Korean J. Math. **22** (2014), No. 4, pp. 725–742
http://dx.doi.org/10.11568/kjm.2014.22.4.725

THE CLASSIFICATION OF SELF-ORTHOGONAL CODES OVER $\mathbb{Z}_{p^2}$ OF LENGTHS $\leq$ 3

Whan-hyuk Choi, Kwang Ho Kim and Sook Young Park*

Abstract. In this paper, we find all inequivalent classes of self-orthogonal codes over $\mathbb{Z}_{p^2}$ of lengths $l \leq 3$ for all primes p, using similar method as in [3]. We find that the classification of self-orthogonal codes over $\mathbb{Z}_{p^2}$ includes the classification of all codes over $\mathbb{Z}_p$. Consequently, we classify all the codes over $\mathbb{Z}_p$ and self-orthogonal codes over $\mathbb{Z}_{p^2}$ of lengths $l \leq 3$ according to the automorphism group of each code.

1. Introduction

As concerns about codes over rings are increasing, many results about the codes over $\mathbb{Z}_m$ for an integer m and especially over $\mathbb{Z}_{p^e}$ for a prime p are published. In [3], [6], [7] and [8], authors found that the construction and classification of the self-dual codes over $\mathbb{Z}_m$ is based on the classification of the self-orthogonal codes over $\mathbb{Z}_p$ and $\mathbb{Z}_{p^2}$ of length 4. In this paper, we focused on the classification of self-orthogonal codes over $\mathbb{Z}_{p^2}$ of length 3 upon which the classfication of codes of length 4 is based.

We begin by giving the necessary definitions and notations. A *code over* $\mathbb{Z}_{p^2}$ *of length* n is a $\mathbb{Z}_{p^2}$-submodule of $\mathbb{Z}_{p^2}^n$. A code $\mathcal{C}$ of length n over $\mathbb{Z}_{p^2}$ has generator matrices permutation equivalent to the *standard*

Received December 1, 2014. Revised December 10, 2014. Accepted December 10, 2014.

2010 Mathematics Subject Classification: 94B05.

Key words and phrases: codes over rings, self-orthogonal codes, classification.

*Corresponding author.

form

$$G = \begin{pmatrix} I_{k_1} & A_1 & B_1 + pB_2 \\ 0 & pI_{k_2} & pC_1 \end{pmatrix}, \tag{1}$$

where the columns are grouped into blocks of sizes k_1, k_2 and $n - k_1 - k_2$ and A_1, B_1, B_2 and C_1 are matrices over $\mathbb{Z}_p$ [7]. A matrix with this standard form is said to be of *type*

$$1^{k_1} p^{k_2}. \tag{2}$$

The number of nonzero rows is called the *rank* of $\mathcal{C}$ and denoted by *rank* $\mathcal{C}$. k_1 is called the *free rank*.

Associated with $\mathcal{C}$ there are two codes over $\mathbb{Z}_p$, the *residue code* $R(\mathcal{C}) = \{x \in \mathbb{Z}_p^n \mid \exists y \in \mathbb{Z}_p^n$ such that $x + py \in \mathcal{C}\}$ and the *torsion code* $T(\mathcal{C}) = \{y \in \mathbb{Z}_p^n \mid py \in \mathcal{C}\}$ which have generator matrices

$$G_1 = \begin{pmatrix} I_{k_1} & A_1 & B_1 \end{pmatrix}, \; G_2 = \begin{pmatrix} I_{k_1} & A_1 & B_1 \\ 0 & I_{k_2} & C_1 \end{pmatrix}$$

respectively.

The *dual code* $\mathcal{C}^\perp$ of $\mathcal{C}$ is defined by

$$\mathcal{C}^\perp = \{\mathbf{v} \in \mathbb{Z}_{p^e}^n | \mathbf{v} \cdot \mathbf{w} = 0 \text{ for all } \mathbf{w} \in \mathcal{C}\}.$$

$\mathcal{C}$ is called *self-orthogonal* (resp. *self-dual*) if $\mathcal{C} \subset \mathcal{C}^\perp$ (resp. $\mathcal{C} = \mathcal{C}^\perp$). For any code $\mathcal{C}$ of length n over $\mathbb{Z}_{p^2}$

$$|\mathcal{C}||\mathcal{C}^\perp| = p^{2n}.$$

Hence if $\mathcal{C}$ is self-orthogonal code over $\mathbb{Z}_{p^2}$ of length n then $|\mathcal{C}| \leq p^n$, and if $\mathcal{C}$ is self-dual then $|\mathcal{C}| = p^n$.

$\mathbb{T}_m^n$, the group of all *monomial transformations* on $\mathbb{Z}_m^n$ is defined by

$$\mathbb{T}_m^n = \{\gamma\sigma \mid \gamma \in \mathbb{D}_m^n, \sigma \in S_n\}.$$

where S_n is the symmetric group of length n and $\mathbb{D}_m^n$ is the set of diagonal matrices with elements $\gamma_i \in \mathbb{Z}_m$ and $\gamma_i^2 = 1$. Note that we take γ_i's in $\mathbb{Z}_p$ or $\mathbb{Z}_p^2$ occasionally according to the context. Any element $t \in \mathbb{T}_m^n$ has a unique representation $t = \gamma\sigma$ for $\gamma \in \mathbb{D}_m^n$ and $\sigma \in S_n$. γ will be called the *sign (part)* of t, and σ will be called the *permutation part* of t.

The group $\mathbb{T}_m^n$ acts on the set of codes over $\mathbb{Z}_m$ by $\mathcal{C}t = \{ct \mid c \in \mathcal{C}\}$. Notice that this is indeed a right action but $\sigma\gamma = \gamma^\sigma\sigma$ as well where $\gamma^\sigma = \sigma\gamma\sigma^{-1}$. Two codes $\mathcal{C}$ and $\mathcal{C}'$ are *equivalent* (denoted $\mathcal{C} \sim \mathcal{C}'$) if there exists an element $t \in \mathbb{T}_m^n$ such that $\mathcal{C}t = \mathcal{C}'$. The group of all automorphisms of $\mathcal{C}$ will be denoted by $\mathrm{Aut}(\mathcal{C})$.

For a subgroup $\mathrm{Aut}(\mathcal{C})$ of $\mathbb{T}_m^n$,

$$p(\mathcal{C}) = \{\sigma \mid \gamma\sigma \in \mathrm{Aut}(\mathcal{C}) \text{ for some } \gamma \in \mathbb{D}_m^n\}$$

is a subgroup of S_n, called the *permutation parts* of $\mathrm{Aut}(\mathcal{C})$. Elements in $s(\mathcal{C}) = \mathrm{Aut}(\mathcal{C}) \cap \mathbb{D}_m^n$ are called the *pure signs* of $\mathrm{Aut}(\mathcal{C})$.

Since what is important to us is the cardinality $k = |s(\mathcal{C})|$ and the group $p(\mathcal{C})$ of permutation parts of $\mathrm{Aut}(\mathcal{C})$, we will write

$$\mathrm{Aut}(\mathcal{C}) = k.p(\mathcal{C}). \tag{3}$$

THEOREM 1.1. *If $\mathcal{C}$ is a code over $\mathbb{Z}_{p^2}$ with type $1^0p^{k_2}$, then* $\mathrm{Aut}(\mathcal{C}) = \mathrm{Aut}(T(\mathcal{C}))$.

Proof. Since $\mathcal{C}$ is of type $1^0p^{k_2}$, it is easily deduced that for a codeword $c \in \mathcal{C}$ there exists a $c' \in T(\mathcal{C})$ such that $c = pc'$ and there is an one-to-one correspondence between $\mathcal{C}$ and $T(\mathcal{C})$. Let $t \in \mathrm{Aut}(\mathcal{C})$. Then for any $c_1 \in \mathcal{C}$ there exists $c_2 \in \mathcal{C}$ such that $c_1 t = c_2$. Then there exist c_1' and c_2' in $T(\mathcal{C})$ such that $c_1 t = pc_1' t = pc_2' = c_2 \Leftrightarrow c_1' t = c_2'$. Therefore $t \in \mathrm{Aut}(T(\mathcal{C}))$. Conversely, let $t \in \mathrm{Aut}(T(\mathcal{C}))$. Then for any $c_1' \in T(\mathcal{C})$ there exists $c_2' \in T(\mathcal{C})$ such that $c_1' t = c_2'$. So $c_1' t = c_2' \Leftrightarrow pc_1' t = pc_2' \Leftrightarrow c_1 t = c_2$. Therefore $t \in \mathrm{Aut}(\mathcal{C})$. □

The following theorems are directly from [3].

