**EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS**
Vol. 10, No. 5, 2017, 1112-1123
ISSN 1307-5543 – www.ejpam.com
Published by New York Business Global

# Optimal Divisible Binary Codes from Gray-Homogeneous Images of Codes over $\mathcal{R}_{k,m}$

Bahattin Yildiz[1,*], Nesibe Tufekci

[1] *Department of Mathematics & Statistics, Northern Arizona University, Flagstaff, AZ 86001, USA*

**Abstract.** In this work, we find a form for the homogeneous weight over the ring $\mathcal{R}_{k,m}$, using the related theoretical results from the literature. We then use the first order Reed-Muller codes to find a distance-preserving map that takes codes over $\mathcal{R}_{k,m}$ to binary codes. By considering cyclic, constacyclic and quasicyclic codes over $\mathcal{R}_{k,m}$ of different lengths for different values of $k$ and $m$, we construct a considerable number of optimal binary codes that are divisible with high levels of divisibility. The codes we have obtained are also quasicyclic with high indices and they are all self-orthogonal when $km \geq 4$. The results, which have been obtained by computer search are tabulated.

**2010 Mathematics Subject Classifications**: 94B05, 94B99

**Key Words and Phrases**: Homogeneous weight, Frobenius rings, divisible codes, self-orthogonal quasicyclic codes, optimal codes

## 1. Introduction

The homogeneous weight was introduced for codes over rings as an alternative to the Hamming weight. The theoretical work on the homogeneous weight and its form for Frobenius rings can be found in such works as [4], [6] and [8]. Different characterizations for the homogeneous weight on Frobenius rings were given in these works. The Mobius function or the generating character of the ring seem to be the prevalent tools used in these constructions.

In most works related to the homogeneous weight, the average weight $\gamma$ is unassigned. In a number of recent works involving different alphabets, $\gamma$ was given a fixed value and then a distance-preserving isometry was defined using different methods and tools. We will call such an isometry a Gray-homogeneous map here. In [17] and [16] an algebraic and a combinatorial construction was given respectively, for the Gray-homogeneous map on Galois rings. In [11], combinatorial constructions using projective geometries were given for the Gray-homogeneous maps on finite chain rings and some other families of rings. In

*Corresponding author.

*Email addresses:* bahattin.yildiz@nau.edu (B. Yildiz), nesibe_tufekci@hotmail.com (N. Tufekci)

 

[15], a construction for the Gray-homogeneous map using Reed-Muller codes was given for codes over the ring family of $R_k$, and many new quasicyclic codes were obtained as images.

In this work, we consider the homogeneous weight on the ring family $\mathcal{R}_{k,m}$, a characteristic 2 family of Frobenius rings, intrduced in [13]. Using the generating character characterization of the homogeneous weight we find a form for the homogeneous weight on $\mathcal{R}_{k,m}$. We assign a value to the average weight $\gamma$, giving algebraic and combinatorial justifications. We then construct the Gray-homogeneous map using Reed-Muller codes. Using the images of cyclic, constacyclic and quasicyclic codes over $\mathcal{R}_{k,m}$ of different lengths with suitable $k, m$ we are able to construct many optimal binary codes that are divisible with high levels of divisibility. The codes we have obtained are also quasicyclic with high indices and they are all self-orthogonal when $km \geq 4$. Thus we obtain many optimal, self-orthogonal quasicyclic binary codes, which have been shown to be of importance in [12], for their connection to difference sets and their near-BCH performance.

The rest of the work is organized as follows. In section 2, we give some preliminaries on the ring family $\mathcal{R}_{k,m}$, mainly citing from [13]. In section 3, we recall the definitions of the homogeneous weight from the relevant literature and applying the definitions to $\mathcal{R}_{k,m}$, we find the homogeneous weight for codes over $\mathcal{R}_{k,m}$. We also construct the Gray-homogeneous map. Section 4 contains the computational results obtained using a computer search, with the help of Magma, [2]. We then finish with concluding remarks in section 5.

## 2. Preliminaries

The ring denoted by $\mathcal{R}_{k,m}$ is a characteristic 2 ring of size $2^{km}$, that was introduced in [13], and is defined as follows for $k \geq m \geq 1$:

$$\mathcal{R}_{k,m} = \mathbb{F}_2[u,v]/\left\langle u^k, v^m, uv - vu \right\rangle.$$

Note that when $k = 2, m = 1$ the ring is $\mathbb{F}_2 + u\mathbb{F}_2$, when $k = m = 2$ the ring is $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, both quite commonly-used in the recent literature of Coding Theory.

Any element of $\mathcal{R}_{k,m}$ can be represented as

$$\sum_{\substack{0\leq i\leq k-1\\ 0\leq j\leq m-1}} c_{ij}u^iv^j,\ c_{ij} \in \mathbb{F}_2. \tag{1}$$

The following lemmas from [13] describes the algebraic structure of these rings.

