Discrete Mathematics Letters
www.dmlett.com

Discrete Math. Lett. **11** (2023) 53–60
DOI: 10.47443/dml.2022.091

Research Article

Linear codes over a general infinite family of rings and MacWilliams-type relations

Irwansyah[1], Djoko Suprijanto[2,*]

[1]*Department of Mathematics, Faculty of Mathematics and Natural Sciences, Universitas Mataram, Mataram, Indonesia*
[2]*Combinatorial Mathematics Research Group, Faculty of Mathematics and Natural Sciences, Institut Teknologi Bandung, Bandung, Indonesia*

(Received: 25 June 2022. Received in revised form: 30 September 2022. Accepted: 11 November 2022. Published online: 23 November 2022.)

Abstract

We study structural properties of linear codes over the ring $\mathcal{R}_k$ which is defined by $R[v_1, v_2, \ldots, v_k]$ with conditions $v_i^2 = v_i$ for $i = 1, 2, \ldots, k$, where R is any finite commutative Frobenius ring. We describe these linear codes in terms of necessary and sufficient conditions involving Gray maps, and we use these characterizations to construct Hermitian and Euclidean self-dual linear codes of this ring of arbitrary given length. We also derive MacWilliams-type relations for these codes with respect to Hamming weight enumerator as well as complete and symmetrized weight enumerators. As an application of the obtained results, we construct several optimal linear codes over $\mathbb{Z}_4$.

Keywords: commutative Frobenius rings; linear codes; complete weight enumeration; symmetrized weight enumeration; MacWilliams-type relations; optimal codes.

2020 Mathematics Subject Classification: 94A15, 94B05.

1. Introduction

Coding theory deals with designs of error-correcting codes for the reliable transmission of information across noisy channels. It was founded in 1948 with the publication of Shannon's paper [16]. Shannon demonstrated the existence of excellent codes among other things there. However, the proof of Shannon's theorem is not constructive. One of the main problems in coding theory is constructing good codes, namely codes with good parameters.

Linear codes over finite rings have been of interest since the work of Hammons, Kumar, Calderbank, Sloane and Solé in 1994 [9] where they proved, among other things, that certain good nonlinear binary codes can be constructed from linear codes over $\mathbb{Z}_4$ via a Gray map. Recently, many people consider some special cases of linear codes over the ring of the form $R[v_1, v_2, \ldots, v_k]$, where $v_i^2 = v_i$ for all $i = 1, 2, \ldots, k$, where $k \geq 1$ and R is a certain finite commutative ring. Among the reasons why it attracts the attention of many researchers in coding theory is because codes over such kind of rings have a lot of nice structures. For example, skew-cyclic codes over the rings $\mathbb{F}_2 + v\mathbb{F}_2, \mathbb{F}_p + v\mathbb{F}_p$ and $\mathbb{F}_{p^r}[v_1, v_2, \ldots, v_k]$ were considered in [1, 6, 11–13] and [14], respectively. Moreover, in [5], [8], [7], and [15] the structures of linear codes over $\mathbb{F}_2[v_1, v_2 \ldots, v_k]$, $\mathbb{Z}_4 + v\mathbb{Z}_4$, $\mathbb{Z}_9 + v\mathbb{Z}_9$, and $\mathbb{Z}_{2^m} + v\mathbb{Z}_{2^m}$ (with $v^2 = v$) were studied respectively, such as MacWilliams-type relations, self-dual codes, cyclic codes, constacyclic codes, *etc*. Also, we can find a construction of good and new $\mathbb{Z}_4$-linear codes in [8] (c.f. [4]).

In this paper, we investigate the structures of linear codes over the ring $R[v_1, v_2, \ldots, v_k]$, where R is any finite commutative Frobenius ring with additional conditions that $v_i^2 = v_i$, for all $i = 1, 2, \ldots, k$. This is a very general ring which covers the rings mentioned above. We define two kind of Gray maps. Several structural properties related to linear codes over the ring are observed. We also derive MacWilliams-type relations for complete and symmetrized weight enumerators. As an application, we construct several optimal linear codes over $\mathbb{Z}_4$.

We follow standard books of coding theory (for instance, see [10]) for undefined terms.

2. Automorphisms and Gray map

Let R be a finite commutative Frobenius ring. For $k \in \mathbb{N}$, let $\mathcal{R}_k$ denote the ring

$$R[v_1, v_2, \ldots, v_k] / \left\langle v_i^2 - v_i \right\rangle_{i=1}^{k}.$$

The ring $\mathcal{R}_k$ can be viewed as a free module over R with dimension 2^k. We have the following immediate property.

Lemma 2.1. *The ring $\mathcal{R}_k$ has cardinality $|R|^{2^k}$ and characteristic equals to $char(R)$.*

*Corresponding author (djoko.suprijanto@itb.ac.id).

