J. Algebra Comb. Discrete Appl.
12(3) • 249–258

Received: 23 October 2024
Accepted: 20 February 2025

Journal of Algebra Combinatorics Discrete Structures and Applications

On additive cyclic codes over $\mathbb{F}_4 + u\mathbb{F}_4$

Research Article

Gyanendra K. Verma*, R. K. Sharma

Abstract: This article studies additive cyclic codes over $R = \mathbb{F}_4 + u\mathbb{F}_4$, where $u^2 = 0$. We obtain generator polynomials for these codes and provide necessary and sufficient conditions for additive codes to be self-orthogonal and self-dual codes over R with respect to the symplectic inner product. Additive self-orthogonal codes over $\mathbb{F}_4$ with respect to the symplectic inner product are used to construct quantum codes. We demonstrate that the Gray image of additive self-orthogonal codes over R results in additive self-orthogonal codes over $\mathbb{F}_4$. Additionally, we prove that binary self-orthogonal codes can be obtained from additive self-orthogonal codes over R with respect to the symplectic inner product.

2020 MSC: Primary 94B05; Secondary 94B99

Keywords: Additive code, Cyclic codes, Quasi cyclic code, Symplectic dual, Gray map

1. Introduction

Linear codes that are invariant under cyclic shifts are known as linear cyclic codes. Cyclic codes are an important class of error-correcting codes due to their rich algebraic properties, which allow us easy implementation. Cyclic codes admit efficient encoding and decoding algorithms, making them particularly useful in various applications. A lot of research has been devoted to linear LCD codes, cyclic codes, quasi-cyclic codes, and constacyclic codes over range alphabets, including finite fields, rings, and mixed alphabets (for details see [3, 8, 10, 11, 13, 20] and reference therein).

In 1998, Delsarte [6] was the first to define additive codes, and constructed several schemes using these codes. Additive codes are generalizations of linear codes in which linearity replaces additivity. Every linear code is an additive code, but the converse is not true. Additive codes have applications in combinatorial mathematics, cryptography, and information theory, especially in the construction of good quantum codes. Calderbank et al. [5] described the structure of additive cyclic codes over $\mathbb{F}_4$ and

* *This author is supported by IRD-IIT Delhi.*
Gyanendra K. Verma; Department of Mathematics, Indian Institute of Technology Delhi, New Delhi 110016, India (email: gkvermaiitdmaths@gmail.com).
R. K. Sharma; Faculty of Mathematics and Computer Science, South Asian University, New Delhi 110068, India (email: rksharmaiitd@gmail.com).

established necessary and sufficient conditions for these codes to be self-orthogonal with respect to the defined symplectic inner product. They presented many new quantum codes derived from additive cyclic codes over $\mathbb{F}_4$. It has been shown that additive codes possess better parameters than linear codes over finite fields. Shi [17] et al. proved that asymptotically good additive cyclic codes exist using the result that quasi-twisted codes of fixed index are asymptotically good. Asymptotic properties of $\mathbb{Z}_p\mathbb{Z}_{p^s}$-additive cyclic codes and $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes were studied in [21, 22]. In 2014, Abualrub et al. [2] studied the structural properties of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes. They showed that dual of $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes are cyclic and provide an infinite family of MDS codes with respect to Singleton bound. Bhaintwal and Srinivasulu [19] studied additive cyclic codes over the mixed alphabet $\mathbb{Z}_2(\mathbb{Z}_2 + u\mathbb{Z}_2)$ and obtained minimal spanning set for these codes.

In recent years, several researchers generalized $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes. In 2017, Aydogdu et al. [4] defined $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive cyclic codes and obtained binary codes with good parameters from these codes. Diao [7] et al. introduced $\mathbb{Z}_p\mathbb{Z}_p[v]$-additive cyclic codes of length (α, β) as $R[x]$-submodules of $\mathbb{Z}_p[x]/\langle x^\alpha - 1\rangle \times R[x]/\langle x^\beta - 1\rangle$, where $R = \mathbb{Z}_p + v\mathbb{Z}_p$ with $v^2 = v$. These mixed alphabets were studied only in single-variable polynomial rings as alphabet sets. In 2020, Abualrub et al. [1] studied the algebraic structure of $\mathbb{F}_2\mathbb{F}_4$-additive codes and constructed several optimal binary codes with the help of Grya map. A code is said to be a Type II code if the Hamming (Lee) weight of each codeword is divisible by 4; otherwise, Type I. Ling and Solé [14] defined Type II codes over $\mathbb{F}_4 + u\mathbb{F}_4$ and showed that Gray image of these codes are binary (self-dual) codes of Type II. Reversible cyclic code over $\mathbb{F} + u\mathbb{F}_4$ has been done in [18], authors gave an application of these codes in DNA codes by constructing cyclic DNA codes. In 2023, Shi et al. [16] studied linear self-dual codes over $\mathbb{F}_4 + u\mathbb{F}_4$ of type I. In [15], the authors explored additive cyclic codes over commutative chain rings by focusing on two types of additivity depending on the construction of dual codes, namely, Galois-additive (trace duality) and Eisenstein-additive (character theoretic duality). However, the study of additive cyclic codes over $\mathbb{F}_4 + u\mathbb{F}_4$ has not been done with respect to the symplectic inner product so far. In this article, we study additive cyclic codes over $\mathbb{F}_4 + u\mathbb{F}_4$. We give a necessary and sufficient condition for the codes to be self-orthogonal and self-dual with respect to the symplectic inner product. We show that we can construct self-orthogonal codes over $\mathbb{F}_4$ and $\mathbb{F}_2$ via Gray maps with respect to the symplectic inner product. These codes can be used to construct good quantum stabilizer codes [12]. Therefore, the study of additive codes over $\mathbb{F}_4 + u\mathbb{F}_4$ is worth it.

