Shahid Chamran University of Ahvaz

Journal of Advanced Mathematical Modeling
ISSN (print): 2251-8088, ISSN (on-line): 2645-6141
Vol. 16 No. 2 (2026), pp. 126-142.
DOI: 10.22055/jamm.2026.49745.2375

ON RANK AND KERNEL OF THE HOMOGENEOUS GRAY IMAGE OF LINEAR CODES OVER THE GALOIS RING $GR(4, m)$

TAHEREH AGHIGHI, HAMIDREZA EYVAZI AND KARIM SAMEI*

Communicated by: M. Haghighi

Abstract. Let $R = GR(4, m)$ be the Galois ring of characteristic 4 and cardinality 4^m, where m is a natural number. Let $\mathcal{C}$ be a linear code of length n over R and Φ be the Homogeneous Gray map on R^n. The Homogeneous Gray image of $\mathcal{C}$, i.e., $C = \Phi(\mathcal{C})$ is a code (possibly nonlinear) of length $N = 2^m n$ over $\mathbb{F}_{2^m}$. In this paper, we show that for any $r \in \{2k_0 + k_1, \ldots, min(n + k_0, 2k_0 + k_1 + \binom{k_0}{2})\}$, there exists an R-linear code C of length $N = 2^m n$ and type $\{k_0, k_1\}$ with $\text{rank}(C) = r$, and vice versa. We also establish a similar result for the kernel, i.e., for any $k \in \{k_0+k_1, k_0+k_1+1, \ldots, 2k_0+k_1-2, 2k_0+k_1\}$, there exists an R-linear code C of length $N = 2^m n$ and type $\{k_0, k_1\}$ with $\text{k}_{2^m}(C) = k$, and vice versa.

1. Introduction

For any positive integer $s \geq 1$, let $\mathbb{Z}_{2^s}$ be the ring of integers modulo 2^s. A Galois ring is defined to be a finite commutative ring R with identity 1 such that the set of zero divisors of R, with 0 added is a principal ideal $\langle p \rangle$ for some prime number p. Let $h(x)$ be a monic basic irreducible polynomial of degree $m > 0$ over $\mathbb{Z}_{2^s}$. It is known that the residue class ring $\frac{\mathbb{Z}_{2^s}[x]}{\langle h(x) \rangle}$ is a Galois ring of characteristic 2^s and cardinality 2^{sm}, and is denoted by

MSC(2025): 94B05, 11T71.

Keywords: Galois ring, Homogeneous Gray map, Linear code, Generator matrix, Rank, Kernel.

Received: 23 May 2025, Accepted: 6 July 2026.

*Corresponding author.

$GR(2^s, m)$. Additionally, it is a local ring with a maximal ideal $\mathfrak{m} = \langle 2 \rangle$. Furthermore, any ideal of $GR(2^s, m)$ is of the form $\langle 2^i \rangle$ for $1 \leq i \leq s$, and there is a chain of ideals:

$$GR(2^s, m) = \langle 1 \rangle \supset \langle 2 \rangle \supset \cdots \supset \langle 2^s \rangle = \{0\}.$$

In this paper, we focus on the special case $s = 2$ (i.e., $GR(4, m)$). Throughout this paper, we denote $GR(4, m)$ by R. The residue classes $a_0 + a_1 x + \cdots + a_{m-1} x^{m-1} + \langle h(x) \rangle$, where $a_0, a_1, \ldots, a_{m-1} \in \mathbb{Z}_4$ are all the distinct elements of R. Let $\xi = x + \langle h(x) \rangle$, so $h(\xi) = 0$, and ξ is also of order $2^m - 1$. Each element of R can be written uniquely in the following form

$$a_0 + a_1 \xi + \cdots + a_{m-1} \xi^{m-1}, \quad a_i \in \mathbb{Z}_4 \, (0 \leq i \leq m-1), \tag{1.1}$$

and $R = \mathbb{Z}_4[\xi]$. The representation (1.1) is called the additive representation of the elements of the Galois ring R. Moreover, $\frac{R}{\langle 2 \rangle} \simeq \mathbb{F}_{2^m}$. Let $\tau = \{0, 1, \ldots, \xi^{2^m - 2}\}$, known as the Teichmüller set. Therefore every element $c \in R$ can be written uniquely as

$$c = a + 2b, \quad (a, b \in \tau = \mathbb{F}_{2^m}).$$

The above representation is called the 2-adic representation of the element $c \in R$, see [24, 22, 23, 15].

For every $u \in \mathbb{Z}_4$, the 2-adic expansion of $u = u_0 + 2u_1$ is denoted by $[u] = [u_0, u_1]$, where $u_0, u_1 \in \mathbb{F}_2$. As stated in [21], three operations "$\odot$", "$\oplus$" and "$\circledast$" are introduced as follows; if $u, v \in \mathbb{Z}_4$, $[u] = [u_0, u_1]$ and $[v] = [v_0, v_1]$, then

$$\begin{aligned} u \odot v &= u_0 v_0 + 2 u_1 v_1, \\ u \oplus v &= u_0 \oplus v_0 + 2(u_1 \oplus v_1), \\ u \circledast v &= 2 u_0 v_0. \end{aligned}$$

Note that $u \circledast v$ has been denoted by $(0, \zeta_1)$ in [21]. It is easy to check that $u + v = u \oplus v \oplus (u \circledast v)$, $u \odot v = v \odot u$, $u \oplus u = 0$ and $u \odot u = u$. The vectors in $\mathbb{Z}_4^n$ are written in the form $(u^1, u^2, \ldots, u^n)$, where $u^i \in \mathbb{Z}_4$ and $[u^i] = [u_0^i, u_1^i]$, for all $i = 1, \ldots, n$. The application of the operation "$\odot$" on $\mathbb{Z}_4$ to $\mathbb{Z}_4^n$ is extended in the natural way; that is, if $\boldsymbol{u} = (u^1, u^2, \ldots, u^n), \boldsymbol{v} = (v^1, v^2, \ldots, v^n) \in \mathbb{Z}_4^n$, then $\boldsymbol{u} \odot \boldsymbol{v} = (u^1 \odot v^1, u^2 \odot v^2, \ldots, u^n \odot v^n)$. Recall that for each $\boldsymbol{u} = (u^1, \ldots, u^n)$ and $\boldsymbol{v} = (v^1, \ldots, v^n)$ belonging to $\mathbb{Z}_4^n$, $\boldsymbol{u} * \boldsymbol{v} = (u^1 v^1, \ldots, u^n v^n)$, and $2(\boldsymbol{u} * \boldsymbol{v}) = 2(\boldsymbol{u} \odot \boldsymbol{v})$.

