Bull. Korean Math. Soc. **55** (2018), No. 5, pp. 1371–1387
https://doi.org/10.4134/BKMS.b170791
pISSN: 1015-8634 / eISSN: 2234-3016

THE CLASSIFICATION OF SELF-DUAL CODES OVER GALOIS RINGS OF LENGTH 4

Whan-Hyuk Choi

Abstract. The classification of the self-dual codes over Galois rings $GR(p,2)$ and $GR(p^2,2)$ of length 4 is completed for all primes p up to equivalence in terms of automorphism group. We obtain all inequivalent classes and the number of each classes of self-dual codes for all primes.

1. Introduction

The first error correcting codes was discovered over the finite field $GF(2)$ by R. Hamming [6]. Since some authors proved that some good non-linear codes are closely related to linear codes over the ring $\mathbb{Z}_4$ in [7], mathematicians have particular interests in studying codes over various rings [3, 4, 10, 16]. Recently many papers are published about codes over finite chain rings which have good properties in some aspects. Every finite chain ring is a homomorphic image of some polynomial ring over a Galois ring [14]. This is one of the motivations we investigate codes over Galois rings.

On the other hand, self-dual codes are one of the most important classes in coding theory which give many 'best codes'. In particular, construction method of self-dual codes over Galois rings are discussed in [10]. It is already known that self-dual codes of length 4 over $GR(p^e,r)$ exist for all prime p and integers n and r [3]. Self-dual codes of length 4 play an important role to construct a self-dual code of moderate length n [8, 11].

Self-dual codes over the finite field $\mathbb{Z}_p = GR(p,1)$ of length 4 are classified in [17]. In this paper, we expand the result up to the ring $GR(p^2,2)$ and investigate self-dual codes of free rank 1 which do not appear in [17]. We classify the self-dual codes of length 4 over Galois rings $GR(p,2)$ and $GR(p^2,2)$ for all primes p up to equivalence in terms of their automorphism groups. We classify all inequivalent classes of self-dual codes of length 4 and obtain the necessary and sufficient conditions for the existence of each class. We also obtain the number of inequivalent classes for all primes.

Received September 12, 2017; Revised November 10, 2017; Accepted March 5, 2018.
2010 *Mathematics Subject Classification.* 94B05.
Key words and phrases. self-dual codes, classification, Galois ring, mass formula.

This paper is organized as follows. Firstly, we introduce some preliminaries to understand self-dual codes over Galois rings in Section 2. We investigate self-dual codes over Galois rings in Section 3 and mass formulas in Section 4. Our main results are given in Sections 5 and 6. Also, we present a concrete classification of self-dual codes for small primes.

All computations in this paper were done with the computer algebra system MAGMA and SAGEMATH.

2. Preliminaries

For a positive integer e and a prime number p, let $\mathbb{Z}_{p^e}$ be a ring of integers modulo p^e, $f(X)$ a polynomial in $\mathbb{Z}_{p^e}[X]$ and $\overline{f(X)}$ a natural projection of $f(X)$ over $\mathbb{Z}_p[X]$. A polynomial $f(X)$ is called *monic basic irreducible* if $f(X)$ is monic irreducible in $\mathbb{Z}_{p^e}[X]$ and $\overline{f(X)}$ is also irreducible in $\mathbb{Z}_p[X]$. If $f(X)$ is a monic basic irreducible polynomial of degree r, then the ring $\mathbb{Z}_{p^e}[X]/(f)$ is called the *Galois ring of characteristic* p^e *and degree* r and denoted by $GR(p^e, r)$. $GR(p^e, r)$ is the Galois extension of degree r over $\mathbb{Z}_{p^e}$ with the residue field $\mathbb{F}_{p^r}$ and the extensions are unique up to isomorphism. $GR(p^e, r)$ is a finite chain ring with ideals of the form $\langle p^i \rangle$ for $0 \leq i \leq e-1$ and also a local ring with the maximal ideal $\langle p \rangle$.

There exists a nonzero element ξ of order $p^r - 1$ in $GR(p^e, r)$, which is a root of a monic basic primitive polynomial $h(X)$ of degree r over $\mathbb{Z}_{p^e}$ and dividing $X^{p^r-1} - 1$ in $\mathbb{Z}_{p^e}[X]$ and

$$GR(p^e, r) = \mathbb{Z}_{p^e}[\xi] = \{a_0 + a_1\xi + \cdots + a_{r-1}\xi^{r-1} \,|\, a_i \in \mathbb{Z}_{p^e}\}.$$

On the other hand, any element $c \in GR(p^e, r)$ can be written uniquely in the p-adic representation, as

$$c = c_0 + c_1 p + c_2 p^2 + \cdots + c_{e-1}p^{e-1},$$

where $\mathcal{T} = \{0, 1, \xi, \ldots, \xi^{p^r-2}\}$ is the *Teichmüller set* and $c_i \in \mathcal{T}$.

We define the map π as the canonical projection,

$$\pi : \mathbb{Z}_{p^e}[X]/\langle f(X)\rangle \to \mathbb{Z}_p[X]/\langle \overline{p(x)}\rangle \simeq \mathbb{F}_{p^r}.$$

For any element $x = c_0 + c_1 p + c_2 p^2 + \cdots + c_{e-1}p^{e-1} \in GR(p^e, r)$, $\pi(x) = c_0$ and x is a unit in $GR(p^e, r)$ if and only if $\pi(x) \neq 0$.

For the further study of Galois rings and their representations, see [5,14,19].

A *linear code* $\mathcal{C}$ *of length* n *over a ring* R is a R-submodule of R^n. An element of $\mathcal{C}$ is called a *codeword*. A matrix whose row vectors generate the complete codewords is called a *generator matrix*.

We assume that every code is a linear code over $GR(p^e, r)$ throughout this paper and p is assumed odd unless otherwise noted.

$GR(p^e, r)^n$ is equipped with the standard inner product by $\mathbf{x}\cdot\mathbf{y} = \sum_{i=1}^{n} x_i y_i$, where $\mathbf{x} = (x_i), \mathbf{y} = (y_i)$ are vectors in $GR(p^e, r)^n$.

A linear code $\mathcal{C}$ of length n over $GR(p^e,r)$ has a generator matrix permutation equivalent to the *standard form*

$$G = \begin{pmatrix} I_{k_0} & A_{01} & A_{02} & A_{03} & \cdots & A_{0,e-1} & A_{0e} \\ 0 & pI_{k_1} & pA_{12} & pA_{13} & \cdots & pA_{1,e-1} & pA_{1e} \\ 0 & 0 & p^2I_{k_2} & p^2A_{23} & \cdots & p^2A_{2,e-1} & p^2A_{2e} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & p^{e-1}I_{k_{e-1}} & p^{e-1}A_{e-1,e} \end{pmatrix} \tag{1}$$

where the columns are grouped into blocks of size $k_0, k_1, \ldots, k_e$ such that k_i's are nonnegative integers adding to n.

