Enumeration of Self-Dual Codes of Length 6 over $\mathbb{Z}_p$

Whan-Hyuk Choi

Department of Mathematics, 1 Gangwondaehakgil, Kangwon National University, Chuncheon 24341, Korea; whchoi@kangwon.ac.kr

Received: 28 August 2019; Accepted: 20 September 2019; Published: 23 September 2019

Abstract: The purpose of this paper is to classify and enumerate self-dual codes of length 6 over finite field $\mathbb{Z}_p$. First, we classify these codes into three cases: decomposable, indecomposable non-MDS and MDS codes. Then, we complete the classification of non-MDS self-dual codes of length 6 over $\mathbb{Z}_p$ for all primes p in terms of their automorphism group. We obtain all inequivalent classes and find the necessary and sufficient conditions for the existence of each class. Finally, we obtain the number of MDS self-dual codes of length 6.

Keywords: self-dual codes; MDS codes; classification; automorphism group; mass formula

1. Introduction

The *classification problem* is one of the fundamental problems in various areas of mathematics. From the time self-dual codes began to attract attention amongst coding theorists, many papers have been published to classify binary self-dual codes [1–3] and non-binary self-dual codes [4–8]. While self-dual codes of moderate lengths are classified over a finite field $\mathbb{Z}_p$ for a *fixed* prime p in these papers, the first efforts are made in [9] to classify self-dual codes of the fixed length 4 over $\mathbb{Z}_p$ for all primes p . In [9], it is also shown that the classification of self-dual codes over $\mathbb{Z}_p$ for all primes p is essential to classify self-dual codes over integer ring $\mathbb{Z}_m$ for arbitrary m .

Let $N(n)$ be the number of all self-dual codes of length n and s be the number of equivalent classes. The main tool for the classification of self-dual codes is the *mass formula*:

$$\sum_{j=1}^s \frac{|\mathcal{M}^n|}{|Aut(\mathcal{C}_j)|} = N(n),$$

where $\mathcal{C}_j$ is a representative of each equivalent class and $\mathcal{M}^n$ is the group of γ -monomial transformations. Therefore, calculating the total number of codes and automorphisms of each equivalence class is critical for the classification of self-dual codes.

It is shown that self-dual codes of length 6 are classified simply into the following three cases by checking the number of zero elements of the standard generator matrix: decomposable case, indecomposable non-MDS case, and MDS case. For the decomposable codes, we need to understand the complete classification of self-dual codes of smaller lengths, which is already completed in [9]. For the indecomposable non-MDS codes, we complete the classification by computing the total number of bisorted standard generator matrices and orbits of each equivalent class. Consequently, with these results, we calculate the exact number of distinct MDS self-dual codes of length 6, so that we can obtain the mass formula for MDS codes.

This paper is organized as follows: first, we introduce some preliminaries to understand self-dual codes over $\mathbb{Z}_p$ in Section 2. In Section 3, we investigate self-dual codes of length 6 over $\mathbb{Z}_p$ and equivalence relations and automorphism groups in Section 4. Our main results are given in Section 5.

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

2. Preliminaries

Let p be a prime number and n be a positive integer. A linear code $\mathcal{C}$ of length n and dimension k over $\mathbb{Z}_p$ is a k -dimensional subspace of $\mathbb{Z}_p^n$. An element of $\mathcal{C}$ is called a *codeword*. A *generator matrix* of $\mathcal{C}$ is a matrix whose rows form a basis of $\mathcal{C}$. Thus, a generator matrix of a linear code $\mathcal{C}$ of length n and dimension k over $\mathbb{Z}_p$ is a $k \times n$ matrix over $\mathbb{Z}_p$. The space $\mathbb{Z}_p^n$ is equipped with the standard inner product, $\mathbf{u} \cdot \mathbf{v} = \sum_{i=1}^n u_i v_i$, where $\mathbf{u} = (u_i)$, $\mathbf{v} = (v_i)$. The *dual code* $\mathcal{C}^\perp$ is defined by

$$\mathcal{C}^\perp = \{\mathbf{u} \in \mathbb{Z}_p^n \mid \mathbf{u} \cdot \mathbf{v} = 0 \text{ for all } \mathbf{v} \in \mathcal{C}\}.$$

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

The *weight* of a codeword is the number of nonzero coordinates of the codeword. The *minimum distance* of $\mathcal{C}$, denoted by $d(\mathcal{C})$, is the smallest Hamming distance between distinct codewords. In determining the error-capability of $\mathcal{C}$, the minimum distance is the most important. For linear codes, the minimum distance equals the minimum weight of the non-zero codewords. It is well-known (see [10] for example) that a linear code of length n and dimension k satisfy the Singleton bound,

$$d(\mathcal{C}) \leq n - k + 1.$$

A code which achieves the equality in the Singleton bound is called *MDS* (*maximum distance separable*) code. Thus, a self-dual code of length $2n$ over $\mathbb{Z}_p$ is MDS if the minimum weight equals $n + 1$.

Let S_n be a group of permutation matrices of length n and $\mathbb{D}^n$ be a group of $n \times n$ diagonal matrices over $\mathbb{Z}_p$ with the diagonal elements γ_k , where $\gamma_k^2 = 1$ for $1 \leq k \leq n$; that is,

$$\mathbb{D}^n = \{\text{diag}(\gamma_i) \mid \gamma_i \in \mathbb{Z}_p, \gamma_i^2 = 1\}.$$

We denote by p_σ the $n \times n$ permutation matrix corresponding $\sigma \in S_n$ and the group of all γ -monomial transformations of length n , $\mathcal{M}^n$ is defined by

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

Since a monomial transformation does not preserve the self-duality in general, we only consider γ -monomial transformation in this paper (see [10], Thm 1.7.6). Two self-dual codes $\mathcal{C}$ and $\mathcal{C}'$ of length $2n$ are called *equivalent* and denoted by $\mathcal{C} \simeq \mathcal{C}'$ if there exists an element $\mu \in \mathcal{M}^{2n}$ such that $\mathcal{C}\mu = \mathcal{C}'$, where $\mathcal{C}\mu = \{\mathbf{u}\mu \mid \mathbf{u} \in \mathcal{C}\}$. An *automorphism* of $\mathcal{C}$ is an element $\mu \in \mathcal{M}^{2n}$ such that $\mathcal{C}\mu = \mathcal{C}$. The set of all automorphisms of $\mathcal{C}$ forms the *automorphism group* $\text{Aut}(\mathcal{C})$ as a subgroup of $\mathcal{M}^{2n}$.

Any element $\mu \in \mathcal{M}^{2n}$ has a unique representation $\mu = p_\sigma \gamma$ for $\gamma \in \mathbb{D}^{2n}$ and $\sigma \in S_{2n}$. Thus, we define groups $p(\mathcal{C}) = \{p_\sigma \mid p_\sigma \gamma \in \text{Aut}(\mathcal{C}) \text{ for some } \gamma \in \mathbb{D}^{2n}\}$ and $s(\mathcal{C}) = \text{Aut}(\mathcal{C}) \cap \mathbb{D}^{2n}$ which are called the *permutation parts* and *sign parts* of $\mathcal{C}$, respectively. Moreover, we denote a code $\mathcal{C}$ with a generator matrix G by $\mathcal{C} : G$ and $|\text{Aut}(\mathcal{C})|$ by $|s(\mathcal{C})| \cdot |p(\mathcal{C})|$. We usually abuse the notations and simply write γ as $(\gamma_1, \dots, \gamma_{2n})$ and p_σ as σ , if there is no confusion.

Let A^T denote the transpose of a matrix A . It is well-known that a self-dual code $\mathcal{C}$ of length $2n$ over $\mathbb{Z}_p$ is equivalent to a code with a standard generator matrix

$$\left(\begin{array}{c|c} I_n & A \end{array} \right), \quad (1)$$

where A is a $n \times n$ matrix satisfying $AA^T = -I_n$.

