CODES OVER LOCAL RINGS OF ORDER 16 AND BINARY CODES

STEVEN T. DOUGHERTY AND ESENGÜL SALTÜRK
Department of Mathematics
University of Scranton
Scranton, PA 18510, USA

STEVE SZABO
Department of Mathematics and Statistics
Eastern Kentucky University Richmond
KY 40475, USA

(Communicated by Heide Gluesing-Luerssen)

Abstract. We study codes over the commutative local Frobenius rings of order 16 with maximal ideals of size 8. We define a weight preserving Gray map and study the images of these codes as binary codes. We study self-dual codes and determine when they exist.

1. Introduction

It has become the standard now in many areas of coding theory to assume that the underlying alphabet of a code is a finite Frobenius ring. One of the early papers using this was [8] in which binary codes were constructed via a non-linear Gray map from quaternary codes. This work was followed by papers where Gray maps were defined from all of the rings of order 4, see [3], and then to other rings, see [2, 7, 12]. In general, Gray maps have been a central feature of the study of codes over rings.

Self-dual and formally self-dual codes are important classes of codes and they have canonical connections to finite designs and unimodular lattices. Formally self-dual and self-dual codes have Hamming weight enumerators that are held invariant by the action of the MacWilliams relations. It is a long standing question to determine if there are codes that correspond to each polynomial, with non-negative integer coefficients, that is held invariant by the action of the MacWilliams relations. One such open question is to determine when there are extremal Type II codes of length $24k$.

In [11], foundational results were given for codes over finite Frobenius rings. Namely, Wood shows that both MacWilliams theorems, namely the theorem which determines the weight enumerator of the orthogonal and the theorem that determines equivalences of codes, hold for codes over these rings. Wood’s results were for codes over arbitrary Frobenius rings, but for the remainder of this paper we shall assume that rings in the paper are commutative. It is well known that any finite commutative Frobenius ring is isomorphic via the Chinese Remainder Theorem

2010 Mathematics Subject Classification: Primary: 11T71, 94B05; Secondary: 13H99.
Key words and phrases: Codes over rings, Gray maps.

Esengül Saltürk would like to thank TUBITAK (The Scientific and Technological Research Council of Turkey) for their support while writing this paper.
to a direct product of local Frobenius rings. This isomorphism carries many of the important structural aspects of a code. Hence, there is a great significance to studying codes over local Frobenius rings. Specifically, codes over local Frobenius rings can be thought of as the foundation of codes in general. In the non-commutative case, we do not have the Chinese Remainder Theorem and so we cannot necessarily reduce many coding theory questions to codes over local rings.

In this paper, we study codes over commutative local Frobenius rings of order 16 with $|J(R)| = 8$. We define a Gray map to the binary Hamming space and define a Lee weight based on the Hamming weight of the Gray image. This Gray map is a canonical extension of the usual Gray maps as defined over the local rings of order 4. Our Gray map is presented in a very general form which can be applied to any local Frobenius ring of order 16 with a maximal ideal of size 8. Then we study self-dual and formally self-dual codes over these rings and examine their binary images.

### 2. Definitions and notations

The rings in this paper, which are used as alphabets for codes, have a multiplicative identity and are assumed to be commutative and finite. A ring is a local ring if it has a unique maximal ideal and a chain ring is a local ring where the ideals are linearly ordered by inclusion. It follows that the ideals in a chain ring are principal and that the ideals are of the form

$$\{0\} \subset \langle \gamma^{e-1} \rangle \subset \langle \gamma^{e-2} \rangle \subset \cdots \subset \langle \gamma \rangle \subset R,$$

with $\gamma^{e-1} \neq 0$. The number $e$ is said to be the index of nilpotency of the ring.

For a module $M$ over a ring $R$ define $\widehat{M} = \text{Hom}_R(M, \mathbb{C}^*)$. Note that $\mathbb{C}^*$ can be replaced with $\mathbb{Q}/\mathbb{Z}$ if we want to use an additive model rather than a multiplicative one. Suppose $R$ is a finite ring. The following are equivalent: (1) $R$ is a Frobenius ring; (2) as a left module, $\widehat{R} \cong R^2$; (3) as a right module $\widehat{R} \cong R^2$. We shall only be concerned with rings that are Frobenius in this paper. It has been established, see [11], that this is the class of rings which can serve as a useful alphabet for codes.

Since we assume all rings are commutative, it simplifies the following definitions. The Jacobson radical $J(R)$ of a ring $R$ can be characterized as the intersection of all maximal ideals. In a commutative local ring the Jacobson radical is necessarily the unique maximal ideal. The socle of a ring $R$, $\text{Soc}(R)$, is defined as the sum of all the minimal ideals of the ring.

In Theorem 3.10 (4a) of [10], the list of local Frobenius rings of order 16 with Jacobson radical of size 8 was presented. Five of the rings are chain rings, $F_2[x]/(x^4)$, $\mathbb{Z}_4[x]/(x^2 - 2), \mathbb{Z}_4[x]/(x^2 - 2x - 2), \mathbb{Z}_4[x]/(x^3 - 2, 2x)$ and $\mathbb{Z}_{16}$ and seven of them are non-chain rings, $F_2[u, v]/(u^2, v^2)$, $F_2[u, v]/(u^2 + v^2, uv)$, $\mathbb{Z}_4[x]/(x^2 - 2x), \mathbb{Z}_4[x]/(x^2), \mathbb{Z}_4[x, y]/(x^2 - 2, xy - 2, y^2, 2x, 2y), \mathbb{Z}_4[x, y]/(x^2 - 2, xy - 2, y^2, 2x, 2y)$ and $\mathbb{Z}_8[x]/(x^2 + 4, 2x)$.

In all of these rings we have that the maximal ideal $\mathfrak{m}$ is the Jacobson radical of the ring and $\mathfrak{m}^2 = \text{Soc}(R)$. For the non-chain rings we have $\mathfrak{m}^2 = \text{Soc}(R)$. For the chain rings we have $\mathfrak{m}^3 = \text{Soc}(R)$. In both cases we have that $|\text{Soc}(R)| = 2$.

