# List Decoding of Rank-Metric Codes with Row-To-Column Ratio Bigger Than $\frac{1}{2}$

**Shu Liu**
The National Key Laboratory on Wireless Communications,
University of Electronic Science and Technology of China, Chengdu, China

**Chaoping Xing**
School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, China

**Chen Yuan**
School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, China

## Abstract

Despite numerous results about the list decoding of Hamming-metric codes, development of list decoding on rank-metric codes is not as rapid as its counterpart. The bound of list decoding obeys the Gilbert-Varshamov bound in both the metrics. In the case of the Hamming-metric, the Gilbert-Varshamov bound is a trade-off among rate, decoding radius and alphabet size, while in the case of the rank-metric, the Gilbert-Varshamov bound is a trade-off among rate, decoding radius and column-to-row ratio (i.e., the ratio between the numbers of columns and rows). Hence, alphabet size and column-to-row ratio play a similar role for list decodability in each metric. In the case of the Hamming-metric, it is more challenging to list decode codes over smaller alphabets. In contrast, in the case of the rank-metric, it is more difficult to list decode codes with large column-to-row ratio. In particular, it is extremely difficult to list decode square matrix rank-metric codes (i.e., the column-to-row ratio is equal to 1).

The main purpose of this paper is to explicitly construct a class of rank-metric codes $\mathcal{C}$ of rate $R$ with the column-to-row ratio up to $2/3$ and efficiently list decode these codes with decoding radius beyond the decoding radius $(1-R)/2$ (note that $(1-R)/2$ is at least half of relative minimum distance $\delta$). In literature, the largest column-to-row ratio of rank-metric codes that can be efficiently list decoded beyond half of minimum distance is $1/2$. Thus, it is greatly desired to efficiently design list decoding algorithms for rank-metric codes with the column-to-row ratio bigger than $1/2$ or even close to 1. Our key idea is to compress an element of the field $\mathbb{F}_{q^n}$ into a smaller $\mathbb{F}_q$-subspace via a linearized polynomial. Thus, the column-to-row ratio gets increased at the price of reducing the code rate. Our result shows that the compression technique is powerful and it has not been employed in the topic of list decoding of both the Hamming and rank metrics. Apart from the above algebraic technique, we follow some standard techniques to prune down the list. The algebraic idea enables us to pin down the message into a structured subspace of dimension linear in the number $n$ of columns. This "periodic" structure allows us to pre-encode the message to prune down the list.

**2012 ACM Subject Classification** Mathematics of computing → Coding theory

**Keywords and phrases** Coding theory, List-decoding, Rank-metric codes

**Digital Object Identifier** 10.4230/LIPIcs.ICALP.2023.89

**Category** Track A: Algorithms, Complexity and Games

**Funding** *Shu Liu*: Research supported in part by the National Key R&D Program of China under Grant 2022YFA1004900, in part by the National Natural Science Foundation of China under Grant 12271084, in part by the National Key Laboratory of Science and Technology on Communications under Contract G02214307.

*Chaoping Xing*: Research supported in part by the National Key Research and Development Projects under Grant 2021YFE0109900 and in part by the National Natural Science Foundation of China under Grant 12031011.

*Chen Yuan*: Research supported in part by the Natural Science Foundation of China under Grant 12101403.

50th International Colloquium on Automata, Languages, and Programming (ICALP 2023).
Editors: Kousha Etessami, Uriel Feige, and Gabriele Puppis; Article No. 89; pp. 89:1–89:14
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

# 1 Introduction

Rank-metric codes were first introduced by Delsarte in [1] and have found various applications [14, 16]. A rank-metric code $\mathcal{C}$ of rate $R$ and relative minimum distance $\delta$ must obey the Singleton bound $1-R \geqslant \delta$ (see Subsection 2.1). The equality $1-R=\delta$ holds if the code $\mathcal{C}$ is maximum rank distance (MRD for short). As for every alphabet size $q$ and ratio $\rho$, one can always construct an MRD code. Therefore, we view decoding radius $(1-R)/2$ as the half of minimum distance decoding radius or unique decoding radius.

The unique decoding algorithms for rank-metric codes have been extensively studied [3, 14]. However, the list decoding algorithm of the rank-metric codes are not understood very well. Despite of many results about the list decoding of Hamming-metric codes in literature, very few were known about the list decoding of rank-metric codes. In particular, for the column-to-row ratio bigger than $\frac{1}{2}$, there are no known explicit constructions of rank-metric codes that can be list decoded beyond half the minimum distance decoding radius. On the other hand, with high probability, a square random rank-metric code of rate $R$ can be list decoded up to its decoding radius $1-\sqrt{R}$ (see [2]). Note that $1-\sqrt{R}$ is always bigger than $(1-R)/2$. This means that with high probability, a random square rank-metric code can be list decoded beyond the half of minimum distance decoding radius.

In the the Hamming-metric case, it is more challenging to list decode codes over small alphabets. As we will see in the next subsection, in contrast, it becomes more difficult to list decode codes with large column-to-row ratio (i.e., the ratio between the numbers of rows and columns). In particular, it is extremely difficult to list decoding of square matrix rank-metric codes (i.e., the column-to-row ratio is equal to 1). Therefore, it is a great challenge to design efficient algorithms to list decode rank-metric codes with the column-to-row ratio close to 1 and decoding radius beyond $(1-R)/2$.

## 1.1 Known results

Let us fix some notations before stating known results. Denote by $\mathbb{F}_q^{t\times n}$ the collection of $t\times n$ matrices over $\mathbb{F}_q$. We may assume that $n\leqslant t$. Otherwise, we can consider transpose of matrices. One can define the rank-metric within $\mathbb{F}_q^{t\times n}$ (see the detailed definition in Subsection 2.1). A subset $\mathcal{C}$ of $\mathbb{F}_q^{t\times n}$ equipped with rank-metric is called a rank-metric code. Unlike Hamming-metric codes, apart from rate and minimum distance there is an important parameter $\rho(\mathcal{C}) := \frac{n}{t}$ which is called the column-to-row ratio.

▶ **Definition 1.** Let $\tau\in(0,1)$ and $L\geqslant 1$ be an integer. A rank-metric code $\mathcal{C}$ is $(\tau, L)$-list decodable if for every $X\in\mathbb{F}_q^{t\times n}$

$$|\mathcal{B}_R(X,\tau n)\cap\mathcal{C}|\leq L,$$

where $\mathcal{B}_R(X,\tau n)$ is a rank-metric ball defined in Subsection 2.1.

Limit to list decodability of rank-metric codes and list decodability of random rank-metric codes are known [2, 15]. More precisely, we have the following result (see [2]):

**(i)** If the ratio $n/t$ tends to a fixed real $\rho$, a rank-metric code $\mathcal{C}\subseteq\mathbb{F}_q^{t\times n}$ of rate $R$ that is $(\tau, L)$-list decodable with $L=\text{poly}(n)$ must obey the Gilbert-Varshamov bound, i.e., $R\leqslant(1-\tau)(1-\rho\tau)$.

**(ii)** With high probability a random rank-metric code can be list decoded up to the Gilbert-Varshamov bound, i.e., a random rank-metric code of rate $R$ in $\mathbb{F}_q^{t\times n}$ is $(\tau, O(1/\varepsilon))$-list decodable with $R=(1-\tau)(1-\rho\tau)-\varepsilon$ for any small real $\varepsilon>0$. In particular, if the ratio $n/t$ is a small constant $\varepsilon$, then with high probability a random rank-metric code of rate $R$ in $\mathbb{F}_q^{t\times n}$ is $(1-R-\varepsilon, O(1/\varepsilon))$-list decodable.

