Southeast-Asian J. of Sciences, Vol 1, No 1 (2012), pp. 78-100

BOUNDS ON THE P^R-ARY IMAGE OF LINEAR BLOCK CODES OVER FINITE SEMI-LOCAL FROBENIUS RING $\mathbb{F}_{p^r} + v\mathbb{F}_{p^r}$

John Mark Lampos and **Virgilio Sison**

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

Abstract

In this paper we give the structure of the p^r-ary image with respect to an ordered basis of a linear block code over the semi-local Frobenius ring $R_p = \mathbb{F}_{p^r} + v\mathbb{F}_{p^r}$, where $v^2 = v$ or 1. A homogeneous weight on R_p was constructed and distance bounds on the p^r-ary image were derived. Further we show examples of new codes that meet these bounds.

1 Introduction

A code of length n over the Galois field $\mathbb{F}_{p^r}$ induces a code of length nr over the base field $\mathbb{F}_p$ by using a basis of $\mathbb{F}_{p^r}$ over $\mathbb{F}_p$. Rabizzoni [11] used the said construction and obtained an upper bound on the minimum Hamming distance of the induced p-ary image of linear block codes over $\mathbb{F}_{p^r}$. Solé and Sison [13] generalized this result for the minimum homogeneous distance of the p^r- ary image of linear block codes over the Galois ring $GR(p^r, m)$. In their paper, they used the concept of subcodes and effective length in the formulation of the generalized bound.

The Gray map in several rings were also used to study and construct bounds on the images of codes especially binary images. The Singleton bound for a

Key words: Frobenius ring, semi-local , Plotkin bound, Rabizzoni bound.

code C of length n over an alphabet of size q with minimum hamming distance d is

$$d \leq n - log_q|C| + 1. \tag{1}$$

Dougherty and Shiromoto [7] developed a bound on the Lee weight of codes over rings of order 4 similar to the Singleton bound given in (1) using the Gray map preimages. They also gave bounds on the minimum distances based on the rank of the code. Further, codes that meet these bounds were characterized in terms of rank and distances. Zhu, Wang and Shi [15] studied the relationship between cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$ and binary cyclic codes using the Gray map on the said ring. In addition, the generator matrix of the associated binary code was derived and the Gray image of the dual of the code was also studied. Betsumiya and Harada [2] gave improved upper bounds on minimum Hamming and Lee weights of self-dual and Type IV self- dual codes over $\mathbb{F}_2 + v\mathbb{F}_2$ by using a characterization which is based on codes obtained by the Gray map and the Chinese Remainder Theorem. Further, using these bounds, they were able to determine the highest minimum Hamming and Lee weights for such codes of length up to 30. Dougherty, et. al. in [5] studied Type IV self- dual codes over the commutative rings of order 4. Several results and bounds using the Chinese Remainder Theorem and the Gray map were also presented.

Lately, codes over $R_3 = \mathbb{F}_3 + v\mathbb{F}_3, v^2 = 1$ are also gaining attention. Cengellenmis [3] made a study similar to [15] on cyclic codes over the said ring. They characterized the said codes using Gray map and the Chinese Remainder Theorem. Further, in [4], he characterized codes over $\mathbb{F}_3$ using the Gray map on R_3. He proved that if n is odd, then every code over $\mathbb{F}_3$ which is the Gray image of a linear cyclic code over R_3 of length n is permutation equivalent to a linear cyclic code.

In the present work, we consider codes over the finite semi-local Frobenius ring $R_p = \mathbb{F}_{p^r} + v\mathbb{F}_{p^r}$ where $v^2 = v$ or 1, p prime and $r \in \mathbb{N}$. The p^r- ary images of the block code were obtained by defining a map from R_p to $\mathbb{F}_{p^r}^2$ with respect to an ordered basis of R_p over $\mathbb{F}_{p^r}$. Further, we gave bounds on the minimum Hamming distance of p^r- ary images of linear block codes over R_p in terms of different parameters such as length, rank, cardinality, and minimum Hamming distance of the block code.

The material is organized as follows. Section 2 gives definitions and theorems that are essential in this study. Section 3 presents the main results of this study. The structural properties of the cross product $\mathbb{F}_{p^r}^2$ were studied in Section 3.1 while a discussion on the structural properties of the semi-local ring R_p can be found in Section 3.2. The Bachoc weight on $\mathbb{F}_p + v\mathbb{F}_p$ and the homogeneous weight on R_p were derived in Section 3.3. Linear block codes and subcodes over R_p and bounds on the minimum Hamming distance of the block code were presented in Section 3.4. The p^r- ary images of linear block

codes over R_p were introduced in Section 3.5 and bounds on minimum Hamming distance of these images were constructed in Section 4. The last section illustrates examples of codes that meet these bounds.

2 Preliminaries and Definitions

Throughout this discussion, we assume that R is a commutative ring with unity $1 \neq 0$ unless otherwise stated. In addition, we let p be a prime number and $r \in \mathbb{N}$.

2.1 The Galois field $\mathbb{F}_{p^r}$ and the Trace Map

Let $f(x)$ be an irreducible polynomial over the field $\mathbb{Z}_p$ with degree r and let α be a root of f. Then the *Galois field* $\mathbb{F}_{p^r}$ is given by the set

$$\mathbb{F}_{p^r} = \{a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_{r-1}\alpha^{r-1} \mid a_i \in \mathbb{Z}_p\}\,.$$

The field $\mathbb{F}_{p^r}$ has cardinality p^r and characteristic p.

Consider the Galois fields $\mathbb{F}_{p^r}$ and $\mathbb{F}_p$. The *trace function* tr is defined by

$$tr : \mathbb{F}_{p^r} \to \mathbb{F}_p$$

$$tr(\alpha) = \alpha + \alpha^p + ... + \alpha^{p^{r-1}}$$

for $\alpha \in \mathbb{F}_{p^r}$.

It is a fact that for any $x, y \in \mathbb{F}_{p^r}$, $tr(x + y) = tr(x) + tr(y)$ and that tr takes on each value in $\mathbb{F}_p$ equally often, that is, p^{r-1} times.

2.2 Semi-local rings and the Chinese Remainder Theorem

For this study, we define a semi-local ring in terms of maximal ideals. A commutative ring R that has finitely many number of maximal ideals is called a *semi-local* ring. Any element of the semi-local ring R that does not belong to any one of the maximal ideals is a unit. If R has exactly one maximal ideal, then R is said to be a *local ring*. Although, by definition, a local ring is also a semi-local ring, we restrict our discussion of semi-local rings in this study to rings having more than one maximal ideals. In this study, we introduce new definitions.

Definition 1. Let R be a semi-local ring with maximal ideals I_1 and I_2. Then, R is said to be **balanced** if the following hold:

a.) $|I_1| = |I_2|$;

b.) If $x \in I_i$, then there exists $y \in I_j$, $i \neq j$ such that $xy = 0$.

Otherwise, we call R an **uneven semi-local ring**. In addition, zero divisors x and y that satisfy condition b.) are said to be **incongruent**.

Two ideals I and I' of R are *coprime* if $I + I' = R$. A set of nonzero ideals $\{I_1, I_2, \ldots, I_n\}$ in a ring R is *pairwise coprime* if $I_j + I_k = R$ for all $j, k = 1, 2, \ldots, n$, $(j \neq k)$.

