Images of Linear Block Codes over $F_q + uF_q + vF_q + uvF_q$

Jane D. Palacio, Virgilio P. Sison
Institute of Mathematical Sciences and Physics, University of the Philippines Los Baños, College, Laguna, Philippines
Email: jdpalacio@uplb.edu.ph, vpsison@uplb.edu.ph

Received 2013

ABSTRACT

In this paper, we considered linear block codes over $F_q + uF_q + vF_q + uvF_q$, where $q = p^m$, $m \in \mathbb{N}$. First we looked at the structure of the ring. It was shown that $R_q$ is neither a finite chain ring nor a principal ideal ring but is a local ring. We then established a generator matrix for the linear block codes and equipped it with a homogeneous weight function. Field codes were then constructed as images of these codes by using a basis of $F_q$. Bounds on the minimum Hamming distance of the image codes were then derived. A code meeting such bounds is given as an example.

Keywords: $q$-ary Images; Distance Bounds

1. Introduction

Let $p$ be a prime number, $m \in \mathbb{N}$, $q = p^m$ and $F_q$ denote the Galois field with $q$ elements. During the late 1990s, C. Bachoc used linear block codes over $F_p + uF_p$ for constructing modular lattices. Its success motivated the study of linear block codes over finite chain rings $F_p + uF_p$. And many of the results from these studies have been extended over finite chain rings of the form $F_q + uF_q + vF_q + uvF_q$. Such rings can be seen as natural extensions of $F_p + uF_p$.

In this work, we will analyze linear block codes over $R_q$. The structure of the ring will be discussed in Section 2. The generator matrix of linear block codes over $R_q$ and weight functions defined on $R_q$ will be tackled in Section 3. The $q$-ary images of these linear block codes and bounds on its minimum Hamming distance will be presented in Sections 4 and 5, respectively. Lastly, a code meeting these bounds is given in Section 6.

2. Preliminaries and Definitions

Structure of the Ring $F_q + uF_q + vF_q + uvF_q$

Let $R_q$ denote the ring $F_q + uF_q + vF_q + uvF_q$ whose elements can be uniquely written as $a + bu + cv + duv$ where $a, b, c, d \in F_q$. An element of $R_q$ is a unit if and only if $a \neq 0$. The ring has $q + 5$ ideals namely $(0), (uv), (v), (u, v), R_q, (u + jv)$ where $j \in F_q$. $R_q$ is not a principal ideal ring since the maximal ideal $(u, v)$ is generated by $u$ and $v$. The cardinality of the ideals are $|uv| = q, |v| = |u + jv| = q^2, |(u, v)| = q^3$, and $|R_q| = q^4$.

The lattice of ideals is shown in Figure 1. As can be seen in the lattice of ideals, $R_q$ is not a finite chain ring. But it is a local, Noetherian and Artinian ring. All zero divisors are the elements of $(u, v) \setminus (0)$ and its units are the elements of $R_q \setminus (u, v)$.

Figure 1. Lattice of ideals of $F_q + uF_q + vF_q + uvF_q$.
Clearly, the ring is isomorphic to \( F_q[x,y]/(x^2+y^2-xy) \). It is also isomorphic to the ring of all \( 4 \times 4 \) matrices of the form
\[
\begin{pmatrix}
a & b & c & d \\
0 & a & 0 & c \\
0 & 0 & a & b \\
0 & 0 & 0 & a
\end{pmatrix}.
\]

Moreover, \( R_q \) is Frobenius with generating character \( \chi : R_q \rightarrow T, a+bu+cv+duv \mapsto e^{\frac{2\pi i}{q}tr(a)} \) where \( tr \) denotes the trace map on \( F_q \) and \( T \) is the multiplicative group of unit complex numbers.

Further, \( R_q \) is a vector space over \( F_q \) with dimension 4. A basis of \( R_q \) over \( F_q \) is given by the set \( \{1,u,v,uv\} \) which we will refer to as the polynomial basis of \( R_q \).