THEOREM 1.2. [3] *If $\mathcal{C}$ is a self-dual code over $\mathbb{Z}_{p^2}$ with type $1^1p^{k_2}$, then* $\mathrm{Aut}(\mathcal{C}) = \mathrm{Aut}(R(\mathcal{C}))$.

Next theorem tells us that the automorphism of rank 1 code can be obtained easily.

THEOREM 1.3. [3] *Let $\mathcal{C}$ be a code over $\mathbb{Z}_{p^e}$ of length 3 for odd prime p with generator matrix $\begin{pmatrix} a_1 & a_2 & a_3 \end{pmatrix}$. Let (ij) and (123) be elements in S_3 and $\omega \in \mathbb{Z}_p$ such that $\omega^6 = 1, \omega \neq \pm 1$.*

(i) *If $a_i^2 = a_j^2$, then $(ij) \in p(\mathcal{C})$.*
(ii) *If $(ij) \in p(\mathcal{C})$ and $a_i^2 \neq a_j^2$, then $a_i^2 = -a_j^2$. Hence if $a_i^4 \neq a_j^4$ then $(ij) \notin p(\mathcal{C})$.*
(iii) *$a_1^2 = a_2^2 = a_3^2$ if and only if $p(\mathcal{C}) = S_3$.*
(iv) *If $a_2^2 = \omega^2 a_1^2$, $a_3^2 = \omega^4 a_1^2$, then $(123) \in p(\mathcal{C})$ and $S_3 \neq p(\mathcal{C})$.*
(v) *If the number of a_i's which are zero is m, then $|s(\mathcal{C})| = 2^{1+m}$. Moreover, this is also true when $\mathcal{C}$ has an arbitrary length with rank 1.*

A code is called *decomposable* if the code is a direct sum of two or more codes. If a code is not decomposable, it is called *indecomposable*. Next theorem tells us about automorphism of a decomposable code.

THEOREM 1.4. [2] *If* $\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2$ *then* $\mathrm{Aut}(\mathcal{C}) \supseteq \mathrm{Aut}(\mathcal{C}_1) \times \mathrm{Aut}(\mathcal{C}_2)$.

2. Mass formula for self-orthogonal codes

THEOREM 2.1. [9, 10] *Let* $\sigma_p(n,k)$ *be the number of self-orthogonal codes of length* n *and dimension* k *over* $\mathbb{Z}_p$, *where* p *is odd prime. Then:*

1. If n *is odd,*

$$\sigma_p(n,k) = \frac{\prod_{i=0}^{k-1}(p^{(n-1-2i)}-1)}{\prod_{i=1}^{k}(p^i-1)}, \quad (k \geq 1).$$

2. If n *is even,*

$$\sigma_p(n,k) = \frac{(p^{n-k}-1-\eta((-1)^{\frac{n}{2}})(p^{n/2-k}-p^{n/2}))\prod_{i=1}^{k-1}(p^{n-2i}-1)}{\prod_{i=1}^{k}(p^i-1)}, (k \geq 2)$$

$$\sigma_p(n,1) = \frac{p^{n-1}-1-\eta((-1)^{\frac{n}{2}})(p^{n/2-1}-p^{n/2})}{p-1}$$

where $\eta(x)$ *is 1 if* x *is a square, -1 if* x *is not a square and 0 if* $x=0$.

Note that $\sigma_p(n,0) = 1$ *for all* n.

The number of self-orthogonal codes of length n over $\mathbb{Z}_{p^2}$ is computed separately by the following theorem.

THEOREM 2.2. [1] *Let* p *be an odd prime. Then the number of distinct self-orthogonal codes of length* n *over* $\mathbb{Z}_{p^2}$ *of type* $1^{k_1}p^{k_2}$ *is*

$$M_{p^2}(k_1,k_2) = \sigma_p(n,k_1)\begin{bmatrix} n-2k_1 \\ k_2 \end{bmatrix}_p p^{k_1(2n-3k_1-1-2k_2)/2}, \tag{4}$$

where

$$\begin{bmatrix} n \\ k \end{bmatrix}_p = \frac{(p^n-1)(p^n-p)\cdots(p^n-p^{k-1})}{(p^k-1)(p^k-p)\cdots(p^k-p^{k-1})}.$$

For given n, p, k_1 and k_2, we now know the total number of self-orthogonal codes of length n over $\mathbb{Z}_{p^2}$ of type $1^{k_1}p^{k_2}$. Thus we can create mass formula which plays a key role in the classfication problem.

$$\sum_i \frac{|\mathbb{T}_m^n|}{|\operatorname{Aut}(\mathcal{C}_i)|} = M_{p^2}(k_1, k_2), \tag{5}$$

where $\mathcal{C}_i$'s are all inequivalent codes of type $1^{k_1}p^{k_2}$.

3. Classification of self-orthogonal codes over $\mathbb{Z}_{p^2}$ of length 1 and 2

From now on p is an odd prime, we will denote a code $\mathcal{C}$ with generator matrix G by $\mathcal{C} : G$. And a solution of $x^2 + 1 = 0$ in $\mathbb{Z}_p$ (or $\mathbb{Z}_{p^2}$) by $\pm i$.

3.1. self-orthogonal codes over $\mathbb{Z}_{p^2}$ of length 1. (p) generates the unique self-orthogonal codes of length 1 over $\mathbb{Z}_{p^2}$. Generally, pI_n generates the unique self-orthogonal codes over $\mathbb{Z}_{p^2}$ of length n and rank n for all primes p with the automorphism $2^n.S_n$. This type of code is called the *trivial code*. Actually, a trivial code over $\mathbb{Z}_{p^2}$ is a self-dual code.

3.2. self-orthogonal codes over $\mathbb{Z}_{p^2}$ of length 2. Since $|\mathcal{C}| \leq p^n$ for a self-orthogonal code $\mathcal{C}$ of length n over $\mathbb{Z}_{p^2}$, we have $p^{2k_1+k_2} \leq p^2$, i.e., $2k_1 + k_2 =$ 1 or 2. Thus there exist only three types of codes of length 2, of 1^0p^2, 1^1p^0 and 1^0p^1. Any self-orthogonal code $\mathcal{C}$ of length 2 over $\mathbb{Z}_{p^2}$ is equivalent to one of following types.

(1) Type 1^0p^2 code, trivial code $p \oplus p : pI_2$.
(2) Type 1^1p^0 code $\mathcal{C}_a^{1,0} : \begin{pmatrix} 1 & a \end{pmatrix}$ where $a \in \mathbb{Z}_{p^2}$.
(3) Type 1^0p^1 code $\mathcal{C}_a^{0,1} : \begin{pmatrix} p & pa \end{pmatrix}$ where $a \in \mathbb{Z}_p$.

Note that $\mathcal{C}_a^{k_1,k_2} \sim \mathcal{C}_{-a}^{k_1,k_2}$.

Theorem 3.1. *There is a unique self-orthogonal code $\mathcal{C}_a^{1,0}$ up to equivalence if and only if $p \equiv 1 \pmod 4$. In this case, $\operatorname{Aut}(\mathcal{C}_a^{1,0}) = 2.S_2$.*

Proof. By Theorem 1.3.(v), the number of pure signs is $2^1 = 2$. By self-orthogonality, a is a solution of $1 + x^2 = 0$ in $\mathbb{Z}_{p^2}$ and we can take $a = i$. It is well-known that this equation has solutions when $p \equiv 1 \pmod 4$. Let $\gamma\sigma = (1, -1)(12) \in \mathbb{T}_{p^2}^2$ act on $\mathcal{C}_i^{1,0} : (1, i)$. Then $(1, i)\gamma\sigma = (i, -1) = i(1, i)$. Thus $(12) \in p(\mathcal{C})$. □

Theorem 3.2. *The self-orthogonal code $\mathcal{C}_a^{0,1}$ is equivalent to one of the following classes of inequivalent codes:*

(i) $\mathcal{C}_a^{0,1}$ *with* $a = 0$, $\operatorname{Aut}(\mathcal{C}_a^{0,1}) = 4.(1)$.