Proof. As we can see, every element $\alpha \in \mathcal{R}_k$ can be written as

$$\alpha = \sum_{i=1}^{2^k} \alpha_{S_i} v_{S_i},$$

for some $\alpha_{S_i} \in R$, where $S_i \subseteq \{1, 2, \ldots, k\}$ and $v_{S_i} = \prod_{j \in S_i} v_j$, for all $1 \leq i \leq 2^k$. Therefore we have that $|\mathcal{R}_k| = |R|^{2^k}$. □

Let Θ_i be a map on $\mathcal{R}_k$ such that

$$\Theta_i(\alpha) = \begin{cases} 1 - v_i, & \alpha = v_i, \\ \alpha, & \text{otherwise.} \end{cases}$$

Then define

$$\Theta_S := \prod_{i \in S} \Theta_i = \Theta_{i_1} \circ \Theta_{i_2} \circ \cdots \circ \Theta_{i_{|S|}},$$

where $S \subseteq \{1, 2, \ldots, k\}$.

Also, let $S_1, S_2 \subseteq \{1, 2, \ldots, k\}$, where $|S_1| = |S_2|$, and $\phi_{S_1,S_2} : \{1, 2, \ldots, k\} \to \{1, 2, \ldots, k\}$ be a map such that it is a bijection from S_1 to S_2 and $\phi_{S_1,S_2}(j) = j$, for all $j \notin S_1$. Define a map Φ_{S_1,S_2} on $\mathcal{R}_k$, where

$$\Phi_{S_1,S_2}(\alpha v_j) = \vartheta(\alpha) v_{\phi_{S_1,S_2}(j)},$$

for some automorphism ϑ of R.

We note that the maps Θ_S and Φ_{S_1,S_2} are both automorphisms on the ring $\mathcal{R}_k$, as are their compositions. In this paper we consider automorphism ϑ as a composition of Θ_S or Φ_{S_1,S_2} (or both of them).

Now, we define two Gray maps from the ring $\mathcal{R}_k$. First, for $j \geq 1$, any element α in $\mathcal{R}_j$ can be written as $\alpha = \alpha_1 + \alpha_2 v_j$, for some $\alpha_1, \alpha_2 \in \mathcal{R}_{j-1}$. For some integer $l_j \geq 2$, define a map $\varphi_j : \mathcal{R}_j \longrightarrow \mathcal{R}_{j-1}^{l_j}$ by

$$\alpha_1 + \alpha_2 v_j \longmapsto \left(\alpha_1, \beta_1\alpha_1 + \beta_1'\alpha_2, \beta_2\alpha_1 + \beta_2'\alpha_2, \ldots, \beta_{l_j-1}\alpha_1 + \beta_{l_j-1}'\alpha_2\right),$$

where β_i, β_i' are some elements in $\mathcal{R}_{j-1}$, for all $1 \leq i \leq l_j - 1$, with β_{l_j-1}' is a unit in $\mathcal{R}_{j-1}$. The following lemma shows that φ_j is an injective map and also a module homomorphism.

Lemma 2.2. *The map φ_j is an injective and also a $\mathcal{R}_{j-1}$-module homomorphism from $\mathcal{R}_j$ to $\mathcal{R}_{j-1}^{l_j}$, for all $1 \leq j \leq k$.*

Proof. For *injectivity*, take any α and α' in $\mathcal{R}_j$, where $\varphi_j(\alpha) = \varphi_j(\alpha')$. Now, let $\alpha = \alpha_1 + \alpha_2 v_j$ and $\alpha' = \alpha_1' + \alpha_2' v_j$, for some $\alpha_1, \alpha_2, \alpha_1'$, and α_2' in $\mathcal{R}_{j-1}$. Since $\varphi_j(\alpha) = \varphi_j(\alpha')$, we have $\alpha_1 = \alpha_1'$. Using the previous fact and by considering the last coordinate of the images under φ_j, we have $\beta_{l_j}'\alpha_2 = \beta_{l_j}'\alpha_2'$. Since β_{l_j}' is a unit in $\mathcal{R}_{j-1}$, we also have $\alpha_2 = \alpha_2'$ as required.

Now, take any α and α' in $\mathcal{R}_j$ and any λ in $\mathcal{R}_{j-1}$. Let $\alpha = \alpha_1 + \alpha_2 v_j$ and $\alpha' = \alpha_1' + \alpha_2' v_j$, for some $\alpha_1, \alpha_2, \alpha_1'$ and α_2' in $\mathcal{R}_{j-1}$. Consider

$$\begin{aligned} \varphi_j(\alpha + \alpha') &= \left(\alpha_1 + \alpha_1', \beta_1(\alpha_1 + \alpha_1') + \beta_1'(\alpha_2 + \alpha_2'), \beta_2(\alpha_1 + \alpha_1') + \beta_2'(\alpha_2 + \alpha_2'), \ldots, \beta_{l_j-1}(\alpha_1 + \alpha_1') + \beta_{l_j-1}'(\alpha_2 + \alpha_2')\right) \\ &= \varphi_j(\alpha) + \varphi_j(\alpha'), \end{aligned}$$

and

$$\varphi_j(\lambda\alpha) = \left(\lambda\alpha_1, \beta_1\lambda\alpha_1 + \beta_1'\lambda\alpha_2, \beta_2\lambda\alpha_1 + \beta_2'\lambda\alpha_2, \ldots, \beta_{l_j-1}\lambda\alpha_1 + \beta_{l_j-1}'\lambda\alpha_2\right) = \lambda\varphi_j(\alpha).$$