Another basis considered in this work is
\[
\{1+u+v+uv,1+v+uv,1+u+uv,1+u+v\}.
\]

3. Linear Block Codes over \( F_q + uF_q + vF_q + uvF_q \)

Any linear block code over a finite commutative ring \( R \) has a generator matrix which can be put in the following form
\[
G = \begin{pmatrix}
a_{1,k_1} & A_{1,2} & A_{1,3} & \cdots & A_{1,j+1} \\
a_{2,k_1} & a_2 & A_{2,3} & \cdots & a_2 & A_{2,j+1} \\
\vdots & \ddots & \ddots & \ddots & \vdots \\
a_{j,k_1} & a_j & A_{j,3} & \cdots & a_j & A_{j,i+j+1}
\end{pmatrix}
\]

(1)

where \( A_{i,j} \) are binary matrices for \( i > 1 \) and are matrices over \( R_q \) for \( i = 1 \). A code of this form has \( \prod_{i=1}^{j}[a,R]^i \) elements, where the \( a_i \)'s define the nonzero equivalence classes \( [a_1],[a_2],\cdots,[a_i] \) under the equivalence relation on \( R \) defined by
\[
a - b \iff a = bu \quad \text{for a unit } u \in R
\]
\[
a_i R = \{x|v = ar \quad \text{for some } r \in R\}; 
\]

and the blanks in \( G \) are to be filled with zeros.

A linear block code \( B \) of length \( n \) over \( R_q \) is an \( R_q \)-submodule of \( R_q^n \). \( B \) has a generator matrix which can be put in the form shown in Figure 2 where \( A_{1,i} \)

are \( k_i \times k_j \) matrices over \( R_q \), \( D_{1,i} \) are \( k_i \times k_j \) matrices over \( F_q \) and the blank parts of \( G[B] \) are to be filled with zeros. Moreover, \( B \) has \( q^{k_i} \cdot q^{21} \cdot q^{k_i+3} \) codewords where \( t = \sum_{i=2}^{q+1} k_i \). A linear block code over \( R_q \) is free if and only if \( k_i = 0 \) for all \( i = 2,\cdots,q+3 \).

Now, we equip \( B \) with two weight functions namely the usual Hamming metric and a homogeneous weight function.

Lemma 2.1. (T. Honold, [2]) Let \( R \) be a Frobenius ring with generating character \( \chi \), then every homogeneous weight \( w_{\text{hom}} \) on \( R \) can be expressed in terms of \( \chi \) as follows
\[
w_{\text{hom}} = \Gamma \left[ 1 - \frac{1}{R'} \sum_{y \in R'} \chi(xy) \right] \tag{1}
\]

where \( R' \) is the group of units of \( R \).

Theorem 2.1. A homogeneous weight \( w_{\text{hom}} \) on \( R_q \) is given by
\[
w_{\text{hom}} (x) = \begin{cases} 
\Gamma & \text{if } x \in R_q \setminus \{uv\} \\
q & \text{if } x \in \{uv\} \setminus \{0\} \\
0 & \text{otherwise}
\end{cases} \tag{2}
\]

Proof: Let \( x = a + bu + cv + dv \in R_q \). Now, using the previous lemma, every homogeneous weight on \( R_q \) can be expressed as
\[
w_{\text{hom}} = \Gamma \left[ 1 - \frac{1}{(q-1)q} \sum_{y \in R} \chi(xy) \right]
\]

Case 1. Let \( x \in R_q' \). There are \( (q-1)q^2 \) units having the same \( d \), for any \( d \in F_q \). But there are \( p^{n-1} \) elements of \( F_q \) that has trace \( j \), for any \( j \in F_p \). Hence,
\[ \sum_{y \in R_q^o} \chi(xy) = (q-1)q^2 \left( p^{m-1} \right) \sum_{j \in F_p} e \frac{2 \pi i j}{p}. \]

But \( \sum e \frac{2 \pi i j}{p} = 0 \). So, \( w_{\text{hom}} = \Gamma. \)

Case 2. Let \( x \in (uv) \setminus \{0\} \). For every \( a \in F_q^o \), there are \( q^2 \) units of the form \( y = a + bu + cv + duv \). Now, \( p^{m-1} \) of these have the same trace value \( j \), for any \( j \in F_p \) while there are \( p^{m-1} - 1 \) of them with trace zero. Hence,

\[ \sum_{y \in R_q^o} \chi(xy) = q^3 \left( p^{m-1} \right) \sum_{j \in F_p} e \frac{2 \pi i j}{p} + q \left( p^{m-1} - 1 \right). \]

But \( \sum e \frac{2 \pi i j}{p} = -1 \). So, \( w_{\text{hom}} = \frac{q}{p-1} \Gamma. \)

Case 3. Let \( x \in (u,v) \setminus (uv) \). There are \( q-1 \) elements of \( (u,v) \setminus (uv) \) that have the same coefficient for \( uv \). For each element \( x \in (u,v) \setminus (uv) \) appears \( q \) copies in the multiset \( \{xy \mid y \in R_q^o, x \in (u,v) \setminus (uv)\} \). Moreover, there are \( p^{m-1} \) elements of \( F_q^o \) that have trace \( j \), for any \( j \in F_p \). Hence

\[ \sum_{y \in R_q^o} \chi(xy) = (q-1)q \left( p^{m-1} \right) \sum_{j \in F_p} e \frac{2 \pi i j}{p} = \Gamma. \]

