EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
Vol. 12, No. 4, 2019, 1701-1716
ISSN 1307-5543 – www.ejpam.com
Published by New York Business Global

Mass Formula for Self-Dual Codes over Galois Rings $GR(p^3, r)$

Trilbe Lizann E. Vasquez[1,*], Gaudencio C. Petalcorin, Jr.[1]

[1] *Department of Mathematics and Statistics, College of Science and Mathematics, Mindanao State University - Iligan Institute of Technology, 9200 Iligan City, Philippines*

Abstract. Let p be an odd prime and r a positive integer. Let $\mathrm{GR}(p^3, r)$ be the Galois ring of characteristic p^3 and cardinality p^{3r}. In this paper, we investigate the self-dual codes over $\mathrm{GR}(p^3, r)$ and give a method to construct self-dual codes over this ring. We establish a mass formula for self-dual codes over $\mathrm{GR}(p^3, r)$ and classify self-dual codes over $\mathrm{GR}(p^3, 2)$ of length 4 for $p = 3, 5$.

2010 Mathematics Subject Classifications: 94B05

Key Words and Phrases: Mass formula, self-dual codes, finite ring, Galois ring, classification

---

1. Introduction

It was shown in [6] that several well-known families of non-linear binary codes can be viewed as linear codes over the ring $\mathbb{Z}_4$ of integers modulo 4. This discovery led to much interest and attention given to codes over the ring $\mathbb{Z}_m$ of integers modulo m and finite rings in general.

Self-dual codes are an important class of linear codes for both theoretical and practical reasons. It is a fundamental problem to classify self-dual codes, that is, to find a representative for each equivalence class of self-dual codes. However, determining the number of equivalence classes is difficult. This task will be made easier by a mass formula, which will tell us when we have a complete set of representatives from each equivalence class.

Mass formula for self-dual codes over the ring $\mathbb{Z}_{p^e}$ for any prime p and for any positive integer e are established by the effort of many authors [1, 5, 9–11]. A classification method of self-dual codes over $\mathbb{Z}_m$ for arbitrary integer m is given in [13]. In particular, self-dual codes of length 4 over $\mathbb{Z}_p$ were classified in [13] for all primes p in terms of their automorphism groups.

The Galois ring $\mathrm{GR}(p^e, r)$, where p is prime, e and r are positive integers, is the unique Galois extension of $\mathbb{Z}_{p^e}$ of degree r. Using a similar argument in [1], the mass formula

---

*Corresponding author.
DOI: https://doi.org/10.29020/nybg.ejpam.v12i4.3565

Email addresses: trilbelizann.vasquez@g.msuiit.edu.ph (T.L. Vasquez), gaudencio.petalcorin@g.msuiit.edu.ph (G. Petalcorin)

for self-dual codes over $\mathrm{GR}(p^2, 2)$ for odd primes p is obtained in [3]. Moreover, self-dual codes of length 4 over $\mathrm{GR}(p, 2)$ and $\mathrm{GR}(p^2, 2)$ are classified in [4] for all primes p up to equivalence in terms of automorphism group.

In this paper, we build on the method in [10] to establish a mass formula for self-dual codes over $\mathrm{GR}(p^3, r)$, where p is an odd prime and r is a positive integer. Using the mass formula, we classify self-dual codes of length 4 over $\mathrm{GR}(p^3, 2)$ for $p = 3, 5$.

2. Preliminaries

Let p be prime and e a positive integer. The modulo p reduction mapping

$$\mu : \mathbb{Z}_{p^e} \to \mathbb{Z}_p, a \mapsto \bar{a} = a \pmod{p}$$

induces the following modulo p reduction mapping between polynomial rings

$$\mu : \mathbb{Z}_{p^e}[x] \to \mathbb{Z}_p[x], f(x) = \sum a_i x^i \mapsto \bar{f}(x) = \sum \bar{a}_i x^i.$$

An irreducible polynomial $f(x)$ in $\mathbb{Z}_{p^e}[x]$ is said to be *basic* if $\bar{f}(x)$ is irreducible.

Let $f(x)$ be a monic basic irreducible polynomial over $\mathbb{Z}_{p^e}[x]$ of degree r. We can choose $f(x)$ so that $\omega = x + \langle f(x) \rangle$ is a primitive $(p^r - 1)$st root of unity. The *Galois ring* $\mathrm{GR}(p^e, r)$ of characteristic p^e and cardinality p^{er} is defined as

$$\mathrm{GR}(p^e, r) = \mathbb{Z}_{p^e}[x]/\langle f(x) \rangle = \mathbb{Z}_{p^e}[\omega].$$

Every element of $\mathrm{GR}(p^e, r)$ can be expressed uniquely in the *ω-adic representation*

$$a_0 + a_1\omega + a_2\omega^2 + \cdots + a_{r-1}\omega^{r-1}, \text{ where } a_i \in \mathbb{Z}_{p^e}.$$

Note that $\mathrm{GR}(p^e, 1) = \mathbb{Z}_{p^e}$ and $\mathrm{GR}(p, r) = \mathbb{F}_{p^r}$, the Galois field of p^r elements.

The modulo p reduction can be naturally extended to

$$\mu : \mathrm{GR}(p^e, r) = \mathbb{Z}_{p^e}[x]/\langle f(x) \rangle \to \mathbb{Z}_p[x]/\langle \bar{f}(x) \rangle = \mathbb{F}_{p^r}, a \mapsto \bar{a} = a \pmod{p}.$$

Let $\mathcal{T}_{p^r} = \{0, 1, \omega, \ldots, \omega^{p^r-2}\}$. Observe that the function $\mu|_{\mathcal{T}_{p^r}} : \mathcal{T}_{p^r} \to \mathbb{F}_{p^r}$ is one-to-one and onto. Any element of $\mathrm{GR}(p^e, r)$ can be written uniquely in the *p-adic representation*

$$b_0 + pb_1 + p^2b_2 + \cdots + p^{e-1}b_{e-1}, \text{ where } b_i \in \mathcal{T}_{p^r}.$$

An element $a \in \mathrm{GR}(p^e, r)$ is a unit if and only if $\bar{a} \neq 0$.

For the further study of Galois rings, see [8, 16].

Let n be a positive integer and let S^n denote the collection of n-tuples over a finite set S. A *code* of length n over a finite field $\mathbb{F}$ or a finite ring $\mathcal{R}$ is a subspace of $\mathbb{F}^n$ or an $\mathcal{R}$-submodule of $\mathcal{R}^n$, respectively. Every element of the code is called a *codeword*. A matrix G is called a *generator matrix* for a code $\mathcal{C}$ if the rows of G generate all the elements of $\mathcal{C}$ and none of the rows can be written as a linear combination of the other rows.

Two codewords $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ are *orthogonal* if their Euclidean inner product $\sum_{i=1}^n x_i y_i$ is zero. The *dual* $\mathcal{C}^\perp$ of a code $\mathcal{C}$ of length n over S consists of all $x \in S^n$ which are orthogonal to every codeword in $\mathcal{C}$. If $\mathcal{C} \subseteq \mathcal{C}^\perp$, then $\mathcal{C}$ is said to be *self-orthogonal.* If $\mathcal{C} = \mathcal{C}^\perp$, then $\mathcal{C}$ is said to be *self-dual.*

A code of length n and dimension k over a finite field $\mathbb{F}$ is called an $[n, k]$ code and contains $|\mathbb{F}|^k$ codewords. An $[n, k]$ code is self-dual if and only if it is self-orthogonal and $k = \frac{n}{2}$. We say that a generator matrix G for an $[n, k]$ code is in *standard form* if $G = [I_k\ A]$, where I_k denotes the $k \times k$ identity matrix and A is some $k \times (n - k)$ matrix.