A finite commutative ring with identity $1 \neq 0$ is called a finite chain ring if its ideals are linearly ordered by inclusion. The Homogeneous Gray map Φ has been generalized for finite chain rings, see [20, 13]. Let S be a finite chain ring and $\mathfrak{m} = \langle \gamma \rangle$ be the unique maximal ideal of S. Inasmuch as S is finite, hence, there exists a number i such that $\langle \gamma^i \rangle = \{0\}$. Consider s to be the minimal number such that $\langle \gamma^s \rangle = \{0\}$. Therefore, s is called the nilpotency index of γ, see [20, 16, 13]. Suppose that the residue field $\frac{S}{\langle \gamma \rangle}$ is $\mathbb{F}_{p^m}$, where p is a prime. For each $r \in S$, there are unique $a_0(r), a_1(r), \ldots, a_{s-1}(r) \in \mathbb{F}_{p^m}$ such that $r = a_0(r) + a_1(r)\gamma + \cdots + a_{s-1}(r)\gamma^{s-1}$. Therefore, every element $\boldsymbol{r} \in S^n$ can be written uniquely as

$$\boldsymbol{r} = a_0(\boldsymbol{r}) + a_1(\boldsymbol{r})\gamma + \cdots + a_{s-1}(\boldsymbol{r})\gamma^{s-1},$$

where $a_i(\boldsymbol{r}) = (r_{i,0}, r_{i,1}, \ldots, r_{i,n-1}) \in \mathbb{F}_{p^m}^n$, for every $0 \leq i \leq s-1$. In [13], for a finite chain ring S, the Homogeneous Gray map from S^n to $\mathbb{F}_{p^m}^{p^{m(s-1)}n}$ is defined. The Homogeneous Gray map $\Phi : S^n \longrightarrow \mathbb{F}_{p^m}^{p^{m(s-1)}n}$ can be written in the following form

$$\Phi(\boldsymbol{r}) = [\boldsymbol{r}]\mathcal{A} = [\widetilde{a_0(\boldsymbol{r})}, \widetilde{a_1(\boldsymbol{r})}, \ldots, \widetilde{a_{s-2}(\boldsymbol{r})}, \widetilde{a_{s-1}(\boldsymbol{r})}]\mathcal{A}, \tag{1.2}$$

where

$$\mathcal{A} = \begin{bmatrix} \alpha_0 & \cdots & \alpha_{p^m-1} & \alpha_0 & \cdots & \alpha_{p^m-1} & \cdots & \cdots & \alpha_0 & \cdots & \alpha_{p^m-1} \\ \alpha_{\bar{\xi}_0(0)} & \cdots & \alpha_{\bar{\xi}_0(0)} & \alpha_{\bar{\xi}_0(1)} & \cdots & \alpha_{\bar{\xi}_0(1)} & \cdots & \cdots & \alpha_{\bar{\xi}_0(p^{m(s-2)}-1)} & \cdots & \alpha_{\bar{\xi}_0(p^{m(s-2)}-1)} \\ \alpha_{\bar{\xi}_1(0)} & \cdots & \alpha_{\bar{\xi}_1(0)} & \alpha_{\bar{\xi}_1(1)} & \cdots & \alpha_{\bar{\xi}_1(1)} & \cdots & \cdots & \alpha_{\bar{\xi}_1(p^{m(s-2)}-1)} & \cdots & \alpha_{\bar{\xi}_1(p^{m(s-2)}-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{\bar{\xi}_{s-3}(0)} & \cdots & \alpha_{\bar{\xi}_{s-3}(0)} & \alpha_{\bar{\xi}_{s-3}(1)} & \cdots & \alpha_{\bar{\xi}_{s-3}(1)} & \cdots & \cdots & \alpha_{\bar{\xi}_{s-3}(p^{m(s-2)}-1)} & \cdots & \alpha_{\bar{\xi}_{s-3}(p^{m(s-2)}-1)} \\ 1 & \cdots & 1 & 1 & \cdots & 1 & \cdots & \cdots & 1 & \cdots & 1 \end{bmatrix}_{s \times p^{m(s-1)}},$$

see [7].

A code of length n over $\mathbb{F}_{2^m}$ is a non-empty subset of $\mathbb{F}_{2^m}^n$, and it called linear if it is a subspace of $\mathbb{F}_{2^m}^n$. A code of length n is linear over R if it is a R-submodule of R^n. Let $\mathcal{C}$ be a linear code of length n over R. The Homogeneous Gray image of $\mathcal{C}$ over R is called an R-linear code of length $N = 2^m n$ over $\mathbb{F}_{2^m}$. Since $\mathcal{C}$ is a subgroup of R^n, it is isomorphic to an abelian structure $R^{k_0} \times \mathbb{F}_{2^m}^{k_1}$, and we say that $\mathcal{C}$, or equivalently $C = \Phi(\mathcal{C})$, is of type $\{k_0, k_1\}$. Note that $\mathcal{C}$ has $4^{mk_0} \times 2^{mk_1}$ codewords.

Addition in $\mathbb{F}_{2^m}$ and R is denoted by "$\oplus$" and "$+$", respectively. A vector $\boldsymbol{c} \in R^n$ is written in the form $(c^1, c^2, \ldots, c^n)$, where $c^i \in R$, and $[c^i] = [u_0^i, u_1^i]$ $(u_0^i, u_1^i \in \mathbb{F}_{2^m})$, for all $i = 1, 2, \ldots, n$. As stated in [7], three operations "$\odot$", "$\oplus$" and "$\circledast$" are introduced as follows; if $a = a_0 + a_1\bar{\xi} + \cdots + a_{m-1}\bar{\xi}^{m-1}$ and $b = b_0 + b_1\bar{\xi} + \cdots + b_{m-1}\bar{\xi}^{m-1}$ belong to $\mathbb{F}_{2^m}$,

where $a_0, a_1, \ldots, a_{m-1}$, $b_0, b_1, \ldots, b_{m-1} \in \mathbb{F}_2$, then we have

$$a \odot b = a_0 b_0 + a_1 b_1 \bar{\xi} + \cdots + a_{m-1} b_{m-1} \bar{\xi}^{m-1},$$
$$a \oplus b = a_0 \oplus b_0 + (a_1 \oplus b_1)\bar{\xi} + \cdots + (a_{m-1} \oplus b_{m-1})\bar{\xi}^{m-1}.$$

One can see that $a \odot b = b \odot a$, $a \odot a = a$, and $a \oplus a = 0$. We extend the application of the operations "$\odot$" and "$\oplus$" on $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}^n$ in the natural way; that is, if $\boldsymbol{a} = (u^1, u^2, \ldots, u^n), \boldsymbol{b} = (v^1, v^2, \ldots, v^n) \in \mathbb{F}_{2^m}^n$, then $\boldsymbol{a} \odot \boldsymbol{b} = (u^1 \odot v^1, u^2 \odot v^2, \ldots, u^n \odot v^n)$, $\boldsymbol{a} \oplus \boldsymbol{b} = (u^1 \oplus v^1, u^2 \oplus v^2, \ldots, u^n \oplus v^n)$. Also, if $c = a_0 + a_1\xi + \cdots + a_{m-1}\xi^{m-1}$ and $c' = a'_0 + a'_1\xi + \cdots + a'_{m-1}\xi^{m-1}$ belong to R, where $a_i = a_{i0} + 2a_{i1}, a'_i = a'_{i0} + 2a'_{i1} \in \mathbb{Z}_4$ for $i = 0, \ldots, m-1$, then we have

$$c \odot c' = a_0 \odot a'_0 + (a_1 \odot a'_1)\xi + \cdots + (a_{m-1} \odot a'_{m-1})\xi^{m-1},$$
$$c \oplus c' = a_0 \oplus a'_0 + (a_1 \oplus a'_1)\xi + \cdots + (a_{m-1} \oplus a'_{m-1})\xi^{m-1},$$
$$c \circledast c' = 2(a_{00}a'_{00} + a_{10}a'_{10}\xi + \cdots + a_{(m-1)0}a'_{(m-1)0}\xi^{m-1}).$$

It is easy to see that $c \odot c' = c' \odot c$ and $c \odot c = c$. The operations "$\odot$", "$\oplus$" and "$\circledast$" can be extended to R^n in an obvious way; in other words, for $\boldsymbol{c} = (u^1, u^2, \ldots, u^n), \boldsymbol{c'} = (v^1, v^2, \ldots, v^n) \in R^n$, we have $\boldsymbol{c} \odot \boldsymbol{c'} = (u^1 \odot v^1, u^2 \odot v^2, \ldots, u^n \odot v^n)$, $\boldsymbol{c} \oplus \boldsymbol{c'} = (u^1 \oplus v^1, u^2 \oplus v^2, \ldots, u^n \oplus v^n)$ and $\boldsymbol{c} \circledast \boldsymbol{c'} = (u^1 \circledast v^1, \ldots, u^n \circledast v^n)$.

