Ternary Images of Self-Dual Codes and Cyclic Codes over $\mathbb{F}_3 + v\mathbb{F}_3$

John Mark Lampos, Richard Urgelles

Institute of Mathematical Sciences and Physics
University of the Philippines Los Baños
College, Laguna 4031, Philippines

jmtlampos@uplb.edu.ph, richardurgelles@yahoo.com

ABSTRACT

In this paper we give the structure of the ternary image of self-dual linear block codes and cyclic linear block codes over the semi-local Frobenius ring $R_3 = \mathbb{F}_3 + v\mathbb{F}_3$, where $v^2 = 1$, with respect to an ordered basis. Sufficient conditions for the ternary image of an R_3-code to be of Type III or cyclic are presented.

Keywords

Frobenius ring, semi-local , Type III codes, cyclic codes.

1. INTRODUCTION

The idea of $p-ary$ image was introduced by Rabizzoni [10] by generating a code of length nr over $\mathbb{F}_p$ from a code of length n over $\mathbb{F}_{p^r}$ using a basis of the Galois field $\mathbb{F}_{p^r}$ over $\mathbb{F}_p$, p prime, and $r \in \mathbb{N}$. This technique was generalized by Solè and Sison [11] to the p^r- ary image of linear block codes over the Galois ring $GR(p^r, m)$.

There are already a number of studies on images of codes. The most notable among these was the discovery of the Kerdock and Preparata codes as Gray images of codes over $\mathbb{Z}_4$ [7]. Recently, images of codes over various types of rings are now being studied, specifically self-dual and cyclic codes over the ring $\mathbb{F}_p + v\mathbb{F}_p$ where $v^2 = v$ when $p = 2$ or $v^2 = 1$ whenever p is an odd prime. The self-dual codes are of great importance because most of the known best codes are self-dual or cyclic. In addition, the said classes of codes possess efficient encoding and decoding schemes most especially in syndrome decoding. Bachoc [1] began the study of self-dual codes over $R_2 = \mathbb{F}_2 + v\mathbb{F}_2$ along with its applications to modular lattices. Further, an upper bound on the minimum Bachoc weight of self-dual codes over the said ring was given and the notion of extremality was introduced in the said paper. Dougherty, et. al. [6], by using the Chinese Remainder Theorem (CRT) and the Gray map images, presented several results on Type IV self- dual codes over the commutative rings of order 4, which includes R_2. Further, in [2], self-dual and Type IV self- dual codes over R_2 were characterized based also on codes obtained by the Gray map and CRT. Self-dual codes over $R_3 = \mathbb{F}_3 + v\mathbb{F}_3$ were shown in [5] to produce 2- modular lattices. In the same paper, they also associated ternary self-dual codes with self dual codes over R_3. On the other hand, Zhu, Wang and Shi [12] studied the relationship between cyclic codes over the ring R_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. This study was followed by Cengellenmis [4] by considering cyclic codes over the ring R_3. Moreover, in [3], codes over $\mathbb{F}_3$ were characterized using the Gray map on R_3. It was shown that for an odd n, 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. Recently, in [8] , linear block codes over the semi-local Frobenius ring $\mathbb{F}_{p^r} + v\mathbb{F}_{p^r}$ were studied. Distance bounds on the minimum Hamming distance of the p^r-ary image of the linear block code in terms of different parameters were derived in the said paper.

In the present work, we also consider self-dual and cyclic codes over the finite semi-local Frobenius rings $R_3 = \mathbb{F}_3 + v\mathbb{F}_3$ where $v^2 = 1$. The ternary images of the block code were obtained by defining a map, which is not necessarily a Gray map, from R_3 to $\mathbb{F}_3^2$ with respect to an ordered basis of R_3 over $\mathbb{F}_3$. Further, we gave sufficient conditions for the self-duality and cyclicity of the image codes.

The material is organized as follows. Section 2 gives the structural properties of the ring R_3. Linear block codes over R_3 were studied in Section 3 while Section 4 is about the ternary image. Results on the images of self-dual and cyclic codes over R_3 were given in Section 5 while the last section presents examples of codes that illustrates the results of this study.

