Finite Fields and Their Applications 50 (2018) 293–303

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Some new non-additive maximum rank distance codes

Kamil Otal *, Ferruh Özbudak

Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, 06800, Ankara, Turkey

ARTICLE INFO

Article history:
Received 21 January 2017
Received in revised form 29 November 2017
Accepted 4 December 2017
Available online xxxx
Communicated by W. Cary Huffman

MSC:
11T71
11H71
94B27

Keywords:
Rank metric codes
Maximum rank distance (MRD) codes
Additive generalized twisted Gabidulin codes
Linearized polynomials

ABSTRACT

In this paper, a construction of maximum rank distance (MRD) codes as a generalization of generalized Gabidulin codes is given. The family of the resulting codes is not covered properly by additive generalized twisted Gabidulin codes, and does not cover all twisted Gabidulin codes. When the basis field has more than two elements, this family includes also non-affine MRD codes, and such codes exist for all parameters. Therefore, these codes are the first non-additive MRD codes for most of the parameters.

* Corresponding author.
E-mail addresses: kamil.otal@gmail.com (K. Otal), ozbudak@metu.edu.tr (F. Özbudak).

https://doi.org/10.1016/j.ffa.2017.12.003

1. Introduction

Most of the maximum rank distance (MRD) codes in the literature are additively closed [3,5,8–15]. As non-additive, up to our knowledge, there is only one construction [2] and its generalization [4] working for some certain parameters. In this paper, we provide a construction of a family of non-additive MRD codes existing for all parameters. Therefore, these codes (that we call *partition codes*) are the first non-additive MRD codes for most of the parameters.

1.1. Rank metric codes

Let $\mathbb{F}_q$ be a finite field of q elements and $\mathbb{F}_q^{m\times n}$ be the set of $m \times n$ matrices over $\mathbb{F}_q$. The d function on $\mathbb{F}_q^{m\times n} \times \mathbb{F}_q^{m\times n}$ given by

$$d(A,B) := \mathrm{rank}(A-B)$$

satisfies the usual axioms of a metric, and is called the *rank distance* on $\mathbb{F}_q^{m\times n}$. A subset $\mathcal{C}$ of $\mathbb{F}_q^{m\times n}$, including at least two elements, with the rank distance is called a *rank metric code*. The *minimum distance* $d(\mathcal{C})$ of a code $\mathcal{C}$ is naturally defined by $d(\mathcal{C}) := \min\{d(A,B) : A,B \in \mathcal{C} \text{ and } A \neq B\}$. A bijective map $\mathbb{F}_q^{m\times n} \to \mathbb{F}_q^{m\times n}$ is called *isometry* if it preserves the rank distance. In [1], using result [18, Theorem 3.4], an equivalence notion on rank metric codes considering isometry is given as follows. Two rank metric codes $\mathcal{C}, \mathcal{C}' \subseteq \mathbb{F}_q^{m\times n}$ are called *equivalent* if there exist $X \in \mathrm{GL}(m,\mathbb{F}_q)$, $Y \in \mathrm{GL}(n,\mathbb{F}_q)$ and $Z \in \mathbb{F}_q^{m\times n}$ such that

$$\begin{aligned} &\mathcal{C}' = X\mathcal{C}^\sigma Y + Z := \{XC^\sigma Y + Z : C \in \mathcal{C}\} \text{ when } m \neq n, \\ &\mathcal{C}' = X\mathcal{C}^\sigma Y + Z \text{ or } \mathcal{C}' = X(\mathcal{C}^t)^\sigma Y + Z := \{X(C^t)^\sigma Y + Z : C \in \mathcal{C}\} \text{ when } m = n, \end{aligned} \tag{1}$$

for some automorphism σ of $\mathbb{F}_q$ acting on the entries of $C \in \mathcal{C}$, where the superscript t denotes the matrix transposition. If both $\mathcal{C}$ and $\mathcal{C}'$ are closed under addition, then Z must be the zero matrix. Similarly, if both $\mathcal{C}$ and $\mathcal{C}'$ are linear over $\mathbb{F}_q$, then σ can be taken as the identity, without loss of generality.

Rank metric codes have a **Singleton-like bound** given in the following proposition.

Proposition 1.1. *[3] Assume $m \geq n$ (without loss of generality). Let $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ be a rank metric code with minimum rank distance d. Then $|\mathcal{C}| \leq q^{m(n-d+1)}$.*

A rank metric code is called *maximum rank distance (MRD) code* if it meets the Singleton-like bound.