**Remark 1.** The nilpotency of $J(R)$ for any ring under consideration is less than or equal to 4. From this we see that the group of units for each ring is isomorphic to either $C_2 \times C_2 \times C_2$ or $C_2 \times C_4$. Of the 12 rings being considered, the only 3 rings with the group of units isomorphic to $C_2 \times C_2 \times C_2$ are $F_2[u, v]/(u^2, v^2)$, $\mathbb{Z}_4[x]/(x^2 - 2x)$ and $\mathbb{Z}_4[x, y]/(x^2, xy - 2, y^2, 2x, 2y)$.
Given a ring $R$, we say that a code of length $n$ is a subset of $R^n$. If the code is a submodule we say that the code is linear. If $C$ is a code then the weight enumerator with respect to a weight, denoted by $\text{wt}$, is

$$W_C(x,y) = \sum_{c \in C} x^{N - \text{wt}(c)} y^{\text{wt}(c)},$$

where $N$ is the maximum weight for a vector of length $n$. We attach to the ambient space the Euclidean inner-product, namely $\langle v, w \rangle = \sum v_i w_i$. We define an orthogonal with respect to this inner-product, namely $C^\perp = \{v | \langle v, w \rangle = 0, \forall w \in C \}$. The code $C^\perp$ is always linear whether or not $C$ is and it follows from the foundational results in [11] that $|C| |C^\perp| = |R|^n$ when $C$ is a linear code over Frobenius ring $R$.

If $C = C^\perp$ we say that the code $C$ is self-dual and if $C \subseteq C^\perp$ we say that the code $C$ is self-orthogonal. If a code $C$ satisfies $W_C(x,y) = W_{C^\perp}(x,y)$ then we say that the code is formally self-dual with respect to that weight.

3. Local rings of order 16

In this section, let $R$ be a local Frobenius ring of order 16 with a maximal ideal of size 8. Then $R/J(R) \cong \mathbb{F}_2$. In any case, there exist $u, v, w \in R$ with $J(R) = \langle u, v \rangle$ and $\text{Soc}(R) = \langle w \rangle = \{0, w\}$. If $R$ is a chain ring, we actually have $J(R) = \langle u \rangle$, $J(R)^2 = \langle v \rangle$ and $\text{Soc}(R) = \langle w \rangle$ where $v = u^2$ and $w = u^3$. The ideals for such a ring are described in Figure 1.

Every element of these rings can be written uniquely in the form $a + bu + cv + dw$ where $a, b, c, d \in \{0, 1\}$. Note that we are not saying that the group structure of the additive group is $C_2^3$, but rather that the elements have a unique representation of this form. We shall use the fact that every element can be written in this form to construct a Gray map for any ring in this family.

There are two local rings of order 4 that are not fields, namely $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{Z}_4$. Both of these have a well known Gray map. It is possible to describe both Gray maps as $\Phi : R \to \mathbb{F}_2^2$ by $\Phi(a + bv) = (b, a + b)$ where $v = 2$ in $\mathbb{Z}_4$ and $v = u$ in

![Figure 1. Diagram for the chain ring](image-url)
\(F_2 + uF_2\). Notice that in both of these rings we are able to write the elements as \(a + bv\) where \(a, b \in F_2\). Note that this is not saying that the group structure is \(C_2 \times C_2\) but rather that the elements can be placed into that form. We can extend these maps to rings where the elements can be written as \(a + bu + cv + dw\) where \(a, b, c, d \in \{0, 1\}\). Namely, we view the elements as being of the form \((a + cv) + (b + dv)u\) and apply the order 4 Gray map twice (allowing for an abuse of notation), that is, once in terms of \(u\) and then in terms of \(v\). Specifically, we apply this Gray map to the element \(\alpha + \beta u\) where \(\alpha = a + bv\) and \(\beta = c + dv\) to get \((\beta, \alpha + \beta)\). Then we apply the Gray map to \(\alpha\) and \(\beta\). Namely, we send \(\alpha\) to \((b, a + b)\) and \(\beta\) to \((d, c + d)\). Hence we make the following definition of the Gray map. For a finite local Frobenius ring \(R\) of order 16 with Jacobson radical of size 8, we define the Gray map \(\phi : R \to F_4^2\) as

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

**Theorem 3.1.** The map \(\phi : R \to F_4^2\) is bijective. Furthermore, \(\phi\) is \(F_2\)-linear if and only if \(\text{char} R = 2\).

**Proof.** If \((d, c + d, b + d, a + b + c + d) = (d', c' + d', b' + d', a' + b' + c' + d'),\) then by comparing the first coordinates \(d = d'\). Comparing the second and third coordinates gives that \(b = b'\) and \(c = c'\). Then comparing the fourth coordinates we have \(a = a'\). Hence the map is bijective.

If the ring does not have characteristic 2, then \(\phi(1 + 1) \neq \phi(1) + \phi(1) = (0, 0, 0, 0)\). If the ring has characteristic 2 it is a simple computation to show linearity. 

The rings of characteristic 2 are \(F_2[u, v]/\langle u^2, v^2 \rangle\), \(F_2[u, v]/\langle u^2 + v^2, uv \rangle\) and \(F_2[x]/\langle x^4 \rangle\). In many ways it is the non-linear case which is the most interesting, as it is in the case for the quaternary Gray map. For the ring \(F_2[u, v]/\langle u^2, v^2 \rangle\) we have that \(\phi(C^\perp) = \phi(C)^\perp\), however this is not true in general for the rings of characteristic 2. For example, it is not true for \(F_2[u, v]/\langle u^2 + v^2, uv \rangle\). 

