Electronic Colloquium on Computational Complexity, Report No. 161 (2015)

A new class of rank-metric codes and their list decoding beyond the unique decoding radius

Chaoping Xing *and* Chen Yuan

School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore.
Emails: xingcp@ntu.edu.sg; yuan0064@e.ntu.edu.sg

Abstract

Compared with classical block codes, efficient list decoding of rank-metric codes seems more difficult. The evidences to support this view include: (i) so far people have not found polynomial time list decoding algorithms of rank-metric codes with decoding radius beyond $(1-R)/2$ (where R is the rate of code) if ratio of the number of rows over the number of columns is constant, but not very small; (ii) the Johnson bound for rank-metric codes does not exist as opposed to classical codes; (iii) the Gabidulin codes can not be list decoded beyond half of minimum distance. Although the list decodability of random rank-metric codes and limits to list decodability have been completely determined, little work on efficient list decoding rank-metric codes has been done. The only known efficient list decoding of rank-metric codes $\mathcal{C}$ gives decoding radius up to the Singleton bound $1-R-\varepsilon$ with positive rate R when $\rho(\mathcal{C})$ is extremely small, i.e., $\Theta(\varepsilon^2)$, where $\rho(\mathcal{C})$ denotes the ratio of the number of rows over the number of columns of $\mathcal{C}$ [17, STOC2013]. It is commonly believed that list decoding of rank-metric codes $\mathcal{C}$ with not small constant ratio $\rho(\mathcal{C})$ is hard.

The main purpose of the present paper is to explicitly construct a class of rank-metric codes $\mathcal{C}$ with not small constant ratio $\rho(\mathcal{C})$ and efficiently list decode these codes with decoding radius beyond $(1-R)/2$. Specifically speaking, let r be a prime power and let c be an integer between 1 and $r-1$. Let $\varepsilon > 0$ be a small real. Let $q = r^\ell$ with $\gcd(r-1, \ell n) = 1$. Then there exists an explicit rank-metric code $\mathcal{C}$ in $\mathbb{M}_{n\times(r-1)n}(\mathbb{F}_q)$ with rate R that is $(\tau, O(\exp(1/\varepsilon^2)))$-list decodable with $\tau = \frac{c}{c+1}\left(1 - \frac{r-1}{r-c} \times R - \varepsilon\right)$. Furthermore, encoding and list-decoding algorithms are in polynomial time $\mathrm{poly}(n, \exp(1/\varepsilon))$. The list size can be reduced to $O(1/\varepsilon)$ by randomizing the algorithm. Note that the ratio $\rho(\mathcal{C})$ for our code $\mathcal{C}$ is $1/(r-1)$. Our key idea is to employ two-variable polynomials $f(x,y)$, where f is linearized in variable x and the variable y is used to "fold" the code. In other words, rows are used to correct rank errors and columns are used to "fold" the code to enlarge decoding radius. Apart from the above algebraic technique, we have to prune down the list. The algebraic idea enables us to pin down the messages into a structured subspace of dimension linear in the number n of columns. This "periodic" structure allows us to pre-encoding the messages to prune down the list. More precisely, we use subspace design introduced in [17, STOC2013] to get a deterministic algorithm with a larger constant list size and employ hierarchical subspace-evasive sets introduced in [16, STOC2012] to obtain a randomized algorithm with a smaller constant list size.

ISSN 1433-8092

1 Introduction

Rank-metric codes were first introduced by Delsarte in [1] and have found applications in network coding [18] and public-key cryptography [9, 23]. These codes are closely related to space-time codes over finite fields [19, 17]. Unique decoding algorithms for rank-metric codes within half minimum distance have been extensively studied [6, 18]. However, efficient list decoding of rank-metric codes seems more difficult than that of classical block codes. There are several evidences to support this view. Firstly, people have not found polynomial-time list decoding algorithms with decoding radius beyond $(1-R)/2$ (where R is the rate of code) if ratio of the number of rows over the number of columns is a constant, but not very small. Secondly, the Johnson bound does not exist as opposed to classical codes [20]. Thirdly, an important class of rank-metric codes introduced by Gabidulin [7] that are similar to Reed-Solomon codes can not be list decoded beyond half of minimum distance [20]. The purpose of this paper to design polynomial time list decoding algorithms for rank-metric codes with decoding radius beyond $(1-R)/2$.

Before introducing known results and our main results in this paper, we first define list decodability of a rank-metric code. A rank-metric code over finite filed $\mathbb{F}_q$ is subset of $\mathbb{M}_{n\times t}(\mathbb{F}_q)$, where $\mathbb{M}_{n\times t}(\mathbb{F}_q)$ denotes the set of $n\times t$ matrices over $\mathbb{F}_q$. Without loss of generality, we always assume $t \geqslant n$ for a rank-metric code in $\mathbb{M}_{n\times t}(\mathbb{F}_q)$.

Definition 1. *The rank-metric ball of center $M \in \mathbb{M}_{n\times t}(\mathbb{F}_q)$ and radius d is defined to be the set $\{X \in \mathbb{M}_{n\times t}(\mathbb{F}_q) : \mathrm{rank}(X-M) \leqslant d\}$. A rank-metric code $\mathcal{C}$ is called (τ, L)-list decodable if, for every matrix $M \in \mathbb{M}_{n\times t}(\mathbb{F}_q)$, there is at most L codewords of $\mathcal{C}$ in the rank-metric ball of center M of radius τn.*

1.1 Known results

Unlike list decoding classical codes, there are very few results in literature for efficient list decoding of rank-metric codes. The only known efficient list decoding of rank-metric codes in the asymptotic sense gives decoding radius up to the Singleton bound $1-R-\varepsilon$ when ratio of the number of rows over the number of columns is $\Theta(\varepsilon^2)$ [17, STOC2013]. On the other hand, list decodability of random rank-metric codes and limits on list decodability of rank-metric codes are completely known [2, 22]. More precisely, we have the following result .

Proposition 1.1. *(see [2]) Let n/t tend to a fixed constant ρ. Then for any real $R \in (0,1)$, a rank-metric code $\mathcal{C} \subseteq \mathbb{M}_{n\times t}(\mathbb{F}_q)$ of rate R that is (τ, L)-list decodable with $L = \mathrm{poly}(n)$ must obey $R \leqslant (1-\tau)(1-\rho\tau)$. On the other hand, with high probability a random rank-metric code of rate R in $\mathbb{M}_{n\times t}(\mathbb{F}_q)$ is $(\tau, O(1/\varepsilon))$-list decodable with $R = (1-\tau)(1-\rho\tau)-\varepsilon$ for any small real $\varepsilon > 0$. In particular, if n/t tends to a fixed small constant ε, then with high probability a random rank-metric code of rate R in $\mathbb{M}_{n\times t}(\mathbb{F}_q)$ is $(1-R-\varepsilon, O(1/\varepsilon))$-list decodable.*

The above result tells that $R = (1-\tau)(1-\rho\tau)$ is the limit to the list decoding of rank-metric codes and moreover most random codes can achieve this limit. The question is how to explicitly construct these codes and efficiently list decode them. It is natural to start with the Gabidulin codes because they are very similar to the classical Reed-Solomon codes. Both of these two classes of codes are constructed from evaluations of polynomials. As the Reed-Solomon codes can be list decoded up to the Johnson bound [13], people hoped to list decode the Gabidulin codes at least beyond half of the minimum distance, i.e., $\tau > (1-R)/2$. Unfortunately, it was first shown in [22] that list decodability of the square Gabidulin codes does not exceed the bound $\tau = 1-\sqrt{R}$ and recently it was shown in [20] that list decodability of the square Gabidulin

codes does not exceed half of the minimum distance, i.e., $(1-R)/2$ for a certain family of parameters. This implies that decoding radius of list decoding the square Gabidulin codes is not better than unique decoding.

Inspired by good list decodability of the folded Reed-Solomon codes [12], people started to consider list decoding of folded Gabidulin codes [19]. However, the rate of the folded Gabidulin code in [19] tends to 0. In 2013, Guruswami and Xing [17] considered subcodes of the Gabidulin codes via point evaluation in a subfield and showed that list decodability of subcodes of the Gabidulin codes achieves the Singleton bound $\tau = 1 - R$. However, the ratio $\rho = n/t$ of the rank-metric code $\mathcal{C} \subseteq \mathbb{M}_{n\times t}(\mathbb{F}_q)$ constructed by Guruswami and Xing [17] is $\Theta(\varepsilon^2)$. This is slightly weaker than random rank-metric codes where the ratio $\rho = n/t$ can achieve $\Theta(\varepsilon)$. So it is still an open problem to explicitly construct rank-metric codes in $\mathbb{M}_{n\times t}(\mathbb{F}_q)$ with ratio $\rho = n/t = \Theta(\varepsilon)$ and decoding radius $\tau = 1 - R - \varepsilon$ and efficiently list decode them.

