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

Trilbe Lizann E. Vasquez\(^1,\ast\), 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 \( GR(p^3, r) \) be the Galois ring of 
characteristic \( p^3 \) and cardinality \( p^{3r} \). In this paper, we investigate the self-dual codes over \( GR(p^3, r) \) 
and give a method to construct self-dual codes over this ring. We establish a mass formula for 
self-dual codes over \( GR(p^3, r) \) and classify self-dual codes over \( GR(p^3, 2) \) 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 representa-
tive 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 \( GR(p^e, r) \), 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
for self-dual codes over $\text{GR}(p^2, 2)$ for odd primes $p$ is obtained in [3]. Moreover, self-dual codes of length 4 over $\text{GR}(p, 2)$ and $\text{GR}(p^2, 2)$ 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 $\text{GR}(p^3, r)$, 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 $\text{GR}(p^3, 2)$ for $p = 3, 5$.

2. Preliminaries

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

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

induces the following modulo $p$ reduction mapping between polynomial rings

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

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 $\bar{\omega} = x + \langle f(x) \rangle$ is a primitive $(p^r - 1)$st root of unity. The Galois ring $\text{GR}(p^e, r)$ of characteristic $p^e$ and cardinality $p^{er}$ is defined as

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

Every element of $\text{GR}(p^e, r)$ can be expressed uniquely in the $\omega$-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 $\text{GR}(p^e, 1) = \mathbb{Z}_{p^e}$ and $\text{GR}(p, r) = \mathbb{F}_{p^e}$, the Galois field of $p^e$ elements.

The modulo $p$ reduction can be naturally extended to

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

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

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

An element $a \in \text{GR}(p^e, r)$ 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 $C$ if the rows of $G$ generate all the elements of $C$ 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 $C^\perp$ of a code $C$ of length $n$ over $S$ consists of
all \( x \in S^n \) which are orthogonal to every codeword in \( C \). If \( C \subseteq C^\perp \), then \( C \) is said to be self-orthogonal. If \( C = C^\perp \), then \( C \) 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 \( C \) be a code of length \( n \) over the Galois ring GR\((p^e, r)\). \( C \) has a generator matrix which, after a suitable permutation of coordinates, can be written as

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

where \( I_{k_i} \) is the \( k_i \times k_i \) identity matrix and the \( A_{i,j} \)s are matrices of appropriate sizes over 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 \( C \) with generator matrix \( G \) as in (1) is said to be of type \( \{k_0, k_1, \ldots, k_{e-1} \} \) and has \( (p^e)^{\sum_{i=0}^{e-1} (e-i)k_i} \) codewords. The dual \( C^\perp \) of \( C \) is of type \( \{k_e, k_{e-1}, \ldots, k_1 \} \). It is known that \( |C||C^\perp| = p^{ern} \). If \( C \) 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

\[ \text{Tor}_i(C) = \{ \bar{v} : p^i \bar{v} \in C \} \]

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

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

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

Two codes over 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 \( C_1 \) and \( C_2 \) of length \( n \) over GR\((p^e, r)\) are equivalent if there exists a monomial matrix \( P \) such that \( C_2 = C_1P = \{cP : c \in C_1 \} \), where \( P \) has exactly one entry \( \pm 1 \) in every row and every column and all the other entries are zero. The automorphism group Aut\((C)\) of a code \( C \) of length \( n \) over GR\((p^e, r)\) is the group of all such matrices \( P \) such that \( C = CP \).
Let $E_n$ be the signed symmetric group of order $|E_n| = 2^n n!$. The number of codes equivalent to a code $C$ over $GR(p^3, r)$ of length $n$ is
\[ \frac{|E_n|}{|\text{Aut}(C)|} \]
and hence the number $N_{p^3, r}(n)$ of distinct self-dual codes over $GR(p^3, r)$ of length $n$ is
\[ N_{p^3, r}(n) = \sum C \frac{|E_n|}{|\text{Aut}(C)|} \]
where the sum runs through all inequivalent self-dual codes $C$ over $GR(p^3, r)$ 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 $GR(p^3, r)$ 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 $\text{char} \mathbb{F}_q \neq 2$, then
\[ \sigma_q(n, k) = \frac{(q^n - k - \epsilon q^{n/2} - k) \prod_{i=1}^{k-1} (q^{n-2i} - 1)}{\prod_{i=1}^k (q^i - 1)}, \quad k \geq 2 \]
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 $GR(p^3, r)$