(ii) $\mathcal{C}_a^{0,1}$ *with* $a^2 = 1$, $\mathrm{Aut}(\mathcal{C}_a^{0,1}) = 2.S_2$.
(iii) $\mathcal{C}_a^{0,1}$ *with* $a^2 = -1$, $\mathrm{Aut}(\mathcal{C}_a^{0,1}) = 2.S_2$.
(iv) $\mathcal{C}_a^{0,1}$ *with* $a \neq 0, a^4 \neq 1$, $\mathrm{Aut}(\mathcal{C}_a^{0,1}) = 2.(1)$.

Proof. By Theorem 1.3.(v), the number of pure signs is obtained easily. To find the permutation parts, by Theorem 1.1, it suffices to classify permutation parts of codes over $\mathbb{Z}_p$ with generator matrix $\begin{pmatrix}1 & a\end{pmatrix}$. For $\gamma\sigma \in \mathbb{T}_p^2$, $\gamma\sigma \in \mathrm{Aut}(\mathcal{C}_a^{0,1})$ if and only if there exists nonzero $k \in \mathbb{Z}_p$ such that

$$(1, a)\gamma\sigma = k(1, a).$$

Thus according to each solution of above equation, we can determine permutation parts.

(i) It is trivial that $p(\mathcal{C}_a^{0,1}) = (1)$ when $a = 0$.
(ii) Let $a = 1$. It is obvious that $(1, 1)(1, 1)(12) = (1, 1)$, it means $(12) \in p(\mathcal{C})$.
(iii) Let $a = i$. $(1, i)(1, -1)(12) = (-i, 1) = -i(1, i)$. Thus $(12) \in p(\mathcal{C})$.
(iv) Suppose that $(12) \in \mathrm{Aut}(\mathcal{C}_a^{0,1})$. This means that there exist γ and k such that $(1, a)(\gamma_1, \gamma_2)(12) = k(1, a)$ i.e., $(a\gamma_2, \gamma_1) = (k, ka)$. Hence $a^2 = \pm 1$. Thus if $a^4 \neq 1$ then $\mathrm{Aut}(\mathcal{C}_a^{0,1}) = (1)$.

□

THEOREM 3.3. *Let N_1, N_2, N_3 and N_4 be the numbers of code $\mathcal{C}_a^{0,1}$ in the class (i),(ii),(iii) and (iv), respectively, up to equivalence. Then,*

(i) *Class (i) code $\mathcal{C}_0^{0,1}$ exists uniquely up to equivalence for all primes p.*
(ii) *Class (ii) code $\mathcal{C}_1^{0,1}$ exists uniquely up to equivalence for all primes p.*
(iii) *Class (iii) code $\mathcal{C}_i^{0,1}$ exists uniquely up to equivalence for all primes $p \equiv 1 \pmod 4$.*
(iv) *Class (iv) codes $\mathcal{C}_a^{0,1}$ exists for all primes $p \geq 7$, and*

$$N_4 = \begin{cases} \frac{p-5}{4}, & p \equiv 1 \pmod 4 \\ \frac{p-3}{4}, & p \equiv 3 \pmod 4). \end{cases}$$

So, N_1, N_2, N_3 and N_4 are determined as the following table.

p(mod 4)	N_1	N_2	N_3	N_4
1	1	1	1	$\frac{p-5}{4}$
3	1	1	0	$\frac{p-3}{4}$

Proof. Class (i), (ii) and (iii) are obvious. In the case of class (iv), we use the mass formula. The total number of distinct self-orthogonal codes $\mathcal{C}_a^{0,1}$ is

$$M_{p^2}(0,1) = \sigma_p(2,0) \begin{bmatrix} 2 \\ 1 \end{bmatrix}_p p^0 = \frac{p^2-1}{p-1} = p+1.$$

By the mass formula (5),

$$\sum_{\mathcal{C}} \frac{2^2 \times 2!}{|\operatorname{Aut}(\mathcal{C})|} = p+1.$$

By Theorem 3.2, this implies that

$$2N_1 + 2N_2 + 2N_3 + 4N_4 = p+1.$$

As a consequence,

$$N_4 = \begin{cases} \frac{p-5}{4}, & p \equiv 1 \pmod 4 \\ \frac{p-3}{4}, & p \equiv 3 \pmod 4). \end{cases}$$

□

4. Classification of self-orthogonal codes over $\mathbb{Z}_{p^2}$ of length 3

By the same argument as in the case of length 2, there are self-orthogonal codes $\mathcal{C}$ of length 3 over $\mathbb{Z}_{p^2}$ equivalent to one of following types.
(1) Type 1^0p^3 code, trivial code $p \oplus p \oplus p : pI_3$.
(2) Type 1^1p^0 code $\mathcal{C}_{a,b}^{1,0} : \begin{pmatrix} 1 & a & b \end{pmatrix}$, where $a, b \in \mathbb{Z}_{p^2}$.
(3) Type 1^0p^1 code $\mathcal{C}_{a,b}^{0,1} : \begin{pmatrix} p & pa & pb \end{pmatrix}$, where $a, b \in \mathbb{Z}_p$.
(4) Type 1^1p^1 code $\mathcal{C}_{a,b}^{1,1} : \begin{pmatrix} 1 & a & b \\ 0 & p & pc \end{pmatrix}$, where $a, c \in \mathbb{Z}_p$, $b \in \mathbb{Z}_{p^2}$ and c is determined by a and b.
(5) Type 1^0p^2 code $\mathcal{C}_{a,b}^{0,2} : \begin{pmatrix} p & 0 & pa \\ 0 & p & pb \end{pmatrix}$, where $a, b \in \mathbb{Z}_p$.
Note that it is obvious that $\mathcal{C}_{a,b}^{k_1,k_2} \sim \mathcal{C}_{a,-b}^{k_1,k_2} \sim \mathcal{C}_{-a,b}^{k_1,k_2} \sim \mathcal{C}_{-a,-b}^{k_1,k_2}$.

4.1. Self-orthogonal codes of type 1^1p^0.

THEOREM 4.1. *Self-orthogonal code* $\mathcal{C}^{1,0}_{a,b}$ *is equivalent to one of the following classes of inequivalent codes:*

(i) $\mathcal{C}^{1,0}_{a,b}$ *with* $a = 0$, $b^2 + 1 = 0$, $\mathrm{Aut}(\mathcal{C}^{1,0}_{a,b}) = 4.\langle(13)\rangle$. *Note that* $\mathcal{C}^{1,0}_{0,b} \sim \mathcal{C}^{1,0}_{b,0}$.

(ii) $\mathcal{C}^{1,0}_{a,b}$ *with* $a^2 = 1$, $\mathrm{Aut}(\mathcal{C}^{1,0}_{a,b}) = 2.S_2$. *Note that* $\mathcal{C}^{1,0}_{1,b} \sim \mathcal{C}^{1,0}_{a,b}$ *when* $a^2 = b^2 \neq 1$.

(iii) $\mathcal{C}^{1,0}_{a,b}$ *with* $a^6 = 1, a^4 \neq 1$, $\mathrm{Aut}(\mathcal{C}^{1,0}_{a,b}) = 2.\langle(123)\rangle$. *In this case* $b^2 = a^4$. *When* $b^6 = 1, b^4 \neq 1$, $\mathcal{C}^{1,0}_{a,b}$ *is also equivalent to the code of this class.*

(iv) $\mathcal{C}^{1,0}_{a,b}$ *with* $ab \neq 0, a^6 \neq 1, b^6 \neq 1, a^4 \neq 1, b^4 \neq 1, a^4 \neq b^2, b^4 \neq a^2$ *and* $a^4 \neq b^4$, $\mathrm{Aut}(\mathcal{C}^{1,0}_{a,b}) = 2.(1)$.

Proof. By the self-orthogonality $1 + a^2 + b^2 \equiv 0 \pmod{p^2}$ and by Theorem 1.3.(v), the number of pure signs is obtained easily.

