On the Construction of Cyclic Codes over the Ring \( \mathbb{Z}_2 + u\mathbb{Z}_2 \)

Taher Abualrub
Department of Mathematics and Statistics, American University of Sharjah, Sharjah-UAE

Irfan Siap
Adiyaman Education Faculty, Gaziantep University, Adiyaman, Turkey
www.gantep.edu.tr/~isiap

Abstract

In this paper we study cyclic codes of any length \( n \) over the ring \( \mathbb{Z}_2 + u\mathbb{Z}_2 \). We find a unique set of generators for these codes. We also study the dual codes and find their unique generating sets. The Hamming distance of these codes is studied as well.

Key-Words: Rings, Cyclic Codes, Dual Codes, Ideals, Minimum Hamming Distance

1 Introduction

Let \( R \) be the ring \( \mathbb{Z}_2 + u\mathbb{Z}_2 = \{0, 1, u, u+1\} \) where \( u^2 = 0 \mod 2 \). A cyclic code of length \( n \) over \( R \) is an ideal in the ring \( R_n = R[x]/(x^n - 1) \). The Hamming weight of a codeword \( u \) is defined by \( w_H(u) = |\{i|u_i \neq 0\}| \), i.e. the number of the nonzero entries of \( u \). The minimum Hamming distance \( d_H(C) \) of a code \( C \) is the smallest possible weight among all its nonzero codewords.

Let \( u = (u_0, \ldots, u_{n-1}) \) and \( v = (v_0, \ldots, v_{n-1}) \) be any two vectors over \( R \). We define an inner product over \( R \) by \( u \cdot v = u_0v_0 + \cdots + u_{n-1}v_{n-1} \). If \( u \cdot v = 0 \), then \( u \) and \( v \) are said to be orthogonal. We define the dual of a cyclic code \( C \) to be the set \( C^⊥ = \{u \in Z_n^2 : u \cdot v = 0 \text{ for all } v \in C\} \). It is clear that \( C^⊥ \) is also a cyclic code.

The parameters of an \( R \)--code \( C \) with \( 4^{k_1}2^{k_2} \) codewords and minimum distance \( d \) is denoted by \( (n, 4^{k_1}2^{k_2}, d) \). Such codes are often referred to as codes of type \( \{k_1, k_2\} \).

The structure of cyclic codes over rings of odd length \( n \) has been discussed in [4, 6, 8, 11]. Calderbank and Sloane [6] and other papers [11] presented a complete structure of cyclic codes over \( \mathbb{Z}_4 \) of odd length. They have shown that cyclic codes are principal ideals (have a single generator) in \( \mathbb{Z}_4[x]/(x^n - 1) \). In [4] Bonnecaze and Udaya studied cyclic codes of odd length over \( R \). They have also shown that cyclic codes are principal ideals in \( R_n = R[x]/(x^n - 1) \).

Blackford [3] studied cyclic codes over \( \mathbb{Z}_4 \) of length \( n = 2k \) when \( k \) is odd. He showed that the ring \( \mathbb{Z}_4[x]/(x^n - 1) \) is not a principal ideal ring and hence ideals might have more than one generator. Cyclic codes over \( \mathbb{Z}_4 \) of length a power of 2 are studied in [1] and [2]. They also showed that the ring \( \mathbb{Z}_4[x]/(x^n - 1) \) is not a principal ideal.

In all of the above work, researchers always put some restrictions on the length \( n \). Either \( n \) is odd or \( n = 2k \) or \( n \) is a power of 2.

In this paper, we investigate the structure of cyclic codes over \( R \) of any length \( n \). There will be no restrictions on the length \( n \). We will give a unique representation for cyclic codes and their duals as ideals in the ring \( R_n = R[x]/(x^n - 1) \). The Hamming distance of these codes will be studied as well.

The remainder of the paper is organized as follows. In Section 2, we will study cyclic codes over \( \mathbb{Z}_2 + u\mathbb{Z}_2 \) and we will find a unique set of generators for them. In Section 3, we study dual codes and their generators. In Section 4, we study the Hamming distance of these codes. Section 5 concludes the paper.

2 Generators for Cyclic Codes over \( \mathbb{Z}_2 + u\mathbb{Z}_2 \)

Consider the ring \( R = \mathbb{Z}_2 + u\mathbb{Z}_2 = \{0, 1, u, u+1\} \) where \( u^2 = 0 \mod 2 \). The ring \( \mathbb{Z}_2 \) is a subring of \( R \). A cyclic code \( C \) in \( R_n = R[x]/(x^n - 1) \) is an ideal in \( R_n \). Our goal is to find a set of generators for \( C \). Note that we have no restrictions on \( n \).

