International Electronic Journal of Algebra
Volume 28 (2020) 206-219
DOI: 10.24330/ieja.768265

BASES AND AUTOMORPHISM MATRIX OF THE GALOIS RING $GR(p^r, m)$ OVER $\mathbb{Z}_{p^r}$

Virgilio P. Sison

Received: 11 November 2019; Revised: 15 February 2020; Accepted: 4 March 2020
Communicated by A. Çiğdem Özcan

Abstract. Let $GR(p^r, m)$ denote the Galois ring of characteristic p^r and cardinality p^{rm} seen as a free module of rank m over the integer ring $\mathbb{Z}_{p^r}$. A general formula for the sum of the homogeneous weights of the p^r-ary images of elements of $GR(p^r, m)$ under any basis is derived in terms of the parameters of $GR(p^r, m)$. By using a Vandermonde matrix over $GR(p^r, m)$ with respect to the generalized Frobenius automorphism, a constructive proof that every basis of $GR(p^r, m)$ has a unique dual basis is given. It is shown that a basis is self-dual if and only if its automorphism matrix is orthogonal, and that a basis is normal if and only if its automorphism matrix is symmetric.

Mathematics Subject Classification (2020): 13M99, 15B33, 94B05
Keywords: Galois ring, Vandermonde matrix, dual basis, normal basis

1. Introduction

This paper is motivated by the code-theoretic problem of finding the homogeneous bounds on the p^r-ary image of a linear block code over the Galois ring $GR(p^r, m)$ with respect to any basis over $\mathbb{Z}_{p^r}$, as proposed in [9] but which constructed distance-optimal $\mathbb{Z}_{p^r}$-codes in terms only of the polynomial basis. It is interesting to consider other bases as well, such as the dual and normal bases, and observe the changes, if any, in the properties of the image codes. The main purpose of this paper is to provide the theory for the existence and uniqueness of the dual basis, and to characterize self-dual basis and normal basis of $GR(p^r, m)$, seen as a unitary module over the integer ring $\mathbb{Z}_{p^r}$, respectively in terms of the orthogonal and symmetric property of a square $m \times m$ matrix, the so-called automorphism matrix, obtained through the action of the generalized Frobenius automorphism on the given basis of $GR(p^r, m)$. Although the code-theoretic implication of a change in basis of $GR(p^r, m)$ is the subject of another paper, we present some preliminary results in this present work.

The author gratefully acknowledges financial support from the UPLB Diamond Jubilee–Development Fund Professorial Chair Award.

Firstly a general formula for the sum of the homogeneous weights of the p^r-ary images of elements of the Galois ring $GR(p^r, m)$ under any basis over $\mathbb{Z}_{p^r}$ is derived in terms of the parameters of $GR(p^r, m)$. This useful result, which extends an earlier specific formula for Galois fields, has immediate application in any linear block code over $GR(p^r, m)$. It is shown here that every basis of the Galois ring $GR(p^r, m)$ over $\mathbb{Z}_{p^r}$ has a unique dual basis following the method in [6] which constructs the dual using matrix algebra involving the generalized Frobenius automorphism. It is proved that a basis of $GR(p^r, m)$ over $\mathbb{Z}_{p^r}$ is self-dual if and only if its automorphism matrix is orthogonal. The notion of normal bases is also generalized from the classical case for Galois fields. Equivalent conditions for a basis of $GR(p^r, m)$ over $\mathbb{Z}_{p^r}$ to be normal are given.

The material is organized as follows: Section 2 gives a thorough set of preliminaries and basic definitions while Section 3 discusses the main results. Several illustrative examples are provided.

2. Preliminaries and definitions

An overview of Galois fields and Galois rings, the Frobenius automorphism and the trace function, is presented in this section. For further treatment of these topics the reader is referred to [4], [5], [9] and [10].

2.1. Galois fields and Galois rings. Let p be a prime number and $r \geq 1$ an integer. Consider the ring $\mathbb{Z}_{p^r}$ of integers modulo p^r. When $r = 1$ the ring $\mathbb{Z}_p$ with p elements is a field and is usually denoted by $\mathbb{F}_p$. Let $\mathbb{Z}_{p^r}[x]$ be the ring of polynomials in the indeterminate x with coefficients in $\mathbb{Z}_{p^r}$.

The Galois field with p^m elements, denoted $\mathbb{F}_{p^m}$, is a field extension $\mathbb{F}_p[\alpha]$ of $\mathbb{F}_p$ by a root α of an irreducible polynomial $\pi(x)$ of degree m in $\mathbb{F}_p[x]$. Thus every element z of $\mathbb{F}_{p^m}$ can be expressed uniquely as a polynomial in α of the form

$$z = a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_{m-1}\alpha^{m-1} \tag{1}$$

with degree at most $m - 1$ with the coefficients a_i coming from $\mathbb{F}_p$, and hence can also be written as an m-tuple $(a_0, a_1, \ldots, a_{m-1})$ in $\mathbb{F}_p^m$. Elements of $\mathbb{F}_{p^m}$ may also be described as residue classes of the polynomials in x with coefficients in $\mathbb{F}_p$ reduced modulo $\pi(x)$. When $m = 1$ we again have the prime field $\mathbb{F}_p$.

The canonical projection homomorphism $\mu : \mathbb{Z}_{p^r} \to \mathbb{F}_p$ is the mod-p reduction map, and can be extended naturally as a map from $\mathbb{Z}_{p^r}[x]$ onto $\mathbb{F}_p[x]$. This extended map is a ring homomorphism with kernel $(p) = \mathbb{Z}_{p^r}[x]p = \{f(x)p \mid f(x) \in \mathbb{Z}_{p^r}[x]\}$.

