Discrete Mathematics 309 (2009) 3408–3412

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Note

A Combinatorial construction of the Gray map over Galois rings

Bahattin Yildiz *

Department of Mathematics, California Institute of Technology, Pasadena, CA 91125, United States

ARTICLE INFO

Article history:
Received 5 July 2007
Received in revised form 2 May 2008
Accepted 2 September 2008
Available online 27 September 2008

This paper is dedicated to my advisor
Prof Richard M. Wilson

Keywords:
Linear codes
Galois rings
Homogenous weights
Gray maps
Affine Geometries
Affine Hyperplanes

ABSTRACT

In this correspondence, we will introduce a new combinatorial method for a coordinate-wise construction of the homogeneous-weight preserving Gray map for Galois rings by using elementary tools from Affine Geometries. Our construction differs in the methods used from the algebraic constructions done previously in [M. Greferath, S.E. Schmidt, Gray Isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code, IEEE Trans. Inform. Theory 45 (1999) 2522–2524; S. Ling, J.T. Blackford, $\mathbb{Z}_{pk+1}$-linear codes, IEEE Trans. Inform. Theory 48 (2002) 2592–2605].

1. Introduction

For the purposes of this correspondence, by a Gray map on Galois rings we will mean a map from $(GR(p^\ell, m)^n$, homogeneous weight) to $(\mathbb{F}_{p^m}^{np^{(\ell-1)m}}$, Hamming weight) that is weight-preserving. The Galois rings and homogeneous weights are going to be defined in the next section.

Gray maps from $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^{2n}$ were effectively used by Hammons et al. in their work [5], as a tool to obtain the binary nonlinear Kerdock, Preparata-like, and Goethals codes as the Gray images of linear codes over $\mathbb{Z}_4$. Their definition of the Gray map is quite a simple one. To define it, they defined maps α, β, γ from $\mathbb{Z}_4$ to $\mathbb{Z}_2$ such that for any $c \in \mathbb{Z}_4$, $c = \alpha(c) + 2\beta(c)$ is the unique 2-adic expansion of c. The identity $\alpha(c) + \beta(c) + \gamma(c) = 0$ completed the definition of those maps. Then, extending these maps in an obvious way to $\mathbb{Z}_4^n$, they defined the Gray map $\phi : \mathbb{Z}_4^n \to \mathbb{Z}_2^{2n}$ as

$$\phi(\overline{c}) = (\beta(\overline{c}), \gamma(\overline{c})), \quad \overline{c} \in \mathbb{Z}_4^n. \tag{1.1}$$

The most important property of this map is that it is a distance preserving map, that is, it is an isometry from

$$(\mathbb{Z}_4^n, \text{Lee distance}) \text{ to } (\mathbb{Z}_2^{2n}, \text{Hamming distance}). \tag{1.2}$$

Carlet, in [1], extended this map to $\mathbb{Z}_{2^k}$ with the homogeneous weight and used this to obtain the generalized Kerdock codes that were non-linear binary codes with large minimum distances. Several other authors, like Ling et al. and Greferath et al. generalized the notion of Gray maps to more general rings with certain homogeneous weights defined on them in [8,3, 4]. In particular, in [8], Ling and Blackford introduced a Gray map from $\mathbb{Z}_{p^{k+1}}^n$ to $\mathbb{Z}_p^{p^k n}$ that is homogeneous-weight-preserving.

* Corresponding address: Department of Mathematics, Fatih University, 34500 Istanbul, Turkey. Fax: +90 212 866 3402.
E-mail address: bahattin@alumni.caltech.edu.

0012-365X/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2008.09.002

Their description of the weight uses algebraic methods applied to the p-adic representation of elements in $\mathbb{Z}_{p^{k+1}}$. While the same methods used can be applied to Galois rings, in fact to any chain rings as was done in [3] by Greferath and Schmidt, we want to introduce a new method that uses elementary tools from Combinatorics.

