On Linear Codes over $\mathbb{Z}_{2^m} + v\mathbb{Z}_{2^m}$

Sri Rosdiana, Intan Muchtadi-Alamsyah, Djoko Suprijanto, and Aleams Barra

***Abstract*—We present structural properties of linear codes over the ring $\mathbb{Z}_{2^m} + v\mathbb{Z}_{2^m}$ where $v^2 = v$ as a generalization of specific Gao's results for the ring $\mathbb{Z}_4 + v\mathbb{Z}_4$ where $v^2 = v$. First, we study a structure of the ring $\mathbb{Z}_{2^m} + v\mathbb{Z}_{2^m}$ where $v^2 = v$ and properties of linear codes over this ring, via a Gray map. Further, we consider MacWilliams relations, MDS codes, as well as Euclidean self-dual codes over this ring.**

***Index Terms*—linear codes, Gray map, euclidean self dual, MacWilliams relations, character.**

I. Introduction

BLAKE introduced codes over finite rings in the 1970s in order to find possible good codes (see [1],[2]). In [1], he studied the construction of codes over $\mathbb{Z}_m$, where m is a product of distinct prime p_i, from cyclic codes over $GF(p_i)$. Then, in [2], he studied the structure of codes over ring $\mathbb{Z}_q$, where $q = p^r$. Blake's result was generalized by Spiegel in [3] and [4] to the codes over $\mathbb{Z}_m$ for any positive integer m. Codes over finite rings started to become more interesting through the work of Hammons Kumar, Calderbank, Sloane, and Solé [5]. Hammons et al. [5] studied a nonlinear binary code associated with a linear code over $\mathbb{Z}_4$. In 2014, Yildiz and Karadeniz [6] studied linear codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, where $u^2 = 0$. Among their results are the MacWilliams relations for Lee, complete, and symmetrized weight enumerators. Recently, certain similar aspects are also studied by Gao and his coauthors for linear codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$ and over $\mathbb{Z}_9 + v\mathbb{Z}_9$, where $v^2 = v$ ([7], [8]).

In this paper, we present the structures and properties of linear codes over a finite ring $\mathbb{Z}_{2^m} + v\mathbb{Z}_{2^m}$, where $v^2 = v$, as a generalization of specific results by Gao et al. in [7]. The basic structure of the ring $\mathbb{Z}_{2^m} + v\mathbb{Z}_{2^m}$ is presented in Section 2, meanwhile in Section 3, we consider linear codes over finite ring $\mathbb{Z}_{2^m} + v\mathbb{Z}_{2^m}$, show the MacWilliams relations for these codes and study MDS codes over the ring. In Section 4, we then observe some properties of self-dual codes over $\mathbb{Z}_{2^m} + v\mathbb{Z}_{2^m}$.

II. Linear Codes over $\mathbb{Z}_{2^m} + v\mathbb{Z}_{2^m}$

A. Basic Structure of $\mathbb{Z}_{2^m} + v\mathbb{Z}_{2^m}$

From now on, we denote the ring $\mathbb{Z}_{2^m} + v\mathbb{Z}_{2^m}$, where $v^2 = v$, by R. Ring R is commutative and has characteristic 2^m. Ring R is isomorphic to $\mathbb{Z}_{2^m}[v]/\langle v^2 - v\rangle$. Any element $r = a + bv \in R$ is unit if and only if a and $a + b$ are both units in $\mathbb{Z}_{2^m}$.

It is shown in Lemma II.1 that R is a principal ideal ring, and by [9], R is a Frobenius ring.

Lemma II.1. *R is a principal ideal ring.*

Proof: Consider the following two surjective ring homomorphisms

$$\varphi : R \ni a + bv \longmapsto a \in \mathbb{Z}_{2^m},$$

and

$$\psi : R \ni a + bv \longmapsto a + b \in \mathbb{Z}_{2^m}.$$

Let I be an ideal in R. Since $\varphi(I) = \{\varphi(r) : r \in I\}$ and $\psi(I) = \{\psi(r) : r \in R\}$ are ideals in the principal ideal ring $\mathbb{Z}_{2^m}$, then $\varphi(I) = \langle c\rangle$ and $\psi(I) = \langle d\rangle$ for some $c, d \in \mathbb{Z}_{2^m}$.

We claim that $I = \langle (1 - v)c + vd\rangle$. Let $r = a + bv \in I$. Since $a = \varphi(r) \in \langle c\rangle$ and $a + b = \psi(r) \in \langle d\rangle$, we can write $a = ce$ and $a + b = df$ for some $e, f \in \mathbb{Z}_{2^m}$. Note that

$$\begin{aligned} r &= a + bv \\ &= a(1 - v) + (a + b)v \\ &= ce(1 - v) + dfv \\ &= (c(1 - v) + dv)\,(e(1 - v) + fv)\,. \end{aligned}$$

It follows that $I \subseteq \langle (1 - v)c + vd\rangle$.

Conversely, since $c \in \varphi(I)$ and $d \in \psi(I)$ there are $c + sv, m + nv \in I$ such that $\varphi(c + sv) = c$ and $\psi(m + nv) = m + n = d$. Note that

$$(1 - v)c = (1 - v)(c + sv) \in I$$

and

$$dv = (m + n)v = (m + nv)v \in I$$

hence $(1 - v)c + dv \in I$ and therefore $\langle (1 - v)c + dv\rangle \subseteq I$. ■

B. Linear Codes over R

A linear code $\mathtt{C}$ of length n over the ring R is an R-submodule of R^n. Ring R can be represented in another way as $R = v\mathbb{Z}_{2^m} \oplus (1 - v)\mathbb{Z}_{2^m}$. Following [10], we define the Lee weight of the elements in $\mathbb{Z}_{2^m}$ as:

$$w_L(x) = \begin{cases} x, & \text{if } x \le 2^{m-1} \\ 2^m - x, & \text{if } x > 2^{m-1} \end{cases} \tag{1}$$

First, we define a Gray map $\phi : R \longrightarrow \mathbb{Z}_{2^m}^2$ by $\phi(a+bv) = (a, a + b)$. Then we extend this map into a Gray map from R^n to $\mathbb{Z}_{2^m}^{2n}$ by

$$\begin{aligned} \phi : R^n &\longrightarrow \mathbb{Z}_{2^m}^{2n} \\ (r_0, r_1, \ldots, r_{n-1}) &\longmapsto (\phi(r_0), \phi(r_1), \ldots, \phi(r_{n-1})). \end{aligned}$$

Manuscript received July 31st, 2020; revised September 28th, 2020.

Sri Rosdiana is with 1) Algebra Research Group, Faculty of Mathematics and Natural Sciences, Institut Teknologi Bandung, Jalan Ganesha No.10 Bandung 40132, Indonesia. 2) Politeknik Siber dan Sandi Negara, Jl. Raya Haji Usa, Putat Nutug, Ciseeng, Putat Nutug, Kec. Ciseeng, Bogor, Jawa Barat 16120, Indonesia. e-mail: sri.rosdiana@s.itb.ac.id, sri.rosdiana@poltekssn.ac.id.

Intan Muchtadi-Alamsyah and Aleams Barra are with Algebra Research Group, Faculty of Mathemathics and Natural Sciences, Institut Teknologi Bandung, Jalan Ganesha No.10 Bandung 40132, Indonesia. e-mail: ntan@math.itb.ac.id, barra@math.itb.ac.id

Djoko Suprijanto is with Combinatorial Mathematics Research Group, Faculty of Mathemathics and Natural Sciences, Institut Teknologi Bandung, Jalan Ganesha No.10 Bandung 40132, Indonesia. e-mail: djoko@math.itb.ac.id

Definition II.2. *The Gray weight for any element of R is defined by*

$$w_G(a+bv) = w_L(a) + w_L(a+b),$$

where $w_L(a)$, $w_L(a+b)$ denotes the Lee weight of elements $a, a+b \in \mathbb{Z}_{2^m}$.

By extending the Definition II.2 we could define the Gray weight on R^n. The Gray weight of $\mathbf{c} := (c_0, c_1, \cdots, c_{n-1}) \in R^n$ is defined as $w_G(\mathbf{c}) = \sum_{i=0}^{n-1} w_G(c_i)$. For $\mathbf{c}_1, \mathbf{c}_2 \in R^n$, the Gray distance between $\mathbf{c}_1$ and $\mathbf{c}_2$ is defined by $d_G(\mathbf{c}_1, \mathbf{c}_2) = w_G(\mathbf{c}_1 - \mathbf{c}_2)$; and Hamming distance is defined by $d_H(\mathbf{c}_1, \mathbf{c}_2) = w_H(\mathbf{c}_1 - \mathbf{c}_2)$. Similarly, the Lee distance between $\mathbf{c} \in R^n$ and $\mathbf{d} \in R^n$ is defined by $d_L(\mathbf{c}, \mathbf{d}) = w_L(\mathbf{c} - \mathbf{d}) = \sum_{i=1}^{n} w_L(c_i - d_i)$.

The following proposition shows that the Gray map is an isometry.

Proposition II.3. *Let $\phi : R^n \to \mathbb{Z}_{2^m}^{2n}$ be the Gray map. Then ϕ is linear over $\mathbb{Z}_{2^m}$and ϕ is a distance preserving map from Gray distance R with length n to Lee distance $\mathbb{Z}_{2^m}$ with length $2n$.*

Proof:

It is clear that ϕ is linear and by using definition of Gray weight, we have $d_G(\mathbf{c}, \mathbf{d}) = w_G(\mathbf{c} - \mathbf{d}) = w_L(\phi(\mathbf{c} - \mathbf{d})) = w_L(\phi(\mathbf{c}) - \phi(\mathbf{d})) = d_L(\phi(\mathbf{c}), \phi(\mathbf{d}))$.