Let $\mathcal{C}$ be a code of length n over the Galois ring $\mathrm{GR}(p^e, r)$. $\mathcal{C}$ has a generator matrix which, after a suitable permutation of coordinates, can be written as

$$G = \begin{bmatrix} I_{k_0} & A_{0,1} & A_{0,2} & \cdots & A_{0,e-1} & A_{0,e} \\ 0 & pI_{k_1} & pA_{1,2} & \cdots & pA_{1,e-1} & pA_{1,e} \\ 0 & 0 & p^2 I_{k_2} & \cdots & p^2 A_{2,e-1} & p^2 A_{2,e} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & p^{e-1} I_{k_{e-1}} & p^{e-1} A_{e-1,e} \end{bmatrix} \tag{1}$$

where I_{k_i} is the $k_i \times k_i$ identity matrix and the A_{ij}s are matrices of appropriate sizes over $\mathrm{GR}(p^e, r)$. The columns are grouped into blocks of sizes $k_0, k_1, \ldots, k_{e-1}, k_e = n - \sum_{i=0}^{e-1} k_i$.

A code $\mathcal{C}$ with generator matrix G as in (1) is said to be of type $\{k_0, k_1, \ldots, k_{e-1}\}$ and has $(p^r)^{\sum_{i=0}^{e-1}(e-i)k_i}$ codewords. The dual $\mathcal{C}^\perp$ of $\mathcal{C}$ is of type $\{k_e, k_{e-1}, \ldots, k_1\}$. It is known that $|\mathcal{C}||\mathcal{C}^\perp| = p^{ern}$. If $\mathcal{C}$ is a self-dual code of type $\{k_0, k_1, \ldots, k_{e-1}\}$, then we must have $k_i = k_{e-i}$ for all i.

For $0 \leq i \leq e - 1$, define

$$\mathrm{Tor}_i(\mathcal{C}) = \{\bar{v} : p^i \bar{v} \in \mathcal{C}\},$$

where $\bar{v}$ is the image of v under the projection $\mu : \mathrm{GR}(p^e, r)^n \to \mathbb{F}_{p^r}^n$. $\mathrm{Tor}_i(\mathcal{C})$ is an $[n, k_0 + \ldots + k_i]$ code over $\mathbb{F}_{p^r}$ and is called the ith *torsion code* of $\mathcal{C}$. In particular, $\mathrm{Tor}_0(\mathcal{C})$ is called the *residue code* and is denoted by $\mathrm{Res}(\mathcal{C})$. If $\mathcal{C}$ has generator matrix G in (1), then $\mathrm{Tor}_i(\mathcal{C})$ has a generator matrix of the form

$$G_i = \begin{bmatrix} I_{k_0} & \overline{A}_{0,1} & \overline{A}_{0,2} & \cdots & \overline{A}_{0,i-1} & \cdots & \overline{A}_{0,e} \\ 0 & I_{k_1} & \overline{A}_{1,2} & \cdots & \overline{A}_{1,i-1} & \cdots & \overline{A}_{1,e} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & I_{k_i} & \cdots & \overline{A}_{i,e} \end{bmatrix},$$

where $\overline{A} = (\bar{a}_{ij})$ whenever $A = (a_{ij})$.

Two codes over $\mathrm{GR}(p^e, r)$ are said to be *equivalent* if one can be obtained from the other by permuting the coordinates and (if necessary) changing the signs of certain coordinates. Thus two codes $\mathcal{C}_1$ and $\mathcal{C}_2$ of length n over $\mathrm{GR}(p^e, r)$ are equivalent if there exists a monomial matrix P such that $\mathcal{C}_2 = \mathcal{C}_1 P = \{\mathbf{c}P : \mathbf{c} \in \mathcal{C}_1\}$, where P has exactly one entry ± 1 in every row and every column and all the other entries are zero. The automorphism group $\mathrm{Aut}(\mathcal{C})$ of a code $\mathcal{C}$ of length n over $\mathrm{GR}(p^e, r)$ is the group of all such matrices P such that $\mathcal{C} = \mathcal{C}P$.

Let E_n be the signed symmetric group of order $|E_n| = 2^n n!$. The number of codes equivalent to a code $\mathcal{C}$ over $\mathrm{GR}(p^3, r)$ of length n is

$$\frac{|E_n|}{|\mathrm{Aut}(\mathcal{C})|}$$

and hence the number $N_{p^3,r}(n)$ of distinct self-dual codes over $\mathrm{GR}(p^3, r)$ of length n is

$$N_{p^3,r}(n) = \sum_{\mathcal{C}} \frac{|E_n|}{|\mathrm{Aut}(\mathcal{C})|}$$

where the sum runs through all inequivalent self-dual codes $\mathcal{C}$ over $\mathrm{GR}(p^3, r)$ of length n. An explicit formula for $N_{p^3,r}(n)$, called the *mass formula*, would thus be useful for finding all inequivalent self-dual codes over $\mathrm{GR}(p^3, r)$ of given length.

For the further study of codes over finite fields and finite rings, see [7, 12].

We will need the following lemmas, the proofs of which are known.

Lemma 1. [14] *Let $\sigma_q(n, k)$ be the number of self-orthogonal codes of even length n and dimension k over $\mathbb{F}_q$. If char $\mathbb{F}_q \neq 2$, then*

$$\sigma_q(n,k) = \frac{\left(q^{n-k} - \epsilon q^{n/2-k} + \epsilon q^{n/2} - 1\right) \displaystyle\prod_{i=1}^{k-1} (q^{n-2i} - 1)}{\displaystyle\prod_{i=1}^{k} (q^i - 1)}, \ k \geq 2$$

where $\epsilon = 1$ if $(-1)^{n/2}$ is a square and $\epsilon = -1$ if $(-1)^{n/2}$ is not a square.

Lemma 2. [15] *Let V be an n-dimensional vector space over $\mathbb{F}_q$. The number $\binom{n}{k}_q$ of subspaces $U \subset V$ of dimension $k \leq n$ is given by*

$$\binom{n}{k}_q = \frac{(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1})}{(q^k - 1)(q^k - q) \cdots (q^k - q^{k-1})}.$$

3. Codes over $\mathbf{GR}(p^3, r)$

Let $\mathcal{C}$ be a code of length n over $\mathrm{GR}(p^3, r)$ and let G be a generator matrix for $\mathcal{C}$. We can write G in the following form:

$$G = \begin{bmatrix} A \\ pB \\ p^2C \end{bmatrix} = \begin{bmatrix} I_k & A_2 & A_3 & A_4 \\ 0 & pI_l & pB_3 & pB_4 \\ 0 & 0 & p^2 I_m & p^2 C_4 \end{bmatrix}, \tag{2}$$

where I_r is the identity matrix of order r, and the other matrices have entries from $\mathrm{GR}(p^3, r)$ and are described as follows. We write A_3, B_4 and A_4 in their p-adic expansions

$A_3 = A_{30} + pA_{31}$, $B_4 = B_{40} + pB_{41}$, $A_4 = A_{40} + pA_{41} + p^2A_{42}$, and the matrices A_2, B_3, C_4, A_{ij} and B_{ij} have entries from $\mathcal{T}_{p^r}$. The columns are grouped in blocks of sizes k, l, m and $h = n - (k + l + m)$. The code $\mathcal{C}$ is said to be of type $\{k, l, m\}$ and has $p^{r(3k+2l+m)}$ codewords. The dual code $\mathcal{C}^\perp$ is of type $\{h, m, l\}$ and has $p^{r(3h+2m+l)}$ codewords.

