Cryptogr. Commun. (2018) 10:1109–1117
https://doi.org/10.1007/s12095-017-0266-1

Cyclic codes over $M_2(\mathbb{F}_2 + u\mathbb{F}_2)$

Rong Luo[1] · **Udaya Parampalli**[2]

Received: 25 December 2016 / Accepted: 3 November 2017 / Published online: 1 December 2017

Abstract Let $A = M_2(\mathbb{F}_2 + u\mathbb{F}_2)$, where $u^2 = 0$, the ring of 2×2 matrices over the finite ring $\mathbb{F}_2 + u\mathbb{F}_2$. The ring A is a non-commutative Frobenius ring but not a chain ring. In this paper, we derive the structure theorem of cyclic codes of odd length over the ring A and use them to construct some optimal cyclic codes over $\mathbb{F}_4$. Let $v^2 = 0$ and $uv = vu$. We also give an isometric map from A to $\mathbb{F}_4 + v\mathbb{F}_4 + u\mathbb{F}_4 + uv\mathbb{F}_4$ using their respective Bachoc weight and Lee weight.

Keywords Cyclic codes · Lee weight · Bachoc weight · Gray map

Mathematics Subject Classification (2010) 94B05 · 94B15

1 Introduction

Cyclic codes over finite rings have been much studied in recent years, particularly after the significant result obtained in [1], where certain interesting nonlinear binary codes were constructed through a Gray map from $\mathbb{Z}_4$ to $\mathbb{F}_2^2$. The Gray map employed in [1] is an isometry from Lee weight over $\mathbb{Z}_4$ to Hamming weight over $\mathbb{F}_2^2$, which helped to explain the apparent duality of the nonlinear binary codes. Since then several recent papers dealt with codes over

This article is part of the Topical Collection on *Special Issue on Sequences and Their Applications*

✉ Rong Luo
luorong@swjtu.edu.cn

Udaya Parampalli
udaya@unimelb.edu.au

[1] School of Mathematics, Southwest Jiaotong University, Chengdu 610031, China

[2] Department of Computing and Information Systems, University of Melbourne, Victoria 3010, Australia

finite commutative rings. The case of noncommutative rings have been studied in different contexts by very few authors (see [2, 4, 5, 7–9]). Recently the ring $M_2(\mathbb{F}_2)$ was studied in the context of space time codes [7]. Subsequently, in [4] the theory of cyclic codes over $M_2(\mathbb{F}_2)$ was developed. One got a characterization of cyclic codes and their duals as right ideals in terms of two generators and the existence of infinitely many nontrivial cyclic codes for the Euclidean product. But these codes were derived in the case of odd length. Thus, a natural question is the generalization to even length.

In this paper, we will focus on cyclic codes of odd length over the ring $A = M_2(\mathbb{F}_2 + u\mathbb{F}_2)$, where $u^2 = 0$, which enables us to construct even length codes over $M_2(\mathbb{F}_2)$ using a Gray map. An important fact is that the ring A is not a finite chain or commutative ring. We will define a Gray map ϕ from $M_2(\mathbb{F}_2+u\mathbb{F}_2)$ to $M_2^2(\mathbb{F}_2)$ which preserves the Bachoc weight [2]. Thus, images of cyclic codes of odd length over A under ϕ are binary quasi-cyclic codes of even length over $M_2(\mathbb{F}_2)$. This is one of the questions introduced in [4].

In Section 2, we will start with a short description of the ring $M_2(\mathbb{F}_2 + u\mathbb{F}_2)$ and show that $M_2(\mathbb{F}_2 + u\mathbb{F}_2) \cong \mathbb{F}_4 + v\mathbb{F}_4 + u\mathbb{F}_4 + uv\mathbb{F}_4$,where $v^2 = 0$ and $uv = vu$. Hence, the ring $M_2(\mathbb{F}_2 + u\mathbb{F}_2)$ has the similar structure of $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ which was introduced in [6], So, refer to that work, we will define a Gray map from $M_2(\mathbb{F}_2 + u\mathbb{F}_2)$ to $\mathbb{F}_4^4$ and extend the definition of Lee weight in [3].