Let $C$ be a code of length $n$ over $GR(p^3, r)$ and let $G$ be a generator matrix for $C$. We can write $G$ in the following form:
\[ G = \begin{bmatrix} A \\ pB \\ p^2C \end{bmatrix} = \begin{bmatrix} I_k & A_2 & A_3 & A_4 \\ 0 & pI_l & pB_3 & pB_4 \\ 0 & 0 & p^2I_m & p^2C_4 \end{bmatrix}, \tag{2} \]
where $I_r$ is the identity matrix of order $r$, and the other matrices have entries from $GR(p^3, r)$ and are described as follows. We write $A_3, B_4$ and $A_4$ in their $p$-adic expansions.
\[ A_3 = A_{30} + pA_{31}, \quad B_4 = B_{40} + pB_{41}, \quad A_4 = A_{40} + pA_{41} + p^2 A_{42}, \]
and the matrices \( A_2, \ B_3, \ C_4, \ A_{ij} \) and \( B_{ij} \) have entries from \( \mathbb{T}_p \). The columns are grouped in blocks of sizes \( k, l, m \) and \( h = n - (k + l + m) \). The code \( C \) is said to be of type \( \{k, l, m\} \) and has \( p^{r(3k+2l+m)} \) codewords. The dual code \( C^\perp \) is of type \( \{h, m, l\} \) and has \( p^{r(3h+2m+l)} \) codewords.

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

\[ T_0 = A \pmod{p} = \begin{bmatrix} I_k & \bar{A}_2 & \bar{A}_{30} & \bar{A}_{40} \end{bmatrix}, \]

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

\[ T_1 = \begin{bmatrix} A \\ B \end{bmatrix} \pmod{p} = \begin{bmatrix} I_k & \bar{A}_2 & \bar{A}_{30} & \bar{A}_{40} \\ 0 & I_l & \bar{B}_3 & \bar{B}_{40} \end{bmatrix}, \]

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

\[ T_2 = \begin{bmatrix} A \\ B \\ C \end{bmatrix} \pmod{p} = \begin{bmatrix} I_k & \bar{A}_2 & \bar{A}_{30} & \bar{A}_{40} \\ 0 & I_l & \bar{B}_3 & \bar{B}_{40} \\ 0 & 0 & I_m & \bar{C}_4 \end{bmatrix}. \]

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

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

\[ \begin{align*}
AA^t & \equiv 0 \pmod{p^3} \quad (6) \\
AB^t & \equiv 0 \pmod{p^2} \quad (7) \\
BB^t & \equiv 0 \pmod{p} \quad (8) \\
AC^t & \equiv 0 \pmod{p}. \quad (9)
\end{align*} \]

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

\[ \begin{align*}
AA^t & \equiv 0 \pmod{p^3} \\
pAB^t & \equiv 0 \pmod{p^3} \\
p^2 BB^t & \equiv 0 \pmod{p^3} \\
p^2 AC^t & \equiv 0 \pmod{p^3},
\end{align*} \]

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

Conversely, let \( C \) 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 \( C \) is a self-orthogonal code, i.e. \( C \subseteq C^\perp \). Moreover, since \( k = h \) and \( l = m \), we then have \( |C| = |C^\perp| \). Therefore \( C = C^\perp \).
Corollary 1. A self-dual code $C$ over $GR(p^3, r)$ of type $\{k, l, l\}$ is of even length $n = 2(k + l)$.

