Homogeneous Weight and Scaled Isometry on $\mathbb{F}_{p^2}$- Linear Map

Dixie F. Falcunit, Jr., Virgilio P. Sison

Institute of Mathematical Sciences and Physics
University of the Philippines, Los Baños
College, Laguna 4031, Philippines

dixiefalcunitjr@ymail.com, vpsison@uplb.edu.ph

ABSTRACT

Let $\mathbb{F}_p$ denote the finite field with p elements where p is prime. We derive the homogeneous weight on the Frobenius matrix ring $M_2(\mathbb{F}_p)$ in terms of its minimal left ideals and idempotent elements. A non-commutative ring, denoted by $\mathcal{F}_{p^2} + v\mathcal{F}_{p^2}$, where v is an involution in $M_2(\mathbb{F}_p)$, is constructed. It is shown that $\mathcal{F}_{p^2} + v\mathcal{F}_{p^2}$ is isomorphic to $M_2(\mathbb{F}_p)$ and is a left $\mathbb{F}_{p^2}$-vector space. The elements of $\mathcal{F}_{p^2}$ are derived from those of $M_2(\mathbb{F}_p)$ where $\mathcal{F}_{p^2} \cong \mathbb{F}_{p^2}$. The unital embedding uses a characterization of $\mathbb{F}_p$ with respect to an irreducible polynomial $f(x) = x^2 + x + (p-1)$. As a result, our study of $M_2(\mathbb{F}_p)$ is restricted to the case where $p \equiv 2$ or $3 \bmod 5$. A scaled isometry from $(M_2(\mathbb{F}_p), w_{\mathtt{nhom}})$ into $(\mathcal{F}_{p^2}^m, w'_{\mathtt{nhom}})$, where **nhom** is the normalized homogeneous weight, is derived. This gives a construction of (m, p^2)-additive codes over $\mathcal{F}_{p^2}$ with minimum Hamming distance $m = |GL(2,p)|$.

Keywords

Frobenius ring, homogeneous weight, generalized Frobenius extension, scaled isometry, group codes, additive codes, matrix ring

1. INTRODUCTION

Since the late 40's of the last century, coding theorists confined themselves to finite fields as code alphabets. In 1994 the Best Paper awarded by the IEEE Information Theory Society used the integer ring $\mathbb{Z}_4$ in unlocking the twenty-year old riddle in coding theory, the formal duality of Kerdock and Preparata codes, using the so-called Gray isometry [7]. Since then numerous papers on codes over rings have been published. Many of these papers focused on *finite Frobenius rings* which are the most appropriate rings for coding theory since the two classical theorems namely the extension theorem and the MacWilliams identities generalize neatly in the case of finite Frobenius rings.

In this study we restrict ourselves to a small class of finite Frobenius rings, the matrix ring over a finite field. In particular, we consider here the matrix ring $M_2(\mathbb{F}_p)$. Until now very few publications on codes over non-commutative rings have been seen. It was only in 2012 that the theory of cyclic codes over $M_2(\mathbb{F}_2)$ was derived [1]. The idea for the construction of cyclic codes over $M_2(\mathbb{F}_2)$ came from [2] where an isometric map from $M_2(\mathbb{F}_2)$ onto $\mathbb{F}_4^2$ was defined using the Bachoc weight and the Hamming weight. It seems that having an isometry over the ring under study can lead us to a possible code construction. In this paper, we derive the homogeneous weight on $M_2(\mathbb{F}_p)$ using the homogeneous weight formula introduced by T. Honold for arbitrary finite Frobenius rings. The connection between the minimal left ideals and the idempotent elements of $M_2(\mathbb{F}_p)$ is used to generalize the homogeneous weight of the said matrix ring. We also employ the unital embedding introduced by Greferath and Schmidt to construct a non-commutative ring that is isomorphic to $M_2(\mathbb{F}_p)$ and is a left $\mathbb{F}_{p^2}$-vector space. This ring is denoted by $\mathcal{F}_{p^2} + v\mathcal{F}_{p^2}$ where v is an involution in $M_2(\mathbb{F}_p)$ and the elements of $\mathcal{F}_{p^2}$ are derived from those of $M_2(\mathbb{F}_p)$ such that $\mathcal{F}_{p^2} \cong \mathbb{F}_{p^2}$. The unital embedding comes from a characterization of the prime field $\mathbb{F}_p$ in terms of an irreducible polynomial $f(x) = x^2 + x + (p-1)$. This polynomial restricts our study to the matrix ring $M_2(\mathbb{F}_p)$ where $p \equiv 2$ or $3 \bmod 5$. As a consequence, scaled isometry from $(M_2(\mathbb{F}_p), w_{\mathtt{nhom}})$ into $(\mathcal{F}_{p^2}^m, w'_{\mathtt{nhom}})$, where **nhom** is the normalized homogeneous weight, is derived. This gives a construction of (m, p^2) - additive codes over $\mathcal{F}_{P^2}$ with minimum Hamming distance $d_{\mathtt{Ham}} = m = |GL(2,p)|$, where $GL(2,p)$ is the set of all invertible matrices of $M_2(\mathbb{F}_p)$.