A code with the generator matrix in this standard form is said to be *of type* $(1)^{k_0}(p)^{k_1}(p^2)^{k_2}\cdots(p^{e-1})^{k_{e-1}}$. $\sum_{i=0}^{e-1} k_i$ is called the *rank* and k_0 is called the *free rank*. A code of type 1^{k_0} is called a *free code*.

Note that a code over $GR(p^e,r)$ with type $(1)^{k_0}(p)^{k_1}(p^2)^{k_2}\cdots(p^{e-1})^{k_{e-1}}$ has $(p^{er})^{k_0}(p^{(e-1)r})^{k_1}(p^{(e-2)r})^{k_2}\cdots(p^r)^{k_{e-1}}$ codewords.

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

$$\mathcal{C}^\perp = \{\mathbf{v} \in GR(p^e,r)^n \mid \mathbf{v}\cdot\mathbf{w} = 0 \text{ for all } \mathbf{w} \in C\}.$$

A code $\mathcal{C}$ is called *self-orthogonal* if $\mathcal{C} \subset \mathcal{C}^\perp$ and *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$.

It is well-known that if $\mathcal{C}$ has type $1^{k_0}(p)^{k_1}\cdots(p^{e-1})^{k_{e-1}}$, then the type of the dual code is $1^{k_e}p^{k_{e-1}}(p^2)^{k_{e-2}}\cdots(p^{e-1})^{k_1}$, where $k_e = n - \sum_{i=0}^{e-1} k_i$. Following propositions are trivial.

Proposition 2.1. *For any code $\mathcal{C}$ of length n over $GR(p^e,r)$*

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

Proposition 2.2. *If $\mathcal{C}$ is a self-orthogonal code of length n and $|\mathcal{C}| = p^{ern/2}$, then $\mathcal{C}$ is self-dual.*

For the further study of linear codes over Galois rings, we refer [3,15].

In [17], the equivalence of self-dual codes are introduced. We review them briefly and use the same terminology as in [17]. Let S_n be a group of permutation matrices of length n and $\mathbb{D}^n$ a set of $n\times n$ diagonal matrices over $GR(p^e,r)$ with the diagonal elements γ_k's such that $\gamma_k^2 = 1$ for $1 \le k \le n$.

Then we define $\mathbb{T}^n$ as the group of all *monomial transformations* on $GR(p^e,r)^n$ by

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

Let $\mathscr{S}^n$ be the set of all distinct self-dual codes of length n over $GR(p^e,r)$. The cardinality of $\mathscr{S}^n$ will be denoted by $N_{p^e,r}(n)$. The group $\mathbb{T}^n$ acts on $\mathscr{S}^n$ by $\mathcal{C}\tau = \{c\tau \mid c \in \mathcal{C}\}$ for each $\tau \in \mathbb{T}^n$. If there exists an element $\tau \in \mathbb{T}^n$ such that $\mathcal{C}\tau = \mathcal{C}'$ for $\mathcal{C}$ and $\mathcal{C}'$ in $\mathscr{S}^n$, then we denote $\mathcal{C} \sim \mathcal{C}'$ and they are called *equivalent*. The group of all automorphisms of $\mathcal{C}$ is denoted by $\mathrm{Aut}(\mathcal{C})$. We define the set of *permutation parts* of $\mathrm{Aut}(\mathcal{C})$ as $p(\mathcal{C}) = \{\sigma \mid \sigma\gamma \in \mathrm{Aut}(\mathcal{C})$ for some $\gamma \in \mathbb{D}^n\}$ and elements in $s(\mathcal{C}) = \mathrm{Aut}(\mathcal{C})\cap\mathbb{D}$ are called the *pure signs* of $\mathcal{C}$.

On classifying self-dual codes, permutation parts and pure signs of the automorphism group play a major role. Hence, we denote a self-dual code $\mathcal{C}$ with its automorphism by $\mathcal{C} : |s(\mathcal{C})|.p(\mathcal{C})$ or $G : |s(\mathcal{C})|.p(\mathcal{C})$ where G is a generator matrix of $\mathcal{C}$.

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*.

It is obvious that if $\mathcal{C} \simeq \mathcal{C}_1 \oplus \mathcal{C}_2$, then $\mathrm{Aut}(\mathcal{C}) \supseteq \mathrm{Aut}(\mathcal{C}_1) \oplus \mathrm{Aut}(\mathcal{C}_2)$ and $|s(\mathcal{C})| = 2 \times |s(\mathcal{C}_1)| \times |s(\mathcal{C}_2)|$ by the definition. For the direct sum of codes, see [9].

3. Self-dual codes over a Galois ring

Lemma 3.1. *For any positive integer n and k, there exists a self-dual code over $GR(p^{2k}, r)$ of length n with automorphism $2^n.S_n$.*

Proof. For any positive integer n, the matrix $p^k I_n$ generates a self-dual code of length n where I_n is the identity matrix of degree n. □

The following Theorem in [3] tells that there exists a self-dual code over $GR(p^e, r)$ of length 4 for any positive integer e and r.

Theorem 3.2 ([3]).

(i) *If there exists $c \in GR(p^e, r)$ such that $c^2 = -1$ in $GR(p^e, r)$, then there exist self-dual codes over $GR(p^e, r)$ for all even lengths.*

(ii) *If e is even, then there exist self-dual codes over $GR(p^e, r)$ for all lengths.*

(iii) *If e is odd and the residue field $GF(p^r)$ has characteristic* $1 \pmod 4$, *then there exist self-dual codes over $GR(p^e, r)$ for all even lengths.*

(iv) *If e is odd and the residue field $GF(p^r)$ has characteristic* $3 \pmod 4$, *then there exist self-dual codes over $GR(p^e, r)$ for all even lengths a multiple of* 4.

A self-dual code $\mathcal{C}$ over a finite field $\mathbb{F}_q$ has a generator matrix permutation equivalent to the *standard form*

$$G = \left(\begin{array}{c|c} I_{n/2} & A \end{array} \right), \tag{2}$$

where $AA^t = -I_{n/2}$, i.e., $A^{-1} = -A^t$. Therefore, when $n = 4$, a self-dual codes $\mathcal{C}$ over a finite field $\mathbb{F}_q$ has a generator matrix permutation equivalent to the standard form

$$\begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & -b & a \end{pmatrix},$$

where $a^2 + b^2 + 1 = 0$.

