CYCLIC CODES OVER LOCAL FROBENIUS RINGS
OF ORDER 16

STEVEN T. DOUGHERTY*
Department of Mathematics, University of Scranton
Scranton, PA 18518, USA

ABIDIN KAYA
Department of Mathematics, Fatih University
Istanbul, 34500, Turkey

ESENGÜL SALTÜRK
Department of Mathematics, University of Scranton
Scranton, PA 18518, USA

(Communicated by Sergio R. Lopez-Permuth)

Abstract. We study cyclic codes over commutative local Frobenius rings of order 16 and give their binary images under a Gray map which is a generalization of the Gray maps on the rings of order 4. We prove that the binary images of cyclic codes are quasi-cyclic codes of index 4 and give examples of cyclic codes of various lengths constructed from these techniques including new optimal quasi-cyclic codes.

1. INTRODUCTION

Cyclic codes are one of the most interesting classes of linear codes both over fields and over rings. This is largely because of their rich algebraic structure. They were first studied by Prange in 1957 in [16] and since this early work, numerous papers have been written examining both their algebraic structure and their applications. The well known paper of Hammons et al. [10], sparked a great deal of interest in codes over rings and especially in rings which have an attached Gray map to the binary space. This present work draws from both sources as we study cyclic codes over a family of finite rings which admit a Gray map to the binary Hamming space.

The rings we consider can be either a chain ring or a non-chain ring. Numerous papers have studied cyclic codes over finite chain rings, see [2, 5, 12, 15, 17] for example. More recently codes over non-chain rings and their structures have been studied in [6, 8, 18].

In [13], Martinez and Szabo have classified the finite commutative local Frobenius rings of order 16. There are 12 such rings of which 7 are non-chain rings and 5 are chain rings. All of those rings are of order 16 with maximal ideal \( m \), \( |m| = 8 \) and \( |\text{Soc}(R)| = 2 \). In [8], generating characters for each ring have been described.

2010 Mathematics Subject Classification: Primary: 94B15, 11T71.
Key words and phrases: Cyclic codes, codes over local rings, Gray maps.

The third author would like to thank TUBITAK (The Scientific and Technological Research Council of Turkey) for their support while writing this paper.

* Corresponding author.
Moreover, MacWilliams relations for symmetrized and complete weight enumerators have been given in a very concrete form for codes over these rings. In [7], a weight preserving Gray map has been defined from these 12 rings to the binary space and self-dual and formally self-dual codes over these rings have been studied.

In this paper, we study the structure of cyclic codes over finite commutative local Frobenius rings of order 16. Since the characterization of cyclic codes over finite chain rings was already studied in [5], we will describe the structure of the ideals of the ring $R[x]/(x^n - 1)$ where $R$ is a local Frobenius non-chain ring of order 16. We prove that the binary images of cyclic codes are quasi-cyclic codes of index 4. Finally, we give some examples of various lengths including some new optimal codes.

2. Definitions and notations

2.1. Rings and codes. We begin by giving the necessary definitions for rings and for codes over rings. Throughout this paper all rings are assumed to be finite, commutative, Frobenius and have a multiplicative identity.

The Jacobson radical of a ring is defined to be the intersection of all maximal ideals of the ring. The socle of the ring is the sum of all the minimal one sided ideals of the ring. For a ring $R$, we denote the Jacobson radical as $J(R)$ and the socle as $Soc(R)$. If $R$ is a finite ring then the following statements are equivalent: (1) $R$ is a Frobenius ring; (2) as a left module, $\hat{R} \cong R_R$; (3) as a right module $\hat{R} \cong R_R$. A local ring is a ring with a unique maximal ideal. If the ideals of a local ring are linearly ordered then it is said to be a chain ring.

A code over a ring $R$ of length $n$ is a subset of $R^n$. If, additionally, it is a submodule, then we say that the code is linear. We attach to the ambient space $R^n$ the standard inner-product, namely $[v, w] = \sum v_i w_i$. The orthogonal is defined in the usual way as $C^\perp = \{v \mid [v, w] = 0, \forall w \in C\}$. Notice that an ideal in a ring $R$ is a code of length 1 and hence we can speak of $a^\perp$ if $a$ is an ideal of $R$.

2.2. Local Frobenius rings of order 16. We shall now describe the structure of the local Frobenius rings of order 16. Let $R$ be a local Frobenius ring with maximal ideal $m$, with $|m| = 8$, such that $|R| = 16$. All local Frobenius rings of order 16 have two elements $u$ and $v$ such that $m = \langle u, v \rangle$. There exists an element $w$ in these rings with $Soc(R) = \langle w \rangle = \{0, w\}$. The following diagram shows an ideal structure for any local Frobenius non-chain ring $R$ of order 16.
Since the ring $R$ is Frobenius we have that $\text{Soc}(R) = m^G$. Any local Frobenius non-chain ring of order 16 has 5 non-trivial ideals. The maximal ideal $m = \langle u, v \rangle$ is of size 8, the socle is of size 2 and the remaining 3 ideals are of size 4.

The classification of local Frobenius rings of order 16 is given in [13]. In this paper, we will deal with rings of order 16 for which we can identify elements $u, v, w$ which define the ideals in the ring and for which we can write each element of the ring uniquely in the form $a + bu + cv + dw$ where $a, b, c, d \in \mathbb{F}_2$. There are 5 local Frobenius chain rings with this structure which are given as follows:

- $\mathbb{F}_2[x]/\langle x^4 \rangle$, $\mathbb{Z}_4[x]/\langle x^2 - 2 \rangle$, $\mathbb{Z}_4[x]/\langle x^2 - 2x - 2 \rangle$, $\mathbb{Z}_4[x]/\langle x^3 - 2, 2x \rangle$, $\mathbb{Z}_{16}$. For chain rings we can identify elements for $u, v$ and $w$ but the ideal structure is a bit different. For example, consider the ring $\mathbb{Z}_{16}$. Here $u = 2, v = 4$ and $w = 8$. This allows us to apply the theory developed in this case even though there are only 5 ideals as opposed to 7 ideals. There are chain rings of order 16 which do not have this property, for example, $\mathbb{F}_4[x]/\langle x^2 \rangle$, which has only 3 ideals. In these cases you cannot find elements $u, v$ and $w$ to correspond to the developed theory. There are 7 local Frobenius non-chain rings which are given as follows:

- $\mathbb{F}_2[u, v]/\langle u^2, v^2 \rangle$, $\mathbb{F}_2[u, v]/\langle u^2 + v^2, uv \rangle$, $\mathbb{Z}_4[x]/\langle x^2 \rangle$, $\mathbb{Z}_4[x]/\langle x^2 - 2x \rangle$, $\mathbb{Z}_4[x, y]/\langle x^2, xy - 2, y^2, 2x, 2y \rangle$, $\mathbb{Z}_4[x, y]/\langle x^2 - 2, xy - 2, y^2, 2x, 2y \rangle$, $\mathbb{Z}_8[x]/\langle x^2 - 4, 2x \rangle$. There are also additional chain rings like $\mathbb{F}_4[x]/\langle x^2 \rangle$ which have only one non-trivial ideal. We shall not deal with these rings here since we do not have the elements $u, v$ and $w$ at our disposal to construct the proper Gray map.

Given the ideal structure of the rings it is possible to write every element of the ring uniquely in the form $a + bu + cv + dw$ where $a, b, c, d \in \mathbb{F}_2$. Note that this does not imply that the additive structure of the ring is $\mathbb{Z}_2^4$. In fact, the possibilities for the additive structure are $\mathbb{Z}_2^4, \mathbb{Z}_4 \times \mathbb{Z}_2^2, \mathbb{Z}_8 \times \mathbb{Z}_2$ and $\mathbb{Z}_{16}$.