---

**Figure 2.** Diagram for the non-chain ring
Let $w_L(x)$ denote the Lee weight of the element $x \in R$ where $w_L(x)$ is defined to be the Hamming weight of $\phi(x)$. It can be seen that

$$w_L(x) = \begin{cases} 
0 & \text{if } x = 0, \\
1 & \text{if } x \in \{1, 1+u, 1+v, 1+u+v+w\} \subset U(R), \\
2 & \text{if } x \in \{u, v, u+v, u+w, v+w, u+v+w\} = J(R) \setminus \text{Soc}(R), \\
3 & \text{if } x \in \{1+u+v, 1+w, 1+u+w, 1+v+w\} \subset U(R), \\
4 & \text{if } x = w \in \text{Soc}(R).
\end{cases}$$

Note that the weight is odd if and only if the element is a unit. This is important in that what we want is that the weights of the elements in the maximal ideal all have even weight and that the non-zero element in the socle has the largest weight. The reason for this becomes apparent in Theorem 4.6. Notice the map $\phi$ is not necessarily linear but it is weight preserving.

In [7], another Gray map equivalent to $\phi$ was defined. It is also possible to define another Gray map on the local rings of order 16 with a maximal ideal of size 8. On the set $\{1, u, v, w\}$ define a poset where $1 \leq u$, $1 \leq v$, $u \leq w$, $v \leq w$ and $u$ and $v$ are not comparable. This poset is given in the following diagram:

```
    w
   / \n u   v
 / \  
1
```

View the elements of the ring as an $F_2$ vector space with basis $1, u, v, w$. For $\alpha \in \{1, u, v, w\}$, define $\psi(\alpha) = c = (c_1, c_u, c_v, c_w)$ where

$$c_\beta = \begin{cases} 
1 & \text{if } \beta \leq \alpha \\
0 & \text{otherwise}.
\end{cases}$$

Then extend $\psi$ linearly over $F_2$. Note that the Lee weight increases with respect to the ordering of the poset and that the Lee weights defined for $\psi$ and $\phi$ are the same. Additionally, this vector space can be viewed as the mod 2 group algebra of the Klein-4 group, where the Hamming weight respect to the basis of group elements corresponds to the Lee weight as we have defined it.

**Theorem 3.2.** The map $\psi$ is equivalent to the map $\phi$ via the permutation $(14)(23)$.

**Proof.** Follows from a straightforward computation. $\square$

The rank of a code $C$ is the minimum number of generators of $C$. Let $d_L(C)$ denote the minimum Lee weight of all non-zero vectors in $C$. Using the same proof as was given in [6], we have the following.

**Theorem 3.3.** Let $C$ be a linear code over $R$, then

$$\left\lfloor \frac{d_L(C) - 1}{4} \right\rfloor \leq n - \text{rank}(C).$$

Using the Lee weight we can now define the following Lee weight enumerator:

$$L_C(x, y) = \sum_{c \in C} x^{4n - w_L(c)}y^{w_L(c)}$$
where \( wt_L(c) \) is the weight of a codeword \( c \in C \). Notice that \( 4n \) is the maximal Lee weight of any vector of length \( n \). This weight enumerator coincides with the Hamming weight enumerator of the image of the code \( \phi(C) \) in the space \( \mathbb{F}_2^n \). That is \( L_C(x, y) = W_{\phi(C)}(x, y) \).

We shall say that a formally self-dual code code is Type II if all Lee weights in the code are doubly-even, Type I if all Lee weights are even and Type 0 otherwise.

**Example 1.** Take the ring \( R = \mathbb{Z}_4[x]/(x^2 - 2x) \). Let \( C \) be a code of length \( n = 2 \) over \( R \) generated by the following vectors \((2, 0)\) and \((0, 2)\). Then \( C = \{(0, 0), (2, 0)(2x, 0), (2 + 2x, 0), (0, 2), (2, 2), (2x, 2), (2 + 2x, 2), (0, 2x), (2, 2x), (2x, 2), (2 + 2x, 2), (0, 2x), (2, 2x), (2x, 2), (2 + 2x, 2)\} \). It can be easily seen that \( C \) is a Type I Lee formally self-dual code since the weights are all even. The Lee weight enumerator of \( C \) is \( L_C(x, y) = (x^2 + y^2)^4 \). Then we get \( L_C(x, y) = \frac{1}{|C|} L_C(x + y, x - y) \).

**Example 2.** Consider the code over \( \mathbb{Z}_{16} \) generated by \((1, 9)\). This code is not Lee formally self-dual nor is it self-dual, however, its image has weight enumerator \( x^8 + 14x^4y^4 + y^8 \) which only has doubly-even weights and is held invariant by the action of the MacWilliams relations. Namely, given the weight enumerator of the code \( C \), \( W_C(x, y) \), we have that \( W_C(x, y) = \frac{1}{|C|} W_C(x + y, x - y) \).

These examples show that this Gray map is useful to study binary codes (possibly non-linear) which have weight enumerators which are held invariant by the action of the MacWilliams relations.

An example of a Type 0 formally self-dual code will be given in Theorem 4.9.

### 4. Self-Dual Codes

Self-dual codes are an important class of codes. They have numerous connections to unimodular lattices and design theory. In this section, we shall describe self-dual codes over local Frobenius rings of order 16 and examine their images under the Gray map.

We shall determine the existence for Type I and Type II self-dual codes. It will be shown that there are no Type 0 self-dual codes.

**Theorem 4.1.** Let \( C \) be a self-dual code over a local Frobenius ring of order 16 with a maximal ideal of size 8. Then \( C \) contains the all \( w \) vector.

**Proof.** Let \( v = (v_i) \) be a vector in \( C \). Then \( \sum v_i^2 = 0 \) which implies there is an even number of units among the \( v_i \). If \( v_i \in m \) then \( v_i w = 0 \). If \( v_i \) is a unit then \( v_i w = w \). This gives that \([v, (w, w, \ldots, w)] = 2\beta w = 0 \) for some integer \( \beta \). Hence \((w, w, \ldots, w) \in C^4 = C \).

This leads to the following corollary.