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

Proof. Suppose $C$ has generator matrix $G$ as in (2). Then the torsion codes $Res(C)$, $Tor_1(C)$ and $Tor_2(C)$ 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 $Res(C)$ is self-orthogonal.

From Conditions (9), (10) and (11) imply that $T_1T_1^t \equiv 0 \pmod{p}$, so that $Tor_1(C)$ is self-orthogonal. Since $C$ is self-dual, then dim $Tor_1(C) = k + l = \frac{n}{2}$. Thus $Tor_1(C)$ is self-dual.

From Conditions (9)-(11), it follows that $T_2T_0^t \equiv 0 \pmod{p}$, so $Tor_2(C) \subseteq Res(C) \perp$.

From Corollary 1, dim $Tor_2(C) = k + 2l = n - k = \text{dim } Res(C) \perp$. Consequently, $|Tor_2(C)| = |Res(C) \perp|$ and so $Tor_2(C) = (Res(C) \perp)$.

$\square$

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

We now use Proposition 1 to construct self-dual codes over $GR(p^3, r)$ with prescribed first torsion code. We start with a self-dual $[n, k + l]$ code $C_1$ over $\mathbb{F}_p$ with generator matrix

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

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 $C$ over $GR(p^3, r)$ such that $Tor_1(C) = C_1$.

Since $C_1$ is self-dual, then $G'G'^t \equiv 0 \pmod{p}$ and we obtain

$$I_k + A'_2A'_2^t + A'_{30}A'_{30}^t + A'_{40}A'_{40}^t \equiv 0 \pmod{p} \tag{12}$$
$$A'_2 + A'_{30}B'_3^t + A'_{40}B'_{40}^t \equiv 0 \pmod{p} \tag{13}$$
$$I_l + B'_3B'_3^t + B'_{40}B'_{40}^t \equiv 0 \pmod{p}. \tag{14}$$

Let $H = \begin{bmatrix} A'_{30} & A'_{40} \\ B'_3 & B'_{40} \end{bmatrix}$ and $J = \begin{bmatrix} I_k & -A'_2 \\ -A'_2^t & I_l + A'_2A'_2 \end{bmatrix}$. 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 \( C_0 \) be the \( k \)-dimensional subspace of \( C_1 \) with generator matrix

\[
A' = \begin{bmatrix} I_k & A_2' & A_{30}' & A_{40}' \end{bmatrix}.
\]

From (12) and (13), \( C_0 \) is a self-orthogonal code and \( C_0 \subseteq C_1 \subseteq C_0^\perp \). Now, the dual of \( C_0^\perp \) has dimension \( n - k = k + 2l \). Hence we can write the generator matrix of \( C_0^\perp \) 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 \( GR(p^e, r) \) satisfying conditions (6)-(9), which are equivalent to

\[
I_k + A_2 A_2' + A_3 A_3' + A_4 A_4' \equiv 0 \pmod{p^3} \tag{15}
\]

\[
A_2 + A_3 B_3' + A_4 B_4' \equiv 0 \pmod{p^2} \tag{16}
\]

\[
I_l + B_3 B_3' + B_4 B_4' \equiv 0 \pmod{p} \tag{17}
\]

\[
A_3 + A_4 C_4' \equiv 0 \pmod{p}. \tag{18}
\]

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: \( A_3 = A_{30} + p A_{31}, B_4 = B_{40} + p B_{41} \) and \( A_4 = A_{40} + p A_{41} + p^2 A_{42} \), where \( A_{31}, B_{41}, A_{41} \) and \( A_{42} \) have entries from \( T_{p^r} \).

