}\varphi_\beta(k_1\alpha_1 + k_2\alpha_2) &= (\mathrm{Tr}(\beta(k_1\alpha_1 + k_2\alpha_2)),\ \mathrm{Tr}(\bar{\beta}(k_1\alpha_1 + k_2\alpha_2)))\\ &= (k_1\mathrm{Tr}(\beta\alpha_1) + k_2\mathrm{Tr}(\beta\alpha_2),\ k_1\mathrm{Tr}(\bar{\beta}\alpha_1) + k_2\mathrm{Tr}(\bar{\beta}\alpha_2))\\ &= k_1\varphi_\beta(\alpha_1) + k_2\varphi_\beta(\alpha_2),\end{aligned}$$

so φ_β is $\mathbb{F}_q$-linear.

To prove injectivity, assume $\varphi_\beta(\alpha_1) = \varphi_\beta(\alpha_2)$. Then

$$\mathrm{Tr}(\beta(\alpha_1 - \alpha_2)) = 0, \quad \mathrm{Tr}(\bar{\beta}(\alpha_1 - \alpha_2)) = 0,$$

which is equivalent to the system

$$\begin{cases}\beta(\alpha_1 - \alpha_2) + \bar{\beta}(\alpha_1 - \alpha_2)^q = 0,\\ \bar{\beta}(\alpha_1 - \alpha_2) + \beta(\alpha_1 - \alpha_2)^q = 0.\end{cases} \tag{3.2}$$

If $\mathrm{char}(\mathbb{F}_{q^2}) = 2$, then (3.2) gives

$$\beta(\alpha_1 + \alpha_2) = \bar{\beta}(\alpha_1 + \alpha_2)^q, \quad \bar{\beta}(\alpha_1 + \alpha_2) = \beta(\alpha_1 + \alpha_2)^q,$$

so both $\beta(\alpha_1 + \alpha_2)$ and $\bar{\beta}(\alpha_1 + \alpha_2)$ lie in $\mathbb{F}_q$. Since β is primitive, this forces $\alpha_1 = \alpha_2$.

Now suppose $\mathrm{char}(\mathbb{F}_{q^2}) \neq 2$. Adding and subtracting the two equations in (3.2) yields

$$\begin{cases}(\beta + \bar{\beta})((\alpha_1 - \alpha_2) + (\alpha_1 - \alpha_2)^q) = 0,\\ (\beta - \bar{\beta})((\alpha_1 - \alpha_2) - (\alpha_1 - \alpha_2)^q) = 0.\end{cases}$$

Note that $\beta + \bar{\beta} \neq 0$ and $\beta - \bar{\beta} \neq 0$; otherwise $\beta^{2q-2} = 1$ or $\beta^{q-1} = 1$, contradicting the fact that β has order $q^2 - 1$ with $q - 1 < 2q - 2 < q^2 - 1$. Hence

$$\begin{cases}(\alpha_1 - \alpha_2) + (\alpha_1 - \alpha_2)^q = 0,\\ (\alpha_1 - \alpha_2) - (\alpha_1 - \alpha_2)^q = 0,\end{cases}$$

which implies $2(\alpha_1 - \alpha_2) = 0$ and therefore $\alpha_1 = \alpha_2$ (since $p \neq 2$). Thus φ_β is injective, and because both spaces have dimension 2 over $\mathbb{F}_q$, it is an isomorphism. □

Remark 3.2. Notice that the mapping φ_β is an $\mathbb{F}_q$-linear isomorphism. Hence any element $\alpha \in \mathbb{F}_{q^2}$ is uniquely determined by $(\mathrm{Tr}(\beta\alpha), \mathrm{Tr}(\bar{\beta}\alpha)) \in \mathbb{F}_q^2$. In fact,

$$\alpha = \frac{1}{\beta - \beta^{2q-1}}\mathrm{Tr}(\beta\alpha) - \frac{\beta^{q-1}}{\beta - \beta^{2q-1}}\mathrm{Tr}(\bar{\beta}\alpha). \tag{3.3}$$

Example 3.3. Let $q = 3$ and let β be a primitive element of $\mathbb{F}_9$. Then the mapping $\varphi_\beta : \mathbb{F}_9 \to \mathbb{F}_3^2$ is given as follows:

α	$\varphi_\beta(\alpha)$
0	$(0,0)$
β^0	$(1,1)$
β	$(0,1)$
β^2	$(1,2)$
β^3	$(1,0)$

α	$\varphi_\beta(\alpha)$
β^4	$(2,2)$
β^5	$(0,2)$
β^6	$(2,1)$
β^7	$(2,0)$

.

According to (3.3) in Remark 3.2, we compute

$$\frac{1}{\beta - \beta^5} = \beta^3, \quad \frac{\beta^2}{\beta - \beta^5} = \beta^5$$

and the identities can be summarized as follows, where $(a, b) = \varphi_\beta(\alpha) = (\mathrm{Tr}(\beta\alpha), \mathrm{Tr}(\bar{\beta}\alpha))$:

$\beta^3 \cdot a - \beta^5 \cdot b$	α
$\beta^3 \cdot 0 - \beta^5 \cdot 0$	0
$\beta^3 \cdot 1 - \beta^5 \cdot 1$	β^0
$\beta^3 \cdot 0 - \beta^5 \cdot 1$	β
$\beta^3 \cdot 1 - \beta^5 \cdot 2$	β^2
$\beta^3 \cdot 1 - \beta^5 \cdot 0$	β^3

$\beta^3 \cdot a - \beta^5 \cdot b$	α
$\beta^3 \cdot 2 - \beta^5 \cdot 2$	β^4
$\beta^3 \cdot 0 - \beta^5 \cdot 2$	β^5
$\beta^3 \cdot 2 - \beta^5 \cdot 1$	β^6
$\beta^3 \cdot 2 - \beta^5 \cdot 0$	β^7

.

