Mathematics

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

AIMS Mathematics, 8(10): 24367–24378.
DOI: 10.3934/math.20231242
Received: 22 June 2023
Revised: 24 July 2023
Accepted: 27 July 2023
Published: 15 August 2023

Research article

The mass formula for self-orthogonal and self-dual codes over a non-unitary commutative ring

Adel Alahmadi[1,*], **Altaf Alshuhail**[1,2] **and Patrick Solé**[3]

[1] Research Group of Algebraic Structures and Applications, Department of Mathematics, Faculty of Science, King Abdulaziz University, Jeddah, Saudi Arabia

[2] Department of Mathematics, Faculty of Science, University of Hail, Hail, Saudi Arabia

[3] I2M, (CNRS, University of Aix-Marseille, Centrale Marseille), Marseilles, France

* **Correspondence:** Email: analahmadi@kau.edu.sa.

Abstract: In this paper, we establish a mass formula for self-orthogonal codes, quasi self-dual codes, and self-dual codes over commutative non-unital rings $I_p = \left\langle a, b \mid pa = pb = 0, a^2 = b, ab = 0 \right\rangle$, where p is an odd prime. We also give a classification of the three said classes of codes over I_p where $p = 3, 5,$ and 7, with lengths up to 3.

Keywords: non-unitary rings; self-dual codes; self-orthogonal codes; quasi self-dual codes; mass formula
Mathematics Subject Classification: 94B05, 16D10

1. Introduction

Mass formulas are combinatorial identities that count the number of equivalence classes of codes weighted by the size of their automorphism groups. They have been instrumental in classifying self-dual codes over finite fields [12–15] and unitary finite rings [3, 6, 10, 11, 17]. When many self-dual codes are generated, by any means whatsoever “not excluding divination” [7], these formulas serve as stopping criteria for the generating effort. Recently, a notion of quasi self-dual code, a subclass of self-orthogonal codes, was introduced over the ring I_p in the list of rings of [9, 16] in the special case of order 4, that is to say,

$$I_2 = \left\langle a, b \mid 2a = 2b = 0, a^2 = b, ab = 0 \right\rangle.$$

Work on the classification of quasi self-dual codes over that ring was done by Alahmadi et al. [1], who classified quasi self-dual codes under coordinate permutation up to length 3, and derived a mass formula for these codes under coordinate permutation.

The present paper extends the latter work to the ring

$$I_p = \left\langle a, b \mid pa = pb = 0, a^2 = b, ab = 0 \right\rangle,$$

where p is an odd prime. In particular, we classify self-orthogonal codes, and quasi self-dual codes of lengths at most three for $p = 3, 5$, and $p = 7$. In addition, we also classify self-dual codes under monomial action over the same ring, building on the structural results of [2], which were not known at the time of writing [1]. With any linear code over this ring is attached an additive $\mathbb{F}_{p^2}$-code, a map which enables us to use the additive code package of Magma [4], and produce the numerical results in the Appendix. Although that package does not afford an automorphism subroutine in odd characteristic, the short length of the codes considered allowed us some simple algorithmic strategies. While additive codes were first introduced over $\mathbb{F}_4$ [5] from a quantum coding motivation, they can also be defined over $\mathbb{F}_{p^2}$, for p odd, with similar motivation and properties. For instance, additive self-dual codes over GF(9) were classified in [8].

The rest of the paper is arranged as follows. The next section consists of notations and notions needed for the other sections. Section 3 studies and constructs codes over I_p. Section 4 derives the three main mass formulas. Section 5 concludes the article. Numerical results are collected in the Appendix (Section 6).

2. Preliminaries

2.1. Codes over $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$

Let p be an odd prime number. A linear code 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 it an $[n, k]$-*code*. The elements of such a code are called *codewords*. Two codewords $\mathbf{x} = (x_1, x_2, ..., x_n)$ 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 C is called the *dual* of C, denoted by $C^\perp$. A linear code is said to be self-orthogonal (resp. self-dual) if $C \subseteq C^\perp$ (resp. $C = C^\perp$).