In [17], the necessary and sufficient conditions for the existence of kernels of all possible sizes for nonlinear perfect binary codes are given. The rank and dimension of the kernel for some families of binary $\mathbb{Z}_4$-linear codes, which are the corresponding binary codes of quaternary linear codes, have been studied, see [3, 5, 4, 14, 19]. Moreover, in [8], by giving lower and upper bounds, the rank and dimension of the kernel for binary $\mathbb{Z}_4$-linear codes have been investigated. Furthermore, the rank of a $\mathbb{Z}_8$-linear Hadamard code, which is the Gray image of a $\mathbb{Z}_8$-linear code, has been computed, see [10]. Also, the kernel of a $\mathbb{Z}_{2^s}$-linear Hadamard code, which is the Gray image of a $\mathbb{Z}_{2^s}$-linear code, has been studied, see [9]. Recently, the kernel and its dimension of $\mathbb{Z}_{p^s}$-linear GH codes have been computed in [2]. The purpose of this paper is to study of the rank and the dimension of the kernel of the Homogeneous Gray image of R-linear codes. The paper is organized as follows. We recall some properties related to R-linear codes in Section 2. In Section 3, we determine all possible values of the rank for R-linear codes and prove the existence of an R-linear code with rank r for all possible values of r. Finally, in Section 4, we establish all possible

values of the dimension of the kernel for R-linear codes and prove the existence of an R-linear code whose kernel has dimension k for all possible values of k.

2. **Preliminaries**

A linear code $\mathcal{C}$ of length n and type $\{k_0, k_1\}$ over R can also be seen as a R-submodule of R^n. Although $\mathcal{C}$ is not a free module in general, every codeword can be uniquely expressed in the form $\sum_{j=1}^{k_0} \mu_j \boldsymbol{v}_j + \sum_{i=1}^{k_1} \lambda_i \boldsymbol{u}_i$, where $\mu_j \in R$, for $1 \leq j \leq k_0$ and $\lambda_i \in \mathbb{F}_{2^m}$, for $1 \leq i \leq k_1$ and $\boldsymbol{v}_j$ and $\boldsymbol{u}_i$ are vectors in R^n of order four and two, respectively.

A matrix G is called a generator matrix for $\mathcal{C}$ if the rows of G span $\mathcal{C}$ and none of them can be written as a linear combination of the other rows of G. A linear code of length n over R is permutation equivalent to a code whose generator matrix $\mathcal{G}$ has the form

$$\mathcal{G} = \begin{bmatrix} I_{k_0} & A & B \\ 0 & 2I_{k_1} & 2F \end{bmatrix}_{(k_0+k_1)\times n}, \tag{2.1}$$

where A and F have entries only from $\mathbb{F}_{2^m}$, and B has entries from R, see [12, 6, 11].

The following lemmas will be used in the next two sections.

Lemma 2.1 ([7]). *For all $\boldsymbol{X}, \boldsymbol{Y} \in R^n$, we have $\Phi(\boldsymbol{X}+\boldsymbol{Y}) = \Phi(\boldsymbol{X}) \oplus \Phi(\boldsymbol{Y}) \oplus \Phi(\boldsymbol{X} \circledast \boldsymbol{Y})$.*

Lemma 2.2 ([7]). *Let $\boldsymbol{X}, \boldsymbol{Y} \in R^n$. Then $\Phi(\boldsymbol{X}+\boldsymbol{Y}+2(\boldsymbol{X} \odot \boldsymbol{Y})) = \Phi(\boldsymbol{X}) \oplus \Phi(\boldsymbol{Y})$.*

Lemma 2.3 ([7]). *Let $\mathcal{C}$ be a linear code of length n over R. Then, $\Phi(\mathcal{C})$ is a linear code if and only if $2(\boldsymbol{X} \odot \boldsymbol{Y}) \in \mathcal{C}$, for all $\boldsymbol{X}, \boldsymbol{Y} \in \mathcal{C}$.*

Lemma 2.4 ([7]). *Let $\mathcal{C}$ be a code of length n over R, $\mathcal{G}$ be a generator matrix of code $\mathcal{C}$ and $\{\boldsymbol{v}_j\}_{j=1}^{k_0}$ be the rows of order four in $\mathcal{G}$. Then, $\Phi(\mathcal{C})$ is a linear code if and only if $2(\boldsymbol{v}_t \odot \boldsymbol{v}_l) \in \mathcal{C}$, for all t, l satisfying $1 \leq t < l < k_0$.*

3. The Rank of R-Linear Codes

One of the structural properties of nonlinear binary codes is their rank. The rank of a binary code C, denoted as rank(C), is simply the dimension of $\langle C\rangle$, which is the linear span of the codewords of C. The rank for binary $\mathbb{Z}_4$-linear codes has been studied in [8]. Throughout this section, we assume that $\mathcal{C}$ is an R-linear code with length n and type $\{k_0, k_1\}$ and $C = \Phi(\mathcal{C})$ is the corresponding R-linear code with length $N = 2^m n$. In this section, we study the rank of these R-linear codes C. We also show that there exists an R-linear code C with $r = \text{rank(C)}$ for any possible value of r. First, we need the following lemmas.

Lemma 3.1. *Let* $\boldsymbol{X}_1, \boldsymbol{X}_2, \ldots, \boldsymbol{X}_t, \boldsymbol{Z} \in R^n$. *Then*

$$2((\boldsymbol{X}_1 + \boldsymbol{X}_2 + \cdots + \boldsymbol{X}_t) \odot \boldsymbol{Z}) = \sum_{i=1}^{t} 2(\boldsymbol{X}_i \odot \boldsymbol{Z}). \tag{3.1}$$

Proof. It is enough to prove (3.1) for the case $n = 1$, it can be proved for R^n in an obvious way. To prove (3.1), we apply induction on t. Let $t = 2$. Inasmuch as $X_1, X_2, Z \in R$, there are $a_0, a_1, \ldots, a_{m-1}$, $b_0, b_1, \ldots, b_{m-1}, c_0, c_1, \ldots, c_{m-1} \in \mathbb{Z}_4$ such that

$$\begin{aligned} X_1 &= a_0 + a_1\xi + \cdots + a_{m-1}\xi^{m-1}, \\ X_2 &= b_0 + b_1\xi + \cdots + b_{m-1}\xi^{m-1}, \\ Z &= c_0 + c_1\xi + \cdots + c_{m-1}\xi^{m-1}. \end{aligned}$$

First we show that, for every $u, v, w \in \mathbb{Z}_4$, $2((u+v)\odot w) = 2(u\odot w)\oplus 2(v\odot w)$. Suppose that the binary expansions of u, v and w over $\mathbb{Z}_4$ are as follows:

$$\begin{aligned} u &= u_0 + 2u_1, \\ v &= v_0 + 2v_1, \\ w &= w_0 + 2w_1. \end{aligned}$$

Then $[u + v] = [u_0 \oplus v_0, u_1 \oplus v_1 \oplus u_0v_0]$. By applying the operation "$\odot$", we have

$$[(u + v) \odot w] = [(u_0 \oplus v_0)w_0, (u_1 \oplus v_1 \oplus u_0v_0)w_1].$$