Let \( C \) be a cyclic code in \( R_n \). Define \( \varphi : C \rightarrow \mathbb{Z}_2[x]/(x^n - 1) \) by \( \varphi(x) = x^2 \).

\( \varphi \) is a ring homomorphism with \( \ker \varphi = \{ur(x) : r(x) \text{ is a binary polynomial in } C\} \). Let \( J = \{r(x) : ur(x) \in \ker \varphi \} \). It is easy to check that \( J \) is an ideal in \( \mathbb{Z}_2[x]/(x^n - 1) \) and hence a
cyclic code in $\mathbb{Z}_2[x]/(x^n-1)$. So $J = \{a(x)\}$ where $a(x)/(x^n-1)$. This implies that $\ker \varphi = \{ua(x)\}$ with $a(x)/(x^n-1) \mod 2$. The image of $\varphi$ is also an ideal and hence a binary cyclic code that has a generator $g(x)$ with $g(x)/(x^n-1)$. This implies that $C = \langle g(x)+up(x), \ ua(x) \rangle$ for some binary polynomial $p(x)$.

Claim 1 We may assume $\deg a(x) > \deg p(x)$, and $a(x) \mid g(x)$.

Proof. Since $C = \langle g(x)+up(x), \ ua(x) \rangle = \langle g(x)+u[p(x)+x'a(x)], \ ua(x) \rangle$, then we may assume $\deg a(x) > \deg p(x)$. Since $up(x) \in \ker \varphi = \{ua(x)\}$, then $a(x) \mid g(x)$. If $g(x) = a(x)$, then $C = \langle g(x)+up(x) \rangle$.

Claim 2 $a(x) \mid p(x) \left( \frac{x^n-1}{g(x)} \right)$.

Proof. $\varphi \left( \frac{x^n-1}{g+up} \right) = \varphi \left( \frac{x^n-1}{g} \right) = 0$ \\implies \left( \frac{x^n-1}{g} \right) \in \ker \varphi = \{ua(x)\} \\implies a(x) \mid \left( \frac{x^n-1}{g} \right)$.

Claim 3 If $C = \langle g(x)+up(x), \ ua(x) \rangle = \langle h(x)+uq(x), \ ub(x) \rangle$ then $g(x) = h(x)$, $a(x) = b(x)$ and $p(x) = q(x) \mod a(x)$.

Proof. From the construction of $C$ we have $J = \{x \in \ker \varphi \} = \{a(x)\} = \{b(x)\}$. Hence $a(x) = b(x)$.

Suppose $C = \langle g(x)+up(x), \ ua(x) \rangle = \langle h(x)+uq(x), \ ub(x) \rangle$. Note that $h(x) \in \varphi(C) = \{g(x)\}$. Hence $h = g(x)\alpha(x)$ and $\deg h(x) \geq \deg g(x)$. By the same means $g(x) = h(x)\beta(x) = g(x)\alpha(x)\beta(x)$ and $\deg g(x) \geq \deg h(x)$. Since $g(x)$, and $h(x)$ are factors of $(x^n-1) \mod 2$ and $(x^n-1)$ factors uniquely over $\mathbb{Z}_2$ into a product of irreducible polynomials then $a(x) = \beta(x) = 1$ and $g(x) = h(x)$.

Since $g(x) + uq(x) \in C$, then $g(x) + uq(x) = [g(x)+up(x)] + ua(x)m(x)$. This implies $u[q(x)-p(x)] = ua(x)m(x)$ Therefore $p(x) = q(x) \mod a(x)$.

Claim 4 Suppose $n$ is odd, then $C = \langle g(x), \ ua(x) \rangle = \langle g(x)+ua(x) \rangle$.

Proof. Suppose $a(x) \mid g(x)$ and $a(x) \mid p(x) \left( \frac{x^n-1}{g(x)} \right)$.

Then $g(x) = a(x)m_1(x)$ and $p(x) \left( \frac{x^n-1}{g(x)} \right) = a(x)m_2(x)$ Since $n$ is odd then $(x^n-1)$ factors uniquely as a product of distinct irreducible polynomials. This implies that $a(x)$ must be a factor of $p(x)$. But $p(x)$ has degree less than $a(x)$. Hence $p(x) = 0$ and $C = \langle g(x), \ ua(x) \rangle$. Let $h(x) = g(x)+ua(x)$.

$$uh(x) = ug(x) \in \langle g(x)+ua(x) \rangle.$$  

Also, $(x^n-1)h(x) = u \left( \frac{x^n-1}{g(x)} \right)a(x) \in \langle g(x)+ua(x) \rangle$.

