EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
Vol. 13, No. 4, 2020, 873-892
ISSN 1307-5543 – www.ejpam.com
Published by New York Business Global

Self-orthogonal Codes over $\mathbb{F}_q + u\mathbb{F}_q$ and $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$

Lucky Erap Galvez[1,*], Rowena Alma Betty[1], Fidel Nemenzo[1]

[1] *Institute of Mathematics, University of the Philippines Diliman, Quezon City, Philippines*

Abstract. In this paper, we establish a mass formula for Euclidean and Hermitian self-orthogonal codes over the finite ring $\mathbb{F}_q + u\mathbb{F}_q$, where $\mathbb{F}_q$ is the finite field of order q and $u^2 = 0$. We also establish a mass formula for Euclidean self-orthogonal codes over the finite ring $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$, with $u^3 = 0$ and characteristic of $\mathbb{F}_q$ is odd. These mass formulas are used to give a classification of Euclidean and Hermitian self-orthogonal codes over $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_3 + u\mathbb{F}_3$ of small lengths.

2020 Mathematics Subject Classifications: 94B05

Key Words and Phrases: Codes over rings, self-orthogonal codes, mass formula

1. Introduction

Self-dual codes have rich mathematical theory and are of great interest to researchers because many of the best known codes are self-dual. A fundamental problem in coding theory is the classification of self-dual codes, that is, an enumeration of a complete set of representatives for the equivalence classes of self-dual codes. In the past years, self-dual codes over finite fields have been extensively studied and classified up to various lengths (see [8, 11]). Since the discovery in 1994 [7] that certain non-linear binary codes can be viewed as linear codes over the ring $\mathbb{Z}_4$, there has been much interest in the study of self-dual codes over various finite rings.

A key problem is to establish an explicit formula for the number of distinct self-dual codes of length n over a ring R, given by

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

where C runs through the set of all inequivalent self-dual codes of length n over R, E_n is the full group of transformations allowed in defining the equivalence for code C and $\mathrm{Aut}(C)$ is the automorphism group. This is called the *mass formula*, and is an important computational tool for the classification of such codes. Mass formulas for self-dual codes

*Corresponding author.
DOI: https://doi.org/10.29020/nybg.ejpam.v13i4.3838

Email addresses: `legalvez@math.upd.edu.ph` (L. E. Galvez), `rabetty@math.upd.edu.ph` (R. A. Betty), `fidel@math.upd.edu.ph` (F. Nemenzo)

over finite rings rings such as $\mathbb{Z}_4$ and $\mathbb{F}_q + u\mathbb{F}_q$ were given in [6], while [3] gave the mass formula for self-dual codes over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$.

In this paper, we focus on the more general mass formula for self-orthogonal codes, which will include the mass formula for self-dual codes as a special case. Mass formulas for self-orthogonal codes over $\mathbb{Z}_{p^2}$, where p is a prime, were given in [2], while the mass formula for even codes over $\mathbb{Z}_8$, i.e., self-orthogonal codes whose codewords have Euclidean weights divisible by 16, was computed in [1].

Codes over $\mathbb{F}_q + u\mathbb{F}_q$ and $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ have an invariant called *type*, denoted by $\{k_0, k_1\}$ and $\{k_0, k_1, k_2\}$, respectively, where k_0, k_1 and k_2 are nonnegative integers. The type of a code is determined by its residue and torsion codes. To obtain the mass formula, we will determine the number of self-orthogonal codes of length n over $\mathbb{F}_q + u\mathbb{F}_q$ with given residue and torsion, and compute the number of self-orthogonal codes of length n over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$, for odd q, with given u^2-Residue and torsion. We also give a classification of Euclidean and Hermitian self-orthogonal codes over $\mathbb{F}_2+u\mathbb{F}_2$ and $\mathbb{F}_3+u\mathbb{F}_3$, up to some short lengths.

2. Codes over $\mathbb{F}_q + u\mathbb{F}_q$

We begin with some basic concepts about codes over rings. A linear code C of length n over a ring R is a submodule of the R^n module. A generator matrix for C is a matrix $G \in M_{k\times n}(R)$ whose rows generate the code. For a matrix $G \in M_{k\times n}(R)$, we denote by R^kG the code $\{aG \mid a \in R^k\}$ of length n over R.

Let q be a power of a prime and $\mathbb{F}_q$ denote the finite field of q elements. Let R_1 be the commutative ring $\mathbb{F}_q[u]/(u^2) = \mathbb{F}_q + u\mathbb{F}_q$, where $u^2 = 0$. This finite chain ring is a local ring with unique maximal ideal (u) and residue field $\mathbb{F}_q + u\mathbb{F}_q/(u) = \mathbb{F}_q$. Every code C of length n over R_1 is permutation-equivalent to a code with the following generator matrix,

$$\begin{bmatrix} I_{k_0} & A + uB \\ 0 & uD \end{bmatrix}, \tag{1}$$

where I_{k_0} is the $k_0 \times k_0$ identity matrix, $A, B \in M_{k_0\times(n-k_0)}(\mathbb{F}_q)$ and $D \in M_{k_1\times(n-k_0)}(\mathbb{F}_q)$. Such a code C is said to be of type $\{k_0, k_1\}$. The code C is said to be *free* if $k_1 = 0$. The type is the analog of the dimension of a code over a finite field. Such a code C contains $q^{2k_0+k_1}$ codewords.

Let $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ be elements of R_1^n. Define the Euclidean inner product on R_1^n as $\langle x, y\rangle_E = \sum_{i=1}^n x_i y_i$. Now, let $z = a + ub \in R_1$ and define $\overline{z} = a - ub$. The Hermitian inner product on R_1^n is defined as $\langle x, y\rangle_H = \sum_{i=1}^n x_i\overline{y_i}$. The set

$$C^\perp = \{x \in R_1^n \mid \langle x, y\rangle = 0 \ \forall y \in C\}$$

is called the Euclidean or Hermitian dual of C, depending on which inner product $\langle x, y\rangle$ is used. The code C is said to be Euclidean or Hermitian self-orthogonal if $C \subseteq C^\perp$. If $C = C^\perp$, then we say C is Euclidean or Hermitian self-dual.

Let C be a code over R_1. The code $\left\{v \in \mathbb{F}_q^n \mid \exists w \in \mathbb{F}_q^n,\, v + uw \in C\right\}$ is called the residue code of C and is denoted by $\mathrm{res}(C)$. The code $\left\{v \in \mathbb{F}_q^n \mid uv \in C\right\}$ is called the torsion code of C and is denoted by $\text{tor}(C)$. If C has generator matrix (1), then $\text{res}(C)$ and $\text{tor}(C)$ are $[n, k_0]$ and $[n, k_0 + k_1]$ codes over $\mathbb{F}_q$, with generator matrices

$$\left[\begin{array}{cc} I_{k_0} & A \end{array}\right] \text{ and } \left[\begin{array}{cc} I_{k_0} & A \\ 0 & D \end{array}\right],$$

respectively. Clearly, $\text{res}(C) \subseteq \text{tor}(C)$ and $|C| = q^{2k_0+k_1} = |\text{res}(C)||\text{tor}(C)|$.

The following lemma shows the relationship between the residue and torsion codes of a self-orthogonal code over R_1. The proof is given in [6].

Lemma 1. *Let C be a (Euclidean or Hermitian) self-orthogonal code over R_1. Then*

(i) res(C) is self-orthogonal, i.e. res$(C) \subseteq$ res$(C)^\perp$;

(ii) tor$(C) \subseteq$ res$(C)^\perp$.

In particular, if C is (Euclidean or Hermitian) self-dual, tor$(C) =$ res$(C)^\perp$.