Let \( A_2, A_{30}, A_{40}, B_3 \) and \( B_{40} \) be the matrices over \( T_{p^r} \) such that \( \overline{A}_2 = A_2', \overline{A}_{30} = A_{30}', \overline{A}_{40} = A_{40}', \overline{B}_3 = B_3', \overline{B}_{40} = B_{40}' \). From (12) and (13), there exist matrices \((f_{ij})\) and \( D \) with entries from \( GR(p^3, r) \) such that

\[
A_2 + A_{30} B_3' + A_{40} B_{40}' = pD \tag{19}
\]

and

\[
I_k + A_2 A_2' + A_{30} A_{30}' + A_{40} A_{40}' = p(f_{ij}). \tag{20}
\]

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

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

and

\[
C_4' \equiv -A_{40}^{-1} A_{30} \pmod{p}, \tag{22}
\]

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 \( C \) is self-dual if and only if

\[
f_{ij} + \overline{A}_{31} A_{31}' + A_{40} A_{40}' + p(A_{31} A_{31}' + A_{41} A_{41}' + A_{40} A_{40}') \equiv 0 \pmod{p^2} \tag{23}
\]

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 \( p^{\frac{rk(k-1)}{2}} \) 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 \( p^{\frac{rk(k-1)}{2}} \) 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 \( C_1 \) over \( \mathbb{F}_{p^r} \). There are \( p^{\frac{rk(k-1)}{2}} \) self-dual codes over \( GR(p^3, r) \) of length \( n \) corresponding to each subspace of \( C_1 \) 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 \( \mathbb{T}_{p^r} \), \( A_{41} \) is determined by

\[
    f_{ij} + \tilde{A}_{31}^t \tilde{A}_{31} + \tilde{A}_{41}^t \tilde{A}_{41} \equiv 0 \pmod{p},
\]

while \( A_{42} \) is determined by

\[
    (h_{ij}) + \tilde{A}_{42}^t \tilde{A}_{42} \equiv 0 \pmod{p},
\]

where

\[
    (f_{ij}) + \tilde{A}_{31}^t \tilde{A}_{31} + \tilde{A}_{41}^t \tilde{A}_{41} + (h_{ij}) + p(A_{31}A_{31}^t + A_{41}A_{41}^t) = p(h_{ij}).
\]

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, \( \binom{m}{k}_{p^r} \) 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 \( GR(p^3, r) \).

**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

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

**Proof.** From Lemma 1, there are \( \sigma_{p^r}(n, m) \) self-dual codes of length \( n \) over \( \mathbb{F}_{p^r} \). Let \( C_1 \) be one such self-dual code. Lemma 2 tells us that there are \( \binom{m}{k}_{p^r} \) subspaces \( C_0 \subseteq C_1 \) of dimension \( k \), where \( 0 \leq k \leq m \). Finally, from Proposition 2, there are \( p^{\frac{rk(m-1)}{2}} \) self-dual codes over \( GR(p^3, r) \) corresponding to \( C_0 \). The result immediately follows. \( \square \)

When \( r = 1 \), Theorem 1 coincides with the result in [10] for \( Z_{p^3} \).

We now give a classification of self-dual codes over \( GR(p^3, 2) \) of length 4 for \( p = 3, 5 \). Our goal is to find a representative for each equivalence class of codes. In defining the equivalence of codes over \( GR(p^3, 2) \), 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 GR($p^3, 2$) of length 4 can be described. Note that a self-dual code of length 4 over 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 $C_{[4]}$ over $F_{p^2}$ of length 4 with generator matrix $[I_2 \ A]$, where $A$ is a 2 × 2 matrix over $F_{p^2}$ and $AA^t \equiv -I_2 \pmod{p}$. Let $C_{[4,k]}$ be a self-dual code over GR($p^3, 2$) of length 4 and type $\{k, l, l\}$ induced from $C_{[4]}$, where $k = 0, 1, 2$ and $l = 2 - k$.

