Korean J. Math. **24** (2016), No. 4, pp. 751–764
https://doi.org/10.11568/kjm.2016.24.4.751

MASS FORMULA OF SELF-DUAL CODES OVER GALOIS RINGS $GR(p^2, 2)$

Whan-hyuk Choi

Abstract. We investigate the self-dual codes over Galois rings and determine the mass formula for self-dual codes over Galois rings $GR(p^2, 2)$.

1. Introduction

As an application of computer science, error correcting codes were firstly defined over GF(2) by Hamming in 1950. Sooner or later mathematicians extended them over arbitrary fields. In [6], Hammons et al. found that some good non-linear codes are obtained from codes over a ring $\mathbb{Z}_4$ via Gray map. More recently, many papers are published about codes over $\mathbb{Z}_m$ for an arbitrary integer m.

On the other hands, many important codes such as Golay code and extended Hamming code are self-dual codes. In 1996, Gaborit calculated the mass formulas for self-dual codes over $\mathbb{Z}_4$ in [4]. This paper motivated Nagata, et al. to find the mass formulas for self-dual codes over $\mathbb{Z}_{p^e}$ in consecutive papers, [1], [10], [11], [12].

And in [13], Park found a method to classify self-dual codes over $\mathbb{Z}_m$ where m is a multiple of distinct primes. To generalize the results in [13], we investigated the classification of self-dual codes over $\mathbb{Z}_{p^e}$ for

Received September 19, 2016. Revised December 20, 2016. Accepted December 26, 2016.
2010 Mathematics Subject Classification: 94B05.
Key words and phrases: codes over Galois ring, self-dual codes, mass formula.

any odd prime p. As a consquence we found the complete classfication of self-orthogonal codes over $\mathbb{Z}_{p^2}$ in small lengths in [3].

It is well-known that the codes over finite chain rings have some good properties. Actually, $\mathbb{Z}_{p^e}$ over which we have investigated the classification of self-dual codes is a Galois ring and every finite chain ring is a homomorphic image of some polynomial ring over a Galois ring. Therefore investigating codes over Galois rings would be necessary to study codes over finite rings.

In this paper, we use the similar argument of Gaborit in [4] and Balmaceda et al. in [1], to generalize the result to the self-dual codes over Galois ring $GR(p^2, 2)$ for odd prime p.

2. Galois rings

Let r be a positive integer and $p(X)$ be a monic basic irreducible polynomial in $\mathbb{Z}_{p^e}[X]$ of degree r that divides $X^{p^r-1} - 1$. We can choose $p(X)$ so that $\zeta = X + \langle p(X) \rangle$ is a primitive $(p^r - 1)$st root of unity. Then, *Galois ring* is defined as

$$GR(p^e, r) = \mathbb{Z}_{p^e}[X]/\langle p(X) \rangle \simeq \mathbb{Z}_{p^e}[\zeta].$$

$GR(p^e, r)$ which is the generalization of Galois field, is the Galois extension of degree r over $\mathbb{Z}_{p^e}$ with the residue field $\mathbb{F}_{p^r}$ and is a finite chain rings with ideals of the form $\langle p^i \rangle$ for $0 \leq i \leq e-1$. The extensions are unique up to isomorphism.

The set $T_r = \{0, 1, \zeta, \ldots, \zeta^{p^r-2}\}$ of coset representatives of $GR(p^e, r)$ modulo $\langle p \rangle$ is a complete set and known as Teichmüller set. The elements of $GR(p^e, r)$ can be uniquely written as the p-adic representation,

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

with $c_i \in T_r$.

The other way of representation of Galois ring is the ζ-adic expansion,

$$b_0 + b_1 \zeta + \cdots + b_{r-1} \zeta^{r-1}$$

with $b_i \in \mathbb{Z}_{p^e}$.

For the further study of Galois rings, see [5, 9, 16].

3. Codes over Galois ring

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

$$(1)\qquad G = \begin{pmatrix} I_{k_0} & A_{01} & A_{02} & A_{03} & \dots & A_{0,e-1} & A_{0e} \\ 0 & pI_{k_1} & pA_{12} & pA_{13} & \dots & pA_{1,e-1} & pA_{1e} \\ 0 & 0 & p^2 I_{k_2} & p^2 A_{23} & \dots & p^2 A_{2,e-1} & p^2 A_{2e} \\ \cdot & \cdot & \cdot & \cdot & \dots & \cdot & \cdot \\ 0 & 0 & 0 & 0 & \dots & p^{e-1} I_{k_{e-1}} & p^{e-1} A_{e-1,e} \end{pmatrix},$$

where the columns are grouped into blocks of sizes $k_0, k_1, \dots, k_{e-1}, k_e$ which are nonnegative integers adding to n [7].