Let ω be a primitive element in $\mathbb{F}_{p^2}$, and let $r = p^2 - 1$. 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 an $\mathbb{F}_p-$additive subgroup of $\mathbb{F}_{p^2}^n$ containing p^k codewords for some integer k in the range $0 \leqslant k \leqslant 2n$. Denote by $wt(\mathbf{x})$ the (Hamming) weight of $\mathbf{x} \in \mathbb{F}_{p^2}$. We use the Magma [4] notation

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

for the weight distribution of a code over $\mathbb{F}_{p^2}$, where A_i is the number of codewords of Hamming weight i.

2.2. Rings

Following [9], we define a ring on two generators a, b by their relations

$$I_p = \left\langle a, b \mid pa = pb = 0, a^2 = b, ab = 0 \right\rangle.$$

Thus, I_p consists of p^2 elements, which can be written as $c_{ij} = ia + jb$ where $0 \leq i, j < p$. From the ring representation of I_p, we infer that I_p is commutative without multiplicative identity, and contains a unique maximal ideal $J_p = \{jb : 0 \leqslant j < p\}$. Thus we can write I_p as

$$I_p = \left\{ax + by \mid x, y \in \mathbb{F}_p\right\}.$$

Define the reduction map modulo J_p as $\alpha : I_p \mapsto I_p/J_p \cong \mathbb{F}_p$ by $\alpha(c_{ij}) = i$ where $0 \leqslant i < p$. This map is extended in the natural way into a map from I_p^n to $\mathbb{F}_p^n$.

3. Codes over I_p

A linear code over I_p or (I_p-code for short) of length n is any submodule $C \subseteq I_p^n$. The inner product between two codewords in $C \subseteq I_p^n$ is defined by $(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} x_i y_i$. The dual of C is a submodule of I_p^n defined as

$$C^{\perp} = \{\mathbf{y} \in I_p^n \mid \forall\, \mathbf{x} \in C, (\mathbf{y}, \mathbf{x}) = 0\}.$$

If $C \subseteq C^{\perp}$ (resp. $C = C^{\perp}$), then C is self-orthogonal (resp. self-dual (SD)). An I_p-code of length n is quasi self-dual (QSD) if it is self-orthogonal and of size p^n.

With an I_p-code C can be attached an additive $\mathbb{F}_{p^2}$-code by the map $\phi : I_p \mapsto \mathbb{F}_{p^2}$

$$\phi(0) = 0, \phi(a) = 1/2, \text{and } \phi(b) = y, \tag{1}$$

for $y \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ such that $(y)^p \equiv -y \bmod p$. One can easily see that $Tr(\phi(\mathbf{u})) = \alpha(\mathbf{u})$ for all $\mathbf{u} \in I_p^n$.

Lemma 1. *(i) For any odd prime p, there is a self-orthogonal code over I_p.*

(ii) For any positive integer n, there exists a QSD code over I_p of length n.

Proof. (i) Let $\mathbf{1}_p$ denote the all-one codeword of length $n = p$. The repetition code of length p is then defined by $R_p = \{u(\mathbf{1}_p) \mid \forall u \in I_p\}$. Clearly R_p is a linear code over I_p. Since I_p has characteristic p with $a^2 = b$, $b\mathbf{x} \in {R_p}^{\perp}$ for all $\mathbf{x} \in \mathbb{F}_p^n$ we have $R_p \subsetneq {R_p}^{\perp}$.

(ii) Let $C = b\mathbb{F}_p^n$, since $u\mathbb{F}_p^n \subset C^{\perp}$ for all $u \in I_p$, and then $C \subsetneq C^{\perp}$ of size p^n.

□

Let C be a linear code over I_p. Two $\mathbb{F}_p$-codes can be associated canonically with C. We define the **residue** code of C as

$$res(C) = \{\mathbf{x} \in \mathbb{F}_p^n \mid \exists\, \mathbf{y} \in \mathbb{F}_p^n \text{ such that } a\mathbf{x} + b\mathbf{y} \in C\},$$

and the **torsion** code as

$$tor(C) = \{\mathbf{y} \in \mathbb{F}_p^n \mid b\mathbf{y} \in C\}.$$

From Eq (1), we have that $res(C) = Tr(\phi(C))$, and that $tor(C)$ is the subfield subcode of $\phi(C)$ defined by $\phi(C) \cap \mathbb{F}_p^n$. Let α_C be the restriction of α to C. We see that $tor(C)b = Ker(\alpha_C)$, and that $res(C) = Im(\alpha_C)$. By writing $a(a\mathbf{x} + b\mathbf{y}) = b\mathbf{x}$, in the definition of $res(C)$, we observe that $res(C) \subseteq tor(C)$. Let $k_1 = \dim(res(C))$ and $k_2 = \dim(tor(C)) - k_1$. We say that C is a linear code of type $\{k_1, k_2\}$. It can be seen that C is free as an I_p-module if and only if $res(C) = tor(C)$. By the first isomorphism theorem applied to α_C we have that $|C| = p^{2k_1+k_2}$.