For $\alpha \in F_{p^r}$, we denote by $\hat{\alpha}$ the element in $T_{p^r}$ such that $\hat{\alpha} = \alpha$. Given a matrix $M = (\alpha_{ij})$ over $F_{p^r}$, we denote by $\hat{M}$ the matrix $(\hat{\alpha}_{ij})$ over $T_{p^r}$.

**Proposition 3.** $C_{[4,0]}$ has generator matrix $m_p(\hat{A}) = \begin{bmatrix} pI_2 & p\hat{A} \\ 0 & p^2I_2 \end{bmatrix}$.

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

We now describe the generator matrix of $C_{[4,1]}$. Let $a_1 \in F_{p^2}$. 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 $F_{p^2}$ of the form

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

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

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

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

**Proposition 4.** $C_{[4,1]}$ has generator matrix

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

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

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

with

$$F = \frac{1}{p}(1 + a^2 + b^2 + c^2).$$
\[ H = \frac{1}{p}(F + 2bx + 2cy + px^2 + py^2) \]
\[ D = \frac{1}{p}(a + bd + ce) \]

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
\[ F + 2bx + 2cy \equiv 0 \pmod{p}, \]
\[ y \equiv -(2c)^{-1}(F + 2bx) \pmod{p}. \]

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
\[ H + 2cz \equiv 0 \pmod{p}, \]
\[ z \equiv -(2c)^{-1}H \pmod{p}. \]

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 \( C_{[4,2]} \). 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 \( s_1, t_1, u_1, v_1 \in F_p \) and \( s_1 \neq 0 \). Let
\[ \hat{A} = \begin{bmatrix} s & t \\ u & v \end{bmatrix}. \]
Since \( s_1 \) is nonzero, then \( s \) is a nonzero element of \( T_{p^2} \), and thus, is a unit of \( \text{GR}(p^3, 2) \).
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. \( C_{[4,2]} \) has generator matrix
\[ m_p(\hat{A}, y_{12}, z_{12}) = [I_2 \hat{A} + pY + p^2Z], \]
where \( y_{12} \) and \( z_{12} \) are arbitrary elements of \( T_p^2 \) and \( Y = (y_{ij}) \) and \( Z = (z_{ij}) \) are matrices over \( T_p^2 \) satisfying

\[
F + \widetilde{\gamma} Y^t \equiv 0 \pmod{p} \\
H + \widetilde{\gamma} Z^t \equiv 0 \pmod{p},
\]

with \( F = \frac{1}{p}(I_2 + \hat{A}^\dagger) \) and \( H = \frac{1}{p}(F + \widetilde{\gamma} Y^t + pY Y^t) \).

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

\[
pF = I_2 + \hat{A}^\dagger,
\]

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

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

Hence \( Y \) satisfies

\[
\begin{align*}
f_{11} + 2s y_{11} + 2t y_{12} & \equiv 0 \pmod{p} \\
f_{22} + 2u y_{21} + 2v y_{22} & \equiv 0 \pmod{p} \\
f_{12} + s y_{21} + t y_{22} + u y_{11} + v y_{12} & \equiv 0 \pmod{p}
\end{align*}
\]

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 \( \hat{A} \) and \( y_{12} \).

Next we compute

\[
pH = F + \widetilde{\gamma} Y^t + pY Y^t
\]

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

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

Using a similar argument as earlier, we see that \( z_{11}, z_{21} \) and \( z_{22} \) are determined by \( \hat{A} \) and \( z_{12} \). \( \square \)

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

We consider \( GR(27, 2) = \mathbb{Z}_{27}[\omega] \), where \( \omega^2 + 5\omega + 26 = 0 \) and \( \omega^8 = 1 \), and \( F_9 = \mathbb{Z}_3[\bar{\omega}] \), where \( \bar{\omega}^2 + 2\bar{\omega} + 2 = 0 \) and \( \bar{\omega}^8 = 1 \).
From [4], there exist two inequivalent self-dual codes of length 4 over $\mathbb{F}_9$: $C_1^{[4]}$ and $C_2^{[4]}$ with generator matrices

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

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

respectively. The matrices

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

and

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

generate codes which are equivalent to $C_1^{[4]}$, while the matrices

$$G_{3,2,0} = [I_2 A_{3,2}]$$

and

$$G_{3,2,\omega} = \begin{bmatrix} 1 & \omega & \omega^3 & \omega^2 \\ 0 & 1 & \omega^4 & 1 \\ \end{bmatrix}$$

generate codes which are equivalent to $C_2^{[4]}$.