There has been no much progress on a more interesting case where the ratio $\rho = n/t$ is not too small. Hence, an even more important open problem in the topic of list decoding rank-metric codes is the following

> **Open Problem.** For a given constant ratio $\rho = n/t \in (0, 1)$ (not very small), explicitly construct rank-metric codes of rate R in $\mathbb{M}_{n\times t}(\mathbb{F}_q)$ with decoding radius $\tau > (1-R)/2$ and efficiently list decode them.

1.2 Our results

The present paper moves the first step towards solving the above Open Problem. We first construct explicit rank-metric codes and then consider list decoding of these rank-metric codes. As a result, we present two decoding algorithms, one deterministic algorithm and one Monte Carlo algorithm. Both the algorithms give the same decoding radius that is bigger than $(1-R)/2$. More precisely, we have the followings.

Theorem 1.2. (Main Theorem) *Let r be a prime power and let c be an integer between 1 and $r-1$. Let $\varepsilon > 0$ be a small real. Let $q = r^\ell$ with $\gcd(r-1, \ell n) = 1$.*

(i) *There exists an explicit rank-metric code in $\mathbb{M}_{n\times(r-1)n}(\mathbb{F}_q)$ with rate R that is $(\tau, O(\exp(1/\varepsilon^2)))$-list decodable with $\tau = \frac{c}{c+1}\left(1 - \frac{r-1}{r-c} \times R - \varepsilon\right)$. Furthermore, encoding and list-decoding algorithms are in polynomial time $\mathrm{poly}(n, \exp(1/\varepsilon))$.*

(ii) *With high probability one can randomly sample a rank-metric code in $\mathbb{M}_{n\times(r-1)n}(\mathbb{F}_q)$ with rate R that is $(\tau, O(1/\varepsilon))$-list decodable with $\tau = \frac{c}{c+1}\left(1 - \frac{r-1}{r-c} \times R - \varepsilon\right)$. Furthermore, encoding and list-decoding algorithms are in polynomial time $\mathrm{poly}(n, \exp(1/\varepsilon))$.*

Remark 1. (i) In the above main theorem, if we fix r and c with $2 \leqslant c \leqslant r-1$, then

$$\frac{c}{c+1}\left(1 - \frac{r-1}{r-c} \times R\right) > \frac{1}{2}(1-R)$$

for any $0 \leqslant R < \frac{r-c}{r+c}$. This means that our decoding radius breaks the unique decoding radius for $R \in \left[0, \frac{r-c}{r+c}\right)$. For instance, taking $r = 3$ and $c = 2$ gives a rank-metric code $\mathcal{C} \subseteq \mathbb{M}_{n\times 2n}(\mathbb{F}_q)$ of rate R and decoding radius $\tau = \frac{2}{3}(1-2R)$ which is bigger than $\frac{1}{2}(1-R)$ for $R < \frac{1}{5}$. In this case, the ratio $\rho = n/t$ is $1/2$.

(ii) By Proposition 1.1, a rank-metric code $\mathcal{C} \subseteq \mathbb{M}_{n\times t}(\mathbb{F}_q)$ of rate R that is (τ, L)-list decodable with $L = \text{poly}(n)$ must obey $R \leqslant (1-\tau)(1-\rho\tau)$, where ρ is the ratio n/t. In our case, the ratio $\rho = n/t = 1/(r-1)$. Thus, we must have $R \leqslant (1-\tau)\left(1-\frac{\tau}{r-1}\right)$. The decoding radius in the above theorem gives $R \approx \frac{r-c}{r-1}\left(1-\frac{c+1}{c}\times\tau\right)$ and indeed, one can easily check that

$$\frac{r-c}{r-1}\left(1-\frac{c+1}{c}\times\tau\right) < (1-\tau)\left(1-\frac{\tau}{r-1}\right).$$

(iii) Unfortunately, our main theorem does not improve the unique decoding bound for square rank-metric codes. To get square matrices, r has to be 2. In this case, we can only take $c = 1$. Then the decoding radius in the above main theorem gives $\tau = \frac{1}{2}(1-R)$ which is the same as the unique decoding radius.

In the above theorem, setting $r = \Theta\left(\frac{1}{\varepsilon^2}\right)$ and $c = \Theta\left(\frac{1}{\varepsilon}\right)$ gives the following corollary.

Corollary 1.3. *Let $\varepsilon > 0$ be a small real. Let $r = \Theta\left(\frac{1}{\varepsilon^2}\right)$ and $q = r^\ell$ with $\gcd(r-1, \ell n) = 1$.*

(i) *There exists an explicit rank-metric code in $\mathbb{M}_{n\times(r-1)n}(\mathbb{F}_q)$ with rate R that is $(\tau, (1/\varepsilon)^{O(\exp(1/\varepsilon^4))})$-list decodable with $\tau = 1-R-\varepsilon$. Furthermore, encoding and list-decoding algorithms are in polynomial time $\text{poly}(n, \exp(1/\varepsilon))$.*

(ii) *With high probability one can randomly sample a rank-metric code in $\mathbb{M}_{n\times(r-1)n}(\mathbb{F}_q)$ with rate R that is $(\tau, O((1/\varepsilon)))$. Furthermore, encoding and list-decoding algorithms are in polynomial time $\text{poly}(n, (\exp(1/\varepsilon))$.*

Remark 2. (i) See Remarks 5 and 6 for discussion of the list sizes in Corollary 1.3.

(ii) The ratio in the above corollary is $\rho = n/t = 1/(r-1) = \Theta(\varepsilon^2)$. This ratio is the same as the one in [17, STOC2013]. Thus, the above corollary matches the result of [17, STOC2013].

1.3 Our techniques

It was shown in [20] that list decodability of a Gabidulin codes is not beyond the unique decoding bound $\tau = (1-R)/2$. In the classical case of Reed-Solomon codes, the decoding radius can be enlarged by folding Reed-Solomon codes. The question is how to properly fold Gabidulin codes to enlarge decoding radius. At the same time, we have to make use of linearized polynomials in order to correct rank errors. Our key idea is to employ two-variable polynomials $f(x, y)$, where f is linearized in variable x and the variable y is used to fold the code. In other words, rows are used to correct rank errors and columns are used to fold the code to enlarge decoding radius.

The algebraic idea enables us to pin down the messages into a structured subspace of dimension linear in the number n of columns and this "periodic" structure allows us to pre-encode the messages to prune down the list. Two approaches are employed to pin down our list, namely subspace design introduced in [17, STOC2013] and hierarchical subspace-evasive (h.s.e. for short) sets introduced in [16, STOC2012]. The coefficients of polynomials in the list form a "periodic" subspace. After pre-encoding with subspace design or h.s.e., the new list becomes a constant.

1.4 Organization

The paper is organized as follows. In Section 2, we provide a new construction of "folded" rank-metric codes and discuss their parameters. Section 3 devotes to list decoding of the rank-metric codes in Section 2, including establishment of interpolation polynomial, solving of certain equations for list and discussion of decoding radius. In the last section, we make use of subspace design and hierarchical subspace-evasive sets to pre-encode the messages and pin down the list. The algorithm from subspace design is deterministic, while the algorithm from hierarchical subspace-evasive sets is Monte Carlo.

2 Construction of rank-metric codes

2.1 Rank-metric codes

Before introducing our construction, we review some basic facts and results on rank-metric code.

Let q be a prime power and denote by $\mathbb{M}_{n\times t}(\mathbb{F}_q)$ the set of $n \times t$ matrices over $\mathbb{F}_q$. One can define the rank distance between two matrices $A, B \in \mathbb{M}_{n\times t}(\mathbb{F}_q)$ to be the rank of $A-B$, i.e., $d(A, B) = \mathrm{rank}(A-B)$. Indeed this defines a distance [7]. A rank-metric code $\mathcal{C}$ is a subset of $\mathbb{M}_{n\times t}(\mathbb{F}_q)$ with rate and distance given by

$$R(\mathcal{C}) = \frac{\log_q |\mathcal{C}|}{nt} \quad \text{and} \quad d(\mathcal{C}) = \min_{A\neq B\in\mathcal{C}}\{d(A, B)\}.$$

Without loss of generality, from now on we may assume that $n \leqslant t$ (otherwise, we can consider transpose of matrices). As in the classical case, one has the following Singleton bound (see [7])

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

A code archiving the above Singleton bound 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. Recently, some MRD codes other than Gabidulin codes have been constructed [21].

