Duality of codes over non-unital rings of order four

Adel Alahmadi, Asmaa Melaibari, Patrick Solé

Duality of codes over non-unital rings of order four

Adel Alahmadi[1], Asmaa Melaibari[2], Patrick Solé[3§]

Abstract

In this paper we present a basic theory of the duality of linear codes over three of the non-unital rings of order four; namely I, E, and H as denoted in (Fine, 1993). A new notion of duality is introduced in the case of E that coincides with the notion of quasi self-dual code introduced in (Alahmadi et al, 2022). We characterize self-dual codes and LCD codes over the three rings, and investigate the properties of their corresponding additive codes over $\mathbb{F}_4$. We study the connection between the dual of any linear code over these rings and the dual of its residue and torsion codes. A MacWilliams formula is established for linear codes over the non-commutative ring E.

Keywords: non-unitary rings, additive codes, self-dual codes, LCD codes
MSC(2010): 94 B05, 16 D10

1 Introduction

There are, up to isomorphism, exactly eleven rings of order four [8, 17]. The only unital ones amongst these are $\mathbb{F}_4$, $\mathbb{Z}_4$, $\mathbb{F}_2 \times \mathbb{F}_2$, $\mathbb{F}_2 + u\,\mathbb{F}_2$. Before [5], these were the only rings of order four used as alphabets in Coding Theory [18]. In a series of papers [5, 1, 2, 3], self-orthogonal codes over three of the non-unitary rings in that list were investigated: namely I, E, and H, as per the notation of Fine [8]. Let $\mathcal{R}$ be one of the rings I, E, or H. Throughout this paper, if the statement does not depend on which ring we are using, we shall denote the ring by $\mathcal{R}$. The goal of this paper is to lay down the foundations of the study of duality of linear codes over these three rings. In particular the classes of self-dual and LCD codes are considered.

Self-dual codes have been given much attention in coding theory and have been widely studied for codes over finite fields and codes over rings [11],[15, Chapt. 3],[10, Chapt. 4] [13]. Due to technical hurdles, the study of self-dual codes over $\mathcal{R}$ was replaced by that of Quasi Self-Dual codes (QSD codes) in the series of papers mentioned above. In the present paper we initiate the study of self-dual codes over $\mathcal{R}$. In the case of the alphabet E, the new notion of (two-sided) self-dual code coincide with that of QSD code.

We then consider another class of codes that can be described in terms of their relationship with their dual. More precisely, it is the class of Linear codes with Complementary Dual (LCD). The notion of LCD codes was introduced by Massey in [12] on codes over finite fields. It was the object of much attention in recent years due to its application in Boolean

[1]Email: analahmadi@kau.edu.sa
[2]Email: amelaibari@uj.edu.sa
[3]Email: sole@enst.fr
[§]AA is with Math Dept, King Abdulaziz University, Jeddah, Saudi Arabia. AM is with University of Jeddah, Jeddah, Saudi Arabia & King Abdulaziz University, Jeddah, Saudi Arabia. PS is with I2M, (Aix Marseille Univ., CNRS, Centrale Marseille), Marseilles, France.

masking, a powerful countermeasure for cryptographic algorithms [7]. The study of LCD codes over non-unital rings first appeared in [19] where the authors investigated left LCD codes over E. We define LCD codes over E and H and explain why such class cannot be defined on codes over I.

We show that self-dual codes and LCD codes over $\mathcal{R}$ can be characterized in terms of their residue and torsion codes. Moreover, we study the duality of the associated additive codes over $\mathbb{F}_4$ with respect to the trace inner product.

To discuss the notions of self-dual codes and LCD codes, we address general properties of the dual of linear codes over $\mathcal{R}$. Through our investigation of duality, we prove a MacWilliams formula [11], which relates the weight enumerator of a linear code to that of its dual, for codes over the non-commutative non-unital ring E, where the dual is our two-sided dual.

The paper consists of six sections. Section 2 recalls some background material on binary codes and additive codes over $\mathbb{F}_4$ as well as general terminologies on linear codes over $\mathcal{R}$. Sections 3, 4, and 5 are devoted to studying codes over I, E, and H, respectively. As a preparation for the study of the main topic, we begin each of these three sections by taking a closer look at the structure of linear codes over each particular ring. Then we proceed to study the duality of codes and prove various specific results on self-dual codes and LCD codes. Section 6 concludes the article.

2 Definitions and notations

2.1 Rings of order four

We describe the main properties of the rings I, E, and H of order four. These rings are defined by relations on two generators a, b, and we shall write $c = a+b$ for all three rings.

The ring I is defined by $I = \langle a, b \mid 2a = 2b = 0, a^2 = b, ab = 0\rangle$ It is a non-unital commutative ring with characteristic two. The ring is local, with maximal ideal $\{0, b\}$, and has the following multiplication table:

$\times$	0	a	b	c
0	0	0	0	0
a	0	b	0	b
b	0	0	0	0
c	0	b	0	b

Table 1: Multiplication table for the ring I

The ring E is defined by $E = \langle a, b \mid 2a = 2b = 0, a^2 = a, b^2 = b, ab = a, ba = b\rangle$. It is a non-unital non-commutative ring with characteristic two. The ring is local with maximal ideal $\{0, c\}$, and has the following multiplication table:

$\times$	0	a	b	c
0	0	0	0	0
a	0	a	a	0
b	0	b	b	0
c	0	c	c	0

Table 2: Multiplication table for the ring E

The ring H is defined by $H = \langle a, b \mid 2a = 2b = 0, a^2 = 0, b^2 = b, ab = ba = 0 \rangle$. It is a non-unital commutative ring with characteristic two. The ring is semi-local with the two maximal ideals $\{0, a\}$, and $\{0, b\}$, and has the following multiplication table:

$\times$	0	a	b	c
0	0	0	0	0
a	0	0	0	0
b	0	0	b	b
c	0	0	b	b

Table 3: Multiplication table for the ring H

For further details on the properties of $\mathcal{R}$, we refer the reader to [1, 2, 3].

2.2 Codes

We recall some preliminary notions and terminologies of binary codes, additive codes over $\mathbb{F}_4$, and codes over $\mathcal{R}$.

2.2.1 Binary linear codes

An $[n, k]$ binary code C of length n and dimension k is a subspace of $\mathbb{F}_2^n$. The (Hamming) **weight** $\mathrm{wt}(\mathbf{x})$ of $\mathbf{x} \in C$ is the number of nonzero coordinates in $\mathbf{x}$. The **dual** $C^\perp$ of C is an $[n, n-k]$ code defined as

$$C^\perp = \{\mathbf{y} \in \mathbb{F}_2^n \mid \mathbf{x} \cdot \mathbf{y} = 0 \text{ for all } \mathbf{x} \in C\}$$

where $\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^n x_i y_i$ denotes the standard inner product in $\mathbb{F}_2^n$. A binary linear code C is **self-dual** if $C = C^\perp$. The length n of a self-dual code is even and its dimension is $n/2$. A binary code C is **linear with complementary dual (LCD)** if $C \cap C^\perp = \{\mathbf{0}\}$. Two binary codes are **permutation equivalent** if there is a permutation of coordinates that maps one to the other.

2.2.2 Additive codes over $\mathbb{F}_4$

Consider the finite field $\mathbb{F}_4$ consisting of the four elements $\{0, 1, \omega, \omega^2\}$ where $\omega^2 = 1 + \omega$. An $(n, 2^k)$ **additive code** over $\mathbb{F}_4$ of length n and size 2^k is an additive subgroup of $\mathbb{F}_4^n$. The **trace inner product** $\langle \mathbf{u}, \mathbf{v} \rangle_T$ of vectors $\mathbf{u}, \mathbf{v} \in \mathbb{F}_4^n$ is defined as

$$\langle \mathbf{u}, \mathbf{v} \rangle_T = \mathrm{Tr}(\mathbf{u} \cdot \mathbf{v}^2) = \mathrm{Tr}\left(\sum_{i=1}^n u_i v_i^2\right)$$

where $\mathrm{Tr} : \mathbb{F}_4 \to \mathbb{F}_2$ is the trace map defined by $\mathrm{Tr}(u) = u + u^2$ extended componentwise to a map from $\mathbb{F}_4^n$ to $\mathbb{F}_2^n$.

The **trace dual** $C^{\perp_T}$ of an additive code C of length n over $\mathbb{F}_4$ is defined as

$$C^{\perp_T} = \{\mathbf{v} \in \mathbb{F}_4^n \mid \langle \mathbf{u}, \mathbf{v} \rangle_T = 0 \text{ for all } \mathbf{u} \in C\}.$$

If C is an $(n, 2^k)$ additive code over $\mathbb{F}_4$, then $C^{\perp_T}$ is an $(n, 2^{2n-k})$ additive code over $\mathbb{F}_4$. An additive code C over $\mathbb{F}_4$ is **trace self-orthogonal** if $C \subseteq C^{\perp_T}$ and **trace self-dual** if $C = C^{\perp_T}$. An additive code C over $\mathbb{F}_4$ is **additive with complementary dual (ACD)** if $C \cap C^{\perp_T} = \{\mathbf{0}\}$.

Remark 1. An $[n, k]$ binary code can be thought of as an $(n, 2^k)$ additive code over $\mathbb{F}_4$ since $\mathbb{F}_2^n$ is an additive subgroup of $\mathbb{F}_4^n$.

2.2.3 Codes over $\mathcal{R}$

A **linear code of length** n **over** $\mathcal{R}$ is a left $\mathcal{R}$-submodule of $\mathcal{R}^n$. The (Hamming) **weight** $\mathrm{wt}(\mathbf{x})$ of $\mathbf{x} \in \mathcal{R}^n$ is the number of nonzero coordinates in $\mathbf{x}$. The **inner product** of $\mathbf{x} = x_1 x_2 \dots x_n$ and $\mathbf{y} = y_1 y_2 \dots y_n$ in $\mathcal{R}^n$ is defined by $\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^n x_i y_i$.

The **left dual** $C^{\perp_L}$ of a linear code C is the left module defined by

$$C^{\perp_L} = \{\mathbf{y} \in \mathcal{R}^n \mid \mathbf{y} \cdot \mathbf{x} = 0 \text{ for all } \mathbf{x} \in C\}.$$

The **right dual** $C^{\perp_R}$ of a linear code C is the right module defined by

$$C^{\perp_R} = \{\mathbf{y} \in \mathcal{R}^n \mid \mathbf{x} \cdot \mathbf{y} = 0 \text{ for all } \mathbf{x} \in C\}.$$

A linear code C is **self-orthogonal** if for any $\mathbf{x}, \mathbf{y} \in C$, $\mathbf{x} \cdot \mathbf{y} = 0$. Thus, any self-orthogonal code C satisfies the inclusion $C \subseteq C^{\perp_L} \cap C^{\perp_R}$. A linear code of length n is **quasi self-dual (QSD)** if it is self-orthogonal and of size 2^n. A linear code C is **left self-dual** (respectively, **right self-dual**) if $C = C^{\perp_L}$ (respectively, $C = C^{\perp_R}$). A linear code C of length n over $\mathcal{R}$ is **left nice** (respectively, **right nice**) if $|C||C^{\perp_L}| = 4^n$ (respectively, $|C||C^{\perp_R}| = 4^n$).

