# Homogeneous and other Weight Functions on $\mathbb{F}_q[u_1, u_1, \ldots, u_l]/\left(u_i^2\right)$

Jane D. Palacio
Institute of Mathematical Sciences and Physics
University of the Philippines Los Baños
College, Laguna 4031, Philippines
jdpalacio@uplb.edu.ph

Pierre Allan K. Santiago
Institute of Mathematical Sciences and Physics
University of the Philippines Los Baños
College, Laguna 4031, Philippines
spierreallan@gmail.com

John Paul V. Guim
Institute of Mathematical Sciences and Physics
University of the Philippines Los Baños
College, Laguna 4031, Philippines
guim28@gmail.com

## ABSTRACT

Let $q = p^m$ be a power of a prime $p$ and $m, l \in \mathbb{N}$. Denote by $\mathbb{F}_q$ the Galois field of characteristic $p$ and cardinality $q$. In this paper, the ring $R(q,l) = \mathbb{F}_q[u_1, u_2, \ldots, u_l]/\left(u_i^2\right)$ which is a non-principal ideal ring Frobenius ring was examined. The ring has been shown to be isomorphic to a ring of polynomials over $\mathbb{F}_q$ and a subring of the ring of $2^l \times 2^l$ upper triangular matrices over $\mathbb{F}_q$. The latter isomorphism was then used to define a weight function on $R(q,l)$ called the $M_B$-weight some of which are egalitarian. Following the definition of the weight defined by Bachoc on $R(p,1)$, a Bachoc weight on $R(2,l)$ was defined. Conditions on the parameters $m$ and $l$ of the ring were determined in order for the Bachoc weight to be homogeneous. Lastly, a generating character on $R(q,l)$ was obtained in order to derive a homogeneous weight on the ring for any $q$ and $l$.

## Keywords

homogeneous weight, Lee weight, Bachoc weight, Frobenius ring, non-principal ideal ring

## 1. INTRODUCTION

Finite principal ideal rings have been studied extensively over the past few years but not much work is done over non-principal ideal rings. The ring $\mathbb{F}_q[u_1, u_2, ..., u_l]/\left(u_i^2\right), l > 2$ is not a principal ideal ring but is a Frobenius ring. Being a Frobenius ring, a homogeneous weight on the ring can be derived in terms of its generating character. Also, finite Frobenius rings are singled out to be the most appropriate rings for coding-theoretic purposes since over such rings, several important theorems on codes over finite fields such as the MacWilliams identities and the extension theorem find nice generalizations.This paper aims to enrich the study on non-principal ideal but Frobenius rings by examining the ring and modular properties of $\mathbb{F}_q[u_1, u_2, ..., u_l]/\left(u_i^2\right), l > 2$ and deriving weight functions on it.

The code-theoretic applications of the ring $R(2,2)$ was first examined by Yildiz and Karadeniz in 2010 [13]. Since $R(2,2)$ is not a principal ideal ring, the standard theory of generating matrices is not applicable for linear codes over $R(2,2)$. Instead, generating sets has been used to study such codes. Other studies on $R(q,2)$ followed soon after ([1],[5],[6],[9],[10],[12], [14]). Dougherty, Yildiz and Karadeniz extended their work over the ring $R(2,l)$ for an arbitrary integer $l$ by defining a homogeneous weight on the ring and deriving an isometry from $R(2,l)$ to a product of binary field elements under the homogeneous and Hamming weight, respectively. Other studies on $R(2,l)$ are done in [7] and [15].

This paper is organized as follows: a brief discussion on Frobenius rings, trace functions on Galois fields and weight functions on a commutative ring is given in Section 2, ring structure and modular properties of $R(q,l)$ in Section 3.1, and the derivation of weight functions on $R(q,l)$ some of which are egalitarian, homogeneous or neither in Section 3.2.

## 2. PRELIMINARIES AND DEFINITIONS

### 2.1 Finite Frobenius Rings

Let $\mathbb{T}$ denote the multiplicative group of unit complex numbers. A character of a finite ring $R$, written additively, is a group homomorphism $\chi : R \to \mathbb{T}$. The set of all characters of $R$ forms a group called the character group $\hat{R}$; the group operation is pointwise multiplication of characters. Moreover, $\hat{R}$ is a left *(resp. right)* $R$-module according to the relation ${}^r\chi(x) = \chi(rx)$ *resp.* $(\chi(x)^r = \chi(rx))$. The character $\chi$ is called a left *(resp. right)* generating character if

$$\phi : R \to \hat{R} \text{ where } r \mapsto {}^r\chi \text{ (resp. } r \mapsto \chi^r)$$

is an isomorphism of left *(resp., right)* $R$-modules.

Alternative definitions of a generating character and a finite Frobenius ring given by J. Wood in [11] will be used in this paper.

Theorem 2.1. (J.Wood, [11]). Let $R$ be a finite ring.

Then the following properties hold:

1. If $\chi$ is a character of $R$, then $\chi$ is a right generating character if and only if $\ker \chi$ does not contain any nonzero right ideal;

2. A character of a finite ring is a left generating character if and only if it is a right generating character; and

3. $R$ is Frobenius if and only if it has a generating character.

## 2.2 The Trace Function on $\mathbb{F}_{p^m}$

The trace function $tr$ is defined by $tr : \mathbb{F}_{p^m} \to \mathbb{F}_p$ where $tr(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{m-1}}$ for $\alpha \in \mathbb{F}_{p^m}$. The trace function on $\mathbb{F}_p$ projects an element of $\mathbb{F}_p$ onto itself, that is, $tr(\alpha) = \alpha$ for every $\alpha \in \mathbb{F}_p$. Listed below are some properties of the trace function that will be used in this work.

