Commun.Fac.Sci.Univ.Ank.Series A1
Volume 63, Number 2, Pages 147–161 (2014)
ISSN 1303–5991

CONSTRUCTING GRAY MAPS FROM COMBINATORIAL GEOMETRIES

ABDULLAH PAŞA AND BAHATTİN YILDIZ

Abstract. The focus of this work is constructing Gray maps for linear codes over a family of Frobenius rings, using tools from combinatorial geometries. The main combinatorial structure that are used are projective geometries $PG_n(q)$, defined over $\mathbb{F}_q$. Codes over $\mathbb{Z}_{p^k}$, Galois rings, finite chain rings and R_k have been considered with respect to homogeneous weights. Using hyperplanes in projective geometries, distance preserving Gray maps from aforementioned rings to residue fields have been constructed. The use of projective geometries serves as a novel approach to what was a primarily algebraic approach in the literature. The constructions also serve as a motivation for using homogeneous weights.

1. Introduction

In the ground-breaking paper [9], it was shown that some well known nonlinear binary codes could be obtained as Gray images of linear codes over $\mathbb{Z}_4$. In this paper, Hammons et al. gave a distance preserving map from $\mathbb{Z}_4$ to $\mathbb{F}_2^2$. This opened up a new venue for Coding Theory, and there has been an extensive amount of research on linear codes over rings. Later the work done in this paper were extended in many different directions with different weights. In [4], Carlet extended this map to $\mathbb{Z}_{2^k}$ with homogeneous weight and used this to obtain the generalized Kerdock codes. In [8], Greferath and Schmidt defined Gray isometries for finite chain rings in their paper. Yildiz gave an inductive construction of the Gray map from $\mathbb{Z}_{p^k}$ to $\mathbb{Z}_p^{p^{k-1}}$ in [14] and he also gave a combinatorial construction of the Gray map for Galois rings by using Affine geometries in [15]. In this paper, we generalize construction of the Gray map for finite chain rings and the family of the ring R_k by using another important tool of Combinatorics, which is projective geometries.

Received by the editors 10.11.2013, accepted: 10.08.2014.

2010 *Mathematics Subject Classification.* 13M99, 94B65.

Key words and phrases. Projective geometries, Hyperplanes, Gray Map, Homogeneous weight, Finite chain rings, R_k.

*This work was partially presented in the proceedings of the 2nd Algerian Turkish International days on Mathematics, İstanbul, TURKEY, 2013.

In section 2, we give a background on finite chain rings and family of the ring R_k together with homogeneous weights.

In section 3, we give basic definitions and properties of projective geometries.

Section 4 will contain our main contributions, which are the construction of the distance preserving Gray maps for finite chain rings and the family of the ring R_k by using tools from projective geometries.

In the last section, we conclude with some final thoughts and possible directions for future work.

2. Codes over Rings and the Homogeneous Weight

Let R be a finite commutative ring. A code over R of length n is a subset of R^n. A linear code over R of length n is an R-submodule of R^n. There are many different types of rings that have been considered in the literature. The largest class of rings that can be studied for coding theory is Frobenius rings [13]. Finite chain rings of the form $\mathbb{Z}_{p^k}$, Galois rings, the R_k family of the rings are special examples of Frobenius rings. Codes over rings differ from codes over finite fields, as for example a ring may have zero divisors, while a field does not. The algebraic structure of the code also changes from a vector space to a module. The notions of weight and distance are similarly defined for rings, only this time other weights than the Hamming weight can be considered. As an example, the homogeneous weight can be considered for rings.

2.1. Codes over Finite Chain Rings.

Definition 2.1. A commutative ring with identity is called a finite chain ring if its ideals are ordered by inclusion.

A finite chain ring R has a unique maximal ideal which we denote by (γ) and let its residue field $R/(\gamma)$ be F_q where q is a prime power. The ideal structure of R can be listed as

$$0 = (\gamma^d) \subset (\gamma^{d-1}) \subset \cdots \subset (\gamma^2) \subset (\gamma) \subset R$$

for some d. This d is called the nilpotency index of R, which is defined to be the smallest positive integer such that $\gamma^d = 0$ where γ is a generator of its maximal ideal.

One can see that, the ring $\mathbb{Z}_{p^k}$ and the Galois ring are examples of finite chain rings.

Definition 2.2. Let R be a finite chain ring. A linear code C of length n over R is an R-submodule of R^n.

The following theorem helps us understand the question of type and size for linear codes over finite chain rings:

Theorem 2.3. [11] *Let R be a finite chain ring with maximal ideal $\langle\gamma\rangle$, where γ is the generator of maximal ideal with nilpotency index d. The generating matrix for a code C over R is permutation equivalent to a matrix of the form:*

$$G = \begin{bmatrix} I_{k_1} & A_{1,1} & . & . & . & A_{1,d} \\ 0 & \gamma I_{k_2} & \gamma A_{2,2} & . & . & \gamma A_{2,d-1} \\ 0 & 0 & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 0 & 0 & . & 0 & \gamma^{d-1} I_{k_d} & \gamma^{d-1} A_{d,1} \end{bmatrix}$$

where the matrices A_i's, B_j's and so on are matrices over R and the columns are grouped into blocks of size k_1, k_2,...,k_d. The size of C is $|R/(\gamma)|^\alpha$, where

$$\alpha = \sum_{i=1}^{d} k_i(d+1-i).$$

In this case, we say that C is of type

$$(k_1, k_2, \ldots, k_d)$$

There is an extensive literature on codes over finite chain rings.We refer to [8], [10] and references therein for further details.