3. Codes over $\mathbb{F}_q + u\mathbb{F}_q$ with prescribed residue and torsion

Let C_1 be a code of length n over $\mathbb{F}_q$ with dimension k_0 and generator matrix

$$\left[\begin{array}{cc} I_{k_0} & A \end{array}\right], \tag{2}$$

and C_2 a code of length n over $\mathbb{F}_q$ of dimension $k_0 + k_1$ and has generator matrix

$$\left[\begin{array}{cc} I_{k_0} & A \\ 0 & D \end{array}\right], \tag{3}$$

where $A \in M_{k_0 \times (n-k_0)}(\mathbb{F}_q)$, and $D \in M_{k_1 \times (n-k_0)}(\mathbb{F}_q)$ is of full row rank.

Lemma 2. *If C is a code of length n over R_1 with* $\text{res}(C) = C_1$ *and* $\text{tor}(C) = C_2$, *then there exists a matrix $N \in M_{k_0 \times (n-k_0)}(\mathbb{F}_q)$ such that the matrix*

$$\left[\begin{array}{cc} I_{k_0} & A + uN \\ 0 & uD \end{array}\right] \tag{4}$$

is a generator matrix of C. Such matrix N is unique if C is a free code.

Proof. Since the residue and torsion codes of C are C_1 and C_2, respectively, then for some $M_1 \in M_{k_0}(\mathbb{F}_q)$ and $M_2 \in M_{k_0 \times (n-k_0)}(\mathbb{F}_q)$,

$$R_1^{k_0+k_1} \left[\begin{array}{cc} I_{k_0} + uM_1 & A + uM_2 \\ 0 & uD \end{array}\right] \subseteq C.$$

By an elementary row operation,

$$\begin{aligned} C &\supseteq R_1^{k_0+k_1} \begin{bmatrix} I_{k_0} - uM_1 & 0 \\ 0 & I_{k_1} \end{bmatrix} \begin{bmatrix} I_{k_0} + uM_1 & A + uM_2 \\ 0 & uD \end{bmatrix} \\ &= R_1^{k_0+k_1} \begin{bmatrix} I_{k_0} & A + u(M_2 - M_1 A) \\ 0 & uD \end{bmatrix}. \end{aligned}$$

Taking $N = M_2 - M_1 A$, we have

$$|C| \geq \left| R_1^{k_0+k_1} \begin{bmatrix} I_{k_0} & A + uN \\ 0 & uD \end{bmatrix} \right| = q^{2k_0+k_1} = |C_1|\,|C_2| = |C|\,.$$

Thus, C has a generator matrix (4).

Suppose C is a free code and there exist $N_1, N_2 \in M_{k_0 \times (n-k_0)}(\mathbb{F}_q)$ such that

$$R_1^{k_0}\,[I \;\; A + uN_1] = R_1^{k_0}\,[I \;\; A + uN_2]\,.$$

Then $A + uN_1 \equiv A + uN_2 \; (u^2)$, which implies that $N_1 \equiv N_2 \; (u)$. ■

For the remainder of this section, assume that $C_1 \subseteq C_2 \subseteq C_1^{\perp}$. Then

$$\begin{aligned} I_{k_0} + AA^T &\equiv 0 \; (u), & (5) \\ DA^T &\equiv 0 \; (u). & (6) \end{aligned}$$

It follows from (5) that A is of full row rank.

Denote by $\mathrm{Sym}_{k_0}(\mathbb{F}_q)$ the set of $k_0 \times k_0$ symmetric matrices, $\mathrm{Alt}_{k_0}(\mathbb{F}_q)$ the set of $k_0 \times k_0$ alternating matrices, and $\mathrm{Skew}_{k_0}(\mathbb{F}_q)$ the set of $k_0 \times k_0$ skew-symmetric matrices over $\mathbb{F}_q$.

Lemma 3. *Let $A \in M_{m \times n}(\mathbb{F}_q)$ where rank $A = m$. We define the mappings*

$$\begin{aligned} \Psi_A : M_{m \times n}(\mathbb{F}_q) &\longrightarrow M_m(\mathbb{F}_q) \\ N &\longmapsto AN^T + NA^T, \end{aligned}$$

and

$$\begin{aligned} \Phi_A : M_{m \times n}(\mathbb{F}_q) &\longrightarrow M_m(\mathbb{F}_q) \\ N &\longmapsto AN^T - NA^T. \end{aligned}$$

Then

$$\Psi_A\left(M_{m \times n}(\mathbb{F}_q)\right) = \begin{cases} \mathrm{Sym}_m(\mathbb{F}_q), & \text{if } q \text{ is odd} \\ \mathrm{Alt}_m(\mathbb{F}_q), & \text{if } q \text{ is even,} \end{cases}$$

and the image of the map Φ_A is $\mathrm{Skew}_m(\mathbb{F}_q)$.

Proof. The image of Ψ_A was shown in [2]. Since rank $A = m$, $A(M_{n\times m}(\mathbb{F}_q)) = M_m(\mathbb{F}_q)$. Indeed,

$$\begin{aligned}\Phi_A(M_{k_0\times(n-k_0)}(\mathbb{F}_q)) &= \left\{AN^T - NA^T \mid N \in M_{k_0\times(n-k_0)}(\mathbb{F}_q)\right\}\\ &= \left\{S - S^T \mid S \in M_{k_0}(\mathbb{F}_q)\right\}\\ &= \mathrm{Skew}_{k_0}(\mathbb{F}_q).\end{aligned}$$

■

Lemma 4. *The number of free Euclidean self-orthogonal codes over R_1 with residue code C_1 is*

$$q^{k_0(2n-3k_0+\epsilon)/2},$$

where $\epsilon = -1$ if q is odd and $\epsilon = 1$ if q is even.

The number of free Hermitian self-orthogonal codes over R_1 with residue code C_1 is

$$q^{k_0(2n-3k_0+1)/2}.$$

Proof. If C is a free code with residue code C_1, then by Lemma 2, C has generator matrix $\begin{bmatrix} I_{k_0} & A + uN\end{bmatrix}$, for some unique $N \in M_{k_0\times(n-k_0)}(\mathbb{F}_q)$. Observe that C is Euclidean self-orthogonal if and only if

$$I_{k_0} + AA^T + u(AN^T + NA^T) \equiv 0 \ (u^2).$$

Hence, the number of free Euclidean self-orthogonal codes C with residue code C_1 is

$$\left|\{N \in M_{k_0\times(n-k_0)} | I_{k_0} + AA^T + u(AN^T + NA^T) \equiv 0 \ (u^2)\}\right|. \tag{7}$$

By (5), we have $AN^T + NA^T \equiv 0 \ (u)$.Therefore, (7) becomes

$$\left|\left\{N \in M_{k_0\times(n-k_0)} | AN^T + NA^T \equiv 0 \ (u)\right\}\right| = |\ker\ \Psi_A| = \frac{\left|M_{k_0\times(n-k_0)}\right|}{|\mathrm{Im}\ \Psi_A|}.$$

Thus, we have

$$|\ker\ \Psi_A| = \begin{cases} q^{\frac{k_0(2n-3k_0-1)}{2}}, & \text{if } q \text{ is odd}\\ q^{\frac{k_0(2n-3k_0+1)}{2}}, & \text{if } q \text{ is even,}\end{cases}$$

by Lemma 3.

Similarly, C is Hermitian self-orthogonal if and only if

$$I_{k_0} + AA^T + u(AN^T - NA^T) \equiv 0 \ (u^2).$$

Hence, by (5) and Lemma 3, the number of free Hermitian self-orthogonal codes C with residue code C_1 is

$$\left|\left\{N \in M_{k_0\times(n-k_0)} | AN^T - NA^T \equiv 0 \ (u)\right\}\right| = |\ker\ \Phi_A| = q^{\frac{k_0(2n-3k_0+1)}{2}}.$$

■

Define the sets

$$\begin{aligned} X &= \left\{ C \mid C \subseteq R_1^n, \text{type } \{k_0, 0\}, C \subseteq C^{\perp}, \text{res}(C) = C_1 \right\} \text{ and} \\ X' &= \left\{ C' \mid C' \subseteq R_1^n, C' \subseteq C'^{\perp}, \text{res}(C') = C_1, \text{tor}(C') = C_2 \right\}, \end{aligned}$$

where self-orthogonality is either in the Euclidean or Hermitian sense.