THEOREM 2.2. (R. Lidl and H. Niederreiter,[8]) The following statements hold for $\alpha, \beta \in \mathbb{F}_{p^m}$ and $c \in \mathbb{F}_p$.

(T1) $tr(\alpha + \beta) = tr(\alpha) + tr(\beta)$;

(T2) $tr(c \cdot \alpha) = c \cdot tr(\alpha)$;

(T3) $tr(\alpha^p) = tr(\alpha)$;

(T4) $tr$ is surjective and $\mathbb{F}_{p^m} / \ker tr \cong \mathbb{F}_p$; and

(T5) $tr$ takes on each value in $\mathbb{F}_p$ equally often, that is, there are $p^{m-1}$ elements of $\mathbb{F}_{p^m}$ mapped to the same element of $\mathbb{F}_p$.

## 2.3 Weight Functions in a Commutative Ring $R$

Let $\mathbb{R}$ be the set of real numbers. A mapping $w : R \to \mathbb{R}$ is called a weight if the following conditions are satisfied:

(W1) $w(x) = 0$ if and only if $x = 0$;

(W2) $w(x) \geq 0$ for all $x \in R$;

(W3) $w(x) = w(-x)$ for all $x \in R$; and

(W4) $w(x + y) \leq w(x) + w(y)$ for all $x, y \in R$.

A weight $w$ on a finite commutative ring $R$ is egalitarian if it satisfies condition (E1) below. If in addition, condition (E2) is satisfied, then $w$ is said to be homogeneous.

(E1) every nonzero ideal $(x)$ of $R$ has the same average weight, that is, there exists a nonnegative real number $\Gamma$ such that

$$\sum_{y \in (x)} w(y) = \Gamma \cdot |(x)|$$

for all $x \in R \setminus \{0\}$.

(E2) for all $x, y \in R$, $(x) = (y)$ implies that $w(x) = w(y)$, that is, associates in $R$ have the same weight; and

A homogeneous weight $w$ will be denoted by $w_{hom}$. Further, if in $w_{hom}, \Gamma = 1$ then the homogeneous weight is said to be normalized.

In [4], it was established that every finite Frobenius ring is equipped with a homogeneous weight and can be expressed in terms of its generating character.

THEOREM 2.3. (T. Honold, [4]) Let $R$ be a Frobenius ring with generating character $\chi$, then every homogeneous weight $w_{hom}$ on $R$ can be expressed in terms of $\chi$ as follows

$$w_{hom}(x) = \Gamma \left[ 1 - \frac{1}{|R^\times|} \sum_{y \in R^\times} \chi(xy) \right].$$

where $R^\times$ is the group of units of $R$.

# 3. RESULTS AND DISCUSSIONS

First we define some notations. Consider the set $S = \{1, 2, ..., l\}$. Define an order in the subsets $s_i$ of $S$ as follows: $s_1 = \{\}, s_2 = \{1\}, s_3 = \{2\}, s_4 = \{1, 2\}, s_5 = \{3\}, s_6 = \{1, 3\}, s_7 = \{2, 3\}, s_8 = \{1, 2, 3\}$. In general, $s_{2^i - j} = s_{2^{i-1} - j} \cup \{i\}$ where $i = 1, 2, ..., l$ and $j = 0, 1, 2, ..., 2^{i-1} - 1$. We know that there will be $2^l$ such subsets of $S$. Now, define $\mathbf{u}_{s_1} = 1$ and $\mathbf{u}_{s_m} = \prod_{i \in s_m} u_i$ whenever $m \neq 1$. To illustrate, let $i = 4$ and $j = 6$, then $\mathbf{u}_{10} = \mathbf{u}_2 \cup \{4\} = u_1 u_4$.

## 3.1 Properties of the Ring $R(q, l)$

Denote by $R(q, l)$ the set whose elements are written in the form $\sum_{m=1}^{2^l} a_m \mathbf{u}_{s_m}$ where $a_m \in \mathbb{F}_q$. For example,

$$R(q, 1) = \{a_1 + a_2 u_1 | a_i \in \mathbb{F}_q\} = \mathbb{F}_q + u_1 \mathbb{F}_q$$

while

$$\begin{aligned} R(q, 2) &= \{a_1 + a_2 u_1 + a_3 u_2 + a_4 u_1 u_2 | a_i \in \mathbb{F}_q\} \\ &= \mathbb{F}_q + u_1 \mathbb{F}_q + u_2 \mathbb{F}_q + u_1 u_2 \mathbb{F}_q. \end{aligned}$$

Define addition and multiplication on these sets as the addition and multiplication in the ring $\mathbb{F}_q[u_1, u_2, \ldots, u_l]$ except that $u_i^2 = 0$ for any $i$. Then $\langle R(q, l), +, \cdot \rangle$ is a commutative ring with unity 1, characteristic $p$ and cardinality $q^{2^l}$. Moreover, for every subsets $A, B$ of $S$, it is easy to see that

$$\mathbf{u}_A \mathbf{u}_B = \begin{cases} 0 & if \quad A \cap B \neq \phi \\ \mathbf{u}_{A \cup B} & if \quad A \cap B = \phi \end{cases}. \tag{1}$$

Also, we note here that every element of the ring $R(q, l)$ can be uniquely written in the form $x + y u_l$ where $x, y \in R(q, l - 1)$. Thus, $R(q, l)$ can be defined recursively by $R(q, l) = R(q, l - 1) + u_l R(q, l - 1)$. Lastly, denote by $a$ the sequence of coefficients $(a_1, a_2, \ldots, a_{2^l})$ of $\sum_{i=1}^{2^l} a_i \mathbf{u}_{s_i}$.

PROPOSITION 3.4. An element of $R(q, l)$ is a unit if and only if the coefficient of $\mathbf{u}_{s_1}$ is nonzero.