To better understand our codes, we briefly review the construction of Gabidulin codes [7]. 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 ℓ if $a_\ell \neq 0$.

Let $0 < k \leq n \leq t$ be integers, and choose $\mathbb{F}_q$-linearly independent elements $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{q^t}$. For every q-linearized polynomial $f \in \mathbb{F}_{q^t}[X]$ of q-degree at most $k-1$, we can encode f by the column vector $A_f = \big(f(\alpha_1), \ldots, f(\alpha_n)\big)^T$ over $\mathbb{F}_{q^t}$. By fixing a basis of $\mathbb{F}_{q^t}$ over $\mathbb{F}_q$, we can also think of A_f as an $n \times t$ matrix over $\mathbb{F}_q$. This yields the Gabidulin code

$$\mathcal{C}_G(q, n, t, k) := \{A_f \in \mathbb{M}_{n\times t}(\mathbb{F}_q) : \ f \in \mathbb{F}_{q^t}[x] \text{ is } q\text{-linearized and } \deg_q(f) \leq k-1\}.$$

The Gabidulin codes are similar to the classical Reed-Solomon codes. However, if applying Sudan's list decoding idea to decoding of the Gabidulin codes, we get only unique decoding (see [18]).

In order to enlarge list decoding radius of the Gabidulin codes, Mahdavifar and Vardy [19] considered folded Gabidulin codes. As a result, the rate tends to 0. In the next subsection, we consider evaluations of two-variable polynomials to obtain rank-metric codes with good list decodabiity.

2.2 Construction

Let us fix some notations at the beginning. Let n, m be positive integers with $m \leqslant n$ (m and n are propositional and both tend to ∞). Let r be a prime power and choose a positive integer k with $k \leqslant r-1$ (both r and k are constant and independent of n, m). Put $q = r^\ell$ for some ℓ with $\gcd(r-1, n\ell) = 1$ (ℓ is a constant and hence q is a constant as well). Fix a primitive element γ of $\mathbb{F}_r^*$.

We have the following facts:

- $x^{r-1} - \gamma$ is irreducible over $\mathbb{F}_r$, and hence it is irreducible over $\mathbb{F}_{q^n}$ as well since $\gcd(r-1, n\ell) = 1$.
- $x^r \equiv \gamma x \mod x^{r-1} - \gamma$.

Consider the two-variable polynomial space over $\mathbb{F}_{q^n}$

$$\mathcal{P}_q(n,k,m)[x,y] := \left\{ \sum_{i=0}^{m-1} f_i(x) y^{q^i} : \ f_i(x) \in \mathbb{F}_{q^n}[x] \text{ and } \deg(f_i(x)) \leqslant k-1 \text{ for all } 0 \leqslant i \leqslant m-1 \right\}.$$

Let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$. For each polynomial $f = \sum_{i=0}^{m-1} f_i(x) y^{q^i} \in \mathcal{P}_q(n,k,m)[x,y]$, we define a matrix

$$M_f := \begin{pmatrix} f(1,\alpha_1) & f(\gamma,\alpha_1) & f(\gamma^2,\alpha_1) & \cdots & f(\gamma^{r-2},\alpha_1) \\ f(1,\alpha_2) & f(\gamma,\alpha_2) & f(\gamma^2,\alpha_2) & \cdots & f(\gamma^{r-2},\alpha_2) \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ f(1,\alpha_n) & f(\gamma,\alpha_n) & f(\gamma^2,\alpha_n) & \cdots & f(\gamma^{r-2},\alpha_n) \end{pmatrix}$$

Each entry in the above matrix is viewed as a row vector of $\mathbb{F}_q^n$. Thus, M_f is an $n \times ((r-1)n)$ matrix over $\mathbb{F}_q$. Set $t = (r-1)n$. Let $\mathcal{C}_q(n,k,m,r)$ be the collection of M_f for all $f \in \mathcal{P}_q(n,k,m)[x,y]$.

Lemma 2.1. *The distance and rate of $\mathcal{C}_q(n,k,m,r)$ satisfy*

$$d(\mathcal{C}_q(n,k,m,r)) \geqslant n-m+1 \quad \textit{and} \qquad R(\mathcal{C}_q(n,k,m,r)) := \frac{\log_q q^{nkm}}{(r-1)n^2} = \frac{k}{r-1} \times \frac{m}{n},$$

respectively.

Proof. The size of $\mathcal{P}_q(n,k,m)[x,y]$ is q^{nkm}. Furthermore, it is easy to see that $\mathcal{C}_q(n,k,m,r)$ is an $\mathbb{F}_q$-linear space. Hence it is sufficient to show that the rank of M_f is at least $n-m+1$ for every nonzero polynomial $f(x,y) \in \mathcal{P}_q(n,k,m)[x,y]$.

Let $f = \sum_{i=0}^{m-1} f_i(x) y^{q^i}$ in $\mathcal{P}_q(n,k,m)[x,y]$ be a nonzero polynomial. Suppose that M_f has rank less than $n-m+1$. Then the solution space $U \subseteq \mathbb{F}_q^n$ of $\mathbf{z}M_f = \mathbf{0}$ has dimension at least m. Let V be the $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}$ given by $V = \{\sum_{i=1}^n u_i \alpha_i : \ (u_1, u_2, \ldots, u_n) \in U\}$. Then $\dim_{\mathbb{F}_q}(V) = \dim_{\mathbb{F}_q}(U) \geqslant m$.

For each $0 \leqslant j \leqslant r-2$, Let $g_j(y) = f(\gamma^j, y)$. Then, every α in V is a root of the polynomial $g_j(y)$. Since $\deg(g_j(y)) \leq m-1$, the polynomial $f(\gamma^j, y) = g_j(y)$ is identical to 0. This means that the coefficients $f_i(\gamma^j)$ of $g_j(y)$ are zero for any $0 \leqslant i \leqslant m-1$. As the degree of $f_i(x)$ is at most $k-1$, we conclude that $f_i(x)$ are the zero polynomials for all $0 \leqslant i \leqslant m-1$. This is a contradiction and the proof is completed. □

Remark 3. The code $\mathcal{C}_q(n,k,m,r)$ is an MRD code if and only if $k = r-1$.

3 List decoding

Suppose that a codeword M_f is transmitted and $Y = (y_{i,j})_{1\leqslant i\leqslant n;0\leqslant j\leqslant r-2}$ is received with at most e errors, i.e., $\mathrm{rank}(M_f - Y) \leqslant e$. Our goal in this section is to recover M_f, or equivalently the polynomial $f(x,y) \in \mathcal{P}_q(n,k,m)[x,y]$. First we prove a lemma on rank of matrices.

Lemma 3.1. *Let $X, Z \in \mathbb{M}_{n\times t}(\mathbb{F}_q)$ with $\mathrm{rank}(X-Z) \leqslant e$. Then $\dim_{\mathbb{F}_q}(\langle X\rangle \cap \langle Z\rangle) \geqslant \dim_{\mathbb{F}_q}(\langle X\rangle) - e$, where $\langle X\rangle$ stands for the row space of X over $\mathbb{F}_q$.*

Proof. It is easy to see that the two $\mathbb{F}_q$-spaces $\langle X\rangle + \langle Z\rangle$ and $\langle X-Z\rangle + \langle Z\rangle$ are equal. Thus,

$$\dim_{\mathbb{F}_q}(\langle X\rangle)+\dim_{\mathbb{F}_q}(\langle Z\rangle)-\dim_{\mathbb{F}_q}(\langle X\rangle\cap\langle Z\rangle) = \dim_{\mathbb{F}_q}(\langle X-Z\rangle)+\dim_{\mathbb{F}_q}(\langle Z\rangle)-\dim_{\mathbb{F}_q}(\langle X-Z\rangle\cap\langle Z\rangle).$$

This gives

$$\dim_{\mathbb{F}_q}(\langle X\rangle \cap \langle Z\rangle) = \dim_{\mathbb{F}_q}(\langle X\rangle) - \dim_{\mathbb{F}_q}(\langle X-Z\rangle) + \dim_{\mathbb{F}_q}(\langle X-Z\rangle \cap \langle Z\rangle) \geqslant \dim_{\mathbb{F}_q}(\langle X\rangle) - e.$$

The proof is completed. □

3.1 Interpolation polynomials

We fix a parameter s with $1 \leqslant s \leqslant r-1$.