In the next theorem, we extend a few results from [1, 2] and for its proof, not written here, we can simply substitute codes over $\mathbb{F}_p$ for binary codes.

Theorem 2. *If k_1, k_2, n are integers with $k_1 + k_2 \leq n$, then*

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

$$\begin{bmatrix} aI_{k_1} & aX & Y \\ 0 & bI_{k_2} & bZ \end{bmatrix}$$

where I_{k_1} and I_{k_2} are identity matrices, the matrix Y has entries in I_p, and X, Z are matrices with entries from $\mathbb{F}_p$.

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

The following theorem states that a self-orthogonal code can be created by combining a self-orthogonal $[n, k_1]$-code over $\mathbb{F}_p$ with an arbitrary supercode of his of dimension $k_1 + k_2$.

Theorem 3. *If $C = aC_1 + bC_2$ is an arbitrary I_p-code, with C_1, C_2 binary codes of the same length, then C is self-orthogonal if and only if the following two statements hold:*

(i) C_1 is a self-orthogonal $[n, k_1]$-code over $\mathbb{F}_p$.

(ii) C_2 is an $[n, k_1 + k_2]$-code over $\mathbb{F}_p$ such that $C_1 \subseteq C_2$.

Proof. For all $\mathbf{c}, \mathbf{c}' \in C$ with $\mathbf{c} = a\mathbf{x} + b\mathbf{y}$, and $\mathbf{c}' = a\mathbf{x}' + b\mathbf{y}'$.

$$(\mathbf{c}, \mathbf{c}') = b(\mathbf{x}, \mathbf{x}') = 0.$$

The result follows by $C_1 = res(C)$. For the second condition, since $C_2 = tor(C)$, $res(C) \subseteq tor(C)$.

Conversely, since C_1 and C_2 are linear codes, C is closed under addition. For the scalar multiplication condition, we assume $c_{ij} \in I_p$ where $0 \leqslant i, j \leqslant p - 1$.

$$c_{ij}C \subseteq ib\,C_1 \subseteq ib\,C_2 \subseteq b\,C_2 \subseteq C.$$

Hence, C is a linear code over I_p, with $|C| = |C_1||C_2| = p^n$. 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 that

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

since C_1 is self-orthogonal. □

Corollary 4. *If $C = aC_1 + bC_2$ is an arbitrary I_p-code, then C is QSD if and only if the following hold:*

(i) C_1 is a self-orthogonal $[n, k]$-code over $\mathbb{F}_p$.

(ii) C_2 is an $[n, n - k]$-code over $\mathbb{F}_p$ such that $C_1 \subseteq C_2$.

Proof. Setting $k_2 = n - 2k$ in the previous theorem yields the result. □

Corollary 5. *If $C = aC_1 + bC_2$ is an arbitrary I_p-code, then C is a free self-orthogonal if and only if C_1 is a self-orthogonal $[n, k]$-code over $\mathbb{F}_p$.*

Unlike other rings of the same size [3, 6, 10], $res(C)^\perp$ is not necessary to be $tor(C)$. For example, see the classification section, when $p = 3, 5$ and $n = 3$.

Proposition 6. *Let $C = a\, res(C) + b\, tor(C)$ be I_p-code. If $res(C)$ is a self-dual $[n, k]$- code over $\mathbb{F}_p$, then one of the following hold:*

(i) If $tor(C) = \mathbb{F}_p^n$, then C will be a SD code.

(ii) If $tor(C) = res(C)$, then C will be a QSD code.

Proof. (i) From Theorem 2 (ii), $C^\perp = a\,(res(C)^\perp) + b\,\mathbb{F}_p^n$, since $res(C)$ is a self dual and $tor(C) = \mathbb{F}_p^n$. Then we have $C^\perp = a\,(res(C)^\perp) + b\,\mathbb{F}_p^n = a\,res(C) + b\,tor(C) = C$.