When $\mathcal{R}$ is commutative, $C^{\perp_R} = C^{\perp_L}$ and thus we omit the adjectives left and right and simply say **dual** and denote it by $C^{\perp}$. We do the same for the notions of **self-dual** and **nice**.

Two linear codes over $\mathcal{R}$ are **permutation equivalent** if there is a permutation of coordinates that maps one to the other.

We note that in the upcoming sections, $\oplus$ denotes the direct sum of vector spaces over $\mathbb{F}_2$. This concept, when applicable, is used to represent linear codes over $\mathcal{R}$ as additive codes over $\mathcal{R}$; where an **additive code** of length n over $\mathcal{R}$ is an additive subgroup of $\mathcal{R}^n$.

3 Results on linear codes over I

We begin this section by summarizing facts and notions essential to our study for linear codes over I. A detailed introduction on such codes can be found in [2].

To every linear code C of length n over I, there is an additive code $\phi_I(C)$ over $\mathbb{F}_4$ such that ϕ_I is defined by the alphabet substitution

$$0 \to 0,\ a \to \omega,\ b \to 1,\ c \to \omega^2,$$

extended in the natural way to a map from C to $\mathbb{F}_4^n$.

There are two binary linear codes of length n associated canonically with every linear code C of length n over I:

(1) the **residue code** $res(C)$ defined by $res(C) = \{\alpha(\mathbf{y}) \mid \mathbf{y} \in C\}$ where $\alpha : I \to \mathbb{F}_2$ is the map defined by $\alpha(0) = \alpha(b) = 0$ and $\alpha(a) = \alpha(c) = 1$, extended componentwise from C to $\mathbb{F}_2^n$,

(2) the **torsion code** $tor(C)$ defined by $tor(C) = \{\mathbf{x} \in \mathbb{F}_2^n \mid b\mathbf{x} \in C\}$.

The two binary codes satisfy the inclusion $res(C) \subseteq tor(C)$ and their sizes are related to the size of C by $|C| = |res(C)||tor(C)|$. Throughout this section, we let $k_1 = \dim(res(C))$ and $k_2 = \dim(tor(C)) - k_1$. The linear code C is said to be of **type** (k_1, k_2). We say that a linear code is **free** if and only if $k_2 = 0$. Equivalently, C is free if and only if $res(C) = tor(C)$.

3.1 Structure of linear codes

As noted in [2, Section 4], two distinct linear codes over I may share the same residue and torsion codes. This means that codes over I do not have a unique algebraic representation via their two associated binary codes. Nevertheless, these two binary codes are useful when studying the structure of codes over I and their dual.

The following theorem gives a connection between any linear code over I and its residue code.

Theorem 1. *If C is a linear code of length n over I, then the following hold:*

(1) *Every codeword $\mathbf{c} \in C$ can be written as $\mathbf{c} = a\mathbf{u} + b\mathbf{v}$ for some $\mathbf{u} \in res(C)$ and $\mathbf{v} \in \mathbb{F}_2^n$.*

(2) *If $\mathbf{u} \in res(C)$, then $a\mathbf{u} + b\mathbf{v}$ is a codeword in C for some $\mathbf{v} \in \mathbb{F}_2^n$.*

Proof. Let $\mathbf{c} \in C$. We can write $\mathbf{c}$ in a $b-$adic decomposition form as $\mathbf{c} = a\mathbf{u} + b\mathbf{v}$ where $\mathbf{u}, \mathbf{v} \in \mathbb{F}_2^n$. Since $\alpha(\mathbf{c}) = \alpha(a\mathbf{u} + b\mathbf{v}) = \mathbf{u}$, $\mathbf{u} \in res(C)$. This proves (1).
Now let $\mathbf{u} \in res(C)$. Then there exists $\mathbf{c} \in C$ such that $\alpha(\mathbf{c}) = \mathbf{u}$. We can write $\mathbf{c}$ in a $b-$adic decomposition form as $\mathbf{c} = a\mathbf{w} + b\mathbf{v}$ where $\mathbf{w}, \mathbf{v} \in \mathbb{F}_2^n$. Observe that $\alpha(a\mathbf{w} + b\mathbf{v}) = \mathbf{w}$. On the other hand, $\alpha(a\mathbf{w} + b\mathbf{v}) = \alpha(\mathbf{c}) = \mathbf{u}$. Hence, $\mathbf{w} = \mathbf{u}$ and so $a\mathbf{u} + b\mathbf{v}$ is a codeword in C. This proves (2). □

Now we study the close connection between the minimum distance of any linear code over I and that of its torsion code.

Theorem 2. *If C is a nonzero linear code over I, then the minimum distance of C equals the minimum distance of $tor(C)$.*

Proof. Let d be the minimum distance of C and let d_t be the minimum distance of $tor(C)$. Then there exists a nonzero $\mathbf{t} \in tor(C)$ such that $\mathrm{wt}(\mathbf{t}) = d_t$. Since $b\,tor(C) \subseteq C$ and $\mathrm{wt}(b\mathbf{t}) = \mathrm{wt}(\mathbf{t}) = d_t$, $d \leq d_t$.
Now we prove that $d \geq d_t$. Let $\mathbf{x} \in C$ such that $\mathrm{wt}(\mathbf{x}) = d$. By Theorem 1, $\mathbf{x} = a\mathbf{u} + b\mathbf{v}$ where $\mathbf{u} \in res(C)$ and $\mathbf{v} \in \mathbb{F}_2^n$. Since C is nonzero, we have the following three cases depending on $\mathbf{u}$ and $\mathbf{v}$:

- If $\mathbf{u} = \mathbf{0}$ and $\mathbf{v} \neq \mathbf{0}$, then $\mathbf{v} \in tor(C)$ and $\mathrm{wt}(\mathbf{x}) = \mathrm{wt}(b\mathbf{v}) = \mathrm{wt}(\mathbf{v}) \geq d_t$.
- If $\mathbf{u} \neq \mathbf{0}$ and $\mathbf{v} = \mathbf{0}$, then $\mathrm{wt}(\mathbf{x}) = \mathrm{wt}(a\mathbf{u}) = \mathrm{wt}(\mathbf{u})$.
- If $\mathbf{u}, \mathbf{v} \neq \mathbf{0}$, then $\mathrm{wt}(\mathbf{x}) \geq \mathrm{wt}(a\mathbf{x}) = \mathrm{wt}(b\mathbf{u}) = \mathrm{wt}(\mathbf{u})$.

Since $\mathbf{u} \in res(C) \subseteq tor(C)$, it follows that $\mathrm{wt}(\mathbf{u}) \geq d_t$. Thus, in all cases, $d = \mathrm{wt}(\mathbf{x}) \geq d_t$. Since $d \leq d_t$ and $d \geq d_t$, it follows that $d = d_t$. □

3.2 Duality

The following theorem gives properties on the residue and torsion codes of the dual of linear codes over I.

Theorem 3. *If C is a linear code of length n over I, then the following hold:*

(1) $res(C^\perp) = res(C)^\perp$.

(2) $tor(C^\perp) = \mathbb{F}_2^n$.

Proof. To prove (1), let $\mathbf{u} \in res(C^\perp)$. By Theorem 1, $a\mathbf{u} + b\mathbf{v}$ is a codeword in $C^\perp$ for some $\mathbf{v} \in \mathbb{F}_2^n$. Let $\mathbf{x} \in res(C)$. By Theorem 1, $a\mathbf{x} + b\mathbf{y}$ is a codeword in C for some $\mathbf{y} \in \mathbb{F}_2^n$. By definition of $C^\perp$,

$$0 = (a\mathbf{u} + b\mathbf{v}) \cdot (a\mathbf{x} + b\mathbf{y}) = b(\mathbf{u} \cdot \mathbf{x}).$$

Hence, $\mathbf{u} \cdot \mathbf{x} = 0$ which implies that $\mathbf{u} \in res(C)^\perp$. Therefore, $res(C^\perp) \subseteq res(C)^\perp$.
Now assume that $\mathbf{u} \in res(C)^\perp$. Let $\mathbf{c} \in C$. By Theorem 1, $\mathbf{c} = a\mathbf{x} + b\mathbf{y}$ where $\mathbf{x} \in res(C)$ and $\mathbf{y} \in \mathbb{F}_2^n$. Observe that

$$a\mathbf{u} \cdot \mathbf{c} = a\mathbf{u} \cdot (a\mathbf{x} + b\mathbf{y}) = b(\mathbf{u} \cdot \mathbf{x}) = 0.$$

Hence, $a\mathbf{u} \in C^\perp$ and $\alpha(a\mathbf{u}) = \mathbf{u}$ which yields $\mathbf{u} \in res(C^\perp)$. Therefore, $res(C)^\perp \subseteq res(C^\perp)$. This proves (1).
To prove (2), we will show that $\mathbb{F}_2^n \subseteq tor(C^\perp)$. Let $\mathbf{u} \in \mathbb{F}_2^n$ and let $\mathbf{c} \in C$. By Theorem 1, $\mathbf{c} = a\mathbf{x} + b\mathbf{y}$ where $\mathbf{x} \in res(C)$ and $\mathbf{y} \in \mathbb{F}_2^n$. Observe that

$$\mathbf{c} \cdot b\mathbf{u} = (a\mathbf{x} + b\mathbf{y}) \cdot b\mathbf{u} = 0.$$

Hence, $b\mathbf{u} \in C^\perp$ and so $\mathbf{u} \in tor(C^\perp)$. Therefore, $\mathbb{F}_2^n = tor(C^\perp)$. This proves (2). □

The dual of a linear code of length n over I can be written uniquely in terms of its residue code and the binary vector space $\mathbb{F}_2^n$ as the following theorem shows.

Theorem 4. *If C is a linear code of length n over I, then $C^\perp = a\, res(C)^\perp \oplus b\, \mathbb{F}_2^n$.*

Proof. Let $\mathbf{z} \in C^\perp$. By Theorems 1 and 3, $\mathbf{z} = a\mathbf{x} + b\mathbf{y}$ where $\mathbf{x} \in res(C^\perp) = res(C)^\perp$ and $\mathbf{y} \in \mathbb{F}_2^n$. This proves that $C^\perp \subseteq a\, res(C)^\perp + b\, \mathbb{F}_2^n$.
Now assume that $\mathbf{w} := a\mathbf{u} + b\mathbf{v} \in a\, res(C)^\perp + b\, \mathbb{F}_2^n$. Let $\mathbf{c} \in C$. By Theorem 1, $\mathbf{c} = a\mathbf{r} + b\mathbf{s}$ where $\mathbf{r} \in res(C)$ and $\mathbf{s} \in \mathbb{F}_2^n$. Observe that

$$\mathbf{w} \cdot \mathbf{c} = (a\mathbf{u} + b\mathbf{v}) \cdot (a\mathbf{r} + b\mathbf{s}) = b(\mathbf{u} \cdot \mathbf{r}) = 0.$$

Hence, $\mathbf{w} \in C^\perp$. Therefore, $a\, res(C)^\perp + b\, \mathbb{F}_2^n \subseteq C^\perp$. This proves that $C^\perp = a\, res(C)^\perp + b\, \mathbb{F}_2^n$. Since $|C^\perp| = |\, res(C^\perp)|\, |\, tor(C^\perp)| = |\, res(C)^\perp|\, |\, \mathbb{F}_2^n\, |$ by Theorem 3, the sum is direct. □

The size of the dual of any type (k_1, k_2) linear code of length n over I equals 2^{2n-k_1}. Thus, we have the following result.

