Mass Formula for Self-Orthogonal and Self-Dual Codes over Non-Unital Rings of Order Four

Adel Alahmadi, Altaf Alshuhail, Rowena Alma Betty, Lucky Galvez, Patrick Solé

▶ **To cite this version:**

Adel Alahmadi, Altaf Alshuhail, Rowena Alma Betty, Lucky Galvez, Patrick Solé. Mass Formula for Self-Orthogonal and Self-Dual Codes over Non-Unital Rings of Order Four. Mathematics , 2023, 11, pp.4736. 10.3390/math11234736 . hal-04301756

HAL Id: hal-04301756
https://hal.science/hal-04301756v1

Submitted on 23 Nov 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

mathematics

MDPI

Article

Mass Formula for Self-Orthogonal and Self-Dual Codes over Non-Unital Rings of Order Four

Adel Alahmadi [1,*], Altaf Alshuhail [1,2], Rowena Alma Betty [3], Lucky Galvez [3] and Patrick Solé [4]

[1] Research Group of Algebraic Structures and Applications, Department of Mathematics, Faculty of Science, King Abdulaziz University, Jeddah 21589, Saudi Arabia
[2] Department of Mathematics, Faculty of Science, University of Hail, Hail 55431, Saudi Arabia
[3] Institute of Mathematics, University of the Philippines Diliman, Quezon City 1101, Philippines
[4] I2M, (CNRS, University of Aix-Marseille, Centrale Marseille), 13009 Marseilles, France
* Correspondence: analahmadi@kau.edu.sa

Abstract: We study the structure of self-orthogonal and self-dual codes over two non-unital rings of order four, namely, the commutative ring $I = \langle a, b \,|\, 2a = 2b = 0,\ a^2 = b,\ ab = 0 \rangle$ and the non-commutative ring $E = \langle a, b \,|\, 2a = 2b = 0,\ a^2 = a, b^2 = b,\ ab = a,\ ba = b \rangle$. We use these structures to give mass formulas for self-orthogonal and self-dual codes over these two rings, that is, we give the formulas for the number of inequivalent self-orthogonal and self-dual codes, of a given type, over the said rings. Finally, using the mass formulas, we classify self-orthogonal and self-dual codes over each ring, for small lengths and types.

Keywords: code over ring; non-unital ring; self-orthogonal code; quasi self-dual; self-dual code; mass formulas

MSC: 94B05; 16D10

check for updates

Citation: Alahmadi, A.; Alshuhail, A.; Betty, R.A.; Galvez, L.; Solé, P. Mass Formula for Self-Orthogonal and Self-Dual Codes over Non-Unital Rings of Order Four. *Mathematics* **2023**, *11*, 4736. https://doi.org/10.3390/math11234736

Academic Editor: Askar Tuganbaev

Received: 22 September 2023
Revised: 17 October 2023
Accepted: 19 October 2023
Published: 23 November 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Coding theory has been classically studied using finite fields as alphabets [1–11]. In the last thirty years, rings have been used instead of finite fields, i.e., linear codes are defined as modules over a ring [12–17]. There have been many studies on codes over different rings, but most of these are commutative rings, and in almost all cases rings with unity. Recently, there has been interest in non-unital rings of order four [18–22]. The nonexistence of a unity in this ring makes it difficult to deal with usual concepts such as self-duality. For this reason, the notion of quasi self-dual (QSD) codes was introduced. Naturally, it is interesting to look at a bigger class of codes called self-orthogonal codes, which contains self-dual, or in this case, QSD codes.

We begin with some basic concepts about codes over rings. A linear code $\mathcal{C}$ of length n over a ring R is an R-submodule of the R^n module if R is a commutative ring or a one-sided R-submodule of the R^n module if R is a noncommutative ring. All codes in this paper are linear codes. Every element of the code is called a codeword. A generator matrix for $\mathcal{C}$ is a matrix $G \in M_{k\times n}(R)$ whose rows generate the code, and none of the rows can be written as a linear combination of the other rows. For a matrix $G \in M_{k\times n}(R)$, we denote by R^kG the code of length n over R with generator matrix G. In this paper, we will consider two non-unital rings of order four, namely, the rings I and E in the classification of [23,24]. These rings are given by

$$I = \langle a, b \,|\, 2a = 2b = 0,\ a^2 = b,\ ab = 0 \rangle$$

and

$$E = \langle a, b \,|\, 2a = 2b = 0,\ a^2 = a, b^2 = b,\ ab = a,\ ba = b \rangle.$$

It is clear from the multiplication tables that both of these rings do not contain a unity and, in addition, the ring I is commutative while the ring E is noncommutative. We will look at the structures of codes over these rings. Like in the case of linear codes over rings with unity of order four, like $\mathbb{Z}_4$ [25] and $\mathbb{F}_2 + u\mathbb{F}_2$ [26], we establish the generator matrix for codes over the rings I and E and introduce the notion of residue and torsion codes. From the dimensions of these codes, we define the type of code. Then, given a generator matrix for a code $\mathcal{C}$ of a given type over the said rings, we also want to obtain the generator matrices for the residue and torsion codes for $\mathcal{C}$. We will look at the conditions for the residue and torsion codes so that $\mathcal{C}$ is self-orthogonal, as well as self-dual. Using these conditions, we will establish a mass formula for self-orthogonal and self-dual codes over each of the rings I and E, similar to the work presented in [27]. Let $\mathcal{C}$ be the class of codes of length n and of the given type we need to classify. Then, counting orbits under the action of the symmetric group S_n on n letters leads to the equation

$$\sum_D \frac{n!}{|Aut(D)|} = |\mathcal{C}|,$$

where D runs over a system of distinct representatives of equivalence classes of codes of $\mathcal{C}$. Classically this equation is written in the form

$$\sum_D \frac{1}{|Aut(D)|} = \frac{|\mathcal{C}|}{n!}.$$

Computing the left-hand side one orbit at a time works as a stopping criterion in the classification of codes when it adds up to reach the quantity in the right-hand side. Calculating $|\mathcal{C}|$ is a challenging problem in linear algebra over rings, and that is what we accomplish in this article.

The material is arranged as follows. Section 2 sets up basic notions and notation for codes over I. Section 3 studies them in light of the residue and torsion codes. Sections 4 and 5 follow the same course as Sections 2 and 3 but for codes over E. The mass formulas are established in Section 6. Section 7 is dedicated to classification in short lengths for fixed types.

2. Codes over I

In this section, we consider the ring I and recall some concepts about this ring from [19,21]. The ring I is given by

$$I = \left\langle a, b \,|\, 2a = 2b = 0,\ a^2 = b,\ ab = 0 \right\rangle.$$

It has characteristic two and consists of four elements: $I = \{0, a, b, c\}$, with $c = a + b$. The addition and multiplication tables are as follows.

$+$	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

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

Observe that I is a non-unital commutative ring. It is a local ring whose maximal ideal is $J = \{0, b\}$ and residue field $\mathbb{F}_2$, the binary field. We define a natural action of $\mathbb{F}_2$ on I by the rule $r0 = 0r = 0$ and $r1 = 1r = r$, for all $r \in I$. For all $r \in I$, this action is distributive in the sense that $r(s \oplus t) = rs + rt$, where $\oplus$ denotes the addition in $\mathbb{F}_2$, $s, t \in \mathbb{F}_2$. Moreover, every $r \in I$ can be written as

$$r = as + bt,$$

where $s, t \in \mathbb{F}_2$. Denote by $\alpha_I : I \to I/J \simeq \mathbb{F}_2$ the map of the reduction modulo J. We have $\alpha_I(0) = \alpha_I(b) = 0$ and $\alpha_I(a) = \alpha_I(c) = 1$. This map can be extended in the natural way from I^n to $\mathbb{F}_2^n$.

A (linear) code over I, or simply an I-code, of length n is an I-submodule of I^n. There are two binary codes associated with a code $\mathcal{C}$ over I, namely,

$$\text{res}(\mathcal{C}) = \{\alpha_I(y) \mid y \in \mathcal{C}\} \text{ and } \text{tor}(\mathcal{C}) = \{x \in \mathbb{F}_2^n \mid bx \in \mathcal{C}\},$$

called the residue and torsion codes of $\mathcal{C}$, respectively. Note that $\text{res}(\mathcal{C}) \subseteq \text{tor}(\mathcal{C})$. If k_1 is the dimension of $\text{res}(\mathcal{C})$ and $k_1 + k_2$ is the dimension of $\text{tor}(\mathcal{C})$, then

$$|\mathcal{C}| = |\text{res}(\mathcal{C})||\text{tor}(\mathcal{C})| = 2^{2k_1+k_2}.$$

Such code $\mathcal{C}$ is said to be of type $\{k_1, k_2\}$. An I-code $\mathcal{C}$ is said to be free if and only if $k_2 = 0$, that is, $\text{res}(\mathcal{C}) = \text{tor}(\mathcal{C})$.

