Cryptography and Communications (2021) 13:601–616
https://doi.org/10.1007/s12095-021-00487-x

G-codes, self-dual G-codes and reversible G-codes over the ring $\mathcal{B}_{j,k}$

S. T. Dougherty[1] · Joe Gildea[2] · Adrian Korban[2] · Serap Şahinkaya[3]

Received: 25 September 2020 / Accepted: 24 March 2021 / Published online: 3 May 2021

Abstract
In this work, we study a new family of rings, $\mathcal{B}_{j,k}$, whose base field is the finite field $\mathbb{F}_{p^r}$. We study the structure of this family of rings and show that each member of the family is a commutative Frobenius ring. We define a Gray map for the new family of rings, study G-codes, self-dual G-codes, and reversible G-codes over this family. In particular, we show that the projection of a G-code over $\mathcal{B}_{j,k}$ to a code over $\mathcal{B}_{l,m}$ is also a G-code and the image under the Gray map of a self-dual G-code is also a self-dual G-code when the characteristic of the base field is 2. Moreover, we show that the image of a reversible G-code under the Gray map is also a reversible $G^{2^{j+k}}$-code. The Gray images of these codes are shown to have a rich automorphism group which arises from the algebraic structure of the rings and the groups. Finally, we show that quasi-G codes, which are the images of G-codes under the Gray map, are also G^s-codes for some s.

Keywords Codes over rings · Gray maps · Self-dual codes · Automorphism groups

Mathematics Subject Classification 2010 94B05 · 16S34

1 Introduction

In [1], a new family of rings,

$$\mathcal{F}_{j,k} = \mathbb{F}_4[v_1, v_2, \ldots, v_j, u_1, u_2, \ldots, u_k]/\langle v_i^2 - v_i, u_i^2 \rangle,$$

was introduced. The base field of this ring is the finite field of order 4, denoted by $\mathbb{F}_4$. This family of rings was used to construct codes which were reversible, which is a desirable quality for DNA codes. In the present work, we generalise the family of rings $\mathcal{F}_{j,k}$ so that

✉ Adrian Korban
adrian3@windowslive.com

[1] University of Scranton, Scranton, PA 18518, USA

[2] Department of Mathematical and Physical Sciences, University of Chester, Thornton Science Park, Pool Ln, Chester, CH2 4NU, England

[3] Faculty of Engineering, Department of Natural and Mathematical Sciences, Tarsus University, Mersin, Turkey

the base field is in an arbitrary finite field $\mathbb{F}_{p^r}$. We also define a Gray map Θ which is a generalization of the Gray map given in [1, 13, 14].

Assume the indeterminates u_i and v_i all commute.

Definition 1.1 Let p be a prime and let $\mathbb{F}_{p^r}$ be the finite field of order p^r. Let

$$\mathcal{B}_{j,k} = \mathbb{F}_{p^r}[v_1, v_2, \ldots, v_j, u_1, u_2, \ldots, u_k]/\langle v_i^2 - v_i, u_i^2 \rangle. \tag{1.1}$$

This definition generalises the definition of $\mathcal{F}_{j,k}$ in [1] as well as the rings $R_k = \mathbb{F}_2[u_1, u_2, \ldots, u_k]/\langle u_i^2 = 0\rangle$ in [6–8], the rings $A_k = \mathbb{F}_2[v_1, v_2, \ldots, v_k]/\langle v_i^2 = v_i\rangle$ in [2] and the rings $\mathbb{F}_{p^r}[v_1, v_2, \ldots, v_k]/\langle v_i^2 - v_i, v_i v_j - v_j v_i\rangle$ given in [11].

In essence, all of the families of rings were studied together with Gray maps to ambient spaces over finite fields. They use the algebraic structure of the family of rings to obtain desirable properties for the codes over finite fields. One desirable property is that one can obtain codes with a rich automorphism group via the algebraic structure of the ring through the Gray map. In this construction, one can find codes that might have been missed by more classical construction techniques, for example, one may find extremal binary self-dual codes with new weight enumerators or with a different orders of the automorphism group. Further in [4], G-codes were used to construct binary self-dual codes from codes over R_k. By combining these techniques, self-dual binary codes with very rich automorphism groups were found which had been missed during the decades long search for binary self-dual codes. The primary reason was that these techniques allowed the authors to find codes that had different automorphism groups than those constructed from the usual techniques. It is precisely this type of scenario we exploit in the present paper. Our goal is to study the algebra of the new family of rings, the corresponding Gray maps, and the group G, so that one can employ our results to construct useful and interesting codes over finite fields that would not be constructed with other techniques. Additionally, we present matrix constructions for self-dual and reversible G- codes and study their properties over the new family of rings.

2 The ring $\mathcal{B}_{j,k}$

We begin by describing the family of rings $\mathcal{B}_{j,k}$. Set

$$\mathcal{B}_{j,k} = \mathbb{F}_{p^r}[v_1, v_2, \ldots, v_j, u_1, u_2, \ldots, u_k]/\langle v_i^2 - v_i, u_i^2 \rangle.$$

For $A \subseteq [j] = \{1, 2, 3, \ldots, j\}$ and $B \subseteq [k] = \{1, 2, 3, \ldots, k\}$, we denote

$$v_A := \prod_{i \in A} v_i \quad \text{and} \quad u_B := \prod_{i \in B} u_i,$$

with $u_\emptyset = 1$ and $v_\emptyset = 1$. Every element in the ring can be written as

$$\sum_{\substack{A \subseteq [j] \\ B \subseteq [k]}} c_{A,B} v_A u_B, \tag{2.1}$$

where $c_{A,B} \in \mathbb{F}_{p^r}$.

It is immediate that

$$u_A u_{A'} = \begin{cases} 0 & if \ \ A \cap A' \neq \emptyset, \\ u_{A \cup A'} & if \ \ A \cap A' = \emptyset. \end{cases} \tag{2.2}$$

Similarly, we have

$$v_A v_{A'} = v_{A \cup A'}. \tag{2.3}$$

By using (2.2) and (2.3), multiplication of two elements in $\mathcal{B}_{j,k}$ is given by:

$$\left(\sum_{A,B} c_{A,B} v_A u_B\right)\left(\sum_{A',B'} c_{A',B'} v_{A'} u_{B'}\right) = \sum_{\substack{A,B,A',B' \\ B\cap B'=\emptyset}} (c_{A,B} c_{A',B'}) v_{A\cup A'} u_{B\cup B'}, \tag{2.4}$$

where A, A' are subsets of $[j]$ and B, B' are subsets of $[k]$.

Lemma 2.1 *The commutative ring $\mathcal{B}_{j,k}$ has characteristic p, and $|\mathcal{B}_{j,k}| = (p^r)^{2^{j+k}}$.*

Proof The commutativity of the ring follows from the fact that $\mathbb{F}_{p^r}$ is commutative and that the indeterminates commute. Since the characteristic of $\mathbb{F}_{p^r}$ is p, then $\mathcal{B}_{j,k}$ has characteristic p. When we look at the representation of elements of $\mathcal{B}_{j,k}$ given in (2.1), we see that there are $2^j 2^k = 2^{j+k}$ subsets and p^r choices for each coefficient $c_{A,B}$. This gives that $\mathcal{B}_{j,k}$ has cardinality $(p^r)^{2^{j+k}}$. □

We now give some structural theorems about the family of rings.

Theorem 2.2 *Let j and k be non-negative integers.*

1. *The ring $\mathcal{B}_{j,k}$ is isomorphic to $\oplus_{i=1}^{2^j} \mathcal{B}_{0,k}$.*
2. *An element a is a unit in $\mathcal{B}_{j,k}$ if and only if the projection to each component of $\oplus_{i=1}^{2^j} \mathcal{B}_{0,k}$ is a unit.*

Proof The ideals $\langle v_j \rangle$ and $\langle 1 + v_j \rangle$ are relatively prime ideals. By Lemma 2.3 in [3], we have that $\mathcal{B}_{j,k} \cong \mathcal{B}_{j-1,k} \times \mathcal{B}_{j-1,k}$. Then, by induction on j, we have the first result.