Proposition 1. *The only nice code over I is the zero code.*

Proof. Suppose C is a type (k_1, k_2) nice code of length n. By the definition of nice codes and Theorem 4,

$$4^n = |C||C^\perp| = 2^{2n+k_1+k_2}$$

which holds if and only if $k_1 + k_2 = 0$. Since $k_1, k_2 \geq 0$, it follows that C is nice if and only if $k_1 = k_2 = 0$. Hence, the only nice code over I is the zero code. □

An interesting fact about the families of QSD codes and self-dual codes of length n over I is the following.

Proposition 2. *Let $\mathcal{Q}$ be the family of all QSD codes of length n over I and let $\mathcal{S}$ be the family of all self-dual codes of length n over I. Then $\mathcal{Q} \cap \mathcal{S} = \emptyset$.*

Proof. Suppose that a linear code C over I is QSD and self-dual. Then C is nonzero and $|C| = |C^{\perp}| = 2^n$ which implies that C is nice. By Proposition 1, no such codes exist. This means that a linear code over I can never simultaneously be both QSD and self-dual. □

3.2.1 Self-dual codes

Self-dual codes over I are characterized by means of their two associated binary codes as the following theorem shows.

Theorem 5. *A linear code C of length n over I is self-dual if and only if the following two conditions are satisfied:*

(1) *$res(C)$ is a self-dual binary code,*

(2) *$tor(C) = \mathbb{F}_2^n$.*

Proof. Suppose that C is self-dual. Then $C = C^{\perp}$. Consequently, $res(C) = res(C^{\perp})$ and $tor(C) = tor(C^{\perp})$. By Theorem 3, $res(C) = res(C)^{\perp}$ and $tor(C) = \mathbb{F}_2^n$.
Conversely, suppose that $res(C) = res(C)^{\perp}$ and $tor(C) = \mathbb{F}_2^n$. By Theorems 1 and 4,

$$C \subseteq a\, res(C) + b\, \mathbb{F}_2^n = a\, res(C)^{\perp} + b\, \mathbb{F}_2^n = C^{\perp}.$$

As $|C| = |\, res(C)||\, tor(C)| = |\, res(C)^{\perp}||\, \mathbb{F}_2^n\, | = |C^{\perp}|$, it follows that $C = C^{\perp}$ and hence C is self-dual. □

Corollary 1. *If B is a self-dual binary code of length n, then B is a residue code of a self-dual code over I.*

Proof. Since B is self-dual and $B \subseteq \mathbb{F}_2^n$, by [2, Theorem 4], the linear code C defined by $C = aB + b\,\mathbb{F}_2^n$ is a self-orthogonal code over I with $res(C) = B$ and $tor(C) = \mathbb{F}_2^n$. By Theorem 5 and the self-duality of B, it follows that C is self-dual. □

By Theorem 5 and Corollary 1, self-dual codes over I exist only for even lengths and there are as many type $(n/2, n/2)$ self-dual codes of length n over I as there are $[n, n/2]$ binary self-dual codes.

Theorem 6. *Two self-dual codes over I are permutation equivalent if and only if their residue codes are permutation equivalent.*

Proof. Let C and C' be two permutation equivalent codes over I. Then there is a permutation matrix P such that $C' = CP$. Since $\alpha(C') = \alpha(CP) = \alpha(C)P$, it follows that $res(C)$ and $res(C')$ are permutation equivalent.
Conversely, suppose that C and C' are self-dual codes over I where $res(C)$ and $res(C')$ are permutation equivalent. Then there is a permutation matrix P such that $res(C') = res(C)P$. As $\mathbb{F}_2^n = \mathbb{F}_2^n\, P$, we have

$$a\, res(C') + b\, \mathbb{F}_2^n = a\, res(C)P + b\, \mathbb{F}_2^n\, P. \tag{1}$$

Since C and C' are self-dual, by Theorems 4 and 5, it follows that $C = a\, res(C) \oplus b\, \mathbb{F}_2^n$ and $C' = a\, res(C') \oplus b\, \mathbb{F}_2^n$. By Equation (1), we obtain $C' = CP$, proving that C and C' are permutation equivalent. □

The following example shows that Theorem 6 may not hold if the codes over I are not self-dual.

Example 1. The linear codes C and C' with generator matrices

$$\begin{pmatrix} a & a & b \\ 0 & b & b \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} a & a & 0 \\ 0 & b & b \end{pmatrix},$$

respectively, have the same residue code. In particular, $res(C) = res(C') = \{000, 110\}$. However, C and C' are not permutation equivalent as shown in the classification of QSD codes in [2, Section 6]. Note that, by Proposition 2, C and C' are not self-dual.

From the results of this subsection, we see that there is a one-to-one correspondence between inequivalent self-dual binary codes and inequivalent self-dual codes over I of the same length. In other words, classifying self-dual codes over I, up to permutation equivalence, is equivalent to classifying self-dual binary codes, up to equivalence. All binary self-dual codes have been classified, up to equivalence, for length n with $2 \leq n \leq 32$ [9, 14, 16]. Using this classification along with Theorem 5 and Corollary 1, the classification of all self-dual codes over I of the same lengths is immediate. We remark that by Theorems 2 and 5, all self-dual codes over I have minimum distance equals 1.

To conclude this subsection, we note that the image of any self-dual code over I under the map ϕ_I is never an additive trace self-dual code over $\mathbb{F}_4$. However, the trace dual of this image is an additive trace self-orthogonal code over $\mathbb{F}_4$.

Proposition 3. *If C is a self-dual code of length $2n$ over I, then $\phi_I(C)^{\perp_T}$ is trace self-orthogonal of size 2^n; in particular, $\phi_I(C)$ is not trace self-dual.*

Proof. By Theorems 4 and 5, the self-duality of C implies that $C = a\, res(C) \oplus b\, tor(C)$ with $|\, res(C)| = 2^n$ and $|\, tor(C)| = |\, \mathbb{F}_2^{2n}\,| = 2^{2n}$. Then, $|\phi_I(C)| = |C| = 2^{3n}$ and $|\phi_I(C)^{\perp_T}| = 2^n$. Comparing cardinalities, we see that $\phi_I(C) \neq \phi_I(C)^{\perp_T}$ which shows that $\phi_I(C)$ is not trace self-dual.
We claim that $res(C) = \phi_I(C)^{\perp_T}$. Let $\mathbf{u} \in res(C)$ and let $\mathbf{x} \in \phi_I(C)$. Then, there exists a codeword $a\mathbf{r} + b\mathbf{t}$ in C where $\mathbf{r} \in res(C)$ and $\mathbf{t} \in tor(C)$ such that $\mathbf{x} = \phi_I(a\mathbf{r} + b\mathbf{t}) = \omega\mathbf{r} + \mathbf{t}$. Observe that

$$\langle \mathbf{x}, \mathbf{u} \rangle_T = \langle \omega\mathbf{r} + \mathbf{t}, \mathbf{u} \rangle_T = \langle \omega\mathbf{r}, \mathbf{u} \rangle_T + \langle \mathbf{t}, \mathbf{u} \rangle_T = \mathrm{Tr}(\omega\mathbf{r} \cdot \mathbf{u}) + \mathrm{Tr}(\mathbf{t} \cdot \mathbf{u}).$$

Since C is self-dual, by Theorem 5, $res(C)$ is self-dual and therefore $\mathbf{r} \cdot \mathbf{u} = 0$ which gives $\mathrm{Tr}(\omega\mathbf{r} \cdot \mathbf{u}) = 0$. As $\mathbf{t} \cdot \mathbf{u} \in \{0, 1\}$, $\mathrm{Tr}(\mathbf{t} \cdot \mathbf{u}) = 0$. Thus, $\langle \mathbf{x}, \mathbf{u} \rangle_T = 0$ proving that $\mathbf{u} \in \phi_I(C)^{\perp_T}$ and consequently $res(C) \subseteq \phi_I(C)^{\perp_T}$. The fact that $|\, res(C)| = 2^n = |\phi_I(C)^{\perp_T}|$ implies that $res(C) = \phi_I(C)^{\perp_T}$ as claimed. Now observe that since $res(C) \subseteq tor(C)$, for any $\mathbf{v} \in res(C)$, $b\mathbf{v} \in C$ and thus $\mathbf{v} = \phi_I(b\mathbf{v}) \in \phi_I(C)$. Hence, we obtain $res(C) \subseteq \phi_I(C)$. In particular, $\phi_I(C)^{\perp_T} \subseteq \phi_I(C)$ which proves that $\phi_I(C)^{\perp_T}$ is trace self-orthogonal. □

3.2.2 LCD codes

Based on the following proposition, the usual notion of LCD codes, as introduced in [12] over finite fields, is not applicable on nonzero codes over I.

Proposition 4. *If C is a nonzero linear code of length n over I, then $C \cap C^{\perp} \neq \{\mathbf{0}\}$.*

Proof. Suppose that $\mathbf{x}$ is a nonzero codeword in C. By Theorem 1, $\mathbf{x} = a\mathbf{u} + b\mathbf{v}$ where $\mathbf{u} \in res(C)$ and $\mathbf{v} \in \mathbb{F}_2^n$. We have two cases depending on $\mathbf{u}$.
If $\mathbf{u} = \mathbf{0}$, then $\mathbf{x} = b\mathbf{v}$. Since $b\,\mathbb{F}_2^n \subseteq C^{\perp}$ and $\mathbf{x} \in C$, it follows that $\mathbf{x} \in C \cap C^{\perp}$.
If $\mathbf{u} \neq \mathbf{0}$, then $a\mathbf{x} = b\mathbf{u}$ is a nonzero codeword in C. Since $b\,\mathbb{F}_2^n \subseteq C^{\perp}$ and $a\mathbf{x} \in C$, it follows that $a\mathbf{x} \in C \cap C^{\perp}$.
This proves that $C \cap C^{\perp} \neq \{\mathbf{0}\}$. □

4 Results on linear codes over E

We begin this section by summarizing facts and notions essential to our study for linear codes over E. A detailed introduction on such codes can be found in [3].

To every linear code C of length n over E, there is an additive code $\phi_E(C)$ over $\mathbb{F}_4$ such that ϕ_E is defined by the alphabet substitution

$$0 \to 0,\ a \to \omega,\ b \to \omega^2,\ c \to 1,$$

extended in the natural way to a map from C to $\mathbb{F}_4^n$.

