DRDO–IISc Programme on
Advanced Research in Mathematical Engineering

Full Rank Distance Codes

(TR-PME-2002-16)
by
K. N. Manoj, B. Sundar Rajan
ECE, IISc, Bangalore
email: bsrajan@ece,.iisc.ernet.in

October 4, 2002

Indian Institute of Science
Bangalore 560 012

Full Rank Distance Codes

K. N. Manoj, B. Sundar Rajan

October 4, 2002

ABSTRACT

Viewing the codewords of an $[n, k]$ linear code over a field F_{q^m} as $m \times n$ matrices over the base field F_q by expanding each entry of the codeword with respect to a basis of F_{q^m} over F_q, the rank weight of a codeword is the rank over F_q of the corresponding matrix and the rank of the code is the minimum rank weight among all the codewords. For the cases $m \geq n-k+1$ codes with maximum possible rank distance, called Maximum Rank Distance (MRD) codes have been studied previously. In this correspondence, we study codes with maximum possible rank distance for the cases $m \leq n-k+1$, calling them Full Rank Distance (FRD) codes. Generator matrices of FRD codes are characterized, and a method to construct FRD codes and codes with a specified minimum rank weight is described. We compare FRD codes with the two known classes of codes which give matrices of maximum rank over F_q: transpose of the MRD codes and codes obtained via stacking construction. We prove that for the case of $q = m = n = 2$, all the three classes coincide. For other values of q and $m = n$ the class of FRD codes has non-trivial intersection with the class of MRD codes and codes via stacking construction.

Keywords: Full rank distance codes, maximum rank distance codes, Rank distance, Space-Time Block codes.

1 Introduction

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 $r_q(\mathbf{c} - \mathbf{c}')$ [4]. The rank of $\mathcal{C}$, denoted by $d_{R,min}$ is defined as the minimum of $r_q(\mathbf{c} - \mathbf{c}')$ 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,

$$d_{R,min} \leq \min\{m, n-k+1\}. \tag{1}$$

The case where $d_{R,min} = n-k+1$ has been studied in [4, 5, 8] and are called MRD (Maximum Rank Distance) codes. In this paper we study codes with $d_{R,min} = m$ calling them "Full Rank Distance (FRD) Codes". Notice that the cases $d_{R,min} = n-k+1$ corresponds to considering only those cases where $m \geq n-k+1$ and the cases $d_{R,min} = m$ corresponds to studying those where $m \leq n-k+1$.

Rank distance codes over finite fields have applications in coding for storage devices (See [5] and the references therein) and coding for multiple antenna transmission [6]. Codes over finite fields with the rank as the metric under consideration, instead of the usual Hamming metric, was first studied by Gabidulin [4]. The same was studied by Roth [5] in the context of coding for storage devices. Using MRD codes for storage applications has been discussed in [5]. FRD codes too can be used in storage devices. Consider a binary $m \times n$ storage array. Roth in [5] 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 [13, 14]. A constructive approach to design codes suitable for such systems, called Space-Time codes was proposed and design criterion were developed in [6]. 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 $\mathbb{C}$. Hammons and El Gamal [7] propose the following construction of such matrices: Take an F_2-subspace C of $\mathbf{M}_{n\times l}^{(2)}$, 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 [7, 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 [7] and for a variety of complex signal sets obtained from Gaussian number fields in [12].

In this correspondence, we

- characterize the generator matrices of FRD codes (Theorem 2).
- present a straight forward upper bound on the size of FRD codes along with a necessary and sufficient condition for the existence of codes meeting this bound (Corollary 1).

- give a method to construct FRD codes and non-FRD codes with a specified rank (Subsection 2.2).
- provide a formula to calculate the rank of a linear code.
- study the interrelationship of FRD codes with those that can be obtained by transposing MRD codes (Section 3), and those obtained by stacking construction(Section 4).

These results essentially supplement the results available on rank distance codes.

The correspondence is organized as follows: In Section 2 the generator matrix characterization of FRD codes is given. Also, a simple upper bound on the size of an FRD code along with a necessary and sufficient condition for an FRD code to meet this bound is obtained. Construction of FRD codes and a formula to calculate the rank of any linear code is presented. Relation of FRD codes to transposed MRD codes are discussed in Section 3. In Section 4 it is shown that the codes obtained by stacking construction constitute a proper subclass of the class of FRD codes and FRD codes that are obtainable by stacking construction are characterized. Finally, Section 5 contains some concluding remarks along with a list of possible directions for further research. The Appendix contains a brief account of Singer cycles and proofs of assertions in the main text involving Singer cycles.

2 Generator Matrix characterization and Construction of FRD Codes

Throughout the paper, we consider only linear codes over F_{q^m}. Also, α will denote a primitive element of F_{q^m}, and $f(x) = x^m - f_{m-1}x^{m-1} - \cdots - f_1 x - f_0$ the minimal polynomial of α over F_q. Treating F_{q^m} as an m-dimensional vector space over F_q, the set $\{1, \alpha, \alpha^2, \cdots, \alpha^{m-1}\}$ forms an F_q-basis (polynomial basis [1]). Therefore every element in F_{q^m} can be seen as a polynomial in α over F_q. For an n-length vector over F_{q^m}, we write every element in it as an m-length vector in the above polynomial basis, which gives us an $m \times n$ matrix over F_q. We denote this way of associating an $m \times n$ matrix to an n-length vector over F_{q^m} by the map

$$\Phi : F_{q^m}^n \longrightarrow \mathbf{M}_{m\times n}^{(q)} \tag{2}$$

where $\mathbf{M}_{m\times n}^{(q)}$ denotes the set of all $m \times n$ matrices over F_q. Note that for any $\mathbf{v} = (v_i)_{i=1}^n \in F_{q^m}^n$, $\Phi(\mathbf{v})$ is the $m \times n$ matrix with the element at the ith column and jth row being the coefficient of α^j in the polynomial representation of v_i. Note that Φ is an F_q-space isomorphism. We will refer to the application of Φ on any vector $\mathbf{v}$ as *expansion* of $\mathbf{v}$. Also, we will use the same symbol Φ for expansion of vectors of different lengths. The length of the vector expanded will be clear from the context. For instance, when Φ is applied to a k-length vector over F_{q^m}, we get an $m \times k$ matrix over F_q.

Note 1 *We have chosen a polynomial basis for expansion of vectors in $F_{q^m}^n$ as matrices. The results would hold for any F_q-basis of F_{q^m}, because transformation from one basis to* *another does not alter rank. This particular choice of basis helps in the analysis and provide concreteness.*

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 of the matrix $\Phi(\mathbf{c}-\mathbf{c}')$ over F_q, denoted by $r_q(\Phi(\mathbf{c}-\mathbf{c}'))$ [4]. The rank of $\mathcal{C}$, denoted by $d_{R,min}$ is defined as:

$$d_{R,min} := \min_{\substack{\mathbf{c},\mathbf{c}' \in \mathcal{C} \\ \mathbf{c} \neq \mathbf{c}'}} r_q(\Phi(\mathbf{c}-\mathbf{c}'))$$

Definition 1 *A linear code $\mathcal{C} \subset F_{q^m}^n$ is called a* Full Rank Distance (FRD) code *if $d_{R,min} = m$.*

Notice that for any n-length FRD code over F_{q^m}, we have $m \leq n-k+1 \leq n$.

