CYCLIC CODES OVER $\mathbb{Z}_4 + u\mathbb{Z}_4$

Rama Krishna Bandi
Department of Mathematics
Indian Institute of Technology Roorkee
Roorkee-247667, INDIA

Maheshanand Bhaintwal
Department of Mathematics
Indian Institute of Technology Roorkee
Roorkee-247667, INDIA

(Communicated by the associate editor name)

Abstract. In this paper, we have studied cyclic codes over the ring $R = \mathbb{Z}_4 + u\mathbb{Z}_4$, $u^2 = 0$. We have considered cyclic codes of odd lengths. A sufficient condition for a cyclic code over $R$ to be a $\mathbb{Z}_4$-free module is presented. We have provided the general form of the generators of a cyclic code over $R$ and determined a formula for the ranks of such codes. In this paper we have mainly focused on principally generated cyclic codes of odd length over $R$. We have determined a necessary condition and a sufficient condition for cyclic codes of odd lengths over $R$ to be $R$-free.

1. Introduction. Cyclic codes are amongst the most studied algebraic codes. Their structure is well known over finite fields [7]. Recently codes over rings have generated a lot of interest after a breakthrough paper by Hammons et al. [5] showed that some well known binary non-linear codes are actually images of some linear codes over $\mathbb{Z}_4$ under the Gray map. Since then, cyclic codes have also been extensively studied over various finite rings. Their structure over finite chain rings is now well known [9]. They have also been studied over other rings such as $\mathbb{F}_2 + u\mathbb{F}_2$, $u^2 = 0$, [3]; $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, $u^2 = v^2 = 0, uv = vu$, [12]; and $\mathbb{F}_2 + v\mathbb{F}_2$, $u^2 = v$, [13].

Bonnecaze and Udaya [3] have studied cyclic codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2$, $u^2 = 0$, and provided their basic framework. The ring $\mathbb{F}_2 + u\mathbb{F}_2$ is useful because it shares many properties of $\mathbb{Z}_4$, and since it has characteristic 2, it also shares properties of the field $\mathbb{F}_4$. In most of these studies length of the cyclic code is relatively prime to the characteristic of the ring. A complete structure of cyclic codes over $\mathbb{Z}_4$ of odd length has been given in [10] and [6].

In this paper, we have studied cyclic codes over the ring $R = \mathbb{Z}_4 + u\mathbb{Z}_4$, $u^2 = 0$. We have considered cyclic codes of odd lengths. Recently, Yildiz and Karadeniz [11] have studied linear codes over $R$. A linear code $C$ over $R$ can be expressed as $C = C_1 + uC_2$, where $C_1, C_2$ are linear codes over $\mathbb{Z}_4$. As usual, a cyclic code of length $n$ over $R$ is an ideal of $R_n = \frac{R[x]}{x^n - 1}$. We have shown that a linear code $C = C_1 + uC_2$ of length $n$ over $R$ is a cyclic code if and only if $C_1, C_2$ are cyclic codes.
of length \(n\) over \(\mathbb{Z}_4\). We have determined a sufficient condition for a cyclic code of odd length over \(R\) to be a \(\mathbb{Z}_4\)-free module. We have provided the general form of the generators of a cyclic code over \(R\), from which we have determined a formula for the ranks of such codes. The ring \(R_n\) is in general not a principal ideal ring, and so a cyclic code over \(R\) is in general not principally generated. In this paper we have mainly focused on cyclic codes of odd length over \(R\) which are principally generated. We have determined a necessary condition and a sufficient condition for principally generated cyclic codes of odd lengths over \(R\) to be \(R\)-free.

The paper is organized as follows: In Section II, we present the preliminaries. In Section III, we have discussed the Galois extensions of \(R\) and the ideal structure of these extensions. In Section IV, we have studied cyclic codes of odd length over \(R\). The forms of the ranks and minimal spanning sets of these codes are presented. In Section V, we have mainly focused to principally generated cyclic codes of odd length over \(R\) and determined a necessary condition and a sufficient condition for cyclic codes over \(R\) to be \(R\)-free. We have also expressed principally generated cyclic codes in terms of the \(n^{th}\) roots of unity.

2. Preliminaries. Throughout the paper, \(R\) denotes the ring \(\mathbb{Z}_4 + u\mathbb{Z}_4 = \{a + ub \mid a, b \in \mathbb{Z}_4\}\) with \(u^2 = 0\). \(R\) can be viewed as the quotient ring \(\mathbb{Z}_4[u]/\langle u^2\rangle\). The units of \(R\) are

\[
1, 3, 1 + u, 1 + 2u, 1 + 3u, 3 + u, 3 + 2u, 3 + 3u ,
\]

and the non-units are

\[
0, 2, u, 2u, 2 + u, 2 + 2u, 3u, 2 + 3u .
\]

\(R\) has six ideals in all: \(\{0\}, \langle u \rangle = \{0, u, 2u, 3u\}, \langle 2 \rangle = \{0, 2, 2u, 2 + u\}, \langle 2u \rangle = \{0, 2u\}, \langle 2 + u \rangle = \{0, 2 + u, 2u, 2 + 3u\}\) and \(\langle 2, u \rangle = \{0, 2, 2u, 3u, 2 + u, 2 + 2u, 2 + 3u\}\).

\(R\) is a local ring of characteristic 4 with \(\langle 2, u \rangle\) as its unique maximal ideal. A commutative ring \(R\) is called a chain ring if its ideals form a chain under the relation of inclusion. From the ideals of \(R\), we can see that they do not form a chain; for instance, the ideals \(\langle u \rangle\) and \(\langle 2 \rangle\) are not comparable. Therefore, \(R\) is a non-chain extension of \(\mathbb{Z}_4\). Also \(R\) is not a principal ideal ring; for example, the ideal \(\langle 2, u \rangle\) is not generated by any single element of \(R\).

We denote the residue field \(R/\langle 2, u \rangle\) of \(R\) by \(\overline{R}\). Since \(\{0 + \langle 2, u \rangle\} \cup \{1 + \langle 2, u \rangle\} = R\), therefore \(\overline{R} \equiv \mathbb{F}_2\). The image of any element \(a \in R\) under the projection map \(\mu : R \to \overline{R}\) is denoted by \(\overline{a}\). The map \(\mu\) is extended to \(R[x] \to \overline{R}[x]\) in the usual way. The image of an element \(f(x) \in R[x]\) in \(\overline{R}[x]\) under this projection is denoted by \(\overline{f}(x)\). A polynomial \(f(x) \in R[x]\) is called basic irreducible (primitive) if \(\overline{f}(x)\) is an irreducible (primitive) polynomial in \(\overline{R}[x]\). Basic irreducible polynomials over finite local rings play approximately the same role as irreducible polynomials play over finite fields.

