

The Mass Formula for Self-Orthogonal and Self-Dual Codes over a Non-Unitary Non-Commutative Ring

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. The Mass Formula for Self-Orthogonal and Self-Dual Codes over a Non-Unitary Non-Commutative Ring. Mathematics , 2024, 12, pp.862. 10.3390/math12060862 . hal-04505889

HAL Id: hal-04505889 https://hal.science/hal-04505889

Submitted on 15 Mar 2024

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





Adel Alahmadi^{1,*}, Altaf Alshuhail^{1,2}, Rowena Alma Betty³, Lucky Galvez³ and Patrick Solé⁴

- Research Group of Algebraic Structures and Applications, Department of Mathematics, Faculty of Science, King Abdulaziz University, Jeddah 21589, Saudi Arabia; ad.alshuhail@uoh.edu.sa
- 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; rabetty@math.upd.edu.ph (R.A.B.); legalvez@math.upd.edu.ph (L.G.)
- ⁴ I2M, (CNRS, University of Aix-Marseille, Centrale Marseille), 13009 Marseilles, France; sole@enst.fr
- Correspondence: analahmadi@kau.edu.sa

Abstract: In this paper, we derive a mass formula for the self-orthogonal codes and self-dual codes over a non-commutative non-unitary ring, namely, $E_p = \langle a, b | pa = pb = 0, a^2 = a, b^2 = b, ab = a, ba = b \rangle$, where $a \neq b$ and p is any odd prime. We also give a classification of self-orthogonal codes and self-dual codes over E_p , where p = 3, 5, and 7, in short lengths.

Keywords: non-unitary non-commutative rings; left self-dual codes; self-dual codes; mass formula

MSC: 94B05; 16D10

1. Introduction

Mass formulas serve as important tools for classifying self-dual codes over finite fields [1–5] and unitary rings [6–11]. When generating nonequivalent self-dual codes, mass formulas serve as terminating flags for the computing effort. Recently, this methodology was extended to the non-unitary ring I, in the terminology of [12], where quasi self-dual codes, a special class of self-orthogonal codes, serve as the central objects for classification [13,14]. Even more recently, a satisfying definition of self-dual codes for non-unitary non commutative rings was introduced in [15]. It is the intersection of the right dual with the left dual. Thus, a non-commutative ring leads to three types of self-dual codes: left self-dual, right self-dual and self-dual.

In the present note, we present mass formulas for self-orthogonal codes, self-dual codes, and left self-dual codes over the non-commutative non-unitary ring of order p^2 , for p an odd prime, and type E in the classification of Fine [12]. This ring is henceforth denoted by E_p . We apply them to the classification of these codes when p = 3, 5, 7 in short lengths. The proof techniques combine self-dual mass formula over finite field, and linear algebra over the ring E_3 which is reminiscent of that on chain rings of depth 2 [9,10].

The content is organized in the following manner: Section 2 introduces essential preliminary concepts and notations necessary for comprehending the remainder of the paper. In Section 3, the framework of linear codes over E_p is established. Section 4 elaborates on the mass formulas. Section 5 is dedicated to the classification in short lengths for fixed types. Finally, Section 6 serves as the conclusion of the article

2. Preliminaries

2.1. Codes over \mathbb{F}_p

Let *p* be an odd prime number. A **linear code** C of length *n* and dimension *k* over a finite field \mathbb{F}_p is an \mathbb{F}_p -subspace of the vector space \mathbb{F}_p^n of dimension *k*. Compactly, we call C an [n, k]-code. The elements of a code are called **codewords**. Two codewords



Citation: Alahmadi, A.; Alshuhail, A.; Betty, R.A.; Galvez, L.; Solé, P. The Mass Formula for Self-Orthogonal and Self-Dual Codes over a Non-Unitary Non-Commutative Ring. *Mathematics* **2024**, *12*, 862. https:// doi.org/10.3390/math12060862

Academic Editor: Askar Tuganbaev

Received: 20 November 2023 Revised: 1 January 2024 Accepted: 5 January 2024 Published: 15 March 2024



Copyright: © 2024 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/). $\mathbf{x} = (x_1, x_2, ..., x_n)$ and $\mathbf{y} = (y_1, y_2, ..., y_n)$ are orthogonal if their standard inner product $(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^n x_i y_i$ is zero, and the vector space consisting of all vectors in \mathbb{F}_p^n that are orthogonal to every codeword in \mathcal{C} is called the **dual** of \mathcal{C} , denoted by \mathcal{C}^{\perp} . \mathcal{C} is said to be **self-orthogonal** (resp. **self-dual**) if $\mathcal{C} \subseteq \mathcal{C}^{\perp}$ (resp. $\mathcal{C} = \mathcal{C}^{\perp}$).

2.2. Additive Codes over \mathbb{F}_{p^2}

Let ω be a primitive element in \mathbb{F}_{p^2} , so that ω has order $r = p^2 - 1$ and $\omega^t \neq 1 \forall 0 \le t \le r$. Then $\mathbb{F}_{p^2} = \{0, 1, \omega, \omega^2, \cdots, \omega^{r-1}\}$. The **trace map**, $Tr : \mathbb{F}_{p^2} \mapsto \mathbb{F}_p$, is defined by $Tr(u) = u + u^p$. An **additive code** of length n over \mathbb{F}_{p^2} is \mathbb{F}_p -additive subgroup of $\mathbb{F}_{p^2}^n$ containing p^k codewords for some integer k in the range $0 \le k \le 2n$.