If the code $\mathcal{C}$ has generator matrix G in (2), then the residue code $\mathrm{Res}(\mathcal{C})$ has dimension k and generator matrix

$$T_0 = A \pmod p = \begin{bmatrix} I_k & \overline{A}_2 & \overline{A}_{30} & \overline{A}_{40} \end{bmatrix}, \tag{3}$$

the first torsion code $\mathrm{Tor}_1(\mathcal{C})$ has dimension $k + l$ and generator matrix

$$T_1 = \begin{bmatrix} A \\ B \end{bmatrix} \pmod p = \begin{bmatrix} I_k & \overline{A}_2 & \overline{A}_{30} & \overline{A}_{40} \\ 0 & I_l & \overline{B}_3 & \overline{B}_{40} \end{bmatrix}, \tag{4}$$

and the second torsion code $\mathrm{Tor}_2(\mathcal{C})$ has dimension $k + l + m$ and generator matrix

$$T_2 = \begin{bmatrix} A \\ B \\ C \end{bmatrix} \pmod p = \begin{bmatrix} I_k & \overline{A}_2 & \overline{A}_{30} & \overline{A}_{40} \\ 0 & I_l & \overline{B}_3 & \overline{B}_{40} \\ 0 & 0 & I_m & \overline{C}_4 \end{bmatrix}. \tag{5}$$

The following proposition gives a characterization of self-duality in $\mathrm{GR}(p^3, r)$.

Proposition 1. *Let $\mathcal{C}$ be a code over $GR(p^3, r)$ with generator matrix G as in (2). Then $\mathcal{C}$ is self-dual if and only if $k = h, l = m$ and the following hold:*

$$AA^t \equiv 0 \pmod{p^3} \tag{6}$$
$$AB^t \equiv 0 \pmod{p^2} \tag{7}$$
$$BB^t \equiv 0 \pmod{p} \tag{8}$$
$$AC^t \equiv 0 \pmod{p}. \tag{9}$$

Proof. Suppose $\mathcal{C}$ is a self-dual code over $\mathrm{GR}(p^3, r)$. We then have $GG^t \equiv 0 \pmod{p^3}$, that is,

$$\begin{aligned} AA^t &\equiv 0 \pmod{p^3} \\ pAB^t &\equiv 0 \pmod{p^3} \\ p^2BB^t &\equiv 0 \pmod{p^3} \\ p^2AC^t &\equiv 0 \pmod{p^3}, \end{aligned}$$

which is equivalent to the set of conditions (6)-(9). Now, $\mathcal{C}$ is of type $\{k, l, m\}$ and its dual code $\mathcal{C}^\perp$ is of type $\{h, m, l\}$. Since $\mathcal{C}$ is self-dual, we then have $k = h$ and $l = m$.

Conversely, let $\mathcal{C}$ be a code such that $k = h, l = m$ and conditions (6)-(9) hold. Now, conditions (6)-(9) imply that $GG^t \equiv 0 \pmod{p^3}$. So $\mathcal{C}$ is a self-orthogonal code, i.e. $\mathcal{C} \subseteq \mathcal{C}^\perp$. Moreover, since $k = h$ and $l = m$, we then have $|\mathcal{C}| = |\mathcal{C}^\perp|$. Therefore $\mathcal{C} = \mathcal{C}^\perp$. □

Corollary 1. *A self-dual code $\mathcal{C}$ over $GR(p^3, r)$ of type $\{k, l, l\}$ is of even length $n = 2(k + l)$.*

Corollary 2. *Let $\mathcal{C}$ be a self-dual code over $GR(p^3, r)$ of length n and of type $\{k, l, l\}$. Then $Res(\mathcal{C})$ is self-orthogonal, $Tor_1(\mathcal{C})$ is self-dual, and $Tor_2(\mathcal{C}) = Res(\mathcal{C})^{\perp}$.*

Proof. Suppose $\mathcal{C}$ has generator matrix G as in (2). Then the torsion codes $\mathrm{Res}(\mathcal{C})$, $\mathrm{Tor}_1(\mathcal{C})$ and $\mathrm{Tor}_2(\mathcal{C})$ have generator matrices T_0, T_1 and T_2 as in (3), (4) and (5) respectively.

From conditions (6) and (7), we obtain

$$AA^t \equiv 0 \pmod{p} \tag{10}$$

$$AB^t \equiv 0 \pmod{p}. \tag{11}$$

It immediately follows from (10) that $T_0T_0^t \equiv 0 \pmod{p}$, and so $\mathrm{Res}(\mathcal{C})$ is self-orthogonal.

Conditions (8), (10) and (11) imply that $T_1T_1^t \equiv 0 \pmod{p}$, so that $\mathrm{Tor}_1(\mathcal{C})$ is self-orthogonal. Since $\mathcal{C}$ is self-dual, then $\dim \mathrm{Tor}_1(\mathcal{C}) = k + l = \frac{n}{2}$. Thus $\mathrm{Tor}_1(\mathcal{C})$ is self-dual.

From Conditions (9)-(11), it follows that $T_2T_0^t \equiv 0 \pmod{p}$, so $\mathrm{Tor}_2(\mathcal{C}) \subseteq \mathrm{Res}(\mathcal{C})^{\perp}$. From Corollary 1, $\dim \mathrm{Tor}_2(\mathcal{C}) = k+2l = n-k = \dim \mathrm{Res}(\mathcal{C})^{\perp}$. Consequently, $|\mathrm{Tor}_2(\mathcal{C})| = |\mathrm{Res}(\mathcal{C})^{\perp}|$ and so $\mathrm{Tor}_2(\mathcal{C}) = \mathrm{Res}(\mathcal{C})^{\perp}$. □

4. Codes over $\mathbf{GR}(p^3, r)$ from a code over $\mathbb{F}_p^r$

We now use Proposition 1 to construct self-dual codes over $\mathrm{GR}(p^3, r)$ with prescribed first torsion code. We start with a self-dual $[n, k + l]$ code $\mathcal{C}_1$ over $\mathbb{F}_{p^r}$ with generator matrix

$$G' = \begin{bmatrix} A' \\ B' \end{bmatrix} = \begin{bmatrix} I_k & A'_2 & A'_{30} & A'_{40} \\ 0 & I_l & B'_3 & B'_{40} \end{bmatrix},$$

where the columns are grouped into blocks of sizes k, l, l and k. Note that $2(k + l) = n$. We want to obtain the number of self-dual codes $\mathcal{C}$ over $\mathrm{GR}(p^3, r)$ such that $\mathrm{Tor}_1(\mathcal{C}) = \mathcal{C}_1$.

Since $\mathcal{C}_1$ is self-dual, then $G'G'^t \equiv 0 \pmod{p}$ and we obtain

$$I_k + A'_2{A'_2}^t + A'_{30}{A'_{30}}^t + A'_{40}{A'_{40}}^t \equiv 0 \pmod{p} \tag{12}$$

$$A'_2 + A'_{30}{B'_3}^t + A'_{40}{B'_{40}}^t \equiv 0 \pmod{p} \tag{13}$$

$$I_l + B'_3{B'_3}^t + B'_{40}{B'_{40}}^t \equiv 0 \pmod{p}. \tag{14}$$

Let $H = \begin{bmatrix} A'_{30} & A'_{40} \\ B'_3 & B'_{40} \end{bmatrix}$ and $J = \begin{bmatrix} I_k & -A'_2 \\ -{A'_2}^t & I_l + {A'_2}^t A'_2 \end{bmatrix}$. Note that H and J are both square matrices of order $k + l$. From (12)-(14), we have

$$H(-H^tJ) \equiv I_{k+l} \pmod{p}.$$

Hence, H is invertible modulo p. By a permutation of columns of H, we can assume that the $k \times k$ matrix A'_{40} is invertible modulo p.