By (1), we know that a self-dual code $\mathcal{C}$ over $GR(p^2, r)$ has a generator matrix G in the standard form as

$$G = \begin{pmatrix} I_{k_0} & A_1 & B_1 + pB_2 \\ 0 & pI_{k_1} & pC_1 \end{pmatrix}.$$

The self-duality of $\mathcal{C}$ ensures that $\mathcal{C}$ has type of $1^{k_0}p^{k_1}$ where $k_1 = n - 2k_0$. We abuse the projection map π on $\mathcal{C}$ naturally to define the *residue codes*, $Res(\mathcal{C})$ as $\pi(\mathcal{C})$. There is also the *torsion code*, $Tor(\mathcal{C}) = \{y \in GR(p,r)^n \mid py \in \mathcal{C}\}$. Associated with the code $\mathcal{C}$, two codes $Res(\mathcal{C})$ and $Tor(\mathcal{C})$ have generator matrices respectively,

$$G_0 = \begin{pmatrix} I_{k_0} & A_1 & B_1 \end{pmatrix}, G_1 = \begin{pmatrix} I_{k_0} & A_1 & B_1 \\ 0 & I_{k_1} & C_1 \end{pmatrix}.$$

Theorem 3.3. *Let $\mathcal{C}$ be a self-dual code over $GR(p^2,r)$ of length n and type $1^{k_0}p^{k_1}$. Then $Res(\mathcal{C})$ is self-orthogonal and $Res(\mathcal{C})^\perp = Tor(\mathcal{C})$.*

Proof. It is trivial that $Res(\mathcal{C})$ is self-orthogonal by the definition. Recall that $Res(\mathcal{C})$ and $Tor(\mathcal{C})$ are codes in $GR(p,r) \simeq \mathbb{F}_{p^r}$ and $2k_0 + k_1 = n$. Let $\mathbf{u}_0 \in Res(\mathcal{C})$ and $\mathbf{w} \in Tor(\mathcal{C})$. Then there exist vectors $\mathbf{u}_1$ such that $\mathbf{u}_0 + p\mathbf{u}_1 \in \mathcal{C}$ and $p\mathbf{w} \in \mathcal{C}$. Again, by the self-duality of $\mathcal{C}$,

$$\begin{aligned} & (\mathbf{u}_0 + p\mathbf{u}_1) \cdot (p\mathbf{w}) \equiv 0 \pmod{p^2} \\ \Rightarrow\ & \mathbf{u}_0 \cdot (p\mathbf{w}) \equiv 0 \pmod{p^2} \\ \Rightarrow\ & p(\mathbf{u}_0 \cdot \mathbf{w}) \equiv 0 \pmod{p^2} \\ \Rightarrow\ & \mathbf{u}_0 \cdot \mathbf{w} \equiv 0 \pmod{p}. \end{aligned}$$

Therefore, $Res(\mathcal{C})^\perp \subset Tor(\mathcal{C})$. The fact that the rank of $Res(\mathcal{C})$ is k_0 and the rank of $Tor(\mathcal{C})$ is k_0+k_1 implies that $|Res(\mathcal{C})| \times |Tor(\mathcal{C})| = (p^r)^{k_0} \times (p^r)^{k_0+k_1} = (p^r)^{2k_0+k_1} = (p^r)^n = |\mathbb{F}_{p^r}^n|$. □

In particular, when $n = 4$, the standard generator matrix of a self-dual code over $GR(p^2, 2)$ is one of the following 3 types.

(i) Type of p^4 (Trivial code).

$$pI_4 : 16.S_4.$$

(ii) Type of 1^2 (Free codes).

$$\begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & -b & a \end{pmatrix},$$

where $a^2 + b^2 + 1 = 0$. We denote the matrix of this type by (a, b).

(iii) Type of 1^1p^2.

$$\begin{pmatrix} 1 & a & b & c \\ 0 & p & 0 & -\frac{a}{c}p \\ 0 & 0 & p & -\frac{b}{c}p \end{pmatrix} \simeq \begin{pmatrix} 1 & a & b & c \\ 0 & cp & 0 & -ap \\ 0 & 0 & cp & -bp \end{pmatrix},$$

where $a^2+b^2+c^2+1 = 0$.We denote the matrix of this type by (a, b, c).

Theorem 3.4. *A self-dual code C over $GR(p^2, r)$ of free rank 1 of length n has a generator matrix permutation equivalent to the standard form*;

$$\begin{pmatrix} 1 = a_1 & a_2 & a_3 & \cdots & a_{n-1} & a_n + pb_1 \\ 0 & p & 0 & \cdots & 0 & pb_2 \\ 0 & 0 & p & \cdots & 0 & pb_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & p & pb_{n-1} \end{pmatrix} \tag{3}$$

where a_i's, b_j's are in $\mathcal{T}$ and

(i) $a_n + pb_1$ *is a unit in* $GR(p^2, 2)$,
(ii) $b_k = -a_k a_n^{-1}$ *for* $k \geq 2$.

Proof. By the previous arguments, it is deduced that if $\mathcal{C}$ is self-dual and has the generator matrix in the form of (1) with $k_1 = 1$, then $k_2 = n - 2$ and $\mathcal{C}$ has the generator matrix of (3) where a_i's, b_j's are in $\mathcal{T}$. From the fact that $(1, a_2, a_3, \ldots, a_n)$ generates the self-orthogonal code $Res(\mathcal{C})$, $1 + \sum_{k=2}^{n} a_k^2 \equiv 0 \pmod{p}$. Therefore not all a_k's are zero for $k \geq 2$ and we can assume a_n is a unit under the permutation equivalence. $a_n + pb_1$ is a unit if and only if $\pi(a_n + pb_1) = a_n \neq 0$ and this proves (i). Self-duality of $\mathcal{C}$ clearly confirms (ii). □

Assume that a self-orthogonal code of rank 1 over $GR(p, r)$ is generated by the vector $(1, a_2, a_3, \ldots, a_n)$. Then the lifted self-dual code with generator matrix of (3) is determined uniquely by b_1. In the other words, by the self-orthogonality of the vector $(1, a_2, a_3, \ldots, a_n + pb_1)$, we can determine b_1 from the equation

$$2pa_n b_1 \equiv -\sum_{k=1}^{n} a_k^2 \pmod{p^2} \tag{4}$$

and b_i's for $2 \leq i \leq n-1$ are also determined uniquely by the previous theorem.

Corollary 3.5. *There is an one-to-one correspondence up to equivalence between the set of self-dual codes over $GR(p^2, r)$ of free rank 1 and the set of self-orthogonal codes over $GR(p, r)$ of rank 1.*

Theorem 3.6. *Let $\mathcal{C}$ be a self-dual code $GR(p^2, r)$ of free rank 1 and $Res(\mathcal{C})$ the residue code of $\mathcal{C}$. Then,* $\mathrm{Aut}(\mathcal{C}) = \mathrm{Aut}(Res(\mathcal{C}))$.