In Section 3, the structure of cyclic codes of odd length over $M_2(\mathbb{F}_2 + u\mathbb{F}_2)$ will be obtained. In Section 4, the Bachoc weight will be introduced over $M_2(\mathbb{F}_2 + u\mathbb{F}_2)$. We will define a right $\mathbb{F}_2$-module isometry from $M_2(\mathbb{F}_2 + u\mathbb{F}_2)$ to $\mathbb{F}_4 + v\mathbb{F}_4 + u\mathbb{F}_4 + uv\mathbb{F}_4$ using their respective Bachoc weight and Lee weight. This ideal for the isometry map comes from [5] in which an isometric map from $M_2(\mathbb{F}_2)$ to $\mathbb{F}_4^2$ was defined. In Section 5, we will give some examples of cyclic codes of length 3 and 5 over $M_2(\mathbb{F}_2+u\mathbb{F}_2)$, and show their images under the Gray maps ϕ are optimal quaternary quasi-cyclic codes of length 12 and 20 over $\mathbb{F}_4$, respectively.

2 Linear codes over $M_2(\mathbb{F}_2 + u\mathbb{F}_2)$

Let $A = M_2(\mathbb{F}_2 + u\mathbb{F}_2)$, where $u^2 = 0$. Then A is a non-commutative ring of matrices of order 2 over the ring $\mathbb{F}_2 + u\mathbb{F}_2$. Clearly $A = M_2(\mathbb{F}_2) + uM_2(\mathbb{F}_2) \simeq M_2(\mathbb{F}_2)[u]/\langle u^2\rangle$. Here we present some preliminaries that are required to introduce linear and cyclic codes over A. Following [2], $M_2(\mathbb{F}_2) = \mathbb{F}_2[\zeta] + i\mathbb{F}_2[\zeta]$, where ζ and i are elements in A satisfying the relation $i\zeta = \zeta^2 i$. A possible choice of ζ and i given by Bachoc [2] are $i = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $\zeta = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. Setting $v = 1 + i$ and identifying the subring $\mathbb{F}_2[\zeta]$ with $\mathbb{F}_4$ follows that $M_2(\mathbb{F}_2) = \mathbb{F}_4 + v\mathbb{F}_4$. This implies that

$$A = \mathbb{F}_4 + v\mathbb{F}_4 + u\mathbb{F}_4 + uv\mathbb{F}_4,$$

where $v^2 = u^2 = 0$ and $uv = vu$.

We recall, in the case of $\mathbb{F}_2+u\mathbb{F}_2$, Lee weight was defined in [3] as $w_L(0) = 0$, $w_L(1) = w_L(1 + u) = 1$, $w_L(u) = 2$, and accordingly a Gray map from $(\mathbb{F}_2 + u\mathbb{F}_2)^n$ to $\mathbb{F}_2^{2n}$ was defined by sending $a + ub$ to $(b, a + b)$ with $a, b \in \mathbb{F}_2^n$. We will adopt a similar technique here to define the Gray map from A to $\mathbb{F}_4^4$. It follows:

$$\theta : A \to \mathbb{F}_4^4, a + bu + cv + duv \to (d, c + d, b + d, a + b + c + d),$$

where a, b, c, d are in $\mathbb{F}_4$. For any $e = a + bu + cv + duv$ in A, we extend the definition of the Lee weight as

$$w_L(e) = w_H(d) + w_H(d + c) + w_H(d + b) + w_H(d + c + b + a),$$

where $w_H(-)$ denotes Hamming weight of the element $-$ of $\mathbb{F}_4$.

Definition 1 (1) A linear code $\mathcal{C}$ of length n over the ring A is an A-submodule of A^n.
(2) Let $c = (c_0, c_1, \cdots, c_{n-1})$ be a vector of A^n. Then Lee weight of c is defined as

$$w_L(c) = w_L(c_0) + w_L(c_1) + \cdots + w_L(c_{n-1}).$$

(3) Let $\mathcal{C}$ be a linear code over A. Then Lee distance of $\mathcal{C}$ is defined as

$$d_L(\mathcal{C}) = \min\{w_L(c) = \sum_{i=0}^{n-1} w_L(c_i) | c = (c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}\}.$$

Extending the map θ to vectors, by definition of Lee distance, we have the following theorem.