By Theorem 1 in [19], every code of length n over I of type $\{k_1, k_2\}$ is permutation-equivalent to a code with a generator matrix

$$\begin{pmatrix} aI_{k_1} & aX & Y \\ 0 & bI_{k_2} & bZ \end{pmatrix}, \tag{1}$$

where I_j is the $j \times j$ identity matrix, X and Z are binary matrices, and $Y \in M_{k_1 \times (n-k_1-k_2)}(I)$. In fact, generator matrices of $\text{res}(\mathcal{C})$ and $\text{tor}(\mathcal{C})$ are given by

$$\begin{pmatrix} I_{k_1} & X & \alpha_I(Y) \end{pmatrix} \text{ and } \begin{pmatrix} I_{k_1} & X & \alpha_I(Y) \\ 0 & I_{k_2} & Z \end{pmatrix},$$

respectively.

We equip I^n with the standard inner product $x \cdot y = \sum_{i=1}^n x_i y_i$, for $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in I^n$. The dual of an I-code $\mathcal{C}$ is defined as $\mathcal{C}^\perp = \{v \in I^n \mid u \cdot v = 0 \text{ for all } u \in \mathcal{C}\}$. We say that a code $\mathcal{C}$ is self-orthogonal if $\mathcal{C} \subseteq \mathcal{C}^\perp$, and self-dual if $\mathcal{C} = \mathcal{C}^\perp$. An I-code $\mathcal{C}$ is self-orthogonal if and only if $\text{res}(\mathcal{C})$ is a binary self-orthogonal code.

Example 1. *Any I-code $\mathcal{C}$ of length n and type $\{0, k_2\}$ is a self-orthogonal code for all $k_2 \leq n$.*

If $\mathcal{C}$ is a self-dual I-code of length n with type $\{k_1, k_2\}$, then $n = 2k_1 + k_2$ (see Theorem 2 in [19]). We state the following useful results from [21].

Theorem 1 (Theorem 5 in [21])**.** *A linear code $\mathcal{C}$ of length n over I is self-dual if and only if the following two conditions are satisfied:*

1. *$res(\mathcal{C})$ is a self-dual binary code;*
2. *$tor(\mathcal{C}) = \mathbb{F}_2^n$.*

Corollary 1 (Corollary 2 in [21])**.** *If B is a self-dual binary code of length n, then B is a residue code of a self-dual code of length n over I.*

A code of length n is called quasi self-dual (QSD) if it is self-orthogonal and of size 2^n. A linear I-code can never simultaneously be both QSD and self-dual (see Proposition 2 in [21]). We end this section with the following proposition.

Proposition 1.

1. *For any positive integer n, there exists a QSD code over I of length n.*
2. *Let $\mathcal{C} = a\,res(\mathcal{C}) + b\,tor(\mathcal{C})$ be an I-code with $tor(\mathcal{C}) = res(\mathcal{C}) = res(\mathcal{C})^\perp$. Then $\mathcal{C}$ will be a QSD code.*

Proof.

1. Let $\mathcal{C} = b\mathbb{F}_2^n$. Since $u\mathbb{F}_2^n \subseteq \mathcal{C}^\perp$ for every $u \in I$, $\mathcal{C} \subsetneq \mathcal{C}^\perp$ of size 2^n.
2. If $\mathrm{tor}(\mathcal{C}) = \mathrm{res}(\mathcal{C})$, then $\mathcal{C}$ is a free code with $n = 2k$, where k is the dimension of $\mathrm{res}(\mathcal{C})$. By Theorem 1 and Corollary 1, we have a self-orthogonal code $\mathcal{C}$ of size $2^{2k} = 2^n$.

□

3. Codes over I with Prescribed Residue and Torsion

Let C_1 be a binary code of length n with dimension k_1 and generator matrix

$$\begin{pmatrix} I_{k_1} & A \end{pmatrix}, \tag{2}$$

and C_2 be a binary code of length n with dimension $k_1 + k_2$ and generator matrix

$$\begin{pmatrix} I_{k_1} & A \\ 0 & D \end{pmatrix}, \tag{3}$$

where $A \in M_{k_1 \times (n-k_1)}(\mathbb{F}_2)$, and $D \in M_{k_2 \times (n-k_1)}(\mathbb{F}_2)$ is of full row rank. Observe that $C_1 \subseteq C_2$.

Lemma 1. *Let $\mathcal{C}$ be a code of length n over I with $\mathrm{res}(\mathcal{C}) = C_1$ and $\mathrm{tor}(\mathcal{C}) = C_2$. Then, there exists a matrix $N \in M_{k_1 \times (n-k_1)}(\mathbb{F}_2)$ such that the matrix*

$$\begin{pmatrix} aI_{k_1} & aA + bN \\ 0 & bD \end{pmatrix} \tag{4}$$

is a generator matrix of $\mathcal{C}$. If $\mathcal{C}$ is a free code, such a matrix N is unique.

Proof. Since the residue and torsion codes of $\mathcal{C}$ are C_1 and C_2, respectively, then for some $M_1 \in M_{k_1 \times k_1}(\mathbb{F}_2)$ and $M_2 \in M_{k_1 \times (n-k_1)}(\mathbb{F}_2)$,

$$I^{k_1+k_2}\begin{pmatrix} aI_{k_1} + bM_1 & aA + bM_2 \\ 0 & bD \end{pmatrix} \subseteq \mathcal{C}.$$

By an elementary row operation,

$$\begin{aligned} \mathcal{C} &\supseteq I^{k_1+k_2}\begin{pmatrix} I_{k_1} + cM_1 & 0 \\ 0 & I_{k_2} \end{pmatrix}\begin{pmatrix} aI_{k_1} + bM_1 & aA + bM_2 \\ 0 & bD \end{pmatrix} \\ &= I^{k_1+k_2}\begin{pmatrix} aI_{k_1} & aA + b(M_2 + M_1A) \\ 0 & bD \end{pmatrix}. \end{aligned}$$

Taking $N = M_2 + M_1A$, we have

$$|\mathcal{C}| \geq \left| I^{k_1+k_2}\begin{pmatrix} aI_{k_1} & aA + bN \\ 0 & bD \end{pmatrix} \right| = 2^{2k_1+k_2} = |C_1||C_2| = |\mathcal{C}|.$$

Therefore, $\mathcal{C}$ has a generator matrix (4). Let $\mathcal{C}$ be a free code and suppose there exist $N_1, N_2 \in M_{k_1 \times (n-k_1)}(\mathbb{F}_2)$ such that

$$I^{k_1}\begin{pmatrix} aI_{k_1} & aA + bN_1 \end{pmatrix} = I^{k_1}\begin{pmatrix} aI_{k_1} & aA + bN_2 \end{pmatrix}.$$

Then, $aA + bN_1 = aA + bN_2$, which implies that $N_1 = N_2$. □

For the remainder of this section, assume that $C_1 \subseteq C_1^\perp$. Then,

$$I_{k_1} + AA^\top = 0. \tag{5}$$

It follows from (5) that A is of full row rank.

