\[ \mathbb{Z}_2 (\mathbb{Z}_2 + u\mathbb{Z}_2) \]  

**Linear Cyclic Codes**

Taher Abualrub, Irfan Siap, and Ismail Aydogdu

**Abstract**—Let \( n = \alpha + 2\beta \). In this paper, we introduce a new type of linear and cyclic codes defined over the ring \( \mathbb{Z}_2 R \) where \( \mathbb{Z}_2 = \{0, 1\} \) is the binary finite field and the ring \( R = \{0, 1, u, u + 1\} \) where \( u^2 = 0 \). We give the definition of these codes as subsets of the ring \( \mathbb{Z}_2^2 \times R^2 \). We give a one-to-one correspondence between elements in \( \mathbb{Z}_2^2 \times R^2 \) and elements in the ring \( R_{\alpha, \beta} = \mathbb{Z}_2[x]/(x^\alpha - 1) \times R[x]/(x^\beta - 1) \), and hence relate these codes to subsets of the ring \( R_{\alpha, \beta} \). We prove that \( C \) is a \( \mathbb{Z}_2 R \)-cyclic code if and only if \( C \) is an \( R[x] \)-submodule of \( R_{\alpha, \beta} \). We provide some examples of \( \mathbb{Z}_2 R \)-linear cyclic codes that produce optimal binary linear codes.

**Index Terms**—Linear codes, \( \mathbb{Z}_2 R \)-linear codes, submodules.

I. INTRODUCTION

Let \( n = \alpha + 2\beta \) where \( \alpha, \beta \) are positive integers. Consider the finite field \( \mathbb{Z}_2 = \{0, 1\} \) and the finite ring \( \mathbb{Z}_2 + u\mathbb{Z}_2 = R = \{0, 1, u, u + 1\} \) where \( u^2 = 0 \). It is known that the ring \( \mathbb{Z}_2 \) is a subring of the ring \( R \). We construct the ring \( \mathbb{Z}_2 R = \{(e_1, e_2) | e_1 \in \mathbb{Z}_2 \) and \( e_2 \in R\} \).

The ring \( \mathbb{Z}_2 R \) is not closed under standard multiplication (mod 2) by the element \( u \) in the ring \( R \). This implies that the ring is NOT an \( R \)-module under the operation of standard multiplication. To make the ring \( \mathbb{Z}_2 R \) an \( R \)-module we need to introduce the following method of multiplications: Define the mapping

\[ \eta : R \rightarrow \mathbb{Z}_2 \]  

\[ \eta(r + uq) = r. \]

So, \( \eta(0) = 0, \eta(1) = 1, \eta(u) = 0 \) and \( \eta(u + 1) = 1 \). It is clear that the mapping \( \eta \) is a ring homomorphism. Now for any element \( d \in R \), define the following multiplication

\[ d \ast (e_1, e_2) = (\eta(d)e_1, de_2). \]

This a well-defined multiplication. In fact this multiplication can be generalized over the ring \( \mathbb{Z}_2^2 \times R^2 \) in the following way: for any \( d \in R \) and \( v = (a_0, a_1, ..., a_{\alpha-1}, b_0, b_1, ..., b_{\beta-1}) \) in \( \mathbb{Z}_2^2 \times R^2 \) define

\[ dv = (\eta(d)a_0, \eta(d)a_1, ..., \eta(d)a_{\alpha-1}, \eta(d)b_0, \eta(d)b_1, ..., \eta(d)b_{\beta-1}) . \]

This definition gives us the following result:

**Lemma 1:** The ring \( \mathbb{Z}_2^2 \times R^2 \) is an \( R \)-module under the above definition.

**Definition 2:** A non-empty subset \( C \) of \( \mathbb{Z}_2^2 \times R^2 \) is called a \( \mathbb{Z}_2 R \)-linear code if \( C \) is an \( R \)-submodule of \( \mathbb{Z}_2^2 \times R^2 \).

II. \( \mathbb{Z}_2 R \)-LINEAR CYCLIC CODES.

**Definition 4:** A subset \( C \) of \( \mathbb{Z}_2^2 \times R^2 \) is called a \( \mathbb{Z}_2 R \)-linear cyclic code if

1. \( C \) is a linear code, and
2. For any codeword \( u = (a_0a_1 \ldots a_{\alpha-1}, b_0b_1 \ldots b_{\beta-1}) \in C \), its cyclic shift
   \[ T(u) = (a_{\alpha-1}0 \ldots a_0, b_{\beta-1}b_0 \ldots b_{\beta-2}) \]
   is also in \( C \).

An element \( c = (a_0a_1 \ldots a_{\alpha-1}, b_0b_1 \ldots b_{\beta-1}) \in \mathbb{Z}_2^2 \times R^2 \) can be identified with a module element consisting of two polynomials

\[ c(x) = \left( \begin{array}{c} a_0 + a_1x + \ldots + a_{\alpha-1}x^{\alpha-1}, \\ b_0 + b_1x + \ldots + b_{\beta-1}x^{\beta-1} \end{array} \right) = (a(x), b(x)) \]

in \( R_{\alpha, \beta} = \mathbb{Z}_2[x]/(x^\alpha - 1) \times R[x]/(x^\beta - 1) \). This identification gives a one-to-one correspondence between elements in \( \mathbb{Z}_2^2 \times R^2 \) and elements in \( R_{\alpha, \beta} \).