2.2. **Codes over R_k.**

Definition 2.4. The ring R_k is defined in [7] as follows:

$$R_k = \mathbb{F}_2[u_1, u_2, \ldots, u_k]/(u_i^2 = 0,\ u_i u_j = u_j u_i)$$

The ring can also be defined recursively,

$$R_k = R_{k-1}[u_k]/(u_k^2 = 0, u_k u_j = u_j u_k) = R_{k-1} + u_k R_{k-1}, \quad j = 1, 2, \ldots, k-1$$

R_k is not a chain ring for $k > 1$, but it has a unique maximal ideal, given by $I_{u_1,u_2,\ldots,u_k} = \langle u_1, u_2, \ldots, u_k\rangle$ and a unique minimal ideal, given by $I_{u_1 u_2 \ldots u_k} = \langle u_1 u_2 ... u_k\rangle$.

First example of the ring R_k is R_1 that is $\mathbb{F}_2 + u\mathbb{F}_2$ which is introduced in [2] for constructing lattices. Codes over this ring have been studied by a number of researchers. We refer to [3], [6], [12] for some of these works. The second example of R_k is R_2 which is $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. The ring R_2 is an extension of R_1. The ring R_2 is introduced by Yildiz and Karadeniz in [16]. Codes over this ring have been studied by them further in [17], [18], [19].

In general, a linear code of length n over R_k is a submodule of R_k^n. Note that since R_k is not a chain ring when $k \geq 2$, the generating matrix is not in a standard form as for codes over chain rings, so we cannot define type in terms of such a matrix.

2.3. **The Homogeneous Weight.** The homogeneous weight was first introduced by I. Constantinescu and W. Heise [5]. This weight may be viewed as a generalization of the Hamming weight for finite rings.

Definition 2.5. A real valued function w on the finite ring R is called a (left) homogeneous weight if $w(0) = 0$ and the followings are true:

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

(H2) There exists a real number δ such that

$$\sum_{y \in Rx} w(y) = \delta |Rx|, \text{ for all} : x \in R \setminus \{0\}.$$

Right homogeneous weights are defined accordingly, and since we are dealing exclusively with commutative rings, we'll simply refer to them as homogeneous weights.

We next introduce the homogeneous weight for linear codes over R_k and linear codes over finite chain rings.

For linear codes over finite chain rings, the homogeneous weight was introduced in [8] as follows:

$$w_{\text{hom}}(u) = \begin{cases} 0 & , \text{ if } u = 0 \\ q^{d-1} & , \text{ if } u \in (\gamma^{d-1}) \backslash \{0\} \\ q^{d-2}(q-1) & , \text{ otherwise,} \end{cases}$$

where $\mathbb{F}_q$ is the residue field of the ring and (γ) is the maximal ideal with the nilpotency index d.

In [18], the homogeneous weight for R_2 is defined as

$$w_{\text{hom}}(r) = \begin{cases} 0 & , \text{ if } r = 0 \\ 8 & , \text{ if } r \in I_{uv} \backslash \{0\} \\ 4 & , \text{ otherwise.} \end{cases}$$

In [5], the notion of a homogeneous weight for codes over Frobenius rings are defined. Applying the conditions to this ring, the ideal structure of R_k dictates a homogeneous weight of the form:

$$w_{\text{hom}}(r) = \begin{cases} 0 & , \text{ if } r = 0 \\ 2\omega & , \text{ if } r \in I_{u_1 u_2 \ldots u_k} \backslash \{0\} \\ \omega & , \text{ otherwise,} \end{cases}$$

where ω is a non-negative real number.

3. Projective Geometries

Most of the material presented here was taken from [1]. Let q be a prime power, $\mathbb{F}_q$ be a finite field of order q and $V = \mathbb{F}_q^k$ be the vector space of k-tuples over $\mathbb{F}_q$. A projective subspace of V is the empty set or a linear vector subspace of V. A projective geometry $PG_{k-1}(\mathbb{F}_q)$ of order $k-1$ over $\mathbb{F}_q$ is defined to be the set of all projective subspaces of $V = \mathbb{F}_q^k$.

In the projective geometry of order $k-1$ over $\mathbb{F}_q$, which is $PG_{k-1}(\mathbb{F}_q)$, points are 1-dimensional subspaces of V, lines are 2-dimensional subspaces of V and hyperplanes are $(k-1)$ -dimensional subspaces of V. Neither $\{0\}$ nor V play a significant role in projective geometries and they are usually ignored. Frequently when working with projective geometries the projective dimension is referred to simply as the *dimension.* The dimension formula for subspaces of V holds in projective geometry as well, provided it is written as follows:

$$\dim(U) + \dim(W) = \dim(U + W) + \dim(U \cap W),$$

where U and W are arbitrary non-zero subspaces of V and $U + W = \langle U \cup W \rangle = \{u + w | u \in U, w \in W\}$. Note that we use $\langle S \rangle$ to denote the subspace generated by the set S. We can easily obtain the following remark:

Remark 3.1. Two distinct hyperplanes in $PG_{k-1}(\mathbb{F}_q)$ intersect in a projective subspace of dimension $k-2$.

The following properties of projective geometries will be used for this work:

(i) Let V be a k-dimensional vector space over $\mathbb{F}_q$, then the number of subspaces of V of dimension s, where $0 < s \le k$, is given by

$$\frac{(q^k - 1)(q^k - q)\cdots(q^k - q^{s-1})}{(q^s - 1)(q^s - q)\cdots(q^s - q^{s-1})}.$$

In particular, the number of points of $PG_{k-1}(\mathbb{F}_q)$ is

$$\frac{q^k - 1}{q - 1} = q^{k-1} + q^{k-2} + \cdots + 1$$

which is the same as the number of the hyperplanes of $PG_{k-1}(\mathbb{F}_q)$.

