On the Minimum Hamming Distance of the p^m-ary Image of Linear Block Codes over the Finite Chain Ring $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{r-1}\mathbb{F}_{p^m}, u^r = 0$

Jane D. Palacio, Virgilio P. Sison, John Mark T. Lampos

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

{ jdpalacio, vpsison, jmtlampos}@uplb.edu.ph

ABSTRACT

Let $\mathbb{F}_{p^m}$ denote the finite field with p^m elements where p is a prime. In this paper, linear block codes over $\mathbb{F}_{p^m}$ are considered as images of linear block codes over the finite chain ring $R(p^m, r) = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{r-1}\mathbb{F}_{p^m}$, where $u^r = 0$ and $m, r \in \mathbb{N}$. An $\mathbb{F}_{p^m}$-linear map is defined from $R(p^m, r)^n$ to $\mathbb{F}_{p^m}^{rn}$. Bounds on the minimum Hamming distance of the resultant codes are derived. These bounds largely depend on the minimum Hamming distance of the linear block code, the average value of the homogeneous weight on the residue field $\mathbb{F}_{p^m}$ and the nilpotency index of the ring. A code meeting these bounds whose image is the extended binary Hamming code of order 3 is also given.

Keywords

finite chain ring, p^m-ary image, distance bounds

1. INTRODUCTION

Bachoc in [7] used linear block codes over $\mathbb{F}_p + u\mathbb{F}_p$ in the construction of modular lattices. This work motivated the study of linear block codes over finite chain rings of the form $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}, u^2 = 0$. In particular, the ring $\mathbb{F}_2 + u\mathbb{F}_2 = \{0, 1, u, 1+u\}, u^2 = 0$ is of special interest since it is additively analogous to $\mathbb{F}_4$ and multiplicatively analogous to $\mathbb{Z}_4$. The properties of linear block code over this ring were studied in papers such as [1],[8],[11],[20] and [23]. Optimal codes, that is, codes that has the maximal minimum distance for a given length and dimension, were obtained in [14] and [15]. Many of the results concerning these rings have been extended over the finite commutative chain rings of the form $R(p^m, r)$ ([2]-[6],[9]-[10],[16]-[17] and [21]).

A code of length n over the Galois field $\mathbb{F}_{p^m}$ induces a code of length nm over the base field $\mathbb{F}_p$ by using a basis of $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$. This construction was used in [22] and an upper bound on the minimum Hamming distance of the p^m-ary image was derived. In [24], a similar construction was used to construct codes over $\mathbb{Z}_{p^m}$ from codes over the Galois ring $GR(p^r, m)$. Bounds on the minimum homogeneous distance of the p^r-ary image were then derived.

In this work, we consider linear block codes over the finite chain ring $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{r-1}\mathbb{F}_{p^m}$ with $u^r = 0$ to construct linear block codes over $\mathbb{F}_{p^m}$ using a basis of $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{r-1}\mathbb{F}_{p^m}$ over $\mathbb{F}_{p^m}$. Bounds on the minimum Hamming distance of the image codes are derived.

The material is organized as follows. A discussion on the preliminary concepts is given in Section 2. In Section 3, bounds on the minimum Hamming distance of the p^m-ary images of linear block codes over $R(p^m, r)$ are presented. A code meeting these bounds is given in the last section.

2. PRELIMINARIES AND DEFINITIONS

2.1 Linear Block Codes over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{r-1}\mathbb{F}_{p^m}$

Let p be prime and $m, r \in \mathbb{N}$. The ring $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m} + \cdots + u^{r-1}\mathbb{F}_{p^m}, u^r = 0$, which we shall denote here by $R(p^m, r)$ is a finite chain ring of length r with maximal ideal (u) and residue field $\mathbb{F}_{p^m}$. Any element a of $R(p^m, r)$ can be written uniquely as

$$a = a_1 + a_2 u + \cdots + a_r u^{r-1}, \quad a_i \in \mathbb{F}_{p^m}.$$

The ideals of $R(p^m, r)$ are $R(p^m, r), (u), (u^2), \ldots, (u^r)$ which are linearly ordered by set inclusion as shown below.

