Galois ring codes and their images under various bases

Virgilio Sison and Gio Carlo Delos Santos
Institute of Mathematical Sciences and Physics, University of the Philippines Los Baños,
College, Laguna 4031, Philippines
E-mail: vpsison@up.edu.ph, gcdelossantos29@gmail.com

Abstract. In this paper we consider linear block codes $B$ of length $n$ over the Galois ring $GR(p^r, m)$ and obtain their images with respect to various bases of $GR(p^r, m)$ seen as a free module of rank $m$ over the residue class ring $\mathbb{Z}_{p^r}$. Interesting new examples of dual, normal and self-dual bases of $GR(p^r, m)$ and their relationships are given. The image of $B$ is a linear block code over $\mathbb{Z}_{p^r}$ of length $mn$ and its generator matrix is formed row-wise by the images of $\beta_i G$, where $\{\beta_i\}_{i=1}^m$ is a chosen basis of $GR(p^r, m)$ and $G$ is a generator matrix of $B$. Certain conditions in which the $p^r$-ary image is distance-invariant after a change in basis are investigated. Consequently a new quaternary code endowed with a homogeneous metric that is optimal with respect to certain known bounds is constructed.

1. Introduction
The motivation for this paper came from finding the $p^r$-ary image of a linear block code $B$ of length $n$ over the Galois ring $R = GR(p^r, m)$ with respect to any $m$-basis of $R$, and placing a bound on its minimum homogeneous distance in terms of the Hamming distance and other code parameters of $B$. The $p^r$-ary image is a linear block code of length $mn$ over the residue class ring $\mathbb{Z}_{p^r}$, and its distance is with respect to the homogeneous metric defined on $GR(p^r, m)$ seen as a finite Frobenius chain ring. The main reference for this result is a previous paper [1] which considers for the most part the so-called polynomial basis of $GR(p^r, m)$. It is worthy to investigate the dual and normal bases to see how a change in basis affects the parameters of the $p^r$-ary image. For a thorough discussion of the bases of $GR(p^r, m)$ over $\mathbb{Z}_{p^r}$ the reader is referred to [2]. This paper constructed the dual basis using matrix algebra involving the generalized Frobenius automorphism. It showed that a basis of $GR(p^r, m)$ is self-dual if and only its automorphism matrix is orthogonal, and is normal if and only its automorphism matrix is symmetric.

The material is organized as follows: Section 2 gives the preliminaries and basic definitions while Section 3 gives the main results. Several new illustrative examples are also provided.

2. Preliminaries and definitions
A quick run-through of the theoretical requisites for this paper is presented in this section. This includes the structure of Galois rings as finite chain rings and Frobenius rings and the homogeneous weight that can be defined on them, the construction of Galois ring codes and their images with respect to a modular basis, and the notions of duality and normality of bases.
of Galois rings which are used in the derivation of optimal image codes. For a more thorough discussion of these topics the reader is referred to [1], [2], [3], [4], and [5].

2.1. Galois rings and homogeneous weight
A Galois ring is, in the most general sense, a finite commutative local ring with identity 1 such that its zero divisors together with the zero element form the unique maximal principal ideal (p1) for some prime p. Consider the ring \( \mathbb{Z}_{p^r}[x] \) of polynomials over the residue class ring \( \mathbb{Z}_{p^r} \) of integers modulo \( p^r \) where \( r \) is a positive integer. Let \( h(x) \) be a monic polynomial of degree \( m \) in \( \mathbb{Z}_{p^r}[x] \) such that its image under the mod-p reduction map, extended coefficient-wise, is irreducible in \( \mathbb{F}_p[x] \). Then the quotient ring \( \mathbb{Z}_{p^r}[x]/(h(x)) \) is a Galois ring with characteristic \( p^r \) and cardinality \( p^rm \). Now let \( \omega \) be a root of \( h(x) \). It follows that \( \mathbb{Z}_{p^r}[x]/(h(x)) \) is ring isomorphic to the Galois extension \( \mathbb{Z}_{p^r}[^m] \) of \( \mathbb{Z}_{p^r} \) in which the elements take the unique additive representation

\[
z = a_0 + a_1\omega + \ldots + a_{m-1}\omega^{m-1}
\]

where \( a_i \in \mathbb{Z}_{p^r} \). Any Galois ring with characteristic \( p^r \) and cardinality \( p^{rm} \) is denoted by \( GR(p^r, m) \). This ring is a finite chain ring of length \( r \) whose \( r+1 \) ideals \((p^i), i = 0, 1, \ldots, r,\) with \( p^{(r-i)m} \) elements, are linearly ordered by inclusion,

\[
\{0\} = (p^r) \subset (p^{r-1}) \subset \ldots \subset (p) \subset \mathcal{R}
\]