Theorem 1 *If $\mathcal{C}$ is a linear code over A of length n, size M and Lee distance d. Then $\theta(\mathcal{C})$ is a code over $\mathbb{F}_4$ of length $4n$, size M and Hamming distance d.*

3 Cyclic codes over $M_2(\mathbb{F}_2 + u\mathbb{F}_2)$

Let $A[x]$ be the ring of polynomials over A. We have a natural homomorphic mapping from A to the field $\mathbb{F}_4$. For any $e \in A$, let $\tilde{e}$ denote the polynomial reduction modulo u and v. Now we define a polynomial reduction mapping $\mu : A[x] \to \mathbb{F}_4[x]$ such that

$$f(x) = \sum_{i=0}^{n-1} e_i x^j \to \sum_{i=0}^{n-1} \tilde{e_i} x^j.$$

A monic polynomial f over $A[x]$ is said to be a basic irreducible polynomial if its projection $\mu(f)$ is irreducible over $\mathbb{F}_4[x]$. As right modules we have the Chinese Remainder Theorem as follows. In the sequel, we will drop interrminate x for polynomials when the context is clear.

Proposition 1 *Let n be an odd number. Then*

$$\frac{A[x]}{\langle x - 1\rangle} = \oplus_{j=1}^{t} \frac{A[x]}{\langle f_j\rangle}$$

where $x^n - 1 = \prod_{j=1}^{t} f_j$ and f_j's are irreducible polynomials over $\mathbb{F}_4$.

Proof The proof follows by a natural application of Chinese Remainder theorem to the right module $\frac{A[x]}{\langle x-1\rangle}$ using the method similar to that given in [7] □

We shall prove the results below using the same techniques in [2] with the condition n being an odd number.

Proposition 2 *If f is an irreducible polynomial over $\mathbb{F}_4$, then the only right A-modules of $R_f = \frac{A[x]}{\langle f\rangle}$ have two types*

I: $\langle 0\rangle, \langle 1\rangle, \langle u\rangle, \langle v\rangle, \langle u\rangle + \langle v\rangle, \langle uv\rangle$.
II: $\langle u + vh_\alpha\rangle$ *where h_α is a unit in* $\frac{\mathbb{F}_4[x]}{\langle f\rangle_{\mathbb{F}_4[x]}}$.

Proof Let I be a nonzero ideal of R_f and let $0 \neq g \in A[x]$ with $g + \langle f\rangle \in I$ and $g \notin \langle f\rangle$. Then there exist $g_1, g_2, g_3, g_4 \in \mathbb{F}_4[x]$ such that $g = g_1 + ug_2 + vg_3 + uvg_4$. Consider the polynomial $g_1(x)$, we obtain that

$$\gcd(g_1(x), f(x)) = f(x) \text{ or } 1.$$

If $\gcd(g_1(x), f(x)) = 1$ for some $g_1(x) \in A[x]$, then there exists $g_1' \in \mathbb{F}_4[x]$ such that $g_1g_1' + \langle f(x)\rangle = 1 + \langle f(x)\rangle$. Let $g' = g_1' - u((g_1')^2g_2 - v((g_1')^2g_3 - vu(g_4(g_1')^2 + 2(g_1')^3g_2g_3)$. Then we have $gg' + \langle f(x)\rangle = 1 + \langle f(x)\rangle$. This means that $I = R_f$. Now assume that $\gcd(g_1(x), f(x)) = f(x)$ for any element $g + \langle f(x)\rangle \in I$, then $g + \langle f(x)\rangle = ug_2 + vg_3 + uvg_4 + \langle f(x)\rangle$.

If $\gcd(g_2(x), f(x)) = f(x)$, then $g+\langle f(x)\rangle = vg_3(x)+uvg_4(x)$. It follows that $I = \langle v\rangle$ or $I = \langle uv\rangle$.

If $\gcd(g_2(x), f(x)) = 1$ exists, arguing as in the proof of $g_1(x)$, one deduces that there is a $g_2^{-1} \in \mathbb{F}_4[x]$ such that $g_2g_2^{-1} = 1$. This implies that $uv = g \cdot vg_2^{-1} \in I$. It follows that $ug_2 + vg_3 = g - uvg_4 \in I$.

If $\gcd(g_3(x), f(x)) = f(x)$, then $u \in I$. This means that $I = \langle u\rangle$.

If $\gcd(g_3(x), f(x)) = 1$, then $u + vh_\alpha \in I$ where $h_\alpha = g_2^{-1}g_3$ is a unit of $\mathbb{F}_4[x]$. Now one obtains two cases as follows:

Case A: $\langle u + vh_\alpha\rangle = I$.