$$(0) \subset (u^{r-1}) \subset \cdots \subset (u^2) \subset (u) \subset R(p^m, r).$$

The cardinality of the ideal (u^i) is $p^{m(r-i)}, i = 0, 1, 2, \ldots, r$. The nilpotent elements of $R(p^m, r)$ are the elements of (u) and its units are the elements of $R(p^m, r) \setminus (u)$. It is easy to show that $R(p^m, r)$ isomorphic to the quotient ring $\mathbb{F}_{p^m}[x]/(x^r)$. Also, the said ring can be shown to be isomorphic to the ring of all $r \times r$ matrices (a_{ij}) where $a_{i+1,j+1} = a_{ij}$, whenever $i \leq j$ and zero elsewhere, and $a_{ij} \in \mathbb{F}_{p^m}$ for all i, j through

the map

$$\sum_{i=1}^{r} a_i u^{i-1} \mapsto \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_r \\ 0 & a_1 & a_2 & \cdots & a_{r-1} \\ 0 & 0 & a_1 & \cdots & a_{r-2} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & a_1 \end{pmatrix}.$$

In addition, $R(p^m, r)$ is a Frobenius ring with generating character $\chi : R(p^m, r) \mapsto \mathbb{T}, \chi\left(\sum_{i=1}^{r} a_i u^{i-1}\right) = e^{\frac{2a_r \pi i}{p}}$, where $\mathbb{T}$ is the multiplicative group of unit complex numbers.

Further, the said ring is a vector space over $\mathbb{F}_{p^m}$ with dimension r. A basis of $R(p^m, r)$ over $\mathbb{F}_{p^m}$ is given by the set

$$\{1, u, u^2, \ldots, u^{r-1}\}.$$

A linear block code of length n over $R(p^m, r)$ is an $R(p^m, r)$-submodule of $R(p^m, r)^n$. It was shown in [19] that any linear block code over a finite chain ring has a unique form of generating matrix. In particular, linear block codes over $R(p^m, r)$ have generator matrices which after a suitable permutation of the coordinates can be written in the form

$$\begin{pmatrix} I_{k_0} & A_{01} & A_{02} & \cdots & A_{0,r-1} & A_{0,r} \\ 0 & uI_{k_1} & uA_{12} & \cdots & uA_{1,r-1} & uA_{1,r} \\ 0 & 0 & u^2 I_{k_2} & \cdots & u^2 A_{2,r-1} & u^2 A_{2,r} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \\ 0 & 0 & 0 & \cdots & u^{r-1} I_{k_{r-1}} & u^{r-1} A_{k-1,r} \end{pmatrix}$$

$$= \begin{pmatrix} A_0 \\ uA_1 \\ u^2 A_2 \\ \vdots \\ u^{r-1} A_{r-1} \end{pmatrix}$$

where the columns are grouped into blocks of sizes

$$k_0, k_1, \ldots, k_{r-1}, n - k$$

with $k_i \geq 0$ and $k = \sum_{i=0}^{r-1} k_i$. Moreover, $|C| = p^{mt}$ where $t = \sum_{i=0}^{r-1} (r-i)k_i$. A linear block code over $R(p^m, r)$ is free if and only if $k = k_0$ [18].

In [13], a homogeneous weight w_h on arbitrary chain rings is defined. We provide here the case of $R(p^m, r)$. The homogeneous weight on $R(p^m, r)$ with $\Gamma = (p^m - 1)p^{m(r-2)}$ is given by

$$w_h(x) = \begin{cases} (p^m - 1)p^{m(r-2)} & \text{if } x \in R \setminus (u^{r-1}) \\ p^{m(r-1)} & \text{if } x \in (u^{r-1}) \setminus \{0\} \\ 0 & \textit{otherwise} \end{cases}.$$

We extend this to a (homogeneous) weight function in $R(p^m, r)^n$: if $x = (x_1, x_2, \ldots, x_n)$ then $w_h(x) = \sum_{i=1}^{n} w_h(x_i)$. Also, we equip a linear block code over $R(p^m, r)$ with the usual Hamming metric which we shall denote by w_H. The homogeneous (resp. Hamming) distance between any distinct vectors $x, y \in R(p^m, r)^n$, denoted by $d_h(x, y)$ (resp. $d_H(x, y)$), is defined as $w_h(x - y)$ (resp. $w_H(x - y)$). We will denote the minimum homogeneous (resp. Hamming) distance of a linear block code over $R(p^m, r)$ by d_h (resp. d_H).