**Lemma 1.** *An element in $\mathcal{R}_{k,m}$ of the form given in (1) is a unit if and only if $c_{00}$ is 1.*

**Lemma 2.** *The ring $\mathcal{R}_{k,m}$ is a local ring with a unique maximal ideal $I_{u,v} = \langle u, v\rangle$. This ideal consists of all non-units and satisfies $|I_{u,v}| = \frac{|\mathcal{R}_{k,m}|}{2}$.*

By $\mathcal{U}(\mathcal{R}_{k,m})$, denote the units of $\mathcal{R}_{k,m}$ and by $\mathcal{D}(\mathcal{R}_{k,m})$, the set of non-units in $\mathcal{R}_{k,m}$. It is easy to see that $|\mathcal{U}(\mathcal{R}_{k,m})| = |\mathcal{D}(\mathcal{R}_{k,m})| = \frac{|\mathcal{R}_{k,m}|}{2}$ and that $\mathcal{U}(\mathcal{R}_{k,m}) = 1 + \mathcal{D}(\mathcal{R}_{k,m})$.

We easily observe that when $m > 1$, $\mathcal{R}_{k,m}$ is not a chain ring. However, as was also pointed out in [13], since $\mathcal{R}_{k,m}/Rad(\mathcal{R}_{k,m}) \simeq Soc(\mathcal{R}_{k,m})$ the ring $\mathcal{R}_{k,m}$ is a Frobenius ring. As a Frobenius ring, $\mathcal{R}_{k,m}$ has a generating character. It was shown in [13] that the generating character of $\mathcal{R}_{k,m}$ is given by

$$\begin{array}{rccc} \chi: & (\mathcal{R}_{k,m},+) & \to & (\{-1,1\},.) \\ & \sum\limits_{\substack{0\le i\le k-1 \\ 0\le j\le m-1}} c_{ij}u^iv^j & \mapsto & (-1)^{w_H(c)} \end{array}, \tag{2}$$

where $c = (c_{ij})$ is the binary vector consisting of all the coefficients $c_{ij}$'s of a typical element in $\mathcal{R}_{k,m}$, and $w_H(c)$ denotes the Hamming weight of $c$.

For example, in the case when $k = 2, m = 1$, i.e., when the ring is $\mathbb{F}_2 + u\mathbb{F}_2$, the generating character takes on the values: $\chi(0) = 1, \chi(1) = \chi(u) = -1$ and $\chi(1+u) = 1$.

A linear code $C$ of length $n$ over $\mathcal{R}_{k,m}$ is an $\mathcal{R}_{k,m}$-submodule of $\mathcal{R}_{k,m}^n$. Special types of codes such as cyclic and quasicyclic codes are also defined over $\mathcal{R}_{k,m}$ in the natural way they are defined over rings.

For more details on the structural properties of the rings as well as a Lee weight and related Gray maps we refer to [13].

## 3. The Homogeneous Weight and the Corresponding Gray Map on $\mathcal{R}_{k,m}$

Homogeneous weights were first introduced in 1997 by Heise and Constantinescu in [4]. They have been studied especially within the context of Frobenius rings. [8] and [6] can be cited for this purpose. The homogeneous weight is defined with two conditions for arbitrary finite rings as follows in [6]:

**Definition 1.** *A real valued function $\omega$ on the finite ring $R$ is called a (left) homogeneous weight if $\omega(0) = 0$ and the following is true:*

*(H1) For all $x, y \in R, Rx = Ry$ implies $\omega(x) = \omega(y)$ holds.*

*(H2) There exists a real number $\gamma$ such that*

$$\sum_{y\in Rx} \omega(y) = \gamma\,|Rx| \text{ for all } x \in R\backslash\{0\}$$

It has been shown that all Frobenius rings are equipped with a homogeneous weight. Different characterizations of the homogeneous weight for Frobenus rings have been given. Some of these use the Mobius function, and some use the generating character of Frobenius rings. In our work we will use the following proposition from [8], which describes the homogeneous weight in terms of the generating character of the ring:

**Proposition 1.** (*[8]*) *The homogeneous weight function for a finite ring $R$ with generating character $\chi$ is of the form*

$$\begin{array}{rccl} \omega: & R & \to & \mathbb{R} \\ & x & \mapsto & \gamma\left[1-\frac{1}{|R^\times|}\sum\limits_{\rho\in R^\times}\chi(x\rho)\right], \end{array} \tag{3}$$

*where $R^\times$, represents the group of units of $R$.*

The $\gamma$ that appears in the weight function is also called the average weight and further satisfies the following property:

**Proposition 2.** (*[8]*) *Let $I$ be either a left or a right ideal of a finite Frobenius ring $R$, and let $y \in R$. Then* $\sum\limits_{r\in I+y}\omega(r) = \gamma\,|I|$.