Lemma 5. *If $C' \in X'$, then $|\{C \in X | C \subseteq C'\}| = q^{k_0 k_1}$.*

Proof. By Lemma 2, C' has a generator matrix (4). Consider the map

$$\begin{aligned} \psi : M_{k_0 \times k_1}(\mathbb{F}_q) &\longrightarrow \left\{ C \in X \mid C \subseteq C' \right\} \\ M &\longmapsto R_1^{k_0} \left[I \ \ A + u(N + MD) \right]. \end{aligned}$$

Clearly, ψ is well-defined. We will show that ψ is bijective. If $M_1, M_2 \in M_{k_0 \times k_1}(\mathbb{F}_q)$ such that $\psi(M_1) = \psi(M_2)$, then

$$R_1^{k_0} \left[I_{k_0} \ \ A + u(N + M_1 D) \right] = R_1^{k_0} \left[I_{k_0} \ \ A + u(N + M_2 D) \right]$$

which means $A + u(N + M_1 D) \equiv A + u(N + M_2 D)$ (u^2). Therefore $N + M_1 D \equiv N + M_2 D$ (u). Since D is of full row rank, we have $M_1 \equiv M_2$ (u). Hence, ψ is injective.

Suppose $C \in X$ and $C \subseteq C'$. By Lemma 2, $C = R_1^{k_0} \left[I_{k_0} \ \ A + uF \right]$, for some matrix F. The inclusion $C \subseteq C'$ implies that

$$A + uF \equiv A + u(N + MD) \ (u^2)$$

for some matrix M. So $F \equiv N + MD$ (u), which shows that ψ is surjective, and hence, bijective. Therefore,

$$\left| \left\{ C \in X | C \subseteq C' \right\} \right| = |M_{k_0 \times k_1}(\mathbb{F}_q)| = q^{k_0 k_1}.$$

■

Lemma 6. *If $C \in X$, then there exists a unique code $C' \in X'$ such that $C \subseteq C'$.*

Proof. Since $C \in X$, C has a generator matrix $[I \ \ A + uN]$ for some unique matrix N, by Lemma 2. Let C'_0 be a code with generator matrix

$$\begin{bmatrix} I_{k_0} & A + uN \\ 0 & uD \end{bmatrix}.$$

The code C'_0 satisfies $\text{res}(C'_0) = C_1$ and $\text{tor}(C'_0) = C_2$.

Clearly, $C \subseteq C'_0$. Since $C \in X$, (6) implies C'_0 is self-orthogonal and hence, $C'_0 \in X'$. Suppose $C \subseteq C'$ for some $C' \in X'$. Because C' has torsion code C_2, by Lemma 2, $R_1^{k_1} [0 \ \ uD] \subseteq C'$ and so $C'_0 \subseteq C'$. Note that $|C'_0| = |C_1| \, |C_2| = q^{2k_0 + k_1} = |C'|$. Hence, $C'_0 = C'$. ■

Next, we count self-orthogonal codes C with given residue code and torsion code.

Theorem 1. *Let C_1 and C_2 be codes of length n over $\mathbb{F}_q$ where $C_1 \subseteq C_2 \subseteq C_1^{\perp}$. If* $\dim C_1 = k_0$ *and* $\dim C_2 = k_0 + k_1$, *then*

(i) the number of Euclidean self-orthogonal codes C of length n over $\mathbb{F}_q + u\mathbb{F}_q$ with $\mathrm{res}(C) = C_1$ *and* $\mathrm{tor}(C) = C_2$ *is*

$$q^{k_0(2n-3k_0-2k_1+\epsilon)/2},$$

where $\epsilon = -1$ if q is odd and $\epsilon = 1$ if q is even, and

(ii) the number of Hermitian self-orthogonal codes C of length n over $\mathbb{F}_q + u\mathbb{F}_q$ with $\mathrm{res}(C) = C_1$ *and* $\mathrm{tor}(C) = C_2$ *is*

$$q^{k_0(2n-3k_0-2k_1+1)/2}.$$

Proof. We may assume without loss of generality that C_1 and C_2 are codes with generator matrices (2) and (3), respectively. Then we have to compute $|X'|$. By Lemma 5 and Lemma 6, we have

$$\begin{aligned} q^{k_0k_1}\left|X'\right| &= \sum_{C'\in X'} \left|\{C \in X | C \subseteq C'\}\right| \\ &= \sum_{C\in X} \left|\{C' \in X' | C \subseteq C'\}\right| \\ &= \sum_{C\in X} 1 \\ &= |X|. \end{aligned}$$

The results follow from Lemma 4. ∎

4. Mass formula for self-orthogonal codes over $\mathbb{F}_q + u\mathbb{F}_q$

Let $\sigma_q(n, k_0)$ denote the number of distinct self-orthogonal codes over $\mathbb{F}_q$ of length n and dimension k_0 (see [9, 10]). We define the *Gaussian coefficient* $\begin{bmatrix} n \\ k \end{bmatrix}_q$ for $k \leq n$ as

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})},$$

which gives the number of subspaces of dimension k contained in an n-dimensional vector space over $\mathbb{F}_q$.

We now have the following mass formula for self-orthogonal codes over R_1.

Theorem 2. *Let $M_q(n,k_0,k_1)_E$ and $M_q(n,k_0,k_1)_H$ denote the number of distinct Euclidean and Hermitian self-orthogonal codes of length n over $\mathbb{F}_q+u\mathbb{F}_q$ of type $\{k_0,k_1\}$, respectively. We have*

$$M_q(n,k_0,k_1)_E=\sigma_q(n,k_0)\begin{bmatrix} n-2k_0 \\ k_1 \end{bmatrix}_q q^{k_0(2n-3k_0-2k_1+\epsilon)/2}$$

where $\epsilon=-1$ if q is odd and $\epsilon=1$ if q is even, and

$$M_q(n,k_0,k_1)_H=\sigma_q(n,k_0)\begin{bmatrix} n-2k_0 \\ k_1 \end{bmatrix}_q q^{k_0(2n-3k_0-2k_1+1)/2}.$$

Proof. If C is a self-orthogonal code of length n over $\mathbb{F}_q+u\mathbb{F}_q$ of type $\{k_0,k_1\}$, then by setting $C_1=\mathrm{res}(C)$ and $C_2=\mathrm{tor}(C)$, we see that C_1 and C_2 satisfies Lemma 1. There are $\sigma_q(n,k_0)$ self-orthogonal codes C_1 of length n over $\mathbb{F}_q$. Given C_1, there are $\begin{bmatrix} n-2k_0 \\ k_1 \end{bmatrix}_q$ codes C_2 such that $C_1\subseteq C_2\subseteq C_1^{\perp}$. Then the result follows from Theorem 1. ■

We have the following mass formula for self-dual codes over R_1 as a direct consequence of the previous theorem.