2. THE RING R_3

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. The ring $R_3 = \mathbb{F}_3 + v\mathbb{F}_3$ where $v^2 = 1$ is commutative with unity 1, characteristic 3, and order 9. Each element of R_3 can be written as $a+bv$ where $a,b \in \mathbb{F}_3$. The units in R_3 are $1, 2, v$ and $2v$ while its zero divisors are $1+v, 2+v, 1-v$ and $2+2v$. Further, R_3 has two proper nontrivial ideals $(1+v) = \{0, 1+v, 2+2v\}$ and $(1+2v) = \{0, 1+2v, 2+v\}$. Since both ideals are maximal and principal, R_3 is a semi-local principal ideal ring. By the Chinese Remainder Theorem, we can view R_3 as the ring

$$\frac{R_3}{(1+v)} \times \frac{R_3}{(1-v)} \cong \mathbb{F}_3 \times \mathbb{F}_3.$$

Further, R_3 is Frobenius with generating character

$$\chi : R_3 \to \mathbb{T}, \ \ \chi(x+vy) = \left(\frac{\sqrt{3}+i}{2}\right)^y.$$

In addition, it can be shown that R_3 is a 2- dimensional vector space over $\mathbb{F}_3$.

3. LINEAR BLOCK CODES OVER R_3

A rate-k/n *linear block code* B over a ring R_3 generated by $G \in R_3^{k\times n}$ is the R_3-submodule given by the set

$$B = \{v \in R_3^n \mid v = uG, u \in R_3^k\}.$$

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. 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.

For the succeeding discussions, we let B be a rate- k/n linear block code over R_3 unless otherwise stated.

From [5], any code B is permutation equivalent to a code generated by

$$G = \begin{pmatrix} I_{k_1} & bB_1 & aA_1 & bA_2 + (1+2v)B_2 & aA_3 + bB_3 \\ 0 & aI_{k_2} & 0 & aA_4 & 0 \\ 0 & 0 & bI_{k_3} & 0 & bB_4 \end{pmatrix} \quad (1)$$

where $a = 1+v$, $b = 1+2v$, A_i and B_j are ternary matrices and $|B| = 9^{k_1}3^{k_2}3^{k_3}$. If $k_2 = k_3 = 0$, then the code B is said to be *free.*

The *Euclidean inner product* $\langle x, y\rangle$ of x and y in R_3^n where $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ is defined as $\langle x, y\rangle = x_1y_1 + \ldots + x_ny_n$. The *dual code* $B^\perp$ with respect to the Euclidean inner product of B is defined as $B^\perp = \{x \in (R_3)^n | \langle x, y\rangle = 0 \ \forall y \in B\}$. B is *Euclidean self-dual* if $B = B^\perp$. For brevity, whenever we use the term *self-dual,* it is understood that we are referring to *Euclidean self-dual.* Ternary self-dual codes are called *Type III codes.*

It was mentioned in [5] that $B = (1+v)B^+ \oplus (1+2v)B^-$ where

$$B^+ = \{s \in \mathbb{F}_3^n | (1+v)s + (1+2v)t \in B\}$$

and

$$B^- = \{t \in \mathbb{F}_3^n | (1+v)s + (1+2v)t \in B\}.$$

In addition, the codes B^+ and B^- are permutation equivalent to the codes with generator matrices given respectively by

$$G[B^+] = \begin{pmatrix} I_{k_1} & 0 & 2A_1 & 2A_2 & 2A_3 \\ 0 & I_{k_2} & 0 & A_4 & 0 \end{pmatrix}$$

and

$$G[B^-] = \begin{pmatrix} I_{k_1} & 2B_1 & 0 & 2B_2 & 2B_3 \\ 0 & 0 & I_{k_3} & 0 & B_4 \end{pmatrix}$$

where A_i and B_i are ternary matrices and $|B^+| = |B^-| = 3^{k_1}3^{k_3}$.

Further,

$$B^\perp = (1+v)(B^+)^\perp \oplus (1+2v)(B^-)^\perp. \quad (2)$$

Also, it was shown that B is self- dual if and only if B^+ and B^- are both Type III.

