Linear Codes over the Ring $R_m = \mathbb{Z}_{2^m} + u\mathbb{Z}_{2^m}$

Javier Diaz-Vargas, Carlos Jacob Rubio-Barrios

Universidad Autónoma de Yucatán, Facultad de Matemáticas
Periférico Norte Tablaje 13615, Mérida, Yucatán, México

Horacio Tapia-Recillas, Juan Armando Velazco-Velazco

Universidad Autónoma Metropolitana-I, Departamento de Matemáticas
09340, Ciudad de México, México

This article is distributed under the Creative Commons by-nc-nd Attribution License.
Copyright © 2021 Hikari Ltd.

Abstract

Linear codes and a Gray map are considered over the non-chain Frobenius ring $R_m = \mathbb{Z}_{2^m} + u\mathbb{Z}_{2^m}$, $u^2 = 0$. The complete Lee weight enumerator for these codes is defined and the MacWilliams Identity is presented.

Mathematics Subject Classification: 94B05, 94B99

Keywords: Linear codes, MacWilliams, Frobenius ring

1 Introduction

Since the introduction to the study of linear codes over finite rings ([1]) this area of research has been very active. Several results on linear codes over various type of finite rings including chain ring have appeared in the literature. Recently, the study of linear codes over finite non-chain Frobenius rings has received the attention of various research groups ([3]). In this note properties of the ring $R_m$ are given, the Lee weight enumerator is introduced and the MacWilliams Identity is proved for linear codes over this ring.
2 The ring $R_m$

In this section results on the structure of the ring $R_m$ are given, particularly the fact that it is a finite, local, non-chain, Frobenius ring.

Let $m$ be a positive integer, $\mathbb{Z}_{2^m}$ the ring of integers modulo $2^m$ and let $R_m = \mathbb{Z}_{2^m} + u\mathbb{Z}_{2^m}$, $u^2 = 0$. It is easy to see that this ring is isomorphic to the ring $\mathbb{Z}_{2^m}[U]/(U^2)$ so that its elements can be written uniquely as $a + bu$ with $a, b \in \mathbb{Z}_{2^m}$. In the sequel we just refer to the ring $R_m$.

**Theorem 2.1.** The ring $R_m$ is a finite local non-chain Frobenius ring.

**Proof.** It is easy to see that this ring has $2^{2^m}$ elements. The ideal generated by the elements 2 and $u$, $\mathcal{M} = \langle 2, u \rangle$, is the unique maximal ideal and the residue field is $R_m/\mathcal{M} \cong \mathbb{F}_2$. In order to see that $R_m$ is a non-chain ring just observe that the ideals $\langle u \rangle$ and $\langle 2 \rangle$ are not contained each other. To see that it is a Frobenius ring, just observe that it has a unique minimal ideal $\langle 2^{m-1}u \rangle$ ([3]).

The lattice of ideals of the ring $R_m$ is quite interesting and just to illustrate it we include the corresponding lattice for the ring $R_3$.

For $\gamma, \delta \in R_3$ let $I_{\gamma, \delta} = \langle \gamma, \delta \rangle$ be the ideal generated by the elements $\gamma$ and $\delta$ and $U_3$, $M_3$ be the group of units and maximal ideal of the ring $\mathbb{Z}_{2^3}$, respectively. Looking at the elements of $R_3$ we have ([2]):

1. $I_0 = \{0\}$.
2. $I_4 = \langle 4 \rangle = \{0, 4, 4u, 4 + 4u\}$.
3. $I_2 = \langle 2 \rangle = \{a + ub : a, b \in M_3\}$.
4. $I_{4 + 2u} = \langle 4 + 2u \rangle = \{0, 4u, 4 + 2u, 4 + 6u\}$.
5. $I_{4u} = \langle 4u \rangle = \{0, 4u\} = 2M_3^2$.
6. $I_{2u} = \langle 2u \rangle = \{0, 2u, 4u, 6u\} = 2M_3$.
7. $I_u = \langle u \rangle = \{0, u, 2u, 3u, 4u, 5u, 6u, 7u\} = uU_3 \cup uM_3$.
8. $I_{4 + u} = \langle 4 + u \rangle = \{0, 2u, 4u, 6u, 4 + u, 4 + 3u, 4 + 5u, 4 + 7u\} = (4 + uU_3) \cup 2uM_3$.
9. $I_{4, 2u} = \langle 4, 2u \rangle = \{0, 2u, 4u, 6u, 4 + 2u, 4 + 4u, 4 + 6u\} = (4 + 2uM_3) \cup 2uM_3$.
10. $I_{4, u} = \langle 4, u \rangle = \{a + bu : a \in \{0, 4\}, b \in \mathbb{Z}_8\}$. 
11. \( I_{2,u} = \langle 2, u \rangle = \{ a + bu : a \in M_3, b \in \mathbb{Z}_8 \} \).

12. \( I_{2+u} = \langle 2 + u \rangle = (uM_3) \cup (4 + uM_3) \cup (2 + uU_3) \cup (6 + uU_3) \).

\[ R_3 = \mathbb{Z}_8 + u \mathbb{Z}_8 \]

\[ M = \langle 2, u \rangle \]

\[ \langle 4, u \rangle \]

\[ \langle 2 + u \rangle \]

\[ \langle 2 \rangle \]

\[ \langle 4 + u \rangle \]

\[ \langle 4, 2u \rangle \]

\[ \langle 4 \rangle \]

\[ \mathcal{M}_3^1 = \langle 4u \rangle \]

\[ \mathcal{M}_4^1 = \langle 0 \rangle \]

Lattice of ideals of \( R_3 \)

### 3 The Gray map and Lee weight

For a positive integer \( n \) let \( R_m^n \) be the cartesian product of \( R_m \) with itself \( n \) times, which is a ring with the obvious operations. The Gray map on \( R_m^n \) can be defined as:

\[ \phi : R_m^n \rightarrow \mathbb{Z}_2^{2m}, \quad \phi(\bar{a}, \bar{b}) = (\bar{b}, \bar{a} + \bar{b}), \quad \bar{a}, \bar{b} \in \mathbb{Z}_2^{2m}. \]

Observe that this is a linear injective mapping.