Multiplying the above expression by 2, we obtain

$$\begin{aligned}[2((u+v)\odot w)] &= [0,(u_0\oplus v_0)w_0] = [0,u_0w_0\oplus v_0w_0] = [0,u_0w_0]\oplus[0,v_0w_0]\\ &= [2(u\odot w)]\oplus[2(v\odot w)].\end{aligned}$$

Consequently $2((u+v)\odot w) = 2(u\odot w)\oplus 2(v\odot w)$. Thus

$$2((X_1+X_2)\odot Z) = 2(X_1\odot Z)\oplus 2(X_2\odot Z).$$

Assume that the induction hypothesis hold for $t=k-1$, i.e.,

$$2(X_1+X_2+\cdots+X_{k-1})\odot Z = \sum_{i=1}^{k-1} 2(X_i\odot Z).$$

For $t=k$, by case $t=2$ and induction hypothesis, we have

$$\begin{aligned}2((X_1+X_2+\cdots+X_{k-1}+X_k)\odot Z) &= 2((X_1+X_2+\cdots+X_{k-1})\odot Z)\oplus 2(X_k\odot Z)\\ &= \sum_{i=1}^{k-1} 2(X_i\odot Z)\oplus 2(X_k\odot Z)\\ &= \sum_{i=1}^{k} 2(X_i\odot Z).\end{aligned}$$

□

Lemma 3.2. *Let $\mathcal{C}$ be a linear code of type $\{k_0,k_1\}$ over R and let $C=\Phi(\mathcal{C})$ be its corresponding code. Let $\mathcal{G}$ be a generator matrix of $\mathcal{C}$ and let $\{\boldsymbol{u}_i\}_{i=1}^{k_1}$ and $\{\boldsymbol{v}_j\}_{j=1}^{k_0}$ be the rows of order two and four in $\mathcal{G}$, respectively. Then, $\langle C\rangle$ is generated by $\{\Phi(\boldsymbol{u}_i)\}_{i=1}^{k_1}$, $\{\Phi(\boldsymbol{v}_j)\}_{j=1}^{k_0}$, $\{\Phi(2\boldsymbol{v}_j)\}_{j=1}^{k_0}$ and $\{\Phi(2(\boldsymbol{v}_l\odot\boldsymbol{v}_k))\}_{1\le l<k\le k_0}$.*

Proof. If $\boldsymbol{x}\in\mathcal{C}$, then $\boldsymbol{x}$ can be expressed as $\boldsymbol{x}=\boldsymbol{v}_{j_1}+\cdots+\boldsymbol{v}_{j_t}+\boldsymbol{w}$, where $\{j_1,\ldots,j_t\}\subseteq\{1,\ldots,k_0\}$ and $\boldsymbol{w}$ is a codeword of order two. By Lemma 2.1, $\Phi(\boldsymbol{x})=\Phi(\boldsymbol{v}_{j_1}+\cdots+\boldsymbol{v}_{j_t})\oplus\Phi(\boldsymbol{w})$. Now, by induction on t, we prove that

$$\Phi(\boldsymbol{v}_{j_1}+\cdots+\boldsymbol{v}_{j_t})) = \sum_{i=1}^{t}\Phi(\boldsymbol{v}_{j_i}) + \sum_{1<l<k<t}\Phi(2(\boldsymbol{v}_{j_l}\odot\boldsymbol{v}_{j_k})).$$

For $t=2$, by Lemma 2.1, we have

$$\Phi(\boldsymbol{v}_1+\boldsymbol{v}_2)=\Phi(\boldsymbol{v}_1)\oplus\Phi(\boldsymbol{v}_2)\oplus\Phi(2(\boldsymbol{v}_1\odot\boldsymbol{v}_2)).$$

Assume that the induction hypothesis holds for $t-1$. For t, again by Lemma 2.1,

$$\Phi(\boldsymbol{v}_{j_1}+\cdots+\boldsymbol{v}_{j_{t-1}}+\boldsymbol{v}_{j_t})=\Phi(\boldsymbol{v}_{j_1}+\cdots+\boldsymbol{v}_{j_{t-1}})\oplus\Phi(\boldsymbol{v}_{j_t})\oplus\Phi(2((\boldsymbol{v}_{j_1}+\cdots+\boldsymbol{v}_{j_{t-1}})\odot\boldsymbol{v}_{j_t})).$$

But from (3.1), we have

$$2((\boldsymbol{v}_{j_1}+\cdots+\boldsymbol{v}_{j_{t-1}})\odot\boldsymbol{v}_{j_t})=\sum_{i=1}^{t-1}2(\boldsymbol{v}_{j_i}\odot\boldsymbol{v}_{j_t}).$$

So, Lemma 2.1 implies that $\Phi(2((\boldsymbol{v}_{j_1}+\cdots+\boldsymbol{v}_{j_{t-1}})\odot\boldsymbol{v}_{j_t}))=\sum_{i=1}^{t-1}\Phi(2(\boldsymbol{v}_{j_i}\odot\boldsymbol{v}_{j_t}))$. By the induction hypothesis (i.e., $t-1$), consequently

$$\Phi(\boldsymbol{v}_{j_1}+\cdots+\boldsymbol{v}_{j_t}))=\sum_{i=1}^{t}\Phi(\boldsymbol{v}_{j_i})+\sum_{1<l<k<t}\Phi(2(\boldsymbol{v}_{j_l}\odot\boldsymbol{v}_{j_k})).$$

On the other hand, $\Phi(\boldsymbol{w})$ is a linear combination of $\{\Phi(\boldsymbol{u}_i)\}_{i=1}^{k_1}$ and $\{\Phi(2\boldsymbol{v}_j)\}_{j=1}^{k_0}$. Therefore, $\Phi(\boldsymbol{x})$ is generator by $\{\Phi(\boldsymbol{u}_i)\}_{i=1}^{k_1}$, $\{\Phi(\boldsymbol{v}_j)\}_{j=1}^{k_0}$, $\{\Phi(2\boldsymbol{v}_j)\}_{j=1}^{k_0}$ and $\{\Phi(2(\boldsymbol{v}_l\odot\boldsymbol{v}_k))\}_{1\le l<k\le k_0}$. □

Lemma 3.3. *There exists a linear code $\mathcal{C}$ of length n and type $\{k_0,k_1\}$ if and only if*

$$k_0,k_1\ge 0,\quad n\ge 0,\quad k_0+k_1\le n. \tag{3.2}$$

Proof. Straightforward from matrix (2.1). □

Theorem 3.4. *Let n,k_0 and k_1 be integer numbers satisfying (3.2) and let $\mathfrak{R}=\{2k_0+k_1,\ldots,min(n+k_0,2k_0+k_1+\binom{k_0}{2})\}$. Then*

(*i*) *The rank of an R-linear code of length $N=2^m n$ and type $\{k_0,k_1\}$ belongs to $\mathfrak{R}$.*

(*ii*) *For each $r\in\mathfrak{R}$, there exists an R-linear code C of length $N=2^m n$ and type $\{k_0,k_1\}$ with $rank(C)=r$.*

Proof. (i) Suppose that

$$G=\begin{array}{c}\\ \boldsymbol{v}_j\\ \boldsymbol{u}_i\\ 2\boldsymbol{v}_j\\ 2(\boldsymbol{v}_l\odot\boldsymbol{v}_k)\end{array}\begin{array}{c}\\ \to\\ \to\\ \to\\ \to\end{array}\begin{bmatrix} I_{k_0} & A & B\\ 0 & 2I_{k_1} & 2F\\ 2I_{k_0} & 2A & 2B\\ 0 & 2W & 2D\end{bmatrix}.$$

