DRDO–IISc Programme on
Advanced Research in Mathematical
Engineering

On the Rank Distance of Cyclic Codes

(TR-PME-2003-04)

by

B. Sundar Rajan and U. Sripati

ECE, IISc., Bangalore

E-mail: bsrajan@ece..iisc.ernet.in, sripati@protocol.ece.iisc.ernet.in

May 12, 2003

Indian Institute of Science
Bangalore 560 012

On the Rank Distance of Cyclic Codes

B. Sundar Rajan and U. Sripati
Department of Electrical Communication Engineering,
Indian Institute of Science,
Bangalore, India 560 012,
email:bsrajan@ece.iisc.ernet.in, sripati@protocol.ece.iisc.ernet.in

June 7, 2003

ABSTRACT

Viewing an n-length vector over the finite field with q^m elements F_{q^m} as an $m \times n$ matrix over F_q by expanding each entry of the vector with respect to a basis of F_{q^m} over F_q, the rank weight of the n- length vector over F_q is the rank of the corresponding matrix over F_q. For an $[n, k]$ linear code over F_{q^m} the rank (rank-distance) of the code is the minimum rank weight among all the codewords. In this report, we study the rank-distance of linear cyclic codes over F_{q^m} using the Discrete Fourier Transform (DFT) description of these codes. We obtain exact expressions for the rank of the primitive length cyclic codes taking non-zero values in the transform domain components of one cyclotomic coset and upper bounds on the rank of the code taking non-zero values in several cyclotomic cosets.

Index terms: Rank-distance, Space-Time codes, Cyclic codes, Discrete Fourier Transform

1 Preliminaries and Motivation

Let $\mathcal{C}$ be an $[n, k]$ linear code over F_{q^m}. For any pair of codewords $\mathbf{c}, \mathbf{c}' \in \mathcal{C}$, the rank distance between them is defined to be the rank over F_q of the $m \times n$ matrix corresponding to $\mathbf{c} - \mathbf{c}'$ obtained by expanding each entry of $\mathbf{c} - \mathbf{c}'$ as an m-tuple along a basis of F_{q^m} over F_q and is denoted by $Rank_q(\mathbf{c} - \mathbf{c}')$ [2]. It is easily verified that this rank distance satisfies the following requirements of a metric: For all $\mathbf{c}, \mathbf{c}', \mathbf{c}'' \in F_{q^m}^n$,

[0]A part of the content of this report has been accepted for presentation in IEEE International Symposium on Information Theory, Yokohama, Japan to be held during June 29-July 4, 2003.

This work was partly supported by DRDO-IISc Program on Mathematical Engineering through a research grant to B.S.Rajan

1. $Rank_q(\mathbf{c}, \mathbf{c}) = 0$.

2. $Rank_q(\mathbf{c}, \mathbf{c}') = Rank_q(\mathbf{c} - \mathbf{c}') = Rank_q(\mathbf{c}' - \mathbf{c}) = Rank_q(\mathbf{c}', \mathbf{c})$.

3. $Rank_q(\mathbf{c}, \mathbf{c}') \leq Rank_q(\mathbf{c}, \mathbf{c}'') + Rank_q(\mathbf{c}'', \mathbf{c}')$.

The rank of $\mathcal{C}$, denoted by $Rank_q(\mathcal{C})$ is defined as the minimum of $Rank_q(\mathbf{c} - \mathbf{c}')$ over all possible pairs of distinct codewords. Clearly, the rank distance between two codewords $\mathbf{c} \neq \mathbf{c}' \in \mathcal{C}$ is at most the Hamming distance between them. Combining this with the Singleton bound one gets, $Rank_q(\mathcal{C}) \leq \min\{m, n - k + 1\}$. The case where $Rank_q(\mathcal{C}) = n - k + 1$ has been studied in [2, 3, 6] and are called MRD (Maximum Rank Distance) codes. In [10, 11] codes with $Rank_q(\mathcal{C}) = m$ calling them "Full Rank Distance (FRD) Codes" have been studied. Notice that the cases $Rank_q(\mathcal{C}) = n - k + 1$ corresponds to considering only those cases where $m \geq n - k + 1$ and the cases $Rank_q(\mathcal{C}) = m$ corresponds to studying those where $m \leq n - k + 1$. These studies have so far been for the general class of linear codes and hence specific results like expressions or tight bounds for the rank of the code given by the description of the code are not known. In this report, we consider the class of cyclic codes over F_{q^m} and obtain such specific results using the Discrete Fourier Transform (DFT) description of these codes. Note that the well known Reed-Solomon codes are included as special cases in our study.

Rank distance codes over finite fields have applications in coding for storage devices (See [3],[12]-[24]) and coding for multiple antenna transmission [4]. Codes over finite fields with the rank as the metric under consideration, instead of the usual Hamming metric, was first studied by Gabidulin [2]. The same was studied by Roth [3] in the context of coding for storage devices. Using MRD codes for storage applications has been discussed in [3]. FRD codes too can be used in storage devices. Consider a binary $m \times n$ storage array. Roth in [3] proves that the minimum of ranks of pairwise differences of matrices that can be stored (called *codeword matrices*) should be maximized. Since $m \leq n$, $d_{R,min}$ of the code can at most be m and FRD codes satisfy $d_{R,min} = m$. We can take any n-length FRD code over F_{2^m} and use the matrices in it in the storage device. We get at most 2^n for storage. It may be noted that by sacrificing on the minimum rank distance, *i.e.*, by choosing another code of smaller minimum rank distance, we can get more matrices.

It is well known that multiple-antenna wireless communication promises very high data rates, especially when the channel is known at the receiver [8, 9]. A constructive approach to design codes suitable for such systems, called Space-Time codes was proposed and design criterion were developed in [4]. An $n \times l$ ($l \geq n$) space time block code (STBC) $\mathcal{C}$ over a complex signal set S is a finite number of $n \times l$ matrices with entries from S. For quasi-static, flat fading channels a primary performance index of $\mathcal{C}$ is the minimum of the rank of the difference of any two codeword matrices, called the rank of the code. $\mathcal{C}$ is of full-rank if its rank is n and is of minimal-delay if $l = n$. For BPSK transmission, we need to construct a set of matrices with entries from $\{-1, +1\}$ satisfying the condition that any pair of matrices in the set has difference of full-rank over the complex field. Hammons and El Gamal [5] propose the following construction of such matrices: Take an F_2-subspace C of $\mathbf{M}^{(2)}_{n\times l}$, the set of $n \times l$ matrices over F_2. Map the matrices in C to matrices over $\{-1, +1\}$ using the following rule: $0 \mapsto +1, 1 \mapsto -1$. Denoting this set of matrices by $\mathcal{C}$, it is proved in [5, Theorem 12] that all pairwise differences of matrices in $\mathcal{C}$ have rank n if and only if all non-zero matrices in C have rank n. Similar correspondence for QPSK modulation is given in [5] and for a variety of complex signal sets obtained from Gaussian number fields in [7].

The remaining content of this report is organized as follows: In Section 2 we give a brief explanation of the well known DFT (Discrete Fourier Transform) domain characterization of cyclic codes over finite fields. Rank-distance properties of one- and two generated (i.e.,(n, k) codes with $k = 1, 2$) cyclic codes are given in Section 3 and illustrated with several examples. Section 4 describes some bounds for codes not necessarily one- or two generated. Section 5 concludes the report with a brief summary and several directions for further research.

2 DFT Description of cyclic codes

A detailed treatment of DFT description of cyclic codes over finite fields can be found in [1]- in this section we briefly describe it mainly for the purpose of establishing the notation and terminology in this report which is at variance from that used in [1].

Let $\mathbf{a} = (a_0, a_1, \cdots, a_{n-1}) \in F^n_{q^m}$ where q is power of a prime and $(n, q) = 1$ (i.e., n and q are relatively prime-which is assumed to hold throughout the report). Also let r be the smallest positive integer such that $n|q^{mr} - 1$ and let $\alpha \in F_{q^{mr}}$ an element of order n. The DFT of $\mathbf{a}$ is defined to be the vector $\mathbf{A} = (A_0, A_1, \cdots, A_{n-1}) \in F^n_{q^{mr}}$ given by

$$A_j = \sum_{i=0}^{n-1} \alpha^{ij} a_i, \qquad j = 0, 1, \cdots, n-1 \tag{1}$$

and the inverse DFT (IDFT) is given by

$$a_i = \frac{1}{(n modulo p)} \sum_{j=0}^{n-1} \alpha^{-ij} A_j \text{ for } 0 \leq i \leq n-1. \tag{2}$$

The vectors **a** and **A** will be referred as the time-domain vector and the corresponding transform domain vector respectively. Denoting the set $\{0, 1, \cdots, n-1\}$ by I_n, for any $j \in I_n$, for any divisor d of m the q^d**-cyclotomic coset of** j **modulo** n is defined to be the set

$$[j]^d = \{i \in I_n | j = iq^{dt} \pmod{n} \text{ for some } t \geq 0\} \tag{3}$$

and we will denote the cardinality of this set by $e_j^{(d)}$. When $d = 1$ we denote the q-cyclotomic coset of j modulo n by $[j]$ and its cardinality by e_j. Simply by "cyclotomic coset", we mean a "q-cyclotomic coset". If $J \subseteq [0, n-1]$, we write $[J]^d = \cup_{j \in J} [j]^d$.

For a code $\mathcal{C}$ we say A_j takes values from $\{\sum_{i=0}^{n-1} \alpha^{ij} a_i | \vec{a} \in \mathcal{C}\} \subset F_{q^{mr}}$. Now, cyclic codes can be characterized in the transform domain as follow:

- The set of j-th transform components of all the codewords of a linear cyclic code is either $F_{q^{me_j^{(m)}}}$ or $\{0\}$, and conversely the set of inverse DFT vectors of all the vectors of a subspace of $DFT(F_{q^m}^n) \subset F_{q^{mr}}^n$, in which transform components in $[j]^m$, $j = 0, 1, ..., n-1$, of every vector take either only the zero value or all the values of $F_{q^{me_j^{(m)}}}$, and transform components in disjoint $[j_1]^m$ and $[j_2]^m$ take values independently, constitute a cyclic code.

From the above characterization, it is clear that to specify a cyclic code, it is sufficient to specify the set $[J]^m$ in which the transform components of all the codewords are zero. For linear cyclic codes A_j takes values from $\{0\}$ or $F_{q^{me_j^{(m)}}}$ and transform components in different q^m-cyclotomic cosets are unrelated and within a q^m-cyclotomic coset are related by $A_{jq^m} = A_j^{q^m}$ (called **conjugacy constraints**). The transform components taking values from $F_{q^{me_j^{(m)}}}$ are called free spectral components. Note that for length $n = q^m - 1$ codes over F_{q^m} each cyclotomic coset is a singleton set and there is no conjugacy constraint. Also we will be using the following sets frequently throughout that are closely related to the cyclotomic cosets:

$$\alpha_{[j]^d} = \{\alpha^i | i \in [j]^d\} \tag{4}$$

and

$$A_{[j]^d} = \{A_i | i \in [j]^d\}. \tag{5}$$

Throughout the report, we consider (n, k) cyclic codes over finite fields over F_{q^m} where when $k = 1$ or $k = 2$ and $n | q^m - 1$. The condition n divides $q^m - 1$ guarantees a DFT characterization of the cyclic codes under consideration as well as makes each q^m--cyclotomic coset modulo n a singleton set. Notice that the case $n = q^m - 1$ is a special case and corresponds to all primitive length cyclic codes.

A_1	A_2	A_4	a_0	a_1	a_2	a_3	a_4	a_5	a_6	F_2-Rank
100	100	100	100	100	100	000	100	000	000	1
010	001	011	000	100	100	100	000	100	000	1
001	011	010	000	000	100	100	100	000	100	1
110	101	111	100	000	000	100	100	100	000	1
011	010	001	000	100	000	000	100	100	100	1
111	110	101	100	000	100	000	000	100	100	1
101	111	110	100	100	000	100	000	000	100	1

Table 1: Codewords corresponding to Example 1

3 Rank-distance of (n, k) cyclic codes

In this section we present several rank-distance properties of (n, k) cyclic codes over finite fields over F_{q^m} where when $k = 1$ or $k = 2$.

The following proposition follows from the fact that a codeword with only the 0-th transform component A_0 nonzero is a constant codeword of the form $(x, x, \cdots, x)$.