We extend this to \( R_q^o \) naturally: if \( x = (x_1, x_2, \ldots, x_n) \) then \( w_{\text{hom}}(x) = \sum_{i=1}^n w_{\text{hom}}(x_i) \). The homogeneous (resp. Hamming) distance between any distinct vectors \( x, y \in R_q^o \), denoted by \( d_{\text{hom}}(x, y) \) (resp. \( d_{\text{H}}(x, y) \), is defined as \( w_{\text{hom}}(x-y) \) (resp. \( w_{\text{H}}(x-y) \)). We will denote the minimum homogeneous distance (resp. Hamming) distance by a linear block code over \( R_q \) by \( d_{\text{hom}} \) (resp. \( d_{\text{H}} \)).

4. The \( q \)-ary Images of Linear Block Codes over \( F_q + uF_q + vF_q + uvF_q \)

Let \( h_0, h_1, h_2, h_3, h_4 \) be distinct elements of an ordered basis of \( R_q \). Then any element of \( R_q \) can be written in the form \( \sum_{i=1}^4 a_i h_i \). Define the mapping \( \phi : R_q \rightarrow F_q \)

\[ \sum_{i=1}^4 a_i h_i \mapsto (a_1, a_2, a_3, a_4) \]

We then extend \( \phi \) to \( R_q^o \) coordinate-wise: if \( x = (x_1, x_2, \ldots, x_n) \) and \( x_i = \sum_{j=1}^4 a_{ij} h_j \) then \( \phi(x) = (a_{11}, \ldots, a_{14}, a_{21}, \ldots, a_{24}, a_{31}, \ldots, a_{34}, \ldots, a_{n1}, \ldots, a_{n4}) \).

It is easy to show that \( \phi \) is an \( F_q \)-module isomorphism.

**Theorem 4.1.** If \( B \) is a linear block code over \( R_q \) of length \( n \), then \( \phi(B) = \{ \phi(x) \mid x \in B \} \) is a linear block code over \( F_q^o \) with length \( 4n \).

**Proof:** First we show that for every \( x \in B, \phi(x) \in F_q^o \).

Let \( x = (x_1, x_2, \ldots, x_n) \in B \). Since \( \phi(x_i) \in F_q^4 \) for any \( i = 1, 2, \ldots, n \), then \( \phi(x) \in F_q^4 \). Next we show that \( \phi(B) \) is a subspace of \( F_q^4 \). Let \( s \in F_q^4 \) and let \( y, y_1 \in \phi(B) \). Then there exist \( x, x_1 \in B \) such that \( y = \phi(x) \) and \( y_1 = \phi(x_1) \). But \( sy + y_1 = \phi(sx + x_1) \) since \( \phi \) is a module homomorphism. Since \( sx + x_1 \in B \), \( sy + y_1 \in \phi(B) \). Thus, \( \phi(B) \) is a subspace of \( F_q^4 \).

**Theorem 4.2.** Let \( G[B] \) be the generator matrix of \( B \) given in Figure 2. Then \( \tilde{G} [\phi(B)] \) has a generator matrix that is permutation-equivalent to the matrix given in Figure 3.

![Figure 3. Generator Matrix of \( \phi(B) \).](image-url)
Proof: Let $B$ have a generator matrix given in Figure 2. Then for every $c \in B$, $c$ can be expressed as $yG$ where $y \in R_q^k$, $k = \sum_{i=1}^{k} k_i$, that is, $c = \sum_{i=1}^{k} s_i z_i$ where $s_i \in R_q$ and the $z_i$'s are the $k$ rows of $G[B]$. Using any basis of $R_q^n$, $c$ can further be written

$$\sum_{i=1}^{k} \sum_{j=1}^{k} d_{i,j} z_i z_j + \sum_{i=1}^{k} \sum_{j=1}^{k} b_{i,j} u z_i + \sum_{i=1}^{k} \sum_{j=1}^{k} c_{i,j} v z_i + \sum_{i=1}^{k} \sum_{j=1}^{k} d_{i,j} u v z_i.$$

Now,

$$\phi(c) = \sum_{i=1}^{k} \sum_{j=1}^{k} a_{i,j} \phi(z_i) + \sum_{i=1}^{k} \sum_{j=1}^{k} b_{i,j} \phi(u z_i) + \sum_{i=1}^{k} \sum_{j=1}^{k} c_{i,j} \phi(v z_i) + \sum_{i=1}^{k} \sum_{j=1}^{k} d_{i,j} \phi(u v z_i).$$