Therefore, we have

$$\Phi(G) = \begin{array}{c} \\ \Phi(\boldsymbol{v}_j) \\ \Phi(\boldsymbol{u}_i) \\ \Phi(2\boldsymbol{v}_j) \\ \Phi(2(\boldsymbol{v}_l \odot \boldsymbol{v}_k)) \end{array} \begin{array}{c} \\ \to \\ \to \\ \to \\ \to \end{array} \begin{bmatrix} \Phi(I_{k_0}) & \Phi(A) & \Phi(B) \\ 0 & \Phi(2I_{k_1}) & \Phi(2F) \\ \Phi(2I_{k_0}) & \Phi(2A) & \Phi(2B) \\ 0 & \Phi(2W) & \Phi(2D) \end{bmatrix}.$$

By Lemma 3.2, $\langle C \rangle$ is generated by $\{\Phi(\boldsymbol{u}_i)\}_{i=1}^{k_1}$, $\{\Phi(\boldsymbol{v}_j)\}_{j=1}^{k_0}$, $\{\Phi(2\boldsymbol{v}_j)\}_{j=1}^{k_0}$ and $\{\Phi(2(\boldsymbol{v}_l \odot \boldsymbol{v}_k))\}_{1\leq l<k\leq k_0}$. On can see that $\mathrm{rank}(C) = 2k_0 + k_1 + r'$, where r' is the number of independent rows of block $\{\Phi(2(\boldsymbol{v}_l \odot \boldsymbol{v}_k))\}_{1\leq l<k\leq k_0}$. Note that, by elementary row operations, the matrix generator of $\langle C \rangle$ is

$$\Phi(G) = \begin{bmatrix} \Phi(I_{k_0}) & \Phi(A) & \Phi(B) \\ 0 & \Phi(2I_{k_1}) & \Phi(2F) \\ \Phi(2I_{k_0}) & \Phi(2A) & \Phi(2B) \\ 0 & 0 & H \end{bmatrix},$$

where the number of columns of H is $n - k_0 - k_1$. On the other hand, the number of rows of H is $\binom{k_0}{2}$, such that probably some of them are zero. Then the number of non-zero rows of H is less than or equal to $\binom{k_0}{2}$. Since column rank and row rank are equal, so, the number of independent rows of H is at most $min(n - k_0 - k_1, \binom{k_0}{2})$. Therefore, $r' \in \{0, \ldots, min(n - k_0 - k_1, \binom{k_0}{2})\}$. Thus $\mathrm{rank}(C) \in \{2k_0 + k_1, \ldots, min(n + k_0, 2k_0 + k_1 + \binom{k_0}{2})\}$.

(ii) Let $\mathcal{C}$ be a code of length n and type $\{k_0, k_1\}$ with generator matrix

$$\mathcal{G} = \underset{(k_0+k_1)\times n}{\begin{bmatrix} I_{k_0} & 0 & B_r \\ 0 & 2I_{k_1} & 2F \end{bmatrix}},$$

where B_r is a matrix of size $k_0 \times (n-k_0-k_1)$, and F is an arbitrary matrix over $\mathbb{F}_{2^m}$ of size $k_1 \times (n-k_0-k_1)$. Assume that $C = \Phi(\mathcal{C})$ be its corresponding R-linear code. Let $\{\boldsymbol{u}_i\}_{i=1}^{k_1}$ and $\{\boldsymbol{v}_j\}_{j=1}^{k_0}$ be the row vectors of order two and four in $\mathcal{G}$, respectively. By Part (i), $\mathrm{rank}(C) = 2k_0 + k_1 + r'$, where $r' \in \{0, \ldots, min(n - k_0 - k_1, \binom{k_0}{2})\}$. In the generator matrix $\mathcal{G}$, the Homogeneous Gray image of the k_1 row vectors $\{\boldsymbol{u}_i\}_{i=1}^{k_1}$ and the $2k_0$ row vectors $\{\boldsymbol{v}_j\}_{j=1}^{k_0}$, $\{2\boldsymbol{v}_j\}_{j=1}^{k_0}$ are independent vectors over $\mathbb{F}_{2^m}$. For any $r' \in \{0, \ldots, min(n - k_0 - k_1, \binom{k_0}{2})\}$, we construct B_r in an appropriate way such that $\mathrm{rank}(C) = 2k_0 + k_1 + r'$.

Suppose that $e_i(t)$ denotes the column vector of length k_0, with a t in the ith coordinate and zeroes elsewhere. For each $r' \in \{0, \ldots, min(n-k_0-k_1, \binom{k_0}{2})\}$, we can construct B_r as a matrix where r' columns there are r' different column vectors $e_l(1)+e_k(1)$ of length k_0, $1 \leq l < k \leq k_0$, and in the remaining columns there is the all-zero column vector. For each one of the r' different column vectors the rank increases by 1. Note that, if the column vector $e_l(1)+e_k(1)$ is included in B_r, then the vector $2(\boldsymbol{v}_l \odot \boldsymbol{v}_k)$ has only a two in the same coordinate where the column vector $e_l(1)+e_k(1)$ is, and $\Phi(2(\boldsymbol{v}_l \odot \boldsymbol{v}_k))$ is independent to the vectors $\{\Phi(\boldsymbol{u}_i)\}_{i=1}^{k_1}$, $\{\Phi(\boldsymbol{v}_j)\}_{j=1}^{k_0}$, $\{\Phi(2\boldsymbol{v}_j)\}_{j=1}^{k_0}$ and $\Phi(2(\boldsymbol{v}_s \odot \boldsymbol{v}_t))$, $\{s,t\} \neq \{l,k\}$. Inasmuch as the maximum number of columns of B_r is $n-k_0-k_1$ and the maximum number of different such columns is $\binom{k_0}{2}$, the result follows.

□

Example 3.5. Let $R = GR(4,2) = \mathbb{Z}_4[\xi]$, where $h(\xi) = 0$ and $h(x) = x^2+x+1$ is a basic irreducible polynomial over $\mathbb{Z}_4$. Suppose that $\mathcal{C}$ is a code of length 10 and type $\{5,3\}$. It follows from Theorem 3.4 part (i), the possible ranks for R-linear codes, $C = \Phi(\mathcal{C})$, of length 40 and type $\{5,3\}$ are $\text{rank}(C) = r \in \{13,14,15\}$. By Theorem 3.4 part (ii), for each possible r, we can construct a code C with $\text{rank}(C) = r$, taking the following generator matrix of $\mathcal{C}$:

$$\mathcal{G} = \begin{bmatrix} I_5 & 0 & B_r \\ 0 & 2I_3 & 2F \end{bmatrix}_{8\times 10}.$$

B_{13}, B_{14} and B_{15} are constructed as follows:

$$B_{13} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}_{5\times 2}, \quad B_{14} = \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}_{5\times 2}, \quad B_{15} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}_{5\times 2}.$$

Example 3.6. Let $R = GR(4,3) = \mathbb{Z}_4[\xi]$, where $h(\xi) = 0$ and $h(x) = x^3+2x^2+x-1$ is a basic irreducible polynomial over $\mathbb{Z}_4$. Assume that $\mathcal{C}$ is a code of length 9 and type $\{4,4\}$. It follows from Theorem 3.4 part (i), the possible ranks for R-linear codes, $C = \Phi(\mathcal{C})$, of length 72 and type $\{4,4\}$ are $\text{rank}(C) = r \in \{12,13\}$. By Theorem 3.4 part (ii), for each

possible r, we can construct a code C with $\text{rank}(C) = r$, taking the following generator matrix of $\mathcal{C}$:

$$\mathcal{G} = \begin{bmatrix} I_4 & 0 & B_r \\ 0 & 2I_4 & 2F \end{bmatrix}_{8\times 9}.$$