Let $\mathcal{C}$ be an n-length FRD code over F_{q^m}. If the first rows of any two matrices in $\Phi(\mathcal{C})$ are same, then the first row of the difference of the two matrices will be an all-zero vector, and the rank of the difference will be less than m. This is true for any other row also. Therefore, we get the following upper bound on the size of an FRD code:

Theorem 1 *Any n-length FRD code over F_{q^m} has at most q^n elements.*

Definition 2 *An n-length FRD code $\mathcal{C}$ over F_{q^m} is called a* Maximal Full Rank Distance (MFRD) code *if $|\mathcal{C}| = q^n$.*

2.1 Generator Matrix Characterization

We denote by M_α the companion matrix [1] of $f(x)$, *i.e.*,

$$M_\alpha = \begin{bmatrix} 0 & 0 & \cdots & 0 & f_0 \\ 1 & 0 & \cdots & 0 & f_1 \\ 0 & 1 & \cdots & 0 & f_2 \\ & & \vdots & & \\ 0 & 0 & \cdots & 1 & f_{m-1} \end{bmatrix} \tag{3}$$

and by M_α^T the transpose of it. The group $\langle M_\alpha \rangle = \{M_\alpha, M_\alpha^2, M_\alpha^3, \cdots, M_\alpha^{q^m-2}, M_\alpha^{q^m-1} = I\}$ generated by M_α will be referred to as **the companion cycle** of α and the group

$$\langle M_\alpha^T \rangle = \{M_\alpha^T, (M_\alpha^T)^2, (M_\alpha^T)^3, \cdots, (M_\alpha^T)^{q^m-2}, (M_\alpha^T)^{q^m-1} = I\}$$

generated by M_α^T as **the transpose companion cycle** of α. The companion cycle (the transpose companion cycle) taken along with the all-zero $m \times m$ matrix over F_q forms a field with q^m elements in which M_α (M_α^T) is primitive [11]. Consequently, M_α^j, $j = 0, \cdots, m-1$ are F_q-linear independent.

Definition 3 *Let $y_{ts}^{(j)}, t, s \in \{1, 2, \cdots, m\}, j \in \{0, 1, \cdots, m-1\}$ denote the element at t-th row and s-th column of M_α^j. For $t \in \{1, 2, \cdots, m\}$, define $\mathcal{M}^{(t)}$, called* **the t-th twisted companion matrix**, *the matrix whose entry at j row and sth column is $y_{ts}^{(j)}$, $0 \le j \le m-1$, $1 \le s \le m$. The set $\mathcal{M}$:$=\{\sum_{t=1}^{m} b_t \mathcal{M}^{(t)} : (b_1, b_2, \cdots, b_m) \ne \mathbf{0} \in F_q^m\}$ consisting of $q^m - 1$ elements will be called* **the twisted companion coset**.

Figure 1 illustrates the construction of $\mathcal{M}^{(t)}$ for $t \in \{1, 2, \cdots, m\}$. Consider the 3-dimensional $m \times m \times m$ array obtained as follows. For $j = 0, 1, \cdots, m-1$, the j-th vertical plane in the array contains M_α^j. Now for $t = 1, 2, \cdots, m$, $\mathcal{M}^{(t)}$ is the matrix in the t-th horizontal plane.

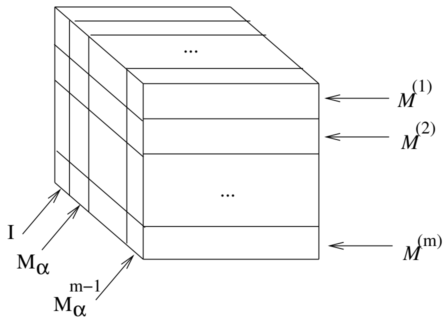

Figure 1: 3-Dimensional Array of M_α^j.

In the Appendix it is shown (Lemma 4) that $\mathcal{M}$ is a coset of $\langle M_\alpha \rangle$ in $GL_m(F_q)$ the group of invertible $m \times m$ matrices over F_q; hence the name "twisted companion coset". Also, it follows that non-trivial F_q-linear combinations of $\mathcal{M}^{(t)}, t = 1, 2, \cdots, m$ are non-singular. In other words, all elements of a twisted companion coset are invertible.

Definition 4 *Let G be a generator matrix of an $[n, k]$ code $\mathcal{C}$ over F_{q^m}. Denote the i-th row of G by $\mathbf{g}_i$, $\Phi(\mathbf{g}_i)$ by $[\mathbf{g}_i]$ and the s-th row of $[\mathbf{g}_i]$ by $\vec{g}_{i,s}$. The $km \times n$ matrix G_{ex} given* *by*

$$G_{ex} := \begin{bmatrix} \vec{g}_{1,1} \\ \cdot \\ \cdot \\ \cdot \\ \vec{g}_{1,m} \\ \vec{g}_{2,1} \\ \cdot \\ \cdot \\ \cdot \\ \vec{g}_{2,m} \\ \vec{g}_{k,1} \\ \cdot \\ \cdot \\ \cdot \\ \vec{g}_{k,m} \end{bmatrix} \tag{4}$$

is called the **Expanded Generator matrix** *corresponding to the generator matrix G. The vector space $\mathcal{K}_{ex}$ over F_q consisting of $k \times m$ matrices is defined by*

$$\mathcal{K}_{ex} := \left\{ \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ & & \ddots & \\ a_{k1} & a_{k2} & \cdots & a_{km} \end{bmatrix} : \sum_{i=1}^{k} \sum_{s=1}^{m} a_{is} \vec{g}_{i,s} = 0 \right\}. \tag{5}$$

The following lemma is useful in obtaining the generator matrix characterization (Theorem (2)) of FRD codes.

Lemma 1 *Let $\mathbf{u} = (u_1, \cdots, u_k) \in F_{q^m}^k$ and $\mathbf{b} = (b_1, \cdots, b_m) \in F_q^m$. Then*

$$\mathbf{b}\Phi(\mathbf{u}G) = \mathbf{0} \quad \textit{iff} \quad \Phi(\mathbf{u})^T \left(\sum_{t=1}^m b_t \mathcal{M}^{(t)}\right) \in \mathcal{K}_{ex}.$$

Proof: We can express $u_i \in F_{q^m}$ as $u_i = \sum_{j=0}^{m-1} u_{ij}\alpha^j$, where for $1 \leq i \leq k$ and $0 \leq j < m$, $u_{ij} \in F_q$. Then

$$\Phi(\mathbf{u})^T = \begin{bmatrix} u_{11} & u_{12} & \cdots & u_{1m} \\ u_{21} & u_{22} & \cdots & u_{2m} \\ & & \ddots & \\ u_{k1} & u_{k2} & \cdots & u_{km} \end{bmatrix}.$$

$\Phi(a\mathbf{v}) = \sum_{i=1}^m a_i M_\alpha^i \Phi(\mathbf{v})$ for all $a = \sum_{i=1}^m a_i \alpha^i \in F_{q^m}$ and $\mathbf{v} \in F_{q^m}^n$. Therefore, $\Phi(\mathbf{u}G) = \Phi(\sum_{i=1}^k u_i \mathbf{g}_i) = \sum_{i=1}^k \sum_{j=0}^{m-1} u_{ij} M_\alpha^j [\mathbf{g}_i]$, and, $\mathbf{b}\Phi(\mathbf{u}G) = \sum_{i=1}^k \sum_{j=0}^{m-1} \sum_{t=1}^m \sum_{s=1}^m u_{ij} b_t y_{ts}^{(j)} \vec{g}_{i,s}$. Consider $\sum_{t=1}^m b_t y_{ts}^{(j)}$. It is the element at jth row and sth column of $\sum_{t=1}^m b_t Y^{(t)}$.
Therefore $\sum_{j=0}^{m-1} \sum_{t=1}^m u_{ij} b_t y_{ts}^{(j)}$ is the element at i-th row and s-th column of $\Phi(\mathbf{u})^T \left(\sum_{t=1}^m b_t \mathcal{M}^{(t)}\right)$.
The equivalence is now obvious. □

Theorem 2 (Generator Matrix Characterization) *Let G be the generator matrix of an $[n,k]$ code $\mathcal{C}$ over F_{q^m}. Then $\mathcal{C}$ is FRD if and only if the km rows of the expanded generator matrix G_{ex} are F_q-linear independent.*

Proof: Suppose $\mathcal{K}_{ex}$ contains a non-zero matrix A. Choose any $Y \in \mathcal{M}$ and let $\mathbf{u}{:=}\Phi^{-1}((AY^{-1})^T)$. Then $\Phi(\mathbf{u})^T Y = A \in \mathcal{K}_{ex}$, so, by Lemma 1, the codeword $\mathbf{u}G$ has rank less than m.□

Corollary 1 *An n-length MFRD code over F_{q^m} exists if and only if m divides n.*

Proof: Let $\mathcal{C}$ be an $[n,k]$ MFRD code over F_{q^m} with the generator matrix G. $|\mathcal{C}| = q^{km} = q^n$, because the km vectors obtained by expansion of rows of G should be F_q-linear independent. Conversely, given n and m dividing n, we can partition an F_q-basis of F_q^n into $k = n/m$ classes each consisting of m vectors. We then write these classes as $m \times n$ matrices. Each matrix, using Φ^{-1}, gets a set of k vectors in $F_{q^m}^n$. Clearly, the code generated by these vectors is an MFRD code.□

2.2 Construction of codes with a given rank

2.2.1 Construction of FRD codes

We now give a method to construct a generator matrix for an $[n,k]$ FRD code over F_{q^m}. It follows from the proof of Corollary 1 that $k \leq \lfloor n/m \rfloor$.