In Section 2, we will introduce Galois rings and the homogeneous weight defined on Galois rings. In Section 3, we will describe the tools from Affine Geometries. In Section 4, we will give our main description of the Gray map on Galois rings by using the tools from Affine Geometries. In the final section we will conclude with some final thoughts and remarks.

2. Galois Rings and the homogeneous weight

Throughout, p denotes a prime number. The introduction given here is taken mainly from [10] and also appears in [12]. Let $\phi(x) \in \mathbb{Z}_{p^\ell}[x]$ be a basic irreducible polynomial of degree m. Then, the Galois ring $GR(p^\ell, m)$ is defined as the quotient $\mathbb{Z}_{p^\ell}[x]/(\phi(x))$. If m_1 is a positive integer such that $m_1|m$, then $GR(p^\ell, m_1)$ is a subring of $GR(p^\ell, m)$. A very important property of Galois rings is that it is a finite chain ring and it also has a unique maximal ideal which is given by $(p) = pGR(p^\ell, m)$ and the quotient field is

$$\frac{GR(p^\ell, m)}{pGR(p^\ell, m)} \simeq F_{p^m}. \tag{2.1}$$

All the ideals of $GR(p^\ell, m)$ can be ordered as

$$\{0\} = p^\ell GR(p^\ell, m) \subset p^{\ell-1}GR(p^e, m) \subset \cdots \subset pGR(p^\ell, m) \subset GR(p^\ell, m). \tag{2.2}$$

What is done for Galois rings in this work can easily be extended to general finite chain rings. A linear code C over the Galois ring $GR(p^\ell, m)$ of length n is a $GR(p^\ell, m)$-submodule of $GR(p^\ell, m)^n$. The following theorem from [6] helps us understand the question of type and size for linear codes over Galois rings:

Theorem 2.1 ([6]). *A $GR(p^\ell, m)$-linear code C is permutation-equivalent to a code with generating matrix of the form*

$$G = \begin{bmatrix} I_{k_1} & A_1 & . & . & . & A_\ell \\ 0 & pI_{k_2} & pB_1 & . & . & pB_{\ell-1} \\ 0 & 0 & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 0 & 0 & . & 0 & p^{\ell-1}I_{k_\ell} & p^{\ell-1}D \end{bmatrix} \tag{2.3}$$

where the matrices A_i's, B_j's and so on are matrices over $GR(p^\ell, m)$ and the columns are grouped into blocks of size $k_1, k_2, \ldots, k_\ell$. The size of C is $p^{m\alpha}$, where

$$\alpha = \sum_{i=1}^{\ell} k_i(\ell + 1 - i). \tag{2.4}$$

In this case, we say that C is of type

$$(p^{\ell m})^{k_1}(p^{(\ell-1)m})^{k_2} \cdots (p^m)^{k_\ell}. \tag{2.5}$$

We next introduce the *homogeneous weight* for linear codes over Galois rings which first appears in [2] and later in [11] as:

$$w_{\text{hom}}(x) := \begin{cases} 0 & \text{if } x = 0 \\ p^{m(\ell-1)} & \text{if } 0 \neq x \in p^{\ell-1}GR(p^\ell, m) \\ (p^m - 1)p^{m(\ell-2)} & \text{otherwise.} \end{cases} \tag{2.6}$$

We naturally extend this definition to codes by letting, for $\overline{c} = (c_1, c_2, \ldots, c_n) \in GR(p^\ell, m)^n$,

$$w_{\text{hom}}(\overline{c}) = \sum_{i=1}^{n} w_{\text{hom}}(c_i). \tag{2.7}$$

3. Combinatorial tools-affine geoemetries

Most of the material presented here was taken from [9], and can be found in any book about finite geometries. For material on finite fields we refer to [7].

An *Affine space* $AG_\ell(p^m)$ of dimension ℓ over $\mathbb{F}_{p^m}$ is defined to be the set $V = \mathbb{F}_{p^m}^\ell$ of all points and all Affine subspaces of V. An *Affine subspace* of V is the empty set or a linear vector subspace of V or a coset of a linear subspace of V in the additive group.