2.3. The Ring E_p

Following [12], we define a ring on two distinct generators *a*, *b* by their relations

$$E_p = \langle a, b \mid pa = pb = 0, a^2 = a, b^2 = b, ab = a, ba = b \rangle.$$

Thus, E_p consists of p^2 elements and has characteristic p. We also define a natural action of \mathbb{F}_p on E_p by the rule rx = xr, for all $r \in E_p$ and for all $x \in \mathbb{F}_p$.

Lemma 1. The ring E_p does not contain a unity element.

Proof. Assume, by contradiction, that there is a unique element *e* in E_p such that eu = ue = u for every $0 \neq u \in E_p$. Since E_p is generated by *a* and *b*, *e* can be written as

$$e = ai + bj$$
, for some $0 \le i, j \le p - 1$.

Choose u = a. By assumption,

$$(ai+bj)a = a(ai+bj) = a,$$

which implies e = a. Also, choose u = a + b. Then

$$a(a + b) = a^2 + ab = a + a = 2a \neq a + b.$$

So *a* is not the unity of E_p , which leads to an inconsistency. Therefore, E_p is a non-unital ring. \Box

From the ring representation of E_p and Lemma 1, E_p is a non-commutative ring without multiplicative identity. Moreover, E_p contains a unique maximal ideal

$$J_p = \{e_{xy} \mid e_{xy} = ax + by \text{ with } x + y \equiv 0 \pmod{p} \text{ where } 0 \le x, y$$

Thus, we can write E_p as

$$E_p = \{c_{xy} = ax + ey \mid x, y \in \mathbb{F}_p\}.$$
(1)

Define the reduction map modulo J_p as $\alpha : E_p \mapsto E_p/J_p \cong \mathbb{F}_p$ by $\alpha(ax + ey) = x$ where $0 \le x < p$. This map can be extended in the natural way from E_p^n to \mathbb{F}_p^n .

3. Codes over E_p

A linear code C of length n over E_p , or simply an E_p -code, is a one-sided E_p -submodule of E_p^n . We denote the (Hamming) weight of $\mathbf{x} \in E_p^n$ by $wt(\mathbf{x})$ and adapt the notation

$$[< 0, 1 >, \cdots, < i, A_i >, \cdots, < n, A_n >],$$

where A_i is the number of codewords of Hamming weight *i*, for the weight distribution of a code over E_p as in Magma [16]. The inner product between two vectors $\mathbf{x} =$

 $(x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_n) \in E_p^n$ is defined as $(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^n x_i y_i$. For an E_p -code *C*, the **right dual** of *C*, defined as

$$\mathcal{C}^{\perp_R} = \{ \mathbf{y} \in E_n^n | \forall \mathbf{x} \in \mathcal{C}, (\mathbf{x}, \mathbf{y}) = 0 \},\$$

is a right module of E_p^n , while the **left dual** of C, defined as

$$\mathcal{C}^{\perp_L} = \{ \mathbf{y} \in E_p^n | \forall \mathbf{x} \in \mathcal{C}, (\mathbf{y}, \mathbf{x}) = 0 \},\$$

is a left module of E_p^n . The two-sided dual of C is $C^{\perp} = C^{\perp_R} \cap C^{\perp_L}$. The code C is said to be **self-orthogonal** if every a codeword in C is orthogonal to every codeword in C, that is, $C \subseteq C^{\perp}$. If $C = C^{\perp_R}$ (resp. $C = C^{\perp_L}$) then C is **right self-dual (RSD)** (resp. **left self-dual** (**LSD**)). If $C = C^{\perp}$, then C is **self-dual (SD)**.

Using the map $\phi : E_p \mapsto \mathbb{F}_{p^2}$ defined as

$$\phi(0) = 0, \phi(a) = \omega, \text{ and } \phi(b) = -\omega + 1,$$
 (2)

we can attach to an E_p -code C an additive \mathbb{F}_{p^2} -code $\phi(C) = \{(\phi(c_1), \phi(c_2), \dots, \phi(c)_n) \mid (c_1, c_2, \dots, c_n) \in C\}$. It can be easily seen that $Tr(\phi(u)) = \alpha(u)$ for all $u \in E_p$.

Lemma 2.

- (*i*) For any positive integer n, there exist a self-orthogonal code over E_p of length n.
- (ii) For any odd prime p, there is a left self-orthogonal code ($C \subseteq C^{\perp_L}$) over E_p .

Proof.

(i) Consider J_p as linear code over E_p of length 1. To prove the self-orthogonality of J_p , for all (ai + bj), $(ai' + bj') \in J_p$, we have that

$$(ai + bj, ai' + bj') = a((i' + j')i) + b((i' + j')j),$$

$$(ai' + bj', ai + bj) = a((i + j)i') + b((i + j)j').$$

Since (ai + bj), $(ai' + bj') \in J_p$, it follows that, $i + j \equiv 0$ and $i' + j' \equiv 0 \pmod{p}$. Then, $J_p \subseteq J_p^{\perp_R} \cap J_p^{\perp_L} = J_p^{\perp}$. Taking the direct sum of *n* copies of this code yields a self-orthogonal code of any length *n*.

(ii) Let *p* be a prime and let $\mathbf{1}_p$ denote the all-one codeword of length *p*. The repetition code of length *p* is then defined by $R_p = \{u(\mathbf{1}_p) | u \in E_p\}$. Clearly R_p is a linear code over E_p . Since E_p has characteristic *p*, then we have that $R_p \subseteq R_p^{\perp_L}$.