Lemma 2. *The number of free self-orthogonal codes over I with residue code C_1 is*

$$2^{k_1(n-k_1)}.$$

Proof. Suppose $\mathcal{C}$ is a free I-code with residue code C_1. Then, by Lemma 1, $\mathcal{C}$ has a generator matrix $\begin{pmatrix} aI_{k_1} & aA+bN \end{pmatrix}$, for some unique $N \in M_{k_1\times(n-k_1)}(\mathbb{F}_2)$. Note that $\mathcal{C}$ is self-orthogonal if and only if

$$\begin{pmatrix} aI_{k_1} & aA+bN \end{pmatrix}\begin{pmatrix} aI_{k_1} & aA+bN \end{pmatrix}^\top = 0.$$

Observe that by (5),

$$(aI_{k_1})(aI_{k_1}) + (aA+bN)(aA+bN)^\top = b(I_{k_1} + AA^\top) = 0,$$

for any $N \in M_{k_1\times(n-k_1)}(\mathbb{F}_2)$. Hence, the number of free self-orthogonal codes $\mathcal{C}$ over I with residue code C_1 is

$$\left|\left\{N \in M_{k_1\times(n-k_1)} | \begin{pmatrix} aI_{k_1} & aA+bN \end{pmatrix}\begin{pmatrix} aI_{k_1} & aA+bN \end{pmatrix}^\top = 0\right\}\right| = 2^{k_1(n-k_1)}. \quad (6)$$

□

Now, we define the sets

$$\begin{aligned} X &= \left\{\mathcal{C} \mid \mathcal{C} \subseteq I^n, \text{type } \{k_1, 0\}, \mathcal{C} \subseteq \mathcal{C}^\perp, \text{res}(\mathcal{C}) = C_1\right\} \text{ and} \\ X' &= \left\{\mathcal{C}' \mid \mathcal{C}' \subseteq I^n, \mathcal{C}' \subseteq \mathcal{C}'^\perp, \text{res}(\mathcal{C}') = C_1, \text{tor}(\mathcal{C}') = C_2\right\}. \end{aligned}$$

Lemma 3. *Suppose $\mathcal{C} \in X$. Then, there exists a unique code $\mathcal{C}' \in X'$ such that $\mathcal{C} \subseteq \mathcal{C}'$.*

Proof. Since $\mathcal{C} \in X$, by Lemma 1, $\mathcal{C}$ has a generator matrix $\begin{pmatrix} aI_{k_1} & aA+bN \end{pmatrix}$ for some unique matrix N. Let $\mathcal{C}_0'$ be a code with generator matrix

$$\begin{pmatrix} aI_{k_1} & aA+bN \\ 0 & bD \end{pmatrix}.$$

The code $\mathcal{C}_0'$ satisfies $\text{res}(\mathcal{C}_0') = C_1$ and $\text{tor}(\mathcal{C}_0') = C_2$.

Clearly, $\mathcal{C} \subseteq \mathcal{C}_0'$. Since $\mathcal{C} \in X$, $\mathcal{C}_0'$ is self-orthogonal and hence, $\mathcal{C}_0' \in X'$. Suppose $\mathcal{C} \subseteq \mathcal{C}'$ for some $\mathcal{C}' \in X'$. Note that $\mathcal{C}'$ has torsion code C_2. Thus, by Lemma 1, $I^{k_2}(0 \;\; bD) \subseteq \mathcal{C}'$ and so $\mathcal{C}_0' \subseteq \mathcal{C}'$. Observe that $|\mathcal{C}_0'| = |C_1||C_2| = 2^{2k_0+k_1} = |\mathcal{C}'|$. Therefore, $\mathcal{C}_0' = \mathcal{C}'$. □

Lemma 4. *If $\mathcal{C}' \in X'$, then $|\{\mathcal{C} \in X | \mathcal{C} \subseteq \mathcal{C}'\}| = 2^{k_1k_2}$.*

Proof. By Lemma 1, $\mathcal{C}'$ has a generator matrix (4). We define the map

$$\begin{aligned} \psi : M_{k_1\times k_2}(\mathbb{F}_2) &\longrightarrow \{\mathcal{C} \in X \mid \mathcal{C} \subseteq \mathcal{C}'\} \\ M &\longmapsto I^{k_1}\begin{pmatrix} aI_{k_1} & aA+b(N+MD) \end{pmatrix}. \end{aligned}$$

Observe that ψ is well defined. Now, we will show that ψ is bijective. If $M_1, M_2 \in M_{k_1\times k_2}(\mathbb{F}_2)$ such that $\psi(M_1) = \psi(M_2)$, then

$$I^{k_1}\begin{pmatrix} aI_{k_1} & aA+b(N+M_1D) \end{pmatrix} = I^{k_1}\begin{pmatrix} aI_{k_1} & aA+b(N+M_2D) \end{pmatrix}.$$

Therefore, $aA + b(N + M_1D) = A + b(N + M_2D)$. Hence, $N + M_1D = N + M_2D$. Since D is of full row rank, we have $M_1 = M_2$. Therefore, ψ is injective.

Suppose $\mathcal{C} \in X$ and $\mathcal{C} \subseteq \mathcal{C}'$. By Lemma 1, $\mathcal{C} = I^{k_1}\begin{pmatrix} aI_{k_1} & aA + bH \end{pmatrix}$, for some matrix H. From the inclusion $\mathcal{C} \subseteq \mathcal{C}'$, we have

$$aA + bH = aA + b(N + MD)$$

for some matrix M. Therefore, $H = N + MD$, which shows that ψ is surjective. Hence, ψ is bijective. Thus,

$$\left|\{\mathcal{C} \in X | \mathcal{C} \subseteq \mathcal{C}'\}\right| = \left|M_{k_1 \times k_2}(\mathbb{F}_2)\right| = 2^{k_1 k_2}.$$

□

Now, we count self-orthogonal I-codes $\mathcal{C}$ with a given residue code and torsion code.

Theorem 2. *Let C_1 and C_2 be binary codes of length n where $C_1 \subseteq C_2$ and $C_1 \subseteq C_1^{\perp}$. If $\dim C_1 = k_1$ and $\dim C_2 = k_1 + k_2$, then the number of self-orthogonal I-codes $\mathcal{C}$ of length n with $res(\mathcal{C}) = C_1$ and $tor(\mathcal{C}) = C_2$ is*

$$2^{k_1(n-k_1-k_2)}.$$

Proof. We may assume without loss of generality that C_1 and C_2 are binary codes with generator matrices (2) and (3), respectively. Now, we compute $|X'|$. By Lemmas 3 and 4, we have

$$2^{k_1 k_2}|X'| = \sum_{\mathcal{C}' \in X'} \left|\{\mathcal{C} \in X | \mathcal{C} \subseteq \mathcal{C}'\}\right| = \sum_{\mathcal{C} \in X} \left|\{\mathcal{C}' \in X' | \mathcal{C} \subseteq \mathcal{C}'\}\right| = \sum_{\mathcal{C} \in X} 1 = |X|.$$

The result follows from Lemma 2. □

Theorem 3. *Let C_1 be a binary self-dual code of length n. Then, the number of self-dual I-codes $\mathcal{C}$ of length n with $res(\mathcal{C}) = C_1$ is equal to the number of self-dual binary codes of length n.*

Proof. From Theorem 1, the number of self-dual I-codes $\mathcal{C}$ depends on the number of self-dual codes over $\mathbb{F}_2$, and $\text{tor}(\mathcal{C}) = \mathbb{F}_2^n$. □

4. Codes over E

In this section, we consider another ring, E. We recall some concepts from [20,21]. The ring E is given by

$$E = \left\langle a, b \,|\, 2a = 2b = 0,\ a^2 = a,\ b^2 = b,\ ab = a,\ ba = b \right\rangle.$$

Similar to I, this ring has characteristic two and consists of four elements: $E = \{0, a, b, c\}$, with $c = a + b$. The addition and multiplication tables are as follows.

$+$	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

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

Observe that E is a non-unital and noncommutative ring. It is a local ring whose maximal ideal is $J = \{0, c\}$ and residue field $\mathbb{F}_2$. We define a natural action of $\mathbb{F}_2$ on E by the rule $r0 = 0r = 0$ and $r1 = 1r = r$ for all $r \in E$. For all $r \in E$, this action is distributive in the sense that $r(s \oplus t) = rs + rt$, where $\oplus$ denotes the addition in $\mathbb{F}_2$, $s, t \in \mathbb{F}_2$. Moreover, every $r \in E$ can be written as

$$r = as + ct,$$

where $s, t \in \mathbb{F}_2$. Denote by $\alpha_E : E \to E/J \simeq \mathbb{F}_2$ the map of reduction modulo J. We have $\alpha_E(0) = \alpha_E(c) = 0$ and $\alpha_E(a) = \alpha_E(b) = 1$. This map can be extended in the natural way from E^n to $\mathbb{F}_2^n$.