Let us introduce the state-of-art results by comparing list decoding of Hamming-metric and rank-metric codes. First of all, we note that both Hamming-metric and rank-metric codes obey the Gilbert-Varshamov bounds in each metric for list decoddability. In the case of the Hamming-metric, the Gilbert-Varshamov bound is a trade-off among rate, decoding radius and alphabet size, while in the case of the rank-metric, the Gilbert-Varshamov bound is a trade-off among rate, decoding radius and column-to-row ratio. Hence, alphabet size and column-to-row ratio play the similar role for list decodability in each metric. We will see from the following paragraph that the small column-to-row ratio for list decoding of rank-metric codes is compatible with large alphabet size for list decoding of Hamming-metric codes and vice versa.

Recall that in the case of the Hamming-metric, the limit on list decodability is the Hamming-metric Gilbert-Varshamov bound $1-H_q(\tau)$, where $H_q(x)$ is the entropy function, and a random code can be list decoded up to the Hamming-metric Gilbert-Varshamov bound [5]. When alphabet size $q=\exp(\Omega(\frac{1}{\varepsilon}))$, the Hamming-metric Gilbert-Varshamov bound $1-H_q(\tau)$ tends to the Singleton bound $1-R-\varepsilon$. Currently, for list decoding of Hamming-metric codes over large alphabet $q$, the best result is that, for $q=O(\frac{1}{\varepsilon^2})$, by making use of folded algebraic geometry codes or algebraic geometry codes with evaluation points in subfields (for convenience let us call them subfield algebraic geometry codes) one can list decode Hamming-metric codes up to the Singleton bound $1-R-\varepsilon$ (see [10, 11, 12]). Thus, for list-decoding of Hamming-metric codes over large alphabet $q$, it remains an open problem to design efficient algorithm to list decode up to $1-R-\varepsilon$ for $q$-ary codes with $q=\Omega(\frac{1}{\varepsilon})$. On the other hand, for sufficiently small column-to-row ratio, say $\rho=O(\varepsilon)$, the rank-metric Gilbert-Varshamov also tends the Singleton bound $1-R-\varepsilon$. Furthermore, when the column-to-row ratio $\rho=O(\varepsilon^2)$, an efficient list decoding of rank-metric codes up to the Singleton bound $1-R-\varepsilon$ was introduced in [11, 12] by making use of subfield Gabidulin codes. Hence again, it remains an open problem to design efficient algorithm to list decode rank-metric codes up to $1-R-\varepsilon$ for with column-to-row ratio $\rho=\Omega(\varepsilon)$.

For the regime of small alphabets $q$ such as $q=2$, there is not much work on efficient list decoding algorithms for Hamming-metric codes except for the concatenation techniques. Precisely speaking, by making use of concatenation technique, one can list decode binary Hamming-metric codes up to the Blokh-Zyablov bound [7]. Similarly, in the case of rank-metric codes, not much work has been done for large column-to-row ratio, in particular, for ratio $\rho=1$, i.e., the square matrix case. The largest column-to-row ratio $\rho$ is $\frac{1}{2}$ for which the list decoding bound lies beyond the unique decoding radius. In [17], by making use of folded Gabidulin codes, one can list decode beyond the unique decoding radius $(1-R)/2$ with the column-to-row ratio $\rho$ arbitrarily close to $1/2$.

## 1.2 Our result

We propose a compression technique which is the key to construct list decodable rank-metric codes with the ratio $\rho$ up to $\frac{2}{3}$. This moves one step further towards the ratio $\rho=1$. Our list decodable rank-metric codes are obtained by compressing folded Gabidulin codes. The following theorem summarizes our main result.

▶ **Main Theorem 1.** *For every constant finite field $\mathbb{F}_q$, any small real $\varepsilon>0$ and integer $s>1$, there exists an explicit constriction of $\mathbb{F}_q$-linear rank metric codes with the ratio $\rho$ and rate $R$ that are $\left(\frac{1-sR}{\rho(s+1)}-\varepsilon, q^{O((s-1)^2/\varepsilon)}\right)$-list-decodable. The algorithm runs in time* *poly*$(n,q)$. *Furthermore, if* $\rho < \frac{2(1-R)}{(s+1)(1-sR)}$*, then the decoding radius* $\tau = \frac{1-sR}{\rho(s+1)} - \varepsilon$ *exceeds the unique decoding radius* $\frac{1-R}{2}$.

▶ Remark 2. If we take $s = 2$, then we get rank-metric codes of the ratio $\rho$ and rate $R$ that are $\left(\frac{1-2R}{3\rho} - \varepsilon, q^{O(1/\varepsilon)}\right)$-list decodable. In particular, if $\rho < \frac{2(1-R)}{3(1-2R)}$, then the list decoding radius is bigger than $(1-R)/2$. Furthermore, when the rate $R$ tends to 0, there exists an explicit construction of rank-metric codes with any ratio $\rho < \frac{2}{3}$. Note that our decoding radius depends on the ratio $\rho$, while the unique decoding radius is independent of the ratio $\rho$. Let us draw a diagram to illustrate our main result.

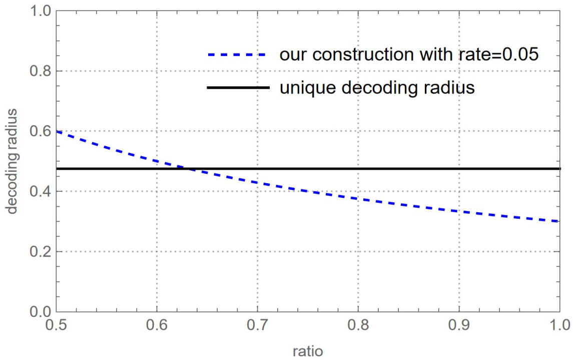

**Figure 1** Comparison of our decoding radius with the unique decoding radius for different ratios.

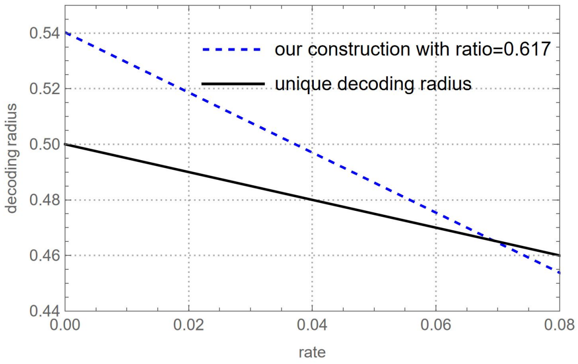

**Figure 2** Comparison of our decoding radius with the unique decoding radius for different rates.

## 1.3 Our Techniques

In the topics of list decoding, folded codes and subfield codes are used to increase decoding radius. In the case of Hamming-metric, folding codes or taking evaluation points from a subfield increases code alphabet size, while in the case of rank-metric, folding codes or taking evaluation points from a subfield would reduce the column-to-row ratio. In the Subsection 1.1, we reviewed some techniques employed in the explicit constructions of list decodable rank-metric codes. We start from a family of list decodable rank-metric codes, i.e., folded Gabidulin codes. The list decoding algorithm for this family was already known

[11, 12, 17]. In this paper, we introduce a new technique, namely the compression technique. By combing our compression technique with the existing techniques of folded codes, we are able to increase the column-to-row ratio.