Case B: $\langle u + vh_\alpha\rangle \lneqq I$. Then there exists $u + vh_\beta \in I$ where $h_\beta \in \mathbb{F}_4[x]$, but it is not in $\langle u + vh_\alpha\rangle$. This implies that $v(h_\alpha - h_\beta) \in I$. Since $h_\alpha - h_\beta \notin \langle f(x)\rangle$, $v \in I$. Thus, we obtain that $I = \langle u\rangle + \langle v\rangle$. □

Let h be a factor of $x^n - 1$ in $\mathbb{F}_4[x]$. We denote by $\hat{h} = \frac{x^n-1}{g}$.

Proposition 3 *Let $x^n - 1 = f_1f_2\cdots f_t$ where $f_i (1 \leq i \leq t)$ are irreducible pairwise-coprime polynomials in $\mathbb{F}_4[x]$. Then any ideal in $\frac{A[x]}{\langle x^n-1\rangle}$ is a sum of ideals of the form $\langle \hat{f}_i + \langle x^n - 1\rangle\rangle, \langle u\hat{f}_i + \langle x^n - 1\rangle\rangle, \langle (u + vh_\alpha)\hat{f}_i + \langle x^n - 1\rangle\rangle$ for $1 \leq i \leq t$. where h_α is a unit of $\frac{\mathbb{F}_4[x]}{\langle x^n-1\rangle}$.*

Proof By the Chinese Remainder Theorem, we have

$$\frac{A[x]}{\langle x^n - 1\rangle} = \frac{A[x]}{\bigcap_{i=1}^m \langle f_i\rangle} = \bigoplus_{i=1}^m \frac{A[x]}{\langle f_i\rangle}.$$

Thus, any ideal of is of the form $\oplus I_i$, where I_i is an ideal of $\frac{A[x]}{\langle f_i\rangle}$. By Proposition 2, for $1 \leq i \leq t$, we have

$$I_i \in \{\langle 1 + \langle f_i\rangle\rangle, \langle u + \langle f_i\rangle\rangle, \langle v + \langle f_i\rangle\rangle, \langle u + vh_\alpha + \langle f_i\rangle\rangle\}.$$

Then I_i correspond to the form $\langle \hat{f}_i + \langle x^n - 1\rangle\rangle, \langle u\hat{f}_i + \langle x^n - 1\rangle\rangle, \langle (u + vh_\alpha)\hat{f}_i + \langle x^n - 1\rangle\rangle$ in $\frac{A[x]}{\langle x^n-1\rangle}$. Consequently, I is sum of ideals of the forms $\langle \hat{f}_i + \langle x^n - 1\rangle\rangle, \langle u\hat{f}_i + \langle x^n - 1\rangle\rangle, \langle (u + vh_\alpha)\hat{f}_i + \langle x^n - 1\rangle\rangle$, where $1 \leq i \leq t$. □

From now on, in order to simplify notation, we will just write $a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}$ for the corresponding coset $a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + \langle x^n - 1\rangle$ in $\frac{A[x]}{\langle x^n-1\rangle}$. Next, we give the main result in this section.

Theorem 2 *Let $\mathcal{C}$ be a cyclic code of odd length n over A. Then there exists a unit h_α in $\frac{\mathbb{F}_4[x]}{\langle x^n-1\rangle}$ and a family pairwise coprime monic polynomials $F_0, F_1, \cdots, F_6$ in $\mathbb{F}_4[x]$ such that $F_0F_1\cdots F_6 = x^n - 1$ and $\mathcal{C} = \langle \hat{F}_1\rangle \oplus \langle u\hat{F}_2\rangle \oplus \langle v\hat{F}_3\rangle \oplus \langle uv\hat{F}_4\rangle \oplus \langle (u + vh_\alpha)\hat{F}_5\rangle \oplus (\langle u\hat{F}_6\rangle + \langle v\hat{F}_6\rangle)$.*