The map φ_β extends componentwise to an $\mathbb{F}_q$-linear isomorphism $\Psi_\beta : \mathbb{F}_{q^2}^n \to \mathbb{F}_q^{2n}$ as follows: for any vector $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{F}_{q^2}^n$,

$$\Psi_\beta(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) = (\varphi_\beta(\alpha_0), \varphi_\beta(\alpha_1), \ldots, \varphi_\beta(\alpha_{n-1})),$$

where each $\varphi_\beta(\alpha_i) = (\mathrm{Tr}(\beta\alpha_i), \mathrm{Tr}(\bar{\beta}\alpha_i))$ is regarded as a pair in $\mathbb{F}_q^2$. Expanding the pairs in the order of all first components followed by all second components, we obtain the explicit coordinate representation

$$\Psi_\beta(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) = (\mathrm{Tr}(\beta\alpha_0), \mathrm{Tr}(\beta\alpha_1), \ldots, \mathrm{Tr}(\beta\alpha_{n-1}), \mathrm{Tr}(\bar{\beta}\alpha_0), \ldots, \mathrm{Tr}(\bar{\beta}\alpha_{n-1})). \tag{3.4}$$

Proposition 3.4. *For any vector $\alpha \in \mathbb{F}_{q^2}^n$ and any integer $i \geq 0$, we have $\Psi_\beta(T^i(\alpha)) = \sigma^i(\Psi_\beta(\alpha))$, where σ and T are the cyclic shift and conjucyclic shift operators defined in* (2.1) *and* (2.2)*, respectively. In other words, the following diagram commutes for all i:*

$$\begin{array}{ccc} \mathbb{F}_{q^2}^n & \xrightarrow{T^i} & \mathbb{F}_{q^2}^n \\ \downarrow \Psi_\beta & & \downarrow \Psi_\beta \\ \mathbb{F}_q^{2n} & \xrightarrow{\sigma^i} & \mathbb{F}_q^{2n}. \end{array}$$

Proof. We first prove the case $i = 1$. For any $\alpha = (\alpha_0, \ldots, \alpha_{n-1}) \in \mathbb{F}_{q^2}^n$, we compute

$$\begin{aligned}\Psi_\beta(T(\alpha)) &= \Psi_\beta(\bar{\alpha}_{n-1}, \alpha_0, \ldots, \alpha_{n-2}) \\ &= (\mathrm{Tr}(\beta\bar{\alpha}_{n-1}), \mathrm{Tr}(\beta\alpha_0), \ldots, \mathrm{Tr}(\beta\alpha_{n-2}), \mathrm{Tr}(\bar{\beta}\bar{\alpha}_{n-1}), \mathrm{Tr}(\bar{\beta}\alpha_0), \ldots, \mathrm{Tr}(\bar{\beta}\alpha_{n-2})),\end{aligned}$$

$$\begin{aligned}\sigma(\Psi_\beta(\alpha)) &= \sigma(\mathrm{Tr}(\beta\alpha_0), \ldots, \mathrm{Tr}(\beta\alpha_{n-1}), \mathrm{Tr}(\bar{\beta}\alpha_0), \ldots, \mathrm{Tr}(\bar{\beta}\alpha_{n-1})) \\ &= (\mathrm{Tr}(\bar{\beta}\alpha_{n-1}), \mathrm{Tr}(\beta\alpha_0), \ldots, \mathrm{Tr}(\beta\alpha_{n-2}), \mathrm{Tr}(\beta\alpha_{n-1}), \mathrm{Tr}(\bar{\beta}\alpha_0), \ldots, \mathrm{Tr}(\bar{\beta}\alpha_{n-2})).\end{aligned}$$

Using the identities $\mathrm{Tr}(\beta\bar{\alpha}_{n-1}) = \mathrm{Tr}(\bar{\beta}\alpha_{n-1})$ and $\mathrm{Tr}(\bar{\beta}\bar{\alpha}_{n-1}) = \mathrm{Tr}(\beta\alpha_{n-1})$ (which follow directly from the definition of the trace), we see that the first component of $\Psi_\beta(T(\alpha))$ coincides with the first component of $\sigma(\Psi_\beta(\alpha))$, and the $(n+1)$-th component of $\Psi_\beta(T(\alpha))$ coincides with the $(n+1)$-th component of $\sigma(\Psi_\beta(\alpha))$. All remaining components are identical by construction. Hence $\Psi_\beta(T(\alpha)) = \sigma(\Psi_\beta(\alpha))$, which establishes the case $i = 1$.

Now assume that $\Psi_\beta(T^{i-1}(\alpha)) = \sigma^{i-1}(\Psi_\beta(\alpha))$ holds for some $i \geq 2$. Then

$$\Psi_\beta(T^i(\alpha)) = \Psi_\beta(T(T^{i-1}(\alpha))) = \sigma(\Psi_\beta(T^{i-1}(\alpha))) = \sigma(\sigma^{i-1}(\Psi_\beta(\alpha))) = \sigma^i(\Psi_\beta(\alpha)).$$

Thus the statement holds for all $i \geq 0$ by induction. □

Consequently, we obtain a bijective correspondence between additive conjucyclic codes and linear cyclic codes.

Theorem 3.5. *A code $C \subseteq \mathbb{F}_{q^2}^n$ is an additive conjucyclic code if and only if $\mathcal{D} = \Psi_\beta(C)$ is a q-ary linear cyclic code of length $2n$. Moreover, the minimum Hamming weight of C equals the minimum symplectic weight of $\mathcal{D}$, i.e., $w_h(C) = w_s(\mathcal{D})$.*

Proof. Suppose C is an additive conjucyclic code of length n over $\mathbb{F}_{q^2}$. Then $\mathcal{D} = \Psi_\beta(C)$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^{2n}$, i.e., a q-ary linear code of length $2n$. By Proposition 3.4, we have $\sigma(\mathcal{D}) = \sigma(\Psi_\beta(C)) = \Psi_\beta(T(C)) = \Psi_\beta(C) = \mathcal{D}$, so $\mathcal{D}$ is cyclic.

Conversely, assume $\mathcal{D}$ is a q-ary linear cyclic code of length $2n$. Since Ψ_β is an $\mathbb{F}_q$-linear isomorphism, $C = \Psi_\beta^{-1}(\mathcal{D})$ is an additive subgroup of $\mathbb{F}_{q^2}^n$. Moreover, $\Psi_\beta(T(C)) = \sigma(\Psi_\beta(C)) = \sigma(\mathcal{D}) = \mathcal{D} = \Psi_\beta(C)$, which implies $T(C) = C$. Hence C is an additive conjucyclic code.

For any codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in C$, it follows from the definition of Ψ_β that $c_i = 0$ if and only if $(\mathrm{Tr}(\beta c_i), \mathrm{Tr}(\bar{\beta} c_i)) = (0, 0)$. Consequently, $w_h(C) = w_s(\mathcal{D})$. □

Remark 3.6. By the theory of cyclic codes [13], the binary cyclic codes derived from additive conjucyclic codes over $\mathbb{F}_4$ in [11] are necessarily repeated-root, since $\gcd(2n, 2) = 2$. It is known that repeated-root cyclic codes are asymptotically inferior to simple-root cyclic codes [14]. In contrast, the construction presented in this work yields q-ary cyclic codes that can be either repeated-root or simple-root, depending on the factorization of $x^{2n} - 1$ over $\mathbb{F}_q$. This flexibility allows us to avoid the asymptotic limitations of repeated-root codes and opens the possibility of constructing quantum codes with better asymptotic parameters.

