Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/100614

On p-Ary Local Frobenius Rings and their Homogeneous Weights

Bahattin Yildiz[1,*] *and Makarim Abdlwahed Abdljabbar*[1,2]

[1] Department of Mathematics, Fatih University, 34500 Buyukcekmece, Istanbul, Turkey
[2] Computer College, University of Al Anbar, Al Anbar, Iraq

Received: 7 Jun. 2016, Revised: 10 Aug. 2016, Accepted: 17 Aug. 2016
Published online: 1 Nov. 2016

Abstract: In this work, a characterization of different properties of p-ary local Frobenius rings and their generating characters is given. Using the generating character, a general form for the homogeneous weights of such rings is described. In particular it is shown that the homogenous weights of all such rings have two non-zero values. Moreover, distance-preserving, linear Gray maps for the homogeneous weights of some classes of p-ary local Frobenius rings are found and using the Gray image, many linear p-ary codes attaining the Griesmer bound are counstructed.

Keywords: local Frobenius rings, Griesmer bound, homogeneous weight, Generalized Reed-Muller codes

1 Introduction

Codes over rings have been an important field of research in Algebraic Coding Theory. In the last two decades many works related to codes over different rings and their applications have been appeared. An important work that in a sense defines this field is the work done by Wood in [13], in which he described Frobenius rings and argued that they are the largest class of rings over which the MacWilliams identities and extensions work. This has led to the belief that Frobenius rings are the largest class of rings to study in Coding Theory. Almost all the rings that have been studied recently in the context of codes have been Frobenius rings.

The homogeneous weight is an alternative to the Hamming weight, that is defined over finite rings. While first introduced in [2], they were explicitly described in [4] for any ring. They are related to such algebraic objects as exponential sums as was shown in [11]. Different characterizations for homogeneous weights were suggested using different tools such as the Mobius function. However, in [8], it was shown that all Frobenius rings are endowed with a homogeneous weight and an explicit characterization of the weight, using the generating character of the ring was given.

In this work, we focus on a special class of Frobenius rings, namely the so-called p-ary local Frobenius rings. These are local Frobenius rings whose residue field is isomorphic to the basic prime field, i.e. to $\mathbb{F}_p \simeq \mathbb{Z}_p$. We characterize these rings in detail, obtaining many of their properties and give many of the oft-studied rings in Coding Theory as special examples. We then give a generating character for these rings after which we prove that the homogeneous weight for all p-ary local Frobenius rings consists of two non-zero weights. We also define a distance preserving isometry for certain special cases and use the map to construct many Griesmer-optimal codes over several prime fields. The rest of the paper is organized as follows. In section 2, we discuss the structural properties of p-ary local Frobenius rings and their examples. In section 3, we describe the generating character explicitly. In section 4, using Honold's characterization of the homogeneous weight with the generating character, we find a form for the homogenous weights of p-ary local Frobenius rings. In particular, we prove that all such weights have two non-zero values. In section 5, we discuss the possible values for the average weight parameter γ that would allow us to define a distance preserving isometry. Using Generalized Reed-Muller codes, we find a linear map for certain examples of the rings. We then construct many optimal p-ary linear codes that attain the Griesmer bound from the images of codes over p-ary local Frobenius rings.

* Corresponding author e-mail: bahattinyildiz@gmail.com

2 p-ary local Frobenius Rings and their properties

The definition of a Frobenius ring in many equivalent forms being given in detail in [13], we will not describe them here. We start with a finite commutative ring R that is a local Frobenius ring. This means that there is a unique maximal ideal M and we further assume that $R/M \simeq \mathbb{F}_p$. Note that the field of size p is unique and it is also isomorphic to $\mathbb{Z}_p$. So, throughout, we will use $\mathbb{F}_p$ and $\mathbb{Z}_p$ interchangeably as the context requires. We call the above-described rings p-ary local Frobenius rings. The following theorem will give some of the structural properties of all local p-ary local Frobenius rings:

Theorem 1.*Let R be a p-ary local Frobenius ring. Then*

a) *R has a unique minimal ideal $\mathfrak{m}$.*

b) *There is $a \in R$ such that $\mathfrak{m} = \{0, a, \ldots, (p-1)a\}$*

c) *If I is any non-zero ideal in R, then $\mathfrak{m} \subseteq I$.*

d) *We have $a^2 = 0$.*

e)

$$x \cdot a = \begin{cases} j \cdot a, \ \ j \in \{1, 2, \ldots p-1\} & \text{if } x \text{ is a unit} \\ 0 & \text{if } x \text{ is a non-unit} \end{cases}$$

*Proof.***a)** This follows from the fact that R is a p-ary local Frobenius ring. By the definition of Frobenius rings, $R/J(R)$ is isomorphic to $soc(R)$ as a module. But $R/J(R)$ being isomorphic to $\mathbb{Z}_p$ as a ring, we must have $soc(R) \simeq \mathbb{Z}_p$ as an additive group. Now, $soc(R)$ is the sum of minimal ideals, so every minimal ideal must be an additive subgroup of $soc(R)$. But since $\mathbb{Z}_p$ does not have any non-trivial subgroups, we see that there has a to be a unique minimal ideal $\mathfrak{m}$.