(ii) Let V be a k-dimensional vector space over $\mathbb{F}_q$ and P be a subspace of dimension r, and s be an integer with $0 \le r < s \le k$. Then the number of subspaces of V of dimension s that contain P is

$$\frac{(q^k - q^r)(q^k - q^{r+1})\cdots(q^k - q^{s-1})}{(q^s - q^r)(q^s - q^{r+1})\cdots(q^s - q^{s-1})}.$$

In particular, the number of hyperplanes that contain the particular point is $q^{k-2} + q^{k-3} + \cdots + 1$.

It is known that the number of hyperplanes is $q^{k-1} + q^{k-2} + \cdots + 1$ and the number of hyperplanes that contain a particular points is $q^{k-2} + q^{k-3} + \cdots + 1$. Hence we have:

Observation 3.2. Let V be a k-dimensional vector space over $\mathbb{F}_q$, then the number of hyperplanes in $PG_{k-1}(\mathbb{F}_q)$ that do not contain a particular point is q^{k-1}.

Let $P = \{\bar{p}_0, \bar{p}_1, \ldots, \bar{p}_{q-1}\}$ be a projective point, which is a 1-dimensional subspace of V, where $\bar{p}_i \in V = \mathbb{F}_q^k$, $i = 0, 1, \ldots, q-1$ and let $H_0, H_1, \ldots, H_{q^{(k-1)}-1}$ be hyperplanes that don't contain point P.

We look at the cosets of these hyperplanes which are defined by $\bar{p}_i + H_m$, such that $\bar{p}_i \in P$, H_m's are hyperplanes that do not contain P and $i = 0, 1, .., q-1$; $m = 0, 1, \ldots, q^{k-1} - 1$.

Let Γ_m be the set of all cosets of H_m. So,

$$\Gamma_m = \{(\bar{p}_0 + H_m), (\bar{p}_1 + H_m), \ldots, (\bar{p}_{q-1} + H_m)\}$$

We prove the following lemma which will be used in the subsequent parts of our work:

Lemma 3.2. *$(\bar{p}_i + H_m) \cap (\bar{p}_j + H_l)$ has q^{k-2} elements for all $i, j = 0, 1, \ldots, q-1$ and $m, l = 1, \ldots, q^{k-1}$ where $m \neq l$.*

Proof. Since hyperplanes are $(k-1)$-dimensional subspaces of V, they both have bases. Let $\{\bar{v}_0, \bar{v}_1, \ldots, \bar{v}_{k-1}\}$ be a basis of V and let H_1 and H_2 be hyperplanes such that $\{\bar{v}_0, \bar{v}_2, \bar{v}_3, \ldots, \bar{v}_{k-1}\}$ is a basis for H_1 and $\{\bar{v}_0, \bar{v}_1, \bar{v}_{3,...,} \bar{v}_{k-1}\}$ is a basis for H_2.

This means all elements of H_1 are of the form $\alpha_1 v_0 + \alpha_2 v_2 + \alpha_3 v_3 + \cdots + \alpha_{k-1} v_{k-1}$ where $\alpha_i \in \mathbb{F}_q$, and all elements of H_2 are of the form $\beta_1 v_0 + \beta_2 v_1 + \beta_3 v_3 + \cdots + \beta_{k-1} v_{k-1}$ where $\beta_j \in \mathbb{F}_q$.

The elements of cosets are of the following form:

$$\bar{p}_i + H_1 \to \bar{p}_i + \alpha_1 v_0 + \alpha_2 v_2 + \alpha_3 v_3 + \cdots + \alpha_{k-1} v_{k-1},$$

$$\bar{p}_j + H_2 \to \bar{p}_j + \beta_1 v_0 + \beta_2 v_1 + \beta_3 v_3 + \cdots + \beta_{k-1} v_{k-1}.$$

To find the number of elements of $(\bar{p}_i + H_m) \cap (\bar{p}_j + H_l)$, it is enough to determine when the following equation holds:

$$\bar{p}_i + \alpha_1 v_0 + \alpha_2 v_2 + \cdots + \alpha_{k-1} v_{k-1} = \bar{p}_j + \beta_1 v_0 + \beta_2 v_1 + \cdots + \beta_{k-1} v_{k-1}.$$

This is equivalent to

$$\bar{p}_j - \bar{p}_i = (\beta_1 - \alpha_1) v_0 + \beta_2 v_1 - \alpha_2 v_2 + (\beta_3 - \alpha_3) v_3 + \cdots + (\beta_{k-1} - \alpha_{k-1}) v_{k-1}.$$

It is known that $\bar{p}_j - \bar{p}_i \in V$ and all elements of V can be expressed by using the basis of V. So $\bar{p}_j - \bar{p}_i$ can be written as

$$\bar{p}_j - \bar{p}_i = \gamma_1 v_0 + \gamma_2 v_1 + \cdots + \gamma_k v_{k-1},\ \gamma_i \in \mathbb{F}_q.$$

Then, we have

$$(\beta_1 - \alpha_1) v_0 + \beta_2 v_1 - \alpha_2 v_2 + (\beta_3 - \alpha_3) v_3 + \cdots + (\beta_{k-1} - \alpha_{k-1}) v_{k-1} = \sum_{j=0}^{k-1} \gamma_j v_{j-1}$$

which leads to the following equations:

$$\begin{aligned}
(\beta_1 - \alpha_1) &= \gamma_1 \\
(\beta_2) &= \gamma_2 \\
(-\alpha_3) &= \gamma_3 \\
(\beta_4 - \alpha_4) &= \gamma_4 \\
&\vdots \\
(\beta_{k-1} - \alpha_{k-1}) &= \gamma_k,
\end{aligned}$$

where the γ_i's are known. So, it is enough to look at α_i's and β_i's. It is easy to observe that $\alpha_3 = -\gamma_3$ and $\beta_2 = \gamma_2$ so, these two are fixed. Thus, there are $(k-2)$ equations that will be considered. They are all of the form $(\beta_i - \alpha_i) = \gamma_i$.