Let $2n = p^\ell n_0$, where $p = \mathrm{char}(\mathbb{F}_q)$ and $\ell \geq 0$, $n_0 > 0$ are integers such that $\gcd(n_0, p) = 1$. Assume that $x^{n_0} - 1$ factorizes into distinct irreducible polynomials in $\mathbb{F}_q[x]$ as

$$x^{n_0} - 1 = g_1(x)g_2(x)\cdots g_t(x),$$

where each $g_i(x)$ is irreducible and $g_i(x) \neq g_j(x)$ for $i \neq j$. Then

$$x^{2n} - 1 = (x^{n_0} - 1)^{p^\ell} = g_1(x)^{p^\ell} g_2(x)^{p^\ell} \cdots g_t(x)^{p^\ell}. \tag{3.5}$$

The set of divisors of $x^{2n} - 1$ over $\mathbb{F}_q$ is therefore

$$\mathrm{Div}_{\mathbb{F}_q}(x^{2n} - 1) = \left\{ g_1(x)^{s_1} g_2(x)^{s_2} \cdots g_t(x)^{s_t} \mid 0 \leq s_1, s_2, \ldots, s_t \leq p^\ell \right\}.$$

Consequently, $x^{2n} - 1$ has $(p^\ell + 1)^t$ distinct monic divisors in $\mathbb{F}_q[x]$. By the isomorphism Ψ_β defined in (3.4), this immediately yields the number of q^2-ary additive conjucyclic codes of length n.

Theorem 3.7. *Assume that the polynomial $x^{2n} - 1$ is factorized as Eq* (3.5)*, then there exist $(p^\ell + 1)^t$ distinct q^2-ary additive conjucyclic codes of length n.*

Let $g(x) = g_1(x)^{s_1} \cdots g_t(x)^{s_t} \in \mathrm{Div}_{\mathbb{F}_q}(x^{2n} - 1)$ with $\deg(g_i(x)) = d_i$. Then the cyclic code $\langle g(x) \rangle$ has dimension $2n - \sum_{i=1}^t s_i d_i$, so $|\langle g(x) \rangle| = q^{2n - \sum s_i d_i}$, which is also the size of the corresponding additive conjucyclic code.

We now turn to the description of generator matrices for additive conjucyclic codes. To this end, we first recall the notion of a generator matrix for $\mathbb{F}_q$-linear additive codes over $\mathbb{F}_{q^2}$.

Definition 3.8. A generator matrix of an $\mathbb{F}_q$-linear additive code C over $\mathbb{F}_{q^2}$ is a matrix whose rows form an $\mathbb{F}_q$-basis of C.

For a polynomial $f(x) = f_0 + f_1 x + \cdots + f_{2n-1} x^{2n-1} \in \mathbb{F}_q[x]/\langle x^{2n} - 1 \rangle$, we denote by $\boldsymbol{f} = (f_0, f_1, \ldots, f_{2n-1}) \in \mathbb{F}_q^{2n}$ its coefficient vector. This notation will be used to relate cyclic codes and their associated additive conjucyclic codes via the isomorphism Ψ_β introduced in (3.4).

Theorem 3.9. *Let C be an additive conjucyclic code over $\mathbb{F}_{q^2}$ of length n and let $\mathcal{D} = \Psi_\beta(C) = \langle g(x) \rangle$ be the corresponding q-ary linear cyclic code of length $2n$, where $g(x) \in \mathrm{Div}_{\mathbb{F}_q}(x^{2n} - 1)$ and $\deg(g(x)) = k$. Denote by $\boldsymbol{g} = (g_0, g_1, \ldots, g_{2n-1})$ the coefficient vector of $g(x)$. Then a generator matrix of C is given by*

$$\hat{G} = \begin{pmatrix} \Psi_\beta^{-1}(\boldsymbol{g}) \\ T(\Psi_\beta^{-1}(\boldsymbol{g})) \\ \vdots \\ T^{2n-k-1}(\Psi_\beta^{-1}(\boldsymbol{g})) \end{pmatrix},$$

where T is the right conjucyclic shift operator defined in (2.2)*.*

Proof. We first show that every codeword $\mathbf{c} \in C$ lies in the row space of $\hat{G}$. Since $\mathcal{D} = \langle g(x) \rangle$ is a cyclic code, its generator matrix is given by

$$G_{\mathcal{D}} = \begin{pmatrix} \boldsymbol{g} \\ \sigma(\boldsymbol{g}) \\ \vdots \\ \sigma^{2n-k-1}(\boldsymbol{g}) \end{pmatrix},$$

where $\boldsymbol{g} = (g_0, g_1, \ldots, g_{2n-1})$ is the coefficient vector of $g(x)$. So there exist scalars $k_0, k_1, \ldots, k_{2n-k-1} \in \mathbb{F}_q$ such that

$$\Psi_\beta(\mathbf{c}) = \sum_{i=0}^{2n-k-1} k_i \sigma^i(\boldsymbol{g}).$$

Applying the inverse isomorphism Ψ_β^{-1} and using Proposition 3.4 which gives $\Psi_\beta^{-1}(\sigma^i(\boldsymbol{g})) = T^i(\Psi_\beta^{-1}(\boldsymbol{g}))$, we obtain

$$\mathbf{c} = \sum_{i=0}^{2n-k-1} k_i T^i(\Psi_\beta^{-1}(\boldsymbol{g})).$$

Thus each codeword is a linear combination of the rows of $\hat{G}$. Moreover, since $|C| = |\mathcal{D}| = q^{2n-k}$ and the rows of $\hat{G}$ are linearly independent over $\mathbb{F}_q$ (as they are images of the basis of $\mathcal{D}$), they form an $\mathbb{F}_q$-basis of C. Consequently, $\hat{G}$ is a generator matrix of C. □

Example 3.10. Let $q = 4$ and $n = 11$. Over $\mathbb{F}_4$, the complete factorization of $x^{22} - 1$ is

$$(1 + x)^2(1 + \omega^2 x + x^2 + x^3 + \omega x^4 + x^5)^2(1 + \omega x + x^2 + x^3 + \omega^2 x^4 + x^5)^2,$$

where ω is a primitive element of $\mathbb{F}_4$. Hence every divisor of $x^{22} - 1$ is of the form $(1 + x)^{i_1}(1 + \omega^2 x + x^2 + x^3 + \omega x^4 + x^5)^{i_2}(1 + \omega x + x^2 + x^3 + \omega^2 x^4 + x^5)^{i_3}$ with $0 \le i_1, i_2, i_3 \le 2$. By Theorem 3.7, there are $3^3 = 27$ distinct additive conjucyclic codes over $\mathbb{F}_{16}$ of length 11.