2. HOMOGENEOUS WEIGHTS

Let S be a finite ring. A weight function $w\colon S \longrightarrow \mathbb{R}$ is called a *left homogeneous*, if $w(0) = 0$ and the following hold:

(H1) If $Sx = Sy$ for $x, y \in S$, then $w(x) = w(y)$.

(H2) There exists $\Gamma > 0$ such that for every nonzero $x \in S$

$$\sum_{y \in Sx} w(y) = \Gamma |Sx|.$$

An analogous definition for a right homogeneous weight holds, and we say that w is *homogeneous* if it is both left homogeneous and right homogeneous. The number Γ is called

the *average value* of w. When $\Gamma = 1$ then w is said to be *normalized*.

It is well known that the normalized homogeneous weight on the finite field $\mathbb{F}_q$, $q = p^k$ $k \in \mathbb{N}$ is given by

$$w_{\text{nhom}}(x) = \begin{cases} 0 & \text{if } x = 0 \\ \dfrac{q}{q-1} & \text{if } x \neq 0. \end{cases}$$

This idea comes from the generalization of the homogeneous weight on a finite chain ring in [6]. But our goal is to develop a generalization of the homogeneous weight on a matrix ring over a finite field, which is not a finite chain ring but is a finite (non-commutative) Frobenius ring.

In the case of finite Frobenius rings, Honold [8] observed that every homogeneous weight on these rings with generating character χ is of the following form:

$$w : S \longrightarrow \mathbb{R}, \quad x \mapsto \Gamma\left[1 - \frac{1}{|S^\times|} \sum_{u \in S^\times} \chi(ux)\right]$$

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

Note that every finite Frobenius ring has a generating character [10]. The generating character of $M_n(\mathbb{F}_q)$ is given by

$$\chi(A) = exp\left\{\frac{2\pi i tr(Tr(A))}{p}\right\}$$

where tr is the trace map on $\mathbb{F}_{p^k}$ to $\mathbb{F}_p$, i.e. $tr(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{k-1}}$, $\alpha \in \mathbb{F}_{p^k}$ and Tr is the classical trace of the matrix $A \in M_n(\mathbb{F}_q)$. The homogeneous weight on $M_n(\mathbb{F}_q)$ is given by

$$w : M_n(\mathbb{F}_q) \longrightarrow \mathbb{R}, \quad A \mapsto \Gamma\left[1 - \frac{1}{|GL(n,q)|} \sum_{u \in GL(n,q)} \chi(uA)\right]$$

where $GL(n,q)$ is the group of all invertible matrices of $M_n(\mathbb{F}_q)$ and $|GL(n,q)| = q^{n(n-1)/2} \prod_{i=1}^{n} (q^i - 1)$ [3].

Our main concern in this section is the homogeneous weight on $M_2(\mathbb{F}_p)$ and before we give the generalized homogeneous weight on $M_2(\mathbb{F}_p)$ we first give the structure of $M_2(\mathbb{F}_p)$.

Remark 1. *The matrix ring $M_n(\mathbb{F}_q)$ has no proper ideals but it has proper left ideals [9]. In particular $M_2(\mathbb{F}_p)$ has $p+1$ minimal left ideals [2]. This idea is essential in this section so we take it as a theorem.*

Theorem 1. *The matrix ring $M_2(\mathbb{F}_p)$ has $p+1$ minimal left ideals and each minimal left ideal contained p^2 elements.*

Proof:

Let $A \in M_2(\mathbb{F}_p)$ where $A = \begin{pmatrix} a_0 & a_1 \\ a_2 & a_3 \end{pmatrix}$ and note that $\begin{pmatrix} 1 & r \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ are nonzero nonunit idempotents of $M_2(\mathbb{F}_p)$ where $r \in \mathbb{F}_p$. Thus, the proper left ideals are of the form $\begin{pmatrix} a_0 & ra_0 \\ a_2 & ra_2 \end{pmatrix}$ and $\begin{pmatrix} 0 & a_1 \\ 0 & a_3 \end{pmatrix}$. Hence, there are $p+1$ minimal left ideals in $M_2(\mathbb{F}_p)$ since the intersection of any two minimal left ideals of $M_2(\mathbb{F}_p)$ is the zero matrix and every minimal left ideals of $M_2(\mathbb{F}_p)$ has p^2 elements. ■

The main problem about the generalization of the homogeneous weight on $M_2(\mathbb{F}_p)$ lies on $\sum_{u \in GL(2,p)} \chi(uA)$ where $A \in M_2(\mathbb{F}_p)$. The case when A is the zero matrix is obvious. Theorem 2 below is on the invertible matrices while Theorem 3 involves the zero divisors.

Theorem 2. $\sum_{u \in GL(2,p)} \chi(u) = \sum_{u \in GL(2,p)} \chi(uA) = p$ *where* $A \in GL(2,p)$.

Proof:

Let D be the set of all the zero divisors in $M_2(\mathbb{F}_p)$. We have $\sum_{A \in M_2(\mathbb{F}_p)} \chi(A) = 0$ [8]. So,

$$\sum_{u \in GL(2,p)} \chi(u) = -\sum_{B \in D} \chi(B) - \chi(0). \tag{1}$$

Since $M_2(\mathbb{F}_p)$ has $p+1$ minimal left ideals, $\chi_{I_L}(A) = \chi(A)$ for all $A \in I_L$ and $\chi_{I_L}(0) = 1$ in [8], where χ_{I_L} is character defined in the minimal left ideal I_L of $M_2(\mathbb{F}_p)$. Hence,

$$\sum_{u \in GL(2,p)} \chi(u) = -(p+1) \sum_{B \in I_L \setminus \{0\}} \chi_{I_L}(B) - 1 \tag{2}$$

$$= -(p+1)(-1) - 1 \tag{3}$$

$$= p. \tag{4}$$

■

Theorem 3. $\sum_{u_k \in GL(2,p)} \chi(u_k B) = p - p^2$ *for all* $B \in I_L \setminus \{0\}$.

Proof:

$$-\sum_{u_k \in GL(2,p)} \chi(u_k B)$$

$$= \left[\sum_{B_j \in I_L \setminus \{0\}} \chi(B_j)\right]\left[\sum_{u_k \in GL(2,p)} \chi(u_k B)\right] \tag{5}$$

$$= \sum_{B_j \in I_L \setminus \{0\}} \sum_{u_k \in GL(2,p)} \chi(u_k B)\chi(B_j) \tag{6}$$

$$= \sum_{B_j \in I_L \setminus \{0\}} \sum_{u_k \in GL(2,p)} \chi(u_k B + B_j) \tag{7}$$

$$= \sum_{u_k \in GL(2,p)} \sum_{B_j \in I_L \setminus \{0\}} \chi(u_k B + B_j) \tag{8}$$

For each $u_r \in GL(2,p)$, there exists $B_s \in I_L\backslash\{0\}$ such that $u_rB + B_s = 0$. Note that B_s is not unique for every u_r. Therefore,

$\sum_{u_k\in GL(2,p)} \sum_{B_j\in I_L\backslash\{0\}} \chi(u_kB + B_j)$

$$= \sum_{u_r\in GL(2,p)} \chi(u_rB + B_s) \tag{9}$$

$$+ \sum_{u_k\in GL(2,p)} \sum_{B_j\in I_L\backslash\{0\}} \chi(u_kB + B_j) \tag{10}$$

where $u_kB + B_j \neq 0$

$$= \sum_{u_r\in GL(2,p)} \chi(0) + \sum_{u_k\in GL(2,p)} \sum_{B_j\in I_L\backslash\{0\}} \chi(u_kB + B_j) \tag{11}$$

where $u_kB + B_j \neq 0$

$$= |GL(2,p)| + \sum_{u_k\in GL(2,p)} \sum_{B_j\in I_L\backslash\{0\}} \chi(u_kB + B_j) \tag{12}$$

where $u_kB + B_j \neq 0$.