■

By using the above proposition, it is easy to prove the following lemma.

Lemma II.4. *If $\mathtt{C}$ is an $[n, M, d_G]$ linear code over R, then $\phi(\mathtt{C})$ is a $[2n, M, d_L]$ linear code over $\mathbb{Z}_{2^m}$.*

III. The Dual and MacWilliams Relations

In section II, we have already learned about the basic structure of linear codes over ring R. In this section, we present the implementation of dual and MacWilliams relations over ring R.

A. The Dual of Linear Codes over R

First, we define the Euclidean inner product on R^n as follows:

$$(x_0, x_1, \cdots, x_{n-1}) \cdot (y_0, y_1, \cdots, y_{n-1}) = x_0y_0 + x_1y_1 + \cdots + x_{n-1}y_{n-1}.$$

Moreover, we define the Euclidean dual code of $\mathtt{C}$ as:

$$\mathtt{C}^{\perp} = \{\mathbf{x} \in R^n : \mathbf{x} \cdot \mathbf{c} = 0 \ \text{ for all } \mathbf{c} \in \mathtt{C}\}$$

A code $\mathtt{C}$ is called Euclidean self-orthogonal if $\mathtt{C} \subseteq \mathtt{C}^{\perp}$, and $\mathtt{C}$ is called Euclidean self-dual if $\mathtt{C} = \mathtt{C}^{\perp}$.

Lemma III.1. 1) *If $\mathtt{C}$ is a linear code, then $\phi(\mathtt{C})^{\perp} = \phi(\mathtt{C}^{\perp})$.*

2) *If $\mathtt{C}$ is Euclidean self-dual, then $\phi(\mathtt{C})$ is Euclidean self-dual.*

Proof:

1) Let $\mathbf{c} = (c_0, c_1, \cdots, c_{n-1}) \in \mathtt{C}$ and $\mathbf{d} = (d_0, d_1, \cdots, d_{n-1}) \in \mathtt{C}^{\perp}$, where $c_i = a_i + b_iv, d_i = e_i + f_iv$, $a_i, b_i, e_i, f_i \in \mathbb{Z}_{2^m},\ i = 0, 1, 2, \cdots, n-1$.

We see that

$$\begin{aligned}\mathbf{c} \cdot \mathbf{d} &= c_0d_0 + c_1d_1 + \cdots + c_{n-1}d_{n-1} \\ &= \sum_{i=0}^{n-1}(a_i + b_iv)(e_i + f_iv) \\ &= \sum_{i=0}^{n-1} a_ie_i + \sum_{i=0}^{n-1}(e_ib_i + a_if_i + b_if_i)v.\end{aligned}$$

Since $\mathbf{c} \cdot \mathbf{d} = 0$, then $\sum_{i=0}^{n-1} a_ie_i = 0$ and $\sum_{i=0}^{n-1}(e_ib_i + a_if_i + b_if_i) = 0$. So,

$$\begin{aligned}\phi(\mathbf{c}) \cdot \phi(\mathbf{d}) &= \phi(c_0, \cdots, c_{n-1}) \cdot \phi(d_0, \cdots, d_{n-1}) \\ &= \phi(a_0 + b_0v, \cdots, a_{n-1} + b_{n-1}v) \cdot \\ &\quad \phi(e_0 + f_0v, \cdots e_{n-1} + f_{n-1}v) \\ &= (a_0, a_0 + b_0, \cdots, a_{n-1}, a_{n-1} + b_{n-1}) \cdot \\ &\quad (e_0, e_0 + f_0, \cdots, e_{n-1}, e_{n-1} + f_{n-1}) \\ &= (a_0e_0 + (a_0 + b_0)(e_0 + f_0) + \cdots + \\ &\quad a_{n-1}b_{n-1} + (a_{n-1} + b_{n-1})(e_{n-1} + f_{n-1}) \\ &= \sum_{i=0}^{n-1} a_ie_i + \sum_{i=0}^{n-1}(e_ib_i + a_if_i + b_if_i) + \sum_{i=0}^{n-1} a_ie_i \\ &= 0.\end{aligned}$$

Now, $\phi(\mathbf{d}) \in \phi(\mathtt{C}^{\perp})$ and $\phi(\mathbf{c}) \cdot \phi(\mathbf{d}) = 0$, hence $\phi(\mathbf{d}) \in \phi(\mathtt{C})^{\perp}$. Therefore, $\phi(\mathtt{C}^{\perp}) \subseteq \phi(\mathtt{C})^{\perp}$.

Moreover, it is easy to verify that ϕ is bijective, and then we have $|\phi(\mathtt{C}^{\perp})| = |\phi(\mathtt{C})^{\perp}|$. Hence, it implies $\phi(\mathtt{C}^{\perp}) = \phi(\mathtt{C})^{\perp}$.

2) Let $\mathtt{C}$ be Euclidean self-dual, $\mathtt{C} = \mathtt{C}^{\perp}$, then $\phi(\mathtt{C}) = \phi(\mathtt{C}^{\perp}) \subseteq \phi(\mathtt{C})^{\perp}$. So $\phi(\mathtt{C})$ is self-orthogonal. By Lemma II.4, we have $|\phi(\mathtt{C})| = |\mathtt{C}| = (2^m)^{n/2}$. Hence, $\phi(\mathtt{C})$ is a Euclidean self-dual.

■

Next, we present a MacWilliams relation of linear codes over the ring R.

B. MacWilliams Relations

Let $\mathtt{C}$ be a linear code with length n over R. For all a in R and $\mathbf{c} = (c_0, c_1, ..., c_{n-1}) \in R^n$, define the weight of vector $\mathbf{c}$ at a to be:

$$w_a(\mathbf{c}) = |\{i :\ c_i = a\}|$$

Let A_i be the number of elements of Gray weight *i* in $\mathtt{C}$. Then, the set of Gray weight distributions of $\mathtt{C}$ is $\{A_0, A_1, \cdots, A_{2^m n}\}$.

The Gray weight enumerator is defined by:

$$\begin{aligned}\mathrm{Gray}_{\mathtt{C}}(S, T) &= \sum_{i=0}^{2^m n} A_iS^{2^m n - i}T^i \\ &= \sum_{\mathbf{c} \in \mathtt{C}} S^{2^m n - w_G(\mathbf{c})}T^{w_G(\mathbf{c})}\end{aligned}$$

Since Gray map ϕ is a distance preserving map from the Gray distance to the Lee distance, we define the Lee weight enumerator of $\phi(\mathtt{C})$ as follows:

$$\mathrm{Lee}_{\phi(\mathtt{C})}(S,T) = \sum_{\phi(\mathbf{c})\in\phi(\mathtt{C})} S^{2^m 2n - w_L(\phi(\mathbf{c}))} T^{w_L(\phi(\mathbf{c}))}.$$

Suppose that the elements of R are $\{0, v, 2v, 3v, \ldots, (2^m-1)v, 1, 1+v, \ldots, 1+(2^m-1)v, \ldots, (2^m-1)+(2^m-1)v\}$ are indexed with the following indexing variables:

$$R = \{S_0, S_1, S_2, S_3, \cdots, S_{(2^m)^2-1}\}.$$

Let a_i denote the elements of Table 1 that relate to S_i.

Define the *complete weight enumerator* of $\mathtt{C}$ over R as follows:

$$\begin{aligned}\mathrm{cwe}_{\mathtt{C}}(S_0, S_1, S_2, \cdots, S_{2^{2m}-1}) &= \sum_{\mathbf{c}\in\mathtt{C}} S_0^{w_{a_0}(\mathbf{c})} S_1^{w_{a_1}(\mathbf{c})} \cdots S_{2^{2m}-1}^{w_{a_{2^{2m}-1}}(\mathbf{c})} \\ &= \sum_{\mathbf{c}\in\mathtt{C}} \prod_{a\in R} S_a^{w_a(\mathbf{c})}.\end{aligned}$$

We say that $w_{a_i}(\mathbf{c})$ is the *complete weight composition* of vector $\mathbf{c}$ in a_i.

Define the number of elements with Gray weight i in codeword $\mathbf{c}$ of $\mathtt{C}$ as:

$$\alpha_i(\mathbf{c}) = \sum_{\substack{a\in R,\\ w_G(a)=i}} w_a(\mathbf{c}), \qquad i = 0, 1, 2, 3, \cdots, 2^m$$

Then the Gray weight $w_G(\mathbf{c})$ of $\mathbf{c} \in \mathtt{C}$ is equal to:

$$w_G(\mathbf{c}) = \sum_{i=0}^{2^m} i\alpha_i(\mathbf{c}).$$

Define the *symmetrized weight enumerator* of $\mathtt{C}$ over R as follows:

$$\mathrm{swe}_{\mathtt{C}}(T_0, T_1, T_2, T_3, \ldots, T_{2^m}) = \sum_{\mathbf{c}\in v} \prod_{i=0}^{2^m} T_i^{\alpha_i(\mathbf{c})},$$

where $T_0, T_1, T_2, T_3, \ldots, T_{2^m}$ represent the elements in R with weights $0, 1, 2, 3, \ldots, 2^m$, respectively.

The Hamming weight enumerator of $\mathtt{C}$ is defined as follows:

$$\mathrm{Ham}_{\mathtt{C}}(S,T) = \sum_{\mathbf{c}\in\mathtt{C}} S^{n-w_H(\mathbf{c})} T^{w_H(\mathbf{c})}$$

where $w_H(\mathbf{c})$ denotes the Hamming weight of a codeword $\mathbf{c}$.