Let C be linear code over E_p . We define the **residue** code of C as

$$\mathbf{res}(\mathcal{C}) = \{ \mathbf{x} \in \mathbb{F}_p^n | \exists \mathbf{y} \in \mathbb{F}_p^n \text{ such that } a\mathbf{x} + e\mathbf{y} \in \mathcal{C} \}.$$

and the **torsion** code of C as

$$\mathbf{tor}(\mathcal{C}) = \{ \mathbf{y} \in \mathbb{F}_p^n | e\mathbf{y} \in \mathcal{C} \}.$$

From Equation (2), we have $\operatorname{res}(\mathcal{C}) = Tr(\phi(\mathcal{C}))$ and $\operatorname{tor}(\mathcal{C})$ is the subfield subcode of $\phi(\mathcal{C})$ defined by $\phi(\mathcal{C}) \cap \mathbb{F}_p^n$. Let $\alpha_{\mathcal{C}}$ be the restriction of α to \mathcal{C} . We have that $e \operatorname{tor}(\mathcal{C}) = Ker \alpha_{\mathcal{C}}$, and that $\operatorname{res}(\mathcal{C}) = Im \alpha_{\mathcal{C}}$. Let $\operatorname{dim}(\operatorname{res}(\mathcal{C})) = k_1$ and $k_2 = \operatorname{dim}(\operatorname{tor}(\mathcal{C})) - k_1$. We say that \mathcal{C} is linear code of **type** $\{k_1, k_2\}$. It can be seen that \mathcal{C} is **free** as an E_p -module if and only if $\operatorname{res}(\mathcal{C}) = \operatorname{tor}(\mathcal{C})$. By the first isomorphism theorem applied to $\alpha_{\mathcal{C}}$ we have $|\mathcal{C}| = p^{2k_1+k_2}$.

In Theorem 1, we will extend a few results from [15,17] by simply substituting codes over \mathbb{F}_p for binary codes in the proofs.

Theorem 1. Suppose C is a linear code over E_p . Let k_1, k_2, n be non-negative integers with $k_1 + k_2 \le n$. Then the following hold:

(*i*) Every linear code C over E_p of length n and type $\{k_1, k_2\}$ is equivalent to a code with generator matrix in standard form

$$\begin{bmatrix} aI_{k_1} & aA + eB \\ 0 & eZ \end{bmatrix}$$
(3)

where I_{k_1} is the identity matrix, the matrices A, B and Z have entries from \mathbb{F}_p .

- (ii) $a \operatorname{res}(\mathcal{C}) \subseteq \mathcal{C} \text{ and } \operatorname{res}(\mathcal{C}) \subseteq \operatorname{tor}(\mathcal{C}).$
- (iii) $C = a \operatorname{res}(C) \oplus e \operatorname{tor}(C)$
- (iv) $\mathcal{C}^{\perp_R} = a \operatorname{tor}(\mathcal{C})^{\perp} \oplus e \mathbb{F}_p^n$.
- (v) $\mathcal{C}^{\perp_L} = a \operatorname{res}(\mathcal{C})^{\perp} \oplus e \operatorname{res}(\mathcal{C})^{\perp}.$
- (vi) $\mathcal{C}^{\perp} = a \operatorname{tor}(\mathcal{C})^{\perp} \oplus e \operatorname{res}(\mathcal{C})^{\perp}$.

If *G* is a $k \times n$ matrix over E_p , we denote by $E_p^k G$ the code of length *n* over E_p with generator matrix *G*.

Next, we make a modification on the construction of self-orthogonal codes, (left or right) self-dual codes, and self-dual codes in [15], to be suitable for an odd prime p.

Theorem 2. If $C = aC_1 \oplus eC_2$ is a linear code over E_p such that C_1 and C_2 be arbitrary linear codes over \mathbb{F}_p , then

- (*i*) C is a self-orthogonal code if and only if $C_1 \subseteq C_2 \subseteq C_1^{\perp}$;
- (*ii*) C is a self-dual if and only if $C_1 \subseteq C_2 = C_1^{\perp}$;
- (iii) *C* is a left self-dual if and only if $C_1 = C_2 = C_1^{\perp}$;
- (iv) C is a right self-dual if and only if $C = e \mathbb{F}_{p}^{n}$.

Proof. First, we will prove that $C_1 = \operatorname{res}(C)$ and $C_2 = \operatorname{tor}(C)$. Observe that $C_1 = \alpha(a C_1) \subseteq \operatorname{res}(C)$. Let $\mathbf{x} \in \operatorname{res}(C)$. Then $a\mathbf{x} + e\mathbf{0} \in C$, so $\mathbf{x} \in C_1$, thus, we have $\operatorname{res}(C) = C_1$. Now, $eC_2 \subseteq C$, so by definition of torsion code, C_2 is a subset of $\operatorname{tor}(C)$. Let $\mathbf{y} \in \operatorname{tor}(C)$. Since the zero vector is in C_1 , $e\mathbf{y} = a\mathbf{0} + e\mathbf{y} \in C$. Therefore, $\mathbf{y} \in C_2$.

(i) Let C be a self-orthogonal code. Note that $C_1 \subseteq C_2$. Suppose that $z \in C_2$. Since C is self-orthogonal, for all $ax + ey \in C$, we have

$$0 = (a\mathbf{x} + e\mathbf{y}, e\mathbf{z}) = e(\mathbf{x}, \mathbf{z}).$$

Hence $C_2 \subseteq C_1^{\perp}$. Conversely, to prove the self-orthogonality of C, for all $\mathbf{x}, \mathbf{x}' \in C_1$ and for all $\mathbf{y}, \mathbf{y}' \in C_2$ we have

$$(\mathbf{c}, \mathbf{c}') = (a\mathbf{x} + e\mathbf{y}, a\mathbf{x}' + e\mathbf{y}')$$

= $a(\mathbf{x}, \mathbf{x}') + 0(\mathbf{x}, \mathbf{y}') + e(\mathbf{y}, \mathbf{x}') + 0(\mathbf{y}, \mathbf{y}')$
= $a(0) + 0 + e(0) + 0 = 0,$

since $C_1 \subseteq C_2 \subseteq C_1^{\perp}$.