Definition 2 (Space of interpolation polynomials)**.** *Let $\mathcal{L}$ be the space of polynomials $Q \in \mathbb{F}_{q^n}[x, y, z_1, z_2, \ldots, z_s]$ of the form $Q(x,y,z_1,z_2,\ldots,z_s) = A_0(x,y) + A_1(x,z_1) + A_2(x,z_2) + \cdots + A_s(x,z_s)$, with $A_0(x,y) \in \mathcal{P}_q(n, r-1, n-e)[x,y]$ and each $A_i(x,z_i) \in \mathcal{P}_q(n, r-k, n-e-m+1)[x,z_i]$ for $i = 1,2,\ldots,s$.*

Lemma 3.2. *If $e < \frac{s(r-k)(n-m+1)}{r-1+s(r-k))}$, then there exists a nonzero polynomial $Q \in \mathcal{L}$ such that $Q(\gamma^j, \alpha_i, y_{i,j}, y_{i,j+1}, \ldots, y_{i,j+s-1}) = 0$ for $i = 1,2,\ldots,n$ and $j = 0,1,2,\ldots,r-2$. Note that if $j+s-1$ is bigger than $r-2$, we replace $y_{i,j+s-1}$ by $y_{i,j+s-1 \bmod r-1}$. Furthermore, such a polynomial Q can be found using $O(n^4)$ operations over $\mathbb{F}_{q^n}$.*

Proof. Note that $\mathcal{L}$ is an $\mathbb{F}_{q^n}$-vector space of dimension $(r-1)(n-e) + s(r-k)(n-e-m+1)$. This dimension is bigger than $n(r-1)$ by our choice of m and k. The conditions to be satisfied in the Lemma give rise to $n(r-1)$ homogeneous linear conditions on Q. Since $n(r-1) < (r-1)(n-e) + s(r-k)(n-e-m+1)$ in our setting, there must exist a nonzero $Q \in \mathcal{L}$ that meets the interpolation conditions $Q(\gamma^j, \alpha_i, y_{i,j}, y_{i,j+1}, y_{i,j+2}, \cdots, y_{i,j+s-1}) = 0$ for $i = 1,2,\ldots,n$ and $j = 0,1,\ldots,r-2$. Finding such a polynomial Q amounts to solving a homogeneous linear system over $\mathbb{F}_{q^n}$ with $n(r-1)$ constraints and $\dim_{\mathbb{F}_{q^n}}(\mathcal{L}) = (r-1)(n-e) + s(r-k)(n-e-m+1)$ unknowns, which can be done in $O(n^4)$ time. □

Lemma 3.3. *Let $f \in \mathcal{P}_q(n,k,m)[x,y]$ be a polynomial. Suppose that the codeword M_f is transmitted and $Y = (y_{i,j})_{n\times(r-1)}$ ($y_{i,j} \in \mathbb{F}_{q^n}$) is received with at most e errors. Assume that $e < \frac{s(r-k)(n-m+1)}{r-1+s(r-k)}$ and let $Q(x,y,z_1,z_2,\ldots,z_s)$ be the interpolation polynomial given in Lemma 3.2. Then*

$$Q(\gamma^j, y, f(\gamma^j, y), f(\gamma^{j+1}, y), f(\gamma^{j+2}, y), \cdots, f(\gamma^{j+s-1}, y)) \equiv 0 \tag{2}$$

for all $j = 0,1,2,\ldots,r-2$. The above $\equiv$ means that the polynomial on the left is identical to 0.

Proof. Note that $e < \frac{s(r-k)(n-m+1)}{r-1+s(r-k))} < n-m+1$. Since e and $n-m$ are both integers, we have $e \leq n-m$. The polynomial $Q(\gamma^j, y, f(\gamma^j, y), f(\gamma^{j+1}, y), f(\gamma^{j+2}, y), \cdots, f(\gamma^{j+s-1}, y))$ has degree at most q^{m-1}, moreover it is q-linearized. Denote by A and B the $n \times rn$ matrices $((\alpha_1, \alpha_2, \ldots, \alpha_n)^T, M_f)$ and $((\alpha_1, \alpha_2, \ldots, \alpha_n)^T, Y)$ over $\mathbb{F}_q$, respectively.

It is clear that $\mathrm{rank}(A-B) = \mathrm{rank}(M_f - Y) \leqslant e$ and $\mathrm{rank}(A) = n$. Thus, by Lemma 3.1 $\dim_{\mathbb{F}_q}(\langle A\rangle \cap \langle B\rangle) \geqslant n - e \geq m$. This implies that exists an $\mathbb{F}_q$-subspace U of $\mathrm{span}\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ of dimension at least m such that, for every $\alpha = \sum_{i=1}^n c_i\alpha_i \in U$ with $c_i \in \mathbb{F}_q$, one has

$$\sum_{i=1}^n c_i y_{i,j+u-1} = \sum_{i=1}^n c_i f(\gamma^{j+u-1}, \alpha_i) = f\left(\gamma^{j+u-1}, \sum_{i=1}^n c_i\alpha_i\right) = f(\gamma^{j+u-1}, \alpha)$$

for $u = 1, 2, \ldots, s$. Hence,

$$\begin{aligned}
0 &= \sum_{i=1}^n c_i Q(\gamma^j, \alpha_i, y_{i,j}, y_{i,j+1}, \cdots, y_{i,j+s-1}) \\
&= \sum_{i=1}^n \left(c_i A_0(\gamma^j, \alpha_i) + \sum_{u=1}^s c_i A_u(\gamma^j, y_{i,j+u-1}) \right) \\
&= A_0\left(\gamma^j, \sum_{i=1}^n c_i\alpha_i\right) + \sum_{u=1}^s A_u\left(\gamma^j, \sum_{i=1}^n c_i y_{i,j+u-1}\right) \\
&= A_0\left(\gamma^j, \alpha\right) + \sum_{u=1}^s A_u\left(\gamma^j, f(\gamma^{j+u-1}, \alpha)\right) \\
&= Q(\gamma^j, \alpha, f(\gamma^j, \alpha), f(\gamma^{j+1}, \alpha), f(\gamma^{j+2}, \alpha), \cdots, f(\gamma^{j+s-1}, \alpha)).
\end{aligned}$$

As the degree of $Q(\gamma^j, y, f(\gamma^j, y), f(\gamma^{j+1}, y), f(\gamma^{j+2}, y), \cdots, f(\gamma^{j+s-1}, y))$ is at most q^{m-1}. The desired result follows. □

Lemma 3.4. *Let $f = \sum_{i=0}^{m-1} f_i(x)y^{q^i} \in \mathcal{P}_q(n,k,m)[x,y]$ be a polynomial. Suppose that the codeword M_f is transmitted and Y is received with at most e errors. Assume that $e < \frac{s(r-k)(n-m+1)}{r-1+s(r-k)}$ and let $Q(x, y, z_1, z_2, \ldots, z_s) = A_0(x,y) + A_1(x,z_1) + A_2(x,z_2) + \cdots + A_s(x,z_s)$ be the interpolation polynomial given in Lemma 3.2. Write $A_0(x,y) = \sum_{i=0}^{n-e-1} A_{0,i}(x)y^{q^i}$ and $A_w(x,z) = \sum_{i=0}^{n-e-m} A_{w,i}(x)z^{q^i}$ for $1 \leqslant w \leqslant s$. Then we have*

$$A_{0,u}(x) + \sum_{w=1}^s \sum_{i+v=u} A_{w,i}(x) f_v^{(i)}(\gamma^{w-1}x) \equiv 0 \tag{3}$$

for all $0 \leqslant u \leqslant n-e-1$, where $g^{(j)}(x)$ stands for $\sum_{i=0}^N g_i^{q^j} x^i$ for a polynomial $g(x) = \sum_{i=0}^N g_i x^i \in \mathbb{F}_{q^n}[x]$.