The manuscript is organized as follows: In Section 2, we give basic definitions and notations that we use throughout the article. In Section 3, we obtain generating polynomials of additive cyclic codes over $\mathbb{F}_4 + u\mathbb{F}_4$ and study the self-duality and orthogonality of these codes. In Section 4, we describe the image of additive cyclic code under defined Gray maps.

2. Preliminaries

Throughout the article, we denote $R = \mathbb{F}_4 + u\mathbb{F}_4$, where $u^2 = 0$ and $\mathbb{F}_4 = \{0, 1, w, \overline{w} = w^2 = w + 1\}$ is the finite field of order 4. A commutative ring with a unique maximal ideal is known as a local ring. A ring that is both local and principal is called a chain ring. One can easily see that the ring R is a chain ring with a unique maximal ideal $\langle u\rangle$. A non-empty additive subgroup of $\mathbb{F}_4^n$ is called an additive code of length n over $\mathbb{F}_4$. If an additive code over $\mathbb{F}_4$ is closed under scalar multiplication over $\mathbb{F}_4$, then the code is said to be linear code over $\mathbb{F}_4$. Let C be a non-empty subset of R^n, we say C is an additive code of length n if C is an additive subgroup of R^n. Elements of C are called codewords. Hamming weight of a vector $x = (x_0, \ldots, x_{n-1}) \in \mathbb{F}_4^n$ is defined as the number of coordinates x_i's non-zero. Hamming distance of two vectors $x, y \in \mathbb{F}_4^n$ is defined as the Hamming weight of $x - y$. For $z = (z_0, \ldots, z_{n-1}) \in \mathbb{F}_4^n$, let $n_0(z)$ be the number of $z_i = 0$ and $n_1(z)$ be the number of $z_i = 1$, then the Lee weight [9] of z is defined as $w_L(z) = n - n_0(z) + n_1(z)$. We define Gray maps in Section 4, in the following table, we list the Gray images and the Lee weight of elements of R.

Define a shift operator S on a given code C of length n as $S(c_0, c_1, \ldots, c_{n-1}) = (c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ for all $(c_0, c_1, \ldots, c_{n-1}) \in C$. An additive code is an additive cyclic code if $S(C) = C$, that is C invariant under the operator S and C is called additive m-quasi-cyclic code or quasi-cyclic code with index m if C

Table 1. Gray images and Lee weights of elements of R

$x \in R$	$w_L(x)$	$\tilde{\rho}(x) \in \mathbb{F}_4^2$	$\psi(\tilde{\rho}(x)) \in \mathbb{F}_2^4$
0	0	$(0,0)$	$(0,0,0,0)$
1	2	$(0,1)$	$(0,1,0,1)$
w	1	$(0,w)$	$(0,1,0,0)$
$\overline{w}$	1	$(0,\overline{w})$	$(0,0,0,1)$
u	4	$(1,1)$	$(1,1,1,1)$
$1+u$	2	$(1,0)$	$(1,0,1,0)$
$w+u$	3	$(1,\overline{w})$	$(1,0,1,1)$
$\overline{w}+u$	3	$(1,w)$	$(1,1,1,0)$
uw	2	(w,w)	$(1,1,0,0)$
$u\overline{w}$	2	$(\overline{w},\overline{w})$	$(0,0,1,1)$
$1+uw$	2	$(w,\overline{w})$	$(1,0,0,1)$
$1+u\overline{w}$	2	$(\overline{w},w)$	$(0,1,1,0)$
$w+u\overline{w}$	3	$(\overline{w},1)$	$(0,1,1,1)$
$\overline{w}+u\overline{w}$	1	$(\overline{w},0)$	$(0,0,1,0)$
$w+uw$	1	$(w,0)$	$(1,0,0,0)$
$\overline{w}+uw$	3	$(w,1)$	$(1,1,0,1)$

is invariant under the map S^m, where S^m is m the time composition of the map S.

We associate an element $(a_0, a_1, \ldots, a_{n-1}) \in R^n$ with a polynomial $a_0+a_1x+\cdots+a_{n-1}x^{n-1} \in R[x]$. Then an additive cyclic code C of length n can be seen as $\mathbb{F}_2[x]$-submodule of $R[x]/\langle x^n-1\rangle$ and an additive cyclic code of length n over $\mathbb{F}_4$ can be seen as $\mathbb{F}_2[x]$-submodule of $\mathbb{F}_4[x]/\langle x^n-1\rangle$.

Definition 2.1. *Let $f(x)$ be a polynomial with degree m over $\mathbb{F}_4$ then the reciprocal of $f(x)$ is denoted by $f^*(x)$ and defined as $f^*(x) = x^m f\left(\frac{1}{x}\right)$.*

Let $X = (a_0, a_1, \ldots, a_{n-1}, b_0, b_1, \ldots, b_{n-1})$ and $Y = (c_0, c_1, \ldots c_{n-1}, d_0, d_1, \ldots, d_{n-1})$ be even length vectors then symplectic inner product is defined as

$$\langle X, Y\rangle_s = \sum_{i=0}^{n-1} a_i d_i + \sum_{i=0}^{n-1} b_i c_i.$$

We define an inner product equivalent to the symplectic inner product by permutation of coordinates. Let vector X permutated to $A = (a_0, b_0, a_1, b_1, \ldots, a_{n-1}, b_{n-1})$ and vector Y permutated to $B = (c_0, d_0, c_1, d_1, \ldots, c_{n-1}, d_{n-1})$. We define the symplectic inner product of vectors A and B by pairing up their components, performing cross multiplication for each pair, and summing over all pairs (vector length is even, so pairing is well defined), that is