b) By (a), we know that $\mathfrak{m} = soc(R)$, which is isomorphic as an additive group to $\mathbb{Z}_p$. Since $\mathbb{Z}_p$ is cyclic, there exists $a \in R$ such that $\mathfrak{m} = \langle a \rangle$. Clearly, then $pa = 0$ and we have $\mathfrak{m} = \{0, a, 2a, \ldots, (p-1)a\}$.

c) Let I be any non-zero ideal in R. Since R is a finite ring, it is Artinian and so every ideal must contain a minimal ideal. Since the minimal ideal is unique, I must contain $\mathfrak{m}$.

d) $a^2 \in \mathfrak{m}$, since $\mathfrak{m}$ is an ideal. Suppose $a^2 = ra$ for $r = 1, 2, \ldots, p-1$. This means that $a(a - r \cdot 1) = 0$. Now, a is a non-unit but $r.1$ is a unit in R. Since R is local, the set of all non-units form the maximal ideal and everything else is a unit. Thus the sum of a unit and a non-unit must be unit which implies $a - r \cdot 1$ must be a unit. This is a contradiction to $a(a - r \cdot 1) = 0$. Thus we must have $a^2 = 0$.

e) Suppose x is a non-unit in R. Since $\mathfrak{m}$ is an ideal, we must have $xa \in \mathfrak{m}$. Now, suppose $xa = ra$ for some $r = 1, 2, \ldots, p-1$. Then we would have $a(x - r.1) = 0$. But then, by the same reason as in (d), we must have $x - r \cdot 1$ as a unit, which would contradict the equality. So we must have $xa = 0$ if x is a non-unit. On the other hand if x is a unit in R, then again we must have $xa \in \mathfrak{m}$. Now if $xa = 0$, this would imply that x is a zero-divisor, which is a contradiction. Hence $xa = ia$, where $i \in \{1, 2, \ldots, p-1\}$.

Another important property of p-ary local Frobenius rings is that their size should be a power of p.

Theorem 2.*Let R be a p-ary local Frobenius ring. Then $|R| = p^m$ for some suitable integer m.*

*Proof.*The minimal ideal $\mathfrak{m}$, which is isomorphic as an additive group to $\mathbb{Z}_p$, is a subgroup of R. So we must have $p||R|$. Now suppose there is another prime q such that $|R|$ is divisible by q. But then, by Cauchy Theorem, we know there would be an additive subgroup of R, which would be isomorphic to $\mathbb{Z}_q$. Since as submodules $\mathbb{Z}_p$ and $\mathbb{Z}_q$ do not contain one another they would both be minimal submodules. This would contradict the uniqueness of $\mathfrak{m}$ as the minimal submodule.

A linear code C of length n over R is defined as an R-submodule of R^n. There is an extensive literature on different aspects of codes over rings. Hence, the definition will suffice here.

2.1 Examples

We next would like to give some examples of p-ary local Frobenius rings. Many of these examples are familiar rings in the context of Coding Theory in recent years. We will consider two separate cases in terms of the characteristic of the ring:

2.1.1 Characteristic p rings

All these rings will have $\mathbb{F}_p$ as a subring. In fact it is easy to see that they will have the further structural property of being vector spaces over $\mathbb{F}_p$. We enumerate some examples below:

– The finite chain rings of the form $\mathbb{F}_p[u]/(u^k)$.

– $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, introduced first in [16], which has been extensively studied from many different aspects related to codes.

– $R_k = \mathbb{F}_2[u_1, u_2, \ldots, u_k]/(u_i^2, u_i u_j - u_j u_i)$, which is an extension of $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, that first appeared in [3] and has since been studied extensively.

– $R_{k,m} = \mathbb{F}_2[u, v]/(u^k, v^m, uv - vu)$, studied in [10].

– Another extension of R_k can be achieved by replacing $\mathbb{F}_2$ by any basic prime field $\mathbb{F}_p$. In other words, we consider rings of the form $\mathbb{F}_p[u_1, u_2, \ldots, u_k]/(u_i^2, u_i u_j - u_j u_i)$. We denote this family of rings by $R_{k,(p)}$. The structural properties of these rings being exactly the same as R_k, we will not go into detail about them.

2.1.2 Rings of non-prime characteristic

The typical examples of these rings involve $\mathbb{Z}_{p^m}$ for some $m > 1$. Thus the following list can be given as a familiar list of rings that fall into this category:

–$\mathbb{Z}_4$ is the first main example of such rings, and there is an extensive literature on codes over this ring.
–$\mathbb{Z}_{2^m}$, $\mathbb{Z}_{p^m}$.
–$\mathbb{Z}_4+u\mathbb{Z}_4=\mathbb{Z}_4[u]/(u^2)$, which was first studied in [17].
–Different extensions of $\mathbb{Z}_{p^m}$ such as $\mathbb{Z}_{p^m}[u]/(u^t)$ or even such extensions as $\mathbb{Z}_{p^m}[u_1,u_2,\ldots,u_k]/(u_i^2,u_iu_j-u_ju_i)$.