Let $x = (x_1, x_2, \ldots, x_n) \in B$. Also, suppose $z \in R_3$ and $\rho : R_3^n \to R_3^n$ given by $\rho(x_1, x_2, , x_n) = (zx_n, x_1, \ldots, x_{n-1})$. A *$z$-cyclic* code B over R_3 is a linear code with the property that if $x \in R_3^n$ then $\rho(x) \in R_3^n$. If $z = 1$, then we simply say that B is *cyclic.* We denote by σ the permutation $\sigma(x) = (x_n, x_1, \ldots, x_{n-1})$. Let φ_s be the quasi-cyclic shift on $(\mathbb{F}_3^n)^s$ given by

$$\varphi_s(a^{(1)}|a^{(2)}|\ldots|a^{(s)}) = (\sigma(a^{(1)})|\sigma(a^{(2)})|\ldots|\sigma(a^{(s)}).$$

Then a code $B \subseteq (\mathbb{F}_3^n)^s$ is *quasi-cyclic* of order s and length ns if $\varphi_s(B) = B$.

The *Hamming weight* $w_H(x)$ of a codeword x is the number of the nonzero coordinates of x. The *minimum Hamming weight* of B is $\min\{w_H(x) \mid x \in B, x \neq 0\}$. The Hamming distance $d(x,y)$ between codewords x and y is defined as $d(x,y) = w_H(x-y)$. Further, the *minimum Hamming distance* d_H 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_H is always equal to the minimum Hamming weight of B.

4. TERNARY IMAGE OF LINEAR BLOCK CODES OVER R_3

Let $\mathcal{B}_2 = \{v_1, v_2\}$ be a basis of R_3 over $\mathbb{F}_3$. Thus, we can uniquely express each element $z \in R_3$ as $av_1 + bv_2$ where $a, b \in \mathbb{F}_3$. Define a mapping $\psi : R_3 \to \mathbb{F}_3^2$ such that $\psi(z) = (a, b)$ which is an $\mathbb{F}_3$- module isomorphism. Though there are several bases of R_3, the main focus of our discussion will be on the ordered bases $\mathcal{A}_1 = \{1, v\}$ and $\mathcal{A}_2 = \{1+v, 1+2v\}$. We note that when the ordered basis is $\mathcal{A}_1$, the resulting map is the Gray map on R_3 which is an isometry from R_3 (Lee weight) to $\mathbb{F}_3^2$ (Hamming weight). We denote by ψ_1 and ψ_2 the mapping ψ using $\mathcal{A}_1$ and $\mathcal{A}_2$ as their respective basis.

The images of each element of R_3 under the mapping ψ_1 and ψ_2 were given in Table 1.

We now extend ψ coordinatewise to R_3^n. If $x = (x_1, x_2, \ldots, x_n) \in B$ and $x_i = a_iv_1 + b_iv_2$, then

$$\psi(x) = (a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n) \in \mathbb{F}_2^{2n}.$$

We refer to the set $\psi(B) = \{\psi(x) | x \in B\}$ as the **ternary image of B under the mapping ψ with respect to the**

Table 1: Image of the elements of R_3 under ψ_1

$z \in R$	$\psi_1(z)$	$\psi_2(z)$
0	(0,0)	(0,0)
1	(1,0)	(2,2)
2	(2,0)	(1,1)
v	(0,1)	(2,1)
$2v$	(0,2)	(1,2)
$1+v$	(1,1)	(1,0)
$1+2v$	(1,2)	(0,1)
$2+v$	(2,1)	(0,2)
$2+2v$	(2,2)	(2,0)

basis $\mathcal{B}_2$. Clearly, $|B| = |\psi(B)|$. In addition, in [8], it was shown that $\psi(B)$ is a linear block code of length $2n$. The generator matrix of the ternary image is given in the next theorem.

