Finite Fields and Their Applications 54 (2018) 273–287

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On the list decodability of self-orthogonal rank-metric codes

Shu Liu [a,b]

[a] *National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu 611731, China*
[b] *Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637371, Republic of Singapore*

ARTICLE INFO

Article history:
Received 22 January 2018
Received in revised form 31 May 2018
Accepted 16 August 2018
Available online xxxx
Communicated by Chaoping Xing

MSC:
11T71
68P30
94BXX

Keywords:
List decoding
Self-orthogonal rank metric codes

ABSTRACT

Guruswami and Resch proved that a random $\mathbb{F}_q$-linear rank-metric code is list decodable with list decoding radius attaining the Gilbert–Varshamov bound [8]. Furthermore, in Hamming metric, random linear self-orthogonal codes can be list decoded up to the Gilbert–Varshamov bound with polynomial list size [11]. Motivated by these two results and the potential applications of self-orthogonal rank-metric codes in network coding and cryptography [20], [18] and [5], we focus on investigating their list decodability. In this paper, we prove that with high probability, a random $\mathbb{F}_q$-linear self-orthogonal rank-metric code over $\mathbb{F}_q^{n\times m}$ can be list decoded up to the Gilbert–Varshamov bound with polynomial list size. In addition, we show that an $\mathbb{F}_{q^m}$-linear self-orthogonal rank-metric code of rate up to the Gilbert–Varshamov bound with exponential list size.

E-mail addresses: shuliu@uestc.edu.cn, SLIU017@ntu.edu.sg.

https://doi.org/10.1016/j.ffa.2018.08.007
1071-5797/

1. Introduction

Rank-metric codes have received many attentions because of their applications in network coding [20], [12], storage systems [19], cryptography [5], [18] and space–time coding [15]. A rank-metric code is a collection of matrices over a finite field and the distance between two codewords is defined as the rank of their difference. In 1951, Loo-Keng Hua [10] introduced rank-metric as "arithmetic distance" and then this metric was considered in coding theory by Delsarte [1]. In 1985, Gabidulin gave a construction of a class of rank-metric codes which achieves the Singleton bound, called Gabidulin codes [4].

A fundamental challenge in coding theory is to efficiently decode the original transmitted message even when a few symbols of the received word are erroneous. To surpass the limit of unique decoding radius, we consider list decoding. In the late 50's, Elias [3] and Wozencraft [23] introduced the concept of list decoding. Compared with unique decoding, list decoding can output a list of codewords which contains the correct transmitted codeword rather than outputting a unique codeword. The information rate, list decoding radius and list size are important parameters in list decoding. Since the information rate and list decoding radius are to represent the efficiency of a code and its error correcting ability, respectively, we want those two parameters to be large. On the other hand, list size is to represent the output size of the decoder and a very large list size is undesirable [7, p. 22, section 1.3, paragraph 3].

Finding good list decodable rank-metric codes attracts more and more researchers. Wachter-Zeh [21] proved that it is impossible to list decode square Gabidulin codes beyond half of the minimum rank distance for some instances of parameters. Moreover, no polynomial-time list decoding algorithms have been found to decode Gabidulin codes beyond half of the minimum rank distance. Furthermore, there exists a rank-metric code whose list size is exponential when the decoding radius is larger than half of the minimum rank distance [22]. Mahdavifar and Vardy [16] showed that one can efficiently list decode folded Gabidulin code up to the Singleton bound. However, the output list size of their algorithm is exponential in the length of the code. Ding [2] revealed that the Singleton bound is the list decoding barrier for any rank-metric code. With high probability, the decoding radius and the rate of random rank-metric codes satisfy the Singleton bound with constant list size. In addition, the Gilbert–Varshamov bound is the list decoding barrier of $\mathbb{F}_q$-linear rank metric codes. Guruswami and Xing [9] gave an explicit construction of subcodes of some Gabidulin codes, which can be list decoded up to the Singleton bound. Based on these results, S. Liu, C. Xing and C. Yuan showed that with high probability, a random subcode of a Gabidulin code can be list decoded with decoding radius far beyond the unique decoding radius in [14]. However, for random $\mathbb{F}_q$-linear rank-metric codes, when the list decoding radius is beyond half of the minimum distance, the list size becomes exponential. Recently, Guruswami and Resch decreased the list size of random $\mathbb{F}_q$-linear rank-metric codes. In [8], the list decodability of random $\mathbb{F}_q$-linear rank-metric codes can attain the Gilbert–Varshamov bound with polynomial