We now state the Chinese Remainder Theorem (CRT) for rings which is a generalization of the Chinese Remainder Theorem from the elementary number theory.

Theorem 1. *(Hungerford,[10]) (Chinese Remainder Theorem) Let $A_1, \ldots, A_n$ be pairwise coprime ideals in a ring R. If $b_1, \ldots, b_n \in R$, then there exists $b \in R$ such that*

$$b \equiv b_i (mod A_i) \ (i = 1, 2, \ldots, n).$$

Furthermore b is uniquely determined up to congruence modulo the ideal

$$A_1 \cap A_2 \cap \ldots \cap A_n.$$

Corollary 1. *(Hungerford,[10]) If $A_1, \ldots, A_n$ are pairwise coprime ideals in a ring R, then, as rings,*

$$R/(A_1 \cap \ldots \cap A_n) \cong R/A_1 \times R/A_2 \times \ldots \times R/A_n.$$

Since every proper nontrivial ideal in a semi-local ring is maximal, by the CRT, every semi-local ring is isomorphic to a direct product of residue fields.

2.3 Frobenius rings and homogeneous weight

Let $\mathbb{T}$ be the multiplicative group of unit complex numbers which is also a one-dimensional torus. A *character* of R (considered as an additive abelian group) is a group homomorphism $\chi : R \to \mathbb{T}$. The set of all characters $\hat{R}$, called the *character module* of R, is a right (resp. left) R-module whose group operation is pointwise multiplication of characters and scalar multiplication is given by $\chi^r(x) = \chi(rx)$ (resp. ${}^r\chi(x) = \chi(xr)$). If the mapping $\phi : R \to \hat{R}$ given by $\phi(r) = \chi^r$ (resp. $\phi(r) = {}^r\chi$) is an isomorphism of right (resp. left) R- modules, then a character χ of R is called a *right (resp. left) generating character*. It is known that for finite rings, a character χ of R is a right generating character if and only if it is a left generating character. In addition, a character χ of R is a right (resp. left) generating character if $\ker \chi$ does not contain any nonzero

right (resp. left) ideal of R [14]. The ring R is *Frobenius* if and only if $\hat{R} \cong R$ as right or left R- modules. Further, from [14], a finite ring is *Frobenius* if and only if it has a generating character.

We equip a ring R with a weight function w. If $x = (x_1, x_2, \ldots, x_n) \in R^n$, then $w(x) = \sum_{i=1}^{n} w(x_i)$. In addition, the *distance* $d(x, y)$ between two vectors $x, y \in R^n$ is defined as $d(x, y) = w(x - y)$.

A weight w on a finite ring R is called a *homogeneous weight* if it satisfies the following conditions:

(1) For all $x, y \in R$, $Rx = Ry$ implies $w(x) = w(y)$ holds.

(2) Every nonzero ideal Rx of R has the same average weight, that is, there exists a nonzero real number Γ such that

$$\sum_{y \in Rx} w(y) = \Gamma \cdot |Rx| \text{ for all } x \in R/\{0\}$$

The number Γ is the *average value* of w on R. As an example, the Hamming weight on $\mathbb{F}_{p^r}$ is a homogeneous weight with $\Gamma = \dfrac{p^r - 1}{p^r}$.

From [9], if R is Frobenius with generating character χ, then every homogeneous weight w on R is of the form:

$$w : R \longrightarrow \mathbb{R}, \quad w(x) = \Gamma \left[1 - \frac{1}{|R^\times|} \sum_{u \in R^\times} \chi(xu) \right],$$

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

2.4 Linear block codes over rings

A rate-k/n *linear block code* over R generated by a $k \times n$ matrix G over the ring R is the R-submodule given by the set $B = \{v \in R^n \mid v = uG, u \in R^k\}$. If no proper subset of the rows of G generates B, then the matrix G is called a *generator matrix* for B. If the columns of G contain the columns of the $k \times k$ identity matrix I_k, then G is said to be *systematic*. A code B is *systematic* if it has a systematic generator matrix. If the first k columns of G is I_k, then G is in *standard form*. In addition, the code B is called *free* if the rows of G are linearly independent. Two codes are said to be *equivalent* if one can be obtained from the other by permuting the coordinates. Codes that differ only by a permutation of coordinates are called *permutation- equivalent*.

From [6], any linear code over a finite ring R has a generator matrix which can be put in the following form:

$$\begin{pmatrix} a_1I_{k_1} & A_{1,2} & A_{1,3} & A_{1,4} & \dots & \dots & A_{1,s+1} \\ 0 & a_2I_{k_2} & a_2A_{2,3} & a_2A_{2,4} & \dots & \dots & a_2A_{2,s+1} \\ 0 & 0 & a_3I_{k_3} & a_3A_{3,4} & \dots & \dots & a_3A_{3,s+1} \\ \vdots & \vdots & 0 & \ddots & \ddots & & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & & \vdots \\ 0 & 0 & 0 & \dots & 0 & a_sI_{k_s} & a_sA_{s,s+1} \end{pmatrix} \tag{2}$$

where $A_{i,j}$ are matrices over R for $i = 1$ and binary matrices for $i > 1$ and $[a_1], [a_2], \dots, [a_s]$ denote the non-zero equivalence classes under the relation $a \sim b$ if $a = bu$ where u is a unit in R. A code of this form is said to be of type $\{k_1, k_2, k_3, \dots, k_s\}$ and has $\prod_{i=1}^{s} |a_iR|^{k_i}$ elements, where $a_iR = \{x | x = a_ir, r \in R\}$.

Suppose B is a block code over R. Then, the *minimum weight* of B is

$$\min\{w(x) \mid x \in B, x \neq 0\}.$$

The distance $d(x, y)$ between codewords x and y is $d(x, y) = w(x-y)$. Further, the *minimum distance* d of B is

$$\min\{d(x, y) \mid x, y \in B, x \neq y\}.$$

It is known that if B is linear, then d is always equal to the minimum weight of B.

3 Results

3.1 The cross product $\mathbb{F}_{p^r} \times \mathbb{F}_{p^r}$

The cross product $\mathbb{F}_{p^r}^2$ is a commutative ring with identity. Its additive identity is $(0, 0)$ and its multiplicative identity is $(1, 1)$.

We state another theorem from [10] that we will use to determine the of ideals of $\mathbb{F}_{p^r}^2$.

Theorem 2. *(Hungerford,[10]) If $R_1, \dots, R_n$ are rings with identity and I an ideal in $\prod_{j=1}^{n} R_j$, then $I = \prod_{j=1}^{n} A_j$ where A_j is an ideal in R_j.*

Using Theorem 2, it is easy to verify that the ideals of $\mathbb{F}_{p^r}^2$ are the following:

i. $\mathbb{F}_{p^r}^2 = ((x, y)), x, y \neq 0$

ii. $\{0\} \times \mathbb{F}_{p^r} = ((0, y)), y \neq 0$

iii. $\mathbb{F}_{p^r} \times \{0\} = ((x, 0)), x \neq 0$

iv. $\{(0, 0)\} = ((0, 0))$

Since every nonzero element x of the field $\mathbb{F}_{p^r}$ is a generator, then each of the ideals $((0, x))$ and $((x, 0))$ has p^r elements. These two ideals are both maximal which makes $\mathbb{F}_{p^r}^2$ a finite balanced semi-local ring. Hence, the nonzero elements of the maximal ideals are the zero divisors of $\mathbb{F}_{p^r}^2$ which are the nonzero multiples of $(0, x)$ and $(x, 0)$. Consequently, there are $2(p^r - 1)$ zero divisors of $\mathbb{F}_{p^r}^2$.