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

Note that a code 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.

We can define the standard inner product over the space $GR(p^e, m)^n$ by

$$(v_1, \cdots, v_n)\cdot(w_1, \cdots, w_n) = v_1 w_1 + \cdots + v_n w_n$$

and the dual code $\mathscr{C}^\perp$ of $\mathscr{C}$ by

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

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

If $\mathscr{C}$ is a code of the form (1) then $\mathscr{C}^\perp$ has a generator matrix of the form

$$G^\perp = \begin{pmatrix} B_{0e} & B_{0,e-1} & \cdots & B_{03} & B_{02} & B_{01} & I_{k_e} \\ pB_{1e} & pB_{1,e-1} & \cdots & pB_{13} & pB_{12} & pI_{k_{e-1}} & 0 \\ p^2 B_{2e} & p^2 B_{2,e-1} & \cdots & p^2 B_{23} & p^e I_{k_{e-2}} & 0 & 0 \\ \cdot & \cdot & \cdots & \cdot & \cdot & \cdot & \cdot \\ p^{e-1} B_{e-1,e} & p^{e-1} I_{k_1} & \cdots & 0 & 0 & 0 & 0 \end{pmatrix}$$

where the column blocks have the same size as in G [2].

Note that if $\mathscr{C}$ has type $1^{k_0}(p)^{k_1}\cdots(p^{e-1})^{k_{e-1}}$ then the dual code has type $1^{k_e} p^{k_{e-1}}(p^2)^{k_{e-2}}\cdots(p^{e-1})^{k_1}$, where $k_e = n - \sum_{i=0}^{e-1} k_i$. This means that if $\mathscr{C}$ is self-dual with the type $(1)^{k_0}(p)^{k_1}(p^2)^{k_2}\cdots(p^{e-1})^{k_{e-1}}$, then $k_i = k_{e-i}$ for all i.

For any code $\mathscr{C}$ of length n over $GR(p^e, r)$

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

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

4. Codes over $GR(p^2, 2)$

From now on, we denote $GR(p^e, 2)$ as R_e.

Recall that an element in R_e can be written as $a+b\zeta$ where $a, b \in \mathbb{Z}_{p^e}$. We use the following three maps for the computation in $GR(p^2, 2)$. One is the natural projection modulo p, $\pi_e : R_e \to R_1$, and the other two non homomorphism maps $\psi_1 : R_e \to \mathbb{Z}_{p^e}$ and $\psi_2 : R_e \to \mathbb{Z}_{p^e}$ defined as $\psi_1(a+b\zeta) = a$ and $\psi_2(a+b\zeta) = b$. We can easily abuse these three maps on the vectors in R_e^n componentwisely.

And let $g_e : \mathbb{Z}_{p^e}^n \to \mathbb{Z}^n$ and $h_e : R_e^n \to R_{e+1}^n$ be two canonical injections componentwise.

Let γ_1 and γ_2 be the composition of $g_e \circ \psi_2$ and $g_e \circ \psi_2$, respectively. We also define the operation $\oplus_{p^e}$ on two vectors $x, y \in \mathbb{Z}^n$ as

$$x \bigoplus_{p^e} y := \left(\lfloor \frac{x+y}{p^e} \rfloor, \lfloor \frac{x+y}{p^e} \rfloor, \cdots, \lfloor \frac{x+y}{p^e} \rfloor \right).$$

One can easily see that

$$h_e(x+y) = h_e(x) + h_e(y) - p^e \left(\gamma_1(x) \bigoplus_{p^e} \gamma_1(y) + \left(\gamma_2(x) \bigoplus_{p^e} \gamma_2(y) \right) \zeta \right).$$

Let $\mathscr{C}$ be a code over R_e. For $0 \le i \le e-1$, we can define the ith *torsion code of* $\mathscr{C}$ as

$$Tor_i(\mathscr{C}) = \{\pi_e(v) \mid p^i v \in \mathscr{C}, v \in R_e^n\}.$$

$Tor_0(\mathscr{C}) = \pi_e(\mathscr{C})$ is usually called the *residue code* and denoted by $Res(\mathscr{C})$.

Especially for the code $\mathscr{C}$ over R_2, we will denote $Tor_1(\mathscr{C})$ as $\mathscr{C}_1$ and $Res(\mathscr{C})$ as $\mathscr{C}_0$ for the brevity.

A code $\mathscr{C}$ over R_2 with type $(1)^{k_0}(p)^{k_1}$ is equivalent to a code with generator matrix in the standard form:

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

where A_1, B_1, B_2 and C_1 are matrices over R_1.

