involve

a journal of mathematics

On distances and self-dual codes over $F_q[u]/(u^t)$

Ricardo Alfaro, Stephen Bennett, Joshua Harvey and Celeste Thornburg

mathematical sciences publishers

2009 Vol. 2, No. 2

INVOLVE 2:2(2009)

On distances and self-dual codes over $F_q[u]/(u^t)$

Ricardo Alfaro, Stephen Bennett, Joshua Harvey and Celeste Thornburg

(Communicated by Nigel Boston)

New metrics and distances for linear codes over the ring $\mathbb{F}_q[u]/(u^t)$ are defined, which generalize the Gray map, Lee weight, and Bachoc weight; and new bounds on distances are given. Two characterizations of self-dual codes over $\mathbb{F}_q[u]/(u^t)$ are determined in terms of linear codes over $\mathbb{F}_q$. An algorithm to produce such self-dual codes is also established.

1. Introduction

Many optimal codes have been obtained by studying codes over general rings rather than fields. Lately, codes over finite chain rings (of which $\mathbb{F}_q[u]/(u^t)$ is an example) have been a source of many interesting properties [Norton and Salagean 2000a; Ozbudak and Sole 2007; Dougherty et al. 2007]. Gulliver and Harada [2001] found good examples of ternary codes over $\mathbb{F}_3$ using a particular type of *Gray map.* Siap and Ray-Chaudhuri [2000] established a relation between codes over $\mathbb{F}_q[u]/(u^2 - a)$ and codes over $\mathbb{F}_q$ which was used to obtain new codes over $\mathbb{F}_3$ and $\mathbb{F}_5$. In this paper we present a certain generalization of the method used in [Gulliver and Harada 2001] and [Siap and Ray-Chaudhuri 2000], defining a family of metrics for linear codes over $\mathbb{F}_q[u]/(u^t)$ and obtaining as particular examples the *Gray map,* the *Gray weight,* the *Lee weight* and the *Bachoc weight.* For the latter, we give a new bound on the distance of those codes. It also shows that the Gray images of codes over $\mathbb{F}_2 + u\mathbb{F}_2$ are more powerful than codes obtained by the so-called u-$(u+v)$ condition.

With these tools in hand, we study conditions for self-duality of codes over $\mathbb{F}_q[u]/(u^t)$. Norton and Salagean [2000b] studied the case of self-dual cyclic codes in terms of the generator polynomials. In this paper we study self-dual codes in terms of linear codes over $\mathbb{F}_q$ that are obtained as images under the maps defined on the first part of the paper. We provide a way to construct many self-dual codes over $\mathbb{F}_q$ starting from a self-dual code over $\mathbb{F}_q[u]/(u^t)$. We also study self-dual codes

MSC2000: primary 94B05, 94B60; secondary 11T71.

Keywords: linear codes over rings, self-dual codes.

This project was partially supported by the Office of Research of the University of Michigan–Flint.

in terms of the torsion codes, and provide a way to construct many self-dual codes over $\mathbb{F}_q[u]/(u^t)$ starting from a self-orthogonal code over $\mathbb{F}_q$. Our results contain many of the properties studied by Bachoc [1997] for self-dual codes over $\mathbb{F}_3+u\mathbb{F}_3$.

2. Metric for codes over $\mathbb{F}_q[u]/(u^t)$

We will use $R(q,t)$ to denote the commutative ring $\mathbb{F}_q[u]/(u^t)$. The q^t elements of this ring can be represented in two different forms, and we will use the most appropriate in each case. First, we can use the polynomial representation with indeterminate u of degree less than or equal to $(t-1)$ with coefficients in $\mathbb{F}_q$, using the notation $R(q,t)=\mathbb{F}_q+u\mathbb{F}_q+u^2\mathbb{F}_q+\cdots+u^{t-1}\mathbb{F}_q$. We also use the u-ary coefficient representation as an $\mathbb{F}_q$-vector space.

Let $B\in M_t(\mathbb{F}_q)$ be an invertible $t\times t$ matrix, and let B act as right multiplication on $R(q,t)$ (seen as $\mathbb{F}_q$-vector space). We extend this action linearly to the $\mathbb{F}_q$-module $(R(q,t))^n$ by concatenation of the images $\phi_B:(R(q,t))^n\to(\mathbb{F}_q)^{tn}$ given by

$$\phi_B(x_1,x_2,\ldots,x_n)=(x_1B,x_2B,\ldots,x_nB)$$

An easy counting argument shows that ϕ_B is an $\mathbb{F}_q$-module isomorphism and if C is a linear code over $R(q,t)$ of length n, then $\phi_B(C)$ is a linear q-ary code of length tn.

Example 1. Consider the ring $R(3,2)=\mathbb{F}_3+u\mathbb{F}_3$ with $u^2=0$. Choosing

$$B=\begin{pmatrix}0&1\\1&1\end{pmatrix},$$

we obtain the *Gray map* $\phi_B:(\mathbb{F}_3+u\mathbb{F}_3)^n\to\mathbb{F}_3^{2n}$ with

$$(a+ub)B=\begin{pmatrix}a&b\end{pmatrix}\begin{pmatrix}0&1\\1&1\end{pmatrix}=\begin{pmatrix}b&a+b\end{pmatrix}$$

used by Gulliver and Harada [2001].

Each such matrix B induces a new metric in the code C.

Definition 1. *Let C be a linear code over $R(q,t)$. Let B be an invertible matrix in $M_t(\mathbb{F}_q)$, and let ϕ_B be the corresponding map. The B-weight of an element $x\in R(q,t)$, $w_B(x)$, is defined as the Hamming weight of xB in $(\mathbb{F}_q)^t$. Also, the B-weight of a codeword $(x_1,\cdots,x_n)\in C$ is defined as*:

$$w_B(x_1,\cdots,x_n)=\sum_{i=1}^{n}w_B(x_i).$$

Similarly, the B-distance between two codewords in C is defined as the B-weight of their difference, and the B-distance, d_B, of the code C is defined as the minimal B-distance between any two distinct codewords.