Moreover, since $\mathbb{F}_{p^r}$ is a field, then every nonzero element x of $\mathbb{F}_{p^r}$ has a multiplicative inverse say x'. Hence, if $(x, y) \in \mathbb{F}_{p^r}^2$ such that $x, y \neq 0$, then there exists $(x', y') \in \mathbb{F}_{p^k}^2$ such that $(x, y)(x', y') = (1, 1)$. Thus, every $(x, y) \in \mathbb{F}_{p^r}^2$ such that $x, y \neq 0$ is a unit and $|(\mathbb{F}_{p^r}^2)^\times| = (p^r - 1)^2$.

From [14], the finite direct sum of Frobenius rings is Frobenius and if the Frobenius rings $R_1, \ldots, R_n$ each have right generating characters $\chi_1, \ldots, \chi_n$, then $R = \oplus R_i$ has generating character $\chi = \prod \chi_i$. Hence, the generating character of $\mathbb{F}_{p^r}^2$ is given by

$$\chi : \mathbb{F}_{p^r}^2 \to \mathbb{T}, \;\; \chi((x, y)) = e^{\frac{2\pi i}{p} tr(x+y)}. \tag{3}$$

Thus, the cross product $\mathbb{F}_{p^r}^2$ is a finite balanced semi-local Frobenius ring.

3.2 Structural Properties of $\mathbb{F}_{p^r} + v\mathbb{F}_{p^r}$

The structure of $R_p = \mathbb{F}_{p^r} + v\mathbb{F}_{p^r}$, p prime, $k \in \mathbb{N}$, will be studied by taking two cases: when $p = 2$ with $v^2 = v$; and when p is an odd prime with $v^2 = 1$. It can be shown that the case when $p = 2$ with $v^2 = 1$ yields the finite chain ring $\mathbb{F}_{2^r} + u\mathbb{F}_{2^r}, u^2 = 0$ and the case when p is odd with $v^2 = v$ is isomorphic to the ring produced when p is odd with $v^2 = 1$. We chose the latter case in this study since the motivation is to generalize $\mathbb{F}_3 + v\mathbb{F}_3$ wherein the condition $v^2 = 1$ is imposed in most of the available literatures instead of $v^2 = v$.

3.2.1 The ring $\mathbb{F}_{2^r} + v\mathbb{F}_{2^r}, v^2 = v$

Although it can be shown by using CRT that $R_{2^r} = \mathbb{F}_{2^r} + v\mathbb{F}_{2^r}, v^2 = v$ is isomorphic to $\mathbb{F}_{2^r}^2$, we can also use the ring isomorphism given by

$$\phi : R_{2^r} \to \mathbb{F}_{2^r}^2$$

$$a + bv \mapsto (a + b, a).$$

Based on the ideals of $\mathbb{F}_{p^r}^2$, we can also construct the lattice of ideals of R_{2^r} given by Figure 1.

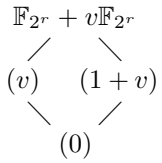

Figure 1: Lattice of Ideals of $\mathbb{F}_{2^r} + v\mathbb{F}_{2^r}, v^2 = v$

The two proper nontrivial ideals (v) and $(1 + v)$ are both maximal which makes R_{2^r} a finite balanced semi-local ring with $|(v)| = |(1 + v)| = 2^r$. Using the isomorphism, we can say that a nonzero element of R_{2^r} is a zero divisor if and only if it is an R_{2^r}- multiple of v or $1 + v$ and there are $2(2^r - 1)$ of them. Indeed, the zero divisors are contained in the two maximal ideals. It is easy to show that an R_{2^r}- multiple of v or $1+v$ is simply an $\mathbb{F}_{2^r}$-multiple of v or $1+v$. Thus, we can write $(v) = \{xv|x \in \mathbb{F}_{2^r}\}$ and $(1 + v) = \{x(1 + v)|x \in \mathbb{F}_{2^r}\}$.Since R_{2^r} is a semi-local ring, then its nonzero element is a unit if and only if it is not an $\mathbb{F}_{2^r}$- multiple of v or $1 + v$ and there are $(2^r - 1)^2$ units. Further, a nonzero element of R_{2^r} is either a unit or a zero divisor.

In addition, R_{2^r} is Frobenius as shown in the next theorem.

Theorem 3. *Let $r \in \mathbb{N}$. The ring $\mathbb{F}_{2^r} + v\mathbb{F}_{2^r}, v^2 = v$ is a finite balanced semi-local Frobenius ring.*

Proof We are left to show that R_{2^r} is Frobenius. The mapping

$$\chi : R_{2^r} \to \mathbb{T}, \;\; \chi(x + vy) = e^{(\pi i)tr(y)}$$

is a character. Now,

$$\begin{aligned} \ker \chi &= \{a + bv \in R_{2^r} | (-1)^{tr(y)} = 1\} \\ &= \{a + bv | tr(b) = 0\}. \end{aligned}$$

Note that there are 2^{r-1} elements of $\mathbb{F}_{2^r}$ whose trace is 0. Hence, $|\ker\chi| = 2^{r-1}$. However, each nonzero proper ideal of R_{2^r} has order $2^r > 2^{r-1}$. Thus, it is impossible for $\ker\chi$ to contain a nonzero proper ideal of R_{2^r}. □

3.2.2 The ring $\mathbb{F}_{p^r} + v\mathbb{F}_{p^r}, v^2 = 1, p \neq 2$

For the succeeding discussions in this subsection, we let p be an odd prime and $v^2 = 1$. We also denote by -1 the additive inverse of 1 in $\mathbb{F}_p$. Note that for any value of p, the element -1 always exists.

Using the CRT, we can show that $R_{p^r} = \mathbb{F}_{p^r} + v\mathbb{F}_{p^r} \cong \mathbb{F}_{p^r}^2$. However, we can also show the same thing using the isomorphism

$$\phi : R_{p^r} \to \mathbb{F}_{p^r}^2$$

$$a + bv \mapsto (a - b, a + b).$$

The lattice of ideals of R_{p^r} is given by Figure 2.

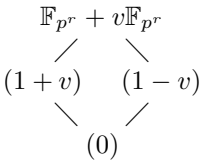

Figure 2: Lattice of Ideals of $\mathbb{F}_{p^r} + v\mathbb{F}_{p^r}, v^2 = 1, p \neq 2$

We can see that R_{p^r} has exactly two maximal ideals namely $(1+v)$ and $(1-v)$ making it a balanced semi-local ring with $|(1+v)| = |(1-v)| = p^r$. A nonzero element of R_{p^r} is a zero divisor if and only if it is an R_{p^r}- multiple of $1+v$ or $1-v$ and there are $2(p^r-1)$ of them. It is easy to show that an R_{p^r}-multiple of $1+v$ or $1-v$ is simply an $\mathbb{F}_{p^r}$-multiple of $1+v$ or $1-v$. Thus, we can write $(1+v) = \{x(1+v)|x \in \mathbb{F}_{p^r}\}$ and $(1-v) = \{x(1-v)|x \in \mathbb{F}_{p^r}\}$. Since R_{p^r} is a semi-local ring, then its nonzero element is a unit if and only if it is not an $\mathbb{F}_{p^r}$- multiple of $1+v$ or $1-v$ and there are $(p^r-1)^2$ of them. Further, a nonzero element of R_{p^r} is either a unit or a zero divisor. In addition, R_{p^r} is Frobenius as shown in the next theorem.