It is worth observing that p-ary local Frobenius rings of characteristic p^m will have a copy of $\mathbb{Z}_{p^m}$ as a subring and they will be of the form $\mathbb{Z}_{p^m}+s\mathbb{Z}_{p^m}+t\mathbb{Z}_{p^m}+\ldots$ for some suitable $s,t,\ldots$.

3 The generating character for p-ary local Frobenius rings

The generating character is an important tool in finding the homogeneous weight and we know that all Frobenius rings possess a generating character. We recall that a character χ defined on a ring R is called a genarating character if it is non-trival, when restricted to any non-zero ideal. In other words, the kernel of a generating character χ does not contain any non-zero ideal of R.

When defining the generating character for p-ary local Frobenius rings, we need to consider two separate cases depending on the characteristic of the ring.

Let R be a p-ary local Frobenius ring of characteristic p with the minimal ideal $\mathfrak{m}=\{0,a,2a,\ldots,(p-1)a\}$. In that case R will be a vector space over $\mathbb{Z}_p$ and one of the basis elements will be a. Then we define the character χ as follows:

$$\chi(r)=e^{\frac{2\pi ic_a}{p}}, \tag{1}$$

where c_a is the coefficient of a in $r\in R$.

If R is a p-ary local Frobenius ring of characteristic p^m, then the minimal ideal will be of the form $\mathfrak{m}=\{0,p^{m-1}b,2p^{m-1}b,\ldots,(p-1)p^{m-1}b\}$ for some $b\in R$. Every element of R can be written in the form $c_0+c_1u_1+\cdots+c_su_s$, with $c_i\in\mathbb{Z}_{p^m}$. One of the u_i's will be b. In that case we define the character χ on R as

$$\chi(r)=e^{\frac{2\pi ic_b}{p^m}}, \tag{2}$$

where c_b is the coefficient of b in $r\in R$.

For example in $\mathbb{Z}_4+u\mathbb{Z}_4=\mathbb{Z}_4[u]/(u^2)$, the character can be defined as $\chi(a+bu)=e^{\frac{2\pi ib}{4}}=(i)^b$. In $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$, the character is defined as $\chi(a+bu+cv+duv)=e^{\frac{2\pi id}{2}}=(-1)^d$.

Theorem 3.*The characters defined in (1) and (2) are generating characters for a p-ary local Frobenius ring of characteristic p and characteristic p^m, respectively.*

*Proof.*We will prove the characteristic p case. The proof of the other case, being similar, will be omitted.

We first note that if $r,s\in R$ such that $r=\cdots+c_aa$ and $s=\cdots+d_aa$, then $r+s=\cdots+(c_a+d_a)a$. Hence we have

$$\chi(r+s)=e^{\frac{2\pi i(c_a+d_a)}{p}}=e^{\frac{2\pi ic_a}{p}}\cdot e^{\frac{2\pi id_a}{p}}=\chi(r)\cdot\chi(s).$$

By Theorem 1, the minimal ideal $\mathfrak{m}$ is contained in all the non-zero ideals of R. Thus, to show that χ is a generating character, it is enough to show that $\chi|_{\mathfrak{m}}$ is non-trivial. This is clear, because $\chi(a)=e^{\frac{2\pi i}{p}}\neq 1$.

4 The Homogeneous weight for p-ary local Frobenius rings:

Homogeneous weights were first introduced in 1997 by Heise and Constantinescu in [2]. They have been studied especially within the context of Frobenius rings. [8] and [4] can be cited for this purpose. The homogeneous weight is defined with two conditions for arbitrary finite rings as follows in [4]:

Definition 1.*A real valued function ω 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 γ 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 χ is of the form*

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

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

The γ that appears in the weight function is also called the average weight.

Before proving the main result about the homogeneous weights of p-ary local Frobenius rings, we will need some auxiliary results. Let M be the unique maximal ideal of R. Then M consists of all the non-units in R and since $R/M\simeq\mathbb{Z}_p$, we have $|M|=|R|/p$. Furthermore we can easily see that $R^\times=(1+M)\cup(2+M)\cup\cdots\cup((p-1)+M)$, gives us a partition of the units. We first start with the following lemma, which will be useful in proving the next result:

Lemma 1. *Let R be a p-ary local Frobenius ring, χ its generating character as described before and x be an element in $R\setminus\mathfrak{m}$. Then there exists a unit $\lambda\in R^\times$ such that $\chi(\lambda x)=1$.*

Proof. We will proceed by considering different cases, depending on x.

If x is a unit, then choosing $\lambda=x^{-1}$, we get $\lambda x=1$, for which we know $\chi(1)=1$.

Now, suppose x is a non-unit that does not contain a multiple of a in its decomposition. Then we can choose $\lambda=1$, and we will have $\chi(\lambda x)=1$.

For the last case, let us assume that x is a non-unit that contains a multiple of a. Without loss of generality we can assume that $x=y+a$, where y is a non-unit that is not in $\mathfrak{m}$. (Otherwise, $x=y+a$ would also be in $\mathfrak{m}$.) Thus y is non-zero, and (y) is a non-zero ideal. Since $\mathfrak{m}\subset(y)$, we see that $(p-1)a=ry$ for some $r\in R$. Note that r must also be a non-unit. Because, otherwise y would be in $(a)=\mathfrak{m}$. Now, since r is a non-unit and R is a local ring, we must have $1+r$ as a unit. Hence choosing $\lambda=1+r$, we see that

$$\lambda x=(1+r)(y+a)=y+a+ry+ra=y+a+(p-1)a+0=y$$

since $ra=0$, by Theorem 1 and with $\mathfrak{m}=\{0,a,\dots,(p-1)a\}$, we have $pa=0$. But now, since (y) does not contain any non-zero multiple of a, we see that $\chi(\lambda x)=\chi(y)=1$.