Proof. By Lemma 3.3, we have

$$\begin{aligned} 0 &\equiv Q(\gamma^j, y, f(\gamma^j, y), f(\gamma^{j+1}, y), f(\gamma^{j+2}, y), \cdots, f(\gamma^{j+s-1}, y)) \\ &= \sum_{u=0}^{n-e-1} A_{0,u}(\gamma^j) y^{q^u} + \sum_{w=1}^{s} \sum_{i=0}^{n-e-m} A_{w,i}(\gamma^j) \left(\sum_{v=0}^{m-1} f_v(\gamma^{w+j-1}) y^{q^v} \right)^{q^i} \\ &= \sum_{u=0}^{n-e-1} A_{0,u}(\gamma^j) y^{q^u} + \sum_{u=0}^{n-e-1} \left(\sum_{w=1}^{s} \sum_{i+v=u} A_{w,i}(\gamma^j) f_v^{(i)}(\gamma^{w+j-1}) \right) y^{q^u} \end{aligned}$$

This gives

$$A_{0,u}(\gamma^j) + \sum_{w=1}^{s} \sum_{i+v=u} A_{w,i}(\gamma^j) f_v^{(i)}(\gamma^{w+j-1}) = 0$$

for all $0 \leqslant u \leqslant n-e-1$ and $0 \leqslant j \leqslant r-2$. This implies that the polynomial

$$A_{0,u}(x) + \sum_{w=1}^{s} \sum_{i+v=u} A_{w,i}(x) f_v^{(i)}(\gamma^{w-1} x)$$

has at least $r-1$ roots. On the other hand, this polynomial has degree at most $k-1 \leqslant r-2$. The desired result follows. □

3.2 Analysis of list and list size

Before discussing the list, let us introduce periodic subspaces that were defined in [16]. For a vector $\mathbf{a} = (a_1, a_2, \ldots, a_N) \in \mathbb{F}_r^N$ 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 3 (Periodic subspaces)**.** *For positive integers u, b, Λ and $\kappa := b\Lambda$, an affine subspace $H \subset \mathbb{F}_r^\kappa$ is said to be $(u, \Lambda, b)_r$-periodic if there exists a subspace $W \subseteq \mathbb{F}_r^\Lambda$ of dimension at most u such that for every $j = 1, 2, \ldots, b$, and every "prefix" $\mathbf{a} \in \mathbb{F}_q^{(j-1)\Lambda}$, the projected affine subspace of $\mathbb{F}_r^\Lambda$ defined as*

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

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

Now we return to finding list of polynomial candidates.

Lemma 3.5. *Let $f = \sum_{i=0}^{m-1} f_i(x) y^{q^i} \in \mathcal{P}_q(n, k, m)[x, y]$ be a polynomial. Suppose that the codeword M_f is transmitted and Y is received with at most e errors. Assume that $e < \frac{s(r-k)(n-m+1)}{r-1+s(r-k)}$. Then solutions of* (3) *form an $(s-1, \ell n(r-1), m)_r$-periodic subspace of size at most $r^{m(s-1)}$.*

Proof. Note that for $u \in [0, n-e-1]$, the solutions of (3) give the list of the candidates.

Let us start with $u = 0$. Then (3) gives the equation

$$A_{0,0}(x) + \sum_{w=1}^{s} A_{w,0}(x) f_0^{(0)}(\gamma^{w-1}x) = 0 \tag{4}$$

Note that $f_0^{(0)}(x) = f_0(x)$. In the residue ring $\mathbb{F}_{q^n}[x]/(x^{r-1} - \gamma)$, the equation (4) becomes

$$A_{0,0}(x) + \sum_{w=1}^{s} A_{w,0}(x)(f_0(x))^{r^{w-1}} \equiv 0 \mod x^{r-1} - \gamma. \tag{5}$$

Since $x^{r-1} - \gamma$ is an irreducible polynomial over $\mathbb{F}_{q^n}$, the residue ring $\mathbb{F}_{q^n}[x]/(x^{r-1} - \gamma) \simeq \mathbb{F}_{q^{n(r-1)}}$ is a field. Because the degree of $f_0(x)$ is at most $r - 2$, all solutions of $f_0(x)$ in the equation (5) form an affine space $W + \mathbf{v}_1$ for some $\mathbf{v}_1 \in \mathbb{F}_{q^n}[x]/(x^{r-1} - \gamma) \simeq \mathbb{F}_r^{\ell n(r-1)}$, where W is the solution space of the $\mathbb{F}_r$-linearized polynomial

$$\sum_{w=1}^{s} A_{w,0}(x) z^{r^{w-1}} \equiv 0 \mod x^{r-1} - \gamma \tag{6}$$

and therefore it has dimension at most $s - 1$ over $\mathbb{F}_r$.

Note that once $f_0(x)$ is recovered, all $f_0^{(j)}$ are recovered as well for $j \geqslant 0$.

By induction, assume that all $f_i(x)$ have been recovered for $0 \leqslant i \leqslant a - 1$. Next, we want to recover $f_a(x)$ from the following equation

$$A_{0,a}(x) + \sum_{w=1}^{s} \sum_{i+v=a} A_{w,i}(x)(f_v^{(i)}(x))^{r^{w-1}} \equiv 0 \mod x^{r-1} - \gamma.$$

Rewrite the above equation into the following

$$A_{0,a}(x) + \sum_{w=1}^{s} \sum_{v=1}^{a-1} A_{w,a-v}(x)(f_v^{(a-v)}(x))^{r^{w-1}} + \sum_{w=1}^{s} A_{w,0}(x)(f_a^{(0)}(x))^{r^{w-1}} \equiv 0 \mod x^{r-1} - \gamma \tag{7}$$

By the similar arguments, one can show that all solutions of $f_a^{(0)}(x) = f_a(x)$ in the equation (7) form an affine space $W + \mathbf{v}_a$ for some $\mathbf{v}_a \in \mathbb{F}_{q^n}[x]/(x^{r-1} - \gamma) \simeq \mathbb{F}_r^{\ell n(r-1)}$. Apparently, all possible $(f_0(x), f_1(x), \ldots, f_{m-1}(x))$ in the list form an $(s - 1, \ell n(r - 1), m)_r$-periodic subspace.

To compute the list size, we note that each $f_i(x)$ has at most r^{s-1} solutions. Thus, the list size is bounded by $r^{m(s-1)}$. □

As m is promotional to n, the list size $r^{m(s-1)}$ in Lemma 3.5 becomes exponential. We will prune down the list size by pre-encoding through the special structure of periodic subspace.

Remark 4. Each $f_i(x)$ is a solution of (7). As $\deg(f_i(x)) \leqslant k - 1$, there exist an $g(x) \in \mathbb{F}_{q^n}[x]$ with $\deg(g(x)) \leqslant k-1$ such that $f(x) \in g(x) + W'$, where $W' = W \cap \{h(x) \in \mathbb{F}_{q^n}[x] : \deg(h) \leqslant k-1\}$ and W is the solution space of (6). This implies that our message $f(x)$ actually belongs to an $(s - 1, \ell nk, m)_r$-periodic subspace of size at most $r^{m(s-1)}$.

3.3 Decoding radius

Finally, let us compute the decoding radius from the list decoding in this section.

Put $e = \left\lfloor \frac{s(r-k)(n-m+1)}{r-1+s(r-k))} \right\rfloor - 1$ and $\tau = e/n$, then we have

$$\tau \approx \frac{s(r-k)}{r-1+s(r-k)} \left(1 - \frac{m}{n}\right) = \frac{s(r-k)}{r-1+s(r-k)} \left(1 - R \times \frac{r-1}{k}\right). \tag{8}$$

If we take $s = r-1$ and $k = r-c$ for some $1 \leqslant c \leqslant r-1$, then we get

$$\tau = \frac{c}{c+1} \left(1 - \frac{r-1}{r-c} \times R\right). \tag{9}$$

4 Pruning list size

In this section, we prune list via subspace design and h.s.e. The subspace design provides a deterministic algorithm with a constant list size, while h.s.e provides a randomized algorithm with a smaller constant list size.

4.1 A deterministic algorithm

The subspace design was first introduced in [17] to pin down list.

Definition 4. *A collection S of $\mathbb{F}_r$-subspaces $H_1, \ldots, H_M \subseteq \mathbb{F}_r^\Lambda$ is called a $(v, A, \Lambda)_r$-subspace design if for every $\mathbb{F}_r$-linear space $W \subset \mathbb{F}_r^\Lambda$ of dimension v,*

$$\sum_{i=1}^{M} \dim_{\mathbb{F}_r}(H_i \cap W) \leq A.$$

In order to pin down the list to a constant size, one has to consider intersection with subspace evasive set introduced in [14].