$$\begin{aligned} A &= (a_0, b_0, \quad a_1, b_1, \quad \ldots, \quad a_{n-1}, b_{n-1}) \\ B &= \underbrace{(c_0, d_0,}_{(a_0d_0 + b_0c_0)} \quad \underbrace{c_1, d_1,}_{+(a_1d_1 + b_1c_1)+} \quad \ldots, \quad \underbrace{c_{n-1}, d_{n-1})}_{+(a_{n-1}d_{n-1} + b_{n-1}c_{n-1})} \end{aligned}$$

$$[A, B]_s = \sum_{i=0}^{n-1} (a_i d_i + b_i c_i).$$

Throughout the article, we denote $[\ ,\ ]_s$ as the above inner product. Define the dual of a code C of length $2n$ over $\mathbb{F}_4$ as $C^{\perp_s} = \{A \in \mathbb{F}_4^{2n} : [A, B]_s = 0\ \forall\ B \in C\}$. A code C of length $2n$ over $\mathbb{F}_4$ is said to be complementary dual code if $C \cap C^{\perp_s} = \{0\}$.

Let $v_1, v_2 \in R^n$, such that $v_1 = x + uy$ and $v_2 = w + uz$ for some $x, y, w, z \in \mathbb{F}_4^n$. Define an inner product over R^n as

$$[v_1, v_2]_R = [x, z] + [y, w],$$

where $[\cdot, \cdot]$ is the usual Euclidean inner product over $\mathbb{F}_4^n$ defined as $[x, z] = \sum_{i=0}^{n-1} x_i z_i$ for $x = (x_0, \ldots, x_{n-1}), z = (z_0, \ldots, z_{n-1}) \in \mathbb{F}_4^n$. We denote the dual of a code C with respect to Euclidean inner product by $C^{\perp_E}$. The dual of a code C over R is defined as $C^{\perp_R} = \{v \in R^n : [v, c]_R = 0 \ \forall c \in C\}$. An additive code C over R is said to be an additive complementary dual (ACD) code if $C \cap C^{\perp_R} = \{0\}$. Note that $[\cdot\ ,\ \cdot]_R$ is a non-degenerated inner product as if $[a + ub, c + ud]_R = 0\ \forall c + ud \in R^n$ then $a + ub = 0$. Therefore $|C^{\perp_R}| = \frac{|R^n|}{|C|} = \frac{4^{2n}}{|C|}$.

3. Additive cyclic codes over $\mathbb{F}_4 + u\mathbb{F}_4$

Let C be an additive code of length n over R, define

$$\begin{aligned} C_1 &= \{x \in \mathbb{F}_4^n | x + uy \in C \text{ for some } y \in \mathbb{F}_4^n\}, \\ C_2 &= \{y \in \mathbb{F}_4^n | x + uy \in C \text{ for some } x \in \mathbb{F}_4^n\}. \end{aligned}$$

It is easy to see that C_1 and C_2 are additive codes of length n over $\mathbb{F}_4$ such that $C = C_1 \oplus uC_2$. We say C_1 and C_2 are component codes of the additive code C. The cardinality of the code C is the product of the cardinality of codes C_1 and C_2. We state this observation in the following proposition.

Proposition 3.1. *If C is an additive code over R then C is of the form $C = C_1 \oplus uC_2$, where C_1 and C_2 are additive codes over $\mathbb{F}_4$. Furthermore, if C_1 and C_2 have parameters $(n, 2^{k_1})$ and $(n, 2^{k_2})$ then C has parameters $(n, 2^{k_1+k_2})$.*

Now, we give the structure of additive cyclic codes of length n over R. First, we state the structure of additive cyclic codes over $\mathbb{F}_4$.

Theorem 3.2. *[5]. Let C be an additive $(n, 2^k)$ cyclic code over $\mathbb{F}_4$. Then $C = \langle \omega p(x) + q(x), r(x) \rangle$ for some $p(x), q(x)$ and $r(x)$ in $\mathbb{F}_2[x]$ such that $p(x)$ and $r(x)$ divide $x^n - 1$, $r(x)$ divides $q(x)\frac{x^n-1}{p(x)}$, and $k = 2n - \deg\ p(x) - \deg\ r(x)$.*

Theorem 3.3. *Let C_1 and C_2 be codes of length n over $\mathbb{F}_4$. Then the code $C = C_1 \oplus uC_2$ is an additive cyclic code of length n over R if and only if C_1 and C_2 are additive cyclic codes of length n over $\mathbb{F}_4$. Moreover, if $C_1 = \langle wp(x) + q(x), r(x) \rangle$ and $C_2 = \langle wp'(x) + q'(x), r'(x) \rangle$, then $C = \langle wp(x) + q(x), r(x), uwp'(x) + uq'(x), ur'(x) \rangle$ and vice versa. Also, $\dim_{\mathbb{F}_2}(C) = 4n - (\deg p(x) + \deg r(x) + \deg p'(x) + \deg r'(x))$.*

Proof. By Proposition 3.1, C is an additive code over R if and only if C_1 and C_2 are additive codes over $\mathbb{F}_4$. Now, let C be an additive cyclic code over R. For any $(c_0, c_1, \ldots, c_{n-1}) \in C_1$ and $(d_0, d_1, \ldots, d_{n-1}) \in C_2$, we have $(c_0 + ud_0, c_1 + ud_1, \ldots, c_{n-1} + ud_{n-1}) \in C$. Consequently, $(c_{n-1} + ud_{n-1}, c_0 + ud_0, \ldots, \ldots, c_{n-2} + ud_{n-2}) \in C$. This implies that $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C_1$ and $(d_{n-1}, d_0, \ldots, d_{n-2}) \in C_2$. Therefore C_1 and C_2 are cyclic codes. Conversely, if C_1 and C_2 are cyclic codes, then uC_2 is a cyclic set and $C_1 \oplus uC_2$ is an cyclic code over R. The rest of the proof follows from Theorem 3.2. □