*Proof:* ($\Rightarrow$) Let $x = \sum_{m=1}^{2^l} a_m \mathbf{u}_{s_m}$ be a nonzero element of $R(q,l)$ with $\mathbf{u}_{s_1} = 0$. Now, $\mathbf{u}_{s_{2^l}} x = 0$ since $s_{2^l} \cap s_m \neq \phi$ for all $m$. Thus, $x$ is a zero divisor. ($\Leftarrow$) Let $x = \sum_{m=1}^{2^l} a_m \mathbf{u}_{s_m}$ be a zero divisor then there is a nonzero element $y = \sum_{n=1}^{2^l} b_n \mathbf{u}_{s_n} \in R(q,l)$ such that $xy = 0$. However, $xy = \sum_{m,n=1}^{2^l} a_m b_n \mathbf{u}_{s_m \cup s_n} = 0$ would imply that $a_m b_n = 0$ whenever $s_m \cap s_n = \phi$. In particular, $a_{s_1} b_n = 0$ for all $n$. Since $b \neq 0, a_{s_1} = 0$. ■

For a unit $x = \sum_{m=1}^{2^l} a_m \mathbf{u}_{s_m}$ in the ring $R(q,l)$, define $T_r = \{m_1, m_2, \ldots, m_r\}$ where $s_{m_1}, s_{m_2}, \ldots, s_{m_r}$ are pairwise disjoint, $\mathbf{a}_{T_r} = \prod_{i \in T_r} a_i$ and $\mathbf{s}_{T_r} = \bigcup_{i \in T_r} s_i$. Then the multiplicative inverse of $x$ is

$$a_1^{-1}\left(1 + \sum_{r=1}^{l} \mathbf{a}_{T_r} \mathbf{u}_{\mathbf{s}_{T_r}} \cdot (-1)^r \cdot \left(a_1^{-1}\right)^r \cdot r!\right).$$

For example in $R(4,3)$, the inverse of $\omega + u_1 + \omega^2 u_2 u_3$ is $\omega^2(1 - \omega^2 u_1 - \omega u_2 u_3 + 2u_1 u_2 u_3)$. While the inverse of $2 + 3u_1 + u_2 + 4u_3 + u_4$ in $R(5,4)$ is $3(1 - 4u_1 - 3u_2 - 2u_3 - 3u_4 + 4u_1u_2 + u_1u_3 + 4u_1u_4 + 2u_2u_3 + 3u_2u_4 + 2u_3u_4 - 4u_1u_2u_3 - 4u_1u_3u_4 - u_1u_2u_4 - 3u_2u_3u_4 + 3u_1u_2u_3u_4)$.

Proposition 3.5. *The ring $R(q,l)$ is a local ring with unique maximal ideal $\mathfrak{M} = \langle u_1, u_2, ..., u_l \rangle$. This ideal contains all zero divisors and has $q^{2^l - 1}$ elements. Also, the ring $R(q,l)$ has a unique minimal ideal $\mathfrak{m} = \langle \mathbf{u}_{s_{2^l}} \rangle = \langle u_1 u_2 \cdots u_l \rangle$ which has $q$ elements.*

*Proof:* All elements of $\mathfrak{M}$ are non-units. By Proposition 3.4, $|\mathfrak{M}| = q^{2^l - 1}$. All elements of $\mathfrak{m}$ are multiples of $\mathbf{u}_{s_{2^l}}$, that is, they are of the form $a\mathbf{u}_{s_{2^l}}$ where $a \in \mathbb{F}_q$. So, $|\mathfrak{m}| = q$. ■

Proposition 3.6. *$R(q,l)$ is a finite chain ring if and only if $l = 1$.*

*Proof:* If $l = 1$, then the maximal ideal coincides with the minimal ideal. Thus, the ideals are linearly ordered by set inclusion making $R(q,l)$ a finite chain ring. If $l \neq 1$, then the maximal ideal is not a principal ideal. Consequently, $R(q,l)$ is not a finite chain ring. ■

Proposition 3.7. *The ideal generated by $\mathbf{u}_s$ has $q^{2^{l-|s|}}$ elements.*

*Proof:* The ideal generated by $\mathbf{u}_s$ contains the elements of the form $\sum_{i=1}^{2^l} a_i \mathbf{u}_{s_i} \mathbf{u}_s$. By equation (1), we wish to count the number of subsets $s_i$ of $S$ with no intersection with $s$. These subsets are exactly the elements of the power set of $S \setminus s$ with has $q^{2^{l-|s|}}$ elements. ■

Proposition 3.8. *Let $A = \{k_j | j = 1, 2, \ldots, r\}$. Then $\langle u_{k_1}, u_{k_2}, \ldots, u_{k_r} \rangle^{\perp} = \langle \mathbf{u}_A \rangle$.*

*Proof:* $\langle \mathbf{u}_s \rangle$ contains elements of the form $\sum_{i=0}^{2^l} a_i \mathbf{u}_{s_i} \mathbf{u}_s$ while $\langle u_{k_1}, u_{k_2}, \ldots, u_{k_r} \rangle$ contains elements of the form $\sum_{i=0}^{2^l} a_i \mathbf{u}_{s_i} \mathbf{u}_{k_j}$ or any linear combination of these. By equation (1), the proposition follows. ■

Proposition 3.9. *The ring $R(q,l)$ is a vector space over $\mathbb{F}_q$ with dimension $2^l$ and a free $R(q,l-1)$-module with dimension 2.*