Hence, $S = \{ \phi(z_i), \phi(u z_i), \phi(v z_i), \phi(u v z_i) | i = 1, 2, \ldots, k \}$ spans $\phi(B)$. But

- $v z_i = 0$ whenever $i = k_i + 1, \ldots, k_i + k_i$ or $i = k - k_y + 1, \ldots, k$;
- $u z_i = 0$ whenever $i = k_i + k_i + 1, \ldots, k_i + k_i + k_i$ or $i = k - k_y + 1, \ldots, k$;
- $u v z_i = 0$ whenever $i > k_i$; and
- $u z_i = j v z_i$ for some $j \in F_q^*$ whenever $i = \sum_{i=1}^{k} k_i + 1, \ldots, \sum_{i=1}^{k} k_i$ for some $i$.

Define the set $\beta$ as the resulting set once the undesirable cases listed above are deduced from the set $S$. Notice that the elements of $\beta$ are the rows of the matrix given in Figure 3 we will denote by $M$. Now, define $B_i$ as the matrix that consists of the rows

$$4 k_i + 2 \sum_{i=2}^{k} k_i + 1, \ldots, 4 k_i + 2 \sum_{i=2}^{k} k_i$$

of $M$ so that $M$ can be written in the form

$$\begin{pmatrix}
B_1 \\
B_2 \\
\vdots \\
B_{k+1}
\end{pmatrix}.$$

We wish to show that the rows of $M$ are linearly independent. Without loss of generality, let $k_i = 1$ for all $i$. Consider a row of $B_i$. Clearly, it cannot be expressed as a linear combination of rows from any of the $B_j$'s, $j > i$. We know that $\phi(1), \phi(u), \phi(v), \phi(u v)$ are linearly independent and so any nonzero linear combination of these vectors is not the zero vector. Thus, any row of $B_i$ cannot be written as a linear combination of rows of any of the $B_j$'s, $j \leq i$. Hence, the rows of $M$ are linearly independent.

The succeeding theorems are direct consequences of Theorem 4.2.

**Corollary 4.3.** If $B$ is free with rank $k$, then $\phi(B)$ is free with rank $4k$.

**Corollary 4.4.** Let $B$ be a free rate $k/n$ linear block code over $R_q$ with generator matrix $(I_A)$, then the generator matrix of the $q$-ary image of $B$ with respect to the basis $\{1 + u + v + uv, 1 + v + uv, 1 + u + uv, 1 + u + v\}$ is permutation-equivalent to

$$\begin{pmatrix}
0 & I_k & I_k & E + F + H & D + E & D + F & D + H \\
I_k & 0 & I_k & 0 & D + E & 0 & D \\
I_k & 0 & 0 & D + F & D & 0 & F \\
I_k & 0 & 0 & I_k & D & 0 & 0 \\
\end{pmatrix}$$

where $A = D + Eu + Fv + Huv$.

**5. Distance Bounds of the Images of Linear Block Codes over $F_q^u + uF_q^v + vF_q^w + uvF_q^w$**

The minimum distance of a code gives a simple indication of the goodness of a code. A field code can correct at most $\frac{\delta - 1}{2}$ errors where $\delta$ is its minimum Hamming distance. Hence, we are interested with upper bounds of the minimum Hamming distance of the images of the linear block codes over $R_q$. For the succeeding discussions, let $B$ be a rate $k/n$ linear block code over $R_q$. Also, we denote by $\delta$ the minimum Hamming distance of $\phi(B)$.

**Theorem 5.1. (Singleton-type Bound)** Let $B$ be free. Then

$$\delta \leq 4(n - k) + 1.$$  

The above theorem is a direct consequence of Corollary 4.3 and the Singleton Bound for codes over fields while the next theorem is a direct consequence of the Plotkin Bound for codes over fields.

**Theorem 5.2. (Plotkin-type Bound)** Let $B$ be free. Then

$$\delta \leq \left\lfloor \frac{4^{k-1}}{q^{k-1}} (q - 1) (4n) \right\rfloor.$$  

The next bound is in terms of the average homogeneous weight $\Gamma$ on $F_q$ and the minimum Hamming distance of $B$.

**Theorem 5.3. (Rains-type bound)** For a code $B$,

$$d_H \leq \delta \leq 4 d_H.$$  

**Proof:** Note that $\delta$ is bounded above by $4n$. If for every $x \in B, w_H(B) = d_H$ then $\delta \leq 4 d_H$. Now, $\delta$ is bounded below by $d_H$ since 1 is the minimum nonzero value of the Hamming weight on $F_q$. Thus, inequality (4) holds.