For every $B_t \in I_L\backslash\{0, B_s\}$ we have $u_rB+B_t \in I_L\backslash\{0, u_rB\}$ $(i.e. B_t + \{I_L\backslash\{0, B_s\}\}=I_L\backslash\{0, u_rB\})$ and for fixed B_t and u_r we can always find l such that $u_l \neq u_r$ and $u_rB+B_t = u_rB$. Thus, we can collect all the elements of $I_L\backslash\{0\}$. And since $|I_L\backslash\{0\}|$ divides $|GL(2,p)|$,

$|GL(2,p)| + \sum_{u_k\in GL(2,p)} \sum_{B_j\in I_L\backslash\{0\}} \chi(u_kB + B_j)$

$$= |GL(2,p)| \tag{13}$$

$$+ \frac{|GL(2,p)||I_L\backslash\{0\}| - |GL(2,p)|}{|I_L\backslash\{0\}|} \sum_{B_j\in I_L\backslash\{0\}} \chi(B_j) \tag{14}$$

$$= (p^2 - p)(p^2 - 1) + (p^2 - p)(p^2 - 2)(-1) \tag{15}$$

$$= p^2 - p. \tag{16}$$

Thus,

$$\sum_{u_k\in GL(2,p)} \chi(u_kB) = p - p^2. \tag{17}$$

■

Theorem 4. *The normalized homogeneous weight on $M_2(\mathbb{F}_p)$ is given by*

$$w_{\mathtt{nhom}}(A) = \begin{cases} 0 & \text{if } A = \mathbf{0} \\ 1 - \dfrac{1}{(p^2-1)(p-1)} & \text{if } A \in GL(2,p) \\ \dfrac{p^2}{(p^2-1)} & \textit{otherwise.} \end{cases}$$

Proof:

If $A = \mathbf{0}$ then

$$w_{\mathtt{nhom}}(A) = 1 - \frac{(p^2-1)(p^2-p)}{(p^2-1)(p^2-p)} \tag{18}$$

$$= 0. \tag{19}$$

If $A \in GL(2,p)$ then

$$w_{\mathtt{nhom}}(A) = 1 - \frac{p}{(p^2-1)(p^2-p)} \tag{20}$$

$$= 1 - \frac{1}{(p^2-1)(p-1)}. \tag{21}$$

If $A \in D$ then

$$w_{\mathtt{nhom}}(A) = 1 - \frac{p-p^2}{(p^2-1)(p^2-p)} \tag{22}$$

$$= \frac{p^2}{p^2-1}. \tag{23}$$

■

3. $\mathbb{F}_{P^2}$-LINEAR MAP

In this section we first characterize the finite field $\mathbb{F}_p$ in such a way that the polynomial $f(x) = x^2 + x + (p-1)$ is irreducible over $\mathbb{F}_p$. Then we give a corresponding cyclic algebra that is isomorphic to $M_2(\mathbb{F}_p)$ and is a left $\mathbb{F}_{p^2}$- vector space.

Lemma 1. *Let $p \equiv 2$ or 3 (mod 5) then the polynomial $f(x) = x^2 + x + (p-1)$ is irreducible over $\mathbb{F}_p$.*

Proof:

The case when $p = 2$ is trivial. Note that the discriminant of the polynomial $f(x)$ is equal to $5 \in \mathbb{F}_p$. Then $f(w)$ is reducible over $\mathbb{F}_p$ if there exists a $y \in \mathbb{F}_p$ such that $y^2 \equiv 5 \pmod p$. By the Law of Quadratic Reciprocity, when p is odd $y^2 \equiv 5 \pmod p$ is solvable iff $p \equiv 1$ or -1 (mod 5). ■

Remark 2. *The numbers p in Lemma 1 are the prime numbers ending in 2, 3,or 7.*

Theorem 5 **(Greferath and Schmidt [5]).** *Let K be an Artinian commutative local ring and let $f = \sum_{i=0}^{n} a_ix_i \in K[x]$ be a monic irreducible polynomial. Then the mapping $\beta\colon K[x] \to M_n(K)$, $g(x) \mapsto g(X)$ induces a unital embedding of $K[x]/f$ into $M_n(K)$ where*

$$X = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

.

Remark 3. *The matrix X is known as the* **companion matrix**.

Proposition 1. *Let $\mathbb{F}_{p^2} = \mathbb{F}_p[\omega]$ where $\omega^2+\omega+(p-1) = 0$ then $\tau\colon \mathbb{F}_{p^2} \longrightarrow M_2(\mathbb{F}_p)$ defined by*

$a + b\omega \mapsto \begin{pmatrix} a & b \\ b & a + (p-1)b \end{pmatrix}$ *is an embedding.*

Proof:

The proof follows immediately from Lemma 1 and Theorem 5. ■

Remark 4. *For the rest of this paper, we denote* $\mathcal{F}_{p^2} := \tau(\mathbb{F}_{p^2})$.