Proof Let $x^n - 1 = f_1f_2\cdots f_m$ be a factorization of $x^n - 1$ into a product of monic basic irreducible pairwise coprime polynomials. By Proposition 3, $\mathcal{C}$ is a sum of ideals of the form $\langle \hat{f}_i + \langle x^n - 1\rangle\rangle$, $\langle u\hat{f}_i + \langle x^n - 1\rangle\rangle$, $\langle (u + vh_\alpha)\hat{f}_i + \langle x^n - 1\rangle\rangle$, where $1 \le i \le t$. After reordering if necessary, we can assume that

$$\begin{aligned}
\mathcal{C} = {} & \langle \hat{f}_{k_1+1}\rangle \oplus \cdots \oplus \langle \hat{f}_{k_1+k_2}\rangle \\
& \oplus \langle u\hat{f}_{k_1+k_2+1}\rangle \oplus \cdots \oplus \langle u\hat{f}_{k_1+k_2+k_3}\rangle \\
& \oplus \langle v\hat{f}_{k_1+k_2+k_3+1}\rangle \oplus \cdots \oplus \langle v\hat{f}_{k_1+\cdots+k_4}\rangle \\
& \oplus \langle uv\hat{f}_{k_1+\cdots+k_4+1}\rangle \oplus \cdots \oplus \langle uv\hat{f}_{k_1+\cdots+k_5}\rangle \\
& \oplus \langle (u + vh_\alpha)\hat{f}_{k_1+\cdots+k_5+1}\rangle \oplus \cdots \oplus \langle (u + vh_\alpha)\hat{f}_{k_1+\cdots+k_6}\rangle \\
& \oplus (\langle u\hat{f}_{k_1+\cdots+k_6+1}\rangle + \langle v\hat{f}_{k_1+\cdots+k_6+1}\rangle) \oplus \cdots \oplus (\langle u\hat{f}_m\rangle + \langle v\hat{f}_m\rangle),
\end{aligned}$$

where $k_1, \cdots, k_6 \ge 0$ and $k_1 + \cdots + k_6 + 1 \le t$.

Let $k_0 = 0$ and k_7 be nonnegative integers such that $k_1 + \cdots + k_7 = t$. Next, we define

$$\begin{aligned}
F_0 &= f_{k_0+1}\cdots f_{k_0+k_1}, & F_1 &= f_{k_0+k_1+1}\cdots f_{k_0+k_1+k_2}, \\
F_2 &= f_{k_0+k_1+k_2+1}\cdots f_{k_0+k_1+k_2+k_3}, & F_3 &= f_{k_0+\cdots+k_3+1}\cdots f_{k_0+\cdots+k_4}, \\
F_4 &= f_{k_0+\cdots+k_4+1}\cdots f_{k_0+\cdots+k_5}, & F_5 &= f_{k_0+\cdots+k_5+1}\cdots f_{k_0+\cdots+k_6}, \\
F_6 &= f_{k_0+\cdots+k_6+1}\cdots f_t.
\end{aligned}$$

Then, by our construction, it is clear that $F_0, F_1, \cdots, F_6$ are pairwise coprime, $F_0F_1\cdots F_6 = x^n - 1$, and

$$\begin{aligned}
\mathcal{C} = {} & \langle \hat{F}_1\rangle \oplus \langle u\hat{F}_2\rangle \oplus \langle v\hat{F}_3\rangle \oplus \langle uv\hat{F}_4\rangle \oplus \langle (u + vh_\alpha)\hat{F}_5\rangle \\
& \oplus (\langle u\hat{F}_6\rangle + \langle v\hat{F}_6\rangle).
\end{aligned}$$

□

Let $R = \frac{\mathbb{F}_4[x]}{\langle x^n-1\rangle_{\mathbb{F}_4[x]}}$ with $\langle x^n - 1\rangle_{\mathbb{F}_4[x]}$ being the ideal of $\mathbb{F}_4[x]$ generated by $x^n - 1$.

Proposition 4 *Let $\mathcal{C}$ be a cyclic code of odd length n over A. Then there exist polynomials F, G, H, K, Q in $\mathbb{F}_4[x]$ which are factors of $x^n - 1$ such that*

$$\mathcal{C} = \langle F\rangle_R + u\langle G\rangle_R + v\langle H\rangle_R + uv\langle K\rangle_R + (u + vh_\alpha)\langle Q\rangle_R,$$

where h_α is a unit of R and $\langle -\rangle_R$ is an ideal of R generated by $-$. Moreover,