(i) Assume $a = 0$. Let $\gamma\sigma = (1, 1, -1)(13) \in \mathbb{T}^3_{p^2}$. Then $(1, 0, i)(1, 1, -1)(13) = -i(1, 0, i)$. Thus $(13) \in p(\mathcal{C})$. Now suppose that $(12) \in p(\mathcal{C})$ such that $\mathcal{C}\gamma(12) = \mathcal{C}$. Then there exist γ and nonzero k such that $(1, 0, i)\gamma(12) = k(1, 0, i)$, which implies $k = 0$, a contradiction. Hence $(12) \notin p(\mathcal{C})$. Similarly, $(23) \notin p(\mathcal{C})$. Suppose that $(123) \in p(\mathcal{C})$. Then there exist γ and nonzero k such that $(1, 0, i)\gamma(123) = k(1, 0, i)$. It implies that $k = 0$, which is a contradiction. Therefore $(123) \notin p(\mathcal{C})$.

(ii) Let $a = 1$. By Theorem 1.3, $(12) \in p(\mathcal{C})$. To show that $(13) \notin p(\mathcal{C})$, suppose that there exists $\gamma = (\gamma_1, \gamma_2, \gamma_3) \in \mathbb{D}^3_{p^2}$ such that $\mathcal{C}\gamma(13) = \mathcal{C}$. Then there exist γ and nonzero k such that $(b\gamma_3, \gamma_2, \gamma_1) = k(1, 1, b)$, which implies $b^2 = 1$. It is a contradiction to the condition $b^2 + 2 = 0$. Similarly, $(23) \notin p(\mathcal{C})$.

Now, Suppose $(123) \in p(\mathcal{C})$. Then there exist γ and nonzero k such that $(1, 1, b)\gamma(123) = k(1, 1, b)$, which implies $b^4 = 1$, a contradiction. Therefore $(123) \notin p(\mathcal{C})$, and along the same lines, $(132) \notin p(\mathcal{C})$.

(iii) By Theorem 1.3.(iv), $(123) \in p(\mathcal{C})$. Thus it suffices to show that $(12) \notin p(\mathcal{C})$. Suppose that there exits γ and nonzero k such that $(a\gamma_2, \gamma_1, b\gamma_3) = k(1, a, b)$, which implies $a^2 = \pm 1$. It is a contradiction to the condition $a^4 \neq 1$. $\mathcal{C}\gamma(12)$ contains $(a\gamma_2, \gamma_1, b\gamma_3)$. Since this element is also in $\mathcal{C}$, $(a\gamma_2, \gamma_1, b\gamma_3) = a\gamma_2(1, a, b)$. However it leads to $a^2 = 1$ which is a contradiction. Hence, $\langle(123)\rangle = p(\mathcal{C})$.

(iv) By Theorem 1.3 and condition $a^4 \neq 1, b^4 \neq 1$ and $a^4 \neq b^4$, $(12), (13), (23) \notin p(\mathcal{C})$. Suppose $(123) \in p(\mathcal{C})$. Then there exist γ and nonzero k such that $(1, a, b)\gamma(123) = k(1, a, b)$. It implies that $b^2 = a^4$, which is a contradiction. Hence $(123) \notin p(\mathcal{C})$. Similarly we can check $(132) \notin p(\mathcal{C})$. Hence $p(\mathcal{C}) = (1)$.

□

THEOREM 4.2. *Let N_1, N_2, N_3 and N_4 be the numbers of class (i),(ii),(iii) and (iv) of self-orthogonal codes over $\mathbb{Z}_{p^2}$ of length 3 up to equivalence, respectively. Then,*

(i) *Class (i) code $\mathcal{C}_{0,b}^{1,0}$ exists uniquely up to equivalence for $p \equiv 1 \pmod 4$.*

(ii) *Class (ii) code $\mathcal{C}_{1,b}^{1,0}$ exists uniquely up to equivalence for $p \equiv 1, 3 \pmod 8$.*

(iii) *Class (ii) code $\mathcal{C}_{a,b}^{1,0}$ exists uniquely up to equivalence for $p \equiv 1 \pmod 6$.*

(iv) *Class (iv) codes $\mathcal{C}_{a,b}^{1,0}$ exists for all primes $p \geq 5$. N_1, N_2, N_3 and N_4 are determined as the following table.*

$p \pmod{24}$	N_1	N_2	N_3	N_4
1	1	1	1	$\frac{p^2+p-26}{24}$
5	1	0	0	$\frac{p^2+p-6}{24}$
7	0	0	1	$\frac{p^2+p-8}{24}$
11	0	1	0	$\frac{p^2+p-12}{24}$
13	1	0	1	$\frac{p^2+p-14}{24}$
17	1	1	0	$\frac{p^2+p-18}{24}$
19	0	1	1	$\frac{p^2+p-20}{24}$
23	0	0	0	$\frac{p^2+p}{24}$

Proof. (i) It is well-known that equation $1 + b^2 = 0$ has solution when $p \equiv 1 \pmod 4$.

(ii) The equation $b^2 + 2 \equiv 0 \pmod{p^2}$ has a solution when $\left(\frac{-2}{p}\right) = 1$, i.e., $p \equiv 1, 3 \pmod 8$.

(iii) $a^6 = 1$ has a solution when $p \equiv 1 \pmod 6$.

(iv) The number of self-orthogonal codes of length 3 and type 1^1p^0 is

$$\begin{aligned} M_{p^2}(1,0) &= \sigma_p(3,1)\begin{bmatrix}3-2\\0\end{bmatrix}_p p^{1(6-3-1)/2} = \sigma_p(3,1)\begin{bmatrix}1\\0\end{bmatrix}_p p \\ &= \frac{p^2-1}{p-1}p = (p+1)p. \end{aligned}$$

And by the mass formula (5), $\sum_{\mathcal{C}} \frac{2^3\times 3!}{|\operatorname{Aut}(\mathcal{C})|} = (p+1)p$. Therefore, $N_4 = \frac{1}{24}\{\ p(p+1) - 6N_1 - 12N_2 - 8N_3\}$.

□

4.2. Self-orthogonal codes of type 1^0p^1.

THEOREM 4.3. *Self-orthogonal code $\mathcal{C}_{a,b}^{0,1}$ is equivalent to one of the following classes of inequivalent codes:*

(i) $\mathcal{C}_{a,b}^{0,1}$ *with* $a=b=0$, $\operatorname{Aut}(\mathcal{C}_{a,b}^{0,1}) = 8.\langle(23)\rangle$.
(ii) $\mathcal{C}_{a,b}^{0,1}$ *with* $b^2=1, a=0$, $\operatorname{Aut}(\mathcal{C}_{a,b}^{0,1}) = 4.\langle(13)\rangle$. *Note that* $\mathcal{C}_{0,1}^{0,1} \sim \mathcal{C}_{1,0}^{0,1}$.
(iii) $\mathcal{C}_{a,b}^{0,1}$ *with* $b^2=-1, a=0$, $\operatorname{Aut}(\mathcal{C}_{a,b}^{0,1}) = 4.\langle(13)\rangle$. *Note that* $\mathcal{C}_{0,b}^{0,1} \sim \mathcal{C}_{b,0}^{0,1}$.
(iv) $\mathcal{C}_{a,b}^{0,1}$ *with* $b^4\neq 1, a=0$, $\operatorname{Aut}(\mathcal{C}_{a,b}^{0,1}) = 4.(1)$. *Note that* $\mathcal{C}_{0,b}^{0,1} \sim \mathcal{C}_{b,0}^{0,1}$.
(v) $\mathcal{C}_{a,b}^{0,1}$ *with* $a^2=1=b^2$, $\operatorname{Aut}(\mathcal{C}_{a,b}^{0,1}) = 2.S_3$.
(vi) $\mathcal{C}_{a,b}^{0,1}$ *with* $b^2=1,\ a^2\neq 0,1$, $\operatorname{Aut}(\mathcal{C}_{a,b}^{0,1}) = 2.\langle(13)\rangle$. *Note that* $\mathcal{C}_{a,1}^{0,1} \sim \mathcal{C}_{1,a}^{0,1} \sim \mathcal{C}_{a,b}^{0,1}$ *when* $a^2=b^2\neq 1$.
(vii) $\mathcal{C}_{a,b}^{0,1}$ *with* $a^6=1,\ a^4\neq 1$ *and* $a^4=b^2$, $\operatorname{Aut}(\mathcal{C}_{a,b}^{0,1}) = 2.\langle(123)\rangle$. *When* $b^6=1, b^4\neq 1, b^4=a^2$, $\mathcal{C}_{a,b}^{0,1}$ *is equivalent to one of this class.*
(viii) $\mathcal{C}_{a,b}^{0,1}$ *with* $ab\neq 0, a^4\neq 1, b^4\neq 1, a^6\neq 1, b^6\neq 1, a^4\neq b^2, b^4\neq a^2$ *and* $a^4\neq b^4$, $\operatorname{Aut}(\mathcal{C}_{a,b}^{0,1}) = 2.(1)$.