Theorem 1 *Let $\mathcal{C}$ be a cyclic code of length n over F_{q^m} with A_0 being one of the free transform domain components. Then $Rank_q(\mathcal{C}) = 1$.*

Identifying codewords with all the components from a proper subfield of F_{q^m} leads to

Theorem 2 *Let a cyclic code $\mathcal{C}$ over F_{q^m} of length $n|q^m - 1$ be characterized by all the free transform domain components in the union of sets of the form $A_{[j]^d}$ for some values of j and all other transform domain components 0. Then $Rank_q(\mathcal{C}) \leq d$.*
In particular, if the free components constitute a single q-cyclotomic coset modulo n (i.e., $d = 1$) then the rank of the code is 1.

Proof: Any codeword of the code satisfying the conditions of the theorem is vector over the subfield F_{q^d} of F_{q^m}. This codeword has rank at most d. Since all the codewords are of this form the rank of the code is $\leq d$.

Example 1 *Consider $\mathcal{C}_1$, the $(7, 3)$ code over F_{2^3} characterized by free transform domain components A_1, A_2, A_4, i.e., $([1] = \{1, 2, 4\})$. All other transform domain components are constrained to 0. We list in Table 1 7 codewords that have F_2-Rank=1.*

Theorem 3 *Let $\mathcal{C}$ be a cyclic code of length $n|q^m - 1$ over F_{q^m} such that the transform domain component $A_{jq^s} \in A_{[j]}, (0 \leq s \leq e_j - 1)$ is free and all other transform domain components are constrained to zero. Then $Rank_q(\mathcal{C}) = e_j$. In other words, for a length $n|q^m - 1$ cyclic code over F_{q^m} with non-zero transform components in only one q^m-cyclotomic coset (and hence only one transform component), the rank of the code is equal to the size of the q-cyclotomic coset to which the free transform component belongs.*

Proof: From the IDFT we have

$$a_i = \sum_{j=0}^{n-1} \alpha^{-ij} A_j = \alpha^{-ijq^s} A_{jq^s} \text{ for } 0 \leq i \leq n-1. \tag{6}$$

That is,

$$\vec{a} = \left(A_{jq^s}, \alpha^{-jq^s} A_{jq^s}, \alpha^{-2jq^s} A_{jq^s} \cdots, \alpha^{-(e_j-1)jq^s} A_j q^s, \alpha^{-e_j jq^s} A_{jq^s}, \cdots, \alpha^{-(n-1)jq^s} A_{jq^s} \right) \tag{7}$$

which for simplicity we write as $\vec{a} = A_{jq^s} \left(1, \alpha^{-jq^s}, \alpha^{-2jq^s}, \cdots, \alpha^{-(e_j-1)jq^s}, \alpha^{-e_j jq^s}, \cdots, \alpha^{-(n-1)jq^s}\right)$. Let

$$\vec{S} = (1, \alpha^{-jq^s}, \alpha^{-2jq^s}, \cdots, \alpha^{-(e_j-1)jq^s}, \alpha^{-e_j jq^s}, \alpha^{-(e_j+1)jq^s}, \cdots, \alpha^{-(n-1)jq^s}) \tag{8}$$

Since, A_{jq^s} is non-zero, the $Rank_q(\vec{a})$ is same as $Rank_q(\vec{S})$. We will show that the elements of

$$S' = \left\{1, \alpha^{-jq^s}, \alpha^{-2jq^s}, \cdots, \alpha^{(e_j-1)jq^s}\right\}$$

are linearly independent and that $\left\{\alpha^{-e_j jq^s}, \alpha^{-(e_j+1)jq^s} \cdots, \alpha^{-(n-1)jq^s}\right\}$ can be expressed as a linear combination of the elements of S': Let us assume on the contrary that the elements of S' are linearly dependent. Then, $\exists$ coefficients $c_0, c_1, \cdots, c_{e_j-1} \in F_q$ not all $c_i = 0$ such that $\sum_{i=0}^{e_j-1} c_i \alpha^{-ijq^s} = 0$ which implies that $\alpha^{-jq^s}$is a root of a polynomial of degree $(e_j - 1)$ over F_q.

But, $\alpha_{[-j]} = \left\{\alpha^{-j}, \alpha^{-jq^s}, \cdots, \alpha^{-(e_j-1)jq^s}\right\}$ corresponds to the q-cyclotomic coset $[-j]$ also of size e_j. Hence the minimal polynomial of $\alpha^{-jq^s}$is of degree e_j. This contradicts our assumption that the elements of S' are linearly dependent. Using the fact that the minimal polynomial of α^{-jq^s} is of degree e_j, it is straight forward to show that other elements of S can be written as linear combinations of elements of S'. Hence, $Rank_q(\mathcal{C}) = e_j$.

In the following theorem we show that for a n-length, $(n|q^m - 1)$, cyclic code over F_{q^m} if all the nonzero transform components belong to only one q-cyclotomic coset of j modulo n, then for every codeword its first e_j components completely determine the rank of that codeword.

Theorem 4 *Let $\mathcal{C}$ be a cyclic code of length $n|q^m-1$ over F_{q^m} with free transform components $A_{jq^{s_1}}$, $A_{jq^{s_2}}$, $A_{jq^{s_3}} \cdots A_{jq^{s_k}}$ and all other transform domain components constrained to 0. For any non-zero codeword $\vec{a}=(a_0,a_1,\cdots,a_{e_j-1},a_{e_j},\cdots,a_{n-1}] \in \mathcal{C}$ the entries of $(a_{e_j},a_{e_j+1},\cdots,a_{n-1})$ can be expressed as linear combination of those of $(a_0,a_1,\cdots,a_{e_j-1})$. In other words, $Rank_q(\vec{a})$=number of linearly independent components in $\left\{a_0,a_1,\cdots,a_{e_j-1}\right\}$.*

Proof: As $A_{jq^{s_1}}, A_{jq^{s_2}}, \cdots A_{jq^{s_k}}$ are the only free transform domain components and all other transform domain components are constrained to 0, we obtain directly from the Inverse DFT,

$$a_i = \alpha^{-ijq^{s_1}} A_{jq^{s_1}} + \alpha^{-ijq^{s_2}} A_{jq^{s_2}} + \cdots + \alpha^{-ijq^{s_k}} A_{jq^{s_k}}. \tag{9}$$

In particular,

$$a_{e_j} = \alpha^{-e_jjq^{s_1}} A_{jq^{s_1}} + \alpha^{-e_jjq^{s_2}} A_{jq^{s_2}} + \cdots + \alpha^{-e_jjq^{s_k}} A_{jq^{s_k}}. \tag{10}$$

Let the minimum polynomial of $\alpha^{-jq^{s_i}}$ for $0 \leq s_i \leq e_j-1$, be

$$E_j(x) = x^{e_j} + c_{e_j-1}x^{e_j-1} + \cdots + c_1x + c_0 \tag{11}$$

where $c_i \in F_q$ for all $0 \leq i \leq e_j-1$ and not all $c_i = 0$. Since

$$\alpha_{[-j]} = \left\{\alpha^{-j}, \alpha^{-jq}, \cdots \alpha^{-jq^{s_1}}, \cdots \alpha^{-jq^{s_2}}, \cdots \alpha^{-jq^{s_k}}, \cdots, \alpha^{-jq^{e_j-1}}\right\}$$

we have,

$$E_j(\alpha^{-jq^{s_1}}) = E_j(\alpha^{-jq^{s_2}}) = \cdots E_j(\alpha^{-jq^{s_k}}) = 0$$

which gives the following set of equations:

$$\alpha^{-e_jjq^{s_1}} = -\sum_{i=0}^{e_j-1} c_i\alpha^{-ijq^{s_1}} \tag{12}$$

$$\alpha^{-e_jjq^{s_2}} = -\sum_{i=0}^{e_j-1} c_i\alpha^{-ijq^{s_2}} \tag{13}$$

$$\vdots \tag{14}$$

$$\alpha^{-e_jjq^{s_k}} = -\sum_{i=0}^{e_j-1} c_i\alpha^{-ijq^{s_k}} \tag{15}$$

$$\tag{16}$$

Using these equations in (10),

$$\begin{aligned} a_{e_j} &= \left(-\sum_{i=0}^{e_j-1} c_i\alpha^{-ijq^{s_1}}\right) A_{jq^{s_1}} + \left(-\sum_{i=0}^{e_j-1} c_i\alpha^{-ijq^{s_2}}\right) A_{jq^{s_2}} + \cdots + \left(-\sum_{i=0}^{e_j-1} c_i\alpha^{-ijq^{s_2}}\right) A_{jq^{s_k}} \quad (17) \\ &= -\sum_{i=0}^{e_j-1} c_i \left\{\alpha^{-ijq^{s_1}} A_{jq^{s_1}} + \alpha^{-ijq^{s_2}} A_{jq^{s_2}} + \alpha^{-ijq^{s_k}} A_{jq^{s_k}}\right\}. \end{aligned}$$

Let $-c_i = c'_i$ for $i = 0, 1, 2, \cdots n-1$, and using (9) in (17) we get

$$a_{e_j} = \sum_{i=0}^{e_j-1} c'_i \left\{ \alpha^{-ijq^{s_1}} A_{jq^{s_1}} + \alpha^{-ijq^{s_2}} A_{jq^{s_2}} + \alpha^{-ijq^{s_k}} A_{jq^{s_k}} \right\} = \sum_{i=0}^{e_j-1} c'_i a_i. \quad (18)$$

Now, we have $a_{e_j+r} = \alpha^{-(e_j+r)jq^{s_1}} A_{jq^{s_1}} + \alpha^{-(e_j+r)jq^{s_2}} A_{jq^{s_2}} + \cdots + \alpha^{-(e_j+r)jq^{s_k}} A_{jq^{s_k}}$ for every $r = 1, 2, \cdots, n-1-e_j$. Consider the term, $\alpha^{-(e_j+r)j} = \alpha^{-rj}\alpha^{-e_j j} = \alpha^{-rj} \sum_{i=0}^{e_j-1} c'_i \alpha^{-ij}$. This implies

$$\alpha^{-(e_j+r)jq^{s_\lambda}} = \alpha^{-rjq^{s_\lambda}} \sum_{i=0}^{e_j-1} c'_i \alpha^{-ijq^{s_\lambda}}; \quad \lambda = 1, 2, \cdots, k$$

which in turn gives

$$a_{e_j+r} = \sum_{i=0}^{e_j-1} c'_i a_{i+r}$$

where a_{i+r} is obtainable from (9).Summarizing, we have shown that a_{e_j+r} for every $r = 0, 1, ..., n-1-e_j$ can be expressed as F_q-linear combinations of the previous e_j entries.

Therefore, $Rank_q(\mathcal{C})$ = number of linear independent elements in the set $\{a_0, a_1, \cdots a_{e_j-1}\}$.

We illustrate both Theorem 3 and Theorem 4 in the following four examples.

Example 2 *Let $\mathcal{C}$ be the primitive length cyclic code over F_{2^4} whose only free transform domain component is A_7. (All other transform domain components $A_i = 0, i = 0, 1, 2, \cdots 6, 8, \cdots 14$ are zero.) Table 3 shows all the codewords and their ranks along with the only nonzero transform component. From the table we see that the time-domain components (a_0, a_1, a_2, a_3) are linearly independent and the components a_4 to a_{14} can be expressed as a linear combination of these four components in accordance with Theorem 4. As $[7]_{15} = \{7, 14, 13, 11\}$ is a 2-cyclotomic coset of size 4, $Rank_2(\mathcal{C}) = 4$. in accordance with Theorem 3. The elements of F_{16} have been shown in "polynomial form",i.e $b_0 + b_1x + b_2x^2 + b_3x^3$, where $b_i \in \{0, 1\}$ with only the listing of the coefficients in juxtaposition $b_0b_1b_2b_3$.*

Example 3 *Let $\mathcal{C}$ be the $(15, 1)$ cyclic code over F_{2^4} defined by the free transform domain component A_5. All other transform components are constrained to 0. Since $[5]_{15} = \{5, 10\}, e_5 = 2$. All the codewords have been displayed in Table 3 along with their rank. Observe that a_0, a_1 are linearly independent and $a_2 - a_{13}$ can be expressed as linear combination of a_0, a_1 in accordance with Theorem 4. and every non-zero codeword has F_2-Rank=2 in accordance with Theorem 3.*