The second result follows immediately from the isomorphisms in the first. □

Since $\mathcal{B}_{j,k}$ is isomorphic to $\oplus_{i=1}^{2^j} \mathcal{B}_{0,k}$, it is natural to look at the structure of the ring $\mathcal{B}_{0,k} = \mathbb{F}_{p^r}[u_1, u_2, \ldots, u_k]/\langle u_i^2 \rangle$ to understand the structure of $\mathcal{B}_{j,k}$.

Lemma 2.3 *Let $\sum_{A\subseteq[k]} c_A u_A \in \mathcal{B}_{0,k}$, with $c_\emptyset = 0$, then*

$$\left(\sum_{A\subseteq[k]} c_A u_A\right)^p = 0$$

where p is the characteristic of $\mathcal{B}_{0,k}$.

Proof First, we note that if $A \neq \emptyset$, then $u_A^2 = 0$. Then, we see that the coefficient of any monomial in this expansion, other than the first or the last is divisible by p and hence 0. Therefore, all of the terms are 0. □

Lemma 2.4 *An element a of the ring $\mathcal{B}_{0,k}$ is a unit if and only if $c_\emptyset \neq 0$.*

Proof We write an element in $\mathcal{B}_{0,k}$ as $c_\emptyset + \sum_{A\subset[k]} c_A u_A$ by hypothesis, with $c_\emptyset \neq 0$. Since the ring has characteristic p and by Lemma 2.3, the inverse of $c_\emptyset + \sum_{A\subset[k]} c_A u_A$ is:

$$\sum_{i=0}^{p-1} \binom{p-1}{i} (c_\emptyset^{-1})^{i+1} \left(\sum_{A\subseteq[k]} c_A u_A\right)^i.$$

The term $c_{\emptyset}^{-1}$ exists if and only if $c_{\emptyset} \neq 0$. □

Theorem 2.5 *An element a of the ring $\mathcal{B}_{0,k}$ is a zero-divisor if and only if $c_{\emptyset} = 0$. The set of all non-units form a maximal ideal and the cardinality of this maximal ideal is $(p^r)^{2^k-1}$ and therefore the ring $\mathcal{B}_{0,k}$ is local.*

Proof For the first statement, we know by Lemma 2.3 that

$$\left(\sum_{A\subseteq[k]} c_A u_A\right)\left(\sum_{A\subseteq[k]} c_A u_A\right)^{p-1} = 0,$$

when $c_{\emptyset} = 0$. Therefore it is a zero-divisor. Lemma 2.4 gives the other direction.

Next, let $\mathfrak{m} = \langle u_1, u_2, \ldots, u_k\rangle$. Elements of this ideal are all of the form, $c_{\emptyset} + \sum_{A\subset[k]} c_A u_A$ where $c_{\emptyset} = 0$. This is necessarily all non-units and is therefore the unique maximal ideal. □

Theorem 2.6 *The ring $\mathcal{B}_{j,k}$ is not local for non-zero j.*

Proof The ring $\mathcal{B}_{j,k}$ is isomorphic to $\oplus_{i=1}^{2^j}\mathcal{B}_{0,k}$ by Theorem 2.2. Then each ideal corresponding to the sum of $(k-1)$ zero-ideals with one copy of $\mathcal{B}_{0,k}$ is a maximal ideal. Therefore, the ring is not local. □

As an example of this, consider the ring $\mathcal{B}_{1,0} = \mathbb{F}_p[v_1]/\langle v_1^2 - v_1\rangle$. The ring is isomorphic via Theorem 2.2 to $\mathbb{F}_p \times \mathbb{F}_p$. This ring has two maximal ideals corresponding to $\mathbb{F}_p \times \{0\}$ and to $\{0\} \times \mathbb{F}_p$. Therefore, the ring is not local.

Given the definition of inner-product and the fact that the ring is commutative it is easy to see that for any ideal I, $Ann(I) = I^{\perp}$. We use this result in the following theorem.

Theorem 2.7 *Let $I_1 = \langle u_{i_1}u_{i_2}\cdots u_{i_s}\rangle$ and $I_2 = \langle u_{i_1}, u_{i_2}, \ldots, u_{i_s}\rangle$ be ideals of $\mathcal{B}_{0,k}$, where $i_\ell \neq i_{\ell'}$, when $\ell \neq \ell'$. Then $|I_1| = (p^r)^{2^{k-s}}$ and $|I_2| = (p^r)^{2^k-2^{k-s}}$.*

Proof Elements of I_1 are in the form of

$$\sum_{A\subseteq[k]} c_A u_A,\ c_A \in \mathbb{F}_{p^r},$$

where $u_{\emptyset} = 1$. It is clear that every u_A must have $\{i_1, i_2, \ldots, i_s\} \subseteq A$. Then there are 2^{k-s} such subsets of $[k]$. Hence $|I_1| = (p^r)^{2^{k-s}}$.

For the second statement, elements of I_2 are in the same form. But this time, the subsets of $[k]$ differ. More precisely, subsets must have at least one of $\{i_1, i_2, \ldots, i_s\}$. It can be easily obtained that there are $2^k - 2^{k-s}$ such subsets. Hence $|I_2| = (p^r)^{2^k-2^{k-s}}$. □

Theorem 2.8 *Let $I_1 = \langle u_{i_1}u_{i_2}\ldots u_{i_s}\rangle$ and $I_2 = \langle u_{i_1}, u_{i_2}, \ldots u_{i_s}\rangle$ be ideals of $\mathcal{B}_{0,k}$. Then $I_2^{\perp} = I_1$.*

Proof We have $I_2^{\perp} \subseteq I_1$ by the fact that $u_{i_j}u_A = 0$ where $A = \{i_1, i_2, \ldots, i_s\}$ and $u_{i_j} \in A$. Equality follows from Theorem 2.7 by using the fact that $\mathcal{B}_{0,k}$ is a Frobenius ring and examining the cardinalities. □

Corollary 2.9 *The ideal $\langle u_i\rangle$ is a self dual code of length 1 for $1 \leq i \leq k$.*

Proof Follows from Theorem 2.7. □

2.1 Gray maps

Gray maps have been one of the most important aspects of codes over rings. In essence, they are a map from the n fold product of the ring to an ambient space where the finite field is the alphabet. This map emanates from the map that sends elements of the ring to elements in the the s fold product of the finite field, where s is determined by the ring. This map, in general, preserves weight and its intention is to create interesting codes over the finite field from codes over the ring.

In this section, we define a Gray map $\Theta : \mathcal{B}_{j,k} \to \mathbb{F}_{p^r}^{2^{j+k}}$. The map we give is a generalization of the map given in [1] as well as those given in [2, 6–8], and [9].

We can view $\mathcal{B}_{j,k}$ as $\mathcal{B}_{j,k-1} + u_k\mathcal{B}_{j,k-1}$ and write each element of $\mathcal{B}_{j,k}$ as $a + bu_k$. Then we can define the map $\Phi : \mathcal{B}_{j,k} \to \mathcal{B}_{j,k-1}^2$ as follows:

$$\Phi(a + bu_k) = (b, a + b). \tag{2.5}$$

We can view $\mathcal{B}_{j,k}$ as $\mathcal{B}_{j-1,k} + v_j\mathcal{B}_{j-1,k}$ and write each element of $\mathcal{B}_{j,k}$ as $a + bv_j$. Then we can define the following map $\Psi : \mathcal{B}_{j,k} \to \mathcal{B}_{j-1,k}^2$ as follows:

$$\Psi(a + bv_j) = (a, a + b). \tag{2.6}$$

We now define the map $\Theta : \mathcal{B}_{j,k} \to \mathbb{F}_{p^r}^{2^{j+k}}$ as follows:

$$\Theta(a) = \Psi^j(\Phi^k(a)). \tag{2.7}$$

Lemma 2.10 *Let C be a linear code over $\mathcal{B}_{j,k}$ of length n. Then $\Theta(C)$ is a linear code of length $n(2^{j+k})$.*

Proof First, we shall show that the map Φ is linear. We have that

$$\begin{aligned}\Phi((a + bu_k) + (a' + b'u_k)) &= \Phi((a + a') + (b + b')u_k)\\ &= (b + b', a + a' + b + b')\\ &= (b, a + b) + (b', a' + b')\\ &= \Phi(a + bu_k) + \Phi(a' + b'u_k).\end{aligned}$$

Then if $c \in \mathcal{B}_{j,k-1}$ we have that

$$\begin{aligned}\Phi(c(a + bu_k)) &= \Phi(ca + cbu_k)\\ &= (cb, ca + cb)\\ &= c(b, a + b) = c\Phi(a + bu_k).\end{aligned}$$

This gives that Φ is linear.