The following bound given in [12], referred to as the Plotkin bound, gives an upperbound on the minimum homogeneous distance of a code over finite Frobenius rings.

THEOREM 2.1. *(M. Greferath and M. E. O'Sullivan, [12]). Let R be a finite Frobenius ring that is equipped with a homogeneous weight w of average value Γ. Let C be a (not necessarily linear) block code of length n over R with minimum w-distance δ_{min}. Then*

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

2.2 The p^m-ary Images of Linear Block Codes over $R(p^m, r)$

Let $\sum_{i=1}^{r} a_i u_i$ be an element of $R(p^m, r)$, i.e., $a_i \in \mathbb{F}_{p^m}$ and the u_i's are distinct elements of a basis for $R(p^m, r)$. Define the mapping

$$\psi : R(p^m, r) \to \mathbb{F}_{p^m}^r$$

$$a_1 u_1 + a_2 u_2 + \cdots + a_r u_r \mapsto (a_1, a_2, \ldots, a_r)$$

We now extend ψ to $R(p^m, r)^n$ coordinate-wise. Suppose $c = (c_1, c_2, \ldots, c_n) \in R(p^m, r)^n$ and $c_i = a_{1_i} u_1 + a_{2_i} u_2 + \cdots + a_{r_i} u_r$. Then, $\psi(c) = (a_{1_1}, a_{2_1}, \ldots, a_{r_1}, \ldots, a_{1_n}, a_{2_n}, \ldots, a_{r_n})$. It is easy to show that ψ is an $\mathbb{F}_{p^m}$-module isomorphism.

THEOREM 2.2. *If B is a linear block code over $R(p^m, r)$ of length n, then $\psi(B) = \{\psi(c) | c \in B\}$ is a linear block code over $\mathbb{F}_{p^m}$ with length rn. Moreover, if B is free with rank k, then $\psi(B)$ is free with rank rk.*

Proof. First we show that for every $c \in B, \psi(c) \in \mathbb{F}_{p^m}^r$. Let $c = (c_1, c_2, \ldots, c_n) \in B$. $\psi(c_j) \in \mathbb{F}_{p^m}^r$ for any $j = 1, 2, \ldots, n$. Thus, $\psi(c) \in \mathbb{F}_{p^m}^{rn}$.

Next we show that $\psi(B)$ is a subspace of $\mathbb{F}_{p^m}^{rn}$. Let $y, y_1 \in \psi(B)$ and $s \in \mathbb{F}_{p^m}$. Then there exist $x, x_1 \in B$ such that $y = \psi(x)$ and $y_1 = \psi(x_1)$. Now, $y + sy_1 = \psi(x) + s\psi(x_1) = \psi(x + sx_1)$ since ψ is a group homomorphism. Moreover, $y + sy_1 \in \psi(B)$ since $x + sx_1 \in B$ whenever $x, x_1 \in B$.

Thus, $\psi(B)$ is a subspace of $\mathbb{F}_{p^m}^{rn}$, i.e., $\psi(B)$ is a linear block code over $\mathbb{F}_{p^m}$ of length rn.

Suppose that B is free with a k-dimensional basis with elements $b_i, i = 1, 2, \ldots, k$. Then every $x \in B$ can be written as

$$x = s_1 b_1 + s_2 b_2 + \cdots + s_k b_k$$

where $s_j = \sum_{i=0}^{r-1} a_i u^i \in R(p^m, r), j = 1, 2, \ldots, k$.