Example 2. In the example above, the corresponding *B-weight* of an element of $\mathbb{F}_3 + u\mathbb{F}_3$ is given by

$$\begin{aligned} w_B(x) &= w_B(a+ub) = w_H((a+ub)B) \\ &= w_H(b, a+b) = \begin{cases} 0 & \text{if } x = 0, \\ 1 & \text{if } x = 1, 2, 2+u, 1+2u, \\ 2 & \text{otherwise,} \end{cases} \end{aligned}$$

which coincides with the *Gray weight* given in [Gulliver and Harada 2001].

Example 3. Consider the matrix

$$B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix};$$

the corresponding *B-weight* of an element of $\mathbb{F}_2 + u\mathbb{F}_2$ is given by

$$w_B(x) = w_B(a+ub) = w_H((a+ub)B) = w_H(a+b, b) = \begin{cases} 0 & \text{if } x = 0, \\ 1 & \text{if } x = 1, 1+u, \\ 2 & \text{if } x = u, \end{cases}$$

which produces the *Lee weight* w_L for codes over $\mathbb{F}_2 + u\mathbb{F}_2$.

Example 4. Consider the matrix

$$B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix};$$

the corresponding *B-weight* of an element of $\mathbb{F}_q + u\mathbb{F}_q$ is given by

$$\begin{aligned} w_B(x) &= w_B(a+ub) = w_H((a+ub)B) \\ &= w_H(b, a) = \begin{cases} 0 & \text{if } x = 0, \\ 1 & \text{if exactly one of } a \text{ or } b \text{ is nonzero}, \\ 2 & \text{if both } a \text{ and } b \text{ are nonzero}, \end{cases} \end{aligned}$$

which produces the Gray weight for codes in [Siap and Ray-Chaudhuri 2000].

The case $B = I_t$ corresponds to the special weight studied in [Ozbudak and Sole 2007] with regards to Gilbert–Varshamov bounds. A theorem similar to [Ozbudak and Sole 2007, Theorem 3] can be obtained using special families of matrices B. The definition leads immediately to the fact that ϕ_B preserves weights and distances between codewords.

When the generator matrix of a code C is of the form $G = (\mathrm{I} \;\; \mathrm{M})$, C is called a *free code* over $R(q, t)$. In this case, we can establish the correspondence between the parameters of the codes; see [Siap and Ray-Chaudhuri 2000, Section 2.2]. The case of nonfree codes will be considered later in Proposition 4.

Proposition 1. *Let B be an invertible matrix over $M_t(\mathbb{F}_q)$, let C be a linear free code over $R(q,t)$ of length n with B-distance d_B, and let ϕ_B be the corresponding map. Then $\phi_B(C)$ is a linear $[tn, tk, d_B]$-code over $\mathbb{F}_q$. Furthermore, the Hamming weight enumerator polynomial of the linear code $\phi_B(C)$ over $\mathbb{F}_q$ is the same as the B-weight enumerator polynomial of the code C over $R(q,t)$.*

Proof. Since B is nonsingular, $\phi_B(C)$ is a linear code over $\mathbb{F}_q$, with the same number of codewords. A basis for $\phi_B(C)$ can be obtained from a (minimal) set of generators for C, say, $y_1, y_2, \dots, y_k$. The set $\{u^i y_j \mid i = 0..(t-1),\ j = 1..k\}$ forms a set of generators for C as an $\mathbb{F}_q$-submodule. Since C is free and B is invertible, it follows that $\{\phi_B(u^i y_j) \mid i = 0..(t-1),\ j = 1..k\}$ are linearly independent over $\mathbb{F}_q$ and form a basis for the linear code $\phi_B(C)$. Hence the dimension of the code $\phi_B(C)$ is tk. The equality of distance follows from the definition. □

In matrix form, we can construct a generator matrix for the linear code $\phi_B(C)$ as follows. Let G be a matrix of generators for C. For each row $(x_1, x_2, \dots, x_n)$ of G consider the matrix representation $(X_1, X_2, \dots, X_n)$ of the elements of $R(q,t)$ given by

$$X_i = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{t-1} \\ 0 & a_0 & a_1 & \cdots & a_{t-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & a_0 \end{pmatrix}.$$

For a free code, the rows of the matrix $(X_1 B, X_2 B, \dots, X_n B)$ produce t linearly independent generators for the linear code $\phi_B(C)$. Repeating this process for each row of G, we will obtain the tk generators for $\phi_B(C)$. We denote this matrix by $\phi_B(G)$. For the case of nonfree linear codes, several rows will become zero and need to be deleted from the matrix. A counting of these rows will be given in Section 3.

Some choices of B can produce some optimal ternary and quintic codes as we now illustrate.

Example 5. Consider a linear code C over $\mathbb{F}_3 + u\mathbb{F}_3$ of length 9 with generator matrix:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & u & 2{+}u & 1{+}u & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & u & 2{+}u & 1{+}u & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & u & 2{+}u & 1{+}u \\ 0 & 0 & 0 & 1 & 1{+}u & 1 & 0 & u & 2{+}u \end{pmatrix}$$

Let

$$B = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

The *B-weight* enumerator polynomial is given by

$$1+98x^7+206x^8+412x^9+780x^{10}+1032x^{11}+1308x^{12}+1224x^{13}$$
$$+828x^{14}+462x^{15}+166x^{16}+40x^{17}+4x^{18}.$$

The corresponding linear ternary code $\phi_B(C)$ is an optimal ternary $[18,8,7]$-code.

Notice that if we take

$$B=\begin{pmatrix}1&2\\1&0\end{pmatrix},$$

we get a linear ternary code $\phi_B(C)$ of length 18, dimension 8, but now, with minimal distance 4. The challenge now is to look for matrices B that produce optimal codes.