Theorem 4. *The ring $\mathbb{F}_{p^r} + v\mathbb{F}_{p^r}, v^2 = 1$ is a finite balanced semi-local Frobenius ring.*

Proof The proof is almost the same as the proof of Theorem 3. The mapping

$$\chi : R_{p^r} \to \mathbb{T}, \;\; \chi(x + vy) = e^{\frac{2\pi i}{p} tr(y)}.$$

is a generating character of R_{p^r}. □

We can also describe a zero divisor based on the ideal that contains it as suggested by the next theorem.

Theorem 5. *Let $R_p = \mathbb{F}_{p^r} + v\mathbb{F}_{p^r}$ where $v^2 = v$ or 1 and p is prime. If $a \in (1+v)$ and $b \neq 0$ such that $ab = 0$, then $b \in (v)$ if $p = 2$ and $b \in (1-v)$ if p is odd. In addition, no such b exists in $(1+v)$.*

Proof Suppose $p = 2$. Then the proper nontrivial ideals of R_2 are (v) and $(1+v)$. If $a = q \cdot 1 + v \in (1+v)$ for some $q \in \mathbb{F}_{2^r}, q \neq 0$, then for $c \in (v)$, $ac = 0$ since $1+v \cdot 1+v = 0$. Let $b = t \cdot 1+v \in (1+v)$, $t \in \mathbb{F}_{2^r}, t \neq 0$. If $ab = 0$, then $q \cdot 1 + v \cdot t \cdot 1 + v = qt \cdot 1 + v = 0$ implying $q = 0$ or $t = 0$, a contradiction. Hence, no such $b \in (1+v)$ exists.

The proof is similar for the case $p \neq 2$ by using the fact that the proper ideals when $p \neq 2$ are $(1-v)$ and $(1+v)$ and that $(1-v)(1+v) = 0$. □

3.3 Weight functions on $\mathbb{F}_{p^r} + v\mathbb{F}_{p^r}$

In this section, we discuss the weight functions that can be defined on R_p such as the so- called Bachoc and homogeneous weights.

3.3.1 Bachoc weight on $\mathbb{F}_p + v\mathbb{F}_p$

Since we have shown that $\mathbb{F}_p + v\mathbb{F}_p$ is isomorphic to $\mathbb{F}_p^2$, then following [1], the Bachoc weight on $\mathbb{F}_2 + v\mathbb{F}_2, v^2 = v$ denoted by w_B is given by

$$w_B(x) = \begin{cases} 0 & if \; x = 0 \\ 1 & if \; x = 1 \\ 2 & if \; x = v, 1+v \end{cases}$$

In addition, if p is an odd prime and $v^2 = 1$, then the Bachoc weight on $\mathbb{F}_p + v\mathbb{F}_p$ is given by

$$w_B(x) = \begin{cases} 0 & if \; x = 0 \\ p & if \; x \; is \; a \; nonzero \; multiple \; of \; 1+v \; or \; 1-v \\ 1 & otherwise \end{cases}$$

3.3.2 Homogeneous weight on $\mathbb{F}_{p^r} + v\mathbb{F}_{p^r}$

We now construct a homogeneous weight on R_p in terms of the generating character of $\mathbb{F}_{p^r}^2$. It can be shown that using the Fundamental Theorem of Sum Calculus,

$$\sum_{j=1}^{p-1} e^{(\frac{2\pi j}{p})i} = -1.$$

The generating character of $\mathbb{F}_{p^r}^2$ is given by (3). Let $S = \mathbb{F}_{p^r}^2$. Based on [9], the homogeneous weight of $(x, y) \in S$ is given by

$$w_{Hom}((x,y)) = \Gamma\left[1 - \frac{1}{(p^r-1)^2} \sum_{(a,b)\in S^\times} e^{\frac{2\pi i}{p} tr(ax+by)}\right].$$

Case 1: Suppose $(x, y) = (0, 0)$. Since $tr(0) = 0$, then $w_{Hom}((0, 0)) = 0$.

Case 2: Suppose (x, y) is a zero divisor. Without loss of generality, suppose $y = 0, x \neq 0$ and let $\mathbb{F}_{p^r}^* = \mathbb{F}_{p^r}\backslash\{0\}$. Thus, $tr(ax + by) = tr(ax), (a, b) \in S^\times$. Note that $|S^\times| = (p^r - 1)^2$. Let $q_i \in \mathbb{F}_{p^r}^*, i = 1, \ldots, p^r - 1$. Hence, $\{q_i x | i = 1, \ldots, p^r - 1\} = \mathbb{F}_{p^r}^*$. Thus, there would be $p^r - 1$ copies of $(q_i x, 0)$ for each x coming from the $p^r - 1$ elements of $S^\times$ whose first component is q_i. Since tr takes on each value of $\mathbb{F}_p$ equally often, that is, p^{r-1} times, and $tr((0, 0)) = 0$, then it follows that the number of $\alpha \in \mathbb{F}_{p^r}^*$ such that $tr(\alpha) = 0$ would be $p^{r-1} - 1$. In addition, for each $j = 1, \ldots, p - 1$, the number of $\beta \in \mathbb{F}_{p^r}^*$ such that $tr(\beta) = j$ is p^{r-1}. Then, we have

$$\begin{aligned}\sum_{(a,b)\in S^\times} e^{\frac{2\pi i}{p} tr(ax)} &= (p^{r-1} - 1)(p^r - 1)(e^{\frac{2\pi i}{p}})^0 + (p^{r-1})(p^r - 1)\textstyle\sum_{j=1}^{p-1} e^{(\frac{2\pi ji}{p})} \\ &= (p^{r-1} - 1)(p^r - 1)(1) + (p^{r-1})(p^r - 1)(-1) \\ &= -(p^r - 1).\end{aligned}$$

Thus, if (x, y) is a zero divisor, then

$$w_{Hom}((x,y)) = \Gamma\left[1 - \frac{1}{(p^r-1)^2}.-(p^r-1)\right] = \Gamma\left(\frac{p^r}{p^r-1}\right).$$

Case 3: Suppose (x, y) is a unit. Since $S^\times$ forms a group under multiplication, then given an element $(x, y) \in S^\times$, $\{(q_i x, s_i y) | (q_i, s_i) \in S^\times\} = S^\times$. Let $j, m \in \mathbb{F}_p\backslash\{0\}$ and consider the following disjoint subsets of $S^\times$.

$$A_{0,0} = \{(x,y)|tr(x) = tr(y) = 0\}$$
$$A_{j,0} = \{(x,y)|tr(x) = j, tr(y) = 0\}$$
$$A_{0,m} = \{(x,y)|tr(x) = 0, tr(y) = m\}$$
$$A_{j,m} = \{(x,y)|tr(x) = j, tr(y) = m\}$$