THEOREM 1. *If G is the generator matrix (1), then $\psi(B)$ is permutation equivalent to the code with generator matrix G_ψ given by*

$$\begin{pmatrix} \psi(v_1 I_{k_1}) & \psi(v_1 bB_1) & \psi(v_1 aA_1) & \psi(v_1(aA_2+bB_2)) & \psi(v_1(aA_3+bB_3)) \\ \psi(v_2 I_{k_1}) & \psi(v_2 bB_1) & \psi(v_2 aA_1) & \psi(v_2(aA_2+bB_2)) & \psi(v_2(aA_3+bB_3)) \\ 0 & \psi(aI_{k_2}) & 0 & \psi(aA_4) & 0 \\ 0 & 0 & \psi(bI_{k_3}) & 0 & \psi(bB_4) \end{pmatrix}$$

where $a = 1+v, b = 1+2v$, A_i's and B_j's are ternary matrices and $|\psi_1(B)| = 9^{k_1}3^{k_2}3^{k_3}$.

The following theorem is immediate from the definition of ψ_1 and ψ_2.

THEOREM 2. *Let A be a $k \times n$ ternary matrix, 0 be a $k \times n$ zero matrix and ($\psi(A)$) be the matrix whose rows are the image of the rows of A under ψ. Then, we have*

$$\begin{pmatrix} \psi_1(A) \\ \psi_1(vA) \\ \psi_1((1+v)A) \\ \psi_1((1+2v)A) \end{pmatrix} = \begin{pmatrix} A & 0 \\ 0 & A \\ A & A \\ A & 2A \end{pmatrix}$$

and

$$\begin{pmatrix} \psi_2(A) \\ \psi_2(vA) \\ \psi_2((1+v)A) \\ \psi_2((1+2v)A) \end{pmatrix} = \begin{pmatrix} 2A & 2A \\ 2A & A \\ A & 0 \\ 0 & A \end{pmatrix}.$$

Hence for $\psi_1(B)$, the generator matrix would be

$$\begin{pmatrix} I_{k_1} & 0 & B_1 & 2B_1 & A_1 & A_1 & D & E & F & J \\ 0 & I_{k_1} & 2B_1 & B_1 & A_1 & A_1 & K & L & M & N \\ 0 & 0 & I_{k_2} & I_{k_2} & 0 & 0 & A_4 & A_4 & 0 & 0 \\ 0 & 0 & 0 & 0 & I_{k_3} & 2I_{k_3} & 0 & 0 & B_4 & 2B_4 \end{pmatrix}$$

where $D = A_2 + B_2$, $E = A_2 + 2B_2$, $F = A_3 + B_3$,$J = A_3 + 2B_3$, $K = A_2 + 2B_2$, $L = A_2 + B_2$, $M = A_3 + 2B_3$, and $N = A_3 + B_3$. In addition, for $\psi_2(B)$, we have

$$\begin{pmatrix} I_{k_1} & 0 & 0 & 0 & 0 & 2A_1 & 2A_2 & 0 & 2A_3 & 0 \\ 0 & I_{k_1} & 0 & 0 & 2B_1 & 0 & 0 & 2B_2 & 0 & 2B_3 \\ 0 & 0 & I_{k_2} & 0 & 0 & 0 & A_4 & 0 & 0 & 0 \\ 0 & 0 & 0 & I_{k_3} & 0 & 0 & 0 & 0 & 0 & B_4 \end{pmatrix}.$$

Based on their generator matrices, it is easy to see that both $\psi_1(B)$ and $\psi_2(B)$ are free codes.

Now we will find the generator matrix of $\psi(B)$ in terms of the associated ternary codes of B. The following lemmas will be used in deriving G_ψ.

LEMMA 1. *Let A be a $k \times n$ ternary matrix and $\psi(A)$ be the matrix whose rows are the image of rows of A under the mapping ψ. Then $\psi(wA) = (aA \otimes bA)$ where $\psi(w) = (a,b), w \in R_3$.*

Proof:

Let $A = (y_1, y_2, \ldots, y_n)$ where each $y_i, 1 \le i \le n$ is $k \times 1$ ternary matrix representing the columns of A. Now, $wA = (wy_1, wy_2, \ldots, wy_n)$ where $w \in \mathbb{F}_3$ and $\psi(w) = (a,b)$.