The following lemma is immediate noting the units in a local ring are the elements not in the maximal ideal.

**Lemma 2.1.** Let $R$ be a local Frobenius ring of order 16. Any element $a + bu + cv + dw$ in $R$ is a unit if and only if $a = 1$.

The following Gray map was defined in [7]:

$$\phi : R \to \mathbb{F}_2^3$$

with $\phi(a + bu + cv + dw) = (d, c + d, b + d, a + b + c + d)$. Note that $\phi$ is a weight preserving map.

This map is formed by taking the classical Gray map for local Frobenius rings of order 4 and applying it recursively. That is, for $\mathbb{Z}_4$ and $\mathbb{F}_2 + u\mathbb{F}_2$, we have the standard Gray map $\phi_1$, with

$$\phi_1(a + bx) = (b, a + b)$$

where $x = 2$ for $\mathbb{Z}_4$ and $x = u$ for $\mathbb{F}_2 + u\mathbb{F}_2$. Then applying this map recursively viewing a local Frobenius ring of order 16 as having $x = u$ for $\phi_1$ and $x = v$ for $\phi_2$ we have the map as defined above.

The following theorem appears in [7].

**Theorem 2.2.** If $C$ is a linear code over $R$, where $R$ is a local Frobenius ring of order 16, of length $n$, size $2^k$ and minimum Lee weight $d$, then $\phi(C)$ is a binary code of length $4n$, size $2^k$ and minimum weight $d$. 

3. Cyclic codes over local Frobenius rings of order 16

In this section, we study the structure of cyclic codes over local Frobenius non-chain rings of order 16. Let \( R \) be a local Frobenius non-chain ring of order 16. A cyclic shift on \( R^n \) is the permutation \( \tau \) defined by

\[
\tau(c_0, c_1, \ldots, c_{n-1}) = (c_{n-1}, c_0, \ldots, c_{n-2}).
\]

A linear code over \( R \) is said to be a cyclic code if it is invariant under the cyclic shift. Any codeword \( c = (c_0, c_1, \ldots, c_{n-1}) \) in \( R^n \) corresponds in the usual way to a polynomial \( c(x) = c_0 + c_1x + \ldots + c_{n-1}x^{n-1} \) in \( R[x] \).

If we consider our polynomials as elements of the ring

\[
\mathbb{R}_n = R[x]/\langle x^n - 1 \rangle,
\]

then \( xc(x) \mod x^n - 1 \) represents the cyclic shift of \( c \). The next theorem follows in the usual way from this discussion.

**Theorem 3.1.** Let \( R \) be a local Frobenius ring of order 16. Then cyclic codes over \( R \) correspond to ideals in \( R[x]/\langle x^n - 1 \rangle \).

In order to understand cyclic codes over \( R \) we shall study the ideals in the ring \( \mathbb{R}_n = R[x]/\langle x^n - 1 \rangle \). Throughout we shall assume \( n \) to be odd so that \( \gcd(n, \text{char}(R)) = 1 \).

3.1. The ring \( \mathbb{R}_n \). Let \( R \) be a local Frobenius ring of order 16. If \( R \) is a finite chain ring and \( n \) is relatively prime to the characteristic of \( R \), then \( R[x]/\langle x^n - 1 \rangle \) is a principal ideal ring (\[5\]).

If \( R \) is not a chain ring then the ring has non-principal ideals. This gives the following lemma.

**Lemma 3.2.** Let \( R \) be a local Frobenius non-chain ring of order 16. Then the ring \( \mathbb{R}_n = R[x]/\langle x^n - 1 \rangle \) is not a principal ideal ring.

For the characterization of units and non-units in \( \mathbb{R}_n \), we will use a group ring representation of the ring \( \mathbb{R}_n \).

Let \( G = (g) \) be the cyclic group of order \( n \) and \( RG \) be the group ring where \( R \) is a local Frobenius ring of order 16 and \( \mathbb{R}_n = R[x]/\langle x^n - 1 \rangle \). We can write \( \mathbb{R}_n \cong RG \) where we map \( a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \) to \( a_0 + a_1g + \cdots + a_{n-1}g^{n-1} \). By following the results given in \[11\], every element in \( RG \) corresponds a circulant matrix in the form:

\[
\sigma(a_0 + a_1x + \cdots + a_{n-1}x^{n-1}) = \begin{pmatrix}
a_0 & a_1 & a_2 & \cdots & a_{n-1} \\
a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
a_1 & a_2 & a_3 & \cdots & a_0
\end{pmatrix}.
\]

Therefore to every element in \( \mathbb{R}_n \), there is a corresponding circulant matrix in the form given above.

By the above description, we can characterize the units and zero divisors in \( \mathbb{R}_n \). Note that the determinant function \( \text{det} \) is a multiplicative map from matrices over a commutative ring \( R \) to the ring \( R \). See \[11\] for a complete description. An element \( \alpha \in \mathbb{R}_n \) is a unit if and only if \( \text{det}(\sigma(\alpha)) \) is a unit in \( R \). We can write this statement as a corollary.
Corollary 3.3. Let $R$ be a local Frobenius non-chain ring of order 16. An element 
$\alpha = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$ is a unit in $R$ if and only if $\det(\sigma(\alpha))$ is a unit in $R$. Hence, $\alpha$ is a non-unit in $R$ if and only if $\det(\sigma(\alpha)) \in m$, where $m$ is the maximal ideal of the ring $R$.

3.2. The structure of cyclic codes over local Frobenius non-chain rings of order 16. Let $R$ be a local Frobenius ring of order 16. We introduce a canonical map which is a homomorphism from $R$ to $F_2$ and study cyclic codes by using this map. We study the case when the length $n$ is odd.

Recall that any element in $R$ has a unique representation as $a + bu + cv + dw$ and that $\mu : R \rightarrow R/m \cong F_2$, where $m$ is the maximal ideal of the ring $R$, is the canonical map defined by $\mu(a + bu + cv + dw) = a$. We can extend the map $\mu$ so that it is defined from the ring of polynomials over $R$ to the ring of polynomials over $F_2$. It is easy to see that the kernel of $\mu$ is the maximal ideal $m$ of the ring $R$. This implies that if $f(x) \in F_2[x]$, there is a polynomial $g(x) \in R[x]$ such that $\mu(g(x)) = f(x)$. Moreover, any two such polynomials $g(x)$ and $h(x)$ which map to $f(x)$ differ by an element $\alpha s_1(x) + \beta v s_2(x) + \gamma w s_3(x)$, where $s_i(x) \in R[x], i \in \{1, 2, 3\}$ and $u, v, w \in m$.

Two polynomials, $f(x)$ and $g(x)$, in $R[x]$ are said to be coprime if $\langle f(x) \rangle + \langle g(x) \rangle = R[x]$. If a ring $R$ is local, then the polynomial ring $R[x]$ may not be a unique factorization domain. However, regular polynomials have the unique factorization property, where a polynomial is said to be regular if it is not a zero divisor in that ring.

Lemma 3.4. Let $R$ be a local Frobenius non-chain ring of order 16. Then $1 + us_1(x) + vs_2(x) + ws_3(x)$ is a unit in $R[x]$, where $s_i(x) \in R[x], i \in \{1, 2, 3\}$ and $u, v, w \in m$.

Proof. Any element $\beta$ in the maximal ideal of a local Frobenius non-chain ring of order 16 satisfies the property that $\beta^4 = 0$. Let $\alpha = 1 + us_1(x) + vs_2(x) + ws_3(x)$ and $\alpha' = (1 + us_1(x) + vs_2(x) + ws_3(x))^3$. Then $\alpha \alpha' = 1 + u^4 s_1^4(x) + v^4 s_2^4(x) + w^4 s_3^4(x) + 2(u^2 s_1^2(x) + v^2 s_2^2(x) + w^2 s_3^2(x)) + u^2 s_1^2(x) v^2 s_2^2(x) + u^2 s_1^2(x) w^2 s_3^2(x) + v^2 s_2^2(x) w^2 s_3^2(x)$.