Let us illustrate our idea by combining the compression technique with the techniques of folded codes. The folded technique for list decoding of rank-metric codes was introduced in [17]. Similar to list decoding of folded Reed-Solomon codes, one can list decode folded Gabidulin codes. However, when Gabidulin codes are folded, the number of columns increases. This means that the column-to-row ratio decreases. In order to make the column-to-row ratio larger for folded Gabidulin codes, one can take a linear map that sends every element of $\mathbb{F}_{q^n}$ to a smaller $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}$. Thus, the number of columns shrinks. At the meantime, we still want a large list decoding radius or at least a list decoding radius exceeding $(1-R)/2$. We can choose the compression map to be a linearized polynomial and use the existing linear algebra list decoding technique [8, 10, 11, 12] to achieve our goal.

## 1.4 Organization of the paper

In Section 2, we introduce some preliminaries including definitions of rank-metric codes and rank-metric balls, Gabidulin codes, subspace design and periodic subspaces. In Section 3, we compress folded rank-metric code and design an efficient list decoding algorithm.

# 2 Preliminaries

## 2.1 Rank-metric codes

We first introduce some basic notations and properties about rank-metric codes. Denote by $\mathbb{F}_q^{t\times n}$ the collection of all $t\times n$ matrices over $\mathbb{F}_q$. Without loss of generality, we assume that $n\le t$ in this paper or otherwise we can consider transpose of matrices. A rank-metric code is a subset of $\mathbb{F}_q^{t\times n}$. Denote by $\rho$ the column-to-row ratio, i.e, $\rho=\frac{n}{t}$, then we always have $\rho\le 1$. For any $X,Y\in\mathbb{F}_q^{t\times n}$, the rank distance between $X$ and $Y$ is defined by

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

where rank denotes the rank of matrices. It is straightforward to verify that $d_R$ is indeed a distance. Similar to classical block codes, we can define minimum rank distance and rate for a rank-metric code $\mathcal{C}$ by

$$d_R(\mathcal{C})=\min_{X\neq Y\in\mathcal{C}}\{\mathrm{rank}(X-Y)\}\quad \textit{and}\quad R(\mathcal{C})=\frac{\log_q|\mathcal{C}|}{nt}.$$

A rank-metric code in $\mathbb{F}_q^{t\times n}$ with $n\leqslant t$ must obey the following Singleton bound

$$d_R(\mathcal{C})\leqslant n-R(\mathcal{C})n+1. \tag{1}$$

The rank-metric ball, an analog to the Hamming ball in classical block codes, is used to count the number of matrices within a given rank distance. The formal definition is given as follows.

▶ **Definition 3.** For a real $\tau\in[0,1]$, the rank-metric ball with center $X\in\mathbb{F}_q^{t\times n}$ and distance $\tau n$ is defined by

$$\mathcal{B}_R(X,\tau n):=\{Y\in\mathbb{F}_q^{t\times n}:\ d_R(X,Y)\le\tau n\}.$$

The size of a rank-metric ball is independent of the center.

For convenience, a vector of length $t$ over $\mathbb{F}_q$ is identified with a column vector of $\mathbb{F}_{q^t}$ under a fixed basis. Thus, a row vector in $\mathbb{F}_{q^t}^n$ can be viewed as an $t\times n$ matrix over $\mathbb{F}_q$. We denote by $d_R(\mathbf{x},\mathbf{y})$ the rank distance $d_R(X,Y)$, where $\mathbf{x},\mathbf{y}$ are vectors in $\mathbb{F}_{q^n}^t$ corresponding to $X,Y$, respectively.

## 2.2 Gabidulin codes

A code achieving the Singleton bound (1) is called Maximal Rank Distance (or MRD for short) code. The most famous MRD codes are Gabidulin codes which are defined by using polynomial evaluations.

To better understand our codes, we briefly review the construction of Gabidulin codes [4]. A polynomial of the form $f(x) = \sum_{i=0}^{\ell} a_i x^{q^i}$ is called $q$-linearized, where coefficients $a_i$ belong to the algebraic closure of $\mathbb{F}_q$. The $q$-degree of $f(x)$, denoted by $\deg_q(f)$, is defined to be $\ell$ if $a_\ell \neq 0$. Denote by $\mathcal{L}_q(n, k)$ the subset

$$\mathcal{L}_q(n,k) := \left\{ \sum_{i=0}^{k-1} a_i x^{q^i} \; : \; a_i \in \mathbb{F}_{q^n} \right\}. \tag{2}$$

Then $\mathcal{L}_q(n, k)$ is an $\mathbb{F}_{q^n}$-vector space of dimension $k$ and it is also an $\mathbb{F}_q$-vector space of dimension $kn$. Denote by $\mathcal{L}_q(n)$ the union $\cup_{k=1}^{\infty} \mathcal{L}_q(n, k)$, i.e., $\mathcal{L}_q(n)$ is the collection of $q$-linearized polynomials over $\mathbb{F}_{q^n}$.

Fix an $\mathbb{F}_q$-linearly independent set $\{\alpha_1, \ldots, \alpha_n\}$ of $\mathbb{F}_{q^t}$. For every $q$-linearized polynomial $f \in \mathbb{F}_{q^t}[X]$ of $q$-degree at most $k-1$ with $1 \leqslant k \leqslant n$, we can encode $f$ by the row vector $\big(f(\alpha_1), \ldots, f(\alpha_n)\big)$ over $\mathbb{F}_{q^t}$. By fixing a basis of $\mathbb{F}_{q^t}$ over $\mathbb{F}_q$, we can also think of this row vector as an $t \times n$ matrix over $\mathbb{F}_q$. This yields the Gabidulin code

$$\mathcal{G}_q(n,k) := \{\big(f(\alpha_1), \ldots, f(\alpha_n)\big) \in \mathbb{F}_q^{t \times n} \; : \; f \in \mathcal{L}_q(n,k)\}. \tag{3}$$

The Gabidulin code $\mathcal{G}_q(n, k)$ is an MRD code with rate $\frac{k}{n}$ and minimum rank distance $n - k + 1$.

## 2.3 Subspace design

Subspace design was introduced in [11] to reduce list size from a structured list. Let us recall the definition.

▶ **Definition 4.** A collection $\mathcal{S}$ of $\mathbb{F}_q$-subspaces $H_1, \ldots, H_M \subseteq \mathbb{F}_q^n$ is called an $(s, \ell, n)_q$-subspace design if for every $\mathbb{F}_q$-linear space $W \subset \mathbb{F}_q^n$ of dimension $s$, one has $\sum_{i=1}^{M} \dim_{\mathbb{F}_q}(H_i \cap W) \leq \ell$.

Random subspace designs are studied in [11]. Guruswami and Kopparty [6] gives an explicit subspace design based on Wronskian determinant.

▶ **Lemma 5.** *For $\varepsilon \in (0, 1)$, any prime power $q$ and positive integers $s, n$ with $s < \varepsilon n/4$, there is an explicit collection of $M = q^{\Omega(\varepsilon n/s)}$ subspaces in $\mathbb{F}_q^n$, each of codimension at most $\varepsilon n$ and form an $(s, 2s^2/\varepsilon, n)_q$-subspace design. Moreover, bases for $N \leqslant M$ elements of this collection can be computed in time* $\mathrm{poly}(N, n, q)$.