A polynomial \(f(x)\) over \(R\) is called a regular polynomial if it is not a zero divisor in \(R[x]\), equivalently, \(f(x)\) is regular if \(\overline{f(x)} \neq 0\). Two polynomials \(f(x), g(x) \in R[x]\) are said to be coprime if there exist \(a(x), b(x) \in R[x]\) such that

\[
a(x)f(x) + b(x)g(x) = 1 .
\]

Now we recall the Hensel’s Lemma and factorization of polynomials in \(\mathbb{Z}_4[x]\). A polynomial \(f(x)\) in \(\mathbb{Z}_4[x]\) is said to be primary if the principal ideal \(\langle f \rangle\) is primary, i.e., whenever \(ab \in \langle f \rangle\), then either \(a \in \langle f \rangle\) or \(b^j \in \langle f \rangle\) for positive integer \(j\).
Theorem 2.1 (Hensel's Lemma [10]). Let \( f \) be a monic polynomial in \( \mathbb{Z}_4[x] \) and assume that \( f \) (mod 2) = \( g_1g_2\cdots g_r \), where \( g_1, g_2, \ldots, g_r \) are pairwise coprime monic polynomials over \( \mathbb{F}_2 \). Then there exist pairwise coprime monic polynomials \( f_1, f_2, \ldots, f_r \) over \( \mathbb{Z}_4 \) such that \( f = f_1f_2\cdots f_r \) in \( \mathbb{Z}_4[x] \) and \( f_i \) (mod 2) = \( g_i \), \( i = 1, 2, \ldots, r \).

A Gray map \( \phi : R^n \to \mathbb{Z}_4^{2n} \) is defined by (see [11])

\[
(\overline{a} + u\overline{b}) \mapsto (\overline{b}, \overline{a} + \overline{b}).
\]

The Lee weight is defined on \( R \) by

\[
w_L(a + ub) = w_L(b, a + b),
\]

where \( w_L(b, a + b) \) is the usual Lee weight of \( (b, a + b) \) in \( \mathbb{Z}_4^2 \). This weight is then extended componentwise to \( R^n \). The Lee weight of an element \( x \in R^n \) is the sum of the Lee weights of the coordinates of \( x \).

Theorem 2.2. [11] The Gray map \( \phi : R^n \to \mathbb{Z}_4^{2n} \) is a distance preserving linear isometry with respect to the Lee weights in \( R^n \) and \( \mathbb{Z}_4^2 \).

A linear code \( C \) of length \( n \) over \( R \) is an \( R \)-submodule of \( R^n \). \( C \) may not be an \( R \)-free module. We can express \( R^n \) as \( R^n = \mathbb{Z}_4^n + u\mathbb{Z}_4^n \), and so a linear code \( C \) of length \( n \) over \( R \) can be expressed as \( C = C_1 + uC_2 \), where \( C_1, C_2 \) are linear codes of length \( n \) over \( \mathbb{Z}_4 \). The Euclidean inner product of any two elements \( x = (x_1, x_2, \ldots, x_n) \) and \( y = (y_1, y_2, \ldots, y_n) \) of \( R^n \) is defined as \( x \cdot y = x_1y_1 + x_2y_2 + \cdots + x_ny_n \), where the operation is performed in \( R \). The dual of a linear code \( C \) is defined as \( C^\perp = \{ y \in R^n \mid x \cdot y = 0 \ \forall x \in C \} \). It follows immediately that if \( C = C_1 + uC_2 \) is a linear code over \( R \), then \( C^\perp = C_1^\perp + uC_2^\perp \). We define the rank of a code \( C \) as the minimum number of generators for \( C \) and the free rank of \( C \) is the rank of \( C \) if \( C \) is a free module over \( R \). There are two other codes associated with \( C \), namely Tor\( (C) \) and Res\( (C) \) and are defined as Tor\( (C) = \{ b \in \frac{\mathbb{Z}_4[x]}{(x^n-1)} : ub \in C \} \) and Res\( (C) = \{ a \in \frac{\mathbb{Z}_4[x]}{(x^n-1)} : a + ub \in C \ \text{for some } b \in \frac{\mathbb{Z}_4[x]}{(x^n-1)} \} \).

3. Galois extension of \( R \). Let \( n \) be an odd integer. We first consider the factorization of \( x^n - 1 \) over \( R \), as it plays a vital role in the study of cyclic codes over \( R \) of length \( n \).

Theorem 3.1. Let \( g(x) \in \mathbb{F}_2[x] \) be a monic irreducible (primitive) divisor of \( x^{2^r-1} - 1 \). Then there exists a unique monic basic irreducible (primitive) polynomial \( f(x) \) in \( R[x] \) such that \( \overline{f(x)} = g(x) \) and \( f(x) \mid (x^{2^r-1} - 1) \) in \( R[x] \).

Proof. Let \( x^{2^r-1} - 1 = g(x)g'(x) \) in \( \mathbb{F}_2[x] \). By Hensel's lemma, there exist \( f(x), f'(x) \in \mathbb{Z}_4[x] \) such that \( x^{2^r-1} - 1 = f(x)f'(x) \) in \( \mathbb{Z}_4[x] \) and \( f(x) \) (mod 2) = \( g(x) \), \( f'(x) \) (mod 2) = \( g'(x) \). Since \( \mathbb{Z}_4 \) is a subring of \( R \), \( f(x) \in R[x] \). Also \( \overline{f(x)} = f(x) \) (mod \( (2, u) \)) = \( g(x) \) and \( f(x) \mid (x^{2^r-1} - 1) \) in \( R[x] \).

We call the polynomial \( f(x) \) in Theorem (3.1) the Hensel lift of \( g(x) \) to \( R \).

Since \( n \) is odd, it follows from [8, Theorem XIII.11] that \( x^n - 1 \) factorizes uniquely into pairwise coprime basic irreducible polynomials over \( R \). Let

\[ x^n - 1 = f_1f_2\cdots f_m \]
be such a factorization of \( x^n - 1 \). Then it follows from the Chinese Remainder Theorem that
\[
\frac{R[x]}{(x^n - 1)} = \bigoplus_{i=1}^{m} \frac{R[x]}{(f_i)}.
\]
Therefore every ideal \( I \) of \( \frac{R[x]}{(x^n - 1)} \) can be expressed as \( I = \bigoplus_{i=1}^{m} I_i \), where \( I_i \) is an ideal of the ring \( \frac{R[x]}{(f_i)} \), \( i = 1, 2, \ldots, m \).

Let us recall the Galois extension of \( \mathbb{Z}_4 \). Let \( h(x) \) be a monic basic irreducible polynomial of degree \( r \) in \( \mathbb{Z}_4[x] \). Then the Galois ring \( GR(4, r) \) over \( \mathbb{Z}_4 \) is defined as the residue class ring \( \frac{\mathbb{Z}_4[x]}{(h(x))} \). The ring \( GR(4, r) \) is a local ring with unique maximal ideal \( (2) \) and the residue field \( \mathbb{F}_2^r \).

Let \( T = \{0, 1, \xi, \xi^2, \ldots, \xi^{2^{r-2}}\} \) be the Teichmüller representatives of \( GR(4, r) \), where \( \xi \) is a root of a basic primitive polynomial of degree \( r \) in \( \mathbb{Z}_4[x] \). Then each element \( a \) of \( GR(4, r) \) can be written as \( a = a_0 + 2a_1 \), where \( a_0, a_1 \in T \). This representation is called the 2-adic representation of elements of \( GR(4, r) \).

