Finite Fields and Their Applications 54 (2018) 216–229

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On deep holes of Gabidulin codes

Weijun Fang[a], Li-Ping Wang[b,c,*], Daqing Wan[d]

[a] *Chern Institute of Mathematics and LPMC, Nankai University, Tianjin 300071, China*
[b] *Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China*
[c] *University of Chinese Academy of Sciences, Beijing, China*
[d] *Department of Mathematics, University of California, Irvine, CA 92697, USA*

ARTICLE INFO

Article history:
Received 14 February 2018
Received in revised form 20 June 2018
Accepted 16 August 2018
Available online xxxx
Communicated by Chaoping Xing

MSC:
94B05
94B35
94B60
94B75

Keywords:
Gabidulin codes
Rank metric
Deep holes
Covering radius

ABSTRACT

In this paper, we study deep holes of Gabidulin codes in both rank and Hamming metrics. Specifically, first, we give a tight lower bound for the distance of any word to a Gabidulin code and a sufficient and necessary condition for achieving this lower bound as well. Then, a class of deep holes of a Gabidulin code are discovered. Furthermore, we obtain some other deep holes for certain Gabidulin codes.

☆ The work of L.-P. Wang was supported in part by the National Natural Science Foundation of China (Grant No. 61872355) and National Cryptography Development Fund (MMJJ 20170124). The work of W. Fang was supported in part by the 973 Program of China (Grant No. 2013CB834204), the National Natural Science Foundation of China (Grant No. 61571243), and the Fundamental Research Funds for the Central Universities of China.

[*] Corresponding author.

E-mail addresses: nankaifwj@163.com (W. Fang), wangliping@iie.ac.cn (L.-P. Wang), dwan@math.uci.edu (D. Wan).

https://doi.org/10.1016/j.ffa.2018.08.008
1071-5797/© 2018 Elsevier Inc. All rights reserved.

1. Introduction

Let $\mathbb{F}_{q^m}^n$ be an n-dimensional vector space over a finite field $\mathbb{F}_{q^m}$ where q is a prime power, and n, m are positive integers. In this paper we only consider the case when $n \leq m$. Let $\beta = (\beta_1, \ldots, \beta_m)$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Let $\mathcal{F}_i$ be the map from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ where $\mathcal{F}_i(u)$ is the i-th coordinate of an element $u \in \mathbb{F}_{q^m}$ in the basis representation with β. To any $\mathbf{u} = (u_1, \ldots, u_n)$ in $\mathbb{F}_{q^m}^n$, we may associate the matrix $\bar{\mathbf{u}} = (\bar{u}_{i,j})_{1 \leq i \leq m, 1 \leq j \leq n} \in \mathcal{M}_{m,n}(\mathbb{F}_q)$ in which $\bar{u}_{i,j} = \mathcal{F}_i(u_j)$. The rank weight of the vector $\mathbf{u}$ can be defined by the rank of the associated matrix $\bar{\mathbf{u}}$, denoted by $w_R(\mathbf{u})$. Thus, we can define the rank distance between two vectors $\mathbf{u}$ and $\mathbf{v}$ in $\mathbb{F}_{q^m}^n$ as $d_R(\mathbf{u}, \mathbf{v}) = w_R(\mathbf{u} - \mathbf{v})$. We refer to [18] for more details on codes for the rank distance.

For integers $1 \leq k \leq n$, a linear rank-metric code C of length n and dimension k over $\mathbb{F}_{q^m}$ is a subspace of dimension k of $\mathbb{F}_{q^m}^n$ embedded with the rank metric. The minimum rank distance of the code C, denoted by $d_R(C)$, is the minimum rank weight of the non-zero codewords in C. A linear rank-metric code C of length n and dimension k over $\mathbb{F}_{q^m}$ is called a maximum rank distance (MRD) code if $d_R(C) = n - k + 1$. A $k \times n$ matrix is called a generator matrix of C if its rows span the code.

The rank distance of any word $\mathbf{u} \in \mathbb{F}_{q^m}^n$ to C is defined as

$$d_R(\mathbf{u}, C) = \min\{d_R(\mathbf{u}, \mathbf{c}) \mid \mathbf{c} \in C\}.$$

It plays an important role in decoding of rank-metric codes. The maximum rank distance

$$\rho_R(C) = \max\{d_R(\mathbf{u}, C) \mid \mathbf{u} \in \mathbb{F}_{q^m}^n\}$$

is called the covering radius of C. If the rank distance from a word to the code C achieves the covering radius of the code, the word is called a deep hole of the code C.

The covering radius and deep holes of a linear code embedded with Hamming metric were studied extensively [1–5,10,12,14,16,22–27], in which MDS codes such as generalized Reed–Solomon codes, standard Reed–Solomon codes and projective Reed–Solomon codes were explored deeply. Gabidulin codes were introduced by Gabidulin in [7] and independently by Delsarte in [6]. Gabidulin codes can be seen as the q-analog of Reed–Solomon codes. Furthermore, Gabidulin codes are MRD codes. Over the last decade there has been increased interest in Gabidulin codes, mainly because of their relevance to network coding [15,19]. The covering radius for a Gabidulin code was also studied in [8,9,20]. However, little is known about deep holes for such a code. In this paper, we give a tight lower bound for the distance of any word to a Gabidulin code in both rank and Hamming metrics, and a sufficient and necessary condition for attaining this lower bound as well. Then, a class of deep holes of a Gabidulin code are discovered. Furthermore, we study the distance of a special class of words to a Gabidulin code and so obtain some other deep holes for certain Gabidulin codes. Note that we refer to rank metric if Hamming metric is not explicitly pointed out in this paper.