Let $\mathcal{C}_0$ be the k-dimensional subspace of $\mathcal{C}_1$ with generator matrix

$$A' = \begin{bmatrix} I_k & A'_2 & A'_{30} & A'_{40} \end{bmatrix}.$$

From (12) and (13), $\mathcal{C}_0$ is a self-orthogonal code and $\mathcal{C}_0 \subseteq \mathcal{C}_1 \subseteq \mathcal{C}_0^{\perp}$. Now, the dual of $\mathcal{C}_0^{\perp}$ has dimension $n-k = k+2l$. Hence we can write the generator matrix of $\mathcal{C}_0^{\perp}$ as

$$\begin{bmatrix} A' \\ B' \\ C' \end{bmatrix} = \begin{bmatrix} I_k & A'_2 & A'_{30} & A'_{40} \\ 0 & I_l & B'_3 & B'_{40} \\ 0 & 0 & I_l & C'_4 \end{bmatrix},$$

where C'_4 is an $l \times k$ matrix over $\mathbb{F}_{p^r}$.

We wish to find matrices A_2, A_3, A_4, B_3, B_4 and C_4 with entries from $\mathrm{GR}(p^e, r)$ satisfying conditions (6)-(9), which are equivalent to

$$I_k + A_2A_2^t + A_3A_3^t + A_4A_4^t \equiv 0 \pmod{p^3} \tag{15}$$
$$A_2 + A_3B_3^t + A_4B_4^t \equiv 0 \pmod{p^2} \tag{16}$$
$$I_l + B_3B_3^t + B_4B_4^t \equiv 0 \pmod{p} \tag{17}$$
$$A_3 + A_4C_4^t \equiv 0 \pmod{p}. \tag{18}$$

The matrices A_2, B_3 and C_4 are considered modulo p, A_3 and B_4 are considered modulo p^2, and A_4 modulo p^3. As previously done, we write the matrices in p-adic expansion: $A_3 = A_{30} + pA_{31}$, $B_4 = B_{40} + pB_{41}$ and $A_4 = A_{40} + pA_{41} + p^2A_{42}$, where A_{31}, B_{41}, A_{41} and A_{42} have entries from $\mathcal{T}_{p^r}$.

Let A_2, A_{30}, A_{40}, B_3 and B_{40} be the matrices over $\mathcal{T}_{p^r}$ such that $\overline{A}_2 = A'_2$, $\overline{A}_{30} = A'_{30}$, $\overline{A}_{40} = A'_{40}$, $\overline{B}_3 = B'_3$ and $\overline{B}_{40} = B'_{40}$. From (12) and (13), there exist matrices (f_{ij}) and D with entries from $\mathrm{GR}(p^3, r)$ such that

$$A_2 + A_{30}B_3^t + A_{40}B_{40}^t = pD \tag{19}$$

and

$$I_k + A_2A_2^t + A_{30}A_{30}^t + A_{40}A_{40}^t = p(f_{ij}). \tag{20}$$

As in [10], B_{41} and C_4 are uniquely determined by

$$B_{41}^t \equiv -A_{40}^{-1}(D + A_{31}B_3^t + A_{41}B_{40}^t) \pmod{p} \tag{21}$$

and

$$C_4^t \equiv -A_{40}^{-1}A_{30} \pmod{p}, \tag{22}$$

which are sufficient conditions for (16) and (18). Since (14) is the same as (17), we only have to look at (15). It then follows that the code $\mathcal{C}$ is self-dual if and only if

$$f_{ij} + \widetilde{A_{30}A_{31}^t} + \widetilde{A_{40}A_{41}^t} + p(A_{31}A_{31}^t + A_{41}A_{41}^t + \widetilde{A_{40}A_{42}^t}) \equiv 0 \pmod{p^2} \tag{23}$$

Our goal is to count the number of matrices A_{31}, A_{41} and A_{42} satisfying (23).

For the remainder of this paper, we assume that p is an odd prime. Following the argument in Section 2.1 of [10], there are p^{rkl} possible choices for A_{31}, $p^{\frac{rk(k-1)}{2}}$ for A_{41} and $p^{\frac{rk(k-1)}{2}}$ for A_{42}. Therefore, we have $p^{rk(\frac{n}{2}-1)}$ possible choices for the matrices A_{31}, A_{41} and A_{42}. We have proved the following result, which is analogous to Proposition 2.2 of [10].

Proposition 2. *Let p be an odd prime. A self-dual code over $GR(p^3, r)$ can be induced from a self-dual code $\mathcal{C}_1$ over $\mathbb{F}_{p^r}$. There are $p^{rk(\frac{n}{2}-1)}$ self-dual codes over $GR(p^3, r)$ of length n corresponding to each subspace of $\mathcal{C}_1$ of dimension k, where $0 \leq k \leq \frac{n}{2}$.*

For the sake of completeness, we describe the matrices A_{31}, A_{41} and A_{42}. A_{31} is an arbitrary $k \times l$ matrix with entries from $\mathcal{T}_{p^r}$, A_{41} is determined by

$$f_{ij} + \widetilde{A_{30}A_{31}^t} + \widetilde{A_{40}A_{41}^t} \equiv 0 \pmod p, \tag{24}$$

while A_{42} is determined by

$$(h_{ij}) + \widetilde{A_{40}A_{42}^t} \equiv 0 \pmod p, \tag{25}$$

where

$$(f_{ij}) + \widetilde{A_{30}A_{31}^t} + \widetilde{A_{40}A_{41}^t} + p(A_{31}A_{31}^t + A_{41}A_{41}^t) = p(h_{ij}). \tag{26}$$

5. Mass Formula and Classification

Recall from Lemma 1 that $\sigma_{p^r}(n, k)$ is the number of self-orthogonal codes of even length n and dimension k over $\mathbb{F}_{p^r}$. Also, from Lemma 2, $\binom{n}{k}_{p^r}$ is the number of k-dimensional subspaces of an n-dimensional vector space over $\mathbb{F}_{p^r}$, where $0 \leq k \leq n$. The following theorem gives the mass formula for self-dual codes over $\mathrm{GR}(p^3, r)$.

Theorem 1. *Let p be an odd prime and let $N_{p^3,r}(n)$ denote the number of distinct self-dual codes of even length $n = 2m$ over $GR(p^3, r)$. Then*

$$N_{p^3,r}(n) = \sigma_{p^r}(n, m) \sum_{k=0}^{m} \binom{m}{k}_{p^r} p^{rk(n/2-1)}.$$

Proof. From Lemma 1, there are $\sigma_{p^r}(n, m)$ self-dual codes of length n over $\mathbb{F}_{p^r}$. Let $\mathcal{C}_1$ be one such self-dual code. Lemma 2 tells us that there are $\binom{m}{k}_{p^r}$ subspaces $\mathcal{C}_0 \subseteq \mathcal{C}_1$ of dimension k, where $0 \leq k \leq m$. Finally, from Proposition 2, there are $p^{rk(m-1)}$ self-dual codes over $\mathrm{GR}(p^3, r)$ corresponding to $\mathcal{C}_0$. The result immediately follows. □

When $r = 1$, Theorem 1 coincides with the result in [10] for $\mathbb{Z}_{p^3}$.