A (linear) code over E, or E-code, of length n is a one-sided E-submodule of E^n. We also associate the two following binary codes with a code $\mathcal{C}$ over E:

$$\mathrm{res}(\mathcal{C}) = \{\alpha_E(y) \mid y \in \mathcal{C}\} \text{ and } \mathrm{tor}(\mathcal{C}) = \{x \in \mathbb{F}_2^n \mid cx \in \mathcal{C}\},$$

called the residue and torsion codes of $\mathcal{C}$, respectively. Note that $\mathrm{res}(\mathcal{C}) \subseteq \mathrm{tor}(\mathcal{C})$. If k_1 is the dimension of $\mathrm{res}(\mathcal{C})$ and $k_1 + k_2$ is the dimension of $\mathrm{tor}(\mathcal{C})$, then

$$|\mathcal{C}| = |\mathrm{res}(\mathcal{C})||\mathrm{tor}(\mathcal{C})| = 2^{2k_1+k_2}.$$

As in I-codes, such a code $\mathcal{C}$ over E is said to be of type $\{k_1, k_2\}$ and an E-code $\mathcal{C}$ is said to be free if and only if $k_2 = 0$, that is, $\mathrm{res}(\mathcal{C}) = \mathrm{tor}(\mathcal{C})$.

By Theorem 1 in [20], every code C of length n over E is permutation-equivalent to a code with the generator matrix

$$\begin{pmatrix} aI_{k_1} & X & Y \\ 0 & cI_{k_2} & cZ \end{pmatrix}, \tag{7}$$

where I_j is the $j \times j$ identity matrix, Z is a binary matrix, $X \in M_{k_1 \times k_2}(E)$, and $Y \in M_{k_1 \times (n-k_1-k_2)}(E)$. In fact, generator matrices of $\mathrm{res}(\mathcal{C})$ and $\mathrm{tor}(\mathcal{C})$ are given by

$$\begin{pmatrix} I_{k_1} & \alpha_E(X) & \alpha_E(Y) \end{pmatrix} \text{ and } \begin{pmatrix} I_{k_1} & \alpha_E(X) & \alpha_E(Y) \\ 0 & I_{k_2} & Z \end{pmatrix},$$

respectively.

We equip E^n with the standard inner product $x \cdot y = \sum_{i=1}^n x_i y_i$, for $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in E^n$. The right dual of $\mathcal{C}$ is the right module defined as

$$\mathcal{C}^{\perp_R} = \{y \in E^n \mid \forall\, x \in \mathcal{C},\, x \cdot y = 0\}$$

and the left dual of $\mathcal{C}$ is the left module defined by

$$\mathcal{C}^{\perp_L} = \{y \in E^n \mid \forall\, x \in \mathcal{C},\, y \cdot x = 0\}.$$

$\mathcal{C}$ is said to be left nice (respectively, right nice) if $|\mathcal{C}||\mathcal{C}^{\perp_L}| = 4^n$ (respectively, $|\mathcal{C}||\mathcal{C}^{\perp_R}| = 4^n$). If it is both left and right nice, it is said to be nice.

Furthermore, $\mathcal{C}$ is called right self-dual if $\mathcal{C} = \mathcal{C}^{\perp_R}$ and left self-dual if $\mathcal{C} = \mathcal{C}^{\perp_L}$. The two-sided dual of $\mathcal{C}$, denoted by $\mathcal{C}^{\perp}$, is given by $\mathcal{C}^{\perp} = \mathcal{C}^{\perp_L} \cap \mathcal{C}^{\perp_R}$. We have $\mathcal{C}$ is self-orthogonal if for all $x, y \in \mathcal{C}$, $x \cdot y = 0$, that is, $\mathcal{C} \subseteq \mathcal{C}^{\perp}$, and self-dual if $\mathcal{C} = \mathcal{C}^{\perp}$. We see that if $\mathcal{C}$ is self-dual and of type $\{k_1, k_2\}$, then $n = 2k_1 + k_2$.

The following lemma shows the relationship between the residue and torsion codes of a self-orthogonal code over E. The proof is given in [20].

Lemma 5. *Let $\mathcal{C}$ be a self-orthogonal code of length n over E. Then,*

1. *$res(\mathcal{C})$ is self-orthogonal, i.e., $res(\mathcal{C}) \subseteq res(\mathcal{C})^{\perp}$;*
2. *$tor(\mathcal{C}) \subseteq res(\mathcal{C})^{\perp}$;*
3. *$tor(\mathcal{C}) = res(\mathcal{C})^{\perp}$ if $|\mathcal{C}| = 2^n$.*

In addition, $\mathcal{C}$ is quasi self-dual (QSD) if it is self-orthogonal and of size 2^n. By Remark 2 in [21], the notions of QSD codes and self-dual codes over E are equivalent. We state the following theorems from [21].

Theorem 4 (Theorem 14 in [21]). *If $\mathcal{C}$ is a linear code of length n over E, then the following hold:*

1. *$\mathcal{C}$ is left self-dual if and only if $\mathcal{C}$ is free and $res(\mathcal{C})$ is self-dual.*
2. *$\mathcal{C}$ is right self-dual if and only if $\mathcal{C}$ is of type $\{0, n\}$.*

Theorem 5 (Theorem 15 in [21]). *A linear code $\mathcal{C}$ over E is self-dual if and only if $res(\mathcal{C}) = tor(\mathcal{C})^{\perp}$.*

5. Codes over E with Prescribed Residue and Torsion

Similar to Section 2, we take C_1 to be a binary code of length n with dimension k_1 and generator matrix (2) and C_2 be a binary code of length n with dimension $k_1 + k_2$ and has a generator matrix (3), where $A \in M_{k_1 \times (n-k_1)}(\mathbb{F}_2)$, and $D \in M_{k_2 \times (n-k_1)}(\mathbb{F}_2)$ is of full row rank. Also, $C_1 \subseteq C_2$.

Lemma 6. *Suppose $\mathcal{C}$ is a code of length n over E with $res(\mathcal{C}) = C_1$ and $tor(\mathcal{C}) = C_2$. Then, there exists a matrix $N \in M_{k_1 \times (n-k_1)}(\mathbb{F}_2)$ such that the matrix*

$$\begin{pmatrix} aI_{k_1} & aA + cN \\ 0 & cD \end{pmatrix} \tag{8}$$

is a generator matrix of $\mathcal{C}$. If $\mathcal{C}$ is a free code, such a matrix N is unique.

Proof. Because the residue and torsion codes of $\mathcal{C}$ are C_1 and C_2, respectively, then for some $M_1 \in M_{k_1}(\mathbb{F}_2)$ and $M_2 \in M_{k_1 \times (n-k_1)}(\mathbb{F}_2)$,

$$E^{k_1+k_2}\begin{pmatrix} aI_{k_1} + cM_1 & aA + cM_2 \\ 0 & cD \end{pmatrix} \subseteq \mathcal{C}.$$

By an elementary row operation,

$$\begin{aligned} \mathcal{C} &\supseteq E^{k_1+k_2}\begin{pmatrix} I_{k_1} + cM_1 & 0 \\ 0 & I_{k_2} \end{pmatrix}\begin{pmatrix} aI_{k_1} + cM_1 & aA + cM_2 \\ 0 & cD \end{pmatrix} \\ &= E^{k_1+k_2}\begin{pmatrix} aI_{k_1} & aA + c(M_2 + M_1A) \\ 0 & cD \end{pmatrix}. \end{aligned}$$

Taking $N = M_2 + M_1A$, we have

$$|\mathcal{C}| \geq \left|E^{k_1+k_2}\begin{pmatrix} aI_{k_1} & aA + cN \\ 0 & cD \end{pmatrix}\right| = 2^{2k_1+k_2} = |C_1||C_2| = |\mathcal{C}|.$$

Therefore, $\mathcal{C}$ has a generator matrix (8). The proof that such matrix N is unique if $\mathcal{C}$ is a free code is similar to Lemma 1. □

For the remainder of this section, assume that $C_1 \subseteq C_2 \subseteq C_1^{\perp}$. Then,

$$I_{k_1} + AA^{\top} = 0, \tag{9}$$

$$DA^{\top} = 0. \tag{10}$$

It follows from (9) that A is of full row rank. We define the mapping

$$\begin{aligned} \beta_X : M_{k\times m}(\mathbb{F}_2) &\longrightarrow M_{k\times k}(\mathbb{F}_2) \\ N &\longmapsto XN^{\top}, \end{aligned}$$

where $X \in M_{k\times m}(\mathbb{F}_2)$. Note that β_X is surjective if X is of full row rank.