If $\mathscr{C}$ has a generator matrix G then $\mathscr{C}_0$ and $\mathscr{C}_1$ have generator matrices

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

respectively, by the definition of $\mathscr{C}_0$ and $\mathscr{C}_1$. Note that $\mathscr{C}_0 \subset \mathscr{C}_1$ and $|\mathscr{C}| = (p^2)^{2k_0}(p^2)^{k_1}$.

We can define a non-homomorphism map $F : \mathscr{C}_0 \to R_1^n/\mathscr{C}_1$ defined by

$$F(x) = \{y \in R_1^n \mid x + py \in \mathscr{C}\}.$$

Then, $\mathscr{C} = \{x + py \mid x \in \mathscr{C}_0, y \in F(x)\}$. Note that

$$F(x+y) = F(x) + F(y) + \left(\gamma_1(x) \bigoplus_{p^e} \gamma_1(y) + \left(\gamma_2(x) \bigoplus_{p^e} \gamma_2(y)\right)\zeta \right).$$

The map F is determined by the matrix B_2 and vice versa. Therefore we can see that the set of codes over R_2 is in one-to-one correspondence with the set of triplets $(\mathscr{C}_0, \mathscr{C}_1, F)$.

5. Self-dual Codes over $GR(p^2, 2)$

From now on, we assume that p is an odd prime and note that a self-dual codes over R_2 of length n has the type of $1^{k_0}p^{k_1}$ such that $2k_0 + k_1 = n$

LEMMA 5.1. *For any positive integer n, there exists a self-dual code over R_2 of length n.*

Proof. The matrix pI_n generates a self-dual code of length n for any n where I_n is the nth identity matrix.

□

The following lemma is well-known.

LEMMA 5.2. *Let $\mathscr{C}$ be self-dual code over R_2. Then $\mathscr{C}_0$ is self-orthogonal and $\mathscr{C}_0^{\perp} = \mathscr{C}_1$*

According to previous argument, to construct self-dual codes over R_2 of length n with type $1^{k_0}p^{k_1}$, above all we find a self-orthogonal code over R_1 of length n and rank k_0. Then we obtain $\mathscr{C}_1$ as the dual code of $\mathscr{C}_0$.

Finally we must choose the map F which satisfies a certain condition for $\mathscr{C}$ to be a self-dual code.

Therefore, to count the number of self-dual codes over R_2, we must know the number of codes over $R_1 = \mathbb{F}_{p^2}$ and the number of distinct map F which satisfies the certain condition. We will investigate it by the same argument from [1] and [4] in the followings.

Let $\mathscr{C}$ be a self-dual codes over R_2 of length n has the type of $1^{k_0}p^{k_1}$ and $\{e_1, e_2, \dots e_{k_0}\}$ be the basis of $\mathscr{C}_0$. we can enlarge the basis to the basis $\{e_1, e_2, \dots e_{k_0}, e_{k_0+1}, \cdots, e_n\}$ of R_2^n. We can consider the dual basis $\{e_1^*, e_2^*, \dots e_{k_0}^*, e_{k_0+1}^*, \cdots, e_n^*\}$ defined by $e_i \cdot e_j^* = \delta_{ij}$, the Kronecker delta. Then

$$R_1^n/\mathscr{C}_1 \simeq \langle e_1^*, \cdots, e_{k_0}^* \rangle$$

where $\langle e_1^*, \cdots, e_{k_0}^* \rangle$ is the subspace generated by $\{e_1^*, e_2^*, \dots e_{k_0}^*\}$.

We can define the map $f : \mathscr{C}_0 \to \langle e_1^*, \cdots, e_{k_0}^* \rangle$ which takes every codeword in $\mathscr{C}_0$ to the unique representative of the map $F : \mathscr{C}_0 \to R_1^n/\mathscr{C}_1$ in $\langle e_{k_0+1}^*, \cdots, e_n^* \rangle$. Thus we can replace F by f.

LEMMA 5.3. *Let $\mathscr{C}$ be a code corresponding to $(\mathscr{C}_0, \mathscr{C}_1, f)$ over R_2 of type $1^{k_0}p^{k_1}$ such that $2k_0 + k_1 = n$. Then $\mathscr{C}$ is self-dual if and only if the following conditions are satisfied:*
(i) $\mathscr{C}_1 = \mathscr{C}_0^\perp$
(ii) $h_1(x) \cdot h_1(x') + p(h_1(f(x)) \cdot h_1(x') + h_1(x) \cdot h_1(f(x'))) \equiv 0 \pmod{p^2}$ for all $x, x' \in \mathscr{C}_0$.