Therefore, the map φ_j is an $\mathcal{R}_{j-1}$-module homomorphism for all $1 \leq j \leq k$. □

We combine the maps φ_j and φ_{j-1} to get a map $\varphi_{j-1} \circ \varphi_j$ from $\mathcal{R}_j$ to $\mathcal{R}_{j-2}^{l_j \times l_{j-1}}$ as

$$\varphi_{j-1} \circ \varphi_j(\alpha_1 + \alpha_2 v_j) = \left(\varphi_{j-1}(\alpha_1), \varphi_{j-1}(\beta_1\alpha_1 + \beta_1'\alpha_2), \varphi_{j-1}(\beta_2\alpha_1 + \beta_2'\alpha_2), \ldots, \varphi_{j-1}(\beta_{l_j-1}\alpha_1 + \beta_{l_j-1}'\alpha_2)\right).$$

By doing it inductively, we will have a Gray map $\Phi_k := \varphi_1 \circ \varphi_2 \circ \cdots \circ \varphi_k$ from $\mathcal{R}_k$ to $R^{l_k \times l_{k-1} \times \cdots \times l_1}$.

We can extend the map φ_j to get a map $\overline{\varphi}_j$ from $\mathcal{R}_j^n$ to $\mathcal{R}_{j-1}^{nl_j}$, naturally, by mapping

$$(\alpha_{1,1} + \alpha_{1,2} v_j, \ldots, \alpha_{n,1} + \alpha_{n,2} v_j)$$

to

$$\left(\alpha_{1,1}, \ldots, \alpha_{n,1}, \beta_1\alpha_{1,1} + \beta_1'\alpha_{1,2}, \ldots, \beta_1\alpha_{n,1} + \beta_1'\alpha_{n,2}, \ldots, \beta_{l_j-1}\alpha_{1,1} + \beta_{l_j-1}'\alpha_{1,2}, \ldots, \beta_{l_j-1}\alpha_{n,1} + \beta_{l_j-1}'\alpha_{n,2}\right).$$

We combine $\overline{\varphi}_j$ and $\overline{\varphi}_{j-1}$ to get a map from $\mathcal{R}_j^n$ to $\mathcal{R}_{j-2}^{nl_jl_{j-1}}$, and inductively, to get a Gray map $\overline{\Phi}_k$ from $\mathcal{R}_k^n$ to $R^{nl_k\cdots l_1}$. The map φ_j and its extensions are a generalization of Gray maps in [5], and also in [14].

Now, let us define a second Gray map. Any α in $\mathcal{R}_k$ can be written as $\alpha = \sum_{i=1}^{2^k} \alpha_{S_i} v_{S_i}$, for some α_{S_i} in R, where $S_i \subseteq \{1, 2, \ldots, k\}$ and $v_{S_i} = \prod_{t\in S_i} v_t$, for all $1 \le i \le 2^k$. Define a map Ψ as follows.

$$\begin{array}{rccc} \Psi: & \mathcal{R}_k & \longrightarrow & R^{2^k} \\ & \sum_{i=1}^{2^k} \alpha_{S_i} v_{S_i} & \longmapsto & \left(\sum_{S\subseteq S_1} \alpha_S, \ldots, \sum_{S\subseteq S_{2^k}} \alpha_S\right) \end{array}.$$

We can check that the map Ψ is a bijection. Moreover, we can also check that the map Ψ is an isomorphism, which implies

$$\mathcal{R}_k \cong \underbrace{R \times R \times \cdots \times R}_{2^k}.$$

This means $\mathcal{R}_k$ is also a finite commutative Frobenius ring.

Let $\overline{\Psi} : \mathcal{R}_k^n \to R^{2^k\times n}$ be a map such that

$$\overline{\Psi}(a_1, \ldots, a_n) = (\Psi(a_1), \ldots, \Psi(a_n)).$$

Then, we can see that $\overline{\Psi}$ is also a bijective map because Ψ is bijective. Let Σ_S and Γ_{S_1,S_2} be two maps such that $\overline{\Psi}\circ\Theta_S = \Sigma_S\circ\overline{\Psi}$ and $\overline{\Psi}\circ\Phi_{S_1,S_2} = \Gamma_{S_1,S_2}\circ\overline{\Psi}$. As we can see, the maps Σ_S and Γ_{S_1,S_2} are bijective maps induced by Θ_S and Φ_{S_1,S_2}, respectively.

3. Linear and self-dual codes

In this section, we describe linear codes over $\mathcal{R}_k$ using the Gray maps defined in Section 2. The theorems below describe the image of a linear code under the gray maps $\overline{\varphi}_j$ and $\overline{\Psi}$. The following theorem provide the image of a linear code under the map $\overline{\varphi}_j$.