Lemma III.2. *Let $\mathtt{C}$ be a linear code with length n over R. Then we have:*

1) $\mathrm{Gray}_{\mathtt{C}}(S,T) = swe_{\mathtt{C}}(S^{2^m}, S^{2^m-1}T, S^{2^m-2}T^2, \cdots, S^{2^m/2}T^{2^m/2}, \cdots, S^2T^{2^m-2}, ST^{2^m-1}, T^{2^m})$
2) $\mathrm{Ham}_{\mathtt{C}}(S,T) = swe_{\mathtt{C}}(S, \underbrace{T, T, \cdots, T}_{2^m})$
3) $\mathrm{Gray}_{\mathtt{C}}(S,T) = Lee_{\phi(\mathtt{C})}(S,T)$

Proof:

1) $\mathrm{Gray}_{\mathtt{C}}(S,T) = \sum_{\mathbf{c}\in\mathtt{C}} S^{2^m n - w_G(\mathbf{c})} T^{w_G(\mathbf{c})}$

$$\begin{aligned}&= \sum_{\mathbf{c}\in\mathtt{C}} S^{2^m(\alpha_0+\alpha_1+\cdots+\alpha_{2^m}) - (0\alpha_0+1\alpha_1+\cdots+2^m\alpha_{2^m})}. \\ &\quad T^{(0\alpha_0+1\alpha_1+2\alpha_2+\cdots+2^m\alpha_{2^m})} \\ &= \sum_{\mathbf{c}\in\mathtt{C}} S^{2^m\alpha_0+(2^m-1)\alpha_1+(2^m-2)\alpha_2+\cdots+\alpha_{(2^m-1)}}. \\ &\quad T^{(0\alpha_0+1\alpha_1+2\alpha_2+\cdots+2^m\alpha_{2^m})} \\ &= \sum_{\mathbf{c}\in\mathtt{C}} S^{2^m\alpha_0}\ (S^{2^m-1}T)^{\alpha_1}\ (S^{2^m-2}T^2)^{\alpha_2}\cdots \\ &\quad (S^{2^m/2}T^{2^m/2})^{\alpha_{2^m/2}}\cdots\ (S^3T^{2^m-3})^{\alpha_{2^m-3}} \\ &\quad (S^2T^{2^m-2})^{\alpha_{2^m-3}}\ (ST^{2^m-1})^{\alpha_{2^m-1}}\ T^{\alpha_{2^m}} \\ &= \mathrm{swe}_{\mathtt{C}}(S^{2^m}, S^{2^m-1}T, S^{2^m-2}T^2, S^{2^m-3}T^3, \cdots, \\ &\quad S^{2^m/2}T^{2^m/2}, \cdots, S^2T^{2^m-2}, ST^{2^m-1}, T^{2^m})\end{aligned}$$

2) $\mathrm{Ham}_{\mathtt{C}}(S,T) = \sum_{\mathbf{c}\in\mathtt{C}} S^{n-w_H(\mathbf{c})}\ T^{w_H(\mathbf{c})}$

$$\begin{aligned}&= \sum_{\mathbf{c}\in\mathtt{C}} S^{(\alpha_0+\alpha_1+\alpha_2+\alpha_3+\cdots+\alpha_{2^m})-(\alpha_1+\alpha_2+\alpha_3+\cdots+\alpha_{2^m})}. \\ &\quad T^{(\alpha_1+\alpha_2+\alpha_3+\cdots+\alpha_{2^m})} \\ &= \sum_{\mathbf{c}\in\mathtt{C}} S^{\alpha_0}\ T^{(\alpha_1+\alpha_2+\alpha_3+\cdots+\alpha_{2^m})} \\ &= \sum_{\mathbf{c}\in\mathtt{C}} S^{\alpha_0}\ T^{\alpha_1}\ T^{\alpha_2}\ T^{\alpha_3}\ \cdots\ T^{\alpha_{2^m}} \\ &= \mathrm{swe}_{\mathtt{C}}(S, \underbrace{T, T, \cdots, T}_{2^m})\end{aligned}$$

3) $\mathrm{Gray}_{\mathtt{C}}(S,T) = \sum_{\mathbf{c}\in\mathtt{C}} S^{2^m n - w_G(\mathbf{c})}\ T^{w_G(\mathbf{c})}$

$$\begin{aligned}&= \sum_{\phi(\mathbf{c})\in\phi(\mathtt{C})} S^{2^m 2n - w_L(\phi(\mathbf{c}))}\ T^{w_L(\phi(\mathbf{c}))} \\ &= \mathrm{Lee}_{\phi(\mathtt{C})}(S,T)\end{aligned}$$

■

Let $\hat{R} = \{\varphi : \text{character of } R\}$ and $\chi \in \hat{R}$. Define $\theta_1 : R \longrightarrow \hat{R}$ and $\theta_2 : R \longrightarrow \hat{R}$ induced by χ as $\theta_1(r) = \chi^r$ and $\theta_2(r) = {}^r\chi$, where $\chi^r(s) = \chi(sr)$ and ${}^r\chi(s) = \chi(rs)$. The character χ is a generating character if θ_1 or θ_2 is an R-module isomorphism.

Proposition III.3. *Let $\pi : R \longrightarrow \mathbb{C}^*$ be a character of R. Then*

$$\sum_{r\in R} \pi(r) = \begin{cases} |R|, & \text{if } \pi = 1 \\ 0, & \text{if } \pi \neq 1 \end{cases}$$

Proof: The similar proof as in Proposition 2.14 [11].

■

Lemma III.4. *For every ideal I in R, there exist I_1, I_2 ideals in $\mathbb{Z}_{2^m}$ such that $I = vI_1 \oplus (1-v)I_2$.*

Proof: We define I_1 and I_2 by

$$\begin{aligned}I_1 &= \{a \in \mathbb{Z}_{2^m} :\ \exists b \in \mathbb{Z}_{2^m},\ va + (1-v)b \in I\} \\ I_2 &= \{b \in \mathbb{Z}_{2^m} :\ \exists a \in \mathbb{Z}_{2^m},\ va + (1-v)b \in I\}\end{aligned}$$

Let $a + vb \in I$, and write $a + vb = v(a+b) + (1-v)a$. This implies that $a + b \in I_1$ and $a \in I_2$, then we get $a + vb \in vI_1 + (1-v)I_2$. Therefore it implies that $I \subseteq vI_1 + (1-v)I_2$. Let $va + (1-v)b \in vI_1 + (1-v)I_2$. We will prove that $va + (1-v)b \in I$. Since $a \in I_1$, and $b \in I_2$, then there

TABLE I
GRAY WEIGHT OF ELEMENTS $\mathbb{Z}_{2^m} + v\mathbb{Z}_{2^m}$

i	Element a_i	Gray image	Gray weight	Corresponding variable
0	0	$(0,0)$	0	S_0
1	v	$(0,1)$	1	S_1
2	$2v$	$(0,2)$	2	S_2
3	$3v$	$(0,3)$	3	S_3
4	$4v$	$(0,4)$	4	S_4
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
2^m-3	$(2^m-3)v$	$(0,2^m-3)$	3	S_{2^m-3}
2^m-2	$(2^m-2)v$	$(0,2^m-2)$	2	S_{2^m-2}
2^m-1	$(2^m-1)v$	$(0,2^m-1)$	1	S_{2^m-1}
2^m	1	$(1,1)$	2	S_{2^m}
2^m+1	$1+v$	$(1,2)$	3	S_{2^m+1}
2^m+2	$1+2v$	$(1,3)$	4	S_{2^m+2}
2^m+3	$1+3v$	$(1,4)$	5	S_{2^m+3}
2^m+4	$1+4v$	$(1,5)$	6	S_{2^m+4}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$2^m+(2^m-2)$	$1+(2^m-2)v$	$(1,1+(2^m-2))$	2	$S_{2^m+(2^m-2)}$
$2^m+(2^m-1)$	$1+(2^m-1)v$	$(1,1+(2^m-1))$	1	$S_{2^m+(2^m-1)}$
$2^{(m+1)}$	2	$(2,2)$	4	$S_{2^{(m+1)}}$
$2^{(m+1)}+1$	$2+v$	$(2,3)$	5	$S_{2^{(m+1)}+1}$
$2^{(m+1)}+2$	$2+2v$	$(2,4)$	6	$S_{2^{(m+1)}+2}$
$2^{(m+1)}+3$	$2+3v$	$(2,5)$	7	$S_{2^{(m+1)}+3}$
$2^{(m+1)}+4$	$2+4v$	$(2,6)$	8	$S_{2^{(m+1)}+4}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$2^{(m+1)+(2^m-2)}$	$2+(2^m-2)v$	$(2,2+(2^m-2))$	2	$S_{2^{(m+1)+(2^m-2)}}$
$2^{(m+1)+(2^m-1)}$	$2+(2^m-1)v$	$(2,2+(2^m-1))$	1	$S_{2^{(m+1)+(2^m-1)}}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
2^{2m-1}	$2^{(m-1)}$	$(2^{(m-1)}, 2^{(m-1)})$	$2\cdot 2^{(m-1)}$	$S^{2^{2m-1}}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$2^{2m}-1$	$2^m-1+(2^m-1)v$	$(2^m-1, 2\cdot 2^m-2)$	3	$S_{2^{2m}-1}$

exists c such that $va+(1-v)c \in I$ and there exists d such that $vd+(1-v)b \in I$, respectively. Therefore,

$$\begin{aligned} va+(1-v)b &= v(va+(1-v)c)+(1-v)(vd+(1-v)b) \\ &\in I \end{aligned}$$