It is known that γ_i's are fixed so for each α_i there is a fixed β_i. Since there are q choices for α_i, there are q choices for each equation. This leads to $q^{(k-2)}$ different solutions for α_i's and β_i's. This means $(\bar{p}_i + H_m) \cap (\bar{p}_j + H_l)$ has $q^{(k-2)}$ elements, i.e., any coset in Γ_m intersects any coset in Γ_l in exactly $q^{(k-2)}$ points. □

4. The Construction of the Gray Maps

4.1. **The Construction of the Gray Map for Finite Chain Rings.** We are now ready to give a coordinate-wise construction of the Gray map from a finite chain ring to its residue field that preserves the homogeneous distance.

First of all, recall how the homogeneous weight is defined for finite chain rings.

$$w_{\text{hom}}(u) = \begin{cases} 0 & , \ \text{if } u = 0 \\ q^{d-1} & , \ \text{if } u \in (\gamma^{d-1})\backslash\{0\} \\ q^{d-2}(q-1) & , \ \text{otherwise.} \end{cases}$$

For the construction of the Gray map for finite chain rings whose residue field is $\mathbb{F}_q$ and maximal ideal (γ) with nilpotency index d, the projective geometry that we will consider is $PG_{d-1}(\mathbb{F}_q)$.

So we can quickly say that the number of hyperplanes that do not contain a particular point P is $q^{(d-1)}$ by using the properties of the projective geometries that are given in the previous section.

Let $P = \{\bar{p}_0, \bar{p}_1, \ldots, \bar{p}_{q-1}\}$ be a particular point. Let H_1 be a hyperplane that does not contain point P and write all cosets of H_1 which we denoted by Γ_1. So,

$$\Gamma_1 = \{(\bar{p}_0 + H_1), (\bar{p}_1 + H_1), \ldots, (\bar{p}_{q-1} + H_1)\},$$

where $\bar{p}_0, \bar{p}_1, \ldots, \bar{p}_{q-1}$ are elements of point P and $(\bar{p}_i + H_1) = \{h_1^j + \bar{p}_i | h_1^j$ is j^{th} element of H_1 and $j = 1, 2, \ldots, q^{d-1}\}$.

Then, write elements of Γ_1, the cosets of H_1 as rows:

$$H = \begin{bmatrix} h_1^1 + \bar{p}_0 & h_1^2 + \bar{p}_0 & \cdots & h_1^{q^{d-1}} + \bar{p}_0 \\ h_1^1 + \bar{p}_1 & h_1^2 + \bar{p}_1 & \cdots & h_1^{q^{d-1}} + \bar{p}_1 \\ \vdots & \vdots & \ddots & \vdots \\ h_1^1 + \bar{p}_{q-1} & h_1^2 + \bar{p}_{q-1} & \cdots & h_1^{q^{d-1}} + \bar{p}_{q-1} \end{bmatrix}.$$

All the other hyperplanes contain only one element from each column in H. Because if a hyperplane contains at least two elements from the same column, it will contain $\bar{p}_i - \bar{p}_j$, and all of P.

Let Γ_m be a set such that it contains all cosets of H_m so,

$$\Gamma_m = \{(\bar{p}_0 + H_m), (\bar{p}_1 + H_m), \ldots, (\bar{p}_{q-1} + H_m)\}.$$

We know that the residue field of R is $\mathbb{F}_q = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$, where α is a primitive element of the field.

Take $\Gamma_1 = \{(\bar{p}_0 + H_1), (\bar{p}_1 + H_1), \ldots, (\bar{p}_{q-1} + H_1)\}$ and match all elements of Γ_1 to $\mathbb{F}_q$ as follows:

$$\begin{array}{rcl} (\bar{p}_0 + H_1) & \rightarrow & (0, 0, \ldots, 0) \\ (\bar{p}_1 + H_1) & \rightarrow & (1, 1, \ldots, 1) \\ (\bar{p}_1 + H_1) & \rightarrow & (\alpha, \alpha, \ldots, \alpha) \\ & \vdots & \\ (\bar{p}_{q-1} + H_1) & \rightarrow & (\alpha^{q-2}, \alpha^{q-2}, \ldots, \alpha^{q-2}) \end{array}$$

Call this set $\Gamma_1^{'} = \{(i, i, \ldots, i) | i = 0, 1, \ldots, \alpha^{q-2}\}$ and each vector is of length $q^{(d-1)}$. Then all other $\Gamma_m^{'}$'s can be obtained by renaming all cosets depending on this labeling.

It is known that all cosets of H_1 are distinct, each coset has q^{d-1} elements and there are total of q cosets. This means all elements of V are labeled. Now we are ready to describe the Gray map.

Definition 4.1. For $u = j \cdot (\gamma^{d-1})$ with $j = 0, 1, \ldots, \alpha^{q-2}$, G_d maps u to elements of Γ_1' bijectively in such a way 0 is mapped to labeled $(\bar{p}_0 + H_1)$ which is $(0, 0, \ldots, 0)$. For $1 \leq j \leq q^{d-1} - 1$, we map the elements of coset $\bar{c}_j = c_j + (\gamma^{d-1})$ to the elements of Γ_{j+1}' bijectively. Here $\{\bar{c}_j = c_j + (\gamma^{d-1}) | j = 1, 2, \ldots, q^{d-1} - 1\}$ denotes the set of cosets of all non-trivial cosets of (γ^{d-1}).