Proof. Let $\mathscr{C}$ be a self-dual code. The first condition is from the previous lemma. The second condition is deduced from the fact that for each $x, x' \in \mathscr{C}_0$, $z = x + pf(x)$, $z' = x' + pf(x')$ are codewords in $\mathscr{C}$ satisfying

$$z \cdot z' = (x + pf(x)) \cdot (x' + pf(x')) \equiv 0 \pmod{p^2}$$

$$\iff h_1(x) \cdot h_1(x') + p(h_1(f(x)) \cdot h_1(x') + h_1(x) \cdot h_1(f(x'))) \equiv 0 \pmod{p^2}.$$

Conversely, the two condition ensure that self-orthogonality of $\mathscr{C}$ and by the type of $\mathscr{C}$, $|\mathscr{C}| = |\mathscr{C}_0| \cdot |\mathscr{C}_1|$. Thus $\mathscr{C}$ is self-dual. □

According to the previous lemma, we can construct distinct self-dual codes over R_2 from each self-orthogonal code over $R_1 = \mathbb{F}_{p^2}$ as follows.

Let $\mathscr{C}_0$ be a self-orthogonal codes over $\mathbb{F}_{p^2}$. Then we can regard $\mathscr{C}_0$ as a residue code of a self-dual codes $\mathscr{C}$ with the generator matrix G. The basis $\{e_1^*, \cdots, e_{k_0}^*\}$ can be taken as the canonical basis from row vectors of the matrix

$$\begin{pmatrix} I_{k_0} & 0 \end{pmatrix}.$$

Then, the map f is characterized by the image of a basis of $\mathscr{C}_0$ which can be taken as the set of row vectors of

$$G_0 = \begin{pmatrix} I_{k_0} & A_1 & B_1 \end{pmatrix}.$$

Let e_i be the ith row vector of G_0 then the map f is defined by the matrix

$$M = (m_{ij})_{1 \le i,j \le k_0} \quad where \quad f(e_i) = \sum_{j=1}^{k_1} m_{ij} e_j^*.$$

Then, we can construct self-dual codes over R_2 by the following lemma.

THEOREM 5.4. *Assume that $\mathscr{C}$ is a code satisfying $\mathscr{C}_1 = \mathscr{C}_0^\perp$ and G_0 is generator matrix of $\mathscr{C}_0$ and G_1 is generator matrix of $\mathscr{C}_1$. Then $\mathscr{C}$ is self-dual with a generator matrix (non standard form)*

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

if and only if

$$I_{k_0} + p(M + M^\top) + A_1 A_1^\top + B_1 B_1^\top \equiv 0 \pmod{p^2}. \tag{2}$$

Proof. Only if part is trivial. $\mathscr{C}_1 = \mathscr{C}_0^\perp$ guarantees that $2k_0 + k_1 = n$ and

$$\begin{pmatrix} I_{k_0} + pM & A_1 & B_1 \\ 0 & pI_{k_1} & pC_1 \end{pmatrix} \begin{pmatrix} I_{k_0} + pM & A_1 & B_1 \end{pmatrix}^\top \equiv 0 \pmod{p^2}$$

Therefore,

$$I_{k_0} + p(M + M^\top) + A_1 A_1^\top + B_1 B_1^\top \equiv 0 \pmod{p^2} \Longrightarrow GG^\top \equiv 0 \pmod{p^2}$$

Hence, $\mathscr{C}$ is self-orthogonal. From the fact that $\mathscr{C}$ has the type $1^{k_0} p^{k_1}$, $|\mathscr{C}| = p^{4^{k_0}} p^{2^{k_1}} = p^{4k_0 + 2k_1} = p^{2n}$. Thus $|\mathscr{C}| = |\mathscr{C}^\perp|$ and $\mathscr{C}$ is self-dual. □

6. Mass Formula

THEOREM 6.1. *[8,11,14,15] Let $\sigma_q(n,k)$ be the number of self-orthogonal codes of length n and dimension k over $\mathbb{F}_q$, where $q = p^m$ for some prime p and an integer m. 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 6.2. *Let p be an odd prime. If $\mathscr{C}_0$ is a self-orthogonal codes over a Galois ring $GR(p,2)$ with rank k. Then the number of distinct self-dual codes over a Galois ring $GR(p^2,2)$ corresponding to $\mathscr{C}_0$ is $(p^2)^{k(k-1)/2}$*

Proof. By the previous argument, we know that the number of distinct matrix $M = (m_{ij})$ determines the number of distinct self-dual codes corresponding to $\mathscr{C}_0$. By the condition of (2), we can deduce that $e_i \cdot e_j + p(m_{ij}+m_{ji}) \equiv 0 \pmod{p^2}$ for all e_i and e_j, ith and jth row vectors of G_0 respectively. Thus, diagonal elements of M is determined by G_0 and we can set any element of $GR(p,2)$ as m_{ij} for $i > j$ and m_{ji} is determined by m_{ij}. So the number of M satisfying (2) is the number of choices of $m'_{ij}s$ for $i > j$. □

Corollary 6.3. *Let p be an odd prime. The number of distinct self-dual codes over a Galois ring $GR(p^2, 2)$ is*

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

where $\sigma_{p^2}(n, k)$ is the number of distinct self-orthogonal codes over $\mathbb{F}_{p^2}$.