Lemma 7. *The number of free self-orthogonal codes over E with residue code C_1 is*

$$2^{k_1(n-2k_1)}.$$

Proof. Suppose $\mathcal{C}$ is a free E-code with residue code C_1. By Lemma 6, $\mathcal{C}$ has a generator matrix $\begin{pmatrix} aI_{k_1} & aA+cN \end{pmatrix}$, for some unique $N \in M_{k_1\times(n-k_1)}(\mathbb{F}_2)$. Note that $\mathcal{C}$ is self-orthogonal if and only if

$$\begin{pmatrix} aI_{k_1} & aA+cN \end{pmatrix}\begin{pmatrix} aI_{k_1} & aA+cN \end{pmatrix}^\top = 0.$$

That is,

$$(aI_{k_1})(aI_{k_1}) + (aA+cN)(aA+cN)^\top = a(I_{k_1} + AA^\top) + cNA^\top = cNA^\top = 0,$$

by (9). Since $c \neq 0$ and $NA^\top$ is a binary matrix, we have $NA^\top = 0$. Hence, the number of free self-orthogonal codes $\mathcal{C}$ with residue code C_1 is

$$\left|\{N \in M_{k_1\times(n-k_1)} | AN^\top = 0\}\right| = |\ker \beta_A| = \frac{\left|M_{k_1\times(n-k_1)}\right|}{|\mathrm{Im}\ \beta_A|} = 2^{k_1(n-k_1)-k_1k_1}, \tag{11}$$

since A is of full row rank. □

Similar to ring I, we define the sets

$$\begin{aligned} Y &= \left\{\mathcal{C} \mid \mathcal{C} \subseteq E^n, \text{type } \{k_1, 0\}, \mathcal{C} \subseteq \mathcal{C}^\perp, \text{res}(\mathcal{C}) = C_1\right\} \text{ and} \\ Y' &= \left\{\mathcal{C}' \mid \mathcal{C}' \subseteq E^n, \mathcal{C}' \subseteq \mathcal{C}'^\perp, \text{res}(\mathcal{C}') = C_1, \text{tor}(\mathcal{C}') = C_2\right\}. \end{aligned}$$

Lemma 8. *Let $\mathcal{C} \in Y$. Then, there exists a unique code $\mathcal{C}' \in Y'$ such that $\mathcal{C} \subseteq \mathcal{C}'$.*

Proof. Since $\mathcal{C} \in Y$, by Lemma 6, $\mathcal{C}$ has a generator matrix $\begin{pmatrix} aI_{k_1} & aA+cN \end{pmatrix}$ for some unique matrix N. Let $\mathcal{C}_0'$ be a code with generator matrix

$$\begin{pmatrix} aI_{k_1} & aA+cN \\ 0 & cD \end{pmatrix}.$$

The code $\mathcal{C}_0'$ satisfies $\text{res}(\mathcal{C}_0') = C_1$ and $\text{tor}(\mathcal{C}_0') = C_2$. Clearly, $\mathcal{C} \subseteq \mathcal{C}_0'$. Since $\mathcal{C} \in Y$, (10) implies $\mathcal{C}_0'$ is self-orthogonal and hence, $\mathcal{C}_0' \in Y'$. Suppose $\mathcal{C} \subseteq \mathcal{C}'$ for some $\mathcal{C}' \in Y'$. Since $\mathcal{C}'$ has torsion code C_2, $E^{k_2}(0\ \ cD) \subseteq \mathcal{C}'$ by Lemma 6. Therefore, $\mathcal{C}_0' \subseteq \mathcal{C}'$. Moreover, $|\mathcal{C}_0'| = |C_1||C_2| = 2^{2k_0+k_1} = |\mathcal{C}'|$. Hence, $\mathcal{C}_0' = \mathcal{C}'$. □

Lemma 9. *If $\mathcal{C}' \in Y'$, then $|\{\mathcal{C} \in Y | \mathcal{C} \subseteq \mathcal{C}'\}| = 2^{k_1k_2}$.*

Proof. By Lemma 6, $\mathcal{C}'$ has a generator matrix (8). Define the map

$$\begin{aligned} \psi : M_{k_1\times k_2}(\mathbb{F}_2) &\longrightarrow \{\mathcal{C} \in X \mid \mathcal{C} \subseteq \mathcal{C}'\} \\ M &\longmapsto E^{k_1}\begin{pmatrix} aI_{k_1} & aA+c(N+MD) \end{pmatrix}. \end{aligned}$$

Clearly, ψ is well-defined. We will show that ψ is bijective. If $M_1, M_2 \in M_{k_1\times k_2}(\mathbb{F}_2)$ such that $\psi(M_1) = \psi(M_2)$, then

$$E^{k_1}\begin{pmatrix} aI_{k_1} & aA+c(N+M_1D) \end{pmatrix} = E^{k_1}\begin{pmatrix} aI_{k_1} & aA+c(N+M_2D) \end{pmatrix}$$

which means $aA + c(N + M_1D) = A + c(N + M_2D)$. Therefore, $N + M_1D = N + M_2D$. Since D is of full row rank, we have $M_1 = M_2$. Hence, ψ is injective.

Suppose $\mathcal{C} \in Y$ and $\mathcal{C} \subseteq \mathcal{C}'$. By Lemma 6, $\mathcal{C} = E^{k_1}\begin{pmatrix} aI_{k_1} & aA + cF \end{pmatrix}$, for some matrix F. The inclusion $\mathcal{C} \subseteq \mathcal{C}'$ implies that

$$aA + cF = aA + c(N + MD)$$

for some matrix M. Therefore, $F = N + MD$. Hence, the map ψ is surjective, and it follows that ψ is bijective. Thus,

$$\left|\{\mathcal{C} \in Y | \mathcal{C} \subseteq \mathcal{C}'\}\right| = \left|M_{k_1 \times k_2}(\mathbb{F}_2)\right| = 2^{k_1 k_2}.$$

□

Now, we count self-orthogonal E-codes $\mathcal{C}$ with a given residue code and torsion code.

Theorem 6. *Let C_1 and C_2 be binary codes of length n where $C_1 \subseteq C_2 \subseteq C_1^{\perp}$. If* $\dim C_1 = k_1$ *and* $\dim C_2 = k_1 + k_2$, *then the number of self-orthogonal E-codes $\mathcal{C}$ of length n with $res(\mathcal{C}) = C_1$ and $tor(\mathcal{C}) = C_2$ is*

$$2^{k_1(n-2k_1-k_2)}.$$

Proof. We may assume without loss of generality that C_1 and C_2 are binary codes with generator matrices (2) and (3), respectively. The codes C_1 and C_2 satisfy the conclusions (1)–(2) of Lemma 5. Now, we have to compute $|Y'|$. By Lemmas 8 and 9, we have

$$2^{k_1 k_2}|Y'| = \sum_{\mathcal{C}' \in Y'} \left|\{\mathcal{C} \in Y | \mathcal{C} \subseteq \mathcal{C}'\}\right| = \sum_{\mathcal{C} \in Y} \left|\{\mathcal{C}' \in Y' | \mathcal{C} \subseteq \mathcal{C}'\}\right| = \sum_{\mathcal{C} \in Y} 1 = |Y|.$$

The result follows from Lemma 7. □

6. Mass Formula for Self-Orthogonal Codes over I and E

Let $\Phi(n, k_1)$ denote the number of distinct self-orthogonal binary codes of length n and dimension k_1, given in [28]. We define the *Gaussian coefficient* $\begin{bmatrix} n \\ m \end{bmatrix}_q$ for $m \leq n$ as

$$\begin{bmatrix} n \\ m \end{bmatrix}_q = \frac{(q^n - 1)(q^n - q) \cdots (q^n - q^{m-1})}{(q^m - 1)(q^m - q) \cdots (q^m - q^{m-1})},$$

which gives the number of subspaces of dimension m contained in an n-dimensional vector space over $\mathbb{F}_q$.

We now have the following mass formula for self-orthogonal codes over I.