Corollary 1. *The number of distinct Euclidean self-dual codes of length n over $\mathbb{F}_q+u\mathbb{F}_q$ is given by*

$$\sum_{0\le k_0\le\lfloor\frac{n}{2}\rfloor}\sigma_q(n,k_0)q^{k_0(k_0+\epsilon)/2}, \tag{8}$$

where $\epsilon=-1$ if q is odd and $\epsilon=1$ if q is even, and the number of distinct Hermitian self-dual codes of length n over $\mathbb{F}_q+u\mathbb{F}_q$ is given by

$$\sum_{0\le k_0\le\lfloor\frac{n}{2}\rfloor}\sigma_q(n,k_0)q^{k_0(k_0+1)/2}. \tag{9}$$

Proof. Note that the number of distinct Euclidean self-dual codes and the number of distinct Hermitian self-dual codes of length n over $\mathbb{F}_q+u\mathbb{F}_q$ are given by

$$\sum_{0\le k_0\le\lfloor\frac{n}{2}\rfloor}M_q(n,k_0,n-2k_0)_E,\ \text{and}\ \sum_{0\le k_0\le\lfloor\frac{n}{2}\rfloor}M_q(n,k_0,n-2k_0)_H,$$

respectively. ■

In [6, Theorem 3], Gaborit establishes the mass formula for Hermitian self-dual codes over $\mathbb{F}_q+u\mathbb{F}_q$, but gives the formula for Euclidean self-dual codes instead. The formula (9) corrects this.

Next, we establish another formula for the number of distinct Euclidean self-orthogonal codes when the given torsion is self-orthogonal.

Corollary 2. *Suppose q is odd. The number of distinct Euclidean self-orthogonal codes of length n over $\mathbb{F}_q + u\mathbb{F}_q$ of type $\{k_0, k_1\}$ with self-orthogonal torsion is*

$$\tilde{M}_q(n, k_0, k_1)_E = \begin{bmatrix} k_0 + k_1 \\ k_0 \end{bmatrix}_q \sigma_q(n, k_0 + k_1) q^{k_0(2n-3k_0-2k_1-1)/2}.$$

Proof. Let C_1 and C_2 be self-orthogonal codes where $\dim C_1 = k_0$, $\dim C_2 = k_0 + k_1$ and $C_1 \subseteq C_2$. By Theorem 2, we have

$$\begin{aligned} \tilde{M}_q(n, k_0, k_1)_E \, q^{-k_0(2n-3k_0-2k_1-1)/2} &= \sum_{C_2 \subseteq C_2^{\perp}} |\{C_1 \mid C_1 \subseteq C_2\}| \\ &= \begin{bmatrix} k_0 + k_1 \\ k_0 \end{bmatrix}_q \left|\left\{C_2 \mid C_2 \subseteq C_2^{\perp}\right\}\right| \\ &= \begin{bmatrix} k_0 + k_1 \\ k_0 \end{bmatrix}_q \sigma_q(n, k_0 + k_1). \end{aligned}$$

■

This corollary will be useful in our mass formula computations on later chapters.

5. Classification of self-orthogonal codes over $\mathbb{F}_q + u\mathbb{F}_q$

Using Theorem 2, we classify Euclidean and Hermitian self-orthogonal codes over $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_3 + u\mathbb{F}_3$, of given type for small lengths. Note that two codes over $\mathbb{F}_2 + u\mathbb{F}_2$ are equivalent if one can be obtained from the other by permuting the coordinates and (if necessary) multiplying certain coordinates by $1 + u$. On the other hand, two Euclidean self-orthogonal codes over $\mathbb{F}_3 + u\mathbb{F}_3$ are equivalent if one can be obtained from the other by permuting the coordinates and (if necessary) multiplying certain coordinates by 2, and two Hermitian self-orthogonal codes over $\mathbb{F}_3 + u\mathbb{F}_3$ are equivalent if one can be obtained from the other by permuting the coordinates and (if necessary) multiplying certain coordinates by r, where $r \in \{2, 1 + u, 1 + 2u, 2 + u, 2 + 2u\}$.

To illustrate, we classify Euclidean self-orthogonal codes over $\mathbb{F}_3 + u\mathbb{F}_3$ of length 4 and type $\{2, 0\}$. Let C_1 and C_2 be inequivalent Euclidean self-orthogonal codes over $\mathbb{F}_3 + u\mathbb{F}_3$ of length 4 and type $\{2, 0\}$ with generator matrices

$$\begin{bmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 0 & 2+2u & 2+u \\ 0 & 1 & 2+u & 1+u \end{bmatrix},$$

respectively. The order of their automorphism groups are 48 and 24, respectively. Hence,

$$\sum_{j=1}^{2} \frac{|E_4|}{|\mathrm{Aut}(C_j)|} = \frac{2^4 \cdot 4!}{48} + \frac{2^4 \cdot 4!}{24} = 8 + 16 = 24.$$

From Theorem 2,

$$M_3(4, 2, 0)_E = \sigma_3(4, 2) \begin{bmatrix} 4 - 2 \cdot 2 \\ 0 \end{bmatrix}_3 3^{2(8-6-0-1)/2} = 8 \cdot 1 \cdot 3 = 24.$$

Therefore, there are two Euclidean self-orthogonal codes of length 4 and type $\{2, 0\}$ over $\mathbb{F}_3 + u\mathbb{F}_3$, up to equivalence.

We note that Euclidean self-orthogonal and Hermitian self-orthogonal codes coincide over $\mathbb{F}_2 + u\mathbb{F}_2$, as well as in codes over $\mathbb{F}_3 + u\mathbb{F}_3$ of type $\{0, k_1\}$.

Table 1 gives the number of inequivalent Euclidean self-orthogonal codes over $\mathbb{F}_2 + u\mathbb{F}_2$ of lengths 2 up to 7, while Table 2 gives the number of inequivalent Euclidean and Hermitian self-orthogonal codes over $\mathbb{F}_3+u\mathbb{F}_3$ of lengths 2 up to 6, for each type. Note that the code of length 1 with generator matrix $[u]$ is a Euclidean self-orthogonal and Hermitian self-orthogonal code over $\mathbb{F}_q+u\mathbb{F}_q$. Therefore, there is a self-orthogonal code for any length n, since one can just form a direct sum of this length 1 code. Our classification of self-orthogonal codes over $\mathbb{F}_2+u\mathbb{F}_2$ agrees with the enumeration in [5] for self-dual codes (codes of type $\{k_0, n-2k_0\}$) up to length $n = 7$. Generators and the order of the automorphism group of each code in Table 1 and Table 2 may be requested by the interested reader from the authors. All computer calculations in this paper were done with the help of MAGMA[4].

Table 1: The number of inequivalent self-orthogonal codes of lengths $2 \le n \le 7$ over $\mathbb{F}_2 + u\mathbb{F}_2$

$\{n, k_0, k_1\}$	Number of Codes	$\{n, k_0, k_1\}$	Number of Codes	$\{n, k_0, k_1\}$	Number of Codes
$\{2,1,0\}$	1	$\{5,2,1\}$	2	$\{6,0,6\}$	1
$\{2,0,1\}$	2	$\{5,0,1\}$	5	$\{7,1,0\}$	12
$\{2,0,2\}$	1	$\{5,0,2\}$	10	$\{7,1,1\}$	54
$\{3,1,0\}$	2	$\{5,0,3\}$	10	$\{7,1,2\}$	100
$\{3,1,1\}$	1	$\{5,0,4\}$	5	$\{7,1,3\}$	73
$\{3,0,1\}$	3	$\{5,0,5\}$	1	$\{7,1,4\}$	24
$\{3,0,2\}$	3	$\{6,1,0\}$	9	$\{7,1,5\}$	3
$\{3,0,3\}$	1	$\{6,1,1\}$	29	$\{7,2,0\}$	43
$\{4,1,0\}$	4	$\{6,1,2\}$	36	$\{7,2,1\}$	74
$\{4,1,1\}$	5	$\{6,1,3\}$	16	$\{7,2,2\}$	40
$\{4,1,2\}$	2	$\{6,1,4\}$	3	$\{7,2,3\}$	5
$\{4,2,0\}$	2	$\{6,2,0\}$	19	$\{7,3,0\}$	22
$\{4,0,1\}$	4	$\{6,2,1\}$	18	$\{7,3,1\}$	5
$\{4,0,2\}$	6	$\{6,2,2\}$	5	$\{7,0,1\}$	7
$\{4,0,3\}$	4	$\{6,3,0\}$	4	$\{7,0,2\}$	23
$\{4,0,4\}$	1	$\{6,0,1\}$	6	$\{7,0,3\}$	43
$\{5,1,0\}$	6	$\{6,0,2\}$	16	$\{7,0,4\}$	43
$\{5,1,1\}$	13	$\{6,0,3\}$	22	$\{7,0,5\}$	23
$\{5,1,2\}$	10	$\{6,0,4\}$	16	$\{7,0,6\}$	7
$\{5,1,3\}$	2	$\{6,0,5\}$	6	$\{7,0,7\}$	1
$\{5,2,0\}$	6				