$$|\mathcal{C}| = 4^{5n-(degF+degG+degH+degK+degQ)}.$$

Proof By Theorem 2, $\mathcal{C} = \langle \hat{F}_1\rangle \oplus \langle u\hat{F}_2\rangle \oplus \langle v\hat{F}_3\rangle \oplus \langle uv\hat{F}_4\rangle \oplus \langle (u+vh_\alpha)\hat{F}_5\rangle \oplus (\langle u\hat{F}_6\rangle + \langle v\hat{F}_6\rangle)$. Note that $\langle \hat{F}_i\rangle = \langle \hat{F}_i\rangle_R + u\langle \hat{F}_i\rangle_R + v\langle \hat{F}_i\rangle_R + uv\langle \hat{F}_i\rangle_R$ for $0 \le i \le 6$, we have

$$\begin{aligned}
\mathcal{C} =\ & \langle \hat{F}_1\rangle_R + u\langle \hat{F}_1\rangle_R + v\langle \hat{F}_1\rangle_R + uv\langle \hat{F}_1\rangle_R \\
& + u\langle \hat{F}_2\rangle_R + uv\langle \hat{F}_2\rangle_R \\
& + v\langle \hat{F}_3\rangle_R + uv\langle \hat{F}_3\rangle_R \\
& + uv\langle \hat{F}_4\rangle_R \\
& + (u + vh_\alpha)\langle \hat{F}_5\rangle_R + uv\langle \hat{F}_5\rangle_R \\
& + u\langle \hat{F}_6\rangle_R + v\langle \hat{F}_6\rangle_R + uv\langle \hat{F}_6\rangle_R \\
=\ & \langle \hat{F}_1\rangle_R \\
& + u(\langle \hat{F}_1\rangle_R + \langle \hat{F}_2\rangle_R + \langle \hat{F}_6\rangle_R) \\
& + v(\langle \hat{F}_1\rangle_R + \langle \hat{F}_3\rangle_R + \langle \hat{F}_6\rangle_R) \\
& + uv(\langle \hat{F}_1\rangle_R + \langle \hat{F}_2\rangle_R + \langle \hat{F}_3\rangle_R + \langle \hat{F}_4\rangle_R + \langle \hat{F}_5\rangle_R + \langle \hat{F}_6\rangle_R) \\
& + (u + vh_\alpha)\langle \hat{F}_5\rangle_R.
\end{aligned}$$

Let

$$\begin{aligned}
F &= \hat{F}_1 \\
G &= \hat{F}_1 + \hat{F}_2 + \hat{F}_6 \\
H &= \hat{F}_1 + \hat{F}_3 + \hat{F}_6 \\
K &= \hat{F}_1 + \hat{F}_2 + \hat{F}_3 + \hat{F}_4 + \hat{F}_5 + \hat{F}_6 \\
Q &= \hat{F}_5.
\end{aligned}$$

Next, we show that $\langle G\rangle_R = \langle \hat{F}_1\rangle_R + \langle \hat{F}_2\rangle_R + \langle \hat{F}_6\rangle_R$, $\langle H\rangle_R = \langle \hat{F}_1\rangle_R + \langle \hat{F}_3\rangle_R + \langle \hat{F}_6\rangle_R$ and $\langle K\rangle_R = \langle \hat{F}_1\rangle_R + \langle \hat{F}_2\rangle_R + \langle \hat{F}_3\rangle_R + \langle \hat{F}_4\rangle_R + \langle \hat{F}_5\rangle_R + \langle \hat{F}_6\rangle_R$.

For any distinct $i, j \in \{0, 1, \cdots, 6\}$, we have $x^n - 1 | \hat{F}_i \hat{F}_j$, so that $F_i F_j = 0$ in $\frac{\Lambda[x]}{\langle x^n - 1\rangle}$. Moreover, for $i = 1, \cdots, 6$, $\{F_i, \hat{F}_i\}$ are coprime pairs, hence, there exist $b_{0i}, b_{1i} \in \mathbb{F}_4[x]$ such that $b_{0i}F_i + b_{1i}\hat{F}_i = 1$.