Now, we show that the map Ψ is also linear. We have

$$\begin{aligned}\Psi((a + bv_j) + (a' + b'v_j)) &= \Psi((a + a') + (b + b')v_j)\\ &= (a + a', a + a' + b + b')\\ &= (a, a + b) + (a', a' + b')\\ &= \Psi(a + bv_j) + \Psi(a' + b'v_j).\end{aligned}$$

If $c \in \mathcal{F}_{j-1,k}$ we have

$$\begin{aligned}\Psi(c(a+bv_j)) &= \Phi(ca+cbv_j)\\ &= (ca, ca+cb)\\ &= c(a, a+b) = c\Psi(a+bv_j).\end{aligned}$$

This gives that Ψ is linear.

Then the map Θ is the composition of $j+k$ linear maps and therefore the map Θ is a linear map. □

Define the swap maps $\sigma_1, \sigma_2, \ldots, \sigma_k$ that act on $\mathbb{F}_{p^r}^{2^{j+k}}$ as follows:

$$\sigma_k(\mathbf{c}_1, \mathbf{c}_2) = (\mathbf{c}_2, \mathbf{c}_1),\ \forall \mathbf{c}_1, \mathbf{c}_2 \in \mathbb{F}_{p^r}^{2^{j+k-1}},$$

$$\sigma_{k-1}(\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4) = (\mathbf{c}_2, \mathbf{c}_1, \mathbf{c}_4, \mathbf{c}_3),\ \forall \mathbf{c}_i \in \mathbb{F}_{p^r}^{2^{j+k-2}}$$

continuing to

$$\sigma_1(\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_{2^{j+k}-1}, \mathbf{c}_{2^{j+k}}) = (\mathbf{c}_2, \mathbf{c}_1, \mathbf{c}_4, \mathbf{c}_3, \ldots, \mathbf{c}_{2^{j+k}}, \mathbf{c}_{2^{j+k}-1}),\ \forall \mathbf{c}_i \in \mathbb{F}_{p^r}^{2^j}.$$

The next theorem shows that the map Θ gives some automorphisms in the image under certain conditions.

Theorem 2.11 *If the base field of $\mathcal{B}_{j,k}$ has characteristic 2 and C is a linear code over $\mathcal{B}_{j,k}$, then $\Theta(C)$ has k swap maps, $\sigma_1, \sigma_2, \ldots, \sigma_k$ in their automorphism group.*

Proof Given an element $a + bu_k$, multiplication by $1 + u_k$ gives $(1 + u_k)(a + bu_k) = a+(a+b)u_k$. We see that $\Phi(a+bu_k) = (b, a+b)$ and $\Phi(a+(a+b)u_k) = (a+b, 2a+b)$. Therefore, if the characteristic of the finite field is 2, then $\Phi(a + (a + b)u_k) = (a + b, b)$. This gives that for characteristic 2, multiplication by the unit $1 + u_i$, for each i induces an automorphism of order 2 in the image that corresponds to a swap map. Finally, let σ_i denote the induced by multiplication by $1 + u_i$. This gives the result. □

We now generalize two results from [2] and [6] respectively, where it is shown that for the maps defined in (2.5) and (2.6), the following two

$$\Phi(C^\perp) = (\Phi(C))^\perp$$

and

$$\Psi(C^\perp) = (\Psi(C))^\perp$$

hold when the base field of the ring is $\mathbb{F}_2$. We now show that the two hold for the ring $\mathcal{B}_{j,k}$ only when the base field is $\mathbb{F}_{2^r}$.

Lemma 2.12 *Let C be a code over $\mathcal{B}_{j,k}$. Let $\Phi : \mathcal{B}_{j,k} \to \mathcal{B}_{j,k-1}^2$ be defined as:*

$$\Phi(a + bu_k) = (b, a + b),$$

and let $\Psi : \mathcal{B}_{j,k} \to \mathcal{B}_{j-1,k}^2$ be defined as:

$$\Psi(a + bv_j) = (a, a + b).$$

Then $\Phi(C^\perp) = (\Phi(C))^\perp$ and $\Psi(C^\perp) = (\Psi(C))^\perp$ if and only if the characteristic of the ring $\mathcal{B}_{j,k}$ is 2.

Proof We prove the result for Φ. The proof for Ψ is similar.

Let $\mathbf{v}_1+\mathbf{w}_1u_k$ and $\mathbf{v}_2+\mathbf{w}_2u_k$ be two orthogonal vectors in $\mathcal{B}_{j,k}$, where $\mathbf{v}_i$, $\mathbf{w}_i$ are vectors in $\mathcal{B}^n_{j,k-1}$. Then

$$[\mathbf{v}_1+\mathbf{w}_1u_k,\mathbf{v}_2+\mathbf{w}_2u_k]=[\mathbf{v}_1,\mathbf{v}_2]+([\mathbf{v}_1,\mathbf{w}_2]+[\mathbf{v}_2,\mathbf{w}_1])u_k=0.$$

Moreover, we have that $[\mathbf{v}_1,\mathbf{v}_2]=0$ and $[\mathbf{v}_1,\mathbf{w}_2]+[\mathbf{v}_2,\mathbf{w}_1]=0$.

The images of the vectors have the following inner-product:

$$[\Phi(\mathbf{v}_1+\mathbf{w}_1u_k),\Phi(\mathbf{v}_2+\mathbf{w}_2u_k)]=[(\mathbf{w}_1,\mathbf{v}_1+\mathbf{w}_1),(\mathbf{w}_2,\mathbf{v}_2+\mathbf{w}_2)]=$$

$$=[\mathbf{v}_1,\mathbf{v}_2]+[\mathbf{v}_1,\mathbf{w}_2]+[\mathbf{v}_2,\mathbf{w}_1]+2[\mathbf{w}_1,\mathbf{w}_2]=2[\mathbf{w}_1,\mathbf{w}_2].$$

This will only be zero if the characteristic of the ring $\mathcal{B}_{j,k}$ is 2, i.e., the base field is $\mathbb{F}_{2^r}$. Assuming that the characteristic of the ring $\mathcal{B}_{j,k}$ is 2 gives that $\Phi(C^\perp)\subseteq(\Phi(C))^\perp$. Since Φ is a bijection we have $\Phi(C^\perp)=(\Phi(C))^\perp$. □

We now have the following result.

Theorem 2.13 *Let C be a linear code over*

$$\mathcal{B}_{j,k}=\mathbb{F}_{2^r}[v_1,v_2,\ldots,v_j,u_1,u_2,\ldots,u_k]/\langle v_i^2-v_i,u_i^2\rangle.$$

Then $\Theta(C^\perp)=\Theta(C)^\perp$.

Proof Follows from Lemma 2.12. □

Corollary 2.14 *Let C be a self-dual code over*

$$\mathcal{B}_{j,k}=\mathbb{F}_{2^r}[v_1,v_2,\ldots,v_j,u_1,u_2,\ldots,u_k]/\langle v_i^2-v_i,u_i^2\rangle$$

of length n, then $\Theta(C)$ is a self-dual code over $\mathbb{F}_{2^r}$ of length $n(2^{j+k})$.