Definition 1. Let $\mathcal{C}_1, \mathcal{C}_2$ be self-dual codes of length $2n$ and $2m$ whose generator matrices are $(I_n \mid A_1)$ and $(I_m \mid A_2)$, respectively. We define the *direct sum of codes* (direct sum of matrices at the same time), $\mathcal{C}_1 \oplus \mathcal{C}_2$ with the direct sum of generator matrices,

$$(I_n \mid A_1) \oplus (I_n \mid A_2) = \left(\begin{array}{c|c|c|c} I_n & A_1 & O & O \\ \hline O & O & I_m & A_2 \end{array} \right).$$

A code is called decomposable if it is equivalent to a direct sum of two codes. If a code is not decomposable, it is called indecomposable.

The next proposition is derived directly from the previous definitions.

Proposition 1. Suppose that $\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2$ for some codes $\mathcal{C}_1$ and $\mathcal{C}_2$. Then,

$$\text{Aut}(\mathcal{C}) \supseteq \text{Aut}(\mathcal{C}_1) \oplus \text{Aut}(\mathcal{C}_2)$$

and

$$|s(\mathcal{C})| = 2 \times |s(\mathcal{C}_1)| \times |s(\mathcal{C}_2)|,$$

where $\text{Aut}(\mathcal{C}_1) \oplus \text{Aut}(\mathcal{C}_2) = \{\mu_1 \oplus \mu_2 \mid \mu_1 \in \text{Aut}(\mathcal{C}_1) \text{ and } \mu_2 \in \text{Aut}(\mathcal{C}_2)\}$.

Proposition 2. Let $\mathcal{C}$ be a self-dual code of length $2n$ over $\mathbb{Z}_p$ with a standard generator matrix $G = (I_n \mid A)$. Then,

$$A^T G = (A^T \mid -I_n)$$

is a generator matrix of $\mathcal{C}$.

Proof. Since $\mathcal{C}$ is self-dual, $AA^T = -I$ and $A^{-1} = -A^T$. Thus, A^T is non-singular. This implies that the rows of matrix $A^T G$ form a basis of the code $\mathcal{C}$ and $A^T G = (A^T I_n \mid A^T A) = (A^T \mid -I_n)$. $\square$

Corollary 1. Let $\mathbf{u} = (\mathbf{x}_n, \mathbf{y}_n)$ be a codeword of $\mathcal{C}$ with a standard generator matrix $G = (I_n \mid A)$, where $\mathbf{x}_n, \mathbf{y}_n \in \mathbb{Z}_p^n$. Then, $\mathbf{x}_n = \mathbf{0}$ if and only if $\mathbf{y}_n = \mathbf{0}$.

Proof. Suppose that $\mathbf{y}_n = \mathbf{0}$. By the self-orthogonality,

$$G\mathbf{u}^T = (I_n \mid A)(\mathbf{x}_n, \mathbf{0})^T = I_n \mathbf{x}_n^T = \mathbf{0}.$$

Thus, $\mathbf{x}_n = \mathbf{0}$. The other direction follows immediately in a similar way with the previous proposition. $\square$

Corollary 2. Let $G = (I_n \mid A)$ and $G' = (I_n \mid A^T)$ be generator matrices of self-dual codes $\mathcal{C}$ and $\mathcal{C}'$, respectively. Then, $\mathcal{C}$ and $\mathcal{C}'$ are equivalent.

Proof. Let $\tau = (1, n+1)(2, n+2) \cdots (n, 2n) \in S_{2n}$ and $\gamma = (\mathbf{1}_n, -\mathbf{1}_n) \in \mathbb{D}^{2n}$, where $\mathbf{1}_n$ denotes all one vector of length n . It is clear that $\mathcal{C}'$ is equal to $\mathcal{C}\tau\gamma$ by Proposition 2. $\square$

Definition 2. A matrix A is called bisorted if the rows and columns of A are sorted in a fixed order. If the submatrix A of a standard generator matrix $G = (I_n \mid A)$ of a self-dual code $\mathcal{C}$ of length $2n$ over $\mathbb{Z}_p$ is bisorted, we call G a bisorted generator matrix of $\mathcal{C}$.

Definition 3. A matrix A is called symmetric if $A^T = A$. If the submatrix A of a standard generator matrix $G = (I_n \mid A)$ of a self-dual code $\mathcal{C}$ of length $2n$ over $\mathbb{Z}_p$ is symmetric, we call G a symmetric generator matrix of $\mathcal{C}$.

Proposition 3. Let $G = (I_n \mid A)$ and $G' = (I_n \mid B)$ be generator matrices of self-dual codes $\mathcal{C}$ and $\mathcal{C}'$, respectively. If $A = \mu_1 B \mu_2$ for some $\mu_1, \mu_2 \in \mathcal{M}^n$, then $\mathcal{C}$ and $\mathcal{C}'$ are equivalent.

Proof. For $\mu = \mu_1^{-1} \oplus \mu_2 \in \mathcal{M}^{2n}$,

$$(I_n \mid A) = (I_n \mid \mu_1 B \mu_2) = (\mu_1^{-1} \mid B \mu_2) = (I_n \mid B) \mu.$$

Therefore, $\mathcal{C}$ and $\mathcal{C}'$ are equivalent. $\square$

This proposition implies the following corollary, which shows that the class of self-dual codes generated by bisorted generator matrices contain representatives of all inequivalent codes.

Corollary 3. *A self-dual code $\mathcal{C}$ of length $2n$ over $\mathbb{Z}_p$ is equivalent to a code with a bisorted generator matrix $(I_n \mid A)$.*

3. Self-Dual Codes of Length 6 over $\mathbb{Z}_p$

It is well known that, for $p \equiv 1 \pmod{4}$, a self-dual of length n over $\mathbb{Z}_p$ exists if and only if $n \equiv 0 \pmod{2}$, and, for $p \equiv 3 \pmod{4}$, a self-dual code of length n over $\mathbb{Z}_p$ exists if and only if $n \equiv 0 \pmod{4}$.

Theorem 1. *Let*

$$C : (I_3 \mid A)$$

be a self-dual code of length 6 over $\mathbb{Z}_p$. Then,

- (i) *$\mathcal{C}$ is decomposable if and only if A has at least two zero elements.*
- (ii) *$\mathcal{C}$ is indecomposable and non-MDS if and only if A has exactly one zero element.*
- (iii) *$\mathcal{C}$ is MDS if and only if A has no zero element.*

Proof. We are only to prove (i) and (iii), since (ii) is deduced directly from (i) and (iii).

Let the matrix $A = (a_{ij})$ for $1 \leq i, j \leq 3$ and $a_{ij} \in \mathbb{Z}_p$. We know that a_{ij} 's are solutions of the following simultaneous quadratic equations:

$$\begin{cases} 1 + a_{i1}^2 + a_{i2}^2 + a_{i3}^2 = 0 & \text{for all } i, \\ a_{i1}a_{j1} + a_{i2}a_{j2} + a_{i3}a_{j3} = 0 & \text{for } i \neq j. \end{cases} \quad (2)$$

Since $(I_3 \mid A^T)$ also generates a self-dual code, a_{ij} 's are solutions of the following simultaneous quadratic equations as well:

$$\begin{cases} 1 + a_{1i}^2 + a_{2i}^2 + a_{3i}^2 = 0 & \text{for all } i, \\ a_{1i}a_{1j} + a_{2i}a_{2j} + a_{3i}a_{3j} = 0 & \text{for } i \neq j. \end{cases} \quad (3)$$

Case (i). The 'only if' part follows from the definition of decomposable codes. For the 'if' part, suppose that there are two zero elements in A and these zero elements are in a row of A . We assume that $a_{11} = a_{12} = 0$ without loss of generality. Then, by Equation (2), we know that a_{13} is non-zero since

$$1 + a_{11}^2 + a_{12}^2 + a_{13}^2 = 1 + a_{13}^2 = 0.$$

This implies that $a_{23} = a_{33} = 0$ since

$$a_{11}a_{21} + a_{12}a_{22} + a_{13}a_{23} = a_{13}a_{23} = 0$$

and

$$a_{11}a_{31} + a_{12}a_{32} + a_{13}a_{33} = a_{13}a_{33} = 0.$$

Thus, $\mathcal{C}$ is decomposable. Suppose that the two zero elements are not in a row of A . Then, the two zero elements are in a column of A , or there is no row or column of A with the two zero elements. If two

zero elements are in a column of A , say $a_{11} = a_{21} = 0$. By following the same argument as above with Equation (3), we have that $a_{32} = a_{33} = 0$. This implies that $\mathcal{C}$ is decomposable. Lastly, suppose that there is no row or column of A with two zero elements. Without loss of generality, we can assume that $a_{11} = a_{22} = 0$. Then, Equation (2) implies that

$$a_{11}a_{21} + a_{12}a_{22} + a_{13}a_{23} = a_{13}a_{23} = 0.$$

This means that $a_{13} = 0$ or $a_{23} = 0$, which is contradictory to the assumption. In addition, this proves the case (i).