Example 6. Consider a linear code C over $\mathbb{F}_5+u\mathbb{F}_5$ of length 5 with a generator matrix:

$$G=\begin{pmatrix}1&0&2u&3+3u&4\\0&1&4&2u&3+3u\end{pmatrix}.$$

Let

$$B=\begin{pmatrix}3&0\\2&3\end{pmatrix}.$$

The linear $\mathbb{F}_5$-code $\phi_B(C)$ is an optimal $[10,4,6]$-code, with generator matrix given by

$$\phi_B(G)=\begin{pmatrix}1&0&0&0&2&3&2&2&0&3\\0&1&0&0&2&3&3&1&2&1\\0&0&1&0&0&3&2&3&2&2\\0&0&0&1&2&1&2&3&3&1\end{pmatrix}.$$

Example 7. Consider a linear code C over $R(5,3)=\mathbb{F}_5+u\mathbb{F}_5+u^2\mathbb{F}_5$ of length 14 with generator matrix obtained by cyclic shifts of the first 5 components and cyclic shift of the last 9 components of the vector:

$$\begin{pmatrix}1&0&0&0&0&u&3+3u&2+4u&4u&0&4&3+u^2&2+u+u^2&u+u^2\end{pmatrix}.$$

Let

$$B=\begin{pmatrix}0&3&3\\0&0&4\\3&3&2\end{pmatrix}.$$

The *B-weight* enumerator polynomial is given by

$$1+24x^{16}+32x^{17}+80x^{18}+150x^{19}+158x^{20}+140x^{21}+82x^{22}+44x^{23}+14x^{24}+4x^{25}$$

and the linear $\mathbb{F}_5$-code $\phi_B(C)$ is an optimal [42, 15, 16]-code over $\mathbb{F}_5$.

3. Metrics using the torsion codes

A generalization of the residue and torsion codes for $\mathbb{F}_2 + u\mathbb{F}_2$ has been studied in [Norton and Salagean 2000b] where a *generator matrix* for a code C over $R(q,t)$ is defined as a matrix G over $R(q,t)$ whose rows span C and none of them can be written as a linear combination of the other rows of G. Recalling that two codes over $R(q,t)$ are *equivalent* if one can be obtained from the other by permuting the coordinates or by multiplying all entries in a specified coordinate by an invertible element of $R(q,t)$, and performing Gauss elimination (remembering not to multiply by nonunits) we can always obtain a generator matrix for a code (or equivalent code) which is in *standard form*, that is, in the form

$$G = \begin{pmatrix} I_{k_1} & B_{1,2} & B_{1,3} & B_{1,4} & \cdots & B_{1,t} & B_{1,t+1} \\ 0 & uI_{k_2} & uB_{2,3} & uB_{2,4} & \cdots & uB_{2,t} & uB_{2,t+1} \\ 0 & 0 & u^2 I_{k_3} & u^2 B_{3,4} & \cdots & u^2 B_{3,t} & u^2 B_{3,t+1} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0 & \cdots & u^{t-1} I_{k_t} & u^{t-1} B_{t,t+1} \end{pmatrix},$$

where $B_{i,j}$ is a matrix of polynomials in $\mathbb{F}_q[u]/(u^t)$ of degrees at most $j-i-1$. In fact, we can think of $B_{i,j}$ as a matrix of the form

$$B_{i,j} = A_{i,j,0} + A_{i,j,1}u + \cdots + A_{i,j,j-i-1}u^{j-i-1},$$

where the matrices $A_{i,j,r}$ are matrices over the field $\mathbb{F}_q$.

We define the following *torsion codes* over $\mathbb{F}_q$:

$$C_i = \{X \in (\mathbb{F}_q)^n \;\mid\; \exists\, Y \in (\langle u^i \rangle)^n \;\, with\;\, Xu^{i-1} + Y \in C\},$$

for $i = 1 \ldots t$. It is then easy to see that these are linear q-ary codes, and we have:

Proposition 2. *Let C be a linear $R(q,t)$ code of length n, and let C_i, $i = 1 \ldots t$ be the torsion codes defined above. Then*

(1) $C_1 \subseteq C_2 \subseteq \cdots \subseteq C_t$;

(2) *a generator matrix for the code C_1 is given by*

$$G_1 = \begin{pmatrix} I_{k_1} & A_{1,2,0} & A_{1,3,0} & \cdots & A_{1,t+1,0} \end{pmatrix};$$

(3) *if G_i is a generator matrix for the code C_i, then a generator matrix G_{i+1} for the code C_{i+1} is given by*

$$G_{i+1} = \begin{pmatrix} & & & G_i & & & \\ 0 & \cdots & 0 & I_{k_{i+1}} & A_{i+1,i+2,0} & \cdots & A_{i+1,t+1,0} \end{pmatrix}.$$

Proof. Let $X \in C_i$, then there exists $Y \in (\langle u^i \rangle)^n \mid z := Xu^{i-1} + Y \in C$. Then $uz \in C$. But $uz = Xu^i + uY \in C$. Hence $X \in C_{i+1}$. Now, let $X \in C_1$. Then there exist vectors $Y_i, i = 1..t-1$ over $(\mathbb{F}_q)^n$ such that $X + Y_1 u + \cdots + Y_{t-1}u^{t-1} \in C$. Thus, the coefficients of X must come from independent coefficients of elements on the first row-group of the generator matrix G. A similar reasoning indicates that at each stage, the remaining generators come from the independent coefficients of elements in the next row-group of the matrix G. $\square$

Note that the code C_i has dimension $k_1 + \cdots + k_i$. The code C then contains all products $[v_1, v_2, \ldots, v_t]G$ where the components of the vectors $v_i \in (R(q,t))^{k_i}$ have degree at most $t-i$. The number of codewords in C is then $q^{(t)k_1+(t-1)k_2+\cdots+k_t}$, which can also be seen as $q^{k_1}q^{k_1+k_2}\ldots q^{k_1+k_2+\cdots k_t}$. For the case $\mathbb{F}_2 + u\mathbb{F}_2$, the code C_1 is called the *residue* code, and the code $C_t = C_2$ is called the *torsion* code.