Applying Proposition 1 to the ring $\mathcal{R}_{k,m}$, we can obtain a form for the homogeneous weight for codes over the ring $\mathcal{R}_{k,m}$:

**Theorem 1.** *The homogeneous weight for the ring $\mathcal{R}_{k,m}$ is of the form*

$$\omega_{hom}(x)\begin{cases} 0 & x=0, \\ 2\gamma, & x=u^{k-1}v^{m-1}, \\ \gamma, & otherwise. \end{cases}$$

*Proof.* We first note that $u^{k-1}v^{m-1}\rho = u^{k-1}v^{m-1}$ for all $\rho \in \mathcal{U}(\mathcal{R}_{k,m})$ and so we have $\chi(u^{k-1}v^{m-1}\rho) = (-1)$ for all $\rho \in \mathcal{U}(\mathcal{R}_{k,m})$. Putting $u^{k-1}v^{m-1}$ into Equation 3 we see that we have

$$\omega_{hom}(u^{k-1}v^{m-1}) = \gamma\left[1-\frac{1}{2^{km-1}}\sum_{\rho\in\mathcal{U}(\mathcal{R}_{k,m})}(-1)\right] = 2\gamma.$$

On the other hand, following the same arguments as were used in [15] we can prove that, for any element $x$ in $\mathcal{R}_{k,m}$ such that $x \neq 0, u^{k-1}v^{m-1}$, we have

$$\sum_{\alpha\in\mathcal{U}(\mathcal{R}_{k,m})}\chi(\alpha x) = 0.$$

Thus we obtain

$$\omega_{hom}(x) = \gamma\left[1-\tfrac{1}{2^{km-1}}0\right] = \gamma$$

for all $x \neq 0, u^{k-1}v^{m-1}$.

Having settled the form of the homogeneous weight, we now want to choose a specific value for $\gamma$ so that we can find a distance preserving isometry from $\mathcal{R}_{k,m}$ to $\mathbb{F}_2^s$ for a suitable $s$. We will call this map the Gray-homogeneous map. We recall some of the work done in this direction. An inductive algebraic construction of a distance preserving Gray map was given by Yildiz from Galois rings with the homogeneous distance to the field of prime size with the Hamming distance in [17] as well as a combinatorial construction

of the Gray map for Galois rings by using Affine geometries in [16]. Later, projective geometries $PG_n(q)$ were used to construct the Gray map for linear codes over a family of Frobenius rings in [11]. Considering the hyperplanes and projective spaces, the work in [11] suggests the use of the projective geometry $PG_{km-1}(\mathbb{F}_2)$. This requires the $s$ to be $2^{km-1}$. However, as was later done in [15], the first order Reed-Muller codes seem to give us a more constructive method of finding this map.

We recall that the first order Reed-Muller codes $RM(1,m)$ are a family of binary linear codes of parameters $[2^m, m+1, 2^{m-1}]$, for each positive integer $m$. The important property of the first order Reed-Muller codes is that there is one codeword with weight $2^m$ and all the other non-zero codewords have weight $2^{m-1}$. Because of the structure of the homogeneous weight, it is clear that first order Reed-Muller codes can be used to construct the Gray map. Since $|\mathcal{R}_{k,m}| = 2^{km}$, we clearly need $RM(1,s)$ where $s+1 = km$. Thus, to define a distance preserving Gray map for the homogeneous weight on $\mathcal{R}_{k,m}$ we use the first order Reed-Muller codes $RM(1, km-1)$, of length $2^{km-1}$. This coincides with length of the image suggested in [11], which adds an added motivation for the choice of $\gamma$ for us. Thus we choose $\gamma = 2^{km-2}$. This means that for us, the homogeneous weight will have the following form:

$$\omega_{hom}(x) \begin{cases} 0 & \text{if } x = 0, \\ 2^{km-1} & \text{if } x = u^{k-1}v^{m-1}, \\ 2^{km-2} & otherwise. \end{cases}$$

Now, in order to define the Gray-homogeneous map on $\mathcal{R}_{k,m}$, we first note that $\mathcal{R}_{k,m}$ can be viewed as an $\mathbb{F}_2$-vector space with a basis

$$\beta = \{1, u, \ldots, u^{k-1}, v, \ldots, v^{m-1}, uv, \ldots, u^{k-1}v^{m-1}\}.$$

$RM(1, 2^{km}-1)$ has exactly $km$ basis elements, which are binary vectors of length $2^{km-1}$, including $(1,1,\ldots,1)$. So, we first let $\phi_{hom}$ map elements of the minimal ideal $I_{u^{k-1}v^{m-1}}$ to the two elements of $RM(1, km-1)$, given by $(0\ldots0)$ and $(1\ldots1)$, respectively. The remaining elements of the basis are mapped to basic generators of $RM(1, km-1)$ except $(1\ldots1)$. Taking all the possible linear combinations, we extend the map $\phi_{hom}$ to $\mathcal{R}_{k,m}$. The map is then extended in the natural way $\mathcal{R}_{k,m}^n$:

$$\begin{array}{rccl} \phi_{hom}: & (\mathcal{R}_{k,m})^n & \to & \mathbb{F}_2^{(2^{km-1})n} \\ & (c_1, c_2, \ldots, c_n) & \mapsto & (\phi_{hom}(c_1), \phi_{hom}(c_2), \ldots, \phi_{hom}(c_n)). \end{array} \tag{4}$$

The properties of the Reed-Muller codes then result in the following:

**Theorem 2.** *$\phi_{hom}$ is a distance preserving isometry from ($\mathcal{R}_{k,m}^n$, homogeneous distance) to ($\mathbb{F}_2^{2^{km-1}n}$, hamming distance). Thus if $C$ is a linear code over $\mathcal{R}_{k,m}$ of length $n$ and minimum homogeneous weight $d$, then $\phi_{hom}(C)$ is a binary linear code of length $2^{km-1}n$, and minimum hamming weight $d$. Moreover, the Homogeneous weight distribution of $C$ is the same as the hamming weight distribution of $\phi_{hom}(C)$.*

We finish this section with a few examples: The homogeneous weight for $\mathcal{R}_{2,1} = \mathbb{F}+u\mathbb{F}_2$ coincides with the Lee weight defined on $\mathbb{F}_2 + u\mathbb{F}_2$ and the Gray-homogeneous map also coincides with the usual Gray map for $\mathbb{F}_2 + u\mathbb{F}_2$, that is well-known in the literature.