(ii) If $tor(C) = res(C)$, then C is a free code with $n = 2k$. From Theorem 3 we have that C is self-orthogonal of size $p^{2k} = p^n$.

□

We apply a similar approach to that used for the computation of a mass formula in [10]. We define a map F by

$$\begin{aligned} F : res(C) &\mapsto \mathbb{F}_p^n/tor(C), \\ \mathbf{x} &\mapsto F(\mathbf{x}) = \{\mathbf{y} \in \mathbb{F}_p^n \mid a\mathbf{x} + b\mathbf{y} \in C\}. \end{aligned}$$

Thus, $C = \{a\mathbf{x} + b\mathbf{y} \mid \mathbf{x} \in res(C) \text{ and } \mathbf{y} \in F(\mathbf{x})\}$.

The map F is determined by the matrix Y in Theorem 2, and vice versa.

We see that the map F is $\mathbb{F}_p-$linear, and the set of codes over I_p is in one to one correspondence with the set of triplets $(res(C), tor(C), F)$.

4. The mass formulas

The number of self-orthogonal I_p-codes to count depends on the number of self-orthogonal codes over $\mathbb{F}_p$, found in [11], and on the number of $tor(C)$, found in Lemma 2 in [1].

Let $\sigma_p(n, k_1)$ denote the number of self-orthogonal $[n, k_1]$codes over $\mathbb{F}_p$ and $\sigma_{I_p}(n, k_1, k_2)$ denote the number of distinct self-orthogonal codes over I_p of length n of type $\{k_1, k_2\}$.

Next, we count self-orthogonal and quasi self-dual codes over I_p, a census which will be used in the mass formula.

Theorem 7. *For all codes of lengths n of type $\{k_1, k_2\}$, the number of self-orthogonal codes over I_p is*

$$\sigma_{I_p}(n, k_1, k_2) = \sigma_p(n, k_1) \binom{n - k_1}{k_2}_p p^{k_1(n-k_1-k_2)}, \tag{2}$$

where $\binom{j}{i}_p$ denotes the p-binomial coefficient for integers $i \leqslant j$.

Proof. Observe that, by Theorem 4.7 in [11], the number of C_1 is $\sigma_p(n, k_1)$, the number of self-orthogonal codes over $\mathbb{F}_p$, and each one can be contained in $\binom{n - k_1}{k_2}_p$ possible C_2, by Lemma 2 in [1]. The $\mathbb{F}_p-$linear map F is arbitrary from $res(C)$ to $\mathbb{F}_p^n/tor(C)$. By Theorem 2, we can write a generator of residue code as $G_1 = [I_{k_1}\ X\ \alpha(Y)]$, where $Y = aA + bB$, and A, B are matrices having entries in $\mathbb{F}_p$. From the definition of F, we have that $F(G_1) = \langle B \rangle$. Since B is an arbitrary matrix, these two vector spaces have dimension k_1 and $n - (\dim(tor(C)))$, respectively. □

Corollary 8. *For all codes of lengths n of type* $\{k, n-2k\}$*, the number of quasi self-dual codes over* I_p *is*

$$\sigma_{I_p}(n,k,n-2k) = \sigma_p(n,k)\binom{n-k}{n-2k}_p p^{k^2}, \tag{3}$$

where $\binom{j}{i}_p$ *denotes the p-binomial coefficient for integers* $i \leqslant j$.

Proof. The result follows immediately from the previous theorem upon setting $k_1 = k$ and $k_2 = n - 2k$. □

Proposition 9. *For all codes of lengths n of type* $\{k, 0\}$*, the number of free self-orthogonal codes over* I_p *is*

$$\sigma_{I_p}(n,k,0) = \sigma_p(n,k)p^{k(n-k)}. \tag{4}$$

Proof. Since $k_2 = 0$, the residue code determines torsion code. There are, by definition, $\sigma_p(n,k)$ such possible residue codes. The representation on a basis of $res(C)$ determines the map F. Hence the number of map F will be $p^{k(n-k)}$. □

The special case of $n = 2k$ leads to a simpler formula.