There are two binary linear codes of length n associated canonically with every linear code C of length n over E:

(1) the **residue code** $res(C)$ defined by $res(C) = \{\alpha(\mathbf{y}) \mid \mathbf{y} \in C\}$ where $\alpha : E \to \mathbb{F}_2$ is the map defined by $\alpha(0) = \alpha(c) = 0$ and $\alpha(a) = \alpha(b) = 1$, extended componentwise from C to $\mathbb{F}_2^n$,

(2) the **torsion code** $tor(C)$ defined by $tor(C) = \{\mathbf{x} \in \mathbb{F}_2^n \mid c\mathbf{x} \in C\}$.

The two binary codes satisfy the inclusion $res(C) \subseteq tor(C)$ and their sizes are related to the size of C by $|C| = |\,res(C)||\,tor(C)|$. Throughout this section, we let $k_1 = \dim(res(C))$ and $k_2 = \dim(tor(C)) - k_1$. The linear code C is said to be of **type** (k_1, k_2). We say that a linear code is **free** if and only if $k_2 = 0$. Equivalently, C is free if and only if $res(C) = tor(C)$.

4.1 Structure of linear codes

The following two theorems improve Lemma 3 and Theorem 6 of [3] by removing the QSD requirement from their statements.

Theorem 7. *If C is a linear code of length n over E, then $a\,res(C) \subseteq C$.*

Proof. Let $\mathbf{u} \in res(C)$. Then there exists $\mathbf{c} \in C$ such that $\alpha(\mathbf{c}) = \mathbf{u}$. We can write $\mathbf{c}$ in a $c-$adic decomposition form as $\mathbf{c} = a\mathbf{x} + c\mathbf{y}$ where $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$. Now observe that $\mathbf{u} = \alpha(\mathbf{c}) = \alpha(a\mathbf{x} + c\mathbf{y}) = \mathbf{x}$. Hence, $\mathbf{c} = a\mathbf{u} + c\mathbf{y}$. By linearity of C, we have $a\mathbf{c} \in C$ and thus $a\mathbf{u} \in C$. Therefore, $a\,res(C) \subseteq C$. □

Theorem 8. *If C is a linear code of length n over E, then $C = a\,res(C) \oplus c\,tor(C)$.*

Proof. Let $\mathbf{c} \in C$. We can write $\mathbf{c}$ in a $c-$adic decomposition form as $\mathbf{c} = a\mathbf{x} + c\mathbf{y}$ where $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$. Since $\alpha(\mathbf{c}) = \alpha(a\mathbf{x}+c\mathbf{y}) = \mathbf{x}$, $\mathbf{x} \in res(C)$. By Theorem 7, $a\mathbf{x} \in C$. By linearity of C, it follows that $c\mathbf{y} \in C$ and hence $\mathbf{y} \in tor(C)$. This proves that $C \subseteq a\,res(C) + c\,tor(C)$. The inclusion $a\,res(C)+c\,tor(C) \subseteq C$ follows from the linearity of C together with the facts that $a\,res(C) \subseteq C$ and $c\,tor(C) \subseteq C$. Hence, $C = a\,res(C) + c\,tor(C)$. The sum is direct since $|C| = |\,res(C)||\,tor(C)|$. □

The following theorem is the analogue of Theorem 2.

Theorem 9. *If C is a nonzero linear code over E, then the minimum distance of C equals the minimum distance of $tor(C)$.*

Proof. Let d be the minimum distance of C and let d_t be the minimum distance of $tor(C)$. Then there exists a nonzero $\mathbf{t} \in tor(C)$ such that $\mathrm{wt}(\mathbf{t}) = d_t$. Since $c\,tor(C) \subseteq C$ and $\mathrm{wt}(c\mathbf{t}) = \mathrm{wt}(\mathbf{t}) = d_t$, $d \leq d_t$.

Now we prove that $d \geq d_t$. Let $\mathbf{x} \in C$ such that $\mathrm{wt}(\mathbf{x}) = d$. By Theorem 8, $\mathbf{x} = a\mathbf{u} + c\mathbf{v}$ where $\mathbf{u} \in res(C)$ and $\mathbf{v} \in tor(C)$. Since C is nonzero, we have the following three cases depending on $\mathbf{u}$ and $\mathbf{v}$:

- If $\mathbf{u} = \mathbf{0}$ and $\mathbf{v} \neq \mathbf{0}$, then $\mathrm{wt}(\mathbf{x}) = \mathrm{wt}(c\mathbf{v}) = \mathrm{wt}(\mathbf{v})$.
- If $\mathbf{u} \neq \mathbf{0}$ and $\mathbf{v} = \mathbf{0}$, then $\mathrm{wt}(\mathbf{x}) = \mathrm{wt}(a\mathbf{u}) = \mathrm{wt}(\mathbf{u})$.
- If $\mathbf{u}, \mathbf{v} \neq \mathbf{0}$, then $\mathrm{wt}(\mathbf{x}) \geq \mathrm{wt}(a\mathbf{x}) = \mathrm{wt}(a\mathbf{u}) = \mathrm{wt}(\mathbf{u})$.

Since $\mathbf{u} \in res(C) \subseteq tor(C)$ and $\mathbf{v} \in tor(C)$, it follows that $\mathrm{wt}(\mathbf{u}), \mathrm{wt}(\mathbf{v}) \geq d_t$. Thus, in all cases $d = \mathrm{wt}(\mathbf{x}) \geq d_t$.
Since $d \leq d_t$ and $d \geq d_t$, it follows that $d = d_t$. □

4.2 Duality

The following theorem gives properties on the residue and torsion codes of the one-sided duals of linear codes over E.

Theorem 10. *If C is a linear code of length n over E, then the following hold:*

(1) $res(C^{\perp_L}) = tor(C^{\perp_L}) = res(C)^{\perp}$.

(2) $res(C^{\perp_R}) = tor(C)^{\perp}$.

(3) $tor(C^{\perp_R}) = \mathbb{F}_2^n$.

Proof. To prove (1), it suffices to show that $tor(C^{\perp_L}) \subseteq res(C)^{\perp} \subseteq res(C^{\perp_L})$.
Let $\mathbf{v} \in tor(C^{\perp_L})$. Then, $c\mathbf{v} \in C^{\perp_L}$. Let $\mathbf{x} \in res(C)$. By Theorem 7, $a\mathbf{x} \in C$. By definition of $C^{\perp_L}$, $0 = c\mathbf{v} \cdot a\mathbf{x} = c(\mathbf{v} \cdot \mathbf{x})$. Hence, $\mathbf{v} \cdot \mathbf{x} = 0$ which implies that $\mathbf{v} \in res(C)^{\perp}$, proving that

$$tor(C^{\perp_L}) \subseteq res(C)^{\perp}. \tag{2}$$

Now assume that $\mathbf{u} \in res(C)^{\perp}$. Let $\mathbf{c} \in C$. By Theorem 8, $\mathbf{c} = a\mathbf{r} + c\mathbf{t}$ where $\mathbf{r} \in res(C)$ and $\mathbf{t} \in tor(C)$. Observe that

$$a\mathbf{u} \cdot \mathbf{c} = a\mathbf{u} \cdot (a\mathbf{r} + c\mathbf{t}) = a(\mathbf{u} \cdot \mathbf{r}) = 0.$$

Hence, $a\mathbf{u} \in C^{\perp_L}$ and $\alpha(a\mathbf{u}) = \mathbf{u}$ which yields $\mathbf{u} \in res(C^{\perp_L})$. Therefore,

$$res(C)^{\perp} \subseteq res(C^{\perp_L}). \tag{3}$$

By Equations (2) and (3), together with the fact that $res(C^{\perp_L}) \subseteq tor(C^{\perp_L})$, we obtain

$$res(C^{\perp_L}) = tor(C^{\perp_L}) = res(C)^{\perp}.$$

To prove (2), assume that $\mathbf{u} \in res(C^{\perp_R})$. By Theorem 7, $a\mathbf{u} \in C^{\perp_R}$. Let $\mathbf{x} \in tor(C)$. Then, $c\mathbf{x} \in C$. By definition of $C^{\perp_R}$, $0 = c\mathbf{x} \cdot a\mathbf{u} = c(\mathbf{x} \cdot \mathbf{u})$. Hence, $\mathbf{x} \cdot \mathbf{u} = 0$ which implies that $\mathbf{u} \in tor(C)^{\perp}$. Therefore, $res(C^{\perp_R}) \subseteq tor(C)^{\perp}$.
Now assume $\mathbf{v} \in tor(C)^{\perp}$. Let $\mathbf{c} \in C$. By Theorem 8, $\mathbf{c} = a\mathbf{r} + c\mathbf{t}$ where $\mathbf{r} \in res(C) \subseteq tor(C)$ and $\mathbf{t} \in tor(C)$. Observe that

$$\mathbf{c} \cdot a\mathbf{v} = (a\mathbf{r} + c\mathbf{t}) \cdot a\mathbf{v} = a(\mathbf{r} \cdot \mathbf{v}) + c(\mathbf{t} \cdot \mathbf{v}) = 0$$

Hence, $a\mathbf{v} \in C^{\perp_R}$. Since $\alpha(a\mathbf{v}) = \mathbf{v}$, $\mathbf{v} \in res(C^{\perp_R})$. Therefore, $tor(C)^{\perp} \subseteq res(C^{\perp_R})$. Thus we obtain $res(C^{\perp_R}) = tor(C)^{\perp}$.
To prove (3), we need to show that $\mathbb{F}_2^n \subseteq tor(C^{\perp_R})$. Let $\mathbf{u} \in \mathbb{F}_2^n$ and $\mathbf{c} \in C$. By Theorem 8, $\mathbf{c} = a\mathbf{x} + c\mathbf{y}$ where $\mathbf{x} \in res(C)$ and $\mathbf{y} \in tor(C)$. Observe that

$$\mathbf{c} \cdot c\mathbf{u} = (a\mathbf{x} + c\mathbf{y}) \cdot c\mathbf{u} = 0.$$

Hence, $c\mathbf{u} \in C^{\perp_R}$ and so $\mathbf{u} \in tor(C^{\perp_R})$. Therefore, $\mathbb{F}_2^n = tor(C^{\perp_R})$. □

Corollary 2. *If C is a linear code of length n over E, then the following hold:*

(1) $C^{\perp_L} = a\, res(C)^{\perp} \oplus c\, res(C)^{\perp}$.

(2) $C^{\perp_R} = a\, tor(C)^{\perp} \oplus c\, \mathbb{F}_2^n$.

Proof. The result follows immediately from Theorems 8 and 10. □

Recall that a linear code C over E is nice if $|C||C^{\perp_L}| = |C||C^{\perp_R}| = 4^n$ [3]. This leads to the following result.