Since $n$ is odd then $\gcd \left( \frac{x^n-1}{g(x)}, \ g(x) \right) = 1$, and hence there exist binary polynomials $f_1(x), \ f_2(x)$ such that

\[ 1 = \left( \frac{x^n-1}{g(x)} \right)f_1(x) + g(x)f_2(x) \]

\[ ua(x) = \left( \frac{x^n-1}{g(x)} \right)f_1 + ua(x)g(x)f_2 \]

\[ \in \langle g(x)+ua(x) \rangle. \]

Hence $g(x) \in \langle g(x)+ua(x) \rangle$ and $C = \langle g(x), \ ua(x) \rangle = \langle g(x)+ua(x) \rangle$.

This is similar to the results obtained in [4] and [6].

We can summarize the above by the following theorem.

Theorem 5 Let $C$ be a cyclic code in $R_n = R_2[x]/(x^n-1)$, $R = \mathbb{Z}_2 + u\mathbb{Z}_2 = \{0,1,u,u+1\}$ and $u^2 = 0 \mod 2$. Then

1. If $n$ is odd then $R_n$ is a principal ideal ring and $C = \langle g(x), \ ua(x) \rangle = \langle g(x)+ua(x) \rangle$ where $g(x), a(x)$ are binary polynomials with $a(x) \mid g(x) \mid (x^n-1) \mod 2$.

2. If $n$ is not odd then

(a) If $g(x) = a(x)$, then $C = \langle g(x)+up(x) \rangle$ where $g(x), p(x)$ are binary polynomials with $g(x) \mid (x^n-1) \mod 2$, and $g(x) \mid p(x) \left( \frac{x^n-1}{g(x)} \right)$. 


(b) \( C = \langle g(x) + up(x), u\alpha(x) \rangle \) where \( g(x), a(x), \) and \( p(x) \) are binary polynomials with \( a(x)|g(x)|(x^n - 1) \mod 2, \)
\( a(x)|p(x) \left( \frac{x^n-1}{g(x)} \right) \) and
\( \deg g(x) > \deg a(x) > \deg p(x). \)

**Corollary 6** Suppose \( n \) is not odd and
\( \left( \frac{x^n-1}{a(x)}, a(x) \right) = 1, \) then \( p(x) = 0. \)

### 3 Dual Codes

**Definition 7** Let \( I \) be an ideal in \( R_n. \) We define \( \text{A}(I) \) to be the set
\[
\text{A}(I) = \{ g(x) : f(x)g(x) = 0 \text{ for all } f(x) \text{ in } I \}. 
\]
The set \( \text{A}(I) \) is called the annihilator of \( I \) in \( R_n. \)

**Definition 8** If \( f(x) = a_0 + a_1x + \cdots + a_rx^r \) is a polynomial of degree \( r \) then the reciprocal of \( f(x) \) is the polynomial \( f^*(x) = ax + a_{r-1}x + \cdots + a_0x^r. \)
Symbolically, \( f^*(x) \) can be expressed by \( f^*(x) = x^r f \left( \frac{1}{x} \right). \)

It is obvious that if \( C \) is a cyclic code with associated ideal \( I \) then the associate ideal of \( C^\perp \) is \( \text{A}(I)^* = \{ f^*(x) : f(x) \in I \}. \)

**Theorem 9** Let \( C \) be a cyclic code of even length.

1. If \( C = \langle g(x) + up(x), \rangle \) with \( p(x) \left( \frac{x^n-1}{g(x)} \right) = g(x)m_2(x) \) then
\[
\text{A}(C) = \left( \frac{x^n-1}{g(x)} + um_2(x) \right) 
\]
2. If \( C = \langle g(x) + up(x), \rangle \) with \( a(x)|g(x)|(x^n - 1), \) \( a(x)|p(x) \left( \frac{x^n-1}{g(x)} \right) \) and
\( \deg g(x) > \deg a(x) > \deg p(x). \) Suppose \( g(x) = a(x)m_1(x), \) \( p(x) \left( \frac{x^n-1}{g(x)} \right) = a(x)m_2(x), \) then
\[
\text{A}(C) = \left( \frac{x^n-1}{a(x)} + um_2(x), \ u \frac{x^n-1}{g(x)} \right) 
\]