For $X \in C_i$, we know there exists $Y \in (\langle u^i \rangle)^n$ such that $Xu^{i-1} + Y \in C$. Y can be written as

$$Y = u^i\overline{Y} + \text{hot}, \quad \text{with } \overline{Y} \in \mathbb{F}_q^n,$$

where 'hot' designates *higher order terms*. With this notation, define the map

$$F_i : C_i \to \mathbb{F}_q^n / C_{i+1}$$

by $F_i(X) = \overline{Y} + C_{i+1}$. If two such vectors $Y_1, Y_2 \in (\langle u^i \rangle)^n$ exist, we have

$$Y_1 = u^i\overline{Y}_1 + \text{hot} \quad \text{and} \quad Y_2 = u^i\overline{Y}_2 + \text{hot}.$$

Then,

$$Y_2 - Y_1 = u^i(\overline{Y}_2 - \overline{Y}_1) + \text{hot} \in C.$$

Therefore $\overline{Y}_2 - \overline{Y}_1 \in C_{i+1}$ and F_i is well defined. It is easy to see that the maps F_i are $\mathbb{F}_q$-morphisms. By its very definition, it can be seen that the image of these maps consist of direct sums of the matrices $A_{i,j,r}$ in a generator matrix G for C in standard form. We then have:

Theorem 1. *Let C be a code over $R(q,t)$ with a generator matrix G in standard form. C is determined uniquely by a chain of linear codes C_i over $\mathbb{F}_q$ and $\mathbb{F}_q$-module homomorphisms $F_i : C_i \to \mathbb{F}_q^n / C_{i+1}$.*

Example 8. If $G = (I_{k_1} A)$ then $C_1 = C_2 = \cdots = C_t$. Also $k_i = 0$ for all $i \geq 2$ and hence the code C has $(q^t)^{k_1}$ elements. These are called *free codes* since they are free $R(q,t)$-modules. Furthermore, if $A = A_0 + uB_1 + u^2B_2 + \cdots + u^{t-1}B_{t-1}$, where B_i is a matrix over $\mathbb{F}_q$, then C_1 determines A_0 and $F_i(C_i)$ determines B_i.

Example 9. Let

$$G = \begin{pmatrix} 1 & 0 & 2 & 2+u & 1+u+u^2 \\ 0 & 1 & 1 & 1+2u & u+u^2 \\ 0 & 0 & u & 2u & u+u^2 \\ 0 & 0 & 0 & u^2 & 2u^2 \end{pmatrix}$$

be a generator matrix for a code C over $R(3,3)$. The corresponding generator matrices for the linear codes are:

$$C_1 = \begin{pmatrix} 1 & 0 & 2 & 2 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}, \qquad \text{a } [5,2,3]\text{-code over } \mathbb{F}_3,$$

$$C_2 = \begin{pmatrix} 1 & 0 & 2 & 2 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 2 & 1 \end{pmatrix}, \qquad \text{a } [5,3,2]\text{-code over } \mathbb{F}_3,$$

$$C_3 = \begin{pmatrix} 1 & 0 & 2 & 2 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix}, \qquad \text{a } [5,4,1]\text{-code over } \mathbb{F}_3,$$

and the code C has $(3^3)^2(3^2)^1(3)^1 = 27^3$ codewords.

Utilizing the torsion codes of C we can define a new weight on C and obtain a bound for their minimum distance.

Definition 2. *Let $x \in R(q,t)$ and let p be the characteristic of the field $\mathbb{F}_q$. Let $i_0 = \max\{i \mid x \in \langle u^i \rangle\}$. Define the p-weight of x as $\omega t_p(x) = p^{i_0}$, if $x \neq 0$ and $\omega t_p(0) = 0$. For an element of $(R(q,t))^n$ define the p-weight as the sum of the p-weights of its coordinates.*

Note. For the case $R(2,2) = \mathbb{F}_2 + u\mathbb{F}_2$, the p-weight coincides with the Lee weight, and for $R(p,2) = \mathbb{F}_p + u\mathbb{F}_p$, the p-weight coincides with the Bachoc weight defined in [Bachoc 1997].

Theorem 2. *Let C be a linear code over $R(q,t)$, and let $C_1, C_2, \ldots, C_t$ be the associated torsion codes over $\mathbb{F}_q$. Let d_i be the Hamming distance of the codes C_i, then the minimum weight d of the code C with respect to the p-weight satisfies*

$$\min\{p^{i-1}d_i \mid i = 1, .., t\} \leq d \leq p^{t-1}d_t.$$

Proof. Let $W = (y_1, y_2, \ldots, y_n) \in C$ with minimum weight. Then for some i, $W = u^i X + Y$ with $Y \in \langle u^{i+1} \rangle$. Thus $X \in C_{i+1}$ and $\omega t_p(W) \geq p^i \cdot \mathrm{wt}_H(X) \geq p^i d_{i+1}$. Now take $X_1 \in C_t$ to be a word of minimum weight d_t, then $u^{t-1}X_1 \in C$, and, by the minimality of W, we have $\omega t_p(W) \leq \omega t_p(u^{t-1}X_1) = p^{t-1}d_t$. □

It is well known [Bonnecaze and Udaya 1999; Ling and Sole 2001], that the Lee weight for a cyclic code C over $\mathbb{F}_2 + u\mathbb{F}_2$ is the lower bound above. Here we show an example over $\mathbb{F}_2 + u\mathbb{F}_2$ that attains the upper bound.

Example 10. Let C be the linear code over $\mathbb{F}_2 + u\mathbb{F}_2$, with generator matrix

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

The codeword (u, u, u, u) has Lee (or 2-) weight 8, while all the other nonzero codewords have weight 4. On the other hand C_1 and C_2 are equal with generator matrix

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

Hence $d_1 = d_2 = 2$, and $\min\{d_1, 2d_2\} = 2 \neq d$.

Since the p-weight coincides with the Lee weight for codes over $\mathbb{F}_2 + u\mathbb{F}_2$, we obtain the general version for the Lee weight of those codes as a corollary of Theorem 2.

Corollary 1. *The minimum Lee weight of a code C over $\mathbb{F}_2 + u\mathbb{F}_2$, satisfies*

$$\min\{d_1, 2d_2\} \leq d \leq 2d_2$$

where d_1, d_2 are respectively the Hamming distance of the residue code C_1 and the torsion code C_2.