Let $g(x)$ be a monic polynomial of degree $m \geq 1$ in $\mathbb{Z}_{p^r}[x]$. If $\mu(g(x))$ is irreducible in $\mathbb{F}_p[x]$, then $g(x)$ is said to be *monic basic irreducible*. If $\mu(g(x))$ is

primitive in $\mathbb{F}_p[x]$, then $g(x)$ is said to be *monic basic primitive*. Clearly, monic basic primitive polynomials in $\mathbb{Z}_{p^r}[x]$ are monic basic irreducible.

In the general sense, a *Galois ring* is a finite commutative local ring with identity $1 \neq 0$ such that the set of zero divisors together with the zero element forms the unique maximal principal ideal $(p1)$ for some prime number p. The residue class ring $\mathbb{Z}_{p^r}[x]/(h(x))$, where $h(x)$ is a monic basic irreducible polynomial of degree m in $\mathbb{Z}_{p^r}[x]$, is a Galois ring with characteristic p^r and cardinality p^{rm}. The elements of $\mathbb{Z}_{p^r}[x]/(h(x))$ are residue classes of the form

$$a_0 + a_1 x + \ldots + a_{m-1}x^{m-1} + (h(x)) \tag{2}$$

where $a_i \in \mathbb{Z}_{p^r}$. The identity is $1 + (h(x))$ and the zero element is $(h(x))$. The principal ideal $(p[1 + (h(x))]) = (p + (h(x)))$ consists of all the zero divisors and the zero element, and is the only maximal ideal.

If $\deg h(x) = 1$ then $\mathbb{Z}_{p^r}[x]/(h(x))$ is the ring $\mathbb{Z}_{p^r}$. If $r = 1$, the canonical homomorphism μ becomes the identity map and

$$\mathbb{Z}_{p^r}[x]/(h(x)) = \mathbb{F}_p[x]/(h(x)) \cong \mathbb{F}_{p^m}.$$

Now let $\omega = x + (h(x))$, then $h(\omega) = 0$ and every element z of $\mathbb{Z}_{p^r}[x]/(h(x))$ can be expressed uniquely in the form

$$z = a_0 + a_1\omega + \ldots + a_{m-1}\omega^{m-1} \tag{3}$$

where $a_i \in \mathbb{Z}_{p^r}$. We can thus think of $\mathbb{Z}_{p^r}[x]/(h(x))$ as a Galois extension $\mathbb{Z}_{p^r}[\omega]$ of $\mathbb{Z}_{p^r}$ by ω. The elements take the *additive representation* (3), a generalization of (1) for $\mathbb{F}_{p^m}$. Since any two Galois rings of the same characteristic and the same cardinality are isomorphic, we simply use the notation $GR(p^r, m)$ for any Galois ring with characteristic p^r and cardinality p^{rm}.

The Galois ring $\mathcal{R} = GR(p^r, m)$ is a finite chain ring of length r, its ideals $p^i\mathcal{R}$ with $p^{(r-i)m}$ elements are linearly ordered by inclusion,

$$\{0\} = p^r\mathcal{R} \subset p^{r-1}\mathcal{R} \subset \ldots \subset p\mathcal{R} \subset \mathcal{R} \tag{4}$$

The quotient ring $\mathcal{R}/p\mathcal{R} \cong \mathbb{F}_{p^m}$ is the residue field of $\mathcal{R}$. There exists a nonzero element ξ of order $p^m - 1$, which is a root of a unique monic basic primitive polynomial $h(x)$ of degree m over $\mathbb{Z}_{p^r}$ and dividing $x^{p^m-1} - 1$ in $\mathbb{Z}_{p^r}[x]$. Consider the set

$$\mathcal{T} = \{0, 1, \xi, \xi^2, \ldots, \xi^{p^m-2}\} \tag{5}$$

of Tëichmuller representatives. In this case, every element z of $GR(p^r, m)$ has a unique *mutiplicative or p-adic representation* as follows

$$z = z_0 + pz_1 + p^2 z_2 + \ldots + p^{r-1}z_{r-1} \tag{6}$$

where $z_i \in \mathcal{T}$. We have that z is a unit if and only if $z_0 \neq 0$, and z is a zero divisor or 0 if and only if $z_0 = 0$. The units form a multiplicative group of order $(p^m - 1)p^{(r-1)m}$, which is a direct product $\langle\omega\rangle \times \mathcal{E}$, where $\langle\omega\rangle$ is a cyclic group of order $p^m - 1$ that is isomorphic to $\mathbb{Z}_{p^m-1}$ and $\mathcal{E} = \{1 + \pi \mid \pi \in (p)\}$ is a group of order $p^{(r-1)m}$. Let $\mu(\xi) = \alpha$. It can be shown that α is a primitive element in $\mathbb{F}_{p^m}$, and thus $\mu(\mathcal{T}) = \mathbb{F}_{p^m}$. The p-adic representation in (6) is a generalization of the power representation of an element of $\mathbb{F}_{p^m}$.

We realize that the Galois ring $\mathcal{R} = \mathbb{Z}_{p^r}[\omega]$ is a free module of rank m over $\mathbb{Z}_{p^r}$ with the set

$$\mathcal{P}_m(\omega) = \{1, \omega, \omega^2, \ldots, \omega^{m-1}\} \tag{7}$$

as a free basis, as seen in (3). The set $\mathcal{P}_m(\omega)$ is called the *standard* or *polynomial basis* of $\mathcal{R}$. The ring $\mathbb{Z}_{p^r}$ satisfies the invariant dimension property, hence any other basis of $\mathcal{R}$, if it exists, will have cardinality m.