It can be easily seen that the right side of the equality is equal to 1 for all local Frobenius non-chain rings of order 16, by noticing that each term other than 1 is either 0 because it is the fourth power of an element in the maximal ideal, which is always 0, or is 2 times something in the socle which has characteristic 2. Hence $\alpha'$ is the inverse of $\alpha$ in $R$, so $\alpha$ is a unit.

Lemma 3.5. Two regular polynomials $f(x)$ and $g(x)$ in $R[x]$ are coprime if and only if $\mu(f(x))$ and $\mu(g(x))$ are coprime.

Proof. If $f(x)$ and $g(x)$ are coprime then there exist polynomials $f'(x)$ and $g'(x)$ in $R[x]$ such that $f(x) f'(x) + g(x) g'(x) = 1$ and so $\mu(f(x)) \mu(f'(x)) + \mu(g(x)) \mu(g'(x)) = 1$, with $\mu(f(x)) \neq 0$ and $\mu(g(x)) \neq 0$ since $f(x)$ and $g(x)$ are regular polynomials. Thus $\mu(f(x))$ and $\mu(g(x))$ are coprime.

Conversely, if $\mu(f(x))$ and $\mu(g(x))$ are coprime then there exist polynomials $f'(x)$ and $g'(x)$ in $R[x]$ such that $f(x) f'(x) + g(x) g'(x) = 1 + us_1(x) + vs_2(x) + ws_3(x)$ where $s_i(x) \in R[x], i \in \{1, 2, 3\}$. Since by Lemma 3.4, $1 + us_1(x) + vs_2(x) + ws_3(x)$ is a unit in $R[x]$, we multiply both sides of the last equation by the inverse of $1 + us_1(x) + vs_2(x) + ws_3(x)$. Then it follows that $f(x)$ and $g(x)$ are coprime.
Definition 1. Let $R$ be a local Frobenius ring of order 16. An ideal $I$ of $R[x]$ is a primary ideal provided $ab \in I$ implies that either $a \in I$ or $b' \in I$ for some positive integer $r$.

In the usual way, we can define a basic irreducible polynomial in a local Frobenius non-chain ring of order 16 as follows.

Definition 2. Let $R$ be a local Frobenius non-chain ring of order 16. A polynomial $f(x)$ in $R[x]$ is basic irreducible if $\mu(f(x))$ is irreducible in $\mathbb{F}_2[x]$. A polynomial $f(x)$ in $R[x]$ is primary if $\langle f(x) \rangle$ is a primary ideal.

In [14], it is proven that any basic irreducible polynomial in a finite ring is primary. Therefore, we have the result in the case for the local Frobenius non-chain rings of order 16.

Lemma 3.6. Let $R$ be a local Frobenius non-chain ring of order 16. If $f(x)$ is basic irreducible polynomial in $R[x]$ then $f(x)$ is primary.

Lemma 3.7. The polynomial $x^n - 1$ is a regular polynomial in $R[x]$.

Proof. Since the polynomial $x^n - 1$ is monic and its coefficients 1 and $-1$ are not elements of the maximal ideal of $R$, it is easy to see that $x^n - 1$ is not a zero divisor in $R[x]$, so it is a unit.

The previous lemma gives the following theorem.

Theorem 3.8. The polynomial $x^n - 1$ has a unique factorization into basic irreducible pairwise coprime polynomials as follows: $x^n - 1 = f_1(x)f_1(x) \cdots f_r(x)$.

The next lemma gives a characterization of the ideals in $R[x]/\langle f(x) \rangle$, where $f(x)$ is a basic irreducible polynomial in $R[x]$.

Lemma 3.9. Let $R$ be a local Frobenius non-chain ring of order 16. If $f(x)$ is a basic irreducible polynomial in $R[x]$ then the possible ideals of $R[x]/\langle f(x) \rangle$ are $\langle 0 \rangle$, $\langle 1 + \langle f(x) \rangle \rangle$, $\langle u + \langle f(x) \rangle \rangle$, $\langle v + \langle f(x) \rangle \rangle$ and $\langle \alpha + \langle f(x) \rangle \rangle$, $\alpha \in \{u, v, u + v, w\}$. That is, the ideals in $R[x]/\langle f(x) \rangle$ are in bijective correspondence with the ideals of $R$.

Proof. Let $I$ be a non-zero ideal of $R[x]/\langle f(x) \rangle$ and let $g(x) + \langle f(x) \rangle \in I$ for some $g(x) \notin \langle f(x) \rangle$. Since $f(x)$ is basic irreducible in $R[x]$ then $\mu(f(x))$ is irreducible in $\mathbb{F}_2[x]$ and so $\gcd(\mu(f(x)), \mu(g(x))) = 1$ or $\langle f(x) \rangle$. If $\gcd(\mu(f(x)), \mu(g(x))) = 1$, by Lemma 3.3 $f(x)$ and $g(x)$ are coprime. Hence there exist polynomials $a(x)$ and $b(x)$ in $R[x]$ such that $f(x)a(x) + g(x)b(x) = 1$. Then $(g(x) + \langle f(x) \rangle)(b(x) + \langle f(x) \rangle) = 1 + \langle f(x) \rangle$. Therefore $g(x) + \langle f(x) \rangle$ is a unit in $I$ and so $I = R[x]/\langle f(x) \rangle$.

On the other hand, if $\gcd(\mu(f(x)), \mu(g(x))) = \mu(f(x))$, then $\mu(f(x))$ divides $\mu(g(x))$ and so there exist polynomials $c(x)$ and $s_i(x), i \in \{1, 2, 3\}$, in $R[x]$ such that $g(x) = f(x)c(x) + us_1(x) + vs_2(x) + ws_3(x)$ and at least for one $i \in \{1, 2, 3\}$, $\gcd(\mu(f(x)), \mu(s_i(x))) = 1$. Multiplying both sides of the last equation by the element $1 + \langle f(x) \rangle$, we get

$$g(x) + \langle f(x) \rangle = us_1(x) + vs_2(x) + ws_3(x) + \langle f(x) \rangle.$$ 

If the equality $\gcd(\mu(f(x)), \mu(s_i(x))) = 1$ is satisfied for $i = 1$ or both $i = 1$ and $i = 3$, then $g(x) + \langle f(x) \rangle \in \langle u + \langle f(x) \rangle \rangle$. If the equality $\gcd(\mu(f(x)), \mu(s_i(x))) = 1$ is satisfied for $i = 2$ or both $i = 2$ and $i = 3$, then $g(x) + \langle f(x) \rangle \in \langle v + \langle f(x) \rangle \rangle$. If it is satisfied for only $i = 3$, then $g(x) + \langle f(x) \rangle \in \langle w + \langle f(x) \rangle \rangle$. Otherwise $g(x) + \langle f(x) \rangle \in \langle u + v + \langle f(x) \rangle \rangle$ or $g(x) + \langle f(x) \rangle \in \langle u + \langle f(x) \rangle, v + \langle f(x) \rangle \rangle$, depending on whether the polynomials $s_i(x), i \in \{1, 2, 3\}$ are equal or not.
Theorem 3.10. Let $\mathbb{R}$ be a ring.