A_7	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	Rank
0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0
1000	1000	1010	0100	0101	0010	1110	0001	0111	1100	1111	0110	1011	0011	1001	1101	4
0100	0100	0101	0010	1110	0001	0111	1100	1111	0110	1011	0011	1001	1101	1000	1010	4
0010	0010	1110	0001	0111	1100	1111	0110	1011	0011	1001	1101	1000	1010	0100	0101	4
0001	0001	0111	1100	1111	0110	1011	0011	1001	1101	1000	1010	0100	0101	0010	1110	4
1100	1100	1111	0110	1011	0011	1001	1101	1000	1010	0100	0101	0010	1110	0001	0111	4
0110	0110	1011	0011	1001	1101	1000	1010	0100	0101	0010	1110	0001	0111	1100	1111	4
0011	0011	1001	1101	1000	1010	0100	0101	0010	1110	0001	0111	1100	1111	0110	1011	4
1101	1101	1000	1010	0100	0101	0010	1110	0001	0111	1100	1111	0110	1011	0011	1001	4
1010	1010	0100	0101	0010	1110	0001	0111	1100	1111	0110	1011	0011	1001	1101	1000	4
0101	0101	0010	1110	0001	0111	1100	1111	0110	1011	0011	1001	1101	1000	1010	0100	4
1110	1110	0001	0111	1100	1111	0110	1011	0011	1001	1101	1000	1010	0100	0101	0010	4
0111	0111	1100	1111	0110	1011	0011	1001	1101	1000	1010	0100	0101	0010	1110	0001	4
1111	1111	0110	1011	0011	1001	1101	1000	1010	0100	0101	0010	1110	0001	0111	1100	4
1011	1011	0011	1001	1101	1000	1010	0100	0101	0010	1110	0001	0111	1100	1111	0110	4
1001	1001	1101	1000	1010	0100	0101	0010	1110	0001	0111	1100	1111	0110	1011	0011	4

Table 2: Codewords corresponding to Example 2

A_5	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	Rank
0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0
1000	1000	1110	0110	1000	1110	0110	1000	1110	0110	1000	1110	0110	1000	1110	0110	2
0100	0100	0111	0011	0100	0111	0011	0100	0111	0011	0100	0111	0011	0100	0111	0011	2
0010	0010	1111	1101	0010	1111	1101	0010	1111	1101	0010	1111	1101	0010	1111	1101	2
0001	0001	1011	1010	0001	1011	1010	0001	1011	1010	0001	1011	1010	0001	1011	1010	2
1100	1100	1001	0101	1100	1001	0101	1100	1001	0101	1100	1001	0101	1100	1001	0101	2
0110	0110	1000	1110	0110	1000	1110	0110	1000	1110	0110	1000	1110	0110	1000	1110	2
0011	0011	0100	0111	0011	0100	0111	0011	0100	0111	0011	0100	0111	0011	0100	0111	2
1101	1101	0010	1111	1101	0010	1111	1101	0010	1111	1101	0010	1111	1101	0010	1111	2
1010	1010	0001	1011	1010	0001	1011	1010	0001	1011	1010	0001	1011	1010	0001	1011	2
0101	0101	1100	1001	0101	1100	1001	0101	1100	1001	0101	1100	1001	0101	1100	1001	2
1110	1110	0110	1000	1110	0110	1000	1110	0110	1000	1110	0110	1000	1110	0110	1000	2
0111	0111	0011	0100	0111	0011	0100	0111	0011	0100	0111	0011	0100	0111	0011	0100	2
1111	1111	1101	0010	1111	1101	0010	1111	1101	0010	1111	1101	0010	1111	1101	0010	2
1011	1011	1010	0001	1011	1010	0001	1011	1010	0001	1011	1010	0001	1011	1010	0001	2
1001	1001	0101	1100	1001	0101	1100	1001	0101	1100	1001	0101	1100	1001	0101	1100	2

Table 3: Codewords corresponding to Example 3

A_3	a_0	a_1	a_2	a_3	a_4	Rank	A_3	a_0	a_1	a_2	a_3	a_4	Rank
0000	0000	0000	0000	0000	0000	0	1000	1000	0011	1111	0001	0101	4
0100	0100	1101	1011	1100	1110	4	0010	0010	1010	1001	0110	0111	4
0001	0001	0101	1000	0011	1111	4	1100	1100	1110	0100	1101	1011	4
0110	0110	0111	0010	1010	1001	4	0011	0011	1111	0001	0101	1000	4
1101	1101	1011	1100	1110	0100	4	1010	1010	1001	0110	0111	0010	4
0101	0101	1000	0011	1111	0001	4	1110	1110	0100	1101	1011	1100	4
0111	0111	0010	1010	1001	0110	4	1111	1111	0001	0101	1000	0011	4
1011	1011	1100	1110	0100	1101	4	1001	1001	0110	0111	0010	1010	4

Table 4: Codewords corresponding to Example 4

Example 4 *Consider the non-primitive length cyclic code $\mathcal{C}$ of length $n = 5$ over F_{2^4} which has A_3 to be the only free transform component. The conjugacy classes are $\{0\},\{1,2,4,3\}$. As $[3]_5 = \{3,1,2,4\}, |[3]_5| = 4$, every codeword has Rank=4. Table 4 shows all the codewords and their ranks.*

Example 5 *Let $\mathcal{C}$ be the non-primitive cyclic code of length $n = 7$ over F_{2^6} with the only free transform component to be A_5. The conjugacy classes are $\{0\},\{1,2,4\},\{3,6,5\}$. Since $[5]_7 = \{5,3,6\}, |[5]_7| = 3$, every codeword has Rank=3. All the codewords of $\mathcal{C}$ are listed in Table 11.*

We shall now study the rank weight distribution of cyclic codes characterized by two free transform domain components ($(n,2)$ codes) from the same q-cyclotomic coset.

Theorem 5 *Consider a cyclic code $\mathcal{C}$ of length $n|q^m - 1$ over F_{q^m} whose free transform domain components are A_{jq^r} and $A_{jq^{r+s}}$, (i.e., the indices of the transform components belong to the same q-cyclotomic coset and s indicates the "separation" between the two transform domain components) $(0 \leq r \leq e_j - 2), (1 \leq s \leq e_j - 1)$ and all other transform domain components be constrained to 0. Then,*

$$Rank_q(\mathcal{C}) = (e_j - gcd(s, e_j)).$$

Moreover, the rank weight distribution of $\mathcal{C}$ is given by

$$N_0 = 1; \quad N_{e_j - gcd(s,e_j)} = (q^m - 1)\tau; \quad N_{e_j} = q^{2m} - N_{e_j - gcd(s,e_j)} - 1 = q^{2m} - (q^m - 1)\tau - 1,$$

where

N_i denotes the number of codewords with rank weight i and
$\tau =$ the number of elements of F_{q^m} that have their $(q^s - 1)$-th root in $F_{q^{e_j}}$.

Proof: Without loss of generality, we can assume that the free transform domain components are A_j and A_{jq^s} (i.e., $r = 0$).
For any $\mathbf{a} = (a_0, a_1, \cdots, a_{n-1}) \in \mathcal{C}$, we have,

$$a_i = \sum_{j=0}^{n-1} \alpha^{-ij} A_j = \alpha^{-ij} A_j + \alpha^{-ijq^s} A_{jq^s}. \tag{19}$$

Let $\mathcal{C}' = \{\mathbf{a} \in \mathcal{C} | A_j = 0\}$ and $\mathcal{C}'' = \{\mathbf{a} \in \mathcal{C} | A_{jq^s} = 0\}$. From Theorem 3, we know that $Rank_q(\mathcal{C}') = Rank_q(\mathcal{C}'') = e_j$.

Denoting $-\mu = \frac{A_j}{A_{jq^s}} \in F_{q^m}$, we rewrite (19) as $a_i = A_{jq^s}\left\{-\mu\alpha^{-ij} + \alpha^{-ijq^s}\right\}$. Letting

$$a'_i = -\mu\alpha^{-ij} + \alpha^{-ijq^s} \tag{20}$$

we have $\mathbf{a'} = \left(a'_0, a'_1, \cdots a'_{n-1}\right)$ and $\mathbf{a} = A_{jq^s}\mathbf{a'}$. Moreover,

$$Rank_q(\mathbf{a}) = Rank_q(\mathbf{a'}). \tag{21}$$

Let $g = gcd(s, e_j)$. Then F_{q^s} and $F_{q^{e_j}}$ contain a subfield isomorphic to F_{q^g}. Let $\{x_1, x_2, \cdots x_g\}$ be a basis of the subfield F_{q^g} over F_q. We will show that if μ has a $(q^s-1)^{th}$ root in $F_{q^{e_j}}$ then $Rank_q(\mathcal{C}) = (e_j - g)$ and if not $Rank_q(\mathcal{C}) = e_j$. So, we will be considering the following two cases: **Case 1:** μ has a $(q^s-1)^{th}$ root in $F_{q^{e_j}}$.
Case 2: μ does not have a $(q^s-1)^{th}$ root in $F_{q^{e_j}}$. **Case 1:** Let $\delta \in F_{q^{e_j}}$ such that $\delta^{q^s-1} = \mu$. Since $\{x_1, x_2, \cdots x_g\}$ is a F_q-basis of F_{q^g}, the elements of $\{\delta x_1, \delta x_2, \cdots \delta x_g\}$ are in $F_{q^{e_j}}$ and also F_q linearly independent. Since F_{q^g} is a subfield of $F_{q^{e_j}}$, it is known that the set $\{\delta x_1, \delta x_2, \cdots \delta x_g\}$ can be can be extended to constitute a basis of $F_{q^{e_j}}$ over F_q. Moreover, it can be shown that $\exists I' \subset \{0, 1, 2, \cdots (e_j - 1)\}$ with $|I'| = e_j - g$ such that $\left\{\alpha^{-ij} | i \in I'\right\} \cup \{\delta x_1, \delta x_2, \cdots \delta x_g\}$ is a basis of $F_{q^{e_j}}$ over F_q. We proceed to show that $\{a'_i | i \in I'\}$ are linearly independent. Towards this end, let us assume the contrary, i.e., the elements of $\{a'_i | i \in I'\}$ are linearly dependent. This means $\exists f_i \in F_q$, not all $f_i = 0$ such that $\sum_{i\in I'} f_i a'_i = 0$ which implies $\sum_{i\in I'} f_i\left\{-\mu\alpha^{-ij} + \alpha^{-ijq^s}\right\} = 0$ which in turn means $\Rightarrow \mu = \left(\sum_{i\in I'} f_i\alpha^{-ij}\right)^{q^s-1}$. Since δ is a $(q^s-1)^{th}$ root of μ in $F_{q^{e_j}}$ and the elements of $\{\delta x_1, \delta x_2, \cdots \delta x_g\}$ are in $F_{q^{e_j}}$ and F_q-linearly independent, we have $\delta\sum_{l=1}^{g} b_l x_l = \sum_{i\in I'} f_i\alpha^{-ij}$. Equivalently, $\sum_{i\in I'} f_i\alpha^{-ij} - \delta\sum_{l=1}^{g} b_l x_l = 0$. Now, setting $b'_l = -b_l$, we get $\sum_{i\in I'} f_i\alpha^{-ij} + \sum_{l=1}^{g} b'_l(\delta x_l) = 0$ which contradicts the fact that $\left\{\alpha^{-ij} | i \in I'\right\} \cup \{\delta x_1, \delta x_2, \cdots \delta x_g\}$ is a basis for $F_{q^{e_j}}$.
Therefore, $\{a'_i | i \in I'\}$ are linearly independent and hence,

$$Rank_q(\mathbf{a'}) \geq e_j - g. \tag{22}$$

We proceed to show that in (22) only equality is possible. Let us assume that $Rank_q(\mathbf{a'}) = r > e_j - g$. Using Theorem 4, this $\Rightarrow \exists I'' \subset \{0, 1, 2, \cdots e_j - 1\}$ where $|I''| = r$ such that $\{a'_i | i \in I''\}$ are linearly independent. Now the elements of $\left\{\alpha^{-ij} | i \in I''\right\} \cup \{\delta x_1, \delta x_2 \cdots \delta x_g\}$ are linearly dependent because $r + g \geq e_j$. This $\Rightarrow \exists$ scalars $c_i \in F_q$ not all equal to 0, such that

$$\sum_{i\in I''} c_i\alpha^{-ij} + b_1(\delta x_1) + b_2(\delta x_2) + \cdots + b_g(\delta x_g) = 0 \sum_{i\in I''} c_i\alpha^{-ij} = -\sum_{l=1}^{g} b_l\delta x_l = \delta z where z = -\sum_{l=1}^{g} b_l x_l. \tag{23}$$

Therefore, $\left(\sum_{i\in I''} c_i\alpha^{-ij}\right)^{q^s-1} = (\delta z)^{q^s-1} = \mu$
$\Rightarrow \left(\sum_{i\in I''} c_i\alpha^{-ij}\right)^{q^s} = \mu\sum_{i\in I''} c_i\alpha^{-ij}$

$\Rightarrow \sum_{i\in I''} c_i \left\{-\mu\alpha^{-ij} + \alpha^{-ijq^s}\right\} = 0$
$\Rightarrow \sum_{i\in I''} c_i a'_i = 0$
which contradicts our assumption that $\{a'_i | i \in I''\}$ are linearly independent. Therefore, $Rank_q(\underline{a'}) = e_j - g = Rank_{F_q}(\mathbf{a})$ when μ has a $(q^s-1)^{th}$ root in $F_{q^{e_j}}$.