Table 2: The number of inequivalent Euclidean and Hermitian self-orthogonal codes of lengths $2 \leq n \leq 6$ over $\mathbb{F}_3 + u\mathbb{F}_3$

$\{n, k_0, k_1\}$	Number of Codes		$\{n, k_0, k_1\}$	Number of Codes	
	Euclidean	Hermitian		Euclidean	Hermitian
$\{2,1,0\}$	0	0	$\{5,2,1\}$	2	1
$\{2,0,1\}$	2	2	$\{5,0,1\}$	5	5
$\{2,0,2\}$	1	1	$\{5,0,2\}$	12	12
$\{3,1,0\}$	2	1	$\{5,0,3\}$	12	12
$\{3,1,1\}$	1	1	$\{5,0,4\}$	5	5
$\{3,0,1\}$	3	3	$\{5,0,5\}$	1	1
$\{3,0,2\}$	3	3	$\{6,1,0\}$	12	5
$\{3,0,3\}$	1	1	$\{6,1,1\}$	57	27
$\{4,1,0\}$	4	2	$\{6,1,2\}$	64	34
$\{4,1,1\}$	6	4	$\{6,1,3\}$	20	13
$\{4,1,2\}$	1	1	$\{6,1,4\}$	2	2
$\{4,2,0\}$	2	1	$\{6,2,0\}$	22	8
$\{4,0,1\}$	4	4	$\{6,2,1\}$	18	9
$\{4,0,2\}$	7	7	$\{6,2,2\}$	4	3
$\{4,0,3\}$	4	4	$\{6,3,0\}$	0	0
$\{4,0,4\}$	1	1	$\{6,0,1\}$	6	6
$\{5,1,0\}$	6	3	$\{6,0,2\}$	20	20
$\{5,1,1\}$	19	11	$\{6,0,3\}$	31	31
$\{5,1,2\}$	10	7	$\{6,0,4\}$	20	20
$\{5,1,3\}$	1	1	$\{6,0,5\}$	6	6
$\{5,2,0\}$	4	2	$\{6,0,6\}$	1	1

6. Codes over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$, where q is odd

For the rest of this paper, let R_2 be the commutative ring $\mathbb{F}_q[u]/(u^3) = \mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$, where $u^3 = 0$ and q is odd. We will only consider Euclidean inner product.

A code C of length n over R_2 is permutation-equivalent to a code with generator matrix

$$\begin{bmatrix} I_{k_0} & A_0 & B_0 + uB_1 + u^2B_2 \\ 0 & uI_{k_1} & uD_1 + u^2D_2 \\ 0 & 0 & u^2F_2 \end{bmatrix} \tag{10}$$

where $F_2 \in M_{k_2 \times (n-k_0-k_1)}(\mathbb{F}_q)$ and $A_0, B_0, B_1, B_2, D_1, D_2$ are matrices of appropriate sizes over $\mathbb{F}_q$. We define the torsion codes of C as follows:

$$\mathrm{tor}_0(C) = \{v \in \mathbb{F}_q^n \mid \exists w, z \in \mathbb{F}_q^n, v + uw + u^2z \in C\} \text{ and}$$

$$\mathrm{tor}_i(C) = \{v \in \mathbb{F}_q^n \mid u^i v \in C\}, \text{ for } i = 1, 2.$$

The code $\mathrm{tor}_0(C)$ is also called the residue code of C. Observe that $\mathrm{tor}_0(C) \subseteq \mathrm{tor}_1(C) \subseteq \mathrm{tor}_2(C)$. If C has generator matrix (10), then the residue code $\mathrm{tor}_0(C)$ has dimension k_0 and generator matrix

$$\begin{bmatrix} I_{k_0} & A_0 & B_0 \end{bmatrix}, \tag{11}$$

$\text{tor}_1(C)$ has dimension $k_0 + k_1$ and generator matrix

$$\begin{bmatrix} I_{k_0} & A_0 & B_0 \\ 0 & I_{k_1} & D_1 \end{bmatrix} \tag{12}$$

and $\text{tor}_2(C)$ has dimension $k_0 + k_1 + k_2$ and generator matrix

$$\begin{bmatrix} I_{k_0} & A_0 & B_0 \\ 0 & I_{k_1} & D_1 \\ 0 & 0 & F_2 \end{bmatrix} \tag{13}$$

where F_2 is of full row rank. The code C is of type $\{k_0, k_1, k_2\}$ and

$$|C| = |\text{tor}_0(C)|\,|\text{tor}_1(C)|\,|\text{tor}_2(C)| = q^{3k_0+2k_1+k_2}.$$

Suppose C is self-orthogonal. Then

$$\begin{aligned} I_{k_0} + A_0A_0^T + B_0B_0^T + u(B_0B_1^T + B_1B_0^T) & \\ +u^2(B_0B_2^T + B_1B_1^T + B_2B_0^T) &\equiv 0\ (u^3) \\ u(A_0 + B_0D_1^T) + u^2(B_1D_1^T + B_0D_2^T) &\equiv 0\ (u^3) \\ u^2(B_0F_2^T) &\equiv 0\ (u^3) \\ u^2(I_{k_1} + D_1D_1^T) &\equiv 0\ (u^3) \end{aligned}$$

which give the following:

$$I_{k_0} + A_0A_0^T + B_0B_0^T \equiv 0\ (u) \tag{14}$$
$$B_0B_1^T + B_1B_0^T \equiv 0\ (u) \tag{15}$$
$$B_0B_2^T + B_1B_1^T + B_2B_0^T \equiv 0\ (u) \tag{16}$$
$$A_0 + B_0D_1^T \equiv 0\ (u) \tag{17}$$
$$B_1D_1^T + B_0D_2^T \equiv 0\ (u) \tag{18}$$
$$F_2B_0^T \equiv 0\ (u) \tag{19}$$
$$I_{k_1} + D_1D_1^T \equiv 0\ (u). \tag{20}$$

From (14), $\text{tor}_0(C)$ is self-orthogonal and by (14), (17) and (20), we have

$$\text{tor}_1(C) \subseteq \text{tor}_1(C)^\perp,$$

that is, $\text{tor}_1(C)$ is self-orthogonal. Moreover, by (14), (17) and (19) we have

$$\text{tor}_0(C) \subseteq \text{tor}_2(C)^\perp.$$

We will introduce another type of residue for a code over R_2.

Definition 1. *Let C be a code over R_2. The code over $\mathbb{F}_q + u\mathbb{F}_q$ obtained from C by reduction modulo u^2 is called the u^2-*Residue of C *and will be denoted by Res*(C).

It is easy to see that a generator matrix for Res(C) is

$$\begin{bmatrix} I_{k_0} & A_0 & B_0 + uB_1 \\ 0 & uI_{k_1} & uD_1 \end{bmatrix}.$$

It is also clear that res(Res(C)) = tor$_0(C)$, tor(Res(C)) = tor$_1(C)$, and Res(C) is of type $\{k_0, k_1\}$.