Now we consider the Galois extension of \( R \). Let \( f(x) \) be a basic irreducible polynomial of degree \( r \) in \( R[x] \). Then the Galois extension of \( R \) is defined as the quotient ring \( \frac{R[x]}{(f(x))} \) and is denoted by \( GR(R, r) \). If \( \alpha \) is a root of \( f(x) \) then the elements of \( GR(R, r) \) can uniquely be written as \( m_0 + m_1\alpha + m_2\alpha^2 + \cdots + m_{r-1}\alpha^{r-1} \), \( m_i \in R \), \( i = 0, 1, \ldots, r-1 \), i.e., \( GR(R, r) \) is free module of rank \( r \) over \( R \) with a basis \( \{1, \alpha, \alpha^2, \ldots, \alpha^{r-1}\} \) and \( |GR(R, r)| = 16^r \). From Theorem (3.5), it follows that the ring \( GR(R, r) \) is a local ring with unique maximal ideal \( \langle 2, u, \langle f \rangle \rangle \) and the residue field \( \mathbb{F}_2^r \). Furthermore,
\[
GR(R, r) \simeq \frac{GR(4, r)[u]}{\langle u^2 \rangle} \simeq GR(4, r) \oplus uGR(4, r),
\]
where \( GR(4, r) \) is the Galois ring of degree \( r \) over \( \mathbb{Z}_4 \) and \( u^2 = 0 \).

Therefore, an element \( x \) of \( GR(R, r) \) can be represented as \( x = a + ub \), where \( a, b \in GR(4, r) \). Using the 2-adic representation of \( a = a_0 + 2a_1 \), \( b = a_2 + 2a_3 \), \( a_0, a_1, a_2, a_3 \in T \), the element \( x \in GR(R, r) \) can further be represented as \( x = a_0 + 2a_1 + ua_2 + 2ua_3 \).

**Lemma 3.2.** A non-zero element \( x = a_0 + 2a_1 + ua_2 + 2ua_3 \) of \( GR(R, r) \) is unit if and only if \( a_0 \neq 0 \) in \( T \).

**Proof.** Since \( x^4 = a_0^4 \) for every non-zero \( x \) in \( GR(R, r) \), the result follows. \( \square \)

Thus the group of units of \( GR(R, r) \), denoted by \( GR(R, r)^* \), is given by
\[
GR(R, r)^* = \{a_0 + 2a_1 + ua_2 + 2ua_3 : a_0, a_1, a_2, a_3 \in T, a_0 \neq 0\}.
\]

**Theorem 3.3.** The group of units \( GR(R, r)^* \) is a direct product of two groups \( GC \) and \( GA \), i.e., \( GR(R, r)^* = GC \times GA \), where \( GC \) is a cyclic group of order \( 2^r - 1 \) and \( GA \) is an abelian group of order \( 8^r \).

**Proof.** Let \( \xi \) be a primitive element of \( GR(R, r) \) and \( GC = T^* = \{1, \xi, \ldots, \xi^{2^{r-2}}\} \). Then \( GC \) is a multiplicative cyclic group of order \( 2^r \). Let \( x = a_0 + 2a_1 + ua_2 + 2ua_3 \in GR(R, r)^* \). Define a mapping \( \Gamma : GR(R, r)^* \to GC \) such that \( \Gamma(x) = a_0 \). It can easily be seen that for any \( a, x, y \in GR(R, r)^* \), \( \Gamma(ax + y) = \Gamma(a)\Gamma(x) + \Gamma(y) \). \( \Gamma \) is obviously a surjective map. Therefore \( \frac{GR(R, r)^*}{\ker \Gamma} \simeq GC \), where \( \ker \Gamma = \{1 + 2a_1 + ua_2 + 2ua_3 : a_1, a_2, a_3 \in T\} \). Denote \( \ker \Gamma \) by \( GA \). Then it can easily be seen that \( GR(R, r) \simeq GC \times GA \). Moreover, \( |GR(R, r)^*| = |GC| \cdot |GA| = 8^r(2^r - 1) \). \( \square \)
The set of all zero divisors of $GR(R, r)$ is given by \( \{2a_1 + ua_2 + 2ua_3 : a_1, a_2, a_3 \in T\} \), which is maximal ideal generated by \( \langle 2, u \rangle \) in $GR(R, r)$.

Now we consider the ideal structure of $GR(R, r)$. We first prove the following Lemma.

**Lemma 3.4.** Let $f(x), g(x) \in R[x]$. Then $f(x), g(x)$ are coprime if and only if their images $\overline{f}(x), \overline{g}(x)$ are coprime in $R[x]$.

**Proof.** If $f(x), g(x)$ are coprime, then it is immediate that $\overline{f}(x)$ and $\overline{g}(x)$ are coprime. Now suppose that $\overline{f}(x), \overline{g}(x)$ are coprime. Then there exist $a(x), b(x) \in R[x]$ such that

$$\overline{a(x)} \overline{f}(x) + \overline{b(x)} \overline{g}(x) = 1.$$ 

Then there exits $r(x), s(x) \in R[x]$ such that

$$a(x)f(x) + b(x)g(x) = 1 + 2r(x) + us(x) . \quad (1)$$

Multiplying (1) by $2r(x)$ and by $us(x)$, we respectively get equations:

$$2r(x)a(x)f(x) + 2r(x)b(x)g(x) = 2r(x) + 2ur(x)s(x) . \quad (2)$$

$$us(x)a(x)f(x) + us(x)b(x)g(x) = us(x) + 2ur(x)s(x) . \quad (3)$$

On adding (2) and (3), we get

$$a(x)(2r(x) + us(x))f(x) + b(x)(2r(x) + us(x))g(x) = 2r(x) + us(x) . \quad (4)$$

Putting the value of $2r(x) + us(x)$ in (1), we get

$$a(x)(1 - 2r(x) - us(x))f(x) + b(x)(1 - 2r(x) - us(x))g(x) = 1 .$$

Therefore $f(x)$ and $g(x)$ are coprime. \( \square \)

Now we consider the ideals of $R[x]/\langle f \rangle$, where $f$ is a basic irreducible polynomial over $R$.

**Theorem 3.5.** Let $f \in R[x]$ be a basic irreducible polynomial. Then the ideals of $R[x]/\langle f \rangle$ are precisely, \( \{0\}, \langle 1 + \langle f \rangle \rangle, \langle 2 + \langle f \rangle \rangle, \langle u + \langle f \rangle \rangle, \langle 2u + \langle f \rangle \rangle, \langle 2 + u + \langle f \rangle \rangle \) and \( \langle \langle 2, u \rangle + \langle f \rangle \rangle \).

**Proof.** Let $I$ be a non-zero ideal of $R[x]/\langle f \rangle$. Let $h + \langle f \rangle \in R[x]/\langle f \rangle$. Since $f$ is basic irreducible, $\overline{f}$ is irreducible in $\overline{R[x]}$. Therefore $\gcd(\overline{f}, \overline{h}) = 1$ or $\overline{f}$. Let $\gcd(\overline{f}, \overline{h}) = 1$. Then $f$ and $h$ are coprime in $R[x]$, and hence there exist $a_1, a_2 \in R[x]$ such that

$$\lambda_1 f + \lambda_2 h = 1 .$$

From this follows that $\lambda_2 h = 1 \pmod{f}$. Thus $h$ is an invertible element of $R[x]/\langle f \rangle$ and so $I = \langle 1 + \langle f \rangle \rangle = R[x]/\langle f \rangle$.