Case 2: In this case, we shall show that $Rank_{F_q}(\mathbf{a}) = e_j$.
Let us assume on the contrary that, $Rank_q(\mathbf{a}) \le (e_j - 1)$. From Theorem 4 we know that $Rank_q(\mathbf{a})$ is determined by the number of linearly independent elements in $\left\{a_0, a_1, \cdots a_{e_j-1}\right\}$. By our assumption there exist coefficients $h_i \in F_q$, not all equal to 0, such that

$$\begin{aligned} \sum_{i=0}^{e_j-1} h_i a'_i = 0 &\Rightarrow \sum_{i=0}^{e_j-1} h_i \left\{-\mu\alpha^{-ij} + \alpha^{-ijq^s}\right\} = 0 \\ &\Rightarrow \mu \sum_{i=0}^{e_j-1} h_i\alpha^{-ij} = \left(\sum_{i=0}^{e_j-1} h_i\alpha^{-ij}\right)^{q^s} \\ &\Rightarrow \mu = \left(\sum_{i=0}^{e_j-1} h_i\alpha^{-ij}\right)^{q^s-1}. \end{aligned}$$

As μ does not have a $(q^s-1)^{th}$ root in $F_{q^{e_j}}$, μ cannot be expressed as above, since $\left(\sum_{i=0}^{e_j-1} h_i\alpha^{-ij}\right)$ represents an element of $F_{q^{e_j}}$,resulting in a contradiction. Therefore, the elements $\left\{a'_0, a'_1, \cdots a'_{e_j-1}\right\}$ are linearly independent.

Combining both the cases we see that $Rank_q(\mathcal{C}) = e_j - g$.

Rank Weight Distribution of $\mathcal{C}$:
Let us divide the q^{2m} codewords of $\mathcal{C}$ into q^m subsets, each comprising of q^m codewords as shown below where α denotes the primitive element of order $(q^m - 1)$ in F_{q^m}:

Subset 1		Subset 2		.	.	.	Subset q^m	
A_j	A_{jq^s}	A_j	A_{jq^s}				A_j	A_{jq^s}
0	0	1	0	.	.	.	α^{q^m-2}	0
0	1	1	1	.	.	.	δ^{q^m-2}	1
0	α	1	α	.	.	.	α^{q^m-2}	α
$\vdots$	$\vdots$	$\vdots$	$\vdots$	.	.	.	$\vdots$	$\vdots$
0	α^{q^m-2}	1	α^{q^m-2}	.	.	.	α^{q^m-2}	α^{q^m-2}

From Theorem 3, all the non zero codewords of Subset 1 have $Rank = e_j$. In all the other Subsets (Subset 2 to Subset q^m) the value of A_j is kept fixed while the value of A_{jq^s} is varied over all the values of F_{q^m}. Since, $\mu \triangleq \frac{A_j}{A_{jq^s}}$, μ ranges over all the (q^m-1) non zero values of F_{q^m} in every Subset from Subset 2 to Subset q^m. We have proved that the Rank of $\mathcal{C}$ is determined by the value of μ. Hence the Rank weight distribution of $\mathcal{C}$ can be determined by the Rank weight distribution of any Block (Block 2 to Block q^m) in the following manner.

Let τ represent the number of elements in F_{q^m} which have their $(q^s-1)^{th}$ root in $F_{q^{e_j}}$. In every Subset, we have τ codewords having $Rank = e_j - gcd(e_j, s)$. Therefore,

A_1	A_4	a_0	a_1	a_2	a_3	Rank
1000	0000	1000	0111	1101	0001	4
1000	1000=α^0	0000	1110	0110	1110	2
1000	0100=α^1	1100	1111	0100	1010	4
1000	0010=α^2	1010	0011	0101	1000	4
1000	0001=α^3	1001	0101	1001	1001	2
1000	1100=α^4	0100	0110	1111	0101	4
1000	0110=α^5	1110	1011	1100	0011	4
1000	0011=α^6	1011	0001	0001	0000	2
1000	1101=α^7	0101	0100	1011	1101	4
1000	1010=α^8	0010	1010	1110	0111	4
1000	0101=α^9	1101	1101	0000	0010	2
1000	1110=α^{10}	0110	0010	0111	1100	4
1000	0111=α^{11}	1111	1001	1000	1011	4
1000	1111=α^{12}	0111	0000	0011	0100	2
1000	1011=α^{13}	0011	1000	1010	1111	4
1000	1001=α^{14}	0001	1100	0010	0110	4

Table 5: Codewords corresponding to Example 6

$N_0 = 1, N_{e_j - gcd(s,e_j)} = \tau(q^m - 1), N_{e_j} = q^{2m} - N_{e_j - gcd(s,e_j)} - 1 = q^{2m} - \tau(q^m - 1) - 1$, where N_i represents the number of codewords having Rank weight i in $\mathcal{C}$.

We shall illustrate Theorem 5 and the result on the Rank distribution of $(n, 2)$ Cyclic codes by the following several examples:

Example 6 Example 6: *Let $\mathcal{C}$ be the $(15, 2)$ cyclic code over F_{2^4} characterize by two free transform domain components A_1 and A_4. Since $[1] = [4] = \{1, 2, 4, 8\}$ we have $e_1 = 4$. The separation between free transform domain components, s=2 and $g = \gcd(s, m) = \gcd(2, 4) = 2$. From Theorem 5, $Rank_2(\mathcal{C}) = m - g = 2$.*
The elements of F_{16} that have $(2^2-1) = 3$-rd root of it in F_{2^4} are $\{1, \alpha^3, \alpha^6, \alpha^9, \alpha^{12}\}$ (α is a primitive element of F_{16}) which means $\tau = 5$. From Theorem 5, the rank weight distribution of this code is given by $N_0 = 1$; $N_2 = 5 \times 16 = 80$; $N_4 = 256 - 80 - 1 = 175$.

We list in Table 5 16 of the 256 codewords of this code with only the first 4 components for every codeword (since this is sufficient to determine the rank weight of the codeword)

Note that the 16 codewords in Table 5 have been listed for the specific value of $A_1 = 1000$ and for all possible values of A_4. It turns out that the rank weight distribution as appearing above remains the same for all nonzero values of A_1- a fact that is true for any code of Theorem 5 and is the main idea in the proof of Theorem 5.

Similarly, let $\mathcal{C}'$ denote the $(63, 2)$ cyclic code over F_{2^6} defined by free transform domain components A_1 and A_8. Since, $[1] = [8] = \{1, 2, 4, 8, 16, 32\}$ we have $e_1 = 6, s = 3$ and $g = 3$. Therefore $Rank_2(\mathcal{C}) = 6 - 3 = 3$.

Example 7 *Consider the non-primitive $(9, 2)$ cyclic code $\mathcal{C}$ over F_{2^6} defined by the free components A_1 and A_8. The 2-cyclotomic cosets modulo 9 are*

A_7	A_{14}	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	Rank
1000	0000	1000	1010	0100	0101	0010	1110	0001	0111	1100	1111	0110	1011	0011	1001	1101	4
1000	1000	0000	1110	0110	0100	1110	1000	0010	1010	0110	1010	1000	1100	1100	0010	0100	3
1000	0100	1100	1000	0101	1001	0100	1101	1100	1101	1001	0001	0001	0100	1000	0000	0101	3
1000	0010	1010	1011	1000	0011	0001	0011	1011	0010	0010	1000	1001	0000	1010	0001	1001	3
1000	0001	1001	0110	0010	0110	1111	0100	0100	1001	1011	0000	1101	0010	1011	1101	1111	3
1000	1100	0100	1100	0111	1000	1000	1011	1111	0000	0011	0100	1111	0011	0111	1011	1100	3
1000	0110	1110	1001	1001	1111	0111	0000	0110	1000	0111	0110	1110	1111	0001	1000	0001	3
1000	0011	1011	0111	1110	0000	1100	1001	1110	1100	0101	0111	0010	1001	0010	0101	1011	3
1000	1101	0101	0000	0001	1011	0101	0001	1010	1110	0100	1011	0100	1010	1111	1111	1110	3
1000	1010	0010	1111	1010	0010	1101	0101	1000	1111	1000	1101	0111	0111	0101	1010	0000	3
1000	0101	1101	0100	0011	1010	1001	0111	1001	0011	1110	1110	1010	1101	0000	0100	0111	3
1000	1110	0110	1101	1011	1110	1011	0110	0101	0101	1101	0011	0000	1000	1110	0011	1000	3
1000	0111	1111	0101	1111	1100	1010	1010	0011	0110	0000	1001	0101	0110	1001	1100	0011	3
1000	1111	0111	0001	1101	1101	0110	1100	0000	1011	1010	1100	1011	0001	0110	0111	1010	3
1000	1011	0011	0011	1100	0001	0000	1111	1101	0001	1111	0010	1100	1110	1101	1110	0010	3
1000	1001	0001	0010	0000	0111	0011	0010	0111	0100	0001	0101	0011	0101	0100	0110	0110	3

Table 6: Codewords corresponding to Example 8

$\{0\}, \{1,2,4,8,7,5\}, \{3,6\}$. *We have* $j = 1, s_1 = 0, s_2 = 3, s_2 - s_1 = 3, gcd(e_j, (s_2 - s_1)) = gcd(6,3) = 3$. *By Theorem 5,* $Rank_2(\mathcal{C}) = e_j - gcd(e_j, (s_2 - s_1)) = 6 - 3 = 3$. *In the Table 12 we have listed only 64 codewords of the 4096 codewords of*$\mathcal{C}$ *defined by* $A_1 = 1$ *and* A_8 *being free to take on all values of* F_{2^6}. *As* μ *takes on all non zero values from* F_{2^6} *in this block,the rank weight distribution of the code can be determined from the rank weight distribution of this block. We will only list components* a_0 *to* a_5, *because from Theorem 3 we know that the components* a_0 *to* $a_{e_j - 1}$ *establish the Rank of any codeword. In the table, the number of codewords having* F_2*-Rank=3=the number of elements of* F_{2^6} *having a* $(2^3 - 1) = 7^{th}$ *root in* F_{2^6} *is 9. Hence the Rank distribution of* $\mathcal{C}$ *is given by,*

$$N_0 = 1, N_3 = 9 \times 63 = 567, N_6 = 4096 - (567 + 1) = 3528.$$

Example 8 *Consider* $\mathcal{C}$ *a* $(15, 2)$ *primitive Cyclic code of length* $n = 15$ *over* F_{2^4} *defined by free transform domain components* A_7, A_{14}. *All other transform domain components are constrained to 0. We have* $[7]_{15} = \{7, 14, 13, 11\}, |[7]_{15}| = 4, j = 7, s_1 = 0, s_2 = 1, s = s_2 - s_1 = 1 - 0 = 1, g = gcd(e_j, s_2 - s_1) = gcd(4, 1) = 1$. *By Theorem 5,* $Rank_2(\mathcal{C}) = e_j - g = 3$. *We have listed only 16 codewords of the 256 codewords of* $\mathcal{C}_7$ *in Table 6. From these, we can establish the rank distribution of* $\mathcal{C}_7$. *As* $(2^s - 1) = 2^1 - 1 = 1$ *and every non zero value of* $\mu = \frac{A_7}{A_{14}}$ *,has a* 1^{st} *root in* F_{2^4} *all the codewords of this table characterized by non zero values of* A_7 *and* A_{14} *have* F_2*-Rank=4-1=3. The Rank distribution of* $\mathcal{C}$ *is given by,*

$$N_0 = 1, N_3 = 15 \times 15 = 225, N_4 = 256 - (225 + 1) = 30.$$

Example 9 *Consider* $\mathcal{C}$ *the* $(31, 2)$ *primitive cyclic code of length* $n = 31$ *over* F_{2^5} *defined by free transform domain components* A_7, A_{25}. *All other transform domain components are constrained to 0. The field* F_{2^5} *is generated by the*