Proof. By Theorem 1.3.(v), the number of pure signs is obtained easily. By Theorem 1.1, it suffices to classify $\begin{pmatrix}1 & a & b\end{pmatrix}$ over $\mathbb{Z}_p$. For $\gamma\sigma\in\mathbb{T}_p^3, k\in\mathbb{Z}_p$, if $\gamma\sigma\in\operatorname{Aut}(\mathcal{C}_{a,b}^{0,1})$ then $(1,a,b)\gamma\sigma = k(1,a,b) \iff (1,a^2,b^2)\sigma = k^2(1,a,b^2)$.

(i) Assume $a=b=0$. It is trivial that $(23)\in p(\mathcal{C})$.

Suppose that $(12)\in p(\mathcal{C})$. Then there exists $\gamma\in\mathbb{D}_p^3$ and nonzero k such that $(1,0,0)\gamma(12) = k(1,0,0)$ which implies $k=0$, a contradiction. Hence $(12)\notin p(\mathcal{C})$. Similarly $(13)\notin p(\mathcal{C})$. Now, suppose that $(123) \in p(\mathcal{C})$. Then there exists γ and nonzero k such that $(1,0,0)\gamma(123) = k(1,0,0)$. It implies $k = 0$, which is a contradiction.

(ii) Let $b = 1, a = 0$. $(1,0,1)(1,1,1)(13) = (1,1,1)$. Hence $(13) \in p(\mathcal{C})$. Suppose that $(12) \in p(\mathcal{C})$. Then there exist γ and nonzero k such that $(1,0,1)\gamma(12) = k(1,0,1)$ which implies $k = 0$, a contradiction. Hence $(12) \notin p(\mathcal{C})$ and similarly $(23) \notin p(\mathcal{C})$.

Suppose that $(123) \in p(\mathcal{C})$. Then there exist $\gamma \in \mathbb{D}_p^3$ and nonzero k such that $(1,0,1)\gamma(123) = (0,\gamma_3,\gamma_1) = k(1,0,1)$. It implies $k = 0$, a contradiction. Similarly $(1,0,1)\gamma(132) = k(1,0,1)$ leads to $k = 0$, a contradiction.

(iii) Let $b = i, a = 0$. Then $(1,0,i)(1,1,-1)(13) = (-i,0,1) = -i(1,0,i)$. Thus $(13) \in p(\mathcal{C})$. Suppose $(12) \in p(\mathcal{C})$. Then there exist γ and nonzero k such that $(1,0,i)\gamma(12) = k(1,0,i)$ which implies $k = 0$, a contradiction. Hence $(12) \notin p(\mathcal{C})$. Also, we can easily check as in (ii), $(23), (123), (132) \notin p(\mathcal{C})$.

(iv) By Theorem 1.3.(ii) and by condition $b^4 \neq 1$, $(12), (13), (23) \notin p(\mathcal{C})$. Suppose that $(123) \in p(\mathcal{C})$. Then there exist γ and nonzero k such that $(1,0,b)\gamma(123) = k(1,0,b)$. It leads to $k = 0$, a contradiction. Hence $(123) \notin p(\mathcal{C})$.

(v) By Theorem 1.3.(iii), it is obvious.

(vi) Let $b = 1$. By Theorem 1.3. (ii), $(13) \in p(\mathcal{C})$. Suppose that $(12) \in p(\mathcal{C})$. Then there exist γ and nonzero k such that $(1,a,1)\gamma(12) = k(1,a,1)$. It leads to $a^4 = 1$ which is a contradiction to the condition $a^2 \neq 1$. Hence $(12) \notin p(\mathcal{C})$. Similarly, $(23) \notin p(\mathcal{C})$.

Suppose that $(123) \in p(\mathcal{C})$. Then there exist γ and nonzero k such that $(1,a,1)\gamma(123) = k(1,a,1)$. It implies $a^4 = 1$, a contradiction.

(vii) By Theorem 1.3.(iv), $(123) \in p(\mathcal{C})$. To show $(13) \notin p(\mathcal{C})$, suppose that there exist γ and nonzero k such that $(1,a,b)\gamma(13) = k(1,a,b)$. However it leads to $b^2 = \pm 1$ which is a contradiction. Thus $(13) \notin p(\mathcal{C})$.

(viii) By Theorem 1.3 and by the conditions $a^4 \neq 1, b^4 \neq 1, a^4 \neq b^4$, $(12), (13), (23) \notin p(\mathcal{C})$. Suppose that $(123) \in p(\mathcal{C})$. Then there eixst γ and nonzero k such that $(1,a,b)\gamma(123) = k(1,a,b)$. It implies that $b^2 = a^4$, which is a contradiction. Hence it is obvious that $p(\mathcal{C}) = (1)$.

□

THEOREM 4.4. *Let $N_1, N_2, N_3, N_4, N_5, N_6, N_7, N_8$ be the number of class (i) - (viii) of codes $\mathcal{C}_{a,b}^{0,1}$ up to equivalence, respectively. $N_i's$ are determined as follows.*

p(mod 12)	N_1	N_2	N_3	N_4	N_5	N_6	N_7	N_8
1	1	1	1	$\frac{p-5}{4}$	1	$\frac{p-3}{2}$	1	$\frac{(p-1)(p-7)}{24}$
5	1	1	1	$\frac{p-5}{4}$	1	$\frac{p-3}{2}$	0	$\frac{(p-3)(p-5)}{24}$
7	1	1	0	$\frac{p-3}{4}$	1	$\frac{p-3}{2}$	1	$\frac{(p-1)(p-7)}{24}$
11	1	1	0	$\frac{p-3}{4}$	1	$\frac{p-3}{2}$	0	$\frac{(p-3)(p-5)}{24}$

Note that we obtained directly all self-orthogonal codes over $\mathbb{Z}_9$ at the next section.

Proof. Note that $\mathcal{C}_{0,b}^{0,1} \sim \mathcal{C}_a^{0,1} \oplus (0)$. N_1, N_2, N_3 and N_4 are same as the results of Theorem 3.3. Existence of class (v) and (vii) and N_5, N_7 are obvious. Now it suffices to find N_6 and N_8.

(vi) $a \in \mathbb{Z}_p, a^2 \neq 0, 1$ imply that the number of choices of a is $p-3$. From the fact that $\mathcal{C}_{a,1}^{0,1} \sim \mathcal{C}_{a,-1}^{0,1}$, we have $N_6 = \frac{p-3}{2}$ for all primes p.

(viii) The number of self-orthogonal codes of length 3 of type 1^0p^1 is

$$M_{p^2}(0,1) = \sigma_p(3,0)\begin{bmatrix}3\\1\end{bmatrix}_p = \frac{p^3-1}{p-1} = p^2+p+1.$$

By the mass formula (5),

$$\sum_C \frac{2^3 \times 3!}{|\operatorname{Aut}(\mathcal{C})|} = p^2+p+1.$$

Hence,

$$N_8 = \frac{1}{24}\{p^2+p+1-3N_1-6N_2-6N_3-12N_4-4N_5-12N_6-8N_7\}.$$

This formula gives N_8.

□

4.3. Self-orthogonal codes of type 1^1p^1. Actually, self-orthogonal codes of type 1^1p^1 are self-dual codes. All theorems in this section are from [3].

THEOREM 4.5. *The self-dual code over $\mathbb{Z}_{p^2}$ of length 3 with type 1^1p^1 is equivalent to one of the following classes of inequivalent codes:*

(i) *Suppose* $a = 0$. *Then,* $\mathrm{Aut}(\mathcal{C}^{1,1}_{0,b}) = 4.\langle(13)\rangle$. *This class exists if and only if when* $p \equiv 1 \pmod 4$.

(ii) *Suppose* $a^6 \equiv 1$ *and* $a \neq \pm 1$. *Then,* $\mathrm{Aut}(\mathcal{C}^{1,1}_{a,b}) = 2.\langle(123)\rangle$. *This class exists if and only if when* $p \equiv 1 \pmod 3$.