Now suppose that $\gcd(\overline{f}, \overline{h}) = \overline{f}$. Then there exists polynomials $g, f_1, f_2 \in R[x]$ such that

$$h = fg + 2f_1 + uf_2 ,$$

and $\gcd(\overline{f}, \overline{f_1}) = 1$ or $\gcd(\overline{f}, \overline{f_2}) = 1$. It follows that $h + \langle f \rangle \in \langle \langle 2, u \rangle + \langle f \rangle \rangle$. Therefore if $I \neq \langle 1 + \langle f \rangle \rangle$, then $I \subseteq \langle \langle 2, u \rangle + \langle f \rangle \rangle$. The non-zero ideals contained in $\langle \langle 2, u \rangle + \langle f \rangle \rangle$ are $\langle 2 + \langle f \rangle \rangle, \langle u + \langle f \rangle \rangle, \langle 2u + \langle f \rangle \rangle, \langle 2 + u + \langle f \rangle \rangle$ and $\langle \langle 2, u \rangle + \langle f \rangle \rangle$ itself. The result follows. \( \square \)

The Galois group $\text{Gal}(GR(R, r))$ of $\text{Gal}(R, r)$ is a cyclic group of order $(2^r - 1)$, which is generated by the Frobenius automorphism $\sigma$ on $GR(R, r)$ defined as $\sigma(x) = a_0^2 + 2a_1^2 + ua_2^2 + 2ua_3^2$, where $x = a_0 + 2a_1 + ua_2 + 2ua_3 \in R$. The automorphism $\sigma$ fixes the ring $R$. 
Example 3.6. Consider the basic irreducible polynomial \( h(x) = x^4 + 3x^3 + 2x^2 + 1 \), which is the Hensel lift to \( R \) of the polynomial \( x^3 + x^3 + 1 \in \mathbb{F}_2[x] \). Let \( \xi \) be a root of \( h(x) \). Then
\[
\xi^4 = \xi^3 + 2\xi^2 + 3, \quad \xi^5 = 3\xi^3 + 2\xi^2 + 3\xi + 3, \quad \xi^6 = \xi^3 + \xi^2 + 3\xi + 1, \\
\xi^7 = 2\xi^3 + \xi^2 + \xi + 3, \quad \xi^8 = 3\xi^3 + \xi^2 + \xi, \quad \xi^9 = 3\xi^2 + 3, \\
\xi^{10} = 3\xi^3 + 3\xi, \quad \xi^{11} = 3\xi^3 + \xi^2 + 1, \quad \xi^{12} = 2\xi^2 + \xi + 1, \\
\xi^{13} = 2\xi^3 + \xi^2 + \xi, \quad \xi^{14} = 3\xi^3 + \xi^2 + 2\xi, \quad \xi^{15} = 1.
\]

Let \( \mathcal{T} = \{0, 1, \xi, \xi^2, \xi^3, \xi^3 + 2\xi^2 + 3, 3\xi^3 + 2\xi^2 + 3\xi + 3, \xi^3 + \xi^2 + 3\xi + 1, 2\xi^3 + \xi^2 + \xi + 3, 3\xi^3 + \xi^2 + 3, 3\xi^3 + 3\xi, 3\xi^3 + \xi^2 + 1, 2\xi^2 + \xi + 1, 2\xi^3 + \xi^2 + \xi, 3\xi^3 + \xi^2 + 2\xi \} \). Then \( GR(R, 4) = \{a_0 + 2a_1 + ua_2 + 2ua_3 : a_i \in \mathcal{T}, i = 0, 1, 2, 3 \} \) and \( |GR(R, 4)| = 4^{16} \).

4. Cyclic codes of odd length over \( \mathbb{Z}_4 + u \mathbb{Z}_4 \). We assume that \( n \) is odd throughout this section. For a finite chain ring \( R \), it is well known that the ring \( R[x] / (x^n - 1) \) is a principal ideal ring [9]. However, in the present case the ring \( R \) is not a chain ring and the situation is not as straightforward. In fact, the ring \( R_n = \frac{R[x]}{(x^n - 1)} \) is not in general a principal ideal ring, as the next result shows. The result is a generalization of [12, Lemma 2.4].

**Theorem 4.1.** The ring \( R_n = \frac{R[x]}{(x^n - 1)} \) is not a principal ideal ring.

**Proof.** Consider the augmentation mapping \( \gamma : \frac{R[x]}{(x^n - 1)} \rightarrow R \) defined by
\[
\gamma(a_0 + a_1x + \ldots + a_{n-1}x^{n-1}) = a_0 + a_1 + \ldots + a_{n-1}.
\]
This is a surjective ring homomorphism. Consider now the ideal \( I = \langle 2, u \rangle \) of \( R \), which we know is not a principal ideal. Let \( J = \gamma^{-1}(I) \). It is well known that the inverse image under a homomorphism of an ideal is an ideal. So \( J \) is an ideal of \( \frac{R[x]}{(x^n - 1)} \). Now if we assume \( J \) to be a principal ideal, then its homomorphic image \( I \) must be principal, a contradiction. Hence \( J \) is not a principal ideal and \( \frac{R[x]}{(x^n - 1)} \) is therefore not a principal ideal ring.

Therefore, a cyclic code of length \( n \) over \( R \) is in general not principally generated. Since \( n \) is odd, the ring \( \frac{Z_4[x]}{(x^n - 1)} \) is a principal ideal ring. Therefore a cyclic code of length \( n \) over \( R \) is of the form \( C = C_1 + uC_2 = \langle g_1 \rangle + u \langle g_2 \rangle \), where \( g_1, g_2 \in \mathbb{Z}_4[x] \) are generator polynomials of the cyclic codes \( C_1, C_2 \), respectively.

Let \( \tau \) be the standard cyclic shift operator on \( R^n \). A linear code \( C \) of length \( n \) over \( R \) is cyclic if \( \tau(c) \in C \) whenever \( c \in C \), i.e., if \( \langle c_0, c_1, \ldots, c_{n-1} \rangle \subset C \) then \( \langle c_{n-1}, c_0, c_1, \ldots, c_{n-2} \rangle \subset C \). As usual, in the polynomial representation, a cyclic code of length \( n \) over \( R \) is an ideal of \( \frac{R[x]}{(x^n - 1)} \).

**Theorem 4.2.** Let \( x^n - 1 = f_1f_2 \cdots f_m \), where \( f_i, i = 1, 2, \ldots, m \) are basic irreducible pairwise coprime polynomials in \( R[x] \). Then any ideal in \( R_n \) is the sum of the ideals of \( R[x]/\langle f_i \rangle \), \( i = 1, 2, \ldots, m \).

**Proof.** It follows from the Chinese Remainder Theorem.

**Corollary 1.** The number cyclic codes over \( R \) is \( 7^m \).

**Proof.** Each ideal of \( R_n \) is a direct sum of the ideals of \( R[x]/\langle f_i \rangle \), \( i = 1, 2, \ldots, m \). From Theorem (3.5) and for each \( i \), \( R[x]/\langle f_i \rangle \) has 7 ideals. The result follows.
Theorem 4.3. A linear code $C = C_1 + uC_2$ of length $n$ over $R$ is cyclic if and only if $C_1$, $C_2$ are cyclic codes of length $n$ over $\mathbb{Z}_4$.