Remark 3.4. *If $\deg q(x) \geq deg\ r(x)$ then by division algorithm there are $h(x), g(x) \in \mathbb{F}_2[x]$ such that $q(x) = r(x)h(x) + g(x)$ and $\deg g(x) < \deg r(x)$. We have*

$$\begin{aligned} \langle wp(x) + q(x), r(x) \rangle &= \langle wp(x) + r(x)h(x) + g(x), r(x) \rangle \\ &= \langle wp(x) + g(x), r(x) \rangle. \end{aligned}$$

So, we can assume that $\deg q(x) < \deg r(x)$. Similarly, we can also assume $\deg q'(x) < \deg r'(x)$.

Proposition 3.5. *If $C = C_1 \oplus uC_2$ is an additive code of length n over R, where C_1 and C_2 are additive codes of length n over $\mathbb{F}_4$, then $C^{\perp_R} = C_2^{\perp_E} \oplus uC_1^{\perp_E}$.*

Proof. Let $a + ub \in C_2^{\perp_E} + uC_1^{\perp_E}$, that is $a \in C_2^{\perp_E}$ and $b \in C_1^{\perp_E}$. For $c_1 + uc_2 \in C = C_1 + uC_2$, we have

$$[a + ub, c_1 + uc_2]_R = [a, c_2] + [b, c_1] = 0.$$

Thus $C_2^{\perp_E} + uC_1^{\perp_E} \subseteq C^{\perp_R}$. Also, $|C^{\perp_R}| = \frac{4^{2n}}{|C|} = \frac{4^{2n}}{|C_1|\cdot|C_2|} = |C_1^{\perp_E}| \cdot |C_2^{\perp_E}| = |C_2^{\perp_E} + uC_1^{\perp_E}|$. Hence $C^{\perp_R} = C_2^{\perp_E} + uC_1^{\perp_E}$. □

Corollary 3.6. *$C = C_1 \oplus uC_2$ is a dual containing additive code over R if and only if $C_1^{\perp_E} \subseteq C_2$ (equivalently $C_2^{\perp_E} \subseteq C_1$).*

Proof. Let $C \supseteq C^{\perp_R}$, that is $C_1 \oplus uC_2 \supseteq C_2^{\perp_E} \oplus uC_1^{\perp_E}$ implies that $C_1 \supseteq C_2^{\perp_E}$ and $C_2 \supseteq C_1^{\perp_E}$. Conversely, let $C_1^{\perp_E} \subseteq C_2$ this implies that $C_2^{\perp_E} \subseteq (C_1^{\perp_E})^{\perp_E} = C_1$. Therefore $C_2^{\perp_E} \oplus uC_1^{\perp_E} \subseteq C_1 \oplus uC_2$. □

Corollary 3.7. *$C = C_1 \oplus uC_2$ is self-orthogonal additive code over R if and only if $C_1 \subseteq C_2^{\perp_E}$ (equivalently $C_2 \subseteq C_1^{\perp_E}$).*

Example 3.8. *Let $C = C_1 \oplus uC_2$ an additive code with parameters $(7, 2^5)$ over R, where C_1 and C_2 are additive codes over $\mathbb{F}_4$ with generator matrix*

$$G_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & w^2 & w \\ 0 & 1 & 0 & w & w & 0 & 1 \\ 0 & 0 & 1 & 1 & w^2 & 1 & 1 \end{bmatrix}$$

and

$$G_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & w \\ 0 & 1 & 0 & 0 & 1 & 0 & w^2 \end{bmatrix},$$

respectively. It is easy to see that $C_2 \subseteq C_1^{\perp_E}$. Hence by Corollary 3.7, C is a self-orthogonal code over R.

Next, we describe the self-orthogonality of additive cyclic codes over R in terms of generator polynomials. By Corollary 3.7, it is sufficient to discuss when $C_1 \subseteq C_2^{\perp_E}$, where C_1 and C_2 are additive cyclic codes over $\mathbb{F}_4$.

Proposition 3.9. *Let $C_1 = \langle wp(x) + q(x), r(x)\rangle$ and $C_2 = \langle wp'(x) + q'(x), r'(x)\rangle$ be additive cyclic codes over $\mathbb{F}_4^n$. Then $C_1 \subseteq C_2^{\perp_E}$ if and only if following holds*

(i) $[wp(x) + q(x), wp'(x) + q'(x)] = 0$,

(ii) $p(x)r'(x^{n-1}) \equiv 0 \mod (x^n - 1)$ *and* $q(x)r'(x^{n-1}) \equiv 0 \mod (x^n - 1)$,

(iii) $q'(x)r(x^{n-1}) \equiv 0 \mod (x^n - 1)$ *and* $p'(x)r(x^{n-1}) \equiv 0 \mod (x^n - 1)$,

(iv) $r'(x)r(x^{n-1}) \equiv 0 \mod (x^n - 1)$ *and* $r'(x^{n-1})r(x) \equiv 0 \mod (x^n - 1)$.