- (ii) Let C be a self-dual code. Then from the preceding case, $C_1 \subseteq C_2 \subseteq C_1^{\perp}$. Now, let $\mathbf{x} \in C_1^{\perp}$ be arbitrary. From Theorem 1 (vi), we have $e\mathbf{x} \in C$. Hence, $\mathbf{x} \in \text{tor}(C) = C_2$. It follows that $C_2 = C_1^{\perp}$. For the converse, suppose that $C_1 \subseteq C_2 = C_1^{\perp}$. From the preceding case, we have $C \subseteq C^{\perp}$. Since $|C| = p^{2k_1+k_2}$ and $C_2 = C_1^{\perp}$, $p^{k_1+(n-k_1)} = p^n$. It follows that $C = C^{\perp}$.
- (iii) C is left self-dual code if and only if $C_1 = C_1^{\perp} = C_2$, by Theorem 1 (iii) and (v).
- (iv) C is right self-dual code if and only if $C_1 = C_2^{\perp}$ (by Theorem 1 (iii) and (iv)). Equivalently, we have $C_1^{\perp} = (C_2^{\perp})^{\perp} = C_2 = \mathbb{F}_p^n$ if and only if $C_1 = \{0\}$ if and only if $C = e \mathbb{F}_p^n$.

4. Computation of the Mass Formula

At the start, we define the notion of equivalence of codes. Two codes C and C' over E_p are **monomially equivalent** if there is an $n \times n$ monomial matrix M (with exactly one entry $\in \{1, -1\}$ in each row and column and all other entries are zero) such that $C' = \{cM : c \in C\}$. The **monomial automorphism** group Aut(C) of code C consists of all M such that C = CM. Let M_n be the signed symmetric group of order $|M_n| = 2^n n!$. The number of codes equivalent to a code C of length n is

$$\frac{|M_n|}{|Aut(\mathcal{C})|}.$$

The mass formula for self-orthogonal codes is given by

$$\sum_{\mathcal{C}} \frac{|M_n|}{|Aut(\mathcal{C})|},$$

where the sum runs through all inequivalent self-orthogonal codes C over E_p of length n.

We apply a similar approach to that used for the computation of a mass formula in [7]. Let C_1 be a code over \mathbb{F}_p of length n with dimension k_1 and generator matrix

$$I_{k_1} \quad A \quad], \tag{4}$$

and C_2 be a code over \mathbb{F}_p of length *n* with dimension $k_1 + k_2$ and generator matrix

$$\begin{bmatrix} I_{k_1} & A \\ 0 & Z \end{bmatrix},$$
(5)

where $A \in M_{k_1 \times (n-k_1)}(\mathbb{F}_p)$, and $Z \in M_{k_2 \times (n-k_1)}(\mathbb{F}_p)$ is of full row rank. Observe that $C_1 \subseteq C_2$, and the code with generator matrix (3) has residue code C_1 and torsion code C_2 . We need the following lemmas to count the number free self-orthogonal E_p -codes.

Lemma 3. If C is a free E_p -code of length n, then the matrix B in Theorem 1 (i) is unique.

Proof. Suppose C is a free code and there exist $B_1, B_2 \in M_{k_1 \times (n-k_1)}(\mathbb{F}_p)$ such that

$$E_p^{k_1}[aI_{k_1} aA + eB_1] = E_p^{k_1}[aI_{k_1} aA + eB_2].$$
(6)

Then $aA + eB_1 = aA + eB_2$. Hence, $B_1 = B_2$.

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

$$K_{k_1} + AA^T = 0,$$
 (7)

and

$$ZA^T = 0. (8)$$

It follows from (7) that A is of full row rank.

Lemma 4. The map f_A defined by

$$f_A: M_{k_1 \times m}(\mathbb{F}_p) \to M_{k_1 \times k_1}(\mathbb{F}_p)$$
$$X \mapsto AX^T$$

is a surjective linear map.

Proof. Note that f_A is a linear map by properties of matrix. To prove the surjective condition, choose an arbitrary matrix G in $M_{k_1 \times k_1}(\mathbb{F}_p)$. Consider the matrix $-G^T A$ in $M_{k_1 \times m}(\mathbb{F}_p)$. We have

$$f_A(-G^T A) = A(-G^T A)^T = -AA^T G = I_{k_1}(G) = G.$$

Now, let us consider the sets

 $\mathbf{X} = \{ \mathcal{C} \mid \mathcal{C} \text{ be a self-orthogonal } E_p \text{-code, with } \mathbf{res}(\mathcal{C}) = C_1 = \mathbf{tor}(\mathcal{C}) \}, \\ \mathbf{X}' = \{ \mathcal{C}' \mid \mathcal{C}' \text{ be a self-orthogonal } E_p \text{-code, with } \mathbf{res}(\mathcal{C}') = C_1, \mathbf{tor}(\mathcal{C}') = C_2 \}.$

Lemma 5. If $C' \in \mathbf{X}'$, then $|\{C \in \mathbf{X} \mid C \subseteq C'\}| = p^{k_1k_2}$.