Proof. Let $c_1 + uc_2 \in C$, where $c_1 \in C_1$ and $c_2 \in C_2$. Then $\tau(c_1 + uc_2) = \tau(c_1) + u\tau(c_2) \in C$, since $C$ is cyclic and $\tau$ is a linear map. So, $\tau(c_1) \in C_1$ and $\tau(c_2) \in C_2$. Therefore $C_1, C_2$ are cyclic codes. Conversely if $C_1$, $C_2$ are cyclic codes, then for any $c_1 + uc_2 \in C$, where $c_1 \in C_1$ and $c_2 \in C_2$, we have $\tau(c_1) \in C_1$ and $\tau(c_2) \in C_2$, and so, $\tau(c_1 + uc_2) = \tau(c_1) + u\tau(c_2) \in C$. Hence $C$ is cyclic. \hfill $\square$

The following result gives a sufficient condition for a cyclic code $C$ over $R$ to be a free $\mathbb{Z}_4$-code.

Theorem 4.4. Let $C = C_1 + uC_2$ be a cyclic code of length $n$ over $R$. If $C_1$, $C_2$ are free codes over $\mathbb{Z}_4$, then $C$ is a free $\mathbb{Z}_4$-module.

Proof. Suppose that $C_1$, $C_2$ are $\mathbb{Z}_4$-free codes of ranks $k_1$, $k_2$, respectively. Let $\{c_{11}, c_{12}, \ldots, c_{1k_1}\}$ and $\{c_{21}, c_{22}, \ldots, c_{2k_2}\}$ be $\mathbb{Z}_4$-bases of $C_1$ and $C_2$, respectively. Then the set $\{c_{11}, c_{12}, \ldots, c_{1k_1}, uc_{21}, uc_{22}, \ldots, uc_{2k_2}\}$ spans $C$, as every element of $C$ can be expressed as a linear combination of elements of this set. Now suppose there exist scalars $a_i, b_j \in \mathbb{Z}_4$ such that

$$\sum_{i=1}^{k_1} a_i c_{1i} + u \sum_{j=1}^{k_2} b_j c_{2j} = 0.$$ 

Then $\sum_{i=1}^{k_1} a_i c_{1i} = 0$ and $\sum_{j=1}^{k_2} b_j c_{2j} = 0$. Since the elements $c_{11}, c_{12}, \ldots, c_{1k_1}$ are independent and so are the elements $c_{21}, c_{22}, \ldots, c_{2k_2}$, therefore $a_i = 0$ and $b_j = 0$ for all $i$ and $j$. Hence $C$ is a $\mathbb{Z}_4$-free module. \hfill $\square$

The converse of the above Theorem is not true in general, i.e., if a cyclic code $C = C_1 + uC_2$ is a free $\mathbb{Z}_4$-module of length $n$ over $R$, then $C_1$ or $C_2$ may not be a free code of length $n$ over $\mathbb{Z}_4$ (see example 4.6). However, if $C$ is an $R$-free module (code) of length $n$ over $R$ then $C_1$ must be a free code of length $n$ over $\mathbb{Z}_4$ (see Theorem 1).

Example 4.5. The polynomial $x^7 - 1$ factorizes into irreducible polynomials over $\mathbb{F}_2$ as $x^7 - 1 = (x - 1)(x^3 + x + 1)(x^3 + x^2 + 1)$. The Hensel lifts of $x^3 + x + 1$ and $x^3 + x^2 + 1$ to $\mathbb{Z}_4$ are $x^3 + 2x^2 + x - 1$ and $x^3 - x^2 - 2x - 1$, respectively. Therefore $x^3 + 2x^2 + x - 1$ and $x^3 - x^2 - 2x - 1$ are divisors of $x^7 - 1$ over $\mathbb{Z}_4$. Define $C = \langle x^3 + 2x^2 + x - 1 \rangle + u \langle x^3 - x^2 - 2x - 1 \rangle$. Then $C$ is a cyclic code of length 7 over $R$, which is also a free $\mathbb{Z}_4$-module.

Example 4.6. Let $C = C_1 + uC_2$ be a free $\mathbb{Z}_4$-cyclic code of length 5 over $R$ generated by $g(x) = u + 2x + ux^2$. Then $C_1$ is a cyclic code of length 5 over $\mathbb{Z}_4$ generated by $g(x) \pmod{u} = 2x$ which is not $\mathbb{Z}_4$-free.

Now we consider the general form of the generators of cyclic codes over $R$.

Define $\psi : R \to \mathbb{Z}_4$ such that $\psi(a + bu) = a \pmod{u}$. It can easily be seen that $\psi$ is a ring homomorphisms with $\ker \psi = \langle u \rangle = u\mathbb{Z}_4$. Extended $\psi$ to the homomorphism $\phi : \mathbb{Z}_4[x]/(x^n - 1) \to \mathbb{Z}_4[x]/(x^n - 1)$ such that $\phi(a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1}) = \psi(a_0) + \psi(a_1) x + \psi(a_2) x^2 + \ldots + \psi(a_{n-1}) x^{n-1}$. Let $C$ be a cyclic code of length $n$ over $R$. Restrict $\phi$ to $C$ and define

$$J = \{ h(x) \in \mathbb{Z}_4[x]/(x^n - 1) : \psi(h(x)) \in \ker \phi \}.$$
Clearly $J$ is an ideal of $\mathbb{Z}_4[x]/(x^4 - 1)$. So $J$ is a cyclic code over $\mathbb{Z}_4$ and $J = \langle a(x) \rangle$ for some $a(x) \in \mathbb{Z}_4[x]$. Therefore $\ker \phi = \langle ua(x) \rangle$. Similarly, the image of $C$ under $\phi$ is an ideal of $\mathbb{Z}_4[x]/(x^4 - 1)$, and $\phi(C) = \langle g(x) \rangle$ for some $g(x) \in \mathbb{Z}_4[x]$. Hence $C = \langle g(x) + up(x), \ ua(x) \rangle$ for some $p(x) \in \mathbb{Z}_4[x]$. Since $ug(x) = u(g(x) + up(x)) \in C$ and $\phi(ug(x)) = 0$, so $a(x) \mid g(x)$. Thus a cyclic code $C$ over $R$ has the form

$$C = \langle g(x) + up(x), \ ua(x) \rangle,$$

where $g(x), p(x), a(x) \in \mathbb{Z}_4[x]$ and $a(x) \mid g(x)$. In particular if $a(x) = g(x)$, we have the following result.

**Theorem 4.7.** Let $n$ be an odd integer and $C$ be a cyclic code of length $n$ over $R$. Then $C = \langle g(x) + up(x), \ ua(x) \rangle$. Hence $C = \langle g(x) + up(x) \rangle$. □

It may be noted here that unlike in the case of finite fields, a generator polynomial of $\ker \phi$ or $\phi(C)$ may not necessarily divide $x^n - 1$. The proof of the following result is straightforward, as the result is well known for codes over finite fields.

**Theorem 4.8.** Let $C$ be a cyclic code of length $n$ over $R$. If $C = \langle g(x) + up(x), \ ua(x) \rangle$ and $\deg g(x) = k_1$ and $\deg a(x) = k_2$, then $C$ has rank $2n - k_1 - k_2$ and a minimal spanning set $A = \{(g(x) + up(x)), x(g(x) + up(x)), x^2(g(x) + up(x)), \ldots, x^{n-k_1-1}(g(x) + up(x)), \ ua(x), xua(x), x^2ua(x), \ldots, x^{n-k_2-1}ua(x)\}$.

In Theorem (4.8), if we put the restriction on $g(x)$ and $a(x)$ such that they are regular and monic polynomials, respectively, over $\mathbb{Z}_4$, then the minimal spanning set of $C$ reduces to that of [1, Theorem 3]. To prove this, we first prove the following lemma, which appears as an exercise (Exercise XIII.6) in [8, p. 273].