We now give a classification of self-dual codes over $\mathrm{GR}(p^3, 2)$ of length 4 for $p = 3, 5$. Our goal is to find a representative for each equivalence classes of codes. In defining the equivalence of codes over $\mathrm{GR}(p^3, 2)$, we allow permutation of coordinates and (if necessary) multiplying certain coordinates by -1. All computations for this paper were done with the computer algebra package MAGMA [2].

5.1. Building-up

Using the construction method discussed in Section 4, a general way to construct self-dual codes over $\mathrm{GR}(p^3, 2)$ of length 4 can be described. Note that a self-dual code of length 4 over $\mathrm{GR}(p^3, 2)$ has one of the following three types: $\{0, 2, 2\}, \{1, 1, 1\}$ or $\{2, 0, 0\}$.

We start with a self-dual code $\mathcal{C}^{[4]_p}$ over $\mathbb{F}_{p^2}$ of length 4 with generator matrix $[I_2\ A]$, where A is a 2×2 matrix over $\mathbb{F}_{p^2}$ and $AA^t \equiv -I_2 \pmod{p}$. Let $\mathcal{C}^{[4,k]_p}$ be a self-dual code over $\mathrm{GR}(p^3, 2)$ of length 4 and type $\{k, l, l\}$ induced from $\mathcal{C}^{[4]_p}$, where $k = 0, 1, 2$ and $l = 2 - k$.

For $\alpha \in \mathbb{F}_{p^r}$, we denote by $\widehat{\alpha}$ the element in $\mathcal{T}_{p^r}$ such that $\overline{\widehat{\alpha}} = \alpha$. Given a matrix $M = (\alpha_{ij})$ over $\mathbb{F}_{p^r}$, we denote by $\widehat{M}$ the matrix $(\widehat{\alpha}_{ij})$ over $\mathcal{T}_{p^r}$.

Proposition 3. *$\mathcal{C}^{[4,0]_p}$ has generator matrix* $\mathfrak{m}_p(\widehat{A}) = \begin{bmatrix} pI_2 & p\widehat{A} \\ 0 & p^2 I_2 \end{bmatrix}$.

Proof. This immediately follows from the construction method discussed in Section 4, where we take $k = 0$ and $l = 2$. □

We now describe the generator matrix of $\mathcal{C}^{[4,1]_p}$. Let $a_1 \in \mathbb{F}_{p^2}$. By adding a_1 times the second row of the matrix $[I_2\ A]$ to its first row, and permuting the last two columns whenever necessary so that the (1,4) entry is nonzero, we obtain a matrix over $\mathbb{F}_{p^2}$ of the form

$$G = \begin{bmatrix} 1 & a_1 & b_1 & c_1 \\ 0 & 1 & d_1 & e_1 \end{bmatrix},$$

where $a_1, b_1, c_1, d_1, e_1 \in \mathbb{F}_{p^r}$ and $c_1 \neq 0$. The code $\mathcal{C}^{[4]_p}$ is equivalent to the code with generator matrix G. Let

$$\widehat{G} = \begin{bmatrix} 1 & a & b & c \\ 0 & 1 & d & e \end{bmatrix}.$$

Since c_1 is nonzero, then c is a nonzero element of $\mathcal{T}_{p^r}$. Thus, c is a unit of $\mathrm{GR}(p^3, 2)$.

Proposition 4. *$\mathcal{C}^{[4,1]_p}$ has generator matrix*

$$\mathfrak{m}_p(\widehat{G}, x) = \begin{bmatrix} 1 & a & b + px & c + py + p^2 z \\ 0 & p & pd & pe + p^2 q \\ 0 & 0 & p^2 & p^2 r \end{bmatrix},$$

where x is an arbitrary element of $\mathcal{T}_{p^r}$ and $y, z, q, r \in \mathcal{T}_{p^r}$ such that

$$\begin{aligned} y &\equiv -(2c)^{-1}(F + 2bx) \pmod{p} \\ z &\equiv -(2c)^{-1}H \pmod{p} \\ q &\equiv -c^{-1}(D + dx + ey) \pmod{p} \\ r &\equiv -c^{-1}b \pmod{p}, \end{aligned}$$

with

$$F = \tfrac{1}{p}(1 + a^2 + b^2 + c^2)$$

$$\begin{aligned} H &= \tfrac{1}{p}(F + 2bx + 2cy + px^2 + py^2) \\ D &= \tfrac{1}{p}(a + bd + ce) \end{aligned}$$

Proof. Let $A_2 = (a)$, $A_{30} = (b)$, $A_{40} = (c)$. From (20), we obtain

$$pF = (1 + a^2 + b^2 + c^2),$$

where $F = (f_{ij})$. The matrices $A_{31} = (x)$ and $A_{41} = (y)$ satisfy (24). Hence, we have

$$\begin{aligned} F + 2bx + 2cy &\equiv 0 \pmod p \\ y &\equiv -(2c)^{-1}(F + 2bx) \pmod p. \end{aligned}$$

Next, we obtain

$$pH = (F + 2bx + 2cy + px^2 + py^2)$$

from (26), where $H = (h_{ij})$. The matrix $A_{42} = (z)$ satisfies (25), which gives us

$$\begin{aligned} H + 2cz &\equiv 0 \pmod p \\ z &\equiv -(2c)^{-1}H \pmod p. \end{aligned}$$

Now, let $C_4 = (r)$. From (22), we have $r \equiv c^{-1}b \pmod p$. Finally, let $B_3 = (d)$, $B_{40} = (e)$ and $B_{41} = (q)$. We compute

$$pD = (a + bd + ce)$$

from (19). Then from (21), it follows that $q \equiv -c^{-1}(D + dx + ey) \pmod p$. □

We now describe the generator matrix of $\mathcal{C}^{[4,2]_p}$. We permute the columns of the matrix $[I_2\ A]$ whenever necessary, so that the (1,1) entry of A is nonzero. We write

$$[I_2\ A] = \begin{bmatrix} 1 & 0 & s_1 & t_1 \\ 0 & 1 & u_1 & v_1 \end{bmatrix},$$

where $s_1, t_1, u_1, v_1 \in \mathbb{F}_{p^r}$ and $s_1 \neq 0$. Let

$$\widehat{A} = \begin{bmatrix} s & t \\ u & v \end{bmatrix}.$$

Since s_1 is nonzero, then s is a nonzero element of $\mathcal{T}_{p^2}$, and thus, is a unit of $\mathrm{GR}(p^3, 2)$. Also, since A has an inverse modulo p, then $\det A = s_1v_1 - t_1u_1 \neq 0$, which implies that $sv - tu \neq 0$ and $(sv - tu)/s = v - tus^{-1}$ has an inverse modulo p.

Proposition 5. *$\mathcal{C}^{[4,2]_p}$ has generator matrix*

$$\mathfrak{m}_p(\widehat{A}, y_{12}, z_{12}) = [I_2\ \widehat{A} + pY + p^2Z],$$

where y_{12} and z_{12} are arbitrary elements of $\mathcal{T}_{p^2}$ and $Y = (y_{ij})$ and $Z = (z_{ij})$ are matrices over $\mathcal{T}_{p^2}$ satisfying

$$\begin{aligned} F + \widetilde{\widehat{A}Y^t} &\equiv 0 \pmod{p} \\ H + \widetilde{\widehat{A}Z^t} &\equiv 0 \pmod{p}, \end{aligned}$$

with $F = \frac{1}{p}(I_2 + \widehat{A}\widehat{A}^t)$ and $H = \frac{1}{p}\big(F + \widetilde{\widehat{A}Y^t} + pYY^t\big)$.