Proof Follows from Theorem 2.13 and Lemma 2.10. □

2.2 Characters

In this section, we show that the ring $\mathcal{B}_{j,k}$ is a Frobenius ring by showing that there is a generating character for the associated character module. Recall that a character of the module M is a homomorphism $\chi: M\to\mathbb{C}^*$. We note that some have the codomain as the rationals and use the additive operation rather than the non-zero complex numbers with multiplication. But we shall maintain the notation given in [3], where one can find a complete description of the relationship between characters and codes.

Denote by $\widehat{M}$ the character module of M. Let R be a Frobenius ring and let $\phi: R\to\widehat{R}$ be the module isomorphism. Set $\chi=\phi(1)$, giving $\phi(r)=\chi^r$ for $r\in R$. We call this character χ a generating character for $\widehat{R}$. Note that there is not a unique generating character. But by providing a generating character for a commutative ring, we show that the ring is, in fact, Frobenius. This is because a finite commutative ring R is Frobenius if and only if $\widehat{R}$ has a generating character, see [3].

In the present situation, we have that the ring $\mathcal{B}_{j,k}$ is isomorphic to $\oplus_{i=1}^{2^j}\mathcal{B}_{0,k}$.

We need only to find a generating character for $\mathcal{B}_{0,k}$ then if $\chi_{\mathcal{B}_{0,k}}$ is the generating character for $\mathcal{B}_{0,k}$, we have that the character χ for R defined by

$$\chi(a) = \prod \chi_{\mathcal{B}_{0,k}}(a_i) \tag{2.8}$$

where a corresponds to $(a_1, a_2, \dots, a_s)$ via the isomorphism, is a generating character for $\mathcal{B}_{j,k}$. To do this, we recall that any finite field of order p^e can be written as $\mathbb{F}_p(\xi)$ where ξ is a root of the irreducible polynomial $q(x)$ of degree e. That is $\mathbb{F}_p(\xi) \cong \mathbb{F}_p[x]/\langle q(x)\rangle$. Then each element in $\mathbb{F}_{p^e}$ can be written as $\sum a_i \xi^i$ where $a_i \in \mathbb{F}_p$. This leads immediately to the following lemma.

Lemma 2.15 *The ring $\mathcal{B}_{0,k} \cong \mathbb{F}_p[\xi, u_1, u_2, \dots, u_k]/\langle q(x), u_i^2\rangle$, where all of the indeterminates commute and $q(x)$ is an irreducible polynomial of degree e. Each element in $\mathcal{B}_{0,k}$ can be written as $\sum_{s=0}^{e-1}\sum_{A\subseteq[k]} \xi^s (d_s)_A u_A$, where $d_S \in \mathbb{F}_p$. Let η be a complex primitive root of p-th root of unity. The generating character for $\mathcal{B}_{0,k}$ is given by $(\eta)^{\sum_{s=0}^{e-1}\sum_{A\subseteq[k]}(d_s)_A}$ showing that the ring is Frobenius.*

Proof We have already explained why each element can be written in that form.

The unique minimal ideal of $\mathcal{B}_{0,k}$ is the orthogonal of the unique maximal ideal. Therefore, the minimal ideal is $\mathfrak{a} = \langle u_1u_2\cdots u_k\rangle$. It follows that any ideal that is contained in $ker(\chi)$ must contain the ideal $\mathfrak{a}$. But we have that $\chi(u_1u_2\cdots u_k) = \eta$ which gives that $ker(\chi)$ contains no non-trivial ideal. It follows that the map is a generating character and then the ring $\mathcal{B}_{0,k}$ is a Frobenius ring. □

The next theorem follows from the fact that the ring decomposes by the Chinese Remainder Theorem.

Theorem 2.16 *Let*

$$\chi_i\left(\sum_{s=0}^{e-1}\sum_{A\subseteq[k]} \xi^s (d_s)_A u_A\right) = (\eta)^{\sum_{s=0}^{e-1}\sum_{A\subseteq[k]}(d_s)_A}.$$

The ring $\mathcal{B}_{j,k} \cong \oplus_{i=1}^{2^j}\mathcal{B}_{0,k}$ has a generating character of the form:

$$\chi = \prod_{i=1}^{2^j} \chi_i,$$

giving that the ring $\mathcal{B}_{j,k}$ is a Frobenius ring.

Proof We have that $\mathcal{B}_{j,k}$ is isomorphic to $\oplus_{i=1}^{2^j}\mathcal{B}_{0,k}$. It follows that the generating character is χ from Lemma 2.15.

Then the ring is Frobenius since it has a generating character. □

Let T be a square $(p^r)^{2^{j+k}}$ by $(p^r)^{2^{j+k}}$ matrix indexed by the elements of $\mathcal{B}_{j,k}$ and let

$$T_{a,b} = \chi_a(b) = \chi(ab), \tag{2.9}$$

where χ is the generating character of $\widehat{\mathcal{B}_{j,k}}$.

Recall that the complete weight enumerator of a code C is defined as

$$cwe_c(x_{a_0}, x_{a_1}, \dots, x_{a_{r-1}}) = \sum_{\mathbf{c}\in C}\prod_{i=0}^{r-1} x_{a_i}^{n_i(\mathbf{c})}, \tag{2.10}$$

where there are $n_i(\mathbf{c})$ occurrences of a_i in the vector $\mathbf{c}$.

It follows that if C is a linear code over $\mathcal{B}_{j,k}$, then

$$cwe_{C^\perp} = \frac{1}{|C|} cwe_C(T \cdot (x_0, x_1, \ldots, x_{r-1})). \tag{2.11}$$

By collapsing T as in [15], we get that if C is a linear code over $\mathcal{B}_{j,k}$, then

$$W_{C^\perp}(x, y) = \frac{1}{|C|} W_c(x + (|\mathcal{B}_{j,k}| - 1)y, x - y),$$

where $W_C(x, y)$ denotes the Hamming weight enumerator of C.

Now recall that the Lee weight enumerator of a code C is defined as:

$$L_C(x, y) = \sum_{\mathbf{c} \in C} x^{N - wt_L(\mathbf{c})} y^{wt_L(\mathbf{c})} \tag{2.12}$$

where N is the length of $\Theta(C)$.

From Section 2, we know that when the characteristic of the finite field is 2, then $\Theta(C^\perp) = \Theta(C)^\perp$ which allows us to find the MacWilliams identities for the Lee weight enumerators of codes over

$$\mathcal{B}_{j,k} = \mathbb{F}_{2^r}[v_1, v_2, \ldots, v_j, u_1, u_2, \ldots, u_k]/\langle v_i^2 - v_i, u_i^2 \rangle$$

in the following way:

$$Lee_{C^\perp}(z) = W_{\Theta(C^\perp)}(z) = W_{\Theta(C)^\perp}(z)$$

where $Lee_C(z)$ is the Lee weight enumerator and W denotes the Hamming weight enumerator. This leads to the following theorem.

Theorem 2.17 *Let C be a code of length n over*

$$\mathcal{B}_{j,k} = \mathbb{F}_{2^r}[v_1, v_2, \ldots, v_j, u_1, u_2, \ldots, u_k]/\langle v_i^2 - v_i, u_i^2 \rangle$$

then

$$Lee_{C^\perp}(z) = \frac{1}{|C|} (1 + z)^{2^{j+k}n} Lee_C \left(\frac{1 - z}{1 + z} \right). \tag{2.13}$$

3 *G*-Codes over $\mathcal{B}_{j,k}$

In this section, we study group codes which we refer to as G-codes, over the ring $\mathcal{B}_{j,k}$. The point of group codes is to construct codes that are invariant canonically by the action of a group G. This technique allows us to construct codes which other construction methods do not find. Moreover, by applying the Gray map we are able to construct codes over a finite field that are quasi-G codes, which mean they are held invariant by a different group and are endowed with algebraic structure of the original ring.