If C is self-orthogonal, by (14), (15) and (17) we have

$$\text{Res}(C) \subseteq \text{Res}(C)^{\perp},$$

that is, Res(C) is self-orthogonal of type $\{k_0, k_1\}$. Also, since

$$\text{tor}(\text{Res}(C)) = \text{tor}_1(C) \subseteq \text{tor}_2(C)$$

and

$$\text{tor}_2(C) \subseteq \text{tor}_0(C)^{\perp} = \text{res}(\text{Res}(C))^{\perp},$$

we have

$$\text{tor}(\text{Res}(C)) \subseteq \text{tor}_2(C) \subseteq \text{res}(\text{Res}(C))^{\perp}$$

which gives the following lemma.

Lemma 7. *Let C be a self-orthogonal code over R_2 of type $\{k_0, k_1, k_2\}$ and let C_1 =Res(C) and C_2 =tor$_2(C)$. Then*

(i) $C_1 \subseteq C_1^{\perp}$,

(ii) tor$(C_1) \subseteq$ tor$(C_1)^{\perp}$, *and*

(iii) tor$(C_1) \subseteq C_2 \subseteq$ res$(C_1)^{\perp}$, dim $C_2 = k_0 + k_1 + k_2$.

7. Codes over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ with prescribed u^2-Residue and torsion

For the rest of this chapter, we let C_1 be a self-orthogonal code over R_1 of type $\{k_0, k_1\}$ such that tor(C_1) is self-orthogonal. We assume without loss of generality that C_1 has generator matrix

$$G_1 = \begin{bmatrix} I_{k_0} & A_0 & B_0 + uB_1 \\ 0 & uI_{k_1} & uD_1 \end{bmatrix}.$$

Since C_1 is self-orthogonal, we have

$$\begin{aligned} I_{k_0} + A_0A_0^T + B_0B_0^T + u(A_0A_1^T + A_1A_0^T + B_0B_1^T + B_1B_0^T) &\equiv 0 \ (u^2) \\ u(A_0 + B_0D_1^T) &\equiv 0 \ (u^2) \end{aligned}$$

which are equivalent to (14), (15) and (17). Moreover, since tor(C_1) is self-orthogonal, we have

$$I_{k_0} + A_0A_0^T + B_0B_0^T \equiv 0 \ (u)$$

$$\begin{aligned} A_0 + B_0 D_1^T &\equiv 0\ (u) \\ I_{k_1} + D_1 D_1^T &\equiv 0\ (u) \end{aligned}$$

which are equivalent to (14), (17) and (19).

Now, notice that from (17), we have

$$A_0 \equiv -B_0 D_1^T\ (u).$$

By (14), we have

$$\begin{aligned} I_{k_0} + B_0 D_1^T D_1 B_0^T + B_0 B_0^T &\equiv 0\ (u) \\ I_{k_0} + B_0 \left(D_1^T D_1 B + I_{k_0} \right) B_0^T &\equiv 0\ (u) \end{aligned}$$

which implies B_0 is of full row rank.

We start by counting the number of self-orthogonal codes C of type $\{k_0, k_1, 0\}$ such that $\mathrm{Res}(C) = C_1$. Similar to what we did in the previous chapter, we first exhibit the generator matrix of such code C.

Lemma 8. *If C is a code over R_2 of type $\{k_0, k_1, 0\}$ and Res$(C) = C_1$, then there exist matrices $N_0 \in M_{k_0 \times (n-k_0-k_1)}(\mathbb{F}_q)$ and $N_1 \in M_{k_1 \times (n-k_0-k_1)}(\mathbb{F}_q)$ such that*

$$\begin{bmatrix} I_{k_0} & A_0 & B_0 + uB_1 + u^2 N_0 \\ 0 & uI_{k_1} & uD_1 + u^2 N_1 \end{bmatrix} \tag{21}$$

is a generator matrix for C. The matrices N_0 and N_1 are unique.

Proof. If C is a code over R_2 of type $\{k_0, k_1, 0\}$ such that $\mathrm{Res}(C) = C_1$, then for some matrices M_1, M_2, M_3, M_4 and M_5 over $\mathbb{F}_q$ of appropriate sizes,

$$R_2^{k_0+k_1} \begin{bmatrix} I_{k_0} + u^2 M_1 & A_0 + u^2 M_2 & B_0 + uB_1 + u^2 M_3 \\ 0 & I_{k_1} + u^2 M_4 & D_1 + u^2 M_5 \end{bmatrix} \subseteq C.$$

Applying elementary row operations,

$$\begin{bmatrix} I_{k_0} - u^2 M_1 & 0 \\ 0 & I_{k_1} - u^2 M_4 \end{bmatrix} \begin{bmatrix} I_{k_0} + u^2 M_1 & A_0 + u^2 M_2 & B_0 + uB_1 + u^2 M_3 \\ 0 & I_{k_1} + u^2 M_4 & D_1 + u^2 M_5 \end{bmatrix} =$$

$$\begin{bmatrix} I_{k_0} & A_0 + u^2(M_2 - M_1 A_0) & B_0 + uB_1 + u^2(M_3 - M_1 B_0) \\ 0 & I_{k_1} & D_1 + u^2(M_5 - M_4 D_1) \end{bmatrix}$$

and

$$\begin{bmatrix} I_{k_0} & -u^2(M_2 - M_1 A_0) \\ 0 & I_{k_1} \end{bmatrix} \begin{bmatrix} I_{k_0} & A_0 + u^2(M_2 - M_1 A_0) & B_0 + uB_1 + u^2(M_3 - M_1 B_0) \\ 0 & I_{k_1} & D_1 + u^2(M_5 - M_4 D_1) \end{bmatrix}$$

$$= \begin{bmatrix} I_{k_0} & A_0 & B_0 + uB_1 + u^2(M_3 - M_1 B_0 - M_2 D_1 + M_1 A_0 D_1) \\ 0 & I_{k_1} & D_1 + u^2(M_5 - M_4 D_1) \end{bmatrix}.$$

Letting

$$\begin{aligned} N_0 &= M_3 - M_1B_0 - M_2D_1 + M_1A_0D_1 \\ N_1 &= M_5 - M_4D_1, \end{aligned}$$

we have

$$R_2^{k_0+k_1}\begin{bmatrix} I_{k_0} & A_0 & B_0+uB_1+u^2N_0 \\ 0 & uI_{k_1} & uD_1+u^2N_1 \end{bmatrix} \subseteq C.$$

Therefore,

$$\begin{aligned} |C| &\geq \left| R_2^{k_0+k_1}\begin{bmatrix} I_{k_0} & A_0 & B_0+uB_1+u^2N_0 \\ 0 & uI_{k_1} & uD_1+u^2N_1 \end{bmatrix} \right| \\ &= q^{k_0+k_1}q^{2k_0+k_1} \\ &= q^{3k_0+2k_1} \\ &= |C| \end{aligned}$$

and hence, (21) is a generator matrix for C.

Next, we show uniqueness of the matrices N_0 and N_1 over $\mathbb{F}_q$. Suppose there exist matrices $N_0' \in M_{k_0\times(n-k_0-k_1)}(\mathbb{F}_q)$ and $N_1' \in M_{k_1\times(n-k_0-k_1)}(\mathbb{F}_q)$ such that

$$R_2^{k_0+k_1}\begin{bmatrix} I_{k_0} & A_0 & B_0+uB_1+u^2N_0' \\ 0 & uI_{k_1} & uD_1+u^2N_1' \end{bmatrix} = \\ R_2^{k_0+k_1}\begin{bmatrix} I_{k_0} & A_0 & B_0+uB_1+u^2N_0 \\ 0 & uI_{k_1} & uD_1+u^2N_1. \end{bmatrix}.$$

This means that

$$\begin{aligned} B_0+uB_1+u^2N_0' &\equiv B_0+uB_1+u^2N_0 \ (u^3) \\ uD_1+u^2N_1' &\equiv uD_1+u^2N_1 \ (u^3) \end{aligned}$$

which imply that

$$\begin{aligned} N_0' &\equiv N_0 \ (u) \\ N_1' &\equiv N_1 \ (u) \end{aligned}$$

and hence, N_0 and N_1 are unique. ■

This shows that the number of self-orthogonal codes C over R_2 of type $\{k_0, k_1, 0\}$ with $\text{Res}(C) = C_1$ is determined by the number of such matrices N_0 and N_1, which will be given in the next lemma.