An *Affine Hyperplane* in $AG_\ell(p^m)$ is defined to be an Affine subspace of V of dimension $\ell - 1$. We observe the following remark:

Remark 3.1. Two hyperplanes in $AG_\ell(p^m)$ are either disjoint or they intersect in an Affine subspace of dimension $\ell - 2$.

Definition 3.2. Suppose A, B are hyperplanes in $AG_\ell(p^m)$. We say that A and B are *parallel* if $A = B$ or A and B are disjoint. We denote this by writing $A \sim B$. The same definition can be made for lines as well.

It is easy to note that

Lemma 3.3. *The relation $\sim$ on the set of all hyperplanes of $AG_\ell(p^m)$ is an equivalence relation.*

Let us define, by a *parallel class* of a hyperplane A, the equivalence class $\bar{A}$ of A with respect to $\sim$. An analogous definition works for lines as well. The following lemma will be quite useful the proof of which we will omit:

Lemma 3.4. *There are exactly p^m hyperplanes in each parallel class and there are $(p^m)^{\ell-1} + (p^m)^{\ell-2} + \cdots + p^m + 1$ parallel classes in $AG_\ell(p^m)$.*

Now, let's look at the parallel classes of lines. We know that in each parallel class of lines, there are exactly $p^{m(\ell-1)}$ lines. Let's fix one such parallel class in $AG_\ell(p^m)$. Suppose it is

$$\bar{L} = \{L_0, L_1, \ldots, L_{p^{m(\ell-1)}-1}\} \tag{3.1}$$

where each L_j is a line in the Affine space $AG_\ell(p^m)$. Let's write the lines in this parallel class as columns:

$$\bar{L} = \left\{ \begin{pmatrix} L_0^1 \\ L_1^1 \\ L_2^1 \\ \vdots \\ L_{p^m-1}^1 \end{pmatrix}, \begin{pmatrix} L_0^2 \\ L_1^2 \\ L_2^2 \\ \vdots \\ L_{p^m-1}^2 \end{pmatrix}, \ldots, \begin{pmatrix} L_0^{p^{m(\ell-1)}} \\ L_1^{p^{m(\ell-1)}} \\ L_2^{p^{m(\ell-1)}} \\ \vdots \\ L_{p^m-1}^{p^{m(\ell-1)}} \end{pmatrix} \right\} \tag{3.2}$$

where we will label each L_0^i by 0 and each L_j^i by α^{j-1} for $j = 1, 2, \ldots, p^m - 2$.

We observe that, if a hyperplane contains two points from a line, it contains the whole line. So, each hyperplane that doesn't contain any of the lines $L_0, L_1, \ldots, L_{p^{m(\ell-1)}-1}$ contains exactly one point from each column in (3.2). Using this observation we will prove the following quick lemma:

Lemma 3.5. *Suppose that a hyperplane A doesn't contain any of the lines $L_0, L_1, \ldots, L_{p^{m(\ell-1)}-1}$. If $B \in \bar{A}$ is any hyperplane, then B doesn't contain any of the lines $L_0, \ldots, L_{p^{m(\ell-1)}-1}$ either.*

Proof. If $B \in \bar{A}$, this means that either $B = A$, in which case the assertion follows or B and A are disjoint. By the above observation, we know that A must contain exactly one point from each line L_j, $j = 0, 1, \ldots, p^{m(\ell-1)} - 1$. But if B contains one of the lines L_j, then we would have $A \cap B \neq \emptyset$, contradicting the fact that A and B are disjoint. □

Remark 3.6. The result of Lemma 3.5 implies that the hyperplanes that don't contain any of the lines $L_0, L_1, \ldots, L_{p^{m(\ell-1)}-1}$ are partitioned into parallel classes of hyperplanes.