Proposition 5. *The only nice code over E is the zero code.*

Proof. Suppose that C is a type (k_1, k_2) nice code of length n over E. By definition and Corollary 2,

$$4^n = |C||C^{\perp_L}| = 2^{2n+k_2} \quad \text{and} \quad 4^n = |C||C^{\perp_R}| = 2^{2n+k_1}.$$

The first equation is true if and only if $k_2 = 0$ and the second equation is true if and only if $k_1 = 0$. Hence, the only nice code over E is the zero code. □

Proposition 6. *If C is a nonzero linear code of length n over E, then $C^{\perp_R} \neq C^{\perp_L}$.*

Proof. Suppose that $C^{\perp_R} = C^{\perp_L}$. By Corollary 2, $tor(C)^{\perp} = res(C)^{\perp} = \mathbb{F}_2^n$ which implies that $tor(C) = res(C) = \{\mathbf{0}\}$ and so C is zero. □

This shows that no self-dual codes over E, as defined in [3], exist. This motivates us to modify the condition of such codes. Thus we define the two-sided dual of a code over E and redefine the self-duality accordingly as follows.

Definition 1. Let C be a linear code over E.

- The **two-sided dual** of C, denoted by $C^{\perp}$, is defined as $C^{\perp} = C^{\perp_L} \cap C^{\perp_R}$.
- C is **self-dual** provided that $C = C^{\perp}$.

Similar to Theorem 10, the following theorem gives properties on the residue and torsion codes of the two-sided dual of linear codes over E.

Theorem 11. *If C is a linear code of length n over E, then the following hold:*

(1) $res(C^{\perp}) = tor(C)^{\perp}$.

(2) $tor(C^{\perp}) = res(C)^{\perp}$.

Proof. By Theorem 10 and the fact that $res(C) \subseteq tor(C)$, it follows that

$$res(C^{\perp}) = res(C^{\perp_L} \cap C^{\perp_R}) = res(C^{\perp_L}) \cap res(C^{\perp_R}) = res(C)^{\perp} \cap tor(C)^{\perp} = tor(C)^{\perp}.$$

Also by Theorem 10, we obtain

$$tor(C^{\perp}) = tor(C^{\perp_L} \cap C^{\perp_R}) = tor(C^{\perp_L}) \cap tor(C^{\perp_R}) = res(C)^{\perp} \cap \mathbb{F}_2^n = res(C)^{\perp}.$$ □

Corollary 3. *If C is a linear code over E, then $C^{\perp} = a\, tor(C)^{\perp} \oplus c\, res(C)^{\perp}$.*

Proof. By Theorems 8 and 11,

$$C^{\perp} = a\, res(C^{\perp}) \oplus c\, tor(C^{\perp}) = a\, tor(C)^{\perp} \oplus c\, res(C)^{\perp}.$$ □

Corollary 4. *If C is a linear code over E, then $(C^{\perp})^{\perp} = C$.*

Proof. By Theorem 11 and Corollary 3,

$$(C^{\perp})^{\perp} = a\, tor(C^{\perp})^{\perp} \oplus c\, res(C^{\perp})^{\perp} = a\, res(C) \oplus c\, tor(C) = C.$$ □

Corollary 5. *If C is a linear code of length n over E, then $|C||C^{\perp}| = 4^n$.*

Proof. By Theorem 8 and Corollary 3,

$$|C||C^{\perp}| = |\,res(C)||\,tor(C)||\,res(C)^{\perp}||\,tor(C)^{\perp}| = 4^n. \qquad \square$$

Corollary 6. *Let C be a linear code of length n over E. The following are equivalent:*

(i) *C is free.*

(ii) *C is left nice.*

(iii) *$C^{\perp} = C^{\perp_L}$.*

Proof. By Theorem 8 and Corollary 2, $|C||C^{\perp_L}| = 2^{2n+k_2}$. Hence, C is free if and only if C is left nice; proving that (i) and (ii) are equivalent. By Corollaries 2 and 3, $C^{\perp} = C^{\perp_L}$ if and only if $tor(C)^{\perp} = res(C)^{\perp}$ or equivalently C is free; hence (i) and (iii) are equivalent. $\square$

Corollary 7. *Let C be a linear code of length n over E. Then $C^{\perp} = C^{\perp_R}$ if and only if $res(C) = \{\mathbf{0}\}$.*

Proof. By Corollaries 2 and 3, $C^{\perp} = C^{\perp_R}$ if and only if $res(C)^{\perp} = \mathbb{F}_2^n$ or equivalently $res(C) = \{\mathbf{0}\}$. $\square$

To prepare for investigating the MacWilliams formula for linear codes over E, we recall from [6, 11] that the *weight enumerator* of any linear or additive code C is the polynomial $W(x, y) = \sum_{i=0}^{n} A_i x^{n-j} y^j$ where the sequence $A_0, \ldots, A_n$ is the *weight distribution* of C. That is, A_i is the number of codewords in C of weight i. We state the following useful theorem without proof.

Theorem 12. [6, Theorem 5]. *If C is an $(n, 2^k)$ additive code over $\mathbb{F}_4$ with weight enumerator $W(x, y)$, the weight enumerator of the trace dual code $C^{\perp_T}$ is given by $2^{-k}W(x+3y, x-y)$.*

To establish the MacWilliams formula for linear codes over E, we also need the following identity.

Theorem 13. *If C is a linear code of length n over E, then $\phi_E(C^{\perp}) = \phi_E(C)^{\perp_T}$.*

Proof. Let $\phi_E(\mathbf{y}) \in \phi_E(C^{\perp})$ and $\phi_E(\mathbf{x}) \in \phi_E(C)$. By Corollary 3 and Theorem 8, $\mathbf{y} = a\mathbf{u} + c\mathbf{v}$ and $\mathbf{x} = a\mathbf{r} + c\mathbf{t}$ such that $\mathbf{u} \in tor(C)^{\perp}, \mathbf{v} \in res(C)^{\perp}, \mathbf{r} \in res(C)$, and $\mathbf{t} \in tor(C)$. Observe that

$$\begin{aligned}
\langle \phi_E(\mathbf{x}), \phi_E(\mathbf{y}) \rangle_T &= \mathrm{Tr}(\phi_E(\mathbf{x}) \cdot (\phi_E(\mathbf{y}))^2) \\
&= \mathrm{Tr}(\phi_E(a\mathbf{r} + c\mathbf{t}) \cdot (\phi_E(a\mathbf{u} + c\mathbf{v}))^2) \\
&= \mathrm{Tr}((\omega\mathbf{r} + \mathbf{t}) \cdot (\omega\mathbf{u} + \mathbf{v})^2) \\
&= \mathrm{Tr}((\omega\mathbf{r} + \mathbf{t}) \cdot (\omega^2\mathbf{u} + \mathbf{v})) \\
&= \mathrm{Tr}(\mathbf{r} \cdot \mathbf{u} + \omega\mathbf{r} \cdot \mathbf{v} + \omega^2\mathbf{t} \cdot \mathbf{u} + \mathbf{t} \cdot \mathbf{v}) \\
&= \mathbf{r} \cdot \mathbf{v} + \mathbf{t} \cdot \mathbf{u} \\
&= 0.
\end{aligned}$$

This proves that $\phi_E(C^{\perp}) \subseteq \phi_E(C)^{\perp_T}$. Since $|\phi_E(C^{\perp})| = |C^{\perp}| = 2^{2n-(2k_1+k_2)} = |\phi_E(C)^{\perp_T}|$, it follows that $\phi_E(C^{\perp}) = \phi_E(C)^{\perp_T}$. $\square$

Theorem 14. *If C is a linear code of type (k_1, k_2) over E with weight enumerator $W_C(x, y)$, then the weight enumerator of the dual code $C^{\perp}$ is given by*

$$W_{C^{\perp}}(x, y) = \frac{1}{2^{(2k_1+k_2)}} W_C(x + 3y, x - y).$$

Proof. Since C is a linear code of type (k_1, k_2) over E, $\phi_E(C)$ is an $(n, 2^{2k_1+k_2})$ additive code over $\mathbb{F}_4$ with $W_C(x,y) = W_{\phi_E(C)}(x,y)$ and $W_{C^\perp}(x,y) = W_{\phi_E(C^\perp)}(x,y) = W_{\phi_E(C)^{\perp_T}}(x,y)$, by Theorem 13. Hence, by Theorem 12,

$$W_{C^\perp}(x,y) = \frac{1}{2^{(2k_1+k_2)}} W_C(x+3y, x-y). \qquad \square$$

4.2.1 Self-dual codes

The following two theorems characterize (one-sided) self-dual codes over E.

Theorem 15. *If C is a linear code of length n over E, then the following hold:*

(1) *C is left self-dual if and only if C is free and $res(C)$ is self-dual.*

(2) *C is right self-dual if and only if C is of type $(0, n)$.*

Proof. We use Theorem 8 and Corollary 2 to establish the results. Observe that $C = C^{\perp_L}$ if and only if $res(C) = res(C)^\perp = tor(C)$. Thus (1) holds. Now observe that $C = C^{\perp_R}$ if and only if $res(C) = tor(C)^\perp$ and $tor(C) = \mathbb{F}_2^n$. Equivalently, $C = C^{\perp_R}$ if and only if $res(C) = \{\mathbf{0}\}$ and $tor(C) = \mathbb{F}_2^n$. Thus (2) now follows. $\square$

Theorem 16. *A linear code C over E is self-dual if and only if $res(C) = tor(C)^\perp$.*

Proof. The result follows immediately from Theorem 8 and Corollary 3. $\square$

Remark 2. In view of Definition 1, the notions of QSD codes and self-dual codes over E are equivalent. To see this, suppose that C is a QSD code of length n. Then $C \subseteq C^\perp$ and $|C| = 2^n$. By Corollary 5, $|C^\perp| = 4^n/2^n = 2^n = |C|$. Hence, $C = C^\perp$ and therefore C is self-dual. Conversely, if C is a self-dual code of length n, then $C = C^\perp$ and $|C| = |C^\perp|$. By Corollary 5, $|C|^2 = 4^n$. Hence $|C| = 2^n$ and therefore C is QSD.

Corollary 8. *Let C be a linear code of length n over E. If C is either left self-dual or right self-dual, then C is self-dual.*

Proof. If C is left self-dual, then by Theorem 15, $res(C) = res(C)^\perp = tor(C)$. In particular, $res(C) = tor(C)^\perp$. By Theorem 16, C is self-dual.
If C is right self-dual, then by Theorem 15, $res(C) = \{\mathbf{0}\}$ and $tor(C) = \mathbb{F}_2^n$ which imply that $res(C) = tor(C)^\perp$. By Theorem 16, C is self-dual. $\square$

The converse of Corollary 8 is not true in general as the following examples show.

Example 2. The repetition code of length 2 defined by $C = \{00, aa, bb, cc\}$ is self-dual and left self-dual but not right self-dual.

- The left dual of C is $C^{\perp_L} = C$.
- The right dual of C is $C^{\perp_R} = \{00, aa, bb, cc, ab, ba, 0c, c0\}$.
- The two-sided dual of C is $C^\perp = C$.