Theorem 4.2. *The map G_d defined above is indeed a distance preserving map.*

Proof. Suppose $u \in (\gamma^{d-1}) \backslash \{0\}$. Then this means that $G_d(u)$ is the element of the set $\Gamma_1' \backslash (0, 0, \ldots, 0)$. But this means $G_d(u)$ does not have any zeros,which means that

$$w_{\text{hom}}(G_d(u)) = q^{d-1}$$

If $v \in R\backslash(\gamma^{d-1})$ then $v \in \bar{c}_j$ for some $j > 1$ so by the definition, this means that, $G_d(v)$ is the element of the set in some Γ'_m with $m \neq 1$. But it is easy to observe that any coset in Γ_m intersects with any coset in Γ_n in q^{d-2} points, if $m \neq 1$. So any element of Γ'_m intersects any element of Γ'_1 in exactly q^{d-2} points and since $(0, 0, \ldots, 0)$ belongs to Γ'_1, $G_d(v)$ has to have exactly q^{d-2} 0's. Hence we have that

$$w_{\text{hom}}(G_d(u)) = q^{d-1} - q^{d-2} = (q-1)q^{d-2}$$

Now, suppose $u, v \in R$ so that $u - v \in (\gamma^{d-1})\backslash\{0\}$. Then by the construction of G_d,we see that $G_d(u)$ and $G_d(v)$ come from two different coset of same hyperplane this means that $G_d(u)$ and $G_d(v)$ are in the same set Γ'_m for some m. Since two different cosets of same hyperplane are distinct, two elements of any set Γ'_m are also distinct. But this means that $G_d(u)$ and $G_d(v)$ are different in each coordinate which means that $d_{\text{hom}}(G_d(u), G_d(v)) = q^{d-1}$. Suppose now that $u - v \in R\backslash(\gamma^{d-1})$ this means that $G_d(u)$ and $G_d(v)$ are elements of Γ'_m and Γ'_n respectively where $m \neq n$. But this means that $G_d(u)$ and $G_d(v)$ come from cosets of different hyperplanes and we know that cosets of different hyperplanes intersect in exactly q^{d-2} points, this means $G_d(u)$ and $G_d(v)$ will have exactly q^{d-2} coordinates where the entries are equal. Hence we see that $d_{\text{hom}}(G_d(u), G_d(v)) = q^{d-1} - q^{d-2} = (q-1)q^{d-2}$. □

Remark 4.3. In [15], Yildiz gave a combinatorial construction for the Gray map of Galois rings with respect to the homogeneous weight using Affine geometries. The construction that we have given generalizes the results in the aforementioned paper in two directions. We extend the construction to all finite chain rings and also we use projective geometries instead of Affine geometries.

4.2. **The Construction of the Gray Map for R_k.** First of all, recall how the homogeneous weight is defined for R_k

$$w_{\text{hom}}(r) = \begin{cases} 0 & , \text{ if } r = 0 \\ 2\omega & , \text{ if } r \in I_{u_1 u_2 \cdots u_k}\backslash\{0\} \\ \omega & , \text{ otherwise,} \end{cases}$$

where ω is a non-negative real number.

The homogeneous weight has not been defined for R_k in general. However by using the definition of the homogeneous weight for Frobenius rings and generalizing what Yildiz and Karadeniz did in [18], we can suggest the homogeneous weight to be defined for $\omega = 2^{2^k-2}$. This requires a Gray map to be an isometry from R_k to $\mathbb{F}_2^{2^{2^k-1}}$.

It is easy to observe that the projective geometry we need to consider is $PG_{2^k-1}(\mathbb{F}_2)$ and it is clear that the number of hyperplanes that don't contain a fixed point P is $2^{(2^k-1)}$.

Let $P = \{\bar{p}_0, \bar{p}_1\}$ be a projective point which is a 1-dimensional subspaces of V, where $\bar{p}_i \in V = \mathbb{F}_2^{2^k}$, $i = 0, 1$ and let H_1 be a hyperplane that doesn't contain point P.

We can easily find the other hyperplanes in the same way that was done for finite chain rings.

Now, find all cosets of H_1 which we call this set as Γ_1 so,

$$\Gamma_1 = \{(\bar{p}_0 + H_1), (\bar{p}_1 + H_1)\},$$

where $(\bar{p}_i + H_1) = \{h_1^j + \bar{p}_i | h_1^j \text{ is } j^{th} \text{ element of } H_1 \text{ and } j = 1, 2, \ldots, 2^{2^k - 1}\}$.

Write elements of Γ_1 which means cosets of H_1 as rows :

$$H = \begin{bmatrix} h_1^1 + \bar{p}_0 & h_1^2 + \bar{p}_0 & \cdots & h_1^{2^{2^k-1}} + \bar{p}_0 \\ \vdots & \vdots & \ddots & \vdots \\ h_1^1 + \bar{p}_1 & h_1^2 + \bar{p}_1 & \cdots & h_1^{2^{2^k-1}} + \bar{p}_1 \end{bmatrix}$$

Now, the other hyperplanes can be obtained by taking only one element from each column in H. We have all hyperplanes that don't contain point P. Let Γ_m be a set which contains all cosets of H_n. So, $\Gamma_m = \{(\bar{p}_0 + H_m), (\bar{p}_1 + H_m)\}$.