Theorem 3.1. *A code C is a linear code of length n over $\mathcal{R}_j$ if and only if the image $\overline{\varphi}_j(C)$ is a linear code of length nl_j over $\mathcal{R}_{j-1}$.*

We have the following consequence (due to the first Gray map $\overline{\Phi}_k$).

Corollary 3.1. *A code C is a linear code of length n over $\mathcal{R}_k$ if and only if the code*

$$\overline{\Phi}_k = \overline{\varphi}_1 \circ \overline{\varphi}_2 \circ \cdots \circ \overline{\varphi}_k(C)$$

is a linear code of length $nl_1\cdots l_k$ over R.

The following theorem describes the image of a linear code under the second Gray map $\overline{\Psi}$.

Theorem 3.2. *A code C is a linear code of length n over $\mathcal{R}_k$ if and only if there exist linear codes, $C_1, C_2, \ldots, C_{2^k}$, of length n over R such that $C = \overline{\Psi}^{-1}(C_1, C_2, \ldots, C_{2^k})$.*

Proof. Similar to the proof of [13, Lemma 16]. □

Now, let us consider Euclidean and Hermitian self-dual codes. Let Θ_S be an automorphism in the ring $\mathcal{R}_k$ as in Section 2, where $S = \{1, 2, \ldots, k\}$. For any $\mathbf{c} = (c_1, \ldots, c_n)$ and $\mathbf{c}' = (c'_1, \ldots, c'_n)$ in $\mathcal{R}_k^n$, define the Hermitian product as follows,

$$[\mathbf{c}, \mathbf{c}'] = \sum_{i=1}^{n} c_i\overline{c'_i} = \sum_{i=1}^{n} c_i\Theta_S(c'_i).$$

Let $C^H = \{\mathbf{c}' : [\mathbf{c}, \mathbf{c}'] = 0\ \forall \mathbf{c} \in C\}$. A code C is called *Hermitian self-orthogonal* if $C \subseteq C^H$, and C is called *Hermitian self-dual* if $C = C^H$. Also, for any $\mathbf{c} = (c_1, \ldots, c_n)$ and $\mathbf{c}' = (c'_1, \ldots, c'_n)$, define the Euclidean product as the following rational sum,

$$\mathbf{c}\cdot\mathbf{c}' = \sum_{i=1}^{n} c_ic'_i.$$

Let $C^\perp = \{\mathbf{c}' : \mathbf{c}\cdot\mathbf{c}' = 0\ \forall \mathbf{c} \in C\}$. A code C is called *Euclidean self-orthogonal* if $C \subseteq C^\perp$, and C is called *Euclidean self-dual* if $C = C^\perp$. The next theorem shows the existence of Hermitian self-dual codes over $\mathcal{R}_k$.

Theorem 3.3. *If $S \neq \emptyset$, then there exist Hermitian self-dual codes over $\mathcal{R}_k$ for all lengths.*

Proof. Take i in S. Let $C_1 = \langle v_i \rangle$, then we have $C_1^H = \langle v_i \rangle = C_1$, because $v_i(1 - v_i) = 0$. So, Hermitian self-dual codes of length 1 over $\mathcal{R}_k$ exist. Now, for any length n, define

$$C = \underbrace{C_1 \times C_1 \times \cdots \times C_1}_{n}.$$

As we can see, $C^H = C$, which means C is an Hermitian self-dual code of length n. □

Note that, the ring $\mathcal{R}_k$ can be written as $\mathcal{R}_k = v_k\mathcal{R}_{k-1} + (1 - v_k)\mathcal{R}_{k-1}$. Consequently, any code C of length n over $\mathcal{R}_k$ can be written as $C = v_kC_1 + (1 - v_k)C_2$, where C_1 and C_2 are codes of length n over $\mathcal{R}_{k-1}$.

Proposition 3.1. *If C is a Hermitian self-dual code of length n over $\mathcal{R}_1$, then C is isomorphic to $C_1 \times C_1^{\perp}$, where C_1 is a code of length n over R.*

Proof. Remember that C can be written as $C = vC_1 + (1 - v)C_2$, where C_1 and C_2 are codes of length n over R. Consider

$$\begin{aligned}
[\mathbf{c}, \mathbf{c}'] &= \sum_i c_i \overline{c_i'} \\
&= \sum_i (vc_{1i} + (1 - v)c_{2i})\, \overline{(vc_{1i}' + (1 - v)c_{2i}')} \\
&= \sum_i (vc_{1i} + (1 - v)c_{2i})\, ((1 - v)c_{1i}' + vc_{2i}') \\
&= v \sum_i c_{1i}c_{2i}' + (1 - v) \sum_i c_{2i}c_{1i}',
\end{aligned} \tag{1}$$

where $(c_{j1}, c_{j2}, \ldots, c_{jn})$ is in C_j, for $j = 1, 2$. If Equation (1) is equal to 0, then it requires $\sum_i c_{1i}c_{2i}' = 0$ and $\sum_i c_{2i}c_{1i}' = 0$. Since C is self dual, we have $C_1 = C_2^{\perp}$ and $C_2 = C_1^{\perp}$. Therefore, C is isomorphic to $C_1 \times C_1^{\perp}$. □

Using the above property, we have the theorem below.