**Corollary 1.** The image of a self-dual code over a local Frobenius ring of order 16 with a maximal ideal of size 8 contains the all-one vector.

**Proof.** The result follows from the previous theorem noting that the image of the all \( w \) vector by the Gray map is the all-one vector.

The following well known lemma is easily proven.
Lemma 4.2. If $C$ and $D$ are self-dual codes over a Frobenius ring $R$ of length $n$ and $m$ respectively then $C \times D$ is a self-dual code of length $nm$. If $C$ and $D$ are formally self-dual codes of length $n$ and $m$ respectively then $C \times D$ is a formally self-dual code of length $nm$.

We shall now examine the existence of self-dual codes.

Lemma 4.3. There exists a Type I self-dual code of length 1 over all local Frobenius rings of order 16.

Proof. Let $R$ be a local Frobenius ring of order 16 with a maximal ideal of size 8 that is not a chain ring. There are precisely 3 ideals of order 4 namely $\langle u \rangle, \langle v \rangle$ and $\langle u + v \rangle$. Given an ideal $a$ of order 4, $a^\perp$ is an ideal of order 4. Take an ideal $a$, if $a = a^\perp$ then there is a self-dual code of length 1. If $a \neq a^\perp$, then $a^\perp$ is one of the other ideals. Hence the third ideal must be a self-dual code of length 1.

If the ring is a chain ring then there is a unique ideal of order 4, hence its orthogonal must be of size 4 so it must be self-dual.

Since all the elements in the self-dual code are in the maximal ideal, the Lee weights must all be even. Hence the code is Type I.

Notice that this lemma implies that there are either one or three self-dual codes of length 1 in this case. For chain rings there can be only one self-dual code of length 1 since there is only one ideal of the proper order. The image under the Gray map of any of these possible length 1 codes is a $[4,2,2]$ binary self-dual code. It is possible that all three ideals are self-dual codes of length 1. For example, in the ring $F_2[u,v]/\langle u^2, v^2, uv = vu \rangle$, the codes $\langle u \rangle, \langle v \rangle$ and $\langle u + v \rangle$ are all self-dual codes of length 1. In the ring $F_2[u,v]/\langle u^2 + v^2, uv \rangle$ only the ideal $\langle u + v \rangle$ is self-dual. In this ring $\langle u \rangle^\perp = \langle v \rangle$.

For the rings in our collection of characteristic 4, we have that $\langle 2 \rangle$ is always a self-dual code of length 1. In the ring $\mathbb{Z}_4[x]/\langle x^2 - 2x \rangle$, $\langle 2 \rangle$ is the only self-dual code of length 1 and in the ring $\mathbb{Z}_4[x]/\langle x^2 \rangle$ there are three, namely $\langle 2 \rangle, \langle x \rangle$ and $\langle x + 2 \rangle$.

Lemma 4.3 leads to the following theorem.

Theorem 4.4. There exist self-dual codes of all lengths for all local Frobenius rings of order 16 with maximal ideal of size 8.

Proof. There exist self-dual codes of length 1 by Lemma 4.3. Then by Lemma 4.2 and noticing that the Cartesian product of Type I codes is Type I, we have that Type I self-dual codes of all lengths exist.

Theorem 4.5. Let $R$ be a local non-chain Frobenius ring of order 16 with a maximal ideal of size 8 where there is only one self-dual code of length 1. Then there exists a Type I Lee formally self-dual code of length 1 that is not self-dual.

Proof. We know that there are three ideals of order 4 in $R$, namely $\langle u \rangle, \langle v \rangle$ and $\langle u + v \rangle$. Moreover, each of these ideals contain the socle which is $\{0, w\}$. If there is only one self-dual code then the other ideals of order 4 are duals of each other. Assume that the ideals $\langle \alpha \rangle$ and $\langle \beta \rangle$ are duals of each other. Then $\langle \alpha \rangle = \{0, \alpha, w, \alpha + w\}$ and $\langle \beta \rangle = \{0, \beta, w, \beta + w\}$. In either case, the ideals have two elements with Lee weight 2, one element with Lee weight 0 and one element with Lee weight 4. Hence they have identical Lee weight enumerators. Thus $\langle \alpha \rangle$ and $\langle \beta \rangle$ are Type I Lee formally self-dual codes that are not self-dual of length 1.
As an example of the previous theorem, consider the ring $F_2[u,v]/(u^2 + v^2, uv)$. The ideals $\langle u \rangle$ and $\langle v \rangle$ are Lee formally self-dual codes that are not self-dual. The image of both of these codes is the linear $[4,2,2]$ binary self-dual code. This shows that the image of Lee formally self-dual code that is not self-dual can in fact be self-dual.

We shall now examine the case for Type II codes.

**Theorem 4.6.** There exist Type II self-dual codes of length 2 for all local non-chain Frobenius rings of order 16 with maximal ideal of size 8.

**Proof.** Let $R$ be a local non-chain Frobenius ring of order 16 with $\text{Soc}(R) = \langle w \rangle$. Consider the code $C = \{(x, x) \mid x \in J(R)\}$. Let $x \in J(R)$, then $[(x, x), (0, w)] = xw = 0$ since $w \in J(R) = \text{Soc}(R)$. Also, $[(x, x), (x, x)] = 2x^2$. Since $J(R)^2 = \text{Soc}(R)$, we have that $x^2 \in \text{Soc}(R)$. Then $2y = 0$ for all $y$ in $\text{Soc}(R)$ since it is isomorphic to the field with two elements. Hence, the code $C$ is self-orthogonal. Then the code has $|C| = 16$ and is of length 2 with $C \subseteq C^\perp$. Therefore $C = C^\perp$ and $C$ is self-dual. If $v \in C - \{0\}$ is of the form $(x, x)$, $x \in J(R)$, then the Lee weight is $2 + 2 = 4$ unless $x = w$ where the Lee weight is $4 + 4 = 8$. If $v \in C$ is of the form $(x, x + w)$, $x \in m$, then if $x \neq w$ the Lee weight is $2 + 2 = 4$ and if $x = w$ then $v$ has Lee weight 4. Hence $C$ is a Type II self-dual code.