Now, we use the concept of subcodes of $B$ generated by $x$ as defined by V. Sison and P. Sole in [4]. The subcode of $B$ generated by $x \in B$, denoted by $B_x$, is the set
\{ax \mid a \in R \}$. A generalization of the Rabizzoni bound was derived in [4]. Here we prove a parallel bound for linear block codes over $R_q$. The proof presented here is based on the proof in [4].

**Lemma 5.4.** Let $x \in B, x \neq 0$. $B_x$ is free if and only if $|B_x| = q^4$.

**Proof:** ($\Rightarrow$) Let $B_x$ be free then the equation $ax = 0$ has only the trivial solution. In particular, $(a-b)x = 0 \Rightarrow a = b$, that is, $a \neq b$ implies $ax \neq bx$. Thus, $|B_x| = q^4$.

($\Leftarrow$) Let $|B_x| = q^4$. Then for any nonzero $a$ and $b$, $a \neq b \Rightarrow ax \neq bx$. That is, $(a-b)x = 0 \Rightarrow a = b$. But $x$ generates $B_x$ by definition. So, $B_x$ is free.

The next statement is a direct consequence of the cardinality of the ideals of $R_q$

**Corollary 5.5.** Let $x \in B$. Then

- $x \in (uv)^n \backslash \{0\}^n$ if and only if $|B_x| = p^n$;
- $x \in (u+jv)^n \backslash (uv)^n$ or $x \in (v)^n \backslash (uv)^n$ if and only if $|B_x| = p^{2n}$;
- $x \in (u,v)^n \backslash S$ if and only if $|B_x| = p^{3n}$ where $S = \bigcup_{j \in F_q} (u+jv)^n \cup (v)^n$.

**Theorem 5.5.** (*Rabizzoni-type Bound*) Let $x$ be a minimum Hamming weight codeword. Then

$$\delta \leq \delta_x \leq \left[ \frac{|B_x|}{|B_x|-1} \frac{q-1}{q} 4d_H \right]. \quad (5)$$

Moreover, if $|B_x|$ is free, then

$$\delta \leq \delta_x \leq \left[ \frac{q^3}{q^3-1} \frac{(q-1)}{q} 4d_H \right]. \quad (6)$$

**Proof:** Let $x$ be a minimum Hamming weight codeword in $B$ then consider subcode $B_x$. Let $\delta_x$ denote the minimum Hamming distance of $\phi(B_x)$. The minimum Hamming distance of $B_x$ is still $d_H$ since $B_x$ is a subcode of $B$. Also $\phi(B_x)$ is a subcode of $\phi(B)$ with $\delta \leq \delta_x$. The effective length of $\phi(B_x)$ is $4d_H$ coming from the $d_H$ nonzero positions in $x$. Direct application of the Rabizzoni bound results to inequality (5) holds. By Lemma 5.4, inequality (6) follows.

### 6. Example

Consider the free rate-1/4 self-orthogonal code $B$ over $R_2$ generated by $G = (1 + v 1 + u + v 1 + u + v)$. If $G = (1 A)$ then $I_1 = 1, D = (1 1 1), E = (0 0 1), F = (1 1 0)$ and $H = (0 0 1)$. A codeword in $B$ either has homogeneous weight 0, 4, or 8. The minimum Hamming distance of $B$ is 4. The binary image of $B$ was obtained with respect to the basis

$$\{1+u+v+uv, 1+v+uv, 1+u+uv, 1+u \}.$$

<table>
<thead>
<tr>
<th>Table 1. Comparison of bounds for $\delta$.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Singleton-type</td>
</tr>
<tr>
<td>Plotkin-type</td>
</tr>
<tr>
<td>Rains-type</td>
</tr>
<tr>
<td>Rabizzoni-type</td>
</tr>
</tbody>
</table>

Using Corollary 4.4, $G[\phi(B)]$ is permutation-equivalent to

$$
\begin{align*}
01111110010000001110 & 0 \\
10101010000001111101 & 1110000011110001110 & 0 \\
10011110000011110000 & 00000011111 & 1110001110 \\
10011110000011110000 & 00000011111 & 1110001110
\end{align*}
$$

The image code has a minimum Hamming distance of 8 and is self-orthogonal. In Table 1, we can see that $B$ meets the upper bound of the Plotkin-type and Rabizzoni-type bound.

### REFERENCES