7. examples

In this chapter we introduce some examples of self-dual codes over $GR(p^2, 2)$ for $p = 3, 5$ which are obtained by following the previous argument. We use the computational algebra system Magma for computation and it represents a Galois ring by a root of some intrinsic irreducible polynomial. Note that we follow the representations of Galois rings in Magma

7.1. Self-dual codes over $GR(9, 2)$ of length 4, type $1^1 3^2$. We can take the irreducible polynomial for $GR(3, 2)$ and $GR(9, 2)$ commonly as $h(x) = x^2 + 2x + 2$. Let ω and $\bar{\omega}$ be roots of $h(x)$ as the representatives of $GR(3, 2)$ and $GR(9, 2)$ respectively. Then, $h_1(\omega) = \bar{\omega}$ and $\omega^2 = \omega + 1 \in \mathbb{Z}_3[\omega]$ and $\bar{\omega}^2 = 7\bar{\omega} + 7 \in \mathbb{Z}_9[\bar{\omega}]$.

There are 4 self-orthogonal codes over $GR(3, 2)$ of length 4 with rank $k = 1$ upto equivalence, whose generator matrices are as follows:

$$G_0^1 = \begin{pmatrix} 1 & 0 & 1 & 1 \end{pmatrix} \qquad G_0^2 = \begin{pmatrix} 1 & 1 & 1+\omega & 1+\omega \end{pmatrix}$$

$$G_0^3 = \begin{pmatrix} 1 & \omega & 1+\omega & 1+2\omega \end{pmatrix} \quad G_0^4 = \begin{pmatrix} 1 & 0 & 0 & 1+\omega \end{pmatrix}.$$

Then we obtain the generator matrices G_1^i's of the torsion code as the dual code of each self-dual codes $\mathscr{C}_0^i$'s over $GR(3,2)$:

$$G_1^1 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 \end{pmatrix} \qquad G_1^2 = \begin{pmatrix} 1 & 1 & 1+\omega & 1+\omega \\ 0 & 1 & 0 & 1+\omega \\ 0 & 0 & 1 & 2 \end{pmatrix}$$

$$G_1^3 = \begin{pmatrix} 1 & \omega & 1+\omega & 1+2\omega \\ 0 & 1 & 0 & 1+\omega \\ 0 & 0 & 1 & 1+2\omega \end{pmatrix} \quad G_1^4 = \begin{pmatrix} 1 & 0 & 0 & 1+\omega \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Then, we can choose the map f as the matrix M. In this case, each residue code has the rank $k = 1$ and is corresponding to only one self-dual code over $GR(9,2)$ of length 4 with type $1^1 3^2$ which has generator matrix in the standard form as follows:

$$G^1 = \begin{pmatrix} 1 & 0 & 1 & 4 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 6 \end{pmatrix} \qquad G^2 = \begin{pmatrix} 1 & 1 & 1+\bar{\omega} & 1+\bar{\omega} \\ 0 & 3 & 0 & 3+3\bar{\omega} \\ 0 & 0 & 3 & 6 \end{pmatrix}$$

$$G^3 = \begin{pmatrix} 1 & \bar{\omega} & 1+\bar{\omega} & 7+8\bar{\omega} \\ 0 & 3 & 0 & 3+3\bar{\omega} \\ 0 & 0 & 3 & 3+6\bar{\omega} \end{pmatrix} \quad G^4 = \begin{pmatrix} 1 & 0 & 0 & 1+\bar{\omega} \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 0 \end{pmatrix}$$

7.2. self-dual codes over $GR(9,2)$ of length 5 with type $1^2 3^1$. Let $\mathscr{C}_0$ be a self-orthogonal code over $GR(3,2)$ of length 5 with rank 2 with generator matrix

$$G_0 = \begin{pmatrix} 1 & 0 & 1 & 2+2\omega & 1+\omega \\ 0 & 1 & 1+\omega & \omega & 2+\omega \end{pmatrix}.$$

Then we obtain a generator matrix G_1 of $\mathscr{C}_1$ as a $\mathscr{C}_0^{\perp}$,

$$G_1 = \begin{pmatrix} 1 & 0 & 1 & 2+2\omega & 1+\omega \\ 0 & 1 & 1+\omega & \omega & 2+\omega \\ 0 & 0 & 1 & \omega & 1+2\omega \end{pmatrix}.$$