3.1 Group rings

We begin by giving the standard definitions of group rings and their algebraic operations. Let G be a finite group of order n and let R be a finite ring, then any element in RG is of the form $v = \sum_{i=1}^{n} \alpha_i g_i$, $\alpha_i \in R$, $g_i \in G$. We note that group rings in general do not require the ring to be finite, but in our setting these are precisely the rings that we are interested in, since we want to use them as alphabets of codes.

Addition in the group ring is done by coordinate addition, namely

$$\sum_{i=1}^{n} \alpha_i g_i + \sum_{i=1}^{n} \beta_i g_i = \sum_{i=1}^{n} (\alpha_i + \beta_i) g_i.$$

The product of two elements in a group ring is given by

$$\left(\sum_{i=1}^{n} \alpha_i g_i\right)\left(\sum_{j=1}^{n} \beta_j g_j\right) = \sum_{i,j} \alpha_i \beta_j g_i g_j.$$

This gives that the coefficient of g_k in the product is $\sum_{g_i g_j = g_k} \alpha_i \beta_j$.

We recall a construction of linear codes in R^n from the group ring RG, where G is a finite group of order n. This construction was first given for codes over fields by Hurley in [10] and this construction was extended to codes over finite commutative Frobenius rings in [4]. Let R be a finite commutative Frobenius ring and let $G = \{g_1, g_2, \ldots, g_n\}$ be a group of order n. Let $v = \alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \cdots + \alpha_{g_n} g_n$ be an element in RG. Then define the following matrix $\sigma(v) \in M(R)$ to be:

$$\sigma(v) = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \alpha_{g_1^{-1}g_3} & \ldots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \alpha_{g_2^{-1}g_3} & \ldots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \alpha_{g_n^{-1}g_3} & \ldots & \alpha_{g_n^{-1}g_n} \end{pmatrix}. \tag{3.1}$$

Note that the elements $g_1^{-1}, \ldots, g_n^{-1}$ are simply the elements of the group G given in some order. There is not a canonical reason for this, but rather this particular order aids in certain proofs and computations.

For a given element $v \in RG$, we define the following code over the ring R:

$$C(v) = \langle \sigma(v) \rangle. \tag{3.2}$$

Namely, the code $C(v)$ is the code formed by taking the row space of the matrix $\sigma(v)$ over the finite ring R. It follows immediately that the code $C(v)$ is a linear code, since it is row space of a generator matrix. We stress that in no way are we assuming that the matrix $C(v)$ is in any way a minimal generating set for the code. In general it is not. We recall the following definitions from [5] that we apply in our setting:

- Let $\mathcal{B}_{j,k}$ be a local Frobenius ring with unique maximal ideal $\mathfrak{m}_i$, and let $\mathbf{w}_1, \ldots, \mathbf{w}_s$ be vectors in $\mathcal{B}_{j,k}^n$. Then $\mathbf{w}_1, \ldots, \mathbf{w}_s$ are modular independent if and only if $\sum \alpha_j \mathbf{w}_j = \mathbf{0}$ implies that $\alpha_j \in \mathfrak{m}_i$ for all j.
- Let $\mathbf{w}_1, \ldots, \mathbf{w}_s$ be non-zero vectors in $\mathcal{B}_{j,k}^n$. Then $\mathbf{w}_1, \ldots, \mathbf{w}_s$ are independent if $\sum \alpha_j \mathbf{w}_j = \mathbf{0}$ implies that $\alpha_j \mathbf{w}_j = \mathbf{0}$ for all j.

In [5], it is shown that if the ring is local, then any modular independent set is a minimal generating set and that if the ring is not local then any set that is both modular independent and independent is a minimal generating set. We shall call such a set a basis for the code.

In [4], it is shown that G-codes are linear codes in R^n if and only if they are left ideals in a group ring. Specifically, let $v \in \mathcal{B}_{j,k}G$ and let $C(v)$ be the corresponding code in $\mathcal{B}_{j,k}^n$. Let $I(v)$ be the set of elements of $\mathcal{B}_{j,k}G$ such that $\sum \alpha_i g_i \in I(v)$ if and only if $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in C(v)$. Then $I(v)$ is a left ideal in $\mathcal{B}_{j,k}G$.

The following is immediate from these results.

Lemma 3.1 *Let $v \in RG$, where R is a finite ring and G is a finite group. Then $Aut(C(v))$ contains G as a subgroup.*

Proof This follows from the fact that the action of G on the coordinates of $C(v)$ necessarily holds the code invariant, since it corresponds to an ideal in the group ring. □

It is also shown in [4] that for a commutative Frobenius ring R, if C is a G-code for some G then its orthogonal $C^{\perp}$ is also a G-code.

The following definition is given in [4].

Definition 3.2 Let G be a finite group of order n and R a finite Frobenius commutative ring. Let D be a code in R^{sn} where the coordinates can be partitioned into n sets of size s where each set is assigned an element of G. If the code D is held invariant by the action of multiplying the coordinate set marker by every element of G then the code D is called a quasi-group code of index s.

The following is immediate from the definition.

Lemma 3.3 *Let C be a linear G-code over $B_{j,k}$, then $\Theta(C)$ is a quasi-G code of index 2^{j+k} in $\mathbb{F}_{p^r}^{n2^{j+k}}$.*

Lemma 3.4 *Let G be a finite group of order n and R a finite Frobenius commutative ring. A quasi-G code of index s in R^{sn} is equivalent to a group code under the action of the finite group G^s.*

Proof Consider a quasi-G code of index s in R^{ns}. Reorder the coordinates of R^{ns} so that the n coordinates in the orbit of a coordinate under the action of group G are grouped together. Then the coordinates in R^{ns} are arranged into s copies of n coordinates where the code is held invariant by the action of the group G on each block of n coordinates. This gives the result. □

These two lemmas lead to the following important theorem.

Theorem 3.5 *Let C be a linear G-code over $B_{j,k}$, then $\Theta(C)$ is a $G^{2^{j+k}}$ code over $\mathbb{F}_{p^r}$, which gives that $Aut(C)$ necessarily contains $G^{2^{j+k}}$ as a subgroup.*

Proof Lemma 3.3 gives that $\Theta(C)$ is a quasi-G code of index 2^{j+k}, then Lemma 3.4 gives that $\Theta(C)$ is a $G^{2^{j+k}}$ code. Finally Lemma 3.1 gives that $Aut(C)$ necessarily contains $G^{2^{j+k}}$ as a subgroup. □

This theorem can be extended even further in the case when the base field has even order.

Corollary 3.6 *Let C be a linear G-code over $B_{j,k}$, where the base field is $\mathbb{F}_{2^r}$. Then $Aut(C)$ necessarily contains $G^{2^{j+k}}$ and k swap maps which generate an additional subgroup.*

Proof Theorem 3.5 gives the first part and Corollary 2.14 gives the second part. □

4 Projections and lifts of self-dual G-codes over $\mathcal{B}_{j,k}$

Define $\pi_{k,m} : \mathcal{B}_{j,k} \to \mathcal{B}_{j,m}$ by $\pi_{k,m}(u_i) = 0$ if $i > m$ and the identity elsewhere. That is, $\pi_{k,m}$ is the projection of $\mathcal{B}_{j,k}$ to $\mathcal{B}_{j,m}$. Note that if $k \leq m$, then $\pi_{k,m}$ is the identity map on $\mathcal{B}_{j,k}$. Also define $\pi_{j,l} : \mathcal{B}_{j,k} \to \mathcal{B}_{l,k}$ by $\pi_{j,l}(v_i) = 0$ if $i > l$ and the identity elsewhere. That is, $\pi_{j,l}$ is the projection of $\mathcal{B}_{j,k}$ to $\mathcal{B}_{l,k}$. Note that if $j \leq l$, then $\pi_{j,l}$ is the identity map on $\mathcal{B}_{j,k}$. Now, let $a \in \mathcal{B}_{j,k}$ and define

$$\Pi_{(j,k),(l,m)} : \mathcal{B}_{j,k} \to \mathcal{B}_{l,m}$$

by

$$\Pi_{(j,k),(l,m)}(a) = \pi_{j,l}(\pi_{k,m}(a)).$$

That is, $\Pi_{(j,k),(l,m)}$ is the projection of $\mathcal{B}_{j,k}$ to $\mathcal{B}_{l,m}$.