Observe that \( GR(p, m) \) is the Galois field \( \mathbb{F}_{p^m} \) and \( GR(p^r, 1) = \mathbb{Z}_{p^r} \). Furthermore, \( GR(p^r, m) \) can be seen as a free module of rank \( m \) over \( \mathbb{Z}_{p^r} \) with the set

\[
\mathcal{P}_m(\omega) = \{1, \omega, \omega^2, \ldots, \omega^{m-1}\}
\]

as a free basis taken from the additive representation of \( GR(p^r, m) \) in (1). The set \( \mathcal{P}_m(\omega) \) is called the standard or polynomial basis of \( GR(p^r, m) \). It is known that any other basis of \( GR(p^r, m) \) has the same cardinality \( m \).

For \( GR(p^r, m) \) we apply the following homogeneous weight as given in [6] for finite chain rings.

\[
w_{hom}(x) = \begin{cases} 
0 & \text{if } x = 0 \\
\frac{p^m(r-1)}{p^m-1} & \text{if } x \in (p^{r-1}) \setminus \{0\} \\
\frac{(p^m-1)p^{m(r-2)}}{p^m-1} & \text{otherwise}
\end{cases}
\]

where \((p^{r-1})\) is the minimal ideal. The ring \( GR(p^r, m) \) is Frobenius since it admits a generating character given by \( \chi(z) = \xi^{bm-1} \), where \( \xi = \exp(2\pi i/p^r) \) for \( z = \sum_{i=0}^{m-1} b_i \omega^i \). It is thus easy to compute from [3] and [7] that the average value of \( w_{hom} \) is equal to

\[
\Gamma = (p^m-1)p^{m(r-2)}
\]

which is its minimum non-zero value.

2.2. Codes over \( GR(p^r, m) \) and their \( p^r \)-ary images
A rate-\( k/n \) linear block code \( B \) of length \( n \) over \( \mathcal{R} = GR(p^r, m) \) is an \( \mathcal{R} \)-submodule of \( \mathcal{R}^n \) generated by a \( k \times n \) matrix \( G \) over \( \mathcal{R} \) whose rows span \( B \) such that no proper subset of the rows of \( G \) generates \( B \). The rows of \( G \) need not be linearly independent. We say that \( B \) is free if the rows of \( G \) form a basis.
Let the set $B_m = \{\beta_0, \beta_1, \ldots, \beta_{m-1}\}$ be a basis of $R$ over $Z_{p^r}$. We use the bijective map $\tau: R \rightarrow Z_{p^r}^m$ given in [1] as follows

$$\tau(z) = (a_0, a_1, \ldots, a_{m-1}) \quad (6)$$

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

$$\tau(c) = (a_{00}, \ldots, a_{0,m-1}, \ldots, a_{n-1,0}, \ldots a_{n-1,m-1}) \quad (7)$$

in $Z_{p^m}^n$. The image $\tau(B)$ of $B$ under $\tau$ with respect to $B_m$ is called the $p^r$-ary image of $B$, and is obtained by simply substituting each element of $R$ by the $m$-tuple of its coordinates over $B$. It is easy to prove that $\tau(B)$ is a linear block code of length $mn$ over $Z_{p^r}$. Since $\tau$ is bijective, $|B| = |\tau(B)|$. For the degenerate case $m = 1$, the block code $B$ is a code over $Z_{p^r}$ and the map $\tau$ is the identity map on $B$. We equip $\tau(B)$ with a homogeneous distance metric with respect to the weight $w_{hom}$ given in (4).

The following proposition in [1] shows how the minimum Hamming weight of $B$ provides a bound for the minimum homogeneous distance of $\tau(B)$.