Definition 5. *A subset S of $\mathbb{F}_r^\Lambda$ is called a $(v, A, \Lambda)_r$-subspace evasive if for any subspace W of $\mathbb{F}_r^\Lambda$ of dimension v, the intersection $S \cap W$ has size at most A.*

The following result tells that one can obtain a small list from intersection of a periodic subspace with a suitable subspace design .

Lemma 4.1. *([17, 15]) Let H be a $(v, \Lambda, b)_r$-periodic subspace, and let $\{H_1, H_2, \ldots, H_b\}$ be a $(v, A, \Lambda)_r$-subspace design. Then $H \cap (H_1 \times \cdots \times H_b)$ is an affine subspace over $\mathbb{F}_r$ of dimension at most A.*

Assume that Λ has a divisor $\lambda \approx 2\log_r \Lambda$ for some $c > 1$ and thus we have $r^\lambda > \Lambda$. Let $q_1 = r^\lambda$ and $\Lambda' = \Lambda/\lambda$.

Lemma 4.2 ([3])**.** *Let $\varepsilon > 0$ be a small real. Let v be a positive integer and set $h \approx v/\varepsilon$ to be a positive integer. Assume that $q_1 \geqslant h$ and let $\gamma_1, \ldots, \gamma_h$ be distinct nonzero elements of $\mathbb{F}_{q_1}$. Let $d_1 > d_2 > \cdots > d_h \geq 1$ be integers. Define $f_1, \ldots, f_v \in \mathbb{F}_{q_1}[x_1, \ldots, x_h]$ as follows:*

$$f_i(x_1, \ldots, x_h) = \sum_{j=1}^{h} \gamma_j^i x_j^{d_j}. \tag{10}$$

Then:

- *The variety* $\mathbf{V} = \{\mathbf{x} \in \overline{\mathbb{F}}_{q_1}^h \mid f_1(\mathbf{x}) = \cdots = f_v(\mathbf{x}) = 0\}$ *satisfies* $|\mathbf{V} \cap H| \leq (d_1)^v$ *for all* v*-dimensional affine subspaces* $H \subset \overline{\mathbb{F}}_{q_1}^h$.
- *If at least* v *of the degrees* d_i *are relatively prime to* $q_1 - 1$*, then* $\left|\mathbf{V} \cap \mathbb{F}_{q_1}^h\right| = q_1^{h-v}$.
- *The product set* $(\mathbf{V} \cap \mathbb{F}_{q_1}^h)^{\Lambda'/h} \subseteq \mathbb{F}_{q_1}^{\Lambda'}$ *is* $(a, (d_1)^a, \Lambda')_{q_1}$*-subspace evasive for all* $a \leq v$.

The below statement follows immediately from Lemma 4.2 and the fact that when the d_j's are powers of r, the polynomials f_i defined in (10) are $\mathbb{F}_r$-linearized polynomials.

Corollary 4.3. *Let* $\varepsilon > 0$ *be a small real. Let* v *be a positive integer and set* $h \approx v/\varepsilon$ *to be a positive integer. Assume that* $q_1 \geqslant h$*. By setting* $d_1 = r^{h-1}, d_2 = r^{h-2}, \ldots, d_h = 1$ *in Lemma 4.2, one obtains an explicit* $(a, r^{a(h-1)}, \Lambda')_{q_1}$*-subspace evasive set* S *of size* $q_1^{(1-\varepsilon)\Lambda'}$ *for all* $1 \leq a \leq v$*. Furthermore,* S *is an* $\mathbb{F}_r$*-linear space of dimension* $(1-\varepsilon)\lambda\Lambda' = (1-\varepsilon)\Lambda$ *and a basis of* S *can be computed in time* $\mathrm{poly}(\Lambda, \log r)$.

Guruswami and Kopparty [10] gives an explicit subspace design based on Wronskian determinant. Their construction implies the following fact.

Lemma 4.4. *For* $\varepsilon \in (0, 1)$*, positive integer* v *with* $v < \varepsilon\Lambda'/4$*, there is an explicit collection of* $M = q_1^{\Omega(\varepsilon\Lambda'/v)}$ *subspaces in* $\mathbb{F}_{q_1}^{\Lambda'}$*, each of codimension at most* $\varepsilon\Lambda'$ *and form a* $(v, 2v/\varepsilon, \Lambda')_{q_1}$*-subspace design. Moreover, bases for* $N \leqslant M$ *elements of this collection can be computed in time* $\mathrm{poly}(N, \Lambda, r)$.

It is required in Lemma 4.4 that $q_1 > \Lambda'$ (see [10]). This condition is satisfied by our choice of parameters since $q_1 = r^\lambda > \Lambda$.

Combined Lemma 4.4 with Corollary 4.3, one can prove the following result.

Proposition 4.5. *For a positive integer* $v \leq \varepsilon\Lambda'/4$*, there exists an explicit* $(v, 2v(h-1)/\varepsilon, \Lambda)_r$*-subspace design* $\{H_1, H_2, \ldots, H_N\}$ *with* $N = q_1^{\Omega(\varepsilon\Lambda'/v)}$ *and* $H_i \subseteq \mathbb{F}_{q_1}^{\Lambda'} = \mathbb{F}_r^{\Lambda}$ *of codimension at most* $2\varepsilon\Lambda$.

Proof. The proof of this proposition can be found in [15, Theorem 3.6] except for adjustment of parameters. To convince the reader of that our parameters work properly, we give a complete proof here. From Lemma 4.4, we can construct $M = q_1^{\Omega(\varepsilon\Lambda'/s)}$ subspaces $V_1, V_2, \ldots, V_M$ with codimension at most $\varepsilon\Lambda'$ over $\mathbb{F}_{q_1}$. By Corollary 4.3, we know that there exists an explicit $\mathbb{F}_r$-linear space S of size $q_1^{(1-\varepsilon)\Lambda'}$ in $\mathbb{F}_{q_1}^{\Lambda'}$ which is $(a, h^{a(\ell-1)}, \Lambda')_{q_1}$-subspace evasive for $a \leq v$. Put $H_i = V_i \cap S$. Since both V_i and S has codimension at most $\varepsilon\Lambda'$ in $F_{q_1}^{\Lambda'}$, the intersection H_i has codimension at most $2\varepsilon\Lambda'$ in $\mathbb{F}_{q_1}^{\Lambda'}$, i.e., H_i has codimension at most $2\varepsilon\Lambda$ in $\mathbb{F}_r^{\Lambda}$. Let W be a v-dimensional $\mathbb{F}_r$-linear subspace in $\mathbb{F}_{q_1}^{\Lambda'}$. Then one can find a v-dimensional $\mathbb{F}_{q_1}$-linear subspace W_1 in $\mathbb{F}_{q_1}^{\Lambda'}$ such that $W \subseteq W_1$.

The subspace design of $\{V_i\}_{i=1}^M$ implies that

$$\sum_{i=1}^{M} \dim_{\mathbb{F}_{q_1}}(V_i \cap W_1) \leq 2v/\varepsilon \tag{11}$$

Denote by v_i the dimension $\dim_{\mathbb{F}_{q_1}}(V_i \cap W_1)$. As $\dim_{\mathbb{F}_{q_1}}(W_1) \leq v$, we have that $v_i \leq v$. Since S is a $(v_i, r^{v_i(h-1)}, \Lambda')_{q_1}$-subspace evasive set, we have $|S \cap (V_i \cap W_1)| \leqslant r^{v_i(h-1)}$. Hence, $\dim_{\mathbb{F}_r}(H_i \cap W_1) \leqslant$

$v_i(h-1) = (h-1)\dim_{\mathbb{F}_{q_1}}(V_i \cap W_1)$. Summing all dimensions up gives

$$\sum_{i=1}^{M} \dim_{\mathbb{F}_r}(H_i \cap W) \leqslant \sum_{i=1}^{M} \dim_{\mathbb{F}_r}(H_i \cap W_1) \leqslant (h-1)\sum_{i=1}^{M} \dim_{\mathbb{F}_{q_1}}(V_i \cap W_1) \leq 2v(h-1)/\varepsilon.$$

The proof is completed. □

Theorem 4.6. [Part (i) of Main Theorem] *Let r be a prime power and let c be an integer between 1 and $r-1$. Let $\widetilde{\varepsilon} > 0$ be a small real. Let $q = r^\ell$ with $\gcd(r-1, \ell n) = 1$. Then there exists an explicit rank-metric code in $\mathbb{M}_{n\times(r-1)n}(\mathbb{F}_q)$ with rate $\widetilde{R}$ that is $(\widetilde{\tau}, O(\exp(1/\widetilde{\varepsilon}^2)))$-list decodable with $\widetilde{\tau} = \frac{c}{c+1}\left(1 - \frac{r-1}{r-c} \times \widetilde{R} - \widetilde{\varepsilon}\right)$. Furthermore, encoding and list-decoding algorithms are in polynomial time* $\mathrm{poly}(n, \exp(1/\widetilde{\varepsilon}))$.