Lemma 2. *Let R be a p-ary local Frobenius ring and x be an element in $R\setminus\mathfrak{m}$. Then*

$$\sum_{\alpha\in R^\times}\chi(\alpha x)=0.$$

Proof. Since χ is a generating character, it is non-trivial when restricted to any non-zero ideal. Since $x\neq 0$, the ideal generated by x is a non-zero ideal. Thus we have

$$\sum_{\alpha\in R}\chi(\alpha x)=0. \tag{4}$$

Now, by the above partition, we know that $M,1+M,2+M,\dots,(p-1)+M$ gives a partition of R. Thus we have

$$\sum_{\alpha\in M}\chi(\alpha x)+\sum_{\alpha\in R^\times}\chi(\alpha x)=0.$$

On the other hand, considering that $R^\times=(1+M)\cup(2+M)\cup\cdots\cup((p-1)+M)$, and the fact that $\chi((s+\alpha)x)=\chi(sx)\chi(\alpha x)$, we have

$$\sum_{\alpha\in M}\chi(\alpha x)(1+\chi(x)+\chi(2x)+\cdots+\chi((p-1)x))=0.$$

Since $\sum_{\alpha\in R^\times}\chi(\alpha x)=-\sum_{\alpha\in M}\chi(\alpha x)$, this last equation reduces to

$$\sum_{\alpha\in R^\times}\chi(\alpha x)(1+\chi(x)+\chi(2x)+\cdots+\chi((p-1)x))=0 \tag{5}$$

Now, since $\chi(2x)=\chi(x+x)=\chi(x)^2$, $\chi(3x)=\chi(x)^3$, and so on, we see that the above equation turns to

$$\left(1+\chi(x)+\chi(x)^2+\cdots+\chi(x)^{p-1}\right)\sum_{\alpha\in R^\times}\chi(\alpha x)=0. \tag{6}$$

Now, if $\chi(x)\neq 1$, then

$$1+\chi(x)+\cdots+\chi(x)^{p-1}=\frac{1-\chi(x)^p}{1-\chi(x)}=0.$$

That is why we cannot immediately conclude from (6) that $\sum_{\alpha\in R^\times}\chi(\alpha x)=0$. However if $\chi(x)=1$, then the sum in the parenthesis is not zero. To get around this difficulty, let us label this sum,

$$F(x)=\sum_{\alpha\in R^\times}\chi(\alpha x).$$

Let λ be any unit in R. As α runs through all the units in R, so does $\lambda\alpha$. Thus it is clear that $F(x)=F(\lambda x)$, for all $\lambda\in R^\times$. Thus replacing x by λx in (6), we see that we have

$$\left(1+\chi(\lambda x)+\chi(\lambda x)^2+\cdots+\chi(\lambda x)^{p-1}\right)F(x)=0 \tag{7}$$

for all $\lambda\in R^\times$. Now, using Lemma 1, we know that $\chi(\lambda x)=1$ for some $\lambda\in R^\times$, which would imply that $F(x)=0$.

We are now ready to describe the homogeneous weight for R:

Theorem 4. *Let R be a p-ary local Frobenius ring, with minimal ideal $\mathfrak{m}$. Then the homogeneous weight on R has the form:*

$$w_{\hom}(x)=\begin{cases}0 & \text{if } x=0\\ \frac{p}{p-1}\gamma & \text{if } x\in\mathfrak{m}\setminus\{0\}\\ \gamma & \text{otherwise.}\end{cases}$$

Proof. Suppose $x=0$. Then $\chi(\alpha x)=1$ for all $\alpha\in R^\times$. Thus by Proposition 1 we have

$$w_{\hom}(0)=\gamma\left(1-\frac{1}{|R^\times|}\sum_{\alpha\in R^\times}1\right)=0.$$

Now assume $x\in\mathfrak{m}\setminus\{0\}$. Without loss of generality, assume that $x=a$. Then as α runs through all the units in R, αa will take the values $a,2a,\dots,(p-1)a$ equally often. Hence we have

$$\sum_{\alpha\in R^\times}\chi(\alpha a)=\frac{|R^\times|}{p-1}\left(\chi(a)+\chi(2a)+\cdots+\chi((p-1)a)\right).$$

Since χ, restricted to $\mathfrak{m}$ is not a trivial character, we have $\chi(0)+\chi(a)+\cdots+\chi((p-1)a)=0$, which implies that $\chi(a)+\chi(2a)+\cdots+\chi((p-1)a)=-1$. Putting this into the above equation, and again using Proposition 1, we obtain

$$w_{\hom}(a)=\gamma\left(1-\frac{1}{|R^\times|}\sum_{\alpha\in R^\times}\chi(\alpha a)\right)$$

$$= \gamma\left(1 - \frac{1}{|R^\times|}\frac{|R^\times|}{p-1}(-1)\right) = \frac{p}{p-1}\gamma.$$

Clearly, this is true for $2a, 3a, \ldots, (p-1)a$ as well.