**Proposition 2.1.** Let $B$ be a linear block code of length $n$ over $R = GR(p^r, m)$ with minimum Hamming distance $d$, and $\tau(B)$ be the $p^r$-ary image of $B$ with respect to a basis of $R$ over $Z_{p^r}$ with minimum homogeneous distance $\delta$. Then

$$\Gamma d \leq \delta \leq p^{r-1}md. \quad (8)$$

The image code $\tau(B)$ is Type $\alpha$ if $\delta = p^{r-1}d_{r}(B)$, where $d_{r}(B)$ is the Hamming distance of $\tau(B)$. The upper bound in (8) is sharpened further in the theorem below.

**Theorem 2.2.** Let $B$ be a linear block code of length $n$ over $R = GR(p^r, m)$ with minimum Hamming distance $d$, $B_x$ the subcode of $B$ generated by a codeword $x$ with $w_H(x) = d$, and $\delta$ the minimum homogeneous distance of the $p^r$-ary image of $B$ with respect to a basis of $R$ over $Z_{p^r}$. If $B_x$ is free, then

$$\delta \leq \left\lfloor \frac{(p-1)p^{rn+r-2md}}{p^{rm}-1} \right\rfloor. \quad (9)$$

The bound of Rabizzoni in [8, Theorem 1] becomes a specific case for Galois fields of Theorem 2.2. It was determined in [1] that the quaternary image of the 3-quasi cyclic rate-2/6 linear block code over $GR(4,2)$ with generator matrix

$$
\begin{pmatrix}
3 + 2\omega & 2 + 3\omega & \omega & \omega & 3 + 2\omega & 2 + 3\omega \\
\omega & 3 + 2\omega & 2 + 3\omega & 3 + 2\omega & 2 + 3\omega & \omega
\end{pmatrix}
$$

(10)

is a Type $\alpha$ code. Furthermore, a minimum-weight codeword $x = (1, 1 + 2\omega, 0, 3 + 2\omega, 3, 0)$ which generates a free code $B_x$ with 16 elements makes the quaternary image to also reach the generalized Rabizzoni upper bound in (9). It should be emphasized that the basis used to get the quaternary image of this code via $\tau$ is the polynomial basis of $GR(4,2)$ given by $\{1, \omega\}$, where $1 + \omega + \omega^2 = 0$.

2.3. Dual and normal bases of $GR(p^r, m)$

Referring to [2], we now consider bases of $R = GR(p^r, m)$ other than the polynomial basis. Two bases $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ and $\{\beta_1, \beta_2, \ldots, \beta_m\}$ are said to be dual if $T(\beta_i\alpha_j) = \delta_{ij}$, where $\delta_{ij}$ is the Kronecker delta and $T$ is the generalized trace map from $R$ down to $Z_{p^r}$. Specifically, the basis $\{\beta_1, \beta_2, \ldots, \beta_m\}$ is self-dual if $T(\beta_i\beta_j) = \delta_{ij}$. It was proved that every basis has a unique dual
basis using the automorphism matrix $\Omega \in \text{GL}(m, \mathbb{R})$ relative to a basis $\{\beta_j\} = \{\beta_1, \beta_2, \ldots, \beta_m\}$ in terms of the generalized automorphism $f$ on $\mathbb{R}$.

$$
\Omega = \begin{pmatrix}
\beta_1 & \beta_1^f & \beta_1^{f^2} & \cdots & \beta_1^{f^{m-1}} \\
\beta_2 & \beta_2^f & \beta_2^{f^2} & \cdots & \beta_2^{f^{m-1}} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\beta_m & \beta_m^f & \beta_m^{f^2} & \cdots & \beta_m^{f^{m-1}}
\end{pmatrix}
$$

(11)

A normal basis of $GR(p^r, m)$ is a basis of the form $\{\alpha, \alpha^f, \alpha^{f^2}, \ldots, \alpha^{f^{m-1}}\}$ where $\alpha \in GR(p^r, m)$. The paper asserted that a basis $\{\beta_j\}$ with automorphism matrix $\Omega$ is self-dual if and only if $\Omega$ is an orthogonal matrix, and that $\{\beta_j\}$ is normal if and only if $\Omega$ is a symmetric matrix, or equivalently, the Frobenius automorphism $f$ is the $m$-cycle $(\beta_1 \beta_2 \ldots \beta_m)$.