The code $\phi(C)$, where $C$ is the code given in Theorem 4.6, is equivalent to the $[8,4,4]$ binary Hamming code. We give an example for a specific ring which describes the code in Theorem 4.6.

**Example 3.** Let $C$ be a code over $R = \mathbb{Z}_4[x]/\langle x^2 - 2x \rangle$ generated by the following matrix

\[
G = \begin{pmatrix}
2 & 2 \\
2 + x & 2 + x \\
0 & 2x
\end{pmatrix}.
\]

Then $G$ generates a Type II self-dual code over $R$.

In [13], the authors find a Type II self-dual code over $F_2[u,v]/(u^2, v^2)$ whose image under $\phi$ is the extended binary Golay code.

Notice that in the chain ring case, $J(R)^2$ may not be $\text{Soc}(R)$ so the above construction may not work. For example, over $\mathbb{Z}_{16}$ which is a chain ring with Jacobson radical of size 8, the construction would give the generator matrix \( \begin{pmatrix} 2 & 2 \\ 0 & 8 \end{pmatrix} \). However, the vector $(2,2)$ has $[(2,2), (2,2)] = 8 \neq 0$ and the vector is not self-orthogonal.

However, we can prove the following similar result.

**Theorem 4.7.** There exist Type II self-dual codes of length 4 for all Frobenius chain rings of order 16 with maximal ideal of size 8.

**Proof.** Let $\gamma$ be the generator of the maximal ideal in a chain ring $R$ of order 16 with $|\langle \gamma \rangle| = 8$. Consider the code generated by the following matrix:

\[
H = \begin{pmatrix}
\gamma & \gamma & \gamma & \gamma \\
0 & \gamma^2 & \gamma^2 & 0 \\
0 & 0 & \gamma^2 & \gamma^2 \\
0 & 0 & 0 & \gamma^3
\end{pmatrix}.
\]

Note that each vector has even Hamming weight in the code generated by the first three rows of the matrix with elements in the maximal ideal. Therefore all of these vectors have doubly-even Lee weight.
The only vectors in the code with odd Hamming weight have a $\gamma^3$ in them which has Lee weight 4 so these vectors have doubly-even Lee weight as well. Then note that $\gamma^3 \in \text{Soc}(R)$ so $\gamma^3 + \gamma^3 = 0$ which gives that the rows are mutually orthogonal. Hence the code is a Type II self-dual code.

**Corollary 2.** There exist Type II codes of all even lengths over local non-chain Frobenius rings of order 16 with maximal ideal of size 8. There exist Type II codes of all lengths a multiple of 4 over local Frobenius chain rings of order 16 with maximal ideal of size 8.

**Proof.** Follows from Lemma 4.2 and noticing that the Cartesian product of Type II codes is Type II.

Of course, if the image of a Type II self-dual code is linear then it must be a self-dual code since it contains only doubly-even binary codewords. However, the binary code may be non-linear and so not self-dual.

**Theorem 4.8.** If $C$ is a self-dual code over a local Frobenius ring of order 16 with maximal ideal of size 8 then it must be Type I or Type II.

**Proof.** Since all the elements in the maximal ideal have even Lee weights, then a vector with odd Lee weight must have an odd number of units. However, a vector $v$ with an odd number of units has an odd number of units in $\{v_i^2\}$ which means it is not self-orthogonal.

While there are no Type 0 self-dual codes, there are Type 0 formally self-dual codes as in the following.

**Theorem 4.9.** There exist Type 0 Lee formally self-dual codes of all even lengths over any Frobenius ring.

**Proof.** The code $\langle (1,0) \rangle$ is a Type 0 Lee formally self-dual code of length 2. Then apply the Cartesian product and we have Type 0 Lee formally self-dual codes of all even lengths.

Of course, if a local Frobenius non-chain ring of order 16 with maximal ideal of size 8 has only one self-dual code of length 1 then there exist Lee formally self-dual codes of length 1. In these cases, Lee formally self-dual codes exist for all lengths.

We can use the generating element of a self-dual code of length 1 to construct other self-dual codes.

**Theorem 4.10.** Let $C$ be a self-orthogonal code of length $n$ over a local Frobenius ring $R$ of order 16 with a maximal ideal of size 8. Let $\alpha$ be a principal generator of the self-dual code of length 1. Then $\langle C, (C^\perp \cap \alpha R^n) \rangle$ is a self-dual code of length $n$.

**Proof.** In the non-chain ring case there exists a self-dual code of length 1 either generated by $u, v$ or $u + v$. Call this element that generates the self-dual code $\alpha$. In the chain ring case there is a unique choice for $\alpha$. Consider vectors $v, v' \in C$ and $\alpha w, \alpha w' \in C^\perp$. Note that $w, w'$ may not be in $C^\perp$, but any vector in this intersection $C^\perp \cap \alpha R^n$ is of the form $\alpha w$ for some vector $w$. Then

$$[v + \alpha w, v' + \alpha w'] = [v, v'] + [v, \alpha w'] + [\alpha w, v'] + [\alpha w, \alpha w']$$

$$= 0 + 0 + 0 + \alpha^2 [w, w'] = 0.$$
since $\alpha^2 = 0$. Hence the code is self-orthogonal. Then we have
\[
\langle C, (C^\perp \cap \alpha R^n) \rangle^\perp = C^\perp \cap (C^\perp \cap \alpha R^n) \cap C^\perp \cap (C, \alpha R^n)
\]
since $(\alpha R^n)^\perp = \alpha R^n$.