Case (iii). The ‘only if’ part follows from the definition of the MDS code. For the ‘if’ part, suppose that $\mathcal{C}$ is not an MDS code, i.e., there is a non-zero codeword $\mathbf{u} = (x_1, x_2, x_3, y_1, y_2, y_3) \in \mathcal{C}$ and $wt(\mathbf{u}) \leq 3$. By Corollary 1, we know that not all x_i ’s and not all y_i ’s are zero. In addition, we recall that $G = (I_3 | A)$ and $A^T G = (A^T | -I_3)$ are both generator matrices of $\mathcal{C}$ by Lemma 2. We note that $wt(\mathbf{u}) \neq 1$ since $\mathbf{u}$ is self-orthogonal. Assume that $wt(\mathbf{u}) = 2$. Then, exactly one x_i and one y_j are non-zero for some i, j where $1 \leq i, j \leq 3$. Say $x_1 \neq 0$ and $y_1 \neq 0$. Then, $a_{21} = 0$ since the inner product of the second row of G and $\mathbf{u}$ equals zero. Thus, A has at least one zero element. Now, assume that $wt(\mathbf{u}) = 3$. There are two cases: exactly two of x_1, x_2, x_3 are zero and exactly one of y_1, y_2, y_3 is zero or vice versa. Assume that $x_1 = x_2 = 0$ and $y_1 = 0$. Then, $a_{31} = 0$ since the inner product of the first row of $A^T G = (A^T | -I_3)$ and $\mathbf{u}$ equals zero. Thus, A has at least one zero element. Other cases are proved similarly and this proves case (iii). $\square$

This theorem does not hold for $n \geq 4$ since there exist non-MDS self-dual codes of length 8 over $\mathbb{Z}_5$ with

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 4 & 1 & 4 \\ 0 & 0 & 1 & 0 & 1 & 1 & 4 & 4 \\ 0 & 0 & 0 & 1 & 1 & 4 & 4 & 1 \end{pmatrix}.$$

Proposition 4. Let

$$G = (I_3 | A) = \begin{pmatrix} 1 & 0 & 0 & 0 & b & c \\ 0 & 1 & 0 & d & e & f \\ 0 & 0 & 1 & g & h & i \end{pmatrix}$$

be a generator matrix of an indecomposable non-MDS self-dual code $\mathcal{C}$ of length 6 over $\mathbb{Z}_p$. Ignoring the signs, all the elements of the matrix G are determined by b and d .

Proof. A matrix A is obtained from a solution of following simultaneous quadratic equations over $\mathbb{Z}_p$:

$$\begin{cases} b^2 + c^2 + 1 = 0, \\ d^2 + e^2 + f^2 + 1 = 0, \\ g^2 + h^2 + i^2 + 1 = 0, \\ be + cf = 0, \\ bh + ci = 0, \\ dg + eh + fi = 0. \end{cases}$$

We note that all variables are non-zero. The first equation determines c as $c^2 = -(1 + b^2)$ and, for the fourth and the fifth equations, we get $f = -bec^{-1}$ and $i = -bhc^{-1}$. From the other three equations, we get

$$\begin{cases} d^2 + e^2 + (bec^{-1})^2 + 1 = 0 \\ g^2 + h^2 + (bhc^{-1})^2 + 1 = 0 \\ dg + eh + (-bhc^{-1})(-bhc^{-1}) = 0 \end{cases} \Rightarrow \begin{cases} c^2d^2 + c^2e^2 + b^2e^2 + c^2 = 0 \\ c^2g^2 + c^2h^2 + b^2h^2 + c^2 = 0 \\ c^2dg + c^2eh + b^2eh = 0. \end{cases}$$

Since $b^2 + c^2 = -1$, we have that

$$\begin{cases} c^2d^2 - e^2 + c^2 = 0 \\ c^2g^2 - h^2 + c^2 = 0 \\ c^2dg - eh = 0 \end{cases} \Rightarrow \begin{cases} e^2 = c^2(1 + d^2) \\ h^2 = c^2(1 + g^2) \\ eh = c^2dg. \end{cases} \quad (4)$$

Equating these equations, we have

$$c^4d^2g^2 = e^2h^2 = c^2(1 + d^2)c^2(1 + g^2).$$

Thus, g is determined by d as

$$d^2g^2 = (1 + d^2)(1 + g^2) \Rightarrow g^2 = -1 - d^2.$$

Substitute g^2 with $g^2 = -1 - d^2$ and c^2 with $c^2 = -(1 + b^2)$ into the Equation (4), we get

$$\begin{cases} e^2 = -(1 + b^2)(1 + d^2), \\ h^2 = (1 + b^2)d^2. \end{cases}$$

Since $f = -bec^{-1}$ and $i = -bhc^{-1}$,

$$\begin{cases} f^2 = b^2e^2c^{-2} = b^2(1 + d^2), \\ i^2 = b^2h^2c^{-2} = b^2(1 + g^2) = -b^2d^2 \end{cases}$$

and this proves the theorem. $\square$

Corollary 4. Let j be a square root of -1 and C be an indecomposable non-MDS self-dual code of length 6 over $\mathbb{Z}_p$. Then, C is equivalent to one of the following:

$$C_{b,c,d,g} : \begin{pmatrix} 1 & 0 & 0 & 0 & b & c \\ 0 & 1 & 0 & d & cgj & -bgj \\ 0 & 0 & 1 & g & -cdj & bdj \end{pmatrix},$$

$$C'_{b,c,d,g} : \begin{pmatrix} 1 & 0 & 0 & 0 & b & c \\ 0 & 1 & 0 & d & -cgj & bgj \\ 0 & 0 & 1 & g & cdj & -bdj \end{pmatrix},$$

where $b^2 + c^2 = 1$ and $d^2 + g^2 = 1$.

Proof. By Proposition 3 and Theorem 1, we know that C is equivalent to a code with a generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & b & c \\ 0 & 1 & 0 & d & e & f \\ 0 & 0 & 1 & g & h & i \end{pmatrix}$$

by applying a suitable column and row permutations. By Proposition 4, it only needs to determine the signs of e, f, h and i . The result follows easily by the direct calculation. $\square$

We point out that $C_{b,c,d,g}$ and $C'_{b,c,d,g}$ are equivalent since $C_{b,c,d,g}\gamma = C'_{b,c,d,g}$ for $\gamma = (1, -1, -1, -1, 1, 1) \in \mathcal{M}^6$. In addition, $C_{b,c,d,g}$ and $C_{d,g,b,c}$ are equivalent by Corollary 2.

Moreover, $C_{b,c,d,g}$, $C_{c,b,d,g}$, $C_{b,c,g,d}$ and $C_{c,b,g,d}$ are all equivalent. We also note that we only need to investigate the bisorted generator matrices to classify self-dual codes of length 6 by Corollary 3.

Since every standard generator matrix $(I | A)$ of an indecomposable non-MDS self-dual code has exactly one zero element in A , we can assume that an indecomposable non-MDS self-dual code length 6 over $\mathbb{Z}_p$ has a generator matrix

$$(I | A) = \begin{pmatrix} 1 & 0 & 0 & 0 & b & c \\ 0 & 1 & 0 & d & e & f \\ 0 & 0 & 1 & g & h & i \end{pmatrix},$$

where A is a bisorted matrix with the order of $b \leq c, d \leq g$ regarding b, c, d and g as integers. Hence, we assume that a bisorted generator matrix of a non-MDS self-dual code of length 6 over $\mathbb{Z}_p$ follows the order defined as above.

The number of solutions of $x^2 + y^2 + 1 = 0$ plays an essential role in this paper. Thus, we give the number of solutions from [11] (Chapter 6) without a proof.

