The defect in rank-metric codes

ISMAEL GUTIÉRREZ GARCÍA

Departamento de Matemáticas y Estadística

Universidad del Norte, Barranquilla, Colombia

Email: isgutier@uninorte.edu.co

ABSTRACT. Let $\mathbb{F}_q$ be the finite field containing q elements and $\mathbb{F}_{q^m}$ be a field extension of $\mathbb{F}_q$ of degree m, with $m \geq 1$. We denote with $\mathbb{F}_q^n$ the n-dimensional row vector space over $\mathbb{F}_q$. Similarly with $\mathbb{F}_{q^m}^n$ we denote the n-dimensional row vector space over $\mathbb{F}_{q^m}$. Let $B = (v_1, \ldots, v_m)$ be a basis of $\mathbb{F}_{q^m}$, seen as an m-dimensional vector space over the field $\mathbb{F}_q$. Let now be $x = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$, then for any $j \in \{1, \ldots, n\}$ there exist coefficients $x_{ij} \in \mathbb{F}_q$ such that, $x_j = \sum_{i=1}^m x_{ij} v_i$. If we write each x_j as an m-dimensional column vector with respect to the basis B, then the vector x is associated with the matrix

$$X = \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & & \vdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{pmatrix}.$$

We denote with $\lambda : \mathbb{F}_{q^m}^n \longrightarrow \mathrm{M}_{m\times n}(\mathbb{F}_q)$ the map that sends x to $\lambda(x) = X$. As proved in [3] the distance function d_R on $\mathbb{F}_{q^m}^n$ defined by

$$d_R(x, y) := \mathrm{rank}(\lambda(x) - \lambda(y)) = \mathrm{rank}(X - Y)$$

is a metric over $\mathbb{F}_{q^m}^n$. It is called the *rank-metric*. Let C be a subset of $\mathbb{F}_{q^m}^n$. Then the minimum rank distance of C is defined as

$$d_R(C) := \text{mín}\{d_R(x, y) \mid x, y \in C,\ x \neq y\}.$$

A code C endowed with the metric d_R is called a *rank-metric code*. A linear $[n, k]$-code C over $\mathbb{F}_{q^m}$ is a k-dimensional subspace of $\mathbb{F}_{q^m}^n$. Let C be a linear $[n, k]$-code C over $\mathbb{F}_{q^m}$ with the Hamming distance $d_H(C)$. Then corresponds to C a rank-metric code $\lambda(C)$ with the rank-distance $d_R(\lambda(C))$. In [3] was established the relation between both distances. There was proved that $d_R(\lambda(C)) \leq d_H(C)$. Due to the Singleton bound we have

$$d_R(\lambda(C)) \leq d_H(C) \leq n - k + 1. \tag{1}$$

A linear $[n, k]$-code C that achieve this bound is called a *maximum-rank-distance codes* (briefly MRD-code). MRD-codes exists for all $m, n, k \in \mathbb{N}$ independent of the size of the field $\mathbb{F}_q$, see [1] and [4].

A linear $[n, k, d]$-code C over the finite field $\mathbb{F}_q$ is called a maximum distance separable code, if the minimum distance d meets the Singleton bound, that is $d = n - k + 1$. Unfortunately, the parameters of an MDS code are severely limited by the size q of the field. Then it is important to look for codes which have minimum distance close to the Singleton bound. The measure of how far C is away from being MDS, that is, the separation of the Singleton bound is called the *defect* of C. This concept was introduced by A. and W. Willems Faldum in [2].

Let C be a $[n, k]$-code over $\mathbb{F}_{q^m}$ with minimum rank distance d. We define the defect of C, denoted by $s(C)$ as follows

$$s(C) := n - k + 1 - d.$$

In classical coding theory, the existence of linear MDS-codes for given n and k depend on q since by Griesmar bound $d = n - k + 1 \leq (s + 1)q = q$, where s is the defect of the code and in this case is equal to 0.

As main result we prove the following lemma.

Theorem 1. *Let C be a $[n, k]$-code over $\mathbb{F}_{q^m}$ with minimum rank distance d. Then*

(a) *If $k \geq 2$, then $d \leq q^m(s + 1)$.*

(b) *If $k \geq 3$ and $d = q^m(s + 1)$, then $s + 1 \leq q^m$*

Keywords. Finite fields, linear code, rank-matrix code, defect of a code.

References

[1] P. Delsarte. Bilinear forms over a finite field, with applications to coding theory. J. Comb. Theory. Ser. A, vol. 25, pp. 226?241, 1978.

[2] A Faldum and W. Willems, *Codes of small defect. Design*, Codes and Cryptography 10,341-350 (1997).

[3] E. M. Gabidulin. Theory of codes with maximum rank distance. Probl. Inf. Transm., vol. 21, no. 1, pp. 1-12, 1985.

[4] R. M. Roth. Maximum-rank array codes and their application to criss-cross error correction. IEEE Trans. Inf. Theory, vol. 37, no. 2, pp. 328?336, Mar. 1991.