Proof. Recall that $Res(\mathcal{C}) = \pi(\mathcal{C})$ and assume $\tau \in \mathrm{Aut}(\mathcal{C})$. Then $\mathcal{C} = \mathcal{C}\tau$ and $\pi(\mathcal{C}) = \pi(\mathcal{C}\tau) = \pi(\mathcal{C})\tau$. Therefore, $\mathrm{Aut}(\mathcal{C}) \subset \mathrm{Aut}(Res(\mathcal{C}))$. Note that $Res(\mathcal{C})$ is a self-orthogonal codes of rank 1. By the previous corollary, there is the one to one map π^{-1} between the set of $Res(\mathcal{C})$ and set of $\mathcal{C}$ and for $\tau \in \mathrm{Aut}(Res(\mathcal{C}))$, it holds that $Res(\mathcal{C}) = Res(\mathcal{C})\tau$ and $\mathcal{C} = \pi^{-1}(Res(\mathcal{C})) = \pi^{-1}(Res(\mathcal{C})\tau) = \pi^{-1}(Res(\mathcal{C}))\tau = \mathcal{C}\tau$. Thus $\mathrm{Aut}(Res(\mathcal{C})) \subset \mathrm{Aut}(\mathcal{C})$. □

Theorem 3.7. *Let C be a code over $GR(p,r)$ of rank 1 of length 4 with generator matrix* $\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \end{pmatrix}$ *and* $(ij),(ijk)$ *be elements in* S_4 *and* $\omega \in GR(p,r)$ *such that* $\omega^6 = 1, \omega \neq \pm 1$.

(i) *If* $a_i^2 = a_j^2$, *then* $(ij) \in p(C)$.

(ii) *If* $(ij) \in p(C)$ *and* $a_i^2 \neq a_j^2$, *then* $a_i^2 = -a_j^2$ *and all the other elements except* a_i *and* a_j *are zero.*

(iii) *If* $(ijk) \in p(C)$ *and* $\langle (ijk),(ij) \rangle \not\subseteq p(C)$, *then* $a_j^2 = \omega^2 a_i^2$, $a_k^2 = \omega^4 a_i^2$ *and the other element except* a_i, a_j *and* a_k *is zero.*

(iv) *If the number of* a_i*'s which are zero is* m, *then* $|s(C)| = 2^{1+m}$.

Proof. (i) is trivial by the definition of $p(C)$.

Without loss of generality, assume that $(12) \in p(C)$. Then there exist $\gamma \in \mathbb{D}^4$ and a unit k which satisfy

$$\begin{pmatrix} a_2 & a_1 & a_3 & a_4 \end{pmatrix} \gamma = k \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \end{pmatrix}.$$

This implies that $a_2^2 = k^2 a_1^2$, $a_1^2 = k^2 a_2^2$ and $k^4 = 1$. $a_i^2 \neq a_j^2$ implies that $k^2 \neq 1$. Thus $k^2 = -1$ and $a_3^2 = -a_3^2$, $a_4^2 = -a_4^2$. This proves (ii). For (iii), without loss of generality, assume that $(123) \in p(C)$ and $(12) \notin p(C)$. Then, there exist again $\gamma \in \mathbb{D}^4$ and a unit k which satisfy

$$\begin{pmatrix} a_2 & a_3 & a_1 & a_4 \end{pmatrix} \gamma = k \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \end{pmatrix}.$$

If $a_4 \neq 0$, then $k^2 = 1$. This implies that $a_1^2 = a_2^2 = a_3^2$ and $(12) \in p(C)$ by (i) which is contradict to the assumption. Therefore $a_4 = 0$, $a_2^2 = k^2 a_1^2$, $a_3^2 = k^2 a_2^2$ and $a_1^2 = k^2 a_3^2$. This implies that $k^6 = 1$ and (iii) is proved. For (iv), by the definition of $s(C)$ we must compute the number of γ's, pure signs which satisfies

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \end{pmatrix} \gamma = \begin{pmatrix} \gamma_1 a_1 & \gamma_2 a_2 & \gamma_3 a_3 & \gamma_4 a_4 \end{pmatrix} = k \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \end{pmatrix}$$

for some k. Because p is not even, $\gamma_1 = \gamma_2 = \gamma_3 = \gamma_4 = k$ if all a_i's are not zero. So $|s(C)| = 2$ if all a_i's are not zero. If an $a_i = 0$, γ_i can be taken 1 or -1 freely and this proves (iv). □

4. Mass formula

The *classification problem* in coding theory is to find a representative from each equivalence class of a certain kind of codes. The main tool for classification problem is the *mass formula*.

Let $N(n)$ be a number of all self-dual codes of length n and s be a number of equivalent classes of self-dual codes. Then we can get the mass formula:

$$\sum_{j=1}^{s} \frac{|\mathbb{T}^n|}{|\mathrm{Aut}(\mathcal{C}_j)|} = N(n).$$

Therefore, the total number of codes and automorphism of each code is the master key for classification of self-dual codes.

Theorem 4.1 ([18]). *Let $\sigma_q(n,k)$ be the number of self-orthogonal codes of length n and dimension k over $GF(q)$, where $q = p^e$ for some prime p and an integer e. Then*

(i) *If n is odd,*

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

(ii) *If n is even, q even,*

$$\sigma_q(n,k) = \frac{(q^{n-k}-1)\prod_{i=1}^{k-1}(q^{n-2i}-1)}{\prod_{i=1}^{k}(q^i-1)} \quad (k \geq 2),$$

$$\sigma_q(n,1) = \frac{q^{n-1}-1}{q-1}.$$

(iii) *If n is even, q odd,*

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

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

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

Note that $\sigma_q(n,0) = 1$ for all n and q.

Theorem 4.2 ([1]). *The number of distinct self-dual codes over a Galois ring $GR(p^2,2)$ for odd prime p is given by*

$$N_{p^2,2}(n) = \sum_{0 \leq k \leq \lfloor n/2 \rfloor} \sigma_{p^2}(n,k)(p^2)^{k(k-1)/2}.$$

Now, we know the number $N_{p^e,r}(4)$ for self-dual codes over $GR(p^e,r)$ of length 4 for $1 \leq e, r \leq 2$ and we are ready to classify the codes using mass formula:

$$\sum_{j=1}^{s} \frac{2^4 \times 4!}{|\mathrm{Aut}(\mathcal{C}_j)|} = N_{p^e,r}(4).$$

The number of solutions of $x^2+y^2+1=0$ plays a role in the classification of self-dual codes of type 1^2. So we give the number of solutions from [13] without proof.

Lemma 4.3. *Let p be an odd prime and $\mathbb{F}_q$ be a finite field with $q = p^r$ elements. For nonzero $k \in \mathbb{F}_q$, the cardinality of the set*

$$S_k = \{(x,y) \in \mathbb{F}_q \mid x^2+y^2 = k\}$$

is given by

$$|S_k| = q - (-1)^{(q-1)/2} = \begin{cases} q-1, & \text{if } q \equiv 1 \pmod 4, \\ q+1, & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

In particular, if $k = 0$, *then* $|S_0| = 1$ *for* $q \equiv 3 \pmod 4$ *and* $|S_0| = 2q - 1$ *for* $q \equiv 1 \pmod 4$.