Lemma 1. Let $\mathbb{F}_q$ be a finite field with $q = p^r$ elements for an odd prime p . For non-zero $k \in \mathbb{F}_q$, the cardinality of the set

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

is given by

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

In addition, $|S_0| = 1$ for $q \equiv 3 \pmod{4}$ and $|S_0| = 2q - 1$ for $q \equiv 1 \pmod{4}$.

Proposition 5. Let $\mathcal{B}_0$ be a set of indecomposable non-MDS self-dual codes length 6 over $\mathbb{Z}_p$ with bisorted generator matrices in the form

$$\begin{pmatrix} 1 & 0 & 0 & 0 & b & c \\ 0 & 1 & 0 & d & e & f \\ 0 & 0 & 1 & g & h & i \end{pmatrix}.$$

Satisfying the order of $b \leq c, d \leq g$ regarding b, c, d and g as integers, then

$$|\mathcal{B}_0| = \begin{cases} \frac{(p-3)^2}{2}, & \text{if } p \equiv 1 \pmod{8}, \\ \frac{(p-5)^2}{2}, & \text{if } p \equiv 5 \pmod{8}. \end{cases}$$

Proof. Since four solutions $(0, \pm j), (\pm j, 0)$ are in S_{-1} , there are $p - 5$ elements $(\alpha, \beta) \in S_{-1}$ with non-zero α and β . If $\alpha \neq \beta$ for all $(\alpha, \beta) \in S_{-1}$, then there are $(\frac{p-5}{2})^2$ choices of (b, c) and (d, g) , where $b < c$ and $d < g$. It is well known that -2 is square if and only if $p \equiv 1, 3 \pmod{8}$. We recall that $p \equiv 1 \pmod{4}$. Therefore, there exist four elements of $(\pm\alpha, \pm\alpha)$ in S_{-1} if $p \equiv 1 \pmod{8}$. Exactly three among these four elements, $(\alpha, \alpha), (-\alpha, -\alpha)$ and one of $(\alpha, -\alpha)$ and $(-\alpha, \alpha)$ can be chosen as (b, c) and (d, g) satisfying the order condition. Thus, if $p \equiv 1 \pmod{8}$, there are $(\frac{p-9}{2} + 3)^2 = (\frac{p-3}{2})^2$ possible choices of (b, c) and (d, g) . Finally, we know that there exist two distinct matrices for one pair of (b, c) and (d, g) by the Corollary 4, and this completes the proof. $\square$

Next, we describe the orbits of $\mathcal{C}_{b,c,d,g}$ in $\mathcal{B}_0$ under the γ -monomial transformation.

For a tuple (b, c) in S_{-1} with non-zero b and c , we let

$$\overline{(b, c)} = \{(b, c), (b, -c), (-b, c), (-b, -c), (c, b), (c, -b), (-c, b), (-c, -b)\}.$$

Since $b^2 + c^2 = -1$, b determines c and the set $\overline{(b, c)}$. Thus, we also define a set

$$\overline{b \otimes d} = [\overline{(b, c)} \times \overline{(d, g)}] \cup [\overline{(d, g)} \times \overline{(b, c)}]$$

for $(b, c), (d, g) \in S_{-1}$, where b, c, d and g are non zero. Then, each element $(u, v, w, t) \in \overline{b \otimes d}$ corresponds to the code $C_{u,v,w,t}$ and $C'_{u,v,w,t}$, which are equivalent to $C_{b,c,d,g}$. If $b \neq \pm c, b \neq \pm d, b \neq \pm g$ and $d \neq \pm g$, $\overline{b \otimes d}$ contains 128 elements and these elements correspond to 256 codes equivalent to $C_{b,c,d,g}$. Moreover, for a tuple (b, c) in S_{-1} with non-zero b and c , $(1/b)^2 + (c/b)^2 = -1$ and $(1/c)^2 + (b/c)^2 = -1$, thus $(1/b, c/b), (1/c, b/c)$ are also elements in S_{-1} . Thus, there exist nine sets:

$$\overline{b \otimes d}, \overline{\frac{1}{b} \otimes d}, \overline{\frac{1}{c} \otimes d}, \overline{b \otimes \frac{1}{d}}, \overline{b \otimes \frac{1}{g}}, \overline{\frac{1}{b} \otimes \frac{1}{d}}, \overline{\frac{1}{b} \otimes \frac{1}{g}}, \overline{\frac{1}{c} \otimes \frac{1}{d}}, \overline{\frac{1}{c} \otimes \frac{1}{g}}.$$

Each of these sets has at most 128 elements corresponding to 256 codes equivalent to $C_{b,c,d,g}$. This means that there exist at most $256 \times 9 = 2304$ codes equivalent to $C_{b,c,d,g}$.

The equivalence of these codes can be checked easily by the direct computation. For example, the generator matrix of $C_{b,c,d,g}(15)(1, -1, -1, -1, 1, 1)$ is

$$\begin{pmatrix} b & 0 & 0 & 0 & 1 & c \\ c g j & -1 & 0 & -d & 0 & -b g j \\ -c d j & 0 & -1 & -g & 0 & b d j \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 & 1/b & c/b \\ 0 & 1 & 0 & d & (c/b) g j & -(1/b) g j \\ 0 & 0 & 1 & g & -(c/b) d j & (1/b) d j \end{pmatrix},$$

and this shows that $C_{1/b, c/b, d, g}$ is equivalent to $C_{b,c,d,g}$.

We note that the number of elements in $\overline{b \otimes d}$ and the number of corresponding codes equivalent to $C_{b,c,d,g}$ depend on the values of b and d . For instance, if $b^2 = d^2$ and $b^2 \neq -1/2$, then $\overline{b \otimes d}$ contains only 64 elements and $\overline{\frac{1}{b} \otimes d} = \overline{b \otimes \frac{1}{d}}, \overline{\frac{1}{c} \otimes d} = \overline{b \otimes \frac{1}{g}}$, and $\overline{\frac{1}{c} \otimes \frac{1}{d}} = \overline{\frac{1}{b} \otimes \frac{1}{g}}$ hold.

The following proposition shows the correspondence between a set $\overline{b \otimes d}$ and elements in $\mathcal{B}_0$.

Proposition 6.

- (i) If b^2, c^2, d^2 and g^2 are all distinct, then $\overline{b \otimes d}$ corresponds to 64 equivalent codes with a bisorted generator matrix.
- (ii) If $b^2 = c^2$ and $d^2 \neq g^2$, then $\overline{b \otimes d}$ corresponds to 48 equivalent codes with bisorted generator matrices.
- (iii) If $b^2 \neq c^2$ and $b = d$, then $\overline{b \otimes d}$ corresponds to at 32 equivalent codes with bisorted generator matrices.
- (iv) If $b^2 = c^2$ and $d^2 = g^2$, then $\overline{b \otimes d}$ corresponds to 18 equivalent codes with bisorted generator matrices.

Proof. (i) If $b^2 \neq c^2$, then there are four elements $(x, y) \in \overline{(b, c)}$ satisfying $x \leq y$. If $b^2 = c^2$, then there are only three elements $(x, y) \in \overline{(b, c)}$ satisfying $x \leq y$. Thus, it is easy to check that, if b^2, c^2, d^2 and g^2 are all distinct, there are 32 elements (u, v, w, t) in $\overline{b \otimes d}$ satisfying $u \leq v$ and $w \leq t$ and this corresponds to the code $C_{u,v,w,t}$ and $C'_{u,v,w,t}$ with bisorted matrices, which are equivalent to $C_{b,c,d,g}$. (ii), (iii) and (iv) are proved similarly. $\square$

4. Automorphism of Self-Dual Codes of Length 6 over $\mathbb{Z}_p$

Due to the results in Section 3, we continue our arguments by discussing the automorphism group of $\mathcal{C}$ with the following proposition.

Proposition 7. Let $\mathcal{C}$ be a self-dual code of length 6 over $\mathbb{Z}_p$ with a standard generator matrix G and let e_k be the k -th column vector of G . If $\sigma \in p(\mathcal{C})$, then both the matrix $(e_{\sigma(1)}, e_{\sigma(2)}, e_{\sigma(3)})$ and the matrix $(e_{\sigma(4)}, e_{\sigma(5)}, e_{\sigma(6)})$ are non-singular.