Then
\[
C^\perp \cap \langle C, \alpha R^n \rangle = \langle C, (C^\perp \cap \alpha R^n) \rangle.
\]

Therefore the code is self-dual. \hfill \Box

Notice that it is possible that there is more than one $\alpha$ that could be used in the previous theorem. We shall now illustrate this point and show two different cases in the construction of this self-dual code. Consider the ring $R = \mathbb{Z}_4[x]/(x^2)$. Let $C$ be the self-orthogonal code $C = \{ (\beta, \beta) \mid \beta \in m \}$, where $m$ is the unique maximal ideal which is $(2, x)$. The code $C$ can be seen as generated by the vectors $(2, 2)$ and $(x, x)$. Take the code $C_1 = \langle C, (C^\perp \cap xR^n) \rangle$. This code $C_1$ can be seen as an element of the code $C^\perp$. As such $\langle C, (C^\perp \cap xR^n) \rangle = \langle C, xC^\perp \rangle$. By the theorem, $C_1$ is a self-dual code of length 2. Now consider the code $C_2 = \langle C, (C^\perp \cap 2R^n) \rangle$. The code $C_2$ can be seen as $\langle C, (\{(2x^2 + 2, 2)\}) \rangle$. Notice here that $C_2 \neq \langle C, 2C^\perp \rangle$ since $(2x^2 + 2, 2) \neq 2(\beta_1, \beta_2)$ for any $(\beta_1, \beta_2) + C^\perp$. Note however that $(2x^2 + 2, 2)$ is in $C^\perp$. These examples show why the theorem requires $\langle C, (C^\perp \cap \alpha R^n) \rangle$ rather than simply $\langle C, \alpha C^\perp \rangle$ and the difference a choice of $\alpha$ can make.

We shall now investigate when free self-dual codes exist. A code $C$ is free if it is isomorphic to $R^k$ for some integer $k$.

**Lemma 4.11.** Let $C$ be a free self-dual code of length $n$ over a local Frobenius ring $R$ of order 16 with a maximal ideal of size 8. Then $n$ is even.

**Proof.** Since $C$ is a free self-dual code, $|C|^2 = |R|^n$. This gives $|R|^{2k} = |R|^n$ for an integer $k$ which gives that $n$ is even. \hfill \Box

**Lemma 4.12.** Let $R$ be a local Frobenius ring of order 16 with Jacobson radical of size 8 such that there exists $a, b \in R$ with $a^2 + b^2 = -1$. Then the following are true:

1. The element $2 \in J(R)^2$.
2. The characteristic of the ring, $\text{char } R \in \{2, 4\}$.
3. If $\text{char } R = 4$ then $U(R) \cong C_2 \times C_2$.

**Proof.** Since $R/J(R) \cong \mathbb{F}_2$ and $1 = -a^2 - b^2$ we have that either $a$ or $b$ is a unit and the other is in $J(R)$. Assume $a$ is a unit. Now, $a^2 = 1 + s$ where $s \in J(R)^2$. Then
\[
-1 + 2 + s = 1 + s = a^2 = -1 - b^2 = -1 - b^2,
\]
which gives that $2 = -(s + b^2) \in J(R)^2$. Since the nilpotency of $J(R)$ is less than or equal to 4 and $2 \in J(R)^2$, $\text{char } R \in \{2, 4\}$. By Remark 1, $U(R)$ is isomorphic to $C_2 \times C_2 \times C_2$ or $C_2 \times C_4$.

Assume $\text{char } R = 4$ and $U(R) \cong C_2 \times C_2 \times C_2$. Then $a^2 = 1 = (1 + b)^2$, which gives
\[
a^2 = (1 + b)^2 = 1 + 2b + b^2 = 1 + 2b - 1 - a^2 = 2b - a^2,
\]
which gives that $0 = 2b - 2a^2 = 2(b - a^2)$. This is a contradiction since $\text{char } R = 4$ and $b - a^2$ is a unit. Hence, if $\text{char } R = 4$ then $U(R) \cong C_2 \times C_4$. \hfill \Box

**Lemma 4.13.** Let $R$ be a local Frobenius ring of order 16.
1. A free self-dual code exists over $R$ for all even lengths if and only if there exists a $\gamma \in R$ such that $\gamma^2 = -1$.

2. A free self-dual code exists over $R$ for all lengths a multiple of 4 if and only if there exist $a, b \in R$ such that $a^2 + b^2 = -1$.

Proof. If there exists $\gamma \in R$ such that $\gamma^2 = -1$, then $(1, \gamma)$ generates a free self-dual code of length 2. Then by Lemma 4.2, there exists self-dual codes of all even lengths.

Assume there exists a free self-dual code of all even lengths. Then there exists a free self-dual code of length 2. This implies that this code is permutation equivalent to a code generated by a vector of the form $(1, b)$ for some $b \in R$. Hence, $1 + b^2 = 0$ showing $b^2 = -1$.

If there exist $a, b \in R$ such that $a^2 + b^2 = -1$, then $(1, 0, a, b)$ and $(1, 0, -b, a)$ generate a free self-dual code of length 4. Then by Lemma 4.2, there exist self-dual codes of all lengths a multiple of 4.

Assume there exists a free self-dual code of all lengths a multiple of 4. Then there exists a free self-dual code of length 4. This implies that this code is permutation equivalent to a code generated by vectors of the form $(1, 0, a, b)$ and $(0, 1, c, d)$ for some $a, b, c, d \in R$. Hence, $1 + a^2 + b^2 = 0$ showing that $a^2 + b^2 = -1$.

Theorem 4.14. Let $R$ be a local Frobenius ring of order 16 with Jacobson radical of size 8 over which there exists a free self-dual code of all even lengths are $\mathbb{F}_2[u, v]/(u^2, v^2)$, $\mathbb{F}_2[u, v]/(u^2 + v^2, uv)$, $\mathbb{Z}_4[x]/(x^2 - 2x - 2)$, $\mathbb{Z}_4[x,y]/(x^2 - 2, xy - 2, y^2, 2x, 2y)$. If there does not exist such a $\gamma$ in $R$ but there exist $a, b \in R$ with $a^2 + b^2 = -1$ then $R$ is isomorphic to $\mathbb{Z}_4[x]/(x^2 - 2)$.