5. Self-dual codes over $GR(p, 2)$ of length 4

The number of self-dual codes of length 4 over $GR(p, 2)$ for odd prime p is given by

$$N_{p,2}(4) = 2(p^2 + 1).$$

When $p = 2$, we take the irreducible polynomial $f(X) = X^2 + X + 1$. Let ζ be a root of $f(X)$ and A_n the alternating subgroup of S_n. Then there exist two inequivalent self-dual codes with generator matrices

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} : \langle (13), (1234) \rangle$$

and

$$\begin{pmatrix} 1 & 0 & \zeta & 1+\zeta \\ 0 & 1 & 1+\zeta & \zeta \end{pmatrix} : A_4.$$

When $p = 3$, we take the irreducible polynomial $f(X) = X^2 + 2X + 2$. Let ζ be a root of $f(X)$. Then there exist two inequivalent self-dual codes with generator matrices

$$\begin{pmatrix} 1 & 0 & 1+\zeta & 0 \\ 0 & 1 & 0 & 1+\zeta \end{pmatrix} : 4.\langle (13), (1234) \rangle$$

and

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 2 & 1 \end{pmatrix} : 2.S_4.$$

Theorem 5.1. *Let* $p \neq 2, 3$ *and* A_4 *be the alternating subgroup of* S_4. *Then the self-dual code* $\mathcal{C}$ *with generator matrix*

$$\begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & -b & a \end{pmatrix}$$

over $GR(p, 2)$ *denoted by* (a, b) *is one of the following four classes of inequivalent codes*:

Class	(a, b)	$\mathrm{Aut}(\mathcal{C})$
(i)	$a^2 + 1 = 0,\ b = 0$	$4.\langle (13), (1234) \rangle$
(ii)	$a^6 = 1,\ a \neq \pm 1$	$2.A_4$
(iii)	$a = 1,\ b^2 + 2 = 0$	$2.\langle (13), (1234) \rangle$
(iv)	*else*	$2.\langle (12)(34), (13)(24) \rangle$

Codes from classes (i), (ii), (iii) *are unique up to equivalence if exist. Classes* (ii), (iii) *and* (iv) *are MDS codes. Moreover,*

(i) *Class* (i) *exist for* $GR(p,2)$ *for all prime* $p \neq 2$,
(ii) *Class* (ii) *and* (ii) *exist for* $GR(p,2)$ *for all prime* $p \neq 2,3$,
(iii) *Class* (iv) *exists for* $GR(p,2)$ *if and only if* $p \geq 7$.

Proof. $GR(p,2) \simeq \mathbb{F}_{p^2}$ and $\mathbb{F}_{p^2}^*$ is also a multiplicative cyclic group of order p^2-1. Thus (i), (ii) and (iii) are proved by the same argument of Theorem 4.5 in [17] with the fact that $p^2 \equiv 1 \pmod 4$ for all prime $p \neq 2$ and $p^2 \equiv 1 \pmod{24}$ for all prime $p \neq 2,3$. With the definition of equivalence, the conditions of a and b in classes (i), (ii) and (iii) ensure the uniqueness.

Class (i), (ii), (iii) and (iv) contributes 12, 16, 24 and 48 codes, respectively, by the mass formula of $|\mathbb{T}^4|/|\mathrm{Aut}(\mathcal{C})|$. For $p \geq 7$, $12+16+24 = 52 < 2(p^2+1)$ and a code of class (iv) exists. □

Theorem 5.2. *For each prime* $p \neq 2,3$*, there exist unique self-dual codes over* $GR(p,2)$ *of length* 4 *in each class* (i), (ii), (iii)*. For* $p \geq 7$*, the number of inequivalent codes of the class* (iv) *is*

$$\frac{p^2-25}{24}.$$

Proof. By the mass formula,

$$\sum_{j=1}^{s} \frac{2^4 4!}{|\mathrm{Aut}(\mathcal{C}_j)|} = N_{p,2}(4) = 2(p^2+1).$$

Let N_4 be the number of inequivalent codes of the class (iv). Because codes of class (i), (ii) and (iii) are unique, the mass formula is obtained as

$$12 + 16 + 24 + 48N_4 = 2(p^2+1).$$

Thus

$$N_4 = \frac{p^2-25}{24}.$$ □

In Table 1, we introduce all examples of self-dual codes over $GR(p,2)$ for $5 \leq p \leq 61$ and the number inequivalent codes of class (iv).

6. Self-dual codes over $GR(p^2,2)$ of length 4

Using the mass formula, we make the following computations.

$$\begin{aligned} N_{p^2,2}(4) &= \sigma_{p^2}(4,0)p^0 + \sigma_{p^2}(4,1)p^0 + \sigma_{p^2}(4,2)(p^2)^1 \\ &= 1 + (p^2+1)^2 + 2(p^2+1)p^2 \\ &= 3p^4 + 4p^2 + 2 \\ &= \sum_{\mathcal{C}} \frac{2^4 \times 4!}{|\mathrm{Aut}(\mathcal{C})|}. \end{aligned}$$

Recall that there are three types of self-dual codes over $GR(p^2,2)$ of length 4 as p^4, 1^2 and 1^1p^2.

TABLE 1. Self-dual codes of length 4 over $GR(p,2)$ $(5 \le p \le 61)$

p	(i)	(ii)	(iii)	(iv)
5	$(2,0)$	$(2\zeta+1,2\zeta+2)$	$(1,2\zeta+4)$	
7	$(\zeta+3,0)$	$(2,3)$	$(1,3\zeta+2)$	1 code
11	$(4\zeta+3,0)$	$(\zeta+3,\zeta+4)$	$(1,3)$	4 codes
13	$(5,0)$	$(3,4)$	$(1,4\zeta+11)$	6 codes
17	$(4,0)$	$(5\zeta+14,5\zeta+15)$	$(1,7)$	11 codes
19	$(5\zeta+7,0)$	$(7,8)$	$(1,6)$	14 codes
23	$(11\zeta+12,0)$	$(4\zeta+7,4\zeta+8)$	$(1,9\zeta+14)$	21 codes
29	$(12,0)$	$(14\zeta+8,14\zeta+9)$	$(1,7\zeta+26)$	34 codes
31	$(4\zeta+27,0)$	$(5,6)$	$(1,\zeta+30)$	39 codes
37	$(6,0)$	$(10,11)$	$(1,6\zeta+25)$	56 codes
41	$(9,0)$	$(19\zeta+12,19\zeta+13)$	$(1,11)$	69 codes
43	$(4\zeta+41,0)$	$(6,7)$	$(1,16)$	76 codes
47	$(23\zeta+24,0)$	$(3\zeta+20,3\zeta+21)$	$(1,20\zeta+27)$	91 codes
53	$(23,0)$	$(24\zeta+31,24\zeta+32)$	$(1,23\zeta+7)$	116 codes
59	$(3\zeta+28,0)$	$(13\zeta+52,13\zeta+53)$	$(1,23)$	144 codes
61	$(11,0)$	$(13,14)$	$(1,6\zeta+58)$	154 codes

Three terms of $N_{p^2}(4)$ in the mass formula show the number of distinct codes of each 3 types;

$$\sigma_p(4,0)p^0 = 1$$

is the number of the self-dual code pI_4 of type p^4 which is the unique trivial code.

$$\sigma_p(4,1)p^0 = (p^2+1)^2$$

is the number of the self-dual codes of type 1^1p^2 and

$$\sigma_p(4,2)p^0 = 2(p^2+1)p^2$$

is the number of the self-dual free codes of type 1^2.