Proof. Let $G = (I_3 \mid A)$ and assume that $\sigma \in p(\mathcal{C})$. Then, the matrix $G\sigma\gamma = (e_{\sigma(1)}, e_{\sigma(2)}, e_{\sigma(3)}, e_{\sigma(4)}, e_{\sigma(5)}, e_{\sigma(6)})\gamma$ is row equivalent to G for some $\gamma \in \mathbb{D}^6$. Thus, $(e_{\sigma(1)}, e_{\sigma(2)}, e_{\sigma(3)})\gamma_1$

is row equivalent to I_3 for some $\gamma_1 \in \mathbb{D}^3$ and $(e_{\sigma(4)}, e_{\sigma(5)}, e_{\sigma(6)})\gamma_2$ is row equivalent to A for some $\gamma_2 \in \mathbb{D}^3$. Since we know that A is non-singular, this proposition holds. $\square$

Let $\mathcal{C}$ be an indecomposable non-MDS self-dual code of length 6 with a bisorted generator matrix $G = (I_3 \mid A)$, where $A = (a_{ij})$. Proposition 7 says what elements of S_6 cannot be in $p(\mathcal{C})$.

For example, the submatrix of the first three columns of $G(14)$ is $\begin{pmatrix} 0 & 0 & 0 \\ a_{21} & 1 & 0 \\ a_{31} & 0 & 1 \end{pmatrix}$ and this has rank 2.

Thus, $(14) \notin p(\mathcal{C})$. In this manner, we check the rank of the submatrix of $G\sigma$ for every $\sigma \in S_6$ and we conclude that 72 elements in Table 1 cannot be in $p(\mathcal{C})$.

Table 1. Seventy-two permutations that are not in $p(\mathcal{C})$ by Proposition 7.

(14),(142),(143),(154),(164),(2536),(2635),(1432),(1423),(1542),(1543),(1564),(1642),(1643),(1654),(24635),(24536),
(25346),(26345),(12536),(12635),(13625),(13526),(15432),(15642),(15643),(15423),(16432),(16542),(16543),(16423),
(124635),(124536),(125346),(126345),(135246),(136245),(134625),(134526),(156432),(156423),(165432),(165423),
(25)(36),(26)(35),(14)(56),(14)(23),(246)(35),(245)(36),(25)(346),(26)(345),(125)(36),(126)(35),(136)(25),(135)(26),
(142)(56),(143)(56),(154)(23),(164)(23),(1246)(35),(1245)(36),(1346)(25),(1345)(26),(1432)(56),(1423)(56),(1564)(23),
(1654)(23),(125)(346),(126)(345),(135)(246),(136)(245),(14)(23)(56)

Furthermore, by the definition of automorphism of $\mathcal{C}$, it holds that the row canonical form of $G\sigma\gamma$ is equal to $G = (I_3 \mid A)$ for some $\gamma \in \mathbb{D}^6$. Since $a_{11} = 0$, by comparing the element of the row canonical form of the matrix $G\sigma$, we check each element $\sigma \in S_6$ whether it is included in $p(\mathcal{C})$ or not. For example, it is easy to check that the row canonical form of the matrix $G(12)$ is

$$\begin{pmatrix} 1 & 0 & 0 & a_{21} & a_{22} & a_{23} \\ 0 & 1 & 0 & 0 & a_{12} & a_{13} \\ 0 & 0 & 1 & a_{31} & a_{32} & a_{33} \end{pmatrix}.$$

Since a_{21} is non-zero, $G(12)\gamma$ is not row equivalent to G for all $\gamma \in \mathbb{D}^6$. Thus, $(12) \notin p(\mathcal{C})$. In this manner, we check all elements $\in S_6$ and find out that 576 elements in Table 2 cannot be included in $p(\mathcal{C})$. Consequently, we have the next proposition.

Proposition 8. Let $\mathcal{C}$ be an indecomposable non-MDS self-dual code of length 6 over $\mathbb{Z}_p$ with the bisorted generator matrix. Then, $|p(\mathcal{C})| \leq 72$.

Proof. As investigated in the previous paragraphs, among 720 elements in S_6 , 72 elements in Table 1 and 576 elements in Table 2 cannot be in $p(\mathcal{C})$. Therefore, $|p(\mathcal{C})| \leq 72$. $\square$

We check all 72 elements $\in S_6$ which can be in $p(\mathcal{C})$ using the computer algebra system. We obtain the necessary condition for each element to be in $p(\mathcal{C})$. We summarize the results in Table 3.

Table 2. 576 permutations which are not in $p(\mathcal{C})$.

(12),(35),(46),(26),(13),(25),(45),(36),(124),(354),(135),(134),(465),(136),(163),(126),(345),(456),(346),(254),(265),(236), (235),(364),(132),(253),(146),(356),(246),(245),(152),(162),(263),(123),(145),(153),(365),(125),(264),(256),(3456),(2546), (1632),(2346),(1462),(2645),(1254),(2543),(2564),(1364),(1264),(2345),(2534),(1562),(1563),(1253),(3564),(1534), (1354),(2365),(2653),(2465),(1526),(1645),(2435),(1463),(1243),(1246),(1346),(2453),(1652),(2463),(1345),(1524), (1523),(2436),(1236),(1623),(1352),(1653),(1356),(1325),(1436),(1456),(3654),(3645),(1532),(1256),(3465),(1453), (1362),(1245),(2563),(1546),(2356),(1425),(1234),(2654),(1634),(1326),(2354),(1263),(2364),(2634),(1635),(1365), (1265),(3546),(2456),(1235),(2643),(1435),(1452),(1342),(1465),(1536),(1624),(1426),(1324),(1625),(16254),(16452), (12465),(23546),(14623),(15426),(13654),(12654),(16524),(14523),(25634),(23465),(16243),(12546),(24563),(12653), (12365),(14253),(12453),(25643),(12354),(15324),(14635),(26534),(25364),(24356),(14632),(14235),(23654),(15362), (14325),(12534),(16534),(14365),(23564),(15462),(23645),(13246),(16245),(16523),(15436),(15326),(13245),(12543), (14536),(12463),(24365),(15632),(13562),(12634),(14526),(15263),(24653),(15236),(16235),(15623),(13652),(13254), (16345),(12436),(12456),(15243),(13456),(16324),(12364),(16354),(14625),(13542),(15463),(15342),(14265),(15264), (13546),(13425),(13256),(16425),(15246),(12346),(16352),(13264),(14256),(26354),(14352),(13265),(15346),(14652), (16532),(13624),(14362),(15234),(16453),(14653),(13465),(15634),(16234),(13642),(14263),(14532),(26435),(15624), (14236),(13524),(16435),(14326),(13564),(14562),(16253),(25436),(12435),(26543),(15364),(26453),(16325),(13625),(1645), (25463),(12645),(12564),(13426),(12563),(13462),(13452),(16342),(23456),(12356),(12643),(14356),(12345),(15463), (136542),(124563),(162534),(146325),(134265),(164253),(154362),(124365),(123654),(154623),(132546),(164325), (165342),(153462),(153426),(123645),(126543),(152436),(145236),(142356),(154236),(164352),(123465),(156342), (124653),(152364),(142635),(135426),(126435),(163452),(153642),(135642),(152634),(142365),(135624),(123546), (142536),(143265),(123564),(132645),(125634),(146235),(142653),(165234),(162543),(145326),(152643),(162345), (143562),(146532),(162453),(162354),(132465),(153624),(132456),(134256),(163254),(123456),(152346),(162435), (153264),(163425),(165243),(134652),(154632),(143256),(143625),(132654),(136425),(143526),(143652),(126534), (153246),(146523),(145623),(134562),(156243),(156234),(124356),(145632),(154326),(164235),(142563),(164532), (163524),(156324),(164523),(154263),(152463),(132564),(125436),(165324),(163542),(125643),(136524),(163245), (23)(46),(12)(46),(15)(46),(12)(36),(15)(36),(12)(34),(24)(35),(26)(45),(14)(25),(13)(24),(12)(56),(13)(46),(16)(25), (23)(45),(14)(36),(15)(26),(14)(35),(12)(45),(24)(36),(16)(35),(13)(45),(35)(46),(13)(56),(14)(26),(12)(35),(25)(34), (13)(25),(13)(26),(25)(46),(26)(34),(16)(45),(36)(45),(153)(24),(142)(36),(15)(236),(16)(235),(14)(236),(132)(46), (13)(245),(136)(24),(25)(364),(13)(456),(152)(46),(14)(263),(163)(24),(16)(345),(14)(253),(23)(465),(146)(35),(126)(34), (14)(256),(12)(346),(145)(23),(123)(56),(14)(356),(163)(25),(16)(254),(125)(46),(143)(25),(123)(46),(12)(465),(135)(46), (145)(36),(124)(35),(153)(46),(163)(45),(162)(45),(256)(34),(146)(25),(12)(356),(13)(246),(24)(356),(135)(24),(123)(45), (134)(26),(16)(354),(162)(35),(154)(36),(124)(56),(236)(45),(132)(45),(136)(45),(134)(56),(126)(45),(13)(254),(153)(26), (142)(35),(12)(456),(15)(263),(263)(45),(14)(365),(15)(246),(13)(264),(265)(34),(152)(34),(164)(25),(23)(456),(16)(253), (14)(265),(16)(245),(254)(36),(15)(364),(12)(364),(134)(25),(12)(365),(162)(34),(15)(346),(13)(256),(13)(265),(152)(36), (12)(345),(154)(26),(143)(26),(15)(264),(264)(35),(14)(235),(24)(365),(13)(465),(146)(23),(125)(34),(132)(56),(235)(46), (253)(46),(124)(36),(26)(354),(12)(354),(164)(35),(145)(26),(16)(2543),(1534)(26),(1235)(46),(16)(2435),(1243)(56), (12)(3456),(1632)(45),(1645)(23),(1532)(46),(1234)(56),(13)(2654),(15)(2634),(13)(2465),(15)(2346),(1653)(24), (1342)(56),(1435)(26),(1536)(24),(1326)(45),(1265)(34),(12)(3564),(1236)(45),(1365)(24),(1634)(25),(1426)(35), (1356)(24),(14)(2563),(1546)(23),(1436)(25),(1456)(23),(1624)(35),(1325)(46),(1465)(23),(1563)(24),(1562)(34), (12)(3654),(1625)(34),(12)(3465),(1526)(34),(1324)(56),(1635)(24),(16)(2354),(15)(2643),(13)(2456),(1623)(45), (1256)(34),(1643)(25),(14)(2356),(1642)(35),(1543)(26),(1652)(34),(14)(2365),(15)(2436),(15)(2463),(14)(2653), (1425)(36),(16)(2453),(16)(2534),(1542)(36),(1523)(46),(13)(2564),(15)(2364),(16)(2345),(1524)(36),(124)(356), (162)(345),(164)(235),(123)(465),(162)(354),(143)(256),(134)(256),(134)(265),(136)(254),(146)(253),(132)(465), (152)(364),(142)(356),(142)(365),(163)(254),(164)(253),(153)(246),(135)(264),(152)(346),(124)(365),(154)(236), (145)(263),(143)(265),(132)(456),(153)(264),(145)(236),(123)(456),(146)(235),(163)(245),(125)(364),(126)(354), (154)(263),(16)(25)(34),(12)(34)(56),(15)(26)(34),(13)(24)(56),(16)(24)(35),(16)(23)(45),(15)(24)(36),(15)(23)(46)
--