1. Take any matrix M in $GL_n(F_q)$.
2. For $1 \leq i \leq k$, let $[\mathbf{g}_i]$ be the $m \times n$ sub-matrix of M containing the rows $(i-1)m + 1, (i-1)m+2, \cdots, im$.
3. Let $\mathbf{g}_i = \Phi^{-1}([\mathbf{g}_i]), 1 \leq i \leq k$.
4. Form the matrix G with $\mathbf{g}_i$ as rows. G is the required generator matrix.

Example 1 *We illustrate the above construction with four FRD codes using the $n \times n$ identity matrix I over F_q for M in Step 1 of the above construction. For the first two codes, m divides n, so the codes obtained are MFRD. For the other two codes, m does not divide n, so the codes obtained are not maximal. In fact, there exists no MFRD codes for these parameters.*

1. *Let $q=2$, $m=2$, $n=4$ and α a primitive element of F_{2^2} with the primitive polynomial $f(x) = 1 + x + x^2$. The code with the generator matrix $G = \begin{bmatrix} 1 & \alpha & 0 & 0 \\ 0 & 0 & 1 & \alpha \end{bmatrix}$ is a MFRD code with the following 16 codewords:*

$$\begin{array}{cccccccc} (0000) & (001\alpha) & (00\alpha\alpha^2) & (00\alpha^2 1) & (1\alpha 00) & (1\alpha 1\alpha) & (1\alpha\alpha\alpha^2) & (1\alpha\alpha^2 1) \\ (\alpha\alpha^2 00) & (\alpha\alpha^2 1\alpha) & (\alpha\alpha^2\alpha\alpha^2) & (\alpha\alpha^2\alpha^2 1) & (\alpha^2 100) & (\alpha^2 11\alpha) & (\alpha^2 1\alpha\alpha^2) & (\alpha^2 1\alpha^2 1) \end{array}$$

2. *Let $q = 3$, $m = 2$, $n = 2$ and α a primitive element of F_{3^2} with the minimal polynomial $f(x) = 1 + x^2$. The with the generator matrix $G = \begin{bmatrix} 1 & \alpha \end{bmatrix}$ is a MFRD code with the following 9 codewords:*

$$(00) \quad (1\alpha) \quad (\alpha\alpha^2) \quad (\alpha^2\alpha^3) \quad (\alpha^3\alpha^4) \quad (\alpha^4\alpha^5)(\alpha^5\alpha^6) \quad (\alpha^6\alpha^7) \quad (\alpha^7 1)$$

3. *Let $q = 2$, $m = 3$, $n = 4$ and α a primitive element of F_{2^3} with the primitive polynomial $f(x) = 1 + x + x^3$. The code with the generator matrix $G = \begin{bmatrix} 1 & \alpha & \alpha^2 & 0 \end{bmatrix}$ is a FRD code, which is not maximal.*

4. *Let $q = 3$, $m = 2$, $n = 3$ and α a primitive element of F_{3^2} with the primitive polynomial $f(x) = 1 + x^2$. The code with the generator matrix $G = \begin{bmatrix} 1 & \alpha & \alpha^2 \end{bmatrix}$ is a non-maximal FRD code.*

2.2.2 Construction of non-FRD Codes with a specified rank.

In this subsection we present a construction for $[n, k]$ codes over F_q in which all codewords have rank weight at least $m - \nu$ for some $1 \leq \nu < m$. The following construction helps us to generate such codes for $km - \nu \leq n \leq q^{km-\nu}$. Choose a non-zero matrix $A = [a_{is}], 1 \leq i \leq k, 1 \leq j \leq m$ over F_q, and a ν-dimensional subspace V of $\langle M_\alpha \rangle \cup \{0\}$. Let $\mathcal{A}$:=$\{AM : M \in V\}$. Consider the $[km, \nu]$ linear code C over F_q given by

$$\left\{ (b_{11}, b_{12}, \cdots, b_{1m}, b_{21}, \cdots, b_{2m}, \cdots, b_{k1}, \cdots, b_{km}) : \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1m} \\ b_{21} & b_{22} & \cdots & b_{2m} \\ & & \ddots & \\ b_{k1} & b_{k2} & \cdots & b_{km} \end{bmatrix} \in \mathcal{A} \right\}.$$

Take its dual code C$^\perp$. It has $q^{km-\nu}$ codewords. Take n codewords in C$^\perp$ such that some $km - \nu$ of them are F_q-linear independent, and write them as columns of a $km \times n$ matrix $\tilde{G}$ over F_q. For $i = 1, \cdots, k$, take the $m \times n$ sub-matrix of $\tilde{G}$ consisting of rows $(i-1)m + 1, (i-1)m + 2, \cdots, im$. Pull back this sub-matrix using Φ to $\mathbf{g}_i \in F_{q^m}^n$. Let G be the $k \times n$ matrix over F_{q^m} with $\mathbf{g}_i, 1 \leq i \leq k$ as its rows. It is easy to see that G has rank k and that the code generated by G has minimum rank distance $m - \nu$.

2.3 A Formula for the Rank of a Linear Code

The following theorem gives a formula for the rank of a linear code.

Theorem 3 *Let G be the generator matrix of an $[n, k]$ code $\mathcal{C}$ over F_{q^m}. For every $\mathbf{u} \in F_{q^m}^k$ let $\mathcal{K}_\mathbf{u}$:=$\{A \in \mathcal{K}_{ex} : A = \Phi(\mathbf{u})^T Y$ for some $Y \in \mathcal{M}\}$. Let $\mathcal{E}_1, \mathcal{E}_2, \cdots, \mathcal{E}_r$ be the equivalence classes into which $\mathcal{E}_{ex}$ is partitioned by the equivalence relation: $A_1, A_2 \in \mathcal{K}_{ex}$ are related if and only if $A_2 = A_1 M_\alpha^i$ for some integer i. Then for all $\mathbf{u} \neq \mathbf{0} \in F_{q^m}^k$, either $\mathcal{K}_\mathbf{u} = \emptyset$ or $\mathcal{K}_\mathbf{u} = \mathcal{E}_i$ for some $1 \leq i \leq r$. Rank of the codeword $\mathbf{u}G$ is $m - \dim(\mathcal{K}_\mathbf{u} \cup \{0\})$. In particular,*

$$d_{R,min} = m - \max_{1 \leq i \leq r} \dim(\mathcal{E}_i \cup \{0\}).$$

Proof: First we show that for any $A_1, A_2 \in \mathcal{K}_{ex}$, $A_2 = A_1 M_\alpha^i$ for some integer i iff $A_1, A_2 \in \mathcal{K}_{\mathbf{u}}$ for some $\mathbf{u} \in F_{q^m}^k$ as follows: Choose any $Y \in \mathcal{M}$ and let $\mathbf{u}{:=}\Phi^{-1}((A_2 Y^{-1})^T)$. Then $\Phi(\mathbf{u})^T Y = A_2 = A_1 M_\alpha^i$. Since $\mathcal{M}$ is a left-coset of $\langle M_\alpha \rangle$, $Y M_\alpha^{-i} \in \mathcal{M}$. Therefore $A_1 \in \mathcal{K}_{\mathbf{u}}$. Conversely, $A_1, A_2 \in \mathcal{K}_{\mathbf{u}} \Rightarrow \exists Y_1, Y_2 \in \mathcal{M}$ such that $A_1 Y_1^{-1} = A_2 Y_2^{-1} = \Phi(\mathbf{u})^T \Rightarrow A_2 = A_1 Y_1^{-1} Y_2$. Since $\mathcal{M}$ is a left-coset of $\langle M_\alpha \rangle$, $Y_1^{-1} Y_2 = M_\alpha^i$ for some integer i.