Theorem 7. *Let $M_I(n, k_1, k_2)$ denote the number of distinct self-orthogonal codes of length n over I of type $\{k_1, k_2\}$. We have*

$$M_I(n, k_1, k_2) = \Phi(n, k_1) \begin{bmatrix} n - k_1 \\ k_2 \end{bmatrix}_2 2^{k_1(n-k_1-k_2)}.$$

Proof. If $\mathcal{C}$ is a self-orthogonal code of length n over I of type $\{k_1, k_2\}$, then by setting $C_1 = \text{res}(\mathcal{C})$ and $C_2 = \text{tor}(\mathcal{C})$, we see that C_1 and C_2 satisfy Lemma 3 in [19] and $\text{res}(\mathcal{C}) \subseteq \text{tor}(\mathcal{C})$. There are $\Phi(n, k_1)$ self-orthogonal binary codes C_1 of length n. Given C_1, there are $\begin{bmatrix} n - k_1 \\ k_2 \end{bmatrix}_2$ codes C_2 such that $C_1 \subseteq C_2 \subseteq \mathbb{F}_2^n$. Then, the result follows from Theorem 2. □

We have the following mass formula for quasi self-dual codes over I as a direct consequence of the previous theorem.

Corollary 2. *The number of quasi self-dual codes of length n over I is given by*

$$\sum_{0\le k_1\le \lfloor \frac{n}{2}\rfloor} \Phi(n,k_1) \begin{bmatrix} n-k_1 \\ n-2k_1 \end{bmatrix}_2 2^{k_1^2}. \tag{12}$$

Proof. Since quasi self-dual codes are self-orthogonal codes of type $\{k_1, n-2k_1\}$, the number of quasi distinct self-dual codes of length n over I is given by

$$\begin{aligned} \sum_{0\le k_1\le \lfloor \frac{n}{2}\rfloor} M_I(n,k_1,n-2k_1) &= \sum_{0\le k_1\le \lfloor \frac{n}{2}\rfloor} \Phi(n,k_1) \begin{bmatrix} n-k_1 \\ n-2k_1 \end{bmatrix}_2 2^{k_1(n-k_1-n+2k_1)} \\ &= \sum_{0\le k_1\le \lfloor \frac{n}{2}\rfloor} \Phi(n,k_1) \begin{bmatrix} n-k_1 \\ n-2k_1 \end{bmatrix}_2 2^{k_1(k_1)}. \end{aligned}$$

□

Note that Corollary 2 agrees with Theorem 5 in [19].

Corollary 3. *For an even integer n, the number of self-dual codes of length n over I is given by*

$$\Phi\Big(n, \frac{n}{2}\Big), \tag{13}$$

where $\Phi\big(n, \frac{n}{2}\big)$ *is the number of self-dual binary codes of length n.*

Proof. By Theorem 3, the number of self-dual I-codes $\mathcal{C}$ of length n depends on the number of self-dual binary residue codes and $\mathrm{tor}(\mathcal{C}) = \mathbb{F}_2^n$. □

And we have the following mass formula for self-orthogonal codes over E.

Theorem 8. *Let* $M_E(n,k_1,k_2)$ *denote the number of distinct self-orthogonal codes of length n over E of type* $\{k_1,k_2\}$. *We have*

$$M_E(n,k_1,k_2) = \Phi(n,k_1) \begin{bmatrix} n-2k_1 \\ k_2 \end{bmatrix}_2 2^{k_1(n-2k_1-k_2)}.$$

Proof. If $\mathcal{C}$ is a self-orthogonal code of length n over E of type $\{k_1,k_2\}$, then by setting $C_1 = \mathrm{res}(\mathcal{C})$ and $C_2 = \mathrm{tor}(\mathcal{C})$, we see that C_1 and C_2 satisfy (1)–(2) of Lemma 5 and $\mathrm{res}(\mathcal{C}) \subseteq \mathrm{tor}(\mathcal{C})$. There are $\Phi(n,k_1)$ self-orthogonal binary codes C_1 of length n. Given C_1, there are $\begin{bmatrix} n-2k_1 \\ k_2 \end{bmatrix}_2$ codes C_2 such that $C_1 \subseteq C_2 \subseteq C_1^{\perp}$. Then, the result follows from Theorem 6. □

We now have the following mass formula for self-dual codes over E as a direct consequence of the previous theorem.

Corollary 4. *The number of self-dual codes of length n over E is given by*

$$\sum_{0\le k_1\le \lfloor \frac{n}{2}\rfloor} \Phi(n,k_1). \tag{14}$$

Proof. Note that self-dual codes are self-orthogonal codes of type $\{k_1, n-2k_1\}$. Therefore, the number of distinct self-dual codes of length n over E is given by

$$\begin{aligned}\sum_{0\le k_1\le \lfloor \frac{n}{2}\rfloor} M_E(n,k_1,n-2k_1) &= \sum_{0\le k_1\le \lfloor \frac{n}{2}\rfloor} \Phi(n,k_1)\begin{bmatrix} n-2k_1 \\ n-2k_1 \end{bmatrix}_2 2^{k_1(n-2k_1-n+2k_1)} \\ &= \sum_{0\le k_1\le \lfloor \frac{n}{2}\rfloor} \Phi(n,k_1).\end{aligned}$$

□

Note that Corollary 4 means classifying self-dual codes over E reduces to a classification of binary self-orthogonal codes, which agrees with [20], page 13.

Corollary 5. *The number of left self-dual codes of length n over E is given by*

$$\Phi(n, \frac{n}{2}). \tag{15}$$

Proof. By Theorem 4, the number of left self-dual codes is given by

$$M_E(n, \frac{n}{2}, 0) = \Phi(n, \frac{n}{2})\begin{bmatrix} n-2\frac{n}{2} \\ 0 \end{bmatrix}_2 2^{\frac{n}{2}(n-2\frac{n}{2}-0)} = \Phi(n, \frac{n}{2}),$$

since left self-dual codes are free codes with self-dual binary residue codes. □

Proposition 2. *There is a unique right self-dual code over E of length n.*

Proof. By Theorem 4, the code $\mathcal{C} = c\mathbb{F}_2^n$ with type $\{0, n\}$ is the unique right self-dual code over E of length n. □

7. Classification

We illustrate how the mass formula can be used in the classification of self-orthogonal codes, that is, we find representatives for the equivalence classes of self-orthogonal codes for each length and type. The set of representatives $\mathscr{C}$ is complete if the mass formula in Theorem 7 or 8 equals

$$\sum_{\mathcal{C}\in\mathscr{C}} \frac{n!}{|\mathrm{Aut}(\mathcal{C})|}$$

where $\mathrm{Aut}(\mathcal{C})$ is the automorphism group of $\mathcal{C}$.

Example 2. *Let $\mathscr{C}$ be the set of self-orthogonal codes of length 3 over I of type $\{1,1\}$ given by the following generator matrices:*

$$\left\{\begin{pmatrix} a & a & 0 \\ 0 & b & 0 \end{pmatrix}, \begin{pmatrix} a & a & 0 \\ 0 & b & b \end{pmatrix}, \begin{pmatrix} a & a & 0 \\ 0 & 0 & b \end{pmatrix}, \begin{pmatrix} a & c & 0 \\ 0 & b & b \end{pmatrix}, \begin{pmatrix} a & c & 0 \\ 0 & 0 & b \end{pmatrix}, \begin{pmatrix} a & a & b \\ 0 & b & 0 \end{pmatrix}\right\}.$$

The codes in $\mathscr{C}$ are inequivalent and each has an automorphism group of order 2. Therefore,

$$\sum_{\mathcal{C}\in\mathscr{C}} \frac{3!}{|Aut(\mathcal{C})|} = 6\left(\frac{6}{2}\right) = 18.$$

From 7,

$$M_I(3,1,1) = \Phi(3,1)\begin{bmatrix} 2 \\ 1 \end{bmatrix}_2 2^{1(3-1-1)} = (3)(3)(2) = 18,$$

which shows that there are exactly six self-orthogonal codes over I of length 3 and type $\{1,1\}$, up to equivalence.

Table 1 is the classification of self-orthogonal codes over I for short lengths.