Proof. We prove (iv), and other proofs follow similarly. Let C_r be a cyclic code generated by $r(x)$. Suppose $C_1 \subseteq C_2^{\perp_E}$, we have $[r(x), r'(x)] = 0$, that is $r'(x)$ belongs to the Euclidean dual of the cyclic code C_r generated by $r(x)$. From the theory of cyclic codes (for instance, see book ref), it is well known that $C_r^{\perp}$ is generated by $h^*(x)$, where $h(x) = (x^n - 1)/r(x)$. Thus, $r'(x) \in C_r^{\perp_E}$ implies that $r'(x) = \left(\frac{x^n-1}{r(x)}\right)^* k'(x)$

for some $k'(x) \in \mathbb{F}_2[x]$. Also, $(x^n-1)^* = x^n - 1 \in \mathbb{F}_2[x]$ and $r^*(x) = x^{d_r} r(x^{n-1}) \mod (x^n-1)$, where d_r is degree of $r(x)$. Consequently, we have $r'(x)r(x^{n-1}) \equiv 0 \mod (x^n-1)$.
Conversely, let $r'(x)r(x^{n-1}) \equiv 0 \mod (x^n-1)$ then $r'(x)x^{d_r}r(x^{n-1}) \equiv 0 \mod (x^n-1)$, that is $r'(x)r^*(x) \equiv 0 \mod (x^n-1)$. Thus $r'(x) = \left(\frac{x^n-1}{r(x)}\right)^* k''(x)$ for some $k''(x) \in \mathbb{F}_2[x]$, that is $r'(x) \in C_r^{\perp_E}$. Consequently, $[r'(x), r(x)] = 0$. Together with $(i), (ii), (iii)$, we have $C_1 \subseteq C_2^{\perp_E}$. □

Corollary 3.10. *$C = C_1 \oplus uC_2$ is self-dual additive code over R if and only if $C_2 = C_1^{\perp_E}$.*

4. Image of additive cyclic code under Gray map

In this section, we study the image of additive cyclic codes over R under the Gray map. Define a Gray maps $\tilde{\rho} : R \to \mathbb{F}_4^2$ as $\tilde{\rho}(a+ub) = (b, a+b)$. Extend the map $\tilde{\rho}$ to $\rho : R^n \to \mathbb{F}_4^{2n}$ as $\rho(a_1+ub_1, \ldots, a_n+ub_n) = (\tilde{\rho}(a_1+ub_1), \ldots, \tilde{\rho}(a_n+ub_n)) = (b_1, a_1+b_1, \ldots, b_n, a_n+b_n)$. Then ρ is a $\mathbb{F}_2$-linear isometry from $(R^n,$ Lee distance) to $(\mathbb{F}_4^{2n},$ Lee distance). The map ρ is equivalent the Gray map defined in [14] denoted by ϕ.

Remark 4.1. *Note that ρ is a bijection. In fact, for any $x = (a_1, a_2, a_3, a_4 \ldots, a_{2n}) \in \mathbb{F}_4^{2n}$, there is a $v = (v_1, v_2, \ldots, v_n) \in R^n$ such that $\rho(v) = x$, where $v_i = (a_{2i} - a_{2i-1}) + ua_{2i-1}$, $1 \le i \le n$.*

Theorem 4.2. *Let C be an additive cyclic code of length n over R, then $\rho(C)$ is an additive 2-quasi-cyclic code of length $2n$ over $\mathbb{F}_4$.*

Proof. Let $x, y \in \rho(C)$ then there be $c, d \in C$ such that $\rho(c) = x$ and $\rho(d) = y$. Let $c = (a_0 + ub_0, \ldots, a_{n-1} + ub_{n-1})$ and $d = (a'_0 + ub'_0, \ldots, a'_{n-1} + ub'_{n-1})$ then $\rho(c) = x = (b_0, a_0 + b_0, b_1, a_1 + b_1, \ldots, b_{n-1}, a_{n-1} + b_{n-1})$ and $\rho(d) = y = (b'_0, a'_0 + b'_0, b'_1, a'_1 + b'_1, \ldots, b'_{n-1}, a'_{n-1} + b'_{n-1})$. Consequently, $\rho(c+d) = \rho(c) + \rho(d) = x + y \in \rho(C)$. Hence $\rho(C)$ is additive code of length $2n$ over $\mathbb{F}_4$.

We have to show $S^2(\rho(C)) = \rho(C)$. Let $c = (c_0, c_1, \ldots, c_{n-1}) \in C$ then $(\rho \circ S)(c) = \rho(S(c)) = \rho(c_{n-1}, c_0, \ldots, c_{n-2}) = (\tilde{\rho}(c_{n-1}), \tilde{\rho}(c_0), \ldots, \tilde{\rho}(c_{n-2}))$ and $\rho(c) = (\tilde{\rho}(c_0), \tilde{\rho}(c_1), \ldots, \tilde{\rho}(c_{n-1}))$. Since $\tilde{\rho}(c_i)$ has length 2, for $0 \le i \le n-1$, therefore $(S^2 \circ \rho)(c) = (\rho \circ S)(c)$. Thus $S^2 \circ \rho = \rho \circ S$. Also, $S(C) = C$ implies that $\rho(S(C)) = \rho(C)$. Hence $S^2(\rho(C)) = (S^2 \circ \rho)(C) = (\rho \circ S)(C) = \rho(S(C)) = \rho(C)$. □

Lemma 4.3. *For any $v_1, v_2 \in R^n$, $[v_1, v_2]_R = [\rho(v_1), \rho(v_2)]_s$.*

Proof. Let $v_1 = x + uy$ and $v_2 = w + uz$ for some $x, y, w, z \in \mathbb{F}_4^n$. Let $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n), w = (w_1, \ldots, w_n)$ and $z = (z_1, \ldots, z_n)$ then

$$[v_1, v_2]_R = [x, z] + [y, w] = \sum_{i=1}^{n} (x_i z_i + y_i w_i).$$

Also, $\rho(v_1) = (y_1, x_1 + y_1, \ldots, y_n, x_n + y_n)$ and $\rho(v_2) = (z_1, w_1 + z_1, \ldots, z_n, w_n + z_n)$, we have

$$[\rho(v_1), \rho(v_2)]_s = \sum_{i=1}^{n} (y_i(w_i + z_i) + z_i(x_i + y_i)) = \sum_{i=1}^{n} (x_i z_i + y_i w_i).$$