Lemma 9. *The number of self-orthogonal codes C of type $\{k_0, k_1, 0\}$ over R_2 such that Res$(C) = C_1$ is*

$$q^{(k_0+k_1)(n-k_0-k_1)-k_0(k_0+1)/2-k_0k_1}.$$

Proof. By Lemma 8, C has generator matrix

$$\begin{bmatrix} I_{k_0} & A_0 & B_0 + uB_1 + u^2 N_0 \\ 0 & uI_{k_1} & uD_1 + u^2 N_1 \end{bmatrix}$$

for some matrices N_0, N_1 over $\mathbb{F}_q$. From this, C is self-orthogonal if and only if

$$\begin{aligned} I_{k_0} + AA_0^T + BB_0^T + u(B_0 B_1^T + B_1 B_0^T) & \\ +u^2(B_1 B_1^T + B_0 N_0^T + N_0 B_0^T) &\equiv 0\ (u^3) \qquad (22) \\ u(A_0 + B_0 D_1^T) + u^2(B_1 D_1^T + B_0 N_1^T) &\equiv 0\ (u^3). \qquad (23) \end{aligned}$$

We want to count the number of such matrices N_0 and N_1 satisfying the above equivalences. First, consider the map

$$\begin{aligned} \Phi_{B_0} : M_{k_0 \times (n-k_0-k_1)}(\mathbb{F}_q) &\longrightarrow M_{k_0}(\mathbb{F}_q) \\ N_0 &\longmapsto B_0 N_0^T + N_0 B_0^T \end{aligned}$$

as defined in the previous chapter. By (14) and (15), (22) becomes

$$B_1 B_1^T + B_0 N_0^T + N_0 B_0^T \equiv 0\ (u).$$

Hence,

$$\begin{aligned} |\{N_0 \in M_{k_0 \times (n-k_0-k_1)} | N_0 \text{ satisfies } (22)\}| &= |\{\Phi_{B_0}^{-1}(-B_1 B_1^T)\}| \\ &= |\ker \Phi_{B_0}| \\ &= \frac{\left|M_{k_0 \times (n-k_0-k_1)}\right|}{\left|\mathrm{Sym}_{k_0}(\mathbb{F}_q)\right|} \\ &= q^{k_0(n-k_0-k_1)-k_0(k_0+1)/2}. \end{aligned}$$

Define another map

$$\begin{aligned} \beta : M_{k_1 \times (n-k_0-k_1)}(\mathbb{F}_q) &\longrightarrow M_{k_0 \times k_1}(\mathbb{F}_q) \\ N_1 &\longmapsto B_0 N_1^T. \end{aligned}$$

This map is surjective because B_0 is of full row rank. Therefore by (17),

$$\begin{aligned} |\{N_1 \in M_{k_1 \times (n-k_0-k_1)} | N_1 \text{ satisfies } (23)\}| &= |\{\beta^{-1}(-B_1 D_1^T)\}| \\ &= |\ker \beta| \\ &= \frac{\left|M_{k_1 \times (n-k_0-k_1)}(\mathbb{F}_q)\right|}{|M_{k_0 \times k_1}(\mathbb{F}_q)|} \\ &= q^{k_1(n-k_0-k_1)-(k_0 k_1)}. \end{aligned}$$

Finally, the number of self-orthogonal codes C of type $\{k_0, k_1, 0\}$ over R_2 such that $\mathrm{Res}(C) = C_1$ is the number of such matrices N_0 satisfying (22) multiplied to the number of such matrices N_1 satisfying (23) which is

$$q^{k_0(n-k_0-k_1)-k_0(k_0+1)/2} q^{k_1(n-k_0-k_1)-k_0 k_1}.$$

The result follows by simplifying the above expression. ∎

For the rest of this chapter, let C_2 be a code over $\mathbb{F}_q$ with dimension $k_0 + k_1 + k_2$ and has a generator matrix

$$G_2 = \begin{bmatrix} I_{k_0} & A_0 & B_0 \\ 0 & I_{k_1} & D_1 \\ 0 & 0 & F_2 \end{bmatrix}$$

where F_2 is of full row rank. We assume that $\mathrm{tor}(C_1) \subseteq C_2 \subseteq \mathrm{res}(C_1)^{\perp}$. Hence,

$$\begin{aligned} I_{k_0} + A_0 A_0^T + B_0 B_0^T &\equiv 0\ (u) \\ A_0 + B_0 D_1^T &\equiv 0\ (u) \\ F_2 B_0^T &\equiv 0\ (u) \end{aligned}$$

which are equivalent to (14), (17) and (19), respectively.

Consider the following sets of codes over R_2:

$$\begin{aligned} Y &= \{C \mid C \text{ is self-orthogonal of type } \{k_0, k_1, 0\}, \mathrm{Res}(C) = C_1\}\,; \\ Y' &= \left\{C' \mid C' \text{ is self-orthogonal}, \mathrm{Res}(C') = C_1, \mathrm{tor}_2(C') = C_2\right\}. \end{aligned}$$

Note that $|Y|$ is already given in Lemma 9. Our next goal is to compute for $|Y'|$. This will be done in the same way as in the previous chapter.

Lemma 10. *If $C \in Y$, then there exists a unique $C' \in Y'$ such that $C \subseteq C'$.*

Proof. Since $C \in Y$, C has generator matrix (21) for some matrices N_0 and N_1. Suppose $C \subseteq C'$ for some $C' \in Y'$ and there exists a code C'' with generator matrix

$$\begin{bmatrix} I_{k_0} & A_0 & B_0 + uB_1 + u^2 N_0 \\ 0 & uI_{k_1} & uD_1 + u^2 N_1 \\ 0 & 0 & u^2 F_2 \end{bmatrix}.$$

Clearly, $C \subseteq C''$. Note that C'' satisfies $\mathrm{Res}(C'') = C_1$ and $\mathrm{tor}_2(C'') = C_2$. Using (19), we conclude that C'' is self-orthogonal. Hence, $C'' \in Y'$.

Next, notice that $R_2^{k_2}[0\ 0\ u^2 F_2] \subseteq C'$. This, together with the fact that $C \subseteq C'$, forces $C'' \subseteq C'$. But

$$\begin{aligned} |C''| &= |C_1||C_2| \\ &= q^{2k_0+k_1} q^{k_0+k_1+k_2} \\ &= q^{3k_0+2k_1+k_2} \\ &= |C'| \end{aligned}$$

and therefore, $C' = C''$. ∎

Lemma 11. *Let $C' \in Y'$. Then $|\{C \in Y \mid C \subseteq C'\}| = q^{(k_0+k_1)k_2}$.*

Proof. Let $C' \in Y'$ whose generator matrix is

$$\begin{bmatrix} I_{k_0} & A_0 & B_0 + uB_1 + u^2N_0 \\ 0 & uI_{k_1} & uD_1 + u^2N_1 \\ 0 & 0 & u^2F_2 \end{bmatrix}.$$

Define the map $\Psi : M_{k_0\times k_2}(\mathbb{F}_q) \times M_{k_1\times k_2}(\mathbb{F}_q) \longrightarrow \{C \in Y \mid C \subseteq C'\}$ as

$$\Psi\left(M', M''\right) = R_2^{k_0+k_1}\begin{bmatrix} I_{k_0} & A_0 & B_0 + uB_1 + u^2(N_0 + M'F_2) \\ 0 & uI_{k_1} & uD_1 + u^2(N_1 + M''F_2) \end{bmatrix}$$

and claim that this map is bijective.