We need the Hensel's Lemma to see the relations between self-dual codes over $GR(p^2,2)$ and self-dual codes over $GR(p,2)$. For the further study of Hensel's Lemma, we refer [12].

Lemma 6.1 (Hensel's Lemma for $\mathbb{Z}_{p^e}$)**.** *Let $F(X) \in \mathbb{Z}_{p^{s+1}}[X]$ where s is a natural number. Suppose that there exists an $\alpha_1 \in \mathbb{Z}_{p^s}$ such that*

$$F(\alpha_1) \equiv 0 \pmod{p^s}, \quad F'(\alpha_1) \not\equiv 0 \pmod{p}.$$

Then there exists a unique $\alpha \in \mathbb{Z}_{p^{s+1}}$ such that $\alpha \equiv \alpha_1 \pmod{p^s}$ and $F(\alpha) = 0$.

6.1. Self-dual codes over $GR(p^2, 2)$ of type 1^2p^0

Theorem 6.2. *Let $p \neq 2, 3$ and A_4 be the alternating subgroup of S_4. Then the self-dual code $\mathcal{C}$ with generator matrix*

$$\begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & -b & a \end{pmatrix}$$

over $GR(p^2, 2)$ denoted by (a, b) is one of the following four classes of inequivalent codes:

Class	(a, b)	$\mathrm{Aut}((a, b))$
(i)	$a^2 + 1 = 0,\ b = 0$	$4.\langle(13), (1234)\rangle$
(ii)	$a^6 = 1,\ a \neq \pm 1$	$2.A_4$
(iii)	$a = 1,\ b^2 + 2 = 0$	$2.\langle(13), (1234)\rangle$
(iv)	*else*	$2.\langle(12)(34), (13)(24)\rangle$

Codes from classes (i), (ii) and (iii) *uniquely exist for $p \geq 5$, up to equivalence and codes from classes* (ii), (iii) *and* (iv) *are MDS codes.*

Proof. This theorem is directly deduced by Hensel's Lemma and Theorem 5.1. □

For the case of $p = 2$, there are 2 codes over $GR(4, 2)$ of type 1^2p^0,

$$(\zeta, \zeta + 1) : 2.A_4 \text{ and } (\zeta, \zeta + 3) : 2.\langle(12)(34), (13)(24)\rangle.$$

For the case of $p = 3$, there are 5 codes over $GR(9, 2)$ of type 1^2p^0,

$$(1 + \zeta, 0) \text{ of class (i) and } (1, 4) \text{ of class (iii)},$$
$$(3\zeta, 1 + \zeta), (3, 1 + \zeta), (3\zeta + 1, 6\zeta + 4) \text{ of class (iv)}.$$

Theorem 6.3. *For $p \neq 2, 3$, there exist unique self-dual codes over $GR(p, 2)$ of length* 4 *in each class* (i), (ii), (iii). *The number of inequivalent codes of class* (iv) *is* $\frac{p^4+p^2-26}{24}$.

Proof. Recall that $\sigma_{p^2}(4, 2)p^2 = 2(p^2 + 1)p^2$. By the same argument with Theorem 5.2, the number of inequivalent codes of class (iv) is obtained by

$$\frac{2(p^2 + 1)p^2 - 12 - 16 - 24}{48}.$$ □

6.2. Self-dual codes over $GR(p^2, 2)$ of length 4 and type 1^1p^2

We will use the following notations for subgroups of S_4 for self-dual codes over $GR(p^2, 1)$ of type 1^1p^2:

$B_2 = \{(1), (12)(34)\}$,

$B_3 = \{(1), (124), (142)\}$,

$B_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$,

$B_4' = \{(1), (14), (23), (14)(23)\}$,

$B_4'' = \{(1), (12)(34), (1324), (1423)\}$,

TABLE 2. Self-dual codes of type 1^2 over $GR(p^2, 2)$ $(p < 29)$

p	(i)	(ii)	(iii)	(iv)
3	$(1+\zeta, 0)$		$(1, 4)$	3 codes
5	$(7, 0)$	$(6+22\zeta, 7+22\zeta)$	$(5\zeta, 7)$	26 codes
7	$(29\zeta+38, 0)$	$(30, 31)$	$(1, 45\zeta+37)$	101 codes
11	$(92\zeta+80, 0)$	$(89\zeta+69, 89\zeta+70)$	$(1, 19)$	614 codes
13	$(70, 0)$	$(146, 147)$	$(1, 43\zeta+89)$	1196 codes
17	$(38, 0)$	$(226\zeta+218, 226\zeta+219)$	$(1, 24)$	3491 codes
19	$(252\zeta+102, 0)$	$(68, 69)$	$(1, 63)$	5444 codes
23	$(34\zeta+357, 0)$	$(441\zeta+398, 441\zeta+399)$	$(1, 515\zeta+382)$	11681 codes

$$B_6 = \{(1), (12), (14), (24), (124), (142)\},$$
$$B_8 = \{(1), (1234), (12)(34), (13)(24), (1432), (13), (14)(23), (24)\},$$
$$B_8' = \{(1), (1324), (13)(24), (12)(34), (1423), (12), (14)(23), (34)\}.$$

Note that there exist two self-dual code over $GR(4, 2)$ of type 1^1p^2.

$$(1, 1, 1) : 8.S_4, (1, 1, 1+2\zeta) : 8.S_4,$$

and there exist four self-dual code over $GR(9, 2)$ of type 1^1p^2.

$$(1, 0, 4) : 4.B_6,$$
$$(0, 0, \zeta+1) : 8.B_4',$$
$$(1, \zeta+1, \zeta+1) : 2.B_8',$$
$$(\zeta, \zeta+1, \zeta+2) : 2.B_2.$$

The following theorem is analogous to Theorem 3.5 in [2],

Theorem 6.4. *Let* $p \neq 2, 3$. *Then self-dual codes* (a, b, c) *of rank* 3 *is equivalent to one of the following inequivalent codes*:

(i) *Suppose* $a = b = 0$. *Then*

$$(0, 0, c) : 8.B_4'.$$

(ii) *Suppose* $a^6 \equiv 1$, $b = 0$ *and* $a^2 \neq 1, c^2 \neq 1$. *Then*

$$(a, 0, c) : 4.B_3.$$

(iii) *Suppose* $a^2 = 1$ *and* $b = 0$. *Then*

$$(1, 0, c) : 4.S_2.$$

(iv) *Suppose* $a \neq 0, a^3 \neq \pm 1, b = 0, c^3 \neq \pm 1$ *and* $a^2 \neq c^2$. *Then*

$$(a, 0, c) : 4.(1).$$

(v) *Suppose* $a^2 \equiv 1$ *and* $b^2 \equiv c^2 \neq 1$. *Then*

$$(a, b, c) : 2.B_8'.$$

(vi) *Suppose* $a^2 \equiv b^2 \equiv 1$. *Then*

$$(a, b, c) : 2.S_3.$$

If $a^2 \equiv b^2 \equiv c^2$, *then the code* (a, b, c) *is equivalent to the one of the codes of this class.*

(vii) *Suppose* $a^2 \equiv 1, b^2 \neq \pm 1, c^2 \neq \pm 1$. *Then*

$$(a, b, c) : 2.S_2.$$

If $a^2 \equiv b^2 \neq \pm 1$ *or* $b^2 \equiv c^2 \neq \pm 1$ *or* $a^2 \equiv c^2 \neq \pm 1$, *the code* (a, b, c) *is equivalent to the one of the codes of this class.*

(viii) *Suppose* $a^2 \equiv -1, b^2 \neq \pm 1$ *and* $b^4 \neq -1$. *Then*

$$(a, b, c) : 2.B_2.$$

(ix) *Suppose* $a^2 \equiv -1$ *and* $b^2 \neq \pm 1$ *and* $b^4 \equiv -1$. *Then*

$$(a, b, c) : 2.B_4''.$$

(x) *Suppose* $abc \neq 0, a^2, b^2, c^2 \neq \pm 1$ *and* a^2, b^2, c^2 *are all distinct. Then*

$$(a, b, c) : 2.(1).$$

Proof. By Theorem 3.6 and Hensel's Lemma, we need to classify the self-orthogonal codes of rank 1 with generator matrix $(1, a, b, c)$ over $GR(p, 2)$.

Automorphisms of class (i), (ii), (iii) and (iv) are easily deduced from the Theorem 3.7.

Suppose $b \neq 0$. For $\tau = \sigma\gamma \in \mathbb{T}, \sigma \in S_4, k \in GR(p, 1)$,

$$(1, a, b, c)\sigma\gamma = k(1, a, b, c) \Longleftrightarrow (1, a^2, b^2, c^2)\sigma = k^2(1, a^2, b^2, c^2).$$

Thus $k^2 = 1, a^2, b^2, c^2$ and σ can be determined once we know the equalities among $1, a^2, b^2, c^2$.

For the class (v), Theorem 3.7 ensures that $(12), (34) \in \mathrm{Aut}(\mathcal{C})$ and $(13) \notin \mathrm{Aut}(\mathcal{C})$. Assume $a = 1$, then the generator matrix is $(1, 1, b, b)$ such that $b^2+1 = 0$. $\frac{1}{b}(b, b, 1, 1) = (1, 1, 1/b, 1/b)$ and for $\gamma = (1, 1, -1, -1)$, $(1, 1, 1/b, 1/b)\gamma = (1, 1, b, b)$. Thus $(14)(23) \in \mathrm{Aut}(\mathcal{C})$. Thus $\mathrm{Aut}(\mathcal{C}) = B_8'$.

The class (vi) case is easily proved by Theorem 3.7. If $a^2 = b^2 = c^2$, say $a = b = c$, then $\frac{1}{a}(1, a, a, a)(14) = (1, 1, 1, 1/a)$. Thus code (a, a, a) is equivalent to a code of $(1, 1, c)$.

Let $\pm i$ be the solutions of $x^2 + 1 = 0$ over $GR(p, 1)$.

For the class (viii) and (ix), $a^2 = -1$ and $b^2 \neq \pm 1$ implies that $c = bi$. Thus $(1, i, b, bi)$ generates the codes of class (vii) and (viii). For $\gamma = (-1, 1, -1, 1)$, $i(1, i, b, bi)(12)(34)\gamma = (1, i, b, bi)$ implies that $(12)(34) \in \mathrm{Aut}(\mathcal{C})$. Assume $b^2 = i$ and $\gamma = (1, 1, 1, -1)$, then we have

$$\begin{aligned}\frac{1}{b}(1, i, b, bi)(1324)\gamma &= \frac{1}{b}(b, bi, i, 1)\gamma = (1, i, \frac{i}{b}, \frac{1}{b})\gamma \\ &= (1, i, b, \frac{b}{i})\gamma = (1, i, b, -bi)\gamma = (1, i, b, bi).\end{aligned}$$

Thus if $b^2 = i$, then $(1324) \in \mathrm{Aut}(\mathcal{C})$ and this proves the case of class (vii) and (ix). The rest of cases are proved similarly. □

Theorem 6.5. *For $p \neq 2, 3$, let $N_1, N_2, \ldots, N_{10}$ be the number of class* (i), (ii), …, (x) *self-dual codes over $GR(p^2, 2)$, respectively. These numbers are determined as follows.*

N_1	N_2	N_3	N_4	N_5	N_6	N_7	N_8	N_9	N_{10}
1	1	1	$\frac{p-25}{24}$	1	1	$\frac{p^2-17}{8}$	$\frac{p^2-9}{8}$	1	$\frac{(p^2+1)^2-28p^2+216}{192}$

Proof. The number of codes of type 1^1p^2 is $\sigma_{p^2}(4,1) \times p^0 = (p^2+1)^2$ and among them $\sigma_{p^2}(3,1) \times p^0 = p^2 + 1$ codes are decomposable, classes from (i) to (iv). The number of codes in one orbit for each cases is 6,8,12,24, respectively. Thus,

$$N_4 = \frac{p^2 + 1 - 6 - 8 - 12}{24}.$$

For class (iii), (v), (vi) and (vii), we must compute the number of solutions of $b^2 + c^2 = k$. In Theorem 4.3, the number of solutions of $b^2 + c^2 = k$ over $\mathbb{F}_q$ is given by $q - 1$ for $q \equiv 1 \pmod 4$ and $q + 1$ for $q \equiv 3 \pmod 4$.

Each number of classes (iii), (v), (vi) and (vii) determined by using the number of solutions of $2 + b^2 + c^2 = 0$. For class (iii), $c^2 = 2$ has 4 solutions and for class (v), $b^2 = c^2 = -1$ has 4 solutions and for class (vi), $3 + c^2 = 0$ has 8 solutions. This means that following holds: $4N_3 + 4N_5 + 8N_6 + 8N_7 = q - 1$ for $q \equiv 3 \pmod 4$ $4N_3 + 4N_5 + 8N_6 + 8N_7 = q + 1$ for $q \equiv 3 \pmod 4$.