▶ Remark 6.

**(i)** If $q > n$, one can improve the intersection size from $2s^2/\varepsilon$ to $2s/\varepsilon$ by applying the subspace design based on the folded Reed-Solomon directly. For $q < n$, the approach in [6] first constructed a weak subspace design and then turn this weak subspace design to a subspace design given in Definition 4. Such transformation yields a $(s, 2s^2/\varepsilon, n)$-subspace design instead of $(s, 2s/\varepsilon, n)$-subspace design.

**(ii)** If $s = \Omega(\log_q n)$, then a construction of subspace designs with better parameters was given in [13]. For our applications, we are interested in the case where $s$ is a constant.

## 2.4 Periodic Subspaces

The periodic subspace was introduced in [10] to characterize the list of candidates outputted by the list decodable codes. By exploiting the structure of periodic subspace, they manage to cut down the list size to polynomial size at cost of losing arbitrary small rate.

For a vector $\mathbf{a} = (a_1, a_2, \ldots, a_N) \in \mathbb{F}_q^N$ and positive integers $t_1 \leqslant t_2 \leqslant m$, we denote by $\mathrm{proj}_{[t_1,t_2]}(\mathbf{a}) \in \mathbb{F}_q^{t_2-t_1+1}$ its projection onto coordinates $t_1$ through $t_2$, i.e., $\mathrm{proj}_{[t_1,t_2]}(\mathbf{a}) = (a_{t_1}, a_{t_1+1}, \ldots, a_{t_2})$. When $t_1 = 1$, we use $\mathrm{proj}_t(\mathbf{a})$ to denote $\mathrm{proj}_{[1,t]}(\mathbf{a})$. These notions are extended to subsets of strings in the obvious way: $\mathrm{proj}_{[t_1,t_2]}(S) = \{\mathrm{proj}_{[t_1,t_2]}(\mathbf{x}) : \mathbf{x} \in S\}$.

▶ **Definition 7.** For positive integers $s, b, n$, an affine subspace $H \subset \mathbb{F}_q^{nb}$ is $(s, n, b)_q$-periodic if there exists a subspace $W \subseteq \mathbb{F}_q^n$ of dimension at most $s$ such that for every $j = 1, 2, \ldots, b$, and every "prefix" $\mathbf{a} \in \mathbb{F}_q^{(j-1)n}$, the projected affine subspace of $\mathbb{F}_q^n$ defined as

$$\{\mathrm{proj}_{[(j-1)n+1,jn]}(\mathbf{x}) : \mathbf{x} \in H \text{ and } \mathrm{proj}_{(j-1)n}(\mathbf{x}) = \mathbf{a}\}$$

is contained in an affine subspace of $\mathbb{F}_q^n$ given by $W + \mathbf{v_a}$ for some vector $\mathbf{v_a} \in \mathbb{F}^n$ dependent on $\mathbf{a}$.

By combining subspace design and periodic affine spaces, we can pin down list of massages in Sections 3 and 4. The detailed result is shown below and was given in [11].

▶ **Lemma 8.** *Suppose $H_1, H_2, \ldots, H_b$ is an $(s, \ell, n)$-subspace design in $\mathbb{F}_q^n$, and $T$ is a $(s, n, b)$-periodic affine subspace of $\mathbb{F}_q^{nb}$. Then the set $\mathcal{T} = \{(\mathbf{f_1}, \mathbf{f_2}, \ldots, \mathbf{f_b}) \in T : \mathbf{f_j} \in H_j \text{ for } j = 1, 2, \ldots, b\}$ is an affine subspace of $\mathbb{F}_q^{nb}$ of dimension at most $\ell$.*

# 3 Compressing the folded Gabidulin codes

In this section, we introduce the compression technique and combine this technique with folded Gabidulin codes in order to increase the ratio of folded Gabidulin codes.

## 3.1 Encoding Algorithm

The encoding algorithm consists of two steps. The first step is to encode a linearized polynomial $f(x)$ to a codeword. In this step, we use $\alpha_1, \ldots, \alpha_n$ as the $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$ and evaluate $f(x)$ as $(f(\alpha_1), \ldots, f(\alpha_n))$. The second step is to choose a linearized polynomial $g(x)$ whose kernel is a $\sigma n$-dimensional subspace of $\mathbb{F}_{q^n}$ for some $\sigma \in (0, 1)$ when $g(x)$ is viewed as an $\mathbb{F}_q$-linear map from $\mathbb{F}_{q^n}$ to itself, then the vector

$$\Big(g(f)(\alpha_1), g(f)(\alpha_2), \ldots, g(f)(\alpha_n)\Big)$$

belongs to a smaller subspace $\mathrm{Im}(g)$, where $\mathrm{Im}(g)$ stands for the image of $g(x)$, i.e., $g(\mathbb{F}_{q^n})$. As $\mathbb{F}_{q^{(1-\sigma)n}} \cong \mathrm{Im}(g)$, the vector $(g(f)(\alpha_1), g(f)(\alpha_2), \ldots, g(f)(\alpha_n))$ can be viewed as a matrix in $\mathbb{F}_q^{(1-\sigma)n\times n}$.

The choice of $g(x)$ can be done as follows. Choose an $\mathbb{F}_q$-subspace $V \subseteq \mathbb{F}_{q^n}$ of dimension $\sigma n$ and define the linearized polynomial $g(x) = \prod_{v\in V}(x - v)$ over $\mathbb{F}_{q^n}$. It follows that $\dim_{\mathbb{F}_q}(\ker(g)) = \sigma n$ and $\dim_{\mathbb{F}_q}(\mathrm{Im}(g)) = (1 - \sigma)n$. For a $q$-linearized polynomial $a(x) = \sum_{i=0}^{\ell} a_i x^{q^i} \in \mathbb{F}_{q^n}[x]$ and $j \geqslant 0$, we denote by $a^{(j)}(x)$ the polynomial $\sum_{i=0}^{\ell} a_i^{q^j} x^{q^i}$, i.e., $a^{(j)}(x)$ is obtained from $a(x)$ by raising each coefficient to its $q^j$-th power.

Denote by $W_j$ the image space of $g^{(j)}(x)$. It is clear that $W_j$ is of dimension $(1 - \sigma)n$ as well. Therefore, one can define the $\mathbb{F}_q$-linear isomorphism $\phi_j : W_j \to \mathbb{F}_q^{(1-\sigma)n}$. Let $\mathcal{F}_k(g) := \{g(f(x)) \in \mathcal{L}_q(n) : \deg_q(f) < k\}$. The following lemma shows that if $k$ is not too large, the elements in $\mathcal{F}_k(g)$ are distinct.

▶ **Lemma 9.** *Let $f_1(x), f_2(x)$ be linearized polynomial of $q$-degree at most $k-1$. If $k+\sigma n \leqslant n$, then $g(f_1(x)) = g(f_2(x))$ if and only if $f_1(x) = f_2(x)$.*

**Proof.** Assume that $g(f_1(x)) = g(f_2(x))$. Suppose that $f_1(x) \neq f_2(x)$. Then as a linear of map from $\mathbb{F}_{q^n}$ to $\mathbb{F}_{q^n}$, the kernel of $f_1 - f_2$ has dimension at most $k-1$. Thus, the image of $f_1 - f_2$ has dimension at least $n-k+1$. Since $g(x)$ is a $q$-linearized polynomial, we have

$$g(f_1(x) - f_2(x)) = g(f_1(x)) - g(f_2(x)) = 0.$$

This means that $g(f_1(x) - f_2(x))$ send every element of $\mathbb{F}_{q^n}$ to 0. Hence, $g(x)$ maps every element in the the image of $f_1 - f_2$ to 0. This implies that the image of $f_1 - f_2$ is contained in the kernel of $g(x)$. On the other hand, the dimension of the kernel of $g(x)$ is at most the $q$-degree of $g(x)$ which is $\sigma n$. This gives that $\sigma n \geqslant n-k+1$, i.e., $k+\sigma n \geqslant n+1$. This contradiction shows that $f_1(x) = f_2(x)$.