Since in $\mathbb{F}_{p^r}^*$, there are $p^{r-1}-1$ elements whose trace is 0 and p^{r-1} elements whose trace is j for each $j = 1, \ldots, p-1$, then we have $|A_{0,0}| = (p^{r-1}-1)^2$, $|A_{j,0}| = |A_{0,m}| = (p^{r-1}-1)p^{r-1}$, and $|A_{j,m}| = (p^{r-1})^2$ for each j, m. Then, given $(x,y) \in S^\times$,

$$\begin{aligned}\sum_{(a,b)\in S^\times} e^{\frac{2\pi i}{p}tr(ax+by)} &= |A_{0,0}|e^{\frac{2\pi i}{p}(0)} + \sum_{j=1}^{p-1}|A_{j,0}|e^{\frac{2\pi i}{p}(j)} + \sum_{m=1}^{p-1}|A_{0,m}|e^{\frac{2\pi i}{p}(m)} \\ &\quad + \sum_{j=1}^{p-1}\sum_{m=1}^{p-1}|A_{j,m}|e^{\frac{2\pi i}{p}(j+m)} \\ &= (p^{r-1}-1)^2 + 2(p^{r-1}-1)p^{r-1}\sum_{j=1}^{p-1}e^{\frac{2\pi i}{p}(j)} \\ &\quad + (p^{r-1})^2\sum_{j=1}^{p-1}e^{\frac{2\pi i}{p}(j)}\sum_{m=1}^{p-1}e^{\frac{2\pi i}{p}(m)} \\ &= (p^{r-1}-1)^2 + 2(p^{r-1}-1)p^{r-1}(-1) + (p^{r-1})^2(-1)(-1) \\ &= 1.\end{aligned}$$

Thus, if (x,y) is a unit, then $w_{Hom}((x,y)) = \Gamma\left(1 - \frac{1}{(p^r-1)^2}\right) = \Gamma\left[\frac{(p^r)(p^r-2)}{(p^r-1)^2}\right]$

Then, we have the next theorem.

Theorem 6. *The normalized homogeneous weight on $\mathbb{F}_{2^r} + v\mathbb{F}_{2^r}, v^2 = v$ is given by*

$$w_{Hom}(x) = \begin{cases} 0 & \text{if } x = 0 \\ \dfrac{2^r}{2^r-1} & \text{if } x \text{ is a nonzero multiple of } v \text{ or } 1+v \\ \dfrac{(2^r)(2^r-2)}{(2^r-1)^2} & \text{otherwise.} \end{cases} \tag{4}$$

Moreover, the normalized homogeneous weight on $\mathbb{F}_{p^r} + v\mathbb{F}_{p^r}, v^2 = 1, p \neq 2$ is

given by

$$w_{Hom}(x) = \begin{cases} 0 & \text{if } x = 0 \\ \dfrac{p^r}{p^r - 1} & \text{if } x \text{ is a nonzero multiple of } 1 - v \text{ or } 1 + v \\ \dfrac{(p^r)(p^r - 2)}{(p^r - 1)^2} & \text{otherwise.} \end{cases} \quad (5)$$

Note that the normalized homogeneous weight on $\mathbb{F}_2 + v\mathbb{F}_2$ does satisfy the positive definite property of weight functions as suggested by the factor $(2^r - 2)$ in (4). In addition, using (5) with $\Gamma = \frac{4}{3}$, we can show that the Lee weight on $\mathbb{F}_3 + v\mathbb{F}_3, v^2 = 1$ is homogeneous on $\mathbb{F}_3 + v\mathbb{F}_3$.

3.4 Linear Block Codes over $\mathbb{F}_{p^r} + v\mathbb{F}_{p^r}$

Following the matrix in (2), we have the following generator matrix for a linear block code over R_p.

Theorem 7. *Any linear block code B over R_{2^r} has a generator matrix which can be put in the following form:*

$$\begin{pmatrix} I_{k_1} & A & C & D \\ 0 & vI_{k_2} & vE & vF \\ 0 & 0 & (1+v)I_{k_3} & (1+v)H \end{pmatrix} \quad (6)$$

where A, C, and D are matrices over R_{2^r} and E, F, and H are binary matrices.

Moreover, any linear block code B over R_{p^r} has a generator matrix which can be put in the following form:

$$\begin{pmatrix} I_{k_1} & A & C & D \\ 0 & (1+v)I_{k_2} & (1+v)E & (1+v)F \\ 0 & 0 & (1-v)I_{k_3} & (1-v)H \end{pmatrix} \quad (7)$$

where A, C, and D are matrices over R_{p^r} and E, F, and H are binary matrices.

In both cases, B is type $\{k_1, k_2, k_3\}$ and $|B| = (p^{2r})^{k_1} \cdot (p^r)^{k_2} \cdot (p^r)^{k_3}$.

Proof Using the equivalence relation defined in (2), we have the equivalence classes $[1], [v]$, and $[1 + v]$ for R_{2^r}, and $[1], [1 + v]$, and $[1 - v]$ for R_{p^r}. Hence we have the matrices. The cardinality of B is computed using the cardinalities of the ideals $(1), (v), (1 + v)$, and $(1 - v)$. □

If $k_2 = k_3 = 0$, then we say that the code B is *free*.

We can characterize the minimum-weight codewords of B based on its coordinates as shown in the next theorem and proposition.

Theorem 8. *If d_H is the minimum Hamming distance of B, then there is a codeword $c \in B$ with $w_H(c) = d_H$ such that all nonzero coordinates of c are contained in a proper ideal.*

Proof Let $a' \in B$ with $w_H(a') = d_H$ whose nonzero coordinates are not contained in a single proper ideal. Since B is linear, then $a = (1+v)a' \in B$ and the coordinates of a are all contained in the ideal $(1+v)$. Since $1+v$ is a zero divisor, then some of the nonzero coordinates of a' that belongs to the other proper ideal, will now be zero after multiplying $1+v$. Thus, $w_H(a) \leq w_H(a') = d_H$. Since d_H is the smallest among all Hamming distances in B, then $w_H(a) = d_H$. The same technique is used in proving the cases of the ideals (v) and $(1-v)$. □

Proposition 1. *Let $x \in B$ such that $w_H(x) = d_H$. Then x is one of the following codewords:*

i.) Type A: the nonzero components of x are units;

ii.) Type B: the component of x are contained in (v) if $p = 2$ or in $(1-v)$ if p is an odd prime; and

iii.) Type C: the components of x are contained in $(1+v)$.

Proof We will only prove the statement when $p = 2$ since the proof is similar when p is an odd prime. Suppose x contains units and zero divisors. Without loss of generality, let $x = (0, u, z_1)$ where u is a unit and z_1 is a zero divisor. Suppose $z_1 \in (v)$. By Theorem 5, there exists a zero divisor $z_2 \in (1+v)$ such that $z_2 x = (0, z_2 u, 0)$. Since B is linear, then $z_2 x \in B$. Thus, $w_H(z_2 x) < w_H(x)$ and hence, x is not a minimum weight word. The same is true when the components of x are zero divisors from two distinct ideals of R_p. Hence, we are left to show the existence of Types A, B, and C codewords. The existence of Type B and C codewords is already ensured by Theorem 8. Since the sum of two divisors coming from two different ideals is a unit, then a Type A codeword exists by adding a Type B and a Type C codewords. □

We now derive a bound on the minimum Bachoc distance d_B and minimum normalized homogeneous distance d_{Hom} of B in terms of d_H.