Hence,

$$\begin{aligned} wA &= ((av_1 + bv_2)y_1, (av_1 + bv_2)y_2, \ldots, (av_1 + bv_2)y_n) \\ &= ((ay_1v_1 + by_1v_2), (ay_2v_1 + by_2v_2), \ldots, (ay_nv_1 + by_nv_2)). \end{aligned}$$

Then, we have

$$\begin{aligned} \psi(wA) &= (ay_1, ay_2, \ldots, ay_n, by_1, by_2, \ldots, by_n) \\ &= (aA \otimes bA). \end{aligned}$$

■

LEMMA 2. *Let x_i and y_i represent the rows of B^+ and B^- respectively. Then,*

$$G = \begin{pmatrix} (1+v)x_{k_1} + (1+2v)y_{k_2} \\ (1+v)x_{k_2} \\ (1+2v)y_{k_3} \end{pmatrix}.$$

Proof:

Let z_i be the ith row of G. For $1 \le i \le k_1$, we have $(1+v)z_i = (1+v)x_i$ and $(1+2v)z_i = (1+2v)y_i$. Also, $z_i = 2((1+v)x_i \oplus (1+2v)y_i)$. Hence, x_{k_1} and y_{k_1} are multiples of $(1+v)x_i \oplus (1+2v)y_i$.

For $k_1 + 1 \le i \le k_1 + k_2$, we have $z_i = (1+v)x_i$. Also, for $k_1 + k_2 + 1 \le i \le k_1 + k_2 + k_3$, $z_i = (1+2v)y_i$. Hence, we have the result. ■

THEOREM 3. *If $\psi(1+v) = (a,b)$ and $\psi(1+2v) = (c,d)$, then*

$$G_\psi = \begin{pmatrix} aG[B^+] & bG[B^+] \\ cG[B^-] & dG[B^-] \end{pmatrix}.$$

Proof:

By Lemma 1, for $1 \le i \le k_1$, we have

$$\begin{aligned} \psi(z_i) &= \psi((1+v)x_i) \oplus \psi((1+2v)y_i) \\ &= (ax_i \otimes bx_i) \oplus (cy_i \otimes dy_i). \end{aligned}$$

Note that $(ax_i \oplus bx_i)$ is not a multiple of $(cy_i \oplus dy_i)$ because of the presence of a, b and c, d.

Further, for $k_1 + 1 \le i \le k_1 + k_2$,

$$\begin{aligned} \psi(z_i) &= \psi((1+v)x_i) \\ &= (ax_i \otimes bx_i). \end{aligned}$$

For $k_1 + k_2 + 1 \le i \le k_1 + k_2 + k_3$,

$$\psi(z_i) = \psi((1+2v)y_i) \\ = (ay_i \otimes by_i).$$

The existence of $(ax_i \oplus bx_i) = (ax_j \oplus bx_j)$ and $(ay_i \oplus by_i) = (ay_j \oplus yx_j)$ is impossible because the rows of B^+ and B^- are linearly independent.

Hence, by Lemma 2,

$$G_\psi = \begin{pmatrix} ax_{k_1} & bx_{k_1} \\ cy_{k_1} & dy_{k_1} \\ ax_{k_2} & bx_{k_3} \\ cy_{k_3} & dy_{k_3} \end{pmatrix} = \begin{pmatrix} ax_{k_1} & bx_{k_1} \\ ax_{k_2} & bx_{k_3} \\ cy_{k_1} & dy_{k_1} \\ cy_{k_3} & dy_{k_3} \end{pmatrix}$$

$$= \begin{pmatrix} aG[B^+] & bG[B^+] \\ cG[B^-] & dG[B^-] \end{pmatrix}.$$

■

5. IMAGES OF SELF-DUAL AND CYCLIC CODES

PROPOSITION 1. *The image of the dual of B is given by:*

$$\psi(B^\perp) = (a(B^+)^\perp \oplus c(B^-)^\perp) \otimes (b(B^+)^\perp \oplus d(B^-)^\perp)$$

where $\psi(1+v) = (a,b)$ and $\psi(1+2v) = (c,d)$.