The theorem follows from the observation that $\mathcal{K}_{\mathbf{u}} = \emptyset \iff r_q(\Phi(\mathbf{u}G)) = m$, which means that the nullity of $\Phi(\mathbf{u}G)$ is dimension of the vector-space $\mathcal{K}_{\mathbf{u}} \cup \{0\}$. $\square$

The following example illustrates the application of the above theorem.

Example 2 *We determine the rank weights of codewords in the* $[3, 2]$ *code over* F_8 *generated by* $G = \begin{bmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha^4 \end{bmatrix}$, *where* α *is a primitive element of* F_8, *with the minimal polynomial* $f(x) = x^3 + x + 1$. *For this case,* $q = 2$, $m = n = 3$ *and* $k = 2$. $M_\alpha = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$.

Codes with similar generator matrices have been given as examples of MRD codes in [4]. G *generates an MRD code; therefore* $d_{R,min} = 3 - 2 + 1 = 2$.

The coset $\mathcal{M}$ *of* $\langle M_\alpha \rangle$ *is*

$$\left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \right\}$$

Expanding the rows of G *we get,*

$$G_{ex} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$$

Then the equivalence classes of $\mathcal{K}_{ex}$ *are*

$$\mathcal{E}_1 = \left\{ \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \right\}, \; \mathcal{E}_2 = \left\{ \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \right\}, \; \mathcal{E}_3 = \left\{ \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \right\}, \; \mathcal{E}_4 = \left\{ \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \right\},$$

$$\mathcal{E}_5 = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \right\}, \; \mathcal{E}_6 = \left\{ \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \right\}, \; \mathcal{E}_7 = \left\{ \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \right\}, \; \mathcal{E}_8 = \left\{ \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \right\}$$

The equivalence classes $\mathcal{E}_i$ *are singleton sets. Rank weights of different codewords are given* *below.*

$\mathbf{u}$	$\mathbf{u}G$	$\mathcal{A}_{\mathbf{u}}$	$r_q(\Phi(\mathbf{u}G))$	$\dim(\mathcal{A}_{\mathbf{u}} \cup \{0\})$
01	$1\alpha^2\alpha^4$	$\emptyset$	3	0
10	$1\alpha\alpha^2$	$\emptyset$	3	0
11	$0\alpha^4\alpha$	$\mathcal{E}_5$	2	1
1α	$\alpha^3\alpha^6\alpha^3$	$\mathcal{E}_2$	2	1
$1\alpha^2$	$\alpha^6\alpha^2 1$	$\mathcal{E}_3$	2	1
$1\alpha^3$	$\alpha\alpha^6\alpha^6$	$\mathcal{E}_6$	2	1
$1\alpha^4$	$\alpha^5\alpha^5\alpha^4$	$\mathcal{E}_4$	2	1
$1\alpha^5$	$\alpha^4\alpha^3 0$	$\mathcal{E}_8$	2	1
$1\alpha^6$	$\alpha^2 0\alpha^5$	$\mathcal{E}_7$	2	1

We indeed see that $d_{R,min} = 2$.

3 FRD Codes vs. MRD Codes

In this section we study the interrelationship between FRD codes and MRD codes. In the next section, we study the interrelationship with codes that can be obtained via stacking construction.

An $[n, k]$ MRD code over F_{q^m} has minimum rank distance $n - k + 1$ [4]. Suppose that an $[n, k]$ MRD code $\mathcal{C}$ over F_{q^m} is FRD also. Then $m = n - k + 1$ and $km \leq n$. This gives $km \leq k + m - 1 \Rightarrow k = 1$ or $m = 1$. Therefore,

Proposition 1 *For $m \geq 2$ the only FRD codes that are MRD also can be only of dimension one.*

From the proposition above it follows that the class of FRD codes that are MRD also constitute a proper subclass of the well studied $[n, 1]$ linear MDS codes over F_{q^m} [11].

3.1 Transpose MRD Codes

In general, for MRD codes $m \geq n - k + 1$. FRD codes are defined for $n - k + 1 \geq m$. Therefore, it is possible that an n-length FRD code over F_{q^m} can be obtained by starting from an m-length MRD code over F_{q^n} and transposing all the matrices of it. Towards identifying such codes, we define

Definition 5 *The length l-code over F_{q^n} obtainable by transposing all the matrices of some n-length MRD code over F_{q^l} is called a Transpose MRD (TMRD) code.*

In this section, we characterize all FRD codes that are TMRD codes. An extension field F_{q^m} of F_q, (as we noted in Subsection 2.1) can be realized as $K{:=}\langle M_\alpha \rangle \cup \{0\}$. It turns out to be convenient to use this realization of F_{q^m} to study TMRD codes. Note that the set of $m \times n$ matrices over F_q denoted by $\mathbf{M}^{(q)}_{m\times n}$ is a K-vector space, where addition is matrix addition and scalar multiplication is left-multiplication of a matrix in $\mathbf{M}^{(q)}_{m\times n}$ by a matrix in K.

Note 2 *The set of invertible F_q-linear operators on F_q^m form a group under composition of operators, denoted by $GL_m(F_q)$. It is a non-Abelian group. We call a subgroup $H \subset GL_m(F_q)$* irreducible *if H does not fix any subspace of F_q^m. Irreducible cyclic subgroups of $GL_m(F_q)$ of order $q^m - 1$ are called Singer cycles [2]. Notice that $\langle M_\alpha \rangle$ and $\langle M_\alpha^T \rangle$ are indeed Singer Cycles. Instead of realizing the field as $K := \langle M_\alpha \rangle \cup \{0\}$, one could realize the field as $K := \langle S \rangle \cup \{0\}$ where S is a generator of the Singer cycle $\langle S \rangle$. Some basic properties of Singer cycles and proofs of results that use some of the properties of Singer cycles are given in the Appendix.*

Let $\mathcal{C}$ be an $[n,k]$ linear code over F_{q^m} and G its generator matrix. Any codeword $\mathbf{c} \in \mathcal{C}$ can be written as $\mathbf{c} = \sum_{i \in I} \alpha^{e_i} \mathbf{g}_i$ for some index set $I \subseteq \{1, 2, \cdots, k\}$ and $0 \leq e_i \leq q^m - 2 \; \forall i \in I$, where α is a primitive element of F_{q^m}. Then

$$\Phi(\mathbf{c}) = \sum_{i \in I} M_\alpha^{e_i} [\mathbf{g}_i],$$

from which it follows that $\Phi(\mathcal{C})$ is a k-dimensional K-subspace of $\mathbf{M}_{m \times n}^{(q)}$. Hence, we will hereafter associate and deal with the corresponding k-dimensional K-subspace $\Phi(\mathcal{C})$ of $\mathbf{M}_{m \times n}^{(q)}$ for an $[n,k]$ linear code over F_{q^m}. With this association, TMRD codes can be alternatively be defined as: A code $\mathcal{C} \subset \mathbf{M}_{m \times n}^{(q)}$ is called *Transpose MRD* (TMRD) if the set of transposes of the matrices in $\mathcal{C}$ is an m-length MRD code over F_{q^n}.