Take $b_{0i}F_i + b_{1i}\hat{F}_i = 1$ for $i = 2, \cdots, 6$, then there exist polynomials $w_1, \cdots, w_6$ in $\mathbb{F}_4[x]$ such that

$$w_1 F_2 \cdots F_6 + w_2 \hat{F}_2 F_3 \cdots F_6 + \cdots + w_6 F_2 \cdots F_5 \hat{F}_6 = 1.$$

Multiplying both sides of the above equation by $\hat{F}_1$ yields

$$\hat{F}_1 = w_1 \hat{F}_1 F_2 \cdots F_6.$$

By the hypothesis, we obtain that

$$G = \hat{F}_1 + \hat{F}_2 + \hat{F}_6,$$

which implies that

$$w_1 F F_2 \cdots F_6 = w_1 \hat{F}_1 F_2 \cdots F_6.$$

Hence

$$w_1 G F_2 \cdots F_6 = \hat{F}_1.$$

This implies that $\hat{F}_1 \in \langle G \rangle_R$. Continuing this process, we have

$$\hat{F}_1, \hat{F}_2, \hat{F}_6 \in \langle G \rangle_R$$
$$\hat{F}_1, \hat{F}_3, \hat{F}_6 \in \langle H \rangle_R$$
$$\hat{F}_1, \hat{F}_2, \hat{F}_3, \hat{F}_4, \hat{F}_5, \hat{F}_6 \in \langle K \rangle_R$$

Consequently, by Theorem 2, $\mathcal{C} = \langle F \rangle_R + u\langle G \rangle_R + v\langle H \rangle_R + uv\langle K \rangle_R + (u + vh_\alpha)\langle Q \rangle_R$. Since $|\mathbb{F}_4| = 4$, $|\langle F \rangle_R| = 4^{n-\deg F}$, hence,

$$|\mathcal{C}| = 4^{5n-(\deg F+\deg G+\deg H+\deg K+\deg Q)}. \qquad \square$$

4 Right $\mathbb{F}_2$-module isometry

We take A as a natural extension of the ring $M_2(\mathbb{F}_2)$, accordingly, we can extend the definition of the Bachoc weight which was introduced in [2] from $M_2(\mathbb{F}_2)$ to this ring. Let W_B be the Bachoc weight over A and w_B be the ordinary Bachoc weight of $M_2(\mathbb{F}_2)$-codes, and so we set

$$W_B(X = X_1 + uX_2) = w_B(X_2) + w_B(X_1 + X_2), \text{ for any } X_1, X_2 \in M_2(\mathbb{F}_2).$$

The definition of the weight immediately leads to a Gray map from A to $M_2^2(\mathbb{F}_2)$ which naturally extends to A^n:

$$\varphi : A \to M_2^2(\mathbb{F}_2), X_1 + uX_2 \to (X_2, X_1 + X_2)$$

Note that φ extends to a distance preserving isometry:

$$\varphi : (A^n, \text{ Bachoc weight}) \to (M_2^{2n}(\mathbb{F}_2),$$

Bachoc weight).

Consider the mapping ϕ defined as

$$\begin{aligned}\phi : M_2(\mathbb{F}_2 + u\mathbb{F}_2) &\longrightarrow \mathbb{F}_4 + u\mathbb{F}_4 + v\mathbb{F}_4 + uv\mathbb{F}_4 \\ \begin{pmatrix} a_1 + ub_1 & a_2 + ub_2 \\ (a_2 + a_3) + u(b_2 + b_3) & (a_1 + a_2 + a_4) + u(b_1 + b_2 + b_4) \end{pmatrix} &\\ \longrightarrow (a_1 + a_2 w) + u(b_1 + b_2 w) + v(a_3 + a_4 w) + uv(b_3 + b_4 w),&\end{aligned}$$

where a_i, b_j in $\mathbb{F}_2$ for $1 \le i, j \le 4$. It is easy to show that ϕ is a left $\mathbb{F}_2$-module isomorphism. Note that $W_B(X = X_1 + uX_2) = w_B(X_2) + w_B(X_1 + X_2) = w_L(\phi(X))$ for all $X \in A$, ϕ is a right $\mathbb{F}_2$-module isometry. Thus, we have the following theorem.

Theorem 3 *If $\mathcal{C}$ is a cyclic code over A of length n, size M and minimum Bachoc distance d, then $\phi(\mathcal{C})$ is a linear code over $\mathbb{F}_4$ of length $4n$, size M and minimum Hamming distance d.*

5 Examples

A linear code $\mathcal{C}$ of length n over A is called an optimal code if the quaternary code $\theta(\mathcal{C})$ in Theorem 1 has the largest minimum Hamming distance for the given length and the dimension. Now, some optimal codes of length 3 and 5 over A are shown as the following examples. All the computations of minimum distance were performed in Magma (http://magma.maths.usyd.edu.au/magma/).