Let us consider $\mathcal{R}_{3,1} = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$. The homogeneous weight then is found to be

$$\omega_{hom}(x) \begin{cases} 0 & \text{if } x = 0, \\ 4 & \text{if } x = u^2, \\ 2 & \textit{otherwise.} \end{cases}$$

The Gray-homogeneous map will then be given by $\phi_{hom}(u^2) = (1,1,1,1)$, $\phi_{hom}(u) = (1,1,0,0)$, $\phi_{hom}(1) = (1,0,1,0)$. The map is then extended to $\mathcal{R}_{3,1}$ by taking the $\mathbb{F}_2$-linear combinations. Consequently we have

$$\phi_{hom}(a + bu + cu^2) = (a+b+c, b+c, a+c, c), \quad a,b,c \in \mathbb{F}_2.$$

## 4. Divisible codes over $\mathcal{R}_{k,m}$

Divisible codes were first introduced by Ward in 1981 in [14]. A code is divisible if the weights of all the codewords have a common divisor $\Delta > 1$. The replicated code, constructed by repeating each coordinate of a selected code a certain number of times is the simplest divisible code. Moreover, Ward proved that a divisible code is equivalent to a $\Delta$-fold replicated code if the divisor $\Delta$ of the code is relatively prime to the field characteristic in [14]. A divisible code is said to be of *"level e"*, if the greatest common divisor of weights of codewords in $C$ equals $p^e$ for some integer $e \geq 1$. Reed-Muller codes are an example of divisible codes, by the following theorem in [10]:

**Theorem 3.** *The weight of every codeword in $RM(r,m)$ is divisible by $2^{[(m-1)/r]}$.*

Because of the homogeneous weight on $\mathcal{R}_{k,m}$ we can easily observe the following:

**Theorem 4.** *Any linear code $C$ over $\mathcal{R}_{k,m}$ is divisible with $\Delta \geq \gamma$. In particular with our choice of $\gamma$, we see that if $C$ is a linear code over $\mathcal{R}_{k,m}$ of length $n$, then $\phi_{hom}(C)$ is a divisible binary code of length $2^{km-1}n$ with $\Delta \geq 2^{km-2}$. Thus any such code is of level $e \geq km-2$.*

It is well known that binary linear divisible codes with $\Delta = 2^k$, $k \geq 2$ are also self-orthogonal. Thus we have the following corollary:

**Corollary 1.** *Let $C$ be any linear code over $\mathcal{R}_{k,m}$. Then $\phi_{hom}(C)$ is a binary self-orthogonal linear code if $km \geq 4$.*

In what follows, we will search for binary divisible codes with various divisors from the Gray-homogeneous images of cyclic, constacyclic and quasicyclic codes over $\mathcal{R}_{k,m}$ of some lengths. Because of the increased size of the rings, we will mostly consider the rings $\mathcal{R}_{3,1}$ , $\mathcal{R}_{4,1}$ and $\mathcal{R}_{5,1}$. The examples that we give are mainly optimal.

### 4.1. Divisible Cyclic Codes Over $\mathcal{R}_{k,m}$

Recall that a linear code $C$ of length $n$ over $\mathcal{R}_{k,m}$ is a cyclic code if $\tau(\bar{c}) = (c_{n-1}, c_0, \ldots, c_{n-2}) \in C$ for all $\bar{c} = (c_0, c_1 \ldots, c_{n-1}) \in C$, where $\tau$ is the cyclic shift. Considering the polynomial correspondence

$$\begin{array}{rccl} \pi: & (\mathcal{R}_{k,m})^n & \to & \mathcal{R}_{k,m}[x] \\ & \bar{c} = (c_0, c_1 \ldots, c_{n-1}) & \mapsto & c_0 + c_1 x + \ldots + c_{n-1}x^{n-1} \end{array}$$

we know that a code $C$ of length $n$ over $\mathcal{R}_{k,m}$ is cyclic if and only if $\pi(C)$ is an ideal in the ring $\mathcal{R}_{k,m}[x]/(x^{n-1})$. There are a lot of results concerning the structural properties of cyclic codes over rings, in particular over finite chain rings. The rings that we consider for the purposes in this section, $\mathcal{R}_{3,1}$, $\mathcal{R}_{4,1}$ being finite chain, we are not going to go into the theoretical aspects of cyclic codes. Instead we will demonstrate how some one-generator cyclic codes over these rings lead to optimal divisible binary linear codes under the Gray-homogeneous map. Since the Gray-homogeneous image of a cyclic code over $\mathcal{R}_{k,m}$ is a $2^{km-1}$-quasicyclic binary code, the binary codes that we have constructed have the additional property that they are 4-quasicyclic or 8-quasicyclic according as we are on the ring $\mathcal{R}_{3,1}$ or $\mathcal{R}_{4,1}$.