3. Results and Discussion

We begin by giving new interesting examples of normal and dual bases of certain Galois rings. MAGMA routines are written to generate the bases of $GR(p^r, m)$, to derive the automorphism matrix and to test for symmetry and orthogonality. Several cases are considered including specifically the Galois fields $GR(p, m)$. We disregard the Galois ring $GR(p^r, 1)$ because it has a trivial basis.

**Example 3.1.** We extend Example 3.8 and Example 3.15 of [2] and verify that none of the four distinct normal bases of $GR(4, 2)$ is self-dual as Table 1 shows. Note that the dual of a normal basis is also normal.

| Normal Basis | Dual |
|--------------|------|
| $\{\omega, 3 + \omega\}$ | $\{2 + \omega, 1 + 3\omega\}$ |
| $\{1 + \omega, 3\omega\}$ | $\{3 + \omega, 2 + 3\omega\}$ |
| $\{2 + \omega, 1 + 3\omega\}$ | $\{\omega, 3 + 3\omega\}$ |
| $\{3 + \omega, 2 + 3\omega\}$ | $\{1 + \omega, 3\omega\}$ |

**Example 3.2.** We extend Example 3.9 and Example 3.16 of [2] and find that there are eight distinct normal bases of $GR(4, 3)$. Table 2 shows these normal bases and their duals. Observe that the first four normal bases are self-dual. For instance, consider the normal basis $\{3 + \omega, 3 + \omega^2, 1 + 3\omega + 3\omega^2\}$. The automorphism matrix relative to this basis is the circulant matrix given by

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

(12)

The Frobenius automorphism on $GR(4, 3)$ is a 3-cycle and $\Omega$ is symmetric. Further, $\Omega$ is orthogonal and the hence the basis is self-dual as well.
Table 2. Normal bases of $GR(4, 3)$ and their duals

| Normal Basis            | Dual                                      |
|------------------------|-------------------------------------------|
| $\{1 + \omega, 1 + \omega^2, 3 + 3\omega + 3\omega^2\}$ | $\{1 + \omega, 1 + \omega^2, 3 + 3\omega + 3\omega^2\}$ |
| $\{3 + \omega, 3 + \omega^2, 1 + 3\omega + 3\omega^2\}$ | $\{3 + \omega, 3 + \omega^2, 1 + 3\omega + 3\omega^2\}$ |
| $\{1 + 3\omega, 1 + 3\omega^2, 3 + 3\omega + 3\omega^2\}$ | $\{1 + 3\omega, 1 + 3\omega^2, 3 + 3\omega + 3\omega^2\}$ |
| $\{3 + 3\omega, 3 + 3\omega^2, 1 + \omega + \omega^2\}$ | $\{3 + 3\omega, 3 + 3\omega^2, 1 + \omega + \omega^2\}$ |
| $\{1 + 2\omega + \omega^2, 3 + 3\omega + 3\omega^2, 1 + 3\omega + 2\omega^2\}$ | $\{1 + 2\omega + \omega^2, 3 + 3\omega + 3\omega^2, 1 + \omega + 2\omega^2\}$ |
| $\{3 + 2\omega + \omega^2, 1 + 3\omega + 3\omega^2, 3 + 3\omega + 2\omega^2\}$ | $\{3 + 2\omega + \omega^2, 1 + 3\omega + 3\omega^2, 3 + \omega + 2\omega^2\}$ |
| $\{1 + \omega + 2\omega^2, 1 + 2\omega + 3\omega^2, 3 + \omega + 3\omega^2\}$ | $\{1 + 3\omega + 2\omega^2, 1 + 2\omega + \omega^2, 3 + 3\omega + \omega^2\}$ |
| $\{3 + \omega + 2\omega^2, 3 + 2\omega + 3\omega^2, 1 + \omega + 3\omega^2\}$ | $\{3 + 3\omega + \omega^2, 3 + 2\omega + \omega^2, 1 + 3\omega + \omega^2\}$ |