Example 11. Return to Example 9 over $R(3, 3)$ with $d_1 = 3$, $d_2 = 2$, $d_3 = 1$. Hence $3 \leq d \leq 9$. The first and second generators combine to form a codeword of p-weight 3. Hence $d = 3$, and in this example the minimum weight attains the lower bound.

Example 12. Let C be the linear code over $\mathbb{F}_3 + u\mathbb{F}_3$, with generator matrix

$$G = \begin{pmatrix} 1 & 0 & u & 2 \\ 0 & 1 & 1+u & u \end{pmatrix}.$$

There are only 4 codewords with 2 zero entries, and they have Bachoc weight (and hence p-weight) 6. There are no codewords with Bachoc weight 3, and the Bachoc distance d of the code is 4. On the other hand the associated ternary codes are

$$C_1 = C_2 = \begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

Thus $d_1 = d_2 = 2$ and the Bachoc weight d lies strictly between the bounds given above.

Corollary 2. *For free codes the p-weight d satisfies*: $d_1 \leq d \leq p^{t-1} d_1$.

We can also use the torsion codes to study the Hamming weight of the code C. The results given here use a straightforward proof in comparison with the proof given in [Norton and Salagean 2000a].

For a code C over $R(q, t)$ and $w \in C$, we denote $w_H(w)$ the usual Hamming weight of w. Accordingly, the minimum Hamming distance of the code will be denoted by $d_H(C)$.

Proposition 3. *Let C be a linear code over $R(q,t)$, and let $C_1, C_2, \dots, C_t$ be the associated torsion codes over $\mathbb{F}_q$. Let d_i be the Hamming distance of the codes C_i, then the minimal Hamming weight d_H of the code C satisfies*

$$dd_H = d_t \le d_{t-1} \le \cdots \le d_1.$$

Proof. Since $C_i \subseteq C_{i+1}$, it follows that $d_{i+1} \le d_i$, for $i = 1..t$ Now let $X \in C_t$. Then $Xu^{t-1} \in C$ and hence $d_H \le d_t$. Conversely, let w^* be a codeword in C with minimum Hamming weight d_H. Let j be the maximum integer such that u^j divides w^*. Then $w^* = u^j v$ and $z = u^{t-j-1}w^* = u^{t-1}v \in C$. Thus $\hat{v} \in C_t$, where $\hat{v}$ denotes the canonical projection from $R(q,t)^n$ into $\mathbb{F}_q^n$. We then have $w_H(w^*) \ge w_H(\hat{v}) \ge d_t$, and therefore $d_H \ge d_t$. □

From the above proof, the Singleton bound for C_t, and the comment after Proposition 2, we have:

Corollary 3. *Let C be a linear code over $R(q,t)$, and let $C_1, C_2, \dots, C_t$ be the associated torsion codes. Then*:

$$d_H \le n - (k_1 + k_2 + \cdots k_t) + 1.$$

Proposition 4. *$\phi_B(C)$ is a $[\,nt,\ \sum_{i=1}^{t} k_i(t-i+1)\ ,\, d^*]$ linear code over $\mathbb{F}_q$, with $d^* \le t d_t$.*

Proof. Since u^{i-1} divides y_j for each y_j in the i-th row-block of G, $u^s y_j = 0$ for $s \ge t-i+1$. Furthermore, the generators $u^s y_j \ne 0$ for $s < t-i+1$ are linearly independent. Since there are k_i such y_j, we have

$$\dim(\phi_B(C)) = \sum_{i=1}^{t} k_i\big(t-(i-1)\big). \qquad \square$$

4. Self-dual codes over $\mathbb{F}_q[u]/(u^t)$ using torsion codes

Duality for codes over $\mathbb{F}_q[u]/(u^t)$ is understood with respect to the inner product $x \cdot y = \sum x_i y_i$, where $x_i,\ y_i \in R(q,t)$. As usual, a code is called *self-dual* if $C = C^\perp$, and is called *self-orthogonal* is $C \subseteq C^\perp$.

First, we give an examples of self-dual codes over $R(q,t)$ of length n when t is even and n is a multiple of p (the characteristic of the field $\mathbb{F}_q$.) The construction mimics the C_n codes studied by Bachoc [1997] for the case $t = 2$.

Example 13. For t even, let $I = \langle u^{t/2} \rangle \subseteq R(q,t)$. Define the set:

$$D_n := \{(x_1, x_2, \dots, x_n) \in R(q,t)^n \mid \sum_{i=1}^{n} x_i = 0 \text{ and } x_i - x_j \in I \text{ for all } i \ne j\}.$$

Let $X, Y \in D_n$,

$$X \cdot Y = \sum_{i=1}^{n} x_i y_i = \sum_{i=1}^{n} (x_i - x_1)(y_i - y_1) + \sum_{i=1}^{n} x_i y_1 + \sum_{i=1}^{n} x_1 y_i - n x_1 y_1.$$

The first term is in $I^2 = 0$, the next two terms are zero by definition and the third term is zero since $p|n$. Thus $D_n \subseteq D_n^{\perp}$. Now, for each $i = 1 \ldots n$, we can write $x_i = a + b_i$ where a is a common polynomial of degree less than $t/2$, and $b_i \in I$ with $\sum b_i = 0$. There are $q^{t/2}$ choices for a, and $(q^{n-1})^{t/2}$ choices for the b_i's, thus

$$|D_n| = q^{t/2}(q^{n-1})^{t/2} = q^{nt/2},$$

and hence D_n is self-dual.

The torsion q-ary codes are as follows: for $i = 1, \ldots t/2$, C_i is the code generated by the **1** word, with $d_i = n$; and for $i = t/2 + 1 \ldots t$, C_i is the parity check code of length n and dimension $n - 1$, thus $d_i = 2$. Applying Theorem 2, we obtain

$$\min\{n, 2p^{t/2}\} \leq d \leq 2p^{t-1}.$$

But 1 and $(0, 0, \ldots, 0, u^{t/2}, -u^{t/2}, 0, \ldots, 0) \in D_n$, hence $d = \min\{n, 2p^{t/2}\}$.