B_{12} and B_{13} are constructed as follows:

$$B_{12} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}_{5\times 1}, \qquad B_{13} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}_{5\times 1}.$$

4. The Dimension of the Kernel of R-Linear Codes

Another structural property of nonlinear binary codes is their dimension of the kernel. The kernel of a binary code C, $\mathrm{K}(C)$, is the set of vectors that leave C invariant under translation, i.e., $\mathrm{K}(C) = \{\boldsymbol{x} \in \mathbb{Z}_2^n | \, \boldsymbol{x} \oplus C = C\}$. If the all-zero vector belongs to C, then $\mathrm{K}(C)$ is a linear subcode of C. Moreover, C can be written as the union of cosets of $\mathrm{K}(C)$, see [1]. Recall that the dimension of the kernel for binary $\mathbb{Z}_4$-linear codes has been studied in [8]. Let $q = p^r$, where p is prime. As stated in [18], the kernel of a q-ary code C over $\mathbb{F}_q$ is $\mathrm{K}_q(C) = \{\boldsymbol{x} \in \mathbb{F}_q^n | \, \lambda\boldsymbol{x} \oplus C = C, \forall \lambda \in \mathbb{F}_q\}$, and the p-kernel of a q-ary code C over $\mathbb{F}_q$ is $\mathrm{K}_p(C) = \{\boldsymbol{x} \in \mathbb{F}_q^n | \, \boldsymbol{x} \oplus C = C\}$. Also, if the zero codeword is in C, then $\mathrm{K}_q(C)$ is a linear subcode of C and $\mathrm{K}_p(C)$ is a p-linear subcode of C. The dimension of the kernel and p-kernel of C is denoted by $\mathrm{k}_q(C)$ and $\mathrm{k}_p(C)$, respectively. Furthermore, the code C is a union of cosets of $\mathrm{K}_q(C)(\mathrm{K}_p(C))$, and $\mathrm{K}_q(C)(\mathrm{K}_p(C))$ is the maximal linear subspace of $\mathbb{F}_q^n$ over $\mathbb{F}_q(\mathbb{F}_p)$ with this property. According to what was said in section 3, throughout this section let $\mathcal{C}$ be an R-linear code of length n and type $\{k_0, k_1\}$ and $C = \Phi(\mathcal{C})$ is the corresponding R-linear code of length $N = 2^m n$. In this section, we investigate the dimension of the kernel of R-linear codes $C = \Phi(\mathcal{C})$. We also show that there exists an R-linear code C with $k = \mathrm{k}_{2^m}(C)$ for any possible value of k. To do this, we first express the following lemma.

Lemma 4.1. *Let $\mathcal{C}$ be a linear code over R and $C = \Phi(\mathcal{C})$ be its corresponding code over $\mathbb{F}_{2^m}$. Then, $K_{2^m}(C) = \{\Phi(\boldsymbol{u}) \mid \boldsymbol{u} \in \mathcal{C}$ and $2(\boldsymbol{u} \odot \boldsymbol{v}) \in \mathcal{C}, \forall \ \boldsymbol{v} \in \mathcal{C}\}$.*

Proof. By Lemma 2.2, for $\boldsymbol{u}, \boldsymbol{v} \in R$, we have $\Phi(\boldsymbol{u} + \boldsymbol{v} + 2(\boldsymbol{u} \odot \boldsymbol{v})) = \Phi(\boldsymbol{u}) \oplus \Phi(\boldsymbol{v})$. Therefore, $\Phi(\boldsymbol{u}) \oplus \Phi(\boldsymbol{v}) \in C$ if and only if $2(\boldsymbol{u} \odot \boldsymbol{v}) \in \mathcal{C}$ for all $\boldsymbol{u}, \boldsymbol{v} \in \mathcal{C}$. So, the result follows. □

Note that if $\mathcal{G}$ is a generator matrix of a linear code $\mathcal{C}$ over R and $C = \Phi(\mathcal{C})$, by Lemmas 4.1 and 3.1, $\Phi(\boldsymbol{u}) \in \mathrm{K}_{2^m}(C)$ if and only if $\boldsymbol{u} \in \mathcal{C}$ and $2(\boldsymbol{u} \odot \boldsymbol{v}) \in \mathcal{C}$ for all $\boldsymbol{v} \in \mathcal{G}$. Also, if $\boldsymbol{u} \in \mathcal{C}$ and $\mathrm{ord}(\boldsymbol{u}) = 2$, then $2\boldsymbol{u} = 0$, from Lemma 4.1, all codewords of order two in $\mathcal{C}$ belong to $\mathrm{K}_{2^m}(C)$.

Lemma 4.2. *Let $\mathcal{C}$ be a linear code over R and $C = \Phi(\mathcal{C})$ be its corresponding code over $\mathbb{F}_{2^m}$. For each $\boldsymbol{u}, \boldsymbol{v} \in \mathcal{C}$, we have $\Phi(\boldsymbol{u}) \oplus \Phi(\boldsymbol{v}) \in K_{2^m}(C)$ if and only if $\Phi(\boldsymbol{u} + \boldsymbol{v}) \in K_{2^m}(C)$.*

Proof. By Lemma 2.2, we have $\Phi(\boldsymbol{u} + \boldsymbol{v} + 2(\boldsymbol{u} \odot \boldsymbol{v})) = \Phi(\boldsymbol{u}) \oplus \Phi(\boldsymbol{v})$. In other words, by Lemma 4.1, $\Phi(\boldsymbol{u} + \boldsymbol{v} + 2(\boldsymbol{u} \odot \boldsymbol{v})) \in \mathrm{K}_{2^m}(C)$ if and only if for all $\boldsymbol{w} \in \mathcal{C}$, $2((\boldsymbol{u} + \boldsymbol{v} + 2(\boldsymbol{u} \odot \boldsymbol{v})) \odot \boldsymbol{w}) = 2((\boldsymbol{u} + \boldsymbol{v}) \odot \boldsymbol{w}) \in \mathcal{C}$, and this means; $\Phi(\boldsymbol{u} + \boldsymbol{v}) \in \mathrm{K}_{2^m}(C)$. Consequently, $\Phi(\boldsymbol{u}) \oplus \Phi(\boldsymbol{v}) \in \mathrm{K}_{2^m}(C)$ if and only if $\Phi(\boldsymbol{u} + \boldsymbol{v}) \in \mathrm{K}_{2^m}(C)$. □

Theorem 4.3. *Let n, k_0 and k_1 be integer numbers satisfying (3.2) and let $\mathfrak{K} = \{k_0 + k_1, \ldots, 2k_0 + k_1 - 2, 2k_0 + k_1\}$. Then*

(*i*) *The dimension of the kernel of an R-linear code of length $N = 2^m n$ and type $\{k_0, k_1\}$ belongs to $\mathfrak{K}$.*

(*ii*) *There exists an R-linear code C of length $N = 2^m n$ and type $\{k_0, k_1\}$ with $k_{2^m}(C) = k$ for any*

$$k \in \begin{cases} \{2k_0 + k_1\} & \text{if } s = 0, \\ \{k_1 + 2(k_0 - \lceil \frac{k_0 - 1}{2} \rceil), \ldots, k_1 + 2(k_0 - 1), 2k_0 + k_1\} & \text{if } s = 1, \\ \{k_0 + k_1, k_0 + k_1 + 1, \ldots, 2k_0 + k_1 - 2, 2k_0 + k_1\} & \text{if } s \geq 2, \end{cases}$$

where $s = n - k_0 - k_1$.