Proposition 10. *For all codes of lengths* $2k$ *of type* $\{k, 0\}$*, then the number of quasi self-dual codes over* I_p *is*

$$\sigma_{I_p}(2k,k,0) = \sigma_p(2k,k,0)p^{k^2}. \tag{5}$$

Proof. Note that a self-dual code $res(C)$ determines the code $tor(C)$ because $tor(C) = res(C)^{\perp}$. There are, by definition, $\sigma_p(2k,k)$ such possible residue codes. The representation on a basis of $res(C)$ determines the map F. Hence the number of F will be p^{k^2}. □

The following theorem shows that the number of quasi self-dual codes over I_p in case a residue code is the zero code. For illustration, see Tables 1 and 2 when $n = 1, 2$.

Theorem 11. *If there is no non zero self-orthogonal code over* $\mathbb{F}_p$ *of length n, then there is a unique QSD* I_p *code.*

Proof. Let $res(C)$ be a zero code of length n, and then $C = b\mathbb{F}_p^n \subset C^{\perp}$ of size p^n. □

We now define the notion of equivalence of codes. Two codes C and C' over I_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 zero) such that $C' = \{cM : c \in C\}$. The monomial automorphism group $Aut(C)$ of code C consists all M such that $C = MC'$.

The following lemma will be needed in the Appendix.

Lemma 12. *(i) Two SD* I_p*-codes are monomially equivalent iff their residue codes are equivalent.*

(ii) Two free I_p*-codes are monomially equivalent iff their residue codes are equivalent.*

Proof. (i) Let C and C' be two SD I_p-codes such that $C = MC'$ for some $M \in Aut(C)$, and then $res(C) = \alpha(C) = \alpha(MC') = Mres(C')$. Conversely, suppose that $res(C) = Mres(C')$ for some $M \in Aut(C)$. Since $\mathbb{F}_p^n = M\mathbb{F}_p^n$, it follows that $C = MC'$.

(ii) Let C and C' be two free I_p-codes such that $C = MC'$ for some $M \in Aut(C)$, and then $res(C) = \alpha(C) = \alpha(MC') = Mres(C')$. Conversely, suppose that $res(C) = Mres(C')$ for some $M \in Aut(C)$. Since $tor(C) = res(C)$, it follows that $C = MC'$.

□

Remark 13. *If any two I_p-codes are monomially equivalent, then their residue and torsion codes are equivalent, but the converse is not necessarily true. For instance, from Table 3, when $n = 3$ the codes C_u, with generator matrix $\begin{pmatrix} a & u & 2a \\ 0 & 0 & b \end{pmatrix}$, where $u \in \{b, 2b, 3b, 4b\}$, all have the same residue and torsion codes, but are not pairwise equivalent.*

We now have three mass formulas: the first and the second one for self-orthogonal codes and QSD codes under monomial equivalence, respectively, and the last one for SD codes.

Proposition 14. *For given integers n, k_1, k_2 with $0 \leq k_1, k_2 \leq n$, we have the identity*

$$\sum_C \frac{1}{|Aut(C)|} = \frac{\sigma_{I_p}(n, k_1, k_2)}{2^n n!}, \tag{6}$$

where C runs over distinct representatives of equivalence classes under monomial action of self-orthogonal I_p-codes of length n and type $\{k_1, k_2\}$.

Proof. By Theorem 6, and the fact that the number of codes in an equivalence class equals the size of the monomial group divided by the size of the common automorphism group the result follows. □

Proposition 15. *For given integers n, k_1, k_2 with $0 \leq k_1, k_2 \leq n$, we have the identity*

$$\sum_C \frac{1}{|Aut(C)|} = \frac{\sigma_{I_p}(n, k_1, k_2)}{2^n n!}, \tag{7}$$

where C runs over distinct representatives of equivalence classes under monomial action of self-orthogonal I_p-codes of length n and type $\{k_1, k_2\}$.