Hence, $va+(1-v)b \in I$. Thus, we can conclude that $vI_1 + (1-v)I_2 = I$.
Let $w \in vI_1 \cap (1-v)I_2$, we get

$$\begin{aligned} w = va &= (1-v)b, \text{for } a \in I_1, b \in I_2 \\ va-(1-v)b &= 0 \\ -b+v(a+b) &= 0 \end{aligned}$$

Hence, $b=0, a=0$, and $w=0$. So, we conclude that $I = vI_1 \oplus (1-v)I_2$. ■

Lemma III.5. *For every $I \neq 0$. If $\sum_{r\in I}\pi(r)=0$, then π is a generating character.*

Proof: Let $\theta : R \longrightarrow \hat{R}$ defined as $\theta(r) = {}^r\pi$, where ${}^r\pi(s) = \pi(rs)$ for all $s \in R$. Suppose π is not a generating character, then

$$\mathrm{Ker}(\theta) = \{r \in R : \ \theta(r)=1\} = \{r \in R : \ {}^r\pi = 1\} \neq \{0\}$$

Hence, there is an $r \neq 0$, where ${}^r\pi = 1$, ${}^r\pi(x) = \pi(rx) = 1$, for all $x \in R$. Thus $rx \in \mathrm{Ker}(\pi)$, for all $x \in R$. In other words, $rR \subseteq \mathrm{Ker}(\pi)$.

Suppose $I = rR$.

$$\begin{aligned} \sum_{a\in rR}\pi(a) &= \pi(a_1)+\pi(a_2)+\cdots+\pi(a_k) \\ &= \underbrace{1+1+\cdots+1}_{k} = 1\cdot k \neq 0, \end{aligned}$$

which contradicts $\sum_{a\in I}\pi(a)=0$ for all I nonzero ideals. ■

Theorem III.6. *Let $\pi : R \longrightarrow \mathbb{C}^*$ be a character of R. Then the following are equivalent:*

1) *for every nonzero ideal I, then $I \not\subseteq \mathrm{Ker}(\pi)$,*
2) *for every nonzero ideal I, then $\sum_{r\in I}\pi(r)=0$.*

Proof:

$(1) \Rightarrow 2)$) Let I be a nonzero ideal with $I \not\subseteq \mathrm{Ker}(\pi)$. We will prove that $\sum_{r\in I}\pi(r)=0$. Since $I \not\subseteq \mathrm{Ker}(\pi)$, there exist $r_0 \in I, \pi(r_0) \neq 1$. By Proposition III.3, $\sum_{r\in I}\pi(r)=0$.

(2) $\Rightarrow$ 1)) Let $I \neq 0$ and $\sum_{r\in I}\pi(r) = 0$. We will prove that $I \not\subseteq \mathrm{Ker}(\pi)$. Suppose that $I \subseteq \mathrm{Ker}(\pi)$. This implies that $\pi(I) = 1$. However this leads to a contradiction, since $\sum_{r\in I}\pi(r) = |I| \neq 0$ by Proposition III.3. ∎

Now, let us consider the function

$$f : R^n \longrightarrow \mathbb{C}[S_0, S_1, ..., S_{2^{2m}-1}].$$

The Hadamard transform of f, denoted by $\hat{f}$, is defined by:

$$\hat{f}(\mathbf{x}) = \sum_{\mathbf{y}\in R^n} \chi(\mathbf{x}\cdot\mathbf{y})f(\mathbf{y}), \qquad \text{for any } \mathbf{x} \in R^n,$$

where for any $r = a + bv$, $\chi(a + bv) = \xi^{2a+b}$, for any $a + bv \in R$, and $\xi = e^{2\pi i/2^m}$ is the primitive 2^m-th root of unity in the complex field $\mathbb{C}$.

Lemma III.7. *Let $\chi : R \longrightarrow \mathbb{C}^*$ be a character of R defined by $\chi(a + bv) = \xi^{2a+b}$ and I be a nonzero ideal of R. Then χ is a generating character.*

Proof:

Because R can be represented by $R = v\mathbb{Z}_{2^m} + (1-v)\mathbb{Z}_{2^m}$, by Lemma III.4, then for any ideal $I \in R$ there are I_1, I_2 ideals in $\mathbb{Z}_{2^m}$ such that $I = vI_1 \oplus (1-v)I_2$. Let $r = a+vb = v(a + b) + (1 - v)a$, then we have

$$\begin{aligned}
\sum_{r\in I}\chi(r) &= \sum_{a+bv\in I}\chi(a + bv)\\
&= \sum_{v(a+b)+(1-v)a\in I}\chi(v(a + b) + (1 - v)a)\\
&= \sum_{a+b\in I_1, a\in I_2}\chi(v(a + b))\ \chi((1 - v)a)\\
&= \sum_{a+b\in I_1, a\in I_2}\xi^{a+b}\ \xi^{a}\\
&= \sum_{a+b\in I_1}\xi^{a+b}\ \sum_{a\in I_2}\xi^{a}
\end{aligned}$$

Since I is nonzero, then at least one of I_1 or I_2 is nonzero. Let

$$\chi : R \longrightarrow \mathbb{C}^*$$
$$r \longmapsto \chi(r) \text{ where } \chi(r) = \chi(a + vb) = \xi^{2a+b}$$

Suppose $I_2 \subseteq Ker(\chi)$ ideal in $\mathbb{Z}_{2^m}$, $I_2 = \langle 2^i\rangle$, for i. Let $r \in I_2$, then $r = t\cdot 2^s$, for $t \in \mathbb{Z}_{2^m}$. Since $\chi(t\cdot 2^s) = \xi^{2t\cdot 2^s} = \xi^{t\cdot 2^{s+1}} = 1$ and $\xi^{2^m} = 1$, then this leads to a contradiction, because $2^m \nmid t \cdot 2^{s+1}$. So we get $I_2 \not\subseteq Ker(\chi)$, therefore, this concludes that $\sum_{a\in I_2}\chi(a) = 0$ by Theorem III.6. Since $\sum_{a\in I_2}\xi^a = 0$, we conclude that $\sum_{r\in I}\chi(r) = 0$ by Proposition III.3. ∎

Lemma III.8. *If $\mathtt{C}$ be a linear code of length n over R, then*

$$\sum_{\mathbf{x}\in\mathtt{C}^\perp} f(\mathbf{x}) = \frac{1}{|\mathtt{C}|}\sum_{\mathbf{x}\in\mathtt{C}}\hat{f}(\mathbf{x}).$$

Proof:

By using the Hadamard transform of $f(\mathbf{x})$, we have

$$\sum_{\mathbf{x}\in\mathtt{C}}\hat{f}(\mathbf{x}) = \sum_{\mathbf{x}\in\mathtt{C}}\sum_{\mathbf{y}\in R^n}\chi(\mathbf{x}\cdot\mathbf{y})f(\mathbf{y}) = \sum_{\mathbf{y}\in R^n} f(\mathbf{y})\sum_{\mathbf{x}\in\mathtt{C}}\chi(\mathbf{x}\cdot\mathbf{y}).$$

Next we consider two cases:

(i) If $\mathbf{y} \in \mathtt{C}^\perp$, then $\mathbf{x}\cdot\mathbf{y} = 0$. Therefore, $\chi(\mathbf{x}\cdot\mathbf{y}) = \chi(0) = 1$ because $\xi = e^0 = \cos(0) + i\ \sin(0) = 1$. So we get $\sum_{\mathbf{x}\in\mathtt{C}}\chi(\mathbf{x}\cdot\mathbf{y}) = |\mathtt{C}|$;

(ii) If $\mathbf{y} \in R^n\backslash\mathtt{C}^\perp$, then $\{\mathbf{x}\cdot\mathbf{y} : \mathbf{x} \in \mathtt{C}\}$ is a nonzero ideal in R. By Lemma III.7, we get $\sum_{\mathbf{x}\in\mathtt{C}}\chi(\mathbf{x}\cdot\mathbf{y}) = 0$.

Therefore, we conclude

$$\sum_{\mathbf{x}\in\mathtt{C}^\perp} f(\mathbf{x}) = \frac{1}{|\mathtt{C}|}\sum_{\mathbf{x}\in\mathtt{C}}\hat{f}(\mathbf{x}).$$

∎

A famous topic in linear code is the MacWilliams relations, which relates the weight enumerators between a linear code and its dual code. Wood have proven the relations with respect to Hamming weight as well as complete weight enumerators for any linear codes over Frobenius rings ([12],[13]). Here we prove relations for complete weight enumerator explicitly in the following lemma.

Lemma III.9. *Let $\mathtt{C}$ be a linear code with length n over R and $\mathtt{C}^\perp$ be its Euclidean dual. Then*

$$\begin{aligned}
&\mathrm{cwe}_{\mathtt{C}^\perp}(S_0, S_1, S_2, S_3, \ldots, S_{2^{2m}-1})\\
&\quad= \frac{1}{|\mathtt{C}|}\mathrm{cwe}_{\mathtt{C}}(M\cdot(S_0, S_1, S_2, S_3, \ldots, S_{2^{2m}-1})^T),
\end{aligned}$$

where $M_{ij} = (\chi(a_i\ a_j))_{2^{2m}\times 2^{2m}}$ for $i, j = 0, 1, 2, 3, ..., 2^{2m} - 1$ and a_i denotes the elements of Table 1 that relate to S_i and the symbol $(S_0, S_1, \cdots, S_{2^{2m}-1})^T$ denotes the transpose of vector $(S_0, S_1, S_2, S_3, \ldots, S_{2^{2m}-1})$.