Consider the code C determined by the divisor

$$g(x) = (1 + \omega^2 x + x^2 + x^3 + \omega x^4 + x^5)^2 = 1 + \omega x^2 + x^4 + x^6 + \omega^2 x^8 + x^{10}.$$

Let $\boldsymbol{g} = (g_0, \ldots, g_{21})$ be the coefficient vector of $g(x)$; explicitly,

$$\boldsymbol{g} = (1, 0, \omega, 0, 1, 0, 1, 0, \omega^2, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \in \mathbb{F}_4^{22}.$$

Choose a primitive element β of $\mathbb{F}_{16}$ and set $\mathbf{w} = \Psi_\beta^{-1}(\boldsymbol{g})$. Then

$$\mathbf{w} = (\beta, 0, \beta^6, 0, \beta, 0, \beta, 0, \beta^{11}, 0, \beta) \in \mathbb{F}_{16}^{11}.$$

According to Theorem 3.9, a generator matrix of C is

$$\hat{G} = \begin{pmatrix} \mathbf{w} \\ T(\mathbf{w}) \\ \vdots \\ T^{2n-k-1}(\mathbf{w}) \end{pmatrix},$$

where $k = \deg(g(x)) = 10$ and thus $2n - k = 12$. Using Magma [15], we find that C is an $(11, 4^{12}, 5)_{16}$ additive code; its weight distribution is

$$1 + 825z^5 + 1980z^6 + 61875z^7 + 391875z^8 + 2025375z^9 + 6045600z^{10} + 8249685z^{11}.$$

The Singleton bound for additive codes over $\mathbb{F}_{q^2}$ (see, e.g., [13]) gives

$$(d \le n - \log_{q^2}(M) + 1 = 11 - 6 + 1 = 6).$$

Since the code attains $d = 5$, it is a near maximum distance separable (MDS) additive code [16, 17], i.e., it misses the Singleton bound by only one.

4. Alternating duality and quantum code construction

For a q^2-ary additive code C, both $C^{\perp_e}$ and $C^{\perp_s}$ are $\mathbb{F}_{q^2}$-linear because the Euclidean and symplectic inner products satisfy $\langle \mathbf{u}, a\mathbf{v}\rangle = a\langle \mathbf{u}, \mathbf{v}\rangle$ for any $a \in \mathbb{F}_{q^2}$. Thus, if $\mathbf{v}$ is orthogonal to C, so is any scalar multiple $a\mathbf{v}$. This makes these conventional inner products ill-suited for studying the dual structure of additive codes.

To remedy this, we introduce an alternating inner product on $\mathbb{F}_{q^2}^n$ that is more suitable for additive codes. We then show that the mapping Ψ_β defined in (3.4) preserves orthogonality between the symplectic inner product on $\mathbb{F}_q^{2n}$ and the alternating inner product on $\mathbb{F}_{q^2}^n$.

Proposition 4.1. *Let β be a primitive element of $\mathbb{F}_{q^2}$. For $\boldsymbol{u} = (u_0, \ldots, u_{n-1})$ and $\boldsymbol{v} = (v_0, \ldots, v_{n-1})$ in $\mathbb{F}_{q^2}^n$, we define*

$$\langle \boldsymbol{u}, \boldsymbol{v}\rangle_{a,\beta} = (\bar{\beta}^2 - \beta^2) \sum_{i=0}^{n-1} (u_i \bar{v}_i - \bar{u}_i v_i). \tag{4.1}$$

Then $\langle \cdot, \cdot \rangle_{a,\beta}$ is a nondegenerate alternating inner product on $\mathbb{F}_{q^2}^n$. In other words, it satisfies the following properties:

(1) $\langle \boldsymbol{u}, \boldsymbol{v}\rangle_{a,\beta} \in \mathbb{F}_q$ for all $\boldsymbol{u}, \boldsymbol{v}$;
(2) $\langle \boldsymbol{u}, \boldsymbol{v}\rangle_{a,\beta}$ is $\mathbb{F}_q$-bilinear;
(3) $\langle \boldsymbol{u}, \boldsymbol{v}\rangle_{a,\beta} = -\langle \boldsymbol{v}, \boldsymbol{u}\rangle_{a,\beta}$ (alternating);
(4) $\langle \boldsymbol{u}, \boldsymbol{u}\rangle_{a,\beta} = 0$ for all $\boldsymbol{u}$;
(5) If $\langle \boldsymbol{u}, \boldsymbol{v}\rangle_{a,\beta} = 0$ for all $\boldsymbol{v} \in \mathbb{F}_{q^2}^n$, then $\boldsymbol{u} = \mathbf{0}$ (nondegeneracy).

Proof. (1) Set $\gamma = \bar{\beta}^2 - \beta^2$. Observe that $\gamma \neq 0$ because $\beta \notin \mathbb{F}_q$. For any $\mathbf{u}, \mathbf{v} \in \mathbb{F}_{q^2}^n$, define $\langle \mathbf{u}, \mathbf{v}\rangle_{a\beta} = \gamma \sum_{i=0}^{n-1} (u_i \bar{v}_i - \bar{u}_i v_i)$. We first show that $\langle \mathbf{u}, \mathbf{v}\rangle_{a\beta} \in \mathbb{F}_q$. Let $S = \sum_{i=0}^{n-1} (u_i \bar{v}_i - \bar{u}_i v_i)$. A direct computation gives $S^q = \sum_i (\bar{u}_i v_i - u_i \bar{v}_i) = -S$. Moreover, $\gamma^q = (\bar{\beta}^2 - \beta^2)^q = \beta^{2q^2} - \beta^{2q} = \beta^2 - \bar{\beta}^2 = -\gamma$. Therefore,

$$(\gamma S)^q = \gamma^q S^q = (-\gamma)(-S) = \gamma S,$$

which implies $\gamma S \in \mathbb{F}_q$. Hence $\langle \mathbf{u}, \mathbf{v}\rangle_{a\beta}$ takes values in $\mathbb{F}_q$.