Proof. By Theorem 1 (i), C' has a generator matrix (3). Consider the map

$$\mu: M_{k_1 \times k_2}(\mathbb{F}_p) \to \{ \mathcal{C} \in \mathbf{X} \mid \mathcal{C} \subseteq \mathcal{C}' \}$$
$$M \mapsto E_p^{k_1}[a I_{k_1} \ aA + e(B + MZ)].$$

Clearly, μ is well defined. Now, we will show that μ is bijective. Suppose $M_1, M_2 \in M_{k_1 \times k_2}(\mathbb{F}_p)$ such that $\mu(M_1) = \mu(M_2)$. Then $aA + e(B + M_1Z) = aA + e(B + M_2Z)$. Since Z is of full row rank, we conclude $M_1 = M_2$, which shows that μ is injective. Now, suppose that $C \in X$ such that $C \subseteq C'$. By Theorem 1 (i), $C = E_p^{k_1}[a I_{k_1} aA + eF]$, for some matrix F. The inclusion $C \subseteq C'$ implies that

$$aA + eF = aA + e(B + MZ)$$

for some matrix *M* of size $k_1 \times k_2$. So F = B + MZ, which shows that μ is surjective, and hence, μ is bijective. Therefore,

$$|\{\mathcal{C} \in \mathbf{X} \mid \mathcal{C} \subseteq \mathcal{C}'\}| = |M_{k_1 \times k_2}(\mathbb{F}_p)| = p^{k_1 k_2}.$$

Lemma 6. If $C \in \mathbf{X}$, then there is a unique code $C' \in \mathbf{X}'$, such that $C \subseteq C'$.

Proof. By Theorem 1 (i) and Lemma 3, C has a generator matrix $[aI_{k_1} \ aA + eB]$ for some unique matrix B. Then the code C'_0 with a generator matrix

$$\begin{bmatrix} aI_{k_1} & aA + eB\\ 0 & eZ \end{bmatrix}$$
(9)

satisfies $\operatorname{res}(\mathcal{C}'_0) = C_1$, and $\operatorname{tor}(\mathcal{C}'_0) = C_2$. Since $\mathcal{C} \in \mathbf{X}$, (8) implies that \mathcal{C}'_0 is a self-orthogonal code, hence $\mathcal{C}'_0 \in \mathbf{X}'$. Now, suppose that $\mathcal{C}' \in \mathbf{X}'$ and $\mathcal{C} \subseteq \mathcal{C}'$. By Theorem 1 (i), we have that $E_p^{k_2} [0 \ eZ] \subseteq \mathcal{C}'$. This, together with $\mathcal{C} \subseteq \mathcal{C}'$ forces $\mathcal{C}'_0 \subseteq \mathcal{C}'$. Since $|\mathcal{C}'_0| = |\mathcal{C}'|$, we have $\mathcal{C}'_0 = \mathcal{C}'$. \Box

Let $\sigma_p(n, k_1)$ be the number of self-orthogonal codes of length n and dimension k_1 over \mathbb{F}_p , which is found in [18–20].

In [21], the number of subspaces of dimension *k* contained in an *n*-dimensional vector space over \mathbb{F}_p is given by the Gaussian coefficient $\begin{bmatrix} j \\ i \end{bmatrix}_p$ for $i \leq j$, where $\begin{bmatrix} i \end{bmatrix} \qquad (p^j - 1)(p^j - p) \dots (p^j - p^{i-1})$

$$\begin{bmatrix} j \\ i \end{bmatrix}_p = \frac{(p^j - 1)(p^j - p)\dots(p^j - p^{i-1})}{(p^i - 1)(p^i - p)\dots(p^i - p^{i-1})}.$$

Let $\sigma_{E_p}(n, k_1, k_2)$ be the number of distinct self-orthogonal codes over E_p of length n. Mass formulas are useful for finding all inequivalent codes of given length. Our goal now is to compute $\sigma_{E_p}(n, k_1, k_2)$. **Theorem 3.** For all codes of length n with type $\{k_1, 0\}$, the number of free self-orthogonal codes over E_p is

$$\sigma_{E_n}(n,k_1,0) = \sigma_p(n,k_1)p^{k_1(n-2k_1)}.$$
(10)

Proof. We may assume without loss of generality that C_1 is a code with generator matrix (4). If C is a self-orthogonal code of length n over E_p of type $\{k_1, 0\}$, then by setting $C_1 =$ **res**(C) = **tor**(C), C_1 satisfies Theorem 2 (i). We have $\sigma_p(n, k_1)$ codes C_1 , which is the number of self-orthogonal codes over \mathbb{F}_p . By Theorem 1 (i), C has generator matrix [$a I_{k_1} aA + eB$]. Finally, we have

$$a^2 I_{k_1} + a^2 A A^T + a e A B^T + e a B A^T + e^2 B B^T = 0$$

so,

$$a(I_{k_1} + AA^T) + e(BA^T) = 0$$

Since $C_1 \subseteq C_1^{\perp}$, then $I_{k_1} + AA^T = 0$. Now, we have find the number of the matrix *B* which satisfies $AB^T = 0$. Setting $m = n - k_1$ in the linear map f_A in Lemma 4,

$$|\{B \in M_{k_1 \times n - k_1}(\mathbb{F}_p) \mid AB^T = 0\}| = |Ker f_A| = \frac{|M_{k_1 \times n - k_1}(\mathbb{F}_p)|}{|Im f_A|} = \frac{p^{k_1(n-k_1)}}{p^{k_1^2}}.$$
 (11)

Example 1. We consider the case n = 3, and p = 3. In Table 1, we give the list of inequivalent selforthogonal codes over the ring E_3 of type $\{1,0\}$. Using the mass formula in Theorem 3, we have the following computations:

$$\sum_{i=1}^{3} \frac{1}{|Aut(\mathcal{C}_i)|} = \frac{1}{12} + \frac{1}{6} = \frac{4 \cdot 3^{1(3-2)}}{48} = \frac{\sigma_{E_3}(3,1,0)}{2^3 \cdot 3!}.$$
(12)

In the next theorem, we give the number of self-orthogonal codes over E_p .