Theorem 3.4. *If C is a Hermitian self-dual code of length n over $\mathcal{R}_k$, then, with proper arrangement of indices, C is isomorphic to*

$$C_1 \times C_1^{\perp} \times \cdots \times C_{2^{k-1}} \times C_{2^{k-1}}^{\perp},$$

where $C_1, \ldots, C_{2^{k-1}}$ are codes of length n over R.

Proof. We can write $C = v_kC' + (1 - v_k)C''$, where C' and C'' are codes of length n over R_{k-1}. Consider

$$\begin{aligned}
[\mathbf{c}_1, \mathbf{c}_2] &= \sum_i c_{1i}\overline{c_{2i}} \\
&= \sum_i (v_kc_{1i}' + (1 - v_k)c_{1i}'')\, \overline{(v_kc_{2i}' + (1 - v_k)c_{2i}'')} \\
&= \sum_i (v_kc_{1i}' + (1 - v_k)c_{1i}'') \left((1 - v_k)\overline{c_{2i}'} + v_k\overline{c_{2i}''}\right) \\
&= v_k \sum_i c_{1i}'\overline{c_{2i}''} + (1 - v_k) \sum_i c_{2i}'\overline{c_{1i}''},
\end{aligned} \tag{2}$$

where $(c_{j1}', c_{j2}', \ldots, c_{jn}')$ is in C' and $(c_{j1}'', c_{j2}'', \ldots, c_{jn}'')$ is in C'', for $j = 1, 2$. If Equation (2) is equal to 0, then it requires

$$\sum_i c_{1i}'\overline{c_{2i}''} = 0 \tag{3}$$

and

$$\sum_i c_{2i}'\overline{c_{1i}''} = 0. \tag{4}$$

If we continue a similar process on Equations (3) and (4), we will have 2^k equations similar to Equation (1) over R. By Proposition 3.1, 2^k equations give 2^{k-1} pairs of Euclidean dual over R. Therefore, we have that C is isomorphic to

$$C_1 \times C_1^{\perp} \times \cdots \times C_{2^{k-1}} \times C_{2^{k-1}}^{\perp},$$

where $C_1, C_2, \ldots, C_{2^{k-1}}$ are codes of length n over R. □

Regarding the Euclidean self-dual codes, we have the necessary and sufficient conditions as follows.

Theorem 3.5. *A code C is an Euclidean self-dual code of length n over $\mathcal{R}_k$ if and only if $C = \overline{\Psi}^{-1}(C_1, C_2, \ldots, C_{2^k})$, where $C_1, \ldots, C_{2^k}$ are also Euclidean self-dual codes over R.*

Proof. Similar to the proof of [12, Proposition 4.1]. □

As an immediate consequence, we have the following.

Corollary 3.2. *Euclidean self-dual codes of length n over $\mathcal{R}_k$ exist if and only if Euclidean self-dual codes of length n over R exist.*

4. Weights and MacWilliams-type relations

Let $wt_H(\mathbf{c})$ be a *Hamming weight* of codeword $\mathbf{c}$. Let $d_H(C)$ be the *Hamming distance* of a code C. The following proposition gives the Hamming distance for codes over the ring $\mathcal{R}_k$.

Proposition 4.1. *If $C = \overline{\Psi}^{-1}(C_1, \ldots, C_{2^k})$, is a code of length n over $\mathcal{R}_k$, then $d_H(C) = \min\limits_{1 \le i \le 2^k} d_H(C_i)$.*

Proof. Let $d_H(C_j) = \min\limits_{1 \le i \le 2^k} d_H(C_i)$, for some j. Also, let $\mathbf{c}_j$ be a codeword in C_j such that $wt(\mathbf{c}_j) = d_H(C_j)$. Then we have that

$$d_H(C) = wt\left(\overline{\Psi}^{-1}(\mathbf{0}, \ldots \mathbf{0}, \mathbf{c}_j, \mathbf{0}, \ldots, \mathbf{0})\right) = d_H(C_j).$$

□

Let

$$W_C(X, Y) = \sum_{\mathbf{c} \in C} X^{n - wt_H(\mathbf{c})} Y^{wt_H(\mathbf{c})},$$

be *the Hamming weight enumerator* of a code C. We have the following relation between Hamming weight enumerator of a code C and its dual.