**Lemma 4.9.** Let $f(x)$ and $g(x)$ be two polynomials in $R[x]$. If $g(x)$ is regular, then there exists polynomials $q(x)$ and $r(x)$ such that $f(x) = g(x)q(x) + r(x)$, $\deg r(x) < \deg g(x)$.

Proof. Since $g(x)$ is regular, by [8, Theorem XIII.6] there exists a monic polynomial $g^*(x) \in R[x]$ such that $g(x) = v(x)g^*(x)$, where $v(x)$ is a unit in $R[x]$.

Since $g^*(x)$ is monic, by division algorithm, there exists $q'(x)$ and $r'(x)$ in $R[x]$ such that $f(x) = g^*(x)q'(x) + r'(x)$, where $\deg r'(x) < \deg g^*(x)$. On multiplying both sides by $v(x)$, we get $v(x)f(x) = v(x)g^*(x)q'(x) + v(x)r'(x)$, from which we get $f(x) = g(x)q(x) + r(x)$, where $q(x) = (v(x))^{-1}q'(x)$.

Since $g^*(x)$ is monic, so $\deg g(x) \geq \deg g^*(x)$, as $\deg g(x) = \deg v(x) + \deg g^*(x)$. From this follows that $\deg r(x) < \deg g(x)$.

The following result is a generalization of [1, Theorem 3] in the present setting.

**Theorem 4.10.** Let $C = \langle g(x) + up(x), \ ua(x) \rangle$ be a cyclic code of length $n$ over $R$, and $g(x)$ is regular and $a(x)$ is monic in $\mathbb{Z}_4[x]$ with $\deg g(x) = k_1$ and $\deg a(x) = k_2$, respectively. Then $C$ has rank $n - k_2$ and a minimal spanning set $B = \{(g(x) + up(x)), x(g(x) + up(x)), x^2(g(x) + up(x)), \ldots, x^{n-k_1-1}(g(x) + up(x)), \ ua(x), xua(x), x^2ua(x), \ldots, x^{k_1-k_2-1}ua(x)\}$.

Proof. Suppose $C = \langle g(x) + up(x), \ ua(x) \rangle$ with $\deg g(x) = k_1$ and $\deg a(x) = k_2$, where $g(x)$ is regular and $a(x)$ is monic in $\mathbb{Z}_4[x]$. To prove $B$ is the minimal spanning set of $C$, it suffices to show that $B$ spans the span of $A = \{(g(x) + up(x)), x(g(x) +
up(x), x^2(g(x) + up(x)), \ldots, x^{n-k_1-1}(g(x) + up(x)), ua(x), xua(x), x^2ua(x), \ldots, x^{n-k_2-1}ua(x)\). For this, we first show that \(x^{k_1-k_2}ua(x) \in \text{Span } B\).

Since \(g(x)\) is regular, then so is \((g(x) + up(x))\). By Lemma (4), \(x^{k_1-k_2}ua(x) = u(g(x)+up(x))q(x)+ur(x)\), where \(r(x) = 0\) or \(\deg r(x) < k_1\), and \(q(x) \in \mathbb{Z}_4[x]\). This implies that \(ur(x) \in C\). Since \(\deg r(x) < \deg (g(x) + up(x))\), so if \(r(x) \neq 0\), then it cannot be expressed as a linear combination of \((g(x) + up(x))\) and its multiples. Therefore, \(ur(x) = ua(x)b(x)\) for some \(b(x) \in R[x]\).

Since \(a(x)\) is monic, so deg \(ur(x) = \deg ua(x) + \deg b(x)\). From this follows that \(\deg b(x) \leq k_1 - k_2 - 1\). Thus, we get \(x^{k_1-k_2}ua(x) = u(g(x)+up(x))q(x)+ua(x)b(x)\) with \(\deg b(x) \leq k_1 - k_2 - 1\). It follows that \(x^{k_1-k_2}ua(x) \in \text{span } B\).

Similarly, we can show that \(x^{k_1-k_2+1}ua(x), x^{k_1-k_2+2}ua(x), \ldots, x^{n-k_1-1}ua(x)\) are in \(\text{span } B\). Hence \(B\) is a minimal generating set of \(C\).

To prove the linear independence of \(B\), assume that \(s(x)(g(x) + up(x)) = 0\) (mod \(x^n - 1\)) and \(ut(x)a(x) = 0\) (mod \(x^n - 1\) for some \(s(x) = s_0 + s_1 x + s_2 x^2 + \cdots + s_{n-k_1-1} x^{n-k_1-1} \in R[x]\) and \(t(x) = t_0 + t_1 x + t_2 x^2 + \cdots + t_{k_1-k_2-1} x^{k_1-k_2-1} \in \mathbb{Z}_4[x]\).

Since \(g(x) + up(x)\) is regular, by [8, Theorem XIII.6] there exists a monic polynomial \(g^*(x) \in R[x]\) such that \((g(x) + up(x)) = v(x)g^*(x)\), where \(v(x)\) is a unit in \(R[x]\). Therefore, \(s(x)v(x)g^*(x) = 0\) (mod \(x^n - 1\)), which implies \(s(x)g^*(x) = 0\) (mod \(x^n - 1\)), as \(v(x)\) is a unit in \(R[x]\). Let \(g^*(x) = g_0^* + g_1^* x + g_2^* x^2 + \cdots + g_t^* x^t\), where \(t \leq n - k_1 - 1\). Then

\[(s_0 + s_1 x + s_2 x^2 + \cdots + s_{n-k_1-1} x^{n-k_1-1}) \left(g_0^* + g_1^* x + g_2^* x^2 + \cdots + g_t^* x^t\right) = 0 \pmod {x^n - 1}.

By comparing the coefficient of highest power of \(x\) on both sides, we get \(s_{n-k_1-1} g_t^* = 0\), from which follows that \(s_{n-k_1-1} = 0\), as \(g_t^*\) is a unit in \(R\). Again by comparing the coefficient of next highest power of \(x\), we get \(s_{n-k_1-1} g_{t-1}^* + s_{n-k_1-2} g_t^* = 0\), which implies that \(s_{n-k_1-2} = 0\). On continuing this way, we get \(s_i = 0\) for \(i = 0, 1, \ldots, n-k_1-3\). Similarly we can show that \(t_i = 0\) for all \(i = 0, 1, \ldots, k_1-k_2-1\). Therefore \(B\) is linearly independent.

**Theorem 4.11.** Let \(C = \langle g(x) + up(x), ua(x) \rangle\) be a cyclic code of length \(n\) over \(R\). Then \(w_H(C) = w_H(\ker \phi)\), i.e., \(w_H(C) = w_H(\langle ua(x) \rangle)\).

**Proof.** Let \(c(x) = c_0(x) + uc_1(x) \in C\). Then \(uc(x) = uc_0(x)\). It is clear that \(w_H(uc(x)) = w_H(uc_0(x)) \leq w_H(c(x))\). So \(w_H(uc) \leq w_H(C)\). Also, since \(uc\) is a subcode of \(C\), \(w_H(C) \leq w_H(uc)\). Hence the result.