We study self-orthogonal and self-dual codes over $R(q, t)$ taking two different approaches. We look at the linear codes $\phi_B(C)$, and also look at the torsion codes corresponding to C.

To study the latter we need some results on the parity check matrix of these codes, which can be defined in terms of block matrices using the recurrence relation

$$D_{i,j} = \sum_{k=i+1}^{t+2-j} -B_{i,k} D_{k,j}$$

for blocks, such that $i + j \leq t + 1$. For blocks such that $i + j = t + 2$, $D_{i,j} = u^{t-j+1} I_{k_j}$ for $i = 2, \ldots, t$ and $D_{t+1,1} = I_{n-(k_1+k_2+\ldots k_t)}$. All remaining blocks are 0. From here a generator matrix for the dual code can be obtained and we easily observe the following relations: $k_1(C^{\perp}) = n - (k_1 + \ldots + k_t)$ and $k_h(C^{\perp}) = k_{t-h+2}(C)$ for $h = 2, \ldots, t$.

A different recurrence relation for the definition of the parity check matrix is given in [Norton and Salagean 2000a].

Proposition 5. *Let C be an $R(q, t)$ code, and let C_i's be its corresponding torsion codes. Then*

$$(C^{\perp})_i = (C_{t-i+1})^{\perp},\ i = 1..t.$$

Proof. Let $w \in (C^{\perp})_i$ and $v \in C_{t-i+1}$. Then there exists $z \in (\langle u^i \rangle)^n$ with $a := w u^{i-1} + z \in C^{\perp}$, and $y \in (\langle u^{t-i+1} \rangle)^n$ with $b := v u^{t-i} + y \in C$. Since $a \cdot b = 0$, we

have
$$0 = (wu^{i-1} + z) \cdot (vu^{t-i} + y) = (w \cdot v)u^{t-1},$$
which implies $w \cdot v = 0$, and $w \in (C_{t-i+1})^{\perp}$. So $(C^{\perp})_i \subseteq (C_{t-i+1})^{\perp}$. Looking at dimensions

$$\begin{aligned}\dim((C^{\perp})_i) &= \sum_{j=1}^{i} k_j(C^{\perp}) = n - (k_1 + \ldots + k_t) + \sum_{j=2}^{i} k_{t-j+2}(C) \\ &= n - \sum_{j=1}^{t-i+1} k_j(C) = n - \dim(C_{t-i+1}) = \dim((C_{t-i+1})^{\perp}). \qquad \square\end{aligned}$$

Using the generator in standard form of a code C and forming the inner products of its row-blocks we obtain:

Proposition 6. *Let C be an $R(q,t)$ code with a generator matrix in standard form. C is self-orthogonal if and only if*

$$\sum_{h=0}^{k} \sum_{j=\max\{i,k\}}^{t+1} A_{i,j,h} A^{t}_{l,j,k-h} = 0, \qquad \textit{for each } k = 0, \ldots, t-(i+l-2)-1.$$

This gives us the first characterization of self-dual codes:

Theorem 3. *Let C be an $R(q,t)$ code; and let C_i's be its corresponding torsion codes. The code C is self-orthogonal and $C_i = C^{\perp}_{t-i+1}$ if and only if C is self-dual.*

Proof. By Proposition 5 we have $(C^{\perp})_i = C^{\perp}_{t-i+1} = C_i$ for all $i = 1 \ldots t$. Furthermore, $\mathsf{rk}(C) = \dim(C_t) = \dim((C^{\perp})_t) = \mathsf{rk}(C^{\perp})$; but C is self-orthogonal, hence $C = C^{\perp}$. Similarly, the converse follows immediately from Proposition 5. $\square$

As an immediate consequence we have:

Corollary 4. *If C is self-dual, then C_i is self-orthogonal for all $i \leq (t+1)/2$.*

Note that when t is odd, $C_{\lfloor (t+1)/2 \rfloor}$ is self-dual and hence n must be even. For the case t even, we can contruct self-dual codes of even or odd length.

Proposition 6 and Theorem 3 provide us with an algorithm to produce self-dual codes over $R(q,t)$ starting from self-orthogonal codes over $\mathbb{F}_q$.

(1) Take a self-orthogonal code C_1 over $\mathbb{F}_q$.

(2) Define $C_t := C_1^{\perp}$.

(3) Choose a set of self-orthogonal words $\{R_1, R_2, ..., R_l\}$ in C_t that are linearly independent from C_1. Define

$$C_2 := \langle C_1 \cup \{R_1, R_2, \ldots, R_l\} \rangle \quad \text{and} \quad C_{t-1} = C_2^{\perp}.$$

(4) Repeat, if possible, the step above defining C_i and $C_{t-i+1} = C_i^{\perp}$ until you produce $C_{\lfloor (t+1)/2 \rfloor}$.

(5) For each $i = 1..t$, multiply the generators of $\{C_{i+1} - C_i\}$ by u^i. This will produce a self-dual code.

Additional self-dual codes are obtained as follows:

(6) Form a generator matrix G in standard form, adding, where appropriate, variables to represent higher powers of u.

(7) Now we find the system of equations on the defined variables arising from Proposition 6. Note that for fixed $i, l = 1 \dots t$ each k will produce a matrix equation, which in turn produces several nonlinear equations.

(8) Write this system of equations in terms of the independent variables. There will be

$$\sum_{i=1}^{\lfloor t/2 \rfloor} \sum_{j=i}^{t-i} (t-i-j+1) k_i k_j$$

equations on

$$\sum_{i=1}^{t-1} \sum_{j=i+2}^{t+1} (j-i-1) k_i k_j \text{ total variables.}$$

(9) By Theorem 3 every solution to this system of equations will produce a self-dual code (some may be equivalent).

We now provide an example of this construction.