Now,

$$x = \left(\sum_{i=0}^{r-1} a_{1,i}u^i\right) b_1 + \left(\sum_{i=0}^{r-1} a_{2,i}u^i\right) b_2 + \cdots + \left(\sum_{i=0}^{r-1} a_{k,i}u^i\right) b_k$$
$$= \sum_{j=1}^{k}\sum_{i=0}^{r-1} a_{j,i}u^i b_j.$$

So,

$$\psi(x) = \sum_{j=1}^{k}\sum_{i=0}^{r-1} a_{j,i}\psi(u^i b_j).$$

That is, $\mathcal{B} = \{\psi(u^i b_j) | i = 0, 1, \ldots, r-1, j = 1, 2, \ldots, k\}$ is a spanning set of $\psi(B)$.

Since ψ is injective, $\psi(x) = 0$ if and only if $x = 0$. So, $\psi\left(\sum_{j=1}^{k}\sum_{i=0}^{r-1} a_{j,i}\psi(u^i b_j)\right) = 0$ if and only if $a_{j,i} = 0$, that is, the elements of $\mathcal{B}$ are linearly independent.

Thus, $\mathcal{B}$ is an rk-dimensional basis for $\psi(B)$.■

3. DISTANCE BOUNDS

A simple way to measure the *goodness* of a code is through its minimum distance. A code over a finite field is able to correct at most $\lfloor \frac{\delta-1}{2} \rfloor$ errors where δ is its minimum distance. Hence, we are interested with upper bounds of the minimum Hamming distance of the images of the linear block codes over $R(p^m, r)$. The simplest of these bounds is similar to the Singleton Bound for fields which gives an upper bound for the size of a code in terms of its rate and the size of the alphabet used. For the succeeding discussions, we let B be a rate-k/n linear block code over $R(p^m, r)$. Also, we denote by δ the minimum Hamming distance of $\psi(B)$.

THEOREM 3.3. *(Singleton-type Bound) Let B be free. Then, we have*

$$\delta \leq r(n-k) + 1. \tag{2}$$

Proof. If B is a free rate-k/n linear block code over $R(p^m, r)$, then $\psi(B)$ is a free rate-rk/rn linear block code over $\mathbb{F}_{p^m}$. Applying the Singleton bound for codes over fields, inequality (2) holds. ■

THEOREM 3.4. *(Plotkin-type Bound) If B is systematic, then*

$$\delta \leq \left\lfloor \frac{p^{m(rk-1)}}{p^{mrk}-1}(p^m - 1)rn \right\rfloor. \tag{3}$$

Proof. Recall that the residue field of $R(p^m, r)$ is $\mathbb{F}_{p^m}$. Since B is free rate-k/n, $\psi(B)$ is free rate-rk/rn. So, $|\psi(B)| = p^{mrk}$. Also, the Hamming weight on $\mathbb{F}_{p^m}$ is homogeneous with $\Gamma = \frac{p^m-1}{p^m}$. Thus, inequality (3) holds. ■

The next bound for the minimum Hamming distance of the image of B is in terms of the average homogeneous weight Γ on $\mathbb{F}_{p^m}$ and the minimum Hamming distance of B.

THEOREM 3.5. *(Rains-type Bound) For a code B, we have*

$$d_H \leq \delta \leq r d_H. \tag{4}$$

Proof. Note that δ is bounded above by rn. If for every $x \in B$, $w_H(x) = d_H$ then $\delta \leq r d_H$. Now, δ is bounded below by d_H since 1 is the minimum nonzero value of the Hamming weight on $\mathbb{F}_{p^m}$. Thus, inequality (4) holds. ■

The next bound requires the concept of subcodes introduced by V. Sison and P. Solè in [24]. Let B be a linear block code over a ring R. Then the *subcode of B generated by the codeword $x \in B$*, denoted by B_x, is the set $\{ax | a \in R\}$. A generalization of the Rabizzoni bound was derived in [24] using the concept of subcodes. Here we prove a parallel bound for linear codes over R. The proof presented here is based on the proof in [24].