Example 16. *We consider the case $n = 3$, and $p = 3$. In Table 1, we give the list of inequivalent self-orthogonal codes over I_3 of Type $\{1, 1\}$. Using the mass formula in Corollary 9, we make the following computations:*

$$\sum_{i=1}^{10} \frac{1}{|Aut(C_i)|} = \frac{5}{4} + \frac{3}{6} + \frac{2}{8} = \frac{\sigma_{I_3}(3, 1, 1)}{48}. \tag{8}$$

Theorem 17. *For a given integer $n \geq 2$ we have the identity*

$$\sum_C \frac{1}{|Aut(C)|} = \frac{\sigma_p(n, n/2, 0)}{2^n n!}, \tag{9}$$

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

Proof. From Proposition 5, the number of SD I_p-codes depends on the number of SD codes over $\mathbb{F}_p$, and $tor(C) = \mathbb{F}_p^n$. □

We can use [12, 14] to find $\sigma_p(n, n/2)$, when $p = 3$, and when $p = 5$.

Example 18. *We consider the case $n = 2$, and $p = 5$. In Table 3, we give the list of necessarily self-orthogonal codes over I_5 of Type $\{1, 0\}$. Using the mass formula in Theorem 11, we make the following computations:*

$$\sum_{i=1}^{5} \frac{1}{|Aut(C_i)|} = \frac{5}{4} = \frac{\sigma_5(2, 1, 0)}{8}. \tag{10}$$

Table 1. Self-orthogonal codes of length ≤ 3 over I_3.

Length	Type	Generator matrices	No. of distinct codes	$\lvert Aut(C)\rvert$	Weight distribution	QSD code
1	$\{0, 1\}$	(b)	1	2	$[< 0, 1 >, < 1, 2 >]$	Yes
2	$\{0, 2\}$	$\begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}$	1	8	$[< 0, 1 >, < 1, 4 >,$ $, < 2, 4 >]$	Yes
3	$\{1, 1\}$	$\begin{pmatrix} u & a & a \\ 0 & 0 & b \end{pmatrix}$ where $u \in \{a, c_{11}, c_{12}, c_{21}, c_{22}\}$	5	4	$[< 0, 1 >, < 1, 2 >,$ $< 2, 2 >, < 3, 22 >]$	Yes
		$\begin{pmatrix} u & a & a \\ 0 & 2b & b \end{pmatrix}$ where $u \in \{a, c_{11}, c_{12}\}$	3	6	$[< 0, 1 >, < 2, 6 >,$ $< 3, 20 >]$	
		$\begin{pmatrix} u & a & a \\ 0 & 2b & b \end{pmatrix}$ where $u \in \{c_{21}, c_{22}\}$	2	8		
	$\{1, 0\}$	$\begin{pmatrix} a & a & u_1 \end{pmatrix}$ where $u_1 \in \{2a, c_{21}, c_{22}\}$ $\begin{pmatrix} a & u_2 & 2a \end{pmatrix}$ where $u_2 \in \{c_{11}, c_{12}\}$ $\begin{pmatrix} a & c_{11} & u_3 \end{pmatrix}$ where $u_3 \in \{c_{21}, c_{22}\}$ $\begin{pmatrix} a & c_{12} & u_4 \end{pmatrix}$ where $u_4 \in \{c_{21}, c_{22}\}$	9	12	$[< 0, 1 >, < 3, 8 >]$	No

Table 2. Self-orthogonal codes of length ≤ 3 over I_7.

Length	Type	Generator matrices	No. of distinct codes	$\lvert Aut(C)\rvert$	Weight distribution	QSD code
1	$\{0,1\}$	(b)	1	2	$[<0,1>,$ $<1,6>]$	Yes
2	$\{0,2\}$	$\begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}$	1	8	$[<0,1>,$ $<1,12>,$ $<2,36>]$	Yes
3	$\{1,0\}$	$\begin{pmatrix} u_1 & 2a & 3a \end{pmatrix}$ where $u_1 \in \{a, c_{11}, c_{12}, c_{13}, c_{14}, c_{15}, c_{16}\}$ $\begin{pmatrix} a & u_2 & 3a \end{pmatrix}$ where $u_2 \in \{c_{21}, c_{22}, c_{23}, c_{24}, c_{25}, c_{26}\}$ $\begin{pmatrix} a & 2a & u_3 \end{pmatrix}$ where $u_3 \in \{c_{31}, c_{32}, c_{33}, c_{34}, c_{35}, c_{36}\}$ $\begin{pmatrix} c_{11} & u_4 & 3a \end{pmatrix}$ where $u_4 \in \{c_{21}, c_{22}, c_{23}, c_{24}, c_{25}, c_{26}\}$ $\begin{pmatrix} c_{11} & u_5 & 2a \end{pmatrix}$ where $u_5 \in \{c_{31}, c_{32}, c_{33}, c_{34}, c_{35}, c_{36}\}$ $\begin{pmatrix} a & u_6 & c_{21} \end{pmatrix}$ where $u_6 \in \{c_{31}, c_{32}, c_{33}, c_{34}, c_{35}, c_{36}\}$ $\begin{pmatrix} a & c_{31} & u_7 \end{pmatrix}$ where $u_7 \in \{c_{21}, c_{22}, c_{23}, c_{24}, c_{25}, c_{26}\}$	49	6	$[<0,1>,$ $<3,48>]$	No