(iii) *Suppose* $a = 1$. *Then,* $\mathrm{Aut}(\mathcal{C}^{1,1}_{1,b}) = 2.\langle(12)\rangle$. *This class exists if and only if when* $p \equiv 1, 3 \pmod 8$.

(iv) *Suppose* $a \neq 0, a^3 \neq \pm 1 \pmod p, b^3 \neq \pm 1 \pmod p$ *and* $a^2 \neq b^2 \pmod p$. *Then,* $\mathrm{Aut}(\mathcal{C}^{1,1}_{a,b}) = 2.\langle(1)\rangle$. *This class exists if and only if when* $p \geq 23$.

THEOREM 4.6. *Let* N_1, N_2, N_3, N_4 *be the number of class (i), (ii), (iii), (iv) codes* $\mathcal{C}^{1,1}_{a,b}$ *over* $\mathbb{Z}_{p^2}$ *of length 3, respectively. These numbers are determined as follows.*

$p \pmod{24}$	N_1	N_2	N_3	N_4
1	1	1	1	$\frac{p-25}{24}$
5	1	0	0	$\frac{p-5}{24}$
7	0	1	0	$\frac{p-7}{24}$
11	0	0	1	$\frac{p-11}{24}$
13	1	1	0	$\frac{p-13}{24}$
17	1	0	1	$\frac{p-17}{24}$
19	0	1	1	$\frac{p-19}{24}$
23	0	0	0	$\frac{p+1}{24}$

4.4. Self-orthogonal codes of type 1^0p^2.

THEOREM 4.7. *Self-orthogonal code* $\mathcal{C}^{0,2}_{a,b}$ *is equivalent to one of the following eight classes of inequivalent codes;*

(i) $\mathcal{C}^{0,2}_{a,b}$ *with* $a = b = 0$, $\mathrm{Aut}(\mathcal{C}^{0,2}_{a,b}) = 8.S_2$.

(ii) $\mathcal{C}^{0,2}_{a,b}$ *with* $a^2 = 1, b = 0$, $\mathrm{Aut}(\mathcal{C}^{0,2}_{a,b}) = 4.\langle(13)\rangle$.

(iii) $\mathcal{C}^{0,2}_{a,b}$ *with* $a^2 = -1, b = 0$, $\mathrm{Aut}(\mathcal{C}^{0,2}_{a,b}) = 4.\langle(13)\rangle$.

(iv) $\mathcal{C}^{0,2}_{a,b}$ *with* $a^4 \neq 1, a \neq 0, b = 0$, $\mathrm{Aut}(\mathcal{C}^{0,2}_{a,b}) = 4.(1)$.

(v) $\mathcal{C}^{0,2}_{a,b}$ *with* $a^2 = b^2 = 1$, $\mathrm{Aut}(\mathcal{C}^{0,2}_{a,b}) = 2.S_3$.

(vi) $\mathcal{C}^{0,2}_{a,b}$ *with* $a^2 = 1, b \neq 0, 1$, $\mathrm{Aut}(\mathcal{C}^{0,2}_{a,b}) = 2.\langle(13)\rangle$.

(vii) $\mathcal{C}^{0,2}_{a,b}$ *with* $a^6 = 1, a^4 = b^2 \neq 1$, $\mathrm{Aut}(\mathcal{C}^{0,2}_{a,b}) = 2.\langle(123)\rangle$.

(viii) $\mathcal{C}^{0,2}_{a,b}$ *with* $a, b \neq 0, a^4 \neq 1, a^2 \neq b^2 \neq 1, a^6 \neq 1, b^2 \neq a^4, a^2 \neq b^4$ *and* $a^4 \neq b^4$, $\mathrm{Aut}(\mathcal{C}^{0,2}_{a,b}) = 2.(1)$.

Note that $\mathcal{C}_{a,b}^{0,2}(12) = \mathcal{C}_{b,a}^{0,2}$, *i.e.,* $\mathcal{C}_{a,b}^{0,2} \sim \mathcal{C}_{b,a}^{0,2}$.

Proof. By Theorem 1.1, it suffices to classify $\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \end{pmatrix}$ over $\mathbb{Z}_p$. Let the generators of this code be $f_1 = (1, 0, a)$ and $f_2 = (0, 1, b)$. At first, we check the pure signs of this code.
If $\gamma = (\gamma_1, \gamma_2, \gamma_3) \in s(\mathcal{C})$, then

$$\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \end{pmatrix} (\gamma_1, \gamma_2, \gamma_3) = \begin{pmatrix} \gamma_1 & 0 & \gamma_3 a \\ 0 & \gamma_2 & \gamma_3 b \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \end{pmatrix}.$$

Thus there exist solutions of the following equations;
$x(\gamma_1, 0, \gamma_3 a) + y(0, \gamma_2, \gamma_3 b) = (1, 0, a)$, and $z(\gamma_1, 0, \gamma_3 a) + w(0, \gamma_2, \gamma_3 b) = (0, 1, b)$.
This leads to

$$\begin{cases} x = \gamma_1, \ y = 0, \gamma_1\gamma_3 a = a \\ z = 0, \ w = \gamma_2, \ \gamma_2\gamma_3 b = b. \end{cases}$$

Accordingly, if $ab \neq 0$, then $\gamma_1\gamma_3 = 1$ and $\gamma_2\gamma_3 = 1$, i.e., $s(\mathcal{C}) = \{\pm(1, 1, 1)\}$ and $|s(\mathcal{C})| = 2$. If $ab = 0$, say $a \neq 0$ and $b = 0$, then $\gamma_2\gamma_3 = 1$ and $\gamma_1 = \pm 1$. i.e., $s(\mathcal{C}) = \{\pm(1, 1, 1), \pm(-1, 1, 1)\}$ and $|s(\mathcal{C})| = 4$. Finally, if $a = b = 0$ then $\gamma_1\gamma_3 = \pm 1$, $\gamma_2\gamma_3 = \pm 1$. Hence $|s(\mathcal{C})| = 8$ and $s(\mathcal{C}) = \{\pm(1, 1, 1), \pm(1, 1, -1), \pm(1, -1, 1), \pm(1, -1, -1)\}$.

Now, we check the permutation parts. Note that $\sigma \in p(\mathcal{C})$ if and only if

$$\begin{cases} xf_3\gamma + yf_4\gamma = f_1 \\ uf_3\gamma + vf_4\gamma = f_2 \end{cases} \tag{6}$$

have solutions x, y, u, v and γ where $f_3 = f_1\sigma$ and $f_4 = f_2\sigma$. Also, note that $\mathcal{C}_{a,b}^{0,2} \sim \mathcal{C}_{-a,b}^{0,2} \sim \mathcal{C}_{a,-b}^{0,2} \sim \mathcal{C}_{-a,-b}^{0,2}$.

(i) It is easily deduced that $\mathcal{C}(12)(1, 1, 1) = \mathcal{C}$ from $a = b = 0$. Thus $(12) \in p(\mathcal{C})$. $\mathcal{C}(13)$ is generated by $f_3 = f_1(13) = (0, 0, 1)$ and $f_4 = f_2(13) = (0, 1, 0)$. However $uf_3\gamma + vf_4\gamma = (1, 0, 0)$ has no solution. Thus $(13) \notin p(\mathcal{C})$. Since $(123) = (12)(13)$, $(123) \notin p(\mathcal{C})$. By the same argument, $(132), (23) \notin p(\mathcal{C})$.

(ii) Say $a = 1$. It is also easily deduced that $\mathcal{C}(13)(1, 1, 1) = \mathcal{C}$. Thus $(13) \in p(\mathcal{C})$. Assume $(12) \in p(\mathcal{C})$. Then from the equations (6), we can see that $(v\gamma_1, u\gamma_2, u\gamma_3) = (0, 1, 0)$ have no solution. Thus

$(12) \notin p(\mathcal{C})$. By the same argument as in (i), $(123), (132), (23) \notin p(\mathcal{C})$.

(iii) Similarly to the case in (ii), we can easily see that $p(\mathcal{C}) = \langle (13) \rangle$.

(iv) Suppose $(12) \in p(\mathcal{C})$. Then the equation $uf_3\gamma + vf_4\gamma = f_2$ must have a solution. But it is obvious that $(v\gamma_1, u\gamma_2, ua\gamma_3) = (0, 1, 0)$ has no solution. Thus $(12) \notin p(\mathcal{C})$.