A_7	A_{25}	a_0	a_1	a_2	a_3	a_4	Rank
10000	00000	10000	01111	11001	10001	00010	5
10000	10000	00000	00101	10111	01001	01101	4
10000	01000	11000	01010	11110	11101	10001	4
10000	00100	10100	11001	01110	10111	11111	4
10000	00010	10010	00100	00110	10010	11000	4
10000	00001	10001	11110	00010	00100	01111	4
10000	10100	00100	10011	00000	01111	10000	4
10000	01010	11010	00001	00001	11110	01011	4
10000	00101	10101	01000	10101	00010	10010	4
10000	10110	00110	11000	11111	01100	01010	4
10000	01011	11011	10000	11010	01011	00110	4
10000	10001	00001	10100	01100	11100	00000	4
10000	11100	01100	10110	00111	00011	00011	4
10000	01110	11110	10111	10110	11000	10110	4
10000	00111	10111	00011	01010	00001	01000	4
10000	10111	00111	01001	00100	11001	00111	4
10000	11111	01111	01100	00011	10101	10100	4
10000	11011	01011	11010	10100	10011	01001	4
10000	11001	01001	10001	01011	10000	10011	4
10000	11000	01000	00000	10000	00101	11110	4
10000	01100	11100	11100	01001	11011	01100	4
10000	00110	10110	10010	10001	10100	00101	4
10000	00011	10011	10101	11101	00111	10101	4
10000	10101	00101	00010	11011	11010	11101	4
10000	11110	01110	11101	11000	00000	11001	4
10000	01111	11111	00110	01101	01101	11011	4
10000	10011	00011	11111	10011	11111	11010	4
10000	11101	01101	00111	11100	10110	01110	4
10000	11010	01010	01011	01111	00110	00100	4
10000	01101	11101	01101	10010	01110	00001	4
10000	10010	00010	01110	01000	01010	10111	4
10000	01001	11001	11011	00101	01000	11100	4

Table 7: Codewords corresponding to Example 9

primitive polynomial $x^5 + x^2 + 1$. *We have* $[7]_{31} = \{7, 14, 28, 25, 19\}, |[7]_{31}| = 5, e_j = 5, j = 7, s_1 = 0$,
$s_2 = 3, s = s_2 - s_1 = 3 - 0 = 3, g = gcd(e_j, s_2 - s_1) = gcd(5, 3) = 1$. *By Theorem 5,* $Rank_{F_2}(\mathcal{C}) = e_j - s = 5 - 1 = 4$. *We have listed only 32 codewords of the 1024 codewords of* $\mathcal{C}_8$ *in Table 7. From these, we can establish the rank distribution of* $\mathcal{C}$. *This is done as follows: Since* $(2^3 - 1) = 8 - 1 = 7$ *and every non zero value of* $\mu = \frac{A_7}{A_{25}}$ *has a* 7^{th} *root in* F_{2^5}, *all the codewords in the table characterized by non zero values of* A_7 *and* A_{25} *have* $F_2 - Rank = 5 - 1 = 4$. *The Rank distribution of* $\mathcal{C}$ *is given by,* $N_0 = 1, N_4 = 31 \times 31 = 961, N_5 = 1024 - (961 + 1) = 62$. *We list only components* $a_0 - a_4$ *because we know from Theorem 3 that components* $a_0 - a_{e_j - 1}$ *establish the rank of the code.*

The following theorem shows that under certain conditions two (n, k) cyclic linear codes over F_{q^m} where $n | q^m - 1$ have identical rank-weight distributions:

Theorem 6 *Let* $\mathcal{C}_1$ *and* $\mathcal{C}_2$ *be two* (n, k) *cyclic codes over* F_{q^m} *where* $n | q^m - 1$ *with free transform components in* $\{A_{q^{s_1}}, A_{q^{s_2}}, \cdots, A_{q^{s_k}}\}$ *and* $\{A_{jq^{s_1}}, A_{jq^{s_2}}, \cdots, A_{jq^{s_k}}\}$ *respectively. If* $gcd(j, n) = 1$ *then the rank-weight distribution of the codes* $\mathcal{C}_1$ *and* $\mathcal{C}_2$ *are identical.*

Proof: Let **a** and **b** denote codewords in $\mathcal{C}_1$ and $\mathcal{C}_2$ characterized by $A_{q^{s_1}} = A_{jq^{s_1}} = x_1$,
$A_{q^{s_2}} = A_{jq^{s_2}} = x_2, \cdots, A_{q^{s_k}} = A_{jq^{s_k}} = x_k$, where $x_1, x_2 \cdots, x_k \in F_{q^m}$.We shall refer to such codewords as corresponding codewords.By the definition of the IDFT,

$$a_i = \sum_{j=0}^{n-1} \alpha^{-ij} A_j, for 0 \leq i \leq n-1 \tag{24}$$

Therefore $a_i = \alpha^{-iq^{s_1}} A_{q^{s_1}} + \alpha^{-iq^{s_2}} A_{q^{s_2}} + \cdots + \alpha^{-iq^{s_k}} A_{q^{s_k}}$

$$\Rightarrow a_i = \alpha^{-iq^{s_1}} x_1 + \alpha^{-iq^{s_2}} x_2 + \cdots + \alpha^{-iq^{s_k}} x_k \tag{25}$$

$\mathbf{a} = [a_0, a_1, \cdots, a_{n-1}]$ where $a_i, 0 \leq i \leq n-1$ is as defined in equation 14. Similarly,

$$b_i = \alpha^{-ijq^{s_1}} x_1 + \alpha^{-ijq^{s_2}} x_2 + \cdots + \alpha^{-ijq^{s_k}} x_k \tag{26}$$

$\underline{b} = [b_0, b_1, \cdots, b_{n-1}]$ where $b_i, 0 \leq i \leq n-1$ is as defined in equation 15.
We see that $b_i = a_{ij modulo n}$, for $0 \leq i \leq n-1$
If $gcd(j, n) = 1$ i.e j and n are relatively prime,then the components of codeword **b** constitute a permutation of the components of codeword **a**. Therefore,

$$Rank_{F_q}(\mathbf{a}) = Rank_{F_q}(\mathbf{b}) \tag{27}$$

Since this condition holds for every pair of corresponding codewords **a** and **b** of $\mathcal{C}_1$ and $\mathcal{C}_2$ we conclude that $\mathcal{C}_1$ and $\mathcal{C}_2$ have the same Rank distribution.

Notice that when n is prime, like 31 or 7, all non-zero cyclotomic cosets are of size m and using Theorem 6 it is sufficient to study codes with free components in $A_{[1]}$, when codes with free spectral components in one cyclotomic coset is under consideration.

Example 10 *Table 8 illustrates Theorem 6 with two length* 7 *cyclic codes* $\mathcal{C}_1$ *and* $\mathcal{C}_2$ *over* F_8*, taking non-zero values in the pairs of spectral components* A_1, A_4 *and* A_3, A_5 *respectively. Observe that in view of Theorem 5 codewords for fixed* A_1 *only have been listed in Table 8.*

Example 11 *In this example we consider two primitive length codes* $\mathcal{C}_1$ *and* $\mathcal{C}_2$ *of length* $n = 7$ *over* F_{2^3} *taking non zero values in pairs of spectral components* (A_1, A_4) *and* (A_3, A_5) *respectively. We have listed 8 codewords of each code characterized by* A_1 *and* A_3 *taking on fixed value equal to 1=*[100] *in Table 9. (This is adequate to illustrate the rank distribution of these codes in view of Theorem 5).*

Example 12 *In this example, we shall illustrate two non primitive cyclic codes with identical rank distributions. Consider the two length* $n = 7$*, non primitive Cyclic codes over* F_{2^6}*,* $\mathcal{C}_1$ *characterized by free transform domain components* A_1, A_4 *and* $\mathcal{C}_2$ *characterized by the free transform domain components* A_3, A_5*.*

$\mathcal{C}_1$						$\mathcal{C}_2$					
A_1	A_4	a_0	a_1	a_2	Rank	A_3	A_5	a_0	a_1	a_2	Rank
100	000	100	101	111	3	100	000	100	011	010	3
100	100	000	011	010	2	100	100	000	010	001	2
100	010	110	110	011	2	100	010	110	101	101	2
100	001	101	010	101	2	100	001	101	000	111	2
100	110	010	000	110	2	100	110	010	100	110	2
100	011	111	001	001	2	100	011	111	110	000	2
100	111	011	111	100	2	100	111	011	111	011	2
100	101	001	100	000	2	100	101	001	001	100	2

Table 8: Codewords corresponding to Example 10

Code 1						Code 2					
A_1	A_4	a_0	a_1	a_2	Rank	A_3	A_5	a_0	a_1	a_2	Rank
100	000	100	011	010	3	100	000	100	101	111	3
100	100	000	010	001	2	100	100	000	011	010	2
100	010	110	101	101	2	100	010	110	110	011	2
100	001	101	000	111	2	100	001	101	010	101	2
100	110	010	100	110	2	100	110	010	000	110	2
100	011	111	110	000	2	100	011	111	001	001	2
100	111	011	111	011	2	100	111	011	111	100	2
100	101	001	001	100	2	100	101	001	100	000	2

Table 9: Codewords corresponding to Example 11

A_1	A_4	A_8	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	Rank
1000	1000	0000	0000	1110	0110	1110	1110	0000	0110	1000	0110	0110	0000	1000	1110	1000	1000	2
1000	1000	1000	1000	0011	1111	1101	0101	0110	1001	0100	0001	0111	1110	1010	1011	1100	0010	
1000	1000	0100	0100	0100	1110	0011	0111	0011	1101	1110	1001	1010	0111	1001	0000	1010	1101	3
1000	1000	0010	0010	1011	0010	0100	0110	1101	1111	1011	1101	0000	1111	0100	1001	1001	0110	3
1000	1000	0001	0001	0000	0100	1011	1010	1010	1110	0101	1111	0101	1011	1110	0001	0100	1111	3
1000	1000	1100	1100	1001	0111	0000	1100	0101	0010	0010	1110	1011	1001	1011	0101	1110	0111	3
1000	1000	0110	0110	0001	1010	1001	1111	1110	0100	1101	0010	1100	1000	0101	0111	1011	0011	4
1000	1000	0011	0011	0101	0000	0001	0010	0111	0111	0110	0100	0011	0100	0010	0110	0101	0001	3
1000	1000	1101	1101	0111	0101	0101	1000	1111	1010	1111	0111	1000	0010	1101	1010	0010	0000	3
1000	1000	1010	1010	0110	1011	0111	1101	1011	0000	0111	1010	0001	0001	0110	1100	1101	1100	3
1000	1000	0101	0101	1010	1100	0110	0011	1001	0101	0011	0000	1001	1100	1111	1111	0110	1010	3
1000	1000	1110	1110	1100	0011	1010	0100	1000	1011	0001	0101	1101	0110	0111	0010	1111	1001	4
1000	1000	0111	0111	1111	1000	1100	1011	0100	1100	0000	1011	1111	0011	0011	1000	0111	0100	3
1000	1000	1111	1111	0010	0001	1111	0000	0010	0011	1100	1100	1110	1101	0001	1101	0011	1110	3
1000	1000	1011	1011	1000	1001	0010	1001	0001	1000	1010	0011	0010	1010	0000	0011	0001	1011	3
1000	1000	1001	1001	1101	1101	1000	0001	1100	0001	1001	1000	0100	0101	1100	0100	0000	0101	3

Table 10: Codewords corresponding to Example 13

The 2-cyclotomic cosets modulo 7 are $\{0\}, \{1,2,4\}$, $\{3,6,5\}$. *We have listed only 64 codewords of* $\mathcal{C}_1$ *(in Table 13) and* $\mathcal{C}_2$ *(in Table 14) to illustrate the identical Rank distributions of these codes. (In view of Theorem 5, this is adequate).*

4 Upper Bounds

An Upper Bound: We can make use of Theorem 4 to obtain an upper bound on the Rank of a code $\mathcal{C}$ characterized by more than two free transform domain components drawn from the same cyclotomic coset as follows:
Let $A_{jq^{s_1}}, A_{jq^{s_2}}, \cdots, A_{jq^{s_l}}, \cdots, A_{jq^{s_i}}, \cdots, A_{jq^{s_k}}$ be the k free transform domain components. Then

$$\begin{aligned} Rank_q(\mathcal{C}) \leq \min_{(i,l),(i>l)} \{e_j - gcd\left[(s_i - s_l), e_j e\right]\} = \\ e_j - \max_{(i,l),(i>l)} \{gcd\left[(s_i - s_j), e_j\right]\}. \end{aligned}$$

Example 13 *Let* $\mathcal{C}$ *be the* $(15,3)$ *primitive cyclic code of length* $n = 15$ *over* F_{2^4} *defined by free transform domain components* A_1, A_4, A_8. *All other transform domain components are constrained to 0. We have* $[1]_{15} = \{1,2,4,8\}, |[1]_{15}| = 4, e_j = 4, j = 1, s_1 = 0, s_2 = 2, s_3 = 3, s_2 - s_1 = 2, s_3 - s_2 = 1, s_3 - s_1 = 3, gcd(e_j, s_2 - s_1) = gcd(4,2) = 2$,
$gcd(e_j, s_3 - s_2) = gcd(4,1) = 1, gcd(e_j, s_3 - s_1) = gcd(4,3) = 1, max_{(i,l),(i>l)} gcd[s_i - s_l, e_j] = 2$. *Therefore by the upper bound,* $Rank_{F_2}(\mathcal{C}) \leq 4 - 2 = 2$. *From the listing of the codewords in Table 10 below, we observe that there are codewords having* F_2 *Rank equal to 2,3,4.*