Proof. Let $A_{40} = \widehat{A}$. From (20), we compute

$$pF = I_2 + \widehat{A}\widehat{A}^t,$$

where $F = (f_{ij})$. Note that F is a symmetric matrix. The matrix $A_{41} = Y = (y_{ij})$, with entries from $\mathcal{T}_{p^2}$, satisfies (24). We then have $F + \widetilde{\widehat{A}Y^t} \equiv 0 \pmod{p}$, that is,

$$\begin{bmatrix} f_{11} & f_{12} \\ f_{12} & f_{22} \end{bmatrix} + \begin{bmatrix} s & t \\ u & v \end{bmatrix} \begin{bmatrix} y_{11} & y_{21} \\ y_{12} & y_{22} \end{bmatrix} + \begin{bmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{bmatrix} \begin{bmatrix} s & u \\ t & v \end{bmatrix} \equiv 0 \pmod{p}.$$

Hence Y satisfies

$$\begin{aligned} f_{11} + 2sy_{11} + 2ty_{12} &\equiv 0 \pmod{p} \\ f_{22} + 2uy_{21} + 2vy_{22} &\equiv 0 \pmod{p} \\ f_{12} + sy_{21} + ty_{22} + uy_{11} + vy_{12} &\equiv 0 \pmod{p} \end{aligned}$$

Observe that y_{11}, y_{21} and y_{22} can each be expressed in terms of y_{12}. Thus y_{11}, y_{21} and y_{22} are determined by $\widehat{A}$ and y_{12}.

Next we compute

$$pH = F + \widetilde{\widehat{A}Y^t} + pYY^t$$

from (26), where $H = (h_{ij})$. The matrix $A_{42} = Z = (z_{ij})$, with entries from $\mathcal{T}_{p^2}$, satisfies (25). Hence Z satisfies $H + \widetilde{\widehat{A}Z^t} \equiv 0 \pmod{p}$, that is,

$$\begin{bmatrix} h_{11} & h_{12} \\ h_{12} & h_{22} \end{bmatrix} + \begin{bmatrix} s & t \\ u & v \end{bmatrix} \begin{bmatrix} z_{11} & z_{21} \\ z_{12} & z_{22} \end{bmatrix} + \begin{bmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{bmatrix} \begin{bmatrix} s & u \\ t & v \end{bmatrix} \equiv 0 \pmod{p}.$$

Using a similar argument as earlier, we see that z_{11}, z_{21} and z_{22} are determined by $\widehat{A}$ and z_{12}. □

5.2. Self-dual codes over GR$(27, 2)$

We consider $\mathrm{GR}(27,2) = \mathbb{Z}_{27}[\omega]$, where $\omega^2 + 5\omega + 26 = 0$ and $\omega^8 = 1$, and $\mathbb{F}_9 = \mathbb{Z}_3[\bar{\omega}]$, where $\bar{\omega}^2 + 2\omega + 2 = 0$ and $\bar{\omega}^8 = 1$.

From [4], there exist two inequivalent self-dual codes of length 4 over $\mathbb{F}_9$: $\mathcal{C}_1^{[4]_3}$ and $\mathcal{C}_2^{[4]_3}$ with generator matrices

$$[I_2\ A_{3,1}] = \begin{bmatrix} 1 & 0 & \bar{\omega}^2 & 0 \\ 0 & 1 & 0 & \bar{\omega}^2 \end{bmatrix} \text{ and } [I_2\ A_{3,2}] = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & \bar{\omega}^4 & 1 \end{bmatrix},$$

respectively. The matrices

$$G_{3,1,0} = \begin{bmatrix} 1 & 0 & 0 & \bar{\omega}^2 \\ 0 & 1 & \bar{\omega}^2 & 0 \end{bmatrix},\ G_{3,1,1} = \begin{bmatrix} 1 & 1 & \bar{\omega}^2 & \bar{\omega}^2 \\ 0 & 1 & 0 & \bar{\omega}^2 \end{bmatrix} \text{ and } G_{3,1,\bar{\omega}} = \begin{bmatrix} 1 & \bar{\omega} & \bar{\omega}^2 & \bar{\omega}^3 \\ 0 & 1 & 0 & \bar{\omega}^2 \end{bmatrix}$$

generate codes which are equivalent to $\mathcal{C}_1^{[4]_3}$, while the matrices

$$G_{3,2,0} = [I_2\ A_{3,2}] \text{ and } G_{3,2,\bar{\omega}} = \begin{bmatrix} 1 & \bar{\omega} & \bar{\omega}^3 & \bar{\omega}^2 \\ 0 & 1 & \bar{\omega}^4 & 1 \end{bmatrix}$$

generate codes which are equivalent to $\mathcal{C}_2^{[4]_3}$.

Table 1: Self-dual Codes of Length 4 over $\mathrm{GR}(27,2)$.

Type	Generator Matrix	No. of Codes	$\lvert\mathrm{Aut}(\mathcal{C})\rvert$
$\{0,2,2\}$	$\mathfrak{m}_3(\widehat{A}_{3,1})$	1	32
	$\mathfrak{m}_3(\widehat{A}_{3,2})$	1	48
$\{1,1,1\}$	$\mathfrak{m}_3(\widehat{G}_{3,1,0},0)$	1	16
	$\mathfrak{m}_3(\widehat{G}_{3,1,1},0)$, $\mathfrak{m}_3(\widehat{G}_{3,1,\bar{\omega}},0)$, $\mathfrak{m}_3(\widehat{G}_{3,2,\bar{\omega}},0)$	3	8
	$\mathfrak{m}_3(\widehat{G}_{3,1,0},x)$, where $x\in\{1,\omega\}$ $\mathfrak{m}_3(\widehat{G}_{3,1,1},x)$, where $x\in\{1,\omega,\omega^2,\omega^3\}$ $\mathfrak{m}_3(\widehat{G}_{3,2,0},0)$, $\mathfrak{m}_3(\widehat{G}_{3,2,\bar{\omega}},x)$, where $x\in\{1,\omega^2,\omega^3,\omega^5\}$	11	4
	$\mathfrak{m}_3(\widehat{G}_{3,1,\bar{\omega}},x)$, where $x\in\{1,\omega\}$, $\mathfrak{m}_3(\widehat{G}_{3,2,0},\omega)$	3	2
$\{2,0,0\}$	$\mathfrak{m}_3(\widehat{A}_{3,1},0,0)$	1	32
	$\mathfrak{m}_3(\widehat{A}_{3,2},0,0)$	1	16
	$\mathfrak{m}_3(\widehat{A}_{3,1},0,z)$, where $z\in\{1,\omega\}$ $\mathfrak{m}_3(\widehat{A}_{3,1},1,z)$, where $z\in\{0,1,\omega,\ldots,\omega^7\}$ $\mathfrak{m}_3(\widehat{A}_{3,1},\omega,z)$, where $z\in\{0,1,\omega,\ldots,\omega^7\}$ $\mathfrak{m}_3(\widehat{A}_{3,2},0,z)$, where $z\in\{1,\omega,\omega^2,\omega^3\}$ $\mathfrak{m}_3(\widehat{A}_{3,2},\omega,z)$, where $z\in\{0,1,\omega,\ldots,\omega^7\}$	33	8

In Table 1, we give the list of inequivalent self-dual codes over $\mathrm{GR}(27,2)$ of length 4. Using the mass formula in Theorem 1, we make the following computations, confirming that Table 1 gives a complete classification.

$$N_{27,2}(4) = \sigma_9(4,2)\sum_{k=0}^{2}\binom{2}{k}_9 3^{2k} = 20+1800+1620 = \sum_{\mathcal{C}} \frac{2^4\cdot 4!}{\lvert\mathrm{Aut}(\mathcal{C})\rvert}.$$

Hence there are 55 self-dual codes of length 4 over $\mathrm{GR}(27,2)$.