The other direction is clear. The proof is completed. ◀

Given linearized polynomials $g(x)$ and $f(x)$, we denote by $g_f$ the linearized polynomial $g(f(x))$. It is easy to see that $g_f^{(i)}(x) = g^{(i)}\big(f^{(i)}(x)\big)$. We encode $g(f(x)) \in \mathcal{F}_k(g)$ to the codeword as follows:

$$M_s(g,f) := \begin{pmatrix} \phi_0\big(g_f(\alpha_1)\big) & \phi_0\big(g_f(\alpha_2)\big) & \cdots & \phi_0\big(g_f(\alpha_n)\big) \\ \phi_1\big(g_f^{(1)}(\alpha_1)\big) & \phi_1\big(g_f^{(1)}(\alpha_2)\big) & \cdots & \phi_1\big(g_f^{(1)}(\alpha_n)\big) \\ \vdots & \vdots & \ddots & \vdots \\ \phi_{s-1}\big(g_f^{(s-1)}(\alpha_1)\big) & \phi_{s-1}\big(g_f^{(s-1)}(\alpha_2)\big) & \cdots & \phi_{s-1}\big(g_f^{(s-1)}(\alpha_n)\big) \end{pmatrix} \in \mathbb{F}_q^{(1-\sigma)sn\times n},$$

where $\phi_j$ is a fixed $\mathbb{F}_q$-linear isomorphism from $W_j$ to $\mathbb{F}_q^{(1-\sigma)n}$. Therefore, $M_s(g,f)$ has $(1-\sigma)sn$ rows and $n$ columns. Each entry in the above matrix is viewed as a row vector of $\mathbb{F}_q^{(1-\sigma)n}$.

Fix a $q$-linearized polynomial $g(x) \in \mathcal{L}_q(n, \sigma n)$ with the kernel of dimension $\sigma n$, let $\mathcal{C}_q(n,k;s,\sigma)$ be the collection of $M_s(g,f)$ for all $f(x) \in \mathcal{L}_q(n,k)$ defined in (2).

▶ **Lemma 10.** *If $k+\sigma n \leqslant n$, then the ratio, distance and rate of $\mathcal{C}_q(n,k;s,\sigma)$ satisfy*

$$\rho = \frac{1}{(1-\sigma)s}, \quad d_R(\mathcal{C}_q(n,k;s,\sigma)) \geq n-k-\sigma n+1, \quad \text{and} \quad R(\mathcal{C}_q(n,k;s,\sigma)) = \frac{k}{s(1-\sigma)n},$$

*respectively.*

**Proof.** The ratio is clear. Given a nonzero linearized polynomial $f(x)$, suppose that $M_s(g,f)$ has rank less than $n-k-\sigma n+1$. The solution space $U$ of $M_s(g,f)x^T = 0$ has dimension at least $k+\sigma n$. Then, $g_f(x)$ has at least $q^{k+\sigma n}$ roots. This implies that $g_f$ is a linearized polynomial of $q$-degree at least $k+\sigma n$. However, the $q$-degree of $g_f$ is upper bounded by $k+\sigma n-1$ as the $q$-degree of $g$ is $\sigma n$ and the $q$-degree of $f$ is at most $k-1$. This is a contradiction. It is easy to see that the map $f \mapsto M_s(g,f)$ is $\mathbb{F}_q$-linear and injective, our rank-metric codes are $\mathbb{F}_q$-linear space and its size is $q^{kn}$. Hence, the rate of this code is $\frac{\log_q(\mathcal{C}_q(n,k,\sigma))}{s(1-\sigma)n^2} = \frac{k}{s(1-\sigma)n}$. ◀

## 3.2 List Decoding Algorithm

The list decoding algorithm consists of two subroutine algorithms. The first algorithm is an interpolation algorithm which outputs the interpolation polynomial that passes through all points in the vector space of the transmitted matrix. The second algorithm is a root-finding algorithm which finds out all roots to the interpolation algorithm that belong to the message space $\mathcal{L}_q(n,k)$. However, if our message space is the whole space of $\mathcal{L}_q(n,k)$, the output of this list decoding algorithm may be exponentially large. To reduce the list size, we make use of the subspace design [6] to "re-encode" our rank-metric codes. As far as we know, this technique was the only known method to construct the explicit list-decodable rank-metric codes [17, 9]. The resulting rank-metric code is a subcode of the original rank-metric code with $\varepsilon$ rate loss. The list size of our resulting rank-metric code is reduced to a constant $q^{O(\frac{1}{\varepsilon})}$.

Fix a positive integer $e \le n-s$. Suppose that a codeword $M_s(g,f)$ is transmitted and $M_y = (y_{i,j})_{0\le i\le s-1, 1\le j\le n}$ is received with at most $e$ errors, i.e., $\mathrm{rank}(M_s(g,f) - M_y) \le e$. Our goal is to recover the linearized polynomial $f(x)$ from $M_y$. Note that $\phi_j$ is an $\mathbb{F}_q$-isomorphism for $j = 0,\dots,s-1$. We define the matrix $M_z = (z_{i,j})_{0\le i\le s-1,1\le j\le n}$, where $z_{i,j} = \phi_i^{-1}(y_{i,j})$. That is, we apply the inverse maps $\phi_0^{-1},\dots,\phi_{s-1}^{-1}$ to $M_y$ to retrieve $sn \times n$ matrix $M_z$ over $\mathbb{F}_q$. Define the matrix

$$M_s'(g,f) := \begin{pmatrix} g_f(\alpha_1) & g_f(\alpha_2) & \cdots & g_f(\alpha_n) \\ g_f^{(1)}(\alpha_1) & g_f^{(1)}(\alpha_2) & \cdots & g_f^{(2)}(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ g_f^{(s-1)}(\alpha_1) & g_f^{(s-1)}(\alpha_2) & \cdots & g_f^{(s-1)}(\alpha_n) \end{pmatrix}$$

The following lemma shows that the error $\mathrm{rank}(M_s(g,f) - M_y)$ does not amplify under the inverse maps $\phi_0^{-1},\dots,\phi_{s-1}^{-1}$.