Table 3. QSD and SD codes of length ≤ 3 over I_5.

n	Type	Generator matrices	No. of distinct codes	$\|Aut(C)\|$	Weight distribution	QSD or SD
1	$\{0,1\}$	(b)	1	2	$[<0,1>,<1,4>]$	QSD
2	$\{1,0\}$	$\begin{pmatrix} u & 2a \end{pmatrix}$ where $u \in \{a, c_{11}, c_{12}, c_{13}, c_{14}\}$	5	4	$[<0,1>,<2,24>]$	QSD
	$\{1,1\}$	$\begin{pmatrix} a & 2a \\ 0 & b \end{pmatrix}$	1	4	$[<0,1>,<1,8>,$ $<2,116>]$	SD
3	$\{1,1\}$	$\begin{pmatrix} a & 0 & 2a \\ 0 & 0 & b \end{pmatrix}$	1	3	$[<0,1>,<1,8>,$ $<2,116>]$	QSD
		$\begin{pmatrix} a & u & 2a \\ 0 & 0 & b \end{pmatrix}$ where $u \in \{b, 2b, 3b, 4b\}$	4	3	$[<0,1>,<1,8>,$ $<2,16>,<3,100>]$	
		$\begin{pmatrix} u & 2a & 0 \\ 0 & b & b \end{pmatrix}$ where $u \in \{a, c_{11}, c_{12}, c_{13}, c_{14}\}$	5	2	$[<0,1>,<2,32>,$ $<3,92>]$	
		$\begin{pmatrix} a & 2a & 0 \\ b & b & 0 \end{pmatrix}$	1	2	$[<0,1>,<1,8>,$ $<2,116>]$	
		$\begin{pmatrix} a & 2a & u \\ b & b & 0 \end{pmatrix}$ where$u \in \{b, 2b, 3b, 4b\}$	4	2	$[<0,1>,<1,8>,$ $<2,16>,<3,100>]$	
		$\begin{pmatrix} u & a & 0 \\ 0 & 0 & b \end{pmatrix}$ where $u \in \{2a, c_{21}, c_{22}, c_{23}, c_{24}, c_{31}, c_{32}, c_{33}, c_{34}\}$	9	3	$[<0,1>,<1,4>,$ $<2,24>,<3,96>]$	
		$\begin{pmatrix} 2a & u & 0 \\ 0 & 0 & b \end{pmatrix}$ where $u \in \{c_{11}, c_{12}, c_{13}, c_{14}\}$	4	3		
		$\begin{pmatrix} 0 & a & u \\ b & b & 0 \end{pmatrix}$ where $u \in \{c_{21}, c_{22}, c_{23}, c_{24}, c_{31}, c_{32}, c_{33}, c_{34}\}$	8	2		

5. Conclusions

In this paper, we have given a mass formula to classify certain self-orthogonal codes over the non-unitary ring I_p, with p an odd prime. In particular we have considered the three main cases of classification, self-orthogonal codes, QSD codes, and SD codes under monomial action.

Concrete classifications in short lengths are given in the next section. 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 rings in the Raghavendran list [9, 16] in odd characteristic.

Appendix

We classify self-orthogonal codes and self-dual I_p-codes of length $n < 4$ and residue dimension $k = 0, 1$, where $p = 3, 5$, and 7, using the building method discussed in Theorem 3, and its corollaries. With the aid of Magma [4], all computer calculations for this work were completed. To compute the automorphism groups of our codes, in lack of an automorphism program for additive codes in odd characteristic, we used two strategies:

- Reduction to the residue code in case of a self-dual and a free code by Lemma 10.
- Computation and enumeration of all equivalent codes images under the monomial group. The order of automorphism group of a code of length n is the number of monomial matrices $2^n n!$ divided by the number of codes equivalent to that code.