Proof:

From (2), $B^\perp = (1+v)(B^+)^\perp \oplus (1+2v)(B^-)^\perp$.

Therefore, by Lemma 1,

$$\psi(B^\perp) = \psi((1+v)(B^+)^\perp) \oplus \psi((1+2v)(B^-)^\perp) \\ = (a(B^+)^\perp \otimes b(B^+)^\perp) \oplus (c(B^-)^\perp \otimes d(B^-)^\perp) \\ = (a(B^+)^\perp \oplus c(B^-)^\perp) \otimes (b(B^+)^\perp \oplus d(B^-)^\perp).$$

■

We now derive sufficient conditions for the image to be self-dual or cyclic.

PROPOSITION 2. *If B is self-dual, then $\psi(B)$ is Type III if $\langle\psi(1+v), \psi(1+2v)\rangle = 0$.*

Proof:

Define $(A,B) = \{(x,y) | x \in A, y \in B\}$ where A and B are linear codes. Let $\psi(1+v) = (a,b)$ and $\psi(1+2v) = (c,d)$. Hence, by Proposition 1,

$$\psi(B) = (aB^+ + cB^-, bB^+ + dB^-)$$

and

$$\psi(B^\perp) = (a(B^+)^\perp + c(B^-)^\perp, b(B^+)^\perp + d(B^-)^\perp).$$

Let $x = (x_1, x_2, \ldots, x_n) \in B$ where $x_i = s_i(1+v) + t_i(1+2v)$ and $y = (y_1, y_2, \ldots, y_n) \in B^\perp$ where $y_i = s'_i(1+v) + t'_i(1-v)$.

Hence,

$$\psi(x) = (as_1 + ct_1, \ldots, as_n + ct_n, bs_1 + dt_1, \ldots, bs_n + dt_n)$$

and

$$\psi(y) = (as'_1 + ct'_1, \ldots, as'_n + c_t n', bs'_1 + dt'_1, \ldots, bs'_n + dt'_n).$$

Thus, $\langle\psi(x), \psi(y)\rangle$

$$= \sum_{i=1}^{n} (as_i + ct_i)(as'_i + ct'_i) + \sum_{i=1}^{n} (bs_i + dt_i)(bs'_i + dt'_i)$$

$$= ac \sum_{i=1}^{n} (s'_i t_i + s_i t'_i) + bd \sum_{i=1}^{n} (s'_i t_i + s_i t'_i)$$

$$= (ac + bd) \sum_{i=1}^{n} (s'_i t_i + s_i t'_i) = 0$$

since $ac + bd = \langle\psi(1+v), \psi(1+2v)\rangle = 0$. Thus, $\psi(B) = \psi(B^\perp) = (\psi(B))^\perp$. ■

Using the previous proposition, the following result is immediate from the images of $1+v$ and $1+2v$ under the mappings ψ_1 and ψ_2.

COROLLARY 1. *If B is a self-dual, then $\psi_1(B)$ and $\psi_2(B)$ are both Type III.*

Using the fact that B is self-dual if both the associated codes are self-dual, then we have the following corollary.

COROLLARY 2. *If B^+ and B^- are both self-dual, then $\psi_1(B)$ and $\psi_2(B)$ are also Type III.*

The following theorem considers cyclic codes.

THEOREM 4. *If B is cyclic, then $\psi(B)$ is quasi-cyclic of order 2.*

Proof:

Let $x = (x_1, x_2, \ldots, x_n)$ where $x_i = s_i v_1 + t_i v_2$. Since B is cyclic, then $\sigma(x) = (x_n, x_1, \ldots, x_{n-1}) \in B$.

Hence,

$$\psi(\sigma(x)) = (s_n, s_1, \ldots, s_{n-1}, t_n, t_1, \ldots, t_{n-1})$$

$$= (\sigma(s), \sigma(t)) = \varphi(\psi(x)) \in \psi(B).$$

Thus, $\psi(B)$ is quasi-cyclic of order 2. ■

We also have the following results.