**Proof.** We will prove (2)

Notes that
\[
\left( \frac{x^n-1}{a(x)} + um_2(x) \right) (g(x) + up(x)) = up(x) \left( \frac{x^n-1}{a(x)} \right) + um_2(x)g(x) = 0,
\]
and
\[
\left( \frac{x^n-1}{a(x)} + um_2(x) \right) u\alpha(x) = 0,
\]
and
\[
u \frac{x^n-1}{g(x)} (g(x) + up(x)) = 0,
\]
and
\[
u \frac{x^n-1}{g(x)} (u\alpha(x)) = 0.
\]

Hence,
\[
J = \left( \frac{x^n-1}{a(x)} + um_2(x), u \frac{x^n-1}{g(x)} \right) \subseteq \text{A}(C).
\]

Now, suppose \( \text{A}(C) = \langle h(x) + uk(x), \rangle, \)
where \( r(x) | h(x), \) and \( r(x)|k(x) \left( \frac{x^n-1}{h(x)} \right). \)

\[
ur(x) [g(x) + up(x)] = ur(x)g(x) = 0 \\
\Rightarrow r(x) = \left( \frac{x^n-1}{g(x)} \right) d(x) \\
\Rightarrow ur(x) \in J. \] Also,
\[
u \alpha(x) [h(x) + uk(x)] = uh(x)a(x) = 0 \\
\Rightarrow h(x) = \left( \frac{x^n-1}{a(x)} \right) t_1(x),
\]
and
\[
(g(x) + up(x)) [h(x) + uk(x)] = \\
g(x)h(x) + ug(x)k(x) + up(x)h(x) = 0.
\]

Since \( h(x) = \left( \frac{x^n-1}{a(x)} \right) t_1, \) then \( g(x)h(x) = 0. \) Hence
\[
0 = ug(x)k(x) + up(x)h(x) \\
= ug(x)k(x) + up(x) \left( \frac{x^n-1}{g(x)} \right) t_1(x) \\
= ug(x)k(x) + ug(x)m_2(x) t_1(x) \\
= ug(x) [k(x) + m_2(x) t_1(x)].
\]

This implies that there exists a binary polynomial \( t_2(x) \) such that
\[
k(x) + m_2(x) t_1(x) = \left( \frac{x^n-1}{g(x)} \right) t_2(x).
\]
Hence,
\[
    h(x) + uk(x) = \left( \frac{x^n - 1}{a(x)} \right) t_1(x) + um_2(x)t_1(x) \\
    + u \left( \frac{x^n - 1}{g(x)} \right) t_2(x) \\
    = \left( \frac{x^n - 1}{a(x)} \right) t_1(x) + um_2(x) \\
    + u \left( \frac{x^n - 1}{g(x)} \right) t_2(x) \\
    \in \J.
\]

Therefore, \( \left( \frac{x^n - 1}{a(x)} + um_2(x), u \frac{x^n - 1}{g(x)} \right) = A(C) \).

As a result of this we get the following theorem:

**Theorem 10** Let \( C \) be a cyclic code of even length \( n \)

1. If \( C = (g(x) + up(x)), \) with \( p(x) \left( \frac{x^n - 1}{g(x)} \right) = g(x)m_2(x) \) then the dual of \( C \) is given by

\[
    C^\perp = \left( \frac{x^n - 1}{g(x)} \right)^* + ux^i(m_2)^*
\]

where \( i = \text{deg} \left( \frac{x^n - 1}{g(x)} \right) - \text{deg} \, (m_2). \)

2. If \( C = (g(x) + up(x), ua(x)) \), then the dual of \( C \) is given by

\[
    C^\perp = \left( \left( \frac{x^n - 1}{a(x)} \right)^* + ux^i(m_2(x))^* \right), \quad u \left( \frac{x^n - 1}{g(x)} \right)^*
\]

4 Minimum Distance

In this section we investigate the minimum Hamming distance of a cyclic code of even length.

Let \( C = (g(x) + up(x), ua(x)) \). We define \( C_u = \{ k(x) | uk(x) \in C \} \). It is clear that \( C_u \) is a cyclic code over \( Z_2 \).