Theorem 9. *Let B be a linear block code over $\mathbb{F}_p + v\mathbb{F}_p$. Then $d_H \leq d_B \leq p d_H$.*

Proof If a Type A codeword exists, then $d_B = d_H$ since the Bachoc weight of a unit is 1. If a Type A codeword does not exist, then d_B will always be greater than d_H. By Theorem 8, there always exists a Type B or C codeword, say x. Then, $w_B(x) = p d_H$ since the Bachoc weight of a zero divisor is p. □

Theorem 10. *If d_{Hom} is the minimum normalized homogeneous distance of B, then*

$$d_{Hom} \leq \frac{p^r}{p^r - 1} d_H.$$

Proof From Theorem 8, there exists a codeword $x \in B$ such that $w_{Ham}(x) = d_H$ and the components of x are all contained in a single proper ideal. Thus, the d_H nonzero coordinates of x are zero divisors. Note that if $y \in R_p$ is a zero divisor, then $w_{Hom}(y) = \frac{p^r}{p^r - 1}$. Since the homogeneous weight of a unit is always less than 1, then the result follows. □

We remark that if every minimum Hamming weight word has components contained in a single proper ideal, then $d_{Hom} = \frac{p^r}{p^r - 1} d_H$.

We now consider a subcode generated by a codeword whose idea came from [13].

Definition 2. Let R be a ring. Then, the *subcode of B generated by the codeword $x \in B$*, denoted by B_x, is the set $\{ax | a \in R\}$.

We present a characterization of the subcode B_x in terms of its order and the components of the generator codeword.

Theorem 11. *Let $x \in B, x \neq 0$. $|B_x| = p^{2r}$ if and only if B_x is free. Moreover, $|B_x| = p^r$ if and only if B_x is not free.*

Proof

Case 1: Suppose x contains a unit u. Without loss of generality, suppose $x = (0, u, \ldots, 0)$. Hence, $B_x = \{(0, r, \ldots, 0) | r \in R_p\}$ since $(u) = R_p$. Thus, $|B_x| = p^{2k}$.

Case 2: Suppose x does not contain a unit and the nonzero components of x belong the maximal ideals (z_1) and (z_2), $z_1 \neq z_2$. Without loss of generality, let $x = (0, z_1, z_2, \ldots, 0)$. Hence, $B_x = \{(0, az_1, az_2, \ldots, 0) | a \in R_p\}$. Since $(z_1) \cap (z_2) = \{0\}$, then there does not exist distinct $a, b \in R_p$, such that $az_1 = bz_1$ and $az_2 = bz_2$ for if there exist such a, b, then $az_1 - bz_1 = (a - b)z_1 = 0$ and $az_2 - bz_2 = (a - b)z_2 = 0$ implying $a - b \in (z_1) \cap (z_2)$ by Theorem 5, a contradiction. Hence, there are $p^r.p^r$ possible combinations for (z_1, z_2). Thus, $|B_x| = p^{2r}$.

Case 3: Suppose x does not contain a unit and the nonzero components of x belong to the maximal ideal (z_1). Without loss of generality, suppose $x = (0, z_1, \ldots, z_{p^r - 1}), z_i \in (z_1)$. Hence, $B_x = \{(0, az_1, \ldots, az_{p^r - 1}) | a \in$

$R_p\}$. Since $z_i \in (z_1)$, then there exists $a_i \in R_p$ such that $a_i z_1 = z_i$ for all $i = 1, \ldots, p^r - 1$. Thus, if $az_1 = bz_1, b \in R_p$, then it follows that $az_i = bz_i$ for $i = 2, \ldots, p^r - 1$. Since $|(z_1)| = p^r$, then there will only be p^r distinct az_1 and consequently, $|B_x| = p^r$.

Note that in Cases 1 and 2, we can show that $\{x\}$ is a basis of B_x over R_p while there is no basis for Case 3. □

Corollary 2. *The subcode B_x is not free if and only if the nonzero components of x belong to a proper ideal of R_p. Moreover, $|B_x| = p^r$ if and only if the nonzero components of x are not contained in a proper ideal of R_p.*

3.5 The p^r- ary image of linear block codes over $\mathbb{F}_{p^r} + v\mathbb{F}_{p^r}$

Let $\mathcal{B}_2 = \{v_1, v_2\}$ be a basis of R_p over $\mathbb{F}_{p^r}$ and $w = av_1 + bv_2 \in R_p$ where $a, b \in \mathbb{F}_{p^r}$. Define the mapping

$$\psi : R_p \to \mathbb{F}_{p^r}^2 \quad , av_1 + bv_2 \mapsto (a, b). \tag{8}$$

Then, ψ is a module homomorphism over $\mathbb{F}_{p^r}$ and is injective.

Let B be a linear block code of length n over R_p. We now extend ψ to R_p^n coordinatewise. If $c = (c_1, c_2, \ldots, c_n) \in B$ and $c_i = a_i v_1 + b_i v_2$, then $\psi(c) = (a_1, b_1, a_2, b_2, \ldots, a_n, b_n) \in \mathbb{F}_{p^r}^{2n}$. We will refer to the set $\psi(B) = \{\psi(c) | \, c \in B\}$ as the *p^r-ary image of B under the mapping ψ with respect to the basis $\mathcal{B}_2$*. Since ψ is injective, then we have $|B| = |\psi(B)|$.

Theorem 12. *If B is a linear block code over R_p of length n, then $\psi(B)$ is a linear block code over $\mathbb{F}_{p^r}$ with length $2n$. In particular, if B is free whose rank is k, then $\psi(B)$ has rank $2k$.*

Proof Let $x = (x_1, x_2, \ldots, x_n) \in B$. Since each $\psi(x_i), 1 \leq i \leq n$, has length 2, then $\psi(B)$ has length $2n$. Using the fact that ψ is an $\mathbb{F}_{p^r}$-module homomorphism, we can show that $\psi(B)$ is an $\mathbb{F}_{p^r}$- subspace of $\mathbb{F}_{p^r}^{2n}$.

Suppose B is free and of rank k, then a basis for B has k elements, say $x_1, x_2, \ldots, x_k$. Hence, if $y \in B$, then

$$y = (a_1 + b_1 v)x_1 + (a_2 + b_2 v)x_2 + \ldots + (a_k + b_k v)x_k, a_i + b_i v \in R_p$$

and

$$\psi(y) = a_1\psi(x_1) + b_1\psi(vx_1) + a_2\psi(x_2) + b_2\psi(vx_2) + \ldots + a_k\psi(x_k) + b_k\psi(vx_k).$$

Thus, the set

$$S = \{\psi(x_1), \ldots, \psi(x_k), \psi(vx_1), \ldots, \psi(vx_k)\}$$

spans $\psi(B)$.