Proposition 3. *Let $x = av_1 + bv_2 \in R_3$. Then, $\psi\rho = \sigma\psi$ if and only if $\forall c \in R_3, zx = bv_1 + av_2$.*

Proof:

Let $x = (x_1, x_2, \ldots, x_n) \in R_3^n$ where $x_i = a_i v_1 + b_i v_2, 1 \leq i \leq n$. Also, let $z \in R_3$ such that $zx_i = a_i v_2 + b_i v_1$. Thus,

$$\begin{aligned}\psi(\rho x) &= \psi(zx_n, x_1, \ldots, x_{n-1}) \\ &= (b_n, a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_{n-1}) \\ &= \sigma(\psi(x))\end{aligned}$$

■

It is worth noting that under ψ_1, if $z \in R_3$ is a unit or equal to $2 + 2v$, then the statement above holds.

Theorem 5. *The ternary image of a linear z-cyclic code C is a linear cyclic code if v_1 and v_2 are units in R_3.*

Proof:

Since v_1 and v_2 are units in R_3, then there exists z such that $zv_1 = v_2$ and $zv_2 = v_1$ Let C be a z-cyclic code over R_3. Then, by Proposition 3, for all $c \in C$, $\sigma(\psi(c)) = \psi(\rho(c)) \in \psi(C)$. Hence, $\psi(C)$ is cyclic ■

6. EXAMPLES

For the following examples, we consider the mapping ψ with respect to the basis $\{1, v\}$. We created a $MAGMA^{®}$ routine to compute for the distances of the following codes. We denote by d_H and δ the Hamming distances of the R_3- code and image code respectively.

Example 1. *The rate-2/4 systematic linear block code B over R_3 with generator matrix*

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

has $d_H = 2$. Then, $\psi(B)$ 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 $|B| = |\psi(B)| = 81$.

Example 2. *The rate-2/4 systematic self-dual linear block code B over R_3 with generator matrix*

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

has $d_H = 3$. Its image $\psi(B)$ is a rate-4/8 systematic self-dual ternary linear block code generated by

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

with $\delta = 3$ and $|B| = |\psi(B)| = 81$.

Example 3. *The rate-2/4 linear block code over R_3 generated by*

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

is cyclic with $d_H = 2$.
Its image under ψ_1 is a rate-4/8 quasi-cyclic ternary linear code of order 2 generated by

$$G_{\psi_1} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 2 \end{pmatrix}$$

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

7. REFERENCES

[1] C. Bachoc. Application of coding theory to the construction of modular lattices. *J. Combin. Theory*, 78:92–119, 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*, IT-50:356–358, 2004.

[3] Y. Cengellenmis. A characterization of codes over $\mathbb{F}_3$. *International Journal of Algebra*, 4(6):261–265, 2010.

[4] Y. Cengellenmis. On the cyclic codes over $\mathbb{F}_3 + v\mathbb{F}_3$. *International Journal of Algebra*, 4(6):253–259, 2010.

[5] R. Chapman, S. Dougherty, P. Gaborit, and P. Solè. 2-modular lattices from ternary codes. *Journal de Theorie des Nombres de Bordeaux*, 14(1):73–85, 2002.

[6] S. Dougherty, P. Gaborit, M. Harada, A. Munemasa, and P. Solè. Type IV self- dual codes over rings. *IEEE Trans. Inform. Theory*, 45(7):2345–2360, 1999.

[7] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solè. The $\mathbb{Z}_4$ -linearity of kerdock, preparata, goethals and related codes. *IEEE Trans. Inform. Theory*, 40:301–319, 1994.

[8] J. M. Lampos and V. Sison. Bounds on the p^r- ary image of linear block codes over finite semi-local frobenius ring $\mathbb{F}_{p^r} + v\mathbb{F}_{p^r}$. *Southeast-Asian J. of Sciences*, 1(1):76–98, 2012.

[9] J. Lapitan and V. Sison. Ternary images of linear block codes over rings of order 9. *Undergraduate Special Problem, University of the Philippines, Los Baños, Laguna*, 2007.

[10] 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*, 388.

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

[12] S. Zhu, Y. Wang, and M. J. Shi. Cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$. *ISIT 2009, Seoul, Korea*, pages 1719–1722, 2009.