Recall that a nonempty subset X of $\mathcal{R}$ is *linearly independent* provided that for distinct $x_1, x_2, \ldots, x_n \in X$ and $r_i \in \mathbb{Z}_{p^r}$, $r_1x_1 + r_2x_2 + \ldots + r_nx_n = 0$ implies that $r_i = 0$ for every i. If X is linearly independent and spans $\mathcal{R}$, that is, every element of $\mathcal{R}$ can be written as a linear combination of elements of X over $\mathbb{Z}_{p^r}$, then X is called a *basis* of $\mathcal{R}$ over the base ring, in this case, $\mathbb{Z}_{p^r}$. It should be remarked that, in general, a unitary module over a ring with identity does not always possess a basis. If it does, then the module is called a *free module* and the basis is called specifically a *free basis*. The *rank* is just the cardinality of the basis.

2.2. Generalized Frobenius automorphism and trace. The *generalized Frobenius map* f on the Galois ring $\mathcal{R} = GR(p^r, m)$ is defined by

$$z^f := z_0^p + pz_1^p + p^2z_2^p + \ldots + p^{r-1}z_{r-1}^p \tag{8}$$

where z has the p-adic representation given in (6). The map f satisfies the following properties.

(i) f is a ring automorphism of $\mathcal{R}$.

(ii) f fixes every element of $\mathbb{Z}_{p^r}$.

(iii) f is of order m and generates the cyclic Galois group of $\mathcal{R}$ over $\mathbb{Z}_{p^r}$.

When $r = 1$, the automorphism f reduces to the usual Frobenius automorphism on $\mathbb{F}_{p^m}$ defined by $z \mapsto z^p$.

The *generalized trace map* T from $\mathcal{R}$ down to $\mathbb{Z}_{p^r}$ is given by

$$T(z) := z + z^f + z^{f^2} + \ldots + z^{f^{m-1}} \tag{9}$$

and satisfies the following properties.

(i) T is surjective and $\mathcal{R}/\ker T \cong \mathbb{Z}_{p^r}$.

(ii) T takes on each value of $\mathbb{Z}_{p^r}$ equally often $p^{r(m-1)}$ times.
(iii) $T(\alpha+\beta) = T(\alpha) + T(\beta)$ for all $\alpha, \beta \in \mathcal{R}$.
(iv) $T(\lambda\alpha) = \lambda T(\alpha)$ for all $\lambda \in \mathbb{Z}_{p^r}, \alpha \in \mathcal{R}$.
(v) $T(\alpha^f) = (T(\alpha))^f = T(\alpha)$ for all $\alpha \in \mathcal{R}$.

Again when $r = 1$ the generalized trace map T reduces to the classical trace map $t : \mathbb{F}_{p^m} \to \mathbb{F}_p$ defined by

$$t(\beta) = \beta + \beta^p + \beta^{p^2} + \ldots + \beta^{p^{m-1}} . \tag{10}$$

2.3. Homogeneous weight on $GR(p^r, m)$. Let R be a finite ring with identity $1 \neq 0$, and $\mathbb{T}$ be the multiplicative group of unit complex numbers. The group $\mathbb{T}$ is a one-dimensional torus. A *character* of R (considered as an additive abelian group) is a group homomorphism $\chi : R \to \mathbb{T}$. The set of all characters $\widehat{R}$ (called the *character module of* R) is a right (resp. left) R-module whose group operation is pointwise multiplication of characters and scalar multiplication is given by $\chi^r(x) = \chi(rx)$ (resp. ${}^r\chi(x) = \chi(xr)$). A character χ of R is called a *right (resp. left) generating character* if the mapping $\phi : R \to \widehat{R}$ given by $\phi(r) = \chi^r$ (resp. $\phi(r) = {}^r\chi$) is an isomorphism of right (resp. left) R-modules. The ring R is called *Frobenius* if and only if R admits a right or a left generating character, or alternatively, if and only if $\widehat{R} \cong R$ as right or left R-modules. It is known that for finite rings, a character χ on R is a right generating character if and only if it is a left generating character. Further χ is a right generating character if and only if $\ker \chi$ contains no non-zero right ideals.

Let $\mathbb{R}$ be the set of real numbers. We define a homogeneous weight on an arbitrary finite ring R with identity in the sense of [3]. Let Rx denote the principal (left) ideal generated by $x \in R$.

Definition 2.1. A weight function $w : R \to \mathbb{R}$ on a finite ring R is called (left) homogeneous if $w(0) = 0$ and the following is true.

(i) If $Rx = Ry$, then $w(x) = w(y)$ for all $x, y \in R$.
(ii) There exists a real number $\Gamma \geq 0$ such that

$$\sum_{y \in Rx} w(y) = \Gamma \cdot |Rx|, \text{ for all } x \in R \setminus \{0\} . \tag{11}$$

Right homogeneous weights are defined accordingly. If a weight is both left homogeneous and right homogeneous, we call it simply as a homogeneous weight. The constant Γ in (11) is called the *average value* of w. A homogeneous weight is said to be *normalized* if its average value is 1. We can normalize the weight w in Definition 2.1 by replacing it with $\widetilde{w} = \Gamma^{-1} w$ [7]. The weight w is extended

naturally to R^n, the free module of rank n consisting of n-tuples of elements from R, via $w(z) = \sum_{i=0}^{n-1} w(z_i)$ for $z = (z_0, z_1, \ldots, z_{n-1}) \in R^n$. The homogeneous distance metric $\delta : R^n \times R^n \longrightarrow \mathbb{R}$ is defined by $\delta(x, y) = w(x - y)$, for $x, y \in R^n$.