There are $(3^2)^1 = 9$ distinct self-dual codes over $GR(9, 2)$ with generator matrices:

$$G^1 = \begin{pmatrix} 1 & 0 & 1 & 2+2\bar{\omega} & 4+4\bar{\omega} \\ 0 & 1 & 1+\bar{\omega} & 6+7\bar{\omega} & 8+\bar{\omega} \\ 0 & 0 & 3 & 3\bar{\omega} & 3+6\bar{\omega} \end{pmatrix} \quad G^2 = \begin{pmatrix} 1 & 0 & 1 & 5+2\bar{\omega} & 7+4\bar{\omega} \\ 0 & 1 & 1+\bar{\omega} & 6+4\bar{\omega} & 2+7\bar{\omega} \\ 0 & 0 & 3 & 3\bar{\omega} & 3+6\bar{\omega} \end{pmatrix}$$

$$G^3 = \begin{pmatrix} 1 & 0 & 1 & 8+2\bar{\omega} & 1+4\bar{\omega} \\ 0 & 1 & 1+\bar{\omega} & 6+\bar{\omega} & 5+4\bar{\omega} \\ 0 & 0 & 3 & 3\bar{\omega} & 3+6\bar{\omega} \end{pmatrix} \quad G^4 = \begin{pmatrix} 1 & 0 & 1 & 8+5\bar{\omega} & 4+7\bar{\omega} \\ 0 & 1 & 1+\bar{\omega} & 3+4\bar{\omega} & 5+\bar{\omega} \\ 0 & 0 & 3 & 3\bar{\omega} & 3+6\bar{\omega} \end{pmatrix}$$

$$G^5 = \begin{pmatrix} 1 & 0 & 1 & 5+5\bar{\omega} & 7+7\bar{\omega} \\ 0 & 1 & 1+\bar{\omega} & 3+\bar{\omega} & 8+7\bar{\omega} \\ 0 & 0 & 3 & 3\bar{\omega} & 3+6\bar{\omega} \end{pmatrix} \quad G^6 = \begin{pmatrix} 1 & 0 & 1 & 8+5\bar{\omega} & 1+7\bar{\omega} \\ 0 & 1 & 1+\bar{\omega} & 3+7\bar{\omega} & 2+4\bar{\omega} \\ 0 & 0 & 3 & 3\bar{\omega} & 3+6\bar{\omega} \end{pmatrix}$$

$$G^7 = \begin{pmatrix} 1 & 0 & 1 & 2+8\bar{\omega} & 4+\bar{\omega} \\ 0 & 1 & 1+\bar{\omega} & \bar{\omega} & 2+\bar{\omega} \\ 0 & 0 & 3 & 3\bar{\omega} & 3+6\bar{\omega} \end{pmatrix} \quad G^8 = \begin{pmatrix} 1 & 0 & 1 & 5+8\bar{\omega} & 7+\bar{\omega} \\ 0 & 1 & 1+\bar{\omega} & 7\bar{\omega} & 5+7\bar{\omega} \\ 0 & 0 & 3 & 3\bar{\omega} & 3+6\bar{\omega} \end{pmatrix}$$

$$G^9 = \begin{pmatrix} 1 & 0 & 1 & 8+8\bar{\omega} & 1+\bar{\omega} \\ 0 & 1 & 1+\bar{\omega} & 4\bar{\omega} & 8+4\bar{\omega} \\ 0 & 0 & 3 & 3\bar{\omega} & 3+6\bar{\omega} \end{pmatrix}.$$

7.3. self-dual code over $GR(25, 2)$ of length 4 with, type 1^2. We can take the irreducible polynomial for $GR(5, 2)$ and $GR(25, 2)$ commonly as $h(x) = x^2 + 4x + 2$. Let ω and $\bar{\omega}$ be roots of $h(x)$ as the representatives of $GR(5, 2)$ and $GR(25, 2)$ respectively. Then, $h_1(\omega) = \bar{\omega}$ and $\omega^2 = \omega + 3 \in \mathbb{Z}_5[\omega]$ and $\bar{\omega}^2 = 21\bar{\omega} + 23 \in \mathbb{Z}_{25}[\bar{\omega}]$.

Let $\mathscr{C}_0$ be a self-orthogonal code over $GR(5, 2)$ of length 4 with rank 2 with generator matrix

$$G_0 = \begin{pmatrix} 1 & 0 & 1 & 1+3\omega \\ 0 & 1 & 1+3\omega & 4 \end{pmatrix}.$$

It is clear that $\mathscr{C}_0$ is self-dual, thus $\mathscr{C}_0 = \mathscr{C}_1$.