Example 3.3. Consider the Galois ring $GR(8, 2) = \mathbb{Z}_8[\omega]$, where $\omega$ is the root of the monic basic irreducible polynomial $x^2 + x + 1 \in \mathbb{Z}_8[x]$. The automorphism matrix with respect to the polynomial basis $P_2(\omega) = \{1, \omega\}$ of $GR(8, 2)$ is given by

$$\Omega_P = \begin{pmatrix} 1 & 1 \\ \omega & 7 + 7\omega \end{pmatrix}$$ (13)

The inverse of $\Omega$ is given by

$$\Omega_P^{-1} = \begin{pmatrix} 3 + 5\omega & 5 + 2\omega \\ 6 + 3\omega & 3 + 6\omega \end{pmatrix}$$ (14)

so that $\{3 + 5\omega, 5 + 2\omega\}$ is the dual of $P_2(\omega)$. Table 3 gives the normal bases of $GR(8, 2)$ and their duals. Note that none of the 16 distinct normal bases of $GR(8, 2)$ is self-dual. But their duals are normal bases also. This can be seen through a simple determination of the automorphism matrix. For instance, the set $\{\omega, 7 + 7\omega\}$ is normal and its automorphism matrix is given by the circulant matrix

$$\Omega_N = \begin{pmatrix} \omega & 7 + 7\omega \\ 7 + 7\omega & \omega \end{pmatrix}$$ (15)

which is symmetric but not orthogonal. In fact, its dual is $\{2 + 5\omega, 5 + 3\omega\}$.

We now specifically consider a free linear block code $B$ over $GR(4, 2)$ and $\tau(B)$ its quaternary image with respect to a basis $\{\beta_1, \beta_2\}$ over $\mathbb{Z}_4$. If $B$ has rate-$k/n$, then $\tau(B)$ has rate-$2k/2n$. Consequently, if $G$ is a generator matrix of $B$, then $\tau(B)$ is generated by the matrix

$$G[\tau(B)] = \begin{pmatrix} \tau(\beta_1 G) \\ \tau(\beta_2 G) \\ \vdots \\ \tau(\beta_m G) \end{pmatrix}$$ (16)

This specific result is generalized in the following theorem.

Theorem 3.4. Let $B$ be a free rate-$k/n$ linear block code of length $n$ over $GR(p^r, m)$ with generator matrix $G$ and $\tau(B)$ be the $p^r$-ary image of $B$ with respect to the basis $\{\beta_1, \beta_2, ..., \beta_m\}$. Then a generator of $\tau(B)$ is given by the $mk \times mn$ matrix

$$\begin{pmatrix} \tau(\beta_1 G) \\ \tau(\beta_2 G) \\ \vdots \\ \tau(\beta_m G) \end{pmatrix}$$
Table 3. Normal bases of $GR(8, 2)$ and their duals

| Normal Basis | Dual          |
|--------------|--------------|
| {$\omega, 7 + 7\omega$} | {$2 + 5\omega, 5 + 3\omega$} |
| {$1 + \omega, 7\omega$}    | {$3 + 5\omega, 6 + 3\omega$} |
| {$2 + \omega, 1 + 7\omega$} | {$5\omega, 3 + 3\omega$} |
| {$3 + \omega, 2 + 7\omega$} | {$1 + 5\omega, 4 + 3\omega$} |
| {$4 + \omega, 3 + 7\omega$} | {$6 + 5\omega, 1 + 3\omega$} |
| {$5 + \omega, 4 + 7\omega$} | {$7 + 5\omega, 2 + 3\omega$} |
| {$6 + \omega, 5 + 7\omega$} | {$4 + 5\omega, 7 + 3\omega$} |
| {$7 + \omega, 6 + 7\omega$} | {$5 + 5\omega, \omega$} |
| {$3\omega, 5 + 5\omega$}    | {$6 + 7\omega, 7 + \omega$} |
| {$1 + 3\omega, 6 + 5\omega$} | {$3 + 7\omega, 4 + \omega$} |
| {$2 + 3\omega, 7 + 5\omega$} | {$4 + 7\omega, 5 + \omega$} |
| {$3 + 3\omega, 5\omega$}    | {$1 + 7\omega, 2 + \omega$} |
| {$4 + 3\omega, 1 + 5\omega$} | {$2 + 7\omega, 3 + \omega$} |
| {$5 + 3\omega, 2 + 5\omega$} | {$7 + 7\omega, \omega$} |
| {$6 + 3\omega, 3 + 5\omega$} | {$7\omega, 1 + \omega$} |
| {$7 + 3\omega, 4 + 5\omega$} | {$5 + 7\omega, 6 + \omega$} |