Since the polynomials $f_i(x)$ are basic irreducible and pairwise coprime, it is easy to show that

\[ \langle x^n - 1 \rangle = \langle f_1(x) \rangle \cap \langle f_2(x) \rangle \cap \cdots \cap \langle f_r(x) \rangle. \]

Applying the Chinese Remainder Theorem, we have

\[ \mathbb{R}_n = \mathbb{R}[x]/\langle f_1(x) \rangle \cap \langle f_2(x) \rangle \cap \cdots \cap \langle f_r(x) \rangle \]

\[ \cong \mathbb{R}[x]/\langle f_1(x) \rangle \oplus \mathbb{R}[x]/\langle f_2(x) \rangle \oplus \cdots \oplus \mathbb{R}[x]/\langle f_r(x) \rangle. \]

Thus, if $I$ is an ideal of $\mathbb{R}_n$, then $I = \oplus I_i$, where $I_i$ is an ideal of the ring $\mathbb{R}[x]/\langle f_i(x) \rangle$ for $i = 1, \ldots, r$. By Lemma 3.9, $I_i$ is equal to one of the following ideals: $\langle 0 \rangle$, $\langle 1 + \langle f(x) \rangle \rangle$, $\langle u + \langle f(x) \rangle \rangle$, $\langle u + v + \langle f(x) \rangle \rangle$, $\langle \alpha + \langle f(x) \rangle \rangle$, $\alpha \in \{u, v, u + v, w\}$.

If $I_i = \langle 1 + \langle f(x) \rangle \rangle$, then it corresponds to the ideal $\langle f_i(x) + \langle x^n - 1 \rangle \rangle$ in the ring $\mathbb{R}_n$. If $I_i = \langle u + \langle f(x) \rangle \rangle$, $\langle v + \langle f(x) \rangle \rangle$, then it corresponds to the ideal $\langle u f_i(x) + \langle x^n - 1 \rangle \rangle, v f_i(x) + \langle x^n - 1 \rangle \rangle$. Hence $I$ is a sum of the following ideals,
\[\langle \hat{f}_1(x) + \langle x^n - 1 \rangle \rangle, \langle u \hat{f}_1(x) + \langle x^n - 1 \rangle, v \hat{f}_1(x) + \langle x^n - 1 \rangle \rangle \text{ and } \langle \alpha \hat{f}_1(x) + \langle x^n - 1 \rangle \rangle, \alpha \in \{u, v, u + v, w\}.\]

The following corollary deals with the number of cyclic codes.

**Corollary 3.11.** Let \( R \) be a local Frobenius ring of order 16. If \( x^n - 1 = f_1(x)f_2(x) \cdots f_r(x) \) then the number of cyclic codes over \( R \) of length \( n \), where \( R \) is a chain ring, is \( 3^r \) if \( R/m \) is \( \mathbb{F}_4 \) or \( 5^r \) if \( R/m \) is \( \mathbb{F}_2 \). The number of cyclic codes over \( R \), where \( R \) is a non-chain ring, is \( 7^r \).

**Proof.** Let \( R \) be a local Frobenius ring of order 16. If \( R \) is a chain ring then it has 3 ideals if \( R/m \) is \( \mathbb{F}_4 \) and 5 ideals if \( R/m \) is \( \mathbb{F}_2 \). If \( R \) is a non-chain ring then it has 7 ideals. By the previous theorem the result follows.

As an example of the chain ring case, the ring \( \mathbb{F}_4[x]/\langle x^2 \rangle \) has 3 ideals where as \( \mathbb{Z}_{16} \) has 5 ideals.

For the rest of the paper, we choose to write the ideals of \( \mathbb{R}_n = R[x]/\langle x^n - 1 \rangle \) dropping the residue part \( \langle x^n - 1 \rangle \). For simplicity we often write the polynomial \( f(x) \) more simply as \( f \).

Let \( x^n - 1 = f_1(x)f_2(x) \cdots f_r(x) \) be the unique factorization of \( x^n - 1 \) into a product of monic basic irreducible pairwise coprime polynomials. Define the following polynomials for integers \( k_i \) with \( \sum k_i = r \):

\[
\begin{align*}
\hat{F}_1 &= f_1f_2 \cdots f_k f_{k+1} \cdots f_r, \\
\hat{F}_2 &= f_1f_2 \cdots f_{k+1} f_{k+2} \cdots f_r, \\
\hat{F}_3 &= f_1f_2 \cdots f_{k+2} f_{k+3} \cdots f_r, \\
\hat{F}_4 &= f_1f_2 \cdots f_{k+3} f_{k+4} \cdots f_r, \\
\hat{F}_5 &= f_1f_2 \cdots f_{k+4} f_{k+5} \cdots f_r, \\
\hat{F}_6 &= f_1f_2 \cdots f_{k+5} f_{k+6} \cdots f_r.
\end{align*}
\]

The next theorem discusses the generators of a cyclic code over a local Frobenius non-chain ring of order 16.

**Theorem 3.12.** Let \( R \) be a local Frobenius non-chain ring of order 16. Let \( C \) be a cyclic code of length \( n \) over \( R \). Then there exists a unique family of pairwise coprime monic polynomials \( F_i \), \( i \in \{0, 1, 2, 3, 4, 5, 6\} \), such that \( F_0F_1 \cdots F_6 = x^n - 1 \) and \( C \) is generated by the following \( \{\hat{F}_1, \hat{K}, u\hat{F}_3, v\hat{F}_4, (u + v)\hat{F}_5, w\hat{F}_6\} \) where \( \hat{K} \) is a combination of the generators of \( \langle u\hat{F}_2, v\hat{F}_2 \rangle \) and \( |C| = 2^s \) with \( s = 4\deg F_1 + 3\deg F_2 + 2(\deg F_3 + \deg F_4 + \deg F_5) + \deg F_6 \).

**Proof.** Let \( R \) be a local Frobenius ring of order 16. Let \( x^n - 1 = f_1(x)f_2(x) \cdots f_r(x) \) be the unique factorization of \( x^n - 1 \) into a product of monic basic irreducible pairwise coprime polynomials. By Theorem 3.10 \( C \) is a direct sum of the following ideals, \( \langle \hat{f}_1(x) + \langle x^n - 1 \rangle \rangle, \langle u \hat{f}_1(x) + \langle x^n - 1 \rangle, v \hat{f}_1(x) + \langle x^n - 1 \rangle \rangle \) and \( \langle \alpha \hat{f}_1(x) + \langle x^n - 1 \rangle \rangle, \alpha \in \{u, v, u + v, w\} \). By reordering, we can suppose that \( C \) is a sum of

\[
\begin{align*}
\langle \hat{f}_{k_1+1} \rangle, \langle \hat{f}_{k_1+2} \rangle, \cdots, \langle \hat{f}_{k_1+k_2} \rangle; \langle u \hat{f}_{k_1+k_2+1}, v \hat{f}_{k_1+k_2+1} \rangle, \cdots; \langle u \hat{f}_{k_1+k_2+k_3+1} \rangle, \cdots; (u + v) \langle \hat{f}_{k_1+k_2+k_3+k_4} \rangle; (u + v) \langle \hat{f}_{k_1+k_2+k_3+k_4} \rangle; \langle w \hat{f}_{k_1+k_2+k_3+k_4} \rangle; \langle w \hat{f}_{k_1+k_2+k_3+k_4} \rangle; \langle w \hat{f}_{k_1+k_2+k_3+k_4} \rangle; \cdots; \langle w \hat{f}_{k_1+k_2+k_3+k_4} \rangle.
\end{align*}
\]
Then
\[ C = \langle f_1 f_2 \cdots f_k, f_{k+1}, \ldots, f_r, \tilde{K}, u f_1 f_2 \cdots f_k, f_{k+1}, \ldots, f_r, v f_1 f_2 \cdots f_k, f_{k+1}, \ldots, f_r, (u+v) f_1 f_2 \cdots f_k, f_{k+1}, \ldots, f_r \rangle, \]
\[ \langle u f_1, f_2, \ldots, f_r, v f_1, f_2, \ldots, f_r, (u+v) f_1, f_2, \ldots, f_r \rangle. \]
where \( \tilde{K} \) is a combination of the generators of the ideal
\[ \langle u f_1, f_2, \ldots, f_r, v f_1, f_2, \ldots, f_r, (u+v) f_1, f_2, \ldots, f_r \rangle. \]

Then, for \( k = 0 \) and \( 0 \leq i \leq 6 \),
\[ F_i = \begin{cases} 1, & k + 1 = 0; k_i + 1 \neq 0. \end{cases} \]
Therefore, it is clear that
\[ (2) \]
\[ C = \langle \tilde{F}_1, \tilde{K}, u \tilde{F}_3, v \tilde{F}_4, (u+v) \tilde{F}_5, w \tilde{F}_6 \rangle \]
where \( \tilde{K} \) is as defined previously and \( F_0, \ldots, F_6 = x^n - 1 = f_1 \cdots f_r \).