*Proof:* $\mathbb{F}_q$ and $R(q,l-1)$ are subrings of $R(q,l)$. Then $R(q,l)$ is an $\mathbb{F}_q$-module. In addition, there exists $1 \in \mathbb{F}_q$ such that $1 \cdot x = 1 \cdot \sum_{m=1}^{2^l} a_m \mathbf{u}_{s_m} = \sum_{m=1}^{2^l} a_m \mathbf{u}_{s_m} = x$ for all $x \in R(q,l)$. Thus, $R(q,l)$ is a unitary $\mathbb{F}_q$-module. Since $\mathbb{F}_q$ is a field, $R(q,l)$ is a vector space over $\mathbb{F}_q$. Clearly, the set $\left\{\mathbf{u}_{s_m} | m = 1, 2, 3, \ldots, 2^l\right\}$ is a basis for $R(q,l)$ as an $\mathbb{F}_q$ vector space while $\{1, u_l\}$ is a basis for $R(q,l)$ as an $R(q,l-1)$-module. ■

Proposition 3.10. *$B$ is a basis for $R(q,l)$ as an $\mathbb{F}_q$-vector space if and only if the columns of $\left(\mathbf{u}_{s_1}, \mathbf{u}_{s_2}, \ldots, \mathbf{u}_{s_{2^l}}\right) M$, where $M$ is a $2^l \times 2^l$ invertible matrix over $\mathbb{F}_q$, are exactly the elements of $B$.*

*Proof:* Since element $x \in R(q,l)$ is uniquely represented by a linear combination of the $\mathbf{u}_i's$, $x = \left(\mathbf{u}_{s_1}, \mathbf{u}_{s_2}, \ldots, \mathbf{u}_{s_{2^l}}\right) m_1$ where $m_1$ is the $2^l \times 1$ matrix coefficient of $x$. Since in a basis the elements must be linearly independent, then its coefficient matrix must be invertible. ■

Denote by $M_B$ the matrix $M$ associated with the basis $B$ for $R(q,l-1)$ as an $\mathbb{F}_q$-vector space.

Corollary 3.11. *The matrices*

$$\begin{pmatrix} M_B & 0 \\ -M_B & M_B \end{pmatrix} \text{ and } \begin{pmatrix} M_B & 0 \\ 0 & M_B \end{pmatrix}$$

*are associated to some basis of $R(q,l+1)$.*

Now, we look at two rings to which $R(q,l)$ is isomorphic to. First, we look into the quotient ring $\mathbb{F}_q[u_1, u_2, ..., u_l]/\langle u_i^2 \rangle$ then into a subring of triangular matrices over $\mathbb{F}_q$. The isomorphism between $R(q,l)$ can be shown with the map that sends $\sum_{m=1}^{2^l} a_m \mathbf{u}_{s_m}$ to $\sum_{m=1}^{2^l} a_m \mathbf{u}_{s_m} + (u_1^2, u_2^2, \ldots, u_l^2)$.

Let $M_1(a_1)$ denote the $2 \times 2$ matrix of the form

$$\begin{pmatrix} a_1 & a_2 \\ 0 & a_1 \end{pmatrix}$$

over $\mathbb{F}_q$, $M_2(a_1)$ denote the $4 \times 4$ matrix of the form

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ 0 & a_1 & 0 & a_3 \\ 0 & 0 & a_1 & a_2 \\ 0 & 0 & 0 & a_1 \end{pmatrix}$$

over $\mathbb{F}_q$, and $M_3(a_1)$ denote an $8 \times 8$ matrix of the form

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 \\ 0 & a_1 & 0 & a_3 & 0 & a_5 & 0 & a_7 \\ 0 & 0 & a_1 & a_2 & 0 & 0 & a_5 & a_6 \\ 0 & 0 & 0 & a_1 & 0 & 0 & 0 & a_5 \\ 0 & 0 & 0 & 0 & a_1 & a_2 & a_3 & a_4 \\ 0 & 0 & 0 & 0 & 0 & a_1 & 0 & a_3 \\ 0 & 0 & 0 & 0 & 0 & 0 & a_1 & a_2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & a_1 \end{pmatrix}.$$

Notice that $M_3(a_1)$ can be written in the form

$$\begin{pmatrix} M_2(a_1) & M_2(a_5) \\ 0 & M_2(a_1) \end{pmatrix}.$$

In general, define $M_l(a_1)$ as the $2^l \times 2^l$ matrix of the form

$$\begin{pmatrix} M_{l-1}(a_1) & M_{l-1}(a_{2^{l-1}+1}) \\ 0 & M_{l-1}(a_1) \end{pmatrix}. \tag{2}$$

PROPOSITION 3.12. The ring of all matrices over $\mathbb{F}_q$ of the form described in (2) is a commutative subring of the ring of all $2^l \times 2^l$ matrices over $\mathbb{F}_q$.

*Proof:* Let $\mathcal{M}_l$ be the collection of all matrices $M_1(a_1)$ described in (2). Clearly, $\mathcal{M}_l$ is a nonempty subset of the ring of all $2^l \times 2^l$ matrices over $\mathbb{F}_q$.

(i) $\mathcal{M}_l$ is closed under matrix subtraction since

$$\begin{pmatrix} M_{l-1}(a_1) & M_{l-1}(a_{2^{l-1}+1}) \\ 0 & M_{l-1}(a_1) \end{pmatrix} - \begin{pmatrix} M_{l-1}(b_1) & M_{l-1}(b_{2^{l-1}+1}) \\ 0 & M_{l-1}(b_1) \end{pmatrix} = \begin{pmatrix} M_{l-1}(a_1 - b_1) & M_{l-1}(a_{2^{l-1}+1} - b_{2^{l-1}+1}) \\ 0 & M_{l-1}(a_1 - b_1) \end{pmatrix} \in M_l.$$

(ii) Next, we show that $\mathcal{M}_l$ is closed under matrix multiplication by induction on $l$.

$$M_1(a_1) \cdot M_1(b_1) = \begin{pmatrix} a_1 b_1 & a_1 b_2 + a_2 b_1 \\ 0 & a_1 b_1 \end{pmatrix} \in M_1.$$