Proof. Suppose the rows of $G$ are $r_1, r_2, \ldots, r_k$. These rows form a basis for $B$. It can be shown by straightforward approach that the set

$$\{\tau(\beta_1 r_1), \ldots, \tau(\beta_1 r_k), \tau(\beta_2 r_1), \ldots, \tau(\beta_2 r_k), \ldots, \tau(\beta_m r_1), \ldots, \tau(\beta_m r_k)\}$$

is a basis for $\tau(B)$. Thus a generator matrix for $\tau(B)$ can have the elements of this basis as rows as shown below.

$$G[\tau(B)] = \begin{pmatrix}
\tau(\beta_1 r_1) \\
\vdots \\
\tau(\beta_1 r_k) \\
\tau(\beta_2 r_1) \\
\vdots \\
\tau(\beta_2 r_k) \\
\vdots \\
\tau(\beta_m r_1) \\
\vdots \\
\tau(\beta_m r_k)
\end{pmatrix} = \begin{pmatrix}
\tau(\beta_1 G) \\
\tau(\beta_2 G) \\
\vdots \\
\tau(\beta_m G)
\end{pmatrix}$$

(17)

This theorem shows that the generator matrix of the $p^r$-ary image is completely determined by the generator matrix $G$ of the free linear block code $B$ over $GR(p^r, m)$ and the chosen basis for $GR(p^r, m)$.

Referring back to the 3-quasi cyclic rate-2/6 linear block code $B$ over $GR(4, 2)$ with generator matrix given in (10) with Hamming distance $d = 4$, its quaternary image $\tau_3(B)$ with respect to the polynomial basis $P_2(\omega) = \{1, \omega\}$ is a rate-4/12 linear block code over $Z_4$ with 256 codewords.
The generator matrix of the quaternary image $\tau_P(B)$ is given by

$$
G[\tau_P(B)] = \begin{pmatrix}
1 & 0 & 0 & 0 & 3 & 1 & 0 & 2 & 3 & 2 & 1 & 1 \\
0 & 1 & 0 & 0 & 3 & 2 & 2 & 2 & 1 & 3 & 0 \\
0 & 0 & 1 & 0 & 3 & 3 & 3 & 2 & 0 & 2 & 1 & 3 \\
0 & 0 & 0 & 1 & 1 & 0 & 2 & 1 & 2 & 1 & 2 & 1
\end{pmatrix}
$$

(18)

Its Lee distance is $d_L = 8$ and Hamming distance $d_{\tau_P(B)} = 4$, making it a Type $\alpha$ code. With a suitable choice of minimum-weight word, the image code is also optimal with respect to the generalized Rabizzoni bound (9).

**Example 3.5.** The dual basis of $P_2(\omega)$ is the set $D = \{3 + \omega, 1 + 2\omega\}$. Given the same $GR(4, 2)$ code $B$ above, the quaternary image $\tau_D(B)$ with respect to $D$ is generated by the matrix

$$
G[\tau_D(B)] = \begin{pmatrix}
1 & 0 & 0 & 0 & 3 & 3 & 0 & 2 & 3 & 2 & 1 & 3 \\
0 & 1 & 0 & 0 & 1 & 2 & 2 & 2 & 1 & 1 & 0 \\
0 & 0 & 1 & 0 & 3 & 1 & 3 & 2 & 0 & 2 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 3 & 0 & 2 & 1 & 2 & 2 & 3
\end{pmatrix}
$$

(19)

Although $\tau_D(B)$ is derived from the same code $B$ via a change in basis, the quaternary image $\tau_D(B)$ is not equal to $\tau_P(B)$ and is an entirely new rate-$4/12$ linear block code over $\mathbb{Z}_4$ with 256 codewords. However, the distances are preserved. Its Lee distance is $d_L = 8$ and Hamming distance is $d_{\tau_D(B)} = 4$, which makes it a Type $\alpha$ code and a Rabizzoni-optimal code as well.