Since the x_i's are linearly independent and $\psi(x) = 0$ if and only if $x = 0$, then

$$\psi\left(\sum_{i=1}^{k}(a_i + b_i v)x_i\right) = 0 \text{ if and only if } a_i = b_i = 0, 1 \leq i \leq k$$

implying

$$\sum_{i=1}^{k} a_i\psi(x_i) + \sum_{i=1}^{k} b_i\psi(vx_i) = 0 \text{ if and only if } a_i = b_i = 0, 1 \leq i \leq k.$$

Hence, S is a basis for $\psi(B)$ with $2k$ elements. □

Corollary 3. *Let B be a free linear block code over R_p generated by the matrix G. Then, a generator matrix of $\psi(B)$ is*

$$G[\psi(B)] = \begin{pmatrix} \psi(G) \\ \psi(vG) \end{pmatrix}$$

4 Bounds on the p^r-ary image

In this section, we derive bounds on the minimum Hamming distance δ of the p^r-ary image of a linear block code B over R_p. We begin with the simplest bound, the Singleton-type bound.

Theorem 13. *(Singleton-type Bound) Let B be a free rate-k/n linear block code over R_p. Then δ satisfies*

$$\delta \leq 2n - 2k + 1 \tag{9}$$

Proof If B is a free rate-k/n code, then $\psi(B)$ is a rate-$2n/2k$ linear binary block code by Theorem 12. Applying the Singleton bound for codes over fields, then we have the bound. □

We now restate the Plotkin bound from [8].

Proposition 2. *(Greferath and O'Sullivan, [8]) Let R be a finite Frobenius ring that is equipped with a homogeneous weight w with average value Γ. Let B be a (not necessarily linear) block code of length n over R with minimum w-distance δ_{min}. Then*

$$\delta_{min} \leq \frac{|B|}{|B|-1}\Gamma n. \tag{10}$$

A direct application of (10) to $\psi(B)$ gives the following Plotkin-type bound.

Theorem 14. *(Plotkin-type bound) Let B be a rate-k/n systematic linear block code over R_p. Then,*

$$\delta \leq \frac{(p^{2rk})}{(p^{2rk}-1)} \cdot \frac{p^r-1}{p^r} \cdot 2n. \tag{11}$$

Proof The length of $\psi(B)$ is $2n$ with $\Gamma = \frac{p^k-1}{p^k}$. Since B is systematic, then $|B| = |\psi(B)| = (p^{2r})^k$ and the rest follows from Proposition 2. □

The minimum Hamming weight can also be used to bound the minimum Hamming weight of the image code as given by the following bound which resembles the bound in [12].

Theorem 15. *(Rains-type bound) Let d_H be the minimum Hamming distance of B. Then,*

$$\frac{(p^r-1)d_H}{p^r} \leq \delta \leq 2d_H. \tag{12}$$

Proof Since Γ is the minimum nonzero value of homogeneous weight, that is, the Hamming weight w_H on $\mathbb{F}_{p^r}$, then $\frac{(p^r-1)d_H}{p^r} \leq \delta$ since $\Gamma = \frac{p^r-1}{p^r}$ on $\mathbb{F}_{p^r}$. Note that δ is bounded above by $2n$ and for all $x \in B$, we have $\delta \leq w_H(\psi(x))$. Thus, if $x \in B$ and $w_H(x) = d_H$, then $\delta \leq 2d_H$. □

Following the proof of the generalized Rabizzoni bound in [13], we can refine the upper bound and the lower bound of (12) as shown in the following Rabizzoni-type bound.

Proposition 3. *(Rabizzoni-type Bound) Let d_H be the minimum Hamming distance of B and B_x be the subcode generated by the codeword x with Hamming weight d_H. Then*

$$d_H \leq \delta \leq \left\lfloor \frac{|B_x|}{|B_x|-1} \cdot \frac{p^r-1}{p^r} \cdot 2d_H \right\rfloor. \tag{13}$$

Moreover, if B_x is free, then

$$d_H \leq \delta \leq \left\lfloor \frac{2p^r d_H}{p^r+1} \right\rfloor. \tag{14}$$

Otherwise,

$$d_H \leq \delta \leq 2d_H. \tag{15}$$

Proof Since for any $x \in B$, $w_H(x) \leq w_H(\psi(x))$, then $d_H \leq \delta$. Note that the minimum Hamming distance of B_x is still d_H since B_x is a subcode of B. Let $\psi(B_x)$ denote the image of B_x under ψ. Hence, $\psi(B_x)$ is also a subcode of $\psi(B)$. Since the length of $\psi(B)$ is twice the length of B, then the effective length of $\psi(B_x)$ is $2d_H$ coming from the d_H nonzero positions in x. Let δ_x and δ be the minimum Hamming distance of $\psi(B_x)$ and $\psi(B)$ respectively. Also, note that $|\psi(B_x)| = |(B_x)|$ and $\Gamma = \frac{p^r-1}{p^r}$ on $\mathbb{F}_{p^r}$. Applying (10) on δ_x, we have

$$\delta_x \leq \left(\frac{|B_x|}{|B_x|-1}\right) \cdot \left(\frac{p^r-1}{p^r}\right) \cdot 2d_H.$$

Since $\delta \leq \delta_x$, then we have the bound (13). The bounds (14) and (15) were obtained by applying Theorem 11 to $|B_x|$. □

It is apparent that the sharpness of (13) depends on the choice of x. Selecting a codeword x that produces a free subcode will always give a sharper bound as suggested by (14) and (15).

5 Examples

For the following examples, we consider the mapping ψ with respect to the basis $\{1, v\}$.

Example 1. *The rate-2/3 linear block code B over $\mathbb{F}_2 + v\mathbb{F}_2$ with generator matrix*

$$G = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1+v & 1+v \end{pmatrix}$$

has minimum Hamming distance $d = 2$. Its image $\psi(B)$ is a rate-3/6 linear block code over $\mathbb{F}_2$ generated by

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

with minimum Hamming distance $\delta = 2$ and $|B| = |\psi(B)| = 8$. Since $x = (1\ 1\ 0) \in B$, then we can obtain a free subcode. Using the Rabizzoni-type bound, we have $2 \leq \delta \leq 2$ implying $\delta = 2$.

Example 2. *The rate-2/6 linear block code B over $\mathbb{F}_2 + v\mathbb{F}_2$ with systematic generator matrix*

$$G = \begin{pmatrix} 1 & 0 & v & v & v & 1+v \\ 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

has minimum Hamming distance $d = 2$. Its image $\psi(B)$ is a rate-4/12 linear block code over $\mathbb{F}_2$ generated by

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

with minimum Hamming distance $\delta = 4$ and $|B| = |\psi(B)| = 16$. There is no minimum weight codeword $x \in B$ that will yield a free subcode. Using the Rabizzoni-type bound, we have $2 \leq \delta \leq 4$. The image code reached the upperbound of the Rabizzoni-type bound.

Example 3. *The rate-2/6 linear block code B over $\mathbb{F}_2 + v\mathbb{F}_2$ with generator matrix*

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1+v & 1+v & 1+v \end{pmatrix}$$

has minimum Hamming distance $d = 3$. Then, $\psi(B)$ is a rate-3/12 binary linear block code generated by

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

with minimum Hamming distance $\delta = 6$ and $|B| = |\psi(B)| = 8$. There is no minimum weight codeword $x \in B$ that will yield a free subcode. Using the Plotkin bound for binary codes, we have $\delta \leq 6$. Using the Rabizzoni-type bound, we have $2 \leq \delta \leq 6$. Hence, the binary code is Plotkin-optimal and Rabizzoni-optimal.