Theorem 4. The number of self-orthogonal codes over E_p of length n with type $\{k_1, k_2\}$ is given by

$$\sigma_{E_p}(n,k_1,k_2) = \sigma_p(n,k_1) \begin{bmatrix} n-2k_1 \\ k_2 \end{bmatrix}_p p^{k_1(n-2k_1-k_2)}.$$
(13)

Proof. We may assume without loss of generality that C_1 and C_2 are codes with generator matrices (4) and (5), respectively. Let C be a self-orthogonal code of length n over E_p of type $\{k_1, k_2\}$. By setting $C_1 = \operatorname{res}(C)$ and $C_2 = \operatorname{tor}(C)$, C_1 and C_2 satisfy Theorem 2 (i). Then, there are $\sigma_p(n, k_1)$ self-orthogonal codes C_1 and we have $\begin{bmatrix} n - 2k_1 \\ k_2 \end{bmatrix}_p^p$ codes C_2 such that $C_1 \subseteq C_2 \subseteq C_1^{\perp}$. Now, we have to compute $|\mathbf{X}'|$. By Lemmas 5 and 6, we have

$$p^{k_1k_2}|\mathbf{X}'| = \sum_{\mathcal{C}'\in\mathbf{X}'} |\{\mathcal{C}\in\mathbf{X}|\mathcal{C}\subseteq\mathcal{C}'\}|$$
$$= \sum_{\mathcal{C}\in\mathbf{X}} |\{\mathcal{C}'\in\mathbf{X}'|\mathcal{C}\subseteq\mathcal{C}'\}|$$
$$= \sum_{\mathcal{C}\in\mathbf{X}} 1$$
$$= |\mathbf{X}|.$$

From Theorem 3, we have that $|\mathbf{X}| = p^{k_1(n-2k_1)}$. Therefore, $|\mathbf{X}'| = p^{k_1(n-2k_1-k_2)}$.

Remark 1. Let C be an E_p -code of length n and of type $\{0, m\}$, where $m \le n$. Then C will be a self-orthogonal code. Furthermore, if m = n, then C will be self-dual.

The following results derive the mass formula for the SD codes and the LSD codes over E_{ν} , respectively.

Theorem 5. For a given integer $n \ge 2$ we have the identity

$$\sum_{\mathcal{C}} \frac{1}{|Aut(\mathcal{C})|} = \frac{\sigma_p(n,k)}{2^n n!}$$

where C runs over distinct representatives of equivalence classes under monomial action of SD E_p -codes of length n and type $\{k, n - 2k\}$.

Proof. From Theorem 2 (ii), the number of SD E_p -codes depends on the number of self-orthogonal codes over \mathbb{F}_p , and $\operatorname{tor}(\mathcal{C}) = \operatorname{res}(\mathcal{C})^{\perp}$. \Box

Example 2. We consider the case n = 3, and p = 3. In Table 1, we give the list of inequivalent self- orthogonal codes over E_3 of type $\{1,1\}$. Using the mass formula in Theorem 5, we make the following computations,

$$\sum_{i=1}^{\infty} \frac{1}{|Aut(\mathcal{C}_i)|} = \frac{1}{12} = \frac{\sigma_{E_3}(3,1,1)}{48} = \frac{\sigma_3(3,1)}{48}.$$
(14)

Corollary 1. For a given even integer $n \ge 2$, we have the identity

$$\sum_{\mathcal{C}} \frac{1}{|Aut(\mathcal{C})|} = \frac{\sigma_p(n, n/2)}{2^n n!}$$

where C runs over distinct representatives of equivalence classes under monomial action of left SD E_p -codes of length n and type $\{n/2, 0\}$.

Proof. From Theorem 2 (iii), the number of left self-dual E_p -codes depends on the number of self-dual codes over \mathbb{F}_p , with **tor**(\mathcal{C}) = **res**(\mathcal{C}). Thus, the result follows. \Box

Proposition 1. For all codes C of length n, there is a unique right self-dual E_p - code.

Proof. The result follows from Theorem 2 (iv), where $C = e \mathbb{F}_p^n$ is the unique code. \Box

Table 1. Self-orthogonal codes of length $n \le 4$ over E_3 .

Length	Туре	Generator Matrices	$ Aut(\mathcal{C}) $	Weight Distribution	RSD Code	LSD Code	SD Code
1	{0,1}	(<i>e</i>)	2	[<0, 1>, <1, 2>]	\checkmark		\checkmark
2	$\{0,1\}$ $\{0,2\}$	$\left(\begin{array}{cc} e & 0 \end{array} \right) \\ eI_2 \end{array}$	4 8	[<0, 1>, <1, 2>] [<0, 1>, <1, 4>, <2, 4>]	\checkmark		\checkmark
3	$\{1,0\}$ $\{0,1\}$ $\{0,2\}$ $\{0,2\}$	$\begin{pmatrix} a & a & a \\ a & c_{11} & c_{12} \\ (e & 0 & 0 \\ ce & 0 & 0 \\ 0 & e & 0 \end{pmatrix}$	12 6 16 16	[<0, 1>, <3, 8>] [<0, 1>, <3, 8>] [<0, 1>, <1, 2>] [<0, 1>, <1, 4>, <2, 4>]	1		(
	$\{0,3\}$ $\{1,1\}$	$ \begin{pmatrix} eI_3 \\ a & a & a \\ 0 & 2e & e \end{pmatrix} $	48 12	[<0, 1>, <1, 6>, <2, 12>, <3, 8>] [<0, 1>, <2, 6>, <3, 20>]	\checkmark		\checkmark