The code in Example 3.5 is the second known example of a $\mathbb{Z}_4$-code with such optimality. It should be observed further that the quaternary image of $B$ with respect to the normal basis $N = \{\omega, 3 + 3\omega\}$ has exactly the same generator matrix as $\tau_P(B)$ and hence $\tau_P(B) = \tau_N(B)$. This example shows that it is possible to construct new good codes over $\mathbb{Z}_{p^r}$ from a given linear block code over $GR(p^r, m)$ with just a suitable change in basis of $GR(p^r, m)$.

It may happen that the $p^r$-ary images of a linear block code $B$ over $GR(p^r, m)$ are all the same under any basis of $GR(p^r, m)$ and thus all distances are retained, such as the case of the non-free rate-$3/4$ $GR(4, 2)$-code generated by

$$
G[B] = \begin{pmatrix}
1 & 1 & 1 & 3 + 2\omega \\
0 & 2 & 0 & 2 \\
0 & 0 & 2 & 2
\end{pmatrix}
$$

(20)

However, there is a case where the image codes have varying homogeneous distances, such as the case of the non-free rate-$2/4$ $GR(4, 3)$-code generated by

$$
G[B] = \begin{pmatrix}
1 & 1 & 0 & \omega^2 \\
0 & 2 & 2\omega^2 & 2 + 2\omega
\end{pmatrix}
$$

(21)

**Example 3.6.** The polynomial basis of $F_4 = F_2[\omega]$ where $\omega^2 + \omega + 1 = 0$ is $P_2(\omega) = \{1, \omega\}$ whose dual is $D = \{1 + \omega, 1\}$, while a normal basis is $N = \{\omega, 1 + \omega\}$. The following identities can be easily verified for any $v \in F_4$.

$$
\tau_P(v) = \tau_D((1 + \omega)v) = \tau_N(\omega v)
$$

$$
\tau_P(\omega v) = \tau_D(v) = \tau_N(1 + \omega)v
$$
Because of this result and by extension, the binary images of a linear block code over $\mathbb{F}_4$ with respect to $P_2(\omega)$, $D$ and $N$ will be the same, so no change in basis is necessary. As a specific case, consider the rate-$3/5$ $\mathbb{F}_4$-linear block code over $\mathbb{F}_4$ generated by
\[ G[B] = \begin{pmatrix} 1 & 0 & 0 & 1 + \omega & \omega \\ 0 & 1 & 0 & \omega & 1 + \omega \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \] (22)

This quaternary code is a $(5, 3, 3)$ maximum distance separable (MDS) code with 64 codewords. The image codes with respect to $P_2(\omega)$, $D$ and $N$ are all $(10, 6, 3)$ binary codes with the same generator matrix given by
\[ G[\tau(B)] = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \] (23)

This extends Example 1 in Section 3 of [9].

Acknowledgments
The first author gratefully acknowledges financial support from the UP Research Dissemination Grant and the UPLB Academic Development Fund.

References
[1] Solé P and Sison V 2007 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 2270–73
[2] Sison V 2016 Bases of the Galois ring $GR(p^r, m)$ over the integer ring $Z_{p^r}$ Preprint gr-qc/0401010
[3] Honold T 2001 A characterization of finite Frobenius rings Arch. Math. (Basel) 76 406–15
[4] MacDonald B 1974 Finite Rings with Identity (Marcel Dekker)
[5] Wan Z-X 2003 Lectures on Finite Fields and Galois Rings (World Scientific)
[6] Greferath M and Schmidt S E 2001 Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code IEEE Trans. Inform. Theory 45 7 2522–24
[7] Greferath M and Schmidt S E 2000 Finite-ring combinatorics and MacWilliams Equivalence Theorem J. Combin Theory Ser. A 92 17–28
[8] Rabizzoni P 1989 Relation between the minimum weight of a linear code over $GF(q^m)$ and its $q$-ary image over $GF(q)$ Lecture Notes in Comput. Sci. 388 209–12
[9] Cerezo B R, Pasion A and Sison V 2006 Binary convolutional codes and linear block codes over $\mathbb{F}_4$ Matimyas Matematika 29 1-2 9–17