THEOREM 3.6. *Let $x \in B, x \neq 0$. The subcode B_x is free if and only if $|B_x| = p^{mr}$.*

Proof. ($\Rightarrow$) Let B_x be free then the equation $ax = 0$ has only the trivial solution $a = 0$. In particular, $(a-b)x = 0$ which infers that $a = b$. Hence, $a \neq b$ implies $ax \neq bx$. Thus, $|B_x| = p^{mr}$.

($\Leftarrow$) Let $|B_x| = p^{mr}$. Then for any nonzero a and b, $ax \neq bx$ provided $a \neq b$. In other words, $a = b$ if $(a-b)x = 0$. But x generates B_x by definition. So, B_x is free. ■

THEOREM 3.7. *(Rabizzoni-type Bound) Let x be a minimum Hamming weight codeword, i.e., $w_H(x) = d_H$. Then*

$$\delta \leq \left\lfloor \frac{|B_x|}{|B_x|-1}\frac{p^m-1}{p^m} r d_H \right\rfloor. \tag{5}$$

Moreover, if B_x is free, then

$$\delta \leq \left\lfloor \frac{p^{m(r-1)}}{p^{rm}-1}(p^m-1) r d_H \right\rfloor. \tag{6}$$

Proof. Let x be a minimum-weight codeword in B, that is, $w_H(x) = d_H$ and consider the subcode $B_x = \{ax | a \in R\}$ of B generated by x. Let δ_x denote the minimum Hamming distance of $\psi(B_x)$.

The minimum Hamming distance of B_x is still d_H since B_x is a subcode of B. Also, $\psi(B_x)$ is a subcode of $\psi(B)$ with $\delta \leq \delta_x$. The effective length of $\psi(B_x)$ is $r d_H$ coming from the d_H nonzero positions in x. Applying Theorem (2.1). results to

$$\delta \leq \delta_x \leq \frac{|B_x|}{|B_x|-1}\frac{p^m-1}{p^m} r d_H.$$

Thus, inequality (5) holds.

By Theorem 3.6, inequality (6) follows. ■

4. EXAMPLE

Consider the free rate-2/4 cyclic code B over $\mathbb{F}_2 + u\mathbb{F}_2$ with generator matrix

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

The codewords of B are $(0,0,0,0), (0,1,u,1), (0,u,0,u), (0,1+u,u,1+u), (1,0,1,u), (1,1,1+u,1+u), (1,u,1,0), (1,1+u,1+u,1), (u,0,u,0), (u,1,0,1), (u,u,u,u), (u,1+u,0,1+u), (1+u,0,1+u,u), (1+u,1,1,1+u), (1+u,u,1+u,0), (1+u,1+u,1,1)$ with homogeneous distances 0 and 4. Also, the code is self-dual. Thus, the code is a Type II code in terms of the homogeneous weight. The minimum Hamming distance of B is $d_H = 2$.

Using the basis $\{1, 1+u\}$ of $\mathbb{F}_2 + u\mathbb{F}_2$ over $\mathbb{F}_2$, the binary image has minimum Hamming distance $\delta = 4$ and is also a Type II code. Moreover, the image is equivalent to the extended binary Hamming Code of order 3.

In the table below, we can see that δ meets the upper bound of all distance bounds except for the Singleton-type bound.

Table 1: Comparison of bounds for δ

Singleton-type	$\delta \leq 5$
Plotkin-type	$\delta \leq 4 = \lfloor 4.2\overline{6} \rfloor$
Rains-type	$1 \leq \delta \leq 4$
Rabizzoni-type	$\delta \leq 4$

Notice that the minimum-weight codeword in B are $(0,u,0,u)$ and $(u,0,u,0)$. Thus, B_x is not free and $|B_x| = 2$.

5. REFERENCES

[1] T. Abualrub. and I. Siap. Constacyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$. *J. Franklin Institute*, 346:520–529, 2009.

[2] T. Abualrub. and I. Siap. Cyclic codes over the rings $\mathbb{Z}_2 + u\mathbb{Z}_2$ and $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2u\mathbb{Z}_2$. *Designs, Codes and Cryptography*, 42:273–287, 2007.

[3] M. Al-Ashker and M. Hamoudeh. Cyclic codes over $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2 + \cdots + u^{k-1}\mathbb{Z}_2$. *Turk. J. Math*, 35:737–749, 2011.