Table 1: Divisible cyclic codes over $\mathcal{R}_{3,1}$ of length $n$ and the binary images

| $n$ | $g(x)$ | $\phi_{hom}(\langle g(x)\rangle)$ | $\Delta$ | $level$ |
|---|---|---|---|---|
| 3 | $u^2x + u^2x^2$ | $[12, 2, 8]$ | 8 | 3 |
| 3 | $1 + x^2$ | $[12, 3, 6]$ | 6 | 1 |
| 4 | $ux + u^2x^2 + ux^3$ | $[16, 4, 8]$ | 8 | 3 |
| 4 | $1 + x + x^2 + (1 + u^2)x^3$ | $[16, 5, 8]$ | 8 | 3 |
| 4 | $x + ux^2 + (u + 1)x^3$ | $[16, 6, 6]$ | 2 | 1 |
| 4 | $x^2 + x^3$ | $[16, 9, 4]$ | 2 | 1 |
| 4 | $x^3$ | $[16, 12, 2]$ | 2 | 1 |
| 5 | $x^3 + x^4$ | $[20, 12, 4]$ | 2 | 1 |
| 5 | $x^3 + (1 + u^2)x^4$ | $[20, 13, 4]$ | 2 | 1 |
| 6 | $ux + ux^2 + u^2x^3 + ux^4 + (u + u^2)x^5$ | $[24, 4, 12]$ | 4 | 2 |
| 6 | $x^4 + x^5$ | $[24, 15, 4]$ | 2 | 1 |
| 6 | $x^4 + (1 + u)x^5$ | $[24, 16, 4]$ | 2 | 1 |
| 7 | $u^2x^2 + u^2x^4 + u^2x^5 + u^2x^6$ | $[28, 3, 16]$ | 16 | 4 |
| 7 | $1 + x + x^2 + (1 + u^2)x^3 + x^4 + (1 + u^2)x^5 + (1 + u^2)x^6$ | $[28, 6, 12]$ | 2 | 1 |
| 7 | $x^2 + x^4 + (1 + u^2)x^5 + (1 + u^2)x^6$ | $[28, 12, 8]$ | 4 | 2 |
| 7 | $x^5 + (1 + u^2)x^6$ | $[28, 19, 4]$ | 2 | 1 |
| 8 | $x^3 + ux^5 + ux^6 + x^7$ | $[32, 14, 8]$ | 2 | 1 |
| 8 | $x^4 + x^5 + (1 + u)x^6 + (1 + u + u^2)x^7$ | $[32, 15, 8]$ | 2 | 1 |

Table 2: Divisible cyclic codes over $\mathcal{R}_{4,1}$ of length $n$ and the binary images

| $n$ | $g(x)$ | $\phi_{hom}(\langle g(x)\rangle)$ | $\Delta$ | $level$ |
|---|---|---|---|---|
| 2 | $u+ux$ | $[16,3,8]$ | 8 | 3 |
| 3 | $u^3x+u^3x^2$ | $[24,2,16]$ | 16 | 4 |
| 3 | $x+x^2$ | $[24,8,8]$ | 4 | 2 |
| 3 | $x+(1+u^3)x^2$ | $[24,9,8]$ | 4 | 2 |
| 4 | $u^2x+u^3x^2+u^2x^3$ | $[32,4,16]$ | 16 | 4 |
| 4 | $1+x+(1+u^3)x^2+(1+u^3)x^3$ | $[32,5,16]$ | 16 | 4 |
| 4 | $1+x+x^2+(1+u^3)x^3$ | $[32,6,16]$ | 16 | 4 |
| 6 | $u^3x+u^3x^2+u^3x^4+u^3x^5$ | $[48,2,32]$ | 32 | 5 |
| 6 | $u^2x+u^2x^2+u^3x^3+u^2x^4+(u^2+u^3)x^5$ | $[48,4,24]$ | 8 | 3 |

**Remark 1.** *All the binary codes given in the above tables are optimal or best known codes, meaning that they either attain upper bounds or have the best known minimum distance according to [5]. The codes given in Table 2 have the additional property that they are all self-orthogonal quasicyclic codes of the best possible parameters.*