▶ **Lemma 11.** *If* $\mathrm{rank}(M_s(g,f) - M_y) \le e$*, then* $\mathrm{rank}(M_s'(g,f) - M_z) \le e$*.*

**Proof.** Since $\mathrm{rank}(M_s(g,f) - M_y) \le e$, the solution space $U \subseteq \mathbb{F}_q^n$ of $(M_s(g,f) - M_y)\mathbf{x}^T = \mathbf{0}$ has dimension at least $n-e$, i.e, for every $(c_1,c_2,\dots,c_n) \in U$ and $i = 0,1,\dots,s-1$,

$$\phi_i\left(g_f^{(i)}\left(\sum_{j=1}^n c_j\alpha_j\right)\right) = \sum_{j=1}^n c_j\phi_i\left(g_f^{(i)}(\alpha_j)\right) = \sum_{j=1}^n c_j y_{i,j}.$$

By taking $\phi_i^{-1}$ on the both sides of the above identity, we get

$$g_f^{(i)}\left(\sum_{j=1}^n c_j\alpha_j\right) = \sum_{j=1}^n \phi_i^{-1}(c_j y_{i,j}) = \sum_{j=1}^n c_j\phi_i^{-1}(y_{i,j}) = \sum_{j=1}^n c_j z_{i,j}.$$

Since it holds for every $(c_1,c_2,\dots,c_n) \in U$, we come to the conclusion that $\mathrm{rank}(M_s'(g,f) - M_z) \le e$. ◀

Assuming $\mathrm{rank}(M_s(g,f) - M_z) \le e$, we will show how to list decode $M_z$. To begin with, we introduce the interpolation polynomials.

▶ **Definition 12.** *Let $\mathcal{L}$ be the space of polynomials $Q \in \mathbb{F}_{q^n}[X, Z_1, Z_2, \dots, Z_s]$ of the form $Q(X, Z_1,\dots,Z_s) = A_0(X) + A_1(Z_1) + \cdots + A_s(Z_s)$ with each $A_0 \in \mathcal{L}_q(n, D+k+\sigma n)$ and $A_i \in \mathcal{L}_q(n,D)$ for $i = 1,\dots,s$.*

The interpolation polynomial $Q(X, Z_1,\dots,Z_s)$ was used to interpolate the points $(\alpha_j, z_{0,j},\dots,z_{s-1,j})$ for $j = 1,\dots,n$. Since our interpolation polynomial is $q$-linearized, it means $Q$ pass all points in the subspace spanned by $(\alpha_j, z_{0,j},\dots,z_{s-1,j})$.

▶ **Lemma 13.** *Assume that $D > \frac{1}{s+1}(n-k-\sigma n)$. There exists a nonzero polynomial $Q \in \mathcal{L}$ such that $Q(\alpha_i, z_{0,i}, \dots, z_{s-1,i}) = 0$ for $i = 1, \dots, n$. Furthermore, $Q$ can be found in time poly$(n, \log q)$.*

**Proof.** We view coefficients of $A_i(X)$ as variables. Since there are $n$ equations and $(s+1)D + k + \sigma n - 1$ unknowns in $Q(X, Z_1, \dots, Z_s)$, we require that $(s+1)D + k + \sigma n - 1 > n$ or equivalently $D > \frac{1}{s+1}(n - k + 1 - \sigma n)$. Note that the $n$ constraints amount to $n$ linear equations. This implies that we can interpolate polynomial $Q$ in running time $O(n^3)$ by Gauss elimination. Moreover, as long as the number of unknowns is bigger than the number of equations, there exists a nonzero polynomial $Q$ satisfying all these $n$ constraints. ◀

We next prove that those codewords with small distance from $M_z$ are the roots of $Q$. Then, it remains to design a root-finding algorithm to find all the roots of $Q$.

▶ **Lemma 14.** *Let $g_f \in \mathcal{F}_k(g)$ be a $q$-linearized polynomial. If $\mathrm{rank}(M'_s(g,f) - M_z) \le e$ and $D + k + \sigma n - 1 < n - e$, then $Q(x, g_f(x), g_f^{(1)}(x), \dots, g_f^{(s-1)}(x)) = 0$.*

**Proof.** The condition that $\mathrm{rank}(M'_s(g,f) - M_z) \le e$ implies that there exists an $\mathbb{F}_q$-linear subspace $U$ of dimension at least $n - e$ such that for every $(c_1, c_2, \dots, c_n) \in U$, we have $\sum_{j=1}^n c_j z_{i,j} = \sum_{j=1}^n c_j g_f^{(i)}(\alpha_j)$ for all $i = 0, 1, \dots, s-1$. This gives

$$\begin{aligned} 0 &= \sum_{j=1}^n c_j Q(\alpha_j, z_{0,j}, \dots, z_{s-1,j}) = Q\left(\sum_{j=1}^n c_j\alpha_j, \sum_{j=1}^n c_j z_{0,j}, \dots, \sum_{j=1}^n c_j z_{s-1,j}\right) \\ &= Q\left(\sum_{j=1}^n c_j\alpha_j, \sum_{j=1}^n c_j g_f(\alpha_j), \dots, \sum_{j=1}^n c_j g_f^{(s-1)}(\alpha_j)\right) \\ &= Q\left(\sum_{j=1}^n c_j\alpha_j, g_f\left(\sum_{j=1}^n c_j\alpha_j\right), \dots, g_f^{(s-1)}\left(\sum_{j=1}^n c_j\alpha_j\right)\right) \end{aligned}$$

Note that $g_f$ is a linearized polynomial of $q$-degree at most $k + \sigma n - 1$. Then, $Q(x, g_f(x), \dots, g_f^{(s-1)}x)$ is a $q$-linearized polynomial of $q$-degree at most $D + k + \sigma n - 1$ which is less than the dimension $n - e$ of the kernel. It must be the case that $Q(x, g_f(x), \dots, g_f^{(s-1)}(x)) = 0$. ◀

▶ **Theorem 15.** *If $e \le \frac{s}{s+1}((1-\sigma)n - k)$, then $Q(x, g_f(x), \dots, g_f^{(s-1)}x) = 0$ holds for all linearized polynomials $g_f(x)$ with rank$(M'_{g_f} - M_z) \le e$.*

**Proof.** Set $D = \left\lfloor \frac{1}{s+1}(n - k - \sigma n) + 1 \right\rfloor$. Then Lemma 14 ensures existence of a polynomial $Q(X, Z_1, \dots, Z_s)$ passing through points $(\alpha_i, z_{0,i}, \dots, z_{s-1,i})$ for $i = 1, \dots, n$. Furthermore, Lemma 13 ensures that all linearized polynomials $g_f(x)$ with $\mathrm{rank}(M'_s(g,f) - M_z) \le e$ is a solution to $Q(x, g_f(x), \dots, g_f^{(s-1)}x) = 0$. This completes the proof. ◀

Recall that the rate of $\mathcal{C}_q(n, k; s, \sigma)$ is $R := \frac{k}{s(1-\sigma)n}$. Plugging $k = sR(1-\sigma)n$ into the expression of $e \le \frac{s}{s+1}((1-\sigma)n - k)$, we obtain the list decoding radius $\tau = \frac{s}{s+1}(1-\sigma)(1-sR)$. As the ratio $\rho = \frac{1}{(1-\sigma)s}$, $\tau$ can be expressed as $\frac{1-sR}{\rho(s+1)}$ in terms of the ratio $\rho$. If we want that the list decoding radius $\tau$ exceeds the unique decoding, i.e., $\tau > \frac{1-R}{2}$, then the rate $R$ must satisfy $R < \frac{2-(s+1)\rho}{2s-(s+1)\rho}$. This implies that $\rho < \frac{2}{s+1}$.

If we set $s = 2$, then for any ratio $\rho \in (0, \frac{2}{3})$, we obtain a list decodable rank-metric code of the ratio $\rho$ that exceeds the unique decoding radius $\frac{1-R}{2}$. However, we still need to make sure that the list size of this code is at most polynomial in $q, n$ and there exists explicit list decoding algorithm to find all candidates. The following lemma tells us the structure of the solutions to $Q(x, g_f(x), g_f^{(1)}(x), \dots, g_f^{(s-1)}(x)) = 0$. We follow the idea given in [9] to show how to obtain the structure of $g(f(x))$ from $Q$ via the root-finding algorithm.