□

Proposition 4.4. *If C is a self-orthogonal code of length n over R, then $\rho(C)$ is a self-orthogonal code of length $2n$ over $\mathbb{F}_4$.*

Lemma 4.5. *Let C be an additive code over R. Then $\rho(C^{\perp_R}) = \rho(C)^{\perp_s}$.*

Proof. Let $x \in \rho(C^{\perp_R})$ then there is a $v_1 \in C^{\perp_R}$ such that $\rho(v_1) = x$. This implies that $[v_1, v_2]_R = 0$ for all $v_2 \in C$. By Lemma 4.3, we have $[\rho(v_1), \rho(v_2)]_s = 0$ for all $v_2 \in C$ implies that $[x, y]_s = 0$ for all $y = \rho(v_2) \in \rho(C)$. Hence $x \in \rho(C)^{\perp_s}$.

Conversely, let $y \in \rho(C)^{\perp_s}$. Then $[y, x]_s = 0$ for all $x \in \rho(C)$ implies that $[y, \rho(v_1)]_s = 0$ for all $v_1 \in C$. By Remark 4.1, there is a $v_2 \in R^n$ such that $\rho(v_2) = y$. So, $[\rho(v_2), \rho(v_1)]_s = 0$ for all $v_1 \in C$, by Lemma 4.3, $[v_2, v_1]_R = 0$ for all $v_1 \in C$. Therefore $v_2 \in C^{\perp_R}$ implies that $y = \rho(v_2) \in \rho(C^{\perp_R})$. □

Lemma 4.6. *Let C be an additive code over R. Then $\rho(C \cap C^{\perp_R}) = \rho(C) \cap \rho(C^{\perp_R})$.*

Proof. Let $\rho(v_1) \in \rho(C \cap C^{\perp_R})$ for some $v_1 \in C \cap C^{\perp_R}$ then $\rho(v_1) \in \rho(C) \cap \rho(C^{\perp_R})$. Hence $\rho(C \cap C^{\perp_R}) \subseteq \rho(C) \cap \rho(C^{\perp_R})$. Conversely, let $y \in \rho(C) \cap \rho(C^{\perp_R})$ then there exist $v_1 \in C$ and $v_2 \in C^{\perp_R}$ such that $\rho(v_1) = \rho(v_2) = y$. Since ρ is a bijection therefore $v_1 = v_2$, consequently, $v_1 \in C \cap C^{\perp_R}$ implies that $y = \rho(v_1) \in \rho(C \cap C^{\perp_R})$. Hence $\rho(C) \cap \rho(C^{\perp_R}) \subseteq \rho(C \cap C^{\perp_R})$. Therefore $\rho(C \cap C^{\perp_R}) = \rho(C) \cap \rho(C^{\perp_R})$. □

Theorem 4.7. *An additive code of length n over R is an additive complementary dual code if and only if $\rho(C)$ is an additive complementary dual code of length $2n$ over $\mathbb{F}_4$.*

Any element $a \in \mathbb{F}_4$ can be written as $a = wa_1 + \overline{w}a_2$ for some $a_1, a_2 \in \mathbb{F}_2$. Define another Gray map [9] $\psi : \mathbb{F}_4^{2n} \to \mathbb{F}_2^{4n}$ as $\psi(w\boldsymbol{u} + \overline{w}\boldsymbol{v}) = (\boldsymbol{u}, \boldsymbol{v})$ for all $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}_2^{2n}$. Then ψ is $\mathbb{F}_2$-linear isometry from $(\mathbb{F}_4^{2n},$ Lee distance) to $(\mathbb{F}_2^{4n},$ Hamming distance).

Proposition 4.8. *For $x, y \in \mathbb{F}_4^{2n}$, if $[x, y]_s = 0$ then $[\psi(x), \psi(y)]_s = 0$, where $\psi(x), \psi(y) \in \mathbb{F}_2^{4n}$.*

Proof. Let $x = (x_0, \ldots, x_{2n-1}) = (wa_0 + \overline{w}b_0, \ldots, wa_{2n-1} + \overline{w}b_{2n-1}) = w\boldsymbol{a} + \overline{w}\boldsymbol{b}$ and $y = (y_0, \ldots, y_{2n-1}) = (wa'_0 + \overline{w}b'_0, \ldots, wa'_{2n-1} + \overline{w}b'_{2n-1}) = w\boldsymbol{a'} + \overline{w}\boldsymbol{b'}$, where $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{a'}, \boldsymbol{b'} \in \mathbb{F}_2^{2n}$. Then

$$\begin{aligned}[x, y]_s &= \sum_{i=0}^{n-1} x_{2i}y_{2i+1} + \sum_{i=0}^{n-1} x_{2i+1}y_{2i} \\ &= [z_1, z'_1] + [z_2, z'_2],\end{aligned}$$

where

$$\begin{aligned} z_1 &= (x_0, x_2, \ldots, x_{2n-2}) = wA_1 + \overline{w}B_1, & z'_1 &= (y_1, y_3, \ldots, y_{2n-1}) = wA'_1 + \overline{w}B'_1, \\ z_2 &= (x_1, x_3, \ldots, x_{2n-1}) = wA_2 + \overline{w}B_2, & z'_2 &= (y_0, y_2, \ldots, y_{2n-2}) = wA'_2 + \overline{w}B'_2 \end{aligned}$$

and

$$\begin{aligned} A_1 &= (a_0, a_2, \ldots, a_{2n-2}) & B_1 &= (b_0, b_2, \ldots, b_{2n-2}) \\ A_2 &= (a_1, a_3, \ldots, a_{2n-1}) & B_2 &= (b_1, b_3, \ldots, b_{2n-1}) \\ A'_1 &= (a'_1, a'_3, \ldots, a'_{2n-1}) & B'_1 &= (b'_1, b'_3, \ldots, b'_{2n-1}) \\ A'_2 &= (a'_0, a'_2, \ldots, a'_{2n-2}) & B'_2 &= (b'_0, b'_2, \ldots, b'_{2n-2}). \end{aligned}$$