5.3. Self-dual codes over GR$(125,2)$

We consider $\mathrm{GR}(125,2) = \mathbb{Z}_{125}[\omega]$, where $\omega^2 + 89\omega + 57 = 0$ and $\omega^{24} = 1$, and $\mathbb{F}_{25} = \mathbb{Z}_5[\bar{\omega}]$, where $\bar{\omega}^2 + 4\omega + 2 = 0$ and $\bar{\omega}^{24} = 1$.

From [4], there exist three inequivalent self-dual codes of length 4 over $\mathbb{F}_{25}$: $\mathcal{C}_1^{[4]_5}$, $\mathcal{C}_2^{[4]_5}$ and $\mathcal{C}_3^{[4]_5}$ with generator matrices $[I_2\ A_{5,1}], [I_2\ A_{5,2}]$ and $[I_2\ A_{5,3}]$ respectively, where

$$A_{5,1} = \begin{bmatrix} \bar{\omega}^6 & 0 \\ 0 & \bar{\omega}^6 \end{bmatrix},\ A_{5,2} = \begin{bmatrix} \bar{\omega}^8 & \bar{\omega}^4 \\ \bar{\omega}^{16} & \bar{\omega}^8 \end{bmatrix} \text{ and } A_{5,3} = \begin{bmatrix} 1 & \bar{\omega}^{21} \\ \bar{\omega}^9 & 1 \end{bmatrix},$$

respectively. $\mathcal{C}_1^{[4]_5}$ is equivalent to codes with generator matrices

$$G_{5,1,0} = \begin{bmatrix} 1 & 0 & 0 & \bar{\omega}^6 \\ 0 & 1 & \bar{\omega}^6 & 1 \end{bmatrix},\ G_{5,1,1} = \begin{bmatrix} 1 & 1 & \bar{\omega}^6 & \bar{\omega}^6 \\ 0 & 1 & 0 & \bar{\omega}^6 \end{bmatrix},\ G_{5,1,\bar{\omega}} = \begin{bmatrix} 1 & \bar{\omega} & \bar{\omega}^6 & \bar{\omega}^7 \\ 0 & 1 & 0 & \bar{\omega}^6 \end{bmatrix},$$

$$G_{5,1,\bar{\omega}^2} = \begin{bmatrix} 1 & \bar{\omega}^2 & \bar{\omega}^6 & \bar{\omega}^8 \\ 0 & 1 & 0 & \bar{\omega}^6 \end{bmatrix} \text{ and } G_{5,1,\bar{\omega}^3} = \begin{bmatrix} 1 & \bar{\omega}^3 & \bar{\omega}^6 & \bar{\omega}^9 \\ 0 & 1 & 0 & \bar{\omega}^6 \end{bmatrix},$$

$\mathcal{C}_2^{[4]_5}$ is equivalent to codes with generator matrices

$$G_{5,2,0} = [I_2\ A_{5,2}],\ G_{5,2,1} = \begin{bmatrix} 1 & 1 & \bar{\omega}^{12} & \bar{\omega}^3 \\ 0 & 1 & \bar{\omega}^{16} & \bar{\omega}^8 \end{bmatrix},$$

$$G_{5,2,\bar{\omega}} = \begin{bmatrix} 1 & \bar{\omega} & \bar{\omega}^{19} & \bar{\omega}^{18} \\ 0 & 1 & \bar{\omega}^{16} & \bar{\omega}^8 \end{bmatrix} \text{ and } G_{5,2,\bar{\omega}^2} = \begin{bmatrix} 1 & \bar{\omega}^2 & \bar{\omega}^{21} & \bar{\omega}^{22} \\ 0 & 1 & \bar{\omega}^{16} & \bar{\omega}^8 \end{bmatrix},$$

while $\mathcal{C}_3^{[4]_5}$ is equivalent to codes with generator matrices

$$G_{5,3,0} = [I_2\ A_{5,3}],\ G_{5,3,1} = \begin{bmatrix} 1 & 1 & \bar{\omega}^{11} & \bar{\omega}^7 \\ 0 & 1 & \bar{\omega}^9 & 1 \end{bmatrix},\ G_{5,3,\bar{\omega}^2} = \begin{bmatrix} 1 & \bar{\omega}^2 & \bar{\omega}^{16} & \bar{\omega}^{11} \\ 0 & 1 & \bar{\omega}^9 & 1 \end{bmatrix},$$

$$G_{5,3,\bar{\omega}^6} = \begin{bmatrix} 1 & \bar{\omega}^6 & \bar{\omega}^2 & \bar{\omega}^8 \\ 0 & 1 & \bar{\omega}^9 & 1 \end{bmatrix} \text{ and } G_{5,3,\bar{\omega}^{15}} = \begin{bmatrix} 1 & \bar{\omega}^{15} & \bar{\omega}^6 & \bar{\omega}^9 \\ 0 & 1 & \bar{\omega}^9 & 1 \end{bmatrix}.$$

Let J_1 and J_2 be subsets of $\mathcal{T}_{25}$, with

$$\begin{aligned} J_1 &= \{0, 1, \omega, \omega^2, \omega^4, \omega^5, \omega^7, \omega^9, \omega^{10}, \omega^{11}, \omega^{13}, \omega^{17}\} \\ J_2 &= \{0, 1, \omega, \omega^2, \omega^4, \omega^5, \omega^6, \omega^7, \omega^{10}, \omega^{11}, \omega^{15}, \omega^{16}\}. \end{aligned}$$

Table 2 gives the list of inequivalent self-dual codes over $\mathrm{GR}(125,2)$ of length 4.

Using the mass formula in Theorem 1, we make the following computations, confirming that Table 2 gives a complete classification.

$$N_{125,2}(4) = \sigma_{25}(4,2) \sum_{k=0}^{2} \binom{2}{k}_{25} 5^{2k} = 52 + 33800 + 32500 = \sum_{\mathcal{C}} \frac{2^4 \cdot 4!}{|\mathrm{Aut}(\mathcal{C})|}.$$

Hence there are 904 self-dual codes of length 4 over $\mathrm{GR}(125,2)$.

Table 2: Self-dual Codes of Length 4 over $\mathrm{GR}(125, 2)$.