## 4.2. Divisible constacyclic codes over $\mathcal{R}_{k,m}$

Constacyclic codes are a natural generalization of cyclic codes. For a unit $\alpha \in R$, a constacyclic shift on $R^n$ is given by $\tau_\alpha(c_0, c_1, \ldots, c_{n-1}) = (\alpha c_{n-1}, c_0, c_1, \ldots, c_{n-2})$. A code $C$ over $R$ is said to be $\alpha$-constacyclic if it is invariant under the $\alpha$-constacyclic shift, i.e., $\tau_\alpha(C) = C$. In exactly the same way as the cyclic codes, constacylic codes are also endowed with an algebraic structure. More precisely, constacyclic codes over $R$ are in one-to-one correspondence with ideals in the quoient ring $R[x]/(x^n - \alpha)$. Structural properties of constacyclic codes over different alphabets have been studied quite extensively in the literature. In [9], Karadeniz and Yildiz studied $(1 + v)$-constacyclic codes over $\mathcal{R}_{2,2} = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. It is well known that if $R$ is a ring of characteristic 2, and $\alpha \in R$ satisfies $\alpha^2 = 1$, then $\alpha$-constacyclic codes over $R$ are also cyclic. In $\mathcal{R}_{2,2}$ as well as in the latter generalizations $R_k$, [15], every unit satisfies this property. So, constacyclic codes over these rings of odd lengths are just cyclic. However, the cases that we look at, namely in $\mathcal{R}_{3,1}$, $\mathcal{R}_{4,1}$ and $\mathcal{R}_{5,1}$ this is not true. If we take $\alpha = 1 + u$, then $(1 + u)^2 \neq 1$ in the rings mentioned above.

In what follows, we have listed some examples of one-generator $(1 + u)$-constacyclic codes over $\mathcal{R}_{k,m}$ and their homogeneous gray images, which turn out to be divisible, optimal and in some cases self-orthogonal:

Table 3: Divisible $(1+u)$-constacyclic codes over $\mathcal{R}_{k,1}$ of length $n$ and the binary images

| $\mathcal{R}_{k,1}$ | $n$ | generator of the code | $\phi_{hom}(\langle g(x)\rangle)$ | $\Delta$ | $level$ |
|---|---|---|---|---|---|
| $\mathcal{R}_{3,1}$ | 6 | $(0,u^2,u^2,0,u^2,u^2)$ | $[24,2,16]$ | 16 | 4 |
| $\mathcal{R}_{3,1}$ | 6 | $(0,0,0,1,u,1)$ | $[24,15,4]$ | 2 | 1 |
| $\mathcal{R}_{3,1}$ | 7 | $(0,0,u^2,0,u^2,u^2,u^2)$ | $[28,3,16]$ | 16 | 4 |
| $\mathcal{R}_{3,1}$ | 7 | $(1,u+1,1,u+1,1,u^2+u+1,u^2+1)$ | $[28,6,12]$ | 2 | 1 |
| $\mathcal{R}_{3,1}$ | 7 | $(0,0,1,0,1,u+1,1)$ | $[28,12,8]$ | 4 | 2 |
| $\mathcal{R}_{3,1}$ | 7 | $(0,0,0,0,0,1,u^2+u+1)$ | $[28,19,4]$ | 2 | 1 |
| $\mathcal{R}_{3,1}$ | 9 | $(0,u^2,u^2,0,u^2,u^2,0,u^2,u^2)$ | $[36,2,24]$ | 24 | |
| $\mathcal{R}_{4,1}$ | 2 | $(u^2,u^2)$ | $[16,3,8]$ | 8 | 3 |
| $\mathcal{R}_{4,1}$ | 3 | $(0,1,u+1)$ | $[24,8,8]$ | 4 | 2 |
| $\mathcal{R}_{4,1}$ | 3 | $(0,1,u^3+u+1)$ | $[24,9,8]$ | 4 | 2 |
| $\mathcal{R}_{4,1}$ | 5 | $(1,u^3+u^2+u+1,u^2+1,u+1,1)$ | $[40,4,20]$ | 20 | |
| $\mathcal{R}_{4,1}$ | 7 | $(0,0,u^3,0,u^3,u^3,u^3)$ | $[56,3,32]$ | 32 | 5 |
| $\mathcal{R}_{5,1}$ | 3 | $(0,u^4,u^4)$ | $[48,2,32]$ | 32 | 5 |
| $\mathcal{R}_{5,1}$ | 3 | $(u,u^2+u,u^3+u)$ | $[48,4,24]$ | 24 | |
| $\mathcal{R}_{5,1}$ | 3 | $(1,1+u+u^4,1+u^2)$ | $[48,5,24]$ | 24 | |
| $\mathcal{R}_{5,1}$ | 5 | $(1,u^3+u^2+u+1,u^4+u^2+1,u+1,u^4+1)$ | $[80,5,40]$ | 40 | |

**Remark 2.** *If $C$ is an $\alpha$-constacyclic code over $\mathcal{R}_{k,m}$, then $\phi_{hom}(C)$ might not be a $2^{km-1}$-quasicyclic binary code, however it can easily be shown that $\phi_{hom}(C)$ is equivalent to a $2^{km-1}$-quasicyclic binary code. Thus all the codes given in the above table are equivalent to binary quasicyclic codes and they are also self-orthogonal when $\Delta \geq 4$.*

### 4.3. Some results on divisible quasicyclic codes over $\mathcal{R}_{k,m}$

Quasicyclic codes are another generalization of cyclic codes and have generated a lot of interest. They have algebraic structure and they also satisfy a modified version of the Gilbert-Varshamov bound. Many optimal good binary codes are quasicyclic. A lot of good codes have been constructed using quasicyclic codes over different alphabets, such as [1] and [3]. A definition can be given from [10]:

**Definition 2.** *A code $C$ of length $n$ is called $\ell-$quasicyclic if $\ell|n$ and $\tau^{\ell}(C)=C$.*

Note that when $\ell = 1$, 1-quasicyclic codes are just cyclic codes. Structurally, the generator matrix of a $t$ generator $\ell-$quasicyclic code can be shown to be of the following form:

$$\begin{bmatrix} C_{00} & C_{01} & \dots & C_{0,\ell-1} \\ C_{10} & C_{11} & \dots & C_{1,\ell-1} \\ \vdots & \vdots & \vdots & \vdots \\ C_{t,0} & C_{t,1} & \dots & C_{t,\ell-1} \end{bmatrix}$$

where $C_{ij}$ are $m \times m$ circulant matrices. In such a case, the length $n$ of the $\ell-$quasicyclic code $C$ is $m \times \ell$. We refer to [12, 3] for more information on quasicyclic codes.

We have searched through one generator $\ell$-quasicyclic codes over $\mathcal{R}_{k,m}$ to get divisible codes of various lengths. We have listed in the following table, divisible, optimal binary codes obtained as the $\phi_{hom}$-images of quasi cyclic codes over $\mathcal{R}_{k,m}$:

Table 4: Divisible $\ell$-quasicyclic codes over $\mathcal{R}_{k,1}$ and the binary images

| $\mathcal{R}_{k,1}$ | $\ell$ | generator of the code | $\phi_{hom}(\langle g(x)\rangle)$ | $\Delta$ | *level* |
|---|---|---|---|---|---|
| | 3 | $(0,1,1,0,1,1+u^2,u,u,u^2)$ | $[36,2,24]$ | 24 | |
| | 3 | $(0,u,u,0,u,u^2+u,u,u,u^2)$ | $[36,5,16]$ | 4 | 2 |
| | 3 | $(0,1,1,0,u,u,1,u^2,u^2+1)$ | $[36,6,16]$ | 4 | 2 |
| | 3 | $(0,1,1,0,1,u^2+1,u,u,u^2)$ | $[36,7,16]$ | 4 | 2 |
| $\mathcal{R}_{3,1}$ | 3 | $(1,1,u^2+1,u^2+1,1,1,u^2+1,u^2+1,1,1,u^2+1,u^2+1)$ | $[48,4,24]$ | 24 | |
| | 3 | $(0,u,u^2,u^2+u,1,1,u^2+1,u^2+1,1,u+1,1,u+1)$ | $[48,5,24]$ | 8 | 3 |
| | 2 | $(0,1,1,u^2,1,u^2+1,u^2+u,1,u^2+u+1,u,1,u+1)$ | $[48,6,24]$ | 8 | 3 |
| | 2 | $(0,0,0,u,u,0,u^2,u,u,u^2)$ | $[40,8,16]$ | 8 | 3 |
| | 3 | $(1,1,1,1,u^2+1,1,1,1,u^2+1,u^2+1,1,1,u^2+1,1,u^2+1)$ | $[60,7,28]$ | 2 | 1 |
| | 3 | $(0,0,0,1,1,0,u,1,u,1,1,u+1,u^2,1,u^2+u+1)$ | $[60,12,24]$ | 4 | 2 |
| | 2 | $(1,1,u^3+1,u^3+1,1,1,u^3+1,u^3+1)$ | $[64,5,32]$ | 32 | 5 |
| | 2 | $(1,1,1,u^3+1,1,1,1,u^3+1)$ | $[64,6,32]$ | 32 | 5 |
| $\mathcal{R}_{4,1}$ | 2 | $(1,1,u^2+1,u^3+u^2+1,1,1,u^3+u^2+1,u^2+1)$ | $[64,7,32]$ | 32 | 5 |
| | 3 | $(1,1,u^3+1,1,1,u^3+1,1,1,u^3+1)$ | $[72,5,36]$ | 12 | |
| | 3 | $(1,1,1,u^3+1,1,1,1,u^3+1,1,1,1,u^3+1)$ | $[96,6,48]$ | 48 | |

**Remark 3.** *It can easily be shown that the Gray-homogeneous image of an $\ell$-quasicyclic code is a $(2^{km-1}\ell)$-quasicyclic binary code. So, the binary codes constructed above are all $(2^{km-1}\ell)$-quasicyclic for the appropriate values of $\ell, k, m$. In all but one of the cases they are self-orthogonal as well. Thus almost all the codes given in the above table are optimal self-orthogonal quasicyclic codes.*

## 4.4. Griesmer Code

The Griesmer bound, introduced in [7] is one of the many bounds that exist for codes, and can be stated as follows: For a linear $[n,k,d]$-code over $\mathbb{F}_q$, we have

$$n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil, \tag{5}$$

where $\lceil x \rceil$ denotes the smallest integer greater than or equal to $x$. Linear codes meeting this bound are called Griesmer Codes.