Proof. In Proposition 4.5, we set $v = s-1$, $\Lambda = n\ell(r-1)$ and $h \approx (s-1)/\varepsilon$. Each H_i can be viewed as an $\mathbb{F}_r$-subspace of the polynomial space $\{g(x) \in \mathbb{F}_{q^n}[x] : \deg(g(x)) \leqslant r-1\}$.

We consider the polynomial set

$$\widetilde{\mathcal{P}}_q(n,k,m)[x,y] := \left\{ \sum_{i=0}^{m-1} f_i(x) y^{q^i} : \ f_i(x) \in H_i \text{ and } \deg(f_i(x)) \leqslant k-1 \text{ for all } 0 \leqslant i \leqslant m-1 \right\}.$$

and the code $\widetilde{\mathcal{C}}_q(n,k,m,r) = \{M_f : \ f \in \widetilde{\mathcal{P}}_q(n,k,m)[x,y]\}$. It is clear that $\widetilde{\mathcal{C}}_q(n,k,m,r)$ is $\mathbb{F}_r$ -linear and it is a subcode of our original code $\mathcal{C}_q(n,k,m,r)$. It is easy to see that

$$\dim_{\mathbb{F}_r}(\widetilde{\mathcal{P}}_q(n,k,m)[x,y]) \geqslant \sum_{i=0}^{m-1} \dim_{\mathbb{F}_r}(H_i \cap \{f_i(x) \in \mathbb{F}_{q^n}[x] : \ \deg(f_i) \leqslant k-1\}) \geqslant m(n\ell k - 2\varepsilon\Lambda). \tag{12}$$

By (12), the rate $\widetilde{R}$ of $\widetilde{\mathcal{C}}_q(n,k,m,r)$ is lower bounded by

$$\widetilde{R} = \frac{\log_q |\widetilde{\mathcal{P}}_q(n,k,m)[x,y]|}{(r-1)n^2} \geqslant \frac{k}{r-1} \times \frac{m}{n} - 2\varepsilon \times \frac{m}{n} \geqslant R - 2\varepsilon. \tag{13}$$

Suppose a codeword M_f with $f \in \widetilde{\mathcal{P}}_q(n,k,m)[x,y]$ was transmitted and Y is received with at most e errors, where $e < \frac{s(r-k)(n-m)}{r-1+s(r-k)}$. Then all list belong to the solution space H of (3) which is an $(s-1, \ell n(r-1), m)_r$-periodic subspace. By Lemma 4.1 and Proposition 4.5, the list size for the code $\widetilde{\mathcal{C}}_q(n,k,m,r)$ is $r^{O(s^2/\varepsilon^2)} = \exp(O(s^2/\varepsilon^2)) = \exp(O(1/\varepsilon^2))$.

The decoding radius of $\widetilde{\mathcal{C}}_q(n,k,m,r)$ is equal to those of $\mathcal{C}_q(n,k,m,r)$. By (9), we have

$$\widetilde{\tau} = \tau \approx \frac{c}{c+1}\left(1 - \frac{r-1}{r-c} \times R\right) \geqslant \frac{c}{c+1}\left(1 - \frac{r-1}{r-c} \times \widetilde{R} - \frac{r-1}{r-c} \times 2\varepsilon\right)$$

for $1 \leqslant c \leqslant r-2$. Setting $\widetilde{\varepsilon} = \frac{r-1}{r-c} \times 2\varepsilon$ gives the desired result. □

Remark 5. In the code $\widetilde{\mathcal{C}}_q(n,k,m,r)$, if we set $s \approx 4/\varepsilon^2$, $r \approx 4/\varepsilon^2$ and $k/(r-1) = \varepsilon/2$, then one gets the list decoding radius $\widetilde{\tau} \approx 1 - \widetilde{R} - \widetilde{\varepsilon}$. In this case, the list size is becomes $(1/\widetilde{\varepsilon})^{O(\exp(1/\widetilde{\varepsilon}^4))}$. This proves Corollary 1.3(i).

4.2 A Monte Carlo algorithm

We first define subspace evasive for a particular famyly of affine spaces.

Definition 6. *[17] Let $\mathcal{F}$ be a family of affine subspace of $\mathbb{F}_r^\kappa$ and each of subspace in $\mathcal{F}$ has dimension at most v. A subset $S \subset \mathbb{F}_r^\kappa$ is called $(\mathcal{F}, v, \kappa, L)_r$-evasive if $|S \cap W| \leqslant L$ for every $W \in \mathcal{F}$.*

Now we are able to state our randomized result. The **HSE** map below is actually defined from hierarchical subspace-evasive sets (see [16, 17]).

Proposition 4.7. *Suppose b, Λ, v, α are positive integers and ζ satisfies the conditions $b \geq (\alpha+1)/\zeta$ and $\Lambda > \frac{2s(\alpha+2)}{\zeta}$. Let $\mathcal{F}$ be a family of (v, Λ, b)-periodic subspaces of $\mathbb{F}_r^\kappa$ with $|\mathcal{F}| \leq r^{\alpha\kappa}$, where $\kappa = b\Lambda$. Then there exists a randomized construction of an injective map $\mathbf{HSE}$: $\mathbb{F}_r^{(1-2\zeta)\kappa} \to \mathbb{F}_r^\kappa$ in time $poly(m\Lambda, 1/\zeta, \log r, v)$ such that with probability at least $1-2^{\Omega(b\Lambda)}$, the image of $\mathbf{HSE}$ is an $(\mathcal{F}, bv, \kappa, \frac{\alpha+1}{\zeta})$-subspace evasive set. Further, given a (v, Λ, b)-periodic subspace $H \in \mathcal{F}$, one can compute the set $\{\mathbf{x} \in \mathbb{F}_r^{(1-2\zeta)\kappa} : \mathbf{HSE}(\mathbf{x}) \in H\}$ of size at most $\frac{\alpha+1}{\zeta}$ in deterministic $poly(m\Lambda, r^v, 1/\zeta)$ time.*

Theorem 4.8. [Part (ii) of Main Theorem] *Let r be a prime power and let c be an integer between 1 and $r-1$. Let $\widehat{\varepsilon} > 0$ be a small real. Let $q = r^\ell$ with $\gcd(r-1, \ell n) = 1$. Then with high probability one can randomly sample a rank-metric code in $\mathbb{M}_{n\times(r-1)n}(\mathbb{F}_q)$ with rate $\widehat{R}$ that is $(\widehat{\tau}, O(1/\widehat{\varepsilon}))$-list decodable with $\widehat{\tau} = \frac{c}{c+1}\left(1 - \frac{r-1}{r-c} \times \widehat{R} - \widehat{\varepsilon}\right)$. Furthermore, encoding and list-decoding algorithms are in polynomial time* $\mathrm{poly}(n, \exp(1/\widehat{\varepsilon}))$.

Proof. In Proposition 4.7, set $v = s-1$, $b = m$ and $\Lambda = n\ell k$. Let $\mathcal{F}$ be the set of all $(s-1, n\ell k, m)_r$-periodic subspaces in $\mathbb{F}_r^{mn\ell k}$. A periodic subspace $H \subseteq \mathbb{F}_r^{mn\ell k}$ consists of a fixed subspace $W \subseteq \mathbb{F}_r^\Lambda$ of dimension at most $s-1$ and affine space $\mathrm{proj}_{[(j-1)\Lambda+1, j\Lambda]}(H) = W + \mathbf{v}_j$ with $\mathbf{v}_j \in \mathbb{F}_{q^n}^k$ for $j = 1, 2, \ldots, m$. Thus, there are at most $N_s \times r^{m\Lambda}$ periodic subspaces in $\mathcal{F}$, where N_s denotes the number of subspaces in $\mathbb{F}_r^\Lambda$ of dimension less than or equal to $s-1$. As m tends to ∞ and s is a constant, one clearly has

$$N_s = \sum_{i=0}^{s-1} \begin{bmatrix} \Lambda \\ i \end{bmatrix}_r \leqslant s \begin{bmatrix} \Lambda \\ s-1 \end{bmatrix}_r \leqslant (s-1) r^{(s-1)\Lambda} \leqslant r^{m\Lambda},$$

where $\begin{bmatrix} \Lambda \\ i \end{bmatrix}_r$ denotes the Gaussian binomial coefficients that is equal to the number of subspaces of $\mathbb{F}_r^\Lambda$ of dimension i. Thus, in total we have $|\mathcal{F}| \leqslant r^{2m\Lambda}$.