The following lemma will give us the number of hyperplanes that don't contain any of those lines:

Lemma 3.7. *There are exactly $p^{m(\ell-1)}$ parallel classes of hyperplanes that don't contain any of the lines $L_0, L_1, \ldots, L_{p^{m(\ell-1)}-1}$, or equivalently there are exactly $p^{m\ell}$ hyperplanes that don't contain any of the lines $L_0, L_1, \ldots, L_{p^{m(\ell-1)}-1}$.*

Proof. Since, by Lemma 3.5, we know that the hyperplanes that don't contain any of the lines $L_0, L_1, \ldots, L_{p^{m(\ell-1)}-1}$ are partitioned into parallel classes, we see that the hyperplanes that contain at least one of the lines $L_0, L_1, \ldots, L_{p^{m(\ell-1)}-1}$ are also partitioned into parallel classes. So, the number of parallel classes of hyperplanes that contain at least one of the lines in $L_0, L_1, \ldots, L_{p^{m(\ell-1)}-1}$ is the same as the number of $(\ell-1)$-dimensional subspaces of an ℓ-dimensional vector space that contains a particular line, which is

$$\begin{bmatrix} \ell-1 \\ \ell-2 \end{bmatrix}_{p^m} = \frac{((p^m)^{\ell-1}-1)((p^m)^{\ell-2}-1)\cdots(p^{2m}-1)}{((p^m)^{\ell-2}-1)((p^m)^{\ell-3}-1)\cdots(p^m-1)} = \frac{(p^m)^{\ell-1}-1}{p^m-1} \tag{3.3}$$

which in turn is equal to

$$p^{m(\ell-2)} + p^{m(\ell-3)} + \cdots + p^m + 1. \tag{3.4}$$

By combining Lemmas 3.4 and 3.5, we see the number of the parallel classes of hyperplanes that don't contain any of the lines $L_0, L_1, \ldots, L_{p^{m(\ell-1)}-1}$ is

$$(p^{m(\ell-1)} + p^{m(\ell-2)} + \cdots + p^m + 1) - (p^{m(\ell-2)} + p^{m(\ell-3)} + \cdots + p^m + 1) = p^{m(\ell-1)}. \tag{3.5}$$

4. The construction of the Gray map

We are now ready to give a coordinate-wise construction of the Gray map from $GR(p^\ell, m)^n$ to $\mathbb{F}_{p^m}^{np^{(\ell-1)m}}$ that preserves the homogeneous distance. Since the map is going to be given coordinate-wise, we will actually construct $\phi : GR(p^\ell, m) \to \mathbb{F}_{p^m}^{p^{(\ell-1)m}}$ such that

$$d_{\text{hom}}(u_1, u_2) = d_{\text{H}}(\phi(u_1), \phi(u_2)) \tag{4.1}$$

for all $u_1, u_2 \in GR(p^\ell, m)$. Here, d_{H} denotes the Hamming distance.

Assume that $\Gamma_0, \Gamma_1, \ldots, \Gamma_{p^{m(\ell-1)}-1}$ are the parallel classes of the hyperplanes that don't contain any of the lines $L_0, L_1, \ldots, L_{p^{m(\ell-1)}-1}$, by the result of Lemma 3.7. So, each hyperplane in these parallel classes is formed by taking one element from each column of (3.2). Suppose, without loss of generality that we have labelled (3.2) in such a way that there exists a hyperplane that corresponds to a labelling of $(0, 0, \ldots, 0)$ and that it is in Γ_0. From now on, by the vector that corresponds to a hyperplane, we will mean the $\{0, 1, \alpha \ldots, \alpha^{p^m-2}\}$-vector of length $p^{m(\ell-1)}$, which comes from the labelling of the elements of the hyperplane in accordance with the labelling of (3.2). So now we are finally ready to describe the Gray map:

Definition 4.1. For $u \in p^{\ell-1}GR(p^\ell, m)$, ϕ maps u to the vector of the hyperplanes of Γ_0 bijectively in such a way that 0 is mapped to the hyperplane denoted by $(0, 0, \ldots, 0)$.