To prove the uniqueness, assume \( H_0, \ldots, H_6 \) are pairwise coprime polynomials in \( R[t] \) such that \( x^n - 1 = H_0 \cdots H_6 \) and \( C = \langle \tilde{H}_1, L, u \tilde{H}_3, v \tilde{H}_4, (u+v) \tilde{H}_5, w \tilde{H}_6 \rangle \)
where \( \tilde{L} \) is a combination of the generators of \( \langle u \tilde{H}_2, v \tilde{H}_2 \rangle \). Therefore \( C = \langle \tilde{H}_1 \rangle + \langle u \tilde{H}_2, v \tilde{H}_2 \rangle + \langle u \tilde{F}_3 \rangle + \langle v \tilde{F}_4 \rangle + \langle (u+v) \tilde{F}_5 \rangle + \langle w \tilde{F}_6 \rangle \). Then there exist non-negative integers \( s_0 = 0, s_1, s_2, \ldots, s_{i+1} \) with \( s_0 + s_1 + \cdots + s_{i+1} = r \) and a permutation \( \{f'_1, f'_2, \ldots, f'_r\} \) of \( \{f_1, f_2, \ldots, f_r\} \) such that \( H_i = f'_{s_0+s_1+\cdots+s_i+1} \cdots f'_{s_0+s_1+\cdots+s_{i+1}} \) for \( i = 0, \ldots, 6 \). Therefore,
\[ C = \langle f'_{s_1+1} \rangle + \cdots + \langle f'_{s_1+s_2} \rangle + \langle u f'_{s_1+s_2+1}, v f'_{s_1+s_2+1} \rangle + \cdots + \langle u f'_{s_1+s_2+s_3}, v f'_{s_1+s_2+s_3} \rangle + \langle u f'_{s_1+s_2+s_3+1} \rangle + \cdots + \langle u f'_{s_1+s_2+s_3+s_4}, v f'_{s_1+s_2+s_3+s_4} \rangle + \langle (u+v) f'_{s_1+s_2+s_3+s_4+1} \rangle + \cdots + \langle (u+v) f'_{s_1+s_2+s_3+s_4+s_5}, v f'_{s_1+s_2+s_3+s_4+s_5} \rangle + \langle (u+v) f'_{s_1+s_2+s_3+s_4+s_5+1} \rangle + \cdots + \langle f'_{s_1+s_2+s_3+s_4+s_5+s_6}, v f'_{s_1+s_2+s_3+s_4+s_5+s_6} \rangle + \cdots + \langle f'_{s_1+s_2+s_3+s_4+s_5+s_6+1} \rangle \]
It follows that \( s_i = k_i \) for \( i = 0, \ldots, 6 \). Furthermore, \( \{f'_{s_0+s_1+\cdots+s_i+1}, \ldots, f'_{s_0+s_1+\cdots+s_{i+1}}\} \) is a permutation of \( \{f_{k_0+\cdots+k_i+1}, \ldots, f_{k_0+\cdots+k_{i+1}}\} \). Therefore, \( H_i = F_i \) for \( i = 0, \ldots, 6 \).

The cardinality of the cyclic code given by (2) is
\[ |C| = 2^{4(n-\deg \tilde{F}_1)+3(n-\deg \tilde{F}_2)+2(n-\deg \tilde{F}_3)+(n-\deg \tilde{F}_4)+(n-\deg \tilde{F}_5)+(n-\deg \tilde{F}_6)} = 2^s. \]
where
\[ s = \sum_{(i,j) \in A} i(\deg (F_j)) \]
with \( A = \{(1,6), (2,3), (2,4), (2,5), (3,2), (4,1)\} \).

**Example 1.** In \( \mathbb{Z}_4[\alpha]/\langle \alpha^2 \rangle \),
\[ x^7 - 1 = (x-1)(x^3 + 2x^2 + x + 3)(x^3 + 3x^2 + 2x + 3) = f_1 f_2 f_3 \]
where \( f_1 = x - 1, f_2 = x^3 + 2x^2 + x + 3 \) and \( f_3 = x^3 + 3x^2 + 2x + 3 \). Let \( F_0 = F_1 = F_2 = F_3 = F_4 = F_5 = 1 \) and \( F_6 = f_2 f_3, F_4 = f_1 \). Consider the cyclic code \( C = \langle \tilde{F}_1, \tilde{K}, u \tilde{F}_3, v \tilde{F}_4, (u+v) \tilde{F}_5, w \tilde{F}_6 \rangle = \langle uf_1, vf_2 f_3 \rangle \), where \( \tilde{K} \) is a combination of the generators of \( \langle u \tilde{F}_2, v \tilde{F}_2 \rangle \). Hence, \( C \) is generated by \( uf_1 + vf_2 f_3 \).

As with cyclic codes over \( R \), where \( R \) is a local Frobenius ring of order 16, we can find generator polynomials of the dual codes. Before studying generators of the dual code, we need to state the following well-known lemma [3].
Lemma 3.13. Let $C$ be a linear code of length $n$ over $R$, where $R$ satisfies $|R| = p^m$. Then $|C| = p^a$ for some integer $a$ and $|C^⊥| = p^b$ with $a + b = nm$.

The next theorem discusses the structure of the generators of the dual code.

Theorem 3.14. Let $(\hat{F}_1, \hat{K}, u\hat{F}_3, v\hat{F}_4, (u+v)\hat{F}_5, w\hat{F}_6)$ be a cyclic code over a local Frobenius non-chain ring of order 16 with $|C| = 2^s$, $s = 4(\deg \hat{F}_1) + 3(\deg \hat{F}_2) + 2((\deg \hat{F}_3) + (\deg \hat{F}_4) + (\deg \hat{F}_5) + (\deg \hat{F}_6))$, where $\hat{K}$ is a combination of the generators of $\langle u\hat{F}_2, v\hat{F}_2 \rangle$ and $x^n - 1 = F_0 \cdots F_6$. Then

$$C^⊥ = \langle \hat{F}_0, \hat{M}^*, u\hat{F}_3^*, v\hat{F}_4^*, (u+v)\hat{F}_5^*, (u+v)\hat{F}_5^*, w\hat{F}_2^* \rangle,$$

where $\hat{F}_i^*$ is the reciprocal polynomial of $\hat{F}_i$, $i = 0, \ldots, 6$, and $\hat{M}^*$ is the reciprocal polynomial of $\hat{M}$, which is a combination of the generators of the ideal $\langle u\hat{F}_6, v\hat{F}_6 \rangle$ and $|C^⊥| = 2^{4\deg \hat{F}_0 + 3\deg \hat{F}_0 + 2(\deg \hat{F}_3 + \deg \hat{F}_4 + \deg \hat{F}_5) + \deg \hat{F}_6}$.