Theorem 6. *Let* $\tau(\omega) = \begin{pmatrix} 0 & 1 \\ 1 & p-1 \end{pmatrix}$ *and* $v = \begin{pmatrix} 1 & 0 \\ p-1 & p-1 \end{pmatrix}$ *then* $v^2 = \mathbf{1}$, $\tau(\omega)^2 + \tau(\omega) + \tau(p-1) = \mathbf{0}$, $\tau(\omega)v = v\tau(\omega)^p$ *and* $\mathcal{F}_{p^2} + v\mathcal{F}_{p^2} \cong M_2(\mathbb{F}_p)$.

Proof:

We just need to note that $\omega^p = (p-1)\omega + (p-1)$ and $\tau(\omega)^p = \begin{pmatrix} p-1 & p-1 \\ p-1 & 0 \end{pmatrix}$ and follow the definition of the isomorphism of rings. ■

4. GENERALIZED FROBENIUS TRACE

The main goal of this section is to define a left generalized Frobenius trace from the noncommutative ring $\mathbb{F}_{p^2} + v\mathbb{F}_{p^2}$ defined above to the field $\mathbb{F}_{p^2}$. As a preparation we review some concepts in [4].

Definition 1 **(Greferath and Nechaev [4]).** *An extension of S of the ring R with the same identity 1 is called a* **left generalized Frobenius extension** *($\mathcal{GF}-$extension) if there exists an isomorphism:*

$$\phi :_S S \to_S Hom(_R S, _R R),$$

for which $w(S) = R$ where $w \in Hom(_R S, _R R)$.

Theorem 7 **(Greferath and Nechaev [4]).** *Let R be a Frobenius ring. Then an extension S of R with the same identity is a Frobenius ring if and only if it is a $\mathcal{GF}$-extension of R.*

Remark 5. *$M_2(\mathbb{F}_p)$ is an extension of $GF(p^2)$ and both $M_2(\mathbb{F}_p)$ and $GF(p^2)$ are finite Frobenius rings in which the 2×2 identity matrix as their identity.*

Definition 2 **(Greferath and Nechaev [4]).** *A homomorphism of left R-modules*

$$Tr_R^S :_R S \to_R R$$

is called (left) generalized Frobenius trace ($\mathcal{GF}-$trace) from S to R if :

(i) $Tr_R^S(S) = R$, *and*

(ii) $\ker(Tr_R^S)$ *does not contain any nonzero left ideal of S.*

Theorem 8. *Let $S = \mathcal{F}_{p^2} + v\mathcal{F}_{p^2}$ where $v^2 = \mathbf{1}$ and $R = \mathcal{F}_{p^2}$. The $\mathcal{GF}$-trace from S to R is given by $Tr_R^S(\alpha + v\beta) = \alpha$ where $\alpha, \beta \in \mathcal{F}_{p^2}$.*

Proof:

It is sufficient to note that $\ker(Tr_R^S) = v\mathcal{F}_{p^2}$ and since $det(v) \neq 0$, then $v\beta \in GL(2,p)$ for all $\beta \in \mathcal{F}_{p^2}$. Thus, $v\mathcal{F}_{p^2}$ is not a left ideal of S. ■

5. GROUP CODES AND SCALED ISOMETRY

Let S be a $\mathcal{GF}-$*extension* of the ring R with $\mathcal{GF}-$*trace*. Let $G = S^\times$ be the multiplicative group of the ring S and let $R[G]$ be the group ring, i.e. the set of all $f : G \to R$ equipped with natural addition, and multiplication * defined by

$$f * g(z) = \textstyle\sum_{x+y=z} f(x)g(y) \text{ for all } f, g \in R[G].$$

To every $\delta \in S$ there corresponds an element $c(\delta) \in R[G]$ defined by

$$c(\delta) : G \to S,\ g \mapsto Tr_R^S(g^{-1}\delta).$$

For every subset J of S we define $C(J) = \{c(\delta) \mid \delta \in J\}$. If $G = \{g_1, g_2, ..., g_m\}$ we can consider $C(J)$ as a code of length m over R:

$$C(J) = \{(Tr_R^S(g_1^{-1}\delta), ..., Tr_R^S(g_m^{-1}\delta)) \mid \delta \in J\}.$$

If w_S is the normalized homogeneous weight of S, and w_R is the normalized homogeneous weight of R. Then for $t \in \mathbb{N}$ and $\gamma > 0 \in \mathbb{R}$, a map $\sigma : S \longrightarrow R^t$ satisfying the condition that for all $a, b \in S$ there holds $w_R(\sigma(a), \sigma(b)) = \gamma w_S(a, b)$ is called an **scaled isometry with scaling factor** γ.