Proposition 4.2. *If C is a code of length n over $\mathcal{R}_k$, then*

$$W_{C^\perp}(X, Y) = \frac{1}{|C|} W_C\left(X + (|R|^{2^k} - 1)Y, X - Y\right).$$

Now, let $\mathrm{wt}_{\mathrm{L}}(\alpha)$ be the Lee weight of any element α in R. Let $a = \sum_{S \subseteq \{1,2,\ldots,k\}} \alpha_S v_S$ be any element in $\mathcal{R}_k$. Define

$$\mathrm{Wt}_{\mathrm{L}}(a) = \sum_{i=1}^{2^k} \mathrm{wt}_{\mathrm{L}}\left(\sum_{S \subseteq S_i} \alpha_S\right)$$

be the Lee weight of a. For any $\mathbf{a} = (a_1, \ldots, a_n)$ in $\mathcal{R}_k^n$, define the Lee weight of $\mathbf{a}$ as follows,

$$\mathrm{Wt}_{\mathrm{L}}(\mathbf{a}) = \sum_{j=1}^{n} Wt_L(a_j).$$

Then we have the following result.

Proposition 4.3. *If $C = \overline{\Psi}^{-1}(C_1, \ldots, C_{2^k})$ is a code of length n over $\mathcal{R}_k$, then*

$$d_L(C) = \min_{1 \le i \le 2^k} d_L(C_i).$$

Proof. Let $d_L(C_j) = \min_{1 \le i \le 2^k} d_L(C_i)$, for some j, and let $\mathbf{c}_j$ be a codeword in C_j such that $\mathrm{Wt}_{\mathrm{L}}(\mathbf{c}_j) = d_L(C_j)$. We have that

$$d_L(C) = \mathrm{Wt}_{\mathrm{L}}\left(\overline{\Psi}^{-1}(\mathbf{0}, \ldots \mathbf{0}, \mathbf{c}_j, \mathbf{0}, \ldots, \mathbf{0})\right) = d_L(C_j).$$

□

Since the ring $\mathcal{R}_k$ is isomorphic to R^{2^k}, the generating character for $\widehat{\mathcal{R}_k}$ is the product of generating character for $\widehat{R}$. Now, if χ is a generating character for R, such that

$$\chi(x) = \xi^{wt_L(x)},$$

for any $x \in R$, then the generating character χ for $\mathcal{R}_k$ is

$$\chi_1(\beta) = \xi^{Wt_L(\overline{\Psi}(\beta))},$$

for any $\beta \in \mathcal{R}_k$.

Define the matrix T indexed by $\alpha, \beta \in \mathcal{R}_k$, as follows

$$T_{\alpha,\beta} = \chi_\alpha(\beta) = \chi(\alpha\beta),$$

and the matrix T_H as follows

$$(T_H)_{\alpha,\beta} = \chi_\alpha(\overline{\beta}) = \chi(\alpha\overline{\beta}),$$

where $\overline{\beta}$ is the conjugate of β induced by Θ_S, for some $S \subseteq \{1, 2, \ldots, k\}$.

Also, define the complete weight enumerator for a code C as follows,

$$\mathrm{cwe}_C(\mathbf{X}) = \sum_{\mathbf{c}\in C} \prod_{b\in\mathcal{R}_k} X_b^{n_b(\mathbf{c})},$$

where $n_b(\mathbf{c})$ is the number of occurrences of the element b in $\mathbf{c}$. Then, by applying Corollary 8.2 in [18], we have the following result.

Theorem 4.1. *If C is a linear code over $\mathcal{R}_k$, then*

$$\mathrm{cwe}_{C^\perp}(\mathbf{X}) = \frac{1}{|C|}\,\mathrm{cwe}_C(T\cdot\mathbf{X}) \tag{5}$$

and

$$\mathrm{cwe}_{C^H}(\mathbf{X}) = \frac{1}{|C|}\,\mathrm{cwe}_C(T_H\cdot\mathbf{X}) \tag{6}$$

Proof. This theorem is a consequence of [18, Corollary 8.2]. □

Note that T is a $|R|^{2^k}$ by $|R|^{2^k}$ matrix indexed by the elements of $\mathcal{R}_k$. Let $\mathcal{R}_k^\times$ be the group of units in the ring $\mathcal{R}_k$ and let $\alpha \sim \alpha'$ if $\alpha' = u\alpha$, for some $u \in G$, where G is a subgroup of $\mathcal{R}_k^\times$. It can be seen that the relation $\sim$ is an equivalence relation, so we define $\mathcal{A} = \{\alpha_1, \ldots, \alpha_t\}$ be the set of representatives. Let S be the t by t matrix indexed by the elements in $\mathcal{A}$. Also, define $S_{\alpha,\beta} = \sum_{\gamma\sim\beta} T_{\alpha,\gamma}$. We have the following lemma.