Proof. We assume that $F_i \neq 1$ for all $0 \leq i \leq 6$. Let $D = \langle \hat{F}_0^*, \hat{M}^*, u\hat{F}_3^*, v\hat{F}_4^*, (u+v)\hat{F}_5^*, (u+v)\hat{F}_5^*, w\hat{F}_2^* \rangle$ where $\hat{M}^*$ is the reciprocal polynomial of $\hat{M}$, which is a combination of generators of the ideal $\langle u\hat{F}_6, v\hat{F}_6 \rangle$. First observe that

$$(\alpha \hat{F}_i)(\beta \hat{F}_i^*)^* = 0 \pmod{(x^n - 1)}$$

where $(\alpha, i)$ and $(\beta, j)$ take the values of the following sets $\{(1, 1), (m, 2), (u, 3), (v, 4), (u+v, 5), (w, 6)\}$ and $\{(1, 0), (m, 6), (u, 5), (v, 4), (u+v, 3), (w, 2)\}$, respectively, where $m$ is a combination of the generators of the ideal $\langle u, v \rangle$. Thus, $D \subseteq C^⊥$. Also, $|D| = 2^t$ where

$$t = \sum_{(i,j) \in A_1} i(\deg(F_j)),$$

where $A_1 = \{(1, 2), (2, 3), (2, 4), (2, 5), (3, 6), (4, 0)\}$.

On the other hand, by Lemma 3.13, $|C^⊥| = p^l$ where $l + s = 4n$. By Theorem 3.12

$$s = \sum_{(i,j) \in A_2} i(\deg(F_j)),$$

where $A_2 = \{(1, 6), (2, 3), (2, 4), (2, 5), (3, 2), (4, 1)\}$. It follows that

$$l = \sum_{(i,j) \in A_3} i(\deg(F_j)),$$

where $A_3 = \{(1, 2), (2, 3), (2, 4), (2, 5), (3, 6), (4, 0)\}$. Hence $C^⊥ = D$ and the proof is complete.

3.3. One Generator Cyclic Codes. In this subsection, we describe one generator cyclic codes over a local Frobenius non-chain ring $R$. Let $p(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ be a polynomial in $R[x]$ and $C$ be the cyclic code of length $n$ generated by $p(x)$ in $R_n$. We will assume that $p(x)$ is not a unit, otherwise the cyclic code generated by $p(x)$ would be the trivial code $R^n$. Hence we assume that $p(x)$ is a non-unit in $R_n$.

Recall that the map $\mu : R \to \mathbb{F}_2$ is the canonical map which was defined previously with $\mu(a + bu + cv + dw) = a$. This means that $\mu$ reduces the elements of $R$ modulo $u, v$. The function $\mu$ maps every unit in $R$ to 1, and every non-unit to 0. Since $\mu$ is a ring homomorphism, we can write

$$det(\sigma(\mu(p(x)))) = \mu(det(\sigma(p(x))))$$.
It can be seen easily that \( \sigma(\mu(p(x))) \) is a matrix with entries 0 or 1. Then, any element \( p(x) \) is a non-unit in \( \mathbb{R}_n \) if and only if \( \sigma(\mu(p(x))) \) is a singular matrix. Hence, \( p(x) \) generates a non-trivial cyclic code \( C \) over \( R \) if and only if \( \sigma(\mu(p(x))) \) is a singular matrix. Hence the binary cyclic code \( \mu(C) \) generated by \( \mu(p(x)) \) is non-trivial. Then, since \( \mu(p(x)) \) is a cyclic code over \( \mathbb{F}_2 \), it is a non-unit in \( \mathbb{F}_2[x]/(x^n-1) \). We know that any polynomial \( \mu(p(x)) \) in \( \mathbb{F}_2[x] \) is a unit in \( \mathbb{F}_2[x]/(x^n-1) \) if and only if \( \gcd(\mu(p(x)), x^n-1) = 1 \). Hence we have proven the following theorem.

**Theorem 3.15.** Let \( p(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \) be a polynomial in \( R[x] \). Then \( \langle p(x) \rangle \) is a non-trivial cyclic code if and only if \( \gcd(\mu(p(x)), x^n-1) \neq 1 \).

4. The binary images of cyclic codes under the Gray map

In this section we study the binary images of cyclic codes under the Gray map. Recall that \( \tau \) is the cyclic shift as defined in Section 3. A code \( C \) is said to be an \( r \)-quasi-cyclic code if it is invariant under \( \tau^r \). Notice that we are not assuming that the code is linear, but rather that it is invariant under \( \tau^r \). We call \( r \) the index of the quasi-cyclic code.

Recall that each element of a local Frobenius non-chain ring \( R \) of order 16 can be written uniquely as \( a + bu + cv + dw \).

Define the map \( \phi : R \rightarrow F_2^4 \) as

\[
\phi(a + bu + cv + dw) = (d, c + d, b + d, a + b + c + d).
\]

Extend the map \( \Phi : R^n \rightarrow F_2^{4n} \) where

\[
\Phi(c_0, c_1, \ldots, c_{n-1}) = (\phi(c_0), \phi(c_1), \ldots, \phi(c_{n-1})).
\]

**Lemma 4.1.** The map \( \phi : R \rightarrow F_2^4 \) is linear if and only if \( \text{char}(R) = 2 \).

**Proof.** We have three rings in this family of rings of characteristic 2, namely

\[
\mathbb{F}_2[u, v]/\langle u^2, v^2 \rangle, \mathbb{F}_2[u, v]/\langle u^2 + v^2, uv \rangle, \mathbb{F}_2[x]/\langle x^2 \rangle.
\]

It can be easily proven that \( \phi \) is linear for these rings.

The map \( \phi : R \rightarrow F_2^4 \) is not a linear map when the characteristic of \( R \) is 4 or 16 since \( \phi(1+3) \neq \phi(1) + \phi(3) \). Also, the map is not linear when \( R = \mathbb{Z}_8[x]/\langle x^2 + 4, 2x \rangle \) since \( \phi(2+6) \neq \phi(2) + \phi(6) \).

**Lemma 4.2.** If \( \tau \) is the cyclic shift, then

\[
\Phi \circ \tau = \tau^4 \circ \Phi.
\]

**Proof.** Take an element \( c \in R^n \), then

\[
(\Phi \circ \tau)(c) = (\phi(c_{n-1}), \phi(c_0), \ldots, \phi(c_{n-2})).
\]

On the other hand we can write

\[
\Phi(c_0, c_1, \ldots, c_{n-1}) = (\phi(c_0), \phi(c_1), \ldots, \phi(c_{n-1}))
\]

where each \( \phi(c_i) \) is of length 4. Then if we apply the cyclic shift four times, we get,

\[
(\tau^4 \circ \Phi)(c) = (\phi(c_{n-1}), \phi(c_0), \ldots, \phi(c_{n-2})).
\]

Hence, we get the proof from (4) and (5).

We have the following theorem.
Theorem 4.3. Let \( R \) be a local Frobenius ring of order 16. Let \( C \) be a cyclic code of length \( n \) over \( R \). Then \( \Phi(C) \) is a 4-quasi-cyclic binary code of length \( 4n \). Moreover, these images are linear when the characteristic of the ring \( R \) is 2.

**Proof.** Since \( C \) is a cyclic code, we have \( \tau(C) = C \) where \( \tau \) is the cyclic shift which is defined above. Apply the map \( \Phi \) to both sides

\[
\Phi(\tau(C)) = \Phi(C).
\]

By the previous lemma, we can write

\[
\Phi(C) = \Phi(\tau(C)) = (\Phi \circ \tau)(C) = \tau^4(\Phi(C)).
\]

This means that \( \Phi(C) \) is invariant under \( \tau^4 \). Hence \( \Phi(C) \) is a 4–quasi-cyclic code.

We shall give some concrete examples of cyclic codes in this setting and summarize our computational results, including optimal codes, in Tables 1, 2, 3 and 4.