▶ **Lemma 16.** *Let* $a(x) = \sum_{i=0}^{\sigma n+k-1} a_i x^{q^i} \in \mathcal{L}_q(n)$. *Then the set of solutions* $(a_0, a_1, \dots, a_{\sigma n+k-1})$ *to the equation*

$$Q(x, a(x), a^{(1)}(x), \dots, a^{(s-1)}(x)) = 0 \tag{4}$$

*forms an* $(s-1, n, \sigma n + k - 1)$*-periodic subspace.*

**Proof.** Let $D = \left\lfloor \frac{1}{s+1}(n - k - \sigma n) + 1 \right\rfloor$. Note that we have already recovered $A_0(x), \dots, A_s(x)$ by interpolation that satisfy the indentity

$$Q(x, a(x), a^{(1)}(x), \dots, a^{(s-1)}(x)) = A_0(x) + A_1(a(x)) + \cdots + A_s(a^{(s-1)}(x)) = 0. \tag{5}$$

Assume that $A_0(X) = \sum_{i=0}^{D+k+\sigma n-1} b_{0,i} x^{q^i}$ and $A_j(x) = \sum_{i=0}^{D-1} b_{j,i} x^{q^i}$. If $b_{0,0}, \dots, b_{s,0}$ are all zero, then (5) gives a new identity $(A_0'(x) + A_1'(a(x)) + \cdots + A_s'(a^{(s-1)}(x)))^q = 0$, i.e.,

$$A_0'(x) + A_1'(a(x)) + \cdots + A_s'(a^{(s-1)}(x)) = 0 \tag{6}$$

with $\deg_q(A_i) \geqslant \deg_q(A_i')$ for all $i = 0, 1, \dots, s$. Moreover, not all $A_i'$ are zero polynomials. Thus, without loss of generality, we may assume that at least one of $b_{0,0}, \dots, b_{s,0}$ is nonzero.

Let $a(x) = \sum_{i=0}^{k+\sigma n-1} a_i x^{q^i}$, where $a_i \in \mathbb{F}_{q^n}$ are variables. Plugging the expression of $a(x)$ into (5) and compareing the coefficient of $x$ on both sides give

$$b_{0,0} + \sum_{i=0}^{s-1} b_{i+1,0} a_0^{q^i} = 0. \tag{7}$$

The solution $a_0$ to $b_{0,j} + \sum_{i=0}^{s} b_{i,j} a_0^{q^{i-1}} = 0$ is an affine subspace of dimension at most $s-1$. For $i = 0, \dots, k + \sigma n - 1$, define the linearized polynomial

$$B_i(x) = \sum_{j=1}^{s-1} b_{j,i} x^{q^j}.$$

Our assumption shows $B_0(x) \neq 0$. The solutions $\beta \in \mathbb{F}_{q^n}$ to $B_0(x)$ forms a subspace $W$ of dimension at most $s-1$. Fix $i \in \{0, \dots, k + \sigma - 1\}$. By comparing the coefficient of $x^{q^i}$ in Equation (5), we get

$$b_{0,i} + B_i(a_0^{q^i}) + B_{i-1}(a_1^{q^{i-1}}) + \cdots + B_1(a_{i-1}^q) + B_0(a_i) = 0.$$

This implies $a_i \in W + \theta_i$ for some $\theta_i \in \mathbb{F}_{q^n}$ that is determined by $a_0, \dots, a_i$. Thus, each choice of $a_{i-1}$ is contained in the coset of $W$. The proof is completed. ◀

▶ Remark 17. For each $a_i$, we may have $q^{s-1}$ solutions. Thus, the list of candidate $g_f(x)$ could be exponentially large. To cut down the list size, we pick a subspace of $\mathcal{L}_q(n, k)$ by subspace design. By imposing some constraints on our codeword, we can prune the list to a constant size. We leave it to the next subsection.

Assume that we are given a solution $a(x)$ to $Q(x, a(x), a^{(1)}(x), \dots, a^{(s-1)}(x))$. Next lemma shows how to obtain $f(x)$ from $a(x)$. Note that not all solutions to

$$Q(x, a(x), a^{(1)}(X), \dots, a^{(s-1)}(x)) = 0$$

are of the form $g(f(x))$.

▶ **Lemma 18.** *Given a linearized polynomial $a(x)$ of $q$-degree at most $k+\sigma n-1$, we can find in time $O(n^2)$ whether there exists an unique linearized polynomial $f(x)$ of $q$-degree at most $k-1$ such that $a(x)=g(f(x))$. Furthermore, $f(x)$ can be uniquely determined if it exists.*

**Proof.** Let $a(x)=\sum_{i=0}^{k+\sigma n-1} a_i x^{q^i}$, $f(x)=\sum_{i=0}^{k-1} f_i x^{q^i}$ and $g(x)=\sum_{i=0}^{\sigma n} g_i x^{q^i}$. Suppose that $a(x)=g(f(x))$. It follows that

$$a(x)=\sum_{i=0}^{\sigma n} g_i f(x)^{q^i}.$$

Comparing the coefficient of $x$ on both sides, we get $f_0 g_0 = a_0$. Recall that the roots of $g(x)$ form a $\sigma n$-dimensional subspace which implies $g(x)$ has $q^{\sigma n}$ different roots including 0. This implies $g_0$ is nonzero and thus $f_0$ is uniquely determined. Assume that $f_0,\dots,f_{i-1}$ are determined. We compare the coefficient of $x^{q^i}$ on both sides

$$a_i = g_0 f_i + g_1 f_{i-1} + g_2 f_{i-2} + \cdots + g_i f_0.$$

Thus, $f_i$ is uniquely determined. After all coefficients of $f(x)$ are determined, we check whether $a(x)=g(f(x))$. If the equation holds, $f(x)$ is the unique solution. Otherwise, there do not exist any solutions. It is easy to see that all operations run in time $O(n^2)$. ◀

## 3.3 Prune the list

We follow the standard list decoding procedure introduced in [10, 11, 12] to pre-encode and prune the list size.

▶ **Theorem 19.** *For every finite field $\mathbb{F}_q$, small real $\gamma>0$ and integer $s>1$, there exists an explicit constriction of $\mathbb{F}_q$-linear rank metric codes with the column-to-row ratio $\rho$ and rate $R$ that are $\left(\frac{(1-sR)}{\rho(s+1)}-\gamma, q^{O((s-1)^2/\gamma)}\right)$-list-decodable. The algorithm runs in time poly$(n,q)$. Furthermore, if $\rho<\frac{2}{s+1}$, then the decoding radius $\tau=\frac{(1-sR)}{\rho(s+1)}-\gamma$ exceeds the unique decoding radius $\frac{1-R}{2}$.*