Example 14 *Let* $\mathcal{C}$ *denote the (31,3) cyclic code over* F_{2^5} *characterized by the three free transform domain components* A_3, A_{12}, A_{17}. *Using the above notation, we have,* $j = 3, s_1 = 0, s_2 = 2, s_3 = 4$ *and* $s_3 - s_1 = 4; s_3 - s_2 = 2; s_2 - s_1 = 1$. *Moreover,* $gcd[5,(s_3 - s_1)] = gcd[5,4] = 1; gcd[5,(s_3 - s_2)] = gcd[5,2] = 1; gcd[5,(s_2 - s_1)] = gcd[5,1] = 1$. *The upper bound suggested by the expression* *above is* $Rank_2(\mathcal{C})$ $m - \max_{(i,l),(i>l)} \{gcd[m,(s_i - s_l)]\} = 5-1 = 4$. *whereas the actual rank of the code is 3.*

Similarly, let $\mathcal{C}'$ *denote the (63,3) cyclic code over* F_{2^6} *characterized by the three free transform domain components* A_2, A_4, A_{32}. *Using the above notation, we have,* $j = 1, s_1 = 1, s_2 = 2, s_3 = 5$ *and* $s_3 - s_1 = 5; s_3 - s_2 = 3; s_2 - s_1 = 1$. *Also,* $gcd[6,(s_3 - s_1)] = gcd[6,5] = 1; gcd[6,(s_3 - s_2)] = gcd[6,3] = 3; gcd[6,(s_2 - s_1)] = gcd[6,1] = 1$. *Therefore, the upper bound on* $Rank_2(\mathcal{C}')$ *is given by* $m - \max_{(i,l),(i>l)} \{gcd[m,(s_i - s_l)]\} = 6 - 3 = 3$ *and which in this case is the actual rank also.*

When e_j is even, we can specify a tighter upper bound in certain cases.

Theorem 7 *[Another upper bound] Let* e_j *be even. Let* $A_{jq^{s_1}}, A_{jq^{s_2}}, \cdots, A_{jq^{s_k}}$ *be the set of all free transform domain components of* $\mathcal{C}$ *where* $s_1, s_2, \cdots, s_k$ *with* $s_1 < s_2 < \cdots < s_{k-1} < s_k \leq e_j - 1$ *are related by*

$$s_2 - s_1 = s_3 - s_2 = \cdots = s_k - s_{k-1} = s_1 - s_k = s' \quad modulo \ e_j.$$

Then

$$Rank_q(\mathcal{C}) \leq s'.$$

Proof: Consider the codeword $\vec{a} \in C$ specified in the transform domain by, $A_{jq^{s_1}} = x^{q^{s_1}}, A_{jq^{s_2}} = x^{q^{s_2}}, \cdots, A_{jq^{s_{k-1}}} = x^{q^{s_{k-1}}}, A_{jq^{s_k}} = x^{s_k}$ where x is a primitive element of $F_{q^{e_j}}$. From the IDFT we have:

$$a_i = \alpha^{-ijq^{s_1}} A_{jq^{s_1}} + \alpha^{-ijq^{s_2}} A_{jq^{s_2}} + \cdots + + \alpha^{-ijq^{s_{k-1}}} A_{jq^{s_{k-1}}} + \alpha^{-ijq^{s_k}} A_{jq^{s_k}} \quad (28)$$

That is, $a_i = \alpha^{-ijq^{s_1}} x^{q^{s_1}} + \alpha^{-ijq^{s_2}} x^{q^{s_2}} + \cdots + + \alpha^{-ijq^{s_{k-1}}} x^{q^{s_{k-1}}} + \alpha^{-ijq^{s_k}} x^{q^{s_k}}$.
$a_i^{q^{s'}} = \left[\alpha^{-ijq^{s_1}} x^{q^{s_1}} + \alpha^{-ijq^{s_2}} x^{q^{s_2}} + \cdots + \alpha^{-ijq^{s_{k-1}}} x^{q^{s_{k-1}}} + \alpha^{-ijq^{s_k}} x^{q^{s_k}}\right]^{q^{s'}}$
$= \alpha^{-ijq^{s_1+s'}} x^{q^{s_1+s'}} + \alpha^{-ijq^{s_2+s'}} x^{q^{s_2+s'}} + \cdots + \alpha^{-ijq^{s_{k-1}+s'}} x^{q^{s_{k-1}+s'}} + \alpha^{-ijq^{s_k+s'}} x^{q^{s_k+s'}}$.
Since, $s_1 + s' = s_2 modulo e_j, s_2 + s' = s_3 modulo e_j, \cdots, s_{k-1} + s' = s_k modulo e_j s_k + s' = s_1 modulo e_j$ we have,
$a_i^{q^{s'}} = \left[\alpha^{-ijq^{s_1}} x^{q^{s_1}} + \alpha^{-ijq^{s_2}} x^{q^{s_2}} + \cdots + \alpha^{-ijq^{s_{k-1}}} x^{q^{s_{k-1}}} + \alpha^{-ijq^{s_k}} x^{q^{s_k}}\right]$ for all $i \in \{0,1,2,\cdots,(n-1)\}$. This means every component $a_i \in \vec{a}$ lies in the subfield $F_{q^{s'}}$ of $F_{q^{e_j}}$. Hence, $Rank_q(\vec{a}) \leq s'$. If $s' < \left\{e_j - \max_{(i,l),(i>l)} gcd\left((s_i - s_l), e_j\right)\right\}$, then we have obtained a tighter upper bound.

Example 15 *Let* $\mathcal{C}$ *be the* $(9,3)$ *cyclic code over* F_{2^6} *defined by the three free transform components* A_1, A_4 *and* A_7. . *The conjugacy classes are* $\{0\}, \{1,2,4,8,7,5\}, \{3,6\}$. *Therefore,* $e_j = 6, [1]_9 = \{1,2,4,8,7,5\}, |[1]_9| = 6$. *We have* $j = 1, s_1 = 0, s_2 = 2, s_3 = 4, s_2 - s_1 = 2, s_3 - s_2 = 2, s_3 - s_1 = 4, e_j = 6$.
$gcd(e_j,(s_2 - s_1)) = gcd(6,2) = 2, gcd(e_j,(s_3 - s_1)) = gcd(6,4) = 2, gcd(e_j,(s_3 - s_2)) = gcd(6,2) = 2$. *From the upper bound above, we obtain,*
$Rank_{F_2}(\mathcal{C}_7) \leq e_j - max_{(i,l),(i>l)} gcd\{e_j,(s_i - s_l)\}$
Therefore, $Rank_{F_2}(\mathcal{C}_7) \leq 6 - 2 = 4$. *From Table 15, we observe that when*

$A_1 = \delta = 010000, A_4 = \delta^4 = 000010, A_7 = \delta^{16} = 110010$, *where* δ *is a primitive element of* F_{2^6} *the corresponding codeword has* F_2 *Rank equal to 2. This can be explained as follows. From the definition of the IDFT,* $a_i = \alpha^{-i}A_1 + \alpha^{-4i}A_4 + \alpha^{-7i}A_7$ *where* α *is a primitive element of order 9 in* F_{2^6}*. Let us denote the primitive element of* F_{2^6} *by* δ*. Therefore,* $\alpha = \delta^7$*. Let us examine the case,* $A_1 = \delta = 010000, A_4 = \delta^4 = 000010, A_{16} = \delta^{16} = 110010$*(*$F_{2^6}$ *is generated by the polynomial* $x^6 + x + 1$*). Therefore,* $a_i = \delta^{-7i}\delta + \delta^{-28i}\delta^4 + \delta^{-49i}\delta^{16} = \left(\delta^{-7i}\delta\right) + \left(\delta^{-7i}\delta\right)^{2^2} + \left(\delta^{-7i}\delta\right)^{2^4}$*. We observe that* $a_i^{2^2} = a_i$ *for all* $i \in [0, 8]$*. Therefore* $a_i \in F_{2^2} \forall i$ *which implies that the the* F_2*-Rank of the corresponding codeword,* $\boldsymbol{a}$ *is* ≤ 2*. This is an example where the tighter upper bound is applicable. We have listed only 64 of the 262144 codewords of* $\mathcal{C}$*.*

Example 16 *Consider the* $(63, 3)$ *cyclic code over* F_{2^6} *defined by the three free transform domain components* A_1, A_4, A_{16}*. In this case* $j = 1, k = 3, s_1 = 0, s_2 = 2, s_3 = 4, e_1 = 6, q = 2$*. Therefore* $s_2 - s_1 = s_3 - s_2 = 2|6(= e_1)$*. From Theorem 7,the rank of this code is upper bounded by 2.*
Let us now compare this value with that given by our earlier upper bound. It can checked that the earlier bound gives the value 4. It turns out that the actual rank of this code is 2.

Both the bounds discussed above give an upper bound even when the free components are from more than one q-cyclotomic cosets. For such a code will have subcodes that have free spectral components in only one q-cyclotomic coset and the minimum of the bounds obtained for such subcodes will obviously be an upper bound for the original code.

5 Discussion

The results earlier obtained and reported in [10, 11] were for the general class of linear codes which did not lead to specific expressions of bounds for the rank-distance of the codes. In an attempt to realize specific expressions we restricted ourselves to the widely studied class of cyclic codes and the results obtained so far have been reported here. Possible directions for further research are :

- Extending the results of this report for cyclic codes for all values of $1 < k < n$.
- Generalizing the results of this report to the wider class of Abelian and quasi-cyclic codes.

Preliminary results have been obtained along these directions and will be reported after succeeding in obtaining more results.

References

[1] R.E.Blahut, *Theory and Practice of Error Control Codes,* Addison Wesley, 1983.

[2] E. M. Gabidulin, "Theory of Codes with Maximum Rank Distance," Problemy Peredachi Informatsii, 21, 99.3-14, Jan.-Mar.1985.

[3] R. M. Roth, "Maximum-rank Array Codes and Their Application to Crisscross Error Correction," IEEE Transactions on Information Theory, 37, pp.328–336, Mar. 1991.

[4] V. Tarokh and N. Seshadri and A. R. Calderbank, "Space-Time Codes for High Data Rate Wireless Communication: Performance Criterion and Code Construction," IEEE Transactions on Information Theory, 44, pp.744-765, Mar.1998.

[5] Roger Hammons, Jr., A. and El Gamal, "On the Theory of Space-Time Codes for PSK Modulation," IEEE Transactions on Information Theory, Vol.46, pp.524-542, Mar.2000.

[6] E. M. Gabidulin and Martin Bossert and P. Lusina, "Space-Time Codes Based on Rank Codes, Proceedings of IEEE International Symposium on Information Theory, p.284, Sorrento, Italy, June 2000.

[7] Martin Bossert and E. Gabidulin and P. Lusina, "Space-Time Codes Based on Gaussian Integers, (Private communication).

[8] E.Teletar, "Capacity of multi-antenna Gaussian channels," AT&T Bell Labs., Tech. Report, June 1995 and European Transactions on Telecommunications, Vol.10, pp.585-595, Nov. 1999.

[9] G.J.Foschini and M.Gans, "On the limits of wireless communication in a fading environment when using multiple antennas," Wireless Personal Communication, March 1998.

[10] K.N.Manoj and B.Sundar Rajan, "Full Rank Distance Codes and Optimal STBC for BPSK Modulation," Proc. IEEE International Symposium on Information Theory, Lausanne, Switzerland, June 30-July 5, 2002, p.276.

[11] K.N.Manoj and B.Sundar Rajan, "Full Rank Distance Codes," Technical Report No:TR-PME-2002-16, Electrical Communication Engineering Department, IISc, Bangalore, India, October 4, 2002.

[12] A.M.Patel and S.J.Hong, "Optimal Rectangular Code for high density magnetic tapes," IBM J.Res.Dev., vol 18,pp 579-588,Nov 1974.

[13] S.Lin and D.J.Costello, "Error Control Coding: Fundamentals and Applications," Englewood Cliffs, Prentice Hall, 1983, Sec 16.2.

[14] M.Blaum and R.J.McEliece, "Coding Protection for Magnetic Tapes: A generalization of the Patel-Hong Code," IEEE Trans. on Information Theory, IT-31, September 1985, pp.690-693.

[15] M.Blaum, P.G.Farrell and H.C.A. van Tilborg, "A class of burst error-correcting array codes," IEEE Trans. on Information Theory, IT-32, 1986, pp.836-839.