(2) The map $\boldsymbol{v} \mapsto \langle \boldsymbol{u}, \boldsymbol{v}\rangle_{a,\beta}$ is a linear combination of the coordinates of $\boldsymbol{v}$ with coefficients in $\mathbb{F}_q$, hence $\mathbb{F}_q$-linear. By symmetry (up to sign), the same holds for the first argument, so the form is $\mathbb{F}_q$-bilinear.

(3) Direct computation gives

$$\langle \boldsymbol{v}, \boldsymbol{u}\rangle_{a,\beta} = \gamma \sum_i (v_i \bar{u}_i - \bar{v}_i u_i) = -\gamma \sum_i (u_i \bar{v}_i - \bar{u}_i v_i) = -\langle \boldsymbol{u}, \boldsymbol{v}\rangle_{a,\beta}.$$

(4) Taking $\boldsymbol{v} = \boldsymbol{u}$ in the previous property yields $\langle \boldsymbol{u}, \boldsymbol{u}\rangle_{a,\beta} = 0$.

(5) Assume $\langle \boldsymbol{u}, \boldsymbol{v}\rangle_{a,\beta} = 0$ for all $\boldsymbol{v} \in \mathbb{F}_{q^2}^n$. For a fixed coordinate j, choose $\boldsymbol{v}$ with $v_j = 1$ and all other entries 0. Then

$$\gamma(u_j \bar{1} - \bar{u}_j \cdot 1) = \gamma(u_j - \bar{u}_j) = 0,$$

so $u_j = \bar{u}_j$, i.e., $u_j \in \mathbb{F}_q$. Next, choose $\boldsymbol{v}$ with $v_j = \beta$ and 0 elsewhere. We obtain

$$\gamma(u_j \bar{\beta} - \bar{u}_j \beta) = \gamma(u_j \beta^q - u_j \beta) = \gamma u_j (\beta^q - \beta) = 0.$$

Since $\gamma \neq 0$ and $\beta^q - \beta \neq 0$ (as $\beta \notin \mathbb{F}_q$), it follows that $u_j = 0$. This holds for every j, hence $\boldsymbol{u} = \mathbf{0}$. □

Remark 4.2. In the special case $q = 2$, we have $\beta^3 = 1$ and the alternating inner product $\langle \cdot, \cdot \rangle_{a,\beta}$ defined in (4.1) reduces to

$$\langle \boldsymbol{u}, \boldsymbol{v} \rangle_{a,\beta} = \sum_{i=1}^{n} (u_i \bar{v}_i + \bar{u}_i v_i) = \mathrm{Tr}\left(\sum_{i=1}^{n} u_i \bar{v}_i \right).$$

Hence, the alternating inner product can be viewed as a generalization of the classical trace-Hermitian inner product introduced in [2].

Proposition 4.3. *For any* $\mathbf{u}, \mathbf{v} \in \mathbb{F}_{q^2}^n$, *we have*

$$\langle \Psi_\beta(\mathbf{u}), \Psi_\beta(\mathbf{v}) \rangle_s = \langle \mathbf{u}, \mathbf{v} \rangle_{a,\beta},$$

where $\langle \cdot, \cdot \rangle_s$ *and* $\langle \cdot, \cdot \rangle_{a,\beta}$ *are the symplectic inner product on* $\mathbb{F}_q^{2n}$ *(see* (2.3)*) and the alternating inner product on* $\mathbb{F}_{q^2}^n$ *(see* (4.1)*), respectively.*

Proof. Write $\mathbf{u} = (u_0, \ldots, u_{n-1})$ and $\mathbf{v} = (v_0, \ldots, v_{n-1})$. Then

$$\Psi_\beta(\mathbf{u}) = (\mathrm{Tr}(\beta u_0), \ldots, \mathrm{Tr}(\beta u_{n-1}), \mathrm{Tr}(\bar{\beta} u_0), \ldots, \mathrm{Tr}(\bar{\beta} u_{n-1})),$$

and similarly for $\Psi_\beta(\mathbf{v})$. Using the definition of the symplectic inner product,

$$\begin{aligned}
\langle \Psi_\beta(\mathbf{u}), \Psi_\beta(\mathbf{v}) \rangle_s &= \sum_{i=0}^{n-1} \Big(\mathrm{Tr}(\bar{\beta} u_i) \mathrm{Tr}(\beta v_i) - \mathrm{Tr}(\beta u_i) \mathrm{Tr}(\bar{\beta} v_i) \Big) \\
&= \sum_{i=0}^{n-1} \Big((\bar{\beta} u_i + \beta \bar{u}_i)(\beta v_i + \bar{\beta} \bar{v}_i) - (\beta u_i + \bar{\beta} \bar{u}_i)(\bar{\beta} v_i + \beta \bar{v}_i) \Big) \\
&= \sum_{i=0}^{n-1} (\bar{\beta}^2 u_i \bar{v}_i + \beta^2 \bar{u}_i v_i - \beta^2 u_i \bar{v}_i - \bar{\beta}^2 \bar{u}_i v_i) \\
&= (\bar{\beta}^2 - \beta^2) \sum_{i=0}^{n-1} (u_i \bar{v}_i - \bar{u}_i v_i) = \langle \mathbf{u}, \mathbf{v} \rangle_{a,\beta},
\end{aligned}$$

which completes the proof. □

Definition 4.4. The alternating dual code of C is defined as

$$C^{\perp_a} = \{ \boldsymbol{v} \in \mathbb{F}_{q^2}^n \mid \langle \boldsymbol{u}, \boldsymbol{v} \rangle_{a,\beta} = 0 \text{ for all } \boldsymbol{u} \in C \}.$$

Theorem 4.5. *Let* C *be an additive conjucyclic code over* $\mathbb{F}_{q^2}$ *of length* n *and* $\mathcal{D} = \Psi_\beta(C)$ *be a* q*-ary linear cyclic code of length* $2n$*. Then we have*

$$C^{\perp_a} = \Psi_\beta^{-1}(\mathcal{D}^{\perp_s}).$$

Proof. For any $\mathbf{c} \in C$ and $\mathbf{d} \in C^{\perp_a}$, by Proposition 4.3, we have $\langle \mathbf{c}, \mathbf{d} \rangle_a = \langle \Psi_\beta(\mathbf{c}), \Psi_\beta(\mathbf{d}) \rangle_s = 0$. Therefore, $\Psi_\beta(\mathbf{d}) \in \mathcal{D}^{\perp_s}$, i.e., $\Psi_\beta(C^{\perp_a}) \subseteq \mathcal{D}^{\perp_s}$ and $C^{\perp_a} \subseteq \Psi_\beta^{-1}(\mathcal{D}^{\perp_s})$. Similarly, we can also prove $\Psi_\beta^{-1}(\mathcal{D}^{\perp_s}) \subseteq C^{\perp_a}$. This concludes the result. □

Let $g(x) \in \mathrm{Div}_{\mathbb{F}_q}(x^{2n}-1)$ with $\deg(g(x)) = k$, and set $h(x) = \frac{x^{2n}-1}{g(x)}$. Define the reciprocal polynomial

$$h^*(x) = \frac{1}{h_{2n-k}} x^{2n-k} h\left(\frac{1}{x}\right).$$

Denote by $\boldsymbol{h^*} = (h_0^*, h_1^*, \ldots, h_{2n-1}^*) \in \mathbb{F}_q^{2n}$ the coefficient vector of $h^*(x)$.