Proof. In any ring of characteristic 2, we have that $-1 = 1 = 1^2$. Therefore, the local Frobenius rings with maximal ideal of size 8 and characteristic 2 have a square that is $-1$. Of the remaining rings, by Lemma 4.12, we need only check the rings $\mathbb{Z}_4[x]/(x^2 - 2)$, $\mathbb{Z}_4[x]/(x^2 - 2x - 2)$, $\mathbb{Z}_4[x]/(x^2 - 2, 2x)$ and $\mathbb{Z}_4[x,y]/(x^2 - 2, xy - 2, y^2, 2x, 2y)$. In each of these rings $(1 + x)^2 \neq 1$. The fact that $U(R) \cong Z_2 \times Z_4$ for any of these rings gives that there is an $a \in R \setminus \{1\}$ where the square of any unit is either 1 or $a$. We see that for the rings $\mathbb{Z}_4[x]/(x^2 - 2)$ and $\mathbb{Z}_4[x]/(x^3 - 2, 2x)$, we have that $(1 + x)^2 \neq -1$ and for the rings $\mathbb{Z}_4[x]/(x^2 - 2x - 2)$ and $\mathbb{Z}_4[x,y]/(x^2 - 2, xy - 2, y^2, 2x, 2y)$, we have that $(1 + x)^2 = -1$. In the ring $\mathbb{Z}_4[x]/(x^2 - 2)$, we have that $1^2 + x^2 = -1$.

Finally, we show that there is no $a, b \in \mathbb{Z}_4[x]/(x^3 - 2, 2x)$ with $a^2 + b^2 = -1$. To that end, assume there is $a, b$ with $a^2 + b^2 = -1$. We have seen in the proof of Lemma 4.12, that we may assume $a$ is a unit and $b \in J(\mathbb{Z}_4[x]/(x^3 - 2, 2x))$. Then $a$ and $1 + b$ are units. Note that since $2 \in Soc(\mathbb{Z}_4[x]/(x^3 - 2, 2x))$, we have that $2b = 0$. Then we have $(1 + b)^2 = 1 + 2b + b^2 = 1 + 2b - 1 - a^2 = 2b - a^2 = -a^2$. This implies $(1 + b)^2a^{-2} = -1$ which is a contradiction.

The following corollary is a direct consequence of Lemma 4.13 and Theorem 4.14.

Corollary 3. The only local Frobenius rings of order 16 with Jacobson radical of size 8 over which there exists a free self-dual code of all even lengths are $\mathbb{F}_2[u, v]/(u^2, v^2)$, $\mathbb{F}_2[u, v]/(u^2 + v^2, uv)$, $\mathbb{Z}_4[x]/(x^2 - 2x - 2)$ and $\mathbb{Z}_4[x,y]/(x^2 - 2, xy - 2, y^2, 2x, 2y)$. In addition to these rings, the only other local Frobenius ring of order 16 with Jacobson radical of size 8 over which there exists a free self-dual code of all lengths a multiple of 4 is $\mathbb{Z}_4[x]/(x^2 - 2)$. 
Lemma 4.15. Let $S$ be a subring of the Frobenius ring $R$. If $C$ is a self-dual code in $S^n$ with generator matrix of the form $(I_n | A)$ then $(C) \subseteq R^n$ is a free self-dual code.

Proof. Since the generator matrix is of the form $(I_n | A)$ then the generated code has size $|R|^n$.

Then if $v_i, w_j \in S^n$ and $\alpha_i, \beta_j \in R$ we have that
$$\sum \alpha_i v_i, \sum \beta_j w_j = \sum \alpha_i \beta_j [v_i, w_j] = 0,$$
giving that the code is self-orthogonal. Therefore, the code is self-dual. \hfill \Box

We can use this lemma to find free self-dual codes even when Lemma 4.13 may not apply. For rings of characteristic 4, the ring contains $Z_4$ as a subring. The following matrix generates a free self-dual code in $Z_8^4$:

$$\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & 3 & 1 & 0 \\
0 & 0 & 1 & 0 & 3 & 3 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 0 & 3 & 1
\end{bmatrix}.$$

For rings of characteristic 8, the ring contains $Z_8$ as a subring. The following matrix generates a free self-dual code in $Z_8^8$:

$$\begin{bmatrix}
1 & 0 & 0 & 0 & 2 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 7 & 7 & 1 & 2 \\
0 & 0 & 1 & 0 & 7 & 2 & 7 & 1 \\
0 & 0 & 0 & 1 & 7 & 1 & 2 & 7
\end{bmatrix}.$$

In our family of rings there is only one ring with characteristic 16, namely $Z_{16}$. The following matrix generates a free self-dual code in $Z_{16}^8$:

$$\begin{bmatrix}
1 & 0 & 0 & 0 & 3 & 2 & 1 & 1 \\
0 & 1 & 0 & 0 & 14 & 3 & 1 & 15 \\
0 & 0 & 1 & 0 & 1 & 13 & 14 & 3 \\
0 & 0 & 0 & 1 & 15 & 14 & 3 & 1
\end{bmatrix}.$$

Then using Lemma 4.15 we have the following theorem.

Theorem 4.16. Let $R$ be a local Frobenius ring of order 16 with Jacobson radical of size 8. Then there exist free self-dual codes of all lengths a multiple of 8 over $R$.

In order to get self-dual codes over the local rings of order 16 which have an element $\gamma$ with $\gamma^2 = -1$, we can apply the building-up construction. Hence, we can obtain self-dual codes over the following rings by the building-up construction: $F_2[u, v]/\langle u^2, v^2 \rangle, F_2[u, v]/\langle u^2 + v^2, uv \rangle, Z_4[x, y]/\langle x^2 - 2, xy - 2, y^2, 2x, 2y \rangle, F_2[x]/\langle x^4 \rangle, Z_4[x]/\langle x^2 - 2x - 2 \rangle$. For more detailed information about the building-up construction see [4].