For $1 \le j \le p^{m(\ell-1)} - 1$, we map the elements of the coset $\overline{c_j} = c_j + p^{\ell-1}GR(p^\ell, m)$ to the vectors of the hyperplanes of Γ_j bijectively. Here, $\{c_j + p^{\ell-1}GR(p^\ell, m) | j = 1, 2, \ldots, p^{m(\ell-1)} - 1\}$ denotes the set of all non-trivial cosets of $p^{\ell-1}GR(p^\ell, m)$.

Note that this is a well-defined map from $GR(p^\ell, m)$ to $\mathbb{F}_{p^m}^{p^{(\ell-1)m}}$.

We will now prove the main result about this map:

Theorem 4.2. *The map ϕ defined above is indeed a distance-preserving map from $GR(p^\ell, m)$ with the homogeneous distance to $\mathbb{F}_{p^m}^{p^{(\ell-1)m}}$ with the Hamming distance.*

Proof. Suppose $u \in p^{\ell-1}GR(p^\ell, m) \setminus \{0\}$. Then this means that $\phi(u)$ is the vector of a hyperplane in Γ_0 that is disjoint from the hyperplane of $(0, 0, \ldots, 0)$. But this means that $\phi(u)$ doesn't have any zeros, which means that

$$w_{\text{H}}(\phi(u)) = p^{m(\ell-1)}. \tag{4.2}$$

If $v \notin p^{\ell-1}GR(p^\ell, m)$ then $v \in \overline{c_j}$ for some $j \ge 1$ and so by the definition of the map, $\phi(v)$ is the vector of a hyperplane in some Γ_j with $j \ne 0$. But since any hyperplane in Γ_j will intersect with any hyperplane in Γ_0 in exactly $p^{m(\ell-2)}$ points and since $(0, 0, \ldots, 0)$ belongs to a hyperplane in Γ_0, we see that $\phi(v)$ has to have exactly $p^{m(\ell-2)}$ 0's. Hence we see that

$$w_{\text{H}}(\phi(v)) = p^{m(\ell-1)} - p^{m(\ell-2)} = (p^m - 1)p^{m(\ell-2)}. \tag{4.3}$$

Now, suppose $u, v \in GR(p^\ell, m)$ so that $u - v \in p^{\ell-1}GR(p^\ell, m) \setminus \{0\}$. This means that u and v are two distinct elements in the same coset of $p^{\ell-1}GR(p^\ell, m)$. Then by the construction of ϕ, we see that $\phi(u)$ and $\phi(v)$ come from two distinct hyperplanes in the same parallel class Γ_j for some j. But this means that $\phi(u)$ and $\phi(v)$ are different in each coordinate since their hyperplanes are disjoint, which means that

$$d_{\text{H}}(\phi(u), \phi(v)) = p^{m(\ell-1)}. \tag{4.4}$$

Suppose now that $u - v \in GR(p^\ell, m) \setminus p^{\ell-1}GR(p^\ell, m)$ and hence u and v are in different cosets of $p^{\ell-1}GR(p^\ell, m)$. This means that $\phi(u)$ and $\phi(v)$ correspond to hyperplanes from Γ_{j_1} and Γ_{j_2}, respectively, where $j_1 \neq j_2$. But since two hyperplanes from different parallel classes must necessarily intersect, and since they intersect in a $(k-2)$-dimensional Affine subspace, we see that $\phi(u)$ and $\phi(v)$ will have exactly $p^{m(\ell-2)}$ coordinates where the entries are equal. Hence we see that

$$d_H(\phi(u), \phi(v)) = p^{m(\ell-1)} - p^{m(\ell-2)} = (p^m - 1)p^{m(\ell-2)}. \quad \square \tag{4.5}$$

5. Conclusion

The methods applied in this correspondence can easily be applied to the special case of $\mathbb{Z}_{p^k}$ by using the Affine space $AG_k(p) = AG_k(\mathbb{F}_p)$ and the same tools that we described here. As a result, we get a combinatorial construction to the Gray map that was described in [8]. It is easy to see that the same methods could be applied to finite chain rings in general.