Proof:

Let $f(\mathbf{y}) = S_0^{w_{a_0}(\mathbf{y})}S_1^{w_{a_1}(\mathbf{y})}\cdots S_{2^{2m}-1}^{w_{a_{2^{2m}-1}}(\mathbf{y})}$, where $\mathbf{y} = (y_0, y_1, \cdots, y_{n-1}) \in R^n$ and $w_{a_i}(\mathbf{y})$ is the complete weight composition of vector $\mathbf{y}$ in a_i.

$$\begin{aligned}
\hat{f}(\mathbf{x}) &= \sum_{\mathbf{y}\in R^n}\chi(\mathbf{x}\cdot\mathbf{y})f(\mathbf{y})\\
&= \sum_{\mathbf{y}\in R^n}\chi(\mathbf{x}\cdot\mathbf{y})S_0^{w_{a_0}(\mathbf{y})}\cdots S_{2^{2m}-1}^{w_{a_{2^{2m}-1}}(\mathbf{y})}.
\end{aligned}$$

For any $r \in R$, we have $w_r(\mathbf{y}) = \delta_{r,y_0} + \delta_{r,y_1} + ... + \delta_{r,y_{n-1}}$, where δ is the Kronecker delta. So we get

$$\begin{aligned}
\hat{f}(\mathbf{x}) &= \sum_{\mathbf{y}\in R^n}(\chi(x_0y_0 + \cdots + x_{n-1}y_{n-1}))\cdot\\
&\quad\left(S_0^{\sum_{i=0}^{n-1}\delta_{a_0,y_i}}\cdots S_{(2^{2m}-1)}^{\sum_{i=0}^{n-1}\delta_{a_{(2^{2m}-1)},y_i}}\right)\\
&= \sum_{\mathbf{y}\in R^n}\left(\prod_{j=0}^{n-1}\chi(x_jy_j)\right)\cdot\left(\prod_{k=0}^{2^{2m}-1}S_k^{\sum_{i=0}^{n-1}\delta_{a_k,y_i}}\right)\\
&= \sum_{\mathbf{y}\in R^n}\left(\chi(x_0y_0)\prod_{k=0}^{2^{2m}-1}S_k^{\delta_{a_k,y_0}}\right)\cdots\\
&\quad\left(\chi(x_{n-1}y_{n-1})\prod_{k=0}^{2^{2m}-1}S_k^{\delta_{a_k,y_{n-1}}}\right)
\end{aligned}$$

$$
\begin{aligned}
&= \left(\sum_{y_0\in R}\chi(x_0y_0)\prod_{k=0}^{2^{2m}-1}S_k^{\delta_{a_k,y_0}}\right)\cdots\\
&\quad\left(\sum_{y_{n-1}\in R}\chi(x_{n-1}y_{n-1})\prod_{k=0}^{2^{2m}-1}S_k^{\delta_{a_k,y_{n-1}}}\right)\\
&= \left(\sum_{k=0}^{2^{2m}-1}\chi(x_0a_k)\ S_k\right)\left(\sum_{k=0}^{2^{2m}-1}\chi(x_1a_k)\ S_k\right)\\
&\quad\cdots\left(\sum_{k=0}^{2^{2m}-1}\chi(x_{n-1}a_k)\ S_k\right)\\
&= \prod_{i=0}^{2^{2m}-1}\left(\sum_{j=0}^{2^{2m}-1}\chi(a_ia_j)\ S_j\right)^{w_{a_i}(\mathbf{x})}.
\end{aligned}
$$

For $\mathbf{c}\in\mathtt{C}$, $f(\mathbf{c}) = S_0^{w_{a_0}(\mathbf{c})}S_1^{w_{a_1}(\mathbf{c})}\cdots S_{2^{2m}-1}^{w_{a_{2^{2m}-1}}(\mathbf{c})}$.
By Lemma III.8, we get:

$$
\begin{aligned}
&\mathrm{cwe}_{\mathtt{C}^\perp}(S_0,S_1,S_2,S_3,\cdots,S_{2^{2m}-1})\\
&= \sum_{\mathbf{c}\in\mathtt{C}^\perp}S_0^{w_{a_0}(\mathbf{c})}S_1^{w_{a_1}(\mathbf{c})}\cdots S_{2^{2m}-1}^{w_{a_{2^{2m}-1}}(\mathbf{c})}\\
&= \sum_{\mathbf{c}\in\mathtt{C}^\perp}f(\mathbf{c})\\
&= \frac{1}{|\mathtt{C}|}\sum_{\mathbf{c}\in\mathtt{C}}\hat{f}(\mathbf{c})\\
&= \frac{1}{|\mathtt{C}|}\sum_{\mathbf{c}\in\mathtt{C}}\prod_{i=0}^{2^{2m}-1}\left(\sum_{j=0}^{2^{2m}-1}\chi(a_i\ a_j)\ S_j\right)^{w_{a_i}(\mathbf{c})}\\
&= \frac{1}{|\mathtt{C}|}\sum_{\mathbf{c}\in\mathtt{C}}\left(\sum_{j=0}^{2^{2m}-1}\chi(a_0\ a_j)\ S_j\right)^{w_{a_0}(\mathbf{c})}\times\cdots\times\\
&\quad\left(\sum_{j=1}^{2^{2m}-1}\chi(a_{2^{2m}-1}\ a_j)\ S_j\right)^{w_{a_{2^{2m}-1}}(\mathbf{c})}\\
&= \frac{1}{|\mathtt{C}|}\mathrm{cwe}_{\mathtt{C}}\left(\sum_{j=1}^{2^{2m}-1}\chi(a_0\ a_j)\ S_j,\ldots,\right.\\
&\quad\left.\sum_{j=1}^{2^{2m}-1}\chi(a_{2^{2m}-1}\ a_j)S_j\right).
\end{aligned}
$$

■

C. MDS Codes over R

Let $\mathtt{C}$ be an $[n,M,d]$ linear code over R. For any Frobenius ring R, the Singleton bound to a code $\mathtt{C}$ with length n over R express as:

$$d_H(\mathtt{C}) \le n - log_{|R|}|\mathtt{C}| + 1,$$

where $d_H(\mathtt{C})$ denotes the minimum Hamming distance of a linear code of $\mathtt{C}$.

A maximum distance separable (MDS) code is another important class of linear codes over R. A code that meets the Singleton bound is called MDS, namely if $d_H(\mathtt{C}) = n - log_{|R|}|\mathtt{C}| + 1$ is fulfilled.

By using a similar argument as in the proof of Lemma III.4, we can decompose $\mathtt{C}$ into $\mathtt{C} = v\mathtt{C}_1 \oplus (1-v)\mathtt{C}_2$, where

$$\mathtt{C}_1 = \{\mathbf{x}\in\mathbb{Z}_{2^m}^n : \exists\mathbf{y}\in\mathbb{Z}_{2^m}^n, v\mathbf{x}+(1-v)\mathbf{y}\in\mathtt{C}\}, \quad (2)$$

and

$$\mathtt{C}_2 = \{\mathbf{y}\in\mathbb{Z}_{2^m}^n : \exists\mathbf{x}\in\mathbb{Z}_{2^m}^n, v\mathbf{x}+(1-v)\mathbf{y}\in\mathtt{C}\}. \quad (3)$$

Theorem III.10. *Let $\mathtt{C} = v\mathtt{C}_1 \oplus (1-v)\mathtt{C}_2$, with $\mathtt{C}_1$ and $\mathtt{C}_2$ in (2) and (3) be a linear code with length n over R. Then:*

1) *$d_G(\mathtt{C}) = \min\{d_L(\mathtt{C}_1), d_L(\mathtt{C}_2)\}$, where d_G, d_L are the Gray distance and the Lee distance, respectively.*
2) *$d_H(\mathtt{C}) = \min\{d_H(\mathtt{C}_1), d_H(\mathtt{C}_2)\}$, where d_H is the Hamming distance;*
3) *Code $\mathtt{C}$ with parameter $[n,M,d]$ is an MDS code over R if and only if $\mathtt{C}_1$ and $\mathtt{C}_2$ with parameters $[n,\sqrt{M},d]$ are MDS code over $\mathbb{Z}_{2^m}$.*

Proof:

1) Since $\mathtt{C} = v\mathtt{C}_1 \oplus (1-v)\mathtt{C}_2$, then the minimum Gray distance is $d_G(\mathtt{C}) = \min\{d_G(v\mathtt{C}_1), d_G(1-v)\mathtt{C}_2\}$. By Proposition II.3, we have $d_G(\mathtt{C}) = \min\{d_L(\phi(v\mathtt{C}_1)), d_L(\phi((1-v)\mathtt{C}_2))\}$.