Example 4.1 Let $\mathcal{B}_{1,1} = \mathbb{F}_3[v_1, u_1]/\langle v_1^2 - v_1, u_1^2\rangle$. Consider the projection of $a = 2 + v_1 + 2u_1 + 2v_1u_1$ from $\mathcal{B}_{1,1}$ to $\mathcal{B}_{0,0} = \mathbb{F}_3$. By the above definition we have that $\Pi_{(1,1),(0,0)}(2 + v_1 + 2u_1 + 2v_1u_1) = \pi_{1,0}(\pi_{1,0}(2 + v_1 + 2u_1 + 2v_1u_1)) = \pi_{1,0}(2 + v_1) = 2$.

We allow j and k to be ∞ as well and denote this map as $\Pi_{(\infty,\infty),(l,m)}$. In this case the ring $B_{\infty,\infty}$ is an infinite ring. If $C = \Pi_{(j,k),(l,m)}(C')$ for some C' and $j > l, k > m$, then C' is said to be a lift of C.

Theorem 4.2 *Let $C(v)$ be a self-dual G-code over $\mathcal{B}_{j,k}$. Then $\Pi_{(j,k),(l,m)}(C(v))$ is a self-orthogonal G-code over $\mathcal{B}_{l,m}$.*

Proof We first show that $\Pi_{(j,k),(l,m)}(C(v))$ is a self-orthogonal code over $\mathcal{B}_{l,m}$. Let $\mathbf{w} = (w_1, w_2, \ldots, w_n)$ and $\mathbf{z} = (z_1, z_2, \ldots, z_n)$ be vectors in $C(v)$. We have that

$$\Pi_{(j,k),(l,m)}\left(\sum w_i z_i\right) = \sum(\Pi_{(j,k),(l,m)}(w_i)\Pi_{(j,k),(l,m)}(z_i)).$$

If $\sum w_i z_i = 0$ in $\mathcal{B}_{j,k}$ then $\Pi_{(j,k),(l,m)}(0) = 0$ so

$$\langle \Pi_{(j,k),(l,m)}(w), \Pi_{(j,k),(l,m)}(z)\rangle_{(l,m)} = 0.$$

Therefore $\Pi_{(j,k),(l,m)}(C(v))$ is self-orthogonal.

To show that $\Pi_{(j,k),(l,m)}(C(v))$ is also a G-code, we notice that the projection $\Pi_{(j,k),(l,m)}(C(v)) = \Pi_{(j,k),(l,m)}(\langle\sigma(v)\rangle)$ corresponds to $\Pi_{(j,k),(l,m)}(v) = \Pi_{(j,k),(l,m)}(\alpha_{g_1})g_1 + \Pi_{(j,k),(l,m)}(\alpha_{g_2})g_2 + \cdots + \Pi_{(j,k),(l,m)}(\alpha_{g_n})g_n$, where $\alpha_{g_i} \in \mathcal{B}_{j,k}$. Thus $\Pi_{(j,k),(l,m)}(C(v))$ is a G-code over $\mathcal{B}_{j,k}$. □

Theorem 4.3 *Let $w \in \mathcal{B}_{l,m}G$ generate a self-dual G-code over $\mathcal{B}_{l,m}$. Then w generates a self-dual code over $\mathcal{B}_{j,k}$ for all $j > l$ and $k > m$. Moreover, the self-dual code over $\mathcal{B}_{j,k}$ is also a G-code.*

Proof Let $C_{j,k}$ be the code generated by $w \in \mathcal{B}_{j,k}G$. We proceed by induction. We know $C_{l,m}$ is a self-dual G-code by assumption.

Assume $C_{j,k}$ is a self-dual G-code. We have that $C_{j,k} = \langle\sigma(w)\rangle$, where $w \in \mathcal{B}_{j,k}G$, $C_{j+1,k} = C_{j,k} \oplus v_{j+1}C_{j,k}$, where $C_{j,k} \cap v_{j+1}C_{j,k} = \emptyset$ and $C_{j,k+1} = C_{j,k} + u_{k+1}C_{j,k}$, where $C_{j,k} \cap u_{k+1}C_{j,k} = \emptyset$. Then we have that $C_{j+1,k} = \langle\sigma(w)\rangle \oplus v_{j+1}\langle\sigma(w)\rangle$, $C_{j,k+1} = \langle\sigma(w)\rangle \oplus u_{k+1}\langle\sigma(w)\rangle$ and $|C_{j+1,k}| = |C_{j,k}||C_{j,k}| = \sqrt{(p^r)^{2^{j+k}}}\sqrt{(p^r)^{2^{j+k}}} =$

$\sqrt{(p^r)^{2^{j+k+1}}} = |C_{j,k+1}|$. Then for vectors $\mathbf{w}, \mathbf{z}, \mathbf{w}', \mathbf{z}' \in C_{j,k}$ we have (since $C_{j,k}$ is self-dual by assumption),

$$\begin{aligned}[\mathbf{w} + v_{j+1}\mathbf{w}', \mathbf{z} + v_{j+1}\mathbf{z}']_{j+1} &= [\mathbf{w}, \mathbf{z}]_j + v_{j+1}[\mathbf{w}, \mathbf{z}']_j \\ &\quad + v_{j+1}[\mathbf{w}', \mathbf{z}]_j + v_{j+1}^2[\mathbf{w}', \mathbf{z}']_j = 0\end{aligned}$$

and

$$\begin{aligned}[\mathbf{w} + u_{k+1}\mathbf{w}', \mathbf{z} + u_{k+1}\mathbf{z}']_{k+1} &= [\mathbf{w}, \mathbf{z}]_k + u_{k+1}[\mathbf{w}, \mathbf{z}']_k \\ &\quad + u_{k+1}[\mathbf{w}', \mathbf{z}]_k + u_{k+1}^2[\mathbf{w}', \mathbf{z}']_k = 0.\end{aligned}$$

Hence $C_{j+1,k}$ and $C_{j,k+1}$ are self-dual codes since both are self-orthogonal and both have the proper cardinality. Therefore by mathematical induction $C_{j,k}$ is a self-dual code for all finite j and k.

Next we prove that $C_{\infty,\infty}$ is self-dual. If $\mathbf{z}, \mathbf{w} \in C_{\infty,\infty}$ then there exist j and k with $\mathbf{z}, \mathbf{w} \in C_{j,k}$ and hence $[\mathbf{z}, \mathbf{w}]_j = [\mathbf{z}, \mathbf{w}]_k = 0$ which implies $[\mathbf{z}, \mathbf{w}]_\infty = 0$. If $\mathbf{w} \in C_{\infty,\infty}^\perp$ then $\mathbf{w} \in C_{j,k}^\perp$ for some j and k which gives that $\mathbf{w} \in C_{j,k}$ and hence in $C_{\infty,\infty}$. Therefore $C_{\infty,\infty}$ is self-dual.