Finally, assume that $x \in R \setminus \mathfrak{m}$. Then by Lemma 2, we know that

$$\sum_{\alpha \in R^\times} \chi(\alpha x) = 0.$$

Then by Proposition 1, we have

$$w_{\text{hom}}(x) = \gamma\left(1 - \frac{1}{|R^\times|}\sum_{\alpha \in R^\times}\chi(\alpha x)\right) = \gamma(1-0) = \gamma.$$

5 The Gray Map for the Homogeneous Weight and Construction of good p-ary codes from the Gray Images.

In the previous section, we proved that the homogeneous weight for each p-ary local Frobenius ring has two non-zero weights. There is a γ parameter, which is the average weight. In order to make use of the homogeneous weight in constructing good p-ary codes, we need a distance preserving Gray map from R to $\mathbb{Z}_p^s$ for some suitable s. This requires assigning a value for γ, as well as finding a suitable map.

When the characteristic is not prime, i.e., when we are in the case of $\mathbb{Z}_{p^m}$ or Galois rings, it was shown that for a suitable γ and a suitable s such a map exists. The map was found using Affine Geometries in [15]. However as in the case $\mathbb{Z}_4$, such a map generally is non-linear.

Recently, Gray maps for the homogeneous weight on such rings as R_k, $R_{k,m}$ and finite chain rings were found using first order binary Reed-Muller codes as well as Projective Geometries in [14], [10] and [9] respectively. It is clear that when the characteristic is 2, first order binary Reed-Muller codes can be used to find linear distance-preserving Gray maps for any 2-ary local Frobenius ring. The main property of first order binary Reed-Muller codes that allows is that they have two non-zero weights, and the ratio of the second weight to the first weight is exactly the same as the case of homogeneous weights.

In [1], it was shown that Generalized Reed-Muller codes (i.e. Reed-Muller codes over $\mathbb{F}_q$) of first order have the same type of properties. More precisely, $GRM_q(m,1)$ is a linear code over $\mathbb{F}_q$ defined in a similar way to the Reed-Muller codes, which is of length q^m, dimension $m+1$ and its the weight enumerator is given by $1 + (q^{m+1} - q)z^{(q-1)q^{m-1}} + (q-1)z^{q^m}$. So, there are $q-1$ codewords of full weight q^m (they are the non-zero multiples of the all 1-vector) and all the remaining vectors have weight $(q-1)q^{m-1}$. Notice that, the ratio of the weights, the number of non-zero weights, the number of elements of the bigger weight are exactly in a match with the case of the homogeneous weight. Thus we can use Generalized Reed-Muller codes of first order to find a linear distance-preserving Gray map for all p-ary local Frobenius rings of characteristic p.

We will illustrate this on a specific ring family and then construct optimal codes using the Gray map.

5.1 The Gray map for the homogeneous weight on $R_{k,(p)}$

Recall that $R_{k,(p)} = \mathbb{F}_p[u_1, u_2, \ldots, u_k]/(u_i^2, u_i u_j - u_j u_i)$, is a p-ary local Frobenius ring of characteristic p, with the unique maximal ideal $M = \langle u_1, u_2, \ldots, u_k\rangle$ and the unique minimal ideal $\mathfrak{m} = \langle u_1 u_2 \ldots u_k\rangle$. $R_{k,(p)}$ can be viewed as an $\mathbb{F}_p$-vector space with basis elements $\{1, u_1, u_2, \ldots, u_1 u_2 \ldots u_k\}$. Since to every subset of $\{1, 2, \ldots, k\}$, there exists a basis element, the size of the ring is given by

$$|R_{k,(p)}| = p^{2^k}. \tag{8}$$

To find a Gray map $\phi : R_{k,(p)} \to \mathbb{F}_p^s$ for a suitable s, we will use the first order Generalized Reed-Muller codes over $\mathbb{F}_p$. The size of the ring forces us to use $GRM_p(2^k - 1, 1)$. In this case we need to assign the average weight $\gamma = (p-1)p^{2^k-2}$. Thus for $R_{k,(p)}$, the homogeneous weight will be given by

$$w_{\text{hom}}(x) = \begin{cases} 0 & \text{if } x = 0 \\ p^{2^k-1} & \text{if } x = i \cdot (u_1 u_2 \ldots u_k),\ i \neq 0 \\ (p-1)(p^{2^k-2}) & \text{otherwise.} \end{cases} \tag{9}$$

Now we define ϕ by mapping $(u_1 u_2 \ldots u_k)$ to $(1, 1, 1, \ldots, 1)$(which is a generator of $GRM_p(2^k - 1, 1)$), and the remaining basis elements of $R_{k,(p)}$ to the remaining generators of $GRM(R_{k,(p)}, 1)$ in a bijective way and then we extend ϕ linearly over $\mathbb{F}_p$ to all the ring $R_{k,(p)}$. ϕ can be extended to $R_{k,(p)}^n$ in an obvious way, by applying it to each component, i.e. $\phi(c_1, c_2, \ldots, c_n) = (\phi(c_1), \phi(c_2), \ldots, \phi(c_n))$. The properties of the Generalized Reed-Muller codes then dictate the following theorem:

Theorem 5. *ϕ is a distance preserving linear isometry from $(R_{k,(p)}^n$, homogeneous distance) to $(\mathbb{F}_p^{p^{2^k-1}n}$, hamming distance). Thus if C is a linear code over $R_{k,(p)}$ of length n and minimum homogeneous weight d, then $\phi(C)$ is a binary linear code of length $p^{2^k-1}n$, and minimum hamming weight d. Moreover, the homogeneous weight distribution of C is the same as the Hamming weight distribution of $\phi(C)$.*

5.2 The ring $R_{2,(p)} = \mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p + uv\mathbb{F}_p$

When we put $k = 2$ in $R_{k,(p)}$, we get a special case, which can also be described by $\mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p + uv\mathbb{F}_p$. In this case the homogeneous weight is given by

$$w_{\text{hom}}(x) = \begin{cases} 0 & \text{if } x = 0 \\ p^3 & \text{if } x = i\cdot(uv),\ i \neq 0 \\ (p-1)(p^2) & \text{otherwise.} \end{cases} \quad (10)$$

We can write down the Gray map explicitly in this case by letting

$$\begin{aligned} \phi(0) &= (0,0,0,\ldots,0), \\ \phi(1) &= (\overline{0}_{p^2}, \overline{1}_{p^2}, \ldots, \overline{(p-1)}_{p^2}), \\ \phi(u) &= (0,1,2,\ldots,(p-1),\ldots,0,1,2,\ldots,p-1), \\ \phi(v) &= (\overline{0}_p, \overline{1}_p, \ldots, \overline{(p-1)}_p, \ldots, \overline{0}_p, \overline{1}_p, \ldots, \overline{(p-1)}_p), \\ \phi(uv) &= (1,1,1,\ldots,1) \end{aligned}$$

The map is then extended to the ring $R_{2,(p)}$ in an F_p-linear way, i.e.

$$\phi(a+ub+vc+uvd) := a\phi(1) + b\phi(u) + c\phi(v) + d\phi(uv) \quad (11)$$

We then obtain the following corollary of Theorem 5

Corollary 1. *If C is a linear (n, p^r, d)-code over $\mathbb{F}_p + u\mathbb{F}_p + v\mathbb{F}_p + uv\mathbb{F}_p$, with p^r denoting the size of the code and d its homogeneous minimum distance, then $\phi(C)$ is a linear $[p^3n, r, d]$ code over $\mathbb{F}_p$ with the usual Hamming minimum distance d.*

5.3 Griesmer-Optimal codes over $\mathbb{F}_p$ from codes over $R_{2,(p)}$

The Griesmer bound, introduced in [5], gives us an upper bound for the minimum distance of a linear code over finite fields. The codes for which the bound is attained are called optimal codes. For a linear $[n,k,d]$-code over $\mathbb{F}_q$, the bound is given by

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

where $\lceil x \rceil$ denotes the smallest integer greater than or equal to x. By a Griesmer-optimal code, we will denote a code that attains this bound. Finding Griesmer-optimal codes over different alphabets has attracted a considerable amount of attention in Coding Theory. Among the many works related to this problem we can refer to [6], [7] and references therein. In what follows, we will construct Griesmer-optimal codes over $\mathbb{F}_p$ for $p = 2, 3$ and 5 using the Gray-homogeneous images of linear codes over $R_{2,(p)}$.

5.3.1 $[p^3n, 4, (p-1)p^2n]_p$ codes

Let us take C to be the linear code over $R_{2,(p)}$ of length n generated by the vector $(1,1,\ldots,1)$. Since every codeword in C is of the form $(a,a,\ldots,a)$ with $a \in R_{2,(p)}$, we see that the minimum homogeneous weight of C is $(p-1)p^2n$. Since the generating vector $(1,1,\ldots,1)$ contains units, we see that $|C| = p^4$. Thus, by taking the Gray image of C, in the light of Corollary 5, we get

Theorem 6. *$\phi(C)$ is a linear code over $\mathbb{F}_p$ with parameters $[p^3n, 4, (p-1)p^2n]$.*

Corollary 2. *If we take $p = 2$, we see that we get binary linear codes with parameters $[8n, 4, 4n]$ which are all Griesmer-optimal for $1 \leq n \leq 6$.*

Corollary 3. *If we take $p = 3$, we get ternary linear codes with parameters $[27n, 4, 18n]$, which are all Griesmer-optimal for $1 \leq n \leq 9$.*

Corollary 4. *If we take $p = 5$, we get linear codes over $\mathbb{F}_5$ with parameters $[125n, 4, 100n]$ which are all Griesmer-optimal for $1 \leq n \leq 15$.*

5.3.2 $[p^4n, 5, (p-1)p^3n]_p$ codes

Theorem 7. *Let C be the linear code over $R_{2,(p)}$ of length p generated by the vectors $\{(1,1,1,\ldots,1), (0,uv,2uv,\ldots,(p-1)uv)\}$. Then C is of size p^5 with minimum homogeneous distance $(p-1)p^3$.*

Proof. The codewords in C are of the form $a\cdot(1,1,\ldots,1) + b(0,uv,2uv,\ldots,(p-1)uv)$ where $a \in R_{2,(p)}$ and $b \in \mathbb{F}_p$. Linear independence can be seen from the first coordinates. So $|C| = p^4 \cdot p = p^5$.