See Tables 1–3 for a summary of our results for $p = 3, 5, 7$, respectively.

Use of AI tools declaration

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

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).

Conflict of interest

Prof. Patrick Solé is the Guest Editor of special issue "Mathematical Coding Theory and its Applications" for AIMS Mathematics. Prof. Patrick Solé was not involved in the editorial review and the decision to publish this article. All authors declare no conflicts of interest in this paper.

References

1. A. Alahmadi, A. Altassan, W. Basaffar, A. Bonnecaze, H. Shoaib, P. Solé, Quasi type IV codes over a non-unital ring, *Appl. Algebra Eng. Commun. Comput.*, **32** (2021), 217–228.
2. A. Alahmadi, A. Melaibari, P. Solé, Duality of codes over non-unital rings of order four, *IEEE Access*, **11** (2023), 53120–53133. https://doi.org/10.1109/ACCESS.2023.3261131
3. J. M. P. Balmaceda, R. A. L. Betty, F. R. Nemenzo, Mass formula for self-dual codes over Z_{p^2}, *Discrete Math.*, **308** (2008), 2984–3002. https://doi.org/10.1016/j.disc.2007.08.024

4. W. Bosma, J. Cannon, C. Playoust, The Magma algebra system I: the user language, *J. Symb. Comput.*, **24** (1997), 235–265. https://doi.org/10.1006/jsco.1996.0125
5. A. R. Calderbank, E. M. Rains, P. M. Shor, N. J. A. Sloane, Quantum error correction via codes over GF(4), *IEEE Trans. Inf. Theory*, **44** (1998), 1369–1387. https://doi.org/10.1109/18.681315
6. W. Choi, Mass formula of self-dual codes over Galois rings $GR(p^2, 2)$, *Korean J. Math.*, **24** (2016), 751–764. https://doi.org/10.11568/kjm.2016.24.4.751
7. J. H. Conway, V. Pless, On the enumeration of self-dual codes, *J. Comb. Theory Ser. A*, **28** (1980), 26–53. https://doi.org/10.1016/0097-3165(80)90057-6
8. L. E. Danielsen, On the classification of Hermitian self-dual additive codes over $GF(9)$, *IEEE Trans. Inf. Theory*, **58** (2012), 5500–5511. https://doi.org/10.1109/TIT.2012.2196255
9. B. Fine, Classification of finite rings of order p^2, *Math. Mag.*, **66** (1993), 248–252. https://doi.org/10.2307/2690742
10. P. Gaborit, Mass formulas for self-dual codes over $\mathbb{Z}_4$ and $\mathbb{F}_p + u\mathbb{F}_p$ rings, *IEEE Trans. Inf. Theory*, **42** (1996), 1222–1228. https://doi.org/10.1109/18.508845
11. K. H. Kim, Y. H. Park, The mass formula of self-orthogonal codes over $GF(q)$, *Korean J. Math.*, **25** (2017), 201–209. https://doi.org/10.11568/kjm.2017.25.2.201
12. J. S. Leon, V. Pless, N. J. A. Sloane, Self-dual codes over $GF(5)$, *J. Comb. Theory Ser. A*, **32** (1982), 178–194. https://doi.org/10.1016/0097-3165(82)90019-X
13. F. J. MacWilliams, N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, 1977.
14. C. L. Mallows, V. Pless, N. J. A. Sloane, Self-dual codes over $GF(3)$, *SIAM J. Appl. Math.*, **31** (1976), 649–666.
15. E. M. Rains, N. J. A. Sloane, Self-dual codes, In: V. S. Pless, W. C. Hufman, *Handbook of coding theory, I*, North Holland, 1998.
16. R. Raghavendran, A class of finite rings, *Compos. Math.*, **22** (1970), 49–57.
17. M. Shi, A. Alahmadi, P. Solé, *Codes and rings: theory and practice*, Academic Press, 2017. https://doi.org/10.1016/C2016-0-04429-7
18. P. Solé, *Codes over rings*, World Scientific, 2008.