Lemma 4.1. *If $\alpha \sim \alpha'$ then the row S_α is equal to the row $S_{\alpha'}$.*

Proof. If $\alpha \sim \alpha'$ then for any column β we have

$$S_{\alpha',\beta} = \sum_{\gamma\sim\beta} T_{\alpha',\gamma} = \sum_{\gamma\sim\beta} \xi^{\mathrm{Wt_L}(\overline{\Psi}(\alpha'\gamma))}.$$

Since $\overline{\Psi}(\alpha\gamma) = \overline{\Psi}(\alpha)\overline{\Psi}(\gamma)$, where the multiplication in the right side of equal sign carried out coordinate-wise, we have that

$$\begin{aligned}\sum_{\gamma\sim\beta} T_{\alpha',\gamma} &= \sum_{\gamma\sim\beta} \xi^{\mathrm{Wt_L}(\overline{\Psi}(\alpha)\overline{\Psi}(u)\overline{\Psi}(\gamma))}\\ &= \sum_{\gamma'\sim\beta} \xi^{\mathrm{Wt_L}(\overline{\Psi}(\alpha)\overline{\Psi}(\gamma'))}\\ &= \sum_{\gamma'\sim\beta} T_{\alpha,\gamma'}\\ &= S_{\alpha,\beta}.\end{aligned}$$

Therefore, $S_\alpha = S_{\alpha'}$ when $\alpha \sim \alpha'$. □

Now, define the symmetrized weight enumerator for a code C to be

$$\mathrm{swe}_C(\mathbf{Y}_\mathcal{A}) = \sum_{\mathbf{c}\in C} \prod_{\alpha\in\mathcal{A}} Y_\alpha^{\mathrm{swc}_\alpha(\mathbf{c})},$$

where $\mathrm{swc}_\alpha(\mathbf{c}) = \sum_{\alpha'\sim\alpha} n_{\alpha'}(\mathbf{c})$. Again, by using Theorem 8.4 in [18], we have the following theorem.

Theorem 4.2. *If C is a linear code over $\mathcal{R}_k$, then*

$$\mathrm{swe}_{C^\perp} = \frac{1}{|C|}\,\mathrm{swe}_C(S\cdot\mathbf{Y}_\mathcal{A}).$$

Remark 4.1. *Theorem 4.1 and 4.2 are Macwilliams-type relations for complete and symmetrized weight enumerators, respectively.*

5. An application

As application, in this section, we use the map φ_1 to obtain linear codes over $\mathbb{Z}_4$ from the codes over $\mathcal{R}_1 = \mathbb{Z}_4 + v\mathbb{Z}_4$, where $v^2 = v$. For any element $\mathbf{x} = (x_1, \ldots, x_n)$ in $\mathbb{Z}_4^n$, the Lee weight of $\mathbf{x}$, denoted by $w_L(\mathbf{x})$, is defined as

$$w_L(\mathbf{x}) = \sum_{i=1}^{n} \min\{|x_i|, |4 - x_i|\}. \tag{7}$$

Using the above weight, we define the Lee distance $d_L(C)$ of a code C as

$$d_L(C) = \min_{\substack{\mathbf{c} \in C \\ \mathbf{c} \neq \mathbf{0}}} w_L(\mathbf{c}).$$

We will give some examples of codes over $\mathbb{Z}_4$ with the highest known maximum Lee distance (see [2], [3]), constructed using the map φ_1.

Example 5.1. *Define a map φ_1 as follows.*

$$\begin{array}{rccc} \varphi_1: & \mathbb{Z}_4 + v\mathbb{Z}_4 & \longrightarrow & \mathbb{Z}_4^2 \\ & \alpha + v\beta & \longmapsto & (\alpha, 2\alpha + \beta). \end{array}$$

Let $C = \langle 1 + v \rangle = \{0, 1 + v, 2 + 2v, 3 + 3v, 2v, 2, 1 + 3v, 3 + v\}$ be a code of length 1 over $\mathcal{R}_1 = \mathbb{Z}_4 + v\mathbb{Z}_4$, where $v^2 = v$. We have,

$$\begin{array}{ll} \varphi_1(1 + v) = (1, 3), & \varphi_1(2 + 2v) = (2, 2), \\ \varphi_1(3 + 3v) = (3, 1), & \varphi_1(2v) = (0, 2), \\ \varphi_1(2) = (2, 0), & \varphi_1(1 + 3v) = (1, 1), \\ \varphi_1(3 + v) = (3, 3). & \end{array}$$

We can see that $d_L(\varphi_1(C)) = 2$ and $|\varphi_1(C)| = 8$.

Example 5.2. *Define a map φ_1 as follows.*

$$\begin{array}{rccc} \varphi_1: & \mathbb{Z}_4 + v\mathbb{Z}_4 & \longrightarrow & \mathbb{Z}_4^3 \\ & \alpha + v\beta & \longmapsto & (\alpha, \beta, \alpha + \beta). \end{array}$$

Let $C = \langle 2 \rangle = \{0, 2, 2v, 2 + 2v\}$. We have that

$$\varphi_1(2) = (2, 0, 2),\ \varphi_1(2v) = (0, 2, 2),\ \varphi_1(2 + 2v) = (2, 2, 0).$$

So, $d_L(\varphi_1(C)) = 4$ and $|\varphi_1(C)| = 4$.