It was proved in [4] that, if R is Frobenius with generating character χ, then every homogeneous weight w on R can be expressed in terms of χ as follows.

$$w(x) = \Gamma \left[1 - \frac{1}{|R^\times|} \sum_{u \in R^\times} \chi(xu) \right] \tag{12}$$

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

For the Galois ring $GR(p^r, m)$ we apply the following homogeneous weight given in [2] for finite chain rings.

$$w_{\mathtt{hom}}(x) = \begin{cases} 0 & \text{if } x = 0 \\ p^{m(r-1)} & \text{if } x \in \left(p^{r-1}\right) \setminus \{0\} \\ (p^m - 1)p^{m(r-2)} & \text{otherwise} \end{cases} \tag{13}$$

where $\left(p^{r-1}\right)$ is the principal ideal generated by the element p^{r-1} of $GR(p^r, m)$. Since the Galois ring $GR(p^r, m)$ is a commutative Frobenius ring with identity whose generating character is $\chi(z) = \xi^{b_{m-1}}$, where $\xi = \exp(2\pi i/p^r)$ for $z = \sum_{i=0}^{m-1} b_i \omega^i$, the weight (13) can be derived from (12). The group of units of $GR(p^r, m)$ has cardinality $p^{m(r-1)}(p^m - 1)$ and it easy to compute from (11) that its average value is equal to

$$\Gamma = (p^m - 1)p^{m(r-2)} \tag{14}$$

which is its minimum non-zero value. When $r = 1$, we have $\Gamma = (p^m - 1)/p^m$ and $w_{\mathtt{hom}}$ is just the usual Hamming weight $w_{\mathtt{Ham}}$ on $\mathbb{F}_{p^m}$. When $m = 1$, the average value is $\Gamma = (p - 1)p^{r-2}$ for the integer ring $\mathbb{Z}_{p^r}$.

2.4. Codes over $GR(p^r, m)$ and homogeneous bounds. A block code C of length n over an arbitrary finite ring R is a nonempty subset of R^n. The code C is called *right (resp. left) R-linear* if C is a right (resp. left) R-submodule of R^n. If C is both left R-linear and right R-linear, we simply call C a linear block code over R. A $k \times n$ matrix over R is called a *generator matrix* of a linear block code C if the rows span C and no proper subset of the rows generates C.

Let the set $\mathcal{B}_m = \{\beta_0, \beta_1, \ldots, \beta_{m-1}\}$ be a basis of the Galois ring $\mathcal{R}$ over $\mathbb{Z}_{p^r}$, and C be a linear block code of length n over $\mathcal{R}$. We consider the map $\tau : \mathcal{R} \longrightarrow \mathbb{Z}_{p^r}^m$ given in [9] and defined by

$$\tau(z) = (a_0, a_1, \ldots, a_{m-1}) \tag{15}$$

for $z = a_0\beta_0 + a_1\beta_1 + \ldots + a_{m-1}\beta_{m-1} \in \mathcal{R}$, $a_i \in \mathbb{Z}_{p^r}$. This map is a bijection and can be extended coordinate-wise to $\mathcal{R}^n$. Thus, if $c \in C$ and $c = (c_0, c_1, \ldots, c_{n-1})$, $c_i = \sum_{j=0}^{m-1} a_{ij}\beta_j$, $a_{ij} \in \mathbb{Z}_{p^r}$, then

$$\tau(c) = (a_{00}, \ldots, a_{0,m-1}, \ldots, a_{n-1,0}, \ldots a_{n-1,m-1}) \tag{16}$$

in $\mathbb{Z}_{p^r}^{mn}$. The image $\tau(C)$ of C under τ with respect to $\mathcal{B}_m$ is called the *p^r-ary image* of C, and is obtained by simply substituting each element of $\mathcal{R}$ by the m-tuple of its coordinates over C. It is easy to prove that $\tau(C)$ is a linear block code of length mn over $\mathbb{Z}_{p^r}$. For the degenerate case $m = 1$, the block code C is a code over $\mathbb{Z}_{p^r}$ and the map τ is the identity map on C. We equip $\tau(C)$ with a homogeneous distance metric with respect to the weight $w_{\mathtt{hom}}$ as given in (13).

The following two theorems from [9] show how the minimum Hamming weight of C provides a bound for the minimum homogeneous distance of the p^r-ary image of C under any chosen basis of the alphabet ring $GR(p^r, m)$ over $\mathbb{Z}_{p^r}$.

Theorem 2.2 (Solé and Sison, 2007)**.** *Let C be a linear block code of length n over $\mathcal{R} = GR(p^r, m)$ with minimum Hamming distance d, and $\tau(C)$ be the p^r-ary image of C with respect to any basis of $\mathcal{R}$ over $\mathbb{Z}_{p^r}$ with minimum homogeneous distance δ. Then*

$$\Gamma d \leq \delta \leq p^{r-1} m d\,. \tag{17}$$

The image code $\tau(C)$ is *Type α* if $\delta = p^{r-1} d_{\tau(C)}$, where $d_\tau(C)$ is the Hamming distance of $\tau(C)$. The upper bound in (17) is further sharpened below.