5. Construction of formally self-dual codes

In this section, we shall investigate a construction technique of formally self-dual codes.

Theorem 5.1. Let $R$ be one of the following rings: $F_2[u, v]/\langle u^2, v^2 \rangle, F_2[u, v]/\langle u^2 + v^2, uv \rangle, Z_4[x]/\langle x^2 - 2x \rangle, Z_4[x]/\langle x^4 \rangle, F_2[x]/\langle x^4 \rangle, Z_4[x]/\langle x^2 - 2 \rangle$ or $Z_4[x]/\langle x^2 - 2x - 2 \rangle$. If $X$ is either an $n \times n$ circulant or symmetric matrix over $R$ then the code generated by the matrix $[I_n | X]$ is a formally self-dual code of length $2n$. 

Advances in Mathematics of Communications Volume 10, No. 2 (2016), 379–391
Proof. In Theorems 5.1 and 5.2 of [14], these results were proven specifically for \( R = \mathbb{Z}_4[x]/\langle x^2 \rangle \). Those proofs work verbatim when \( R \) is \( \mathbb{F}_2[u,v]/\langle u^2,v^2 \rangle \), \( \mathbb{F}_2[u,v]/\langle u^2 + v^2, uv \rangle \), \( \mathbb{Z}_4[x]/\langle x^2 - 2x \rangle \), \( \mathbb{Z}_4[x]/\langle x^4 \rangle \), \( \mathbb{Z}_4[x]/\langle x^2 - 2 \rangle \) or \( \mathbb{Z}_4[x]/\langle x^2 - 2x - 2 \rangle \) since in these rings, for any element \( c \in R \) we have \( w_L(c) = w_L(-c) \).

Note that the matrix \( G = [I_n][X] \) does not have to generate a formally self-dual code over \( \mathbb{Z}_4[x,y]/\langle x^2, xy - 2, y^2, 2x, 2y \rangle \), \( \mathbb{Z}_4[x,y]/\langle x^2 - 2, xy - 2, y^2, 2x, 2y \rangle \), \( \mathbb{Z}_8[x]/\langle x^2 + 4, 2x \rangle \), \( \mathbb{Z}_4[x]/\langle x^3 - 2, 2x \rangle \) or \( \mathbb{Z}_{16} \) since \( w_L(c) \) may not be \( w_L(-c) \). For example, in \( \mathbb{Z}_4[x,y]/\langle x^2, xy - 2, y^2, 2x, 2y \rangle \), \( w_L(1) = 1 \neq 3 = w_L(3) \).

**Example 4.** Let \( C \) be a code over one of the following rings: \( \mathbb{F}_2[u,v]/\langle u^2,v^2 \rangle \), \( \mathbb{F}_2[u,v]/\langle u^2 + v^2, uv \rangle \), \( \mathbb{Z}_4[x]/\langle x^2 - 2x \rangle \), \( \mathbb{Z}_4[x]/\langle x^4 \rangle \), \( \mathbb{Z}_4[x]/\langle x^2 - 2 \rangle \) or \( \mathbb{Z}_4[x]/\langle x^2 - 2x - 2 \rangle \) generated by the following matrix

\[
G = \begin{pmatrix}
1 & 0 & u & 1 + w \\
0 & 1 & 1 + w & u
\end{pmatrix}.
\]

Then \( G \) generates a formally self-dual code where \( w \) is the generator of the socle of the corresponding ring and \( u \) is a generator of one of the ideals of order 4.

**References**

[1] J. H. Conway and N. J. A. Sloane, *A new upper bound on the minimal distance of self-dual codes*, *IEEE-IT*, 36 (1990), 1319–1333.

[2] S. T. Dougherty and C. Fernandez-Cordoba, Codes over \( \mathbb{Z}_{2^k} \), Gray maps and self-dual codes, *Adv. Math. Commun.*, 5 (2011), 571–588.

[3] S. T. Dougherty, P. Gaborit, M. Harada, A. Munemasa and P. Solé, *Type IV self-dual codes over rings*, *IEEE-IT*, 45 (1999), 2345–2360.

[4] S. T. Dougherty, J. L. Kim, H. Kulosman and H. Liu, *Self-dual codes over Frobenius rings*, *Finite Fields Appl.*, 16 (2010), 14–26.

[5] S. T. Dougherty and H. Liu, *Independence of vectors in codes over rings*, *Des. Codes Crypt.*, 51 (2009), 55–68.

[6] S. T. Dougherty and K. Shiromoto, *Maximum distance codes over rings of order 4*, *IEEE-IT*, 47 (2001), 400–404.

[7] S. T. Dougherty, B. Yildiz and S. Karadeniz, *Codes over \( R_k \), Gray maps and their binary images*, *Finite Fields Appl.*, 17 (2011), 205–219.

[8] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, *The \( Z_4 \)-linearity of Kerdock, Preparata, Goethals and related codes*, *IEEE-IT*, 40 (1994), 301–319.

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

[10] E. Martinez-Moro and S. Szabo, *On codes over local Frobenius non-chain rings of order 16*, *Contemp. Math.*, 634 (2015), 227–242.

[11] J. Wood, *Duality for modules over finite rings and applications to coding theory*, *Amer. J. Math.*, 121 (1999), 555–575.

[12] B. Yildiz and S. Karadeniz, *Linear codes over \( \mathbb{F}_2 + u \mathbb{F}_2 + v \mathbb{F}_2 + uv \mathbb{F}_2 \)*, *Des. Codes Crypt.*, 54 (2010), 61–81.

[13] B. Yildiz and S. Karadeniz, *A new construction for the extended binary Golay code*, *Appl. Math. Inf. Sci.*, 8 (2014), 69–72.

[14] 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.

Received August 2014; revised February 2015.

E-mail address: prof.steven.dougherty@gmail.com
E-mail address: esensalturk@gmail.com
E-mail address: Steve.Szabo@eku.edu