Note that $p^2 \equiv 1 \pmod 4$ for all odd prime p. Thus

$$N_7 = \frac{p^2 - 17}{8}.$$

Similarly, each number of inequivalent codes of class (i), (viii), (ix) is determined by the solutions of $b^2+c^2 = 0$ which is also given $2q-1$ for $q \equiv 1 \pmod 4$ and 0 for $q \equiv 3 \pmod 4$. For class (ix), there are $(\pm\alpha, \pm\alpha i)$ and $(\pm\alpha i, \pm\alpha)$ for $i^2 = -1$, totally 8 solutions. For class (viii), there are 16 solutions. So $16N_8 + 8N_9 = 2(q - 1) - 8$ for $q \equiv 1 \pmod 4$. Therefore,

$$N_8 = \frac{2(q-1) - 8 - 8N_9}{16}.$$

For N_{10}, we use the mass formula: $12N_1+32N_2+48N_3+96N_4+24N_5+32N_6+96N_7 + 96N_8 + 48N_9 + 192N_{10} = (p^2 + 1)^2$. Thus

$$N_{10} = \frac{(p^2 + 1)^2 - 28p^2 + 216}{192}.$$

□

Table 3. Class (i) to (iii) of self-dual codes of type 1^1p^2 over $GR(p^2,2)$

p^2	(i)	(ii)	(iii)
Aut(C)	$8.B_4'$	$4.B_3$	$4.S_2$
5^2	$(0,0,7)$	$(2\zeta+1,0,12\zeta+12)$	$(1,0,7\zeta+14)$
7^2	$(0,0,29\zeta+38)$	$(2,0,17)$	$(1,0,45\zeta+37)$
11^2	$(0,0,92\zeta+80)$	$(\zeta+3,0,12\zeta+37)$	$(1,0,102)$
13^2	$(0,0,70)$	$(3,0,43)$	$(1,0,43\zeta+89)$
17^2	$(0,0,38)$	$(5\zeta+14,0,175\zeta+253)$	$(1,0,24)$
19^2	$(0,0,252\zeta+102)$	$(7,0,46)$	$(1,0,63)$
23^2	$(0,0,34\zeta+357)$	$(4\zeta+7,0,4\zeta+77)$	$(1,0,515\zeta+382)$

Table 4. Class (v), (vi) and (ix) of self-dual codes of type 1^1p^2 over $GR(p^2,2)$

p^2	(v)	(vi)	(ix)
Aut(C)	$2.B_8$	$2.S_3$	$2.B_4''$
5^2	$(1,2,12)$	$(1,1,6\zeta+12)$	$(2,\zeta+2,2\zeta+4)$
7^2	$(1,\zeta+3,8\zeta+24)$	$(1,1,37)$	$(\zeta+3,2\zeta+1,9\zeta+39)$
11^2	$(1,4\zeta+3,59\zeta+36)$	$(1,1,57\zeta+18)$	$(4\zeta+3,5\zeta+5,5\zeta+63)$
13^2	$(1,5,135)$	$(1,1,45)$	$(5,\zeta+6,57\zeta+4)$
17^2	$(1,4,72)$	$(1,1,126\zeta+141)$	$(2,4,93)$
19^2	$(1,5\zeta+7,138\zeta+197)$	$(1,1,137)$	$(4\zeta+1,4\zeta+14,195\zeta+140)$
23^2	$(1,11\zeta+12,57\zeta+173)$	$(1,1,353\zeta+268)$	$(7\zeta+2,7\zeta+7,494\zeta+81)$

7. Conclusion

In this paper, we classified the self-dual codes of length 4 over Galois rings $GR(p,2)$ and $GR(p^2,2)$ for all primes p up to equivalence and presented examples of self-dual codes for small primes. Subsequently, we are to classify the self-dual codes of length 8 for there exist self-dual codes over $GR(p^e,r)$ of a length of a multiple of 4 for any e, r and prime p. However, there are too many self-dual codes of length 8 to classify which are beyond the limit of computational approach. Even, there is no optimized algorithm for equivalence test between codes over $GR(p^e,r)$ for a large e or r. Some algorithms of constructing self-dual codes of longer length from a smaller one are presented in [8, 10, 11] and we expect that the results in this paper would be a cornerstone to classify the self-dual codes of length 8 in the future.

References

[1] W.-H. Choi, *Mass formula of self-dual codes over Galois rings $GR(p^2,2)$*, Korean J. Math. **24** (2016), no. 4, 751–764.

[2] W.-H. Choi and Y. H. Park, *Self-dual codes over $\mathbb{Z}_{p^2}$ of small lengths*, Korean J. Math. **25** (2017), no. 3, 379–388.

[3] S. T. Dougherty, J.-L. Kim, and H. Liu, *Constructions of self-dual codes over finite commutative chain rings*, Int. J. Inf. Coding Theory **1** (2010), no. 2, 171–190.
[4] S. T. Dougherty and Y. H. Park, *Codes over the p-adic integers*, Des. Codes Cryptogr. **39** (2006), no. 1, 65–80.
[5] F. Q. Gouvêa, *p-Adic Numbers*, second edition, Universitext, Springer-Verlag, Berlin, 1997.
[6] R. W. Hamming, *Error detecting and error correcting codes*, Bell System Tech. J. **29** (1950), 147–160.
[7] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The* $\mathbf{Z}_4$*-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), no. 2, 301–319.
[8] S. Han, J.-L. Kim, H. Lee, and Y. Lee, *Construction of quasi-cyclic self-dual codes*, Finite Fields Appl. **18** (2012), no. 3, 613–633.
[9] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.
[10] J.-L. Kim and Y. Lee, *Construction of MDS self-dual codes over Galois rings*, Des. Codes Cryptogr. **45** (2007), no. 2, 247–258.
[11] ———, *An efficient construction of self-dual codes*, Bull. Korean Math. Soc. **52** (2015), no. 3, 915–923.
[12] S. Lang, *Algebraic Number Theory*, second edition, Graduate Texts in Mathematics, **110**, Springer-Verlag, New York, 1994.
[13] R. Lidl and H. Niederreiter, *Finite Fields*, second edition, Encyclopedia of Mathematics and its Applications, **20**, Cambridge University Press, Cambridge, 1997.
[14] B. R. McDonald, *Finite Rings with Identity*, Marcel Dekker, Inc., New York, 1974.
[15] G. H. Norton and A. Salagean, *On the Hamming distance of linear codes over a finite chain ring*, IEEE Trans. Inform. Theory **46** (2000), no. 3, 1060–1067.
[16] ———, *On the structure of linear and cyclic codes over a finite chain ring*, Appl. Algebra Engrg. Comm. Comput. **10** (2000), no. 6, 489–506.
[17] Y. H. Park, *The classification of self-dual modular codes*, Finite Fields Appl. **17** (2011), no. 5, 442–460.
[18] V. Pless, *The number of isotropic subspaces in a finite geometry*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **39** (1965), 418–421.
[19] Z.-X. Wan, *Finite Fields and Galois Rings*, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2012.

Whan-Hyuk Choi
Department of Mathematics
Kangwon National University
Chuncheon 24341, Korea
Email address: whanhyuk@gmail.com