Length	Туре	Generator Matrices	$ Aut(\mathcal{C}) $	Weight Distribution	RSD	LSD	SD
					Code	Code	Code
4	{1,0}	(a a a 0)	24	[<0, 1>, <3, 8>]			
		$(a c_{11} c_{12} 0)$	12	[<0, 1>, <3, 8>]			
		(a a a e)	12	[<0, 1>, <3, 8>]			
		$(a c_{11} c_{12} e)$	6	[<0, 1>, <3, 2>, <4, 6>]			
	{2,0}	$ \left(\begin{array}{cccc} a & 0 & 2a & 2a \\ 0 & a & 2a & a \end{array}\right) $	48	[<0, 1>, <3, 32>, <4, 48>]		\checkmark	
	$\{0, 1\}$	$(e \ 0 \ 0 \ 0)$	96	[<0, 1>, <1, 2>]			
	{0,2}	$ \left(\begin{array}{cccc} e & 0 & 0 & 0 \\ 0 & e & 0 & 0 \\ e & 0 & 0 & 0 \end{array}\right) $	64	[<0, 1>, <1, 4>, <2, 4>]			
	{0,3}	$\left(\begin{array}{ccc} 0 & e & 0 & 0 \\ 0 & e & 0 & 0 \\ 0 & 0 & e & 0 \end{array}\right)$	96	[<0, 1>, <1, 6>, <2, 12>, <3, 8>]			
	{0,4}	e I ₄	384	[<0, 1>, <1, 8>, <2, 24>, <3, 32>, <4, 16>]	\checkmark		\checkmark

Table 1. Cont.

5. Classification

We classify self-orthogonal codes and self-dual codes of length $n \le 4$ with given residue of dimension $k_1 = 0, 1, 2$, where p = 3, 5. Also, we classify self-orthogonal codes and self-dual codes of length $n \le 3$ with given residue of dimension $k_1 = 0, 1$, where p = 7using the building method discussed in Theorem 2. To carry out the the classification, we represent codes over E_p by their associated additive codes over \mathbb{F}_{p^2} under the mapping ϕ defined in (2), and considered the action of the group of monomial matrices (with 1 and -1as nonzero entries) to directly calculate the automorphism group. These calculations are performed using MAGMA [16]. See Tables 1–3 for a summary of our results for p = 3, 5, 7, respectively.

Table 2. Self-orthogonal codes of length $n \le 4$ over E_5 .

Length	Туре	Generator Matrices	$ Aut(\mathcal{C}) $	Weight Distribution	RSD Code	LSD Code	SD Code
1	{0,1}	<i>(e)</i>	2	[<0, 1>, <1, 4>]	\checkmark		\checkmark
2	{0,1}	(e 0)	4	[<0, 1>, <1, 4>]			
	{0,2}	eI_2	8	[<0, 1>, <1, 8>, <2, 16>]	\checkmark		\checkmark
	$\{1, 0\}$	(a 2a)	4	[<0, 1>, <2, 24>]		\checkmark	\checkmark
3	{0,1}	$(e \ 0 \ 0)$	16	[<0, 1>, <1, 4>]			
	{0,2}	$\begin{pmatrix} eI_2 & 0 \end{pmatrix}$	16	[<0, 1>, <1, 8>, <2, 16>]			
	{0,3}	eI ₃	48	[<0, 1>, <1, 12>, <2, 48>, <3, 64>]	\checkmark		\checkmark
	{1,0}	(a 2a 0)	8	[<0, 1>, <2, 24>]			
		(a 2a e)	2	[<0, 1>, <2, 4>, <3, 20>]			
	{1,1}	$\left(\begin{array}{cc} a & 0 & 2a \\ 0 & e & 0 \end{array}\right)$	8	[<0, 1>, <1, 4>, <2, 24>, <3, 96>]			\checkmark
4	{1,0}	(a 2a 0 0)	32	[<0, 1>, <2, 24>]			
		$(a \ a \ 2a \ 2a)$	16	[<0, 1>, <4, 24>]			
		(a 2a e 0)	4	[<0, 1>, <2, 4>, <3, 20>]			
		(a 2a e e)	4	[<0, 1>, <2, 4>, <3, 20>]			
		$(a c_{11} c_{21} c_{21})$	4	[<0, 1>, <4, 24>]			
		$(a c_{14} c_{22} c_{21})$	2	[<0, 1>, <4, 24>]			
		$(a c_{12} c_{22} c_{22})$	4	[<0, 1>, <4, 24>]			
		$(a c_{13} 2a c_{21})$	4	[<0, 1>, <4, 24>]			
		$(a c_{11} 2a c_{22})$	4	[<0, 1>, <4, 24>]			
		$(a \ 2a \ e \ 2e)^{\prime}$	4	[<0, 1>, <2, 4>, <4, 20>]			
	{2,0}	$\left(\begin{array}{rrrr}a&0&2a&0\\0&a&0&2a\end{array}\right)$	32	[<0, 1>, <2, 48>, <4, 576>]		\checkmark	\checkmark