Take $\Gamma_1 = \{(\bar{p}_0 + H_1), (\bar{p}_1 + H_1)\}$. Then, label all elements of Γ_1 to $\mathbb{Z}_2$ as follows

$$\begin{array}{rcl} (\bar{p}_0 + H_1) & \rightarrow & (0, 0, \ldots, 0), \\ (\bar{p}_1 + H_1) & \rightarrow & (1, 1, \ldots, 1). \end{array}$$

Call the set $\Gamma_1^{'} = \{(i, i, \ldots, i) | i = 0, 1\}$, where each vector is of length $2^{(2^k-1)}$. Then, find all $\Gamma_m^{'}$'s by renaming all cosets depending on this labeling.

It is known that all cosets of H_1 are distinct, each coset has 2^{2^k-1} element and there are total of 2 cosets. Thus we labeled all elements of V. Now, Gray map can be described as follows:

Definition 4.4. For $u = j.u_1 u_2 \cdots u_k$, $j = 0, 1$ $G_{2^{2^k}}$ maps u to elements of Γ_1' bijectively in such a way 0 is mapped to labeled $(\bar{p}_0 + H_1)$ which is $(0, 0, \ldots, 0)$. For $1 \leq j \leq 2^{(2^k-1)} - 1$, we mapped the elements of coset $\bar{c}_j = c_j + I_{u_1 u_2 \cdots u_k}$ to the elements of Γ'_{j+1} bijectively. Here $\{\bar{c}_j = c_j + I_{u_1 u_2 \cdots u_k} | j = 1, 2, \ldots, 2^{(2^k-1)} - 1\}$ denotes the set of cosets of all non-trivial cosets of $I_{u_1 u_2 \cdots u_k}$.

Theorem 4.5. *The map $G_{2^{2^k}}$ defined above is indeed distance preserving map.*

Proof. The proof, being very similar to the proof of Theorem 4.2, has been omitted here. □

Example 4.6. Construction of the Gray map for R_2.

By letting $p = 2$ and $k = 2$, this becomes a special case for our construction, where the projective geometry is $PG_3(\mathbb{F}_2)$.

This means that hyperplanes will be 3-dimensional subspaces of $V = \mathbb{F}_2^4$ and points will be 1-dimensional subspaces of $V = \mathbb{F}_2^4$. There are $2^3 + 2^2 + 2 + 1 = 15$ points and there are 2^3 hyperplanes that don't contain a particular point.

List all points as follows:

$$
\begin{array}{ll}
P_1 = \{(0000),(0001)\} & P_9 = \{(0000),(0101)\} \\
P_2 = \{(0000),(0010)\} & P_{10} = \{(0000),(0011)\} \\
P_3 = \{(0000),(0100)\} & P_{11} = \{(0000),(1110)\} \\
P_4 = \{(0000),(1000)\} & P_{12} = \{(0000),(1101)\} \\
P_5 = \{(0000),(1100)\} & P_{13} = \{(0000),(1011)\} \\
P_6 = \{(0000),(1010)\} & P_{14} = \{(0000),(0111)\} \\
P_7 = \{(0000),(1001)\} & P_{15} = \{(0000),(1111)\} \\
P_8 = \{(0000),(0110)\} &
\end{array}
$$

Now, take a point $P_1 = \{(0000),(0001)\}$ and call it P. Then find a hyperplane that does not contain this point and call it H_1.

$$H_1 = \{(0000),(0010),(0100),(1000),(0110),(1010),(1100),(1110)\}.$$

Then, take Γ_1 to be the set of all cosets of H_1, i.e.,

$$\bar{p}_0 + H_1$$
$$H_1 = \{(0000),(0010),(0100),(1000),(0110),(1010),(1100),(1110)\}$$

$$\bar{p}_1 + H_1$$
$$H_1^{'} = \{(0001),(0011),(0101),(1001),(0111),(1011),(1101),(1111)\}$$

Write these cosets as rows of $\bar{H}$. So,

$$\bar{H} = \left\{ \begin{array}{cccccccc} (0000) & (0010) & (0100) & (1000) & (0110) & (1010) & (1100) & (1110) \\ (0001) & (0011) & (0101) & (1001) & (0111) & (1011) & (1101) & (1111) \end{array} \right\}$$

Now, to get all the other hyperplanes, it is enough to take one element each from 2^{nd} , 3^{rd} and 4^{th} columns of $\bar{H}$, since hyperplanes have dimension 3. Next, all hyperplanes can be listed as follows:

$$
\begin{array}{l}
H_1 = \{(0000),(0010),(0100),(1000),(0110),(1010),(1100),(1110)\} \\
H_2 = \{(0000),(0010),(0100),(1001),(0110),(1011),(1101),(1111)\} \\
H_3 = \{(0000),(0010),(0101),(1000),(0111),(1010),(1101),(1111)\} \\
H_4 = \{(0000),(0010),(0101),(1001),(0111),(1011),(1100),(1110)\} \\
H_5 = \{(0000),(0011),(0100),(1000),(0111),(1011),(1100),(1111)\} \\
H_6 = \{(0000),(0011),(0100),(1001),(0111),(1010),(1101),(1110)\} \\
H_7 = \{(0000),(0011),(0101),(1000),(0110),(1011),(1101),(1110)\} \\
H_8 = \{(0000),(0011),(0101),(1001),(0110),(1010),(1100),(1111)\}
\end{array}
$$

Determine the set Γ_m's which are cosets of these hyperplanes, defined by $\bar{p}_i + H_m$ where $i = 0, 1$, $m = 1, 2, 3, 4$. Since elements of point P are $\bar{p}_0 = (0000)$ and