There are $(5^2)^1 = 25$ self-dual codes corresponding the code $\mathscr{C}_0$ over $GR(25, 2)$:

$$G^1 = \begin{pmatrix} 1 & 0 & 1+5\bar{\omega} & 21+3\bar{\omega} \\ 0 & 1 & 21+3\bar{\omega} & 24+20\bar{\omega} \end{pmatrix} \qquad G^2 = \begin{pmatrix} 1 & 0 & 1+10\bar{\omega} & 6+13\bar{\omega} \\ 0 & 1 & 6+13\bar{\omega} & 24+15\bar{\omega} \end{pmatrix}$$

$$G^3 = \begin{pmatrix} 1 & 0 & 1+15\bar{\omega} & 16+23\bar{\omega} \\ 0 & 1 & 16+23\bar{\omega} & 24+10\bar{\omega} \end{pmatrix} \qquad G^4 = \begin{pmatrix} 1 & 0 & 1+20\bar{\omega} & 1+8\bar{\omega} \\ 0 & 1 & 1+8\bar{\omega} & 24+5\bar{\omega} \end{pmatrix}$$

$$G^5 = \begin{pmatrix} 1 & 0 & 6+5\bar{\omega} & 11+23\bar{\omega} \\ 0 & 1 & 11+23\bar{\omega} & 19+20\bar{\omega} \end{pmatrix} \qquad G^6 = \begin{pmatrix} 1 & 0 & 11+20\bar{\omega} & 6+23\bar{\omega} \\ 0 & 1 & 6+23\bar{\omega} & 14+5\bar{\omega} \end{pmatrix}$$

$$G^7 = \begin{pmatrix} 1 & 0 & 21+15\bar{\omega} & 1+3\bar{\omega} \\ 0 & 1 & 1+3\bar{\omega} & 4+10\bar{\omega} \end{pmatrix} \qquad G^8 = \begin{pmatrix} 1 & 0 & 21+5\bar{\omega} & 6+8\bar{\omega} \\ 0 & 1 & 6+8\bar{\omega} & 4+20\bar{\omega} \end{pmatrix}$$

$$G^9 = \begin{pmatrix} 1 & 0 & 1 & 11+18\bar{\omega} \\ 0 & 1 & 11+18\bar{\omega} & 24 \end{pmatrix} \qquad G^{10} = \begin{pmatrix} 1 & 0 & 21+10\bar{\omega} & 16+18\bar{\omega} \\ 0 & 1 & 16+18\bar{\omega} & 4+15\bar{\omega} \end{pmatrix}$$

$$G^{11} = \begin{pmatrix} 1 & 0 & 11 & 16+8\bar{\omega} \\ 0 & 1 & 16+8\bar{\omega} & 14 \end{pmatrix} \qquad G^{12} = \begin{pmatrix} 1 & 0 & 11+5\bar{\omega} & 1+18\bar{\omega} \\ 0 & 1 & 1+18\bar{\omega} & 14+20\bar{\omega} \end{pmatrix}$$

$$G^{13} = \begin{pmatrix} 1 & 0 & 21 & 21+23\bar{\omega} \\ 0 & 1 & 21+23\bar{\omega} & 4 \end{pmatrix} \qquad G^{14} = \begin{pmatrix} 1 & 0 & 16+15\bar{\omega} & 11+8\bar{\omega} \\ 0 & 1 & 11+8\bar{\omega} & 9+10\bar{\omega} \end{pmatrix} \quad .$$

$$G^{15} = \begin{pmatrix} 1 & 0 & 6+10\bar{\omega} & 21+8\bar{\omega} \\ 0 & 1 & 21+8\bar{\omega} & 19+15\bar{\omega} \end{pmatrix} \qquad G^{16} = \begin{pmatrix} 1 & 0 & 16 & 6+3\bar{\omega} \\ 0 & 1 & 6+3\bar{\omega} & 9 \end{pmatrix}$$

$$G^{17} = \begin{pmatrix} 1 & 0 & 11+15\bar{\omega} & 21+13\bar{\omega} \\ 0 & 1 & 21+13\bar{\omega} & 14+10\bar{\omega} \end{pmatrix} \qquad G^{18} = \begin{pmatrix} 1 & 0 & 21+20\bar{\omega} & 11+13\bar{\omega} \\ 0 & 1 & 11+13\bar{\omega} & 4+5\bar{\omega} \end{pmatrix}$$