Length	Туре	Generator Matrices	$ Aut(\mathcal{C}) $	Weight Distribution	RSD Code	LSD Code	SD Code
1	{0,1}	(<i>e</i>)	2	[<0, 1>, <1, 6>]	\checkmark		\checkmark
2	$\{0,1\}$ $\{0,2\}$	(e 0) eI ₂	4 8	[<0, 1>, <1, 6>] [<0, 1>, <1, 12>, <2, 36>]	\checkmark		\checkmark
3	{0,1}	$\begin{pmatrix} e & 0 & 0 \end{pmatrix}$	16	[<0, 1>, <1, 6>]			
	{0,2}	$\left(\begin{array}{ccc} e & 0 & 0 \\ 0 & e & 0 \end{array}\right)$	16	[<0, 1>, <1, 12>, <2, 36>]			
	{0,3}	eI ₃	48	[<0, 1>, <1, 18>, <2, 108>, <3, 216>]	\checkmark		\checkmark
	{1,0}	(a 2a 3a)	6	[<0, 1>, <3, 48>]			
		$(2a \ b \ c_{35})$	2	[<0, 1>, <3, 48>]			
		$(4a \ 6b \ c_{53})$	2	[<0, 1>, <3, 48>]			
	{1,1}	$\left(\begin{array}{rrrr}a&2a&3a\\0&e&4e\end{array}\right)$	6	[<0, 1>, <2, 18>, <3, 324>]			\checkmark

Table 3. Self-orthogonal codes of length $n \leq 3$ over E_7 .

6. Conclusions and Open Problems

In this paper, we have given a mass formula to classify certain self-orthogonal codes over the non-unitary non-commutative ring E_p , with p an odd prime. Particularly, we were considering the two main cases of classification self-orthogonal codes, and SD codes under monomial action. In the previous section, concrete classifications in short lengths are given. Extension of these results to higher lengths would require more programming or more computing power. Similar theoretical and experimental questions remain open for other non-unitary non-commutative rings in the Rhagavandran list [12,22] in an odd characteristic.

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

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

Data Availability Statement: Data are 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).

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

References

- 1. Conway, J.H.; Pless, V. On the enumeration of self-dual codes. J. Comb. Theory Ser. A 1980, 28, 26–53. [CrossRef]
- 2. Huffman, W.C.; Pless, V. Fundamentals of Error-Correcting Codes; Cambridge University Press: Cambridge, MA, USA, 2003.
- 3. Leon, J.S.; Pless, V.; Sloane, N.J.A. Self-dual codes over GF(5). J. Comb. Theory Ser. A 1982, 32, 178–194. [CrossRef]
- 4. Mallows, C.L.; Pless, V.; Sloane, N.J.A. Self-dual codes over *GF*(3). *SIAM J. Appl. Math.* **1976**, *31*, 649–666. [CrossRef]
- Rains, E.M.; Sloane, N.J.A. Self-dual codes, Chapter 3. In *Handbook of Coding Theory, I*; Pless, V.S., Hufman, W.C., Eds.; Elsevier: North Holland, The Netherlands, 1998.
- 6. Balmaceda, J.M.; Betty, R.A.; Nemenzo, F. Mass formula for self-dual codes over \mathbb{Z}_{p^2} . *Discret. Math.* **2008**, 308, 2984–3002. [CrossRef]
- 7. Betty, R.A.; Munemasa, A. Mass formula for self-orthogonal codes over \mathbb{Z}_{p^2} . J. Comb. Inf. Syst. Sci. 2009, 34, 51–66.
- 8. Choi, W.-H. Mass formula of self-dual codes over galois rings $GR(p^2, 2)$. Korean J. Math. 2016, 24, 751–764. [CrossRef]
- 9. Gaborit, P. Mass formulas for self-dual codes over \mathbb{Z}_4 and $\mathbf{F}_q + u\mathbf{F}_q$ rings. *IEEE Trans. Inf. Theory* **1996**, 42, 1222–1228. [CrossRef]
- 10. 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]

- 11. Fields, J.; Gaborit, P.; Leon, J.; Pless, V. All self-dual ℤ₄ codes of length 15 or less are known. *IEEE Trans. Inf. Theory* **1998**, 44, 311–322. [CrossRef]
- 12. Fine, B. Classification of finite rings of order p^2 . Math. Mag. 1993, 66, 248–252. [CrossRef]
- 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. [CrossRef]
- 14. 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]
- Alahmadi, A.; Melaibari, A.; Solé, P. Duality of codes over non-unital rings of order four. *IEEE Access* 2023, 11, 53120–53133. [CrossRef]
- 16. Bosma, W.; Cannon, J.; Playoust, C. The Magma algebra system. I. The user language. J. Symb. Comput. 1997, 24, 235–265. [CrossRef]
- 17. 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]
- 18. Kim, K.H.; Park, Y.H. The mass formula of self-orthogonal codes over *GF*(*q*). *Korean J. Math.* **2017**, *25*, 201–209.
- 19. Pless, V. Number of isotropic subspaces in a finite geometry. *Atti Della Accad. Naz. Dei Lincei-Rend.-Cl. Sci.-Fis.-Mat. Nat.* **1965**, *39*, 418–421.
- 20. Pless, V. On the uniqueness of the golay codes. J. Comb. Theory 1968, 5, 215–228. [CrossRef]
- 21. Van Lint, J.; Wilson, R. A Course in Combinatorics, 2nd ed.; Cambridge University Press: Cambridge, UK, 2001.
- 22. Raghavendran, R. A class of finite rings. Compos. Math. 1970, 22, 49–57.

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.