Let us consider a one generator cyclic code $C_{km}$ of length $n$ over $\mathcal{R}_{k,m}$ with the generator vector $(11\ldots1)$. This is actually the repetition code. It is clear to see that the Gray-homogeneous image of this code is a binary linear code of the parameters $[2^{km-1}n, km, 2^{km-2}n]$. Thus, the images of this code are binary divisible codes with divisor at least $2^{km-2}$. We may construct many optimal linear codes, which otherwise may

have complicated constructions, in a relatively easier way from $C_{km}$. As an illustration of this idea, consider, the Gray-homogeneous images of $C_{51}$ and $C_{32}$ of length $n$. These will be binary codes of parameters $[16n, 5, 8n]$ and $[32n, 6, 16n]$, respectively. According to [5], these codes are all optimal when $1 \leq n \leq 8$.

We finish this section by noticing that $\phi_{hom}(C_{km})$s are Griesmer codes, when $n = 1$, for all $k$ and $m$.

**Theorem 5.** *The binary linear code $\phi_{hom}(C_{km})$ is a Griesmer code for $n = 1$, and for all $k, m$.*

*Proof.* When $n = 1$, $\phi_{hom}(C_{km})$ is a $km$-dimensional linear code with minimum distance $2^{km-2}$. Calculating the Griesmer lower bound according to 5, we see that the lower bound must be

$$\begin{aligned}\sum_{i=0}^{km-1} \lceil \frac{d}{2^i} \rceil &= \lceil \frac{2^{km-2}}{2^0} \rceil + \lceil \frac{2^{km-2}}{2^1} \rceil + \cdots + \lceil \frac{2^{km-2}}{2^{km-2}} \rceil + \lceil \frac{2^{km-2}}{2^{km-1}} \rceil \\ &= 2^{km-2} + 2^{km-3} + \cdots + 1 + 1 \\ &= (2^{km-1} - 1) + 1 = 2^{km-1},\end{aligned}$$

which is precisely the length of $\phi_{hom}(C_{km})$, when $n = 1$.

## 5. conclusion

Finding optimal binary codes is a relevant question in coding theory. The database given in [5] is a dynamic source of such codes together with different suggested constructions. In our work, we were able to reconstruct many of the optimal codes by using different constructions over the rings $\mathcal{R}_{k,m}$. The codes that are obtained, are not only all optimal, but they possess some further properties such as being divisible with high levels of divisibility, and in many cases self-orthogonal. They are also quasicyclic with high indices. This means that the binary codes that we have obtained from the Gray-homogeneous images of codes over $\mathcal{R}_{k,m}$ are rather special examples of codes that appear in [5]. Considering that many of the codes we have obtained fall into the class of self-orthogonal quasicyclic codes, they are of interest within the context of [12] as well. The relative ease with which we obtained the codes and usually simple constructions suggest that, the idea of using $\mathcal{R}_{k,m}$ and the Gray-homogeneous map is worth pursuing in many other contexts as well.

## References

[1] N Aydin, S Karadeniz and B Yildiz. Some new binary quasi-cyclic codes from codes over the ring $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$, *Applicable Algebra in Engineering, Communication and Computing*, 24:355-367, 2013.

[2] W Bosma, J Cannon and C Playoust. The Magma algebra system I. The user language, *Journal of Symbolic Computation*, 24:235–265, 1997.

[3] Z Chen. Six new binary quasi-cyclic codes, *IEEE Transactions on Information Theory*, 40(5):1666–1667, 1994.

[4] I Constantinescu and W Heise. A metric for codes over residue class rings of integers, *Problemy Peredachi Informatsii*, 33(3):22–28, 1997.

[5] M Grassl. Bound on the minimum distance of linear codes and quantum codes, Online available at: www.codetables.de(Accessed on 2015/12/01).

[6] M Greferath and M E OSullivan. On bounds for codes over Frobenius rings under homogeneous weights, *Discrete Mathematics*, 289:11-24, 2004.

[7] J H Griesmer. A bound for error correcting codes, *IBM Journal of Research and Development*, 4:532–542, 1960.

[8] T Honold. A Characterization of finite Frobenius rings, *Archiv der Mathematik*, 76:406-415, 2001.

[9] S Karadeniz and B Yildiz. $(1 + v)$-constacylic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, *Journal of the Franklin Institute*, 348:2625–2632, 2011.

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

[11] A Pasa and B Yildiz. Constructing Gray maps from combinatorial geometries, *Communications de la Facult des Sciences de l'Universit d'Ankara Serie A1*, 63:147–161, 2014.

[12] R L Townsend and E Weldon. Self-orthogonal quasi-cyclic codes, *IEEE Transactions on Information Theory*, 13(2):183–195, 1967.

[13] N Tufekci and B Yildiz. On codes over $\mathcal{R}_{k,m}$ and constructions for new binary self-dual codes, *Mathematica Slovaca*, 66(6):1511–1526, 2016.

[14] H N Ward. Divisible codes, *Archive der Mathematik*, 36:485-499, 1981.

[15] B Yildiz and I G Kelebek. The homogeneous weight for $\mathcal{R}_k$, related Gray map and new binary quasicyclic codes, *ArXiv: 1504.04111*, 2014.

[16] B Yildiz. A Combinatorial construction of the Gray map over Galois rings, *Discrete Mathematics*, 309:3408–3412, 2009.

[17] B Yildiz. Weight enumerators and Gray maps of linear codes over rings, *Ph.D. Thesis: California Institute of Technology*, 2006.