Now, suppose an $[n,k]$ FRD code $\mathcal{C}$ over F_{q^m} is TMRD. Denote the set of transposes of the matrices in $\mathcal{C}$ by $\mathcal{C}^T$. This is an m-length MRD code over F_{q^n}. Let k' be the dimension of $\mathcal{C}^T$. (Note that this dimension refers to the dimension of $\mathcal{C}^T$ as a linear code over F_{q^n}). Then $|\mathcal{C}^T| = q^{nk'}$. Equating the size of $\mathcal{C}$ and $\mathcal{C}^T$, we get

$$q^n \geq q^{km} = |\mathcal{C}| = |\mathcal{C}^T| = q^{nk'}, \tag{6}$$

from which it follows that $k' = 1$ and $k = n/m$. That m divides n is clear from Corollary 1, because if an $[n,k]$ FRD code over F_{q^m} that is TMRD has q^n elements then it is MFRD and hence m divides n. This proves:

Theorem 4 *If an $[n,k]$ FRD code $\mathcal{C}$ over F_{q^m} is TMRD, then it is MFRD. (That the converse is not true follows from Example 4).*

3.2 Square FRD codes

In this subsection, we study FRD codes consisting of square matrices, i.e., $m = n$ that are TMRD. For such a code, the dimension $k = 1$. FRD codes of square matrices are important for application to space-time block codes since they result in what is known as *minimal-delay* codes [6]. Clearly, any $[m, 1]$ FRD code $\mathcal{C}$ over F_{q^m} can be written as $\mathcal{C} = \{MZ : M \in K\}$ for some $Z \in GL_m(F_q)$, where $Z = \Phi(\mathbf{g_i})$.

Theorem 5 *Let α be a primitive element of F_{q^m}, M_α its companion matrix and $K = \langle M_\alpha \rangle \cup 0$. Then the FRD code $\mathcal{C} = \{MZ : M \in K\}$ generated by $Z \in GL_m(F_q)$ is TMRD if and only if $Z^{-1} \langle M_\alpha \rangle Z = \langle M_\alpha^T \rangle$.*

Proof: Since $Z^T \in \mathcal{C}^T$, $\mathcal{C}^T$ is MRD $\iff$ $\mathcal{C}^T = \{MZ^T : M \in K\}$ $\iff$ $M_\alpha Z = Z(M_\alpha^r)^T$ for some r such that $(M_\alpha^r)^T$ has order $q^m - 1$ in $GL_m(F_q)$ $\iff$ $Z^{-1}M_\alpha Z = (M_\alpha^r)^T$, for some $0 \le r \le q^m - 2$, r co-prime to $q^m - 1$ $\iff$ $Z^{-1}\langle M_\alpha \rangle Z = \langle M_\alpha^T \rangle$. □

Corollary 2 *For any m, there exist $(m, 1)$ FRD codes over F_{q^m} that are TMRD.*□

Proof: Since $\langle M_\alpha \rangle$ and $\langle M_\alpha^T \rangle$ are Singer cycles, from the properties of Singer cycles discussed in the Appendix, it follows that there exists $Z \in GL_m(F_q)$ for every m such that $Z^{-1}\langle M_\alpha \rangle Z = \langle M_\alpha^T \rangle$. □

Lemma 2 *For $m = 2$, $M_\alpha^T \in \langle M_\alpha \rangle$ iff $f(x) = x^2 - f_1 x - 1$ for some $f_1 \in F_q$. For $m > 2$, $M_\alpha^T \notin \langle M_\alpha \rangle$*

Proof: Given in the Appendix. □

Let us denote the normalizer of $\langle M_\alpha^T \rangle$ in $GL_m(F_q)$ by $N(\langle M_\alpha^T \rangle)$. Then

Lemma 3 *The set $\mathcal{A} = \{A \in GL_m(F_q) : A^{-1}\langle M_\alpha \rangle A = \langle M_\alpha^T \rangle\}$ forms a right coset of $N(\langle M_\alpha^T \rangle)$ in $GL_m(F_q)$. Further, if $m = 2$, $\mathcal{A} = N(\langle M_\alpha^T \rangle)$ iff $f(X) = X^2 - f_1 X - 1$ for some $f_1 \in F_q$. For $m > 2$, $\mathcal{A} \neq N(\langle M_\alpha^T \rangle)$.*

Proof: Given in the Appendix. □

Theorem 6 *There exist precisely $|N(\langle M_\alpha^T \rangle)| = m(q^m - 1)$ matrices $Z \in GL_m(F_q)$ such that the FRD code $\mathcal{C} = \{MZ : M \in K\}$ generated by Z is TMRD.*

Proof:$N(\langle M_\alpha^T \rangle)$ has $m(q^m - 1)$ elements [2]. Now the theorem follows from combining Theorem 5 and Lemma 3. □

Example 3 *Consider length 2 FRD codes over over F_{2^2}. They are 2×2 matrices over F_2. The only degree 2 primitive polynomial over F_2 is $f(x) = x^2 + x + 1$, so*

$$M_\alpha = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

M_α has order 3 in $GL_2(F_2)$, which has 6 elements. Therefore $\langle M_\alpha \rangle$ has index 2 in $GL_2(F_2)$, and, hence is normal in $GL_2(F_2)$. Therefore $N(\langle M_\alpha^T \rangle) = GL_2(F_2)$. Moreover, it is clear from the definition that any such FRD codes is the union of a coset of $\langle M_\alpha \rangle$ and $\{0\}$, so there are only two FRD codes with these parameters. We state this as a theorem.

The only $[2, 1]$ FRD codes over F_2 are

$$\left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\} \text{ and } \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\}.$$

Both codes are TMRD.

Example 4 *The previous example lists all* $[2,1]$ *FRD codes over* F_{2^2}*. All of them are TMRD. Below we list examples of* $[3,1]$ *FRD codes* F_2^3*. These examples below have been obtained using the tables Singer cycles and their normalizers given in [3]. The primitive polynomial used is* x^3+x+1 *and the corresponding companion matrix is* $M_\alpha = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$.

A code that is FRD but not TMRD: Let $A = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$*. Then* $A \in N(\langle M_\alpha^T \rangle)$ *[3]. Therefore the FRD code generated by A is not TMRD, as seen below. The FRD code generated by A is*

$$\left\{ \begin{bmatrix} 0&0&0\\0&0&0\\0&0&0 \end{bmatrix}, \begin{bmatrix} 1&0&1\\1&1&0\\1&0&0 \end{bmatrix}, \begin{bmatrix} 1&0&0\\0&0&1\\1&1&0 \end{bmatrix}, \begin{bmatrix} 1&1&0\\0&1&0\\0&0&1 \end{bmatrix}, \begin{bmatrix} 0&0&1\\1&1&1\\0&1&0 \end{bmatrix}, \begin{bmatrix} 0&1&0\\0&1&1\\1&1&1 \end{bmatrix}, \begin{bmatrix} 1&1&1\\1&0&1\\0&1&1 \end{bmatrix}, \begin{bmatrix} 0&1&1\\1&0&0\\1&0&1 \end{bmatrix} \right\}$$

while the MRD code generated by A^T *is*

$$\left\{ \begin{bmatrix} 0&0&0\\0&0&0\\0&0&0 \end{bmatrix}, \begin{bmatrix} 1&1&1\\0&1&0\\1&0&0 \end{bmatrix}, \begin{bmatrix} 1&0&0\\0&1&1\\0&1&0 \end{bmatrix}, \begin{bmatrix} 0&1&0\\1&1&0\\0&1&1 \end{bmatrix}, \begin{bmatrix} 0&1&1\\0&0&1\\1&1&0 \end{bmatrix}, \begin{bmatrix} 1&1&0\\1&0&1\\0&0&1 \end{bmatrix}, \begin{bmatrix} 0&0&1\\1&1&1\\1&0&1 \end{bmatrix}, \begin{bmatrix} 1&0&1\\1&0&0\\1&1&1 \end{bmatrix} \right\}.$$