Table 1: Self-dual Codes of Length 4 over GR(27, 2).

| Type   | Generator Matrix | No. of Codes | $|\text{Aut}(C)|$ |
|--------|------------------|--------------|------------------|
| {0, 2, 2} | $m_3(3, 1)$ | 1 | 32 |
| | $m_3(3, 2)$ | 1 | 48 |
| {1, 1, 1} | $m_3(G_{3,1,0}, 0)$ | 1 | 16 |
| | $m_3(G_{3,1,1, 0})$, $m_3(G_{3,1,\omega, 0})$, $m_3(G_{3,2,\omega, 0})$ | 3 | 8 |
| | $m_3(G_{3,1,0}, x)$, where $x \in \{1, \omega\}$ | 11 | 4 |
| | $m_3(G_{3,1,1, x})$, where $x \in \{1, \omega, \omega^2, \omega^3\}$ | 3 | 2 |
| | $m_3(G_{3,2,0}, 0)$ | | |
| | $m_3(G_{3,2,\omega, x})$, where $x \in \{1, \omega^2, \omega^3, \omega^5\}$ | | |
| | $m_3(G_{3,1,\omega, x})$, where $x \in \{1, \omega\}$ | | |
| | $m_3(G_{3,2,0}, \omega)$ | | |
| {2, 0, 0} | $m_3(3, 1, 0, 0)$ | 1 | 32 |
| | $m_3(3, 2, 0, 0)$ | 1 | 16 |
| | $m_3(3, 1, 0, z)$, where $z \in \{1, \omega\}$ | 33 | 8 |
| | $m_3(3, 1, 1, z)$, where $z \in \{0, 1, \omega, \ldots, \omega^7\}$ | | |
| | $m_3(3, 1, \omega, z)$, where $z \in \{0, 1, \omega, \ldots, \omega^7\}$ | | |
| | $m_3(3, 2, 0, z)$, where $z \in \{1, \omega, \omega^2, \omega^3\}$ | | |
| | $m_3(3, 2, \omega, z)$, where $z \in \{0, 1, \omega, \ldots, \omega^7\}$ | | |

In Table 1, we give the list of inequivalent self-dual codes over 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.

$$N_{27,2}(4) = |\sigma_0(4, 2)| \sum_{k=0}^2 \binom{2}{k} \cdot 32^k = 20 + 1800 + 1620 = \sum_C \frac{2^4 \cdot 4!}{|\text{Aut}(C)|}.$$
Hence there are 55 self-dual codes of length 4 over GR(27, 2).

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

We consider GR(125, 2) = Z_{125}[\omega], where \omega^2 + 89\omega + 57 = 0 and \omega^{24} = 1, and \mathbb{F}_{25} = 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}_5: C_1^{[4]}, C_2^{[4]} and C_3^{[4]} with generator matrices [I_2 A_{5,1}], [I_2 A_{5,2}] and [I_2 A_{5,3}] respectively, where