Example 14. Self-dual codes in $R(3,4)$:

Consider the self-orthogonal code

$$C_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 2 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Define

$$C_4 := C_1^{\perp} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 2 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Since there are no more self-orthogonal words in C_4 to append to C_1, we let $C_2 := C_1$, and since $C_2^{\perp} = C_4$ we let $C_3 := C_4$. Multiplying the rows in $C_3 - C_2$ by u^2 we obtain a generator matrix for a self-dual code over $R(3,4)$:

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

Now we can form a generator matrix using variables to represent higher powers of u obtaining

$$\begin{pmatrix} 1 & 0 & au & bu & 1+cu+du^2+eu^3 & 2+fu+gu^2+hu^3 \\ 0 & 1 & iu & ju & 1+ku+lu^2+mu^3 & 1+nu+pu^2+qu^3 \\ 0 & 0 & u^2 & 0 & ru^3 & su^3 \\ 0 & 0 & 0 & u^2 & tu^3 & vu^3 \end{pmatrix}.$$

The equation

$$\sum_{h=0}^{k} \sum_{j=\max\{i,k\}}^{t+1} A_{i,j,h} A^t_{l,j,k-h} = 0$$

produces a system of equations over $\mathbb{F}_q$. For example, for $i = 1, l = 2, k = 3$ we obtain the equation

$$\begin{aligned} a + r + 2s &= 0, \\ b + t + 2v &= 0, \\ i + r + s &= 0, \\ j + t + v &= 0. \end{aligned}$$

Likewise, the remaining equations can be obtained, and we solve in terms of a set of independent variables $\{a, b, h, i, j, n, p\}$:

$$\begin{aligned} c &= n, \\ d &= ai + bj + i^2 + j^2 + p + 2a^2 + 2b^2, \\ e &= n(ai + bj + i^2 + j^2 + 2n^2 + p) + h, \\ f &= n, \\ g &= a^2 + b^2 + ai + bj + i^2 + j^2 + n^2 + p, \\ k &= 2n, \\ l &= i^2 + j^2 + 2p + 2n^2, \\ m &= n(i^2 + j^2 + 2a^2 + 2b^2 + ai + bj) + 2h, \\ q &= n(a^2 + b^2 + p + 2ai + 2bj + 2n^2) + h, \\ r &= a - 2i, \\ s &= i - a, \\ t &= b - 2j, \\ v &= j - b. \end{aligned}$$

These equations allow us to generate up to 3^7 self-dual codes over $R(3,4)$. As an example, letting all the independent variables take the value 1 except for $b=0$, we obtain the self-dual code

$$\begin{pmatrix} 1 & 0 & u & 0 & 1+u+u^3 & 2+u+u^3 \\ 0 & 1 & u & u & 1+2u+u^3 & 1+u+u^2+u^3 \\ 0 & 0 & u^2 & 0 & 2u^3 & 0 \\ 0 & 0 & 0 & u^2 & u^3 & u^3 \end{pmatrix}.$$

5. Self-dual codes over $\mathbb{F}_q[u]/(u^t)$ using linear images

As discussed in Section 2, given a code C over $R(q,t)$ of length n and a nonsingular $t \times t$ matrix B over $\mathbb{F}_q$, we can define a linear code $\phi_B(C)$ over $\mathbb{F}_q$ of length nt. In this section, we will consider an element $x \in R(q,t)$ in its polynomial representation, and will use $\overline{x}$ for its vector representation.

Let $w = (w_1, w_2, \ldots, w_n)$ be a codeword in C. Recall that

$$\phi_B(w) = (\overline{w}_1 B, \overline{w}_2 B, \ldots, \overline{w}_n B).$$

Let E denote the square matrix

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \iddots & \\ \vdots & \iddots & & \\ 1 & & & 0 \end{pmatrix} \quad \text{over } \mathbb{F}_q.$$

Theorem 4. *If C is self-orthogonal and $BB^T = cE$ where $c \neq 0 \in \mathbb{F}_q$, then $\phi_B(C)$ is self-orthogonal.*

Proof. Let R_j denote the j-th row of B. Then $R_j R_k^T = c$, for all $j+k < t+2$ and $R_j R_k^T = 0$, for all $j+k \geq t+2$. If $w, v \in C$, then

$$\begin{aligned} &\phi_B(w)\phi_B(v) \\ &\quad = \sum_{i=1}^{n} \overline{w}_i B(\overline{v}_i B)^T = \sum_{i=1}^{n} \overline{w}_i BB^T \overline{v}_i \\ &\quad = \sum_{i=1}^{n} \sum_{j,k=0}^{t-1} w_{i,j} R_{j+1} R_{k+1}^T v_{i,k} = c \sum_{i=1}^{n} \sum_{j+k<t} w_{i,j} v_{i,k} + 0 \sum_{i=1}^{n} \sum_{j+k\geq t}^{2t-2} w_{i,j} v_{i,k}, \end{aligned}$$

but since C is self-orthogonal, the sum in the first term is 0. Therefore,

$$\phi_B(w)\phi_B(v) = 0,$$

and thus $\phi_B(C)$ is self-orthogonal. $\square$

Corollary 5. *If C is self-dual, $BB^T = cE$, and*

$$\sum_{i=2}^{t} k_i(t-2i+2) = 0,$$

then $\phi_B(C)$ is self-dual.