Example 3. The linear code defined by $C = \{00, 0c, c0, cc\}$ is self-dual and right self-dual but not left self-dual.

- The left dual of C is $C^{\perp_L} = E^2$.
- The right dual of C is $C^{\perp_R} = C$.
- The two-sided dual of C is $C^\perp = C$.

Example 4. The linear code defined by $C = \{000, a0a, b0b, c0c, 0c0, ccc, aca, bcb\}$ is self-dual but neither left self-dual nor right self-dual.

- The left dual of C is $C^{\perp_L} = \{000, a0a, 0a0, aaa, b0b, 0b0, bbb, c0c, 0c0, ccc, aba, aca, bcb, bab, cac, cbc\}$.
- The right dual of C is $C^{\perp_R} = \{000, a0a, b0b, c00, 0c0, 00c, cc0, c0c, 0cc, ccc, b0a, aca, a0b, bca, acb, bcb\}$.
- The two-sided dual of C is $C^{\perp} = C$.

From Theorem 15 it follows that for each positive integer n, the linear code $c\,\mathbb{F}_2^n$ is the unique right self-dual code of length n over E. To classify left self-dual codes, we need the following theorem.

Theorem 17. *Two free codes over E are permutation equivalent if and only if their residue codes are permutation equivalent.*

Proof. Let C and C' be two permutation equivalent codes over E. Then there is a permutation matrix P such that $C' = CP$. Since $\alpha(C') = \alpha(CP) = \alpha(C)P$, it follows that $res(C)$ and $res(C')$ are permutation equivalent.
Conversely, suppose that C and C' are free codes over E where $res(C)$ and $res(C')$ are permutation equivalent. By Theorem 8 and the freeness of the codes, $C = a\,res(C) \oplus c\,res(C)$ and $C' = a\,res(C') \oplus c\,res(C')$. As $res(C)$ and $res(C')$ are permutation equivalent, there is a permutation matrix P such that $res(C') = res(C)P$. Thus, we have

$$C' = a\,res(C') \oplus c\,res(C') = a\,res(C)P \oplus c\,res(C)P = CP$$

which proves that C and C' are permutation equivalent. □

The following example shows that Theorem 17 may not hold if the codes are not free.

Example 5. The linear codes C and C' with generator matrices

$$\begin{pmatrix} a & a & 0 \\ 0 & c & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} a & 0 & a \\ 0 & c & 0 \end{pmatrix},$$

respectively, have residue codes $res(C) = \{000, 110\}$ and $res(C') = \{000, 101\}$ which are permutation equivalent. However, C and C' are not permutation equivalent as they have weight distributions $[< 0, 1 >, < 1, 2 >, < 2, 5 >]$ and $[< 0, 1 >, < 1, 1 >, < 2, 3 >, < 3, 3 >]$, respectively. Note that C and C' are not free.

As all left-self dual codes over E are necessarily free codes by Theorem 15, the following corollary is a special case of Theorem 17.

Corollary 9. *Two left self-dual codes over E are permutation equivalent if and only if their residue codes are permutation equivalent.*

Similar to the case of self-dual codes over I, using the classification of self-dual binary codes along with Theorem 15, the classification of all left self-dual codes over E of the same lengths is immediate.

To conclude this subsection, we note that the image of any self-dual or one-sided self-dual code over E under the map ϕ_E is an additive trace self-dual code over $\mathbb{F}_4$.

Corollary 10. *If C is a self-dual code over E, then $\phi_E(C)$ is trace self-dual.*

Proof. The result follows immediately from Theorem 13. □

Corollary 11. *If C is a left self-dual code over E, then $\phi_E(C)$ is trace self-dual.*

Proof. By Theorem 15, C is free. By Corollary 6, $C^{\perp} = C^{\perp_L}$ and thus C is self-dual. By Corollary 10, $\phi_E(C)$ is trace self-dual. □

Corollary 12. *If C is a right self-dual code of length n over E, then $\phi_E(C)$ is trace self-dual.*

Proof. By Theorem 15, $C = c\,\mathbb{F}_2^n$ and thus $\phi_E(C) = \mathbb{F}_2^n$ which is an additive trace self-dual code over $\mathbb{F}_4$. □

The converse of the preceding three corollaries is not true in general. The $(12, 2^{12}, 6)$ dodecacode D is trace self-dual [6] but $\phi_E^{-1}(D)$ is not a linear code over E [3, Example 2].

4.2.2 LCD codes

The study of LCD codes over non-unital rings first appeared in [19] where the authors investigated left LCD codes over E and defined this notion as follows:

Definition 2. A code C over E is **left linear with complementary dual (left LCD)** if it is left nice and $C \cap C^{\perp_L} = \{\mathbf{0}\}$.

We define LCD codes over E where $C^{\perp} = C^{\perp_L} \cap C^{\perp_R}$ as follows:

Definition 3. A code C over E is **linear with complementary dual (LCD)** if $C \cap C^{\perp} = \{\mathbf{0}\}$.

LCD codes over E can be characterized via their residue and torsion codes as in the following theorem.

Theorem 18. *Let C be a linear code over E. Then the following hold:*

(1) *If C is LCD, then $res(C)$ and $tor(C)$ are binary LCD codes.*

(2) *If C is free and $res(C)$ is a binary LCD code, then C is LCD.*

Proof. First assume that C is an LCD code over E. By definition, $C \cap C^{\perp} = \{\mathbf{0}\}$. By Theorem 8 and Corollary 3, $res(C) \cap tor(C)^{\perp} = \{\mathbf{0}\}$ and $tor(C) \cap res(C)^{\perp} = \{\mathbf{0}\}$. Suppose that $\mathbf{x} \in res(C) \cap res(C)^{\perp}$. Since $res(C) \subseteq tor(C)$, $\mathbf{x} \in tor(C) \cap res(C)^{\perp}$. Hence, $\mathbf{x} = \mathbf{0}$ which implies that $res(C)$ is LCD. Similarly, suppose that $\mathbf{x} \in tor(C) \cap tor(C)^{\perp}$. Since $tor(C)^{\perp} \subseteq res(C)^{\perp}$, $\mathbf{x} \in tor(C) \cap res(C)^{\perp}$. Hence, $\mathbf{x} = \mathbf{0}$ which implies that $tor(C)$ is LCD. This proves (1).
Now assume that $res(C)$ is LCD and C is free. Then we have $res(C) \cap res(C)^{\perp} = \{\mathbf{0}\}$ and $res(C) = tor(C)$. In particular, $res(C) \cap tor(C)^{\perp} = \{\mathbf{0}\}$ and $tor(C) \cap res(C)^{\perp} = \{\mathbf{0}\}$. By Theorem 8 and Corollary 3, $C \cap C^{\perp} = \{\mathbf{0}\}$ and so C is LCD. This proves (2). □

For free codes over E, there is no distinction between LCD and left LCD codes.

Theorem 19. *A linear code over E is left LCD if and only if it is LCD and free.*

Proof. Suppose that C is left LCD. By definition, C is left nice and $C \cap C^{\perp_L} = \{\mathbf{0}\}$. By Corollary 6, C is free. By definition of $C^{\perp}$, $C \cap C^{\perp} \subseteq C \cap C^{\perp_L}$. This implies that C is LCD. For the converse, suppose that C is LCD and free. By Corollary 6, C is left nice and $C \cap C^{\perp_L} = C \cap C^{\perp} = \{\mathbf{0}\}$. Hence C is left LCD. □

The following simple examples illustrate Theorems 18 and 19.

Example 6. The linear code defined by $C = \{00, a0, b0, c0\}$ is LCD and left LCD.

- The left dual of C is $C^{\perp_L} = \{00, 0a, 0b, 0c\}$.
- The two-sided dual of C is $C^{\perp} = \{00, 0a, 0b, 0c\}$.

The binary code $res(C) = \{00, 10\}$ is LCD and C is free as $tor(C) = res(C)$.

Example 7. The linear code defined by $C = \{00, a0, b0, c0, 0c, cc, bc, ac\}$ is neither LCD nor left LCD.

- The left dual of C is $C^{\perp_L} = \{00, 0a, 0b, 0c\}$.
- The two-sided dual of C is $C^{\perp} = \{00, 0c\}$.

The binary codes $res(C) = \{00, 10\}$ and $tor(C) = \{00, 10, 01, 11\}$ are LCD. However, C is not free.

In the next results we investigate the LCD property of the dual of LCD codes over E.

Corollary 13. *If C is an LCD code over E, then $C^{\perp}$ is LCD.*

Proof. The result follows immediately from Corollary 4 and the definition of LCD codes. □

Corollary 14. *If C is a free LCD code over E, then $C^{\perp_L}$ is LCD.*

Proof. By Corollary 6, since C is free, C is left nice and $C^{\perp_L} = C^{\perp}$. Since C is LCD, $C^{\perp}$ is LCD by Corollary 13. Thus, $C^{\perp_L}$ is LCD. □

Corollary 15. *If C is a nonzero linear code of length n over E, then $C^{\perp_R}$ is not LCD.*

Proof. By Theorem 10 and Corollary 3,

$$(C^{\perp_R})^{\perp} = a\, tor(C^{\perp_R})^{\perp} \oplus c\, res(C^{\perp_R})^{\perp} = c\, tor(C) \subseteq c\,\mathbb{F}_2^n \subseteq C^{\perp_R}$$

where the last inclusion follows from Corollary 2. Since C is nonzero, $tor(C)$ must also be nonzero and thus $C^{\perp_R} \cap (C^{\perp_R})^{\perp} \neq \{\mathbf{0}\}$. This proves that $C^{\perp_R}$ is not LCD. □

The image of any LCD or left LCD code over E under the map ϕ_E is an ACD.

Corollary 16. *If C is an LCD code over E, then $\phi_E(C)$ is ACD.*

Proof. Since C is an LCD code over E and ϕ_E is a bijective map,

$$\{\mathbf{0}\} = \phi_E(\{\mathbf{0}\}) = \phi_E(C \cap C^{\perp}) = \phi_E(C) \cap \phi_E(C^{\perp}) = \phi_E(C) \cap \phi_E(C)^{\perp_T}$$

where the last equality follows from Theorem 13. □

Corollary 17. *If C is a left LCD code over E, then $\phi_E(C)$ is ACD.*

Proof. By Theorem 19, C is LCD. By Corollary 16, $\phi_E(C)$ is ACD. □

The converse of Corollaries 16 and 17 are not true in general as the next example shows.

Example 8. Let D be the $(4, 2^4)$ additive code over $\mathbb{F}_4$ with generator matrix

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ \omega & \omega & 0 & \omega \\ 0 & \omega & \omega & \omega \end{pmatrix}.$$

Then D is ACD [20, Example 2]. The residue and the torsion codes of C over E where $\phi_E(C) = D$ are $res(C) = \{0000, 1101, 0111, 1010\}$ and $tor(C) = \{0000, 1100, 0011, 1111\}$. Since $res(C) \not\subseteq tor(C)$, C is not linear and thus not LCD.