To show that $C_{j,k}$ is also a G-code, let $w = \alpha_{g_1}g_1 + \alpha_{g_2}g_2 + \cdots + \alpha_{g_n}g_n$, where $\alpha_{g_i} \in \mathcal{B}_{l,m}$. Then we see that $C_{j+1,k} = \langle\sigma(w)\rangle \oplus v_{j+1}\langle\sigma(w)\rangle$ corresponds to $w + v_{j+1}w = (\alpha_{g_1} + v_{j+1}\alpha_{g_1})g_1 + (\alpha_{g_2} + v_{j+1}\alpha_{g_2})g_2 + \cdots + (\alpha_{g_n} + v_{j+1}\alpha_{g_n})g_n$ in $\mathcal{B}_{j+1,k}G$. Similarly, $C_{j,k+1} = \langle\sigma(w)\rangle \oplus u_{k+1}\langle\sigma(w)\rangle$ corresponds to $w + u_{k+1}w = (\alpha_{g_1} + u_{k+1}\alpha_{g_1})g_1 + (\alpha_{g_2} + u_{k+1}\alpha_{g_2})g_2 + \cdots + (\alpha_{g_n} + u_{k+1}\alpha_{g_n})g_n$ in $\mathcal{B}_{j,k+1}G$. Thus $C_{j,k}$ is a G-code. □

As a consequence of the above theorem, we have the following result.

Corollary 4.4 *If C is a self-dual G-code over $\mathcal{B}_{l,m}$ then there exists a self-dual code C' over $\mathcal{B}_{j,k}$, for $j > l$ and $k > m$ with $\Pi_{(j,k),(l,m)}(C') = C$.*

5 The gray image of *G*-codes over $\mathcal{B}_{j,k}$

In this section, we restrict our attention to the ring $\mathcal{B}_{j,k} = \mathbb{F}_{2^r}[v_1, v_2, \ldots, v_j, u_1, u_2, \ldots, u_k]/\langle v_i^2 - v_i, u_i^2\rangle$ and employ the Gray map defined in Section 2. We extend the Gray map Θ linearly to all of $\mathcal{B}_{j,k}$ and define the Lee weight of an element in $\mathcal{B}_{j,k}$ to be the Hamming weight of its image. We get a linear distance preserving map from $\mathcal{B}_{j,k}^n$ to $\mathbb{F}_{2^r}^{2^{j+k}n}$.

From Theorem 2.13 we know that for any linear code over $\mathcal{B}_{j,k}$ we have $\Theta(C^\perp) = \Theta(C)^\perp$. As a consequence of this, we get the following result.

Corollary 5.1 *Let C be a G-code over $\mathcal{B}_{j,k}$. Then $\Theta(C^\perp) = \Theta(C)^\perp$.*

Proof From the definition of a G-code, we know that C is linear. The rest follows from Theorem 2.13. □

Theorem 5.2 *If C is a self-dual G-code of length n over $\mathcal{B}_{j,k}$, then $\Theta(C)$ is a self-dual G-code of length $n(2^{j+k})$ over $\mathbb{F}_{2^r}$.*

Proof If $C = C^\perp$, then $\Theta(C) = \Theta(C^\perp) = \Theta(C)^\perp$ and we have that $\Theta(C)$ is self-dual. To show that $\Theta(C)$ is also a G-code, we see that $\Theta(C) = \Theta(\langle\sigma(v)\rangle)$ corresponds to $\Theta(v) = \Theta(\alpha_{g_1})g_1 + \Theta(\alpha_{g_2})g_2 + \cdots + \Theta(\alpha_{g_n})g_n$ in $\mathbb{F}_{2^r}G$. Thus, $\Theta(C)$ is a G-code. □

Theorem 5.3 *Let C be a self-dual G-code over $\mathcal{B}_{j,k}$ of length n, then $\Theta(C)$ is a self-dual G^n-code of length $n(2^{j+k})$ over $\mathbb{F}_{2^r}$. If the base field is the binary field and the Lee weight of every codeword is $0 \pmod 4$, then $\Theta(C)$ is a Type II binary code.*

Proof If $C = C^{\perp}$ then by Corollary 5.1, $\Theta(C^{\perp}) = \Theta(C)^{\perp}$. □

Since Θ is distance preserving, the following corollary immediately follows from the bounds given in [12]. Note that for $j \geq 1$ and $k \geq 1$, the length of the binary image of a code over $\mathcal{B}_{j,k}$ will always be divisible by 4, hence the case $n \equiv 22 \pmod{24}$ is not possible for the image of an $\mathcal{B}_{j,k}$ code.

Corollary 5.4 *Let $d_L(n, I)$ and $d_L(n, II)$ denote the minimum distance of a Type I and Type II G-code over $\mathcal{B}_{j,k}$ of length n, respectively, where the base field is $\mathbb{F}_2$. Then, for $j \geq 1$ and $k \geq 1$, we have*

$$d_L(n, I), d_L(n, II) \geq 4 \left\lfloor \frac{2^{(j-1)+(k-1)}n}{6} \right\rfloor + 4.$$

6 Reversible *G*-codes over $\mathcal{B}_{j,k}$

Lastly in this paper, we extend some results from [1] on reversible G-codes. We start with a definition.

Definition 6.1 A code C is said to be reversible of index α if $\mathbf{a}_i$ is a vector of length α and $\mathbf{c}^{\alpha} = (\mathbf{a}_0, \mathbf{a}_1, \ldots, \mathbf{a}_{s-1}) \in C$ implies that $(\mathbf{c}^{\alpha})^r = (\mathbf{a}_{s-1}, \mathbf{a}_{s-2}, \ldots, \mathbf{a}_1, \mathbf{a}_0) \in C$.

For the remainder of this section, we fix the listing of the group elements as follows. Let G be a finite group of order $n = 2l$ and let $H = \{e, h_1, h_2, \ldots, h_{l-1}\}$ be a subgroup of index 2 in G. Let $\beta \notin H$ be an element in G, with $\beta^{-1} = \beta$. We list the elements of $G = \{g_1, g_2, \ldots, g_n\}$ as follows:

$$\{e, h_1, \ldots, h_{l-1}, \beta h_{l-1}, \beta h_{l-2}, \ldots, \beta h_2, \beta h_1, \beta\}. \tag{6.1}$$

In [1], the following is proven.

Theorem 6.2 *Let R be a finite ring. Let G be a finite group of order $n = 2l$ and let $H = \{e, h_1, h_2, \ldots, h_{l-1}\}$ be a subgroup of index 2 in G. Let $\beta \notin H$ be an element in G with $\beta^{-1} = \beta$. List the elements of G as in (6.1), then any linear G-code in R^n (a left ideal in RG) is a reversible code of index 1.*

We now employ the map defined in Section 2 and prove the following result.

Theorem 6.3 *Let G be a finite group of order $n = 2l$ and let $H = \{e, h_1, h_2, \ldots, h_{l-1}\}$ be a subgroup of index 2 in G. Let $\beta \notin H$ be an element in G with $\beta^{-1} = \beta$ and list the elements of G as in (6.1). If C is a linear G-code in $\mathcal{B}_{j,k}$ (a left ideal in $\mathcal{B}_{j,k}G$), then $\Theta(C)$ is a reversible $G^{2^{j+k}}$-code over $\mathbb{F}_{p^r}$.*

Proof By Theorem 6.2, we have that C is a reversible code. Therefore, if $(c_0, c_1, \ldots, c_{n-1}) \in C$ we have that $(c_{n-1}, c_{n-2}, \ldots, c_1, c_0) \in C$, where $c_i \in \mathcal{B}_{j,k}$. Then $\Theta(C)$ is a vector of length 2^{j+k}. This gives that

$$(\Theta(c_0), \Theta(c_1), \ldots, \Theta(c_{n-1})) \in \Theta(C)$$

and then

$$(\Theta(c_{n-1}), \Theta(c_{n-2}), \ldots, \Theta(c_1), \Theta(c_0)) \in \Theta(C).$$

This gives the first part of the result.

The last statement comes from Theorem 3.5. □

The following result can also be found in [1].