**Theorem 11** Let \( C = (g(x) + up(x), ua(x)) \). Then, \( C_u = \langle a(x) \rangle \) and \( d_H(C) = d_H(C_u) \).

**Proof.** Let \( ub(x) \in C \). Then \( ub(x) \in \ker \varphi = \langle ua(x) \rangle \). Hence \( C_u = \langle a(x) \rangle \). Further, let \( l(x) = l_1(x) + ul_1(x) \in C \) where \( l_1(x), l_2(x) \in Z_2[x] \). Since \( ul(x) = ul_1(x) \in C \) and \( d_H(ul(x)) = d_H(l(x)) \) and \( uC \) is a subcode of \( C \) with \( d_H(uC) \leq d_H(C) \) it is sufficient to focus on the subcode \( uC \) in order to compute the Hamming weight of \( C \). Since \( uC = \langle ua(x) \rangle \) thus \( d_H(C) = d_H(C_u) \).

Cyclic codes over finite fields with the lengths divisible by the characteristic of the field, which are referred as repeated root cyclic codes are investigated in [7] and [9]. Here, in order to investigate the lower bounds of cyclic code of length \( n \) which are divisible by \( 2 \) over a \( R \) we shall use the results obtained in [7].

Let \( C \) be a binary repeated-root cyclic code of length \( n = 2^k\pi \) where \( (2, \pi) = 1 \). Let

\[
    g(x) = \prod_{i=1}^{l} m_i(x)^{\varepsilon_i}
\]

be a generator polynomial of the code \( C \) with distinct irreducible polynomials \( m_i(x) \) of multiplicity \( \varepsilon_i \). For all \( 0 \leq t \leq 2^k - 1 \), \( \eta_t(x) \) is defined as the multiplication of \( m_i(x)^{\varepsilon_i} \) with \( t < \varepsilon_i \). Then the simple-root cyclic code \( \overline{C} \) of length \( \overline{\pi} \) is generated by \( \eta_t(x) \).

Prior stating the theorem we refer to some of the definitions given in [7].

\[
    w_H((x - 1)^t) = P_t
\]

where

\[
    P_t = \prod_{i}(t_i + 1)
\]

and \( t_i \)'s are the coefficients of the radix-\( p \) expansion of \( t \).

**Theorem 12** [7] Let \( C \) be a binary repeated-root cyclic code of length \( n = 2^k\pi \) where \((2, \pi) = 1\). Then, \( d_H(C) = P_1 d_H(C_7) \) for some \( 7 \in \{ t+1, t+2, \ldots, 2^k - 1 \} \).

Now combining Theorems 11 and 12 we obtain the following theorem:

**Theorem 13** Let \( C = (g(x) + up(x), ua(x)) \) be a cyclic code over \( R \) of length \( n = 2^k\pi \) where \((2, \pi) = 1\). Let \( D = C_u \). Then, \( d_H(C) = P_{e-q} d_H(C_{t-e}) \) for some \( 7 \in \{ t+1, t+2, \ldots, 2^k - 1 \} \)

**Definition 14** Let \( s = b_{e-q-1}2^{e-1} + b_{e-2}2^{e-2} + \cdots + b_22^2 + b_02^0 \) be the 2-adic expansion of \( s \). Let \( b_{e-1} = b_{e-2} = \cdots = b_{e-q-1} = 1 \) where \( e-q > 0 \) and \( b_{e-q-1} = 0 \).

1. If \( b_{e-i} = 0 \) for all \( i \in \{ q+2, q+3, \ldots, e-1 \} \), then \( s \) is said to have a 2-adic length \( q \) zero expansion.

2. If \( b_{e-i} \neq 0 \) for some \( i \in \{ q+2, q+3, \ldots, e-1 \} \), then \( s \) is said to have a 2-adic length \( q \) nonzero expansion.

If \( e = q \) then, \( s \) is said to have 2-adic length \( e \) expansion or 2-adic full expansion.
Example 15 5 = 2^2 + 2^1 and hence q = 1, and 5 has a 2-adic length 1 nonzero expansion. 6 = 2^2 + 2^1 has a 2-adic length 2 zero expansion. 7 = 2^2 + 2^1 + 2^0 and hence q = 3, and 7 has a 2-adic full expansion.

Lemma 16 Let C be a binary cyclic of length 2^e where e is a positive integer. Assume that C = (a(x)) where a(x) = (x^{2^e-1} - 1)h(x) for some h(x). If h(x), generates a cyclic code of length 2^{e-1} and minimum distance d, then d(C) = 2d.