Lemma 4.6. *Let $\mathcal{D} = \langle g(x) \rangle$ be a q-ary linear cyclic code of length $2n$. Then a generator matrix of the symplectic dual code $\mathcal{D}^{\perp_s}$ is given by*

$$H_s = \begin{pmatrix} \tau(\boldsymbol{h^*}) \\ \tau(\sigma(\boldsymbol{h^*})) \\ \vdots \\ \tau(\sigma^{k-1}(\boldsymbol{h^*})) \end{pmatrix},$$

where σ is the cyclic shift operator defined in (2.1) *and τ is the linear transformation defined by*

$$\tau(\mathbf{v}) = (v_0, v_1, \ldots, v_{2n-1}) \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} = (-v_n, \ldots, -v_{2n-1}, v_0, \ldots, v_{n-1})$$

for any $\mathbf{v} = (v_0, v_1, \ldots, v_{2n-1}) \in \mathbb{F}_q^{2n}$, with I_n the $n \times n$ identity matrix.

Proof. By the theory of cyclic codes [13], the Euclidean dual code $\mathcal{D}^{\perp_e}$ is generated by the matrix

$$H_e = \begin{pmatrix} \boldsymbol{h^*} \\ \sigma(\boldsymbol{h^*}) \\ \vdots \\ \sigma^{k-1}(\boldsymbol{h^*}) \end{pmatrix}.$$

For any codeword $\mathbf{d} \in \mathcal{D}$ and any $i \in \{0, \ldots, k-1\}$, we have

$$\langle \mathbf{d}, \tau(\sigma^i(\boldsymbol{h^*})) \rangle_s = \langle \mathbf{d}, \sigma^i(\boldsymbol{h^*}) \rangle_e = 0.$$

Hence, the rows of H_s belong to $\mathcal{D}^{\perp_s}$. Moreover, since $H_s = H_e \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$, we have that $\mathrm{rank}(H_s) = \mathrm{rank}(H_e) = k$. Therefore, H_s is a generator matrix of $\mathcal{D}^{\perp_s}$. □

Theorem 4.7. *Let C be a q^2-ary additive conjucyclic code of length n corresponding to the q-ary linear cyclic code $\mathcal{D} = \langle g(x) \rangle$, where $g(x) \in \mathrm{Div}_{\mathbb{F}_q}(x^{2n}-1)$ and $\deg(g(x)) = k$. Then a generator matrix of the alternating dual code $C^{\perp_{a,\beta}}$ is given by*

$$\hat{H}_a = \begin{pmatrix} \Psi_\beta^{-1}(\tau(\boldsymbol{h^*})) \\ \Psi_\beta^{-1}(\tau(\sigma(\boldsymbol{h^*}))) \\ \vdots \\ \Psi_\beta^{-1}(\tau(\sigma^{k-1}(\boldsymbol{h^*}))) \end{pmatrix}, \tag{4.2}$$

where $\boldsymbol{h^*} \in \mathbb{F}_q^{2n}$ is the coefficient vector of $h^*(x)$, σ is the cyclic shift operator, and T is the right conjucyclic shift operator defined in (2.2).

Proof. By Theorem 4.5, we have $C^{\perp_{a,\beta}} = \Psi_\beta^{-1}(\mathcal{D}^{\perp_s})$. Lemma 4.6 provides a generator matrix H_s of $\mathcal{D}^{\perp_s}$ whose rows are $\tau(\sigma^i(\boldsymbol{h}^*))$ for $i = 0, \ldots, k-1$. Since Ψ_β^{-1} is an $\mathbb{F}_q$-linear isomorphism, applying it to each row of H_s yields a generator matrix of $\Psi_\beta^{-1}(\mathcal{D}^{\perp_s}) = C^{\perp_{a,\beta}}$, namely the matrix $\hat{H}_a$ as defined above. Hence $\hat{H}_a$ is a generator matrix of $C^{\perp_{a,\beta}}$. □

Remark 4.8. The generator matrix $\hat{H}_a$ of $C^{\perp_{a,\beta}}$ can also be regarded as a parity-check matrix for C. Indeed, C is completely characterized by $\hat{H}_a$ via the condition

$$C = \left\{ \mathbf{c} \in \mathbb{F}_{q^2}^n \mid \hat{H}_a \cdot \mathbf{c}^\top = \mathbf{0} \right\},$$

where the product is taken with respect to the alternating inner product, i.e., each row of $\hat{H}_a$ is orthogonal to every codeword under $\langle \cdot, \cdot \rangle_{a,\beta}$.

Corollary 4.9. *If* $\mathrm{char}(\mathbb{F}_{q^2}) = 2$*, then the generator matrix* $\hat{H}_a$ *of* $C^{\perp_{a,\beta}}$ *in* (4.2) *can be simplified as*

$$\hat{H}_a = \begin{pmatrix} \Psi_\beta^{-1}(\tau(\boldsymbol{h}^*)) \\ T(\Psi_\beta^{-1}(\tau(\boldsymbol{h}^*))) \\ \vdots \\ T^{k-1}(\Psi_\beta^{-1}(\tau(\boldsymbol{h}^*))) \end{pmatrix}.$$