[16] M.Blaum, P.G.Farrell and H.C.A. van Tilborg, "Multiple burst correcting array codes," IEEE Trans. on Information Theory, IT-34, 1988, pp.1061-1066.

[17] P.Prusinkiewicz and S.Budkowski, "A double track error correction code for magnetic tape," IEEE Trans. on Comput. C-19, 1976, pp.642-645.

[18] A.M.Patel, "Adaptive Cross Parity Code for high density magnetic tape subsystem," IBM Jr.Res.Dev.,29(1985), pp.546-562.

[19] T.Fuja, C.Heegard and M.Blaum, "Cross parity check Convolutional Codes," IEEE Trans. on Information Theory, IT-35, 1989, pp.1264-1276.

[20] R.Goodman and M.Sayano, "Size limits on phased burst error correcting Array Codes," Electron.Lett. 26, (1990), pp.55-56.

[21] M.Blaum, J.Bruck and A.Vardy, "MDS array codes with independent parity symbols," IEEE Trans. on Information Theory, vol 42, pp.529-542.

[22] M.Blaum and R.M Roth, "New Array Codes for multiple phased burst correction," IEEE Trans. on Information Theory, vol 39, Jan 1993.

[23] M.Blaum and R.M Roth, "On lowest density MDS code," IEEE Trans. on Information Theory, vol 45, Jan. 1999, pp.46-59.

[24] L.Xu and J.Bruck, "MDS Array codes with Optimal Encoding," IEEE Trans. on Information Theory, vol 45, Jan 1999, pp.272-276.

A_5	a_0	a_1	a_2	a_3	a_4	a_5	a_6	Rank
000000	000000	000000	000000	000000	000000	000000	000000	0
100000	100000	111100	011010	111010	000110	011100	100110	3
010000	010000	011110	001101	011101	000011	001110	010011	3
001000	001000	001111	110110	111110	110001	000111	111001	3
000100	000100	110111	011011	011111	101000	110011	101100	3
000010	000010	101011	111101	111111	010100	101001	010110	3
000001	000001	100101	101110	101111	001010	100100	001011	3
110000	110000	100010	010111	100111	000101	010010	110101	3
011000	011000	010001	111011	100011	110010	001001	101010	3
001100	001100	111000	101101	100001	011001	110100	010101	3
000110	000110	011100	100110	100000	111100	011010	111010	3
000011	000011	001110	010011	010000	011110	001101	011101	3
110001	110001	000111	111001	001000	001111	110110	111110	3
101000	101000	110011	101100	000100	110111	011011	011111	3
010100	010100	101001	010110	000010	101011	111101	111111	3
001010	001010	100100	001011	000001	100101	101110	101111	3
000101	000101	010010	110101	110000	100010	010111	100111	3
110010	110010	001001	101010	011000	010001	111011	100011	3
011001	011001	110100	010101	001100	111000	101101	100001	3
111100	111100	011010	111010	000110	011100	100110	100000	3
011110	011110	001101	011101	000011	001110	010011	010000	3
001111	001111	110110	111110	110001	000111	111001	001000	3
110111	110111	011011	011111	101000	110011	101100	000100	3
101011	101011	111101	111111	010100	101001	010110	000010	3
100101	100101	101110	101111	001010	100100	001011	000001	3
100010	100010	010111	100111	000101	010010	110101	110000	3
010001	010001	111011	100011	110010	001001	101010	011000	3
111000	111000	101101	100001	011001	110100	010101	001100	3
011100	011100	100110	100000	111100	011010	111010	000110	3
001110	001110	010011	010000	011110	001101	011101	000011	3
000111	000111	111001	001000	001111	110110	111110	110001	3
110011	110011	101100	000100	110111	011011	011111	101000	3
101001	101001	010110	000010	101011	111101	111111	010100	3
100100	100100	001011	000001	100101	101110	101111	001010	3
010010	010010	110101	110000	100010	010111	100111	000101	3
001001	001001	101010	011000	010001	111011	100011	110010	3
110100	110100	010101	001100	111000	101101	100001	011001	3
011010	011010	111010	000110	011100	100110	100000	111100	3
001101	001101	011101	000011	001110	010011	010000	011110	3
110110	110110	111110	110001	000111	111001	001000	001111	3
011011	011011	011111	101000	110011	101100	000100	110111	3
111101	111101	111111	010100	101001	010110	000010	101011	3
101110	101110	101111	001010	100100	001011	000001	100101	3
010111	010111	100111	000101	010010	110101	110000	100010	3
111011	111011	100011	110010	001001	101010	011000	010001	3
101101	101101	100001	011001	110100	010101	001100	111000	3
100110	100110	100000	111100	011010	111010	000110	011100	3
010011	010011	010000	011110	001101	011101	000011	001110	3
111001	111001	001000	001111	110110	111110	110001	000111	3
101100	101100	000100	110111	011011	011111	101000	110011	3
010110	010110	000010	101011	111101	111111	010100	101001	3
001011	001011	000001	100101	101110	101111	001010	100100	3
110101	110101	110000	100010	010111	100111	000101	010010	3
101010	101010	011000	010001	111011	100011	110010	001001	3
010101	010101	001100	111000	101101	100001	011001	110100	3
111010	111010	000110	011100	100110	100000	111100	011010	3
011101	011101	000011	001110	010011	010000	011110	001101	3
111110	111110	110001	000111	111001	001000	001111	110110	3
011111	011111	101000	110011	101100	000100	110111	011011	3
111111	111111	010100	101001	010110	000010	101011	111101	3
101111	101111	001010	100100	001011	000001	100101	101110	3
100111	100111	000101	010010	110101	110000	100010	010111	3
100011	100011	110010	001001	101010	011000	010001	111011	3
100001	100001	011001	110100	010101	001100	111000	101101	3

Table 11: Codewords corresponding to Example 5

A_1	A_8	a_0	a_1	a_2	a_3	a_4	a_5	Rank
100000	000000	100000	111110	010110	010111	110100	001110	6
100000	100000	000000	100110	011100	100000	111010	111010	3
100000	010000	110000	110010	010011	111100	110011	010100	6
100000	001000	101000	111000	100100	110010	000111	000011	6
100000	000100	100100	111101	001111	110101	011101	111000	6
100000	000010	100010	001111	101010	000110	010000	010101	6
100000	000001	100001	010110	001000	101111	100110	110011	6
100000	110000	010000	101010	011001	001011	111101	100000	6
100000	011000	111000	110100	100001	011001	000000	011001	3
100000	001100	101100	111011	111101	010000	101110	110101	6
100000	000110	100110	001100	110011	100100	111001	100011	6
100000	000011	100011	100111	110100	111110	000010	101000	6
100000	110001	010001	000010	000111	110011	101111	011101	6
100000	101000	001000	100000	101110	000101	001001	110111	6
100000	010100	110100	110001	001010	011110	011010	100010	6
100000	001010	101010	001001	011000	100011	100011	011000	3
100000	000101	100101	010101	010001	001101	001111	000101	6
100000	110010	010010	011011	100101	011010	011001	111011	6
100000	011001	111001	011100	111111	100001	010010	100100	6
100000	111100	011100	101111	110010	001100	100111	011011	6
100000	011110	111110	000110	000100	101010	001101	110100	6
100000	001111	101111	100010	011111	111001	011000	010011	6
100000	110111	010111	110000	100010	000000	100010	110000	3
100000	101011	001011	111001	001100	101100	111111	010001	6
100000	100101	000101	001101	011011	111010	000001	110001	6
100000	100010	000010	010111	100000	110001	011110	100001	6
100000	010001	110001	011010	001101	000100	100001	101001	6
100000	111000	011000	101100	101011	101110	001110	101101	6
100000	011100	111100	110111	111000	111011	101001	101111	6
100000	001110	101110	001010	000001	000001	001010	101110	3
100000	000111	100111	100100	101101	011100	101011	011110	6
100000	110011	010011	110011	111011	100010	001011	000110	6
100000	101001	001001	001000	110000	111101	011011	001010	6
100000	100100	000100	100101	000101	000010	010011	001100	6
100000	010010	110010	000011	101111	101101	010111	001111	6
100000	001001	101001	010000	111010	001010	010101	111110	6
100000	110100	010100	101001	000000	101001	010100	010110	3
100000	011010	111010	000101	011101	001000	100100	000010	6
100000	001101	101101	010011	100011	101000	111100	001000	6
100000	110110	010110	011000	111100	111000	110000	001101	6
100000	011011	111011	101101	000011	110000	110110	111111	6
100000	111101	011101	000111	101100	110100	110101	100110	6
100000	101110	001110	010010	001011	110110	000100	011010	6
100000	010111	110111	101000	101000	110111	101100	000100	3
100000	111011	011011	110101	001001	000111	111000	001011	6
100000	101101	001101	001011	101001	011111	110010	111100	6
100000	100110	000110	010100	111001	010011	110111	010111	6
100000	010011	110011	101011	110001	010101	000101	110010	6
100000	111001	011001	000100	110101	010110	011100	010000	6
100000	101100	001100	100011	110111	100111	100000	000001	6
100000	010110	110110	000000	110110	001111	111110	111001	3
100000	001011	101011	100001	000110	011011	110001	100101	6
100000	110101	010101	000001	011110	010001	000110	101011	6
100000	101010	001010	010001	010010	010100	101101	101100	6
100000	010101	110101	011001	010100	100110	001000	011111	6
100000	111010	011010	011101	010111	111111	101010	110110	6
100000	011101	111101	011111	100110	000011	111011	010010	6
100000	111110	011110	011110	001110	011101	000011	000000	3
100000	011111	111111	101110	011010	010010	011111	001001	6
100000	111111	011111	110110	010000	100101	010001	111101	6
100000	101111	001111	111010	010101	001110	010110	100111	6
100000	100111	000111	111100	100111	101011	100101	101010	6
100000	100011	000011	111111	111110	001001	001100	011100	6
100000	100001	000001	001110	000010	011000	101000	000111	6

Table 12: Codewords corresponding to Example 7

A_1	A_4	a_0	a_1	a_2	a_3	a_4	a_5	a_6	Rank
100000	000000	100000	111010	100110	011010	011100	111100	000110	3
100000	100000	000000	100110	011100	100110	111010	111010	011100	2
100000	010000	110000	110100	111011	000100	001111	111111	001011	3
100000	001000	101000	111101	011000	010101	100101	001101	110000	3
100000	000100	100100	001001	111001	101101	110000	010100	011101	3
100000	000010	100010	010011	011001	110001	001010	101000	111011	3
100000	000001	100001	011110	001001	111111	010111	110110	101000	3
100000	110000	010000	101000	000001	111000	101001	111001	010001	3
100000	011000	111000	110011	000101	001011	110110	001110	111101	3
100000	001100	101100	001110	000111	100010	001001	100101	101011	3
100000	000110	100110	100000	000110	000110	100110	000000	100000	2
100000	000011	100011	110111	110110	010100	000001	100010	010101	3
100000	110001	010001	001100	101110	011101	100010	110011	111111	3
100000	101000	001000	100001	100010	101001	000011	001011	101010	3
100000	010100	110100	000111	100100	110011	100011	010111	010000	3
100000	001010	101010	010100	100111	111110	110011	011001	001101	3
100000	000101	100101	101101	010110	001000	111011	011110	110011	3
100000	110010	010010	000001	111110	010011	111111	101101	101100	3
100000	011001	111001	010111	101010	101110	111101	000100	010011	3
100000	111100	011100	011100	100000	000000	111100	100000	111100	2
100000	011110	111110	101001	100101	010111	001100	110010	011011	3
100000	001111	101111	000011	010111	101100	010100	111011	111000	3
100000	110111	010111	010110	001110	000001	011000	001111	011001	3
100000	101011	001011	101100	110010	100111	011110	010101	111001	3
100000	100101	000101	110001	101100	110100	011101	011000	101001	3
100000	100010	000010	001111	100011	001101	101100	101110	100001	3
100000	010001	110001	010000	010100	100001	000100	110101	100101	3
100000	111000	011000	101111	111111	110111	010000	001000	100111	3
100000	011100	111100	000000	011010	111100	011010	100110	100110	2
100000	001110	101110	100111	111000	001001	011111	110001	010110	3
100000	000111	100111	000100	101001	100011	101101	001010	001110	3
100000	110011	010011	100101	010001	110110	110100	100111	000010	3
100000	101001	001001	000101	001101	001100	001000	000001	000100	3
100000	100100	000100	010101	000011	010001	010110	010010	000111	3
100000	010010	110010	011101	000100	101111	011001	101011	110110	3
100000	001001	101001	011001	110111	110000	101110	000111	011110	3
100000	110100	010100	011011	011110	001111	000101	010001	001010	3
100000	011010	111010	011010	111010	100000	100000	011010	000000	2
100000	001101	101101	101010	101000	000111	000010	101111	000101	3
100000	110110	010110	110010	100001	100100	010011	000101	110111	3
100000	011011	111011	111110	010101	000101	101011	010000	101110	3
100000	111101	011101	111000	001111	100101	110111	101010	010010	3
100000	101110	001110	111011	000010	110101	111001	110111	001100	3
100000	010111	110111	001010	110100	111101	111110	001001	000011	3
100000	111011	011011	100010	101111	111001	001101	010110	110100	3
100000	101101	001101	110110	010010	111011	100100	101001	011111	3
100000	100110	000110	111100	111100	111010	000000	000110	111010	2
100000	010011	110011	111001	101011	001010	010010	100001	011000	3
100000	111001	011001	001011	010000	010010	011011	000010	001001	3
100000	101100	001100	010010	111101	011110	101111	100011	110001	3
100000	010110	110110	101110	011011	011000	110101	000011	101101	3
100000	001011	101011	110000	001000	011011	111000	010011	100011	3
100000	110101	010101	111111	110001	101010	001110	011011	100100	3
100000	101010	001010	001000	011101	000010	010101	011111	010111	3
100000	010101	110101	100011	001011	010110	101000	011101	111110	3
100000	111010	011010	000110	000000	011100	000110	011100	011010	2
100000	011101	111101	100100	110101	011001	010001	101100	001000	3
100000	111110	011110	110101	011111	101011	101010	110100	000001	3
100000	011111	111111	001101	001010	110010	000111	111000	110101	3
100000	111111	011111	010001	110000	001110	100001	111110	101111	3
100000	101111	001111	011111	101101	010000	110010	111101	100010	3
100000	100111	000111	011000	010011	011111	001011	001100	010100	3
100000	100011	000011	101011	001100	101000	100111	100100	001111	3
100000	100001	000001	000010	110011	000011	110001	110000	110010	3