Theorem 2.3 (Solé and Sison, 2007)**.** *Let B be a linear block code of length n over $\mathcal{R} = GR(p^r, m)$ with minimum Hamming distance d, C_x the subcode of C generated by a codeword x with $w_H(x) = d$, and δ the minimum homogeneous distance of the p^r-ary image of C with respect to any basis of $\mathcal{R}$ over $\mathbb{Z}_{p^r}$. Then*

$$\delta \leq \left\lfloor \frac{|C_x|}{|C_x| - 1}\, \Gamma m d \right\rfloor\,. \tag{18}$$

Moreover, if C_x is free, then

$$\delta \leq \left\lfloor \frac{(p-1)p^{rm+r-2} m d}{p^{rm} - 1} \right\rfloor\,. \tag{19}$$

The paper [9] has in fact exhibited a *Type α* linear block code over $\mathbb{Z}_4$ that also meets the upper bound in (19). This quaternary code given in Example 4.3 of [9] is obtained via τ with respect to the polynomial basis of $GR(4, 2)$ over $\mathbb{Z}_4$.

The following lemma from [1] is quite useful in the succeeding discussion.

Lemma 2.4 (Constantinescu, Heise and Honold, 1996)**.** *For any linear block code $C \subseteq \mathbb{Z}_{p^r}^n$ we have*

$$\frac{w_{\mathtt{hom}}(C)}{|C|} = \Gamma \cdot |\{i \mid \pi_i(C) \neq 0\}|$$

where $w_{\mathtt{hom}}(C)$ is the sum of the homogeneous weights of all codewords of C, and π_i is the projection from $\mathbb{Z}_{p^r}^n$ onto the i-th coordinate.

3. Results and discussion

3.1. Sum of weights. Initially we derive a simple formula for the sum of the homogeneous weights of the p^r-ary images of elements of the Galois ring $GR(p^r, m)$ under any basis over $\mathbb{Z}_{p^r}$, in terms only of the parameters of $GR(p^r, m)$. We denote by $w_{\mathtt{hom}}(S)$ the sum of the homogeneous weights of the elements of a non-empty set S, that is,

$$w_{\mathtt{hom}}(S) = \sum_{x \in S} w_{\mathtt{hom}}(x) \,. \tag{20}$$

Proposition 3.1. *For any basis $\mathcal{B}_m = \{\beta_0, \beta_1, \ldots, \beta_{m-1}\}$ of $GR(p^r, m)$ over $\mathbb{Z}_{p^r}$ we have*

$$\sum_{x \in GR(p^r, m)} w_{\mathtt{hom}}(\tau(x)) = m(p-1)p^{rm+r-2} \,. \tag{21}$$

Proof. Let $S = \{x \mid x \in GR(p^r, m)\}$. Then $\tau(S)$ is a linear block code over $\mathbb{Z}_{p^r}$ of length m and cardinality p^{rm}. Applying Lemma 2.4 to $\tau(S)$ gives us

$$\frac{w_{\mathtt{hom}}(\tau(S))}{|\tau(S)|} = \Gamma \cdot w_s(\tau(S)) \,.$$

Therefore we have $w_{\mathtt{hom}}(\tau(S)) = |\tau(S)| \cdot \Gamma \cdot w_s(S)$. The value of Γ is given in (14), and the support size $w_s(\tau(S))$ of $\tau(S)$ is m. Using the notation in (20), the result follows. □

Proposition 3.1 gives the simple corollary below which is used to prove the bound of Rabizzoni in [8, Theorem 1]. The bound of Rabizzoni is generalized to Galois ring codes in Theorem 2.3.

Corollary 3.2. *For any basis $\mathcal{B}_m = \{\beta_0, \beta_1, \ldots, \beta_{m-1}\}$ of $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$ we have*

$$\sum_{x \in \mathbb{F}_{p^m}} w_{\mathtt{Ham}}(\tau(x)) = m(p-1)p^{m-1} \,.$$

Proof. The Galois ring $GR(p, m)$ is the Galois field $\mathbb{F}_{p^m}$, and the homogeneous weight $w_{\mathtt{hom}}$ given in (13) is the Hamming weight $w_{\mathtt{Ham}}$ on $\mathbb{F}_p$ with $\Gamma = (p-1)/p$. □

3.2. Dual and normal bases. Denote by $\mathtt{Mat}_m(\mathcal{R})$ the ring of $m \times m$ matrices over the Galois ring $\mathcal{R} = GR(p^r, m)$. It is known that a matrix A in $\mathtt{Mat}_m(\mathcal{R})$ is nonsingular (or invertible) if and only if $\det A$ is a unit in $\mathcal{R}$. We also use the usual notation $|A|$ for the determinant of A. The matrix A is *symmetric* if and only if $A = A^t$, and is *orthogonal* if and only if $AA^t = A^tA = I$, where A^t is the transpose of A and I is the identity matrix. We propose the following definition.

Definition 3.3. Two bases $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ and $\{\beta_1, \beta_2, \ldots, \beta_m\}$ of $GR(p^r, m)$ over $\mathbb{Z}_{p^r}$ are said to be *dual* if $T(\beta_i\alpha_j) = \delta_{ij}$, where δ_{ij} is the Kronecker delta.

Lemma 3.4. *Given the Galois ring $\mathcal{R} = GR(p^r, m)$ with polynomial basis $\mathcal{P}_m(\omega)$. The matrix $\Omega \in \mathtt{Mat}_m(\mathcal{R})$ given by*

$$\Omega = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ \omega & \omega^f & \omega^{f^2} & \ldots & \omega^{f^{m-1}} \\ \omega^2 & (\omega^2)^f & (\omega^2)^{f^2} & \ldots & (\omega^2)^{f^{m-1}} \\ \vdots & & & & \vdots \\ \omega^{m-1} & (\omega^{m-1})^f & (\omega^{m-1})^{f^2} & \ldots & (\omega^{m-1})^{f^{m-1}} \end{pmatrix}$$

is nonsingular.