Table 1. Inequivalent self-orthogonal codes of length $n \leq 3$ over I .

n	$\{k_1, k_2\}$	Generator Matrix	$\lvert \mathrm{Aut}(\mathcal{C}) \rvert$	Weight Distribution
2	$\{0,1\}$	$\begin{pmatrix} 0 & b \end{pmatrix}$	1	$[<0,1>,<1,1>]$
		$\begin{pmatrix} b & b \end{pmatrix}$	2	$[<0,1>,<2,1>]$
	$\{0,2\}$	$\begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}$	2	$[<0,1>,<1,2>,<2,1>]$
	$\{1,0\}$	$\begin{pmatrix} a & u \end{pmatrix}$ $u \in \{a,c\}$	2	$[<0,1>,<2,3>]$
	$\{1,1\}$	$\begin{pmatrix} a & a \\ 0 & b \end{pmatrix}$	2	$[<0,1>,<1,2>,<2,5>]$
3	$\{0,1\}$	$\begin{pmatrix} b & 0 & 0 \end{pmatrix}$	2	$[<0,1>,<1,1>]$
		$\begin{pmatrix} b & b & 0 \end{pmatrix}$	2	$[<0,1>,<2,1>]$
		$\begin{pmatrix} b & b & b \end{pmatrix}$	6	$[<0,1>,<3,1>]$
	$\{0,2\}$	$\begin{pmatrix} b & 0 & 0 \\ 0 & b & 0 \end{pmatrix}$	2	$[<0,1>,<1,2>,<2,1>]$
		$\begin{pmatrix} b & 0 & b \\ 0 & b & 0 \end{pmatrix}$	2	$[<0,1>,<1,1>,<2,1>,<3,1>]$
		$\begin{pmatrix} b & 0 & b \\ 0 & b & b \end{pmatrix}$	6	$[<0,1>,<2,3>]$
	$\{0,3\}$	$\begin{pmatrix} b & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & b \end{pmatrix}$	6	$[<0,1>,<1,3>,<2,3>,<3,1>]$
	$\{1,0\}$	$\begin{pmatrix} a & u & 0 \end{pmatrix}$ $u \in \{a,c\}$	2	$[<0,1>,<2,3>]$
		$\begin{pmatrix} a & u & b \end{pmatrix}$ $u \in \{a,c\}$	2	$[<0,1>,<2,1>,<3,2>]$
	$\{1,1\}$	$\begin{pmatrix} a & a & 0 \\ 0 & b & 0 \end{pmatrix}$	2	$[<0,1>,<1,2>,<2,5>]$
		$\begin{pmatrix} a & u & 0 \\ 0 & b & b \end{pmatrix}$ $u \in \{a,c\}$	2	$[<0,1>,<2,5>,<3,2>]$
		$\begin{pmatrix} a & u & 0 \\ 0 & 0 & b \end{pmatrix}$ $u \in \{a,c\}$	2	$[<0,1>,<1,1>,<2,3>,<3,3>]$
		$\begin{pmatrix} a & a & b \\ 0 & b & 0 \end{pmatrix}$	2	$[<0,1>,<1,2>,<2,1>,<3,4>]$
	$\{1,2\}$	$\begin{pmatrix} a & a & 0 \\ 0 & b & 0 \\ 0 & 0 & b \end{pmatrix}$	2	$[<0,1>,<1,3>,<2,7>,<3,5>]$

Example 3. *Consider the self-orthogonal code $\mathcal{C}$ of length 3 over E of type $\{1,1\}$ given by the generator matrix $\begin{pmatrix} a & a & 0 \\ 0 & 0 & c \end{pmatrix}$. Its automorphism group has order two and hence,*

$$\frac{3!}{|Aut(\mathcal{C})|} = \frac{6}{2} = 3.$$

From Theorem 8, $M_E(3,1,1) = \Phi(3,1)\begin{bmatrix} 3-2 \\ 1 \end{bmatrix}_2 2^{3-2-1} = 3$. Therefore, there is a unique self-orthogonal code over E of length 3 and type $\{1,1\}$, up to equivalence.

We also have the classification of self-orthogonal codes over E for short lengths in Table 2.

Table 2. Inequivalent self-orthogonal codes of length $n \leq 4$ over E. The generator matrices for the codes where $k_1 = 0$ are the same as those in Table 1, but with b replaced with c.

n	$\{k_1, k_2\}$	Generator Matrix	$\lvert\mathbf{Aut}(\mathcal{C})\rvert$	Weight Distribution
2	$\{1,0\}$	$\begin{pmatrix} a & a \end{pmatrix}$	2	$[<0,1>,<2,3>]$
3	$\{1,0\}$	$\begin{pmatrix} a & a & 0 \end{pmatrix}$	2	$[<0,1>,<2,3>]$
		$\begin{pmatrix} a & a & c \end{pmatrix}$	2	$[<0,1>,<2,1>,<3,2>]$
	$\{1,1\}$	$\begin{pmatrix} a & a & 0 \\ 0 & 0 & c \end{pmatrix}$	2	$[<0,1>,<1,1>,<2,3>,<3,3>]$
4	$\{1,0\}$	$\begin{pmatrix} a & a & 0 & 0 \end{pmatrix}$	4	$[<0,1>,<2,3>]$
		$\begin{pmatrix} a & a & a & a \end{pmatrix}$	24	$[<0,1>,<4,3>]$
		$\begin{pmatrix} a & a & b & b \end{pmatrix}$	8	$[<0,1>,<4,3>]$
		$\begin{pmatrix} a & a & c & 0 \end{pmatrix}$	2	$[<0,1>,<2,1>,<3,2>]$
		$\begin{pmatrix} a & a & c & c \end{pmatrix}$	4	$[<0,1>,<2,1>,<4,2>]$
	$\{1,1\}$	$\begin{pmatrix} a & a & 0 & 0 \\ 0 & 0 & c & 0 \end{pmatrix}$	2	$[<0,1>,<1,1>,<2,3>,<3,3>]$
		$\begin{pmatrix} a & a & 0 & 0 \\ 0 & 0 & c & c \end{pmatrix}$	4	$[<0,1>,<2,4>,<4,3>]$
		$\begin{pmatrix} a & a & c & 0 \\ 0 & 0 & 0 & c \end{pmatrix}$	2	$[<0,1>,<1,1>,<2,1>,<3,3>,<4,2>]$
		$\begin{pmatrix} a & u & a & u \\ 0 & 0 & c & c \end{pmatrix}$ $u \in \{a,b\}$	8	$[<0,1>,<2,2>,<4,5>]$
		$\begin{pmatrix} a & a & c & 0 \\ 0 & 0 & c & c \end{pmatrix}$	4	$[<0,1>,<2,2>,<3,4>,<4,1>]$
	$\{1,2\}$	$\begin{pmatrix} a & a & 0 & 0 \\ 0 & 0 & c & 0 \\ 0 & 0 & 0 & c \end{pmatrix}$	4	$[<0,1>,<1,2>,<2,4>,<3,6>,<4,3>]$
		$\begin{pmatrix} a & a & a & a \\ 0 & c & c & 0 \\ 0 & 0 & c & c \end{pmatrix}$	24	$[<0,1>,<2,6>,<4,9>]$
	$\{2,0\}$	$\begin{pmatrix} a & a & 0 & 0 \\ 0 & 0 & a & a \end{pmatrix}$	8	$[<0,1>,<2,6>,<4,9>]$

The generators, order of automorphism group, and weight distribution of inequivalent self-orthogonal I-codes for $n = 4,5$ and inequivalent self-orthogonal E-codes for $n = 5$ may be requested by the interested reader from the authors.

In Table 3, we give a summary of the number of inequivalent self-orthogonal codes for small lengths over both the rings I and E of every possible type. The computations were performed in the MAGMA computer algebra system [29] using the so-called additive generator matrix, similar to the method used in [19,20].