Table 13: Codewords of code C_4 corresponding to Example 12

A_3	A_5	a_0	a_1	a_2	a_3	a_4	a_5	a_6	Rank
100000	000000	100000	011010	000110	100110	111100	111010	011100	3
100000	100000	000000	100110	011100	011100	111010	100110	111010	2
100000	010000	110000	000100	001011	111011	111111	110100	001111	3
100000	001000	101000	010101	110000	011000	001101	111101	100101	3
100000	000100	100100	101101	011101	111001	010100	001001	110000	3
100000	000010	100010	110001	111011	011001	101000	010011	001010	3
100000	000001	100001	111111	101000	001001	110110	011110	010111	3
100000	110000	010000	111000	010001	000001	111001	101000	101001	3
100000	011000	111000	001011	111101	000101	001110	110011	110110	3
100000	001100	101100	100010	101011	000111	100101	001110	001001	3
100000	000110	100110	000110	100000	000110	000000	100000	100110	2
100000	000011	100011	010100	010101	110110	100010	110111	000001	3
100000	110001	010001	011101	111111	101110	110011	001100	100010	3
100000	101000	001000	101001	101010	100010	001011	100001	000011	3
100000	010100	110100	110011	010000	100100	010111	000111	100011	3
100000	001010	101010	111110	001101	100111	011001	010100	110011	3
100000	000101	100101	001000	110011	010110	011110	101101	111011	3
100000	110010	010010	010011	101100	111110	101101	000001	111111	3
100000	011001	111001	101110	010011	101010	000100	010111	111101	3
100000	111100	011100	000000	111100	100000	100000	011100	111100	2
100000	011110	111110	010111	011011	100101	110010	101001	001100	3
100000	001111	101111	101100	111000	010111	111011	000011	010100	3
100000	110111	010111	000001	011001	001110	001111	010110	011000	3
100000	101011	001011	100111	111001	110010	010101	101100	011110	3
100000	100101	000101	110100	101001	101100	011000	110001	011101	3
100000	100010	000010	001101	100001	100011	101110	001111	101100	3
100000	010001	110001	100001	100101	010100	110101	010000	000100	3
100000	111000	011000	110111	100111	111111	001000	101111	010000	3
100000	011100	111100	111100	100110	011010	100110	000000	011010	2
100000	001110	101110	001001	010110	111000	110001	100111	011111	3
100000	000111	100111	100011	001110	101001	001010	000100	101101	3
100000	110011	010011	110110	000010	010001	100111	100101	110100	3
100000	101001	001001	001100	000100	001101	000001	000101	001000	3
100000	100100	000100	010001	000111	000011	010010	010101	010110	3
100000	010010	110010	101111	110110	000100	101011	011101	011001	3
100000	001001	101001	110000	011110	110111	000111	011001	101110	3
100000	110100	010100	001111	001010	011110	010001	011011	000101	3
100000	011010	111010	100000	000000	111010	011010	011010	100000	2
100000	001101	101101	000111	000101	101000	101111	101010	000010	3
100000	110110	010110	100100	110111	100001	000101	110010	010011	3
100000	011011	111011	000101	101110	010101	010000	111110	101011	3
100000	111101	011101	100101	010010	001111	101010	111000	110111	3
100000	101110	001110	110101	001100	000010	110111	111011	111001	3
100000	010111	110111	111101	000011	110100	001001	001010	111110	3
100000	111011	011011	111001	110100	101111	010110	100010	001101	3
100000	101101	001101	111011	011111	010010	101001	110110	100100	3
100000	100110	000110	111010	111010	111100	000110	111100	000000	2
100000	010011	110011	001010	011000	101011	100001	111001	010010	3
100000	111001	011001	010010	001001	010000	000010	001011	011011	3
100000	101100	001100	011110	110001	111101	100011	010010	101111	3
100000	010110	110110	011000	101101	011011	000011	101110	110101	3
100000	001011	101011	011011	100011	001000	010011	110000	111000	3
100000	110101	010101	101010	100100	110001	011011	111111	001110	3
100000	101010	001010	000010	010111	011101	011111	001000	010101	3
100000	010101	110101	010110	111110	001011	011101	100011	101000	3
100000	111010	011010	011100	011010	000000	011100	000110	000110	2
100000	011101	111101	011001	001000	110101	101100	100100	010001	3
100000	111110	011110	101011	000001	011111	110100	110101	101010	3
100000	011111	111111	110010	110101	001010	111000	001101	000111	3
100000	111111	011111	001110	101111	110000	111110	010001	100001	3
100000	101111	001111	010000	100010	101101	111101	011111	110010	3
100000	100111	000111	011111	010100	010011	001100	011000	001011	3
100000	100011	000011	101000	001111	001100	100100	101011	100111	3
100000	100001	000001	000011	110010	110011	110000	000010	110001	3

Table 14: Codewords of code C_2 corresponding to Example 12

A_1	A_4	A_7	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	Rank
010000	000010	000000	010010	000100	111010	101000	100110	010010	111010	100010	101000	4
010000	000010	100000	110010	001110	110100	111111	011000	001010	001101	010110	111110	6
010000	000010	010000	000010	000001	111101	010011	111001	011110	010001	111000	100011	6
010000	000010	001000	011010	110110	001001	000101	011001	010100	011111	101111	011101	6
010000	000010	000100	010110	011101	010011	001110	001001	010001	011000	010100	000010	4
010000	000010	000010	010000	111000	011110	111011	000001	100011	101011	111001	111101	6
010000	000010	000001	010011	011010	101000	010001	000101	111010	000010	011111	010010	6
010000	000010	110000	100010	001011	110011	000100	000111	000110	100110	001100	110101	6
010000	000010	011000	001010	110011	001110	111110	000110	011000	110100	110101	010110	6
010000	000010	001100	011110	101111	100000	100011	110110	010111	111101	011001	110111	6
010000	000010	000110	010100	100001	110111	011101	101110	100000	001001	001111	010111	6
010000	000010	000011	010001	100110	001100	000010	100010	001011	010011	000100	000111	6
010000	000010	110001	100011	010101	100001	111101	100100	101110	011110	110001	001111	6
010000	000010	101000	111010	111100	000111	010010	100111	001100	101000	011011	001011	6
010000	000010	010100	000110	011000	010100	110101	010110	011101	110011	001110	001001	6
010000	000010	001010	011000	001010	101101	010110	111110	100101	001110	110100	001000	6
010000	000010	000101	010111	000011	000001	110111	101010	111001	100000	101001	111000	6
010000	000010	110010	100000	110111	010111	010111	100000	110111	110111	010111	100000	2
010000	000010	011001	001011	101101	011100	000111	100101	110000	001100	001000	101100	6
010000	000010	111100	101110	100000	101001	001111	010111	000011	100001	110111	101010	6
010000	000010	011110	001100	010110	000011	001011	001110	101010	000111	011000	101001	6
010000	000010	001111	011101	001101	010110	001001	110010	001110	010100	111111	011000	6
010000	000010	110111	100101	110000	101100	001000	101100	011100	101101	011100	110000	4
010000	000010	101011	111001	011110	110001	111000	100011	010101	000001	111101	100100	6
010000	000010	100101	110111	001001	001111	100000	010100	100001	010111	011101	101110	6
010000	000010	100010	110000	110010	010000	101100	111111	111011	011100	001101	101011	6
010000	000010	010001	000011	011111	101111	101010	011010	110110	101001	000101	011001	4
010000	000010	111000	101010	111001	000000	101001	111000	000000	000011	000001	000000	4
010000	000010	011100	001110	101010	100111	011000	101001	011011	010110	000011	111100	4
010000	000010	001110	011100	010011	000100	110000	010001	100110	101100	000010	100010	6
010000	000010	000111	010101	111111	100101	100100	001101	001000	110001	110010	101101	6
010000	000010	110011	100001	101001	000101	101110	000011	011111	001111	101010	011010	6
010000	000010	101001	111011	100010	010101	101011	000100	100100	010000	100110	110001	6
010000	000010	100100	110110	010111	011101	011001	110111	001001	101111	100000	010100	6
010000	000010	010010	000000	111101	011001	000000	011110	101111	000000	100011	110110	4
010000	000010	001001	011011	101000	011011	111100	111010	111100	100111	010010	100111	4
010000	000010	110100	100110	010010	011010	100010	101000	000101	000100	111010	011111	6
010000	000010	011010	001000	001111	101010	101101	100001	101001	100101	101110	000011	4
010000	000010	001101	011111	110001	110010	011010	010101	111111	000101	100100	001101	6
010000	000010	110110	100100	101110	111110	110001	001111	110100	010101	100001	001010	4
010000	000010	011011	001001	010001	111000	010100	000010	000001	011101	010011	111001	6
010000	000010	111101	101111	111110	111011	110110	110100	101011	011001	001010	010000	6
010000	000010	101110	111100	011001	001010	100111	101111	111110	011011	110110	110100	4
010000	000010	010111	000101	111010	100010	011111	010010	000100	011010	101000	100110	6
010000	000010	111011	101001	011011	110110	000011	111100	011001	101010	100111	101111	6
010000	000010	101101	111111	111011	111100	001101	101011	100111	110010	010000	011011	6
010000	000010	100110	110100	101011	111001	001010	010000	111000	111110	111011	000001	6
010000	000010	010011	000001	100011	001011	111001	111101	000111	111000	011110	001100	6
010000	000010	111001	101011	100111	010010	010000	011011	101000	111011	111100	111010	6
010000	000010	101100	111110	100101	101110	110100	001000	001111	001010	101101	100001	6
010000	000010	010110	000100	100100	110000	100110	110001	101100	100010	010101	011100	6
010000	000010	001011	011001	010100	111111	101111	011101	001101	110110	001001	110010	4
010000	000010	110101	100111	001100	001000	011011	001011	101101	111100	000111	100101	6
010000	000010	101010	111000	000000	100011	000001	000000	111101	111001	000000	011110	4
010000	000010	010101	000111	000110	000110	001100	110101	110101	001011	110011	110011	4
010000	000010	111010	101000	000101	100100	111010	011111	110001	010010	011010	010101	6
010000	000010	011101	001111	110100	110101	100001	001010	110011	101110	111110	000110	6
010000	000010	111110	101100	011100	001101	011100	110000	110010	110000	101100	111111	4
010000	000010	011111	001101	001000	010001	110010	101101	000010	111111	100101	010011	6
010000	000010	111111	101101	000010	011111	100101	010011	011010	001000	010001	000101	6
010000	000010	101111	111101	000111	011000	011110	001100	010110	100011	001011	001110	6
010000	000010	100111	110101	110101	101011	110011	110011	010000	000110	000110	111011	4
010000	000010	100011	110001	101100	000010	010101	011100	010011	100100	110000	010001	6
010000	000010	100001	110011	010000	100110	000110	111011	100010	110101	101011	000100	6

Table 15: Codewords corresponding to Example 15