Proof. (i) The upper bound $2k_0 + k_1$ comes from the linear case. Inasmuch as, there are $(2^m)^{k_0 + k_1}$ codewords of order two in $\mathcal{C}$, Lemma 4.1 implies that the Homogeneous Gray images of all these codewords are in $\mathrm{K}_{2^m}(C)$. Furthermore, note that if C is

not linear, then by Lemma 2.3 the dimension of the kernel is equal to or less than $2k_0 + k_1 - 2$. Thus, $\mathrm{k}_{2^m}(C) \in \{k_0 + k_1, \ldots, 2k_0 + k_1 - 2, 2k_0 + k_1\}$.

(ii) Let $\mathcal{C}$ be an R-linear code of length n and type $\{k_0, k_1\}$ with generator matrix

$$\mathcal{G} = \begin{bmatrix} I_{k_0} & 0 & B_k \\ 0 & 2I_{k_1} & 0 \end{bmatrix}_{(k_0+k_1)\times n},$$

where B_k is a matrix of size $k_0 \times (n-k_0-k_1)$ and let $C = \Phi(\mathcal{C})$ be its corresponding R-linear code. If $n = k_0 + k_1$, then the code C is a linear code over $\mathbb{F}_{2^m}$. Thus, $\mathrm{k}_{2^m}(C) = k = 2k_0 + k_1$.

When $n = k_0 + k_1 + 1$, for every $k' \in \{2, 4, \ldots, 2\left\lceil \frac{k_0-1}{2} \right\rceil\}$ and $k = 2k_0 + k_1 - k'$, we can construct a matrix B_k over R of size $k_0 \times 1$ with an even number of ones, k', and zeros elsewhere. In this case, it is easy to see that $\mathrm{k}_{2^m}(C) = k = 2k_0 + k_1 - k'$.

Finally, when $n \geq k_0 + k_1 + 2$, for each $k' \in \{2, 3, \ldots, k_0\}$ and $k = 2k_0 + k_1 - k'$, we can construct a matrix B_k over R of size $k_0 \times s$, such that only in the last $k_0 - k'$ row vectors all components are zero and, furthermore, in the first k' coordinates of each column vector there are an even number of ones and zeros elsewhere. In this case, it is easy to check that $\mathrm{k}_{2^m}(C) = k = 2k_0 + k_1 - k'$.

□

Let t be a positive integer. Let $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_t\}$ be a set of vectors in R^n and $I = \{i_1, \ldots, i_l\} \subseteq \{1, \ldots, t\}$. The vector $\boldsymbol{v}_{i_1} + \cdots + \boldsymbol{v}_{i_l}$ is denoted by $\boldsymbol{v}_I$. Also if $I = \emptyset$, we have $\boldsymbol{v}_I = \boldsymbol{0}$.

Proposition 4.4. *Let $\mathcal{C}$ be a linear code of type $\{k_0, k_1\}$ with generator matrix $\mathcal{G}$, and suppose that $C = \Phi(\mathcal{C})$ be its corresponding code with $k_{2^m}(C) = 2k_0 + k_1 - k'$, where $k' \in \{2, \ldots, k_0\}$. Therefore, there exists a set $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_{k'}\}$ of row vectors of order four in $\mathcal{G}$ such that*

$$C = \bigcup_{I \subseteq \{1,\ldots,k'\}} (K_{2^m}(C) + \Phi(\boldsymbol{v}_I)).$$

Note that, by Lemma 4.2, if $\mathcal{C}$ is a linear code over R, then $\mathrm{K}_{2^m}(C)$ is a subcode of C. We denote the kernel of a linear code $\mathcal{C}$ of type $\{k_0, k_1\}$ over R by $\mathcal{K}(\mathcal{C})$, and we have $\mathcal{K}(\mathcal{C}) = \Phi^{-1}(\mathrm{K}_{2^m}(C))$. Lemma 4.1, implies that $\mathcal{K}(\mathcal{C}) = \{\boldsymbol{u} \mid \boldsymbol{u} \in \mathcal{C} \text{ and } 2(\boldsymbol{u} \odot \boldsymbol{v}) \in \mathcal{C}, \forall\, \boldsymbol{v} \in \mathcal{C}\}$. It is easy to check that $\mathcal{K}(\mathcal{C})$ is a linear subcode of $\mathcal{C}$ of type $4^{mk_0-k'}2^{mk_1+k'}$.

Also, if $\mathcal{C}$ is a linear code over R with a generator matrix $\mathcal{G}$, by Proposition 4.4 there exists a set $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_{k'}\}$ of row vectors of order four in $\mathcal{G}$ such that

$$\mathcal{C} = \bigcup_{I \subseteq \{1,\ldots,k'\}} (\mathcal{K}(\mathcal{C}) + \boldsymbol{v}_I).$$

Example 4.5. Let $R = GR(4,2) = \mathbb{Z}_4[\xi]$, where $h(\xi) = 0$ and $h(x) = x^2 + x + 1$ is a basic irreducible polynomial over $\mathbb{Z}_4$. Let $\mathcal{C}$ be an R-linear code of length 9 and type $\{4,2\}$. It follows from Theorem 4.3 part (i), the possible dimensions of the kernel for R-linear codes of length 36 and type $\{4,2\}$ are $\mathrm{k}_{2^m}(C) = k \in \{6,7,8,10\}$. By Theorem 4.3 part (ii), for each possible k, we can construct a code C with $\mathrm{k}_{2^m}(C) = k$, taking the following generator matrix of $\mathcal{C}$:

$$\mathcal{G} = \begin{bmatrix} I_4 & 0 & B_k \\ 0 & 2I_2 & 0 \end{bmatrix}_{6\times 9},$$

where B_{10}, B_8, B_7 and B_6 are constructed as follows:

$$B_{10} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}_{4\times 3}, \quad B_8 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}_{4\times 3}, \quad B_7 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}_{4\times 3}, \quad B_6 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}_{4\times 3}.$$

Example 4.6. Let $R = GR(4,3) = \mathbb{Z}_4[\xi]$, where $h(\xi) = 0$ and $h(x) = x^3 + 2x^2 + x - 1$ is a basic irreducible polynomial over $\mathbb{Z}_4$. Let $\mathcal{C}$ be an R-linear code of length 10 and type $\{5,1\}$. It follows from Theorem 4.3 part (i), the possible dimensions of the kernel for R-linear codes of length 80 and type $\{5,1\}$ are $\mathrm{k}_{2^m}(C) = k \in \{6,7,8,9,11\}$. By Theorem 4.3 part (ii), for each possible k, we can construct a code C with $\mathrm{k}_{2^m}(C) = k$, taking the following generator matrix of $\mathcal{C}$:

$$\mathcal{G} = \begin{bmatrix} I_5 & 0 & B_k \\ 0 & 2I_1 & 0 \end{bmatrix}_{6\times 10},$$

where B_{11}, B_9, B_8, B_7 and B_6 are constructed as follows:

$$B_{11} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}_{5\times 4}, \quad B_9 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}_{5\times 4}, \quad B_8 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}_{5\times 4},$$

$$B_7 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}_{5\times 4}, \quad B_6 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}_{5\times 4}.$$

5. **Conclusion**

For an R-linear code C of length $N = 2^m n$ and type $\{k_0, k_1\}$, by establishing lower and upper bounds, we studied the rank and dimension of the kernel of the R-linear code $C = \Phi(\mathcal{C})$. We also gave the construction of an R-linear code with rank r (resp. dimension of the kernel k) for each possible value r (resp. k). As a future research, it would be interesting to establish the bounds of the rank, once the dimension of the kernel is fixed, and give the construction of an R-linear code with rank r and kernel dimension k for each possible pair (r, k) or interesting to establish the bounds of the kernel, once the dimension of the rank is fixed, and give the construction of an R-linear code with rank r and kernel dimension k for each possible pair (r, k) or interesting to study lower and upper bounds for the rank and dimension of the kernel of the $GR(2^s, m)$-linear (for $s > 2$) code $C = \Phi(\mathcal{C})$.