Notice that matrices in one set are not transposes of those in the other set.
An FRD code that is TMRD: We saw earlier that the matrices $\mathcal{M}^{(1)}, \mathcal{M}^{(2)}, \cdots, \mathcal{M}^{(m)}$ *are valid choices for* A^{-1} *so that the FRD code generated by A is TMRD. Let* $A^{-1} = \mathcal{M}^{(1)} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$*. Then* $A = A^{-1}$*. It is easy to verify that the following FRD code generated by A is TMRD.*

$$\left\{ \begin{bmatrix} 0&0&0\\0&0&0\\0&0&0 \end{bmatrix}, \begin{bmatrix} 1&0&0\\0&0&1\\0&1&0 \end{bmatrix}, \begin{bmatrix} 0&1&0\\1&1&0\\0&0&1 \end{bmatrix}, \begin{bmatrix} 0&0&1\\0&1&1\\1&1&0 \end{bmatrix}, \begin{bmatrix} 1&1&0\\1&1&1\\0&1&1 \end{bmatrix}, \begin{bmatrix} 0&1&1\\1&0&1\\1&1&1 \end{bmatrix}, \begin{bmatrix} 1&1&1\\1&0&0\\1&0&1 \end{bmatrix}, \begin{bmatrix} 1&0&1\\0&1&0\\1&0&0 \end{bmatrix} \right\}$$

Take any FRD code described in the example above. It is an F_q-subspace of $\mathbf{M}_{m\times m}(q)$. Take one of its cosets. Then any two matrices in such a set have difference with rank m, but the set is not F_q-linear. Such codes are not of much use to our discussion.

$N(\langle M_\alpha^T \rangle)$ has $m(q^m-1)$ elements [2]. Therefore $N(\langle M_\alpha^T \rangle) = GL_m(F_q)$ only for $q = m = 2$; for other values of q and m, it is a proper subset. From Lemma 4 in the Appendix, we know that inverses of all non-trivial linear combinations of $\mathcal{M}^{(1)}, \mathcal{M}^{(2)}, \cdots, \mathcal{M}^{(m)}$ are in this coset because for any non-trivial linear combination Y of these matrices satisfies $YM_\alpha Y^{-1} = M_\alpha^T$.

Classes of square FRD and TMRD codes and their interrelationship is shown in Figure 2. When $q = m = 2$, it follows from Theorem 3 that (3) depicts FRD codes and TMRD codes; for other values of q and m, the non-trivial intersection of regions (3) and (4) in Figure 2 follows from the results of Lemma 3. Since FRD codes and MRD codes are F_q-linear, the relation of regions (3) and (4) to region (2) is obvious.

4 Stacking Construction and FRD codes

In [7] Hammons and El Gamal obtain an F_2-subspace of $\mathbf{M}^{(2)}_{m\times n}$ in which all non-zero matrices have full rank, i.e., rank = $\min\{m,n\}$ by a method called *stacking construction* described

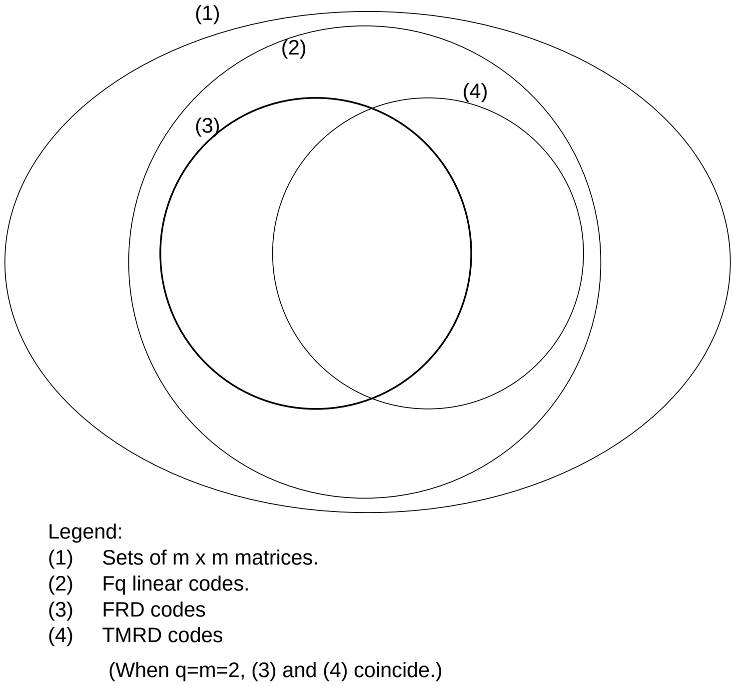

Figure 2: Square FRD and TMRD Codes.

below: Let $T_1, T_2, \cdots, T_m$ be linear vector-space transformations from F_2^k to F_2^n, and let $\mathcal{C}$ be the following set of $m \times n$ matrices.

$$\mathcal{C} = \left\{ \begin{bmatrix} T_1(\mathbf{x}) \\ T_2(\mathbf{x}) \\ \vdots \\ T_m(\mathbf{x}) \end{bmatrix} : \mathbf{x} \in F_2^k \right\}. \tag{7}$$

In [9, 10], stacking construction has been studied in detail for the case of two transmit antennas.
The following result characterizes sets of linear transformations that give full-rank codes with stacking construction.

Proposition 2 ([7, Theorem 12]) *Let $T_1, T_2, \cdots, T_m$ be linear vector space transformations from F_2^k to F_2^n, and let $\mathcal{C}$ be the $m \times n$ (two-dimensional) linear code of dimension k over F_2 consisting of the codeword matrices*

$$C(\mathbf{x}) = \begin{bmatrix} T_1(\mathbf{x}) \\ T_2(\mathbf{x}) \\ \vdots \\ T_m(\mathbf{x}) \end{bmatrix}$$

where $\mathbf{x}$ *denotes an arbitrary* k*-tuple of information bits and* $n \geq m$*. Then* $\mathcal{C}$ *is of rank* m *if and only if* $T_1, T_2, \cdots, T_m$ *have the property that* $\forall a_1, a_2, \cdots, a_m \in F_2$, $T = a_1 T_1 + a_2 T_2 + \cdots + a_m T_m$ *is nonsingular unless* $a_1 = a_2 = \cdots = a_m = 0$*.*

4.1 Square FRD codes from Stacking Construction

All non-zero matrices in $\mathcal{C}$ given by equation (7) has rank m if and only if all non-trivial linear combinations of $T_1, T_2, \cdots, T_m$ are non-singular, *i.e.*, injective transformations from F_q^k to F_q^n (*Cf.* Proposition 2). Linear transformations from F_q^k to F_q^n are not injective if $k > n$. Therefore it is necessary to have $k \leq n$ for stacking construction to give full rank matrices. Since there are q^k vectors in F_q^k, the size of a code so constructed is $q^k \leq q^n$, with equality if and only if $k = n$. Moreover, from Proposition 2, we see that for stacking construction to work, all non-trivial linear combinations of $T_1, T_2, \cdots, T_m$ have to be of rank k. Look at these linear transformations as $k \times n$ matrices over F_q. At any given row, no two of these matrices can be identical; if it were so, the difference, which too is an F_q-linear combination of $T_1, T_2, \cdots, T_m$, would have an all-zero vector at that row, and rank less than k. There are q^m F_q-linear combinations of $T_1, T_2, \cdots, T_m$. Thus $m \leq n$.

In view of the above, we investigate below $[m, 1]$ FRD codes over F_{2^m} obtainable via stacking construction for the cases $k = n = m$; the first equality is necessary to obtain codes with the largest size of size 2^m and the second for square matrices.