**5. One generator cyclic codes over \(R\).** We now consider cyclic codes over \(R\) which are principal ideals in \(\frac{R[x]}{(x^n - 1)}\). For a finite chain ring \(R\), the ring \(\frac{R[x]}{(x^n - 1)}\) is a principal ideal ring and the form of the generator of an ideal of \(\frac{R[x]}{(x^n - 1)}\) is well known [9]. Using the form of this generator, a necessary and sufficient condition for cyclic codes over \(\mathbb{Z}_4\) to be free is provided in [2, Proposition 1]. However, in the present case, \(R\) is not a chain ring and the form of the generator of a principally generated ideal of \(\frac{R[x]}{(x^n - 1)}\) is not known. Below we generalize [2, Proposition 1] for the present case and provide a necessary condition (Theorem (5.1)) and a sufficient condition (Theorem (5.2)) for the cyclic codes over \(R\) to be free.

**Theorem 5.1.** Let \(C\) be a principally generated cyclic code of length \(n\) over \(R\) generated by \(g(x) \in R[x]\). If \(g(x) \mid x^n - 1\), then \(C\) is \(R\)-free.

**Proof.** Suppose that \(g(x) \mid x^n - 1\) and \(x^n - 1 = g(x)h(x)\). Since \(x^n - 1\) is a regular polynomial, \(g(x)\) and \(h(x)\) must also be regular polynomials. By [8, Theorem
XIII.6], there exist monic polynomials \( g'(x), h'(x) \) such that \( g(x) = v_1(x)g'(x) \) and \( h(x) = v_2(x)h'(x) \) and \( \overline{g}(x) = \overline{g}'(x) \) and \( \overline{h}(x) = \overline{h}'(x) \), where \( v_1(x), v_2(x) \in R[x] \) are units. Therefore, \( x^n - 1 = g(x)h(x) = v_1(x)v_2(x)g'(x)h'(x) \). Since \( x^n - 1, g'(x) \) and \( h'(x) \) are all monic, we must have \( v_1(x)v_2(x) = 1 \) and \( x^n - 1 = g'(x)h'(x) \). Let deg \( g'(x) = n - k \). Then deg \( h'(x) = k \). We have \( C = \langle g(x) \rangle = \langle v_1(x)g'(x) \rangle = \langle g'(x) \rangle \), as \( v_1(x) \) is a unit. Obviously the set \( S = \{ g'(x), xg'(x), \ldots, x^{k-1}g'(x) \} \) spans \( C \).

Now suppose \( a(x)g'(x) = 0 \) (mod \( x^n - 1 \)) for some \( a(x) \in R[x] \) with deg \( a(x) < k \). Then \( x^n - 1 \mid a(x)g'(x) \), which implies that \( x^n - 1 \mid a(x) \), i.e., \( h'(x) \mid a(x) \). Since \( h'(x) \) is monic polynomial of degree \( k \), it cannot divide a non-zero polynomial of degree less than \( k \). It follows that \( a(x) = 0 \). So the set \( S \) is linearly independent and thus forms a basis for \( C \). Hence \( C \) is an \( R \)-free code.

We have following converse of Theorem (5.1).

**Theorem 5.2.** Let \( C \) be a principally generated cyclic code of length \( n \) over \( R \) generated by \( g(x) \in R[x] \). If \( C \) is \( R \)-free, then there exists a monic generator \( g'(x) \) of \( C \) such that \( g'(x) \mid x^n - 1 \).

**Proof.** Suppose that \( C \) is an \( R \)-free code. Since \( g(x) \) generates an \( R \)-free code, \( g(x) \) must be a regular polynomial. Therefore there exist a monic polynomial \( g'(x) \in R[x] \) such that \( g(x) = v(x)g'(x) \) and \( \overline{g}(x) = \overline{g}'(x) \), where \( v(x) \) is a unit in \( R[x] \). Let the \( R \)-rank of \( C \) be \( s \) and \( S = \{ c_1, c_2, \ldots, c_s \} \) an \( R \)-basis of \( C \). Then the set \( \{ \overline{c}_1, \overline{c}_2, \ldots, \overline{c}_s \} \) forms a basis for the cyclic code \( \overline{C} \) over the finite field \( \overline{R} \). Since \( C = \langle g(x) \rangle \), so \( \overline{C} = \langle \overline{g}(x) \rangle = \langle g'(x) \rangle \). Since \( \overline{g}(x) \) is monic, therefore it is the generator polynomial of \( \overline{C} \). Let deg \( \overline{g}'(x) = n - k \). Then the set \( \{ \overline{g}'(x), x\overline{g}'(x), \ldots, x^{k-1}\overline{g}'(x) \} \) forms a basis for \( \overline{C} \). So we must have \( s = k \).

Now \( C = \langle g(x) \rangle = \langle g'(x) \rangle \). Clearly, the elements \( g'(x), xg'(x), x^2g'(x) \ldots \) span \( C \). Also, the elements \( \{ g'(x), xg'(x), \ldots, x^{k-1}g'(x) \} \) are linearly independent over \( R \); for if they are not, then they give a dependence relation among the elements \( \overline{g}'(x), \overline{xg}'(x), \ldots, \overline{x^{k-1}g}'(x) \), a contradiction. Now since \( x^k g'(x) \) is a codeword, we can write \( x^k g'(x) \) as a linear combination of the elements \( x^i g'(x), i = 0, 1, \ldots, k - 1 \). Let

\[
x^k g'(x) = \sum_{i=0}^{k-1} a_i x^i g'(x)
\]

which can be written as \( \sum_{i=0}^{k} a_i x^i g'(x) = 0 \) with \( a_k = 1 \), or \( a(x)g'(x) = 0 \). Then \( x^n - 1 \mid a(x)g'(x) \) and since \( a(x)g'(x) \) is a monic polynomial of degree \( n \), we must have \( x^n - 1 = a(x)g'(x) \). Therefore, \( g'(x) \mid x^n - 1 \).

The following result follows from Theorem (5.1) and Theorem (5.2).

**Proposition 1.** Let \( C \) be a principally generated cyclic code of length over \( R \). Then \( C \) is free if and only if there exists a monic generator \( g(x) \) in \( C \) such that \( g(x) \mid x^n - 1 \). Furthermore, \( C \) has free rank \( n - \deg g(x) \) and the elements \( g(x), xg(x), \ldots, x^{n-\deg g(x)-1}g(x) \) form a basis for \( C \).

**Example 5.3.** Consider the cyclic code \( C \) of length 7 over \( R \) generated by the polynomial \( g(x) = x^3 + 2x^2 + x - 1 \). \( g(x) \) is the Hensel lift of \( x^3 + x + 1 \in \mathbb{F}_2[x] \) to \( R \). The cyclic code \( C = \langle g(x) \rangle \) an \( R \)-free cyclic code of length 7 and the free rank 4.

**Theorem 5.4.** If \( C = C_1 + uC_2 \) is free cyclic code over \( R \) then so is \( C_1 \) over \( \mathbb{Z}_4 \).
Proof. From Proposition (1), if $C$ is a free cyclic code over $R$ with generator polynomial $g(x)$ then $x^n - 1 = g(x)h(x)$. Since $R = \mathbb{Z}_4 + u\mathbb{Z}_4$, we can express $g(x) = g'(x) + ug''(x)$ and $h(x) = h'(x) + uh''(x)$, where $g'(x), g''(x), h', h''(x) \in \mathbb{Z}_4[x]$. Then $x^n - 1 = g(x)h(x) \pmod{u}$. The result follows.