Now, suppose $(123) \in p(\mathcal{C})$. Again, $uf_3\gamma + vf_4\gamma = f_2$ i.e., $(v\gamma_1, ua\gamma_2, u\gamma_3) = (0, 1, 0)$ has no solution. Thus $(123) \notin p(\mathcal{C})$. It is clear that $p(\mathcal{C}) = (1)$ by the same argument.

(v) It suffices to show $(12), (123) \in p(\mathcal{C})$.

Let $\sigma = (12)$. From the equations (6),

$$\begin{cases} x(0,1,a)\gamma + y(1,0,b)\gamma = (1,0,a) \\ u(0,1,a)\gamma + v(1,0,b)\gamma = (0,1,b), \end{cases}$$

it is clear that $x = 0, v = 0, y = \gamma_1$ and $u = \gamma_2$. Thus these equations hav a solution if and only if $yb\gamma_3 = a$ and $ua\gamma_3 = b$, i.e., $a^2 = b^2$. Thus $(12) \in p(\mathcal{C})$ if and only if $a^2 = b^2$. Therefore $(12) \in p(\mathcal{C})$.

Without loss of generality, assume $a = b = 1$. Now, let $\sigma = (123)$. It is also clear that the equations,

$$\begin{cases} x(0,1,1)\gamma + y(1,1,0)\gamma = (1,0,1) \\ u(0,1,1)\gamma + v(1,1,0)\gamma = (0,1,1) \end{cases}$$

has a solution $x = -1, y = 1, u = -1, v = 0, \gamma = (1, -1, -1)$. Therefore $(123) \in p(\mathcal{C})$.

(vi) By the argument in (v), $(12) \notin p(\mathcal{C})$, since $a^2 \neq b^2$.

Let $a = 1$ and $\sigma = (13)$. Then it is clear that the equations

$$\begin{cases} x(1,0,1)\gamma + y(b,1,0)\gamma = (1,0,1) \\ u(1,0,1)\gamma + v(b,1,0)\gamma = (0,1,b) \end{cases}$$

has a solution $x = 1, y = 0, u = b, v = -1$ and $\gamma = (1, -1, 1)$. Thus $(13) \in p(\mathcal{C})$ and $(123) \notin p(\mathcal{C})$ since $(12) \notin p(\mathcal{C})$. Consequently, $p(\mathcal{C}) = \langle (13) \rangle$.

Note that if $(13) \in p(\mathcal{C})$, then $a^4 = 1$. Because the first part of equations (6), $x(a,0,1)\gamma + y(b,1,0)\gamma = (1,0,a)$ tells that $y = 0$ and $xa\gamma_1 = 1$, $x\gamma_3 = a$. Thus $x^2a^2 = 1$ and $x^2 = a^2$ implies that $a^4 = 1$.

(vii) For neither $a^2 \neq b^2$ nor $a^4 \neq 1$, we can deduce that $(12), (13) \notin p(\mathcal{C})$.

Without loss of generality, assume $a^3 = 1$ and $b = a^2$. Now, let $\sigma = (123)$. It is also clear that the equations,

$$\begin{cases} x(0,a,1)\gamma + y(1,a^2,0)\gamma = (1,0,a) \\ u(0,a,1)\gamma + v(1,a^2,0)\gamma = (0,1,a^2) \end{cases}$$

has a solution $x = -a, y = 1, u = -a^2, v = 0, \gamma = (1,-1,-1)$. Therefore $(123) \in p(\mathcal{C})$.

(viii) By the condition $a^4 \neq b^4$, $(12) \notin p(\mathcal{C})$ and by the condition $a^4 \neq 1$, $(13) \notin p(\mathcal{C})$.

Assume that $(123) \in p(\mathcal{C})$. The first part of equations (6), $x(0,a,1)\gamma + y(1,b,0)\gamma = (1,0,a)$ tells that $x\gamma_3 = a, y = \gamma_1$ and $xa\gamma_2 + yb\gamma_2 = 0$. Thus $x^2 = a^2, y^2 = 1$ and $x^2a^2 = b^2$. Consequently $b^2 = a^4$. The second part of equations (6), $u(0,a,1)\gamma + v(1,b,0)\gamma = (0,1,b)$ tells that $v = 0$ and $ua\gamma_2 = 1$, $u\gamma_3 = b$. Thus $u^2a^2 = 1$ and $u^2 = b^2$. Therefore $a^2b^2 = 1$. $a^2b^2 = 1$ and $b^2 = a^4$ implies that $a^6 = 1$ which is contradict to the condition. Thus $(123) \notin p(\mathcal{C})$.

□

THEOREM 4.8. *Let $N_1, N_2, N_3, N_4, N_5, N_6, N_7$, and N_8 be the number of class (i) - (viii) of codes $\mathcal{C}_{a,b}^{0,2}$ up to equivalence, respectively. $N_i's$ are determined as follows.*

p(12)	N_1	N_2	N_3	N_4	N_5	N_6	N_7	N_8
1	1	1	1	$\frac{p-5}{4}$	1	$\frac{p-3}{2}$	1	$\frac{(p-1)(p-7)}{24}$
5	1	1	1	$\frac{p-5}{4}$	1	$\frac{p-3}{2}$	0	$\frac{(p-3)(p-5)}{24}$
7	1	1	0	$\frac{p-3}{4}$	1	$\frac{p-3}{2}$	1	$\frac{(p-1)(p-7)}{24}$
11	1	1	0	$\frac{p-3}{4}$	1	$\frac{p-3}{2}$	0	$\frac{(p-3)(p-5)}{24}$

Proof. $\mathcal{C}_{a,0}^{0,2} \sim \mathcal{C}_a^{0,1} \oplus (p)$. Thus N_1, N_2, N_3 and N_4 are exactly same as Theorem 3.3. N_5, N_6 and N_7 are obtained by the same argument as in the Theorem 4.4.

The number of self-orthogonal codes of length 3 of type 1^0p^2 is

$$M_{p^2}(0,2) = \sigma_p(3,0)\begin{bmatrix}3\\2\end{bmatrix}_p = \frac{(p^3-1)(p^3-p)}{(p^2-1)(p^2-p)} = p^2 + p + 1.$$

By the mass formula (5),

$$\sum_{C} \frac{2^3 \times 3!}{|\operatorname{Aut}(\mathcal{C})|} = p^2 + p + 1.$$

Hence,

$$N_8 = \frac{1}{24}\{p^2 + p + 1 - 3N_1 - 6N_2 - 6N_3 - 12N_4 - 4N_5 - 12N_6 - 8N_7\}.$$

□

5. Examples

Self-orthogonal codes of length 3 over $\mathbb{Z}_{p^2}$ for all primes $p \leq 13$ are shown in the following table.