   Denote the component-wise multiplication of two vectors with operation $*$ as follows:
   $(x_1,x_2)*(y_1,y_2,\cdots,y_n)$
   $= (x_1y_1, x_2y_1, x_1y_2, x_2y_2, \cdots, x_1y_n, x_2y_n)$
   Recall the Gray map

$$\begin{aligned}\phi : R^n &\longrightarrow \mathbb{Z}_{2^m}^{2n}\\ (a_0+vb_0,\cdots,a_{n-1}+vb_{n-1}) &\longmapsto (a_0, a_0+b_0,\cdots,\\ &\qquad a_{n-1}, a_{n-1}+b_{n-1}).\end{aligned}$$

   We will show that $\phi(v\mathtt{C}_1) = (0,1)*\mathtt{C}_1$. Let $c'\in\phi(v\mathtt{C}_1)$, where

$$\begin{aligned}c' = \phi(v\mathbf{x}), &\text{with } \mathbf{x} = (x_0,x_1,\cdots,x_{n-1})\in\mathtt{C}_i.\text{Then}\\ \phi(v\mathbf{x}) &= \phi(vx_0, vx_1,\cdots,vx_{n-1})\\ &= (0,x_0,0,x_1,\cdots,0,x_{n-1})\\ &\in (0,1)*\mathtt{C}_1,\end{aligned}$$

   so we get $\phi(v\mathtt{C}_1)\subseteq(0,1)*\mathtt{C}_1$.
   Let $c' = (0,1)*\mathbf{x}\in(0,1)*\mathtt{C}_1$. Then

$$\begin{aligned}c' &= (0,1)*(x_0,x_1,\cdots,x_{n-1})\\ &= (0,x_0,0,x_1,\cdots,0,x_{n-1})\\ &\in\phi(v\mathtt{C}_1),\end{aligned}$$

   hence we get $(0,1)*\mathtt{C}_1\subseteq\phi(v\mathtt{C}_1)$.
   So we conclude that $\phi(v\mathtt{C}_1) = (0,1)*\mathtt{C}_1$.
   Next we will show that
   $\phi((1-v)\mathtt{C}_2) = (1,0)*\mathtt{C}_2$. Let $c'\in\phi((1-v)\mathtt{C}_2)$, where $c' = \phi((1-v)\mathbf{y})$, $\mathbf{y} = (y_0,y_1,\cdots,y_{n-1})\in\mathtt{C}_2$.
   Then

$$\begin{aligned}\phi((1-v)\mathbf{y}) &= \phi((1-v)y_0,(1-v)y_1,\cdots,(1-v)y_{n-1})\\ &\in(1,0)*\mathtt{C}_2.\end{aligned}$$

And hence $\phi((1-v)\mathtt{C}_2) \subseteq (1,0) * \mathtt{C}_2$.

Let $c' = (1,0) * \mathbf{y} \in (1,0) * \mathtt{C}_2$. Then

$$\begin{aligned} c' &= (1,0) * (y_0, y_1, \cdots, y_{n-1}) \\ &= (y_0, 0, y_1, 0 \cdots, y_{n-1}, 0) \\ &\in \phi((1-v)\mathtt{C}_2). \end{aligned}$$

Then we get $(1,0) * \mathtt{C}_2 \subseteq \phi((1-v)\mathtt{C}_2)$.
So we conclude that $\phi((1-v)\mathtt{C}_2) = (1,0) * \mathtt{C}_2$, which implies that

$$\begin{aligned} d_G(\mathtt{C}) &= \min\{d_G(v\mathtt{C}_1), d_G(1-v)\mathtt{C}_2\} \\ &= \min\{d_L(\phi(v\mathtt{C}_1)), d_L(\phi((1-v)\mathtt{C}_2))\} \\ &= \min\{d_L(\mathtt{C}_1), d_L(\mathtt{C}_2)\}. \end{aligned}$$

2) It is easy to see that

$$d_H(\mathtt{C}) = \min\{d_H(v\mathtt{C}_1), d_H(1-v)\mathtt{C}_2\}.$$

Moreover, since $\forall \mathbf{c} = v\mathbf{c}_1 + (1-v)\mathbf{c}_2 \in \mathtt{C}$, we have $\mathbf{c} = 0$ if and only if $\mathbf{c}_1 = 0 = \mathbf{c}_2$, then

$$d_H(\mathtt{C}) = \min\{d_H(\mathtt{C}_1)), d_H(\mathtt{C}_2)\}.$$

3) Let $\mathtt{C}$ is an MDS code of parameter $[n, M, d]$. Denote $d_H(\mathtt{C}_1)$ as the minimum Hamming distance of $\mathtt{C}_1$ and $d_H(\mathtt{C}_2)$ as the minimum Hamming distance of $\mathtt{C}_2$.
Suppose

$$\begin{aligned} d = d_H(\mathtt{C}) = d_H(\mathtt{C}_1) &\text{ and from point 2,} \\ d_H(\mathtt{C}) = \min\{d_H(\mathtt{C}_1), d_H(\mathtt{C}_2)\}&, \text{ then} \\ d_H(\mathtt{C}_2) \geq d_H(\mathtt{C}_1)&. \end{aligned}$$

Since

$$d = n - \log_{2^{2m}} M + 1 = n - \log_{2^m} \sqrt{M} + 1 = d_H(\mathtt{C}_1)$$

So we get that $\mathtt{C}_1$ is MDS with parameter $[n, \sqrt{M}, d]$. Since $d_H(\mathtt{C}_1) \leq d_H(\mathtt{C}_2)$, then we get

$$n - \log_{2^m} \sqrt{M} + 1 = d_H(\mathtt{C}_1) \leq d_H(\mathtt{C}_2) \leq n - \log_{2^m} \sqrt{M} + 1.$$

From this equation, so we get $d_H(\mathtt{C}_2) = n - \log_{2^m} \sqrt{M} + 1$. The consequence are $\mathtt{C}_1$ and $\mathtt{C}_2$ are MDS codes.

Now suppose $\mathtt{C}_1$ and $\mathtt{C}_2$ with parameters $[n, \sqrt{M}, d]$ are MDS codes, then $d_H(\mathtt{C}_1) = n - \log_{2^m} \sqrt{M} + 1$ and $d_H(\mathtt{C}_2) = n - \log_{2^m} \sqrt{M} + 1$.

Assume by point 2 of $d_H(\mathtt{C}) = d_H(\mathtt{C}_1)$, then $d_H(\mathtt{C}) = n - \log_{2^m} \sqrt{M} + 1 = n - \log_{2^{2m}} M + 1$. As a result, $\mathtt{C}$ is an MDS code.
Therefore, we conclude that code $\mathtt{C}$ with parameter $[n, M, d]$ is an MDS code over R if and only if $\mathtt{C}_1, \mathtt{C}_2$ with parameter $[n, \sqrt{M}, d]$ are MDS codes over $\mathbb{Z}_{2^m}$. ■

IV. Self-Dual Code over R

A. Self-Dual Codes

In this section, the properties of self-dual linear codes over R will be studied. The codes $\mathtt{C}_1$ and $\mathtt{C}_2$ are linear code over $\mathbb{Z}_{2^m}$ with length n. A linear code $\mathtt{C}$ with length n over R can be stated uniquely as:

$$\mathtt{C} = v\mathtt{C}_1 \oplus (1-v)\mathtt{C}_2$$

Proposition IV.1. *Let $\mathtt{C}$ be a linear code with length n over R, then $\mathtt{C}^\perp = v\mathtt{C}_1^\perp \oplus (1-v)\mathtt{C}_2^\perp$. The code $\mathtt{C}$ is Euclidean self-dual if and only if $\mathtt{C}_1$ and $\mathtt{C}_2$ are both Euclidean self-dual over $\mathbb{Z}_{2^m}$.*

Proof:
Define:

$$\hat{\mathtt{C}}_1 = \{\mathbf{x} \in \mathbb{Z}_{2^m}^n : \exists \mathbf{y} \in \mathbb{Z}_{2^m}^n, v\mathbf{x} + (1-v)\mathbf{y} \in \mathtt{C}^\perp\}$$

and

$$\hat{\mathtt{C}}_2 = \{\mathbf{y} \in \mathbb{Z}_{2^m}^n : \exists \mathbf{x} \in \mathbb{Z}_{2^m}^n, v\mathbf{x} + (1-v)\mathbf{y} \in C^\perp\}$$

We will prove $\mathtt{C}^\perp = v\hat{\mathtt{C}}_1 + (1-v)\hat{\mathtt{C}}_2$. Let $\mathbf{c}' \in \mathtt{C}^\perp$, where $\mathbf{c}' = \mathbf{a} + v\mathbf{b}$. We can represent $\mathbf{c}' = v(\mathbf{a}+\mathbf{b}) + (1-v)\mathbf{a}$. Then $(\mathbf{a}+\mathbf{b}) \in \hat{\mathtt{C}}_1$ and $\mathbf{a} \in \hat{\mathtt{C}}_2$. So $\mathbf{c}' \in v\hat{\mathtt{C}}_1 + (1-v)\hat{\mathtt{C}}_2$. As a result $\mathtt{C}^\perp \subseteq v\hat{\mathtt{C}}_1 + (1-v)\hat{\mathtt{C}}_2$.