Now, $[z_1, z'_1] = [wA_1 + \overline{w}B_1, wA'_1 + \overline{w}B'_1] = \overline{w}[A_1, A'_1] + [A_1, B'_1] + [B_1, A'_1] + w[B_1, B'_1]$, since $w + \overline{w} = 1$ therefore,

$$[z_1, z'_1] = w([B_1, B'_1] + [A_1, B'_1] + [B_1, A'_1]) + \overline{w}([A_1, A'_1] + [A_1, B'_1] + [B_1, A'_1]),$$

and

$$[z_2, z'_2] = w([B_2, B'_2] + [A_2, B'_2] + [B_2, A'_2]) + \overline{w}([A_2, A'_2] + [A_2, B'_2] + [B_2, A'_2]).$$

If $[x, y]_s = 0$ then $[z_1, z'_1] + [z_2, z'_2] = 0$, that is, the coefficients of w and $\overline{w}$ in $[z_1, z'_1] + [z_2, z'_2]$ are 0. So we have

$$\begin{aligned} [B_1, B'_1] + [A_1, B'_1] + [B_1, A'_1] + [B_2, B'_2] + [A_2, B'_2] + [B_2, A'_2] &= 0, \\ [A_1, B_1] + [A_1, B'_1] + [B_1, A'_1] + [A_2, A'_2] + [A_2, B'_2] + [B_2, A'_2] &= 0. \end{aligned}$$

By adding the above two equations, we have

$$[A_1, A_1'] + [A_2, A_2'] + [B_1, B_1'] + [B_2, B_2'] = 0. \tag{1}$$

Also, $\psi(x) = (\boldsymbol{a}, \boldsymbol{b}) = (a_0, a_1, \ldots, a_{2n-1}, b_0, b_1, \ldots, b_{2n-1})$ and
$\psi(y) = (\boldsymbol{a'}, \boldsymbol{b'}) = (a_0', a_1', \ldots, a_{2n-1}', b_0', b_1', \ldots, b_{2n-1}')$ are vectors in $\mathbb{F}_2^{4n}$.

$$\begin{aligned}
[\psi(x), \psi(y)]_s =& (a_0a_1' + a_0'a_1) + (a_2a_3' + a_2'a_3) + \cdots + (a_{2n-2}a_{2n-1}' + a_{2n-2}'a_{2n-1}) \\
&+ (b_0b_1' + b_0'b_1) + (b_2b_3' + b_2'b_3) + \cdots + (b_{2n-2}b_{2n-1}' + b_{2n-2}'b_{2n-1}) \\
=& (a_0a_1' + a_2a_3' + \cdots + a_{2n-2}a_{2n-1}') + (a_0'a_1 + a_2'a_3 + \cdots + a_{2n-2}'a_{2n-1}) \\
&+ (b_0b_1' + b_2b_3' + \cdots + b_{2n-2}b_{2n-1}') + (b_0'b_1 + b_2'b_3 + \cdots + b_{2n-2}'b_{2n-1}) \\
=& [A_1, A_1'] + [A_2, A_2'] + [B_1, B_1'] + [B_2, B_2'].
\end{aligned}$$

Therefore, by Equation 1, $[\psi(x), \psi(y)]_s = 0$. □

Proposition 4.9. *If C is a self-orthogonal code of length $2n$ over $\mathbb{F}_4$, then $\psi(C)$ is a self-orthogonal code of length $4n$ over $\mathbb{F}_2$.*

Define a map $\chi : R^n \to \mathbb{F}_2^{4n}$ as $\chi(v) = (\psi \circ \rho)(v)$ for all $v \in R^n$. Then χ is a Gray map ($\mathbb{F}_2$-linear isometry) from $(R^n, \text{Lee distance})$ to $(\mathbb{F}_2^{4n}, \text{Hamming distance})$. We have the following result from Proposition 4.4 and 4.9.

Theorem 4.10. *If C is an additive self-orthogonal code of length n over R, then $\chi(C)$ is a binary self-orthogonal code of length $4n$.*

5. Conclusion

We have determined the generating polynomials of additive cyclic codes over the chain ring $R = \mathbb{F}_4 + u\mathbb{F}_4,\ u^2 = 0$. We have provided necessary and sufficient conditions for the self-orthogonality and self-duality of these codes with respect to the symplectic inner product. Quantum codes play a crucial role in enabling reliable quantum computation and communication by correcting quantum errors. There are two ways to construct binary quantum from classical code. The first one is to find a self-orthogonal code of length $2n$ with respect to the symplectic inner product, and the second is to find self-orthogonal codes of length n over $\mathbb{F}_4$ with respect to the trace inner product[5]. In this article, we further showed that self-orthogonal codes over $\mathbb{F}_4$ can be obtained from additive cyclic codes over R with respect to the symplectic inner product using Gray maps. The following results showed that binary quantum stabilizer codes can be constructed from symplectic self-orthogonal codes over R.