Proof. By Theorem 4.7, the rows of $\hat{H}_a$ are $\Psi_\beta^{-1}(\tau(\sigma^i(\boldsymbol{h}^*)))$ for $i = 0, \ldots, k-1$. When $\mathrm{char}(\mathbb{F}_{q^2}) = 2$, a direct computation shows that τ commutes with the cyclic shift σ; i.e., $\tau(\sigma(\mathbf{v})) = \sigma(\tau(\mathbf{v}))$ for any $\mathbf{v} \in \mathbb{F}_q^{2n}$. Hence $\tau(\sigma^i(\boldsymbol{h}^*)) = \sigma^i(\tau(\boldsymbol{h}^*))$ for all i. Applying Proposition 3.4, we have $\Psi_\beta^{-1}(\sigma^i(\tau(\boldsymbol{h}^*))) = T^i(\Psi_\beta^{-1}(\tau(\boldsymbol{h}^*)))$. Therefore

$$\Psi_\beta^{-1}(\tau(\sigma^i(\boldsymbol{h}^*))) = T^i(\Psi_\beta^{-1}(\tau(\boldsymbol{h}^*))),$$

and the claimed simplified form follows. □

Corollary 4.10. *Let* C *be a* q^2*-ary additive conjucyclic code. If* $\mathrm{char}(\mathbb{F}_{q^2}) = 2$*, then the alternating dual code* $C^{\perp_{a,\beta}}$ *is also additive conjucyclic.*

Proof. When $\mathrm{char}(\mathbb{F}_{q^2}) = 2$, Corollary 4.9 shows that the alternating dual code $C^{\perp_{a,\beta}}$ admits a generating set consisting of the vectors $T^i(\mathbf{w})$ for $i = 0, \ldots, k-1$, where $\mathbf{w} = \Psi_\beta^{-1}(\tau(\boldsymbol{h}^*))$. Since T is the right conjucyclic shift operator, the $\mathbb{F}_q$-linear span of these vectors is closed under T. Consequently, $C^{\perp_{a,\beta}}$ is an additive conjucyclic code. □

Remark 4.11. In [11], it was shown that for a quaternary additive conjucyclic code C, its trace dual code

$$C^{\mathrm{Tr}} = \{ \mathbf{v} \in \mathbb{F}_4^n \mid \mathrm{Tr}(\langle \mathbf{u}, \mathbf{v} \rangle_e) = 0 \text{ for all } \mathbf{u} \in C \}$$

is also additive conjucyclic. This result can now be seen as a special case of Corollary 4.10. Indeed, when $q = 2$, the alternating inner product reduces to the trace-Hermitian form, and one verifies that $C^{\mathrm{Tr}} = (C^{\perp_{a,\beta}})^2$, where $(\cdot)^2$ denotes componentwise squaring. Since Corollary 4.10 guarantees that $C^{\perp_{a,\beta}}$ is additive conjucyclic, the same property follows immediately for C^{Tr}. Thus the present work not only generalizes the known result to arbitrary q but also places it within a unified algebraic framework.

The connection between classical codes and QECCs is well established via the stabilizer formalism, where the symplectic inner product serves as the key link [18, 19].

Lemma 4.12. *[18] If C is a symplectic dual-containing linear code with parameters $[2n, k]_q$, then there exists an $[[n, k-n, \geq w_s(C)]]_q$ QECC that is pure to $w_s(C)$.*

As a direct consequence of the established correspondence and the properties of the alternating inner product, we obtain the following quantum code construction.

Theorem 4.13. *Let C be an $(n, M = q^k, w_h(C))_{q^2}$ additive conjucyclic code satisfying $C^{\perp_{a\beta}} \subseteq C$. Then there exists a pure $[[n, k-n, \geq w_h(C)]]_q$ QECC.*

Proof. By Theorem 3.5, the code C corresponds to a q-ary linear cyclic code $\mathcal{D} = \Psi_\beta(C)$ of length $2n$ with $|\mathcal{D}| = q^k$. Moreover, Theorem 3.5 also gives $w_h(C) = w_s(\mathcal{D})$. Since $C^{\perp_{a\beta}} \subseteq C$, Proposition 4.3 implies $\mathcal{D}^{\perp_s} \subseteq \mathcal{D}$. Thus $\mathcal{D}$ is a symplectic dual-containing linear code with parameters $[2n, k]_q$. Applying Lemma 4.12 yields a pure $[[n, k-n, \geq w_s(\mathcal{D})]]_q = [[n, k-n, \geq w_h(C)]]_q$ QECC, as desired. □

Example 4.14. We continue with the same parameters as in Example 3.10: Let $q = 4$, $n = 11$, and let C be the additive conjucyclic code over $\mathbb{F}_{16}$ determined by the divisor

$$g(x) = (1 + \omega^2 x + x^2 + x^3 + \omega x^4 + x^5)^2 = 1 + \omega x^2 + x^4 + x^6 + \omega^2 x^8 + x^{10},$$

where ω is a primitive element of $\mathbb{F}_4$. With the same primitive element β of $\mathbb{F}_{16}$ as before, we now examine the dual side.

Set

$$(h(x) = \frac{x^{22} - 1}{g(x)} = 1 + \omega x^2 + \omega x^4 + \omega^2 x^8 + \omega^2 x^{10} + x^{12}),$$

then

$$h^*(x) = 1 + \omega^2 x^2 + \omega^2 x^4 + \omega x^8 + \omega x^{10} + x^{12},$$

and its coefficient vector is

$$\boldsymbol{h^*} = (1, 0, \omega^2, 0, \omega^2, 0, 0, 0, \omega, 0, \omega, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \in \mathbb{F}_4^{22}.$$

Applying the linear transformation τ from Lemma 4.6 yields

$$\tau(\boldsymbol{h^*}) = (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, \omega^2, 0, \omega^2, 0, 0, 0, \omega, 0, \omega, 0) \in \mathbb{F}_4^{22}.$$

Set $\mathbf{u} = \Psi_\beta^{-1}(\tau(\boldsymbol{h^*}))$; explicitly,

$$\mathbf{u} = (\beta^4, \beta, \beta^{14}, 0, \beta^{14}, 0, 0, 0, \beta^9, 0, \beta^9) \in \mathbb{F}_{16}^{11}.$$

Since $\mathrm{char}(\mathbb{F}_{16}) = 2$, by Corollary 4.10, a generator matrix of the alternating dual code $C^{\perp_{a\beta}}$ is

$$\hat{H}_a = \begin{pmatrix} \mathbf{u} \\ T(\mathbf{u}) \\ \vdots \\ T^9(\mathbf{u}) \end{pmatrix}.$$

One verifies directly that $C^{\perp_{a\beta}} \subseteq C$; thus C is alternating dual-containing. Applying Theorem 4.13 we obtain a pure $[[11, 1, 5]]_4$ QECC. Its weight enumerator is

$$825z^5 + 1155z^6 + 61050z^7 + 361350z^8 + 91904925z^9 + 5664615z^{10} + 7734720z^{11}.$$

This code not only exceeds the quantum Gilbert–Varshamov bound [20] and improves upon the previously known $[[19, 1, 5]]_4$ code listed in [21], but is in fact optimal according to Grassl's code tables [22]. Moreover, unlike the optimal stabilizer codes recorded in the tables—whose stabilizer matrices typically lack algebraic structure and thus require large storage—our construction yields a generator matrix with a cyclic structure, which significantly reduces the memory requirement.