In Proposition 4.7, we set $\alpha = 2$. Let $\mathbf{HSE}$ be the injective map given in Proposition 4.7: $\mathbb{F}_r^{(1-2\zeta)m\Lambda} \to \mathbb{F}_r^{m\Lambda}$. As $\mathbb{F}_r^{m\Lambda} \simeq \mathcal{P}_q(n, k, m)[x, y]$, we can identify these two spaces under a fixed basis and hence $\mathbf{HSE}(\mathbf{x})$ can be viewed as a polynomial in $\mathcal{P}_q(n, k, m)[x, y]$. Now our encoding becomes

$$\mathbb{F}_r^{(1-2\zeta)m\Lambda} \to \mathbb{F}_r^{m\Lambda} \simeq \mathcal{P}_q(n, k, m)[x, y] \to \mathbb{M}_{n\times(r-1)n}(\mathbb{F}_q); \quad \mathbf{x} \mapsto \mathbf{HSE}(\mathbf{x}) \mapsto M_{\mathbf{HSE}(\mathbf{x})}.$$

Denote by $\widehat{\mathcal{C}}_q(n, k, m, r)$ the image of the above map. Thus the rate of the code $\widehat{\mathcal{C}}_q(n, k, m, r)$ is

$$\widehat{R} = \frac{\log_q r^{(1-2\zeta)m\Lambda}}{n^2(r-1)} = (1-2\zeta) \times \frac{k}{r-1} \times \frac{m}{n} = (1-2\zeta)R \geqslant R - 2\zeta, \tag{14}$$

where R is the rate of $\mathcal{C}_q(n, k, m, r)$.

Suppose a codeword $M_{\mathbf{HSE}(\mathbf{x})}$ was transmitted and Y is received with at most e errors, where $e < \frac{s(r-k)(n-m)}{r-1+s(r-k)}$. By Remark 4, $\mathbf{HSE}(\mathbf{x})$ belongs to an $(s-1, \Lambda, m)_r$-periodic subspace. By Proposition 4.7, we obtain a list of solutions of size $O(1/\zeta)$. Furthermore, by [16] the list can be computed in time $\mathrm{poly}(n, r^{\zeta})$.

The decoding radius of $\widehat{\mathcal{C}}_q(n,k,m,r)$ is the same as the one of $\mathcal{C}_q(n,k,m,r)$. By (9), we have

$$\widehat{\tau} = \tau \approx \frac{c}{c+1}\left(1 - \frac{r-1}{r-c} \times R\right) \geqslant \frac{c}{c+1}\left(1 - \frac{r-1}{r-c} \times \widehat{R} - \frac{r-1}{r-c} \times 2\zeta\right)$$

for $1 \leqslant c \leqslant r-2$. Setting $\widehat{\varepsilon} = \frac{r-1}{r-c} \times 2\zeta$ gives the desired result. □

Remark 6. In the code $\widehat{\mathcal{C}}_q(n,k,m,r)$, if we set $s \approx 4/\varepsilon^2$, $r \approx 4/\varepsilon^2$ and $k/(r-1) = \varepsilon/2$, then one gets the list decoding radius $\widehat{\tau} \approx 1 - \widehat{R} - \widehat{\varepsilon}$. The list size is $O(1/\zeta) = O(1/\widehat{\varepsilon})$. This proves Corollary 1.3(ii).

References

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

[2] Y. Ding, On List-Decodability of Random Rank Metric Codes and Subspace Codes. IEEE Transactions on Information Theory, **61(1)**(2015), 51–59. 1

[3] Z. Dvir and S. Lovett, *Subspace evasive sets,* In *Proceedings of the 44th ACM Symposium on Theory of Computing*, pages 351–358, 2012. 10

[4] T. Etzion and N. Silberstein, *Error-correcting codes in projective spaces via rank-metric codes and ferrers diagrams,* IEEE Transactions on Information Theory, **55(7)**(2009),2909–2919.

[5] C. Faure, *Average number of Gabidulin codewords within a sphere,* In *Int. Workshop on Alg. Combin. Coding Theory (ACCT)*, pages 86–89, 2006.

[6] M. A. Forbes and A. Shpilka, *On identity testing of tensors, low-rank recovery and compressed sensing,* In Proceedings of the 44th ACM Symposium on Theory of Computing, pages 163–172, 2012. 1

[7] E. M. Gabidulin. Theory of codes with maximal rank distance. *Problems of Information Transmission*, **21(7)**(1985), 1-12. 1, 4

[8] E. M. Gabidulin, *A fast matrix decoding algorithm for rank-error-correcting codes,* LNCS **573**, pages 126–133. Springer, 1991.

[9] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov, *Ideals over a non-commutative ring and their applications in cryptology, EUROCRYPT*, LNCS **547**, pages 482–489, 1991. 1

[10] V. Guruswami and S. Kopparty, *Explicit subspace designs,* In *Proceedings of the 54th IEEE Symposium on Foundations of Computer Science*, 2013. 11

[11] V. Guruswami, S. Narayanan, and C. Wang. List decoding subspace codes from insertions and deletions. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, pages 183–189, January 2012.

[12] V. Guruswami and A. Rudra, *Explicit codes achieving list decoding capacity: error correction with optimal redundancy,* IEEE Trans. on Inform. Theory, **54(1)**(2008), 135–150. 2

[13] V. Guruswami and M. Sudan, *Improved Decoding of Reed-Solomon and Algebraic-Geometric codes,* IEEE Trans. on Inform. Theory, **45(3)**(1999), 1757-1767. 1

[14] V. Guruswami and C. Wang. Linear-algebraic list decoding for variants of Reed-Solomon codes. *IEEE Transactions on Information Theory*, 59(6):3257–3268, 2013. 10

[15] V. Guruswami, C. Wang and C. Xing, *Explicit rank-metric and subspace codes list-decodable with optimal redundancy,* http://arxiv.org/abs/1311.7084, 2013. 10, 11

[16] V. Guruswami and C. Xing, *Folded codes from function field towers and improved optimal rate list decoding, Electronic Colloquium on Computational Complexity (ECCC)*, 19:36, 2012. Extended abstract appeared in the *Proceedings of the 44th ACM Symposium on Theory of Computing (STOC'12)*. 0, 3, 8, 13, 14

[17] V. Guruswami and C. Xing, *List decoding Reed-Solomon, Algebraic-Geometric, and Gabidulin subcodes up to the Singleton bound, Electronic Colloquium on Computational Complexity (ECCC)*, 19:146, 2012. Extended abstract appeared in the *Proceedings of the 45th ACM Symposium on Theory of Computing (STOC'13)*. 0, 1, 2, 3, 10, 13

[18] R. Koetter and F. R. Kschischang, *Coding for errors and erasures in random network coding,* IEEE Transactions on Information Theory, **54(8)**(2008), 3579–3591. 1, 4

[19] H. Mahdavifar and A. Vardy, *List-decoding of subspace codes and rank-metric codes up to Singleton bound, CoRR*, abs/1202.0866, 2012. 1, 2, 4

[20] N. Raviv and A. Wachter-Zeh, *Some Gabidulin Codes cannot be List Decoded Efficiently at any Radius,* http://arxiv.org/abs/1501.04272, 2015. 1, 3

[21] J. Sheekey, *A new family of linear maximum rank distance codes,* http://arxiv.org/pdf/1504.01581.pdf, 2015. 4

[22] A. Wachter-Zeh, *Bounds on List Decoding of Rank-Metric Codes,* IEEE Transactions on Information Theory, **59(11)**(2013), 7268–7277. 1

[23] H. Wang and C. Xing and R. Safavi-Naini, *Linear authentication codes: Bounds and constructions,* IEEE Transactions on Information Theory, **49(4)**(2003), 866–872. 1

ECCC ISSN 1433-8092

http://eccc.hpi-web.de