[4] R. Alfaro. Linear codes over $\mathbb{F}_q[u]/(u^t)$. *Contemporary Mathematics*, 537:1–11, 2011.

[5] R. Alfaro and S. Bennett and J. Harvey and C. Thornburg. On distances and self-dual codes over $\mathbb{F}_q[u]/(u^t)$. *Involve*, 2(2):177–194, 2009.

[6] M. Al-Ashker and M. Hamoudeh. Cyclic codes over $\mathbb{Z}_2 + u\mathbb{Z}_2 + u^2\mathbb{Z}_2 + \cdots + u^{k-1}\mathbb{Z}_2$. *Turk. J. Math.*, 35:737–749, 2011.

[7] C. Bachoc. Application of coding theory to the construction of modular lattices. *J. Combin. Theory*, 78:92–119, 1997.

[8] A. Bonnecaze and P. Udaya. Cyclic Codes and Self-Dual Codes Over $\mathbb{F}_2 + u\mathbb{F}_2$. *IEEE Trans. Inform. Theory*, 45(4):1250–1255, 1999.

[9] Y. Cengellenmis. On some special codes over $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$. *Applied Mathematics Computation*, 218:720–722, 2011.

[10] Y. Cengellenmis. Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + \cdots + u^m\mathbb{F}_2$. *Int. J. Contemp. Math. Sciences*, 5(12):595–602, 2010.

[11] S. Dougherty and P. Gaborit and M. Harada and P. Solè. Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$. *IEEE Trans. Inform. Theory*, 45(1):32–45, 1999.

[12] M. Greferath and M. E. O' Sullivan. On bounds for codes over Frobenius rings under homogeneous weights. *Discrete Math.*, 289:11–24, 2004.

[13] M. Greferath and S. E. Schmidt. Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code. *IEEE Trans. Inform. Theory*, 45(7):2522–2524, 1999.

[14] T. Gulliver and M. Harada. Codes over $\mathbb{F}_3 + u\mathbb{F}_3$ and improvements to the bounds on ternary linear codes. *Designs, Codes and Cryptography*, 22:89–96, 2001.

[15] T. Gulliver and M. Harada. Construction of optimal type IV self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$. *IEEE Trans. Inform. Theory*, 45(7):2520–2521, 1999.

[16] M. Han and Y. Ye and S. Zhu and C. Xu and B. Don. Cyclic codes over $R = \mathbb{F}_p + u\mathbb{F}_p + \cdots + u^{k-1}\mathbb{F}_p$ with length $p^s n$. *Information Sciences*, 181:926–934, 2011.

[17] X. Kai and S. Zhu and P. Li. $(1+\lambda u)$ -Constacyclic codes over $\mathbb{F}_p[u]/(u^m)$. *Journal of the Franklin Institute*, 347:751–762, 2010.

[18] G. H. Norton and A. Sălăgean. On the Hamming distance of linear codes over finite chain rings. *IEEE Trans. Inform. Theory*, 46:1060–1067, 2000.

[19] G. H. Norton and A. Sălăgean. On the structure of linear and cyclic codes over a finite chain ring. *Appl. Algebra Engrg. Comm Comput.*, 10:489–506, 2000.

[20] J. Qian and L. Zhang and S. Zhu. $(1+u)$constacyclic and cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$. *Applied Mathematics Letters*, 820–823, 2006.

[21] J. Qian and L. Zhang and S. Zhu. DFT for cyclic codes over $\mathbb{F}_p + u\mathbb{F}_p + \cdots + u^{k-1}\mathbb{F}_p$. *J. Appl. Math and Computing*, 22(1-2):159–167, 2006.

[22] 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*, 388:209–212, 1989.

[23] I. Siap. Linear codes over $\mathbb{F}_2 + u\mathbb{F}_2$ and their complete weight enumerators. *Ohio State Univ. Math. Res Inst. Publ*, 10:259–271, 2002.

[24] V. Sison and P. Solè. 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)(6):2270–2273, 2007.