Proof. By the definition of the generalized Frobenius automorphism (8), it easy to show that $(\omega^j)^{f^i} = (\omega^{p^i})^j$ for $i, j = 0, 1, \ldots, m-1$. Hence,

$$\Omega = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ \omega & \omega^p & \omega^{p^2} & \ldots & \omega^{p^{m-1}} \\ \omega^2 & (\omega^p)^2 & (\omega^{p^2})^2 & \ldots & (\omega^{p^{m-1}})^2 \\ \vdots & & & & \vdots \\ \omega^{m-1} & (\omega^p)^{m-1} & (\omega^{p^2})^{m-1} & \ldots & (\omega^{p^{m-1}})^{m-1} \end{pmatrix}$$

which is a Vandermonde matrix whose determinant is

$$\det \Omega = \prod_{j=1}^{m-1} \prod_{i=j+1}^{m} (\omega^{p^{i-1}} - \omega^{p^{j-1}}). \tag{22}$$

Each factor in this product is a unit of $\mathcal{R}$ so that $\det \Omega$ is a unit in $\mathcal{R}$. □

Lemma 3.5. *Let $\{\beta_j\} = \{\beta_1, \beta_1, \ldots, \beta_m\}$ be a basis of $GR(p^r, m)$ over $\mathbb{Z}_{p^r}$. The matrix*

$$B = \begin{pmatrix} \beta_1 & \beta_1^f & \beta_1^{f^2} & \ldots & \beta_1^{f^{m-1}} \\ \beta_2 & \beta_2^f & \beta_2^{f^2} & \ldots & \beta_2^{f^{m-1}} \\ \vdots & & & & \vdots \\ \beta_m & \beta_m^f & \beta_m^{f^2} & \ldots & \beta_m^{f^{m-1}} \end{pmatrix} \tag{23}$$

is invertible.

Proof. Express the polynomial basis $\mathcal{P}_m(\omega)$ in (7) in terms of the basis $\{\beta_j\}$ as follows.

$$\begin{pmatrix} 1 \\ \omega \\ \omega^2 \\ \vdots \\ \omega^{m-1} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ a_{31} & a_{32} & \dots & a_{3m} \\ \vdots & & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mm} \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \\ \beta_3 \\ \vdots \\ \beta_m \end{pmatrix}$$

where $A = (a_{ij})$ is a nonsingular matrix over $\mathbb{Z}_{p^r}$. We compute the matrix product AB. The fact that the Frobenius automorphism f fixes each a_{ij} implies that AB is the Vandermonde matrix Ω. Hence by Lemma 3.4, $\det AB$ is a unit in $\mathcal{R}$. Consequently, $\det B$ is a unit in $\mathcal{R}$. □

We shall call the matrix B the *automorphism matrix* of $GR(p^r, m)$ relative to the basis $\{\beta_j\}$.

Corollary 3.6. $(\det B)^2$ *is a unit in* $\mathbb{Z}_{p^r}$.

Proof. It can be shown that

$$BB^t = \begin{pmatrix} T(\beta_1^2) & T(\beta_1\beta_2) & \dots & T(\beta_1\beta_m) \\ T(\beta_2\beta_1) & T(\beta_2^2) & \dots & T(\beta_2\beta_m) \\ \vdots & & & \vdots \\ T(\beta_m\beta_1) & T(\beta_m\beta_2) & \dots & T(\beta_m^2) \end{pmatrix} \tag{24}$$

which is a matrix over $\mathbb{Z}_{p^r}$. It follows that $(\det B)^2$ is an element of $\mathbb{Z}_{p^r}$. By Lemma 3.5, we get the result. □

Of course, $\det B$ is not necessarily a unit in the base ring $\mathbb{Z}_{p^r}$, although it is a unit in $GR(p^r, m)$ according to Lemma 3.5. Please see Example 3.8.

Theorem 3.7. *Every basis of* $GR(p^r, m)$ *over* $\mathbb{Z}_{p^r}$ *has a unique dual.*

Proof. We show the proof for $m = 3$ without loss of essential generality. Let $\{\beta_1, \beta_2, \beta_3\}$ be a basis, and consider the automorphism matrix

$$B = \begin{pmatrix} \beta_1 & \beta_1^f & \beta_1^{f^2} \\ \beta_2 & \beta_2^f & \beta_2^{f^2} \\ \beta_3 & \beta_3^f & \beta_3^{f^2} \end{pmatrix}$$

which is nonsingular by Lemma 3.5. Let adj B = (b_{ij}) where $b_{ij} = (-1)^{i+j}|B_{ji}|$. Then

$$\text{adj B} = \begin{pmatrix} \lambda_1 & \lambda_2 & \lambda_3 \\ \lambda_1^f & \lambda_2^f & \lambda_3^f \\ \lambda_1^{f^2} & \lambda_2^{f^2} & \lambda_3^{f^2} \end{pmatrix}$$

where $\lambda_1 = \beta_2^f \beta_3^{f^2} - \beta_2^{f^2} \beta_3^f$, $\lambda_2 = \beta_1^{f^2} \beta_3^f - \beta_1^f \beta_3^{f^2}$, and $\lambda_3 = \beta_1^f \beta_2^{f^2} - \beta_1^{f^2} \beta_2^f$ so that $B^{-1} = |B|^{-1}$ adj B. Note that

$$BB^{-1} = |B|^{-1} \begin{pmatrix} T(\beta_1\lambda_1) & T(\beta_1\lambda_2) & T(\beta_1\lambda_3) \\ T(\beta_2\lambda_1) & T(\beta_2\lambda_2) & T(\beta_2\lambda_3) \\ T(\beta_3\lambda_1) & T(\beta_3\lambda_2) & T(\beta_3\lambda_3) \end{pmatrix}. \tag{25}$$

