Full Rank Distance Codes and Optimal STBC for BPSK Modulation

K. N. Manoj and B. Sundar Rajan¹

Dept. of Electrical Communication Engineering,
Indian Institute of Science, Bangalore,
Karnataka, India. PIN: 560 012.

kummini@ieee.org, bsrajan@ece.iisc.ernet.in

Abstract — Viewing the codewords of an $[n, k]$ linear code over a field F_{q^m} as $m \times n$ matrices over F_q by expanding each entry of the codeword with respect to an F_q -basis of F_{q^m} , 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 non-zero codewords. For $m \geq n - k + 1$, codes with maximum possible rank distance, called Maximum Rank Distance (MRD) codes have been studied previously. In this paper, 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.

I. INTRODUCTION

Let F_q denote the Galois field with q elements and m and n be positive integers. Let $\mathcal{M}_{m \times n}^{(q)}$ denote the set of all $m \times n$ matrices over F_q . For any matrix M , we denote the rank of M over F_q by $r_q(M)$.

Let $f(x) = x^m - f_{m-1}x^{m-1} - \dots - f_1x - f_0$ be a primitive polynomial over F_q . Let $\alpha \in F_{q^m}$ be a root of $f(x)$. The set $\{1, \alpha, \alpha^2, \dots, \alpha^{m-1}\}$ forms a polynomial basis for F_{q^m} seen as a vector space over F_q [1]. Therefore every element in F_{q^m} can be seen as a polynomial in α over F_q . The map

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

is defined as follows: 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 i th column and j th row being the coefficient of α^j in the polynomial expansion of v_i . Φ is an F_q -space isomorphism.

Let $\mathcal{C}$ be an n -length code over F_{q^m} i.e. $\mathcal{C} \subset F_{q^m}^n$. For any pair of codewords $\mathbf{c}, \mathbf{c}' \in \mathcal{C}$, the rank distance between them is defined to be $r_q(\Phi(\mathbf{c} - \mathbf{c}'))$ [2]. The rank $d_{R, \min}$ of $\mathcal{C}$ is given by:

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

Since the rank distance between two codewords $\mathbf{c}, \mathbf{c}' \in \mathcal{C}$ is at most the Hamming distance between them, we have,

$$d_{R, \min} \leq \min\{m, n - \log_{q^m} |\mathcal{C}| + 1\}$$

Codes with $n < m$ and $d_{R, \min} = n - \log_{q^m} |\mathcal{C}| + 1$ has been studied in [2, 3, 4] and are called MRD (Maximum Rank Distance) codes. We consider codes with $d_{R, \min} = m$ and call them Full Rank Distance (FRD) codes.

Note 1. For any n -length FRD code over F_{q^m} , $m \leq n$.

¹This work was partly supported by IISc-DRDO programme on Advanced Research in Mathematical Engineering through a research grant to B. S. Rajan.

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

Definition 1. An n -length FRD code $\mathcal{C}$ over F_{q^m} is called a Maximal Full Rank Distance (MFRD) code if $|\mathcal{C}| = q^n$.

II. CHARACTERIZATION OF FRD CODES

Theorem II.1. Let $\mathcal{C}$ be an $[n, k]$ linear code over F_{q^m} and G be its generator matrix. Using the map $\Phi: F_{q^m}^n \longrightarrow \mathcal{M}_{m \times n}^{(q)}$, each of them can be expanded to matrices in $\mathcal{M}_{m \times n}^{(q)}$ giving a total of km row vectors in F_q^n . Then $\mathcal{C}$ is FRD if and only if the km vectors obtained as above are F_q -linear independent.

Theorem II.2. An n -length MFRD code over F_{q^m} exists iff m divides n .

III. SPACE-TIME BLOCK CODES FROM FRD CODES

A space-time block code (STBC) $\mathcal{C}$, for a channel with m transmit antennas and a quasi-static interval of n is a finite set of $m \times n$ matrices with entries from a signal set $S \subset \mathbb{C}$ [5]. With perfect CSI, the diversity of $\mathcal{C}$ is directly proportional to the minimum of ranks of pairwise differences of matrices in $\mathcal{C}$ over the complex field $\mathbb{C}$ [5]. Optimal STBC for BPSK modulation has been constructed as follows: let $\mathcal{C}$ be an nm -length linear code over F_2 . Let σ be a parser that maps vectors in $\mathcal{C}$ to $m \times n$ matrices over F_2 . Let $\mathcal{C}$ be the $m \times n$ STBC obtained by mapping matrices in $\sigma(\mathcal{C})$ using the map $0 \mapsto +1, 1 \mapsto -1$. $\mathcal{C}$ achieves full spatial diversity m if and only if every nonzero matrix in $\mathcal{C}$ is a matrix of full rank over F_2 [6]. FRD codes can be used to get STBCs that achieve full diversity.

FRD codes can be also used to obtain FRD codes based on Gaussian number fields [7].

REFERENCES

- [1] R. Lidl and H. Niederreiter: *Finite Fields*, Cambridge University Press.
- [2] E. M. Gabidulin, "Theory of Codes with Maximum Rank Distance," *Probl. Pered. Inform.*, vol. 21, pp. 3–16, Jan.–Mar. 1998.
- [3] R. M. Roth: "Maximum-rank Array Codes and Their Application to Crisscross Error Correction," *IEEE Trans. Inform. Theory*, vol. 37, pp. 328–336, Mar. 1991.
- [4] E. M. Gabidulin, Martin Bossert and P. Lusina "Space-Time Codes Based on Rank Codes," *Proc. IEEE International Symposium on Information Theory*, Sorrento, Italy, 25–30 June 2000, p. 284.
- [5] V. Tarokh, N. Seshadri and A. R. Calderbank: "Space-Time Codes for High Data Rate Wireless Communication: Performance Criterion and Code Construction," *IEEE Trans. Inform. Theory*, vol. 44, pp. 744–765, Mar. 1998.
- [6] A. Roger Hammons, Jr., and Hesham El Gamal: "On the Theory of Space-Time Codes for PSK Modulation," *IEEE Trans. Inform. Theory*, vol. 46, pp. 524–542, Mar. 2000.
- [7] Martin Bossert, E. Gabidulin, and P. Lusina, "Space-Time Codes Based on Gaussian Integers," *Private communication*, 2002.