**Proof.** Note that the message space of our rank metric code is $\mathcal{F}_k(g)=\{g(f): f\in\mathcal{L}_q(n,k)\}$. Lemma 5 says that there exists an explicit construction of $((s-1), 2(s-1)^2/\varepsilon, n)_q$-subspace design $H_0,\dots,H_{\sigma n+k-1}\subseteq\mathbb{F}_{q^n}$, each has the $\mathbb{F}_q$-dimension $n(1-\varepsilon)$. Define the polynomial set $\mathcal{S}=\{h(x)=\sum_{i=0}^{\sigma n+k-1} h_i x^{q^i} : h_i\in H_i\}$. Our new message space is $\mathcal{F}'_k(g)=\mathcal{F}_k(g)\cap\mathcal{S}$. Note that

$$\begin{aligned}\dim_{\mathbb{F}_q}(\mathcal{F}'_k(g)) &= \dim_{\mathbb{F}_q}(\mathcal{F}_k(g))+\dim_{\mathbb{F}_q}(\mathcal{S})-\dim_{\mathbb{F}_q}(\mathcal{F}_k(g)+\mathcal{S})\\ &\geqslant \dim_{\mathbb{F}_q}(\mathcal{F}_k(g))+\dim_{\mathbb{F}_q}(\mathcal{S})-\dim_{\mathbb{F}_q}(\mathbb{F}_{q^n}^{\sigma n+k})\\ &= kn+(\sigma n+k)(1-\varepsilon)n-(\sigma n+k)n = n(k-\varepsilon(\sigma n+k))\end{aligned}$$

Given a linearized polynomial $g(f(x))\in\mathcal{F}'_k(g)$, we encode it into the codeword $M_s(g,f)$. The new rank-metric code becomes $\mathcal{C}'(n,k;s,\sigma)$. The rate of this code is $R=\frac{n(k-\varepsilon(\sigma n+k))}{n^2 s(1-\sigma)}=\frac{1}{1-\sigma}\left(\frac{k}{n}-\frac{\varepsilon}{s}\left(\sigma+\frac{k}{n}\right)\right)\geqslant\frac{1}{1-\sigma}\left(\frac{k}{n}-\varepsilon\right)=R'-\frac{\varepsilon}{1-\sigma}$ where $R'$ is the rate of $\mathcal{C}(n,k;s,\sigma)$ in Lemma 10.

Since our new code is a subcode of the rank metric code proposed in the Subsection 3.1. The same encoding and list decoding algorithm can be applied to this code. Assume that there are at most $\tau n=\frac{(1-sR')n}{\rho(s+1)}$ rank errors, Lemma 16 says that all candidates $(a_0,\dots,a_{\sigma n+k-1})\in\mathcal{F}_k(g)$ are contained in an $(s-1,n,\sigma n+k)$-periodic subspace. This implies that the collection of such candidates $(a_0,\dots,a_{\sigma n+k-1})\in\mathcal{F}'_k(g)$ is contained in an affine space of dimension at most $(s-1)^2/\varepsilon$ followed by the property of subspace design Lemma 8. This implies there are at most $q^{(s-1)^2/\varepsilon}$ codewords in the list. Put $\gamma = \frac{2\varepsilon s}{\rho(1-\sigma)(s+1)}$, then $\tau = \frac{(1-sR')}{\rho(s+1)} = \frac{(1-sR)}{\rho(s+1)} - \gamma$.

It takes at most $O(n^3 q^{(s-1)^2/\gamma})$ time to find all candidates. Thus, this list decoding algorithm runs in polynomial time. Our proof is completed. ◀

## References

1 Philippe Delsarte. Bilinear forms over a finite field, with applications to coding theory. *J. Comb. Theory, Ser. A*, 25(3):226–241, 1978. doi:10.1016/0097-3165(78)90015-8.

2 Yang Ding. On list-decodability of random rank metric codes and subspace codes. *IEEE Trans. Inf. Theory*, 61(1):51–59, 2015. doi:10.1109/TIT.2014.2371915.

3 Michael A. Forbes and Amir Shpilka. On identity testing of tensors, low-rank recovery and compressed sensing. In Howard J. Karloff and Toniann Pitassi, editors, *Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012*, pages 163–172. ACM, 2012. doi:10.1145/2213977.2213995.

4 Ernst Gabidulin. Theory of codes with maximum rank distance (translation). *Problems of Information Transmission*, 21:1–12, January 1985.

5 Venkatesan Guruswami. *List decoding of error correcting codes.* PhD thesis, Massachusetts Institute of Technology, 2001. URL: http://dspace.mit.edu/handle/1721.1/8700.

6 Venkatesan Guruswami and Swastik Kopparty. Explicit subspace designs. In *54th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2013, 26-29 October, 2013, Berkeley, CA, USA*, pages 608–617. IEEE Computer Society, 2013. doi:10.1109/FOCS.2013.71.

7 Venkatesan Guruswami and Atri Rudra. Better binary list decodable codes via multilevel concatenation. *IEEE Trans. Inf. Theory*, 55(1):19–26, 2009. doi:10.1109/TIT.2008.2008124.

8 Venkatesan Guruswami and Carol Wang. Linear-algebraic list decoding for variants of reed-solomon codes. *IEEE Trans. Inf. Theory*, 59(6):3257–3268, 2013. doi:10.1109/TIT.2013.2246813.

9 Venkatesan Guruswami, Carol Wang, and Chaoping Xing. Explicit list-decodable rank-metric and subspace codes via subspace designs. *IEEE Trans. Inf. Theory*, 62(5):2707–2718, 2016. doi:10.1109/TIT.2016.2544347.

10 Venkatesan Guruswami and Chaoping Xing. Folded codes from function field towers and improved optimal rate list decoding. In Howard J. Karloff and Toniann Pitassi, editors, *Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012*, pages 339–350. ACM, 2012. doi:10.1145/2213977.2214009.

11 Venkatesan Guruswami and Chaoping Xing. List decoding reed-solomon, algebraic-geometric, and gabidulin subcodes up to the singleton bound. In Dan Boneh, Tim Roughgarden, and Joan Feigenbaum, editors, *Symposium on Theory of Computing Conference, STOC'13, Palo Alto, CA, USA, June 1-4, 2013*, pages 843–852. ACM, 2013. doi:10.1145/2488608.2488715.

12 Venkatesan Guruswami and Chaoping Xing. Optimal rate list decoding over bounded alphabets using algebraic-geometric codes. *J. ACM*, 69(2):10:1–10:48, 2022. doi:10.1145/3506668.

13 Venkatesan Guruswami, Chaoping Xing, and Chen Yuan. Subspace designs based on algebraic function fields. In Ioannis Chatzigiannakis, Piotr Indyk, Fabian Kuhn, and Anca Muscholl, editors, *44th International Colloquium on Automata, Languages, and Programming, ICALP 2017, July 10-14, 2017, Warsaw, Poland*, volume 80 of *LIPIcs*, pages 86:1–86:10. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2017. doi:10.4230/LIPIcs.ICALP.2017.86.

14 Ralf Koetter and Frank R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Trans. Inf. Theory*, 54(8):3579–3591, 2008. doi:10.1109/TIT.2008.926449.

15 Antonia Wachter-Zeh. Bounds on list decoding of rank-metric codes. *IEEE Trans. Inf. Theory*, 59(11):7268–7277, 2013. doi:10.1109/TIT.2013.2274653.

16 Huaxiong Wang, Chaoping Xing, and Reihaneh Safavi-Naini. Linear authentication codes: bounds and constructions. *IEEE Trans. Inf. Theory*, 49(4):866–872, 2003. doi:10.1109/TIT.2003.809567.

17 Chaoping Xing and Chen Yuan. A new class of rank-metric codes and their list decoding beyond the unique decoding radius. *IEEE Trans. Inf. Theory*, 64(5):3394–3402, 2018. doi:10.1109/TIT.2017.2780848.