Theorem 7 *Let* $x^m - f_{m-1}x^{m-1} - \cdots - f_1 x - f_0$ *be any primitive polynomial of degree* m *over* F_q*. The* $m \times m$ *code obtained via stacking construction using* $m \times m$ *binary matrices* $M_i, i = 1, 2, \cdots, m$ *is FRD if and only if* $f_0 M_m M_1^{-1} = (M_1 + f_1 M_m) M_2^{-1} = (M_2 + f_2 M_m) M_3^{-1} = \cdots = (M_{m-1} + f_{m-1} M_m) M_m^{-1}$*. In particular, when* $m = 2$*, all such codes are FRD codes. For* $m > 2$*, there exist* $m \times m$ *FRD codes that cannot be obtained via stacking construction and* vice versa. $\square$

Proof: Let $M_1, M_2, \cdots, M_m$ be the matrix representation of the linear operators $T_1, T_2, \cdots, T_m$ on F_2^m. Stacking construction gives the following code:

$$\left\{ \begin{bmatrix} \mathbf{x}M_1 \\ \mathbf{x}M_2 \\ \cdots \\ \mathbf{x}M_m \end{bmatrix} : \mathbf{x} \in F_2^m \right\}.$$

Suppose that this is an FRD code. Take any arbitrary $\mathbf{x} \in F_2^m$. Then there exists $\mathbf{y} \in F_2^m$ such that

$$\begin{bmatrix} \mathbf{y}M_1 \\ \mathbf{y}M_2 \\ \cdots \\ \mathbf{y}M_m \end{bmatrix} = M_\alpha \begin{bmatrix} \mathbf{x}M_1 \\ \mathbf{x}M_2 \\ \cdots \\ \mathbf{x}M_m \end{bmatrix},$$

from which we obtain,

$$\begin{array}{rcl} \mathbf{x}f_0M_mM_1^{-1} & = & \mathbf{x}(M_1+f_1M_m)M_2^{-1} \\ & = & \mathbf{x}(M_2+f_2M_m)M_3^{-1} \\ & & \vdots \\ & = & \mathbf{x}(M_{m-1}+f_{m-1}M_m)M_m^{-1}. \end{array} \tag{8}$$

for all $\mathbf{x} \in F_2^m$. This is possible if and only if $f_0M_mM_1^{-1} = (M_1+f_1M_m)M_2^{-1} = (M_2 + f_2M_m)M_3^{-1} = \cdots = (M_{m-1}+f_{m-1}M_m)M_m^{-1}$. We analyze two cases.

Case I: $m = 2$. $f_0M_2M_1^{-1} = (M_1+f_1M_2)M_2^{-1}$. The only irreducible polynomial over F_2 with degree 2 is x^2+x+1; therefore $f_0 = f_1 = 1$ and $M_2M_1^{-1} = M_1M_2^{-1} + I$. This gives $(M_1M_2^{-1})^2 + M_1M_2^{-1} + I = 0$. Therefore the minimal polynomial of $M_1M_2^{-1}$ divides X^2+X+1. Since this polynomial is irreducible, it is the minimal polynomial. Since the characteristic polynomial of $M_1M_2^{-1}$ has degree 2, it is the characteristic polynomial. It follows that the 2×2 code obtained via stacking construction using M_1 and M_2 is FRD if and only if the characteristic polynomial of $M_1M_2^{-1}$ is X^2+X+1. On the other hand, by Theorem 1 of [9], if the stacking construction with M_1 and M_2 is to work, $M_1M_2^{-1}$ should have the characteristic polynomial X^2+X+1. Therefore all 2×2 codes over F_2 that can be constructed via stacking construction are FRD codes.

Case II: $m > 2$. We note that the choice $M_i = M_\alpha^{i-1}, i = 1,2,\cdots,m$ does not satisfy Equation 8. Therefore the code obtained via stacking construction using this choice of M_i is not an FRD code. $\square$

Figure 3 shows these results as a Venn diagram. Notice that the codes represented by the region marked (4) but not in the region (3) can be full rank codes but they are not linear over F_{2^m} (they can be F_2-linear).

5 Discussion

We gave the properties of generator matrices of linear codes that determine the rank weights of different codewords. Generator matrices of full rank distance codes have been characterized and a construction of FRD codes was given. We presented a method to construct a class of codes with a specified rank distance that are not FRD. We later used the properties of Singer cycles to study the relation of FRD codes to MRD codes. We studied the relation of FRD codes to codes obtained via stacking construction.

Possible directions for further research are:

- Neither in [7] nor in our discussion, is the coding advantage [6] of the code dealt with. While it is the minimum rank that chiefly contributes to reducing the probability of the transmitted matrix being erroneously decoded into another matrix, for codes of same minimum rank, the coding advantage is of importance.

- Whether TMRD codes can be constructed via stacking is unknown. More importantly, it is not known if FRD codes, TMRD codes, and those obtained via stacking construction exhaust optimal STBC for BPSK transmission.

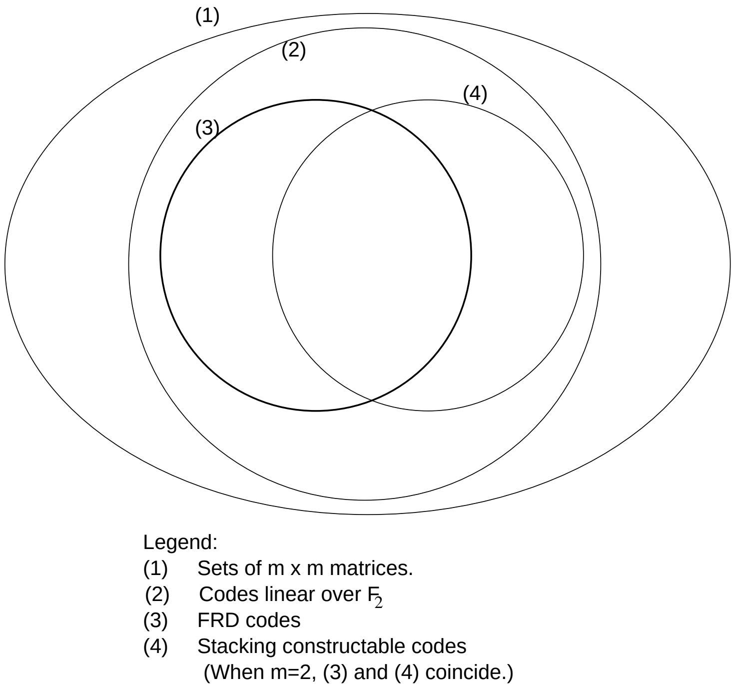

Figure 3: Square FRD and Stacking Construction Codes over F_2.

- STBCs which do not have full rank may outdo full rank STBCs if there is a large number of matrices in such a code. It is not known which rank weight distribution reduces the probability of error.
- FRD codes are F_{q^m}-linear. Such a structure may simplify decoding of an STBC obtained from an FRD code.

Appendix
Singer Cycles

We present basic definitions and properties of Singer cycles [2]. The set of invertible F_q-linear operators on F_q^m form a group under composition of operators, denoted by $GL_m(F_q)$. It is a non-Abelian group. We call a subgroup $H \subset GL_m(F_q)$ *irreducible* if H does not fix any subspace of F_q^m. Irreducible cyclic subgroups of order $q^m - 1$ are called Singer cycles.

The normalizer of a Singer cycle in $GL_m(F_q)$ has order $m(q^m - 1)$. The centralizer of a Singer cycle is the Singer cycle itself. Singer cycles in $GL_m(F_q)$ fall into one conjugacy class. (For $H \subset G$ groups, the conjugacy class of H in G is the set $\{g^{-1}Hg : g \in G\}$ of subgroups of G.) Therefore there are

$$\frac{1}{m}\left[(q^m - q)(q^m - q^2)\cdots(q^m - q^{m-1})\right]$$

Singer cycles in $GL_m(F_q)$.

Let $f = X^m - f_{m-1}X^{m-1} - \cdots - f_1 X - f_0 \in F[X]$ be a primitive irreducible polynomial with a root $\alpha \in F_{q^m}$. Then the companion matrix of f given by equation 3 has order $q^m - 1$ in $GL_m(F_q)$. Since f is the characteristic polynomial of M_α, it has no eigenvalues in F, and does not fix any subspace of F_q^m. Therefore the subgroup $\langle M_\alpha \rangle \subset GL_m(F_q)$ is a Singer cycle.

By Cayley-Hamilton Theorem, any $m \times m$ matrix over F_q is algebraic over F_q. Since the characteristic polynomial of M_α is irreducible, the polynomial ring $F_q[M_\alpha]$ is a field. Therefore $M_\alpha^j, j = 0, \cdots, m-1$ are F_q-linear independent.