Suppose for some arbitrary $1 < i < l$, $\mathcal{M}_1, \mathcal{M}_2, ..., \mathcal{M}_{i-1}$ are closed under multiplication. Now

$$M_i(a_1) \cdot M_i(b_1) = \begin{pmatrix} M_{i-1}(a_1) & M_{i-1}(a_{2^{i-1}+1}) \\ 0 & M_{i-1}(a_1) \end{pmatrix} \cdot \begin{pmatrix} M_{i-1}(b_1) & M_{i-1}(b_{2^{i-1}+1}) \\ 0 & M_{i-1}(b_1) \end{pmatrix} = \begin{pmatrix} M_{i-1}(a_1) M_{i-1}(b_1) & A \\ 0 & M_{i-1}(a_1) M_{i-1}(b_1) \end{pmatrix}$$

where

$$A = M_{i-1}(a_1) M_{i-1}(b_{2^{i-1}+1}) + M_{i-1}(a_{2^{i-1}+1}) M_{i-1}(b_1).$$

So, $\mathcal{M}_i$ is also closed under matrix multiplication. Specifically, we can conclude that $\mathcal{M}_l$ is closed under matrix multiplication.

(iii) Lastly, multiplication is commutative in $\mathcal{M}_l$.

$$M_1(a_1) \cdot M_1(b_1) = \begin{pmatrix} a_1 b_1 & a_1 b_2 + a_2 b_1 \\ 0 & a_1 b_1 \end{pmatrix} = \begin{pmatrix} b_1 a_1 & b_2 a_1 + b_1 a_2 \\ 0 & b_1 a_1 \end{pmatrix} = M_1(b_1) \cdot M_1(a_1).$$

Suppose for some arbitrary $1 < i < l$, matrix multiplication is commutative on $\mathcal{M}_1, \mathcal{M}_2, ..., \mathcal{M}_{i-1}$. Now

$$M_i(a_1) \cdot M_i(b_1) = \begin{pmatrix} M_{i-1}(a_1) M_{i-1}(b_1) & A \\ 0 & M_{i-1}(a_1) M_{i-1}(b_1) \end{pmatrix}.$$

But

$$A = M_{i-1}(b_1) M_{i-1}(a_{2^{i-1}+1}) + M_{i-1}(b_{2^{i-1}+1}) M_{i-1}(a_1) = M_{i-1}(b_1) M_{i-1}(a_{2^{i-1}+1}) + M_{i-1}(b_{2^{i-1}+1}) M_{i-1}(a_1).$$

Thus,

$$M_i(a_1) \cdot M_i(b_1) = \begin{pmatrix} M_{i-1}(a_1) M_{i-1}(b_1) & A \\ 0 & M_{i-1}(a_1) M_{i-1}(b_1) \end{pmatrix} = M_i(b_1) \cdot M_i(a_1).$$

By mathematical induction, $\mathcal{M}_l$ is commutative.

Therefore, $\mathcal{M}_l$ is a commutative subring of the ring of all $2^l \times 2^l$ matrices over $\mathbb{F}_q$.

PROPOSITION 3.13. The ring $R(q,l)$ is isomorphic to the subring $\mathcal{M}_l$ described in Proposition 3.12.

*Proof:* Define $\phi : R(q,l) \to \mathcal{M}_l$ where $x = \sum_{m=1}^{2^l} a_m \mathbf{u}_{s_m} \mapsto M_l(a_1)$. We shall also denote this mapping by $\mathbf{M}_l(x)$.

(i) $\phi$ is a group homomorphism since

$$\phi\left(\sum_{m=1}^{2^l} a_m \mathbf{u}_{s_m} + \sum_{m=1}^{2^l} b_m \mathbf{u}_{s_m}\right) = \phi\left(\sum_{m=1}^{2^l} (a_m + b_m) \mathbf{u}_{s_m}\right) = \begin{pmatrix} M_{l-1}(a_1 + b_1) & M_{l-1}(a_{2^{l-1}+1} + b_{2^{l-1}+1}) \\ 0 & M_{l-1}(a_1 + b_1) \end{pmatrix} = \begin{pmatrix} M_{l-1}(a_1) & M_{l-1}(a_{2^{l-1}+1}) \\ 0 & M_{l-1}(a_1) \end{pmatrix} +$$

$$\begin{pmatrix} M_{l-1}(b_1) & M_{l-1}(b_{2^{l-1}+1}) \\ 0 & M_{l-1}(b_1) \end{pmatrix}$$
$$= \phi\left(\sum_{m=1}^{2^l} a_m \mathbf{u}_{s_m}\right) + \phi\left(\sum_{m=1}^{2^l} b_m \mathbf{u}_{s_m}\right).$$

(ii) $\phi$ is a ring homomorphism since
$$\phi\left(\sum_{m=1}^{2^l} a_m \mathbf{u}_{s_m} \cdot \sum_{n=1}^{2^l} b_n \mathbf{u}_{s_m}\right)$$
$$= \phi\left(\sum_{m,n=1}^{2^l} a_m b_n \mathbf{u}_{s_m \cup s_n}\right)$$
$$= \begin{pmatrix} M_{i-1}(a_1)M_{i-1}(b_1) & A \\ 0 & B \end{pmatrix}$$
$$= \begin{pmatrix} M_{i-1}(a_1) & M_{i-1}(a_{2^{i-1}+1}) \\ 0 & M_{i-1}(a_1) \end{pmatrix} \cdot$$
$$\begin{pmatrix} M_{i-1}(b_1) & M_{i-1}(b_{2^{i-1}+1}) \\ 0 & M_{i-1}(b_1) \end{pmatrix}$$
$$= M_i(a_1)\cdot M_i(b_1) = \phi\left(\sum_{m=1}^{2^l} a_m \mathbf{u}_{s_m}\right) \cdot \phi\left(\sum_{n=1}^{2^l} b_n \mathbf{u}_{s_m}\right)$$
where
$A = M_{i-1}(a_1)M_{i-1}(b_{2^{i-1}+1}) + M_{i-1}(a_{2^{i-1}+1})M_{i-1}(b_1)$
and $B = M_{i-1}(a_1)M_{i-1}(b_1)$.

iii.) $\phi$ is a monomorphism since
$$\ker\phi = \left\{ \sum_{m=1}^{2^l} a_m \mathbf{u}_{s_m} \;\middle|\; \phi\left(\sum_{m=1}^{2^l} a_m \mathbf{u}_{s_m}\right) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$$
contains only 0.

iv.) $\phi$ is clearly an epimorphism.