Theorem 9. *Let $S = M_2(\mathbb{F}_p)$, $R = \mathcal{F}_{p^2}$ and $m = |GL(2,p)|$. Then the map $M_2(\mathbb{F}_p) \longrightarrow \mathcal{F}_{p^2}^m$, $\delta \mapsto c(\delta)$ is an $\mathbb{F}_{p^2}$-linear scaled isometry from $(M_2(\mathbb{F}_p), w_S)$ into $(\mathcal{F}_{p^2}^m, w_R)$ such that $w_R(c(\delta)) = m w_S(\delta)$ for all δ in S.*

Proof:

Since $M_2(\mathbb{F}_p) \cong \mathcal{F}_{p^2} + v\mathcal{F}_{p^2}$ and $\mathcal{F}_{p^2} \cong \mathbb{F}_{p^2}$ then the proof follows from Theorem 22 in [4] and Theorem 7 above. ■

Theorem 10. *Let J be a minimal left ideal of $M_2(\mathbb{F}_p)$ then $C(J)$ is an (m, p^2)-additive code over $\mathcal{F}_{p^2}$ with $d_{\mathtt{Ham}} = m = |GL(2,p)|$.*

Proof:

Clearly, the length of $C(J)$ is m. We only need to show that $|C(J)| = p^2$ and $C(J)$ has the minimum Hamming distance $d_{\text{Ham}} = m$.

Let $\delta \in J$ such that $\delta = \alpha + v\beta$ where $\alpha, \beta \in \mathcal{F}_{p^2}$ and $v = \begin{pmatrix} 1 & 0 \\ p-1 & p-1 \end{pmatrix}$. Also let $f\colon J \longrightarrow \mathcal{F}_{p^2}$ such that $f(\delta) = \alpha$. Then f is a monomorphism since $\mathcal{F}_{p^2} \cong \mathbb{F}_{p^2}$ and $\ker(f) = \{\alpha + v\beta | f(\alpha + v\beta) = \mathbf{0}\} = \{v\beta\} = \{\mathbf{0}\}$. Thus, $|C(J)| = p^2$.

Let w'_{nhom} be the normalized homogeneous weight on $C(J)$. From Theorem 4 and Theorem 9,

$$w'_{\text{nhom}}(c(\delta)) = (p^2 - p)(p^2 - 1)\left(\frac{p^2}{p^2 - 1}\right)$$

for all $\delta \in J\backslash\{\mathbf{0}\}$. Thus, $w_{\text{Ham}}(c(\delta)) = (p^2 - p)(p^2 - 1)$ for all $\delta \in J\backslash\{\mathbf{0}\}$ since $w_{\text{nhom}}(x) = \dfrac{p^2}{p^2 - 1}$ for all $x \in \mathbb{F}_{p^2}\backslash\{0\}$. Hence, the minimum Hamming distance of $C(J)$ is $d_{\text{Ham}} = (p^2 - p)(p^2 - 1) = m$. ■

6. ACKNOWLEDGEMENT

The authors would like to thank the IMSP Coding Theory and Cryptography Cluster for helpful discussions. The first author acknowledges financial support from the DOST-ASTHRDP.

7. REFERENCES

[1] Alamadhi A.. Sboui H.. Solé P. Yemen O.:, Cyclic Codes over $M_2(\mathbb{F}_2)$. available on arXiv:1201.6533v1. (2012).

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

[3] Biggs C.. White I.: Permutation groups and combinatorial structure, Cambridge University Press, London (1979).

[4] Greferath M.. Nechaev A.: Generalized Frobenius Extensions of Finite Rings and Trace Functions. IEEE Information Theory Workshop-ITW Dublin. (2010).

[5] Greferath M.. Schmidt S. E.: Linear Codes and Rings of Matrices. Proceedings of AAECC 13 Hawaii, Springer LNCS 1719, 160-169 (1999).

[6] Greferath M.. Schmidt S. E.: Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code. IEEE Trans. Inf. Theory, vol. 45, no. 7, pp. 2522–2524, November 2001.

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

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

[9] Hungeford T. W.: Algebra (Graduate Texts in Mathematics **73**). Springer-Verlag, New York (1974).

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