Theorem 6.4 *Let R be a finite ring. Let $G_1, G_2, \ldots, G_n$ be finite groups, each of order 2ℓ and let $H_1, H_2, \ldots, H_n$, where $H_i = \{e_i, h_{i_1}, h_{i_2}, \ldots, h_{i_{\ell-1}}\}$, be subgroups of index 2 in $G_1, G_2, \ldots, G_n$ respectively. Let $\beta_i \notin H_i$ be an element in G_i with $\beta_i^{-1} = \beta_i$. List the elements of G_i as*

$$e_i, h_{i_1}, h_{i_2}, \ldots, h_{i_{\ell-1}}, \beta_i h_{i_{\ell-1}}, \beta_i h_{i_{\ell-2}}, \ldots, \beta_i h_{i_2}, \beta_i h_{i_1}, \beta_i. \tag{6.2}$$

Then any linear code D generated by the matrix

$$M = \begin{bmatrix} \sigma(v_1) & \sigma(v_2) & \sigma(v_3) & \ldots & \sigma(v_n) \\ \sigma(v_n) & \sigma(v_{n-1}) & \sigma(v_{n-2}) & \ldots & \sigma(v_1) \end{bmatrix},$$

where $v_i \in RG_i$, is a reversible code of index 1.

With the above theorem, our ring $\mathcal{B}_{j,k}$ and the Gray map from Section 2, we have the following result.

Theorem 6.5 *Let R be a finite ring. Let $G_1, G_2, \ldots, G_n$ be finite groups, each of order 2ℓ and let $H_1, H_2, \ldots, H_n$, where $H_i = \{e_i, h_{i_1}, h_{i_2}, \ldots, h_{i_{\ell-1}}\}$, be subgroups of index 2 in $G_1, G_2, \ldots, G_n$ respectively. Let $\beta_i \notin H_i$ be an element in G_i with $\beta_i^{-1} = \beta_i$. List the elements of G_i as*

$$e_i, h_{i_1}, h_{i_2}, \ldots, h_{i_{\ell-1}}, \beta_i h_{i_{\ell-1}}, \beta_i h_{i_{\ell-2}}, \ldots, \beta_i h_{i_2}, \beta_i h_{i_1}, \beta_i. \tag{6.3}$$

If D is a linear code in $\mathcal{B}_{j,k}^n$ generated by the matrix

$$M = \begin{bmatrix} \sigma(v_1) & \sigma(v_2) & \sigma(v_3) & \ldots & \sigma(v_n) \\ \sigma(v_n) & \sigma(v_{n-1}) & \sigma(v_{n-2}) & \ldots & \sigma(v_1) \end{bmatrix},$$

where $v_i \in \mathcal{B}_{j,k}G_i$, then $\Theta(D)$ is a reversible code over $\mathbb{F}_{p^r}$ of index 2^{j+k}.

Proof By Theorem 6.4, we have that D is a reversible code of index 1. Therefore, if

$$((a_0^1, a_1^1, \ldots, a_{2\ell-1}^1), (a_0^2, a_1^2, \ldots, a_{2\ell-1}^2), \ldots, (a_0^n, a_1^n, \ldots, a_{2\ell-1}^n)) \in D$$

we have that

$$((a_{2\ell-1}^n, a_{2\ell-2}^n, \ldots, a_0^n), (a_{2\ell-1}^{n-1}, a_{2\ell-2}^{n-1}, \ldots, a_0^{n-1}), \ldots, (a_{2\ell-1}^1, a_{2\ell-2}^1, \ldots, a_0^1)) \in D,$$

where $a_i^m \in \mathcal{B}_{j,k}$ with $i \in \{0, 1, 2, \ldots, 2\ell-1\}$ and $m \in \{1, 2, 3, \ldots, n\}$. Then $\Theta(a_i^m)$ is a vector of length 2^{j+k}. This gives that

$$((\Theta(a_0^1), \Theta(a_1^1), \ldots, \Theta(a_{2\ell-1}^1)), (\Theta(a_0^2), \Theta(a_1^2), \ldots, \Theta(a_{2\ell-1}^2)), \ldots,$$
$$(\Theta(a_0^n), \Theta(a_1^n), \ldots, \Theta(a_{2\ell-1}^n))) \in \Theta(D)$$

then

$$((\Theta(a_{2\ell-1}^n), \Theta(a_{2\ell-2}^n), \ldots, \Theta(a_0^n)), \Theta((a_{2\ell-1}^{n-1}), \Theta(a_{2\ell-2}^{n-1}), \ldots, \Theta(a_0^{n-1})), \ldots,$$
$$(\Theta(a_{2\ell-1}^1), \Theta(a_{2\ell-2}^1), \ldots, \Theta(a_0^1))) \in \Theta(D).$$

This proves the result. □

7 Conclusion

In this work, we studied G-codes, self-dual G-codes and reversible G-codes over a new family of rings $\mathcal{B}_{j,k}$. In particular, we showed that the projection of a G-code over $\mathcal{B}_{j,k}$ to a code over $\mathcal{B}_{l,m}$ is also a G-code, we defined a Gray map for the new family of rings and showed that the image of a self-dual G-code under this Gray map is also a self-dual G-code. We also proved that the image of a reversible G-code under the Gray map is a reversible $G^{2^{j+k}}$-code and that the images of G-codes under the Gray map are G^s-codes for some s. A suggestion for future research is to search for self-dual G-codes or other families of codes over our new family of rings. We believe that many interesting codes can be obtained as Gray images of the codes over the ring $\mathcal{B}_{j,k}$ since as we showed in this work, the Gray images of the codes over the ring $\mathcal{B}_{j,k}$ have rich automprphism groups.

References

1. Cengellenmis, Y., Dertli, A., Dougherty, S.T., Korban, A., Sahinkaya, S.: Reversible DNA Codes (in submission)
2. Cengellenmis, Y., Dertli, A., Dougherty, S.T.: Codes over an infinite family of rings with a Gray map. Designs, Codes and Cryptography **72**, 559–580 (2014)
3. Dougherty, S.T.: Algebraic coding theory over finite commutative rings. Springer Briefs in Mathematics, Springer (2017)
4. Dougherty, S.T., Gildea, J., Taylor, R., Tylshchak, A.: Group rings, G-codes and constructions of self-dual and formally self-dual codes. Designs, Codes and Cryptography **86**, 2115–2138 (2018)
5. Dougherty, S.T., Liu, H.: Independence of vectors in codes over rings. Designs, Codes and Cryptography **51**, 55–68 (2009)
6. Dougherty, S.T., Yildiz, B., Karadeniz, S.: Codes over R_k, Gray maps and their binary images. Finite Fields Appl. **17**, 205–219 (2011)
7. Dougherty, S.T., Yildiz, B., Karadeniz, S.: Cyclic Codes over R_k. Designs, Codes and Cryptography **63**, 113–126 (2012)
8. Dougherty, S.T., Yildiz, B., Karadeniz, S.: Self-dual Codes over R_k and Binary Self-Dual Codes. European Journal of Pure and Applied Mathematics **6**, 89–106 (2013)
9. Dougherty, S.T., Yildiz, B., Karadeniz, S.: Constructing Formally Self-Dual Codes over R_k. Discret. Appl. Math. **167**, 188–196 (2014)
10. Hurley, T.: Group rings and rings of matrices. Int. J. Pure Appl. Math. **31**, 319–335 (2006)
11. Irwansyah, D.: Suprijanto, Structure of linear codes over the ring B_k. J. Appl. Math. Comput. **58**, 755–775 (2018)
12. Rains, E.M.: Shadow Bounds for Self-Dual Codes. IEEE Trans. Inform. Theory **44**, 134–139 (1998)
13. collab=Minjia Shi, Yue Guan, Chengchen Wang, Patrick Sole: Few-weight codes from trace codes over R_k. Bull. Aust. Math. Soc. **98**, 167–174 (2018)
14. Shi, M.injia., Rongsheng, W.u., Liu, Y.an., Sole, P.atrick.: Two and three weight codes over $\mathbb{F}_p + u\mathbb{F}_p$. Cryptography and Communications Discrete Structures, Boolean Functions and Sequences **9**, 637–646 (2017)
15. Wood, J.: Duality for modules over finite rings and applications to coding theory. Amer. J. Math. **121**, 555–575 (1999)

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.