Table 3. Number of inequivalent self-orthogonal codes over I and E of length $n \leq 5$. Entries marked with * are QSD codes, and those marked with ** are self-dual codes.

n	$\{k_1, k_2\}$	I-Codes	Remark	E-Codes	Remark
2	$\{0,1\}$	2		2	
	$\{0,2\}$	1	*	1	**, [20]
	$\{1,0\}$	2	*, [19]	1	**, [20]
	$\{1,1\}$	1	**	-	
3	$\{0,1\}$	3		3	
	$\{0,2\}$	3		3	
	$\{0,3\}$	1	*	1	**, [20]
	$\{1,0\}$	4		2	
	$\{1,1\}$	6	*, [19]	1	**, [20]
	$\{1,2\}$	1		-	
4	$\{0,1\}$	4		4	
	$\{0,2\}$	6		6	
	$\{0,3\}$	4		4	
	$\{0,4\}$	1	*	1	**, (Table 1 in [20])
	$\{1,0\}$	9		5	
	$\{1,1\}$	23		6	
	$\{1,2\}$	14	*	2	**, (Table 1 in [20])
	$\{1,3\}$	2		-	
	$\{2,0\}$	10	*	1	**, (Table 1 in [20])
	$\{2,1\}$	7		-	
	$\{2,2\}$	1	**	-	
5	$\{0,1\}$	5		5	
	$\{0,2\}$	10		10	
	$\{0,3\}$	10		10	
	$\{0,4\}$	5		5	
	$\{0,5\}$	1	*	1	**, (Table 2 in [20])
	$\{1,0\}$	14		8	
	$\{1,1\}$	59		18	
	$\{1,2\}$	66		12	
	$\{1,3\}$	24	*	2	**, (Table 2 in [20])
	$\{1,4\}$	2		-	
	$\{2,0\}$	36		3	
	$\{2,1\}$	60	*	1	**, (Table 2 in [20])
	$\{2,2\}$	17		-	
	$\{2,3\}$	1		-	

8. Conclusions and Open Problems

In the present paper, we have derived mass formulas for self-dual and self-orthogonal codes over two non-unitary rings of order four, namely, E and I in the notation of Fine [23]. These formulas have been employed to classify these codes in short lengths and small types. To reach higher lengths would require more computer power or sharper algorithms.

A natural generalization would be to consider similar rings of order p^2 for p being a prime greater than 2.

Author Contributions: Conceptualization, A.A. (Adel Alahmadi), R.A.B., L.G. and P.S.; methodology, A.A. (Adel Alahmadi), R.A.B., L.G. and P.S.; validation, A.A. (Adel Alahmadi), A.A. (Altaf Alshuhail), R.A.B., L.G. and P.S.; investigation, A.A. (Adel Alahmadi), A.A. (Altaf Alshuhail), R.A.B., L.G. and P.S.; resources, A.A. (Adel Alahmadi) and R.A.B.; writing—original draft preparation, R.A.B. and L.G.; writing—review and editing, A.A. (Adel Alahmadi), A.A. (Altaf Alshuhail) and P.S.; supervision, A.A. (Adel Alahmadi) and P.S. All authors have read and agreed to the published version of the manuscript.

Funding: The Deanship of Scientific Research (DSR) at King Abdulaziz University (KAU), Jeddah, Saudi Arabia has funded this project, under grant no. (KEP.-PhD: 99-130-1443).

Data Availability Statement: Data is available upon request to the corresponding author.

Acknowledgments: The Deanship of Scientific Research (DSR) at King Abdulaziz University (KAU), Jeddah, Saudi Arabia has funded this project, under grant no. (KEP.-PhD: 99-130-1443). Also, R.A.B. and L.G. acknowledge the support by the Computational Research Program of the Institute of Mathematics, University of the Philippines Diliman. The authors also acknowledge the anonymous reviewers for their comments and suggestions to improve the presentation of this manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Assmus, E.F., Jr.; Mattson, H.F., Jr. New 5-designs. *Comb. Theory* **1969**, *6*, 122–151. [CrossRef]
2. Bose, R.C.; Ray-Chaudhuri, D.K. On a class of error correcting binary group codes. *Inf. Control* **1960**, *3*, 68–79. [CrossRef]
3. Betsumiya, K.; Gulliver, T.A.; Harada, M.; Munemasa, A. On type II codes over $\mathbb{F}_4$. *IEEE Trans. Inform. Theory* **2001**, *47*, 2242–2248. [CrossRef]
4. Hocquenghem, A. Codes correcteurs d'erreurs. *Chiffres (French)* **1959**, *2*, 147–156.
5. Huffman, W.C.; Pless, V. *Fundamentals of Error-Correcting Codes*; Cambridge University Press: Cambridge, MA, USA, 2003.
6. Hartmann, C.R.P.; Tzeng, K.K. Generalizations of the BCH bound. *Inf. Control* **1972**, *20*, 489–498. [CrossRef]
7. Massey, J.L. Linear codes with complementary duals. *Discret. Math.* **1992**, *106*, 337–342. [CrossRef]
8. Massey, J.L. Reversible codes. *Inf. Control* **1964**, *7*, 369–380. [CrossRef]
9. Roos, C. A generalization of the BCH bound for cyclic codes, including the Hartmann-Tzeng bound. *J. Comb. Theory Ser. A* **1982**, *33*, 229–232. [CrossRef]
10. Conway, J.H.; Sloane, N.J.A. *Sphere Packings, Lattices and Groups*, 3rd ed.; Springer: New York, NY, USA, 1999.
11. van Lint, J.H.; Wilson, R. On the minimum distance of cyclic codes. *IEEE Trans. Inf. Theory* **1986**, *32*, 23–40. [CrossRef]
12. Abualrub, T.; Oehmke, R. Cyclic codes of length 2^e over $\mathbb{Z}_4$. *Discret. Appl. Math.* **2003**, *128*, 3–9. [CrossRef]
13. Blackford, T. Cyclic codes of oddly even length over $\mathbb{Z}_4$. *Discret. Appl. Math.* **2003**, *128*, 27–46 [CrossRef]
14. Dougherty, S.T.; Ling, S. Cyclic codes over $\mathbb{Z}_4$ of even length. *Des. Codes Cryptography* **2006**, *39*, 127–153. [CrossRef]
15. Jitman, S.; Sangwisut, E.; Udomkavanich, P. Hulls of cyclic codes over $\mathbb{Z}_4$. *Discret. Math.* **2020**, *343*, 111621. [CrossRef]
16. Pless, V.; Qian, Z. Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$. *IEEE Trans. Inf. Theory* **1996**, *42*, 1594–1600. [CrossRef]
17. Prakash, O.; Yadav, S.; Verma, R.K. Constacyclic and linear complementary dual codes over $\mathbb{F}_q + u\mathbb{F}_q$. *Def. Sci. J.* **2020**, *70*, 626–632. [CrossRef]
18. Alahmadi, A.; Alkathiry, A.; Altassan, A.; Basaffar, W.; Bonnecaze, A.; Shoaib, H.; Solé, P. Type IV codes over a non-local non-unital ring. *Proyecciones (Antofagasta)* **2020**, *39*, 963–978. [CrossRef]
19. Alahmadi, A.; Altassan, A.; Basaffar, W.; Bonnecaze, A.; Shoaib, H.; Solé, P. Quasi type IV codes over a non-unital ring. *Appl. Algebra Eng. Commun. Comput.* **2021**, *32*, 217–228. [CrossRef]
20. Alahmadi, A.; Altassan, A.; Basaffar, W.; Shoaib, H.; Bonnecaze, A.; Solé, P. Type IV codes over a non-unital ring. *J. Algebra Its Appl.* **2022**, *21*, 2250142. [CrossRef]
21. Alahmadi, A.; Melaibari, A.; Solé, P. Duality of codes over non-unital rings of order four. *IEEE Access* **2023**, *11*, 53120–53133. [CrossRef]
22. Kim, J.-L.; Ohk, D.E. DNA codes over two noncommutative rings of order four. *J. Appl. Math. Comput.* **2022**, *68*, 2015–2038. [CrossRef]
23. Fine, B. Classification of finite rings of order p^2. *Math. Mag.* **1993**, *66*, 248–252. [CrossRef]
24. Raghavendran, R. A class of finite rings. *Compos. Math.* **1970**, *22*, 49–57.
25. Hammons, A.R.; Kumar, P.V.; Calderbank, A.R.; Sloane, N.J.A.; Solé, P. The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Trans. Inf. Theory* **1994**, *40*, 301–319. [CrossRef]
26. Dougherty, S.T.; Gaborit, P.; Harada, M.; Solé, P. Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$. *IEEE Trans. Inf. Theory* **1999**, *45*, 32–45. [CrossRef]
27. Galvez, L.; Betty, R.A.; Nemenzo, F. Self-orthogonal Codes over $\mathbb{F}_q + u\mathbb{F}_q$ and $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$. *Eur. J. Pure Appl. Math.* **2020**, *13*, 873–892. [CrossRef]

28. Hou, X.-D. On the number of inequivalent binary self-orthogonal codes. *IEEE Trans. Inf. Theory* **2007**, *53*, 2459–2479.
29. Bosma, W.; Cannon, J.; Playoust, C. The Magma algebra system. I. The user language. *J. Symb. Comput.* **1997**, *24*, 235–265. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.