Indeed, Ψ is injective because F_2 is of full row rank. Now, suppose $C \in Y$ such that $C \subseteq C'$. Then by Lemma 8, C has generator matrix

$$\begin{bmatrix} I_{k_0} & A_0 & B_0 + uB_1 + u^2F' \\ 0 & uI_{k_1} & uD_1 + u^2F'' \end{bmatrix}$$

for some matrices F' and F''. Since $C \subseteq C'$, there exist matrices M' and M'' such that

$$\begin{bmatrix} I_{k_0} & A_0 & B_0 + uB_1 + u^2F' \\ 0 & uI_{k_1} & uD_1 + u^2F'' \end{bmatrix} \equiv$$

$$\begin{bmatrix} I_{k_0} & 0 & M' \\ 0 & I_{k_1} & M'' \end{bmatrix}\begin{bmatrix} I_{k_0} & A_0 & B_0 + uB_1 + u^2N_0 \\ 0 & uI_{k_1} & uD_1 + u^2N_1 \\ 0 & 0 & u^2F_2 \end{bmatrix}(u^3).$$

Then we have $F' = N_0 + M'F_2$ and $F_2 = N_1 + M''F_2$, so Ψ is surjective and hence, bijective.

Therefore,

$$\begin{aligned} |\left\{C \in Y \mid C \subseteq C'\right\}| &= |M_{k_0\times k_2}(\mathbb{F}_q) \times M_{k_1\times k_2}(\mathbb{F}_q)| \\ &= q^{k_0k_2}q^{k_1k_2} \\ &= q^{(k_0+k_1)k_2}. \end{aligned}$$

■

Given C_1 and C_2, we can now count the number of self-orthogonal codes over R_2 having u^2-Residue C_1 and torsion C_2.

Theorem 3. *Suppose C_1 is a self-orthogonal code over $\mathbb{F}_q + u\mathbb{F}_q$, where q is odd, of type $\{k_0, k_1\}$ such that* $\operatorname{tor}(C_1)$ *is self-orthogonal and C_2 is a code over $\mathbb{F}_q$ of dimension $k_0 + k_1 + k_2$ such that* $\operatorname{tor}(C_1) \subseteq C_2 \subseteq \operatorname{res}(C_1)^\perp$. *Then the number of self-orthogonal codes C' of length n over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$ such that* $\operatorname{Res}(C') = C_1$ *and* $\operatorname{tor}_2(C') = C_2$ *is*

$$q^{k_0(2n-3k_0-6k_1-2k_2-1)/2+k_1(n-k_1-k_2)}.$$

Proof. Without loss of generality, we assume that C_1 has generator matrix G_1 and C_2 has generator matrix G_2. Then we compute for $|Y'|$. By Lemma 10 and Lemma 11, we have

$$\begin{aligned} q^{(k_0+k_1)k_2}\left|Y'\right| &= \sum_{C'\in Y'}\left|\{C\in X|C\subseteq C'\}\right| \\ &= \sum_{C\in Y}\left|\{C'\in X'|C\subseteq C'\}\right| \\ &= \sum_{C\in Y} 1 \\ &= |Y|. \end{aligned}$$

The results follow from Lemma 9. ■

8. Mass formula for self-orthogonal codes over $\mathbb{F}_q+u\mathbb{F}_q+u^2\mathbb{F}_q$, where q is odd

We now have the following theorem.

Theorem 4. *Suppose q is odd. The number of distinct self-orthogonal codes over $\mathbb{F}_q+u\mathbb{F}_q+u^2\mathbb{F}_q$ of length n and type $\{k_0,k_1,k_2\}$, denoted by $M_{R_2}(n,k_0,k_1,k_2)$ is*

$$\begin{bmatrix} n-2k_0-k_1 \\ k_2 \end{bmatrix}_q \begin{bmatrix} k_0+k_1 \\ k_0 \end{bmatrix}_q \sigma_q(n,k_0+k_1)q^{k_0(2n-3k_0-4k_1-k_2-1)+k_1(n-k_1-k_2)}.$$

Proof. If C is a self-orthogonal code of length n over $\mathbb{F}_q+u\mathbb{F}_q+u^2\mathbb{F}_q$ of type $\{k_0,k_1,k_2\}$, then by setting $C_1=\mathrm{Res}(C)$ and $C_2=\mathrm{tor}_2(C)$, we see that C_1 and C_2 satisfies (i)–(iii) of Lemma 7. The number of self-orthogonal codes with given u^2-Residue C_1 and torsion C_2 is given in Theorem 3. The number of self-orthogonal codes C_1 over $\mathbb{F}_q+u\mathbb{F}_q$ satisfying (i) and (ii) is given in Corollary 2. The number of codes C_2 satisfying (iii) is $\begin{bmatrix} n-2k_0-k_1 \\ k_2 \end{bmatrix}_q$. The value of $M_{R_2}(n,k_0,k_1,k_2)$ is obtained by the product of these. ■

We now have the following mass formula for self-dual codes over R_2 as a direct consequence of Theorem 4.

Corollary 3. *Suppose q is odd. The number of distinct self-dual codes of even length n over $\mathbb{F}_q+u\mathbb{F}_q+u^2\mathbb{F}_q$ is given by*

$$\sum_{k_0=0}^{\frac{n}{2}} M_{R_2}(n,k_0,\frac{n}{2}-k_0,\frac{n}{2}-k_0). \tag{24}$$

Proof. By [3], we have $k_1=k_2$ and $n=2(k_0+k_1)$. The result follows from Theorem 4. ■

The formula (24) agrees with [3, Theorem 1].

Acknowledgements

The authors gratefully acknowledge the support of the University of the Philippines Office of the Vice President for Academic Affairs for this project. The authors also thank Dr. Markus Grassl for useful suggestions and the reviewers for their valuable comments.

References

[1] Koichi Betsumiya, Rowena Alma Betty, and Akihiro Munemasa. Mass formula for even codes over $\mathbb{Z}_8$. *Lecture Notes in Computer Science*, 5921:65–77, 2009.

[2] Rowena Alma Betty and Akihiro Munemasa. Mass formula for self-orthogonal codes over $\mathbb{Z}_{p^2}$. *Journal of Combinatorics, Information and System Sciences*, 34:51–66, 2009.

[3] Rowena Alma Betty, Trilbe Lizann Vasquez, and Fidel Nemenzo. Mass formula for self-dual codes over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$. *Journal of Applied Mathematics and Computing*, 57:523–546, 2018.

[4] Wieb Bosma, John Cannon, and Catherine Playoust. The magma algebra system I: The user language. *Journal of Symbolic Computation*, 24(3-4):235–265, 1997.

[5] Steven Dougherty, Philippe Gaborit, Masaaki Harada, and Patrick Solé. Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$. *IEEE Transactions on Information Theory*, 45(1):32–45, 1999.

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

[7] A Roger Hammons, P Vijay Kumar, A Robert Calderbank, Neil JA Sloane, and Patrick Solé. The z_4-linearity of Kerdock, Preparata, Goethals, and related codes. *IEEE Transactions on Information Theory*, 40(2):301–319, 1994.

[8] W Cary Huffman and Vera Pless. *Fundamentals of error-correcting codes.* Cambridge University Press, 2010.

[9] Vera Pless. Number of isotropic subspaces in a finite geometry. *Atti della accademia nazionale dei lincei rendiconti-classe di scienze fisiche-matematiche & naturali*, 39(6):418, 1965.

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

[11] Eric M Rains and NJA Sloane. Self-dual codes, in Handbook of coding theory. *Elsevier, Amsterdam*, pages 177–294, 1998.