The upper bounds on the previous examples are summarized in Table 1. It can be noticed that the Rabizzoni-type bound gives the sharpest upper bound among the other.

Example 4. *The rate-2/4 systematic linear block code B over $\mathbb{F}_3 + v\mathbb{F}_3, v^2 = 1$ with generator matrix*

$$\begin{pmatrix} 1 & 0 & v & 1+2v \\ 0 & 1 & 2+2v & 2v \end{pmatrix}$$

Table 1: Bounds on δ for Codes over $\mathbb{F}_2 + v\mathbb{F}_2$

Code	k	n	$\lvert B\rvert$	d_H	δ	Rabizzoni	Rains	Plotkin	Singleton
Example 1	2	3	8	2	2	2	4	3	4
Example 2	2	6	16	2	4	4	4	6	9
Example 3	2	6	8	3	6	6	6	6	10

has $d_H = 2$. The, $\psi(B)$ is a rate-4/8 ternary linear block code generated by

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 2 \\ 0 & 1 & 0 & 0 & 1 & 0 & 2 & 1 \\ 0 & 0 & 1 & 0 & 2 & 2 & 0 & 2 \\ 0 & 0 & 0 & 1 & 2 & 2 & 2 & 0 \end{pmatrix}$$

with minimum Hamming distance $\delta = 4$ and $|B| = |\psi(B)| = 81$.

There is no minimum weight word in B that produces a free subcode. Hence, using the Rabizzoni-type bound, we have $2 \leq \delta \leq 4$. Thus, the ternary code is Rabizzoni-optimal.

Example 5. *The rate-2/4 linear block code B over $\mathbb{F}_3 + v\mathbb{F}_3, v^2 = 1$ with generator matrix*

$$\begin{pmatrix} 1+2v & 2+v & 2+v & 0 \\ 0 & 2+2v & 1+v & 2+2v \end{pmatrix}$$

has $d_H = 3$. Its image $\psi(B)$ is a rate-2/8 ternary linear block code generated by

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 2 \\ 0 & 1 & 0 & 0 & 1 & 0 & 2 & 1 \\ 0 & 0 & 1 & 0 & 2 & 2 & 0 & 2 \\ 0 & 0 & 0 & 1 & 2 & 2 & 2 & 0 \end{pmatrix}$$

with minimum Hamming distance $\delta = 6$ and $|B| = |\psi(B)| = 9$.

There is no minimum weight word in B that produces a free subcode. Hence, using the Rabizzoni-type bound, we have $3 \leq \delta \leq 6$. In addition, using the Plotkin bound for ternary codes, we obtain $\delta \leq 6$. Thus, the ternary code is Rabizzoni-optimal and Plotkin-optimal.

Example 6. *The rate-2/6 linear block code B over $\mathbb{F}_3 + v\mathbb{F}_3, v^2 = 1$ with generator matrix*

$$\begin{pmatrix} 1+v & v & 1+v & v & 1+v & v \\ 1+2v & 2+v & 1+2v & 2+v & 1+2v & 2+v \end{pmatrix}$$

has $d_H = 3$. The image $\psi(B)$ is a rate-3/12 ternary linear block code generated by

$$\begin{pmatrix} 1 & 0 & 0 & 2 & 1 & 0 & 0 & 2 & 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 2 & 0 & 1 & 0 & 2 & 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 2 & 0 & 0 & 1 & 2 & 0 & 0 & 1 & 2 \end{pmatrix}$$

with minimum Hamming distance $\delta = 6$ and $|B| = |\psi(B)| = 27$.

There is no minimum weight word in B that produces a free subcode. Hence, using the Rabizzoni-type bound, we have $3 \leq \delta \leq 6$. Thus, the ternary code is Rabizzoni-optimal.

The upper bounds on the previous examples are summarized in Table 2. Again, we can see that the Rabizzoni-type bound gives the sharpest upper bound among the other.

Table 2: Bounds on δ for Codes over $\mathbb{F}_3 + v\mathbb{F}_3$

Code	k	n	$\lvert B\rvert$	d_H	δ	Rabizzoni	Rains	Plotkin	Singleton
Example 4	2	4	81	2	4	4	4	5	5
Example 5	2	4	9	3	6	6	6	6	7
Example 6	2	6	27	3	6	6	6	8	10

References

[1] C. Bachoc,"Application of coding theory to the construction of modular lattices,"*J. Combin. Theory Ser A*, vol. 78, pp. 92-119, 1997.

[2] K. Betsumiya and M. Harada, "Optimal self-dual codes over $\mathbb{F}_2 \times \mathbb{F}_2$ with respect to the Hamming weight, "*IEEE Trans. Inform. Theory*, vol. IT-50, pp. 356-358, 2004.

[3] Y. Cengellenmis, "On the cyclic codes over $\mathbb{F}_3+v\mathbb{F}_3$," *International Journal of Algebra*, vol. 4, no. 6, pp. 253-259, 2010.

[4] Y. Cengellenmis, "A Characterization of Codes over $\mathbb{F}_3$," *International Journal of Algebra*, vol. 4, no. 6, pp. 261-265, 2010.

[5] S. Dougherty, P. Gaborit, M. Harada, A. Munemasa, P. Solè, P., "Type IV self- dual codes over rings," *IEEE Trans. Inform. Theory*, vol. 45, no. 7, pp. 2345-2360, 1999.

[6] S. Dougherty, M. Gupta, and K. Shiromoto, "On Generalized weights for codes over finite rings,"*preprint*, Nov. 2002.

[7] S. Dougherty and K. Shiromoto,"Maximum distance codes over rings of order 4," *IEEE Trans. Inform. Theory*, vol. 47, no. 1, pp. 400- 404, Jan. 2001.

[8] M. Greferath and M.E. O' Sullivan, "On bounds for codes over Frobenius rings under homogeneous weights,"*Discrete Math.*, vol. 289, pp. 11-24, 2004.

[9] T. Honold, "A characterization of finite Frobenius rings,"*Arch. Math. (Basel)*, vol. 76, pp. 406- 415, 2001.

[10] T. W. Hungerford, *Algebra (Graduate Texts in Mathematics* **73***)*. New York: Springer-Verlag, 1974.

[11] P. Rabizzoni, "Relation between the minimum weight of a linear code over $GF(q^m)$ and its q-ary image over $GF(q)$," *Lecture Notes in Computer Science*, vol. 388, Berlin, Germany: Springer-Verlag, 1989, pp. 209 - 212.

[12] E. Rains, "Optimal self-dual codes over $\mathbb{Z}_4$," *Discrete Math.*, vol. 203, pp. 215-228, 1999.

[13] P. Solé and V. Sison, "Bounds on the minimum homogeneous distance of the p^r- ary image of linear block codes over the Galois ring $GR(p^r, m)$," ISIT 2007, Nice, France, June 24- 29, 2007.

[14] J. Wood, "Duality for modules over finite rings and applications to coding theory,"*Amer. J. Math*, vol. 121, pp. 555- 575, 1999.

[15] S.X. Zhu, Y. Wang, and M.J. Shi, "Cyclic Codes over $\mathbb{F}_2 + v\mathbb{F}_2$," *ISIT 2009, Seoul, Korea*, pp. 1719-1722, 2009.