Example 5.5. Consider again the cyclic code $C$ of length 7 generated by $g(x) = x^3 + 2x^2 + x - 1$. Then $C$ is free over $R$ since $x^7 - 1$ is a divisor of $x^7 - 1$ over $R$. As $x^3 + 2x^2 + x - 1$ is a divisor of $x^7 - 1$ over $\mathbb{Z}_4$ as well, $C_1$ is a free cyclic code of length 7 over $\mathbb{Z}_4$.

A polynomial $e(x)$ in $R[x]$ is said to be an idempotent if $e(x)^2 = e(x) \pmod{x^n - 1}$. The following theorems are the generalization of [10, Theorem 5, 6].

Theorem 5.6. Let $C$ be a cyclic code of length $n$ over $R$.

1. If $C = \langle g \rangle$ and $g|x^n - 1$, then $C$ has an idempotent generator in $R$.
2. If $C = \langle ug \rangle$ with $g|x^n - 1$, then $C = \langle ue \rangle$, where $e$ is an idempotent generator of $C$.

Proof. Let $x^n - 1 = gh$ for some $h$ in $R[x]$. Since $x^n - 1$ has distinct factors over $R$, there exist $\lambda_1, \lambda_2$ in $R[x]$ such that $g\lambda_1 + h\lambda_2 = 1$.

Let $e = g\lambda_1$. Then $e \in \langle g \rangle$. Since $g\lambda_1 + h\lambda_2 = 1$, $e = 1 - h\lambda_2$ and $e^2 = e(1 - h\lambda_2) = e \pmod{x^n - 1}$. Now $ge = g(1 - h\lambda_2) = g \pmod{x^n - 1} = g$. This implies that $g \in \langle e \rangle$. Hence $\langle e \rangle = \langle g \rangle$.

The second result can be proved similarly.

Theorem 5.7. If $C$ be a free cyclic code of length $n$ over $R$ with idempotent generator $e(x)$ in $R[x]$ then $C^\perp$ has the idempotent generator $1 - e(x^{-1})$.

Proof. Similar to the finite fields case.

5.1. One generator cyclic codes as $n^{th}$ roots of unity. Since $(n, 4) = 1$, $x^n - 1$ factorizes uniquely into coprime monic basic irreducible polynomials. From Theorem (3.1), there exists a primitive $n^{th}$ root of unity in $GR(R, r)$. Let $\xi_1, \xi_2, \ldots, \xi_k$ be $n^{th}$ roots of unity in $GR(R, r)$. Define the minimal polynomial $M_i(x)$ of $\xi^i$ as the monic polynomial of least degree having a root $\xi^i$ over $R$. Then a cyclic code $C$ of length $n$ over $R$ can also be described in terms of $n^{th}$ roots of unity. Then the cyclic code $C$ can be defined as

$$C = \{c(x) \in R_n : c(\xi^j) = 0, \ 1 \leq j \leq k\}.$$ 

The generator polynomial $g(x)$ of $C$ is the least common multiple of minimal polynomials of $\xi^j$, $1 \leq j \leq k$. Then $g(x) \mid (x^n - 1)$. Hence $C$ is a free code over $R$.

The following is a straightforward generalization of [2, Proposition 2].

Proposition 2. [2] Suppose that the generator polynomial $g(x)$ of a cyclic code $C$ of length $n$ over $R$ divides $(x^n - 1)$ and has as roots $\xi^6, \xi^{b+1}, \ldots, \xi^{b+\delta-1}$, where $\xi$ is a primitive $n^{th}$ root of unity in a Galois extension of $R$. Then $d(C) \geq \delta$.

Example 5.8. Let $\xi$ be a root of the basic primitive polynomial $f(x) = x^4 + 3x^3 + 2x^2 + 1$, which is a factor of $x^{15} - 1$ over $R$. Let the generator polynomial of a cyclic code of length 15 over $R$ is defined as $g(x) = \text{lcm}(M_0(x), M_1(x), M_2(x), M_3(x), M_4(x), M_5(x), M_6(x))$, where $M_i(x)$ are the minimal polynomials of $\xi^i$, $i = 0, 1, 2, 3, 4, 5, 6$, respectively. We have $M_0(x) = x - 1$, $M_1(x) = M_2(x) = M_4(x) = x^4 + 3x^3 + 2x^2 + 1$,
$M_3(x) = M_6(x) = x^4 + x^3 + x^2 + x + 1$ and $M_5(x) = x^2 + x + 1$. Therefore, $g(x) = x^{11} + 2x^9 + 3x^8 + 3x^7 + x^6 + 2x^4 + 3x^3 + x^2 + 3x + 3$. The cyclic code $C$ generated by $g(x)$ is a free code of rank 4. Since $g(x)$ has 7 consecutive roots, $d(C) \geq 8$, where $d(C)$ denotes the minimum Hamming distance of $C$. Also since $2g(x) = 8$, we must have $d(C) = 8$.

6. **Conclusion.** In this paper we have studied some structural properties of cyclic codes of odd length over the ring $R = \mathbb{Z}_4 + u\mathbb{Z}_4$, $u^2 = 0$. The general form of the generators of cyclic codes over $R$ is provided and a formula for their ranks is determined. We have mainly focused on cyclic codes over $R$ that are principally generated. We have also obtained a necessary condition and a sufficient condition for such codes to be free $R$-modules.

REFERENCES

[1] T. Abualrub and I. Siap, Cyclic codes over the rings $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2$, Des. Codes Cryptogr., 42, No. 3 (2007), 273–287.

[2] M. Bhaintwal and S. K. Wasan, Quasi-cyclic codes over $\mathbb{Z}_4$, Appl. Algebra Engrg. Comm. Comput., 45, No. 20 (2009), 459–480.

[3] P. Bonneauze and P. Udaya, Cyclic codes and self-dual codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory, 45, No. 4 (1999), 1250–1255.

[4] H. Q. Dinh and S. R. L. Permouth, Cyclic codes and negacyclic codes over finite chain ring, IEEE Trans. Inform. Theory, 50, No. 8 (2004), 1728–1744.

[5] J. Hammons, 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, No. 4 (1994), 301–319.

[6] P. Kanwar and S. R. L. Permouth, Cyclic codes over integers modulo $p^m$, Finite Fields Appl., 3, (1997), 334–354.

[7] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error Correcting Codes, North Holland, 1977.

[8] B. R. McDonald, Finite Rings with Identity, Marcel Dekker, 1974.

[9] G. Norton and A. Salagean, On the structure of linear and cyclic codes over a finite chain ring, Appl. Algebra Engrg. Comm. Comput., 10, No. 6 (2000), 489–506.

[10] V. S. Pless and Z. Qian, Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory, 42, No. 5 (1996), pp. 1594–1600.

[11] B. Yildiz and S. Karadeniz, Linear codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$, MacWilliams identities, projections, and formally self-dual codes, Finite Fields Appl., 27 (2014), 24–40.

[12] B. Yildiz and S. Karadeniz, Cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + u\mathbb{v}\mathbb{F}_2$, Des. Codes Cryptogr., 58, No. 3 (2011), 221–234.

[13] S. Zhu, Y. Wang and M. Shi Some results on cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$, IEEE Trans. Inform. Theory, 56, No. 4 (2010), 1680–1684.

Received xxxx 20xx; revised xxxx 20xx.

E-mail address: bandi.ramakrishna@gmail.com
E-mail address: mahesfma@iitr.ac.in