Following [2] we can define the Lee weight on the ring \( R_m \). We first observe that in \( \mathbb{Z}_{2^m} \), \( k + (2^m - k) = 0 \), i.e., they are additive inverse to each other and define the Lee weight on \( \mathbb{Z}_{2^m} \) as

\[ wt_L(k) = wt_L(2^m - k) = k, \quad k = 0, 1, 2, \ldots, (2^m - 1). \]

The Lee weight on \( R_m \) is defined as

\[ wt_L(a + ub) = wt_L(b, a + b) \]
where \( wt_L(b, a + b) \) is the Lee weight on \( \mathbb{Z}_{2^m} \) given above. The Lee distance is defined as: \( d_L(x, y) = wt_L(x - y) \). From the above definitions it can be easily seen that,

**Theorem 3.1.** The Gray map introduced above is a linear distance preserving isometry.

Recall that a linear code of length \( n \) over the ring \( \mathbb{R}_m \) is just a submodule of the ring \( \mathbb{R}_m^n \). Thus if \( C \) is such a code, \( \phi(C) \) is a linear code over \( \mathbb{Z}_{2^m} \) of length \( 2n \) and both codes have the same Lee weight enumerator.

## 4 Complete Weight Enumerator and MacWilliams Identity

Recall that the Euclidean inner product on \( \mathbb{R}_m^n \) is

\[
(\overline{x}, \overline{y}) = \overline{x} \cdot \overline{y}^t
\]

where \( \overline{x} = (x_1, \ldots, x_n), \overline{y} = (y_1, \ldots, y_n) \) and \( (\ast)^t \) means the transpose.

If \( C \) is a \( \mathbb{R}_m \)-linear code, its dual code with respect to the Euclidean inner product is:

\[
C^\perp = \{ \overline{c} \in \mathbb{R}_m^n : (\overline{c}, \overline{y}) = 0 \ \forall \ \overline{y} \in C \}.
\]

It can be easily seen that \( C^\perp \) is a \( \mathbb{R}_m \)-linear code of length \( n \). Since the alphabet of the codes is a Frobenius ring, \( |C| \cdot |C^\perp| = 2^{2n} \) ([3]).

Let \( \mathbb{R}_m = \{ t_1, \ldots, t_r \} \) where \( r = 2^{2m} \), be the elements of \( \mathbb{R}_m \). The complete weight enumerator of a \( \mathbb{R}_m \)-linear code \( C \) is defined as follows:

\[
CWE_C(\overline{X}) = \sum_{\overline{c} \in C} X_1^{n_{t_1}(\overline{c})} \cdots X_r^{n_{t_r}(\overline{c})}
\]

where \( \overline{X} = (X_1, \ldots, X_r) \) and \( n_{t_i}(\overline{c}) \) is the number of appearances of \( t_i \) in the codeword \( \overline{c} \).

Observe that the polynomial is homogeneous of degree \( n \) where each monomial has this degree. Also, \( CWE_C(1, \ldots, 1) = |C| \).

Since the ring \( \mathbb{R}_m \) is Frobenius, the MacWilliams Identity for the complete weight enumerator is satisfied ([3]). In order to obtain this identity explicitly we observe the following,
Linear codes over the ring \( R_m = \mathbb{Z}_{2^m} + u\mathbb{Z}_{2^m} \).

**Proposition 4.1.** Let \( R_m = \mathbb{Z}_{2^m} + u\mathbb{Z}_{2^m} \). Then, a generating character for \( \hat{R}_m \), the dual ring, is given by

\[
\chi(a + ub) = \eta_l^{a+b},
\]

where

\[
\eta_l = e^{\frac{i\pi}{2^m-1}} \text{ with } \gcd(2^m, l) = 1,
\]

i.e., \( \eta_l \) is a primitive \( 2^m - 1 \)th root of unity.

**Proof.** It is easy to see that \( 2^{m-1}u \) is the generator of \( \text{Soc}(R_m) \), the socle of the ring \( R_m \). Then

\[
\chi(2^{m-1}u) = \eta_l^{2^{m-1}} = e^{l\pi i} = -1,
\]

since \( \gcd(2^m, l) = 1 \) implies \( l \) is an odd integer. Therefore, \( \chi \) is non-trivial on \( \text{Soc}(R_m) \).

If \( M \) is a \( 2^{2n} \times 2^{2n} \) matrix defined as \( M(i,j) = \chi(t_it_j) \), from [3] it follows,

**Theorem 4.2.** Let \( C \) be a linear code of length \( n \) over the ring \( R_m \) and let \( C^\perp \) be its dual code. Then,

\[
\text{CWE}_{C^\perp}(X) = \frac{1}{|C|} \text{CWE}_C(M \cdot \bar{X}).
\]

**Acknowledgements.** The first and third authors were partially supported by SNI, and the fourth author by fellowship No.764803, CONACYT, México.

**References**


Received: August 23, 2021; Published: September 6, 2021