5. Conclusions

In this paper, we have developed the algebraic theory of additive conjucyclic codes over $\mathbb{F}_{q^2}$. We first established a one-to-one correspondence between q^2-ary additive conjucyclic codes and q-ary linear cyclic codes via the trace map, which allows us to determine the enumeration of such codes and provide explicit forms of their generator matrices. We then introduced an alternating inner product on $\mathbb{F}_{q^2}^n$ and, under this inner product, derived a necessary and sufficient condition for these codes to be dual-containing, from which we obtained explicit parity-check matrices and a construction method for q-ary QECCs. This work provides a systematic treatment of additive conjucyclic codes over general $\mathbb{F}_{q^2}$ and their application to non-binary quantum error correction. We hope that the framework established herein will inspire further research on constructing QECCs with good parameters from additive conjucyclic codes.

Author contributions

Jingjie Lv: Writing – original draft, formal analysis, validation; Xian Lian: Conceptualization, methodology, investigation; Ruihu Li: Conceptualization, funding acquisition; Hanxu Hou: Data curation, formal analysis, funding acquisition, supervision. All authors have read and approved the final version of the manuscript.

Use of Generative-AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

This research is supported in part by National Key Research and Development Program of China under Grant No. 2025YFA1017200, the National Natural Science Foundation of China under Grant No. 62401144, the Natural Science Foundation of Guangdong Province under Grant No. 2026A1515012796.

Conflict of interest

The authors declare no conflict of interest.

References

1. P. Delsarte, An algebraic approach to the association schemes of coding theory, *Philips Res. Repts. Suppl.*, **10** (1973).
2. A. R. Calderbank, E. M. Rains, P. W. Shor, N. J. A. Sloane, Quantum error correction via GF(4), *IEEE Trans. Inf. Theory*, **44** (1998), 1369–1387. http://dx.doi.org/10.1109/18.681315
3. K. Abdukhalikov, D. Ho, On the equivalence between additive and linear codes, *arXiv:2603.15071*, 2026. https://doi.org/10.48550/arXiv.2603.15071
4. S. Bhowmick, K. Deka, A. F. Tabue, E. Martínez-Moro, Trace duality and additive complementary pairs of additive cyclic codes over finite chain rings, *Finite Fields Appl.*, **110** (2026), 102732. http://dx.doi.org/10.1016/j.ffa.2025.102732
5. M. Shi, N. Liu, J. L. Kim, P. Solé, Additive complementary dual codes over $\mathbb{F}_4$, *Des. Codes Cryptogr.*, **91** (2023), 273–284. https://doi.org/10.1007/s10623-022-01106-3
6. W. C. Huffman, Additive cyclic codes over $\mathbb{F}_4$, *Adv. Math. Commun.*, **1** (2007), 427–459. http://dx.doi.org/10.3934/amc.2007.1.427
7. J. Bierbrauer, Cyclic additive codes, *J. Algebra*, **372** (2012), 661–672. http://dx.doi.org/10.1016/j.jalgebra.2012.08.031
8. C. Güneri, F. Özbudak, F. Özdemir, On complementary dual additive cyclic codes, *Adv. Math. Commun.*, **11** (2017), 353–357. https://doi.org/10.3934/amc.2017028
9. M. Shi, R. Wu, P. Sole, Asymptotically good additive cyclic codes exist, *IEEE Commun. Lett.*, **22** (2018), 1980–1983. https://doi.org/10.1109/LCOMM.2018.2863370
10. R. Dastbasteh, K. Shivji, Polynomial representation of additive cyclic codes and new quantum codes, *Adv. Math. Commun.*, **19** (2025), 49–68. https://doi.org/10.3934/amc.2023036
11. T. Abualrub, Y. Cao, S. T. Dougherty, Algebraic structure of additive conjucyclic codes over $\mathbb{F}_4$, *Finite Fields Appl.*, **65** (2020), 101678. http://dx.doi.org/10.1016/j.ffa.2020.101678
12. T. Abualrub, S. T. Dougherty, Additive and linear conjucyclic codes over $\mathbb{F}_4$, *Adv. Math. Commun.*, **16** (2022), 1–15. https://doi.org/10.3934/amc.2020096
13. W. C. Huffman, V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, 2003. https://doi.org/10.1017/CBO9780511807077
14. G. Castagnoli, J. L. Massey, P. A. Schoeller, N. von Seeman, On repeated-root cyclic codes, *IEEE Trans. Inf. Theory*, **37** (1991), 337–342. https://doi.org/10.1109/18.75249
15. W. Bosma, J. Cannon, C. Playoust, The MAGMA algebra system I: The user language, *J. Symb. Comput.*, **24** (1997), 235–265. https://doi.org/10.1006/jsco.1996.0125
16. Z. Heng, C. Li, X. Wang, Constructions of MDS, near MDS and almost MDS codes from cyclic subgroups of $\mathbb{F}_{q^2}^*$, *IEEE Trans. Inf. Theory*, **68** (2022), 7817–7831. http://dx.doi.org/10.1109/TIT.2022.3194914
17. C. Ding, C. Tang, Infinite families of near MDS codes holding t-designs, *IEEE Trans. Inf. Theory*, **66** (2020), 5419–5428. http://dx.doi.org/10.1109/TIT.2020.2990396

18. A. Ashikhmin, E. Knill, Nonbinary quantum stabilizer codes, *IEEE Trans. Inf. Theory*, **47** (2001), 3065–3072. https://doi.org/10.1109/18.959288

19. A. Ketkar, A. Klappenecker, S. Kumar, P. K. Sarvepalli, Nonbinary stabilizer codes over finite fields, *IEEE Trans. Inf. Theory*, **52** (2006), 4892–4914. https://doi.org/10.1109/TIT.2006.883612

20. K. Feng, Z. Ma, A finite Gilbert–Varshamov bound for pure stabilizer quantum codes, *IEEE Trans. Inf. Theory*, **50** (2004), 3323–3325. https://doi.org/10.1109/TIT.2004.838088

21. Y. Edel, *Table of quantum twisted codes*, 2026. Available from: `https://www.yvesedel.de/Matritzen/QTBCH/QTBCHIndex.html`.

22. M. Grassl, *Code tables: Bounds on the parameters of various types of codes*, 2026. Available from: `http://www.codetables.de`.

AIMS Press