Since $\mathbb{F}_p$ is a field, for a nonzero $b \in \mathbb{F}_p, b\cdot(0,uv,2uv,\ldots,(p-1)uv)$ is just a permutation of $(0,uv,2uv,\ldots,(p-1)uv)$. This means every nonzero codeword $\overline{c}$ of C is a permutation of $(a, a+uv, a+2uv, \ldots, a+(p-1)uv)$ for some $a \in R_{2,(p)}$. Now if $a \notin \{0,uv,\ldots,(p-1)uv\}$, then $\overline{c}$ contains all nonzero coordinates which means $w_{hom}(\overline{c}) \geq p\cdot(p-1)p^2 = (p-1)p^3$. If $a \in \{0,uv,\ldots,(p-1)uv\}$, then $\overline{c}$ is a permutation of $(0,uv,2uv,\ldots,(p-1)uv)$ and hence $w_{hom}(\overline{c}) = (p-1)p^3$.

Corollary 5. *By taking the repetitions of the generators in Theorem 7 and applying the Gray map, we get linear codes over $\mathbb{F}_p$ with parameters $[p^4n, 5, (p-1)p^3n]$.*

Corollary 6. *If we take $p = 2$, we obtain binary linear codes with parameters $[16n, 5, 8n]$, which are Griesmer-optimal for $1 \leq n \leq 8$.*

Corollary 7. *If we take $p = 3$, we obtain ternary linear codes with parameters $[81n, 5, 54n]$ which are all Griesmer-optimal for $1 \leq n \leq 12$.*

Corollary 8. *If we take $p = 5$, we obtain linear codes over $\mathbb{F}_5$ with parameters $[625n, 5, 500n]$ which are all Griesmer-optimal for $1 \leq n \leq 20$.*

5.3.3 $[p^5n, 6, (p-1)p^4n]_p$ codes

Theorem 8.*Let C be the linear code over $R_{2,(p)}$ of length p^2 generated by the vectors $\{\overline{1} = (1,1,1,\ldots,1), \overline{b} = (0,b_1,b_2,\ldots,b_{p^2-1})\}$, where*

$$\{0,b_1,\ldots,b_{p^2-1}\} = u\cdot(R_{2,(p)}).$$

Then C is of size p^6 with minimum homogeneous distance $(p-1)p^4$.

*Proof.*Every codeword in C is of the form $x\cdot\overline{1} + y\cdot\overline{b}$ where $x \in R_{2,(p)}$, $y \in \mathbb{F}_p + v\mathbb{F}_p$. Since linear independence is obvious from the first coordinates, we see that $|C| = p^4\cdot p^2 = p^6$.

Now, because of the structure of the ring $R_{2,(p)}$, every nonzero codeword in C is either of the form $(x,x,x,\ldots,x)$ which has weight $\geq p^2\cdot(p-1)p^2 = (p-1)p^4$; or a permutation of $(0,b_1,b_2,\ldots,b_{p^2-1})$, which has weight $(p-1)\cdot p^3 + (p^2-p)(p-1)p^2 = (p-1)p^4$; or is of the form $\overline{c} = (x,x+yb_1,\ldots,x+yb_{p^2-1})$ where $x \in R_{2,(p)}$ and $y \in \mathbb{F}_p + v\mathbb{F}_p$. Now, if y is a unit and $x \notin u(R_{2,(p)})$, then $\overline{c}$ is just a permutation of $(x,x+b_1,\ldots,x+b_{p^2-1})$, which has no zero coordinates and hence $w_{hom}(\overline{c}) \geq p^2\cdot(p-1)p^2 = (p-1)p^4$. If $x \in u(R_{2,(p)})$ and y is a unit, then $\overline{c}$ will have exactly one zero coordinate and $p-1$ coordinates that are multiples of uv. Thus $w_{\text{hom}}(\overline{c}) = (p-1)\cdot p^3 + (p^2-p)(p-1)p^2 = (p-1)p^4$. Finally, if y is a multiple of v, then $(0,yb_1,\ldots,yb_{p^2-1})$ will have exactly p zero coordinates and p^2-p coordinates that are multiples of uv which has weight $(p^2-p)p^3 = (p-1)p^4$. The case when $x \neq 0$ with this last case is very similar to the case handled before.

*Remark.*Note that, by taking the repetitions of the generators in the previous theorem, and then applying the Gray map one can obtain linear codes over $\mathbb{F}_p$ with parameters $[p^5n, 6, (p-1)p^4n]$.

Corollary 9.*If we take $p = 2$, we obtain binary linear codes with parameters $[32n, 6, 16n]$, which are all Griesmer-optimal when $1 \leq n \leq 10$.*

Corollary 10.*If we take $p = 3$, we obtain ternary linear codes with parameters $[243n, 6, 162n]$, which are all Griesmer-optimal when $1 \leq n \leq 15$.*

*Remark.*We do actually obtain similar results for $p = 5$ that are optimal for even more values of n, but since the lengths of the codes must be multiples of 3125, it is not very practical to study them.