Theorem 5.1. *[12, Corollary 16] Let C be an (n, p^{n-k}) additive code over F_{p^2} . Then there exists an $[[n, k, d]]_p$ quantum stabilizer code if C is a symplectic self-orthogonal, where $d = min\{wt(x) : x \in C^{\perp_s} \backslash C\}$ if $k > 0$ and $d = min\{wt(x) : x \in C\}$ if $k = 0$.*

Theorem 5.2. *Let C be an additive cyclic code over R with parameters $(n, 2^k)$ which satisfies the self-orthogonality conditions, then there exists an $[[2n, 2n - 2k, d]]$ binary quantum stabilizer code, where $d = min\{wt(\rho(x)) : x \in C^{\perp_R} \setminus C\}$ if $k > 0$ and $d = min\{wt(\rho(x)) : x \in C\}$ if $k = 0$.*

It will be interesting to apply the above theorem and construct good quantum codes. Additionally, one could explore using a general chain ring by defining an appropriate inner product and Gray maps that lead to symplectic self-orthogonal codes over fields.

Acknowledgements

We would like to thank the anonymous reviewers and the editor for their comments and suggestions. The authors also acknowledge Prof. Maheshanand Bhaintwal (IIT Roorkee) for insightful discussions on

Proposition 3.9. The first author acknowledges the financial support provided by IRD-IIT Delhi.

Disclosure statement

Data Availability Statement: The authors declare that [the/all other] data supporting the findings of this study are available within the article. Any clarification may be requested from the corresponding author, provided it is essential.

Competing interests: The authors declare that there is no conflict of interest regarding the publication of this manuscript.

References

[1] T. Abualrub, N. Aydin, I. Aydogdu, Optimal binary codes derived from $\mathbb{F}_2\mathbb{F}_4$-additive cyclic codes, J. Appl. Math. Comput., 64(1-2) (2020) 71–87.
[2] T. Abualrub, I. Siap, aN. Aydin, $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes, IEEE Trans. Inform. Theory, 60(3) (2014) 1508–1514.
[3] A. Agrawal, G. K. Verma, R. K. Sharma, Galois LCD codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, Bulletin of the Australian Mathematical Society, 107(2) (2022) 330–341.
[4] I. Aydogdu, T. Abualrub, I. Siap, On $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes, Int. J. Comput. Math., 92(9) (2015) 1806–1814.
[5] A. R. Calderbank, E. M. Rains, P. W. Shor, N. J. A. Sloane, Quantum error correction via codes over GF(4), IEEE Trans. Inform. Theory, 44(4) (1998) 1369–1387.
[6] P. Delsarte, V. I. Levenshtein, Association schemes and coding theory, IEEE Trans. Inform. Theory, 44(6) (1998) 2477–2504.
[7] L. Diao, J.Gao, J. Lu, Some results on $\mathbb{Z}_p\mathbb{Z}_p[v]$-additive cyclic codes, Adv. Math. Commun., 14(4) (2020) 555–572.
[8] C. Ding, Cyclic codes over finite fields, Designs from Linear Codes, (2018) 89–109.
[9] P. Gaborit, V. Pless, P. Solé, O. Atkin, Type II codes over $\mathbb{F}_4$, Finite Fields Appl., 8(2) (2002) 171–183.
[10] H. Islam, E. Martinez-Moro, O. Prakash, Cyclic codes over a non-chain ring $R_{e,q}$ and their application to LCD codes, Discret. Math., 344 (2021) 112545.
[11] H. Islam, O. Prakash, A study of cyclic and constacyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4$, Int. J. Inf. Coding Theory, 5 (2018) 155–168.
[12] A. Ketkar, A. Klappenecker, S. Kumar, P. K. Sarvepalli, Nonbinary stabilizer codes over finite fields, IEEE Trans. Inform. Theory, 52(11) (2006) 4892–4914.
[13] C. Li, C. Ding, S. Li, LCD cyclic codes over finite fields, IEEE Trans. Inform. Theory, 63 (2016) 4344–4356.
[14] S. Ling, P. Solé, Type II codes over $\mathbb{F}_4 + u\mathbb{F}_4$, Eur. J. Comb., 22 (2001) 983–997.
[15] E. Martinez-Moro, K. Otal, F. Ozbudak, Additive cyclic codes over finite commutative chain rings, Discrete Math., 341(7) (2018) 1873–1884.
[16] M. Shi, S. Chu, J-L. Kim, Classification of type I codes over $\mathbb{F}_4+u\mathbb{F}_4$, Journal of Applied Mathematics and Computing, 69 (2023) 3021–3037.
[17] M. Shi, R. Wu, P. Solé, Asymptotically good additive cyclic codes exist, IEEE Communications Letters, 22(10) (2018) 1980–1983.
[18] B. Srinivasulu, M. Bhaintwal, Reversible cyclic codes over $\mathbb{F}_4 + u\mathbb{F}_4$ and their applications to DNA codes, 7th International Conference on Information Technology and Electrical Engineering (ICITEE), (2015) 101–105.

[19] B. Srinivasulu, M. Bhaintwal, $\mathbb{Z}_2(\mathbb{Z}_2 + u\mathbb{Z}_2)$-additive cyclic codes and their duals, Discret. Math. Algorithms Appl., 8(2) (2016) 1650027.
[20] M. Sucheta Dutt, R. Sehmi, On cyclic codes over finite chain rings, Journal of Physics: Conference Series, 1850(2021).
[21] T. Yao, S. Zhu, $\mathbb{Z}_p\mathbb{Z}_{p^s}$-additive cyclic codes are asymptotically good, Cryptogr. Commun., 12(2) (2020) 253–264.
[22] T. Yao, S. Zhu, X. Kai, Asymptotically good $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$-additive cyclic codes, Finite Fields Appl., 63 (2020) 101633.