Type	Aut.	$\mathbb{Z}_{2^2}$	$\mathbb{Z}_{3^2}$	$\mathbb{Z}_{5^2}$	$\mathbb{Z}_{7^2}$	$\mathbb{Z}_{11^2}$	$\mathbb{Z}_{13^2}$
$\mathcal{C}_{a,b}^{1,0}$	$4.\langle(13)\rangle$			$\mathcal{C}_{0,7}^{1,0}$			$\mathcal{C}_{0,70}^{1,0}$
	$2.\langle(12)\rangle$		$\mathcal{C}_{1,4}^{1,0}$			$\mathcal{C}_{1,19}^{1,0}$	
	$2.\langle(123)\rangle$				$\mathcal{C}_{18,19}^{1,0}$		$\mathcal{C}_{22,23}^{1,0}$
	$2.(1)$			$\mathcal{C}_{5,7}^{1,0}$	$\mathcal{C}_{2,7}^{1,0}$, $\mathcal{C}_{4,9}^{1,0}$	$\mathcal{C}_{3,56}^{1,0}$, $\mathcal{C}_{4,15}^{1,0}$, $\mathcal{C}_{7,26}^{1,0}$, $\mathcal{C}_{10,25}^{1,1}$, $\mathcal{C}_{18,37}^{1,1}$	$\mathcal{C}_{3,43}^{1,0}$, $\mathcal{C}_{9,16}^{1,0}$, $\mathcal{C}_{13,70}^{1,0}$, $\mathcal{C}_{26,70}^{1,0}$, $\mathcal{C}_{29,61}^{1,1}$ $\mathcal{C}_{48,68}^{1,1}$, $\mathcal{C}_{52,70}^{1,1}$
$\mathcal{C}_{a,b}^{1,1}$	$4.\langle(13)\rangle$			$\mathcal{C}_{0,7}^{1,1}$			$\mathcal{C}_{0,70}^{1,1}$
	$2.\langle(12)\rangle$		$\mathcal{C}_{1,4}^{1,0}$			$\mathcal{C}_{1,19}^{1,1}$	
	$2.\langle(123)\rangle$				$\mathcal{C}_{2,32}^{1,1}$		$\mathcal{C}_{3,126}^{1,1}$
	$2.(1)$						
$\mathcal{C}_{a,b}^{0,1}$	$8.\langle(23)\rangle$	$\mathcal{C}_{0,0}^{0,1}$	$\mathcal{C}_{0,0}^{0,1}$	$\mathcal{C}_{0,0}^{0,1}$	$\mathcal{C}_{0,0}^{0,1}$	$\mathcal{C}_{0,0}^{0,1}$	$\mathcal{C}_{0,0}^{0,1}$
	$4.\langle(13)\rangle$	$\mathcal{C}_{0,1}^{0,1}$	$\mathcal{C}_{0,1}^{0,1}$	$\mathcal{C}_{0,1}^{0,1}$	$\mathcal{C}_{0,1}^{0,1}$	$\mathcal{C}_{0,1}^{0,1}$	$\mathcal{C}_{0,1}^{0,1}$
	$4.\langle(13)\rangle$			$\mathcal{C}_{0,2}^{0,1}$			$\mathcal{C}_{0,5}^{0,1}$
	$4.(1)$				$\mathcal{C}_{0,2}^{0,1}$	$\mathcal{C}_{0,2}^{0,1}$, $\mathcal{C}_{0,3}^{0,1}$	$\mathcal{C}_{0,2}^{0,1}$, $\mathcal{C}_{0,3}^{0,1}$
	$2.S_3$	$\mathcal{C}_{1,1}^{0,1}$	$\mathcal{C}_{1,1}^{0,1}$	$\mathcal{C}_{1,1}^{0,1}$	$\mathcal{C}_{1,1}^{0,1}$	$\mathcal{C}_{1,1}^{0,1}$	$\mathcal{C}_{1,1}^{0,1}$
	$2.\langle(12)\rangle$			$\mathcal{C}_{1,2}^{0,1}$	$\mathcal{C}_{1,2}^{0,1}$, $\mathcal{C}_{1,3}^{0,1}$	$\mathcal{C}_{1,2}^{0,1}$, $\mathcal{C}_{1,3}^{0,1}$, $\mathcal{C}_{1,4}^{0,1}$, $\mathcal{C}_{1,5}^{0,1}$	$\mathcal{C}_{1,2}^{0,1}$, $\mathcal{C}_{1,3}^{0,1}$, $\mathcal{C}_{1,4}^{0,1}$, $\mathcal{C}_{1,5}^{0,1}$, $\mathcal{C}_{1,6}^{0,1}$
	$2.\langle(123)\rangle$				$\mathcal{C}_{2,3}^{1,1}$		$\mathcal{C}_{3,4}^{0,1}$
	$2.(1)$					$\mathcal{C}_{2,3}^{0,1}$, $\mathcal{C}_{2,4}^{0,1}$	$\mathcal{C}_{2,3}^{0,1}$, $\mathcal{C}_{2,4}^{0,1}$ $\mathcal{C}_{2,5}^{0,1}$
$\mathcal{C}_{a,b}^{0,2}$	$8.\langle(12)\rangle$	$\mathcal{C}_{0,0}^{0,2}$	$\mathcal{C}_{0,0}^{0,2}$	$\mathcal{C}_{0,0}^{0,2}$	$\mathcal{C}_{0,0}^{0,2}$	$\mathcal{C}_{0,0}^{0,2}$	$\mathcal{C}_{0,0}^{0,2}$
	$4.\langle(13)\rangle$	$\mathcal{C}_{1,0}^{0,2}$	$\mathcal{C}_{1,0}^{0,2}$	$\mathcal{C}_{1,0}^{0,2}$	$\mathcal{C}_{1,0}^{0,2}$	$\mathcal{C}_{1,0}^{0,2}$	$\mathcal{C}_{1,0}^{0,2}$
	$4.\langle(13)\rangle$			$\mathcal{C}_{2,0}^{0,2}$			$\mathcal{C}_{2,0}^{0,2}$
	$4.(1)$				$\mathcal{C}_{2,0}^{0,2}$	$\mathcal{C}_{2,0}^{0,2}$, $\mathcal{C}_{3,0}^{0,2}$	$\mathcal{C}_{2,0}^{0,2}$, $\mathcal{C}_{3,0}^{0,2}$
	$2.S_3$	$\mathcal{C}_{1,1}^{0,2}$	$\mathcal{C}_{1,1}^{0,2}$	$\mathcal{C}_{1,1}^{0,2}$	$\mathcal{C}_{1,1}^{0,2}$	$\mathcal{C}_{1,1}^{0,2}$	$\mathcal{C}_{1,1}^{0,2}$
	$2.\langle(13)\rangle$			$\mathcal{C}_{1,2}^{0,2}$	$\mathcal{C}_{1,2}^{0,2}$, $\mathcal{C}_{1,3}^{0,2}$	$\mathcal{C}_{1,2}^{0,2}$, $\mathcal{C}_{1,3}^{0,2}$, $\mathcal{C}_{1,4}^{0,2}$, $\mathcal{C}_{1,5}^{0,2}$	$\mathcal{C}_{1,2}^{0,2}$, $\mathcal{C}_{1,3}^{0,2}$, $\mathcal{C}_{1,4}^{0,2}$, $\mathcal{C}_{1,5}^{0,2}$, $\mathcal{C}_{1,6}^{0,2}$
	$2.\langle(123)\rangle$				$\mathcal{C}_{2,3}^{0,2}$		$\mathcal{C}_{3,4}^{0,2}$
	$2.(1)$					$\mathcal{C}_{2,3}^{0,2}$, $\mathcal{C}_{2,4}^{0,2}$	$\mathcal{C}_{2,3}^{0,2}$, $\mathcal{C}_{2,4}^{0,2}$ $\mathcal{C}_{2,5}^{0,2}$

References

[1] R.A.L. Betty and A. Munemasa, *Mass formula for self-orthogonal codes over* $\mathbb{Z}_{p^2}$, Journal of combinatorics, information & system sciences **34** (2009), 51–66.

[2] W. Cary Huffman and Vera Pless, *Fundamentals of error correcting codes*, Cambridge University Pless, New York, 2003.

[3] W. Choi and Y.H. Park, *Self-dual codes over* $\mathbb{Z}_{p^2}$ *of length 4*, preprint.

[4] J.H. Conway and N.J.A. Sloane, *Self-dual codes over the integers modulo 4*, J. Comin. Theory Ser. A. **62** (1993), 30–45.

[5] S.T. Dougherty, T.A. Gulliver, Y.H. Park, J.N.C. Wong, *Optimal linear codes oner* $\mathbb{Z}_m$, J. Korean. Math. Soc. **44** (2007), 1136–1162.

[6] Y. Lee and J. Kim, *An efficient construction of self-dual codes*, CoRR, 2012.

[7] K. Nagata, F. Nemenzo and H. Wada, *Constructive algorithm of self-dual error-correcting codes*, 11th International Workshop on Algebraic and Combinatorial Coding Theory, 215–220, 2008.

[8] Y.H. Park, *The classification of self-dual modular codes*, Finite Fields and Their Applications **17** (5) (2011), 442–460.

[9] V.S. Pless, *The number of isotropic subspace in a finite geometry*, Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei **39** (1965), 418–421.

[10] V.S. Pless, *On the uniqueness of the Golay codes*, J. Combin. Theory **5** (1968), 215–228.

Whan-hyuk Choi
Department of Mathematics
Kangwon National University
Chuncheon 200-701, Korea
E-mail: whanhyuk@gmail.com

Kwang Ho Kim
Department of Mathematics
Kangwon National University
Chuncheon 200-701, Korea
E-mail: prime229@gmail.com

Sook Young Park
Department of Mathematics
Kangwon National University
Chuncheon 200-701, Korea
E-mail: erestugypsy@gmail.com