Thus, $\phi$ is an isomorphism. ∎

## 3.2 Weight Functions on the Ring $R(q, l)$

### 3.2.1 $M_B$-weight

Now, we will use the matrix $M$ associated with basis $B$ of $R(q, l)$ as a vector space over $\mathbb{F}_q$ to define a weight function on $R(q, l)$.

THEOREM 3.14. Let $B$ be a basis for $R(q, l)$ as an $\mathbb{F}_q$-vector space. The mapping $\psi : R(q, l) \to \mathbb{F}_q^{2^l}$ where $\sum_{m=1}^{2^l} a_m \mathbf{u}_{s_i} \mapsto aM_B$ is an $\mathbb{F}_q$-module isomorphism.

*Proof:* Let $x = \sum_{i=1}^{2^l} a_i \mathbf{u}_{s_i}$ and $y = \sum_{i=1}^{2^l} b_i \mathbf{u}_{s_i}$ and $r \in \mathbb{F}_q$.

(i) $\psi(x+y) = \sum_{i=1}^{2^l} (a_i + b_i)\mathbf{u}_{s_i} = (a+b)M_B = aM_B + bM_B = \psi(x) + \psi(y)$.

(ii) $\psi(rx) = \psi\left(\sum_{i=1}^{2^l} ra_i \mathbf{u}_{s_i}\right) = raM_B = r\psi(x)$.

(iii) $\ker\psi = \left\{ x = \sum_{i=1}^{2^l} a_i \mathbf{u}_{s_i} \;\middle|\; \psi(x) = 0 \right\}$
$= \left\{ x = \sum_{i=1}^{2^l} a_i \mathbf{u}_{s_i} \;\middle|\; aM_B = 0 \right\} = \{0\}$ since the rows of $M_B$ are linearly independent.

(iv) Let $(a_1, a_2, \ldots, a_{2^l}) \in \mathbb{F}_q^{2^l}$. Take $x$ as the element of $R(q, l)$ with coefficient sequence $(a_1, a_2, \ldots, a_{2^l})\, M_B^{-1}$. Then $\psi(x) = (a_1, a_2, \ldots, a_{2^l})$, that is, $Im\psi = \mathbb{F}_q^{2^l}$.

Thus, $\psi$ is an $\mathbb{F}$-module isomorphism. ∎

Let $x = \sum_{i=1}^{2^l} a_i \mathbf{u}_{s_i}$. Define the $M_B$-weight of $x$, as the Hamming weight of $aM_B$ and is denoted by $w_{M_B}(x)$. In particular, if $L_1 = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$ and $L_l = \begin{pmatrix} L_{l-1} & 0 \\ -L_{l-1} & L_{l-1} \end{pmatrix}$, the $M_{L_l}$-weight of $x$ is called the Lee weight of $x$ and is denoted by $w_L(x)$. This definition is consistent with the Lee weight on $R(2, l)$ defined in [3]. It is easy to show that the Lee weight on $R(2, 2)$ is egalitarian but not homogeneous.

PROPOSITION 3.15. There are $\binom{2^l}{i}$ elements of $R(q, l)$ of $M_B$-weight $i$. In particular, only $\mathbf{u}_{2^l}$ has Lee weight $2^l$ and only units have odd Lee weights in the ring $R(2, l)$.

*Proof:* In $\binom{n}{i}$, let $i$ be the number of nonzero entries in an $n$-tuple. Recall that $\binom{n}{0} + \binom{n}{2} + \cdots + \binom{n}{n} = \binom{n}{1} + \binom{n}{3} + \cdots + \binom{n}{n-1}$ for any positive even integer $n$. So, half of the elements of $R(q, l)$ are of odd weight. It suffices that if $x$ is a unit then $w_{L_l}(x)$ is odd. The proof is by induction on $l$. In $R(2, 1)$, the units have Lee weight 1. In $R(2, 2)$, the units have Lee weights of either 1 or 3. Suppose now that for some $k \in \mathbb{N}$, the units of the ring $R(2, l)$ have odd lengths. In $R(2, l+1)$, units are of the form $x + yu_l$ for some unit $x = \sum_{i=1}^{2^l} a_i \mathbf{u}_{s_i}$ and $y \sum_{i=1}^{2^l} b_i \mathbf{u}_{s_i}$ in $R(2, l)$. Denote by $m$ the Lee weight of $x$ in $R(2, l)$, $n$ the Lee weigt on $y$ in $R(2, l)$, $t_1$ the number of $i$ such that $a_i = b_i = 1$, $t_2$ the number of $i$ such that $a_i = 1$ but $b_i = 0$ and $t_3$ the number of $i$ such that $a_i = 0$ but $b_i = 1$. Then $w_{L_{l+1}}(x + yu_l) = t_2 + t_3 + n$ where $t_1 + t_2 = m, t_1 + t_3 = n$.