Recall that an additive code D over $\mathbb{F}_4$ is ACD if $D \cap D^{\perp_T} = \{\mathbf{0}\}$.

Theorem 20. [20, Theorem 3]. *If C is an $(n, 2^k)$ ACD code over $\mathbb{F}_4$, then k is even.*

Corollary 18. *If C is a type (k_1, k_2) LCD code over E, then k_2 is even.*

Proof. By Corollary 16, $\phi_E(C)$ is an $(n, 2^{2k_1+k_2})$ ACD code over $\mathbb{F}_4$. By Theorem 20, $2k_1+k_2$ is even which yields that k_2 is even. □

Remark 3. We restrict our investigation in this section on LCD and left LCD codes over E without mentioning right LCD codes since there are no such codes over E, as shown in [19, Remark 1].

5 Results on linear codes over H

We begin this section by summarizing facts and notions essential to our study for linear codes over H. A detailed introduction on such codes can be found in [1].

To every linear code C of length n over H, there is an additive code $\phi_H(C)$ over $\mathbb{F}_4$ such that ϕ_H is defined by the alphabet substitution

$$0 \to 0,\ a \to \omega,\ b \to 1,\ c \to \omega^2,$$

extended in the natural way to a map from C to $\mathbb{F}_4^n$.

There are two binary linear codes, namely C_a and C_b, of length n associated canonically with every linear code C of length n over H;

(1) $C_a = \alpha_b(C)$ where $\alpha_b : H \to \mathbb{F}_2$ is the map defined by $\alpha_b(0) = \alpha_b(b) = 0$ and $\alpha_b(a) = \alpha_b(c) = 1$, extended componentwise from C to $\mathbb{F}_2^n$,

(2) $C_b = \alpha_a(C)$ where $\alpha_a : H \to \mathbb{F}_2$ is the map defined by $\alpha_a(0) = \alpha_a(a) = 0$ and $\alpha_a(b) = \alpha_a(c) = 1$, extended componentwise from C to $\mathbb{F}_2^n$.

Any linear code C over H can be written as $C = aC_a \oplus bC_b$.

5.1 Structure of linear codes

Due to the fact that the two binary codes C_a and C_b associated to any linear code C over H are not necessarily related to each other, the minimum distance of C depends on the minimum distances of both binary codes.

Theorem 21. *Let $C = aC_a \oplus bC_b$ be a linear code over H where C_a and C_b are nonzero binary codes. The minimum distance d of C is $d = \min\{d_1, d_2\}$ where d_1 and d_2 are the minimum distances of C_a and C_b, respectively.*

Proof. Since d_1 and d_2 are the minimum distances of C_a and C_b, respectively, there exist nonzero binary vectors $\mathbf{u} \in C_a$ and $\mathbf{v} \in C_b$ such that $\mathrm{wt}(\mathbf{u}) = d_1$ and $\mathrm{wt}(\mathbf{v}) = d_2$. Since $aC_a \subseteq C$ and $bC_b \subseteq C$, it follows that $a\mathbf{u}, b\mathbf{v} \in C$ with $\mathrm{wt}(a\mathbf{u}) = \mathrm{wt}(\mathbf{u}) = d_1$ and $\mathrm{wt}(b\mathbf{v}) = \mathrm{wt}(\mathbf{v}) = d_2$. This means that $d \leq \min\{d_1, d_2\}$.
Now we prove that $d \geq \min\{d_1, d_2\}$. Let $\mathbf{w} \in C$ such that $\mathrm{wt}(\mathbf{w}) = d$. Then, $\mathbf{w} = a\mathbf{x} + b\mathbf{y}$ where $\mathbf{x} \in C_a$ and $\mathbf{y} \in C_b$. Since C is nonzero, we have the following three cases depending on $\mathbf{x}$ and $\mathbf{y}$:

- If $\mathbf{x} = \mathbf{0}$ and $\mathbf{y} \neq \mathbf{0}$, then $\mathrm{wt}(\mathbf{w}) = \mathrm{wt}(b\mathbf{y}) = \mathrm{wt}(\mathbf{y}) \geq d_2 \geq \min\{d_1, d_2\}$.
- If $\mathbf{x} \neq \mathbf{0}$ and $\mathbf{y} = \mathbf{0}$, then $\mathrm{wt}(\mathbf{w}) = \mathrm{wt}(a\mathbf{x}) = \mathrm{wt}(\mathbf{x}) \geq d_1 \geq \min\{d_1, d_2\}$.

- If $\mathbf{x}, \mathbf{y} \neq \mathbf{0}$, then $\mathrm{wt}(\mathbf{w}) \geq \mathrm{wt}(b\mathbf{w}) = \mathrm{wt}(b\mathbf{y}) = \mathrm{wt}(\mathbf{y}) \geq d_2 \geq \min\{d_1, d_2\}$.

In all cases, $d = \mathrm{wt}(\mathbf{w}) \geq \min\{d_1, d_2\}$.
Since $d \leq \min\{d_1, d_2\}$ and $d \geq \min\{d_1, d_2\}$, it follows that $d = \min\{d_1, d_2\}$. □

The following result shows the relationship between the permutation equivalence of two linear codes over H and that of their constituents.

Theorem 22. *Let $C = aC_a \oplus bC_b$ and $C' = aC'_a \oplus bC'_b$ be two linear codes over H. Then C and C' are permutation equivalent if and only if there is a permutation which sends (C_a, C_b) to (C'_a, C'_b).*

Proof. Let C and C' be two permutation equivalent codes over H. Then there is a permutation matrix P such that $C' = CP$. Since $\alpha_a(C') = \alpha_a(CP) = \alpha_a(C)P$ and $\alpha_b(C') = \alpha_b(CP) = \alpha_b(C)P$, it follows that P sends (C_a, C_b) to (C'_a, C'_b).
Conversely, suppose that P is a permutation matrix which sends (C_a, C_b) to (C'_a, C'_b). Then,

$$aC'_a \oplus bC'_b = aC_aP \oplus bC_bP$$

and thus $C' = CP$, proving that C and C' are permutation equivalent. □

5.2 Duality

To prepare for the study of self-dual and LCD codes over H, we need the following theorem.

Theorem 23. *If $C = aC_a \oplus bC_b$ is a linear code of length n over H, then $C^\perp = a\,\mathbb{F}_2^n \oplus bC_b^\perp$.*

Proof. Let $\mathbf{c} \in C^\perp$. We can write $\mathbf{c}$ as $\mathbf{c} = a\mathbf{u} + b\mathbf{v}$ where $\mathbf{u}, \mathbf{v} \in \mathbb{F}_2^n$. To prove that $\mathbf{v} \in C_b^\perp$, let $\mathbf{t} \in C_b$. As $bC_b \subseteq C$, $b\mathbf{t} \in C$. By definition,

$$0 = \mathbf{c} \cdot b\mathbf{t} = (a\mathbf{u} + b\mathbf{v}) \cdot b\mathbf{t} = b(\mathbf{v} \cdot \mathbf{t}).$$

Hence, $\mathbf{v} \cdot \mathbf{t} = 0$ which implies that $\mathbf{v} \in C_b^\perp$ and $\mathbf{c} \in a\,\mathbb{F}_2^n + bC_b^\perp$. Therefore, $C^\perp \subseteq a\,\mathbb{F}_2^n + bC_b^\perp$.
Now assume that $\mathbf{c} = a\mathbf{u} + b\mathbf{v} \in a\,\mathbb{F}_2^n + bC_b^\perp$. Let $\mathbf{w} \in C$. Then, $\mathbf{w} = a\mathbf{x} + b\mathbf{y}$ where $\mathbf{x} \in C_a$ and $\mathbf{y} \in C_b$. Observe that

$$\mathbf{c} \cdot \mathbf{w} = (a\mathbf{u} + b\mathbf{v}) \cdot (a\mathbf{x} + b\mathbf{y}) = b(\mathbf{v} \cdot \mathbf{y}) = 0.$$

Hence, $\mathbf{c} \in C^\perp$. Therefore, $a\mathbb{F}_2^n + bC_b^\perp \subseteq C^\perp$. This proves the equality $C^\perp = a\,\mathbb{F}_2^n + bC_b^\perp$. The sum is direct since $a\,\mathbb{F}_2^n$ and $bC_b^\perp$ have a trivial intersection. □

Corollary 19. *Let $C = aC_a \oplus bC_b$ be a linear code of length n over H. Then, $(C^\perp)^\perp = C$ if and only if $C_a = \mathbb{F}_2^n$.*

Proof. By Theorem 23, $(C^\perp)^\perp = a\,\mathbb{F}_2^n \oplus bC_b$. Hence, $(C^\perp)^\perp = C$ if and only if $C_a = \mathbb{F}_2^n$. □

Corollary 20. *Let $C = aC_a \oplus bC_b$ be a linear code of length n over H. Then, C is nice if and only if $C_a = \{\mathbf{0}\}$.*

Proof. Let k_a and k_b denote the dimensions of C_a and C_b, respectively. Then we have $|C| = |C_a||C_b| = 2^{k_a+k_b}$ and $|C^\perp| = |\,\mathbb{F}_2^n\,||C_b^\perp| = 2^{2n-k_b}$ from Theorem 23. Therefore, $|C||C^\perp| = 2^{2n+k_a}$. Hence, $|C||C^\perp| = 4^n$ if and only if $k_a = 0$. Equivalently, C is nice if and only if $C_a = \{\mathbf{0}\}$. □

5.2.1 Self-dual codes

We characterize self-dual codes over H through their additive components.

Theorem 24. *A linear code $C = aC_a \oplus bC_b$ of length n over H is self-dual if and only if the following two conditions are satisfied:*

(1) *C_b is a self-dual binary code,*

(2) *$C_a = \mathbb{F}_2^n$.*

Proof. The result follows immediately from Theorem 23 and the definition of self-dual codes. □

By Theorem 24, self-dual codes over H exist only for even lengths and there are as many self-dual codes of length n over H as there are $[n, n/2]$ binary self-dual codes.

Corollary 21. *Let $C = aC_a \oplus bC_b$ and $C' = aC'_a \oplus bC'_b$ be two self-dual codes over H. Then C and C' are permutation equivalent if and only if C_b and C'_b are permutation equivalent.*

Proof. The self-duality of C and C' imply that $C_a = C'_a = \mathbb{F}_2^n$ by Theorem 24. Thus, by Theorem 22, C and C' are permutation equivalent if and only if C_b and C'_b are permutation equivalent. □

From the preceding results, we see that there is a one-to-one correspondence between inequivalent self-dual binary codes and inequivalent self-dual codes over H of the same length. Similar to the case of self-dual codes over I, using the classification of self-dual binary codes along with Theorem 24, the classification of all self-dual codes over H of the same lengths is immediate. We remark that by Theorems 21 and 24, all self-dual codes over H have minimum distance equals 1.

The same observations on self-dual codes over I in Propositions 2 and 3 apply for self-dual codes over H as well.