Example 5.3. *Define a map φ_1 as follows.*

$$\begin{array}{rccc} \varphi_1: & \mathbb{Z}_4 + v\mathbb{Z}_4 & \longrightarrow & \mathbb{Z}_4^5 \\ & \alpha + v\beta & \longmapsto & (\alpha, \beta, \alpha + \beta, \alpha, \alpha + \beta). \end{array}$$

Let $C = \langle 2 \rangle$. We can see that,

$$\begin{array}{ll} \varphi_1(2) = (2, 0, 2, 0, 2), & \varphi_1(2v) = (0, 2, 2, 0, 2), \\ \varphi_1(2 + 2v) = (2, 2, 0, 2, 0). & \end{array}$$

Therefore, we have $d_L(\varphi_1(C)) = 6$ and $|\varphi_1(C)| = 4$.

6. Conclusion

In this paper, we considered several aspects of linear codes over a very general ring, $\mathcal{R}_k = R[v_1, v_2, \ldots, v_k] / \left\langle v_i^2 - v_i \right\rangle_{i=1}^{k}$, where R is a finite commutative Frobenius ring. MacWilliams-type relations with respect to complete weight as well as symmetrized weight enumerators are proved. As an application, we provide examples to constructed optimal linear codes over $\mathbb{Z}_4$. Other concrete examples of linear codes constructed in this way can be found, for examples, in [4, 8, 15].

There are several directions for further investigation. We are now working on investigating structural properties of cyclic, quasi-cyclic and skew cyclic codes over the ring $\mathcal{R}_k$, together with applications in constructing quantum error-correcting codes from the codes over rings (c.f. [17]).

Acknowledgement

This research is supported by the Institut Teknologi Bandung (ITB) and the Ministry of Education, Culture, Research and Technology (*Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi (Kemdikbudristek)*), Republic of Indonesia.

References

[1] T. Abualrub, N. Aydin, P. Seneviratne, On θ-cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$, *Australas. J. Combin.* **54** (2012) 115–126.

[2] N. Aydin, T. Asamov, A database of $\mathbb{Z}_4$ codes, *J. Comb. Inf. Syst. Sci.* **34** (2009) 1–12.

[3] N. Aydin, T. Asamov, Online database of $\mathbb{Z}_4$ codes, available at https://web.archive.org/web/20220518191122/https://quantumcodes.info/Z4.

[4] Bustomi, A. P. Santika, D. Suprijanto, Linear codes over the rings $\mathbb{Z}_4 + u\mathbb{Z}_4 + v\mathbb{Z}_4 + w\mathbb{Z}_4 + uv\mathbb{Z}_4 + uw\mathbb{Z}_4 + vw\mathbb{Z}_4 + uvw\mathbb{Z}_4$, *IAENG Int. J. Comput. Sci.* **48** (2021) 686–696.

[5] Y. Cengellenmis, S. Dougherty, D. Abdullah, Codes over an infinite family of rings with a Gray map, *Des. Codes Cryptogr.* **72** (2014) 559–580.

[6] J. Gao, Skew cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$, *J. Appl. Math. Inform.* **31** (2013) 337–342.

[7] J. Gao, Self-dual codes and quadratic residue codes over the ring $\mathbb{Z}_9 + u\mathbb{Z}_9$, arXiv:1405.3347v3 [cs.IT].

[8] J. Gao, F.-W. Fu, 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, *Appl. Algebra Engin. Comm. Comput.* **28** (2017) 131–153.

[9] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes, *IEEE Trans. Inform. Theory* **40** (1994) 301–319.

[10] W. C. Huffman, V. Pless, *Fundamentals of Error Correcting Codes*, Cambridge University Press, 2003.

[11] Irwansyah, A. Barra, S. T. Dougherty, A. Muchlis, I. Muchtadi-Alamsyah, P. Solé, D. Suprijanto, O. Yemen, Θ_S-cyclic codes over A_k, *Int. J. Comput. Math. Comput. Syst. Theory* **1** (2016) 14–31.

[12] Irwansyah, A. Barra, I. Muchtadi-Alamsyah, A. Muchlis, D. Suprijanto, Codes over infinite family of algebras, *J. Algebra Combin. Discrete Struct. Appl.* **4** (2016) 131–140.

[13] Irwansyah, A. Barra, I. Muchtadi-Alamsyah, A. Muchlis, D. Suprijanto, Skew-cyclic codes over B_k, *J. Appl. Math. Comput.* **57** (2018) 69–84.

[14] Irwansyah, D. Suprijanto, Structure of linear codes over the ring B_k, *J. Appl. Math. Comput.* **58** (2018) 755–775.

[15] S. Rosdiana, M. I. Detiena, D. Suprijanto, A. Barra, On linear codes over $\mathbb{Z}_{2^m} + v\mathbb{Z}_{2^m}$, *IAENG Int. J. App. Math.* **51** (2021) 133–141.

[16] C. E. Shannon, A mathematical theory of communication, *Bell Syst. Tech. J.* **27** (1948) 379–423.

[17] D. Suprijanto, H. C. Tang, Quantum codes constructed from cyclic codes over a finite non-chain ring, *IAENG Int. J. Comput. Sci.* **49** (2022) 695–700.

[18] J. Wood, Duality for modules over finite rings and applications to coding theory, *Amer. J. Math.* **121** (1999) 555–575.