Acknowledgments

The authors thank the anonymous referees for their valuable comments, which enabled them to improve the quality of the paper.

References

[1] Bauer, H., Ganter, B. and Hergert, F., 1983. Algebraic techniques for nonlinear codes. *Combinatorica 3*, pp.21–33. doi: 10.1007/BF02579339

[2] Bhunia, D. K., Fernández-Córdoba, C. and Villanueva, M., 2022. On the linearity and classification of $\mathbb{Z}_{p^s}$-linear generalized hadamard codes. *Des. Codes Cryptogr, 90*(4), pp.1037–1058. doi: 10.1007/s10623-022-01026-2

[3] Borges, J. Fernández, C. and Phelps, K.T., 2005. Quaternary Reed-Muller codes. *IEEE Trans. Inf. Theory, 51*(7), pp.2686–2691. doi: 10.1109/TIT.2005.850148

[4] Borges, J., Phelps, K.T. and Rifà, J., 2003. The rank and kernel of extended 1-perfect $\mathbb{Z}_4$-linear and additive non-$\mathbb{Z}_4$-linear codes. *IEEE Trans. Inf. Theory, 49*(8), pp.2028–2034. doi: 10.1109/TIT.2003.814490

[5] Borges, J., Phelps, K.T., Rifà, J. and Zinoviev, V.A., 2003. On $\mathbb{Z}_4$-linear Preparata-like and Kerdock-like codes. *IEEE Trans. Inf. Theory, 49*(11), pp.2834–2843. doi: 10.1109/TIT.2003.819329

[6] Calderbank, A. R. and Sloane, N. J. A., 1995. Modular and p-adic cyclic codes. *Des. Codes Cryptogr, 6*(1), pp.21–35. doi: 10.1007/BF01390768

[7] Eyvazi, H., Samei, K. and Savari, B., 2023. The Homogeneous Gray image of linear codes over the Galois ring $GR(4, m)$. *Cryptogr. Commun, 16*, pp.531-540. doi: 10.1007/s12095-023-00683-x

[8] Fernández-Córdoba, C., Pujol, J. and Villanueva, M., 2008. On rank and kernel $\mathbb{Z}_4$-linear codes. *LNCS*, pp.46–55. doi: 10.1007/978-3-540-87448-5_6

[9] Fernández-Córdoba, C., Vela, C. and Villanueva, M., 2019. On $\mathbb{Z}_{2^s}$-linear Hadamard codes, kernel and partial classification. *Des. Codes Cryptogr, 87*, pp.417–435. doi: 10.1007/s10623-018-0546-6

[10] Fernández-Córdoba, C., Vela, C. and Villanueva, M., 2020. On $\mathbb{Z}_8$-linear Hadamard codes, rank and classification. *IEEE Trans. Inf. Theory, 66*(2), pp.970–982. doi: 10.1109/TIT.2019.2952599

[11] Gupta, M. K., Bhandari, M. C. and Lal, A. K., 2005. On linear codes over $\mathbb{Z}_{2^s}$. *Des. codes Cryptogr, 36*(3), pp.227–244. doi: 10.1007/s10623-004-1717-1

[12] Huffman, W. C., 1998. Decompositions and extremal type II codes over $\mathbb{Z}_4$, *IEEE Trans. Inf. Theory, 44*, pp.800–809. doi: 10.1109/18.661525

[13] Jitman, S. and Udomkavanich, P., 2010. The Gray image of codes over finite chain rings. *Int. J. Contemp. Math. Sciences, 5*(10), pp.449–458. doi: 10.48550/arXiv.0907.3397

[14] Krotov, D. S., 2001. $\mathbb{Z}_4$-Linear Hadamard and extended perfect codes. *Electron. Notes Discret. Math, 6*, pp.107–112. doi: 10.1016/S1571-0653(04)00161-1

[15] McDonald, B. R., 1974. Finite rings with identity. *PAMJ, Marcel Dekker Inc, New York*. doi: /SO166-218X(18)30087-8/sb12

[16] Norton, G. H. and Sălăgean, A., 2000. On the hamming distance of linear codes over a finite chain ring. *IEEE Trans. Inf. Theory, 46*(3), pp.1060–1067. doi: 10.1109/18.841186

[17] Phelps, K.T. and Levan, M., 1995. Kernels of nonlinear Hamming codes. *Des. Codes Cryptogr, 6*(3), pp.247–257. doi: 10.1007/BF01388478

[18] Phelps, K.T., Rifà, J. and Villanueva, M., 2005. Kernels and p-kernels of p^r-ary 1-perfect Codes. *Des. Codes Cryptogr, 37*, pp.243–261. doi: 10.1007/s10623-004-3989-x

[19] Phelps, K.T., Rifà, J. and Villanueva, M., 2006. On the additive ($\mathbb{Z}_4$-linear and non-$\mathbb{Z}_4$-linear) Hadamard codes: rank and kernel. *IEEE Trans. Inf. Theory, 52*(1), pp.316–319. doi: 10.1109/TIT.2005.860464

[20] Qain, J. F., Ma, W. and Wang, X., 2008. On the Gray image of cyclic codes over finite chain rings. *IEICE Tran. Elec, EA91-A*, pp.2685–2687. doi: 10.1093/ietfec/e91-a.9.2685

[21] Tapia-Recillas, H. and Vega, G., 2003. On $\mathbb{Z}_{2^k}$-linear and quaternary codes. *SIAM J. Discr. Math, 17*(1), pp.103–113. doi: 10.1137/S0895480101397219

[22] Wan, Z. X., 1999. Cyclic codes over Galois rings. *Algebra Colloq, 6*(3), pp.291–304. doi: 10.1007/BF02574846

[23] Wan, Z. X., 2003.Lectures on finite fields and Galois rings. *World Scientific, Singapore*. doi: 10.1142/5350

[24] Wan, Z. X., 1997. Quaternary codes. *World Scientific, Singapore*. doi: 10.1142/3603

Tahereh Aghighi
Department of Mathematics,
Faculty of Mathematical Sciences,
Bu Ali Sina University of Hamedan,
Hamedan, Iran
Email: t.aghighi@sci.basu.ac.ir

Hamidreza Eyvazi
Department of Mathematics,
Faculty of Mathematical Sciences,
Bu Ali Sina University of Hamedan,
Hamedan, Iran
Email: h.eyvazi@sci.basu.ac.ir

Karim Samei
Department of Mathematics,
Faculty of Mathematical Sciences,
Bu Ali Sina University of Hamedan,
Hamedan, Iran
Email: samei@basu.ac.ir, samei@ipm.ir

©2025 Shahid Chamran University of Ahvaz, Ahvaz, Iran. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution-NonComertial 4.0 International (CC BY-NC 4.0 license) (http://creativecommons.org/licenses/by-nc/4.0/).