One of the advantages of our construction is that it gives us more freedom in constructing the Gray map, as we have a lot of ways of constructing the bijections described above, considering that there are $n!$ different bijections that can be defined between two sets of size n.

One of the questions of interest in this regard is to show that the maps described by Ling and Greferath in [8,3] are just special cases of our more general construction. Even if we cannot prove this at the moment, we can see this on an example.

Carlet in [1] described the generalized Gray map G from $\mathbb{Z}_8$ to $\mathbb{Z}_2^4$ by letting

$$G(0) = (0, 0, 0, 0); \quad G(1) = (0, 1, 0, 1); \quad G(2) = (0, 0, 1, 1); \quad G(3) = (0, 1, 1, 0);$$
$$G(4) = (1, 1, 1, 1); \quad G(5) = (1, 0, 1, 0); \quad G(6) = (1, 1, 0, 0); \quad G(7) = (1, 0, 0, 1);$$

which is a map that is mentioned as a special case of the constructions described in [3,8]. This turns out to be a special case for our construction as well, because letting $p = 2$, $\ell = 3$ and $m = 1$ in our construction and taking a parallel class of lines

$$\bar{L} = \left\{ \begin{pmatrix} (000) \\ (111) \end{pmatrix}, \begin{pmatrix} (010) \\ (101) \end{pmatrix}, \begin{pmatrix} (100) \\ (011) \end{pmatrix}, \begin{pmatrix} (110) \\ (001) \end{pmatrix} \right\} \tag{5.1}$$

in $AG_3(\mathbb{F}_2)$, we label the first coordinate in each column by 0 and the second coordinate by 1. So to show that Carlet's map is a special case of our construction, all we need to do is show that the corresponding 4-element sets that we get are hyperplanes. This is easy to verify. For example, $0 \in \mathbb{Z}_8$ should be mapped to (0000), which is represented by ((000), (010), (100), (110)) which is a subspace of $\mathbb{F}_2^3$ and hence is a hyperplane. $4 \in Z_8$ should be represented by ((111), (101), (011), (001)) which is (111) + ((000), (010), (100), (110)) and hence is a hyperplane. Similarly the other correspondences can easily be seen to give us hyperplanes which means we can actually get Carlet's map from our construction.

Acknowledgements

The work presented here was part of the author's thesis at Caltech under the supervision of Prof Richard Wilson and the author wishes to thank Prof Wilson for his contributions and guidance.

References

[1] C. Carlet, $\mathbb{Z}_{2^k}$-linear Codes, IEEE Trans. Inform. Theory 44 (1998) 1543–1547.
[2] I. Constantinescu, T. Heise, A metric for codes over residue class rings of integers, Probl. Peredachi Inform. 33 (1997) 22–28.
[3] M. Greferath, S.E. Schmidt, Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code, IEEE Trans. Inform. Theory 45 (1999) 2522–2524.
[4] T.A. Gulliver, M. Harada, Codes over $\mathbb{F}_3 + u\mathbb{F}_3$ and improvements to the bounds on ternary linear codes, Des. Codes Cryptogr. 22 (2001) 89–96.
[5] 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. Inform. Theory 40 (1994) 301–319.
[6] W.C. Huffman, Decompositions and extremal Type II codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory 44 (1998) 800–809.
[7] D. Jungnickel, Finite Fields: Structure and Arithmetics, Wissenschaftsverlag, Mannheim, 1993.
[8] S. Ling, J.T. Blackford, $\mathbb{Z}_{p^{k+1}}$-linear codes, IEEE Trans. Inform. Theory 48 (2002) 2592–2605.
[9] J.H. van Lint, R.M. Wilson, A Course in Combinatorics, Cambridge University Press, 2001.
[10] B.R. MacDonald, Finite Rings with Identity, Marcel Dekker, New York, 1974.
[11] J.F. Voloch, J.L. Walker, Homogeneous weights and exponential sums, Finite Fields Appl. (2003) 310–321.
[12] B. Yildiz, Weights modulo p^e of linear codes over rings, Des. Codes Cryptogr. 43 (2007) 147–165.