There is only one Singer cycle in $GL_2(F_2)$. It is the set

$$\left\{ \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}$$

This cycle has index 2 in $GL_2(F_2)$, so it is normal in $GL_2(F_2)$.

A listing of Singer cycles and their normalizers for several values of m and q is available in [3].

Proof of Lemma 2

Suppose that $M_\alpha^T \in \langle M_\alpha \rangle$. Then $M_\alpha = M_\alpha^k = \sum_{i=0}^{m-1} a_i M_\alpha^i$ for some $a_i \in F_q, 0 \le i \le m-1$. Look at the first columns of the matrices $M_\alpha^i, 0 \le i \le m-1$ and M_α^T. For $0 \le i \le m-1$, the first column of M_α^i contains 1 at the $i+1$th row and 0 elsewhere. The first column of M_α^T contains f_0 in the last row, and 0 elsewhere. Therefore, $M_\alpha = \sum_{i=0}^{m-1} a_i M_\alpha^i \Rightarrow a_0 = a_1 = \cdots = a_{m-2} = 0$ and $a_{m-1} = f_0$. Hence, $M_\alpha^T \in \langle M_\alpha \rangle \Rightarrow M_\alpha^T = f_0 M_\alpha^{m-1}$.

Now let $m = 2$. Then

$$M_\alpha^T = f_0 M_\alpha^{m-1} \Rightarrow \begin{bmatrix} 0 & 1 \\ f_0 & f_1 \end{bmatrix} = f_0 \begin{bmatrix} 0 & f_0 \\ 1 & f_1 \end{bmatrix} \Rightarrow f_0 = 1$$

which implies that $f(x) = x^2 - f_1 x - 1$ for some $f_1 \in F_q$. Conversely, if $f(x) = x^2 - f_1 x - 1$ for some $f_1 \in F_q$, $M_\alpha^T = M_\alpha \in \langle M_\alpha \rangle$.

Now let $m > 2$. Then

$$\begin{aligned} M_\alpha^{m-1} &= (f_0)^{-1} M_\alpha^T \\ &= \begin{bmatrix} 0 & 1/f_0 & 0 & \cdots & 0 \\ 0 & 0 & 1/f_0 & \cdots & 0 \\ & & \vdots & & \\ 0 & 0 & 0 & \cdots & 1/f_0 \\ 1 & f_1/f_0 & f_2/f_0 & \cdots & f_{m-1}/f_0 \end{bmatrix}. \end{aligned}$$

For $1 \le i \le m-1$, the ith column of M_α contains 1 at $(i+1)$th row and 0 elsewhere. Hence the ith column of M_α^j is the $(i+1)$th column of M_α^{j-1}. Therefore the second column of M_α^{m-1} is the mth column of M_α, which gives the co-efficients of $f(x)$. Thus

$$\begin{aligned} f(x) &= x^m - f_{m-1}x^{m-1} - \cdots - f_1 x + f_0 \\ &= x^m - f_1/f_0 x^{m-1} - 1/f_0 \end{aligned}$$

from which we find that $f_0 = 1/f_0$ and that $f_1 = f_2 = \cdots = 0$. Therefore f_0 is a square-root of unity in F_q, and $f(x) = x^m - f_0$.

For a field F_q to have a square-root of unity different from 1, q must be odd. For odd q, F_q has one square-root of unity different from 1, and, since α is a primitive element of F_{q^m}, this must be $\alpha^{(q^m-1)/2}$. However,

$$f(x) = x^m - \alpha^{(q^m-1)/2}$$

cannot be the minimal polynomial of α, because α is not a root of $x^m - \alpha^{(q^m-1)/2}$ for any q and any $m > 2$. This contradicts the assumption. $\square$

Proof of Lemma 3

Let $A_1, A_2 \in \mathcal{A}$. Then

$$A_2 A_1^{-1} \langle M_\alpha \rangle A_1 A_2^{-1} = A_2 \langle M_\alpha^T \rangle A_2^{-1} = \langle M_\alpha \rangle$$

Therefore $A_2 A_1^{-1} \in N(\langle M_\alpha^T \rangle)$. Thus $\mathcal{A}$ is a right coset of $N(\langle M_\alpha^T \rangle)$. Now suppose that $\mathcal{A} = N(\langle M_\alpha^T \rangle)$, which is a group. Then for every $A \in \mathcal{A}$, $A^{-1} \in \mathcal{A}$. Therefore $\langle M_\alpha \rangle = A \langle M_\alpha^T \rangle A^{-1} = \langle M_\alpha^T \rangle$ if and only if $M_\alpha^T \in \langle M_\alpha \rangle$. For $m = 2$, this is true if and only if $f(X) = X^2 - f_1 X - 1$ for some $f_1 \in F_q$. If $m > 2$, $M_\alpha^T \notin \langle M_\alpha \rangle$, by Lemma 2. $\square$

Lemma 4 *The twisted companion coset $\mathcal{M}$ is a left coset of $\langle M_\alpha \rangle$ and hence every element of it is invertible.*

Proof: First we show that for all $A \in \mathcal{M}, A M_\alpha A^{-1} = M_\alpha^T$. Matrices $\mathcal{M}^{(t)}, t = 1, \cdots, m$ and their F_q-linear combinations are of the form

$$\begin{bmatrix} \mathbf{b} \\ \mathbf{b} M_\alpha \\ \vdots \\ \mathbf{b} M_\alpha^{m-1} \end{bmatrix}$$

for some $\mathbf{b} \in F_q^m$. (To be precise, for $t = 1, \cdots, m$, $\mathcal{M}^{(t)}$ corresponds to the choice of the tth vector in the standard basis of F_q^m for $\mathbf{b}$.) The characteristic polynomial of M_α is $f(x)$, so by Cayley-Hamilton Theorem,

$$M_\alpha^m = \sum_{r=0}^{m-1} f_r M_\alpha^r. \tag{9}$$

Now,

$$M_\alpha^T A = \begin{bmatrix} \mathbf{b}M_\alpha \\ \mathbf{b}M_\alpha^2 \\ \vdots \\ \mathbf{b}\sum_{r=0}^{m-1} f_r M_\alpha^r \end{bmatrix} = \begin{bmatrix} \mathbf{b}M_\alpha \\ \mathbf{b}M_\alpha^2 \\ \vdots \\ \mathbf{b}M_\alpha^m \end{bmatrix} = AM_\alpha,$$

which follows from Equation 9. Let $A_1, A_2 \in \mathcal{M}$. Then $A_1^{-1}A_2M_\alpha A_2^{-1}A_1 = M_\alpha, \Rightarrow A_1^{-1}A_2 \in \langle M_\alpha\rangle, \Rightarrow \mathcal{M}$ is a left-coset of $\langle M_\alpha\rangle$. $\square$

References

[1] R. Lidl and H. Niederreiter, Finite Fields, Encyclopaedia of Mathematics and its Applications, volume 20, Cambridge University Press, 1987.

[2] M. W. Short, The Primitive Soluble Permutation Groups of Degree less than 256, Lecture Notes in Mathematics, 1519, Springer Verlag, 1992.

[3] A. A. Zain, An Algebraic Approach to MDS and Dual Group Codes over Finite Abelian Groups, Indian Institute of Technology, Delhi, 1996.

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

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] Andrew M. Guidi and Alex J. Grant and Steven S. Pietrobon, "Full Diversity PSK Space-Time Codes, Proceedings of IEEE International Symposium on Information Theory, p.150, Washington, DC, USA, June 2001.

[10] Andrew M. Guidi and Alex J. Grant and Steven S. Pietrobon, "Algebraic Constructions for PSK Space-Time Coded Modulation," S. Boztas and I. E. Shparlinski (Eds), AAECC–14, Lecture Notes in Computer Science, 2227, pp.387–396, 2001.

[11] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error Correcting Codes, North-Holland, Amsterdam, 1981.

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

[13] 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.

[14] 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.