$\bar{p}_1 = (0001)$, cosets are given as folows:

$$\begin{aligned}
H_1^{'} &= \{(0001),(0011),(0101),(1001),(0111),(1011),(1101),(1111)\}\\
H_2^{'} &= \{(0001),(0011),(0101),(1000),(0111),(1010),(1100),(1110)\}\\
H_3^{'} &= \{(0001),(0011),(0100),(1001),(0110),(1011),(1100),(1110)\}\\
H_4^{'} &= \{(0001),(0011),(0100),(1000),(0110),(1010),(1101),(1111)\}\\
H_5^{'} &= \{(0001),(0010),(0101),(1001),(0110),(1010),(1101),(1110)\}\\
H_6^{'} &= \{(0001),(0010),(0101),(1000),(0110),(1011),(1100),(1111)\}\\
H_7^{'} &= \{(0001),(0010),(0100),(1001),(0111),(1010),(1100),(1111)\}\\
H_8^{'} &= \{(0001),(0010),(0100),(1000),(0111),(1011),(1101),(1110)\}
\end{aligned}$$

Then set $\Gamma_m = \{\{H_m\},\{H_m^{'}\}\}$ and construct Γ_1' by labeling Γ_1 in such a way that label all elements of H_1 to 0 and all elements of H_1' to 1 as follows:

$$\begin{array}{ll}
(0000)\to 0 & (0001)\to 1\\
(0010)\to 0 & (0011)\to 1\\
(0100)\to 0 & (0101)\to 1\\
(1000)\to 0 & (1001)\to 1\\
(0110)\to 0 & (0111)\to 1\\
(1010)\to 0 & (1011)\to 1\\
(1100)\to 0 & (1101)\to 1\\
(1110)\to 0 & (1111)\to 1
\end{array} \quad \text{then } \Gamma_1' = \{(0,0,0,0,0,0,0,0),(1,1,1,1,1,1,1,1)\}$$

Then, label all cosets depending on this label. The labeling of cosets will be as follows:

$$\begin{array}{ll}
H_1 = (0,0,0,0,0,0,0,0) & H_1^{'} = (1,1,1,1,1,1,1,1)\\
H_2 = (0,0,0,1,0,1,1,1) & H_2^{'} = (1,1,1,0,1,0,0,0)\\
H_3 = (0,0,1,0,1,0,1,1) & H_3^{'} = (1,1,0,1,0,1,0,0)\\
H_4 = (0,0,1,1,1,1,0,0) & H_4^{'} = (1,1,0,0,0,0,1,1)\\
H_5 = (0,1,0,0,1,1,0,1) & H_5^{'} = (1,0,1,1,0,0,1,0)\\
H_6 = (0,1,0,1,1,0,1,0) & H_6^{'} = (1,0,1,0,0,1,0,1)\\
H_7 = (0,1,1,0,0,1,1,0) & H_7^{'} = (1,0,0,1,1,0,0,1)\\
H_8 = (0,1,1,1,0,0,0,1) & H_8^{'} = (1,0,0,0,1,1,1,0)
\end{array}$$

So, all Γ_i''s are given by:

$$\begin{aligned}
\Gamma_1' &= \{(0,0,0,0,0,0,0,0),(1,1,1,1,1,1,1,1)\}\\
\Gamma_2' &= \{(0,0,0,1,0,1,1,1),(1,1,1,0,1,0,0,0)\}\\
\Gamma_3' &= \{(0,0,1,0,1,0,1,1),(1,1,0,1,0,1,0,0)\}\\
\Gamma_4' &= \{(0,0,1,1,1,1,0,0),(1,1,0,0,0,0,1,1)\}\\
\Gamma_5' &= \{(0,1,0,0,1,1,0,1),(1,0,1,1,0,0,1,0)\}\\
\Gamma_6' &= \{(0,1,0,1,1,0,1,0),(1,0,1,0,0,1,0,1)\}\\
\Gamma_7' &= \{(0,1,1,0,0,1,1,0),(1,0,0,1,1,0,0,1)\}\\
\Gamma_8' &= \{(0,1,1,1,0,0,0,1),(1,0,0,0,1,1,1,0)\}
\end{aligned}$$

We define $\bar{c}_j = c_j + I_{u_1u_2\ldots u_k}$ as the set of all non-trivial cosets of $I_{u_1u_2\ldots u_k}$ for the case for R_k, where $j = 1, 2, \ldots, 2^{(2^k-1)} - 1$. For R_2 this definition becomes that $\bar{c}_j = c_j + I_{uv}$ is the set of all non-trivial cosets of I_{uv} ,where $j = 1, 2, \ldots, 7$ and $I_{uv} = \{0, uv\}$. Without loss of generality, write c_j's and $\bar{c}_j$'s as follows:

$$\begin{array}{ll} c_1 = u & \bar{c}_1 = \{u, u+uv\} \\ c_2 = v & \bar{c}_2 = \{v, v+uv\} \\ c_3 = 1 & \bar{c}_3 = \{1, 1+uv\} \\ c_4 = u+v & \bar{c}_4 = \{u+v, u+v+uv\} \\ c_5 = 1+u & \bar{c}_5 = \{1+u, 1+u+uv\} \\ c_6 = 1+v & \bar{c}_6 = \{1+v, 1+v+uv\} \\ c_7 = 1+u+v & \bar{c}_7 = \{1+u+v, 1+u+v+uv\} \end{array}$$

By construction, we map

0 and uv to elements of Γ'_1 respectively,
u and $u + uv$ to elements of Γ'_2 respectively,
v and $v + uv$ to elements of Γ'_3 respectively,
1 and $1 + uv$ to elements of Γ'_4 respectively,
$u + v$ and $u + v + uv$ to elements of Γ'_5 respectively,
$1 + u$ and $1 + u + uv$ to elements of Γ'_6 respectively,
$1 + v$ and $1 + v + uv$ to elements of Γ'_7 respectively,
$1 + u + v$ and $1 + u + v + uv$ to elements of Γ'_8 respectively.