Table 3. Possible permutations to be in $p(\mathcal{C})$ and their conditions.

$\sigma \in p(\mathcal{C})$	Necessary Cond.	$\sigma \in p(\mathcal{C})$	Necessary Cond.
(1)	None	(34)	$g^2 = 1$
(15)	$b^2 = 1$	(56)	$b^2 = c^2$
(23)	$d^2 = g^2$	(24)	$d^2 = 1$
(16)	$c^2 = 1$	(243)	$d^6 = 1$
(165)	$b^6 = 1$	(234)	$d^6 = 1$
(156)	$b^6 = 1$	(16)(34)	$c^2 = 1, g^2 = 1$
(24)(56)	$b^2 = c^2, d^2 = 1$	(15)(23)	$b^2 = 1, d^2 = g^2$
(15)(34)	$b^2 = 1, g^2 = 1$	(16)(24)	$c^2 = 1, d^2 = 1$
(16)(23)	$c^2 = 1, d^2 = g^2$	(23)(56)	$b^2 = c^2, d^2 = g^2$
(15)(24)	$b^2 = 1, d^2 = 1$	(34)(56)	$b^2 = c^2, g^2 = 1$
(16)(243)	$c^2 = 1, d^6 = 1$	(156)(34)	$b^6 = 1, g^2 = 1$
(156)(24)	$b^6 = 1, d^2 = 1$	(165)(24)	$b^6 = 1, d^2 = 1$
(165)(23)	$b^6 = 1, d^2 = g^2$	(165)(34)	$b^6 = 1, g^2 = 1$
(243)(56)	$b^2 = c^2, d^6 = 1$	(15)(243)	$b^2 = 1, d^6 = 1$
(15)(234)	$b^2 = 1, d^6 = 1$	(234)(56)	$b^2 = c^2, d^6 = 1$
(156)(23)	$b^6 = 1, d^2 = g^2$	(16)(234)	$c^2 = 1, d^6 = 1$
(126354)	$b^6 = 1, b^2 = g^2$	(135462)	$b^6 = 1, c^2 = g^2$
(146352)	$b^6 = 1, b^2 = d^2$	(136452)	$b^6 = 1, b^2 = g^2$
(126453)	$b^6 = 1, b^2 = d^2$	(146253)	$b^6 = 1, c^2 = d^2$
(145263)	$b^6 = 1, b^2 = d^2$	(136254)	$b^6 = 1, b^2 = d^2$
(135264)	$b^6 = 1, b^2 = g^2$	(125364)	$b^6 = 1, b^2 = d^2$
(125463)	$b^6 = 1, c^2 = d^2$	(145362)	$b^6 = 1, c^2 = d^2$
(1253)(46)	$b^2 = 1, d^2 = g^2$	(14)(2635)	$b^2 = c^2 = d^2 = g^2$
(1462)(35)	$c^2 = 1, d^2 = 1$	(13)(2546)	$b^2 = c^2, d^2 = 1$
(12)(3645)	$b^2 = c^2, g^2 = 1$	(1463)(25)	$b^2 = g^2, c^2 = 1, g^2 = 1$
(1264)(35)	$c^2 = 1, d^2 = 1$	(1354)(26)	$b^2 = 1, g^2 = 1$
(1452)(36)	$b^2 = 1, d^2 = 1$	(1352)(46)	$b^2 = 1, d^2 = g^2$
(1362)(45)	$c^2 = 1, d^2 = g^2$	(1254)(36)	$b^2 = 1, d^2 = 1$
(12)(3546)	$b^2 = c^2, g^2 = 1$	(14)(2536)	$b^2 = d^2 = c^2 = g^2$
(13)(2645)	$b^2 = c^2, d^2 = 1$	(1364)(25)	$b^2 = d^2, c^2 = 1, g^2 = 1$
(1453)(26)	$b^2 = 1, g^2 = 1$	(1263)(45)	$c^2 = 1, d^2 = g^2$
(165)(243)	$b^6 = 1, d^6 = 1$	(156)(234)	$b^6 = 1, d^6 = 1$
(165)(234)	$b^6 = 1, d^6 = 1$	(156)(243)	$b^6 = 1, d^6 = 1$
(12)(35)(46)	$b^2 d^2 = g^2, c^2 d^2 = 1$	(12)(36)(45)	$b^2 d^2 = 1, c^2 d^2 = g^2$
(14)(26)(35)	$b^2 = g^2, c^2 = d^2$	(14)(25)(36)	$b^2 = d^2, c^2 = g^2$
(13)(25)(46)	$b^2 g^2 = d^2, c^2 g^2 = 1$	(13)(26)(45)	$b^2 g^2 = 1, c^2 g^2 = d^2$

5. Enumeration of Self-Dual Codes of Length 6 over $\mathbb{Z}_p$

The number of self-dual codes of length n over $\mathbb{Z}_p$ is given by the following mass formula ([12], Chapter 19).

Theorem 2. The number of self-dual codes of length n over $\mathbb{Z}_p$ for odd p is given by

$$N_p(n) = 2 \prod_{i=1}^{n/2-1} (p^i + 1).$$

Thus, there are $N_p(6) = 2(p+1)(p^2+1)$ self-dual codes of length 6 over $\mathbb{Z}_p$ for $p \equiv 1 \pmod{4}$.