Let \( f(x) = f_0 + f_1x + \ldots + f_nt^t \in R[x] \), \( (g(x), h(x)) \in R_{\alpha, \beta} \) and consider the following multiplication

\[ f(x) \ast (g(x), h(x)) = (\eta(f(x))g(x), f(x)h(x)). \]
where
\[ \eta(f(x)) = \eta(f_0) + \eta(f_1)x + \ldots + \eta(f_x)x^t \]

This multiplication operation on \( R_{a,\beta} \) leads to the following easily proven theorem.

**Theorem 5:** The multiplication above is well-defined. Moreover, \( R_{a,\beta} \) is an \( R[x] \)-module with respect to this multiplication.

As is common in the discussion of cyclic codes, we can regard codewords of a cyclic code \( C \) as vectors or as polynomials interchangeably. In either case, we use the same notation \( C \) to denote the set of all codewords. We follow this convention in the definition below and in the rest of the paper.

**Definition 6:** A subset \( C \subseteq R_{a,\beta} \) is called a \( Z_2R \)-cyclic code if

1) \( C \) is a subgroup of \( R_{a,\beta} \), and
2) If

\[
c(x) = \begin{pmatrix}
a_0 + a_1x + \ldots + a_{\alpha-1}x^{\alpha-1}, \\
b_0 + b_1x + \ldots + b_{\beta-1}x^{\beta-1}
\end{pmatrix} \in C,
\]

then for any \( a \in R \), we have

\[
a \cdot x \cdot c(x) = \begin{pmatrix}
\eta(a)(a_0 + a_1x + \ldots + a_{\alpha-2}x^{\alpha-1}) \\
\eta(a)(b_0 + b_1x + \ldots + b_{\beta-2}x^{\beta-1})
\end{pmatrix}
\]

is also in \( C \).

**Theorem 7:** A code \( C \) is a \( Z_2R \)-cyclic code if and only if \( C \) is an \( R[x] \)-submodule of \( R_{a,\beta} \).

### III. Examples

In this section we introduce some examples within this family of codes which have good parameters.

**Example 8:** Let \( R_{2,3} = Z_2[x]/(x^2 - 1) \times R[x]/(x^3 - 1) \) and consider a \( Z_2R \)-linear cyclic code of the form \( \mathcal{C} = ((x - 1),(x^2 + x + 1) + u) \). The code \( \mathcal{C} \) has \( 2^2 \times 2^2 = 16 \) codewords.

\[
\mathcal{C} = \begin{cases}
(0,0,0,0), (1,1,1 + u, 1), (1, 1, 1 + u, 1 + u, 1), \\
(1, 1, 1 + u, 1), (1, 1, 1 + u, 1 + u, 1 + u), \\
(1, 1, 1, 1 + u), (1, 1, 1 + u, 1 + u), (1, 1, 1 + u, 1 + u), \\
(1, 1, 1, 1), (0, 0, u, u), (0, 0, u, u), (0, 0, 0, u, u), \\
(0, 0, 0, u, 0), (0, 0, 0, 0, u), (0, 0, 0, 0, u)
\end{cases}
\]

**Example 9:** Let \( \mathcal{C} \) be a \( Z_2\overline{R} \)-linear cyclic code of type \((7, 3, 0, 3)\) in the form of \( \mathcal{C} = (1 + x + x^2 + x^4, u(1 + x)) \). Therefore \( \mathcal{C} \) has the generator matrix,

\[
\begin{bmatrix}
1 & 1 & 1 & 0 & 1 & 0 & 0 & u & u & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & u & u & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & u & u & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & u & u & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & u & u & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & u & u
\end{bmatrix}
\]

The Gray image gives the optimal binary linear code with parameters \([21, 6, 8]\).

**Example 10:** Let \( \mathcal{C} \) be a \( Z_2\overline{R} \)-linear cyclic code of type \((15, 15; 4, 1, 0)\) in the form of

\[
\mathcal{C} = \begin{pmatrix}
1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}, 1 + x + x^2 + \\
+ x^{14} + u(1 + x + x^2 + x^4 + x^5 + x^8 + x^{10})
\end{pmatrix}
\]

The Gray image gives the binary linear code which has good parameters \([45, 6, 22]\).

### IV. Conclusion

In this work, linear and cyclic codes are introduced over the ring \( Z_2R \) where \( Z_2 = \{0, 1\} \) is the binary finite field and the ring \( R = \{0, 1, u, u + 1\} \) where \( u^2 = 0 \). Their algebraic structure is studied. It is shown that code \( C \) is a \( Z_2R \)-cyclic code if and only if \( C \) is an \( R[x] \)-submodule of \( R_{a,\beta} \). Our examples show that these codes can be used to construct optimal binary linear codes.

### References