Proof. Splitting the equation from the hypothesis we have

$$\sum_{i=2}^{t} k_i(t-i+1) = \sum_{i=2}^{t} k_i(i-1),$$

$$2\sum_{i=2}^{t} k_i(t-i+1) = \sum_{i=2}^{t} k_i(i-1) + \sum_{i=2}^{t} k_i(t-i+1) = \sum_{i=2}^{t} tk_i,$$

$$2\sum_{i=1}^{t} k_i(t-i+1) = 2k_1t + \sum_{i=2}^{t} tk_i.$$

Since C is self-dual, we know

$$C_1^{\perp} = C_t \quad \text{and} \quad \dim(C_t) = \mathsf{rk}(C).$$

Thus,

$$\dim(C_1^{\perp}) = \mathsf{rk}(C) \quad \text{and} \quad n - k_1 = \sum_{i=1}^{t} k_i.$$

Therefore,

$$2\sum_{i=1}^{t} k_i(t-i+1) = nt,$$

making the length of $\phi_B(C)$ twice its dimension. By Theorem 4, $\phi_B(C)$ is self-orthogonal and hence $\phi_B(C)$ is self-dual. □

Let M, N be two matrices over $\mathbb{F}_q$. We say they are *root-equivalent* ($M \sim N$) if M can be obtained from N by a column permutation, or a column multiplication by an element $\alpha \in \mathbb{F}_q$ such that $\alpha^2 = 1$. This implies $MM^T = NN^T$, and by the definition of ϕ_B, we obtain the following

Corollary 6. *If $B \sim D$ in the hypothesis of Corollary 5 then $\phi_B(C)$ and $\phi_D(C)$ are equivalent self-dual codes.*

Example 15. For R(3,3), all matrices B that satisfy $BB^t = cE$ are root-equivalent, and therefore produce equivalent codes. Hence we can restrict ourselves to just one such matrix, for example,

$$B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 2 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

The cases of $R(2,2)$ and $R(3,3)$ are singular. For $R(3,4)$ we have 6 different classes of root-equivalent matrices.

In general, note that there exist self-dual codes A and matrices B with $BB^T \neq cE$ whose image $\phi_B(A)$ is self-dual. For example, consider the self-dual code A over $R(3,4)$ with a generator matrix

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1{+}2u{+}u^2 & 1{+}2u & 1{+}2u{+}u^2 & 1{+}2u & 1{+}2u{+}u^2 & 1{+}2u \\ 1{+}u^2 & 1{+}u^2 & 1{+}u^2 & 1 & 1 & 1 \\ u{+}u^2 & u & u & u{+}u^2 & u{+}u^2 & u \\ 0 & 0 & 0 & 0 & u^2 & 2u^2 \end{pmatrix}.$$

Passing to standard form,

$$G_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & u^2 & 0 & 0 & 0 & 2u^2 \\ 0 & 0 & u^2 & 0 & 0 & 2u^2 \\ 0 & 0 & 0 & u^2 & 0 & 2u^2 \\ 0 & 0 & 0 & 0 & u^2 & 2u^2 \end{pmatrix}.$$

Consider the matrix

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 2 & 1 & 1 \\ 0 & 1 & 2 & 1 \\ 2 & 1 & 1 & 0 \end{pmatrix},$$

for which $BB^T \neq cE$ for any c. The image code $\phi_B(A)$ is a self-dual code:

$$\phi_B(A) = \begin{pmatrix}
1&0&0&0&0&0&2&2&0&0&2&2&0&0&2&2&0&0&2&2&2&0&1&1 \\
0&1&0&0&0&0&1&2&0&0&1&2&0&0&1&2&0&0&1&2&0&2&2&1 \\
0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0 \\
0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1 \\
0&0&0&0&1&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&2&0&2&2 \\
0&0&0&0&0&1&2&1&0&0&0&0&0&0&0&0&0&0&0&0&0&2&1&2 \\
0&0&0&0&0&0&0&0&1&0&1&1&0&0&0&0&0&0&0&0&2&0&2&2 \\
0&0&0&0&0&0&0&0&0&1&2&1&0&0&0&0&0&0&0&0&0&2&1&2 \\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&1&0&0&0&0&2&0&2&2 \\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&2&1&0&0&0&0&0&2&1&2 \\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&1&2&0&2&2 \\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&2&1&0&2&1&2
\end{pmatrix}.$$

References

[Bachoc 1997] C. Bachoc, "Applications of coding theory to the construction of modular lattices", *J. Combin. Theory Ser. A* **(78)** (1997), pp. 92–119.

[Bonnecaze and Udaya 1999] A. Bonnecaze and P. Udaya, "Cyclic codes and self-dual codes over $F_2 + uF_2$", *IEEE Trans. Inform. Theory* **(45)** (1999), pp. 1250–1255.

[Dougherty et al. 2007] S. Dougherty, A. Gulliver, Y. Park, and J. Wong, "Optimal linear codes over $\mathbb{Z}_m$", *J. Korean Math. Soc.* **(44)** (2007), pp. 1139–1162.

[Gulliver and Harada 2001] T. A. Gulliver and M. Harada, "Codes over $F_3 + uF_3$ and improvements to the bounds on ternary linear codes", *Design, Codes and Cryptography* **(22)** (2001), pp. 89–96.

[Ling and Sole 2001] S. Ling and P. Sole, "Duadic codes over $F_2 + uF_2$", *AAECC* **(12)** (2001), pp. 365–379.

[Norton and Salagean 2000a] G. Norton and A. Salagean, "On the Hamming distance of linear codes over a finite chain ring", *IEEE Transactions on Information Theory* **(46)** (2000), pp. 1060–1067.

[Norton and Salagean 2000b] G. Norton and A. Salagean, "On the structure of linear and cyclic codes over a finite chain ring", *AAECC* **(10)** (2000), pp. 489–506.

[Ozbudak and Sole 2007] F. Ozbudak and P. Sole, "Gilbert-Varshamov type bounds for linear codes over finite chain rings", *Advances in Mathematics of Communications* **(1)** (2007), pp. 99–109.

[Siap and Ray-Chaudhuri 2000] I. Siap and D. Ray-Chaudhuri, "New linear codes over F_3 and F_5 and improvements on bounds.", *Design, Codes and Cryptography.* **(21)** (2000), pp. 223–233.

Received: 2008-08-21 Revised: 2008-12-10 Accepted: 2009-01-13

ralfaro@umflint.edu *Mathematics Department, University of Michigan–Flint, Flint, MI 48502, United States*

stbennet@umflint.edu *Mathematics Department, University of Michigan–Flint, Flint, MI 48502, United States*

joshuaha@umflint.edu *Mathematics Department, University of Michigan–Flint, Flint, MI 48502, United States*

cthornbu@umflint.edu *Mathematics Department, University of Michigan–Flint, Flint, MI 48502, United States*