This means that

$$\begin{array}{ll} G(0) = (0,0,0,0,0,0,0,0) & G(uv) = (1,1,1,1,1,1,1,1) \\ G(u) = (0,0,0,1,0,1,1,1) & G(u+uv) = (1,1,1,0,1,0,0,0) \\ G(v) = (0,0,1,0,1,0,1,1) & G(v+uv) = (1,1,0,1,0,1,0,0) \\ G(1) = (0,0,1,1,1,1,0,0) & G(1+uv) = (1,1,0,0,0,0,1,1) \\ G(u+v) = (0,1,1,1,0,0,0,1) & G(u+v+uv) = (1,0,0,0,1,1,1,0) \\ G(1+u) = (0,1,0,0,1,1,0,1) & G(1+u+uv) = (1,0,1,1,0,0,1,0) \\ G(1+v) = (0,1,0,1,1,0,1,0) & G(1+v+uv) = (1,0,1,0,0,1,0,1) \\ G(1+u+v) = (0,1,1,0,0,1,1,0) & G(1+u+v+uv) = (1,0,0,1,1,0,0,1) \end{array}$$

This defines a distance preserving map from R_2 to $\mathbb{F}_2^8$.

5. Conclusion

The construction we have given uses combinatorial tools to obtain the Gray maps for the homogeneous weights of codes over rings. The most common constructions for these Gray maps in literature are algebraic constructions.As can be seen from the constructions, by choosing the projective point, we get many different equivalent Gray maps for the same ring. The freedom of choice provided by the combinatorial structure makes us believe that all the other constructions can be obtained as a special case of our constructions.

The strong connection between the homogeneous weight and the combinatorial geometries may provide an additional motivation for homogeneous weights in coding theory. Thus, reversing the process, other weights and associated Gray maps may be found through other combinatorial structures.

Acknowledgement

The authors would like to thank the anonymous referees for their valuable remarks that improved the presentation of this paper.

References

[1] E.F. Assmus, J.D. Key, *Polynomial codes and finite geometries*, in V.S. Pless, W.C. Hufman Handbook of Coding Theory, **2-2** (1998), 1269-1343.
[2] C. Bachoc, *Applications of coding theory to the construction of modular lattices*, J. Comb. Theory, Ser. A, **78** (1997), 92-119.
[3] A. Bonnecaze, P. Udaya, *Cyclic codes and self-dual codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inf. Theory **45** (1998), 1250-1255.
[4] C. Carlet, $\mathbb{Z}_{2^k}$*-linear Codes*, IEEE Trans. Inf. Theory **44** (1998), 1543-1547.
[5] I. Constantinescu, W. Heise, *A metric for codes over residue class rings of integers*, Probl. Peredachi Inf. **33** (1997), 22-26.
[6] S.T. Dougherty, M. Harada, P. Gaborit, P. Solé, *Type II codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inf. Theory **45** (1999), 32-45.
[7] S.T. Dougherty, B. Yildiz, S. Karadeniz, *Codes over* R_k*, Gray maps and their binary images*, Finite Fields Appl. **17** (2011), 205-219.
[8] M. Greferath, S.E. Schmidt, *Gray isometries for finite chain rings and a nonlinear ternary* $(36, 3^{12}, 15)$ *code*, IEEE Trans. Inf. Theory **45** (1999), 2522-2524.
[9] A.R. Hammons, V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé, *The* $\mathbb{Z}_4$*-linearity of Kerdock, Preparata, Goethals and related codes*, IEEE Trans. Inf. Theory **40** (1999), 301-319.
[10] T. Honold, I. Landjev, *Linear codes over finite chain rings*, Electron. J. Comb. **7** (1998), 116-126.
[11] W.C. Huffman, *Decompositions and extremal Type II codes over* $\mathbb{Z}_4$, IEEE Trans. Inf. Theory **44** (1998) 800-809.
[12] P. Solé, S. Ling, *Duadic codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, Appl. Algebra Eng. Commun. Comput. **12** (2001), 365-379.
[13] J. Wood, *Duality for modules over nite rings and application to coding theory*, Am. J. Math. **121** (1999), 551-575.
[14] B. Yildiz, *Weight enumerators and Gray maps of linear codes over rings*, Ph.D. Thesis, California Institute of Technology, 2006.
[15] B. Yildiz, *A Combinatorial construction of the Gray map over Galois rings*, Discrete Math. **309** (2009), 3408-3412.
[16] B. Yildiz, S. Karadeniz, *Linear Codes over* $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, Des. Codes Cryptography **54** (2010), 61-81.
[17] B. Yildiz, S. Karadeniz, *Self Dual Codes over* $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, J. Franklin Inst. **347** (2010), 1888-1894.
[18] B. Yildiz, S. Karadeniz, *Cyclic Codes over* $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, Des. Codes Cryptography **58** (2011), 221-234.
[19] B. Yildiz, S. Karadeniz, *Double circulant and bordered-double circulant constructions for self-dual codes over* $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, Adv. Math. Commun. **6** (2012), 193–202.

Current address: Department of Mathematics, Fatih University, 34500 Istanbul, Turkey
E-mail address: abdpasa@gmail.com, byildiz@fatih.edu.tr
URL: http://math.science.ankara.edu.tr