Let $v\mathbf{a}+(1-v)\mathbf{b} \in v\hat{\mathtt{C}}_1+(1-v)\hat{\mathtt{C}}_2$, where $\mathbf{a} \in \hat{\mathtt{C}}_1$ meaning that there is $\mathbf{y}_1$ such that $v\mathbf{a} + (1-v)\mathbf{y}_1 \in \mathtt{C}^\perp$, and $\mathbf{b} \in \hat{\mathtt{C}}_2$ meaning that there is $\mathbf{x}_1$ such that $v\mathbf{x}_1 + (1-v)\mathbf{b} \in \mathtt{C}^\perp$.

$$\begin{aligned} v(v\mathbf{a} + (1-v)\mathbf{y}_1) = v\mathbf{a} &\in v\mathtt{C}^\perp \subseteq \mathtt{C}^\perp \\ v\mathbf{a} &\in \mathtt{C}^\perp \end{aligned}$$

and

$$\begin{aligned} (1-v)(v\mathbf{x}_1 + (1-v)\mathbf{b}) = (1-v)\mathbf{b} &\in (1-v)\hat{\mathtt{C}}_2 \subseteq \mathtt{C}^\perp \\ (1-v)\mathbf{b} &\in \mathtt{C}^\perp \end{aligned}$$

Then we get $v\mathbf{a}+(1-v)\mathbf{b} \in \mathtt{C}^\perp$. Hence $\mathtt{C}^\perp = v\hat{\mathtt{C}}_1+(1-v)\hat{\mathtt{C}}_2$. Let $\mathbf{z} \in v\hat{\mathtt{C}}_1 \cap (1-v)\hat{\mathtt{C}}_2$, meaning that $\mathbf{z} \in v\hat{\mathtt{C}}_1$ with $\mathbf{z} = v\mathbf{a}$, where $\mathbf{a} \in \hat{\mathtt{C}}_1$; and $\mathbf{z} \in (1-v)\hat{\mathtt{C}}_2$ with $\mathbf{z} = (1-v)\mathbf{b}$, where $\mathbf{b} \in \hat{\mathtt{C}}_2$. Thus

$$\begin{aligned} v\mathbf{a} &= (1-v)\mathbf{b} \\ v\mathbf{a} - (1-v)\mathbf{b} &= \mathbf{0} \\ -\mathbf{b} + v(\mathbf{a}+\mathbf{b}) &= \mathbf{0} \end{aligned}$$

implying that $\mathbf{a} = \mathbf{0}$ and $\mathbf{b} = \mathbf{0}$. Then $\mathbf{z} = \mathbf{0}$. So we conclude $\mathtt{C}^\perp = v\hat{\mathtt{C}}_1 \cap (1-v)\hat{\mathtt{C}}_2$.

Now, we will prove $\hat{\mathtt{C}}_1 = \mathtt{C}_1^\perp$. Let $\hat{\mathbf{a}}_1 \in \hat{\mathtt{C}}_1$, there is a $\mathbf{b}_1 \in \mathbb{Z}_{2^m}^n$ such that $v\hat{\mathbf{a}}_1 + (1-v)\mathbf{b}_1 \in \mathtt{C}^\perp$. Let $\mathbf{x} \in \mathtt{C}_1$, there is a $\mathbf{y} \in \mathbb{Z}_{2^m}^n$ such that $v\mathbf{x} + (1-v)\mathbf{y} \in \mathtt{C}$. Then, $(v\hat{\mathbf{a}}_1 + (1-v)\mathbf{b}_1) \cdot (v\mathbf{x} + (1-v)\mathbf{y}) = 0$, which implies that $\hat{\mathbf{a}}_1 \cdot \mathbf{x} = 0$. Since $\hat{\mathbf{a}}_1 \in \hat{\mathtt{C}}_1$ and $\hat{\mathbf{a}}_1 \cdot \mathbf{x} = 0$, then $\hat{\mathbf{a}}_1 \in \hat{\mathtt{C}}_1^\perp$ and we get $\hat{\mathtt{C}}_1 \subseteq \mathtt{C}_1^\perp$. Let $\mathbf{c}_1 \in \mathtt{C}_1^\perp$, since for $\mathbf{x} \in \mathtt{C}_1$ there is a $\mathbf{y} \in \mathbb{Z}_{2^m}^n$ such that $v\mathbf{x} + (1-v)\mathbf{y} \in \mathtt{C}$, then $\mathbf{c}_1 \cdot (v\mathbf{x}+(1-v)\mathbf{y}) = v\mathbf{c}_1 \cdot \mathbf{x} + (1-v)\mathbf{c}_1 \cdot \mathbf{y} = 0 + (1-v)\mathbf{c}_1\mathbf{y}$.

Let $\mathbf{c} = v\mathbf{x}+(1-v)\mathbf{y} \in \mathtt{C}$, with $\mathbf{x} \in \mathtt{C}_1$ and $\mathbf{y} \in \mathtt{C}_2$. Then we multiply both sides, $v\mathbf{c}_1 \cdot \mathbf{c} = v\mathbf{c}_1 \cdot (v\mathbf{x} + (1-v)\mathbf{y} = 0$. So we get $v\mathbf{c}_1 \in \mathtt{C}^\perp$.

Since $\mathtt{C}^\perp = v\hat{\mathtt{C}}_1 + (1-v)\hat{\mathtt{C}}_2$, then $\mathbf{c}_1 \in \hat{\mathtt{C}}_1$ and $\mathtt{C}_1^\perp \subseteq \hat{\mathtt{C}}_1$. Therefore, we conclude that $\hat{\mathtt{C}}_1 = \mathtt{C}_1^\perp$. In the same way, we may prove that $\hat{\mathtt{C}}_2 = \mathtt{C}_2^\perp$. Therefore $\mathtt{C}^\perp = v\mathtt{C}_1^\perp + (1-v)\mathtt{C}_2^\perp$.

Next, we will prove that if $\mathtt{C}_1$ and $\mathtt{C}_2$ are Euclidean self-dual over $\mathbb{Z}_{2^m}$, then $\mathtt{C}$ is Euclidean self-dual. From $\mathtt{C} = v\mathtt{C}_1 \oplus (1-v)\mathtt{C}_2$ and the proof $\mathtt{C}^\perp = v\mathtt{C}_1^\perp + (1-v)\mathtt{C}_2^\perp$,

and because of $\mathtt{C}_1 = \mathtt{C}_1^{\perp}$ and $\mathtt{C}_2 = \mathtt{C}_2^{\perp}$, then $\mathtt{C} = \mathtt{C}^{\perp}$. So $\mathtt{C}$ must be Euclidean self-dual.

Vice versa, we will prove that if $\mathtt{C}$ is Euclidean self-dual, then $\mathtt{C}_1$ and $\mathtt{C}_2$ are Euclidean self-dual over $\mathbb{Z}_{2^m}$. By hypothesis $\mathtt{C} = \mathtt{C}^{\perp}$, then $v\mathtt{C}_1 + (1-v)\mathtt{C}_2 = v\mathtt{C}_1^{\perp} + (1-v)\mathtt{C}_2^{\perp}$. Hence, we have to prove that $\mathtt{C}_1 = \mathtt{C}_1^{\perp}$ and $\mathtt{C}_2 = \mathtt{C}_2^{\perp}$.

Let $\mathbf{c}_1 \in \mathtt{C}_1$, then

$$v\mathbf{c}_1 \in \mathtt{C} = \mathtt{C}^{\perp} = v\mathtt{C}_1^{\perp} \oplus (1-v)\mathtt{C}_2^{\perp}$$
$$v\mathbf{c}_1 = v\mathbf{x} + (1-v)\mathbf{y}, \text{ for } \mathbf{x} \in \mathtt{C}_1^{\perp}, \mathbf{y} \in \mathtt{C}_2^{\perp}$$

So $\mathbf{y} = 0$, then we get $v\mathbf{c}_1 = v\mathbf{x} \in \mathtt{C}_1^{\perp}$ and hence $\mathtt{C}_1 \subseteq \mathtt{C}_1^{\perp}$. In the same way we get $\mathtt{C}_2 \subseteq \mathtt{C}_2^{\perp}$.

Let $\mathbf{a} \in \mathtt{C}_1^{\perp}$, then there is $\mathbf{y} \in \mathtt{C}_2^{\perp}$ such that $v\mathbf{a} + (1-v)\mathbf{y} \in \mathtt{C}^{\perp}$. Since $\mathtt{C}^{\perp} = \mathtt{C}$, then $\mathbf{a} \in \mathtt{C}_1$. Hence $\mathtt{C}_1^{\perp} = \mathtt{C}_1$. In the same way, we get $\mathtt{C}_2^{\perp} = \mathtt{C}_2$. As a result $\mathtt{C}_1$ and $\mathtt{C}_2$ are both Euclidean self-dual.

■

V. Examples

In this section, we will give four examples. First, let $\mathtt{C} = \{(0,1),(2v,1+v)\}$ be a linear code over $R_1 = \mathbb{Z}_4 + v\mathbb{Z}_4$, where $v^2 = v$.

1) The length, number of codewords and minimum Gray distance of $\mathtt{C}$ respectively, are $[2,2,2]$. By using Gray map, then we get $\phi(\mathtt{C}) = \{(0,0,1,1),(0,2,1,2)\}$ is a linear code with parameter $[4,2,2]$ over R_1.

2)
$$\begin{aligned}\mathrm{Gray}_{\mathtt{C}}(S,T) &= \sum_{i=0}^{8} A_i S^{8-i}T^i \\ &= S^6T^2 + S^3T^5.\end{aligned}$$

$$\begin{aligned}\mathrm{Lee}_{\phi(\mathtt{C})}(S,T) &= \sum_{i=0}^{16} A_i S^{8-i}T^i \\ &= S^{12}T^4 + S^6T^{10}.\end{aligned}$$

3)
$$\mathrm{cwe}_{\mathtt{C}}(S_0,S_1,S_2,\cdots,S_{15}) = S_0S_4 + S_2S_5.$$
$$\mathrm{swe}_{\mathtt{C}}(T_0,T_1,T_2,T_3,T_4) = T_0T_2 + T_2T_3.$$
$$\mathrm{Ham}_{\mathtt{C}}(S,T) = ST + T^2.$$

4)
$$\mathrm{Gray}_{\mathtt{C}}(S,T) = S^4(S^2T^2) + (S^2T^2)(ST^3).$$
$$\mathrm{Ham}_{\mathtt{C}}(S,T) = \mathrm{swe}_{\mathtt{C}}(S,T,T,T,T).$$
$$\mathrm{Gray}_{\mathtt{C}}(S,T) = \mathrm{Lee}_{\phi(\mathtt{C})}(S,T).$$

The second, let $\mathtt{C} = \{(0,0),(4v,4+4v)\}$ be a linear code over $R_2 = \mathbb{Z}_8 + v\mathbb{Z}_8$, where $v^2 = v$.