$$G^{19} = \begin{pmatrix} 1 & 0 & 6+15\bar{\omega} & 6+18\bar{\omega} \\ 0 & 1 & 6+18\bar{\omega} & 19+10\bar{\omega} \end{pmatrix} \qquad G^{20} = \begin{pmatrix} 1 & 0 & 11+10\bar{\omega} & 11+3\bar{\omega} \\ 0 & 1 & 11+3\bar{\omega} & 14+15\bar{\omega} \end{pmatrix}$$

$$G^{21} = \begin{pmatrix} 1 & 0 & 16+10\bar{\omega} & 1+23\bar{\omega} \\ 0 & 1 & 1+23\bar{\omega} & 9+15\bar{\omega} \end{pmatrix} \qquad G^{22} = \begin{pmatrix} 1 & 0 & 6 & 1+13\bar{\omega} \\ 0 & 1 & 1+13\bar{\omega} & 19 \end{pmatrix}$$

$$G^{23} = \begin{pmatrix} 1 & 0 & 16+20\bar{\omega} & 21+18\bar{\omega} \\ 0 & 1 & 21+18\bar{\omega} & 9+5\bar{\omega} \end{pmatrix} \qquad G^{24} = \begin{pmatrix} 1 & 0 & 6+20\bar{\omega} & 16+3\bar{\omega} \\ 0 & 1 & 16+3\bar{\omega} & 19+5\bar{\omega} \end{pmatrix}$$

$$G^{25} = \begin{pmatrix} 1 & 0 & 16+5\bar{\omega} & 16+13\bar{\omega} \\ 0 & 1 & 16+13\bar{\omega} & 9+20\bar{\omega} \end{pmatrix}.$$

References

[1] Jose Maria P. Balmaceda, Rowena Alma L. Betty, and Fidel R. Nemenzo, *Mass formula for self-dual codes over* $\mathbb{Z}_{p^2}$, Discrete Mathematics **308** (14) (2008), 2984–3002.

[2] A. R. Calderbank and N. J. A. Sloane, *Modular and p-adic cyclic codes*, Des. Codes Cryptography, **6** (1) (1995), 21–35.

[3] Whan-Hyuk Choi, Kwang Ho Kim, and Sook Young Park, *The classification of self-orthogonal codes over* $\mathbb{Z}_{p^2}$ *of length* ≤ 3, Korean Journal of Mathematics **22** (4) (2014), 725–742.

[4] Philippe Gaborit, *Mass formulas for self-dual codes over* $\mathbb{Z}_4$ *and* $\mathbb{F}_q + u\mathbb{F}_q$ *rings*, Information Theory IEEE Transactions on **42** (4) (1996) 1222–1228.

[5] Fernando Q. Gouvêa, *p-adic Numbers*, Springer, 1997.

[6] Roger A. Hammons, Vijay P. Kumar, A. Robert Calderbank, N. Sloane, and Patrick Solé, *The* Z_4*-linearity of Kerdock, Preparata, Goethals, and related codes*, Information Theory IEEE Transactions on **40** (2) (1994), 301–319.

[7] Jon-Lark Kim and Yoonjin Lee, *Construction of MDS self-dual codes over Galois rings*, Designs, Codes and Cryptography, **45** (2) (2007), 247–258.

[8] Rudolf Lidl and Harald Niederreiter, *Finite fields: Encyclopedia of mathematics and its applications*, Computers & Mathematics with Applications **33** (7) (1997), 136–136.

[9] Bernard R. McDonald, *Finite rings with identity*, volume 28. Marcel Dekker Incorporated, 1974.

[10] Kiyoshi Nagata, Fidel Nemenzo, and Hideo Wada, *Constructive algorithm of self-dual error-correcting codes* In Proc. of 11th International Workshop on Algebraic and Combinatorial Coding Theory, pages 215–220, 2008.

[11] Kiyoshi Nagata, Fidel Nemenzo, and Hideo Wada, *The number of self-dual codes over* $\mathbb{Z}_{p^3}$, Designs, Codes and Cryptography **50** (3) (2009), 291–303.

[12] Kiyoshi Nagata, Fidel Nemenzo, and Hideo Wada, *Mass formula and structure of self-dual codes over* $\mathbb{Z}_{2^s}$, Designs, codes and cryptography **67** (3) (2013), 293–316.

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

[14] Vera Pless, *The number of isotropic subspaces in a finite geometry* Atti. Accad. Naz. Lincei Rendic **39** (1965), 418–421.

[15] Vera Pless, *On the uniqueness of the golay codes*, Journal of Combinatorial theory **5** (3) (1968), 215–228.

[16] Zhe-Xian Wan, *Finite Fields And Galois Rings*, World Scientific Publishing Co., Inc., 2011.

Whan-hyuk Choi
Department of Mathematics
Kangwon National University
Chuncheon, 24341 Korea
E-mail: whanhyuk@gmail.com