Proposition 7. *Let $\mathcal{Q}$ be the family of all QSD codes of length n over H and let $\mathcal{S}$ be the family of all self-dual codes of length n over H. Then $\mathcal{Q} \cap \mathcal{S} = \emptyset$.*

Proof. Suppose that a linear code C over H is QSD and self-dual. Then $|C| = |C^\perp| = 2^n$ which implies that $|C||C^\perp| = 4^n$. By Corollary 20, $C_a = \{\mathbf{0}\}$ contradicting part (2) of Theorem 24. This means that a linear code over H can never simultaneously be both QSD and self-dual. □

Proposition 8. *If $C = aC_a \oplus bC_b$ is a self-dual code of length $2n$ over H, then $\phi_H(C)^{\perp_T}$ is trace self-orthogonal of size 2^n; in particular, $\phi_H(C)$ is not trace self-dual.*

Proof. By Theorems 23 and 24, the self-duality of C implies $|C_a| = |\mathbb{F}_2^{2n}| = 2^{2n}$ and $|C_b| = 2^n$. Then, $|\phi_H(C)| = |C| = 2^{3n}$ and $|\phi_H(C)^{\perp_T}| = 2^n$. Comparing cardinalities, we see that $\phi_H(C) \neq \phi_H(C)^{\perp_T}$ which shows that $\phi_H(C)$ is not trace self-dual.
We claim that $\omega C_b = \phi_H(C)^{\perp_T}$. Let $\mathbf{w} \in C_b$ and let $\mathbf{x} \in \phi_H(C)$. Then, $\omega\mathbf{w} \in \omega C_b$ and there exists a codeword $a\mathbf{u}+b\mathbf{v}$ in C where $\mathbf{u} \in C_a$ and $\mathbf{v} \in C_b$ such that $\mathbf{x} = \phi_H(a\mathbf{u}+b\mathbf{v}) = \omega\mathbf{u}+\mathbf{v}$. Observe that

$$\langle \mathbf{x}, \omega\mathbf{w} \rangle_T = \langle \omega\mathbf{u} + \mathbf{v}, \omega\mathbf{w} \rangle_T = \langle \omega\mathbf{u}, \omega\mathbf{w} \rangle_T + \langle \mathbf{v}, \omega\mathbf{w} \rangle_T = \mathrm{Tr}(\mathbf{u} \cdot \mathbf{w}) + \mathrm{Tr}(\omega^2\mathbf{v} \cdot \mathbf{w}).$$

Since C is self-dual, by Theorem 24, C_b is self-dual and therefore $\mathbf{v} \cdot \mathbf{w} = 0$ which gives $\mathrm{Tr}(\omega^2\mathbf{v}\cdot\mathbf{w}) = 0$. As $\mathbf{u}\cdot\mathbf{w} \in \{0, 1\}$, $\mathrm{Tr}(\mathbf{u}\cdot\mathbf{w}) = 0$. Thus, we obtain $\langle \mathbf{x}, \omega\mathbf{w} \rangle_T = 0$ proving that $\omega\mathbf{w} \in \phi_H(C)^{\perp_T}$ and consequently $\omega C_b \subseteq \phi_H(C)^{\perp_T}$. The fact that $|C_b| = 2^n = |\phi_H(C)^{\perp_T}|$ implies that $\omega C_b = \phi_H(C)^{\perp_T}$ as claimed. Now observe that since $C_b \subseteq \mathbb{F}_2^{2n} = C_a$, we have $aC_b \subseteq aC_a \subseteq C$ and thus $\omega C_b = \phi_H(aC_b) \subseteq \phi_H(C)$. In particular, $\phi_H(C)^{\perp_T} \subseteq \phi_H(C)$ which proves that $\phi_H(C)^{\perp_T}$ is trace self-orthogonal. □

5.2.2 LCD codes

We define LCD codes over H as follows:

Definition 4. A code C over H is **linear with complementary dual (LCD)** if $C \cap C^{\perp} = \{\mathbf{0}\}$.

The following theorem provides a characterization of LCD codes over H.

Theorem 25. *A linear code $C = aC_a \oplus bC_b$ of length n over H is LCD if and only if C is nice and C_b is LCD.*

Proof. Suppose that C is LCD. By definition, $C \cap C^{\perp} = \{\mathbf{0}\}$. By Theorem 23, $C_a \cap \mathbb{F}_2^n = \{\mathbf{0}\}$ and $C_b \cap C_b^{\perp} = \{\mathbf{0}\}$, proving that C_a is zero and C_b is LCD. By Corollary 20, C is nice and C_b is LCD.
Conversely, suppose that C is nice and C_b is LCD. By Corollary 20, C_a is zero. Thus, $C_a \cap \mathbb{F}_2^n = \{\mathbf{0}\}$ and $C_b \cap C_b^{\perp} = \{\mathbf{0}\}$. By Theorem 23, $C \cap C^{\perp} = \{\mathbf{0}\}$, proving that C is LCD. □

Corollary 22. *Let $C = aC_a \oplus bC_b$ and $C' = aC'_a \oplus bC'_b$ be two LCD codes over H. Then C and C' are permutation equivalent if and only if C_b and C'_b are permutation equivalent.*

Proof. Since C and C' are LCD, by Theorem 25, $C_a = C'_a = \{\mathbf{0}\}$. Thus, by Theorem 22, C and C' are permutation equivalent if and only if C_b and C'_b are permutation equivalent. □

The classification of LCD codes over H reduces to that of LCD binary codes. A complete classification of binary LCD codes was done in [5] for lengths up to 13. Using this classification along with Theorem 25, the classification of all LCD codes over H of the same lengths is immediate.

To conclude this subsection, we note that the image of any LCD code over H under the map ϕ_H is never an ACD. However, it is an additive trace self-orthogonal code over $\mathbb{F}_4$.

Proposition 9. *If $C = aC_a \oplus bC_b$ is a nonzero LCD code of length n over H, then $\phi_H(C)$ is trace self-orthogonal; in particular, $\phi_H(C)$ is not ACD.*

Proof. By Theorem 25 and Corollary 20, $C = bC_b$. Then, $\phi_H(C) = \phi_H(bC_b) = C_b$ and so $\phi_H(C)^{\perp_T} = C_b^{\perp_T}$. Observe that for any $\mathbf{x}, \mathbf{y} \in C_b$, $\langle \mathbf{x}, \mathbf{y} \rangle_T = \mathrm{Tr}(\mathbf{x} \cdot \mathbf{y}^2) = \mathrm{Tr}(\mathbf{x} \cdot \mathbf{y}) = 0$. This proves that $C_b \subseteq C_b^{\perp_T}$ and $\phi_H(C) \subseteq \phi_H(C)^{\perp_T}$. Hence, $\phi_H(C)$ is trace self-orthogonal. Since C is nonzero, $\phi_H(C) \cap \phi_H(C)^{\perp_T} \neq \{\mathbf{0}\}$, proving that $\phi_H(C)$ is not ACD. □

6 Conclusion

In the present paper we have aimed to lay down the theoretical foundation of the duality of codes over three non unitary rings of order four. The classes of self-orthogonal, self-dual, quasi self-dual, and LCD codes have been considered for each ring in turn. The properties of their residue and torsion codes, as well as that of their quaternary images have been established.

The main direction opened by this study is to extend these results to non-unitary rings of higher order. In particular self-orthogonal codes over certain non-unitary rings of order 6 have been studied in [4]. This is a concrete motivation for such an extension.

References

[1] Alahmadi, A., Alkathiry, A., Altassan, A., Basaffar, W., Bonnecaze, A., Shoaib, H., and Solé, P. (2020). Type IV codes over a non-local non-unital ring. Proyecciones (Antofagasta), 39(4), 963-978.

[2] Alahmadi, A., Altassan, A., Basaffar, W., Bonnecaze, A., Shoaib, H., and Solé, P. (2021). Quasi Type IV codes over a non-unital ring. Applicable Algebra in Engineering, Communication and Computing, 32(3), 217-228.

[3] Alahmadi, A., Altassan, A., Basaffar, W., Shoaib, H., Bonnecaze, A., and Solé, P. (2022). Type IV codes over a non-unital ring. Journal of Algebra and Its Applications, 21(07), 2250142.

[4] Adel Alahmadi, Amani Alkathiry, Alaa Altassan, Widyan Basaffar, Alexis Bonnecaze, Hatoon Shoaib, Patrick Solé, Quasi self-dual codes over non-unital rings of order six, vol. 39, N. 4, Proyecciones (2020) (Antofagasta), 1083–1095.

[5] Araya, M. and Harada, M. (2019). On the classification of linear complementary dual codes. Discrete Mathematics, 342(1), 270-278.

[6] Calderbank, A. R., Rains, E. M., Shor, P. M., and Sloane, N. J. (1998). Quantum error correction via codes over $GF(4)$. IEEE Transactions on Information Theory, 44(4), 1369-1387.

[7] C. Carlet, S. Guilley, Complementary Dual Codes for Counter-measures to Side-Channel Attacks. IACR Cryptol. ePrint Arch. 2015: 603 (2015)

[8] Fine, B. (1993). Classification of finite rings of order p^2. Mathematics magazine, 66(4), 248-252.

[9] Huffman, W. C. (2005). On the classification and enumeration of self-dual codes. Finite Fields and Their Applications, 11(3), 451-490.

[10] W. Cary Huffman, J-L. Kim, P. Solé, *Concise Encyclopedia of Coding Theory*, CRC Press (2021).

[11] MacWilliams, F. J. and Sloane, N. J. A. (1977). *The theory of error correcting codes* (Vol. 16). Elsevier.

[12] Massey, J. L. (1992). Linear codes with complementary duals. Discrete Mathematics, 106, 337-342.

[13] G. Nebe, E.M. Rains, N.J.A. Sloane, *Self-dual codes and invariant theory*, Alg. and Comp. in Math (Vol. 17), Springer, (2006).

[14] Pless, V. (1972). A classification of self-orthogonal codes over $GF(2)$. Discrete Mathematics, 3(1-3), 209-246.

[15] Pless, V., Brualdi, R. A., and Huffman, W. C. (1998). *Handbook of coding theory*. Elsevier Science Inc.

[16] Pless, V. and Sloane, N. J. (1975). On the classification and enumeration of self-dual codes. Journal of Combinatorial Theory, Series A, 18(3), 313-335.

[17] Raghavendran, R. (1969). Finite associative rings. Compositio Mathematica, 21(2), 195-229.

[18] Shi, M., Alahmadi, A., and Solé, P. *Codes and Rings: Theory and Practice*, North-Holland (2017).

[19] Shi, M., Li, S., Kim, J. L., and Solé, P. (2022). LCD and ACD codes over a noncommutative non-unital ring with four elements. Cryptography and Communications, 14(3), 627-640.

[20] Shi, M., Liu, N., Kim, J. L., and Solé, P.(2022). Additive complementary dual codes over $\mathbb{F}_4$. Designs, Codes and Cryptography, 1-12. https://arxiv.org/pdf/2207.01938.pdf