1) The length, number of codewords and minimum Gray distance of $\mathtt{C}$ respectively, are $[2,2,2]$. By using Gray map, then we get $\phi(\mathtt{C}) = \{(0,0,0,0),(0,4,4,0)\}$ is a linear code with parameter $[4,2,2]$ over R_2.

2)
$$\begin{aligned}\mathrm{Gray}_{\mathtt{C}}(S,T) &= \sum_{i=0}^{16} A_i S^{16-i}T^i \\ &= S^{16} + S^8T^8.\end{aligned}$$

$$\begin{aligned}\mathrm{Lee}_{\phi(\mathtt{C})}(S,T) &= \sum_{i=0}^{32} A_i S^{32-i}T^i \\ &= S^{32} + S^8T^{24}.\end{aligned}$$

3)
$$\mathrm{cwe}_{\mathtt{C}}(S_0,S_1,S_2,\cdots,S_{64}) = S_0^2 + S_4S_{36}.$$
$$\mathrm{swe}_{\mathtt{C}}(T_0,T_1,T_2,\cdots,T_8) = T_0^2 + T_4^2.$$
$$\mathrm{Ham}_{\mathtt{C}}(S,T) = S^2 + T^2.$$

4)
$$\mathrm{Gray}_{\mathtt{C}}(S,T) = S^{16} + (S^4T^4)^2.$$
$$\mathrm{Ham}_{\mathtt{C}}(S,T) = \mathrm{swe}_{\mathtt{C}}(S,T,T,T,T,T,T,T,T).$$
$$\mathrm{Gray}_{\mathtt{C}}(S,T) = \mathrm{Lee}_{\phi(\mathtt{C})}(S,T).$$

The third, let $\mathtt{C} = \{(0,0,0,1,2),(2v,v,0,0,1),(2,1,1,v,1+v)\}$ be a linear code over R_1 where $v^2 = v$.

1) The length, number of codewords and minimum Gray distance of $\mathtt{C}$ respectively, are $[5,3,4]$. By using Gray map, then we get $\phi(\mathtt{C}) = \{(0,0,0,0,0,0,1,1,2,2),\ (0,2,0,1,0,0,0,0,1,1),\ (2,2,1,1,1,1,0,1,1,2)\}$ is a linear code with parameter $[10,3,4]$ over R_1.

2)
$$\begin{aligned}\mathrm{Gray}_{\mathtt{C}}(S,T) &= \sum_{i=0}^{20} A_i S^{20-i}T^i \\ &= S^{15}T^5 + S^{14}T^6 + S^8T^{12}.\end{aligned}$$

$$\begin{aligned}\mathrm{Lee}_{\phi(\mathtt{C})}(S,T) &= \sum_{i=0}^{40} A_i S^{40-i}T^i \\ &= S^{30}T^{10} + S^{28}T^{12} + S^{16}T^{24}.\end{aligned}$$

3)
$$\begin{aligned}\mathrm{cwe}_{\mathtt{C}}(S_0,S_1,S_2,\cdots,S_{64}) &= S_0^3S_4S_8 \\ &\quad + S_2S_1S_0^2S_4 \\ &\quad + S_8S_4^2S_1S_5.\end{aligned}$$

$$\begin{aligned}\mathrm{swe}_{\mathtt{C}}(T_0,T_1,T_2,\cdots,T_8) &= T_0^3T_1T_4 \\ &\quad + T_2^2T_1T_0^2 \\ &\quad + T_4T_2^2T_1T_3.\end{aligned}$$

$$\mathrm{Ham}_{\mathtt{C}}(S,T) = S^3T^2 + S^2T^3 + T^5.$$

4)
$$\begin{aligned}\mathrm{Gray}_{\mathtt{C}}(S,T) = {} & S^{12} + (S^2T^2)T^4 + \\ & S^8(S^2T^2)^2(S^3T) + \\ & T^4(S^2T^2)^2(S^3T)(ST^3).\end{aligned}$$
$$\mathrm{Ham}_{\mathtt{C}}(S,T) = \mathrm{swe}_{\mathtt{C}}(S,T,T,T,T,T,T,T,T)$$
$$\mathrm{Gray}_{\mathtt{C}}(S,T) = \mathrm{Lee}_{\phi(\mathtt{C})}(S,T)$$

The fourth, let $R_1 = \mathbb{Z}_4 + v\mathbb{Z}_4$ and $\mathtt{C} = v(2,1) \oplus (1-v)(1,1)$ be a linear code over R_1. By Theorem III.10, then we have $\mathtt{C}_1 = (2,1)$, $\mathtt{C}_2 = (1,1)$ are linear codes with length 2 over $\mathbb{Z}_4$ and we get:

1) $d_G(\mathtt{C}) = 2 = \min d_L(\mathtt{C}_1), d_L(\mathtt{C}_2)$.
2) $d_H = 2 = \min d_H(\mathtt{C}_1), d_H(\mathtt{C}_2)$.

VI. Conclusion

Structure of linear codes over R are investigated through a Gray map from R^n to $\mathbb{Z}_{2^m}^{2n}$. MacWilliams relations for both a Gray weight enumerators and a complete weight enumerator of linear codes over R are given. Necessary and sufficient condition to the MDS as well as self-dual codes over R are also provided.

References

[1] I. F. Blake, "Codes over certain rings," *Information and Control*, vol. 20, pp. 396–404, 1972.

[2] ——, "Codes over integer residue rings," *Information and Control*, vol. 29, pp. 295–300, 1975.

[3] Speigel, "Codes over $\mathbb{Z}_m$," *Information and Control*, vol. 35, pp. 48–51, 1977.

[4] ——, "Codes over $\mathbb{Z}_m$," *Information and Control*, vol. 37, pp. 100–104, 1978.

[5] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. Sloane, and P. Solé, "The $\mathbb{Z}_4-$linearity of kerdock, preparata, goethals, and related codes," *IEEE Transactions on Information Theory*, vol. 40, no. 2, pp. 301–319, 1994.

[6] B. Yildiz and S. Karadeniz, "Linear codes over $\mathbb{Z}_4+u\mathbb{Z}_4$: Macwilliams identities, projections, and formally self-dual codes," *Finite Fields and Their Application*, vol. 27, pp. 24–40, 2014.

[7] J. Gao, F.-W. Fu, and Y. Gao, "Some classes of linear codes over $\mathbb{Z}_4 + v\mathbb{Z}_4$ and their applications to construct good and new $\mathbb{Z}_4$-linear codes," *Applicable Algebra in Engineering, Communication and Computing*, vol. 28, no. 2, pp. 131–153, 2017.

[8] J. Gao, "Linear codes over $\mathbb{Z}_9 + u\mathbb{Z}_9$ macwilliams identity, self-dual codes, quadratic residue codes and constacyclic codes," *CoRR*, vol. abs/1405.3347, 2014. [Online]. Available: http://arxiv.org/abs/1405.3347

[9] M. Shi, A. Alahmadi, and P. Solé, *Codes and Rings: Theory and Practice*. Academic Press, 2017.

[10] B. Yildiz and Z. O. Ozger, "Generalization of the lee weight to $\mathbb{Z}_{p^k}$," *TWMS Journal of Applied and Engineering Mathematics*, vol. 2, no. 2, pp. 145–153, 2012.

[11] A. Barra, *Equivalence Theorems and the Local-Global Property*. Theses and Dissertations-Mathematics, 2012.

[12] J. A. Wood, "Duality for modules over finite rings and applications to coding theory," *American journal of Mathematics*, pp. 555–575, 1999.

[13] J. Wood, "Applications of finite frobenius rings to the foundations of algebraic coding theory," *Proceedings of the 44th Symposium on Ring Theory and Representation Theory, 223-245, Symp. Ring Theory Represent. Thoery Organ. Comm, Nagoya*, p. 224, 2012.

Sri Rosdiana is a lecturer at Politeknik Siber dan Sandi Negara, Bogor, Indonesia. She graduated from the Department of Mathematics, Universitas Indonesia and received her master degree in Mathematics from Institut Pertanian Bogor. At present, she is a Ph.D. student in Mathematics at Faculty of Mathematics and Natural Sciences, Institut Teknologi Bandung. Her research topics are Algebra and Cryptography.

Intan Muchtadi-Alamsyah received M.Sc and Ph.D. in Mathematics, University of Picardy, France. At present, she is an associate professor in Algebra Research Group, Faculty of Mathematics and Natural Sciences, Institut Teknologi Bandung, Indonesia. She is also appointed as a Vice President of South East Asian Mathematical Society, and a member of International Center of Pure and Applied Mathematics (CIMPA). Her research topics are Representation Theory, Ring Theory and Applications of Algebra in Coding Theory and Cryptography.

Djoko Suprijanto received M.Sc in Mathematics, Institut Teknologi Bandung and Ph.D. in Mathematics from Kyushu University, Japan. At present, he is an associate professor in Combinatorial Mathematics Research Group, Faculty of Mathematics and Natural Sciences, Institut Teknologi Bandung, Indonesia. He is also appointed as the Head of Combinatorial Mathematics Research Group. His research topics are Algebraic Combinatorics, Coding Theory and Graph Theory.

Aleams Barra received M.Sc in Mathematics, Institut Teknologi Bandung and Ph.D. in Mathematics from the University of Kentucky, USA. At present, he is a lecturer in Algebra Research Group, Faculty of Mathematics and Natural Sciences, Institut Teknologi Bandung, Indonesia. His research topics are Algebraic Coding Theory and General Algebra.