Example 1. There exists a unique self-dual code of length 6 over $\mathbb{Z}_2$,

$$\mathcal{C}_2^1 : \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

$\mathcal{C}_2^1$ is decomposable and $|\text{Aut}(\mathcal{C}_2^1)| = 48$.

There exist two inequivalent self-dual codes of length 6 over $\mathbb{Z}_5$; one is decomposable and the other is MDS :

$$C_5^1 : \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 & 2 & 0 \\ 0 & 0 & 1 & 2 & 0 & 0 \end{pmatrix}, \text{ and } C_5^2 : \begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 2 \\ 0 & 1 & 0 & 2 & 1 & 3 \\ 0 & 0 & 1 & 2 & 3 & 1 \end{pmatrix}.$$

We note that $|Aut(C_5^1)| = 8 \cdot 48$ and $|Aut(C_5^2)| = 2 \cdot 120$.

The following proposition is deduced directly from Theorem 4.5 and Theorem 4.10 in [9].

Proposition 9 (Decomposable codes). *Let $p \equiv 1 \pmod{4}$ and $p \neq 5$ and j be a root of -1 . Then, the decomposable self-dual code of length 6 over $\mathbb{Z}_p$ with generator matrix*

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & j \\ 0 & 1 & 0 & d & e & 0 \\ 0 & 0 & 1 & -e & d & 0 \end{pmatrix}$$

is equivalent to one of the following four classes of inequivalent codes:

Class	d	$p(\mathcal{C})$	$ s(\mathcal{C}) \cdot p(\mathcal{C}) $
(i)	$d = 0$	$\langle (23)(45), (123654) \rangle$	8.48
(ii)	$d^6 = 1, d^2 \neq 1$	$\langle (25)(34), (16)(354) \rangle$	4.24
(iii)	$d = 1$	$\langle (16), (35), (2345) \rangle$	4.16
(iv)	$de \neq 0, d^4 \neq 1, d^6 \neq 1, d^2 \neq e^2$	$\langle (16), (24)(35), (23)(45) \rangle$	4.8

The code from class (i) is unique, if it exists, up to equivalence and has the weight enumerator

$$W_1(x, y) = x^6 + 3(p-1)x^4y^2 + 3(p-1)^2x^2y^4 + (p-1)^3y^6.$$

Codes from class (ii) and (iii) are unique, if they exist, up to equivalence and have the weight enumerator

$$W_2(x, y) = x^6 + (p-1)x^4y^2 + 4(p-1)x^3y^3 + (p-1)(p-3)x^2y^4 + 4(p-1)^2xy^5 + (p-1)^2(p-3)y^6.$$

Proof. This proposition is deduced directly from Theorem 4.5 in [9] and the definition of a decomposable code. $\square$

Proposition 10. *Let N'_k be the number of k -th class of decomposable self-dual codes of length 6 over $\mathbb{Z}_p$. These numbers are determined as in the following table:*

$p \pmod{24}$	N'_1	N'_2	N'_3	N'_4
1	1	1	1	$\frac{p-25}{24}$
5	1	0	0	$\frac{p-5}{24}$
13	1	1	0	$\frac{p-13}{24}$
17	1	0	1	$\frac{p-17}{24}$

Proof. This proposition is deduced directly from Theorem 4.10 in [9]. $\square$

Proposition 11 (indecomposable non-MDS codes). *An indecomposable non-MDS self-dual code $\mathcal{C}$ of length 6 with generator matrix*

$$\begin{pmatrix} 1 & 0 & 0 & 0 & b & c \\ 0 & 1 & 0 & d & e & f \\ 0 & 0 & 1 & g & h & i \end{pmatrix}$$

over $\mathbb{Z}_p$ is in the one of the following seven classes:

Class	b, c, d, g	$p(\mathcal{C})$	$ s(\mathcal{C}) \cdot p(\mathcal{C}) $
(i)	$b \neq 1, b^6 = 1, d = b$	$\langle (146352), (243) \rangle$	2.18
(ii)	$b \neq 1, b^6 = 1, d = 1$	$\langle (165)(24) \rangle$	2.6
(iii)	$b \neq 1, b^6 = 1, d^2 \neq 1, d^2 \neq b^2, d^2 \neq g^2$	$\langle (156) \rangle$	2.3
(iv)	$b = d = 1$	$\langle (24), (14)(25)(36) \rangle$	2.8
(v)	$b = 1, d^6 \neq 1, d^4 \neq 1$	$\langle (15) \rangle$	2.2
(vi)	$b^6 \neq 1, b^4 \neq 1, d = b$	$\langle (14)(25)(36) \rangle$	2.2
(vii)	else	$\langle (1) \rangle$	2.1

Codes from classes (i),(ii),(iv) are unique up to equivalence and all codes have the weight enumerator

$$W_3(x, y) = x^6 + 2(p-1)x^3y^3 + 9(p-1)x^2y^4 + 6(p-1)(p-3)xy^5 + (p-1)(p^2 - 5p + 8)y^6.$$

Proof. Clearly, $s(\mathcal{C}) = \{\pm I\}$ for each code $\mathcal{C}$ in all classes. The permutation part $p(\mathcal{C})$ of each class is obtained directly from the conditions in Table 3. $\square$

Proposition 12. Let $\mathcal{O}_k$ be the number of self-dual codes in $\mathcal{B}_0$ equivalent to a code in the k -th class. These numbers are determined as in the following table:

$\mathcal{O}_1$	$\mathcal{O}_2$	$\mathcal{O}_3$	$\mathcal{O}_4$	$\mathcal{O}_5$	$\mathcal{O}_6$	$\mathcal{O}_7$
32	112	192	98	336	288	576

Proof. By Proposition 6, it is routine to count and sum the number of self-dual codes in $\mathcal{B}_0$ corresponding to each of the nine sets: $\overline{b \otimes d}$, $\overline{\frac{1}{b} \otimes d}$, $\overline{\frac{1}{c} \otimes d}$, $\overline{b \otimes \frac{1}{d}}$, $\overline{b \otimes \frac{1}{g}}$, $\overline{\frac{1}{b} \otimes \frac{1}{d}}$, $\overline{\frac{1}{b} \otimes \frac{1}{g}}$, $\overline{\frac{1}{c} \otimes \frac{1}{d}}$, and $\overline{\frac{1}{c} \otimes \frac{1}{g}}$.

Three conditions $b^2 + c^2 + 1 = 0$, $b \neq 1$ and $b^6 = 1$ in class (i) imply that $b^2 \pm b + 1 = 0$ and $c^2 = \pm b$, thus $c^2 = (b/c)^2$. Since $(b/c)^2 + 1 + (1/c)^2 = 0$, it also holds that $b^2 = (1/c)^2$. Thus, $\overline{(b, c)} = \overline{(1/c, b/c)} = \overline{(c/b, 1/b)}$. Furthermore, $b = d$ implies that $\overline{(d, g)} = \overline{(1/d, g/d)} = \overline{(1/g, d/g)}$. This means that

$$\overline{b \otimes d} = \overline{\frac{1}{b} \otimes d} = \overline{\frac{1}{c} \otimes d} = \overline{b \otimes \frac{1}{d}} = \overline{b \otimes \frac{1}{g}} = \overline{\frac{1}{b} \otimes \frac{1}{d}} = \overline{\frac{1}{b} \otimes \frac{1}{g}} = \overline{\frac{1}{c} \otimes \frac{1}{d}} = \overline{\frac{1}{c} \otimes \frac{1}{g}}$$

and, by Proposition 6, we know that $\overline{b \otimes d}$ corresponds to 32 equivalent codes in $\mathcal{B}_0$. This proves the case of class (i). All of the other cases are proved similarly. $\square$

Theorem 3. Let N_k be the number of k -th class of self-dual codes of length 6 over $\mathbb{Z}_p$. These numbers are determined as in the following table:

$p \pmod{24}$	N_1	N_2	N_3	N_4	N_5	N_6	N_7
1	1	1	$\frac{p-25}{24}$	1	$\frac{p-25}{24}$	$\frac{p-25}{24}$	$\frac{p^2-74p+1225}{1152}$
5	0	0	0	0	0	$\frac{p-5}{24}$	$\frac{p^2-34p+145}{1152}$
13	1	0	$\frac{p-13}{24}$	0	0	$\frac{p-13}{24}$	$\frac{p^2-50p+481}{1152}$
17	0	0	0	1	$\frac{p-17}{24}$	$\frac{p-17}{24}$	$\frac{p^2-58p+697}{1152}$

Proof. We note that $p \equiv 1 \pmod{4}$ for all prime p . The existence of (i) and (iii) follows from the fact that $\mathbb{Z}_p^*$ is a multiplicative cyclic group of order $p-1$. The existence of (ii), (iv) and (v) follows from the fact that -2 is a quadratic residue in $\mathbb{Z}_p$ if and only if $p \equiv 1, 3 \pmod{8}$. For the uniqueness in (i), (ii) and (iv), it is easy to show by checking the equivalence of codes corresponding to the roots of $x^6 = 1$ or $x^2 + 2 = 0$.