We claim that the set $\{|B|^{-1}\lambda_1, |B|^{-1}\lambda_2, |B|^{-1}\lambda_3\}$ is the unique dual of $\{\beta_j\}$. To prove this, it is sufficient to show that $\{\lambda_1, \lambda_2, \lambda_3\}$ is linearly independent. Let $\sum_{i=1}^3 r_i\lambda_i = 0$, where $r_i \in \mathbb{Z}_{p^r}$. For β_k, $k = 1, 2, 3$, we get $\sum_{i=1}^3 r_i\beta_k\lambda_i = 0$. Then applying the generalized trace gives $\sum_{i=1}^3 r_i T(\beta_k\lambda_i) = 0$. It follows from (25) that $0 = r_k \cdot T(\beta_k\lambda_k) = r_k \cdot 1 = r_k$. □

Example 3.8. The polynomial basis of $GR(4, 2)$ over $\mathbb{Z}_4$ is the set $\{1, \omega\}$ where $1 + \omega + \omega^2 = 0$. The automorphism matrix is

$$B = \begin{pmatrix} 1 & 1 \\ \omega & 3 + 3\omega \end{pmatrix}$$

with determinant $3 + 2\omega$ which is a unit in $GR(4, 2)$. Observe that $(3 + 2\omega)^2 = 1$ is a unit in $\mathbb{Z}_4$. The inverse

$$B^{-1} = \begin{pmatrix} 3 + \omega & 1 + 2\omega \\ 2 + 3\omega & 3 + 2\omega \end{pmatrix}$$

gives $\{3 + \omega, 1 + 2\omega\}$ as the dual of the polynomial basis.

Example 3.9. The polynomial basis of $GR(4, 3)$ over $\mathbb{Z}_4$ is the set $\{1, \omega, \omega^2\}$ where ω is the root of the basic primitive polynomial $x^3 + 2x^2 + x - 1$ over $\mathbb{Z}_4$. The automorphism matrix is given by

$$B = \begin{pmatrix} 1 & 1 & 1 \\ \omega & \omega^2 & \omega^4 \\ \omega^2 & \omega^4 & \omega \end{pmatrix}$$

with determinant 3. The inverse is given by

$$B^{-1} = \begin{pmatrix} \omega + 3\omega^3 & w + 3\omega^4 & w^2 + 3\omega^4 \\ \omega^2 + 3\omega^6 & 3\omega + \omega^2 & 3\omega + \omega^4 \\ \omega^4 + 3\omega^5 & 3\omega^2 + \omega^4 & \omega + 3\omega^2 \end{pmatrix}$$

so that $\{3 + 2\omega + 2\omega^2, 2 + 2\omega + \omega^2, 2 + \omega + 2\omega^2\}$ is the dual basis.

Example 3.10. The dual of the polynomial basis of $\mathbb{Z}_8[\omega]$, where ω is the root of the basic primitive polynomial $7 + 5x + 6x^2 + x^3$ over $\mathbb{Z}_8$, is the set $\{3 + 6\omega + 6\omega^2$, $6 + 2\omega + 5\omega^2$, $6 + 5\omega + 2\omega^2\}$.

3.3. Automorphism matrix. We apply Definition 3.3 for the notion of a self-dual basis.

Definition 3.11. A basis $\{\beta_1, \beta_2, \ldots, \beta_m\}$ of $GR(p^r, m)$ over $\mathbb{Z}_{p^r}$ is *self-dual* if $T(\beta_i\beta_j) = \delta_{ij}$.

Definition 3.12. A normal basis of $GR(p^r, m)$ over $\mathbb{Z}_{p^r}$ is a basis of the form

$$\{\alpha, \alpha^f, \alpha^{f^2}, \ldots, \alpha^{f^{m-1}}\}$$

where $\alpha \in GR(p^r, m)$ and f is the generalized Frobenius automorphism given in (8). In this case we say that α generates the basis.

We have the following immediate results.

Theorem 3.13. *Let $\{\beta_j\}$ be a basis of $GR(p^r, m)$ over $\mathbb{Z}_{p^r}$ with automorphism matrix B. Then B is orthogonal if and only if $\{\beta_j\}$ is self-dual.*

Proof. From (24) we get $BB^t = I \Leftrightarrow T(\beta_i\beta_j) = \delta_{ij}$. □

Theorem 3.14. *Let $\{\beta_j\}$ be a basis of $GR(p^r, m)$ over $\mathbb{Z}_{p^r}$ with automorphism matrix B. Then the following statements are equivalent.*

(i) *The basis $\{\beta_j\}$ is a normal basis.*
(ii) *The automorphism matrix B is a symmetric matrix.*
(iii) *The Frobenius automorphism f is the m-cycle given by*

$$\beta_1 \mapsto \beta_2, \beta_2 \mapsto \beta_3, \ldots, \beta_m \mapsto \beta_1.$$