**Example 2.** Let \( C \) be the cyclic code of length 23 over \( \mathbb{F}_2[u,v] / \langle u^2 + v^2, uv \rangle \) generated by the polynomial

\[
f(x) = (u + v^2)(x^{22} + x^{15} + x^7) + vx^{21} + (v + v^2)(x^{20} + x^{17}) + (1 + u + v^2)(x^{18} + x^4) + x^{10} + x^{13} + x^6 + x^3 + v^2(x^{14} + x^{11}) + (1 + u)(x^9 + x^8) + (1 + v^2)(x^{12} + x^2 + x + 1) + (u + v + v^2)x^5.
\]

The Gray image of the code is a binary 4-quasi-cyclic \([92, 66, 8]^*\) code. The code \( \phi(C) \) is an optimal linear code with weight distribution:

\[
1 + 3933z^8 + 212152z^{10} + 10786632z^{12} + 375617232z^{14} + 9396110535z^{16} + \cdots.
\]

The automorphism group of \( C \) has order \( 2^2 \times 23 \).

**Example 3.** Let \( C = \langle f(x), g(x) \rangle \) be the cyclic code of length 7 over \( \mathbb{F}_2[u,v] / \langle u^2 + v^2, uv \rangle \) where

\[
f(x) = (v + v^2)(x^6 + 1) + v^2(x^5 + x^2 + x) + ux^4 + (u + v^2)x^3,
\]

\[
g(x) = u(x^6 + x^5) + v^2x^4 + (u + v)x + u + v + v^2.
\]

Then, the Gray image of the code is an optimal binary \([28, 15, 6]^*\) code.

**Example 4.** Let \( R = \mathbb{Z}_4[u] / \langle u^2 - 2 \rangle \) then the ideal

\[
C = \langle u(x^6 + 3x^4 + 2x^3 + 2x^2 + 3x + 1) \rangle
\]

in \( R[x] / \langle x^7 - 1 \rangle \) corresponds to a cyclic code of length 7. The binary image of the code is a \([28, 12, 8]^*\) code which is an optimal linear code. The \( \mathbb{Z}_4 \)-image of the code is a \([14, 4^3, 2^6, 8]\) code and it is the first such code with respect to the online database [1].

**Example 5.** Let \( C \) be the cyclic code of length 3 over \( \mathbb{Z}_8[u] / \langle u^2 - 4, 2u \rangle \) generated by \( f(x) = (2 + u)x^2 + (7 + u)x + 7 \) then the weight distribution of \( C \) is \( 1 + 24z^4 + 18z^6 + 15z^8 + 6z^{10} \). The code \( \phi(C) \) is a \([12, 2^6, 4]^*\) code.
TABLE 1. One-generator cyclic codes over $\mathbb{F}_2[u,v]/\langle u^2 + v^2, uv \rangle$

| $n$  | $f(x)$ | $\phi(C)$ |
|------|--------|-----------|
| 3    | $(0, z_4, z_4)$ | $[12, 2, 8]^*_2$ |
| 3    | $(z_7, z_2, z_8)$ | $[12, 4, 6]^*_2$ |
| 3    | $(z_1, z_8, z_6)$ | $[12, 6, 4]^*_2$ |
| 3    | $(y_7, y_5, y_2)$ | $[12, 8, 3]^*_2$ |
| 5    | $(z_7, z_2, z_2, z_7, z_1)$ | $[20, 8, 8]^*_2$ |
| 5    | $(y_4, y_1, y_3, y_2, y_5)$ | $[20, 12, 4]^*_2$ |
| 7    | $(z_4, z_1, z_4, z_1, z_4, z_4)$ | $[28, 3, 16]^*_2$ |
| 7    | $(z_7, z_5, z_7, z_6, z_5, z_1)$ | $[28, 6, 12]^*_2$ |
| 7    | $(z_6, z_5, z_6, z_3, z_3, z_5, z_4)$ | $[28, 7, 12]^*_2$ |
| 7    | $(z_7, z_2, z_2, z_4, z_5, z_7, z_4)$ | $[28, 8, 10]^*_2$ |
| 7    | $(z_5, z_2, z_2, z_4, z_7, z_4)$ | $[28, 12, 8]^*_2$ |
| 7    | $(y_1, y_1, y_4, z_2, y_6, z_8, z_5)$ | $[28, 19, 4]^*_2$ |
| 7    | $(y_2, y_4, y_4, z_8, y_1, z_5, z_1)$ | $[28, 20, 4]^*_2$ |
| 9    | $(z_8, z_8, z_3, z_4, z_3, z_6, z_2, z_5, z_3)$ | $[36, 16, 8]^*_2$ |
| 9    | $(y_7, z_6, y_2, y_5, z_1, y_8, y_2, z_1, y_8)$ | $[36, 20, 6]^*_2$ |
| 15   | $(z_6, z_3, z_4, z_1, z_4, z_6, z_7, z_5, z_7, z_1, z_3, z_6, z_3, z_4, z_7)$ | $[60, 20, 10]^*_2$ |
| 15   | $(z_4, y_7, z_7, z_1, y_5, z_5, z_3, y_8, z_8, z_6, y_4, z_2, z_3, z_6, z_7)$ | $[60, 50, 4]^*_2$ |
| 17   | $(z_7, z_1, z_2, z_8, y_2, y_7, y_7, z_1, z_3, y_2, y_3, z_6, z_3, y_4, y_4, z_1, z_6)$ | $[68, 48, 6]^*_2$ |
| 21   | $(z_4 y_1 y_8 z_3 y_2 z_3 z_2 z_2 y_2 y_2 y_2 y_2 y_2 y_8 z_1 z_2 y_3 y_6 y_1 z_6 z_1)$ | $[84, 58, 8]^*_2$ |
| 21   | $(y_2 y_6 y_4 y_7 y_5 z_8 z_3 z_1 z_5 y_8 y_4 z_4 y_3 z_2 z_3 z_7 z_4 z_6 z_8 z_3 y_8)$ | $[84, 62, 6]^*_2$ |
| 21   | $(y_2 z_2 z_6 y_8 z_3 y_1 y_3 z_1 z_6 z_8 z_2 y_1 z_7 z_2 y_1 y_4 z_8 y_5 z_7)$ | $[84, 72, 4]^*_2$ |
| 23   | $(y_4 y_4 y_4 y_6 z_8 y_1 z_6 y_2 y_2 z_1 z_4 y_1 z_4 z_6 y_1 z_7 z_6 z_1 z_7 z_3 z_6)$ | $[92, 66, 8]^*_2$ |

Example 6. The cyclic code of length 7 over $\mathbb{Z}_{16}$ generated by

$$f(x) = 8x^5 + 2x^4 + 10x^3 + 6x^2 + 12x + 10$$

is of type $16^683^40^20$. A generator matrix in standard form is

$$\begin{bmatrix}
2I_3 & 2 & 4 & 14 & 10 \\
6 & 14 & 14 & 12 \\
4 & 14 & 10 & 2
\end{bmatrix}.$$

The weight enumerator of the code is

$$1 + 84x^{10} + 42x^{12} + 280x^{14} + 7x^{16} + 84x^{18} + 14x^{20}.$$ 

The binary image of the code is a $(28, 20, 10)^*_2$ code that has the same minimum distance as the corresponding optimal binary linear code.

For the following tables a polynomial $f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_2x^2 + a_1x + a_0$ is abbreviated as $(a_0, a_1, a_2, \ldots, a_{n-2}, a_{n-1})$. Throughout the tables, the symbols * and b denote that the corresponding binary code is optimal or the best known code with respect to the online database of linear codes [9].