5.3.4 $[p^6n, 7, (p-1)p^5n]_p$ codes

With a similar argument we can find linear codes over $R_{2,(p)}$ of length p^3, size p^7 and minimum homogeneous weight $(p-1)p^5$. The generators one can take to construct this code would be $(1,1,1\ldots,1)$ and $(0,b_1,\ldots,b_{p^3-1})$ where the set $\{0,b_1,\ldots,b_{p^3-1}\}$ is the set of all zero-divisors of the ring $R_{2,(p)}$. This code would have minimum homogeneous weight $(p-1)p^5$, the proof of which, being similar to the previous ones, will be omitted. Then, taking repetitions of the generators and applying the Gray map, we would obtain linear codes over $\mathbb{F}_p$ with parameters $[p^6n, 7, (p-1)p^5n]$. We could analyze the optimality of these codes using the Griesmer bound but since the lengths of the codes are quite restrictive(the length being multiple of 64 for binary codes, of 729 for ternary codes, etc.), we will omit that for practical reasons.

6 Conclusion

We have shown that the homogeneous weight for any p-ary local Frobenius ring has two non-zero values. The weight of an element simply depends on whether it is in the minimal ideal or not. We believe that the same is true for any local Frobenius ring. In that case the generating character has to change in order to accommodate for the change of the residue field.

An important property of the homogeneous weight is that we get divisible codes as a result. Because the two non-zero values are described in terms of powers of the prime p, many of the codes that we have obtained in section 5.3 fall into the category of divisible codes, described by Ward in [12]. This makes the codes we obtained even more special because they are Griesmer-optimal and divisible. The relative ease with which we obtained Griesmer-optimal codes, which are otherwise hard to obtain, increases the relevance of the tools we have discussed.

For applications, we focused on a rather special class of p-ary local Frobenius rings. We believe that similar results can be obtained for other examples of such rings. We also think that many of the results and characterizations can be carried over to more general classes of rings.

Acknowledgement:

The authors are grateful to the anonymous referee(s) for a careful checking of the details and for helpful comments that improved this paper.

References

[1] E.F. Assmus Jr and J.D. Key, Designs and Their Codes, Cambridge Tracts in Mathematics, Cambridge University Press, 1992.

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

[3] S.T. Dougherty, B. Yildiz and S. Karadeniz, Codes over R_k, Gray Maps and their Binary Images, Finite Fields Appl., **17**, 205–219 (2011).
[4] M. Greferath and M.E. O'Sullivan, On bounds for codes over Frobenius rings under homogeneous weights, Discrete Mathematics, **289**, 11–24 (2004).
[5] J.H. Griesmer, A bound for error correcting codes, IBM J. Res. Dev., **4**, 532–542 (1960).
[6] N. Hamada, A Necessary and sufficident condition for the existence of some ternary $[n,k,d]$ codes meeting the Griesmer bound, Designs Codes and Cryptography, **10**, 41–56 (1997).
[7] T. Helleseth, Further Classifications of Codes Meeting the Griesmer Bound, IEEE Trans. Inform. Theory, **30**, 395–403 (1984).
[8] T. Honold, A Characterization of finite Frobenius rings, Arch. Math.(Basel), **76**, 406–415 (2001).
[9] A. Pasa and B. Yildiz, Constructing Gray maps from combinatorial geometries, Commun. Fac. Sci. Univ. Ank. Serie A1, **63**, 147–161 (2014).
[10] N. Tufekci and B. Yildiz, On codes over $\mathscr{R}_{k,m}$ and constructions for new binary self-dual codes, **to appear** in Mathematica Slovaca.
[11] J.F. Voloch and J.L. Walker, Homogeneous weights and exponential sums, Finite Fields and Their Applications, **9**, 310–321 (2003).
[12] H.N. Ward, Divisible codes, Arch. Math., **36**, 485–499 (1981).
[13] J. Wood, Duality for modules over finite rings and applications to coding theory, Amer. J. Math., **121**, 555–575 (1999).
[14] B. Yildiz and I.G. Kelebek, The homogeneous weight for R_k, related Gray map and new binary quasicyclic codes, ArXiv: 1504.04111, 2014.
[15] B. Yildiz, A Combinatorial construction of the Gray map over Galois rings, Discrete Mathematics, **309**, 3408–3412 (2009).
[16] 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**, 61–81 (2010).
[17] 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 and Applications, **27**, 24–240, (2014).

Bahattin YILDIZ is Associate Professor of Mathematics at Fatih University, Istanbul Turkey. He received his PhD degree from California Institute of Technology(CALTECH), CA, USA in 2006. His research interests are in the areas of Coding Theory, Combinatorics and Applied Algebra.

Makarim Abdlwaheed Abdljabbar is a PhD student at Fatih University, Istanbul-TURKEY. She received her Bachelors degree from the College of Education in Al Anbar University (Iraq) in 1995 and her Masters degree from College of Education in Al Mustansiriya University(Iraq) in 2003. Her research area is in the field of Algebraic Coding Theory.