Proof. This equivalence is evident from the construction of the automorphism matrix in (23). The basis $\mathcal{B}_m = \{\beta_j\}$ is normal $\Leftrightarrow$ β_1 generates $\mathcal{B}_m$, that is, $\beta_2 = \beta_1^f, \beta_3 = \beta_2^f = \beta_1^{f^2}, \beta_3 = \beta_2^f = \beta_1^{f^3}, \ldots, \beta_{m-1} = \beta_{m-2}^f = \beta_1^{f^{m-1}}, \beta_m = \beta_{m-1}^f = \beta_1^{f^{m-1}}, \beta_m^f = \beta_1^{f^m} = \beta_1 \Leftrightarrow B$ is symmetric $\Leftrightarrow f$ is the m-cycle $\beta_1 \mapsto \beta_2, \beta_2 \mapsto \beta_3, \ldots, \beta_m \mapsto \beta_1$. □

Example 3.15. The set $\mathcal{B}_2 = \{\omega, \omega^2 = 3 + 3\omega\}$ is a normal basis $\mathbb{Z}_4[x]/(x^2 + x + 1)$ over $\mathbb{Z}_4$. The automorphism matrix relative to this basis is given by

$$\begin{pmatrix} \omega & 3 + 3\omega \\ 3 + 3\omega & \omega \end{pmatrix}$$

which is not orthogonal, hence $\mathcal{B}_2$ is not self-dual. However B is symmetric.

Example 3.16. The set $\mathcal{B}_3 = \{1+\omega, 1+\omega^2, 3+3\omega+3\omega^2\}$ of $GR(4,3) = \mathbb{Z}_4[x]/(x^3+2x^2+x+3)$ is a self-dual normal basis since the automorphism matrix is both orthogonal and symmetric.

3.4. Image codes under various bases. Using the above results, we are able to write MAGMA algorithms to generate the dual and normal bases of $GR(p^r, m)$ at bounded values of the parameters p, r and m, to derive the automorphism matrix and test whether it is orthogonal or symmetric.

If G is the generator matrix of a rate-k/n linear block code C over $GR(p^r, m)$, it can be shown that the generator matrix of the p^r-ary image of C with respect to the basis $\{\beta_i\}_{i=1}^m$ is an $mk \times mn$ matrix over $\mathbb{Z}_{p^r}$ that is formed row-wise by the τ-images of $\beta_i G$. It is not always the case that the p^r-ary images under different bases are the same, and certain conditions in which the p^r-ary images are distance-invariant are investigated. Consequently, new $\mathbb{Z}_{p^r}$-codes endowed with a homogeneous metric that are optimal with respect to the bounds (17) or (19) can be constructed.

For instance, let us consider the code C in Example 4.3 of [9]. Let P be the polynomial basis and D the dual basis of $GR(4,2)$. Although $\tau_D(C)$ is derived from the same code C, the quaternary image $\tau_D(C)$ is not equal to $\tau_P(C)$ and is an entirely new rate-4/12 linear block code over $\mathbb{Z}_4$ with 256 codewords. However, the distances are preserved. The Lee distance is $d_L = 8$ and the Hamming distance is $d_{\tau_D(C)} = 4$, making this new quaternary code a Type α and a Rabizzoni-optimal code as well. Therefore, a suitable change in basis of $GR(p^r, m)$ over $\mathbb{Z}_{p^r}$ can give rise to another distance-optimal code over $\mathbb{Z}_{p^r}$ derived from the same linear block code over $GR(p^r, m)$. The relation between the image codes can be studied further.

Acknowledgement. The author would like to sincerely thank the referees for their helpful comments and suggestions.

References

[1] I. Constantinescu, W. Heise and T. Honold, *Monomial extensions of isometries between codes over* $\mathbb{Z}_M$, Proceedings of the 5^{th} International Workshop on Algebraic and Combinatorial Coding Theory (ACCT '96), Unicorn Shumen, (1996), 98-104.

[2] M. Greferath and S. E. Schmidt, *Gray isometries for finite chain rings and a nonlinear ternary* $(36, 3^{12}, 15)$ *code*, IEEE Trans. Inform. Theory, 45(7) (1999), 2522-2524.

[3] M. Greferath and S. E. Schmidt, *Finite-ring combinatorics and MacWilliams' Equivalence Theorem*, J. Combin. Theory Ser. A, 92 (2000), 17-28.

[4] T. Honold, *Characterization of finite Frobenius rings*, Arch. Math. (Basel), 76 (2001), 406-415.

[5] B. R. MacDonald, Finite Rings with Identity, Pure and Applied Mathematics, 28, Marcel Dekker, Inc., New York, 1974.

[6] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, I, North-Holland Mathematical Library, 16, North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.

[7] A. A. Nechaev and T. Honold, *Fully weighted modules and representations of codes*, Problems Inform. Transmission, 35(3) (1999), 205-223.

[8] P. Rabizzoni, *Relation between the minimum weight of a linear code over $GF(q^m)$ and its q-ary image over $GF(q)$*, Coding theory and applications (Toulon, 1988), Lecture Notes in Comput. Sci., Springer, New York, 388 (1989), 209-212.

[9] P. Solé and V. Sison, *Bounds on the minimum homogeneous distance of the p^r-ary image of linear block codes over the Galois ring $GR(p^r, m)$*, IEEE Trans. Inform. Theory, 53(6) (2007), 2270-2273.

[10] Z.-X. Wan, Lectures on Finite Fields and Galois Rings, World Scientific Publishing Co., Inc., River Edge, NJ, 2003.

Virgilio P. Sison
Institute of Mathematical Sciences and Physics
University of the Philippines Los Baños
College, Laguna 4031, Philippines
e-mail: vpsison@up.edu.ph