Example 1 The case when $n = 3$, we see the factorization of $x^3 - 1 = (x + 1)(x + w)(x + w^2)$. Now,let $f_1 = x + 1$, $f_2 = x + w$ and $f_3 = x + w^2$, some optimal codes of length 3 over A are shown as follows:

Generators	Imθ
$\langle f_3, uf_1, vf_1\rangle$	$[12, 11, 2]^*$
$\langle f_1, vf_2f_3\rangle$	$[12, 10, 2]$
$\langle f_1, (u + v)f_2f_3\rangle$	$[12, 10, 2]$
$\langle uf_1, vf_1, (u + v)f_2f_3\rangle$	$[12, 8, 4]^*$
$\langle uf_1, vf_1, uvf_2f_3\rangle$	$[12, 7, 4]$

Example 2 The case when $n = 5$, we see the factorization of $x^5 - 1 = (x + 1)(x^2 + wx + 1)(x^2 + w^2x + 1)$. Now, let $f_1 = x + 1$, $f_2 = x^2 + wx + 1$ and $f_3 = x^2 + w^2x + 1$, some optimal codes of length 5 over A are shown as follows:

Generators	Imθ
$\langle f_1, vf_2f_3\rangle$	$[20, 18, 2]^*$
$\langle f_1, (u + v)f_2f_3\rangle$	$[20, 18, 2]^*$
$\langle f_3, (u + v)f_1f_2\rangle$	$[20, 16, 3]$
$\langle uf_2, vf_2, (u + v)f_1\rangle$	$[20, 15, 4]^*$

6 Conclusion

In [4], a theory of cyclic codes over $M_2(\mathbb{F}_2)$ was developed giving a characterization of cyclic codes and their duals as right ideals in terms of two generators, and showing the existence of infinitely many nontrivial cyclic codes for the Euclidean product. But these codes were derived in the case of odd length. In this paper, based on these results, we derive the structure theorem of cyclic codes of odd length over the ring $M_2(\mathbb{F}_2 + u\mathbb{F}_2)$ which leads to even length codes over $M_2(\mathbb{F}_2)$. We also provide some optimal cyclic codes of even length over $\mathbb{F}_4$. Also we obtain an isometric map from $M_2(\mathbb{F}_2 + u\mathbb{F}_2)$ to $\mathbb{F}_4 + v\mathbb{F}_4 + u\mathbb{F}_4 + uv\mathbb{F}_4$ using their respective Bachoc weight and Lee weight.

Acknowledgments The authors would like to thank the Editor and anonymous reviewers for their valuable suggestions and comments that have much improved the quality of this paper. This research is supported in part by the National Natural Science Foundation of China Under Grants 11401488.

References

1. Hammons, A.R. Jr., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A., Sole, P.: The $\mathbb{Z}_4$-linearity of kerdock, preparata, goethals, and related codes. IEEE Trans. Inf. Theory **40**, 301–319 (1994)
2. Bachoc, C.: Applications of coding theory to the construction of modular lattices. J. Combinatorial Theory A **78-1**, 92–119 (1997)
3. Bonnecaze, A., Udaya, P.: Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$. IEEE Trans. Inf. Theory **45**, 1250–1255 (1999)
4. Alahmadi, A., Sboui, H., Sole, P., Yemen, O.: Cyclic codes over $M_2(\mathbb{F}_2)$. J. Franklin Institute **350**, 2837–2847 (2013)

5. Falcunit, D.F., Sison, V.P.: Cyclic codes over matrix ring $M_2(\mathbb{F}_p)$ and their isometric images over $\mathbb{F}_{p^2} + u\mathbb{F}_{p^2}$. International Zurich Seminar on Communications(IZS) 26–28 (2014)
6. Yildiz, Y.B., Karadeniz, S.: Cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. Des. Codes Crypt. **58**, 221–234 (2011)
7. Oggier, F., Sole, P., Belfiore, J.C.: Codes over matrix rings for space-time coded modulations. IEEE Tra. Inf. Theory IT **58**, 734–746 (2012)
8. Greferath, M., Schmidt, S.E.: Linear codes and rings of matrices. Proceeding of AAEECC Hawaii, Springer LNCS **1719**, 160–169 (1999)
9. Wood, J.: Duality for modules over finite rings and applications to coding theory. American J. Math. **121**, 555–575 (1999)