In order to fit the upcoming tables regarding the results, we label the elements of $\mathbb{F}_2[u,v]/\langle u^2 + v^2, uv \rangle$ as follows:
Table 1. These codes are the first quasi-cyclic codes of these parameters with respect to the online database [4].

Table 2. Two-generator cyclic codes over $\mathbb{F}_2[u,v] / \langle u^2 + v^2, uv \rangle$

Table 3. These codes are the first quasi-cyclic codes of these parameters which are the best known quasi-cyclic code with respect to the online database [4].

Some examples of cyclic codes over the ring $\mathbb{Z}_4[u] / \langle u^2 - 2 \rangle$ are given in Table 3. Every element can be expressed as $a + bu$, $a, b \in \mathbb{Z}_4$. In order to fit the table $a + bu$ is expressed as $ab$.

### REFERENCES

[1] N. Aydin and T. Asamov, A database of $\mathbb{Z}_4$-codes, available at [http://www.asamov.com/Z4Codes](http://www.asamov.com/Z4Codes)

[2] A. Bonnecaze and P. Udaya, Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$ Des. Codes Cryptogr., 42 (2007), 273–287.
### Table 3. Some cyclic codes over $\mathbb{Z}_4[u] / \langle u^2 - 2 \rangle$

| $n$  | $f(x)$          | $\phi_{\mathbb{Z}_4}(C)$     | $\phi(C)$             |
|------|-----------------|--------------------------------|-----------------------|
| 3    | (00)02|202   | (3, 4$^2$2, 8)                  | 12, 2, 8$^2$        |
| 3    | (03)03|003   | (3, 4$^2$2, 6)                  | 12, 3, 6$^2$        |
| 3    | (01)00|012   | (3, 4$^2$2, 6)                  | 12, 7, 4$^2$        |
| 5    | (21)21|212121 | (10, 4$^3$2, 10)                | 20, 3, 10$^2$       |
| 5    | (01)22|01012  | (10, 4$^2$2, 4)                 | 20, 212, 4$^2$      |
| 5    | (03)21|21200  | (10, 4$^2$2, 4)                 | 20, 13, 4$^2$       |
| 7    | (00)02|00202  | (14, 4$^2$2, 8)                 | 28, 3, 16$^2$       |
| 7    | (23)21|212321 | (14, 4$^2$2, 8)                 | 28, 6, 12$^2$       |
| 7    | (22)23|00123  | (14, 4$^2$2, 8)                 | 28, 12, 8$^2$       |
| 7    | (11)13|230223 | (14, 4$^2$2, 8)                 | 28, 215, 6$^2$      |
| 7    | (23)00|3011   | (14, 4$^2$2, 4)                 | 28, 219, 4$^2$      |
| 7    | (33)30|11220  | (14, 4$^2$2, 4)                 | 28, 221, 4$^2$      |
| 7    | (32)01|33112  | (14, 4$^2$2, 4)                 | 28, 222, 4$^2$      |
| 9    | (33)23|320332 | (18, 4$^2$10, 4)                | 36, 226, 4$^2$      |
| 9    | (12)02|113221 | (18, 4$^2$10, 4)                | 36, 227, 4$^2$      |
| 17   | (02)20|013032 | (34, 4$^2$24, 4)                | 68, 257, 4$^2$      |

### Table 4. Some cyclic codes over $\mathbb{Z}_{16}$

| $n$  | $f(x)$ | $C$   | $\phi(C)$ |
|------|--------|-------|-----------|
| 3    | (8, 8, 0) | 3, 2$^4$, 8 | (12, 2$^4$, 8)$^2$ |
| 3    | (6, 6, 6) | 3, 2$^4$, 6 | (12, 2$^4$, 6)$^2$ |
| 3    | (12, 4, 8) | 3, 2$^4$2$^4$, 4 | (12, 2$^4$, 4)$^2$ |
| 3    | (4, 6, 6) | 3, 2$^4$, 4 | (12, 2$^4$, 4)$^2$ |
| 3    | (2, 2, 4) | 3, 2$^4$2$^4$, 4 | (12, 2$^4$, 4)$^2$ |
| 3    | (11, 3, 12) | 5, 2$^4$, 4 | (12, 2$^4$, 4)$^2$ |
| 5    | (14, 10, 6, 12) | 5, 2$^4$, 4 | (20, 2$^4$, 4)$^2$ |
| 5    | (12, 14, 8, 4, 2) | 5, 2$^4$2$^4$, 4 | (20, 2$^4$, 4)$^2$ |
| 5    | (13, 6, 7, 10, 12) | 5, 2$^4$2$^4$, 4 | (20, 2$^4$, 4)$^2$ |
| 5    | (7, 5, 3, 11, 14) | 5, 2$^4$2$^4$, 4 | (20, 2$^4$, 4)$^2$ |
| 7    | (10, 12, 6, 10, 2, 8, 0) | 7, 2$^4$, 10 | (28, 2$^4$, 10)$^2$ |
| 7    | (7, 2, 12, 6, 12, 14, 6) | 7, 2$^4$2$^4$, 8 | (28, 2$^4$, 8)$^2$ |
| 7    | (13, 11, 7, 13, 1, 5, 7) | 7, 2$^4$2$^4$, 8 | (28, 2$^4$, 8)$^2$ |
| 7    | (1, 4, 14, 7, 11, 7, 4) | 7, 2$^4$2$^4$, 8 | (28, 2$^4$, 8)$^2$ |

---

[3] A. R. Calderbank and N. J. A. Sloane, Modular and $p$-adic cyclic codes, *Des. Codes Cryptogr.*, 6 (1995), 21–35.

[4] E. Z. Chen, A database of quasi-twisted codes, available at [http://moodle.tec.hkr.se/~chen/research/codes](http://moodle.tec.hkr.se/~chen/research/codes)

[5] H. Q. Dinh and S. Lopez-Permouth, Cyclic and negacyclic codes over finite chain rings, *IEEE Trans. Inform. Theory*, 50 (2004), 1728–1744.

[6] S. T. Dougherty, S. Karadeniz and B. Yildiz, Cyclic codes over $R_k$, *Des. Codes Cryptogr.*, 63 (2012), 113–126.
[7] S. T. Dougherty, E. Salturk and S. Szabo, Codes over local rings of order 16 and binary codes, Adv. math. Comm., 10 (2016), 379 - 391.
[8] S. T. Dougherty, E. Salturk and S. Szabo, On codes over local rings: generator matrices, generating characters and MacWilliams identities, submitted.
[9] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, available at http://codetables.de
[10] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes, IEEE Trans. Inform. Theory, 40 (1994), 301–319.
[11] T. Hurley, Group rings and rings of matrices, Int. J. Pure Appl. Math., 3 (2006), 319–335.
[12] P. Kanwar and S. Lopez-Permouth, Cyclic codes over the integers modulo $p^m$, Finite Fields Appl., 3 (1997), 334–352.
[13] E. Martinez-Moro and S. Szabo, On codes over local Frobenius non-chain rings of order 16, Contemp. Math., to appear.
[14] B. R. McDonald, Finite Rings with Identity, Dekker, New York, 1974.
[15] V. Pless, P. Solé and Z. Qian, Cyclic self-dual $\mathbb{Z}_4$-codes, Finite Fields Appl., 3 (1997), 48–69.
[16] E. Prange, Cyclic Error-Correcting Codes in Two Symbols, Air Force Cambridge Research Center 1957.
[17] J. Wolfmann, Negacyclic and cyclic codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory, 45 (1999), 2527–2532.
[18] B. Yildiz and S. Karadeniz, Cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, Des. Codes Cryptogr., 58 (2011), 221–234.

Received for publication June 2015.

E-mail address: prof.steven.dougherty@gmail.com
E-mail address: abidin.kaya@bou.edu.tr
E-mail address: esengulsalturk@gmail.com