Type	Generator Matrix	No. of Codes	$\lvert\mathrm{Aut}(\mathcal{C})\rvert$
{0,2,2}	$\mathfrak{m}_5(\widehat{A}_{5,1})$	1	32
	$\mathfrak{m}_5(\widehat{A}_{5,2})$	1	24
	$\mathfrak{m}_5(\widehat{A}_{5,3})$	1	16
{1,1,1}	$\mathfrak{m}_5(\widehat{G}_{5,1,0}, 0)$	1	16
	$\mathfrak{m}_5(\widehat{G}_{5,1,1}, 0)$, $\mathfrak{m}_5(\widehat{G}_{5,1,\bar{\omega}^3}, 0)$, $\mathfrak{m}_5(\widehat{G}_{5,3,\bar{\omega}^{15}}, 0)$	3	8
	$\mathfrak{m}_5(\widehat{G}_{5,2,0}, 0)$, $\mathfrak{m}_5(\widehat{G}_{5,2,1}, 0)$	2	6
	$\mathfrak{m}_5(\widehat{G}_{5,1,\bar{\omega}}, 0)$, $\mathfrak{m}_5(\widehat{G}_{5,1,\bar{\omega}^2}, 0)$,$\mathfrak{m}_5(\widehat{G}_{5,3,0}, 0)$, $\mathfrak{m}_5(\widehat{G}_{5,1,0}, x)$, where $x \in \{1, \omega, \dots, \omega^5\}$, $\mathfrak{m}_5(\widehat{G}_{5,1,1}, x)$, where $x \in \{1, \omega, \dots, \omega^{11}\}$, $\mathfrak{m}_5(\widehat{G}_{5,2,\bar{\omega}}, x)$, where $x \in \{0, 1, \omega, \dots, \omega^{23}\}$, $\mathfrak{m}_5(\widehat{G}_{5,3,\bar{\omega}^6}, x)$, where $x \in \{0, 1, \omega, \dots, \omega^{23}\}$, $\mathfrak{m}_5(\widehat{G}_{5,3,\bar{\omega}^{15}}, x)$, where $x \in \{1, \omega, \dots, \omega^{11}\}$	83	4
	$\mathfrak{m}_5(\widehat{G}_{5,1,\bar{\omega}}, x)$, where $x \in \{1, \omega, \dots, \omega^{11}\}$ $\mathfrak{m}_5(\widehat{G}_{5,1,\bar{\omega}^2}, x)$, where $x \in \{1, \omega, \dots, \omega^{11}\}$ $\mathfrak{m}_5(\widehat{G}_{5,1,\bar{\omega}^3}, x)$, where $x \in \{1, \omega, \dots, \omega^5\}$ $\mathfrak{m}_5(\widehat{G}_{5,2,0}, x)$, where $x \in \{1, \omega, \dots, \omega^7\}$ $\mathfrak{m}_5(\widehat{G}_{5,2,1}, x)$, where $x \in \{1, \omega, \dots, \omega^7\}$ $\mathfrak{m}_5(\widehat{G}_{5,2,\bar{\omega}^2}, x)$, where $x \in \{0, 1, \omega, \dots, \omega^{23}\}$ $\mathfrak{m}_5(\widehat{G}_{5,3,0}, x)$, where $x \in \{1, \omega, \dots, \omega^{11}\}$ $\mathfrak{m}_5(\widehat{G}_{5,3,1}, x)$, where $x \in \{0, 1, \omega, \dots, \omega^{23}\}$ $\mathfrak{m}_5(\widehat{G}_{5,3,\bar{\omega}^2}, x)$, where $x \in \{0, 1, \omega, \dots, \omega^{23}\}$	133	2
{2,0,0}	$\mathfrak{m}_5(\widehat{A}_{5,1}, 0, 0)$	1	32
	$\mathfrak{m}_5(\widehat{A}_{5,2}, 0, 0)$	1	24
	$\mathfrak{m}_5(\widehat{A}_{5,3}, \omega^{21}, \omega^3)$	1	16
	$\mathfrak{m}_5(\widehat{A}_{5,1}, 0, z)$, where $z \in \{1, \omega, \dots, \omega^5\}$ $\mathfrak{m}_5(\widehat{A}_{5,1}, y, z)$, where $y \in \{1, \omega, \dots, \omega^5\}, z \in \mathcal{T}_{25}$ $\mathfrak{m}_5(\widehat{A}_{5,2}, 0, z)$, where $z \in \{1, \omega, \dots, \omega^7\}$ $\mathfrak{m}_5(\widehat{A}_{5,2}, y, z)$, where $y \in \{1, \omega, \dots, \omega^7\}, z \in \mathcal{T}_{25}$ $\mathfrak{m}_5(\widehat{A}_{5,3}, y, z)$, where $y \in J_1$, $z \in \mathcal{T}_{25}$, $\mathfrak{m}_5(\widehat{A}_{5,3}, \omega^{21}, z)$, where $z \in J_2$	676	8

6. Conclusion

We discussed a method to construct self-dual codes over $\mathrm{GR}(p^3, r)$ from a self-dual code over $\mathbb{F}_{p^r}$, where p is an odd prime and r is a positive integer. This construction method led to a mass formula and classification of self-dual codes of length 4 over $\mathrm{GR}(p^3, 2)$ for $p = 3, 5$.

In this study, we only dealt with the case when p is an odd prime. Letting $p = 2$ in

(24), we obtain

$$f_{ij} + \widetilde{A_{30}A_{31}^t} + \widetilde{A_{40}A_{41}^t} \equiv 0 \pmod 2.$$

Since the diagonal entries of $\widetilde{X}$ are all 0, then we must have $f_{ii} \equiv 0 \pmod 2$ for each i. Hence, from (20), the diagonal entries of $I_k + A_2A_2^t + A_{30}A_{30}^t + A_{40}A_{40}^t = 2(f_{ij})$ must be doubly even.

Thus, in the case of $p = 2$, the construction algorithm becomes more complicated because we need an additional property for the self-dual codes over $\mathbb{F}_{2^r}$. We are still investigating the mass formula for self-dual codes over $\mathrm{GR}(8, r)$.

Acknowledgements

This research is funded by the Department of Science and Technology - Accelerated Science and Technology Human Resource Development Program (DOST-ASTHRDP).

References

[1] JM Balmaceda, RA Betty, and F Nemenzo. Mass formula for self-dual codes over $\mathbb{Z}_{p^2}$. *Discrete Math.*, 308:2984–3002, 2008.

[2] W Bosma, J Cannon, and C Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] W-H Choi. Mass formula for self-dual codes over Galois rings $\mathrm{GR}(p^2, 2)$. *Korean J. Math.*, 24 (4):751–764, 2016.

[4] W-H Choi. The classification of self-dual codes over Galois rings of length 4. *Bulletin of the Korean Mathematical Society*, 55:1371–1387, 2018.

[5] P Gaborit. Mass formulas for self-dual codes over $\mathbb{Z}_4$ and $\mathbb{F}_q + u\mathbb{F}_q$ rings. *IEEE Trans. Inform. Theory*, 42:1222–1228, 1996.

[6] AR Hammons, PV Kumar, AR Calderbank, NJA Sloane, and P Solé. The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Trans. Inform. Theory*, 40 (2):301–319, 1994.

[7] WC Huffman and V Pless. *Fundamentals of Error-Correcting Codes.* Cambridge University Press, United Kingdom, 2004.

[8] BR McDonald. *Finite Rings with Identity.* Marcel Dekker, Inc., New York, 1974.

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

[10] K Nagata, F Nemenzo, and H Wada. The number of self-dual codes over $\mathbb{Z}_{p^3}$. *Des. Codes Cryptogr.*, 50:291–303, 2009.

[11] K Nagata, F Nemenzo, and H Wada. Mass formula and structure of self-dual codes over $\mathbb{Z}_{2^s}$. *Des. Codes Cryptogr.*, 67:293–316, 2013.

[12] GH Norton and A Sălăgean. On the structure of linear and cyclic codes over a finite chain ring. *AAECC*, 10(3):489–506, 2000.

[13] YH Park. The classification of self-dual modular codes. *Finite Fields and Their Applications*, 17:442–460, 2011.

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

[15] JH van Lint and RM Wilson. *A Course in Combinatorics.* Cambridge University Press, United Kingdom, 1993.

[16] Z-X Wan. *Finite Fields and Galois Rings.* World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2012.