If $y$ is not a unit, then $n$ is even and $t_2, t_3$ are not both even nor both odd. In either case, $m + n$ is odd. If $y$ is a unit, then $n$ is odd and either $t_2, t_3$ are both even or both odd. In either case, $m + n$ is odd. Thus, units in $R(2, k+1)$ have odd Lee weights. ∎

### 3.2.2 Bachoc weight

C. Bachoc defined in [2] a weight function on certain classes of rings $R$ as

$$w_B(x) = \begin{cases} p & if \quad x \in R \setminus \left(R^\times \cup \{0\}\right) \\ 1 & if \quad x \in R^\times \\ 0 & if \quad x = 0 \end{cases}.$$

Now, we extend the Bachoc weight on $R(2,1)$ to a weight function on $R(2^m, l)$ and show that it is indeed a weight function on $R(2^m, l)$.

THEOREM 3.16. The function defined by

$$w_B(x) = \begin{cases} 2 & if \quad x \text{ is a zero divisor} \\ 1 & if \quad x \text{ is a unit} \\ 0 & if \quad x = 0 \end{cases}$$

is a weight function on $R(2^m, l)$.

*Proof:* It is obvious from the definition of $w_B$ that $w_B(x) = 0$ if and only if $x = 0$ and that $w_B(x) \geq 0$. (W3) is also satisfied since in $R(2^m, l)$, the additive inverse of a zero divisor is also a zero divisor and the additive inverse of a unit is also a unit. For (W4), we will look at all possible sums of two elements in $R(2^m, l)$. The sum of two zero divisors is zero, a zero divisor or a unit. Whichever is the case, (W4) holds since $w_B(x) + w_B(y) = 4 > 1 > 0$. The sum of two units is zero, a zero divisor or a unit. Whichever is the case, (W4) holds since $w_B(x) + w_B(y) = 2 \geq 2 > 1 > 0$. Lastly, the sum of a unit and a zero divisor is a unit and $w_B(x) + w_B(y) = 3 > 1$. Thus, $w_B$ is a weight function on $R(2^m, l)$. ■

Clearly, the Bachoc weight on $R(2^m, l)$ satisfies condition (E2). However, it does not satisfy (E1) for any $m, l > 1$. The average weight in the minimal ideal is $2 - \dfrac{2}{2^m}$ while the average weight in the ideal $(u_1)$ is $2 - \dfrac{2}{(2^m)^{2^l - 1}}$. Thus, the Bachoc weight is egalitarian only if $l = 1$. Now, the average weight in $R(2^m, 1)$ is $\dfrac{3}{2} - \dfrac{2}{2^{2m}}$. So, $m$ must be 1 as well. Thus, the Bachoc weight is egalitarian only if $m = l = 1$. Consequently, it is homogeneous if and only if $m = l = 1$.

### 3.2.3 Homogeneous Weight

To derive a homogeneous weight on $R(q, l)$, we first develop a generating character on the ring.

PROPOSITION 3.17. The map $\chi$ from $R(q, l)$ to $\mathbb{T}$ where

$$\sum_{m=1}^{2^l} a_m \mathbf{u}_{s_m} \mapsto e^{\frac{2\pi i}{p} tr(a_{2^l})}$$

is a generating character of $R(q, l)$.

*Proof:*

(i) $\chi$ is a group homomorphism since

$$\begin{aligned} &\chi\left(\sum_{m=1}^{2^l} a_m \mathbf{u}_{s_m} + \sum_{m=1}^{2^l} b_m \mathbf{u}_{s_m}\right) \\ &= \chi\left(\sum_{m=1}^{2^l} (a_m + b_m) \mathbf{u}_{s_m}\right) \\ &= e^{\frac{2\pi i}{p} tr(a_{2^l} + b_{2^l})} = e^{\frac{2\pi i}{p} tr(a_{2^l})} \cdot e^{\frac{2\pi i}{p} tr(b_{2^l})} \\ &= \phi\left(\sum_{m=1}^{2^l} a_m \mathbf{u}_{s_m}\right) \cdot \phi\left(\sum_{m=1}^{2^l} b_m \mathbf{u}_{s_m}\right). \end{aligned}$$

(ii) $$\begin{aligned} \ker \chi &= \left\{ \sum_{m=1}^{2^l} a_m \mathbf{u}_{s_m} \,\middle|\, e^{\frac{2\pi i}{p} tr(a_{2^l})} = 1 \right\} \\ &= \left\{ \sum_{m=1}^{2^l} a_m \mathbf{u}_{s_m} \,\middle|\, tr(a_{2^l}) = 0 \right\}. \end{aligned}$$

Recall that $R(q, l)$ has a unique minimal ideal $\mathfrak{m}$ which contains the elements of the form $c\mathbf{u}_{2^l}, c \in \mathbb{F}_q$. With $q = p^m$, there are only $p^{m-1}$ elements $c$ of $\mathbb{F}_q$ such that $tr(c) = 0$. Since $|\mathfrak{m}| = p^m > p^{m-1} = |\ker \chi|$, $\ker \chi$ can not contain any nonzero ideal of $R(q, l)$.

Thus, $\chi$ is a generating character of $R(q, l)$. ■

With the existence of a generating character, $R(q, l)$ is a Frobenius ring. Moreover, a homogeneous weight on $R(q, l)$ can now be derived from its generating character.

THEOREM 3.18. The homogeneous weight on $R(q, l)$ is given by

$$w_{hom}(x) = \begin{cases} \Gamma & if \quad x \in R(q, l) \setminus \mathfrak{m} \\ \frac{q}{q-1}\Gamma & if \quad x \in \mathfrak{m} \setminus \{0\} \\ 0 & if \quad x = 0 \end{cases}.$$

*Proof:* Denote by $R^\times$ the set of all units in $R(q, l)$. By Theorem 2.5, the homogeneous weight of $x \in R(q, l)$ is given by

$$w_{hom}(x) = \Gamma\left[1 - \frac{1}{|R^\times|} \sum_{y \in R^\times} \chi(xy)\right].$$

By Proposition 3.4, $|R^\times| = (q-1)q^{2^l - 1}$. Now, we consider the multiset $M = \{xy | y \in R^\times\}$ for each $x \in R(q, l)$.