Proof. Suppose h(x) generates a cyclic subcode of minimum distance d. Since a(x) = (x^{2^e-1} - 1)h(x) is the generator of C then for c \in C we have c = (x^{2^e-1} - 1)l(x)h(x) for some l(x). Since l(x)h(x) \in (h(x)) for all l(x) and w(c) = w(x^{2^e-1}l(x)h(x)) + w(l(x)h(x)) we obtain the result. ■

Lemma 17 Let C be a cyclic code over R of length 2^e where e is a positive integer. Then, C = (g(x) + up(x), ua(x)) where g(x) = (x - 1)^t and a(x) = (x - 1)^s for some t > s > 0.

If s < 2^{e-1}, then d(C) = 2.

Proof. Let 2^{e-1} = s + m. Then
\[
u\left(x^{2^{e-1}} - 1\right) = u(x - 1)^{2^{e-1}}
\]
\[
= u(x - 1)^m (x - 1)^s \in C.
\]
Therefore, d(C) = 2. ■

Lemma 18 Let C be a cyclic code over R of length 2^e where e is a positive integer. Then, C = (g(x) + up(x), ua(x)) where g(x) = (x - 1)^t and a(x) = (x - 1)^s for some t > s > 0. Suppose s \geq 2^{e-1}.

Then, s has 2-adic length q \geq 1 expansion

1. If s has a 2-adic length q zero expansion. Then, 
\[d(C) = 2^1.
\]

2. If s has a 2-adic length q nonzero expansion. Then, 
\[d(C) = 2^{q+1}.
\]

Proof. Since s \geq 2^{e-1}.

1. If s has a 2-adic length q zero expansion. Then,
\[
s = 2^{e-1} + 2^{e-2} + \ldots + 2^{e-q},
\]
\[
a(x) = (x - 1)^s
\]
\[
= (x - 1)^{2^{e-1}}(x - 1)^{2^{e-2}}\ldots(x - 1)^{2^{e-q}}
\]
\[
= (x^{2^{e-1}} - 1)(x^{2^{e-2}} - 1)\ldots(x^{2^{e-q}} - 1).
\]

Now, h(x) = ((x^{2^{e-q}} - 1)) generates a cyclic code with minimum Hamming distance 2. By Lemma 16, the subcode generated by (x^{2^{e-(q-1)}} - 1)h(x) has minimum Hamming distance twice as the subcode generated by h(x) which is 4. By induction on q we conclude that the code generated by a(x) has minimum Hamming distance 2^q and hence d(C) = 2^q.

2. If s has a 2-adic length q nonzero expansion. Then,
\[
s = 2^{e-1} + 2^{e-2} + \ldots + 2^{e-q} + t
\]
where 2^{e-1} > t > 0, and e - q - 1 = 0. Now
\[
a(x) = (x - 1)^s
\]
\[
= (x - 1)^{2^{e-1}+2^{e-2}+\ldots+2^{e-q}+t}
\]
\[
= (x^{2^{e-1}} - 1)(x^{2^{e-2}} - 1)\ldots(x^{2^{e-q}} - 1)(x + 1)^t.
\]

Since 2^{e-1} > t, let 2^{e-1} = t + j for some nonzero j. Then,
\[
(x^{2^{e-1}} - 1) = (x - 1)^{2^{e-1}}
\]
\[
= (x + 1)^j (x + 1)^t.
\]

Hence, the subcode generated by h(x) = (x + 1)^t has minimum Hamming distance 2. By Lemma 16, the subcode generated by (x^{2^{e-q}} - 1)h(x) has minimum Hamming distance twice as the subcode generated by h(x) which is 4. By induction on q we conclude that the code generated by a(x) has minimum Hamming distance equals to 2^{q+1} and hence d(C).

Example 19 If n = 8, then x^8 - 1 = (x - 1)^8 = g(x)^8. Due to Lemma 17, the dimensions may change but the minimum distance equals to 1, 2, 4 or 8. For example, by Lemma 17, if a(x) = g^t then 7 has 2-adic length 3 full expansion, hence the minimum distance will equal to 8. On the other hand, if a(x) = g^t then 5 has 2-adic length 1 nonzero expansion, hence the minimum distance will equal to 4. Also, if a(x) = g^t then 6 has 2-adic length 2 zero expansion, hence the minimum distance will equal to 4.

5 Conclusion

In this paper, we studied cyclic codes of any length n over the ring \( \mathbb{R} = \mathbb{Z}_2 + u\mathbb{Z}_2 \). We have constructed a unique set of generators for theses codes and their duals. We also studied the minimum Hamming distance for these codes. Open problems include the
study of self-dual codes and their properties. Also, it will be interesting to construct a decoding algorithm for these codes that works for any length n.

References