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

respectively. C_1^{[4]} is equivalent to codes with generator matrices

\[ G_{5,1,0} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & \bar{\omega}^6 \\ 0 & \bar{\omega}^6 & 1 \end{bmatrix}, \quad G_{5,1,1} = \begin{bmatrix} 1 & 1 & \bar{\omega}^6 \\ 0 & 0 & \bar{\omega}^6 \\ \bar{\omega}^6 & \bar{\omega}^6 & 1 \end{bmatrix}, \quad G_{5,1,\omega} = \begin{bmatrix} 1 & \bar{\omega} & \bar{\omega}^6 \\ 0 & 1 & 0 \\ 0 & 0 & \bar{\omega}^6 \end{bmatrix}, \]

\[ G_{5,1,\omega^2} = \begin{bmatrix} 1 & \bar{\omega}^2 & \bar{\omega}^6 \\ 0 & 0 & \bar{\omega}^6 \\ \bar{\omega}^6 & \bar{\omega}^6 & 1 \end{bmatrix} \quad \text{and} \quad G_{5,1,\omega^3} = \begin{bmatrix} 1 & \bar{\omega}^3 & \bar{\omega}^6 \\ 0 & 0 & 0 \\ \bar{\omega}^6 & \bar{\omega}^6 & 0 \end{bmatrix}, \]

C_2^{[4]} is equivalent to codes with generator matrices

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

\[ G_{5,2,\omega} = \begin{bmatrix} 1 & \bar{\omega} & \bar{\omega}^{19} \\ 0 & 0 & \bar{\omega}^{16} \\ \bar{\omega}^{16} & \bar{\omega}^{16} & 1 \end{bmatrix} \quad \text{and} \quad G_{5,2,\omega^2} = \begin{bmatrix} 1 & \bar{\omega}^2 & \bar{\omega}^{21} \\ 0 & 0 & \bar{\omega}^{16} \\ \bar{\omega}^{16} & \bar{\omega}^{16} & 1 \end{bmatrix}, \]

while C_3^{[4]} is equivalent to codes with generator matrices

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

\[ G_{5,3,\omega^2} = \begin{bmatrix} 1 & \bar{\omega}^6 & \bar{\omega}^{10} \\ 0 & 0 & \bar{\omega}^{9} \\ \bar{\omega}^{9} & \bar{\omega}^{9} & 1 \end{bmatrix} \quad \text{and} \quad G_{5,3,\omega^3} = \begin{bmatrix} 1 & \bar{\omega}^{15} & \bar{\omega}^9 \\ 0 & 0 & \bar{\omega}^{9} \\ \bar{\omega}^{9} & \bar{\omega}^{9} & 1 \end{bmatrix}. \]

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

\[ J_1 = \{0, 1, \omega, \omega^2, \omega^4, \omega^5, \omega^7, \omega^9, \omega^{10}, \omega^{11}, \omega^{13}, \omega^{17}\} \]
\[ J_2 = \{0, 1, \omega, \omega^2, \omega^4, \omega^5, \omega^6, \omega^7, \omega^{10}, \omega^{11}, \omega^{15}, \omega^{16}\}. \]

Table 2 gives the list of inequivalent self-dual codes over 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.

\[ N_{125,2}(4) = 32 \sum_{k=0}^{2} \binom{2}{k} 5^{2k} = 52 + 33800 + 32500 = \sum_{c} \frac{2^4 \cdot 4!}{|\text{Aut}(C)|}. \]

Hence there are 904 self-dual codes of length 4 over GR(125, 2).
We discussed a method to construct self-dual codes over GR($p^3$, $r$) from a self-dual code over $\mathbb{F}_p$, 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 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
\[ f_{ij} + \tilde{A}_{30}A_{31} + \tilde{A}_{40}A_{41} = 0 \pmod{2}. \]
Since the diagonal entries of $\tilde{X}$ are all 0, then we must have $f_{ii} \equiv 0 \pmod{2}$ for each $i$. Hence, from (20), the diagonal entries of $I_k + A_2A_2' + A_3A_3' + A_4A_4' = 2(f_{ij})$ 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 $F_{2^r}$. We are still investigating the mass formula for self-dual codes over $GR(8, r)$.

Acknowledgements

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

References