Case 1. Suppose $x = 0$. Then $\sum_{y \in R^\times} \chi(0) = \sum_{n=1}^{|R^\times|} e^{\frac{2\pi i}{p} tr(0)} = |R^\times|$.

Case 2. Suppose $x \in R^\times$. Then $xy \in R^\times$ and in the multiset $M$, every $y \in R^\times$ would appear exactly once. Moreover, there are $(q-1)q^{2^l - 2}$ of them with the same coefficient $a$ of $\mathbf{u}_{s_{2^l}}$ for every $a \in \mathbb{F}_q$. But $p^{m-1}$ elements of $\mathbb{F}_q$ have the same trace $j, \forall j = 0, 1, 2, \ldots, p-1$. Thus,

$$\sum_{y \in R^\times} \chi(xy) = \sum_{y \in R^\times} \chi(y) = (q-1)q^{2^l - 2} p^{m-1} \sum_{j \in \mathbb{F}_p} e^{\frac{2\pi i}{p} j} = 0.$$

Case 3. Suppose $x \in \mathfrak{m} \setminus \{0\}$. Then $x = a\mathbf{u}_{2^l}, a \in \mathbb{F}_q \setminus \{0\}$ and in the multiset $M$, every $x \in \mathfrak{m} \setminus \{0\}$ would appear $\frac{|R^\times|}{q-1}$ number of times. Also, of the $q-1$ elements of $\mathfrak{m} \setminus \{0\}$, $p^{m-1}$ will have trace $j, \forall j = 1, 2, \ldots, p-1$ while $p^{m-1} - 1$ will have trace 0 (since $x \neq 0$). Thus,

$$\sum_{y \in R^\times} \chi(xy) = \frac{|R^\times|}{q-1} \left[ p^{m-1} \sum_{j \in \mathbb{F}_q \setminus \{0\}} e^{\frac{2\pi i}{p} j} + (p^{m-1} - 1)e^0 \right]$$

which is equal to $\frac{|R^\times|}{1-q}$

Case 4. Suppose $x \in \mathfrak{M} \setminus \mathfrak{m}$. Then $xy \in \mathfrak{M} \setminus \mathfrak{m}$ and in the multiset $M$, every element $x \in \mathfrak{M} \setminus \mathfrak{m}$ would appear $\frac{|R^\times|}{q^{2^l-1}-q}$ number of times. Of the $q^{2^l-1} - q$ elements of $\mathfrak{M} \setminus \mathfrak{m}$, $q^{2^l-2} - 1$ will have the same coefficient $a$ of $\mathbf{u}_{s_{2^l}}$ for each $a \in \mathbb{F}_q$ and $p^{m-1}$ of these will have the same trace $j, \forall j = 0, 1, 2, \ldots, p-1$. Thus,

$$\sum_{y \in R^\times} \chi(xy) = \frac{|R^\times|}{q^{2^l-1} - q} (q^{2^l-2} - 1) p^{m-1} \sum_{j \in \mathbb{F}_q} e^{\frac{2i\pi}{p} j} = 0.$$

■

## 4. ACKNOWLEDGEMENT

The first author was supported by UPLB-OVCRE Basic Research Grant Program. Also, the authors would like to thank the evaluators for their valuable comments for the improvement of the paper.

## 5. REFERENCES

[1] N. Aydin, S. Karadeniz and B. Yildiz. Some new quasi-cyclic codes from codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. *Applicable Algebra in Engineering, Communication and Computing*, 5: 205 219, 2011.

[2] C. Bachoc. Application of coding theory to the construction of modular lattices. *J. Combin. Theory*, 78:92–119, 1997.

[3] S. Dougherty, B. Yildiz and S. Karadeniz. Codes over $R_k$, Gray maps and their images. *Finite Fields and Their Applications*, 17:205-219, 2011.

[4] T. Honold. A characterization of finite Frobenius rings. *Arch. Math (Basel)*, 76:406–415, 2001.

[5] S. Karadeniz and B. Yildiz. $(1+v)-$ Constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. *Journal of the Franklin Institute*, 348: 2652 2632, 2011.

[6] S. Karadeniz and B. Yildiz. Double-circulant and bordered-double-circulant construction for self-dual codes over $R_2$. *Advances in Mathematics of Communication*, 6 (2): 193 202, 2012.

[7] S. Karadeniz and B. Yildiz. New extremal binary self-dual codes of length 66 as extensions of self-dual codes over $R_2$. *Journal of the Franklin Institute*, 350 (8): 1963 1973, 2013.

[8] R. Lidl and H. Niederreiter. Finite fields. Cambridge University Press, New York, 1997.

[9] J. Palacio and V. Sison. Images of linear block codes over $F_q + uF_q + vF_q + uvF_q$. *Open Journal of Applied Sciences*, 3 (1B1): 27 31, 2013.

[10] X. Xu and X. Liu. On the structure of cyclic codes over $F_q + uF_q + vF_q + uvF_q$. *Wuhan University Journal of Natural Sciences*, 16: 457 460, 2011.

[11] J. Wood. Duality for modules over finite rings and applications to coding theory. *Amer. J. Math*, 121: 555-575, 1999.

[12] T. Yao, M. Shi and P. Solé. Skew cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$. *preprint*, April 2015.

[13] B. Yildiz and S. Karadeniz. Linear codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. *Designs, Codes and Cryptography*, 54: 61 81, 2010.

[14] B. Yildiz and I. Karadeniz. Self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. *Journal of the Franklin Institute*, 347: 1888 1894, 2010.

[15] B. Yildiz and I. Kelebek. The homogeneous weight for $R_k$, related Gray map and new binary quasicyclic codes. *preprint*, April 2015.