(iii) It is easy to show that the number of codes with bisorted generator matrix equivalent to $\mathcal{C}_{b,c,d,g}$, where $b^6 = 1$ is $8(p-7)$ if $p \equiv 1 \pmod{8}$ and $8(p-9)$ if $p \equiv 5 \pmod{8}$, which is equal to the total number of distinct codes in classes (i), (ii) and (iii). Among them, there are 32 codes equivalent to the code in class (i) and there are 112 codes equivalent to the code in class (ii). Since $\mathcal{O}_3 = 192$, we have that

$$N_3 = \begin{cases} \frac{8(p-7)-32-64-48}{192} & \text{if } p \equiv 1 \pmod{24}, \\ \frac{8(p-9)-32}{192} & \text{if } p \equiv 13 \pmod{24}. \end{cases}$$

(v) To calculate N_5 , we get the number of codes equivalent to $\mathcal{C}_{1,c,d,g}$, which is equal to the total number of distinct codes in classes (ii), (iv) and (v). The result follows by a similar argument as in case (iii).

(vi) At first, we count the number of symmetric generator matrices. Each element $(b, c) \in S_{-1}$ corresponds to two symmetric generator matrices of $\mathcal{C}_{b,c,b,c}$ and $\mathcal{C}'_{b,c,b,c}$, thus there exist $2(p-5)$ symmetric generator matrices. In class (i), if any, there are 16 symmetric generator matrices equivalent to the unique code of class (i). Similarly, in the class (iv), there are 16 symmetric generator matrices corresponding to $(1, \sqrt{2}j)$ and there are another eight symmetric generator matrices corresponding to $(\frac{1}{\sqrt{2}}j, \frac{1}{\sqrt{2}}j)$. Since $b^3 \neq 1$ and $b^4 \neq 1$ in the class (vi), (b, c) , $(1/c, b/c)$ and $(c/b, 1/b)$ are all distinct. This implies that, for each code in the class (vi), there are 48 equivalent codes with symmetric generator matrices. Thus, the following equality holds:

$$48N_6 = 2(p-5) - 16N_1 - 24N_4.$$

(vii) By Proposition 12, we have that

$$|\mathcal{B}_0| = 32N_1 + 112N_2 + 192N_3 + 98N_4 + 336N_5 + 288N_6 + 576N_7,$$

and we obtain N_7 . This completes the proof. $\square$

Corollary 5. The number of MDS self-dual codes of length 6 over $\mathbb{Z}_p$ for an odd prime p is

$$2p^3 - 18p^2 + 142p - 318.$$

Proof. We compute the number of non-MDS self-dual codes of length 6 over $\mathbb{Z}_p$ using the mass formula,

$$\sum_{j=1}^s \frac{2^6 \times 6!}{|Aut(\mathcal{C}_j)|},$$

where $\mathcal{C}_j$ is a representative of each equivalent class.

(i) For $p \equiv 1 \pmod{24}$,

$$\begin{aligned} & 120 + 480 + 720 + 1440 \cdot \frac{p-25}{24} + 1280 + 3840 + 7680 \cdot \frac{p-25}{24} \\ & + 2880 + 11520 \cdot \frac{p-25}{24} + 11520 \cdot \frac{p-25}{24} + 23040 \cdot \frac{p^2 - 74p + 1225}{1152} \\ & = 20p^2 - 140p + 320. \end{aligned}$$

(ii) For $p \equiv 5 \pmod{24}$,

$$\begin{aligned} & 120 + 1440 \cdot \frac{p-5}{24} + 11520 \cdot \frac{p-5}{24} + 23040 \cdot \frac{p^2 - 34p + 145}{1152} \\ & = 20p^2 - 140p + 320. \end{aligned}$$

(iii) For $p \equiv 13 \pmod{24}$,

$$\begin{aligned} & 120 + 480 + 1440 \cdot \frac{p-13}{24} + 1280 + 7680 \cdot \frac{p-13}{24} + 11520 \cdot \frac{p-13}{24} \\ & + 23040 \cdot \frac{p^2 - 50p + 481}{1152} = 20p^2 - 140p + 320. \end{aligned}$$

(iv) For $p \equiv 17 \pmod{24}$,

$$\begin{aligned} & 120 + 720 + 1440 \cdot \frac{p-17}{24} + 2880 + 11520 \cdot \frac{p-17}{24} + 11520 \cdot \frac{p-17}{24} \\ & + 23040 \cdot \frac{p^2 - 58p + 697}{1152} = 20p^2 - 140p + 320. \end{aligned}$$

Finally, the number of MDS self-dual codes of length 6 over $\mathbb{Z}_p$ for every prime $p \equiv 1 \pmod{4}$ is obtained as

$$2(p+1)(p^2+1) - (20p^2 - 140p + 320) = 2p^3 - 18p^2 + 142p - 318$$

and this completes the proof. $\square$

Funding: This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2018R1A6A3A01013052).

Acknowledgments: The author wishes to thank the reviewers for valuable remarks that helped to improve this article.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Huffman, W.C. On the classification and enumeration of self-dual codes. *Finite Fields Appl.* **2005**, *11*, 451–490. [\[CrossRef\]](#)
2. Pless, V. A classification of self-orthogonal codes over GF (2). *Discret. Math.* **1972**, *3*, 209–246. [\[CrossRef\]](#)
3. Pless, V.; Sloane, N.J.A. On the classification and enumeration of self-dual codes. *J. Combin. Theory Ser. A* **1975**, *18*, 313–335. [\[CrossRef\]](#)
4. Betsumiya, K.; Georgiou, S.; Gulliver, A.; Harada, M.; Koukouvinos, C. On self-dual codes over some prime fields. *Discret. Math.* **2003**, *262*, 37–58. [\[CrossRef\]](#)
5. Leon, J.S.; Pless, V.; Sloane, N.J.A. Self-dual codes over GF (5). *J. Combin. Theory Ser. A* **1982**, *32*, 178–194. [\[CrossRef\]](#)
6. MacWilliams, F.J.; Odlyzko, A.M.; Sloane, N.J.A.; Ward, H.N. Self-dual codes over GF (4). *J. Combin. Theory Ser. A* **1978**, *25*, 288–318. [\[CrossRef\]](#)
7. Pless, V.; Sloane, N.J.A.; Ward, H. Ternary codes of minimum weight 6 and the classification of the self-dual codes of length 20. *IEEE Trans. Inform. Theory* **1980**, *26*, 305–316. [\[CrossRef\]](#)
8. Pless, V.; Tonchev, V. Self-dual codes over GF (7). *IEEE Trans. Inform. Theory* **1987**, *33*, 723–727. [\[CrossRef\]](#)
9. Park, Y.H. The classification of self-dual modular codes. *Finite Fields Appl.* **2011**, *17*, 442–460. [\[CrossRef\]](#)
10. Huffman, W.C.; Pless, V. *Fundamentals of Error-Correcting Codes*; Cambridge University Press: Cambridge, UK, 2010.

11. Lidl, R.; Niederreiter, H. *Finite Fields*; Cambridge University Press: Cambridge, UK, 1997.
12. Mac Williams, F.J.; Sloane, N.J.A. *The Theory of Error-Correcting Codes*; North Holland Publishing Co.: Amsterdam, The Netherlands, 1977.

© 2019 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).